EUROPEAN COMMISSION

Brussels, 10.2.2026
C(2026) 960 final

PUBLIC VERSION

In the published version of this decision, some information has been omitted pursuant to Article 17(2) of Council Regulation (EC) No 139/2004 concerning non-disclosure of business secrets and other confidential information. The omissions are shown thus […]. Where possible the information omitted has been replaced by ranges of figures or a general description.

Google LLC
Amphitheatre Parkway 1600
Mountain View
CA 94043
United states of America

Subject: **Case M.11964 – GOOGLE / WIZ**
Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004 ([1]) and Article 57 of the Agreement on the European Economic Area ([2])

Dear Sir or Madam,

(1) On 6 January 2026, the European Commission received notification of a proposed concentration pursuant to Article 4 of the Merger Regulation by which Google LLC (together with its affiliates, '**Google**' or '**Notifying Party**', USA) intends to acquire sole control of Wiz, Inc. ('**Wiz**' or '**Target**', USA), within the meaning of Article 3(1)(b) of the Merger Regulation (the '**Transaction**'). ([3]) Google and Wiz are designated hereinafter as the '**Parties**'.

([1]) OJ L 24, 29.1.2004, p. 1 (the '**Merger Regulation'**). With effect from 1 December 2009, the Treaty on the Functioning of the European Union ('**TFEU**') has introduced certain changes, such as the replacement of 'Community' by 'Union' and 'common market' by 'internal market'. The terminology of the TFEU will be used throughout this decision.
([2]) OJ L 1, 3.1.1994, p. 3 (the '**EEA Agreement**').
([3]) OJ C, C/2026/261, 14.01.2026.

1. THE PARTIES

(2) **Google** is a Delaware limited liability company, headquartered in Mountain View, California. It is a wholly owned subsidiary of Alphabet Inc. ('**Alphabet**'), a Delaware corporation. Google comprises two divisions: Google Services and Google Cloud. Only the latter is relevant for the Transaction. Google Cloud offers **Google Cloud Platform ('GCP')**, which is a public cloud infrastructure (also referred to as a cloud service provider ('**CSP**')). GCP owns, manages, and operates infrastructure (a set of physical assets, such as servers, storage, and networking devices) and virtual resources, such as virtual machines, and software that are contained and run in datacentres around the world. Through these assets and resources, GCP provides customers a set of cloud services including computing, data storage, data analytics, and machine learning on an Infrastructure-as-a-Service ('**IaaS**') and Platform-as-a-Service ('**PaaS**') basis. ([4]) It allows developers to build, deploy, and scale cloud applications, websites, and services. In 2024, GCP accounted for approximately [information on the Parties' revenues]% of Google's total revenues. ([5])

(3) Google also offers some cloud security products and services. Its activities focus primarily on reactive security ([6]), where Google is active with its SecOps, Threat Intelligence, and Mandiant Managed Defence, Response & Consulting ('**Mandiant**') products and services, securing workloads deployed on GCP, other CSPs, and in private datacentres on-premises. Google also has some limited activities in proactive security ([7]) with its Security Command Center ('**SCC**'), which offers a foundational layer of proactive security on GCP workloads, and Security Command Center Enterprise ('**SCCE**') products, which also focuses on GCP workloads but, unlike SCC, includes, among other things, some limited support for other public CSPs, which renders it a cloud-native application protection platform ('**CNAPP**'). In 2024, Google's security products accounted for [information on the Parties' revenues]% of GCP's revenues and [information on the Parties' revenues]% of Google's total revenues. ([8])

(4) **Wiz** is a Delaware corporation, headquartered in New York. Founded in 2020, Wiz helps organizations secure workloads across multi-cloud ([9]) and on-premises environments. Wiz offers a CNAPP, which comprises Wiz's Cloud, Defend and

---

([4]) Infrastructure-as-a-Service or IaaS is a cloud computing model that provides on-demand access to infrastructure resources (such as compute power, storage, networking and virtualisation) over the internet, whereby cloud providers manage the underlying physical hardware and virtualisation layer and customers are responsible for managing the operating systems, virtual machines, applications and associated data. Platform-as-a-Service or PaaS is a cloud computing model that provides a fully managed environment for developing, running, and managing applications.

([5]) Form CO, paragraphs 4-6.

([6]) Reactive security products and services address attacks after they have taken place.

([7]) Proactive security products and services are primarily dedicated to identifying and addressing potential weaknesses before they can be exploited.

([8]) Form CO, paragraph 7.

([9]) 'Multi-cloud' refers to a way of organizing workloads by allocating them to different cloud infrastructures, including public clouds, as opposed to centralizing them with a single cloud infrastructure provider. Wiz secures workloads on Azure, AWS, GCP, Alibaba Cloud, Linode Cloud, and Oracle Cloud Infrastructure, as well as VMware's vSphere virtualization platform. Wiz products can also protect on-premises deployments and therefore address hybrid cloud needs. Additionally, Wiz is currently considering an integration with [information on the Parties' commercial strategy] due to its strong presence and customer use [information on the Parties' commercial strategy]. Likewise, Wiz identified sufficient customer demand to integrate with [information on the Parties' commercial strategy and product roadmaps] (Response to RFI 17, page 25).

Sensor software, and Wiz's Code software – all of which offer primarily proactive security features for multi-cloud environments. In 2024, Wiz achieved total worldwide revenues of [information on the Parties' revenues], of which only [information on the Parties' revenues] were generated in the EEA. ([10])

(5) The core of Wiz's CNAPP platform is Wiz Cloud, which, like all CNAPPs provides an overlay of security across all relevant cloud layers ([11]) and across different CSPs. [information on the Parties' customers' workloads]% of the workloads secured by Wiz are deployed on cloud infrastructure offered by Amazon (AWS) and Microsoft (Azure). Wiz Cloud generated global revenues of USD [information on the Parties' revenues] million in 2024, accounting for [information on the Parties' revenues]% of Wiz's overall revenues.

(6) Wiz Cloud can be combined with Wiz Defend and Wiz Sensor, which provide real-time threat monitoring. In 2024, Wiz Defend and Wiz Sensor generated global revenues of USD [information on the Parties' revenues] and USD [information on the Parties' revenues], accounting for [information on the Parties' revenues]% and [information on the Parties' revenues]% of Wiz's overall revenues respectively. Wiz Cloud can also be combined with Wiz Code, which helps developers to identify potential security threats in code before it is deployed and provides developers with cloud context. In 2024, Wiz Code generated global revenues of USD [information on the Parties' revenues], accounting for [information on the Parties' revenues]% of Wiz's overall revenues. ([12])

2. THE OPERATION AND CONCENTRATION

(7) The Transaction consists in the acquisition of sole control by Google of Wiz. Under an Agreement and Plan of Merger signed on 18 March 2025, Google will acquire control of Wiz via the purchase of all of its issued share capital for approximately EUR 29.6 billion (USD 32 billion) in cash. The closing of the Transaction is subject to the satisfaction of customary closing conditions including obtaining merger control clearance and foreign direct investment approvals.

(8) Therefore, the Transaction constitutes a concentration within the meaning of Article 3(1)(b) of the Merger Regulation.

3. UNION DIMENSION

(9) The Transaction does not have an EU dimension within the meaning of Article 1(2) of the Merger Regulation, because the aggregate EU-wide turnover of the Target does not exceed EUR 250 million. Nor does the Transaction have a Union dimension according to Article 1(3) of the Merger Regulation since, first,

([10]) Form CO, paragraphs 8-9.

([11]) These layers are not vertical components that can be peeled apart; rather they represent different aspects of operating a cloud computing instance. The relevant cloud layers covered by CNAPPs include: (i) the configuration layer, which covers the settings that define how cloud services are accessed and used, (ii) the network layer, which covers the network infrastructure that enables communication, resource access, and data transmission amongst cloud components, (iii) the data layer, which covers the information stored or transferred in the cloud, such as files, databases, and backups, and (iv) the identity layer, which defines how access is granted and managed within the cloud. By contrast, code and runtime are orthogonal to the cloud layers - they are 'environments' that run through each of the different layers.

([12]) Form CO, paragraph 10.

the turnover of the Target does not exceed EUR 25 million in each of at least three Member States where the combined aggregate turnover of all undertakings concerned exceeds EUR 100 million and, second, the aggregate EU-wide turnover of the Target does not exceed EUR 100 million.

(10) On 4 July 2025, the Commission received a referral request from the Notifying Party by means of a reasoned submission, pursuant to Article 4(5) of the Merger Regulation, according to which the Transaction was capable of being reviewed under the national competition laws of at least three Member States, namely the mandatory regime of Cyprus as well as the voluntary and call-in regimes of Ireland and Sweden. ([13]) The Commission transmitted this submission to all Member States on 4 July 2025. None of the Member States competent to examine the Transaction expressed their disagreement to the request for referral within 15 working days of receiving the reasoned submission.

(11) As a result, the Transaction was referred to the Commission pursuant to Article 4(5) of the Merger Regulation and is deemed to have an EU dimension.

4. RELEVANT MARKETS

4.1. Introduction

(12) Google and Wiz are both active in IT software for enterprise customers. The Parties' software activities overlap in several plausible markets or market segments. Further, some of Google's software may be complementary to Wiz's software. Google is also active as a cloud service provider and a developer and supplier of generative AI models.

(13) When providing its views on the relevant product and geographic markets, the Notifying Party relied on previous Commission decisions when possible. The Notifying Party also relied on the segmentation proposed by market intelligence companies such as International Data Corporation ('**IDC**') and/or Gartner, Inc. ('**Gartner**').

(14) As set out in further detail in Section 4.2, the Commission has drawn inspiration from IDC and/or Gartner segmentations in past decisions.

(15) As will be explained in Section 5.4, the Transaction gives rise to one horizontally affected market: the potential worldwide or EEA-wide market for cloud security posture management ('**CSPM**') (Gartner terminology).This Decision will also assess the competitive dynamics in the potential CNAPP market (IDC terminology), even though it is not a horizontally affected market based on the available market shares.

(16) This Decision will further assess two vertical relationships between the upstream market for cloud infrastructure and data analytics and the downstream market for CNAPP.

(17) Lastly, this Decision will assess a number of conglomerate relationships between the activities of Google (on the market for cloud infrastructure and data analytics and on a potential market for specialised generative AI) and Wiz (on the potential market for CNAPP).

([13]) In addition, the Transaction may have been subject to the deal value-based threshold in Germany, which could, however, been left open.

4.2. Security software

4.2.1. Introduction

4.2.1.1. IDC terminology

(18) IDC categorizes the software industry into four levels: (i) primary markets; (iii) secondary markets; (iii) functional markets; and (iv) sub-markets.

(19) IDC identifies the primary markets for (i) Applications; (ii) Application Development & Deployment; and (iii) System Infrastructure Software.

(20) IDC sub-segments the primary market for System Infrastructure Software into the secondary markets for (i) system and service management software; (ii) network, (iii) security, (iv) storage, (v) endpoint management, and (vi) physical and virtual computing.

(21) IDC further sub-segments the secondary market for security software into seven functional markets: (i) **CNAPP**, (ii) identity and access management, (iii) endpoint security, (iv) network security, (v) security analytics, (vi) information and data security and (vii) governance, risk and compliance. ([14])

(22) IDC describes CNAPP as 'security solutions that provide hybrid cloud and multicloud visibility from a single pane of glass'. ([15]) Under IDCs definition, CNAPP tools must provide CSPM and any three of the following components: cloud workload protection platform ('**CWPP**'), cloud infrastructure entitlement management ('**CIEM**'), Kubernetes Security Posture Management ('**KSPM**'), Infrastructure-as-Code ('**IaC**'), Software Composition Analysis, AI Security Posture Management, Cloud Detection and Response, Data Security Posture Management, application programming interface ('**API**') security and vulnerability management. ([16])

4.2.1.2. Gartner terminology

(23) Gartner categorizes the software industry into three levels: (i) macro markets, (ii) sub-segments, and for some sub-segments, (iii) categories.

(24) Gartner identifies the macro markets for: (i) IT operations management software; (ii) security software; and (iii) application infrastructure and middleware.

(25) Gartner breaks down its Security Software market into 22 subsegments:

- Within **infrastructure protection**:(i) endpoint protection platforms, (ii) secure email gateway, (iii) security information and event management, (iv) secure web gateway and (v) threat intelligence;
- Within **cloud security**: (vi) cloud access security brokers, (vii) CWPP ([17]), **(viii) CSPM;**

([14]) IDC Worldwide Software Taxonomy (2025), Annex III.A.8 to the Form CO. IDC does not provide any further sub-segmentations of this market.

([15]) IDC Worldwide Software Taxonomy (2025), Annex III.A.8 to the Form CO, page 108.

([16]) IDC MarketScape: Worldwide Cloud-Native Application Protection Platform 2025 Vendor Assessment, Annex II.A.6 to the Form CO.

([17]) According to Gartner, CWPPs provide visibility and control for physical machines, virtual machines (VMs), containers and serverless workloads in hybrid, multi-cloud environments. CWPP offerings protect the workload using a combination of system integrity protection, application control, behavioural monitoring, intrusion prevention and optional anti-malware protection. The

- Within **application security**: (ix) application security testing, (x) vulnerability assessment, (xi) web application firewalls;
- Within **identity access management**: (xii) identity governance and administration, (xiii) access management, (xiv) privileged access management, (xv) user authentication;
- Within **data security and privacy**: (xvi) enterprise data loss prevention, (xvii) encryption, (xviii) tokenization, (xix) consent and preference management platforms, (xx) subject rights request automation, (xxi) consumer security software,
- Finally, (xxii) other security software. ([18])

(26) Gartner defines CSPM as 'offerings continuously manage IaaS and PaaS security postures by preventing, detecting and responding to cloud infrastructure risks. The core of CSPM offerings is applying common compliance frameworks, regulatory requirements and enterprise policies to proactively and reactively discover and assess the risk and trust of cloud services' configuration and security settings. If an issue is identified, remediation options (automated or human-driven) are provided'. ([19])

(27) Gartner does not include CNAPP as a subsegment of security software, thus, does not provide market shares on this market. ([20]) Nevertheless, it has provided a definition of CNAPPs as security software offerings with a 'unified and tightly integrated set of security and compliance capabilities, designed to protect cloud-native infrastructure and applications.' ([21])

(28) Under Gartner's taxonomy CNAPPs must 'at a minimum [integrate with] Amazon Web Services, Microsoft Azure, and Google Cloud Platform and Kubernetes' and commonly include 'options for integration with lesser-common cloud and Kubernetes platforms.' In addition to multi-cloud capabilities, Gartner indicates that CNAPPs optionally provide 'support for on-premises deployments.' ([22]) Lastly, unlike IDC, Gartner considers that CNAPPs must provide as core capabilities CSPM, CWPP, KSPM, IaC, CIEM container and container risk scanning. ([23])

4.2.1.3. Comparison between Gartner and IDC terminologies

(29) Gartner and IDC have minor differences in their understanding of what a CNAPP entails, **Table 1** compares Gartner and IDC definitions of CNAPP:

Transaction does not give rise to an affected market on CWPP, and thus, it will not be further discussed.

([18]) Gartner, Market Definitions and Methodology: Software, 3 July 2025, Annex RFI 11, Q.1.2 to the Form CO, pages 65-71.

([19]) Gartner, Market Definitions and Methodology: Software, 3 July 2025, Annex RFI 11, Q.1.2 to the Form CO, page 67.

([20]) The market shares provided in this decision are based on a [third-party report prepared for the Parties] by the Parties.

([21]) Gartner, Market Guide for Cloud-Native Application Protection Platforms, 22 July 2024, Annex I.A.4 to the Form CO, page 2-3.

([22]) Gartner, Market Guide for Cloud-Native Application Protection Platforms, 22 July 2024, Annex I.A.4 to the Form CO, page 3.

([23]) Gartner, Market Guide for Cloud-Native Application Protection Platforms, 22 July 2024, Annex I.A.4 to the Form CO, pages 18-19.

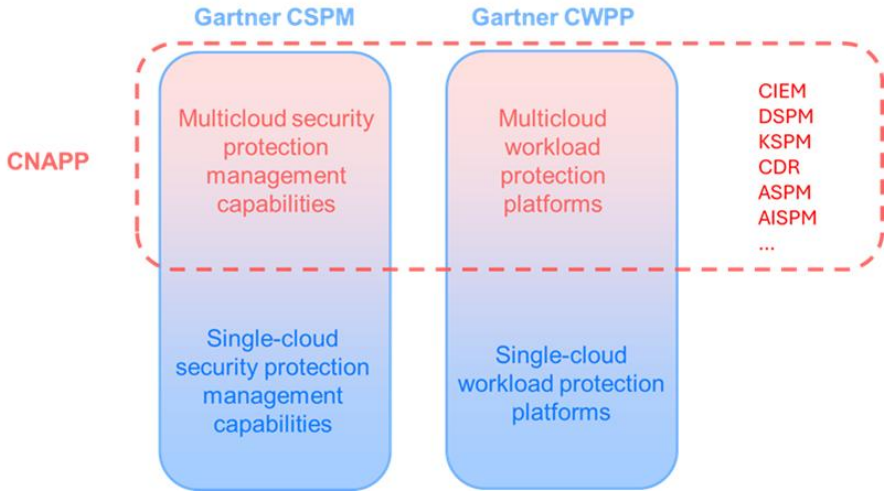
Table 1: Comparison on definition on CNAPP between Gartner and IDC

	Gartner	IDC
Multi-cloud ([24])	Yes	Yes
Hybrid cloud	Optional	Yes
Core capabilities	CSPM, CWPP, KSPM, IaC, CIEM, container and container risk scanning.	CSPM (mandatory) and any three of the following components: CWPP, CIEM, KSPM, IaC, SCA, AI-SPM, CDR, DSPM, API security, and vulnerability management.

Source: Form CO, page 98.

(30) Lastly, IDC and Gartner definitions of CNAPP interact in the following way with Gartner's CSPM and CWPP subsegments:

Figure 1: Comparison between CNAPP and CSPM subsegments



Source: Form CO, page 100.

4.2.2. Product market definition

4.2.2.1. Commission's precedents

(31) The Commission has in the past considered a classification of software products on the basis of functionality, the end-user (**enterprise software** vs. consumer software) and the specific sector ([25]) in which the software is used (e.g., healthcare software). ([26])

(32) In relation to functionality, the Commission considered a division of software products into: (i) **infrastructure software**; (ii) middleware (i.e., integration

([24]) Multi-cloud functionalities are security software offerings that can work on different clouds, in contrast with single-cloud functionalities, which only operate within a single cloud.

([25]) The segmentation by sector in which the software is used is not relevant in the context of the Transaction. Both Parties supply their enterprise software to a wide range of sectors and do not focus on sector-specific software solutions. Therefore, the Commission will not discuss further a potential segmentation by sector for the purpose of the present decision.

([26]) Commission decision of 20 June 2011 in case M.6237 – Computer Sciences Corporation/iSoft Group, paragraphs 22-25 and Commission decision of 8 March 2017 in case M.8223 – Micro Focus/HPE Software Business, paragraph 17.

platforms); (iii) application software and office software; and (iv) operating/browser software. ([27])

(33) Within infrastructure software, the Commission has considered the following additional sub-segmentation: (i) **security software**; (ii) IT operations management ("ITOM") software; (iii) application development software; and (iv) storage management software. ([28])

(34) In prior decisions, the Commission has used the most granular segmentations as presented by Gartner at the time but ultimately left open the exact product market definition.

(35) In Cisco / Splunk, the Commission considered Gartner's segmentation of the market for Security software into 12 subsegments, including application security testing, SIEM, enterprise data loss prevention, and access management. The Commission's market investigation did not suggest any alternative product market definition. Ultimately, the Commission left the exact market definition for security software open. ([29])

(36) In HPE / Juniper, the Commission refers to its precedent in Broadcom / Symantec, where it considered the further segmentation of Enterprise Security Software into 9 subsegments, which included application security testing (dynamic and static). Ultimately, the Commission left the exact product market definition of enterprise network security solutions open. ([30])

(37) In Broadcom/Symantec Enterprise Security Business, the Commission relied on Gartner's segmentation of the time, which / delineated the overall security software segment into 9 sub-segments: (i) application security testing (dynamic and static); (ii) data loss prevention; (iii) enterprise endpoint protection; (iv) identity governance and administration; (v) secure e-mail gateways; (vi) secure web gateways; (vii) security information and event management; (viii) (web) access management; and (ix) other security software. ([31]) Ultimately, the Commission left the exact market definition for security software open

(38) The Commission has not previously defined a market for CNAPP or for CSPM.

4.2.2.2. The Notifying Party's views

(39) The Notifying Party submits that the relevant market for assessing the horizontal relationship between the Parties is a market for CNAPP, as defined by IDC. In this regard, the Notifying Party submits that the market is evolving towards convergence in CNAPP, thus, individual capabilities segmentation, such as CSPM are not warranted. ([32])

([27]) Commission decision of 20 June 2011 in case M.6237 – Computer Sciences Corporation/iSoft Group, paragraph 23; Commission decision of 15 December 2014 in case M.7458 – IBM/INF Business of Deutsche Lufthansa, paragraph 35; and Commission decision of 8 March 2017 in case M.8223 – Micro Focus/HPE Software Business, paragraph 18.

([28]) Commission decision of 8 March 2017 in case M.8223 – Micro Focus/HPE Software Business, paragraph 19, Commission decision of 30 October 2019 in case M.9538 – Broadcom/Symantec Enterprise Security Business, paragraph 16.

([29]) Commission decision of 13 March 2024 in case M.11320 – Cisco/Splunk, paras. 17, 28, 78-79, 80-81, 85, and 133-150.

([30]) Commission decision of 16 December 2024, in case M.11457 – HPE /Juniper, paras. 69 to 77.

([31]) Commission decision of 30 October 2019 in case M.9538 – Broadcom/Symantec Enterprise Security Business, paragraphs 15, 16 and 18.

([32]) Form CO, paragraphs 164 – 170.

(40) According to the Notifying Party, from a demand-side perspective, customers increasingly demand integrated solutions that address all of their proactive cloud security needs. From a supply perspective, many standalone proactive cloud security software providers expanded or combined their capabilities to offer a full CNAPP that covers all functionalities.

(41) The Notifying Party adopts IDC's definition of CNAPPs which covers both multi-cloud and hybrid cloud applications. The Notifying Party's approach is more conservative than Gartner's definition, which identifies hybrid cloud capabilities as an 'optional' but not 'core' criterion for inclusion in the list of CNAPP providers.

(42) In any event, the Notifying Party submits that the precise product market definition can be left open, as the Transaction does not give rise to any competition concerns under any plausible market definition.

4.2.2.3. The Commission's assessment

(43) In the present case, the Commission tested in the market investigation whether the security software market must be segmented into CNAPP (under IDC segmentations) or CSPM (under Gartner segmentations).

4.2.2.3.1. The potential CNAPP product market

(44) Wiz is active in the CNAPP market with Wiz Cloud. ([33]) Google is also active in the CNAPP market with its SCCE tool.

(45) According to IDC, CNAPPs are a unified and tightly integrated set of security and compliance capabilities, designed to protect cloud-native infrastructure and applications. Bringing together several functionalities that were previously sold separately (e.g., CSPM and CWPP), CNAPPs provide a unified, continuous 'single pane of glass' through which customers can manage all relevant security capabilities, configurations and risks across different cloud environments within the same platform.

(46) In the market investigation, the Commission tested whether a segmentation of the security software market into CNAPP and other functionalities is warranted. The majority of respondents to the market investigation confirmed that CNAPP is a distinct market within a broader security software market. ([34])

(47) Having regard the minor discrepancies between IDC and Gartner on the functionalities of a CNAPP, the market investigation has focused on what are the components that a CNAPP must encompass.

(48) The majority of respondents (customers, cloud infrastructure or CSP competitors and CNAPP competitors) identified the provision of CSPM, CWPP, CIEM as core functionalities to be offered by a CNAPP tool. ([35]) Customers and CNAPP competitors also considered that vulnerability management is a core functionality

([33]) Wiz Cloud can be combined with Wiz Defend, Wiz Sensor and Wiz Code for additional capabilities.

([34]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, D.A.A.1.

([35]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.A.4; Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) question D.A.A.6.

for a CNAPP tool. ([36]) Lastly, the majority of CNAPP competitors also considered IaC and KSPM as core CNAPP functionalities. ([37])

(49) The majority of respondents to the market investigation confirmed that both multi-cloud and single-cloud customers purchase CNAPP tools. ([38])

(50) The majority of respondents (customers and CNAPP competitors) also confirmed that CNAPP tools provide both reactive and proactive security solutions. ([39]) Customers explain that "From a proactive perspective, they focus on risk prevention through capabilities such as CSPM, IaC security, CIEM, and KSPM. From a reactive perspective, they include runtime protection and detection capabilities, such as CWPP and CDR, to identify and respond to active exploitation or anomalous behavior in cloud environments." ([40]) Some CNAPP competitors explain that "CNAPP solutions are not purely proactive; they also include reactive capabilities. While their core focus is proactive risk reduction such as posture management, workload hardening, and identity governance, most CNAPP platforms incorporate Cloud Detection and Response (CDR) for runtime threat detection and incident response." ([41])

4.2.2.3.2. The potential CSPM product market

(51) The market investigation also tested whether a standalone CSPM market should be defined within the security software market, separately from a CNAPP market. In this regard, the market investigation yielded mixed results. Whereas most of the respondents that expressed a view consider that CNAPP tools are alternatives to standalone CSPM offerings, many respondents note that in some cases CNAPP tools cannot be considered as alternative to standalone CSPM offerings. ([42])

(52) One customer states that "Whether a CNAPP tool can replace a stand-alone CSPM tool will depend on detailed functionality, that in many cases will be customer specific, at least for customers with complex networks and multi-cloud environments.". Other customer notes that "In some cases, particularly for less complex or single-cloud environments, CNAPP tools may act as an alternative to standalone CSPM solutions. However, for large and complex organisations with multi-cloud environments and specific regulatory requirements, standalone CSPM tools may still be used alongside CNAPP platforms to address depth, scale or compliance-related needs. In such cases, in our view, CNAPP may not fully substitute standalone CSPM." ([43]) One CNAPP competitor notes that "It depends

([36]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question D.A.A.4; Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) question D.A.A.6.

([37]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) question D.A.A.6.

([38]) Replies to Questionnaire 1 – Phase I market investigation – Competitors (CSP), question D.A.A.6; Questionnaire 3 - Phase I market investigation – Customers, question D.A.A.10; Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) question D.A.A.12.

([39]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question D.A.A.8; Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) question D.A.A.10.

([40]) Reply to Questionnaire 3 - Phase I market investigation – Customers, question D.A.A.8.1.

([41]) Reply to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) question D.A.A.10.1.

([42]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.A.2.

([43]) Replies to Questionnaire 3 - Phase I market investigation – Customers, D.A.A.2.1.

on how the customer's security architecture is set up and how important it is for them to have an integrated solution." ([44])

(53) With regard to future trends, the majority of customers consider that CNAPP technology is rendering standalone CSPM offerings less relevant. However, 35% of customers that expressed a view note that in some cases standalone CSPM offerings continue to be relevant. ([45]) For example, one customer states that "a standalone CSPM may be the right product or tool to purchase or build depending on the capabilities needed. CSPM capability is likely to serve needs related to inventory, ownership, and configuration information. Firms often start with CSPMs and evolve toward other capabilities available in CNAPP suites. Some CSPM products have free-to-use tiers that are likely to be used when budget is a constraint." ([46])

(54) On the other hand, most cloud infrastructure competitors and the majority of CNAPP competitors state that, regarding future trends, in some cases CSPM standalone offerings will continue to be relevant. ([47]) For example, one CNAPP competitor notes that "CNAPP includes CSPM, so it will sometimes replace existing CSPM offerings. At the same time, not all the buyers require the full functionality of a CNAPP suite, so adoption of vertical tools is not going to disappear", other CNAPP competitor notes that "Generally speaking, customers are increasingly looking for an integrated CNAPP as a complete cloud security solution. However, many customers value a standalone CSPM that can integrate with native CWPP capabilities." ([48])

(55) On the supply side, the majority of CNAPP competitors confirm that a CSPM-only vendor could not easily develop and commercialise a CNAPP solution in a short period of time, as it is technically complex and entails significant financial investment. ([49])

4.2.2.3.3. Conclusion

(56) For the purposes of this decision, the Commission considers that the relevant market is the provision of security software services ([50]) and cannot exclude that the market may have to be further segmented into CNAPP or CSPM. Nevertheless, the exact product market definition can be left open, as the Transaction does not give rise to competition concerns under any potential further segmentation.

([44]) Reply Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), D.A.A.2.1.

([45]) Replies to Questionnaire 3 - Phase I market investigation – Customers, D.A.A.3.

([46]) Reply Questionnaire 3 - Phase I market investigation – Customers, D.A.A.3.1.

([47]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question D.A.A.2 and D.A.A.3.

([48]) Reply Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), D.A.A.3.1.

([49]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question D.A.A.4.

([50]) For the purposes of this Decision, it is not necessary to conclude on a precise definition of a potential market for "other security software". Even under the narrowest plausible market definition, Google's market share would remain below 5%. This Decision nevertheless assesses in Section 5.6.3.2 whether the Transaction would have an effect on any of the other markets for security software other than CSPM/CNAPP as a result of a potential bundling strategy with Wiz's CNAPP.

4.2.3. Geographic market definition

4.2.3.1. Commission's precedents

(57) In Intel/McAfee, the Commission considered that the market for endpoint security was worldwide or at least EEA-wide, noting that larger organisations tend to prefer global sourcing of security software products. ([51])

(58) In Symantec/Veritas, the Commission left the geographic scope of the security software market open but noted that vendors typically supply their software products globally and that larger organizations tended to source software products globally. ([52])

(59) In Cisco/Splunk, the market investigation pointed towards a worldwide market because procurement in security software primarily takes place on a worldwide level, but the Commission ultimately left the geographic market definition open. ([53])

(60) In Broadcom/Symantec Enterprise Security Business, the Commission considered security software as part of the broader market for infrastructure software and ultimately left open whether the market is global or at least EEA-wide. ([54])

4.2.3.2. The Notifying Party's views

(61) With respect to the geographic scope of the security software market and any potential CNAPP or CSPM segmentations, the Parties consider the scope to be global or, at least, EEA-wide. ([55])

(62) This is because cloud-native security solutions are global in design and distribution. Enterprise customer demand is global in nature, and the same competitive conditions apply across jurisdictions.

(63) In any event, the Notifying Party submits that the precise geographic market definition can be left open, as the Transaction does not raise competition concerns under any plausible geographic market definition.

4.2.3.3. The Commission's assessment

(64) In the market investigation, the majority of respondents expressing an opinion considered that competition in the potential CNAPP market takes place at a worldwide level. ([56])

(65) For the purposes of this Decision, the Commission considers that the exact geographic market definition with regard to the supply of security software and any potential segmentations can be left open, as the Transaction does not give rise to any competition concerns regardless of whether a worldwide or EEA-wide market is considered.

([51]) Commission decision of 26 January 2011 in case M.5984 – Intel/McAfee, paragraph 55.
([52]) Commission decision of 15 March 2005 in case M.3697 – Symantec/Veritas, paragraphs 18-21.
([53]) Commission decision of 13 March 2024 in case M.11320 – Cisco/Splunk, paragraph 85.
([54]) Commission decision of 30 October 2019 in case M.9538 – Broadcom/Symantec Enterprise Security Business, paragraph 28.
([55]) Form CO, paragraphs 171-173.
([56]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.B.A.1.

4.3. Cloud infrastructure and data analytics

(66) Google is active in the market for cloud infrastructure and data analytics with its cloud platform, GCP. Wiz is not active in that market.

4.3.1. Product market definition

4.3.1.1. Commission's precedents

(67) In previous decisions, the Commission identified the market for the provision of cloud infrastructure and data analytics as a separate product market. ([57])

(68) In Microsoft/Nuance, the Commission initially considered segmenting the market further based on the service model (IaaS and PaaS) before ultimately concluding that such segmentation was not warranted. ([58]) Nevertheless, in recent cases considering cloud services, the Commission has also considered potential segmentations of the IT services market between (i) IaaS, PaaS and Software as a Service ("**SaaS**"), (ii) deployment type (public, hybrid and private cloud services); (iii) ANSSI-certified sovereign cloud services and non-ANSSI-certified cloud services; (iv) infrastructure implementation services and managed services; and (v) application implementation and managed services, but ultimately left open the exact market definition. ([59])

4.3.1.2. The Notifying Party's views

(69) The Notifying Party considers that the relevant market is the overall market for the provision of cloud infrastructure and data analytics.

(70) The Notifying Party does not consider it appropriate to further segment the relevant market, including by (i) service models (IaaS or PaaS) or (ii) deployment type (public, hybrid and private cloud services). ([60])

(71) The Notifying Party also submits that a potential segmentation by customer type, size or activity sector is not warranted because, on the demand-side, different customer types (regardless of size, type or activity) ultimately need the same cloud services. From the supply-side, cloud providers generally allow customers to flexibly scale their workloads, as well as the control they have over them. ([61]) In particular, the Notifying Party does not consider a separate market for AI workloads, as enterprise AI workloads are often integrated into existing relationships with cloud infrastructure providers and all major cloud infrastructure providers support a variety of workloads – including notably AI workloads. ([62])

(72) In any case, the Notifying Party submits that for the purposes of this decision, the exact product market definition for the cloud infrastructure and data analytics market, including any potential further segmentations thereof, can be left open, as

---

([57]) Commission decision of 21 December 2021 in case M.10290 – Microsoft/Nuance, paragraph 52. See also Google/Fitbit where the Commission identified cloud computing services as a separate product market, defining it as the provision of cloud infrastructure and data analytics. Commission decision of 17 December 2020 in case M.9660 – Google/Fitbit, paragraphs 266 and 272-274.

([58]) Commission decision of 21 December 2021 in case M.10290 – Microsoft/Nuance, paragraph 56.

([59]) Commission decision of 12 June 2023 in case M.10855 – Capgemini/Orange, paragraphs 32 to 39. A similar approach was followed in Microsoft/GitHub-, where the Commission considered the markets for IaaS and PaaS but ultimately left the exact product market definition open. Commission decision of 19 October 2018 in case M.8994 – Microsoft/GitHub, paragraph 61.

([60]) Annex II.C.1 to the Form CO, page 3.

([61]) Annex II.C.1 to the Form CO, page 3.

([62]) Parties' response to RFI 19, Question 1.

the Transaction does not give rise to competition concerns regardless of the exact product market definition.

4.3.1.3. The Commission's assessment

(73) The majority of respondents to the market investigation consider that, for the purposes of this decision, the relevant market should be cloud infrastructure and data analytics, without segmenting the market further based on service model (IaaS or PaaS) or deployment type. ([63])

(74) The market investigation also tested a potential segmentation of the cloud infrastructure and data analytics market by customer type, size or activity sector.

(75) First, the majority of customers and competitors who expressed a view considered that even if some differences exist between cloud-native and hybrid cloud customers, they do not warrant a further segmentation of this market based on these differences. ([64])

(76) One customer notes that "Cloud-native customers prioritize elasticity, container orchestration, and DevOps integration, while hybrid cloud customers focus on interoperability with on-premises systems and legacy workloads. These differences shape architecture choices but do not create separate markets, as providers offer flexible solutions for both. Customer needs vary widely by industry, compliance, and performance requirements, making segmentation based solely on deployment models overly simplistic compared to broader structural and technological factors." ([65]) Other customer notes that "requirements differ but still are met by the same providers just offering different technical features/services to meet the requirements." ([66])

(77) Second, as regards a potential segmentation of the market between AI workloads and general-purpose cloud infrastructure, the market investigation yielded mixed results. Most customers and competitors that expressed a view state that cloud infrastructure used primarily for AI workloads does not differ sufficiently from general-purpose cloud infrastructure to justify a separate market, except for certain AI workloads like large-scale training or specialized Graphics Processing Units. ([67])

(78) For the purposes of this decision, the Commission considers that the exact product market definition for the cloud infrastructure and data analytics market can be left open, as the Transaction does not give rise to competition concerns under any potential further segmentation.

([63]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.B.1.

([64]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.B.3.

([65]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.B.3.

([66]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.B.3.

([67]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.B.2

4.3.2. Geographic market definition

4.3.2.1. Commission's precedents

(79) In Google/Fitbit, the Commission considered that the market for cloud infrastructure and data analytics was at least EEA-wide and perhaps worldwide in scope but ultimately left the geographical market definition open. ([68])

(80) Similarly, in Microsoft/GitHub and Capgemini/Orange/JV, the Commission considered that the markets for IaaS and PaaS and IT services and IT software, respectively, were at least EEA-wide and perhaps worldwide, but ultimately left the geographical market definition open. ([69])

(81) In Microsoft/Nuance, the Commission defined the market for cloud infrastructure and data analytics services as global in scope. ([70])

4.3.2.2. The Notifying Party's views

(82) The Notifying Party relies on previous Commission decisions and considers that the relevant geographic market is worldwide as suppliers are active globally, demand is global in nature and there are no physical restrictions based on geography. ([71])

(83) In any event, the Notifying Party submits that the precise market definition can be left open, as the Transaction does not raise competition concerns under any plausible geographic market definition.

4.3.2.3. The Commission's assessment

(84) In the market investigation, the majority of respondents expressing an opinion considered that competition in cloud infrastructure and data analytics takes place worldwide. ([72])

(85) For the purposes of this Decision, the Commission considers that the exact geographic market definition for the supply of cloud infrastructure and data analytics can be left open, as the Transaction does not give rise to any competition concerns regardless of whether a worldwide or EEA-wide market is considered.

4.4. Generative AI

4.4.1. Product market definition

(86) According to Gartner, the potential market of generative AI can be segmented into two potential sub-markets: foundation and specialised generative AI models:

(1) **Foundation generative AI models** are AI systems that are trained on a broad range of datasets, such as text, images or audio.

([68]) Commission decision of 17 December 2020 in case M.9660 – Google/Fitbit, paragraphs277 and 278.

([69]) Commission decision of 19 October 2018 in case M.8994 – Microsoft/GitHub, paragraph 64, Commission decision of 12 June 2023 in case M.10855 – Capgemini/Orange/JV, paragraphs 42 to 44.

([70]) Commission decision of 21 December 2021 in case M.10290 – Microsoft/Nuance, paragraph 60.

([71]) Annex II.C.1 to the Form CO paragraph 7.

([72]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.B.B.1.

(2) **Specialised generative AI models** are models that focus on fulfilling a limited set of targeted or domain-specific tasks. They specialise in a specific context or category of information, such as a topic, industry, or problem set. These models can be created by fine-tuning, refining, or filtering a foundation model. They can also be created directly from a large corpus of unique data and/or strong domain knowledge using generative AI techniques. These models also include small-language models - which are lightweight, compute-efficient models with a smaller number of parameters than large-language models - even if those small-language models are not domain-specific.

(87) Google is active in the development of generative AI models, in particular, in the potential market for specialised generative AI models. Wiz is not active in that market.

4.4.1.1. Commission's precedents

(88) The Commission has not previously defined a market for generative AI models, nor has addressed its potential segmentations between foundation and specialised generative AI models.

(89) In the NVIDIA/Run:ai referral decision, the Commission referred to generative AI as being 'a specific form of AI that is capable of generating new content, such as text, images, music, and code, by learning from existing data.' ([73])

(90) In the Competition in Generative AI and Virtual Worlds policy paper the Commission mentioned a potentially relevant market 'for the sale or supply of generative AI foundation model services.' In the policy paper, the Commission identified possible segmentations to be explored in future cases, notably 'between consumer-facing and business models, cloud-based and on-device models, **general-purpose and specific-purpose models**, or unimodal and multimodal models.' ([74])

4.4.1.2. The Notifying Party's views

(91) The Notifying Party considers that the exact market segmentation can be left open as the Transaction does not give rise to any competition concerns regardless of the exact segmentation. ([75])

(92) Nevertheless, the Notifying Party submits that the potential segmentation of the generative AI models between general-purpose (foundation generative AI) and specific-purpose (specialised generative AI) models is not warranted as this distinction is increasingly outdated:

(1) From the demand-side, the Notifying Party considers that security software customers can choose between foundation and specialised generative AI models for many applications, such as coding, assistant functionalities or prompt engineering.

(2) From the supply-side, the Notifying Party considers that most Generative AI software vendors (OpenAI, Microsoft, Mistral AI, Databricks, Cohere and

([73]) Commission decision of 31 October 2024 in case M.11766 – NVIDIA/Run:ai, paragraph 44.
([74]) European Commission, Competition Policy Brief, Competition in Generative AI and Virtual Worlds, September 2024.
([75]) Form CO, paragraph 298.

Google) offer a wide variety of Generative AI models, addressing both general and specialised purposes.

4.4.1.3. The Commission's assessment

(93) For the purposes of this decision, the market investigation has yielded mixed results on whether foundation and specialised generative AI are interchangeable when used in combination with security software.

(94) In particular, most respondents to the market investigation that expressed a view confirmed that both foundation and specialised generative AI models are used in security software products, but only for specific or limited functionalities. ([76])

(95) Further, most respondents to the market investigation that expressed a view consider foundation and specialised generative AI models as partially interchangeable when used in security software, since foundation generative AI models can be used for security software, but specialised generative AI is preferred or required for certain use cases. ([77])

(96) In any event, the Commission considers that the question whether the market for the provision of generative AI services should distinguish between foundation and specialised generative AI models can be left open, as the Transaction does not raise competition concerns under any possible segmentation.

4.4.2. Geographic market definition

4.4.2.1. Commission's precedents

(97) The Commission has not previously defined a geographic market for generative AI models, nor for any of its possible segmentations.

4.4.2.2. The Notifying Party's views

(98) The Notifying Party considers that the potential geographic market for generative AI is global, or at least EEA-wide. The Notifying Party considers that generative AI models are global in design and distribution, and its demand is global. Lastly, there are no insurmountable trade barriers preventing the cross-border supply of generative AI models. ([78])

(99) In any event, the Notifying Party considers that the precise market definition can be left open, as the Transaction does not raise competition concerns under any plausible geographic market definition. ([79])

4.4.2.3. The Commission's assessment

(100) In the market investigation, the vast majority of respondents expressing an opinion considered that competition in the potential generative AI market takes place at a worldwide level. ([80])

([76]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, questions D.A.C.1 and D.A.C.2.

([77]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.A.C.3.

([78]) Form CO, paragraph 300.

([79]) Form CO, paragraph 301.

([80]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), Questionnaire 2 - Phase I market investigation – Competitors (CNAPP) and Questionnaire 3 - Phase I market investigation – Customers, question D.B.C.1.

(101) For the purposes of this Decision, the Commission considers that the exact geographic market definition for the potential market for generative AI models and for any of its potential segmentations can be left open, as the Transaction does not give rise to any competition concerns regardless of whether a worldwide or EEA-wide market is considered.

5. COMPETITIVE ASSESSMENT

5.1. Introduction

(102) Under Article 2(2) and (3) of the Merger Regulation, the Commission must assess whether a proposed concentration would significantly impede effective competition in the internal market or in a substantial part of it, in particular through the creation or strengthening of a dominant position.

(103) In this respect, a merger may entail horizontal and/or non-horizontal (namely, vertical or conglomerate) effects. Horizontal effects are those deriving from a concentration where the undertakings concerned are actual or potential competitors of each other in one or more of the relevant markets concerned. Vertical effects are those deriving from a concentration where the undertakings concerned are active on different levels of the supply chain. Conglomerate effects are those deriving from a concentration where the undertakings concerned are in a relationship which is neither horizontal nor vertical. A concentration may involve all three types of effects. In such a case, the Commission will appraise horizontal and non-horizontal effects in accordance with the guidance set out in the relevant notices, that is to say the Horizontal Merger Guidelines ([81]) and the Non-Horizontal Merger Guidelines. ([82])

5.2. Rationale of the Transaction

(104) The Notifying Party submits that the acquisition of Wiz will enable Google to (i) further develop and improve Wiz's CNAPP platform; (ii) complement and broaden Google's cloud security activities; and (iii) facilitate the adoption of multi-cloud operations by addressing customers' security concerns more comprehensively, thereby increasing competition and opportunities in public cloud. ([83])

(105) First, the Transaction creates an opportunity to develop and improve Wiz's products in the CNAPP market, by enabling Wiz to draw on Google's technical expertise and resources, including its expertise in AI and cloud infrastructure, accelerating innovation. The Transaction will also enable Wiz to operate more efficiently, generating synergies in distribution, general and administrative, cost of cloud infrastructure and headcount, which are expected to generate significant savings. ([84])

(106) Second, the Transaction broadens Google's cloud security portfolio, enabling it to address both proactive and reactive security needs. The Transaction will

([81]) Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings ('**Horizontal Merger Guidelines**'), OJ C31, 5.2.2004, p. 5.

([82]) Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings ('**Non-Horizontal Merger Guidelines**'), OJ C 265, 190.2008.

([83]) Form CO, paragraph 132.

([84]) Form CO, paragraphs 133-136, paragraph 355.

combine Wiz's software, which is primarily proactive, with Google's primarily reactive tools, improving their ability to prevent breaches, detect threats, and respond to them. Google's and Wiz's security rivals tend to offer a broader portfolio of the security capabilities that are most relevant for cloud applications and workstreams, spanning proactive and reactive security. Therefore, the Transaction will enable Google and Wiz to provide a coherent, seamless cloud security platform that can compete more directly with their larger rivals. ([85])

(107) Third, the Transaction will enhance competition in public cloud services by facilitating the adoption of multi-cloud operations. Security concerns and complexity limit customers' willingness to diversify their workload allocation across CSPs. The improvements to multi-cloud security enabled by the Transaction will mitigate these concerns and will therefore facilitate customers' deployment of workloads across multiple clouds, as well as moving workloads from one public cloud to another. The enhanced multi-cloud security offering enabled by the Transaction will remove the friction arising from security concerns, allowing customers to more freely choose where to deploy workloads across public clouds, and thereby increase competition amongst public CSPs. ([86])

5.3. Market shares

(108) According to the Horizontal Merger Guidelines and the Non-Horizontal Merger Guidelines, ([87]) in the assessment of the effects of a merger, market shares constitute a useful first indication of the structure of the markets at stake and of the competitive importance of the relevant players.

(109) In this Section, the Commission presents the market shares of the Parties in all the relevant markets described in Section 4 above.

5.3.1. Security software

(110) The Notifying Party submitted revenue-based market share estimates for the security software market worldwide and in Europe. These estimates are based on data from IDC and Gartner. This data covers both EEA and other European (non-EEA) countries, and EEA-specific market shares are not available. ([88]) However, the Notifying Party submits that EEA-wide market shares should not be materially different given the global nature of demand and supply and that there are no

([85]) Form CO, paragraphs 137-140.
([86]) Form CO, paragraphs 141-143.
([87]) Horizontal Merger Guidelines, paragraph 14; Non-Horizontal Merger Guidelines, paragraph 24.
([88]) Annexes III.A.1 and Annex III.A.3 to the Form CO.
In particular, IDC data for Europe covers the 'Rest of Western Europe', which encompasses Andorra, Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Monaco, the Netherlands, Norway, Portugal, San Marino, Saint Pierre and Miquelon, Spain, Svalbard, Sweden, Switzerland, and Vatican City, as well as 'Central and Eastern Europe', which includes Czech Republic, Hungary, Poland, Romania, Russia, Albania, Armenian Azerbaijan, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Estonia, Georgia, Kazakhstan, Kosovo, Kyrgyzstan, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Serbia, Slovakia, Slovenia, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.
Gartner data for Europe includes country-specific data for Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Netherlands, Norway, Poland, Portugal, Spain, Sweden, as well as aggregated data for the 'Rest of Europe' as defined by Gartner, which includes the following EEA countries: Bulgaria, Croatia, Cyprus, Estonia, Iceland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Romania, Slovakia, and Slovenia; as well as the following non-EEA countries: Albania, Andorra, Armenia, Belarus, Bosnia and Herzegovina, Georgia, Kosovo, North Macedonia, Moldova, Montenegro, Russia, Serbia, and Ukraine.

significant differences in the distribution of business among suppliers in the EEA and in non-EEA countries. ([89])

(111) **Table 2** to **Table 5** below present the IDC and Gartner market share estimates worldwide and Europe-wide for the Parties and their competitors in the market for security software in 2022, 2023 and 2024.

Table 2: The Parties' and their competitors' revenues and shares in the security software market according to IDC (Unadjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Gen Digital	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[70-80]%	[...]	[70-80]%	[...]	[70-80]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

Table 3: The Parties' and their competitors' revenues and shares in the security software market according to IDC (Unadjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Gen Digital	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[70-80]%	[...]	[70-80]%	[...]	[70-80]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

([89]) Form CO, footnote 261.

Table 4: The Parties' and their competitors' revenues and shares in the security software market according to Gartner (Unadjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	-	-	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[5-10]%	[...]	[10-20]%	[...]	[10-20]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Gen Digital	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
McAfee	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[70-80]%	[...]	[70-80]%	[...]	[70-80]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

Table 5: The Parties' and their competitors' revenues and shares in the security software market according to Gartner (Unadjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	-	-	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[5-10]%	[...]	[5-10]%	[...]	[10-20]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Broadcom	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[80-90]%	[...]	[80-90]%	[...]	[80-90]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

(112) Based on the IDC market share estimates for 2024, the Parties' combined share in the market for security software is [0-5]% worldwide and [0-5]% in Europe, and based on Gartner estimates, the Parties' combined market share is [0-5]% worldwide and [0-5]% in Europe.

(113) The Notifying Party has also submitted adjusted revenue-based market share estimates, combining their actual sales data with the market size estimates from IDC and Gartner.

(114) **Table 6** to **Table 9** below present worldwide and Europe-wide revenue-based market share estimates adjusted to the Parties actual sales in 2022, 2023 and 2024. The Notifying Party allocated the difference between their actual revenues and those reported by IDC and Gartner to the 'Others' vendor category, leaving the market size constant.

Table 6: The Parties' and their competitors' revenues and shares in the security software market according to IDC (Adjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Gen Digital	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[70-80]%	[...]	[70-80]%	[...]	[70-80]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

Table 7: The Parties' and their competitors' revenues and shares in the security software market according to IDC (Adjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Gen Digital	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[70-80]%	[...]	[70-80]%	[...]	[70-80]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

Table 8: The Parties' and their competitors' revenues and shares in the security software market according to Gartner (Adjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[5-10]%	[...]	[10-20]%	[...]	[10-20]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Gen Digital	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
McAfee	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[70-80]%	[...]	[70-80]%	[...]	[70-80]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

Table 9: The Parties' and their competitors' revenues and shares in the security software market according to Gartner (Adjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[5-10]%	[...]	[5-10]%	[...]	[10-20]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Broadcom	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[80-90]%	[...]	[80-90]%	[...]	[80-90]%
Total	**[...]**	**100%**	**[...]**	**100%**	**[...]**	**100%**

Source: Form CO, Market shares data pack

(115) Based on the adjusted IDC market share estimates for 2024, the Parties' combined market share in the market for security software is [0-5]% worldwide and [0-5]% in Europe, and based on Gartner estimates, the Parties' combined market share is [0-5]% worldwide and [0-5]% in Europe.

5.3.1.1. CNAPP

(116) The Notifying Party submitted revenue-based market share estimates for the CNAPP market worldwide and in Europe. These estimates are based on data from IDC and Gartner. As described above, in section 5.3.1, this data covers both EEA and other European (non-EEA) countries, and EEA-specific market shares are not available. However, the Notifying Party submits that EEA market shares would not be materially different from those in Europe given the global nature of demand and supply and that there are no significant differences in the distribution of business among suppliers in the EEA and in non-EEA countries. ([90])

(117) The Notifying Party has also submitted adjusted revenue-based market shares, claiming that the estimates of the Parties' revenues provided by IDC and Gartner are overstated. The adjusted market shares combine the Parties' actual sales data with the market size and the competitors' sales estimated by IDC and Gartner. In addition, the Notifying Party has also provided a proxy for volume-based market shares.

5.3.1.1.1. IDC revenue-based market share estimates

(118) **Table 10** and **Table 11** below present worldwide and Europe-wide revenue-based market share estimates for the Parties and their main competitors in 2022, 2023 and 2024 in the functional market for CNAPP reported in the IDC Software Tracker 2024.

(119) As indicated above, in section 5.3.1, IDC data is only available for 'Western Europe' and 'Central & Eastern Europe', which covers the EEA, but also several non-EEA countries. However, the Notifying Party submits that EEA-specific market shares would not be materially different from those in Europe given the global nature of demand and supply and that there are no significant differences in the distribution of business among suppliers in the EEA and in non-EEA countries. ([91])

([90]) Form CO, footnote 261.
([91]) Form CO, footnote 261.

Table 10: The Parties' and their competitors' revenues and shares in the CNAPP functional market according to IDC (Unadjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Microsoft	[...]	[5-10]%	[...]	[5-10]%	[...]	[10-20]%
CrowdStrike	[...]	[5-10]%	[...]	[10-20]%	[...]	[5-10]%
Trend Micro	[...]	[10-20]%	[...]	[5-10]%	[...]	[5-10]%
Palo Alto Networks	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Check Point	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Fortinet (Lacework)	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Trellix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Sophos	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
SentinelOne	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Broadcom	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[30-40]%	[...]	[30-40]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 15.

Table 11: The Parties' and their competitors' revenues and shares in CNAPP functional market according to IDC (Unadjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[5-10]%	[...]	[10-20]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[5-10]%**	**[...]**	**[10-20]%**
Microsoft	[...]	[5-10]%	[...]	[10-20]%	[...]	[10-20]%
CrowdStrike	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Trend Micro	[...]	[20-30]%	[...]	[10-20]%	[...]	[10-20]%
Palo Alto Networks	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Check Point	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Fortinet (Lacework)	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Trellix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Sophos	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
SentinelOne	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Broadcom	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[30-40]%	[...]	[30-40]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 16.

(120) Based on the IDC market share estimates for 2024, the Parties' combined activities in CNAPP are [5-10]% worldwide and [10-20]% in Europe.

(121) **Table 12** below presents the Parties' forward-looking revenues and projected shares in the IDC CNAPP market for the years 2025 to 2029. The Parties' forward-looking revenues were estimated [information on Google's market share projections]. For the calculation of the market shares, the market size was estimated using IDC's forecasts for the CNAPP market. ([92])

([92]) Form CO, paragraphs 210-213 and the Parties' response to RFI 6, Question 4.

Table 12: The Parties' forward-looking revenues and projected shares in the CNAPP functional market according to IDC (Worldwide, 2025-2029)

Vendor	2025		2026		2027		2028		2029	
	Rev.	Share (%)	Rev.	Share (%)	Rev.	Share (%)	Rev.	Share (%)	Rev.	Share (%)
Google	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
Wiz	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
Combined	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**
Total	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**	**[...]**

Source: Form CO, Table 21.

(122) The projected market shares based on IDC data and [information on Google's market share projections] ([93]) result in a combined worldwide market share of [market share projections]%.

5.3.1.1.2. Gartner revenue-based market share estimates

(123) **Table 13** and

(124) **Table 14** below present worldwide and Europe-wide revenue-based market share estimates for the Parties and their main competitors in 2022, 2023 and 2024 based on the [third-party report prepared for the Parties]. The [third-party report prepared for the Parties] was [information on Google's business strategy] and tracks a CNAPP subsegment rather than the legacy CSPM and CWPP subsegments included in Gartner's Enterprise Software Tracker 2024.

(125) The [third-party report prepared for the Parties] provides country-specific data for 13 EEA countries and for the aggregated regions 'Rest of Western Europe', 'Rest of Benelux' and Rest of Central and Eastern Europe', comprising both EEA and non-EEA countries. ([94]) However, the Notifying Party submits that EEA-specific market shares would not be materially different from those in Europe given the global nature of demand and supply and that there are no significant differences in the distribution of business among suppliers in the EEA and in non-EEA countries. ([95])

([93]) Form CO, paragraph 213. The growth projections in [information on Google's deal valuation], thereby overstating Google's revenues in the CNAPP market.

([94]) Parties' response to RFI 7, Annex Q7.3. In particular, [third-party report] provides country-specific data for France, Germany, Italy, the Netherlands, Spain, Sweden, Austria, Poland, Portugal, Ireland, Norway, Denmark and Finland. The 'Rest of Western Europe' region includes Greece, Andorra, Cyprus, Iceland, Lichenstein and Malta, the 'Rest of Benelux' includes Belgium and Luxembourg, and the 'Rest of Central and Eastern Europe', which includes the following EEA countries: Bulgaria, Croatia, Czech Republic, Hungary, Romania, Slovakia, Slovenia, Estonia, Latvia, and Lithuania; as well as the following non-EEA countries: Russia, Ukraine, Serbia, Albania, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Georgia, Kosovo, North Macedonia, Moldova, Montenegro, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan.

([95]) Form CO, footnote 261.

Table 13: The Parties' and their competitors' shares in CNAPP according to the [third-party report prepared for the Parties] (Global, Unadjusted, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Wiz	[...]	[5-10]%	[...]	[10-20]%	[...]	[10-20]%
Combined	**[...]**	**[20-30]%**	**[...]**	**[20-30]%**	**[...]**	**[30-40]%**
Microsoft	[...]	[20-30]%	[...]	[10-20]%	[...]	[10-20]%
Amazon	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Palo Alto Networks	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
CrowdStrike	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
ServiceNow	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Datadog	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Alibaba Group	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
GitLab	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Citrix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[5-10]%	[...]	[10-20]%	[...]	[5-10]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex III.A.10 – Annex 1, Table 1.1.

Table 14: The Parties' and their competitors' shares in CNAPP according to the [third-party report prepared for the Parties] (Europe, Unadjusted, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[20-30]%	[...]	[10-20]%	[...]	[10-20]%
Wiz	[...]	[5-10]%	[...]	[10-20]%	[...]	[10-20]%
Combined	**[...]**	**[20-30]%**	**[...]**	**[20-30]%**	**[...]**	**[20-30]%**
Microsoft	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Amazon	[...]	[10-20]%	[...]	[5-10]%	[...]	[5-10]%
Palo Alto Networks	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
ServiceNow	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Datadog	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Alibaba Group	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
GitLab	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Citrix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex III.A.10 – Annex 1, Table 1.2.

(126) Based on the [third-party report prepared for the Parties], the Parties' combined market share in the CNAPP market in 2024 was [30-40]% worldwide and [20-30]% in Europe. However, the Notifying Party claims that the [third-party report prepared for the Parties] are unreliable. In particular, the Notifying Party submits that the report overstates Google's CNAPP revenues by [information on the Parties' revenues]% and that the product mapping contains several errors, such as presenting Wiz as a Google product and erroneously allocating Google SecOps' revenues to the CNAPP market. ([96]) For this reason, the competitive assessment relies on the market share estimates based on IDC data.

5.3.1.1.3. Adjusted revenue-based market share estimates

(127) As described in sections 5.3.1.1.1 and 5.3.1.1.2, the Notifying Party submits that the numbers reported in the unadjusted market shares provided by Gartner and IDC are overstated. In particular, the [third-party report prepared for the Parties] overestimates Google's CNAPP revenues by around [information on the Parties' revenues]% and Wiz's revenues by [information on the Parties' revenues]%,

([96]) Parties' response to RFI 7 and Annex III.A.10 to the form CO.

while estimating a relatively small overall CNAPP market size. ([97]) Likewise, IDC overstates Google's worldwide revenues by [information on the Parties' revenues]% and Wiz's revenues by [information on the Parties' revenues]%, and in Europe Google's revenues are overstated by [information on the Parties' revenues]% and Wiz's revenues by [information on the Parties' revenues]%. ([98])

(128) **Table 15** to **Table 18** below present worldwide and Europe-wide revenue-based market share estimates adjusted to the Parties' actual revenues in 2022, 2023 and 2024. The Notifying Party allocated the difference between their actual revenues and those reported by IDC and Gartner to the 'Others' vendor category, leaving the market size constant. ([99])

(129) As set out above in Sections 5.3.1.1.1 and 5.3.1.1.2, neither IDC nor Gartner provide EEA-specific market share data. However, the Notifying Party submits that EEA shares would not materially differ from those in Europe.

Table 15: The Parties' and their competitors' revenues and shares in the CNAPP functional market according to IDC (Adjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Microsoft	[...]	[5-10]%	[...]	[5-10]%	[...]	[10-20]%
CrowdStrike	[...]	[5-10]%	[...]	[10-20]%	[...]	[5-10]%
Trend Micro	[...]	[10-20]%	[...]	[5-10]%	[...]	[5-10]%
Palo Alto Networks	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Check Point	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Fortinet (Lacework)	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Trellix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Sophos	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
SentinelOne	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Broadcom	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[30-40]%	[...]	[30-40]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 17.

([97]) Annex III.A.10, paragraphs 6-8.
([98]) Form CO, paragraph 178.
([99]) If the total market size was adjusted downwards to reflect the Parties' actuals, the combined CNAPP shares would be [5-10]% globally and [0-5]% in Europe, in 2024, [5-10]% globally and [0-5]% in Europe, in 2023, and [0-5]% globally and [0-5]% in Europe, in 2022, based on IDC data.

Table 16: The Parties' and their competitors' revenues and shares in the CNAPP functional market according to IDC (Adjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**
Microsoft	[...]	[5-10]%	[...]	[10-20]%	[...]	[10-20]%
CrowdStrike	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Trend Micro	[...]	[20-30]%	[...]	[10-20]%	[...]	[10-20]%
Palo Alto Networks	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Check Point	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Fortinet (Lacework)	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Trellix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Sophos	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
SentinelOne	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Broadcom	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[40-50]%	[...]	[30-40]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 18.

Table 17: The Parties' and their competitors' shares in CNAPP according to the [third-party report prepared for the Parties] (Global, Adjusted, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[5-10]%	[...]	[5-10]%	[...]	[10-20]%
Combined	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[10-20]%**
Microsoft	[...]	[20-30]%	[...]	[10-20]%	[...]	[10-20]%
Amazon	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Palo Alto Networks	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
CrowdStrike	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
ServiceNow	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Datadog	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Alibaba Group	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
GitLab	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Citrix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex III.A.10 – Annex 1, Table 2.1.

Table 18: The Parties' and their competitors' shares in CNAPP according to the [third-party report prepared for the Parties] (Europe, Adjusted, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[5-10]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[10-20]%**
Microsoft	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Amazon	[...]	[10-20]%	[...]	[5-10]%	[...]	[5-10]%
Palo Alto Networks	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
ServiceNow	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Cisco	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Datadog	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Alibaba Group	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
GitLab	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Citrix	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[40-50]%	[...]	[40-50]%	[...]	[30-40]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex III.A.10 – Annex 1, Table 2.2.

(130) Adjusting the revenue-based market share estimates based on IDC and Gartner with the Parties' actual revenue results in combined shares of, respectively, [5-10]% and [10-20]% worldwide, and [0-5]% and [10-20]% in Europe, in 2024. However, given that the adjustments provided by the Parties apply only to their own revenues and do not extend to competitors, the competitive assessment relies on unadjusted market shares.

5.3.1.1.4. Volume-based market share estimates

(131) The Notifying Party also aimed to provide volume-based market share estimates. Neither IDC nor Gartner provide volume-based shares for security software, including CNAPP. ([100]) Therefore, the Parties sought to proxy volume-based market share estimates based on (i) customer counts; (ii) 'workloads' from the perspective of CNAPP billable units, (iii) 'workloads' from the perspective of virtual machine counts, and (iv) API calls.

(132) First, volume shares based on customer counts measure how many CNAPP customers each of the Parties have compared to the total market. For the

([100]) Form CO, paragraph 144.

estimation of their share in the marker, the Parties collected the number of Wiz and Google SCCE customers in 2025. As of July 2025, Wiz served [information on Parties' customer count] customers globally, of which [information on Parties' customer count] ([information on the Parties' customers' workloads]%) have workloads on Google's cloud infrastructure. In the EEA, Wiz had [information on Parties' customer count] customers, of which [information on Parties' customer count]([information on the Parties' customers' workloads]%) deploy workloads on Google's cloud infrastructure. As of Q1 2025, Google SCCE reported [information on Parties' customer count] customers globally, all of which are assumed to deploy workloads on Google's cloud infrastructure. Out of these SCCE customers, [information on Parties' customer count] are in the EEA. ([101])

(133) For the estimation of the market size, the Parties are not aware of any source providing data on the total pool of CNAPP customers, nor is there any data available from Google that indicates whether or not a GCP customer is a CNAPP customer. The total market size was therefore estimated by proxy. In the absence of a more direct means for estimating the addressable market by identifying GCP customers that may use a CNAPP, Google has used those with 'meaningful spend' as a proxy. ([102]) In January to May 2025, GCP had [information on Parties' customer count] customers globally, including c. [information on Parties' customers' purchasing decisions] customers with meaningful spend. In the EEA, GCP had [information on Parties' customer count] customers, [information on Parties' customers' purchasing decisions] with meaningful spend. ([103])

(134) Further, the Notifying Party submits that third-party sources expect CNAPPs to have a 2025 penetration rate of 75%. ([104]) Applying the CNAPP penetration rate to the addressable market of GCP customers with meaningful GCP spend, Google calculated a total market for CNAPP usage on GCP of [information on Parties' customer count and customers' preferences] customers, including [information on Parties' customer count and customers' preferences] in the EEA. ([105])

(135) Applying this methodology, the Parties estimate Wiz to have a share of [0-5]% and SCCE a share of [0-5]% within the worldwide addressable market for CNAPP usage on GCP. In the EEA, the estimated shares are [0-5]% for Wiz and [0-5]% for SCCE. ([106])

(136) Second, the Parties considered that proxying volume shares based on 'secured workloads' could constitute a meaningful proxy for volume-based shares. This approach would involve comparing the number of workloads secured by Wiz and Google SCCE against the total number of workloads secured by CNAPPs. However, workloads are not a precisely defined industry-wide unit, and each vendor maintains its own definitions of the notion within its products. As an alternative, the Parties considered providing volume shares based on billable units, which CNAPP vendors use to calculate the bill for the customer. However,

([101]) Form CO, paragraph 190.
([102]) The Parties submit that small, private customers are unlikely to use a CNAPP.
([103]) Form CO, paragraph 190.
([104]) Form CO, footnote 279. See the Cloud Security Alliance (CSA), Cloud Native Application Protection Platform (CNAPP) Survey Report, 2023, available at: https://cloudsecurityalliance.org/blog/2023/08/24/cloud-native-application-protection-platforms-key-findings-challenges-from-the-csa-survey
([105]) Form CO, paragraph 190.
([106]) Form CO, paragraph 191.

even billable units are not comparable across vendors. ([107]) Therefore, the Parties were not able to compute volume shares on this basis.

(137) Third, volume shares based on virtual machines approximate the number of cloud-hosted assets protected by a given CNAPP. ([108]) In a cloud setting, a virtual machine is a software-based emulation of a physical computer stored on the cloud. To calculate market shares based on the virtual machines proxy, the Parties estimated the average number of unique GCP-hosted virtual machines scanned by Wiz and by SCCE per day, against the number of unique virtual machines hosted on GCP per day, in July 2025. ([109])

(138) In July 2025, Wiz estimates that it scanned on average c. [information on the Parties' customers' workloads] unique virtual machines per day in, including c. [information on the Parties' customers' workloads] on GCP. Google estimates that SCCE scanned on average c. [information on the Parties' customers' workloads] unique virtual machines in a day, which are assumed to be in GCP, since SCCE cannot currently scan virtual machines on AWS or Azure. ([110])

(139) Further, Google estimates that GCP hosted on average c. [information on the Parties' customers' workloads] unique virtual machines, of which [information on the Parties' customers' workloads] (approximately [information on the Parties' customers' workloads]) are expected to relate to business customers. Assuming the CNAPP 2025 penetration rate of 75%, Google projected an addressable market of c. [information on the Parties' customers' workloads] virtual machines on GCP. ([111])

(140) Applying this methodology results in a combined share of [0-5]% ([0-5]% for Wiz and [0-5]% for SCCE) in the addressable GCP-specific market for virtual machines. ([112])

(141) Fourth, the Parties considered estimating volume shares based on API calls, counting the number of API-based data extraction requests CSPs receive from different CNAPPs. However, the Parties were unable to estimate market shares on this basis as it is not possible to identify CNAPP API calls. ([113])

(142) Nonetheless, the Notifying Party submits that value-based shares are more representative of CNAPP vendors' market positions than volume-based shares. In particular, the Parties' CNAPPs are directly revenue-generating, are not part of a bundle or offered free of charge, are not priced materially below other offerings in the market and are not subject to revenue allocation issues. Therefore, the Notifying Party submits that there is no prospect of value-based metrics understating the Parties' competitive position. ([114]) For this reason, the competitive assessment relies on value-based market shares.

([107]) Billing can reflect vendors' choices in workload definition. However, even if vendors agreed to a definition of workload, not all vendors bill based on workloads, and among those that do, conversion ratios, from workload to billable unit differ.

([108]) Among the assets secured by CNAPPs, including, among others, virtual machines, container hosts, serverless functions, serverless containers and asset metadata, the Parties consider virtual machines as one of the most consistently defined assets across cloud infrastructures and constitute the largest component of Wiz's revenues.

([109]) Form CO, paragraph 194.

([110]) Form CO, paragraph 194.

([111]) Form CO, paragraph 194.

([112]) Form CO, paragraph 194.

([113]) Form CO, paragraph 195.

([114]) Form CO, paragraphs 183-186.

5.3.1.2. CSPM

(143) The Notifying Party provided revenue-based market share estimates for the potential market for CSPM worldwide and Europe-wide. These estimates are based on data reported by Gartner. As indicated in section 5.3.1, Gartner provides country-specific market share data for 17 EEA countries and for the aggregated 'Rest of Europe' region, which includes other EEA countries but also other European non-EEA countries. ([115]) However, the Notifying Party submits that, given the global nature of demand and supply, EEA-specific market shares would not be materially different from Europe. ([116])

(144) The Notifying Party has also provided adjusted revenue-based market shares, combining their actual sales data with the competitors and market size estimates from Gartner.

5.3.1.2.1. Gartner revenue-based market shares estimates

(145) **Table 19** and **Table 20** below present the worldwide and Europe-wide revenue-based market share estimates for the Parties and their main competitors in 2022, 2023 and 2024 in the potential market for CSPM, as reported in the Gartner Enterprise Software 2024 tracker.

Table 19: The Parties' and their competitors' revenues and shares in CSPM according to Gartner (Unadjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[10-20]%	[...]	[10-20]%
Wiz	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Combined	**[...]**	**[10-20]%**	**[...]**	**[20-30]%**	**[...]**	**[20-30]%**
Microsoft	[...]	[0-5]%	[...]	[10-20]%	[...]	[10-20]%
Palo Alto Networks	[...]	[20-30]%	[...]	[10-20]%	[...]	[5-10]%
Amazon	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Tenable	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Check Point	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Orca Security	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Rapid7	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Qualys	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[20-30]%	[...]	[10-20]%	[...]	[10-20]%
Total	[...]	**100.0%**	[...]	**100.0%**	[...]	**100.0%**

Source: Form CO, Table 25

([115]) Annex RFI 2 Q13 to the Form CO.
([116]) Form CO, footnote 261.

Table 20: The Parties' and their competitors' revenues and shares CSPM according to Gartner (Unadjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[10-20]%	[...]	[10-20]%
Wiz	[...]	[5-10]%	[...]	[10-20]%	[...]	[10-20]%
Combined	**[...]**	**[5-10]%**	**[...]**	**[20-30]%**	**[...]**	**[20-30]%**
Microsoft	[...]	[0-5]%	[...]	[20-30]%	[...]	[20-30]%
Palo Alto Networks	[...]	[10-20]%	[...]	[0-5]%	[...]	[0-5]%
Amazon	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Tenable	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Check Point	[...]	[20-30]%	[...]	[0-5]%	[...]	[0-5]%
Orca Security	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Rapid7	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Qualys	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[20-30]%	[...]	[20-30]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 25

(146) Based on the market share data reported by Gartner, the Parties' combined market share in the CSPM market in 2024 was [20-30]% worldwide and [20-30]% in Europe.

5.3.1.2.2. Adjusted revenue-based market share estimates

(147) In particular, Gartner overstates Google's CSPM worldwide revenues by [information on the Parties' revenues]% and Wiz's revenues by [information on the Parties' revenues]%, and in Europe, Google's revenues are overstated by [information on the Parties' revenues]% and Wiz's revenues by [information on the Parties' revenues]%. ([117])

(148) As set out above in Section 5.3.1.2.1, Gartner does not provide EEA-specific market share data. However, the Notifying Party submits that EEA shares would not materially differ from those in Europe.

(149) **Table 21** and **Table 22** below present worldwide and Europe-wide revenue-based market share estimates adjusted to the Parties' actual revenues in 2022, 2023 and 2024. The Notifying Party allocated the difference between their actual revenues

([117]) Form CO, paragraph 224.

and those reported by Gartner to the 'Others' vendor category, leaving the market size constant. ([118])

Table 21: The Parties' and their competitors' revenues and shares in CSPM according to Gartner (Adjusted, Worldwide, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[5-10]%
Combined	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Microsoft	[...]	[0-5]%	[...]	[10-20]%	[...]	[10-20]%
Palo Alto Networks	[...]	[20-30]%	[...]	[10-20]%	[...]	[5-10]%
Amazon	[...]	[0-5]%	[...]	[5-10]%	[...]	[5-10]%
Tenable	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Check Point Software Technologies	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
Orca Security	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Rapid7	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Qualys	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[30-40]%	[...]	[40-50]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex RFI 2 Q13, Table 1.

([118]) Form CO, footnote 343. If the total market size was adjusted downwards to reflect the Parties' actuals, the combined CSPM shares would be [5-10]% globally and [5-10]% in Europe, in 2024, [5-10]% globally and [5-10]% in Europe, in 2023, and [5-10]% globally and [0-5]% in Europe, in 2022.

Table 22: The Parties' and their competitors' revenues and shares in CSPM according to Gartner (Adjusted, Europe, 2022-2024)

Vendor	2022		2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Wiz	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Combined	**[...]**	**[0-5]%**	**[...]**	**[0-5]%**	**[...]**	**[5-10]%**
Microsoft	[...]	[0-5]%	[...]	[20-30]%	[...]	[20-30]%
Palo Alto Networks	[...]	[10-20]%	[...]	[0-5]%	[...]	[0-5]%
Amazon	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Tenable	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Check Point Software Technologies	[...]	[20-30]%	[...]	[0-5]%	[...]	[0-5]%
Orca Security	[...]	[5-10]%	[...]	[0-5]%	[...]	[0-5]%
CrowdStrike	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Rapid7	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Qualys	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[40-50]%	[...]	[40-50]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex RFI 2 Q13, Table 2.

(150) Adjusting the revenue-based market share estimated based on Gartner with the Parties' actuals results combined shares of, respectively, [5-10]% worldwide, and [5-10]% in Europe, in 2024. However, given that the adjustments provided by the Parties apply only to their own revenues and do not extend to competitors, the competitive assessment relies on unadjusted market shares.

5.3.1.3. Other security software

(151) The Notifying Party submitted revenue-based market share estimates for other security software market segments defined by IDC and Gartner, which give rise to a technical conglomerate relationship between Google and Wiz's activities in CNAPP and other security software.

(152) **Table 23** below presents an overview the worldwide and Europe revenue-based market share estimates for the Parties and their main competitors in 2024 in the IDC markets for Governance, Risk and Compliance Software, Information and Data Security Software, Identity and Access Management Software, Security Analytics Software, and Network Security Software, where Google operates.

Table 23: The Parties' and their competitors' revenue shares in other security software market segments according to IDC (Unadjusted, Worldwide and Europe, 2024)

IDC functional market	Google's share (Unadjusted, 2024)		Top 5 competitors (WW%; Europe%)
	Worldwide	Europe	
Governance, Risk, and Compliance Software	[0-5]%	-	Diligent ([5-10]%; [5-10]%) Archer ([5-10]%; [0-5]%) NAVEX ([5-10]%; [0-5]%) ServiceNow ([5-10]%; [5-10]%) Workiva ([0-5]%; [0-5]%)
Information and Data Security Software	[0-5]%	[0-5]%	Microsoft ([10-20]%; [20-30]%) Proofpoint ([10-20]%; [5-10]%) Thales ([5-10]%; [5-10]%) Broadcom ([0-5]%; [0-5]%) IBM ([0-5]%; [5-10]%)
Identity and Access Management Software	[0-5]%	[0-5]%	Microsoft ([30-40]%; [30-40]%) Okta ([10-20]%; [5-10]%) Oracle ([0-5]%; [0-5]%) CyberArk Software ([0-5]%; [0-5]%) Thales ([0-5]%; [0-5]%)
Security Analytics Software	[0-5]%	[0-5]%	Cisco ([10-20]%; [5-10]%) Microsoft ([5-10]%; [5-10]%) Tenable ([0-5]%; [0-5]%) Darktrace ([0-5]%; [0-5]%) Qualys ([0-5]%; [0-5]%)
Network Security Software	[0-5]%	[0-5]%	Zscaler ([10-20]%; [10-20]%) Palo Alto Networks ([10-20]%; [10-20]%) Akamai ([5-10]%; [5-10]%) Cisco ([5-10]%; [5-10]%) Cloudflare ([0-5]%; [5-10]%)

Source: Form CO, Table 30.

(153) **Table 24** below presents an overview of the worldwide and Europe revenue-based market share estimates for the Parties and their main competitors in 2024 in the Gartner market for Security Information and Event Management (SIEM), where Google operates.

Table 24: The Parties' and their competitors' revenue shares in the SIEM market segments according to Gartner (Unadjusted, Worldwide and Europe, 2024)

IDC functional market	Google's share (Unadjusted, 2024)		Top 5 competitors (WW%; Europe%)
	Worldwide	Europe	
Security Information and Event Management (SIEM)	[0-5]%	[0-5]%	Cisco ([30-40]%; [10-20]%) Microsoft ([10-20]%; [20-30]%) IBM ([10-20]%, [20-30]%) Exabeam ([0-5]%; [0-5]%) Palo Alto Networks ([0-5]%; [0-5]%)

Source: Form CO, Table 31.

(154) Based on the 2024 market share estimates, the Parties' combined share in the IDC and Gartner other security software markets where Google is active are below 5%, both worldwide and in Europe. Therefore, the Notifying Party submits that the Transaction does not give rise to any affected conglomerate relationship between Parties' activities in CNAPP and other security software.

5.3.2. Cloud infrastructure and data analytics

(155) The Notifying Party submitted revenue-based market share estimates for the cloud infrastructure and data analytics market. These estimates are based on data from IDC and Gartner. The market shares based on IDC data are only available worldwide and for the region of Europe, Middle East and Africa ('**EMEA**'). Gartner market shares are available worldwide and for Europe, including both EEA and non-EEA countries. However, the Notifying Party submits that these are not expected to be materially different from EEA-wide market shares, given the global nature of supply and demand and that there are no significant differences in the distribution of business among suppliers in the EEA and in non-EEA countries.

5.3.2.1. IDC revenue-based market share estimates

(156) **Table 25** to **Table 30** below present the worldwide and EMEA-wide revenue-based market share estimates for the Parties and their main competitors in 2021, 2022 and 2023 in the functional markets for IaaS+PaaS (the overall market for cloud infrastructure and data analytics), and separately for the IaaS and PaaS potential market segments, as reported on IDC's Semi-annual Public Cloud Services Tracker 2023H2.

(157) IDC market share estimates for cloud infrastructure and data analytics are only available to the aggregate of the EMEA region and for six EEA countries, France, Germany, Italy, Netherlands, Spain, and Sweden, as well as the UK, Switzerland and Israel, for which country-specific data is available. The Notifying Party has provided market share data for the EMEA region, excluding the UK, Switzerland and Israel. However, the Notifying Party submits that the EEA-wide market shares would not be materially different. In particular, the results do not materially change when considering the narrower European scope, including only the six

EEA countries for which country-specific data is available, with Google's IaaS+PaaS unadjusted share being [5-10]% in 2023. ([119])

Table 25: The Parties' and their competitors' revenues and shares in the IaaS + PaaS functional market according to IDC (Unadjusted, Worldwide, 2021-2023)

Vendor	2021		2022		2023	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Amazon Web Services	[...]	[30-40]%	[...]	[30-40]%	[...]	[30-40]%
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Alibaba Group	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Salesforce	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Huawei	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
China Telecom	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Tencent	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Snowflake	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 2.

([119]) Form CO, footnote 425 and Annex II.C.1.1. to the Form CO.

Table 26: The Parties' and their competitors' revenues and shares in the IaaS + PaaS functional market according to IDC (Unadjusted, EMEA excluding UK, Switzerland and Israel, 2021-2023)

Vendor	2021		2022		2023	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Amazon Web Services	[...]	[30-40]%	[...]	[30-40]%	[...]	[30-40]%
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Salesforce	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
SAP	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Atlassian	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Orange	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
OVHcloud	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
T-Systems	[...]	[0-5]%	[...]	N/A	[...]	N/A
MongoDB	[...]	N/A	[...]	[0-5]%	[...]	N/A
Open AI	[...]	N/A	[...]	N/A	[...]	[0-5]%
Others	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 2.

Table 27: The Parties' and their competitors' revenues and shares in the IaaS functional market according to IDC (Unadjusted, Worldwide, 2021-2023)

Vendor	2021		2022		2023	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Amazon Web Services	[...]	[40-50]%	[...]	[40-50]%	[...]	[40-50]%
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Alibaba Group	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Huawei	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
China Telecom	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Tencent	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
China Mobile	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Inspur	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Baidu	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 2.

Table 28: The Parties' and their competitors' revenues and shares in the IaaS functional market according to IDC (Unadjusted, EMEA excluding UK, Switzerland and Israel, 2021-2023)

Vendor	2021		2022		2023	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Amazon Web Services	[...]	[50-60]%	[...]	[50-60]%	[...]	[50-60]%
Microsoft	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Orange	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
OVHcloud	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
T-Systems	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Huawei	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	N/A	[...]	N/A	[...]	[0-5]%
ATOS	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IONOS	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Vodafone	[...]	[0-5]%	[...]	[0-5]%	[...]	N/A
Others	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 2.

Table 29: The Parties' and their competitors' revenues and shares in the PaaS functional market according to IDC (Unadjusted, Worldwide, 2021-2023)

Vendor	2021		2022		2023	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Microsoft	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Amazon Web Services	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Salesforce	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Alibaba Group	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
SAP	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Snowflake	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Atlassian	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
ServiceNow	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[30-40]%	[...]	[30-40]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 2.

Table 30: The Parties' and their competitors' revenues and shares in the PaaS functional market according to IDC (Unadjusted, EMEA excluding UK, Switzerland and Israel, 2021-2023)

Vendor	2021		2022		2023	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Microsoft	[...]	[20-30]%	[...]	[20-30]%	[...]	[20-30]%
Amazon Web Services	[...]	[10-20]%	[...]	[10-20]%	[...]	[10-20]%
Salesforce	[...]	[5-10]%	[...]	[5-10]%	[...]	[5-10]%
SAP	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Atlassian	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Open AI	[...]	N/A	[...]	N/A	[...]	[0-5]%
MongoDB	[...]	[0-5]%	[...]	[0-5]%	[...]	[0-5]%
Snowflake	[...]	N/A	[...]	[0-5]%	[...]	[0-5]%
ServiceNow	[...]	[0-5]%	[...]	[0-5]%	[...]	N/A
OpenText	[...]	[0-5]%	[...]	N/A	[...]	N/A
Others	[...]	[30-40]%	[...]	[30-40]%	[...]	[30-40]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 2.

(158) Based on the IDC market share estimates for 2023, the Parties combined market share in the IaaS+PaaS functional market is [5-10]% worldwide and [5-10]% in the EMEA region, excluding UK, Switzerland and Israel. In the IaaS functional market, the Parties combined activities are [5-10]% worldwide and [5-10]% in Europe. Finally, in the PaaS functional market, the Parties combined market share is [5-10]% worldwide and [5-10]% in the EMEA region, excluding UK, Switzerland and Israel.

5.3.2.2. Gartner revenue-based market share estimates

(159) **Table 31** and **Table 32** below present the worldwide and Europe-wide revenue-based market share estimates for the Parties and their main competitors in 2021, 2022 and 2023 in the IaaS market segment, as reported on the Gartner Services Report 2024.

(160) Gartner shares for Europe are computed as the aggregation of the 17 EEA countries for which country-specific data is available, and the 'Rest of Europe' region, as defined by Gartner, which includes EEA and other European (non-EEA) countries, excluding the UK. ([120]) However, the Notifying Party submits

([120]) Annex II.C.1.1. to the Form CO. Gartner records country-specific data for the following 17 EEA countries: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece,

that the results do not materially change when considering the narrower European scope, comprising only the seventeen EEA countries for which country-specific data is available, with Google's IaaS market share being [10-20]% in 2024. ([121])

Table 31: The Parties' and their competitors' revenues and shares in the IaaS segment according to Gartner (Unadjusted, Worldwide, 2023-2024)

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[5-10]%**	**[...]**	**[5-10]%**
Amazon	[...]	[30-40]%	[...]	[30-40]%
Microsoft	[...]	[20-30]%	[...]	[20-30]%
Alibaba Group	[...]	[5-10]%	[...]	[5-10]%
Huawei	[...]	[0-5]%	[...]	[0-5]%
Tencent	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%
Inspur Cloud	[...]	[0-5]%	[...]	[0-5]%
China Telecom	[...]	[0-5]%	[...]	[0-5]%
China Unicom	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[5-10]%	[...]	[5-10]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 4.

Hungary, Ireland, Italy, Netherlands, Norway, Poland, Portugal, Spain, Sweden., as well as the UK. The 'Rest of Europe' region includes the following EEA countries: Bulgaria, Croatia, Cyprus, Estonia, Iceland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Romania, Slovakia, and Slovenia; as well as the following non-EEA countries: Albania, Andorra, Armenia, Belarus, Bosnia and Herzegovina, Georgia, Kosovo, North Macedonia, Moldova, Montenegro, Russia, Serbia, and Ukraine.

([121]) Form CO, footnote 438 and Annex II.C.1.1. to the Form CO.

Table 32: The Parties' and their competitors' revenues and shares in the IaaS segment according to Gartner (Unadjusted, Europe, 2023-2024)

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[10-20]%**	**[...]**	**[10-20]%**
Amazon	[...]	[40-50]%	[...]	[40-50]%
Microsoft	[...]	[20-30]%	[...]	[20-30]%
OVH	[...]	[0-5]%	[...]	[0-5]%
IBM	[...]	[0-5]%	[...]	[0-5]%
Oracle	[...]	[0-5]%	[...]	[0-5]%
Tietoevry	[...]	[0-5]%	[...]	[0-5]%
Atos	[...]	[0-5]%	[...]	[0-5]%
T-Systems	[...]	[0-5]%	[...]	[0-5]%
Telefonica	[...]	[0-5]%	[...]	[0-5]%
DigitalOcean	[...]	[0-5]%	[...]	[0-5]%
Other competitors	[...]	[5-10]%	[...]	[5-10]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Annex II.C.1.1., Table 4.

(161) **Table 33** below presents worldwide revenue-based market share estimates for the Parties in 2023 and 2024 in the markets for IaaS, PaaS and IaaS+PaaS. The market share estimates in IaaS + PaaS are obtained by adding the revenues, and market size, in the IaaS segment, as reported in the Gartner Services 2024 Report, and the PaaS segment, as reported in the Gartner Platform as a Service Market Share 2024 report. ([122])

Table 33: Google unadjusted revenues and shares in Cloud Infrastructure and Data Analytics according to Gartner (Worldwide, 2023-2024)

Segment	Year	Worldwide		
		Google Revenue (USD)	Google share (%)	Total Market Size (USD Mln)
IaaS	2023	[...]	[5-10]%	[...]
	2024	[...]	[5-10]%	[...]
PaaS	2023	[...]	[5-10]%	[...]
	2024	[...]	[5-10]%	[...]
IaaS+PaaS	2023	[...]	[5-10]%	[...]
	2024	[...]	[5-10]%	[...]

Source: Annex RFI 17 Q 10.1.

([122]) Annex RFI 10 Q 10.1.

(162) Based on the Gartner market share estimates for 2024, Google's market share in the IaaS market segment is [5-10]% worldwide and [10-20]% in Europe. In the PaaS market segment, Google's market share is [5-10]% worldwide. Combining the estimates from the IaaS and the PaaS segments into the IaaS + PaaS market segment, Google's market share is [5-10]% worldwide.

(163) The Notifying Party also submitted adjusted market shares, comparing Google's actual revenues against the available Gartner total market sizes. These estimates are presented in **Table 34** below.

Table 34: Google adjusted shares in Cloud Infrastructure and Data Analytics according to Gartner (Worldwide, 2023-2024)

Segment	Year	Worldwide		
		Google Revenue (USD)	Google share (%)	Total Market Size (USD Mln)
IaaS	2023	[...]	[5-10]%	[...]
	2024	[...]	[5-10]%	[...]
PaaS	2023	[...]	[5-10]%	[...]
	2024	[...]	[10-20]%	[...]
IaaS+PaaS	2023	[...]	[5-10]%	[...]
	2024	[...]	[10-20]%	[...]

Source: Annex RFI 17 Q 12.1.

(164) Based on the adjusted market shares, combined Google's actual revenues with Gartner's market size estimates, the Parties' combined worldwide market shares in 2024 are [5-10]% in IaaS, [10-20]% in PaaS and [10-20]% in IaaS+PaaS.

(165) The Notifying Party submits that its market share on a potential segmentation of the market for cloud infrastructure and data analytics for AI workloads would not materially differ from the market shares for the overall market for cloud infrastructure and data analytics, as presented above according to Gartner and IDC. ([123])

(166) Given the lack of Gartner market share estimates for the Parties' competitors in the market for IaaS+PaaS in 2024, the competitive assessment relies on the market share estimates based on IDC data.

5.3.3. Generative AI

(167) The Notifying Party submitted revenue-based market shares estimates for the generative AI models market, worldwide and in Europe, based on data from Gartner. In addition, the Notifying Party provided revenue-based market share data for the potential market segment of specialised generative AI, also worldwide and in Europe.

(168) As set out in above in Section 5.3.1.2.1, Gartner covers the region encompassing the EEA and other European (non-EEA) countries, and it does not provide EEA-specific market share data. However, the Notifying Party submits that EEA-wide market shares would not be materially different from those in Europe given the global nature of demand and supply and that there are no significant differences

([123]) Parties' response to RFI 19, Question 1.

in the distribution of business among suppliers in the EEA and in (non-EEA) countries.

(169) **Table 35** and **Table 36** below present the worldwide and Europe-wide revenue-based market share estimates for the Parties and their main competitors in 2023 and 2024 in the market for generative AI models, as reported in the Gartner Enterprise Software Tracker 2024.

Table 35: Google's and its competitors' revenues and shares in the market for generative AI models according to Gartner (Unadjusted, Worldwide, 2023-2024)

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[10-20]%	[...]	[20-30]%
OpenAI	[...]	[40-50]%	[...]	[20-30]%
Anthropic	[...]	[5-10]%	[...]	[10-20]%
Mistral AI	[...]	[0-5]%	[...]	[5-10]%
Midjourney	[...]	[0-5]%	[...]	[0-5]%
Databricks	[...]	[0-5]%	[...]	[0-5]%
Alibaba	[...]	[0-5]%	[...]	[0-5]%
Cohere	[...]	-	[...]	[0-5]%
Tencent	[...]	-	[...]	[0-5]%
Reka AI	[...]	[0-5]%	[...]	[0-5]%
Meta AI	[...]	-	[...]	[0-5]%
xAI	[...]	-	[...]	[0-5]%
Microsoft	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[10-20]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 34.

Table 36: Google's and its competitors' revenues and shares in the market for generative AI models according to Gartner (Unadjusted, Europe, 2023-2024)

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	[...]	[10-20]%	[...]	[20-30]%
OpenAI	[...]	[40-50]%	[...]	[20-30]%
Anthropic	[...]	[0-5]%	[...]	[0-5]%
Mistral AI	[...]	[5-10]%	[...]	[30-40]%
Midjourney	[...]	-	[...]	-
Databricks	[...]	[0-5]%	[...]	[0-5]%

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Alibaba	[...]	-	[...]	-
Cohere	[...]	-	[...]	-
Tencent	[...]	-	[...]	-
Reka AI	[...]	-	[...]	-
Meta AI	[...]	-	[...]	-
xAI	[...]	-	[...]	-
Microsoft	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[30-40]%	[...]	[5-10]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 34

(170) Based on the Gartner market share estimates for 2024, the Parties' combined market share for generative AI is [20-30]% worldwide and [20-30]% in Europe.

5.3.3.1. Specialised generative AI

(171) The Notifying Party submitted revenue-based market share estimates for the potential market for specialized generative AI worldwide and in Europe based on data from Gartner. As set out above, in Section 5.3.3, Gartner does not provide EEA-specific market shares data. However, the Notifying Party submits that EEA-wide market shares would not be materially different from those in Europe.

(172) **Table 37** and **Table 38** below present the worldwide and Europe-wide revenue-based market share estimates for the Parties and their main competitors in 2023 and 2024 in the potential market for specialized generative AI, as reported in the Gartner Enterprise Software Tracker.

Table 37: Google's and its competitors' revenues and shares in specialized generative AI according to Gartner (Unadjusted, Worldwide, 2023-2024)

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[20-30]%**	**[...]**	**[30-40]%**
Tencent	[...]	[0-5]%	[...]	[10-20]%
OpenAI	[...]	[40-50]%	[...]	[10-20]%
Mistral AI	[...]	[0-5]%	[...]	[5-10]%
Databricks	[...]	[0-5]%	[...]	[5-10]%
NVIDIA	[...]	[0-5]%	[...]	[0-5]%
Reka AI	[...]	[0-5]%	[...]	[0-5]%
Stability AI	[...]	[0-5]%	[...]	[0-5]%
Cohere	[...]	[0-5]%	[...]	[0-5]%

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
01.AI	[...]	[0-5]%	[...]	[0-5]%
Hugging Face	[...]	[0-5]%	[...]	[0-5]%
Microsoft	[...]	[0-5]%	[...]	[0-5]%
Amazon	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[20-30]%	[...]	[0-5]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 38

Table 38: Google's and its competitors' revenues and shares in specialized generative AI according to Gartner (Unadjusted, Europe, 2023-2024)

Vendor	2023		2024	
	Revenue (USD M)	Share (%)	Revenue (USD M)	Share (%)
Google	**[...]**	**[30-40]%**	**[...]**	**[30-40]%**
Tencent	[...]	[0-5]%	[...]	[0-5]%
OpenAI	[...]	[40-50]%	[...]	[10-20]%
Mistral AI	[...]	[0-5]%	[...]	[40-50]%
Databricks	[...]	[0-5]%	[...]	[0-5]%
NVIDIA	[...]	[0-5]%	[...]	[0-5]%
Reka AI	[...]	[0-5]%	[...]	[0-5]%
Stability AI	[...]	[0-5]%	[...]	[0-5]%
Cohere	[...]	[0-5]%	[...]	[0-5]%
01.AI	[...]	[0-5]%	[...]	[0-5]%
Hugging Face	[...]	[0-5]%	[...]	[0-5]%
Microsoft	[...]	[0-5]%	[...]	[0-5]%
Amazon	[...]	[0-5]%	[...]	[0-5]%
Others	[...]	[20-30]%	[...]	[0-5]%
Total	**[...]**	**100.0%**	**[...]**	**100.0%**

Source: Form CO, Table 38

(173) Based on the Gartner market share estimates for 2024, the Parties combined market share in the potential market for specialized generative AI is [30-40]% worldwide and [30-40]% in Europe.

5.4. Horizontal effects

5.4.1. Legal framework

(174) The Horizontal Merger Guidelines ([124]) describe two main ways in which horizontal mergers may significantly impede effective competition, in particular, by creating or strengthening a dominant position: (i) by eliminating important competitive constraints on one or more firms, which consequently would have increased market power, without resorting to coordinated behaviour (non-coordinated effects); or (ii) by changing the nature of competition in such a way that firms that previously were not coordinating their behaviour, are significantly more likely to coordinate and raise prices or otherwise harm effective competition (coordinated effects).

(175) A merger giving rise to horizontal non-coordinated effects might significantly impede effective competition by creating or strengthening the dominant position of a single firm, one which, typically, would have an appreciably larger market share than the next competitor post-merger. Moreover, also mergers that do not lead to the creation of or the strengthening of a single firm's dominant position may create competition concerns under the substantive test set out in Article 2(2) and Article 2(3) of the Merger Regulation. Regarding mergers in oligopolistic markets, the Merger Regulation clarifies that 'under certain circumstances, concentrations involving the elimination of important competitive constraints that the merging parties exerted upon each other, as well as a reduction of competitive pressure on the remaining competitors, may, even in the absence of a likelihood of coordination between the members of the oligopoly, result in a significant impediment to effective competition.' ([125])

(176) The Horizontal Merger Guidelines list a number of factors which may influence whether or not significant horizontal non-coordinated effects are likely to result from a merger, such as the large market shares of the merging firms, the fact that the merging firms are close competitors, the limited possibilities for customers to switch suppliers, or the fact that the merger would eliminate an important competitive force. Not all those factors need to be present to make significant non-coordinated effects likely and it is not an exhaustive list. ([126])

5.4.2. Horizontally affected markets

(177) As previously mentioned, the Transaction gives rise to one horizontally affected market: the potential worldwide market for CSPM. Nevertheless, the Commission's market investigation also focused on the assessment of competitive dynamics in the CNAPP market, even though it is not an affected market based on the available market shares. The Commission has investigated this potential market further given that some competitors and customers during pre-notification calls suggested that Wiz may have a more important position on that market than the available market shares may suggest. ([127])

([124]) Horizontal Merger Guidelines, paragraph 22.

([125]) Merger Regulation, recital 25. Similar wording is also found in paragraph 25 of the Horizontal Merger Guidelines.

([126]) Horizontal Merger Guidelines, paragraph 26.

([127]) As shown in Section 5.3.1, the combined market shares of the Parties in the overall security software market are below 2%. The Commission will therefore not separately assess this horizontal overlap arising from the Transaction.

5.4.3. CNAPP

5.4.3.1. The Notifying Party's views

(178) The Notifying Party submits that under IDC's segmentation, the Parties' activities overlap only in CNAPP, however, the IDC data makes clear that the Parties' combined activities in this space are limited with a combined worldwide market share of [5-10]% and a combined Europe-wide market share of [10-20]% in value. ([128]) The Notifying Party submits that these shares overstate the Parties' actual revenues and therefore, IDC's value-based shares provide a conservative view of the Parties' positions in the CNAPP market. ([129])

(179) Given the modest combined share, the IDC functional market for CNAPP does not constitute an affected market in view of market shares calculated in value. The Parties also provided an analysis of proxies for volume-based market shares which remained below [0-5]%. However, the Notifying Party submits that IDC's value-based approach is more representative of the CNAPP market and does not understate the Parties' competitive position in the market, given that their products are revenue-generating, not part of a bundle or offered for free, and are not priced materially below other offerings in the market. ([130])

(180) The Notifying Party submits that the Transaction does not raise competition concerns in the potential market for CNAPP either globally or in the EEA for the following reasons.

(181) First, the Notifying Party submits that the provided market shares do not understate Wiz's market position and certainly not to an extent that could suggest a significant degree of market power. For Wiz to have even a 30% share – which would not in itself suggest market power – all 20 publicly reported total market size estimates available to the Parties would have to be overestimated by a factor of at least [market share information], and often much more. ([131])

(182) Second, the Parties are not close competitors as there are significant differences between Wiz's and Google's CNAPPs. Google SCC cannot secure multi-cloud environments and is not an option for customers looking for multi-cloud support. While Google SCCE has some multi-cloud coverage for Azure and AWS (in addition to Google's cloud infrastructure), it has failed to gain traction. In 2024, multi-cloud revenues accounted for [information on the Parties' revenues]% of SCCE's (and less than [information on the Parties' revenues]% of the broader SCC(E)) revenue. ([132]) By contrast, Wiz developed its CNAPP as a natively multi-cloud tool from the start and it is used by customers as one. Wiz considers [information on the Parties' assessment of their competitors] to be its closest [information on the Parties' assessment of their competitors] competitors. Google is [information on the Parties' assessment of their competitors]. ([133])

(183) The Notifying Party submitted diversion ratios between the Parties based on Wiz's win-loss data. ([134]) In the first quarter of 2025, the diversion ratio between the Parties, estimated as the number of lost contract renewals from Wiz to Google

([128]) Form CO, paragraphs 20-21.
([129]) Form CO, paragraphs 179-180.
([130]) Form CO, paragraphs 183-186.
([131]) Annex IV.B.7 to the Form CO.
([132]) Form CO, paragraph 203.
([133]) Form CO, paragraph 203.
([134]) Annex 5.5.1. to the Form CO. Wiz doesn't [information on Wiz's win-loss data]. However, Wiz tracks [information on Wiz's win-loss data].

SCC(E) over the total number of lost contract renewals, was [information on Wiz's win-loss data]% in terms of the number of opportunities and [information on Wiz's win-loss data]% in terms of total annual contract value, and in the fiscal year of 2025, the estimated diversion ratio was [information on Wiz's win-loss data]% in terms of opportunities and [information on Wiz's win-loss data]% in terms of annual contract value. However, in the calendar year of 2024, the estimated diversion ratio was [information on Wiz's win-loss data]% in terms of opportunities and [information on Wiz's win-loss data]% in terms of contract value, and [information on Wiz's win-loss data]% and [information on Wiz's win-loss data]% across all years from 2020 to 2025. ([135]) The Notifying Party submits that the accuracy of this data is limited given its scope, ([136]) and the reliance on human reporting, information provided by customers and non-mandatory fields. ([137]) In particular, the Notifying Party submits that the diversion ratios between Wiz and Google SCC(E) are [information on Wiz's win-loss data]. ([138]) In the fiscal year of 2025, there were only [information on Wiz's win-loss data] contract renewal opportunities lost by Wiz where Google SCC(E) is the identified competitor. Further, based on Google's records, only [information on Google's win-loss data] out of these [information on Wiz's win-loss data] opportunities did actually switch to SCCE(E). ([139]) Taking this into account, the recalculated diversion ratio in the fiscal year of 2025 is [information on Wiz's win-loss data]% in terms of opportunities. Regarding the diversion ratio in terms of annual contract value, the Notifying Party submits that [information on Wiz's win-loss data] of the total annual contract value lost to SCC(E) in contract renewals since 2020, which is drastically inflating the diversion ratio. Excluding this specific renewal lost from Wiz to Google would result in a [information on Wiz's win-loss data] and more representative diversion ratio. In fact, according to the Notifying Party, the average contract value of the renewal opportunities lost to SCC(E) is typically [information on Wiz's win-loss data] of the average contract value of all other lost renewals. ([140]) The Notifying Party thus submits that the diversion ratios based on Wiz's win-loss data provides a conservative view of the Parties' closeness of competition in the CNAPP market.

(184) Further, the Notifying Party states that the [information on Google's win-loss data] instances of customers that actually switched from Wiz to SCCE in 2025 are not true multi-cloud customers and do not require the multi-cloud capabilities offered by Wiz. In particular, [information on the Parties' customers' preferences]. ([141]) The Notifying Party therefore submits that only single-cloud customers would consider switching from Wiz to Google SCC(E), suggesting that the Parties are not close competitors.

(185) The Notifying Party also provided diversion ratios between the Parties estimated as the number of opportunities lost where Google SSC(E) [information on Wiz's win-loss data] over the total number of opportunities in Wiz's win-loss data. ([142]) Based on this data, in the first quarter of 2025, the estimated diversion between the Parties was [information on Wiz's win-loss data]% in terms of the number of

([135]) Annex 1 to the Parties' response to RFI 13, Question 1.
([136]) [information on Wiz's win-loss data].
([137]) Annex 5.5.1. to the Form CO and Parties' responses to RFI 9 and RFI 13.
([138]) Annex 5.5.1. to the Form CO. [information on Wiz's win-loss data].
([139]) Parties' response to RFI 13, Question 3.
([140]) Parties' response to RFI 13, Question 3.
([141]) Parties' response to RFI 13, Question 3.
([142]) For which the [information on Wiz's win-loss data] was identified.

opportunities and [information on Wiz's win-loss data]% in terms of annual contract value. ([143])

(186) Third, the Notifying Party submits that it will continue to face competition from numerous CNAPP competitors, including CrowdStrike, Palo Alto Networks and Fortinet (Lacework) that Wiz considers to be among its closest competitors as well as leading solutions from Trend Micro and Microsoft. ([144])

(187) The Notifying Party submitted win rates against competitors, reflecting the share of opportunities Wiz won against a specific competitor, when considering only opportunities in which this competitor was identified as the [information on Wiz's win-loss data]. However, the Notifying Party submits that these win rates are heavily skewed by the limited reporting of opportunities and competitor information in the [information on Wiz's win-loss data]. In addition, the Notifying Party argues that the competitor information recorded in the [information on Wiz's win-loss data] is unreliable. In particular, Wiz's sales team can select [information on Wiz's win-loss data], which is difficult to validate. ([145]) As a result, competitors [information on Wiz's win-loss data] may also have participated in a given opportunity, and the solution ultimately adopted by the customer may differ from the one identified. Moreover, the identified [information on Wiz's win-loss data] may not have actually competed for the opportunity. Further, sales teams are more likely to record competitor information in opportunities won than for opportunities lost. In fact, Wiz's sales team recorded the company they won against in ca. [information on Wiz's win-loss data]% of won opportunities, but the company they lost to in only ca. [information on Wiz's win-loss data]% of lost opportunities. ([146]) When comparing the sales opportunities won by Wiz against all sales opportunities in the database, Wiz won [information on Wiz's win-loss data]% in terms of the number of opportunities and [information on Wiz's win-loss data]% in terms of annual contract value. ([147]) Therefore, the Notifying Party considers that the win rates against each competitor materially overstate Wiz's competitive strength.

(188) Fourth, the Notifying Party submits that Wiz is not a 'must-have' product. Wiz does not have unique capabilities compared to CNAPP competitors that would make it a must-have CNAPP. Wiz is not even the largest player, and its rivals include sophisticated cloud-security companies including Palo Alto Networks, CrowdStrike, Orca Security and Fortinet (Lacework). ([148])

(189) Fifth, the CNAPP market is growing rapidly, and the Notifying Party expects the expansion to continue. There have been significant examples of entry in recent years including Wiz (2020), Palo Alto Networks (2021), Orca (2022), Uptycs (2022), Upwind (2023), Sysdig (2023), and Sweet Security (2024) among others. According to IDC, the CNAPP market is expanding rapidly, and has grown from USD 2.7 billion in 2022 to USD 5.2 billion in 2024. IDC forecasts the global CNAPP market to grow from USD 6.6 billion in 2025 to USD 15.0 billion in 2029, at a compound annual growth rate of 23.0%. Given the nascency of the

([143]) Annex 2 – Q3 to the Parties' response to RFI 13.
([144]) Form CO, paragraph 23. All these market shares reflect IDC's estimates for calendar year 2024.
([145]) Annex 5.5.1. to the Form CO and the Parties' response to RFI 3, Question 23.
([146]) Parties' response to RFI 9.
([147]) Annex 1 to the Parties' response to RFI 13, Question 1.
([148]) Annex IV.B.7, Form CO.

market, the Parties expect it to continue to develop with existing and new players. ([149])

(190) Sixth, the Notifying Party submits that the combined shares will remain modest even on the basis of the Parties' aspirational forward-looking growth projections. Applying [forward-looking assumptions from Google's deal valuation] to the IDC market size forecast results in a modest combined 2029 CNAPP share of [forward-looking market-share projections]%, with an increment of [forward-looking market-share projections]%. However, this projection represents highly conservative estimates and is likely to significantly overstate Google's expected market position absent the Transaction. This is because [information concerning Google's SCC/SCCE revenue projections]. ([150])

5.4.3.2. The Commission's assessment

(191) First, according to the IDC data, the Parties' combined shares in the potential CNAPP market are small with a combined worldwide market share of [5-10]% and a combined EEA-wide market share of [10-20]% in value. ([151]) Even though there are some doubts as to reliability of the data and as to whether it correctly represents Wiz's market position in the CNAPP market, is it unlikely that Wiz's share is so significant that it would confer a significant degree of market power. In that respect, the Notifying Party submitted that it had undertaken a thorough exercise by reviewing 20 publicly reported total market size estimates available to the Parties. ([152])

(192) Second, Google's CNAPP offering will only modestly increase Wiz's position. The increment contributed by Google in the potential CNAPP market amounts to [0-5]% worldwide and [0-5]% in the EEA.

(193) Third, the merged entity will continue to compete with a large number of CNAPP suppliers, including CrowdStrike ([5-10]% globally and [5-10]% in the EEA), Palo Alto Networks ([5-10]% globally and [5-10]% in the EEA), Check Point ([0-5]% globally and [5-10]% in the EEA), Fortinet (Lacework) ([0-5]% globally and [0-5]% in the EEA) as well as Trend Micro ([5-10]% globally and [10-20]% in the EEA) and Microsoft ([10-20]% globally and [10-20]% in the EEA).

(194) In this regard, respondents (customers, CNAPP competitors and competing cloud infrastructure providers) to the market investigation confirmed that, in addition to Google, there are many suppliers competing with Wiz's Wiz Cloud, including Amazon, CrowdStrike, Fortinet, Microsoft, Orca Security, Palo Alto Networks, SentinelOne, Sysdig, Tenable and other. ([153])

(195) The majority of customers and CNAPP competitors expressing an opinion considered that the current level of competition on a potential market for CNAPP is high or very high. ([154]) For example, one customer explained that the CNAPP market is experiencing high competition, with numerous established vendors and

([149]) Form CO, paragraphs 204-208.
([150]) Form CO, paragraphs 210-214.
([151]) In this section, given that IDC includes the data for "Europe" and not the EEA, the Commission has used the data for "Europe" as a proxy for EEA-wide data.
([152]) As explained in further detail above, the Notifying Party argues that the numbers reported in IDC and Gartner market shares are overstated. Please refer to Section 5.3 for adjusted market shares.
([153]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.1.
([154]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.7; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.7.

innovative startups actively developing and enhancing cloud-native security platforms. ([155]) Similarly, a CNAPP competitor explained that 'The market is fast-moving, with frequent innovation and acquisitions, and most solutions offer overlapping capabilities such as CSPM, CWPP, and CIEM. This results in strong competition on features, pricing, and integration, making differentiation challenging for vendors.' ([156]) One customer explained that 'The cloud security landscape is evolving at an unprecedented pace. As cloud workloads continue to expand and new capabilities are introduced frequently, organizations need robust tools to maintain visibility and enforce controls that secure these environments', while another one noted that 'the market is very dynamic with a fast-changing competitive landscape and many players.' ([157]) Similarly, a customer echoes that, by explaining that the CNAPP market is characterised by active competition and a number of capable suppliers with substitutable offerings. ([158]) One customer explained that 'there appear to be multiple, strong offerings in the market from well-established companies. Some companies are good at a narrow set of sub-components while others are better with some solution sets.' ([159])

(196) The CNAPP market is also novel, fast-paced and characterised by a race of quality and innovation between the main suppliers. ([160]) A few respondents mention Wiz as a particularly innovative player; however, others mention CrowdStrike, Palo Alto Networks, Microsoft, Orca Security, Tenable, Upwind, ARMO, Aqua Security, KubeArmor, JupiterOne, Aikido Security, Qualys, SentinelOne, Sysdig or Trend Vision One as particularly innovative suppliers. ([161])

(197) Nonetheless, when ranking the different providers in terms of strength and quality of the CNAPP tools offered by each company, the majority of customers and CNAPP competitors ranked Wiz as first. ([162]) In addition, the majority of customers and CNAPP competitors expressing an opinion indicated that Wiz Cloud has features that other CNAPP providers do not have. ([163]) Respondents mentioned e.g., the following features: clear and user-friendly interface; agent list topology and attack path analysis; ability to classify and prioritize cloud vulnerabilities based on deployment and infrastructure locations; end to end visibility from exposure perspective; the correlation of multiple risk signals across vulnerabilities, configurations, identities and exposure, or sophisticated cross-cloud CSPM layer. ([164]) However, all of Palo Alto Networks, Orca Security, Fortinet or CrowdStrike offer similar functionalities with regard to (i) risk

([155]) Respondent to Questionnaire 3 - Phase I market investigation – Customers, question E.A.7.1.
([156]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.A.7.1.
([157]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.7.1.
([158]) Respondent to Questionnaire 3 - Phase I market investigation – Customers, question E.A.7.1.
([159]) Respondent to Questionnaire 3 - Phase I market investigation – Customers, question E.A.7.1.
([160]) Respondent to Questionnaire 3 - Phase I market investigation – Customers, question E.A.8.1.
([161]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.8.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.8.1; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.8.1.
([162]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.3; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.3.
([163]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.4; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.4.
([164]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.4.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.4.1; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.4.1.

prioritisation and correlation ([165]), (ii) agent-based and agentless approaches ([166]), (iii) multi-cloud CSPM ([167]), and (iv) end-to-end visibility. ([168])

(198) Further, the estimated win rates against competitors submitted by the Parties, are intended to reflect the strength of Wiz against each specific competitor. According to this data, in 2024, Wiz's win rates against competitors, in opportunities where both Wiz and the relevant competitor participated in ([169]), reach [information on Wiz's win-loss data]% in a number of opportunities and [information on Wiz's win-loss data]. However, when considering the share of sales opportunities won by Wiz over all the sales opportunities in the Database, Wiz's win rate is [information on Wiz's win-loss data]%, which adds up to [information on Wiz's win-loss data]% in contract value. ([170]) As such, the win rates are likely to be skewed due to the limited scope of the [information on Wiz's win-loss data] and the unreliability of the competitor information. In particular, [information on Wiz's win-loss data]. In addition, [information on Wiz's win-loss data]. ([171])

([165]) See, for example: Palo Alto's attack path analysis offerings (See Palo Alto Networks, CSPM - Palo Alto Networks, available at: https://www.paloaltonetworks.com/prisma/cloud/cloud-security-posture-management#:~:text=%2A%20); Orca's attack path analysis offerings (See Orca Security, Attack Path Analysis | Orca Security, available at: https://orca.security/glossary/attack-path-analysis/#:~:text=1,entry%20points%20and%20showing%20how); Fortinet's attack path analysis offerings (See Fortinet, Attack Path Analysis | Fortinet, available at: https://www.fortinet.com/uk/products/forticnapp/attack-path-analysis); CrowdStrike's attack path analysis offerings (See CrowdStrike, CrowdStrike Traces Attack Paths to Sensitive Data in the Cloud, available at: https://www.crowdstrike.com/en-us/blog/crowdstrike-traces-attack-paths-sensitive-data-cloud/#:~:text=The%20Attack%20Path%20Analysis%20dashboard,at%20resources%20storing%20sensitive%20data)

([166]) See, for example: Palo Alto introduced agentless scanning for Prisma Cloud in July 2024 (See Palo Alto Networks, Prisma Cloud's Innovative Agentless Scanning, CNAPP, available at: https://live.paloaltonetworks.com/t5/community-blogs/prisma-cloud-s-innovative-agentless-scanning/ba-p/592846)); Orca as the first platform to offer agentless capabilities (See Orca Security, Agentless vs. Agent-Based Security | Orca Security, available at: https://orca.security/resources/blog/agentless-vs-agent-based-security/); Fortinet's agentless capabilities (See Fortinet, Agentless mode | FortiPAM 1.8.0, available at: https://docs.fortinet.com/document/fortipam/1.8.0/administration-guide/354559/agentless-mode); CrowdStrike as the industry's most comprehensive agent-based and agentless platform (See CrowdStrike, CrowdStrike Falcon Cloud Security Delivers the Future of CNAPP, available at: https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-cloud-security-delivers-future-of-cnapp/).

([167]) For example, Palo Alto's Prisma cloud offers an evidence graph to 'provide risk clarity by visualizing attack paths' (See Palo Alto Networks, CSPM - Palo Alto Networks, available at: https://www.paloaltonetworks.com/prisma/cloud/cloud-security-posture-management#:~:text=%2A%20; CrowdStrike offers 'real-time attack path visualization' (See CrowdStrike, CrowdStrike Falcon® Exposure Management, available at: https://www.crowdstrike.com/en-us/platform/exposure-management/attack-path-analysis/#:~:text=Real).

([168]) This is evident from rival CNAPPs' marketing: Palo Alto's Prisma Cloud 'secures applications from code to cloud and across multicloud environments' (See Palo Alto Networks, Shift Happens, Be Ready With Code-to-Cloud, available at: https://www.paloaltonetworks.com/blog/2022/09/code-to-cloud-cnapp/); Aqua Security confirms that its CNAPP adopts a Code-to-Cloud approach (See Aqua Security, Code to Cloud & Cloud to Code: Cloud Native Security, Reloaded, available at: https://www.aquasec.com/cloud-native-academy/cspm/code-to-cloud/); and Fortinet (Lacework) markets FortiCNAPP as a Code-to-Cloud solution (See Fortinet, Fortinet Strengthens Code-to-Cloud Security, available at: https://www.fortinet.com/uk/corporate/about-us/newsroom/press-releases/2025/fortinet-strengthens-code-to-cloud-security-with-cnapp-enhancements-and-aws-marketplace-expansion).

([169]) Based on the [information on Wiz's win-loss data].

([170]) Annex 1 to the Parties' response to RFI 13, Question 1.

([171]) Parties' response to RFI 9.

Further, [information on Wiz's win-loss data]. ([172]) ([173]) As a result, the identified competitor may not reflect the full set of alternatives considered by the customer or the solution ultimately adopted by the customer. Therefore, loss rates of Wiz against each competitor do not reflect the relative strength of the competitor, as losses may be attributable to other competing solutions. Given the limitations of the data, Wiz's win rates do not indicate a strong competitive position and are consistent with the finding that Wiz will continue to face strong competition from alternative CNAPPs.

(199) Fourth, the Parties are not close competitors. The majority of customers and competitors expressing an opinion confirmed that Wiz Cloud and Google SCCE focus on different customer needs. ([174]) For example, one competing cloud infrastructure provider explained that Google SCCE is primarily optimized for securing workloads running on Google's cloud infrastructure. While both Wiz's and Google's tools include certain similar functional elements, such as posture management and threat detection, differences in cloud coverage, deployment model, and customer use cases mean that they are not generally viewed as close substitutes, particularly by multi-cloud customers. ([175]) In addition, a CNAPP competitor explained that Wiz and Google's SCCE do compete where customers want cloud risk and security visibility, but Wiz is more multi-cloud and platform-agnostic with broader CNAPP positioning, while SCCE is the strongest within the Google Cloud ecosystem. Many enterprise buyers evaluate both based on their cloud footprint and architectural priorities rather than choosing one purely as a substitute for the other. ([176]) Many customers also noted that Wiz and Google SCCE focus on different customer needs, as Wiz has been designed as a cloud-agnostic platform used to provide a unified security posture across multiple cloud service providers, while Google SCCE is a native tool optimised for Google's cloud infrastructure and its coverage for other clouds is not as complete as Wiz's. ([177])

(200) Further, the estimated diversion ratios between the Parties, estimated as the lost contract renewals from Wiz to Google SCC(E) over the total number of lost contract renewals in Wiz's win-loss data, do not suggest that the Parties are close competitors. The high diversion ratios of [information on Wiz's win-loss data]%, based on the number of opportunities, and [information on Wiz's win-loss data]%, based on the annual contract value, between Wiz and Google SCC(E) in the first quarter of 2025 ([178]) can be explained by the limited sample size and accuracy of the competitor information. Accordingly, considering both contract renewals and new business, the diversion between the Parties, estimated as the number of opportunities lost where Google SCC(E) was [information on Wiz's win-loss data] over the total number of opportunities in Wiz's win-loss data ([179]), materially fall to [information on Wiz's win-loss data]%, in terms of

([172]) Parties' response to RFI 3, Question 23.
([173]) Annex 5.5.1. to the Form CO.
([174]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.9; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.9; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.9.
([175]) Respondent to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.9.1.
([176]) Respondent to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.9.1
([177]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.9.1.
([178]) Annex RFI 13 Question 1.
([179]) For which the competing solution was identified.

opportunities, and [information on Wiz's win-loss data]% in terms of annual contract value. ([180]) Moreover, the estimated diversion ratio between the Parties in the calendar year of 2024 was [information on Wiz's win-loss data]%, in terms of opportunities, and [information on Wiz's win-loss data]% in terms of contract value, and [information on Wiz's win-loss data]% and [information on Wiz's win-loss data]% across all years from 2020 to 2025 ([181]), which does not suggest the Parties' to be close competitors.

(201) Fifth, switching CNAPP suppliers is possible. The majority of customers and competitors expressing an opinion consider that switching CNAPP providers is complex and needs some time but is a real option. ([182]) The market investigation shows that such a switch could take between 1 month and more than 1 year, depending on the level of the customer's technical integration with the CNAPP provider as well as the size and the complexity of the customer's cloud environment. ([183]) For instance, one competing cloud infrastructure provider explained that customers need time to plan the migration, set up integrations with multiple cloud environments, replicate or redesign security policies, and ensure data continuity for compliance and reporting purposes. The transition also requires retraining teams on the new platform, testing configurations, and validating that the new tool covers all necessary workloads and compliance requirements. While smaller environments may switch faster, most enterprise-scale deployments face enough complexity that a multi-month timeline is realistic. ([184]) Some CNAPP competitors consider that switching CNAPP providers typically takes 4-6 months, especially if this concerns a complex migration involving agent deployments or large environments. However, less complex or primarily agentless migrations can often be completed in under 4 months. Customers usually align the switch with renewal cycles and internal change-management timelines, making it a deliberate but achievable transition rather than a quick swap. ([185])

(202) Indeed, there are examples of Wiz's customers that have moved away to another CNAPP provider. The absolute number of Wiz customers churning or contracting their contract value ([186]) has [information on the Parties' customers' purchasing decisions] over time on both a worldwide basis (from [information on the Parties' customers' purchasing decisions] in FY2024 to [information on the Parties' customers' purchasing decisions] in FY2026) and in the EEA (from [information on the Parties' customers' purchasing decisions] in FY2024 to [information on the Parties' customers' purchasing decisions] in FY2026). ([187])

(203) Sixth, new entry in the CNAPP market is likely. The majority of customers and CNAPP competitors expressing an opinion consider that it is likely that a new

([180]) Annex RFI 13 Question 3.
([181]) Annex RFI 13 Question 1.
([182]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.13; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.14; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.13.
([183]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.14.
([184]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.14.1.
([185]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.15.1.
([186]) Churned customers are customers that fully discontinued their use of Wiz's products. Contracted customers are customers that continue with Wiz but at a reduced level of spend relative to their previous contractual position.
([187]) Parties' response to RFI 10, Question 15.

provider could launch a competitive CNAPP offering in the next two years. ([188]) Respondents mention Upwind, Sweet Security and Aikido Security as examples of recent entry. ([189]) In addition, a CNAPP competitor explains that CNAPP is a reasonably straightforward extension for vendors already in the CSPM or the virtual machine space. Some vendors in the Security Development Operations space would also be well placed for this type of extension. ([190]) Another CNAPP competitor pointed out that the increasing prevalence of AI-driven workloads and tools is also disrupting the market and creating opportunities for new and existing entrants. ([191]) This is also confirmed by one of Wiz's customers who explained that the rapid evolution of AI-driven automation and analytics tools allows entrants to quickly match or even surpass the capabilities of established providers, potentially accelerating innovation and market entry within the CNAPP space. ([192]) Overall, many customers confirmed that CNAPP is a rapidly growing market, with ample opportunities for innovation and new entry. ([193])

(204) Finally, the majority of customers and CNAPP competitors expressing an opinion considered that the impact of the Transaction in the CNAPP market would be positive or neutral. ([194]) In addition, the majority of CNAPP competitors and almost all customers consider that the impact of the Transaction on their overall business would be positive or neutral. ([195])

(205) For all the above reasons, the Commission concludes that the Transaction would not raise serious doubts as to its compatibility with the internal market as a result of horizontal effects in the market for CNAPP in the EEA or worldwide.

5.4.4. CSPM

5.4.4.1. The Notifying Party's views

(206) As discussed in Section 4.2.2.2 above, the Notifying Party considers that Gartner's CSPM subsegment does not constitute relevant antitrust markets and that the data Gartner provides within them is not a reliable indication of market shares. ([196]) Regardless of the exact market definition, the Notifying Party submits that the Transaction does not raise competition concerns in the potential market for CSPM either globally or in the EEA for the following reasons.

(207) First, the Notifying Party submits that Gartner suffers from a demonstrable quantitative error: the Gartner Enterprise Software 2024 tracker overstates Google's CSPM revenues by [information on the Parties' revenue data]% (by [information on the Parties' revenue data]) and Wiz's revenues by [information on the Parties' revenue data]% (by [information on the Parties' revenue data])

([188]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.12; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.12.
([189]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.12.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.12.1.
([190]) Respondent to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.12.1.
([191]) Respondent to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.12.1.
([192]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.12.1.
([193]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.12.1.
([194]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question F.2; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question F.2.
([195]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question F.1; replies to Questionnaire 3 - Phase I market investigation – Customers, question F.1.
([196]) Form CO, paragraph 161.

globally. In Europe, it overestimates Google's revenues by [information on the Parties' revenue data]% (by [information on the Parties' revenue data]) and Wiz's revenues by [information on the Parties' revenue data]% (by [information on the Parties' revenue data]). ([197])

(208) Even under the narrowest segmentations presented by Gartner and even using numbers that are demonstrably significantly inflated, the Transaction results in a potential horizontally affected market only in CSPM ([20-30]% worldwide, [20-30]% in Europe). ([198]) Even under Gartner's erroneous revenue allocation, the combined share is moderate, which is well below the levels that could confer a significant degree of market power. ([199])

(209) Second, the Notifying Party submits that numerous competitors will remain post-Transaction. Gartner itself lists 33 players offering a CSPM functionality including: Microsoft (Microsoft Defender), Palo Alto Networks (Prisma Cloud), Amazon (AWS Security Hub) and Tenable (Tenable Cloud Security). ([200])

(210) Third, the Notifying Party considers that Google and Wiz are not close competitors, as set out in more detail in Section 5.4.3.1. Google SCC and Wiz Cloud do not meaningfully compete: Google SCC is limited to securing workloads on Google's own cloud infrastructure and is not a viable option for multi-cloud customers. Google SCCE does offer some multi-cloud functionality; however, its capabilities are limited and have failed to gain traction to date. ([201])

(211) Fourth, the Notifying Party submits that Wiz has many close competitors in CSPM. Rather than being a separate segment, CSPM capabilities are among the core components of a CNAPP. All of Wiz's CNAPP competitors necessarily offer comprehensive CSPM capabilities. ([202])

(212) Fifth, the Notifying Party considers that the Parties' customers are large, sophisticated buyers with substantial in-house IT capabilities, purchasing power, and expertise. They are equipped to switch providers easily. ([203])

5.4.4.2. The Commission's assessment

(213) First, according to the Gartner data, the Parties' combined shares in the potential CSPM market are moderate ([20-30]% worldwide, [20-30]% in the EEA). ([204])([205])

(214) Second, as discussed in Section 5.3.1.2 the merged entity will continue to compete with a large number of suppliers including: Microsoft (Microsoft Defender) ([10-20]% share worldwide and [20-30]% in the EEA), Palo Alto Networks (Prisma Cloud) ([5-10]% share worldwide and [0-5]% in the EEA), Amazon (AWS Security Hub) ([5-10]% share worldwide and [5-10]% in the EEA) and

([197]) Form CO, paragraph 26.
([198]) Form CO, paragraph 28.
([199]) Form CO, paragraph 229.
([200]) Form CO, paragraph 230.
([201]) Form CO, paragraph 231.
([202]) Form CO, paragraph 232.
([203]) Form CO, paragraph 233.
([204]) As explained in further detail above, the Notifying Party argues that the numbers reported in IDC and Gartner market shares are overstated. Please refer to Section 5.3 for adjusted market shares.
([205]) In this section, given that Gartner only includes data for Europe and not the EEA, the Commission has used the data for "Europe" as a proxy for EEA-wide data.

Tenable (Tenable Cloud Security) ([0-5]% share worldwide and [5-10]% in the EEA).

(215) In this regard, respondents (customers, CNAPP and competing cloud infrastructure providers) to the market investigation confirmed that in addition to Google, there are many CSPM suppliers competing with Wiz's Wiz Cloud, including Amazon, CrowdStrike, Fortinet, Microsoft, Orca Security, Palo Alto Networks, SentinelOne, Sysdig, Tenable and others. ([206])

(216) Further, the majority of customers and CNAPP competitors expressing an opinion considered that the current level of competition on a potential market for CSPM is the same as for CNAPP, i.e., high or very high. ([207]) One respondent explained that the level of competition for CSPM is even higher than for CNAPP, as CSPM is more mature, largely commoditised and highly substitutable. By contrast, CNAPP competition is 'high' rather than 'very high' because differentiation still exists around attack-path analysis, identity correlation, and risk prioritization, whereas CSPM by itself competes mostly on price, coverage parity and bundling. ([208])

(217) Nonetheless, when ranking the different providers in terms of strength and quality of the CSPM tools offered by each company, the majority of customers and CNAPP competitors ranked Wiz as first. ([209]) In addition, the majority of customers and competitors expressing an opinion indicated that Wiz's CSPM has features that other CSPM providers do not have. ([210]) Respondents mentioned, for instance, the following features: agent list topology and attack path analysis; clear and user-friendly interface; ability to classify and prioritize cloud vulnerabilities based on deployment and infrastructure locations; end to end visibility from exposure perspective; providing visibility and correlation of risks across cloud configurations, identities, workloads, and network paths or the most sophisticated cross-cloud CSPM layer in the market. ([211]) In particular, one customer explained in detail that Wiz's primary differentiating feature is its security graph, which provides deep, contextualized risk analysis and attack path visualization by correlating insights across the entire cloud stack (infrastructure, identities, data, and workloads) in a unified, agentless platform. ([212]) However, as discussed in Section 5.4.3.2 above, all of Palo Alto Networks, Orca Security, Fortinet or CrowdStrike offer similar functionalities.

(218) As regards innovation, the majority of the market participants that expressed an opinion confirmed that their answer as to whether there are any particularly qualitative or innovative suppliers in the CSPM market would be the same as for

([206]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.1.

([207]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.7.2; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.7.2.

([208]) Respondent to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.7.2

([209]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.5; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.5.

([210]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.6; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.6; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.6.

([211]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.6.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.6.1; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.6.1.

([212]) Respondent to Questionnaire 3 - Phase I market investigation – Customers, question E.A.6.1.

the CNAPP market. ([213]) For CNAPP, a few respondents mentioned Wiz as a particularly innovative player; however, others mention CrowdStrike, Palo Alto Networks, Microsoft Defender, Orca Security, Tenable, Upwind, ARMO, Aqua Security, KubeArmor, JupiterOne, Aikido Security, Qualys, SentinelOne, Sysdig or Trend Vision One as particularly innovative suppliers. ([214]) However, some respondents note that the CSPM market is more mature than CNAPP and the core functionalities are well established, with similar functionalities offered by all major leaders. As a result, CSPM innovation tends to be incremental rather than disruptive. ([215])

(219) Third, as discussed in Section 5.4.3.2 above, the Parties are not close competitors. The majority of customers and competitors expressing an opinion confirmed that Wiz Cloud and Google SCCE focus on different customer needs. ([216])

(220) Fourth, switching CSPM suppliers is possible. Many respondents consider that the cost of the investment and time required to switch from a CSPM supplier would be the same as to switch from a CNAPP supplier, however, many other respondents consider that switching CSPM providers is generally easier and less complex. ([217]) Some CSPM competitors explain that CSPM solutions have a narrower technical scope, require less specialized expertise, and demand fewer internal resources. CSPM tools are more standardized, largely agentless, and less embedded in operational workflows. With fewer integrations, no runtime components, and more commoditized capabilities, switching is more straightforward. ([218]) One customer underlined that even though switching costs may be generally lower than for CNAPP, they can vary significantly depending on the operational processes and the level of integration within the organisation. ([219])

(221) Fifth, new entry in the CSPM market is likely. The majority of customers and CNAPP competitors expressing an opinion confirmed that their views with regard to the likelihood and timeframe of entry in the CSPM market are the same as for CNAPP, namely they consider entry in the CSPM market is also likely within the next two years. ([220]) However, some customers indicated that likelihood and timeliness of entry would be higher for CSPM than for CNAPP, as CSPM is considerably less complex. This is confirmed by a few CNAPP competitors who stated that entry barriers to the CSPM market are lower, which implies that

([213]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.8.2; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.8.2; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.8.2.

([214]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.8.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.8.1; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.8.1.

([215]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.8.2; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.8.2; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.8.2.

([216]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.9; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.9; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.9.

([217]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.13.2; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.14.2; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.A.13.2.

([218]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.14.2.

([219]) Respondent to Questionnaire 3 - Phase I market investigation – Customers, question E.A.13.2.

([220]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.12.2; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.12.2.

narrower-scope vendors can launch faster. Entry is more likely than for CNAPP as CSPM is a more mature and commoditised market with well-defined capability and lower architectural complexity. ([221]) At the same time, a few customers indicated that likelihood of new entry in the CSPM market is lower than CNAPP – standalone CSPM tools are less likely to be released given that all vendors and most customers are moving to CNAPP. ([222])

(222) Finally, the majority of CNAPP competitors and almost all customers consider that the impact of the Transaction on their overall business would be positive or neutral. ([223])

(223) For all the above reasons, the Commission concludes that the Transaction would not raise serious doubts as to its compatibility with the internal market as a result of horizontal effects in the market for CSPM in the EEA or worldwide.

5.4.5. Conclusion

(224) In light of the above, the Commission concludes that the Transaction does not raise serious doubts as to its compatibility with the internal market as a result of any horizontal overlaps between the Parties' activities in the markets for CNAPP and CSPM in the EEA or worldwide.

5.5. Vertical effects

5.5.1. Introduction

(225) The Transaction gives rise to two vertical relationships between the upstream market for cloud infrastructure and data analytics and the downstream market for CNAPP.

(226) First, cloud infrastructure may constitute an input for CNAPP suppliers, as CNAPP suppliers (like all cloud-based software vendors) may use cloud infrastructure providers to host and provide the necessary computing power that supports their services. ([224]) ([225])

(227) Second, in order to run security scans on customers' cloud deployments, a CNAPP collects metadata on customers' cloud environments. The Transaction

([221]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.A.12.2.

([222]) Respondent to Questionnaire 3 - Phase I market investigation – Customers, question E.A.12.2.

([223]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question F.1; replies to Questionnaire 3 - Phase I market investigation – Customers, question F.1.

([224]) As shown in Section 5.3.1.2, Wiz does not have a market share exceeding 30% in the potential market for CSPM. The Commission will not separately assess the vertical relationship between the market for cloud infrastructure and data analytics on the one hand and the market for CSPM on the one hand, as the results of the market investigation pointed out that there is no material difference in their responses when distinguishing between CNAPP and CSPM respectively. Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), questions E.C.2.2, E.C.3.2, E.C.4.2, E.C.5; replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), questions E.C.A.1.2, E.C.A.2.2, E.C.A.3.2, E.C.A.4, E.C.B.1.2, E.C.B.2.2, E.C.B.3.2, E.C.B.4.2, E.C.B.5; replies to Questionnaire 3 - Phase I market investigation – Customers, questions E.C.A.1.2, E.C.A.2.2, E.C.A.3.2, E.C.A.4, E.C.B.1.2, E.C.B.2.2, E.C.B.3.2, E.C.B.4.2, E.C.B.5.

([225]) As shown in Section 5.3.1, the combined market shares of the Parties in the overall security software market are below 2%. The Commission will therefore not separately assess the vertical relationship between the market for cloud infrastructure and data analytics on the one hand and the market for overall security software on the other.

could provide Google access to data collected by Wiz on how customers use competing cloud environments.

(228) This Decision assesses whether, post-Transaction, the merged entity could foreclose competing CNAPP suppliers through a degradation of access to Google's cloud infrastructure (Section 5.5.3) ([226]), as well as whether Google would obtain access to commercially sensitive information on competing cloud infrastructure providers resulting in a significant impediment to effective competition (Section 5.5.4).

5.5.2. Legal framework

(229) According to the Non-Horizontal Guidelines, ([227]) non-coordinated effects may significantly impede effective competition as a result of a vertical merger if such merger gives rise to foreclosure. Foreclosure occurs where actual or potential competitors' access to supplies or markets is hampered or eliminated as a result of the merger, thereby reducing those companies' ability and/or incentive to compete. ([228]) Such foreclosure may discourage entry or expansion of competitors or encourage their exit. ([229])

(230) The Non-Horizontal Guidelines distinguish between two forms of foreclosure. First, input foreclosure occurs where the merger is likely to raise the costs of downstream competitors by restricting their access to an important input. ([230]) Foreclosure may also take more subtle forms, such as the degradation of the quality of input supplied. In its assessment, the Commission may consider a series of alternative or complementary possible strategies. ([231]) Second, customer foreclosure occurs where the merger is likely to foreclose upstream competitors by restricting their access to a sufficient customer base. ([232])

(231) In assessing the likelihood of an anticompetitive foreclosure scenario, the Commission examines, first, whether the merged entity would have, post-merger, the ability to substantially foreclose access to inputs or customers; second, whether it would have the incentive to do so; and third, whether a foreclosure strategy would have a significant detrimental effect on competition. In practice, these factors are often examined together as they are closely intertwined. ([233])

(232) Pursuant to Article 2(2) of the Merger Regulation, a concentration which would not significantly impede effective competition, in the internal market or in a substantial part of it, shall be declared compatible with the internal market. Conversely, pursuant to Article 2(3) of the Merger Regulation, a concentration which would significantly impede effective competition, in the internal market or

---

([226]) For reasons similar to what is set out in Section 5.5.3, the Commission considers it unlikely that the merged entity will remove competing CNAPPs from Google Cloud Marketplace, as it would make GCP less attractive. Furthermore, as explained in more detail in this Section, competing CNAPPs have many alternatives, including in terms of sales channels, as Google Cloud Marketplace is one of many means of distribution to reach GCP customers. Moreover, a customer that downloads a CNAPP from a rival marketplace can run the same CNAPP on GCP and other cloud environments without needing to repurchase the software. Therefore, the effects of a potential delisting of all other CNAPPs from Google Cloud Marketplace on the market for CNAPP would be minimal.

([227]) Non-Horizontal Guidelines, pages 6-25.

([228]) Non-Horizontal Guidelines, paragraph 18.

([229]) Non-Horizontal Guidelines, paragraph 29.

([230]) Non-Horizontal Guidelines, paragraph 30.

([231]) Non-Horizontal Guidelines, paragraph 33.

([232]) Non-Horizontal Guidelines, paragraph 30.

([233]) Non-Horizontal Guidelines, paragraph 32.

in a substantial part of it, shall be declared incompatible with the internal market. In that regard, it is sufficient for the Commission to establish that the Transaction is likely to lead to a significant impediment of effective competition.

5.5.3. Foreclosure of rival CNAPP providers by imposing discriminatory conditions on their usage of Google's cloud infrastructure

(233) CNAPP suppliers (like all cloud-based software vendors) may use cloud infrastructure providers to host and provide the necessary computing power that supports their services.

(234) This Decision assesses whether the merged entity could impose discriminatory conditions on CNAPP rivals who rely only on Google's cloud infrastructure as an input to provide their own services, thereby leading to their partial foreclosure from the CNAPP market (input foreclosure).

5.5.3.1. The Notifying Party's views

(235) The Notifying Party submits that the merged entity would not have the ability to partially foreclose rival CNAPP providers through the imposition of discriminatory conditions on their usage of Google's cloud infrastructure for the reasons set out below.

(236) First, the Notifying Party submits that Google's cloud infrastructure activities are not an upstream input for CNAPPs. According to the Notifying Party, cloud infrastructure is purchased for a CNAPP's own internal needs and is not a component of any CNAPP solution.

(237) Second, the Notifying Party submits that, the Transaction does not give rise to competition concerns even if public cloud infrastructure were considered an input for CNAPPs. While a number of Wiz's CNAPP rivals – such as Palo Alto Networks and Fortinet – currently host services on Google's cloud infrastructure, Google does not have market power on the market for cloud infrastructure and data analytics as its market shares are well below 30% (worldwide share of [5-10]% and EEA-wide ([234]) share of [5-10]%) ([235]), and well below shares held by AWS (worldwide share of [30-40]% and EEA-wide share of [30-40]%) and Microsoft Azure (worldwide share of [10-20]% and EEA-wide share of [10-20]%). ([236])

5.5.3.2. The Commission's assessment

(238) For the reasons set out below, the Commission considers that the merged entity would not have the ability to partially foreclose rivals in the CNAPP market by imposing discriminatory conditions on their use of Google's cloud infrastructure (input foreclosure). Therefore, given that the conditions under the Non-Horizontal Guidelines are cumulative ([237]), the Commission does not need to take a position of whether the second or third conditions are satisfied.

([234]) In this section, given that IDC only includes data for Europe and not the EEA, the Commission has used the data for "Europe" as a proxy for EEA-wide data.

([235]) As explained in further detail above in Section 5.3, based on the Gartner market share estimates for 2024, Google's market share in the IaaS market segment is [5-10]% worldwide and [10-20]% in Europe. In the PaaS market segment, Google's market share is [5-10]% worldwide. Combining the estimates from the IaaS and the PaaS segments into the IaaS + PaaS market segment, Google's market share is [5-10]% worldwide.

([236]) Form CO, footnote 374.

([237]) Non-Horizontal Guidelines, paragraphs 93-118.

5.5.3.2.1. Ability to foreclose

(239) For the reasons set out below, the Commission considers that the merged entity would not have the ability to foreclose rivals in the CNAPP market by imposing discriminatory conditions on their use of Google's cloud infrastructure (input foreclosure).

(240) For the purposes of this Decision, the Commission considers that Google is behind Amazon and Microsoft in terms of market shares and does not have a significant degree of market power in the market for cloud infrastructure and data analytics at this stage. While market shares show that Google has been benefiting from the highest growth in the market for cloud infrastructure and data analytics, also Microsoft continues to grow, while Amazon's market share is at least stable.

(241) First, the results of the market investigation confirmed that there are alternative providers to Google. As mentioned in Section 5.3.2 above, in 2023, Google had a worldwide market share of [5-10]% and an EEA-wide ([238]) market share of [5-10]% in the market for cloud infrastructure and data analytics. ([239]) Competing providers include Amazon (with a worldwide market share of [30-40]% and an EEA-wide market share of [30-40]%) and Microsoft (with a worldwide market share of [10-20]% and an EEA-wide market share of [10-20]%). ([240])

(242) In the market investigation, the majority of customers and the majority of cloud infrastructure and CNAPP competitors expressing an opinion considered that several companies supply products that compete with Google's cloud infrastructure. Such providers include amongst others Amazon, Microsoft, IBM, Alibaba, Oracle and OVH. ([241])

(243) Further, the majority of customers and CNAPP competitors expressing an opinion considered that competition on the market for cloud infrastructure and data analytics is very high or high, whilst the majority of cloud infrastructure competitors consider competition to be very high, high or moderate at this stage. ([242]) At the same time, some market participants explain that the three hyperscalers are ahead of other cloud infrastructure providers, with Google being behind Amazon and Microsoft. For example, one cloud infrastructure competitor explains that 'global hyperscalers (AWS, Azure, GCP) leading and regional players (Alibaba Cloud, Oracle, IBM, OVH) less relevant.' ([243]) In this context, it should be noted that CNAPP customers generally apply a multi-cloud approach

([238]) In this section, given that IDC only includes data for Europe and not the EEA, the Commission has used the data for "Europe" as a proxy for EEA-wide data.

([239]) As explained in further detail above in Section 5.3, based on the Gartner market share estimates for 2024, Google's market share in the IaaS market segment is [5-10]% worldwide and [10-20]% in Europe. In the PaaS market segment, Google's market share is [5-10]% worldwide. Combining the estimates from the IaaS and the PaaS segments into the IaaS + PaaS market segment, Google's market share is [5-10]% worldwide. In any event, Google's share in all potential segments is below the level that would indicate a significant degree of market power.

([240]) As explained in further detail above in Section 5.3, based on the Gartner market share estimates for 2024, Google's market share in the IaaS market segment is [5-10]% worldwide and [10-20]% in Europe. In the PaaS market segment, Google's market share is [5-10]% worldwide. Combining the estimates from the IaaS and the PaaS segments into the IaaS + PaaS market segment, Google's market share is [5-10]% worldwide.

([241]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.B.1; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.B.1.

([242]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.B.3; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.B.3.

([243]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.B.3.1.

and therefore are a subsegment of cloud customers familiar with combining offers from various cloud service suppliers.

(244) Second, the majority of customers and half of CNAPP competitors expressing an opinion indicated that switching would take more than a year. The majority of customers and CNAPP competitors also considered that switching from one cloud infrastructure provider to another is technically very complex and needs some time. ([244]) Customers and CNAPP competitors alike explained that the complexity of switching depends on, inter alia, the size of the company, how its cloud infrastructure is set up, the services that it is using and the type of workloads. ([245]) Still, customers and CNAPP competitors expressed that switching is not excluded. In this context, it should be noted that CNAPP customers generally apply a multi-cloud approach and therefore are a subsegment of cloud customers familiar with combining offers from various cloud service suppliers.

(245) Finally, the majority of CNAPP competitors and customers expressing an opinion considered that the impact of the Transaction in the market for CANPP would be positive or neutral. ([246])

(246) For the reasons described above, the Commission considers that the merged entity would not have the ability to engage in an input foreclosure strategy as Google does not have a significant degree of market power on the cloud infrastructure and data analytics market.

5.5.4. Access to Wiz's customers' data

(247) Cloud services providers could derive a competitive advantage from their access to certain types of customer data. This Decision assesses whether, as a result of the Transaction, the merged entity would obtain access to commercially sensitive information from Wiz's customers that could allow the merged entity to price less aggressively in the market for cloud infrastructure and data analytics to the detriment of consumers or put competitors at a competitive disadvantage. ([247]) In particular, through Wiz's CNAPP workload scanning tool, Google could get access to information on how Wiz's customers set up their cloud infrastructure (e.g., the cloud infrastructure providers they use, the number of workloads they use per provider or the usage of a given workload per provider). This could potentially lead to a reduction of competition upstream, at the level of cloud infrastructure.

5.5.4.1. Legal framework

(248) Separate from foreclosure, as set out in paragraph 78 of the Non-Horizontal Merger Guidelines, non-horizontal non-coordinated effects can also arise when

([244]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.B.9.
([245]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.B.9.1 and E.B.10.
([246]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question F.3; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question F.3; replies to Questionnaire 3 - Phase I market investigation – Customers, question F.3.
([247]) CISPE (Cloud Infrastructure Services Providers in Europe) initially voiced a concern on its website that Google could benefit from unfair insights into customer data, behaviour and usage metrics on third party clouds (see Surely Not Again, European Commission must avoid making the same mistakes as with Broadcom when examining Google's acquisition of Wiz, available at: https://www.cispe.cloud/surely-not-again/). However, based on the discussion during the Commission's meeting with CISPE's Secretariat and the limited level of concern conveyed by CISPE members to CISPE's Secretariat in response to the latter's subsequent consultation with them , CISPE decided not to submit a formal response to the Commission's inquiry.

the merged entity, by vertically integrating, gains access to commercially sensitive information regarding the upstream or downstream activities of rivals. ([248])

(249) This theory of harm differs from the vertical non-coordinated effects described in paragraphs 29 to 77 of the Non-Horizontal Merger Guidelines in so far as it does not require the merged entity to engage in a conduct that ultimately forecloses rivals. Rather, the competitive harm is linked to the possibility to access commercially sensitive information on the merged entity's rivals as a result of the merger. Therefore, the Commission needs to establish that the access to commercially sensitive information likely results in a significant impediment to effective competition. Paragraph 78 of the Non-Horizontal Merger Guidelines mentions two examples of competitive harm: the access to commercially sensitive information could allow the merged entity to price less aggressively to the detriment of consumers or put competitors at a competitive disadvantage.

5.5.4.2. The Notifying Party's views

(250) The Notifying Party explains that Wiz collects metadata from three primary sources: (i) public APIs; (ii) export logs; and (iii) agents (where deployed).

- **Public API integration.** Agentless CNAPPs like Wiz may use public API-based integration to take snapshots of customers' cloud environments – or subsets of them – to detect any cloud security vulnerabilities. This allows CNAPPs to inspect cloud environments without installing any software agents on the systems being scanned. ([249])

  The snapshots that CNAPPs take of the cloud environments via these public APIs enable them to see how customer environments – or subsets of these environments – are used. In Wiz's case, the snapshot is scanned to identify vulnerabilities, malware, and misconfiguration data to provide customers with insights into security issues in their environments. The snapshots contain information that is largely generic in nature (e.g., installed packages and versions, programming languages etc.) and are promptly deleted. Wiz stores only limited metadata and access to such metadata is strictly controlled. ([250])

  Through APIs, Wiz collects: (i) metadata on the customer's cloud infrastructure, objects and configuration (i.e., how the customer's cloud network is set up) (**Infrastructure Metadata**), which are collected to identify misconfigurations and other vulnerabilities in the cloud environment; and (ii) metadata about applications, the customer's operating system, installed packages and security patches, libraries, certificates, and access keys collected by scanning the customers' cloud workloads to identify malware, exposed secrets, and other issues (**Security Metadata**). ([251])

([248]) Non-Horizontal Merger Guidelines, paragraph 78. The legal soundness of paragraph 78 of the Non-Horizontal Merger Guidelines was confirmed by the General Court in its judgment of 18 May 2022 in case T-251/19 - Wieland-Werke v Commission, EU:T:2022:296, paragraph 88.

([249]) Form CO, paragraph 246.

([250]) Form CO, paragraph 246.

([251]) Form CO, paragraph 247. In more detail, depending on the features used by the customers, the data that Wiz stores on behalf of customers falls into the following broad categories of metadata:

- **Logs.** Logs are exported by cloud infrastructure providers and made available to customers. It is the customer that grants CNAPPs permission to access the logs. These logs provide event and activity metadata that any CNAPP can ingest. ([252])
- **Agents.** Workload-level metadata is obtainable via agents. These agents are not unique to Wiz. Many other CNAPP competitors deploy agents to gather runtime information from a workload. ([253])

(251) The Notifying Party submits that none of the customer information to which Wiz has access involves commercially sensitive information of other cloud infrastructure providers – let alone 'critical information' – within the ambit of paragraph 78 of the Non-Horizontal Merger Guidelines.

(252) The Notifying Party submits that the Infrastructure and Security Metadata is not commercially sensitive for the following reasons.

(253) First, Infrastructure and Security Metadata relate to the technical state of a customer's own cloud environment – such as infrastructure configuration, cloud objects, operating systems, and workloads. The information is about the customer's cloud configurations and does not reveal any commercially sensitive information that would provide insights into rival cloud infrastructure providers' pricing, commercial strategy, capacity planning, or future competitive behaviour, or enable Google to influence or predict competitive dynamics in the cloud infrastructure market. ([254])

(254) Second, Wiz collects metadata from customer's cloud environments and workloads through public APIs. Other third parties – including rival cloud infrastructure providers – can access the same metadata if customers grant them access. ([255])

(255) Third, Google's SecOps and Mandiant solutions already access much of the same security metadata that Wiz accesses for its security assessments. ([256])

(256) Fourth, Google receives information on customers' cloud configuration during contract negotiations for cloud infrastructure and migration plans. During such discussions, customers share information with cloud infrastructure providers on their exact configurations and needs to identify technical migration requirements, size potential usage and compare costs across different cloud infrastructure providers. For any Wiz customers that are interested in working with Google's cloud infrastructure, this is the sort of information Google would receive anyway. ([257])

Resource inventory and configuration; Network configuration; Users, service accounts, groups, permissions and roles, Host Configuration Finding evidence – metadata of actual values (e.g., file paths, file names, username strings; Cloud IdP, and other SaaS events and logs, including network logs; Data security metadata findings (limited to the reacted portion of the detected content and metadata about where it was found); Wiz Runtime Sensor – aggregated runtime event data and application network insights, including runtime execution data and suspicious activity alerts, Wiz Forensics – Logs and artifacts from virtual machine disks; Cloud Cost – Cloud cost and usage data; Data points from Wiz integration partners that are enabled by the customer; Ask AI – AI inputs and outputs). See Form CO, footnote 388.

([252]) Parties' response to RFI 10, Question 4.
([253]) Parties' response to RFI 10, Question 4.
([254]) Parties' response to RFI 16, Question 1.
([255]) Revised Annex RFI 6 Q 13.
([256]) Revised Annex RFI 6 Q 13.
([257]) Parties' response to RFI 17, Question 2.

(257) The Notifying Party further submits that Wiz does not receive data from cloud infrastructure providers with respect to confidential, bespoke or roadmap features as (i) cloud infrastructure providers do not share roadmap information with CNAPPs as they have no need to, and (ii) Wiz integrates with cloud infrastructure providers based on publicly available APIs and therefore does not secure private or gated features that are generally made available by cloud infrastructure providers through private APIs. As such, Wiz cannot become aware of such data on new features. ([258]) The Notifying Party also explained that cloud infrastructure providers may release some newly developed features to customers on a restricted basis before making the features available to all partners or customers including (i) private preview features that are made available to a small, invited group of partners for real-world testing and feedback, and (ii) gated features that more controlled releases, accessible only to partners meeting certain eligibility criteria (e.g., partner tier, region, or business type). Unlike cloud infrastructure providers' publicly available features – which are accessible through publicly available APIs – private preview and gated features are generally accessible only through private APIs to restrict usage to invited partners. ([259])

(258) The Notifying Party further considers that Google would not have the ability to access to the Infrastructure and Security Metadata and the any data on new features, as Wiz's access to customer information is governed by strict commercial contracts. Under these agreements, customers grant access only to the specific data sources they decide to share with Wiz. The agreements also limit the timespan Wiz can store such data. ([260]) In addition, customers also receive contractual protections with respect to the use of their data. Under the Wiz Subscription Agreement, Wiz may only use the customer data it receives for the purpose of providing its service to that particular customer, with a limited carve-out that permits Wiz to use 'usage data' to improve the Wiz product, so long as this use is otherwise consistent with Wiz's confidentiality and use obligations under the contract. ([261]) Wiz is also required to protect customer data under its Security Addendum, which is incorporated into and made a part of the Wiz Subscription Agreement. ([262])

(259) In any event, Wiz's size relative to the market for cloud infrastructure and data analytics means competing cloud infrastructure providers would not be dissuaded from entering or expanding, whatever the competitive value of Wiz's data. Wiz's customer base is simply too small as a portion of the market for cloud infrastructure and data analytics to affect rival cloud infrastructure providers' incentives. Wiz only represents [5-10]% of the CNAPP market, which means that Wiz – given the overall usage levels of CNAPPs - only serves [5-10]% of the market for cloud infrastructure and data analytics. ([263])

5.5.4.3. The Commission's assessment

(260) Paragraph 78 of the Non-Horizontal Merger Guidelines discusses mergers that provide access to commercially sensitive data of rivals of the merging parties. Although the data at hand is made available to Wiz by Wiz's customers (and could

([258]) Parties' response to RFI 17.
([259]) Parties' response to RFI 17, Question 1.
([260]) Parties' response to RFI 16, Question 1.
([261]) Wiz Standard Subscription Agreement, 7 November 2025, available at https://wiz.pactsafe.io/legal#wiz-subscription-agreement.
([262]) Parties' response to RFI 16, Question 1.
([263]) Parties' response to RFI 16, Question 1.

become available to Google), it effectively includes information about Google's rivals in the market for cloud infrastructure and data analytics. Therefore, the Commission considers that the framework developed under paragraph 78 of the Non-Horizontal Merger Guidelines is the most adequate framework for assessment in this scenario.

5.5.4.3.1. Data available to Wiz

(261) The Commission considers that Wiz has access to the following types of data that will be discussed in detail below: (i) Infrastructure and Security Metadata and (ii) data on new or custom-made features.

(262) First, all CNAPP and cloud infrastructure competitors expressing an opinion confirm that CNAPPs obtain visibility on how the customers' cloud infrastructure is set up across the different providers. ([264]) The vast majority of the customers and competitors that expressed an opinion confirmed that CNAPPs have access to the following data for the purpose of scanning customers' workloads: (i) cloud infrastructure metadata (including details on how the customer's network is set up across cloud infrastructure providers), (ii) configuration metadata for virtual machines, containers, gateways, and Identity and Access Management ('**IAM**') tools, and (iii) metadata about the applications, operating systems, installed packages, security patches, libraries, and access keys residing within the customer's cloud workloads (e.g., VMs, containers). ([265]) It therefore follows that CNAPPs have access to the Infrastructure and Security Metadata.

(263) In particular, one CNAPP competitor explained that 'CNAPPs do not have access to the actual data stored in the customer's cloud, but they have a view of the "resources" that hold the data and that are configured into the customer's applications.' Another CNAPP competitor stated that: 'CNAPP providers need metadata about applications, OS, resources, and configurations because it gives essential context for security. This metadata enables accurate risk assessment, compliance checks, threat detection, dependency mapping, and prioritization. Without it, CNAPP cannot differentiate critical assets from low-risk ones or provide effective posture management and protection.' ([266])

(264) Second, the market investigation revealed that CNAPPs may also have access to data on new features. Most customers and some competitors who expressed an opinion consider that CNAPPs can obtain information on all new cloud features through workload scanning, including custom-made cloud features for a given customer. Many customers and half of CNAPP competitors who expressed an opinion consider that information on new cloud features is publicly available. However, the market feedback on this question is mixed as another significant customer group considers that CNAPPs can obtain information on all new cloud

([264]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.1; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.1.

([265]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.B.1; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.2; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.2.

([266]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.2.1.

features through workload scanning, except custom-made cloud features for a given customer. ([267])

(265) In view of these mixed views on the type of data that may be available to rival CNAPPs, data on new or custom-made features will be assessed as a separate category of data.

(266) Based on the differences between the different types of data discussed above, the Commission considers that the Infrastructure and Security Metadata and the data on new or custom-made features constitute two distinct sets of information and, accordingly, this Decision assesses these types of data separately.

5.5.4.3.1.1. Commercially sensitive nature of data available to Wiz

5.5.4.3.1.1.1. Infrastructure and Security Metadata

(267) The Commission considers that the Infrastructure and Security Metadata is unlikely to constitute commercially sensitive data within the meaning of paragraph 78 of the Non-Horizontal Merger Guidelines for the following reasons.

(268) First, the Infrastructure and Security Metadata does not constitute commercially sensitive information in view of its nature. On the one hand, through Infrastructure and Security Metadata, Wiz has no access to a cloud infrastructure provider's internal systems, proprietary code, non-public interfaces or product roadmaps or other commercially sensitive technical information. ([268]) Instead, both sets of metadata to which Wiz has access relate to the technical state of a customer's own cloud environment – such as infrastructure configuration, cloud objects, operating systems, and workloads. On the other hand, Wiz does not get access to any commercial terms governing the relationship between Wiz's customers and cloud infrastructure providers. The metadata to which Wiz has access does not provide insight into rival cloud infrastructure providers' pricing, commercial strategy, capacity planning, or future competitive behaviour, nor does it enable Google to influence or predict competitive dynamics in the cloud infrastructure and data analytics market. ([269]) As noted by a CNAPP competitor in the response to the Commission's market investigation: 'This data reflects configuration state and exposure signals after features are publicly available, not product roadmaps, usage analytics at scale, or commercially sensitive insights that could inform GCP product development, and it cannot be repurposed without violating contractual and regulatory obligations.' ([270])

(269) Second, the data is already available to other third parties, including rival cloud service providers and other security software providers, if customers grant access, and thus should not be considered as commercially sensitive. In particular, Wiz as well as rival CNAPPs access such data through public APIs, which can be accessed by any security software provider, if a customer grants permission. ([271])

(270) Indeed, much of the same information is already accessed today by Google's existing security offerings, including SecOps and Mandiant. For instance, SecOps

([267]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.B.2; Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.3; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.5.

([268]) M.11964 - Google/Wiz: Technical Teach In, 24 November 2025.

([269]) Parties' response to RFI 16, Question 1.

([270]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.9.1.

([271]) Parties' response to RFI 14, Question 1.

has routine access to events data, as it ingests event logs from AWS and Azure to provide its services. ([272]) SecOps can also access configuration data either because the customer directly exports the configuration data into SecOps ([273]) or through integrations with existing scanners such as Amazon Inspector or Tenable. ([274])

(271) Further, similar to SecOps, Google Threat Intelligence and Mandiant Consulting Services also collect event and configuration data for multi-cloud customers. Google Threat Intelligence collects customer cloud configuration data that allow for threat detection and response and to tailor information related to threats to formulate each CSP's cloud threats. ([275]) When providing incident response and consulting services, subject to customer permission, Mandiant's consulting arm obtains access to customers' cloud environment data. ([276]) Through Mandiant's consulting services, Google, therefore, already receives security data similar to those that CNAPPs collect, including on customers' AWS and Azure infrastructure and configurations. In fact, to the extent necessary to solve the customer's problem (e.g., devise a response plan for an existing attack), Mandiant's consulting arm may receive more granular information about the customer's cloud infrastructure and configuration than what a CNAPP may collect. ([277])

(272) All of Google's cloud security offerings (except SCC) are multi-cloud in nature, which means that they already have access to events and cloud configuration data not only for Google's cloud infrastructure but for that of rival cloud infrastructure providers. In particular, Google expects the large majority of Mandiant Consulting customers and over half of SecOps customers to be multi-cloud. ([278]) Further, Microsoft has access to similar data that Wiz collects through its own CNAPP offering, Microsoft Defender. Microsoft Defender is a multi-cloud solution that works on AWS and GCP, in addition to Azure. ([279]) Like Wiz, Microsoft Defender collects security-related data and scans customers' multi-cloud environments to assess vulnerabilities. ([280])

(273) These findings are confirmed by the market investigation. The vast majority of cloud infrastructure competitors expressing an opinion confirmed that data on customers' cloud infrastructure is available to other providers (i.e., not only to CNAPPs). ([281]) Cloud infrastructure competitors explain that 'Other security

([272]) See Google, Cloud Threats category overview | Google Security Operations | Google Cloud Documentation; available at https://docs.cloud.google.com/chronicle/docs/detection/cloud-threats-category#:~:text=This%20document%20provides%20an%20overview,AWS%20environments%20using%20AWS%20data.

([273]) See for example, Google, Integrate AWS CloudTrail with Google SecOps | Google Security Operations | Google Cloud Documentation, available at: https://docs.cloud.google.com/chronicle/docs/soar/marketplace-integrations/aws-cloud-trail

([274]) Parties' response to RFI 17, Question 2.

([275]) See Google, Cloud Threats category overview | Google Security Operations | Google Cloud Documentation, available at:

([276]) See Google Cloud, M-Trends 2025: Data, Insights, and Recommendations From the Frontlines | Google Cloud Blog, available at: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025, 23 April 2025.

([277]) Parties' response to RFI 10, Question 4.

([278]) Parties' response to RFI 17, Question 2.

([279]) Microsoft Defender for Cloud Overview - Microsoft Defender for Cloud | Microsoft Learn, 10 September 2025, available at: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction.

([280]) Microsoft Defender for Cloud data security - Microsoft Defender for Cloud | Microsoft Learn, 11 August 2025, https://learn.microsoft.com/en-us/azure/defender-for-cloud/data-security.

([281]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.3.

products like SIEM, vulnerability management tools, IAM monitoring, and compliance platforms also need similar metadata' and 'Many other categories of cloud security solutions, such as CSPM tools, vulnerability management platforms, SIEM systems, and specialized workload protection tools, also access infrastructure metadata, configuration details, and workload information to perform their functions.' Another cloud infrastructure competitor further explains that this depends on the integration method, as 'it is likely that other security software uses some of the same APIs and has access to some of the same information' and 'In most cases, any third-party security tool authorized by the customer and designed to integrate with cloud APIs can retrieve similar types of data for security and monitoring purposes.' ([282])

(274) The vast majority of cloud infrastructure competitors expressing an opinion also confirm that the same APIs that are relied upon by CNAPP providers for integration with cloud infrastructure services are used by other security software providers, i.e., not only by CNAPPs. ([283]) Cloud infrastructure competitors explain that 'reliance on cloud provider APIs is widespread across the security software market' and 'the APIs provided by CSPs are typically general purpose and provide events across the Cloud environments that can be used by EDR, CNAPP, SIEM, SOAR or XDR solutions' and 'CSPM solutions, vulnerability management platforms, SIEM systems, SOAR tools, and identity security products often use the same APIs to collect data for analysis, compliance checks, threat detection, and incident response.' ([284])

(275) The market investigation also confirmed the Notifying Party's argument that it is within the customer's discretion to make such data available to other security software providers (i.e., not only to CNAPPs). A cloud infrastructure competitor explains that 'The availability of this data depends on the level of access granted by the customer through roles, permissions, or service accounts, as well as the capabilities of the tool to connect to and process information from the CSP.' ([285])

(276) In view of the above considerations, the Commission considers that the Infrastructure and Security Metadata is unlikely to constitute commercially sensitive information.

5.5.4.3.1.1.2. Data on new or custom-made features

(277) The Commission considers that the data related to new features of cloud infrastructure is unlikely to constitute commercially sensitive data within the meaning of paragraph 78 of the Non-Horizontal Merger Guidelines for the following reasons.

(278) First, the data is already available to other third parties, including rival cloud service providers and other security software providers, if customers grant access, and thus should not be considered as commercially sensitive. Wiz's cloud infrastructure integrations are exclusively based on publicly available APIs, and Wiz onboards new features once released by cloud infrastructure providers via those APIs. Private preview or gated features, on the other hand, are generally made available to cloud infrastructure customers through private APIs. Wiz, therefore, has no visibility into, nor access to, such features (even if they are used

([282]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.3.1.
([283]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.4.
([284]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.4.1.
([285]) Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.3.1.

by its customers). The relevant features would have to be released via a publicly available API to be capable of being seen and supported by Wiz. Accordingly, the same arguments as in Section 5.5.4.3.1.1.1 above apply, i.e., such features can be accessed by any security software providers, including rival CNAPPs, if a customer grants permission, and much of the same information is already accessed today by Google's existing security offerings, including SecOps and Mandiant.

(279) These findings are confirmed by the market investigation. The market investigation confirms that the data on new features is typically obtained through publicly available sources, including public APIs. Some customers explain that 'Information about new cloud features is typically obtained through public cloud provider documentation, release notes, and APIs rather than through security scanning of customer workloads' and 'workload scanning only inspects existing resources and configurations, but new features would be detectable by APIs.' ([286]) A CNAPP competitor explains that 'CNAPPs learn about new cloud features primarily through public CSP APIs, service metadata, release notes, and updated configuration schemas, which allow them to detect and assess newly introduced services and settings once they appear in customer environments. However, custom-built or private features created specifically for an individual customer are not generally visible to CNAPPs beyond how they manifest through standard, exposed configurations or APIs.' ([287]) A cloud infrastructure competitor also confirms that 'CNAPPs discover new cloud services through API enumeration and provider documentation, meaning they depend on cloud providers publishing updated APIs and schemas to support new features.' ([288])

(280) Second, the Commission's market investigation also examined the potential ability and incentive of the merged entity to access and use information on new cloud features available to Wiz's customers which may be regarded as commercially sensitive information.

(281) While the majority of customers expressing an opinion considered that the merged entity could get access to information on new cloud features available to Wiz's customers, ([289]) feedback from CNAPP and cloud infrastructure competitors was more mixed insofar as a number of them took the opposite view. ([290])

(282) Even if such information were to be technically available to the merged entity, many customers point out to the contractual protections that would prevent the merged entity using this information: 'CNAPPs can only discover resources to which the customer grants access. The customer is responsible for assigning the permission'; 'It is possible for new types of services and resources to be discovered by a CNAPP with access. It is just as easy for the customer to restrict access to prevent new discovery' or 'In practice, the ability to use such information as an input for developing GCP-related products is strongly constrained by contractual, technical and operational safeguards.' ([291]) A

([286]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.B.2.1.
([287]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.3.1.
([288]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.5.1.
([289]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.B.7.
([290]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.8; Replies to Questionnaire 1 - Phase I market investigation – Competitors (CSP), question E.D.B.7.
([291]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.B.7.1.

customer also points out that the merged entity would unlikely have the incentive to pursue such a strategy as engaging in such practices would erode market and customer trust. ([292])

(283) Further, some respondents confirm that new cloud features are publicly available. One customer confirms that 'Information on new cloud features is publicly available.' ([293]) One CNAPP competitor explains 'the merged entity would not gain privileged access to information on new cloud features beyond what is already publicly available or exposed through standard CSP APIs and documentation. CNAPPs observe only security-relevant metadata once features are generally released and enabled in customer environments; they do not receive advance notice, roadmap insight, or non-public details about upcoming cloud features specific to Wiz's customers.' ([294]) Another CNAPP competitor confirms that 'Having an understanding of which services are used in other clouds could be used as input when developing GCP. With that said, most clouds have largely the same set of features and those features are generally publicly documented.' ([295])

(284) In view of the above considerations, the Commission considers that data on new features is unlikely to constitute commercially sensitive information.

5.5.5. Conclusion

(285) In view of the above considerations and in light of the results of the market investigation and the evidence and information available to it, the Commission concludes that the Transaction would not raise serious doubts as to its compatibility with the internal market as a result of vertical effects, notably (i) by foreclosing CNAPP providers through degradation of access to Google's cloud infrastructure and (ii) by accessing to Wiz's customers data (including the Infrastructure and Security Metadata and data on new features), as this does not constitute commercially sensitive information that could be used to reduce competition on the upstream market for cloud infrastructure and data analytics.

5.6. Conglomerate effects

5.6.1. Introduction

(286) The Transaction gives rise to a number of conglomerate relationships between the activities of Google and Wiz. As described above in Section 5.2 and as shown in **Table 39** below**,** Google and Wiz do not have an individual or combined market share exceeding 30% on the markets for cloud infrastructure and data analytics and CNAPP respectively, or on any potential relevant market defined in this Decision. Nevertheless, in order to fully cover some of the concerns arising from the Transaction, this Decision assesses the conglomerate effects that may arise

([292]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.B.7.1.
([293]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.B.7.1.
([294]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.8.1.
([295]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.B.9.1.

from the close relationship between the CNAPP market ([296]) ([297]) and the market for cloud infrastructure and data analytics ([298]), as well as other markets that are closely related to the market for CNAPP. ([299]) ([300]) Accordingly, the Decision examines the following concerns:

([296]) As shown in Section 5.3.1.2, the merged entity does not have a market share exceeding 30% in the potential market for CSPM either. The Commission will not separately assess the conglomerate relationship between the market for CSPM on the one hand, and the markets for cloud infrastructure and other security on the other hand, as the results of the market investigation pointed out that there is no material difference in their responses when distinguishing between CNAPP and CSPM respectively. Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), questions E.C.2.2, E.C.3.2, E.C.4.2, E.C.5; replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), questions E.C.A.1.2, E.C.A.2.2, E.C.A.3.2, E.C.A.4, E.C.B.1.2, E.C.B.2.2, E.C.B.3.2, E.C.B.4.2, E.C.B.5; replies to Questionnaire 3 - Phase I market investigation – Customers, questions E.C.A.1.2, E.C.A.2.2, E.C.A.3.2, E.C.A.4, E.C.B.1.2, E.C.B.2.2, E.C.B.3.2, E.C.B.4.2, E.C.B.5.

([297]) As shown in Section 5.3.1, the combined market shares of the Parties in the overall security software market are below 2%. The Commission will therefore not separately assess the conglomerate relationship between the market for overall security software on the one hand and the market for cloud infrastructure and data analytics on the other.

([298]) The Commission considers that an assessment on the basis of a potential narrower segmentation of the market for cloud infrastructure and data analytics specifically for AI workloads would not be materially different. As confirmed in Section 5.3.2, Google's market share in such a segment would be at most comparable to its share in the overall market. Respondents to the market investigation also considered that Google's GCP is not particularly suited to a specific pool of customers (Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.B.6; replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.B.6; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.B.6). Furthermore, the effects of any putative foreclosure theory of harm would be limited given that CNAPP secure all types of workloads, including but not limited to AI workloads. GCP's AI workloads represent only a fraction of its share on the overall market for cloud infrastructure and data analytics. The Commission will thus not separately assess the competitive effects of the Transaction specifically in relation to a potential narrower segment for cloud infrastructure and data analytics for AI workloads.

([299]) The Commission's investigation of conglomerate effects as a result of the Transaction does not concern other activities in relation to which Google's market share may exceed 30% but which are not closely related to the markets on which Wiz is active, such as email applications ([30-40]% worldwide, [30-40]% in the EEA), advertising applications ([20-30]% worldwide, [30-40]% in the EEA), and non-relational database management systems ([20-30]% worldwide, [50-60]% in the EEA), see Section 5.3. These products are purchased for unrelated use cases and are not generally used or integrated together. By reason of the distant relationship between these markets, the Commission finds it unlikely that the Transaction would raise serious doubts as to the compatibility of the Transaction with the internal market.

([300]) Wiz is also currently developing a cost optimisation tool allowing customers to optimise their cloud costs. For the purpose of this tool, [information on the Parties' product or sales roadmaps and unreleased features]. This feature is optional and not part of Wiz's core product offering. It is currently in limited testing (available to approx. [information on the Parties' product or sales roadmaps and unreleased features]), is only available for Azure, AWS, and more recently Google's cloud infrastructure, and is not generally available to Wiz customers. This type of data is not discussed further as cost optimisation is an add-on offering to a CNAPP. In addition to CNAPPs (e.g., Wiz, Datadog, Sysdig, Orca), many other providers including cloud infrastructure providers (e.g., Amazon, Microsoft, Alibaba or IBM) and other providers (e.g., Broadcom VMware, CloudZero, Finout, Flexera, PointFive, Ternary or Vantage) offer similar cost optimisation solutions. In any event, the APIs used to access the [information on the Parties' product or sales roadmaps and unreleased features] are public and different to the publicly available APIs used to provide CNAPP services. As a result, any provider (with the requisite customer permissions) can access the APIs to pull the relevant [information on the Parties' product or sales roadmaps and unreleased features], and a CNAPP's existing access to a CSP's publicly available API provides it with no advantage.

(1) The potential foreclosure of rival cloud infrastructure providers through the degradation of the interoperability of Wiz's security software (namely CNAPP) with other clouds (Section 5.6.3); ([301])

(2) The potential foreclosure of rival CNAPP providers through the degradation of their interoperability with Google's cloud infrastructure (Section 5.6.4);

(3) The potential commercial bundling of Wiz's CNAPP with Google's cloud infrastructure (Section 5.6.5.1) as well as with Google's other (non-CNAPP) security software (Section 5.6.5.2).

(287) Furthermore, the Transaction gives rise to a conglomerate relationship between a potential market for specialised generative AI, where Google holds a share of more than 30%, and the market for CNAPP. This Decision will therefore also assess whether the Transaction could lead to a significant impediment of effective competition on the market for CNAPP (Section 5.6.6).

Table 39: Conglomerate relationships assessed by the Decision

Primary Market	Market share	Neighbouring market	Market share
CNAPP (Merged entity)	[5-10]% (worldwide) ([302]) [10-20]% (Europe) ([303])	Cloud infrastructure and data analytics (Google)	[5-10]% (worldwide) [5-10]% (Europe) ([304])
		Other security software (Google) ([305])	<5%
Specialized generative AI (Google)	[30-40]% (worldwide) [30-40]% (Europe)	CNAPP (Merged entity)	[5-10]% (worldwide) ([306]) [10-20]% (Europe) ([307])

([301]) For reasons similar to what is set out in Section 5.6.3, the Commission considers it unlikely that the merged entity will remove Wiz from the marketplaces of competing cloud infrastructure providers, as they constitute Wiz's largest sales channels. Furthermore, as explained in more detail in this Section, the effects of a potential move of all Wiz customers to GCP on the market for cloud infrastructure and data analytics would be minimal.

([302]) As explained in further detail above, the Notifying Party argues that the numbers reported in IDC and Gartner market shares are overstated. Please refer to Section 5.3 for adjusted market shares.

([303]) As explained in further detail above, the Notifying Party argues that the numbers reported in IDC and Gartner market shares are overstated. Please refer to Section 5.3 for adjusted market shares.

([304]) As explained in further detail above in Section 5.3, based on the Gartner market share estimates for 2024, Google's market share in the IaaS market segment is [5-10]% worldwide and [10-20]% in Europe. In the PaaS market segment, Google's market share is [5-10]% worldwide. Combining the estimates from the IaaS and the PaaS segments into the IaaS + PaaS market segment, Google's market share is [5-10]% worldwide.

([305]) These markets include the following segments as identified by Gartner: (i) Information and data security ([0-5]% worldwide, [0-5]% Europe); (ii) Identity and access management ([0-5]% worldwide, [0-5]% Europe); (iii) Security analytics ([0-5]% worldwide; [0-5]% Europe); (iv) Network security ([0-5]% worldwide, [0-5]% Europe). Given that Google's market shares are minimal in each of these markets, the competitive assessment groups each of these markets under the broader umbrella of Google's other, non-CNAPP security software.

([306]) As explained in further detail above, the Notifying Party argues that the numbers reported in IDC and Gartner market shares are overstated. Please refer to Section 5.3 for adjusted market shares.

([307]) As explained in further detail above, the Notifying Party argues that the numbers reported in IDC and Gartner market shares are overstated. Please refer to Section 5.3 for adjusted market shares.

5.6.2. Legal framework

(288) According to the Non-Horizontal Guidelines, in the majority of circumstances, conglomerate mergers will not lead to any competition problems. ([308])

(289) However, foreclosure effects may arise when the combination of products in related markets may confer on the merged entity the ability and incentive to leverage a strong market position from one market to another closely related market by means of tying or bundling or other exclusionary practices. While tying and bundling have often no anticompetitive consequences, in certain circumstances such practices may lead to a reduction in actual or potential competitors' ability or incentive to compete. This may reduce the competitive pressure on the merged entity allowing it to increase prices. ([309])

(290) In assessing the likelihood of such a scenario, the Commission examines, first, whether the merged firm would have the ability to foreclose its competitors, ([310]) second, whether it would have the economic incentive to do so ([311]) and, third, whether a foreclosure strategy would have a significant detrimental effect on competition, thus causing harm to consumers. ([312]) These factors are cumulative and often examined together as they are closely intertwined.

(291) In order to be able to foreclose competitors, the merged entity must have a significant degree of market power, which does not necessarily amount to dominance, in one of the markets concerned. The effects of bundling or tying can only be expected to be substantial when at least one of the merging parties' products is viewed by many customers as particularly important and there are few relevant alternatives for that product. ([313]) Further, for foreclosure to be a potential concern, it must be the case that there is a large common pool of customers, which is more likely to be the case when the products are complementary. ([314]) Finally, bundling is less likely to lead to foreclosure if rival firms are able to deploy effective and timely counterstrategies, such as single-product companies combining their offers. ([315])

(292) The incentive to foreclose competitors through bundling or tying depends on the degree to which this strategy is profitable. ([316]) Bundling and tying may entail losses or foregone revenues for the merged entity. ([317]) However, they may also allow the merged entity to increase profits by gaining market power in the tied goods market, protecting market power in the tying good market, or a combination of the two. ([318])

(293) It is only when a sufficiently large fraction of market output is affected by foreclosure resulting from the concentration that the concentration may significantly impede effective competition. If there remain effective single-product players in either market, competition is unlikely to deteriorate following

([308]) Non-Horizontal Guidelines, paragraph 92.
([309]) Non-Horizontal Guidelines, paragraphs 91 and 93.
([310]) Non-Horizontal Guidelines, paragraphs 95-104.
([311]) Non-Horizontal Guidelines, paragraphs 105-110.
([312]) Non-Horizontal Guidelines, paragraphs 111-118.
([313]) Non-Horizontal Guidelines, paragraph 99.
([314]) Non-Horizontal Guidelines, paragraph 100.
([315]) Non-Horizontal Guidelines, paragraph 103.
([316]) Non-Horizontal Guidelines, paragraph 105.
([317]) Non-Horizontal Guidelines, paragraph 106.
([318]) Non-Horizontal Guidelines, paragraph 108.

a conglomerate concentration. ([319]) The effect on competition needs to be assessed in light of countervailing factors such as the presence of countervailing buyer power or the likelihood that entry would maintain effective competition in the upstream or downstream markets. ([320])

5.6.3. Foreclosure of rival cloud infrastructure providers through degradation of the interoperability of Wiz's security software with other clouds

(294) End-customers purchase both cloud infrastructure and CNAPPs that protect these cloud environments. This Decision assesses whether the merged entity could degrade the interoperability of Wiz's CNAPP with cloud infrastructure providers that compete with Google to coerce Wiz customers to move their cloud demand to Google's cloud infrastructure, thereby leading to the partial foreclosure of rival cloud infrastructure providers.

5.6.3.1. The Notifying Party's views

(295) The Notifying Party submits that the merged entity would not have the ability or incentive to degrade the interoperability of Wiz's CNAPP with rival cloud infrastructure providers, and that any putative attempts at partial foreclosure would not result in anticompetitive effects for the reasons set out below.

(296) First, the Notifying Party submits that the merged entity would not enjoy market power to engage in a foreclosure strategy because Wiz's market shares are well below 30% on the CNAPP market (worldwide share of [5-10]% and EEA-wide ([321]) share of [10-20]%). ([322]) According to the Notifying Party, Wiz faces competition from numerous rivals and is not a must-have CNAPP. Alternative suppliers of CNAPPs which offer the set of capabilities as Wiz include Palo Alto Networks, CrowdStrike, Orca Security and Lacework. ([323])

(297) On technical ability ([324]), the Notifying Party submits that Wiz can technically be set up in a way that prevents it from reading the cloud infrastructure providers' publicly available APIs, but this would reflect a product design choice and does not fall within the remit of 'interoperability'. According to the Notifying Party, any refusal to read rival cloud infrastructure providers' publicly available APIs would cripple Wiz and have grave consequences: Wiz would no longer support the key criteria customers demand of CNAPPs, which is 'multi-cloud' security. This would render Wiz largely unusable to over 80% of cloud infrastructure customers which do not use Google's cloud infrastructure today. It would erode Wiz's customer base and revenues – which are largely based on uptake by AWS and Azure customers.

(298) Second, the Notifying Party submits that the merged entity would have no incentive to engage in a foreclosure strategy. This is because customers are unlikely to switch cloud infrastructure providers for access to, or better integration with their preferred CNAPP. CNAPP spend represents a small fraction of overall

([319]) Non-Horizontal Guidelines, paragraph 113.
([320]) Non-Horizontal Guidelines, paragraph 114.
([321]) In this section, given that IDC only includes data for Europe and not the EEA, the Commission has used the data for "Europe" as a proxy for EEA-wide data.
([322]) The Notifying Party argues that these shares overstate the Parties' actual revenues and therefore, IDC's value-based shares provide a conservative view of the Parties' positions in the CNAPP market. Please refer to Section 5.3 for the Parties' adjusted market shares.
([323]) Form CO, Annex RFI 6 Q 16.1, pages 2-4.
([324]) Please see Section 5.6.4.1 below for further details on how CNAPP tools integrate with cloud infrastructure.

cloud expenditure, and customers are therefore more likely to switch to a rival CNAPP provider rather than to another cloud infrastructure providers. Moreover, according to the Notifying Party, Wiz's overall value proposition is inextricably linked to its multi-cloud capabilities (in particular for AWS and Microsoft Azure), and without multi-cloud support, Wiz would not qualify as a CNAPP. This would devalue its products and results in a loss of business due to customers switching to rivals. Further, any foreclosure attempt would also result in reputational damage, leading to lost sales for a range of other Google products. ([325])

(299) Lastly, the Notifying Party submits that, even assuming that the merged entity was to pursue a foreclosure strategy, it would not significantly alter competitive dynamics in the market. According to the Notifying Party, even in the unrealistic scenario that all of Wiz's customers moved their cloud infrastructure demand to Google, rival cloud infrastructure providers would not be foreclosed since these CNAPP customers only represent a small fraction of overall cloud infrastructure demand. Wiz only represents [5-10]% of the CNAPP market, and Wiz's CNAPP is used to secure only [5-10]% of overall cloud infrastructure demand. ([326]) Further, any foreclosure strategy could be defeated by rivals (such as Microsoft, IBM, Oracle and Alibaba), which have broad portfolios covering both CNAPPs and cloud infrastructure and could match any putative technical foreclosure mechanism. ([327])

5.6.3.2. The Commission's assessment

(300) For the reasons set out below, the Commission considers that the merged entity would have neither the ability nor the incentive to foreclose rivals in the market for cloud infrastructure and data analytics by degrading the interoperability of Wiz's security software (namely CNAPP) with rival cloud infrastructure. Therefore, given that the conditions under the Non-Horizontal Guidelines are cumulative ([328]), the Commission does not need to take a position of whether the third other condition is satisfied.

5.6.3.2.1. Ability to foreclose

(301) For the reasons set out below, the Commission considers that the merged entity would not have the ability to foreclose rivals in the market for cloud infrastructure and data analytics by degrading the interoperability of Wiz's security software (namely CNAPP) with rival cloud infrastructure .

(302) For the purposes of this Decision, the Commission considers that Wiz does not have a significant degree of market power in the market for CNAPP.

(303) First, as set out above in Section 5.5.3.2.1, the Commission considers that Wiz does not have a significant degree of market power in the market for CNAPP, given its limited market share, the many alternatives available and the competitive and dynamic nature of the market.

([325]) Form CO, Annex RFI 6 Q 16.1, pages 4-5.

([326]) The Notifying Party explains that Wiz's global adjusted share in the IDC CNAPP functional market is [5-10]% in 2024. Based on the Cloud Security Alliance, Cloud Native Application Protection Platform (CNAPP) Survey Report, 2023, p. 7, CNAPPs have an approximately 75% penetration rate. On this basis, Wiz's estimated share in the overall market for cloud infrastructure and data analytics that is addressed by CNAPPs is equal to approximately [5-10]% ([5-10]% * 75% = [5-10]%).

([327]) Form CO, Annex RFI 6 Q 16.1, pages 7-8.

([328]) Non-Horizontal Guidelines, paragraphs 93-118.

(304) Second, the market investigation confirmed that switching between CNAPP providers is possible. As explained in further detail above in Section 5.4.3.2, the majority of customers expressing an opinion considered that although switching from one CNAPP supplier to another is technically complex and needs some time, it is a real option. ([329])

(305) Finally, the majority of customers and CNAPP competitors expressing an opinion considered that the impact of the Transaction in the CNAPP market would be positive or neutral. ([330])

(306) The market feedback on the **technical ability** of the merged entity to foreclose was mixed. ([331]) While the majority of customers and half of the CNAPP competitors expressing an opinion considered that it would not be possible for the merged entity to degrade the quality or delay interoperability between Wiz Cloud and cloud infrastructure providers other than Google, the majority of competing cloud infrastructure providers expressing an opinion indicated that it would be possible. ([332]) One competing cloud infrastructure provider explained that this could be done by 'altering Wiz's development priorities, scaling back investment in integrations with non-GCP environments, delaying support for new features or APIs released by other CSPs, or reducing the level of testing and optimization for those platforms' while another one said that this could be achieved by 'adding new features that might only work on GPC.' ([333]) However, as explained in further detail below in Section 5.6.3.2.2 on incentive, competitors also indicated that such a foreclosure strategy would be unlikely.

(307) Despite of the mixed feedback on technical ability, the Commission considers that the merged entity would not have the ability to engage in a foreclosure strategy as Wiz does not have a significant degree of market power on the CNAPP market.

5.6.3.2.2. Incentive to foreclose

(308) For the reasons set out below, the Commission considers that the merged entity would not have the incentive to foreclose rivals in the market for cloud infrastructure and data analytics by degrading the interoperability of Wiz's security software (namely CNAPP) with rival cloud infrastructure.

(309) Market participants confirmed that the merged entity would have no incentive to degrade the interoperability of Wiz's security software (namely CNAPP) with competing cloud infrastructure as it would lead to Wiz no longer being multi-cloud, and because customers are unlikely to switch cloud infrastructure providers for access to, or better integration with, their preferred CNAPP tool.

(310) Both competing CNAPP and cloud infrastructure providers explained that – while the merged entity could have the technical ability to degrade the interoperability of Wiz's security software (namely CNAPP)– it would be unlikely to do so as it would lead to Wiz no longer being multi-cloud. One competing cloud

([329]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.13.

([330]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question F.2; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question F.2; replies to Questionnaire 3 - Phase I market investigation – Customers, question F.2.

([331]) Please see paragraphs (315)-(318) below for further details on how CNAPP tools integrate with cloud infrastructure.

([332]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.D.A.10; replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.D.A.11; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D

([333]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.D.A.10.1.

infrastructure provider noted that it would be 'commercially irrational since multi-cloud support is Wiz's core value proposition and most Wiz customers run on AWS' while another one explained that 'intentionally degrading Wiz Cloud's interoperability with other CSPs could alienate existing multi-cloud customers and weaken Wiz's competitive market position. It might also raise anti-trust and fair competition concerns, especially for customers that depend on consistent multi-cloud visibility and security. While technically feasible, the commercial, reputational, and legal consequences make it improbable that the merged entity would deliberately restrict or delay non-GCP integrations.' ([334]) Similarly, one CNAPP competitor explained that 'This would have the impact of losing business for Wiz Cloud with anyone using any other CSPs. As such, it is hard for us to imagine they would engage in this tactic.' ([335])

(311) Further, the majority of customers expressing an opinion confirmed that, in a hypothetical scenario where the interoperability between Wiz and the cloud infrastructure of providers other than Google would be degraded or delayed, they would move away from Wiz and switch to another CNAPP provider that continues to interoperate with other cloud infrastructure. ([336]) Customers emphasized their need for a cloud-agnostic CNAPP. One customer explained that 'we would continue to look for a cloud-agnostic CNAPP', while another one noted that 'we generally select a CNAPP product that works with many cloud providers since our goal is to achieve a single solution for cloud security in general.' Customers also explained that it is easier to switch between CNAPP providers than between cloud infrastructure providers. One customer indicated that they would 'change CNAPP to ensure good coverage on all CSP we have. It is easier to move CNAPP rather than migrate from one CSP to another', while another explained that 'We are multi-cloud and leverage the best features of each cloud provider. Therefore, if the security solution no longer meets our needs, we would change the security solution rather than switching CSPs.' ([337])

(312) In light of the above, the Commission considers that the merged entity would not have the incentive to engage in a foreclosure strategy.

5.6.3.2.3. Conclusion

(313) In light of the above, the Commission concludes that the Transaction would not significantly impede effective competition on the market for cloud infrastructure and data analytics as a result of foreclosure of rival cloud infrastructure providers through the degradation of interoperability of Wiz's security software (namely CNAPP) with other clouds.

5.6.4. Foreclosure of rival CNAPP providers through the degradation of their interoperability with Google's cloud infrastructure

(314) End-customers purchase both cloud infrastructure and CNAPPs that protect these cloud environments. This Decision assesses whether the merged entity could degrade the interoperability of Google's cloud infrastructure with competing CNAPPs providers to coerce Google's cloud infrastructure customers to move their CNAPP demand to Wiz, thereby foreclosing rival CNAPP providers.

([334]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.D.A.10.2.
([335]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.D.A.11.2.
([336]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.28.
([337]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.29.

5.6.4.1. Technical integration between cloud infrastructure and CNAPP tools

(315) At a technical level, there are three principal ways in which CNAPPs and cloud infrastructures interact: (i) via APIs, (ii) via agents, and (iii) via log exports.

(316) CNAPPs can use **API integrations** with cloud infrastructures to take snapshots of the cloud infrastructure environment (agentless scanning) and/or connect to specific cloud infrastructure components (e.g., compute engine).

(317) In addition to the agentless, public API-based snapshot approach, CNAPPs can also integrate with cloud infrastructures via **agents.** An agent can be deployed immediately on any cloud. Agent-based scanning involves the installation of lightweight agents directly on compute resources like virtual machines, containers, or Kubernetes nodes to perform specific security or monitoring functions. The agent monitors and collects data on the security state of the cloud environment and sends data to the CNAPP for processing and visualization of alerts, risk scores, and remediation suggestions.

(318) **Logs** are formatted text records that capture events and activities as they occur in a cloud environment. Each cloud infrastructure provider has its own syntax or log format that is specific to that cloud, but the syntax or log format is well-documented and made available to allow customers to collect and process the data as needed without the need to deploy additional sensors or agents or provide API access to their workloads. Customers can configure their cloud infrastructures to export different types of logs (i.e., focusing on different types of events). Of these, CNAPPs collect security-related logs – such as cloud identity security logs, network activity logs, and DNS logs – to enable security visibility, risk detection, and compliance monitoring. Log exports are pulled by a CNAPP (with the requisite customer permissions). ([338])

5.6.4.2. The Notifying Party's views

(319) The Notifying Party submits that the merged entity would not have the ability or incentive to remove or degrade the interoperability of Google's cloud infrastructure with rival CNAPP providers, and that any putative attempts at (partial) foreclosure would not result in anticompetitive effects for the reasons set out below.

(320) First, the Notifying Party submits that the merged entity would not enjoy market power – let alone have a significant degree of market power – to engage in a foreclosure strategy because Google's market shares in 2023 were well below 30% on the market for cloud infrastructure and data analytics (worldwide share of [5-10]% and EEA-wide ([339]) share of [5-10]%), and well below shares held by AWS (worldwide share of [30-40]% and EEA-wide share of [30-40]%) and Microsoft Azure (worldwide share of [10-20]% and EEA-wide share of [10-20]%). ([340]) ([341])

([338]) Form CO, paragraphs 245-254.

([339]) In this section, given that IDC only includes data for Europe and not the EEA, the Commission has used the data for "Europe" as a proxy for EEA-wide data.

([340]) Response to Preliminary Market Feedback, page 10.

([341]) As explained in further detail above in Section 5.3, based on the Gartner market share estimates for 2024, Google's market share in the IaaS market segment is [5-10]% worldwide and [10-20]% in Europe. In the PaaS market segment, Google's market share is [5-10]% worldwide. Combining the estimates from the IaaS and the PaaS segments into the IaaS + PaaS market segment, Google's market share is [5-10]% worldwide.

(321) Second, the Notifying Party submits that the merged entity would not have the technical ability to selectively refuse or degrade interoperability. According to the Notifying Party, CNAPPs principally interoperate with cloud infrastructures through public APIs that are also used for other use cases, and Google cannot turn off these APIs or degrade them without damaging the features and integrations of Google's cloud infrastructure beyond CNAPP. Moreover, Google cannot target degradations at CNAPPs using the APIs because it does not know what third party is calling what API. ([342])

(322) Third, the Notifying Party submits that the merged entity would not have any incentive to degrade its interoperability with rival CNAPP providers as this would lead to lower-quality security on Google's cloud infrastructure and would make it a less attractive platform. This would also be against the deal rationale, which is to promote multi-cloud configurations to the benefit of Google's cloud infrastructure. Further, according to the Notifying Party, Google is highly unlikely to accept losses in cloud activities in an effort to seek out an advantage in the CNAPP market as the total cloud infrastructure market is approximately 50 times larger than the CNAPP market. ([343])

5.6.4.3. The Commission's assessment

(323) For the reasons set out below, the Commission considers that the merged entity would not have either the ability or the incentive to foreclose rivals in CNAPP market by degrading the interoperability of Google's cloud infrastructure with rival CNAPP providers. Therefore, given that the conditions under the Non-Horizontal Guidelines are cumulative ([344]), the Commission does not need to take a position of whether the third condition on whether there would be a significant detrimental effect on competition is satisfied.

5.6.4.3.1. Ability to foreclose

(324) For the purposes of this Decision, for the reasons set out above in Section 5.5.3.2.1, the Commission considers that Google does not have a significant degree of market power in the market for cloud infrastructure and data analytics.

Technical ability

(325) The market feedback on technical ability was mixed.

(326) **APIs.** The majority of customers indicated that it would not be possible for the merged entity to block access to APIs used by competing CNAPP providers to prevent them from securing workloads on Google's cloud infrastructure. Similarly, the majority of customers considered that it would not be possible for the merged entity to degrade the quality or delay interoperability between Google's cloud infrastructure and the competing CNAPP tools of other providers based on APIs. However, the majority of cloud infrastructure competitors and half of the CNAPP competitors considered that it would be possible for the merged entity to block access to APIs, while the majority of both cloud infrastructure and

([342]) Response to Preliminary Market Feedback, page 15.
([343]) Response to Preliminary Market Feedback, page 16.
([344]) Non-Horizontal Guidelines, paragraphs 93-118.

CNAPP competitors considered that delaying quality or degrading interoperability through APIs would be possible. ([345])

(327) Some competitors explained that blocking access to APIs would be possible as Google owns the underlying infrastructure. For example, one cloud infrastructure competitor explained that it would be possible for the merged entity to block access to APIs as 'Google governs the terms of use of GCP and the technical implementation supporting access to APIs, and consequently controls what services may connect through its APIs.'

(328) Conversely, some competitors explained that blocking APIs would not be possible, as they are standardized and public, and relied upon by many third-party software providers. One cloud infrastructure competitor who considered that it would not be possible to block access to APIs explained that 'cloud provider APIs are public and standardized—all CNAPP vendors use the same GCP APIs (Cloud Asset Inventory, IAM, Compute, etc.) to scan infrastructure, so blocking competitors would require restricting public APIs…' while another one noted that 'most visibility APIs are public, but in certain cases, a private or unpublished API might be leveraged by the merged entity to gain operational advantages on the GCP platform.' ([346]) Similarly, a CNAPP competitor explained that 'In practice, blocking access to the GCP APIs used by competing CNAPP providers would be technically and commercially difficult, because these APIs are standardized, broadly used by many third-party tools, and deeply embedded in customer operations and partner ecosystems. Restricting them selectively would risk breaking legitimate customer integrations, violating platform neutrality expectations, and triggering regulatory, contractual, and customer backlash, making such behavior unlikely and unsustainable in reality.' ([347])

(329) On the degradation of interoperability, one cloud infrastructure competitor explained that it would be possible 'Because GCP controls the design, performance, and availability of its APIs, the merged entity could technically make changes that reduce the speed, reliability, or completeness of data available to competing CNAPP providers. This could involve altering API endpoints, limiting the frequency of queries, or delaying the release of new API features needed for full interoperability.' ([348])

(330) Conversely, one CNAPP competitor explained that while the degradation of interoperability could be theoretically possible, it would be hard to sustain as APIs are public: 'While a merged entity could theoretically introduce API changes or slower feature exposure, materially degrading or delaying interoperability for competing CNAPP tools would be difficult to sustain. GCP's APIs are public, standardized, and used broadly by customers and thousands of third-party integrations; selectively disadvantaging CNAPP providers would risk breaking customer workflows, triggering partner and regulatory scrutiny, and undermining GCP's own ecosystem credibility. In practice, competitive CNAPP tools would

([345]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), questions E.D.A.2 and E.D.A.6; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.A.2 and E.D.A.6; Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.1 and E.D.A.12.

([346]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.D.A.2.1.

([347]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.D.A.2.1.

([348]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.D.A.6.4.

continue to function via stable APIs, and any minor delays would be temporary and non-discriminatory, not a durable foreclosure mechanism.' ([349])

(331) **Log exports**. The majority of customers and CNAPP competitors indicated that it would not be possible for the merged entity to block access to log exports used by competing CNAPP providers to prevent them from securing workloads on Google's cloud infrastructure or to degrade the quality or delay interoperability between Google's cloud infrastructure and the competing CNAPP tools of other providers based on logs. However, the majority of cloud infrastructure competitors indicated that it would be possible for the merged entity to do both. ([350])

(332) While competing cloud infrastructure providers explained that blocking access to log exports would be technically possible, they also note that it would have a significant impact on customer operations as well as other third-party software providers and would therefore be unlikely. According to competitors, such actions could also lead to regulatory scrutiny. One competing cloud infrastructure provider that considered that access to logs could be blocked explained that 'Yes, it would be possible for the merged entity to block access to log exports used by competing CNAPP providers because control over GCP's logging services and export mechanisms rests with Google. These exports, such as those from Cloud Logging, are essential for third-party CNAPP tools to analyze events, detect threats, and monitor compliance. By restricting permissions, altering export formats, or limiting integration capabilities, the merged entity could technically prevent competitors from ingesting logs needed to secure workloads. However, such action could significantly impact customer operations, raise interoperability concerns, and attract regulatory scrutiny, so while possible, it would be a sensitive and potentially controversial move.' Similarly, another competing cloud infrastructure provider explained that 'While technically possible, log-based integration is customer-configured, and blocking it would be highly disruptive and legally risky. It is possible in theory, but practically and legally very problematic.' ([351])

(333) Similarly, one CNAPP competitor explained that 'It's highly unlikely that GCP would block access to log exports because the platform must maintain interoperability with other security products. Restricting access would harm their reputation and customer trust', while another one noted that 'Blocking access to GCP log exports (e.g., Cloud Audit Logs, VPC Flow Logs) for competing CNAPP providers would be difficult to implement selectively without disrupting customers' own security, compliance, and observability workflows, which rely on exporting logs to SIEMs and third-party tools. Any attempt to restrict or degrade log exports would likely impact customers directly, conflict with established platform commitments and contracts, and create significant commercial and regulatory risk, making such blocking unlikely in practice.' ([352])

([349]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.D.A.6.1.

([350]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), questions E.D.A.3 and E.D.A.7; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.A.3 and E.D.A.7; Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.4 and E.D.A.15.

([351]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.D.A.3.1.

([352]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.D.A.3.1.

(334) On the degradation of interoperability through logs, competitors explain that while it would be technically possible, it could be difficult for Google to target specific CNAPP competitors, and such action would have an impact on other security vendors as well. One competing cloud infrastructure provider explains that it would be possible 'Because GCP controls the configuration, permissions, and delivery mechanisms for log exports, the merged entity could technically make changes that reduce the timeliness, completeness, or accessibility of logs used by competing CNAPP providers. This might involve altering export formats, introducing delays in log delivery, or limiting integrations to certain destinations. Such changes could hinder competitors' ability to monitor workloads and detect threats effectively', while another notes that 'in certain scenarios it may be more difficult to restrict access unless the merged entity was able to analyze other data (such as IP addresses and traffic patterns) to a degree sufficient to identify competing CNAPP providers.' ([353]) Similarly, one CNAPP competitor explained that 'Degrading or delaying interoperability based on log exports would be difficult to do selectively, because GCP log export mechanisms (e.g., Cloud Audit Logs, VPC Flow Logs, Cloud Logging sinks) are customer-configured, standardized services used broadly for SIEM, compliance, observability, and billing use cases. Any reduction in log quality, timeliness, or availability would directly impact customers and a wide range of third-party tools, not just CNAPP providers, creating significant operational disruption and commercial and regulatory risk, making such behavior unlikely in practice.' ([354])

(335) **Agents**. The majority of customers and CNAPP competitors indicated that it would not be possible for the merged entity to block competing CNAPP providers from installing agents on Google's cloud infrastructure to prevent them from securing Google's cloud infrastructure or to degrade the quality or delay interoperability between Google's cloud infrastructure and the competing CNAPP tools of other providers based on agents. However, the majority of competing cloud infrastructure providers indicated that it would be possible for the merged entity to do both. ([355])

(336) While competing cloud infrastructure providers explained that preventing the installation of agents would be technically possible, they also note that it would have a significant impact on customer operations. One competing cloud infrastructure provider that considered that competing CNAPP providers could be prevented from installing agents explained that 'It would be possible for the merged entity to block competing CNAPP providers from installing agents on GCP workloads. Because GCP controls the underlying infrastructure, permissions, and policies governing workload operation, it could implement restrictions that prevent the deployment or execution of third-party security agents on virtual machines, containers, or other compute services. This could be done through changes to platform policies, service configurations, or allowed integration frameworks. However, such actions would impact customer flexibility, limit interoperability, and could provoke strong negative reactions and

([353]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.D.A.7.1.

([354]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.A.7.1.

([355]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), questions E.D.A.4 and E.D.A.8; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.D.A.4 and E.D.A.8; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.7 and E.D.A.18.

potential regulatory or antitrust scrutiny, making this a technically feasible but commercially and legally sensitive move.'

(337) According to CNAPP competitors, preventing the installation of agents or the degradation of interoperability based on agents would not possible as it is the customer who controls them. CNAPP competitors explain that 'Preventing competing CNAPP providers from installing agents on GCP workloads would be difficult because agent deployment is controlled by the customer, not the cloud provider. Customers install agents within their own VMs, containers, or Kubernetes clusters using standard OS and orchestration mechanisms; selectively blocking third-party agents would risk breaking legitimate customer workloads, violate expectations of platform neutrality, and raise significant commercial and regulatory concerns, making such behavior unlikely in practice' and that 'Agent installation on cloud workloads is controlled by the customer. CSPs do not typically restrict customer-selected agents at the workload level', and that 'it is typical for a customer to drive agent based integrations, although CSPs do have their own native agents for other uses.' ([356])

(338) While the feedback on technical ability was mixed, customers and competitors alike explained that such strategy would be unlikely. In any event, the Commission considers that the merged entity would not have the ability to engage in a foreclosure strategy as Google does not have a significant degree of market power on the cloud infrastructure and data analytics market.

5.6.4.3.2. Incentive to foreclose

(339) For the reasons set out below, the Commission considers that the merged entity would not have the incentive to foreclose rivals in the CNAPP market by degrading the interoperability of Google's cloud infrastructure with rival CNAPP providers.

(340) As set out in further detail above in Section 5.6.4.3.1 on ability to foreclose, competitors explained that – while the merged entity could have the technical ability to degrade the interoperability of Google's cloud infrastructure with rival CNAPP providers – it would be unlikely to do so as this would have a negative impact on customer operations and lead to reputational damage and regulatory scrutiny.

(341) Indeed, half of the customers expressing an opinion indicated that, in a hypothetical scenario where the interoperability between Google's cloud infrastructure and their CNAPP tool (other than Wiz) would be degraded or delayed, they would move away from Google and switch to other cloud infrastructure provider, or that they would do nothing (i.e., stay with the rival CNAPP provider). Only a minority of customers indicated that they would switch to Wiz. ([357]) Customers explained that such a degradation of interoperability would not be aligned with Google's previous practices, and that it would impact its relationship with customers. One customer notes that 'We believe that customers for Google and other cloud providers expect interoperability with stand-alone security tools as part of an established ecosystem and these customers would complain to Google if they found that this interoperability had been impacted. We would also expect all CNAPP vendors to also complain to Google, which could impact Google's relationship with such vendors in other commercial

([356]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.4.1.
([357]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.23.

areas.' Similarly, another customer explains that 'This does not align with Google's approach to date. Google's current native offering does not restrict - rather Google looks to support multi-cloud. We would not expect, therefore, the hypothetical scenario to become a reality.' ([358])

5.6.4.3.3. Conclusion

(342) In light of the above, the Commission concludes that the Transaction would not significantly impede effective competition on the market for CNAPP as a result of foreclosure of rival CNAPP suppliers through the degradation of their interoperability with Google's cloud infrastructure.

5.6.5. Bundling of CNAPP with cloud infrastructure and/or other security software

(343) The Notifying Party has identified two activities that can be considered as closely related to the CNAPP market in which Google is active, namely (i) the supply of cloud infrastructure, and (ii) the supply of other security software.

(344) As explained in Section 5.3, the Parties' market shares for neither of these latter activities exceed 30%. Nevertheless, for completeness, the Commission will assess in the next sections whether the Transaction will have a significant impact as a result of a potential bundling strategy, whereby the merged entity would start bundling Wiz's CNAPP with Google's cloud infrastructure or vice versa (Section 5.6.5.1) and or would start bundling Wiz's CNAPP with Google's other security software (Section 5.6.5.2). ([359])

5.6.5.1. Commercial bundling of Wiz's CNAPP and Google's cloud infrastructure

(345) Customers that purchase a CNAPP also purchase cloud infrastructure. Google's activities as a provider of cloud infrastructure can therefore be considered as closely related to the supply of CNAPP, where Wiz is active.

(346) The Commission investigated whether the merged entity would have the ability and incentive to start bundling Wiz's CNAPP with Google's cloud infrastructure, either no longer offering Wiz's CNAPP on a standalone basis and forcing customers to use Google's cloud infrastructure (tying), or offering Wiz's CNAPP at a cheaper price as part of a bundle with Google's cloud infrastructure than on a standalone basis.

5.6.5.1.1. The Notifying Party's views

(347) While there is complementarity and commonality of customers between cloud infrastructure and CNAPPs, the Notifying Party considers that this conglomerate relationship does not raise competition concerns.

(348) First, the Notifying Party submits that CNAPPs are generally purchased separately from cloud computing solutions, often by different teams within a

([358]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.D.A.24.

([359]) CISPE (Cloud Infrastructure Services Providers in Europe) initially voiced a concern on its website that Google would be able to lock-in customers into its growing cloud infrastructure through its control of Wiz (see Surely Not Again, European Commission must avoid making the same mistakes as with Broadcom when examining Google's acquisition of Wiz, available at: https://www.cispe.cloud/surely-not-again/). However, based on the discussion during the Commission's meeting with CISPE's Secretariat and the limited level of concern conveyed by CISPE members to CISPE's Secretariat in response to the latter's subsequent consultation with them, CISPE decided not to submit a formal response to the Commission's inquiry.

customer organisation: the development team for cloud computing versus the security team for CNAPPs. The Notifying Party further explains that customers can purchase CNAPPs through various distribution channels, which include software developers, system integrator resellers, or cloud marketplaces. ([360])

(349) Second, the Notifying Party submits that neither Wiz as a CNAPP nor Google as a cloud infrastructure provider has the requisite degree of market power that could trigger any tying or bundling concerns, referring to Wiz's and Google's market shares in the markets for CNAPP and cloud infrastructure respectively. ([361])

5.6.5.1.2. The Commission's assessment

(350) For the reasons set out below and based on the results of the market investigation, the Commission considers, for the purposes of the present Decision, that the merged entity would not neither the ability nor the incentive to bundle Wiz's CNAPP with Google's cloud infrastructure. Therefore, given that the conditions under the Non-Horizontal Guidelines are cumulative ([362]), the Commission does not need to take a position of whether the third condition on whether there would be a significant detrimental effect on competition is satisfied.

5.6.5.1.2.1. Ability to foreclose

(351) For the reasons set out below, the Commission considers that the merged entity would not have the ability to engage in a strategy of bundling Wiz's CNAPP with Google's cloud infrastructure.

(352) First, as set out above in Sections 5.4.3.2 and 5.5.3.2.1 respectively, the Commission considers that Wiz does not have a significant degree of market power in the market for CNAPP and that Google does not have a significant degree of market power in the market for cloud infrastructure and data analytics.

(353) Second, the majority of respondents to the market investigation indicated that CNAPP and cloud infrastructure are typically purchased separately. ([363]) In general, respondents to the market investigation explain that cloud infrastructure is typically purchased first and CNAPP will follow at a later stage, when a customers' cloud activity is more mature. Some customers explain that customers first purchasing a cloud infrastructure solution, in particular if they initially operate on a single cloud, may rely on the cloud-native solution for a while before switching to a third-party vendor. ([364])

(354) While some customers have a single department dealing with the procurement of CNAPP and cloud infrastructure, most customers indicate having separate departments, such as a security department deciding on the CNAPP and the IT operations department deciding on cloud infrastructure. ([365]) A majority of

([360]) Form CO, paragraph 326.
([361]) Form CO, paragraph 326.
([362]) Non-Horizontal Guidelines, paragraphs 93-118.
([363]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.C.2; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.A.1; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.1.
([364]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.C.2.1; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.A.1.1; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.1.1.
([365]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.2 and E.C.A.2.1.

CNAPP suppliers and cloud infrastructure providers also indicate that they usually deal with different departments on the part of the customer. ([366])

(355) In any case, it is clear that the purchasing patterns for each product vary. Indeed, the market investigation confirmed by vast majority that CNAPP and cloud infrastructure are typically not procured around the same time. ([367]) Again, customers refer to different lifecycles of the products and the sequencing of the purchase.

(356) On the different lifecycles of the products, one customer submits that 'it rarely happens simultaneously due to the different roles they play in our technology lifecycle', and another explains that 'Usually renewals are annual and originally they would not have been procured at the same time and so are different.' One more customer sets out that 'Procurement cycles, budget allocation, and project priorities for infrastructure and security tooling tend to be separate.' ([368])

(357) On the sequencing of the purchases, one customer explains that 'cloud-infrastructure procurement precedes security-layer decisions, since CNAPP solutions can only be meaningfully evaluated once the underlying cloud environment has been selected.' Another customer explains that there is a phased approach, and that 'when it [the cloud infrastructure] becomes important enough for the organisation and running business activities, CNAPP can be purchased to secure these environments, and shall be separated form cloud services to ensure independence.' ([369])

(358) Third, while a slight majority of CNAPP competitors and competing cloud infrastructure providers believe that a company offering a CNAPP tool together with cloud infrastructure would gain a competitive advantage over single-product competitors ([370]), an overwhelming majority of customers does not. ([371])

(359) While some customers highlight that there may be pricing benefits or simplified vendor management, many explain that there could only be an advantage 'provided that the quality of the platform is high' and that 'it depends on how good the CNAPP tool offered is, the pricing model, and how innovative the solution offered is.' ([372]) Furthermore, companies would still consider standalone suppliers, explaining that 'there are many third-party vendors that provide CNAPP/CSPM. Choosing cloud infrastructure providers is driven by technology requirements.' ([373]) One customer indicates that 'It is a competitive advantage, but would not leave others unable to compete effectively.' ([374]) This is supported by a CNAPP competitors explaining that customers may have a 'fear of being

([366]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.C.3; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.A.2.
([367]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.C.4; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.A.3; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.3.
([368]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.3.1.
([369]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.3.1.
([370]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question E.C.5; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.A.4.
([371]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.4.
([372]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.4.
([373]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.4.
([374]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.4.

locked into a single vendor', that 'all clouds already offer security products and that doesn't create a concern.' ([375])

(360) Fourth, customers purchase cloud infrastructure and CNAPP from different vendors today, as is shown by the fact that [information on the Parties' customers' workloads]% of workloads secured by Wiz run on AWS and Microsoft Azure ([376]), even if those competing cloud infrastructure providers offer their own CNAPP as well. Similarly, some customers of Google's cloud infrastructure secure their workloads on GCP by using Microsoft's CNAPP, Defender. ([377]) This reflects the essence of the multi-cloud feature of a CNAPP, and is further supported by customer statements that they will look for the best product in its category or the product that best fits its needs: one customer explained that they would 'likely [be] drawn toward market leaders and best of breed capabilities, irrespective of the cloud infrastructure provider's relationship with CNAPP services' ([378]) Along the same lines, another customer said that 'Most organizations acquire CNAPP tools and cloud infrastructure independently, selecting best-of-breed security solutions to complement their chosen cloud provider.' ([379])

(361) Finally, the majority of respondents expressing an opinion considered that the impact of the Transaction in the market for CNAPP and the market for cloud infrastructure and data analytics would be positive or neutral. ([380])

(362) In light of the above, taking into consideration the overall market results and, in particular, given the different purchasing patterns of CNAPP and cloud infrastructure, for the purposes of the present Decision the Commission considers that the merged entity would not have the ability to engage in a strategy of bundling Wiz's CNAPP with Google's cloud infrastructure.

5.6.5.1.2.2. Incentive to foreclose

(363) For completeness, even if the Commission finds that the merged entity would not have the ability to engage in a strategy of bundling Wiz's CNAPP with Google's cloud infrastructure, the Commission also finds that the merged entity would not have the incentive to engage in such a strategy.

(364) Indeed, a majority of customers expressing a view indicated that they would switch to other CNAPP providers if Wiz's CNAPP was only offered as a bundle with Google's cloud infrastructure. Moreover, while a few customers would consider taking the bundle only for existing workloads on Google's cloud infrastructure, not a single customer indicated that they would switch workloads to Google's cloud infrastructure in order to get the bundle. ([381]) This results from Wiz's CNAPP core value as a multi-cloud software and is broadly reflected in the responses to the market investigation: one customer indeed explains that its response would depend on 'if Wiz's offer continue to support multi cloud', while

([375]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.A.4.1.
([376]) Form CO, paragraph 9.
([377]) Form CO, paragraph 203.
([378]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.1.1.
([379]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.1.1.
([380]) Replies to Questionnaire 1 - Phase I market investigation - Competitors (CSP), question F.3; replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question F.3; replies to Questionnaire 3 - Phase I market investigation – Customers, question F.3.
([381]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.5.

another sets out in more detail that 'if the solution cannot run independently of the cloud service provider and cannot scale across multiple clouds, multi-cloud enterprises will be very hesitant to choose it.' ([382]) In relation to the cloud infrastructure, one customer indicates that 'Using and paying GCP for only Wiz while other workloads are on a different CSP would not make sense for us cost-wise' and that 'a forced migration to GCP is unacceptable', and another customer submits that 'we wouldn't want to be obliged to use services we don't want to.' ([383])

(365) If Wiz's CNAPP were available more cheaply as a bundle with Google's cloud infrastructure, some customers indicate that they would not take the combined offering, and others indicate that they would consider it only for existing workloads on Google's cloud infrastructure. However, only two customers (5% of all respondents expressing a view) submit that they would consider moving additional workloads to Google's cloud infrastructure in order to get the cheaper offer. ([384]) It must be clarified that one of these customers is a single-cloud Google customer already, and the other customer indicates that its key business priority is cutting down on cost. ([385]) In general, however, customers note that price is not the only factor and that things like 'the specific terms (e.g., discounts)', 'the quality, features, ability to work with other CSPs' and 'the challenges to be solved within an organisation' weigh into the decision, as reported by a number of different customers. ([386]) These considerations indicate that companies consider that they would consider alternatives to accepting Wiz at a discounted price as part of a bundled offer.

(366) Finally, as set out in detail in Sections 5.4.3.2 and 5.5.3.2.1 respectively, switching between CNAPP suppliers and cloud infrastructure providers is not excluded.

(367) In light of the above, taking into consideration the overall market results and, in particular, the possibility for customers to resist taking a potential bundled offer of Google's cloud infrastructure and Wiz's CNAPP, for the purposes of this Decision the Commission considers that the merged entity would not have the incentive to engage in a successful strategy of bundling Wiz's CNAPP with Google's cloud infrastructure.

5.6.5.1.2.3. Conclusion

(368) In view of the above considerations and in light of the market investigation and the evidence and information available to it, for the purposes of the present Decision, the Commission concludes that the Transaction would not significantly impede effective competition as a result of bundling of Wiz's CNAPP with Google's cloud infrastructure, considering that the merged entity would not have the ability nor incentive to engage in such a strategy.

5.6.5.2. Commercial bundling of Wiz's CNAPP with Google's other security software

(369) Customers that purchase a CNAPP often also purchase other security software. Google's activities as a supplier of non-CNAPP, reactive security software can

([382]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.5.1.
([383]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.5.1.
([384]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.6.
([385]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.6.1.
([386]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.A.6.1.

therefore be considered as closely related to the supply of CNAPP, where Wiz is active.

(370) The Commission investigated whether the merged entity would have the ability and incentive to start bundling Wiz's CNAPP with Google's other, non-CNAPP security software, either no longer offering Wiz's CNAPP as a standalone product and forcing customers to buy other (potentially unwanted) software in addition to Wiz's CNAPP (tying), or offering Wiz's CNAPP at a cheaper price as part of a bundle than on a standalone basis.

5.6.5.2.1. The Notifying Party's views

(371) The Notifying Party submits that there is indeed some complementarity and commonality of customers between CNAPPs and other security software that may give rise to a bundling relationship. Indeed, the Notifying Party explains that this combination of Wiz's software with Google's primarily reactive software underpins part of the rationale for the Transaction and that it will create valuable synergies, enabling it to improve the effectiveness and quality of its security software. ([387])

(372) Nevertheless, the Notifying Party considers that this conglomerate relationship does not raise competition concerns.

(373) First, the Notifying Party submits that neither Wiz as a CNAPP nor Google as a supplier of any other security software have the requisite degree of market power that could trigger any tying or bundling concerns, referring to Wiz's and Google's market shares in the markets for CNAPP and other security software respectively. ([388])

(374) Second, the Notifying Party submits that offering a broader portfolio of security capabilities will allow the Parties to compete more effectively against rivals that already offer a broader portfolio of security capabilities most relevant for cloud applications and workstreams, such as Microsoft, Amazon, TrendMicro, Palo Alto Networks, Fortinet, CrowdStrike, and Broadcom, among others. Neither Google nor Wiz provide an equivalent broad portfolio. ([389])

(375) Third, the Notifying Party sets out that Wiz would be damaged if customers could not mix-and-match a Wiz's CNAPP with third-party reactive security offerings. ([390]) Furthermore, Google's current and past commercial strategy has been to maintain the ability to mix-and-match security products, as is shown by SecOps, Threat Intelligence and Mandiant being available for purchase on a standalone basis. ([391]) The Notifying Party considers that this is in line with industry practice and submits that no other security software vendors offer their CNAPP exclusively under a broader security bundle without standalone sales, allowing to meet the needs of a broad and diverse customer base (including phased adoption strategies or the purchase of a third-party product in another product category). ([392]) The Notifying Party further confirms that it does not have

([387]) Form CO, paragraph 326.
([388]) Form CO, paragraph 326.
([389]) Form CO, paragraph 326.
([390]) Parties' response to RFI 17, paragraph 4.7.
([391]) Parties' response to RFI 17, paragraph 4.7.
([392]) Parties' response to RFI 17, paragraph 4.7.

any existing plans to stop offering Wiz as a standalone tool, for instance by pursuing a pure bundling strategy. ([393])

5.6.5.2.2. The Commission's assessment

(376) For the reasons set out below and based on the results of the market investigation, the Commission considers, for the purposes of the present Decision, that the merged entity would not have the ability nor the incentive to bundle Wiz's CNAPP with Google's other security software. Therefore, given that the conditions under the Non-Horizontal Guidelines are cumulative ([394]), the Commission does not need to take a position as to whether the third condition relating to the existence of a significant detrimental effect on competition is satisfied.

5.6.5.2.2.1. Ability to foreclose

(377) For the reasons set out below, the Commission considers that the merged entity would not have the ability to engage in a strategy of bundling Wiz's CNAPP with Google's other security software.

(378) First, as set out above in Section 5.4.3.2, the Commission considers that Wiz does not have a significant degree of market power in the market for CNAPP.

(379) Second, the majority of CNAPP competitors and customers expressing a view in the market investigation indicated that CNAPP and other security software are typically purchased separately. ([395]) A significant number of customers explain that this because they will always choose the best tool for each business need at the time when it is needed. ([396])

(380) While the market investigation clearly confirms that CNAPP and other security software are often procured by a single department within a company, as confirmed by approximately 80% of customers expressing a view ([397]), the same proportion of customers expressing a view indicate that the purchasing patterns for CNAPP and other security software vary. ([398]) Some customers point at the different lifecycle of security software as the cause, with one customer explaining that 'different vendors offer multi-year agreements that may not co-terminate with other products.' Others indicate that the choice and timing of the security software typically follow the needs of the business, with customers explaining that 'the procurement of security tools typically follows the internal priorities', that 'tools are typically procured based on capability maturity needs', or that the decision is 'based on specific project needs, budget cycles, and organizational priorities.' ([399])

(381) Third, a majority of CNAPP competitors and customers taking a view believe that a company offering a CNAPP tool together with other security software would

([393]) Parties' response to RFI 17, paragraph 4.6.
([394]) Non-Horizontal Guidelines, paragraphs 93-118.
([395]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.B.2; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.2.
([396]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.B.2.1; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.2.1.
([397]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.B.3; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.3.
([398]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.4.
([399]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.4.1.

gain a competitive advantage over single-product competitors. ([400]) Some customers explain that a centralised platform may bring increased quality and cost reductions. In addition, a number of customers clarify that a broader portfolio would bring advantages if the tools were fully integrated and not offered as silos within a single bundle, in line with a market trend to consolidate cybersecurity solutions. However, some customers who believe that a bundled offer could present a competitive advantage emphasise that this would not block other suppliers from competing. Some of the almost 30% of customers who do not believe that a bundled offer would present a competitive advantage highlight that this could dilute the competitiveness of a CNAPP solution by bundling less performant software with a strong security solution. ([401])

(382) Finally, the majority of CNAPP competitors and almost all customers consider that the impact of the Transaction on their overall business would be positive or neutral. ([402])

(383) In light of the above, taking into consideration the overall market results and, in particular, given the different purchasing patterns of CNAPP and other security software, for the purposes of the present Decision the Commission considers that the merged entity would not have the ability to engage in a successful strategy of bundling Wiz's CNAPP with Google's other security software.

5.6.5.2.2.2. Incentive to foreclose

(384) For completeness, even if the Commission finds that the merged entity would not have the ability to engage in a strategy of bundling Wiz's CNAPP with Google's other security software, the Commission also finds that the merged entity would not have the incentive to engage in such a strategy.

(385) Indeed, a majority of customers expressing a view indicated that they would switch to other CNAPP providers if Wiz was only offered as a bundle with Google's other security software. ([403]) Other customers generally indicated that they would consider the value proposition of the bundle and decide on that basis, indicating that they consider that they have an option to reject the bundle if it does not fit their business needs. A few customers indicate that they are already customers of Google for its other security software, and a bundle would therefore not make a difference in practice. ([404])

(386) If Wiz's CNAPP were available more cheaply as a bundle with Google's other security software, of all customers who expressed a view in the market investigation, more said they would not take the bundle than those who said they would. ([405]) Most customers remain undecided, however, and explain that they would at least consider the bundle looking at quality and capabilities of the software involved, the overall price, and the security needs of their company. ([406])

([400]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question E.C.B.5; replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.5.
([401]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.5.1.
([402]) Replies to Questionnaire 2 - Phase I market investigation – Competitors (CNAPP), question F.1; replies to Questionnaire 3 - Phase I market investigation – Customers, question F.1.
([403]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.6.
([404]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.6.1.
([405]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.7.
([406]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.C.B.7 and E.C.B.7.1.

This is consistent with the Notifying Party's view that customers value the ability to mix-and-match.

(387) While it is clear that customers consider that there could be some benefits to a bundle, it is clear that they consider they have the opportunity to reject the bundle if they are not interested and would react if they were forced to take the bundle. Furthermore, as set out in detail in Section 5.4.3.2, switching between CNAPP suppliers is a real option.

(388) In light of the above, taking into consideration the overall market results and, in particular, the possibility for customers to resist taking a potential bundled offer of Wiz and Google's other security software, for the purposes of this Decision the Commission considers that the merged entity would not have the incentive to engage in a strategy of bundling Wiz's CNAPP with Google's cloud infrastructure.

5.6.5.2.2.3. Conclusion

(389) In view of the above considerations and in light of the market investigation and the evidence and information available to it, for the purposes of the present Decision, the Commission concludes that the Transaction would not significantly impede effective competition as a result of bundling of Wiz's CNAPP with Google's other security software, considering that the merged entity would not have the ability nor incentive to engage in such a strategy.

5.6.6. Leveraging of Google's position in specialised generative AI

(390) The Notifying Party has identified one potential market where Google's market share exceeds 30% that may be considered as being closely related to the market for CNAPP, namely a potential market for specialised generative AI.

(391) Some CNAPPs integrate third-party generative AI tools to improve threat detection and response capabilities or enhance user interfaces (e.g., chatbots) without the customer needing to separately license generative AI tools from third parties. Others rely on in-house generative AI technologies. Customers can also use their preferred generative AI models to process inputs or outputs of CNAPPs with or without integration. ([407])

(392) Generative AI is used thus as an input for CNAPPs, and Google has a market share of [30-40]% in a potential market for specialised generative AI, as described above in Section 5.3.3.

(393) The Commission has examined whether the merged entity would have the ability and incentive, post-Transaction, to foreclose rival providers of CNAPPs by leveraging Google's position in the market for specialised generative AI. In this regard, in its market investigation, the Commission has sought to verify whether the merged entity would likely have the ability and the incentive to refuse or degrade access to Google's specialised generative AI.

5.6.6.1.1. The Notifying Party's views

(394) The Notifying Party submits that there may be some complementarity and commonality of customers between generative AI models and CNAPPs, but that this relationship does not give rise to competition concerns.

([407]) Form CO, paragraph 235.

(395) First, the Notifying Party points out that the market shares as reported by Gartner ([408]) are modest and vitiated by several methodological errors. The Notifying Party explains that the subsegment for specialised generative AI as reported on by Gartner includes generative AI models that focus on fulfilling domain-specific tasks as well as small-language models that are not domain-specific. The segment is agnostic as to the type of use case for which the model is deployed. ([409]) Furthermore, the Notifying Party submits that any generative AI models that are currently integrated with CNAPPs are foundation models rather than specialised models, and that Google does not offer any specialised generative AI model that is used for cybersecurity.

(396) In any event, the Notifying Party submits that the Transaction would not give rise to foreclosure concerns for the following reasons.

(397) In terms of **ability**, the Notifying Party submits that Google does not have a significant degree of market power in specialised generative AI with a market share of [30-40]% globally and [30-40]% in Europe. Furthermore, foreclosure would not be possible given that no CNAPP provider currently needs or uses Google's specialised generative AI models. Finally, Google would continue to be constrained by many competitors. ([410])

(398) In terms of **incentives**, the same arguments preclude Google from commercially tying or bundling these products together. In view of their relative sizes, the Notifying Party submits that there is no incentive to sacrifice in the generative AI market in an attempt to benefit in the CNAPP market, and that any upside of foreclosure would be minor and speculative. ([411])

(399) In terms of **effects**, the Notifying Party submits that Google will continue to face competition from similarly integrated rivals such as Microsoft, and non-integrated CNAPP rivals who could partner with the more than 10 alternative specialised generative AI providers to replicate the bundle. ([412])

5.6.6.1.2. The Commission's assessment

(400) Contrary to the Notifying Party's submission, the results of the market investigation indicate that specialised generative AI is used in combination with CNAPP. Indeed, 58% of CNAPP competitors indicated that specialised generative AI is used in security software products, either for specific functionality or more broadly ([413]), and 39% of CNAPP competitors responded that they integrate specialised generative AI into their CNAPP tool. ([414]) This was also confirmed by a significant number of customers, 50% of which confirmed that specialised generative AI is used in security products to some extent. ([415]) Given that the market investigation confirms the complementarity between both products, this Section assesses whether the merged entity would have the ability or incentive to foreclose competing CNAPP suppliers by refusing or degrading their access to Google's specialised generative AI.

([408]) See Section 5.3.3.
([409]) Form CO, paragraph 32.
([410]) Form CO, paragraphs 32 and 326.
([411]) Form CO, paragraph 326.
([412]) Form CO, paragraph 326.
([413]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question D.A.C.2.
([414]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.A.17.
([415]) Replies to Questionnaire 3 - Phase I market investigation – Customers, question D.A.C.2.

(401) For the reasons set out below and based on the results of the market investigation, the Commission considers, for the purposes of the present Decision, that the merged entity would not have the ability to foreclose competing CNAPP suppliers by refusing or degrading their access to Google's specialised generative AI. Therefore, given that the conditions under the Non-Horizontal Guidelines are cumulative ([416]), the Commission does not need to take a position as to whether the second condition relating to the merged entity's incentive to engage in such practice, or the third condition relating to the existence of a significant detrimental effect on competition, are satisfied.

5.6.6.1.2.1. Ability to foreclose

(402) For the reasons set out below and based on the results of the market investigation, the Commission has reached the conclusion that the merged entity would not have the ability to engage in a foreclosure strategy vis-à-vis rival CNAPP suppliers by refusing or degrading access to Google's specialised generative AI models.

(403) First, Google does not have a significant degree of market power in a potential worldwide market for specialised generative AI. The market investigation confirmed that there are many alternatives to Google in the generative AI space, including specialised generative AI. These alternatives include OpenAI, Mistral AI and Databricks, ([417]) as is confirmed by Gartner's report mentioned in Section 5.3.3. ([418]) Today, Google does not offer specialised generative AI models for cybersecurity use cases.

(404) Second, only 23% of CNAPP competitors consider specialised generative AI to be a material input for CNAPP tools. ([419]) While a large majority of CNAPP competitors and approximately half of the responding customers expects significant developments in terms of the integration of specialised generative AI within CNAPP tools ([420]), the overall feedback from the market investigation shows that a lot of continued innovation is expected, including from new companies attracting investments. ([421]) One respondent explained that '[t]he cloud computing industry, including cloud security, is highly dynamic, rapidly evolving, and characterised by unprecedented levels of investment and innovation' and that '[t]he increasing prevalence of AI-driven workloads and tools is also disrupting the market and creating opportunities for new and existing entrants.' Another respondent said that they expect to see continued innovation and 'significant VC funding, new companies all the time.' ([422])

(405) Therefore, the Commission concludes that the merged entity would not have the ability to engage in any foreclosure strategy by refusing or degrading access to Google's specialised generative AI models.

([416]) Non-Horizontal Guidelines, paragraphs 93-118.

([417]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.A.21: Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.21.

([418]) See Table 37 in Section 5.3.3.

([419]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.A.19.

([420]) Replies to Questionnaire 2 - Phase I market investigation - Competitors (CNAPP), question E.A.20; Replies to Questionnaire 3 - Phase I market investigation – Customers, question E.A.20.

([421]) Replies to Questionnaire 2 – Phase I market investigation – Competitors (CNAPP), question E.A.20.1.

([422]) Replies to Questionnaire 2 – Phase I market investigation – Competitors (CNAPP), question E.A.20.1.

5.6.6.1.2.2. Conclusion

(406) In light of the above, the Commission concludes that the Transaction would not significantly impede effective competition on the market for CNAPP as a result of foreclosure of rival CNAPP suppliers by refusing or degrading access to Google's specialised generative AI models.

5.6.7. Conclusion

(407) In view of the above considerations and in light of the results of the market investigation and the evidence and information available to it, the Commission concludes that the Transaction does not raise serious doubts as to its compatibility with the internal market as a result of conglomerate effects, notably by foreclosing rival competitors in the markets for cloud infrastructure, CNAPP, or other security software, considering that the merged entity would have neither the ability nor the incentive to engage in such strategy.

6. CONCLUSION

(408) For the above reasons, the European Commission has decided not to oppose the notified operation and to declare it compatible with the internal market and with the EEA Agreement. This decision is adopted in application of Article 6(1)(b) of the Merger Regulation and Article 57 of the EEA Agreement.

For the Commission

(Signed)
Teresa RIBERA
Executive Vice-President