Google

21 June 2023

FTC INQUIRY INTO CLOUD COMPUTING BUSINESS PRACTICES
Docket ID FTC-2023-0028
Google Cloud's response to the FTC's call for public comments

Google Cloud welcomes the opportunity to comment on the FTC's sector inquiry into the business practices of cloud computing providers in the U.S. Google Cloud is competing with large incumbent providers with large established cloud customer bases,[1] and we are proud to have championed a procompetitive, multicloud[2] approach that empowers customers to multihome[3] and choose multiple providers best suited to specific customer needs. This multicloud approach increases reliability, security, and redundancy within the cloud system overall by reducing the risk of a single point of failure. Multicloud has also been shown to drive price competition and innovation in cloud services. Google Cloud urges the FTC to closely examine any practices that seek to undermine customers' ability to deploy a multicloud strategy by locking in customers and ultimately preventing customers from reaping the full economic, efficiency, and security benefits that cloud computing has to offer.

1. INTRODUCTION

Cloud computing is an important development in the economy in the last decade. It has reduced costs, improved security, simplified portability and interoperability, and delivered services with unprecedented reach. The cloud services industry plays an important role in the growth of U.S. businesses and delivers substantial benefits to the U.S. economy, allowing businesses to rapidly scale, significantly reduce their IT spend, and facilitate digital transformations. Indeed, the value of this migration to the cloud is reflected in the Federal Government's IT modernization effort, which is designed to capture the additional savings, security, and faster services that the cloud can offer.[4]

At Google Cloud, our design principles start with a deep belief that a secure, open cloud[5] approach will best serve our customers. Google Cloud believes customers should have the choice, flexibility, and openness they need to build optimal solutions for their business problems. So we aim to offer customers flexibility to run their businesses how they want. To do this, we encourage a multicloud, hybrid architecture designed to quickly adapt as a customer's organization evolves, regardless of the cloud platform(s) from which they wish to run their businesses. By pioneering key technologies that facilitate multicloud adoption, Google Cloud empowers customers to mix-and-match between different cloud services. More than anything else, Google Cloud believes customers should use our services because of the value that our services provide in supporting business objectives, not because they are locked in.[6]

While interoperability and open source technologies are prevalent across the industry (including in response to increasing demand from customers seeking to deploy a multicloud approach), a small number of legacy on-premises software providers, such as Microsoft, Oracle, and others, are using their strong positions in non-cloud markets, such as productivity software, server operating systems

---

[1] See for example, para 6.44 of Ofcom, Interim report (April 2023) published as part of its ongoing market study.
[2] Multicloud is when an organization uses cloud computing services from at least two cloud providers to run their applications. The freedom to create a strategy that utilizes multiple vendors enables customers to pick and choose the capabilities that best suit their specific business needs and minimize vendor lock-in. See also Google Cloud, What is multicloud? Definition and Benefits.
[3] Multihome is the practice of configuring one computer with more than one network connection and IP address.
[4] See Federal Cloud Computing Strategy, From Cloud First to Cloud Smart for more detail on the U.S. government's Cloud Smart strategy. See also FedRAMP, Securing cloud services for the Federal Government for more detail on Federal Risk and Authorization Management Program.
[5] See Google Cloud, Why open cloud?.
[6] See Google Cloud, Data Portability and Interoperability (January 2023).

and applications, and desktop operating systems, to give their own cloud products an unearned advantage and lock customers into their cloud ecosystems.

The cloud industry is currently at an inflection point in the contest between legacy software constructs—restrictive licensing, closed ecosystems, and creating anticompetitive barriers—and the cloud's original promise and potential—open, elastic, and free from artificial lock-ins. At this critical moment, anticompetitive licensing restrictions on cloud services are causing a wide range of harms, from higher costs for businesses and end-consumers, to government waste for taxpayers, to more security breaches, to a chilling effect on local cloud and software providers.[7] Google Cloud urges the FTC to closely scrutinize and address such practices.

We set out below some broad observations relevant to the FTC's questions on competition in cloud and cloud security, including an overview of cloud computing, the importance of multicloud to unlock the benefits and security of cloud—a core principle of Google Cloud's own offering—and the risks to fair competition and security in the cloud as a result of the harmful practices of certain legacy on-premises players.

2. CLOUD COMPUTING AT A GLANCE

For most businesses, managing their own IT infrastructure is burdensome and costly. Public cloud computing offerings dramatically reduce these burdens by offering quick deployment, scalability, affordability, and ease of maintenance, thereby enabling companies to refocus resources on their core businesses. Unlike traditional on-premises IT, cloud computing allows customers to store data remotely and access software programs on demand. This means that any business with an internet connection can access a wide range of cloud-based tools and services, from infrastructure to artificial intelligence (AI) and data analytics capabilities.

Due to its flexible consumption model, cloud computing is highly adaptable to individual customer needs, whether they are large international financial institutions, telecommunications providers and broadcasters, or small and medium-sized start-ups. Customers can "self-serve," using cloud computing systems immediately on a pay-per-use basis. This allows customers to scale up their use of cloud services as demand increases and scale it back (or shut it down entirely) if demand drops. Companies using the cloud for their IT needs do not need to hire or train personnel to operate the stack of hardware and software underlying the services that they use, which are fully managed by the cloud provider. Cloud computing thereby minimizes the high costs and delays that characterize the provision of IT services in the pre-cloud era.[8]

The shift to cloud also allows greater workload flexibility, better server utilization rates, and a more energy-efficient infrastructure.[9] In addition to these operational efficiencies, cloud-enabled businesses are better empowered to understand how best to serve their own customers via cloud-based services and technologies. This accelerates innovation across the economic value chain.

Cloud services are typically classified according to their service models: infrastructure-as-a-service

[7] See Google Cloud, Ensuring fair and open competition in the cloud (October 20, 2022).
[8] See for example, page 12 of ACM, Market Study Cloud services (August 2022).
[9] A Google Cloud data center is twice as energy efficient as a typical enterprise data center and matches 100% of Google Cloud's annual electricity use with renewable energy. For further details see Google Cloud, Cloud Sustainability.

(IaaS),[10] platform-as-a-service (PaaS),[11] and software-as-a-service (SaaS).[12] The service models are differentiated by the level of control the customer has over the management and maintenance of the computing resources.[13] However, the level of control that an enterprise has over its workloads can be scaled up and down far more flexibly than the IaaS/PaaS/SaaS segmentation suggests. Consequently, segmentation based on these categories would be artificial and would not provide a solid basis for conclusions on market definition. Google does not itself allocate products and services between the IaaS, PaaS, and SaaS categories in the normal course of business. In addition, some services do not 'fit' neatly into these service models. Recently the UK regulator Ofcom acknowledged that their most suitable 'placement' is a topic of ongoing discussion in the wider professional community.[14] Some suppliers of cloud services instead may group their services by different computing capabilities. Cloud providers may split cloud services into categories such as virtual machines, storage as a service, container as a service (CaaS), database as a service (DBaaS), and disaster recovery as a service (DRaaS).[15]

Google Cloud incorporates Google's IaaS and PaaS offerings[16] and officially launched in 2012[17] as a competitor to well-established players like Amazon Web Services (AWS) and legacy hardware and software vendors like Microsoft, IBM, and Oracle.[18] Google Cloud was launched with a mission to accelerate every organization's ability to digitally transform and reimagine its business through data-powered innovation.

According to data from Synergy Research Group and Statista, AWS and Microsoft Azure are the two largest players in the provision of cloud infrastructure services by some margin.[19] This is also reflected in Ofcom's findings as part of its market study into cloud services where AWS and

---

[10] Infrastructure services provide access to raw computing resources for processing workloads and storing data. These are in the form of servers and networking equipment owned and managed by the IaaS provider (and are typically held on racks in a remote data center).

[11] Platform services provide access to a virtual environment for customers to develop, test, deploy, and run applications. Key categories of PaaS products include databases, analytics platforms, and containers. The overall virtual environment and the underlying raw computing resources are typically owned and managed by the same cloud provider. However, the individual PaaS services may be supplied by the cloud provider or by independent software vendors. The customer has less control over the cloud stack compared to IaaS: they still manage applications and data, but not the PaaS computing platform.

[12] Software solutions are complete applications. Cloud software applications can be offered by the cloud provider that owns the underlying raw computing resources or by an independent software vendor (ISV). The provider of the SaaS manages all hardware and software. In general, most modern consumer and business facing applications are SaaS, including communications services (e.g., Gmail and WhatsApp), productivity software (e.g., Google Workspace), and CRM software (e.g., Salesforce Sales Cloud).

[13] See para 3.18 of Ofcom, Interim report (April 2023) for descriptions of IaaS, PaaS, and SaaS. See also NIST, NIST Definition of Cloud Computing (2011). The NIST Definition of Cloud Computing also sets out the different cloud deployment models: (i) private (cloud infrastructure provisioned for use by a single organization), (ii) community cloud (provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns), (iii) public cloud (provisioned for open use by the general public), and (iv) hybrid cloud (composition of two or more distinct cloud infrastructures, e.g., private, community, or public, that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability).

[14] See para 3.17 of Ofcom, Interim report (April 2023).

[15] *Id*., para 3.22.

[16] *Id*., para 3.58.

[17] Google's first cloud products, including its first PaaS offering, Google App Engine, were released in 2008 as a preview version. Google App Engine became generally available in November 2011. Google's first IaaS offering, Compute Engine was released in June 2012, in the same year that Google's specialist cloud team, Google Cloud, was created, which later combined with the initial team that marketed Google Apps to form the Google Cloud business (as it is known today) in September 2016.

[18] See para 1.8 of Ofcom, Interim report (April 2023).

[19] See Synergy Research Group, Cloud Spending Growth Rate Slows But Q4 Still Up By $10 Billion from 2021; Microsoft Gains Market Share (February 6, 2023). See also Statista, Big Three Dominate the Global Cloud Market (April 28, 2023).

Microsoft are stated to be "the clear market leaders" in cloud infrastructure.[20] Beyond these two largest players is a dynamic set of smaller competitors such as Google Cloud, Alibaba, Kyndryl (formerly part of IBM), Oracle, VMWare, Cloudera, and Colt, among others. There are also a plethora of cloud software providers who offer SaaS products (e.g., communications, HR, finance, productivity, and customer relationship management software). In addition, partners such as resellers of cloud products and services and independent software vendors (ISVs) also play a key role in ensuring that end customers have a strategic partner who can advise on all their cloud services needs.

Google Cloud entered the market without building on pre-existing positions in on-premises software or legacy IT products. Google Cloud and others have focused on growing their businesses by responding to customer dissatisfaction with traditional IT service providers and offering flexible and innovative products that support and enable a multicloud approach.[21]

3. INTEROPERABILITY AND OPENNESS ARE AT THE HEART OF GOOGLE CLOUD'S PROPOSITION AND ENSURE ROBUST COMPETITION, CUSTOMER CHOICE, AND INCREASED SECURITY

Multicloud refers to using services from more than one public cloud provider at the same time. The primary goal of Google Cloud's multicloud strategy is to give customers flexibility to operate with the best computing environment for each workload even if these are from different cloud providers. Multicloud deployments interconnect services from separate cloud environments for different purposes without having to connect the third-party clouds.[22]

A multicloud approach provides many customer benefits including (i) allowing customers to choose the best from each cloud to optimize workloads based on factors like speed, performance, reliability, geographical location, security, and compliance requirements; (ii) avoiding vendor lock-in; (iii) increased cost efficiency; (iv) benefiting from new innovations from different cloud providers; and (v) increased reliability and redundancy.[23]

This level of flexibility is facilitated through interoperability, a term which is used to describe the ability for different systems to interact and work together. For cloud service providers (CSPs), interoperability refers to the ability for cloud services and customer systems to understand each other's application programming interfaces (APIs), configurations, authentication, and customer data formats. In the era of the distributed cloud,[24] openness and interoperability empower faster innovation, tighter security, and freedom from vendor lock-in.[25]

From the outset, Google Cloud has been a strong advocate of facilitating interoperability, multicloud, and customer choice (as explained here) by investing heavily in open source technologies,[26] ensuring that its APIs are freely available and facilitating data portability.[27]

---

[20] See para 1.6 of Ofcom, Interim report (April 2023).
[21] According to IDC, multicloud has become a preferred way for the public sector to address regulatory concerns and leverage the best services from different providers.
[22] See Google Cloud, What is multicloud? Definition and Benefits.
[23] *Id*.
[24] See Google Cloud, Google Distributed Cloud on how the distributed cloud allows you to run public cloud infrastructure in multiple locations.
[25] See Google Cloud, Data Portability and Interoperability (January 2023).
[26] As discussed above, open source is a foundational element of Google's strategy. Since starting out, Google has initiated 9,000 active open source projects that it continues to maintain today. See IDC, IDC Research: The Power of the Database for the Cloud: SaaS Developer Perspectives (January 2020) on how businesses can modernize their applications with open source software using Google Cloud.
[27] See Google Cloud, Data Portability and Interoperability (January 2023) for additional detail.

Open source and Open APIs

Open source and open source-based technologies (such as containers, open APIs, and open source databases) are enablers of multicloud and often go hand-in-hand with increasing customer choice, as they support movement of workloads and data across different cloud environments.[28]

Google Cloud has a long history of sharing technology through open source for the wider benefit of the cloud community. For example, Google invented, developed, and subsequently made open source Kubernetes. Kubernetes has since become the industry standard in container portability and interoperability in the cloud driving competition. Another example is TensorFlow, a free and open source software library for machine learning and artificial intelligence originally developed by Google and made open source. Google Cloud is also a top contributor to the Cloud Native Computing Foundation—an open source development community—with 50%+ of code commits. This is a key differentiator of Google Cloud and lies at the heart of its customer-centric proposition.

APIs are the gateways that connect different data sources to each other. Open APIs are openly accessible and thereby preserve the cloud ecosystem's ability to build on each other's work, improve software iteratively and collaboratively, and adopt multicloud strategies. Google Cloud strives to make as many of its APIs open and by doing so enables third-party developers (including competing developers) to freely develop products and services that can be deployed using Google Cloud's infrastructure.

Data portability

Cloud data portability is facilitated through common technical standards that allow for the exporting of customer data in a way that can be readily uploaded and utilized across different platforms, including other CSPs. It provides customers with several advantages—from providing flexibility on how workloads can be structured and reducing third-party concentration risk, to increasing operational resilience in the event of an outage. Cloud data portability also enables customers to gain access to new and emerging cloud technologies with minimal friction or barriers, which is a key attraction for customers seeking to increase their utilization of cloud services. Importantly, cloud data portability allows customers to easily transfer their workloads between cloud environments, adopt a multicloud or hybrid cloud strategy, and even migrate back to on-premises environments as needed.[29]

Google Cloud offers a number of services that directly facilitate customers' use of multiple cloud providers—from our managed application platform (Anthos), to our fully-managed, multicloud analytics solution (BigQuery Omni)—allowing customers to harness the power of data and AI through our open APIs, machine learning services, and analytics engines on any of the major cloud platforms.

In April 2022, Google Cloud announced a new Data Cloud Alliance to make data more portable and accessible across disparate business systems, platforms, and environments—with a goal of ensuring that access to data is never a barrier to digital transformation. Data Cloud Alliance works with industry leaders with the aim of promoting open standards and interoperability.

Security and operational resilience in cloud

In its 2023 U.S. National Cybersecurity Strategy, the Biden Administration affirmed the benefits of cloud computing in terms of cybersecurity and the resilience of how cloud protects U.S. critical

[28] See for example, IDC, How a multicloud strategy can help regulated organizations mitigate risks in cloud (March 2021) regarding the benefits of multicloud.
[29] See Google Cloud, Data Portability and Interoperability (January 2023).

infrastructure: "[c]loud-based services enable better and more economical cybersecurity practices at scale, but they are also essential to operational resilience across many critical infrastructure sectors."[30] The strategy similarly recognizes cloud computing as a critical enabler of U.S. government modernization and transition to secure architectures, with direct benefits for the U.S. public: "[r]eplacing legacy systems with more secure technology, including through accelerating migration to cloud-based services, will elevate the cybersecurity posture across the Federal Government and, in turn, improve the security and resilience of the digital services it provides to the American people."

We could not agree more. Cloud computing is one of the single-most important tools in our nation's effort to improve cybersecurity and defend critical infrastructure, American businesses, and consumers from malicious cyber activity. This is because cloud computing lowers the barriers to achieving state-of-the-art security for organizations of all sizes and budgets. Cloud takes advantage of economies of scale to minimize the marginal cost of additional investments in security controls and expertise and of implementing them at global scale. This benefits customers, especially small- and mid-sized businesses, who may not have the resources or access to expertise to implement comparable cyber defenses on their own.[31] In a recent blog post, Eric Goldstein, Executive Assistant Director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), urged "all [small and mid-sized businesses] with on-prem systems to migrate to secure cloud-based alternatives as soon as possible."[32]

One of the reasons that customers choose Google Cloud is its ability to offer high levels of security at scale. Google Cloud embraces the principles of security-by-design and security-by-default with robust security controls, including multiple layers of encryption, purpose-built security chips, and strong default security configurations embedded in our infrastructure. Google Cloud maintains high standards for our hardware and software supply chains to minimize the risk of compromise. Google Cloud works continuously to deliver new secure tools and features, as well as resources and guidance to help our customers minimize configuration errors and achieve security in the cloud.

Google was an early pioneer of Zero Trust—the idea of achieving security by continuously monitoring and validating every user, device, and service in exchange for access to systems and data—and Google Cloud implements Zero Trust throughout its global infrastructure by default. In addition, Google Cloud offers customers an integrated suite of security SaaS tools to help customers evaluate their cyber defenses, hunt for anomalous activity on their networks and devices, detect intrusion, and respond in real-time. With our acquisition of Mandiant, we're actively providing our customers new capabilities to anticipate threats before they occur with industry-leading threat intelligence and enabling them to automate and accelerate their incident response efforts.[33] Most importantly, Google Cloud is committed to an open end-to-end ecosystem and opens its security platform to integrations from competitors, as well as offering new plug-ins for other vendors' security tools to the benefit of overall cloud security and customers.[34]

---

[30] See The White House, National Cybersecurity Strategy (March 2023).
[31] See Google Cloud, Megatrends drive cloud adoption—and improve security for all on how a focus on security can help to fuel cloud adoption (January 12, 2022).
[32] See Cybersecurity and Infrastructure Security Agency, Accelerating Our Economy Through Better Security: Helping America's Small Businesses Address Cyber Threats (May 2, 2023).
[33] See Google Cloud, Megatrends drive cloud adoption—and improve security for all (January 11, 2022).
[34] See Axios, Exclusive: Google opens its security tools to competitors' platforms (April 24, 2023) on Google's recently announced plans to allow customers to integrate various threat intelligence and product security solutions into its offerings.

In addition, as set out above, Google Cloud is a leader in multicloud computing—a fundamental tool to build resilience within the system and improve security. Multicloud can address sovereignty and security requirements by reducing technical dependencies on a single vendor. Google Cloud's products have openness and multicloud at their core. We apply the same Zero Trust innovations that protect Google's own infrastructure, employees, and data to secure the connections between applications running in Google Cloud, in our competitors' clouds, and in our customers' on-premises environments. By enabling customers to distribute applications and data securely across multiple cloud environments, multicloud significantly reduces the risk of unplanned downtime or outages through removing a single point of failure. As a result, an outage in one cloud won't necessarily impact services in other clouds, and if a customer's primary cloud provider goes down, computing needs can be routed to another cloud that's ready to go, and ultimately results in a more secure and resilient cloud architecture.[35]

4. UNFAIR LICENSING RESTRICTIONS FROM LEGACY ON-PREMISES PROVIDERS ARE UNDERMINING THE SUBSTANTIAL BENEFITS OF CLOUD COMPUTING

Cloud computing in the U.S. is innovative, dynamic, and competitive with low barriers to entry. New entrants do not need to incur significant capital costs to begin supplying cloud infrastructure services.[36]

Google Cloud nevertheless shares a concern, which many others, including customers and partners have also voiced (see below), that licensing terms enforced by Microsoft, Oracle, and other legacy on-premises software providers distort competition in the cloud. With overly complex agreements that seek to lock in clients to their ecosystems, these legacy software providers are aiming to turn their on-premises software monopolies into anticompetitive cloud monopolies. In doing so, they are not only forcing customers toward a monolithic cloud model but also limiting choice, increasing costs for customers, and disrupting growing and thriving digital ecosystems in the U.S. and around the world.[37]

Microsoft provides a significant example. It recognizes customers rely on its dominant, on-premises software products, such as Windows Server and Microsoft Office, and seeks to unfairly leverage that dominance into the nascent cloud market. It uses restrictive and discriminatory licensing and other harmful practices, such as limiting the technical interoperability of must-have security software (e.g., Active Directory) on non-Azure cloud infrastructure. For example, enterprise and public sector customers with expansive portfolios of previously purchased, on-premises Microsoft software are faced with increasing restrictions, prohibitions, and surcharges when they attempt to migrate those on-premises workloads to an Azure competitor. These restrictions don't have any technical justification and didn't otherwise exist when those customers originally bought the software from Microsoft. Instead, Microsoft has over time rolled out a series of changes to previously purchased, on-premises software licenses that essentially force customers to migrate the software to Azure. In 2019, for example, Microsoft announced Windows Server would no longer be eligible to migrate to certain Azure competitors.[38] Other software like SQL Server could be eligible to migrate only if

[35] See Google Cloud, Data Portability and Interoperability (January 2023).
[36] For example, instead of building the infrastructure from scratch, a newer provider can reduce the time and capital cost of entry by leveraging third-party telecommunications networks and data center services (e.g., space, power, HVAC, and physical security). There are many such third-party providers, including in the U.S. By way of example, OVH started as a small web hosting service provider in France in 1999. By 2001, it had already opened its first (rented) data center in Paris, followed by a wholly-owned data center two years later. Today, it has 33 data centers in 8 countries around the globe, including in the U.S. See OVHcloud, The OVH Story: 20 years of Innovation.
[37] See Google Cloud, Ensuring fair and open competition in the cloud (October 20, 2022).
[38] See Microsoft, Updated Microsoft licensing terms for dedicated hosted cloud services (August 1, 2019).

customers also purchased an add-on benefit for a surcharge. Notably, Microsoft applied these licensing changes inconsistently across its software, and targeted customers who were considering using select Azure competitors.[39] Many of these restrictions, however, are not applicable if the customer migrates these applications to Azure.

Microsoft's complex web of licensing restrictions prevents customers, particularly its existing on-premises enterprise clients, from choosing any other cloud provider at the time of migration into the cloud and ultimately locks those customers into its Azure ecosystem. As a result, competition on the merits is prevented, depriving customers of the ability to choose the best cloud services for their needs and denying their ability to implement an effective multicloud strategy with associated security and resiliency benefits. These harmful practices stifle competition in the growing cloud services market and result in significant additional costs for U.S. customers who wish to deploy on any cloud provider that is not Microsoft Azure.

Concerns surrounding Microsoft's behavior in leveraging its dominance in adjacent markets into cloud are widespread across the industry. Many customers state these practices make it difficult for them to choose any other provider (despite the availability of potentially better offerings to suit their security or other needs). Partners, too, who have built businesses by servicing end-customers are having to rethink their entire business models, including by potentially abandoning established partnerships with certain Azure competitors.[40] This is because Microsoft recently announced yet another licensing change[41] that will prohibit these third-party partners from selling managed services that incorporate Microsoft software if those solutions are hosted on AWS, Google Cloud, or Alibaba Cloud. Customer feedback collected by Ofcom as part of its cloud services study noted customers' "[f]ear of de facto lock-in and inability to switch"[42] and that their "cloud relationship with Microsoft is a continuation of the de facto lock-in experienced around the wider Microsoft offer."[43] Smaller companies specifically called out that Microsoft "want[s] to tie you into contracts."[44]

CISPE, a non-profit trade association for cloud providers in Europe, has made a formal antitrust complaint to the European Commission regarding Microsoft's alleged anticompetitive software licensing practices impacting the cloud.[45] CISPE has also publicly called for Fair Licensing Principles in response to these types of concerns.[46] Anticompetitive software licenses as enforced by "legacy software companies" are further identified as the key source of anticompetitive harm in cloud

[39] As part of its Fall 2019 licensing changes, Microsoft identified a group of Azure competitors as "Listed Providers." They include AWS, Google Cloud, and Alibaba Cloud. Customers who wish to migrate previously purchased, on-premises Microsoft software to Listed Providers are subject to these new restrictions. While Azure is technically included in the group of Listed Providers, Microsoft effectively exempts Azure customers from those restrictions through an incentive called the Azure Hybrid Benefit, further promoting lock-in of Microsoft on-premises software and Azure cloud infrastructure.
[40] See CPO Magazine, Licensing or Lock-in? Evaluating Microsoft's New Approach to Cloud Competition (November 16, 2022).
[41] See Microsoft, New licensing benefits make bringing workloads and licenses to partners' clouds easier (March, 30 2023).
[42] See page 56 of Ofcom, Cloud Services Market Research - Summary of Findings (March 2023).
[43] *Id.*, page 59.
[44] *Id.*, page 58.
[45] For completeness, CISPE's complaint was the second such complaint filed with the European Commission. A prior complaint was filed by OVHCloud, Aruba, and the Danish Cloud Community, alleging similar anticompetitive conduct. Google understands from press reports that Microsoft may be entering into a private settlement with OVHCloud, Aruba, and the Danish Cloud Community in efforts to have these cloud providers withdraw their complaint without having to directly address or remediate its alleged conduct.
[46] See Fairsoftware.cloud, Ten Principles of Fair Software Licensing for Cloud Customers.

infrastructure services in a 2021 report by Professor Frederic Jenny.[47] In particular, the report highlights Microsoft's use of market power in enterprise, productivity, and database software to steer business customers to its own cloud infrastructure services and ultimately harm consumers.[48] Professor Jenny's recent research also highlights around €1.01 billion in "potentially unfair" surcharges that have been incurred in 2022 for those users that have opted for a non-Microsoft cloud. In addition, this research highlights that as a conservative assumption Microsoft's 2019 licensing changes are costing European customers approximately €550 million annually, with absolutely no justification, technical or otherwise.[49] Given the global nature of cloud markets, we can assume that similar costs are being incurred by U.S.-based customers. These concerns have also been explicitly called out in Ofcom's recent interim report where an entire chapter is dedicated to concerns from a number of stakeholders about Microsoft's licensing practices.[50]

Anticompetitive licensing restrictions by legacy providers undermine security and resilience in the cloud

The anticompetitive licensing practices of legacy on-premises software providers not only undermine competition and raise customer costs, they pose direct risks for U.S. national cybersecurity and cyber resilience. As noted above, legacy on-premises providers entrench their dominant position in productivity software, server and desktop operating system, and database software by making it difficult for customers to migrate their software to any cloud infrastructure but their own through these restrictive licensing rules and other artificial and anticompetitive hurdles.[51]

These practices financially coerce customers to rely on Microsoft or other legacy on-premises providers for their complete technology stack (i.e., infrastructure, platforms, and software) and make it harder to weigh factors other than price—including whether the products are secure or not—when making buying decisions. And when customers are unable to properly factor cybersecurity into buying decisions, risks emerge.

In recent years, legacy on-premises providers, especially Microsoft, have been at the center of some of our nation's most troubling cybersecurity incidents. The 2020 attack on the U.S. government and dozens of companies colloquially known as "SolarWinds" was the result of vulnerabilities in Microsoft Exchange Server, causing untold damage to U.S. national security.[52] In February, security researchers discovered that a misconfigured Microsoft server belonging to the U.S. Department of Defense had caused three terabytes of sensitive emails and personnel records to spill online.[53] Senior Defense Department officials have quietly raised concerns about overreliance on a Microsoft "monoculture"[54] after discovering that the Russian military had been exploiting a Microsoft Outlook vulnerability to access their systems for more than a year. Members of Congress are now similarly concerned.[55] To make matters worse, reports from researchers at Orca Security suggest that Microsoft's Azure cloud

---

[47] See Professor Frederic Jenny (for CISPE), Cloud Infrastructure Services: An analysis of potentially anti-competitive practices (October 2021).
[48] *Id.*, section 3.1.
[49] See Tagesspiegel Background, Konzentration am Cloud-Markt verursacht Milliardenkosten (July 19, 2023).
[50] See Chapter 7 of Ofcom, Interim report (April 2023).
[51] See Professor Frederic Jenny (for CISPE), Cloud Infrastructure Services: An analysis of potentially anti-competitive practices (October 2021). See also Chapter 7 of Ofcom, Interim report (April 2023).
[52] See GAO, Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents (January 13, 2022).
[53] See TechCrunch, Sensitive US Military Emails Spill Online (February 21, 2023).
[54] See Newsweek, Pentagon Hacking Fears Fueled by Microsoft's Monopoly on Military IT (May 16, 2023).
[55] See Newsweek, Pentagon's Microsoft Monopoly Raises Concerns in Congress (June 7, 2023).

infrastructure is more prone to cross-tenant vulnerabilities than that of its competitors—weaknesses that could allow infections to spread from one compromised cloud customer to others.[56]

Microsoft is finding itself increasingly in the crosshairs of leading U.S. cybersecurity leaders, including CISA Director Jen Easterly, who suggested in February that the company isn't doing enough to implement security features like multi-factor authentication by default.[57] She and Goldstein subsequently built on that argument in an op-ed calling on legacy technology companies to "stop passing the buck on cybersecurity."[58]

Despite urgent security concerns, an analysis by market research firm Omdia found that Microsoft maintains a commanding 85% market share in productivity software among U.S. federal agencies.[59] According to Omdia, "[w]hile no company is immune from attacks, having such a large dependence on a single source makes the attack surface critically high and a clear high value and profile target." Omdia found that diversity in software providers could "serve to add redundancy to these critical systems."[60] Government employees agree: in a recent study, 60% of government workers surveyed responded that the government's reliance on Microsoft has made it more vulnerable to cyberattacks.[61] Yet in some cases, the trend is worsening, as evidenced by the Department of Defense's recent decision to abandon its use of diverse security tool vendors in favor of off-the-shelf Microsoft tools.[62]

For cloud customers, being forced into IT monoculture comes with real risks, especially when secure alternative solutions, such as Google Workspace, are readily available. According to a recent study by cyber risk insurer At-Bay, which analyzed insurance claims data from 40,000 small and mid-sized policyholders, Google Workspace is the most secure cloud-based email provider on the market.[63] The study found that Google Workspace customers saw far fewer security incidents than Microsoft customers and that using Workspace could enable enterprises to save as much as 50% on their cyber risk insurance premiums.[64]

Monoculture exacerbates the risks that a single vulnerability or compromise will lead to cascading effects throughout the enterprise. It also undermines customers' ability to take advantage of more resilient multicloud architectures. That way, if one cloud provider goes offline, the customer can failover workloads to its other clouds. That's why Google Cloud is committed to providing an open cloud ecosystem and enhancing interoperability with dozens of security software partners, as well as our biggest cloud competitors.[65] Promoting an approach to cloud security grounded in openness and interoperability is key to improving our nation's security baseline.

---

[56] See Protocol, 6 'Nightmare' Cloud Security Flaws were found in Azure in the Last Year. Does Microsoft have Work to do? (June 1, 2022).
[57] See Bloomberg, US Cyber Official Urges Microsoft, Twitter to Boost Security (February 27, 2023).
[58] See Foreign Affairs, Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (February 1, 2023). The authors praised a handful of companies, including Google, Amazon, and Salesforce for their attention to product security.
[59] See Omdia, The Case for Vendor Diversity: The Need for Change in Government Technology and Procurement Practices (November 2021).
[60] *Id.*
[61] See Google Cloud, Government workers say Microsoft tech makes them less secure: new survey (April 1, 2022).
[62] See Newsweek, Pentagon Hacking Fears Fueled by Microsoft's Monopoly on Military IT (May 16, 2023).
[63] See Tech Radar Pro, Google Workspace is apparently the best choice for keeping your workplace secured (February 15, 2023).
[64] See At-Bay, At-Bay reveals Google Workspace customers experience 40% fewer security email incidents than average (February 14, 2023).
[65] See Axios, Exclusive: Google opens its security tools to competitors' platforms (April 24, 2023).

CONCLUSION

Cloud computing is delivering transformational benefits across the U.S. The benefits of cloud can be reinforced by strong competition across all layers of cloud services, allowing customers to choose from a wide array of services, product propositions, and payment models that best suit their needs. Widespread adoption of multicloud strategies and switching practices have enhanced competition in this space, which has seen cloud providers competing vigorously to develop new technologies and solutions to meet evolving customer needs / use cases. The benefits of a competitive cloud industry based on interoperability, portability, and open source solutions cannot be overstated. However, ultimately, these initiatives can only achieve their envisaged customer benefits if all industry players are willing to play by the same principles of fairness and openness.