Participant's information

In what capacity or on whose behalf are you participating in this public consultation?
Coalition of cloud service providers and enterprise customer companies

Full name (of the participant or represented institution):
Coalition for Fair Software Licensing

Do you wish to make your name publicly available with your answer or keep it confidential (in which case it will be published as an anonymous answer)?
Public

Contact email (will remain confidential)
[CONFIDENTIAL]

Market functioning

1. In your opinion, what will be the main factors that will drive the growth of the sector in the coming years? (max. 300 words).
Cloud services provide access to computing resources on demand, via the internet. The customer pays to access the computing resources as a service, without having to buy, own, and maintain the hardware and software necessary to operate similar resources on premises. For many customers, cloud computing is more efficient than "do it yourself" IT solutions by offering quick deployment, scalability, affordability and ease of maintenance, thereby enabling companies to refocus resources on their core businesses. Demand for cloud computing services has exploded in recent years as enterprise customers increasingly migrate from on-premise to the cloud and run their workloads in the cloud. For example, Gartner forecasts worldwide end-user spending on public cloud services to grow 20.7% to total $591.8 (~551€) billion in 2023, up from $490.3 (~ 456€) billion in 2022, with the highest end-user spending growth in IaaS (29.8%). (See Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023,https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023, 31 October 2022).

2. How would you classify the different types of agents/operators involved in the cloud market value chain? (max. 300 words).
Agents and operators providing cloud computing services share three key elements:
(1) Computing Resources: these include hardware (servers and network equipment) and software (applications) that are used to process workloads and store data.
(2) On Demand: the computing resources are available on a scalable and elastic basis. This typically involves the dynamic provision of virtualized computing resources. Users are typically billed for the amount of resources used.
(3) Via a Network: the transit of data to and from the cloud provider may be over the public internet or a private connection. This allows location-independent access to the cloud.
(See U.S. Department of Commerce National Institutes of Standards and Technology, The NIST Definition of Cloud Computing,

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#page=6, September 2011)

There are currently thousands of global agents and operators that provide cloud computing services. However, they can generally be classified into one of a handful of service models, including but not limited to:
- Data Center Infrastructure
- Cloud Infrastructure Services
- Cloud Software Services
- Independent Software Vendors (ISVs)
- Professional Service Providers

4. In your opinion, what are the main elements that determine the dynamics of competition among cloud service providers? In your opinion, which other markets can affect the competitive dynamics in the provision of cloud services? (max. 300 words).
The Coalition believes that the most important factors for determining customer choice should be quality of innovation of services, reliability as a strategic partner, and data security / privacy. We have found, though, that historical software dependance and vendor software licensing policies increasingly outweigh these other considerations.

Before the emergence of cloud computing, entities generally managed their own IT systems, including software and hardware. They licensed software, including for use on servers they owned or leased, with no restrictions as to how they would deploy the software (i.e., location of the servers, brand of the hardware, etc.). Customers had the expectation of flexibility and control when they purchased perpetual, on-premises licenses.

When cloud computing first emerged, there were few restrictions for those entities choosing to move their systems to the cloud. Entities were generally able to bring their on-premises software with them into the cloud. This ability to take on-premises software into the cloud not only proved efficient, but also facilitated competition by lowering switching costs between cloud / on-premises solutions and among cloud providers. As the cloud developed, providers and customers alike understood that if you were moving from physical, on-premises servers to a cloud service provider, you would be permitted to bring your own license ("BYOL") for any software license you owned. However, since 2019, Microsoft has continuously taken steps to limit customers' ability to run its key software in any environment that is not its own, at a steep cost to competition in cloud IT services. Specifically, Microsoft's: (1) 2019 restrictions (https://www.microsoft.com/en-us/licensing/news/updated-licensing-rights-for-dedicated-cloud) preventing customers from using already paid-for Windows Server licenses on cloud infrastructure provided by its closest rivals, and (2) 2022 announcement (https://partner.microsoft.com/en-US/blog/article/new-licensing-benefits-make-bringing-workloads-and-licenses-to-partners-clouds-easier) that from October 2025 ISVs will no longer be free to sell Microsoft software if hosted on certain third party cloud platforms.

5. In your opinion, when contracting cloud services from an operator, how do the main providers' offers differ from each other? (max. 300 words).
Nearly all cloud infrastructure providers supply customers with core computing services such as compute, storage, networking, database and data analytics on demand and over a network. However, Microsoft has increasingly used a set of distinct yet interrelated business practices that threaten competition throughout the cloud stack and in information technology. Specifically, Microsoft uses its dominance in desktop operating, server, and productivity software (See U.K. Competition & Markets Authority, Cloud Services Market Investigation: Licensing Working Paper,

https://assets.publishing.service.gov.uk/media/666196c287d3bfaf688c86a1/Licensing_practices__final.pdf, 6 June 2024) to impose additional costs on or outright prohibit customers from licensing software for use on competing cloud providers, tie adjacent product market offerings together, and limit integration capabilities with competing cloud service providers to lock customers into products and services throughout the Microsoft ecosystem. The result is that customers face a series of Hobson's choices pitting real interests in low prices, preferred service and better cyber resiliency against each other, and limiting the benefits cloud computing was intended to provide in the first place.

6. When contracting cloud services from an operator, describe in order of importance the factors that, in your opinion, are the main determinants of the contracting decision, such as, among others, price, technical quality of the service, the provider's portfolio of services, security, transparency of the contract, nationality of the provider, previous relationship with the same provider, previous knowledge by the staff, etc. (max. 300 words).
Historical software product dependance and pre-existing contractual relationships that impose licensing restrictions and limitations on software deployment significantly influence the cloud decisions of enterprise customers.

Enterprise customers that have heavily invested in must-have software need to be able to continue using that software as they migrate from on-premises data centers to the cloud. Microsoft holds a dominant position in: (1) operating systems (OSs) for personal computers and servers (i.e., Windows (desktop) 10 and 11; Windows Server) (See Case COMP/C-3/39.530 – Microsoft (Tying), Commission Decision, https://ec.europa.eu/competition/antitrust/cases/dec_docs/39530/39530_2671_5.pdf, 16 December 2009 (client PC operating systems); COMP/C-3/37.792 – Microsoft, Commission Decision, https://your.caselex.eu/storage/announcement/37792_4177_3.pdf, 24 March, 2004, (client PC operating systems and work group server operating systems). See also CMA, Anticipated acquisition by Microsoft of Activision Blizzard, Inc. Final Report, https://assets.publishing.service.gov.uk/media/644939aa529eda000c3b0525/Microsoft_Activision_Final_Report_.pdf, 26 April 2023 (findings on Microsoft's position in PC operating systems); (2) productivity software for PCs (i.e., Office and Microsoft 365 (cloud-based)) (See Case M.8124 – Microsoft/LinkedIn, Commission Decision, https://ec.europa.eu/competition/mergers/cases1/202231/M_10290_8431645_854_3.pdf, 6 December 2016 (findings on Microsoft's market shares in productivity software); and (3) enterprise mail server software and services (i.e., Exchange Server) (See Ioana Patringenaru, Who's got your mail? Google and Microsoft, mostly, UC San Diego Today, https://today.ucsd.edu/story/IMC2021_savage, 6 December 2021.) Microsoft's licensing terms restrict customers from using previously purchased licenses for Windows, Office, etc on competing cloud services, but not on Azure. Microsoft has never justified this conduct. As a result, historical enterprise software customers are heavily skewed towards using Azure as their primary cloud service provider.

Given the increasing regulatory requirements for enterprise customers - especially those in financial and health care sectors - it is important for customers to make their cloud choices based on the data privacy and cybersecurity practices of providers. However, this will only be possible if restrictive licensing practices that leverage their historical software dependence are addressed.

7. When contracting cloud services from an operator, assess the extent to which contract terms and conditions are negotiable (max. 300 words).
Most customers contract for cloud services via bilateral negotiations that are structured around a cloud provider's standard form terms of service. Microsoft's licensing practices are extraordinarily complex and often opaque. Microsoft has hundreds of different licensing options consisting of

overlapping suites of services that are used to negotiate special deals with enterprise customers. Notwithstanding the expansive number of different possible Microsoft Enterprise License Agreements (ELAs), there is little transparency around the price of individual products included in them, or general ability for customers to take an a la carte approach and to choose which Microsoft products and services they want to use.

Over time, Microsoft has incorporated an increasing number of products from its vertical stack into their 365 packages to drive adoption and dependence on the Microsoft ecosystem. Many of these products are included even if customers have little or no initial interest in them, inhibiting competition by disincentivizing adoption of similar products offered by alternative providers. Microsoft's customer success managers (CSMs) use them to drive broader product adoption within a customer's existing install base, using multi-year discounts and rebates to further entice adoption. Once a customer has sufficiently adopted a particular product offering, Microsoft can and does use customer dependencies to begin charging separately for those offerings.

All of this is accomplished through a web of agreements that enterprise customers often cannot see together to understand their current entitlements or needs. As a result, it is not uncommon for entities of varying sizes to have individual users assigned multiple, overlapping Microsoft licenses who are not aware of the full slate or actual cost of the services. Beyond tying, this opacity limits customer choice and effective competition.

9. Assess the transparency of contract terms and conditions and indicate whether changes in contract terms and conditions are common (max. 300 words).
The Coalition for Fair Software Licensing advocates for the industry-wide adoption of nine key Principles for Fair Software Licensing (https://www.fairsoftwarelicensing.com/our-principles/). The first of these is that licensing terms should be clear and intelligible; written in a way that allows customers to readily determine their licensing costs, and permit customers to determine their obligations easily. The principles further provide that permitted uses of software should be reliable and predictable; noting that software vendors should not make material changes to license terms that restrict customers from previously permitted uses, especially when customers may have become reliant on those uses, unless required by law or due to security concerns. While these principles may seem obvious, we have found it necessary to advocate for their adoption due to the failure of some legacy vendors to adhere to them.

Barriers to competition

13. Assess whether there are significant barriers to entry in the cloud services or cloud infrastructure market. If so, indicate and describe what type of barriers (e.g., regulatory, investment size, availability of qualified staff, other) and indicate which services or cloud layer (IaaS, PaaS, SaaS) are affected by each barrier (max. 300 words).
There are no significant legal, economic or regulatory barriers which restrict new entrants from developing and offering cloud computing solutions. Rather, the most significant barrier that new market entrants in cloud computing services face is the entrenchment of legacy providers, such as Microsoft. Restrictive software licensing and lock-in practices have led to Microsoft's growth across the cloud stack - at the expense of smaller and arguably more innovative providers (See Frederic Jenny, Unfair Software Licensing Practices: A Quantification of the Costs to Cloud Customers, https://cispe.cloud/website_cispe/wp-content/uploads/2023/06/Quantification-of-Cost-of-Unfair-Software-Licensing_Prof-Jenny_-June-2023_web.pdf, 21 June 2023).

While Microsoft leverages discriminatory and restrictive practices with the explicit aim of pushing adoption of Azure, its anticompetitive and discriminatory software licensing practices extend across

all layers of its cloud service offerings and, therefore, impacts competitors and new market entrants at every layer. This includes but is not limited to:
- OneDrive and SharePoint, cloud file hosting product and collaboration tool: under the SPLA, cloud service providers may not be licensed to provide a similar service to OneDrive.
- Defender, cybersecurity tool: all Microsoft 365 customers have Defender for Individuals forcibly installed on their devices. Steering customers toward one cybersecurity solution itself creates a cybersecurity problem.
- Azure Active Directory and Intune, user identity, authentication, and device management: Microsoft does not provide sufficient Application Programming Interfaces ("APIs") needed to allow interoperability between Microsoft products ActiveDirectory, Azure ActiveDirectory, Intune and third-party identity and device management products.

As Microsoft ties several software products to its 365 suites, the net result of which is vendor lock-in and a less secure cloud experience for users.

14. In your opinion, assess which cloud layers (IaaS, PaaS, SaaS) present the greatest competitive challenges and explain why (max. 300 words).
Microsoft's licensing and tying practices, which leverage its dominant desktop operating, server, and productivity software products to its adjacent product market offerings throughout the Microsoft ecosystem, have clear anticompetitive effects across the cloud in the form of price increases, less customer choice, reduced innovation, and poorer quality products. Of course, Microsoft's anticompetitive licensing and tying practices have also negatively impacted competitive conditions relating to IT services in the cloud. In addition to the myriad of cloud customers, Microsoft's competitors, large and small, have borne the costs of being foreclosed from competing effectively on the merits of their products, even where users may actively prefer the user experience offered by non-Microsoft products.

The requirement that customers re-license their existing licenses in order to deploy those on competing cloud services; the discriminatory treatment of competing cloud providers wishing to offer customers the ability to use Microsoft products on their own cloud infrastructure; and tying numerous software products to Microsoft's dominant positions are having an outsized and negative impact on cloud customers and end-consumers, while also stifling competition from other cloud service providers. This is of particular concern at a time when more companies across Spain and globally are considering the use of cloud services for the security, flexibility, and other benefits they can deliver.

15. For companies already present in the cloud market, what are the main obstacles to their activity and to competition in the sector? (max. 300 words).
For cloud providers, the vast majority of the addressable market is made up of workloads that are currently running in an on-premises environment. Traditional enterprises, which generally have a significant Microsoft software footprint, represent a vast majority of the customers that are running workloads in an on-premises environment. It follows therefore that Microsoft software-related workloads account for a comfortable majority of all workloads that have not yet migrated to the cloud.

All of Microsoft's licensed products, which are integral to the workloads of Spanish and global businesses and customers, are more expensive for end-users when used on third-party cloud service providers. As Wes Miller, an analyst at research firm Directions on Microsoft put it: "[y]ou can still run all of these products in someone else's cloud, but you must be willing to pay a premium to do that." (See Richard Waters, Microsoft's Tactics to Win Cloud Battle Lead to New Antitrust Scrutiny, Financial Times, https://www.ft.com/content/350e7fed-cd52-4a0a-9902-5f2d9ebc3fe7, 12 April

2022.)

Because of the opacity in pricing of individual products and services, customers are prevented from being able to effectively price shop for the services they actually need. As one customer noted in Ofcom's Market Research report: "[We] can't do a straight comparison of costs. We have to do calculations with both separately. There is an element of them trying to muddy the waters in terms of costing – Microsoft tend to bundle things. They tell you it's cheaper to do things in Azure because they include an element of the license in the subscription – always a case of bundling and it being more expensive but explaining to you why it's cheaper because it includes things." (See Ofcom, Cloud Services Market Research - Summary of Findings, https://www.ofcom.org.uk/__data/assets/pdf_file/0031/256459/context-consulting-cloud-services-market-research-summary-of-findings.pdf, April 2023.)

18. In your opinion, what are the difficulties in contracting the services of more than one cloud provider? In your answer, please assess aspects of vertical interoperability (between services located in different cloud layers), horizontal interoperability (between services located in the same cloud layer) and interoperability of the data produced when using different cloud services. In your opinion, what solutions could be implemented? (max. 300 words).
As noted earlier, Microsoft not only uses restrictive licensing terms but also tying of software products to its 365 suites with limited integration capabilities. This results not only in vendor lock-in but also a less secure cloud experience for users. While there are examples of these practices throughout its product suite, the most notable example is that of identity and access management services.

Microsoft has long tied its ActiveDirectory (AD) and Azure ActiveDirectory (AD) services to the license for its dominant offerings, including for Windows OS and Office productivity suite. This allowed Microsoft to capture a market leader position in the identity and access management market. It also created another barrier layer for customers to choose alternative providers; not only for operating systems or productivity, but also identity management. If you chose an alternative operating system or productivity suite, you would struggle with identity and authentication because a customer could not efficiently connect that to AD historically and now Azure AD. Conversely, if you chose an alternative identity management provider which used Microsoft's Windows OS or productivity tools, you would struggle for equivalent connectivity as with AD / Azure AD. As Microsoft has moved to Microsoft 365 enterprise agreements, customers are now required to use an Azure AD identity – and for some licenses, Microsoft Intune endpoint management – to access these products. That identity then serves as the core identity on Azure and Windows devices, making it difficult to connect to tools and services provided by competitors. Unless a customer solution is exclusively based on Azure AD, third party IAM providers cannot fully manage identities in Microsoft 365. This represents a significant technical barrier to those seeking to use Microsoft 365 on competing cloud infrastructure, in particular, in hybrid and/or multi-cloud environments where Microsoft products run alongside other applications.

22. Assess the existing obstacles to competition in the public procurement of cloud services, and indicate the solutions that could be implemented in your opinion (max. 300 words).
The U.S. Government Accountability Office ("GAO") has issued a number of reports examining the impact of restrictive software licensing practices on the public procurement of IT services. (See GAO, Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings, https://www.gao.gov/products/gao-24-105717, 29 January 2024). While each of these reports examined different elements of the U.S. government, each consistently found that the government is inefficiently tracking its spending on software licenses and other cyber-related investments, resulting in duplicative purchases and missed opportunities for cost savings. In addition to missed cost-

savings, they have found that restrictive IT licenses can increase a federal agency's cybersecurity risks and leave them vulnerable to attack. Further, the GAO found that multiple software products may be bundled into a single license with a vendor, and agencies may not have usage data for each product individually. When examining the impact on defense spending, the GAO found that restrictive licensing practices: (1) Increased the cost of cloud computing through additional fees; and (2) limited choice of commercial cloud service providers and imposed arduous requirements. (See GAO, DOD Software Licenses: Better Guidance and Plans Needed to Ensure that Restrictive Practices Are Mitigated, https://www.gao.gov/products/gao-23-106290, 12 September 2023).

The Coalition believes that it is imperative for the governments to have greater insight into not only how much they spend on IT but the contractual terms that dictates its use. To that end, we believe that it is imperative for government agencies and departments to conduct a comprehensive assessment / accounting of their respective software licensing contracts to garner key insights on costs, management, and cybersecurity risk as they enter into vendor agreements. (See S. 931 (https://www.congress.gov/bill/118th-congress/senate-bill/931) / H.R. 1695 (https://www.congress.gov/bill/118th-congress/house-bill/1695), the Strengthening Agency Management and Oversight of Software Assets Act, for an example of legislatively mandating such a mandate.)

23. Provide additional comments on other barriers, distorting factors or issues that you consider relevant to the functioning of this sector (max. 500 words).
It is vital that customers have the ability to choose which IT services / providers best meet their needs. Microsoft's practices inhibit that choice, undermine competition, and threaten security.

Microsoft's tying is preventing customers from accessing the benefits that competitors in cybersecurity, communication and collaboration, IAM, and other sectors may offer. The end-user is thus forced into choosing a provider on which it can run the software it relies on (i.e., Microsoft), rather than the provider that is best suited to serving its specific IT needs.

The anticompetitive practices in question have also directly prevented innovation in precisely the technology that enables customers to make the most and best use of cloud computing: virtualization. Virtual Desktop Infrastructure (VDI) permits individuals to access a "virtual desktop" in the cloud, where they can perform all of their normal office functions from multiple devices and work remotely. It is a critical component of the modern workplace and an invaluable contribution to productivity from cloud computing. Third-party providers like Citrix, VMware, Cameyo and Ivanti have attempted to develop their own VDI offerings, but Microsoft charges additional license costs to use its technologies for remote connection and refuses to make certain software products (e.g., Microsoft 365 and Windows Desktop) available under the SPLA. As outlined above, the 2019 licensing changes also prohibit the Listed Providers from being able to offer or host (BYOL) Microsoft 365 at all, therefore preventing them from offering a viable VDI solution for many customers. Microsoft has since developed its own VDI offering for its clients on Azure.

One of the less discussed and increasingly concerning consequences of Microsoft's anticompetitive restrictive licensing and tying practices is that of increased cybersecurity risk. By driving customers to adopt a single cybersecurity product for reasons unrelated to the quality of security (namely, its inclusion in a Microsoft 365 suite of otherwise unrelated products), Microsoft is removing the market mechanism for improving overall cybersecurity in favor of creating customer dependency on a single layer of defense. Reliance on a single cybersecurity provider creates a less secure IT environment and runs counter to general recommendations for ensuring organizational cyber-resiliency. Further, it creates a concentrated and easier to access target for bad actors to identify vulnerabilities or common misconfigurations associated with the platform. One need look no further than the number

of recent security related events stemming from permeations of Microsoft products in recent years to see how real this threat is (See U.S. Cyber Safety Review Board, Review of the Summer 2023 Microsoft Exchange Online Intrusion, https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf, 20 March 2024).

Further, Microsoft's practices are distorting competition in cybersecurity. One manner they are doing this is by offering Microsoft Defender "for free" with its cloud or productivity software. By tying Defender to other products, Microsoft is effectively cloaking the true cost of Defender through its licensing structure. This practice removes the market mechanism for valuing cybersecurity solutions, undermining and skewing competition in the current and future cybersecurity market, and reducing incentives for innovation and improvement overall.

Coalition for Fair Software Licensing

To: La Comisión Nacional de los Mercados y la Competencia (CNMC)
dp.estudios@cnmc.es

From: Coalition for Fair Software Licensing

Re: Estudio de Servicios de Nube

Date: 21 junio 2024

The Coalition for Fair Software Licensing appreciates the opportunity to supplement our responses to the questionnaire for the CNMC's study of cloud services. In addition to the points raised in our responses, the below comments focus on the anticompetitive licensing practices that have been repeatedly deployed by one software vendor in particular – Microsoft. The below comments briefly outline the harmful impact that the software giant's restrictive licensing tactics have continued to have on customer choice, competition, and cybersecurity in the cloud.

About the Coalition for Fair Software Licensing

The Coalition for Fair Software Licensing is a global initiative that brings together information technology providers, customers and users with operations throughout Europe, Americas and APAC. The Coalition, which launched in September 2022, is part of a larger international movement dedicated to protecting fair and transparent software licensing terms, and working against the limiting impact that unfair and oblique licensing practices have on growth, opportunity, investment, and security. The Coalition seeks to do this by advocating for the industry-wide adoption of the *Principles for Fair Software Licensing*.

Summary of Views

Virtually every business - both globally and in Spain - uses software to conduct its operations and generally licenses it from the vendors who design it. Software customers invest significant sums in these licenses expecting flexibility and control over how and where the software is deployed, be it on desktops, on-premises servers, leased data centers, or whatever combination best meets their needs. This freedom of hardware choice is a widespread software policy known as "bring your own license" or "BYOL," which has greatly benefitted software customers.

As cloud technology has become a viable alternative to legacy IT systems, customers want the same flexibility and control they were accustomed to on-premises when they migrate to the cloud. This includes the ability to deploy licenses for software on the cloud that they were already paying for on-premises. This allows customers to select cloud providers based on the price and quality of the service they provided – not on the cost of the software or services run on it. Software and cloud providers alike have largely embraced BYOL with the emerging cloud, and most continue this practice today.

Microsoft, however, which has long dominated operating and productivity software, approaches licensing differently. Rather than supporting customer choice, Microsoft is unfairly leveraging customer dependencies to its own benefit. Specifically, Microsoft is using its market power and restrictive and discriminatory licensing terms to: coerce customers into using Azure cloud infrastructure and lock them into the Azure ecosystem; tie products in the vertical stack of Microsoft ecosystem into an ever-growing suite of services, regardless of customer preferences, to advantage its products over competitors; limit integration capabilities of competing services on equal terms with its own products; and set its own products as defaults.

While this behavior has evolved over the past several years, much of its origins can be traced to 2019 when the company effectuated a monumental change to its licensing practices. This change presented existing software customers with a Hobson's choice: forego their previously purchased (often perpetual) software licenses and incur the additional cost of purchasing a second license to use the cloud provider of their choice; or migrate to Microsoft cloud services and have previously purchased licenses (and their beneficial terms) transferred to cloud-based subscription licenses at no additional cost.

Instead of offering a better cloud product and competing on the merits, Microsoft's licensing and tying practices force customers into the Microsoft ecosystem and limit their choice by making it more difficult, if not impossible, to access key software without also using their other cloud products. Customers do not benefit, and the practices have elicited outcry from them. Microsoft, for its part, has offered nothing by way of justification. These practices skew competition in IT services in Microsoft's own favor, reduce choice, drive up costs, disincentivize innovation and create cybersecurity risks for customers large and small. That is why Microsoft's licensing and tying practices have already drawn the attention of competition agencies abroad.

The Coalition believes these practices raise serious concerns and respectfully encourages the CNMC to investigate them and their impact on both customers and competitors in the Spanish market.

The Impact of Microsoft's Restrictive Software Licensing

In 2019, Microsoft offered existing software customers to purchase a second license to use the cloud provider of their choice or migrate to Microsoft for no additional cost – but forfeiting their perpetual license for a subscription model service. Microsoft's restrictive licensing practices constitute violations of U.S. antitrust law.

- **Microsoft has continuously taken steps to limit customers' ability to run its key software in any environment that is not its own, at a steep cost to competition in cloud IT services.**

  Microsoft is leveraging its dominant position in desktop operating, server, and productivity software – including customer dependence on "must-have" products like Windows, Word, Excel, and PowerPoint - to force the adoption of Azure. Specifically, Microsoft does this by:

  - **Restricting "Bring Your Own License" (BYOL):** In August 2019, Microsoft announced that, beginning in October 2019, customers would need to repurchase their existing licenses to operate software on Microsoft, Alibaba, Amazon (including VMware Cloud on AWS), and Google. Customers would need to purchase a new license to use another cloud provider, in addition to the Microsoft license they already had. For some software, there was no option to run it on a non-Microsoft cloud.

  - **Discriminatory Licensing:** The Services Provider License Agreement is utilized by other cloud service providers, and the Cloud Solution Provider Program is utilized by resellers who host products on Microsoft's cloud servers. Around the same time that Microsoft was ending BYOL for its customers, it was increasing the cost of SPLA – but not the CSPP. Microsoft began to charge more to those cloud providers who compete with Azure.

  - **Tying:** Microsoft ties several software products to its 365 office product suites, resulting in vendor lock-in and a less secure cloud experience for users. This results in price increases, less customer choice, reduced innovation, and poorer quality products. Meanwhile, rivals in cybersecurity, videoconferencing, IAM, and other consumer products are finding it harder to compete effectively. Nascent competitors have fewer incentives to enter the market.

Due to Microsoft's anticompetitive practices, customers have to choose between low prices, superior service, and better cybersecurity. Many Gartner clients, for example, report frustration with watching their Azure costs increase over time without knowing why. These tactics have contributed to the accelerated growth of Azure, which is now growing at a faster pace than its competitors.

Key Considerations Raised in Global Filings

The Coalition has participated in the cloud studies of other global regulators, most notably that of the UK Competition & Markets Authority. We would like to ensure that some key points made in that filing are brought to your attention, as noted below:

- **On Microsoft's Software Licensing Policies:** While purporting to address competition concerns in Europe, without any justification Microsoft refused to stop its practices with respect to Listed Providers, ensuring that its restrictive licensing continued to apply to its key competitors and maintaining significant restrictions on customer choice. The changes the company adopted were aimed at mollifying some critics, but clearly do not resolve the systemic issues … What had been an anticompetitive policy was now also anticompetitive and facially discriminatory.

- **On Microsoft Driving Up Costs for Customers:** Microsoft has made recent proposals that it suggests resolves these concerns. However, these proposals do nothing for, and indeed make no reference to, the effects of higher pricing for software running on other cloud service providers that results directly from their product license terms – significantly higher prices that many of the Coalition's members today must endure. Nor do they address broader industry concerns. Indeed, Microsoft continues to impose key restrictions on Listed Providers and, in fact, introduced additional restrictions on SPLA partners hosting on Listed Provider infrastructure.

    - The licensing changes and discriminatory treatment of SPLA have led to increased prices — sometimes more than $100M for a single customer — for Microsoft customers that wished to use Listed Providers' cloud services.

    - Professor Frederic Jenny estimates that Microsoft's practices have imposed $400M in Europe.

    - Among customers that experienced a price increase when renewing their contract, the mean reported increase was around 20%.

- **On Microsoft Undermining Customers' Cybersecurity:** By driving customers to adopt single cybersecurity product for reasons unrelated to the quality of security (namely, its inclusion in a Microsoft 365 suite of otherwise unrelated products), Microsoft is removing the market mechanism for improving overall cybersecurity in favor of creating customer dependency on a single layer of defense … Microsoft's practices of locking customers into the Microsoft ecosystem (by increasing the switching costs for failing to use Azure) inhibits movement to potentially more secure cloud providers and removes incentive for Microsoft to innovate and continuously improve cybersecurity within its solutions.
    - Recent high-profile cyber hacks underscore the risks of this approach – just look at the 2023 breaches of U.S. government agencies and global customers by hacking groups in China and Russia using Azure AD vulnerabilities and groups in Russia manipulating approval prompts in Teams. The U.S. Department of Homeland Security (DHS)'s Cyber Safety Review Board (CSRB) report on Microsoft's Summer 2023 hack that impacted government officials even found that the breach was worsened by licensing restrictions.

    - Attached is a timeline of significant Microsoft cyber events (2020-2024).

Conclusion

The cloud was built to offer customers pay-as-you-go choice and flexibility. Instead, Microsoft is doubling down on the restrictive licensing models that made products like Windows and Office ubiquitous in the workplace to drive adoption of Azure and the growth of its other business units, including security.

Many recall the "Browser Wars" of the 1990s when Microsoft illegally leveraged its dominance in desktop operating systems to gain a foothold in internet browsers. Few realize that Microsoft is using that same playbook today. Only this time, the software giant is leveraging its dominant position in desktop operating and productivity software to lock customers in the cloud. It's a new take on an old problem that global regulators have successfully tackled before. Now, there are higher stakes – customers' security is being threatened. It's time for regulators to step in again.

Attachment: A Timeline of Microsoft Cyber Events and the Company's Inadequate Responses (2020-2024)

A Timeline of Microsoft Cyber Events and the Company's Inadequate Responses (2020-2024)

Total Zero Days: 77

Date	Events

2020	**Total Zero Days: 8**
	
	Relevant Reporting:
	• **General**
	  ○ January 22 - *Forbes:* Microsoft Security Shocker As 250 Million Customer Records Exposed Online
	  ○ April 23 - *Forbes:* New Microsoft Hack Hits Private Equity Firms In Million Dollar Heist: Here's How It Happened
	• **Windows**
	  ○ January 14 - *CyberScoop:* The NSA discovered a severe flaw in Microsoft Windows 10
	  ○ January 22 - *Fierce Healthcare:* Healthcare faces 'double-barreled' threat from Microsoft vulnerabilities
	  ○ April 15 - *Forbes:* Windows OneDrive Security Vulnerability Confirmed: All You Need To Know
	  ○ July 14 - *The Hacker News:* 17-Year-Old Critical 'Wormable' RCE Vulnerability Impacts Windows DNS Servers
	• **Teams**
	  ○ April 26 - *ZDNet:* This is how viewing a GIF in Microsoft Teams triggered account hijacking bug
	• **Sharepoint**
	  ○ July 22 - *SecurityWeek:* PoC Released for Critical Vulnerability Exposing SharePoint Servers to Attacks

February 2019 - December 2020	**Russian-Backed Groups Illegally Access SolarWinds Customers' Data, Resulting in the *Largest Hack Ever Recorded*** **Microsoft Vice Chair Brad Smith deflects blame, comparing the hack to 9/11 and World Wars.** • "This latest cyber-assault is effectively an attack on the United States and its government and other critical institutions, including security firms. It illuminates the ways the cybersecurity landscape continues to evolve and become even more dangerous..." *(Source)* • "Put simply, **we need a more effective national and global strategy to protect against cyberattacks**. It will need multiple parts, but perhaps most important, it must start with the recognition that governments and the tech sector will need to act together." *(Source)* • "The new year creates an opportunity to turn a page on recent American unilateralism and focus on the collective action that is indispensable to cybersecurity protection. The United States did not win **World War II, the Cold War** or even its own independence by fighting alone." *(Source)* • "First, we need to take a major step forward in the sharing and analysis of threat intelligence. In a new year that will mark the **20th anniversary of 9/11**, we should remember one of the lessons from the tragic day that the 9/11 Commission called 'a shock but not a surprise.'" *(Source)*

Date	Events

2021	**Total Zero Days: 24**
	
	Relevant Reporting:
	• **General**
	  ○ March 15 - *VentureBeat:* Russian hackers exploited MFA and 'PrintNightmare' vulnerability in NGO breach, U.S. says
	  ○ December 21 - *The Wall Street Journal:* The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw
	  ○ December 22 - *Help Net Security:* Attackers bypass Microsoft patch to deliver Formbook malware
	• **Active Directory**
	  ○ December 21 - *SecurityWeek:* Microsoft Urges Customers to Patch Recent Active Directory Vulnerabilities
	• **Azure**
	  ○ August 13 - *Bleeping Computer:* Windows 365 exposes Microsoft Azure credentials in plaintext
	  ○ September 15 - *The Hacker News:* Critical Flaws Discovered in Azure App That Microsoft Secretly Installs on Linux VMs
	  ○ May 11 - *SC Magazine:* Vulnerability attacks weakness in Microsoft Azure virtual machine extensions
	• **Windows**
	  ○ August 25 - *Bleeping Computer:* Microsoft: Russian malware hijacks ADFS to log in as anyone in Windows
	  ○ October 28 - *Bleeping Computer:* All Windows versions impacted by new LPE zero-day vulnerability
	  ○ December 23 - *Bleeping Computer:* Stealthy BLISTER malware slips in unnoticed on Windows systems
	• **Edge**
	  ○ June 29 - *BankInfoSecurity:* Microsoft Edge Vulnerabilities Let Hackers Steal Data
	• **Exchange**
	  ○ August 21 - *Bleeping Computer:* Microsoft Exchange servers being hacked by new LockFile ransomware
	  ○ September 2 - *Dark Reading:* 'ProxyToken' Flaw Heightens Concerns Over Security of Microsoft Exchange Server
	  ○ September 23 - *TechTarget:* Autodiscover flaw in Microsoft Exchange leaking credentials
	  ○ April 13 - *CyberScoop:* NSA says it found new critical vulnerabilities in Microsoft Exchange Server
	• **Teams**
	  ○ December 23 - *The Hacker News:* Researchers Disclose Unpatched Vulnerabilities in Microsoft Teams Software

February 23, 2021	**Microsoft Executives Testify Before Congress, Blaming *Consumers* for Security Lapses.** **Microsoft Vice Chair Brad Smith blames consumers for the recent hack during testimony before the U.S. Senate Intelligence Committee.** • "We've looked at the customers that use Microsoft software that we were able to identify had been hacked in this incident, and what we have found repeatedly is that they could've better protected themselves simply by applying the many cybersecurity best practices the world has recognized already, that we've encouraged customers to apply already." (Source) • "In some ways, what happened here was, you know, for example, it is like leaving your keys on the kitchen table, and when you do that, somebody can go steal your car, you know. The cloud may be, in this case, you know, your email that they access." (Source)

Date	Events
	Smith acknowledges in testimony that only Microsoft customers who purchase Microsoft 365 E5 have the most advanced security. • "[Microsoft 365 E5] is the service that we offer that includes security and other advanced features. We offer a range of choices to our customers. E5 is absolutely what we hope and expect and recommend that our customers purchase. Some people don't want to buy it, and we honor that, but it is absolutely what we encourage. Well, you know, we are a for-profit company. Everything that we do is designed to generate a return other than our philanthropic work." (Source) **Smith says the government should be the ones to step in and support better security.** • "I think we can count on the government to have higher levels of cybersecurity precautions in place for secret and top-secret workloads… as a cloud services provider, Microsoft…stands up secret and top-secret workloads for the U.S. Government, and…what we consistently find is what you would expect…the people in government agencies who are working in this space are, by definition, going to be more rigorous, so…,we should assume that there are more vigorous attacks or hacks. We should also count on stronger protection for those kinds of workloads"
February 23, 2021	**Microsoft Again Deflects Blame and Releases Another Call for "A Digital Strategy to Defend the Nation."** **Microsoft Vice Chair Brad Smith again issues another public letter, deflecting blame and renewing calls for a national cybersecurity strategy.** • "The recent SolarWinds cyberattack on the tech sector's supply chain was a wake-up call…We need to strengthen our software and hardware supply chains and modernize IT infrastructure. We must also promote broader sharing of threat intelligence, including for real-time responses during cyber incidents. Let's start with the need for more open sharing of information. Today, too many cyberattack victims keep information to themselves. We will not solve this problem through silence. It's imperative that we encourage and sometimes even require better information sharing, including by tech companies." (Source)
January – March 2021	**China-Backed Groups Breach Microsoft Exchange Servers, Impacting +60,000 Companies Worldwide ("Hafnium" Hack).** **In January, Microsoft detected multiple zero-day exploits being used to attack on-premises versions of Microsoft Exchange Server.** • "Pressed for a date when it first became aware of the problem, Microsoft told KrebsOnSecurity it was initially notified "in early January." So far the earliest known report came on Jan. 5…" (Source) **Over the next few days, attackers were able to breach +30K organizations in the U.S. and +60K globally.** • At least 30,000 organizations across the United States — including a significant number of small businesses, towns, cities and local governments — have over the past few days been hacked by an unusually aggressive Chinese cyber espionage unit that's focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting four newly-discovered flaws in Microsoft Exchange Server email software, and has seeded hundreds of thousands of victim organizations worldwide with tools that give the attackers total, remote control over affected systems." (Source) **On March 12, the Microsoft Security Team writes a blog admitting two cyberattacks in the last four months.**

Date	Events
	• "This is the second time in the last four months that nation state actors have engaged in cyberattacks with the potential to affect businesses and organizations of all sizes…Microsoft is deeply committed to supporting our customers against these attacks, to innovating on our security approach, and to partnering closely with governments and the security industry to help keep our customers and communities secure." (Source)
May 12, 2021	**The Biden Administration Issues Executive Order Calling for Public-Private Cooperation on Cybersecurity** • "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy…Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace." (Source)
July 2021	**PrintNightmare Hack** **Remote code execution of Microsoft Windows print spooler service allowed malicious actors to gain access to cloud and email accounts.** • New Windows 10 vulnerability allows anyone to get admin privileges (Source)
August 2021	**CosmosDB & Omigod Hack** **A vulnerability in Microsoft Azure's managed database service allowed hackers to read and write access to Azure databases, compromising thousands of enterprises.** • "Worst cloud vulnerability you can imagine" discovered in Microsoft Azure (Source)
September 2021	**Active Directory Federation Services Hack** **Russian state actors use FoggyWeb backdoor to steal configuration databases and security tokens.** • Russia-linked Nobelium APT group uses custom backdoor to target Windows domains (Source)
2022	**Total Zero Days: 15** **Relevant Reporting:** • **General** ○ January 5 - *ZDNet:* Malsmoke hackers abuse Microsoft signature verification in ZLoader cyberattacks ○ December 13 - *Ars Technica:* Microsoft digital certificates have once again been abused to sign malware ○ December 14 - *SecurityWeek:* CISA Warns Veeam Backup & Replication Vulnerabilities Exploited in Attacks • **Azure** ○ March 7 - *VentureBeat:* Major Microsoft Azure cross-tenant vulnerability caught by Orca Security

Date	Events
	○ April 29 - *TechRadar:* Microsoft Azure bug left a bunch of cloud databases wide open ○ August 19 - *Bleeping Computer:* Russian APT29 hackers abuse Azure services to hack Microsoft 365 users ○ November 2 - *Dark Reading:* Critical Vulnerability in Microsoft Azure Cosmos DB Opens Up Jupyter Notebooks • **Windows** ○ February 4 - *Bleeping Computer:* CISA orders federal agencies to patch actively exploited Windows bug ○ July 12 - *Bleeping Computer:* CISA orders agencies to patch new Windows zero-day used in attacks ○ August 1 - *TechRadar:* Windows Defender hacked to deploy this dangerous ransomware ○ October 16 - *The Verge:* Microsoft's out-of-date driver list left Windows PCs open to malware attacks for years ○ November 30 - *Bleeping Computer:* New Windows malware also steals data from victims' mobile phones ○ December 15 - *Bleeping Computer:* Ukrainian govt networks breached via trojanized Windows 10 installers ○ December 15 - *Cybersecurity News:* Windows SmartScreen & DirectX Graphics Zero-day Flaw Let Attacker Gain Admin Privilege ○ December 19 - *Ars Technica:* Critical Windows code-execution vulnerability went undetected until now • **Office** ○ May 22 - *Bleeping Computer:* PDF smuggles Microsoft Word doc to drop Snake Keylogger malware ○ May 30 - *The Register:* Zero-day vuln in Microsoft Office: 'Follina' will work even when macros are disabled ○ October 17 - *The Hacker News:* Researchers Say Microsoft Office 365 Uses Broken Email Encryption to Secure Messages • **Exchange** ○ June 30 - *Bleeping Computer:* Microsoft Exchange servers worldwide backdoored with new malware ○ October 11 - *Bleeping Computer:* Microsoft Exchange servers hacked to deploy LockBit ransomware • **Teams** ○ July 14 - *SC Magazine:* Researcher finds vulnerability in Microsoft Teams that could have led to XSS attacks
March 2022	**Lapsus$ Breaches Microsoft Admin Account, Steals Part of Company's Source Code From Bing & Cortana** **Microsoft publishes lengthy blog post on the hack, saying no customer data was impacted but confirmed an account was compromised.** • "Over time, we have improved our ability to track this actor and helped customers minimize the impact of active intrusions and in some cases worked with impacted organizations to stop attacks prior to data theft or destructive actions. Microsoft is committed to providing visibility into the malicious activity we've observed and sharing insights and knowledge of actor tactics that might be useful for other organizations to protect themselves." (Source)
September 2022	**SQL Server FARGO Ransomware Hack.** **Hackers targeted vulnerable Microsoft SQL servers with FARGO ransomware.** • Microsoft SQL servers hacked in TargetCompany ransomware attacks. (Source) • Hackers use PowerPoint files for 'mouseover' malware delivery. (Source)

Date	Events
September 2022	**Mouseover Malware Hack.** **Russian hackers used a vulnerability in mouse movement on PowerPoint presentations to gain access to a malicious PowerShell script, targeting governments and the defense sector in Europe.** • Hackers use PowerPoint files for 'mouseover' malware delivery. (Source)
September 2022	**OAuth Hack.** **Chinese threat actors used malicious Oauth applications to take control of an unknown number of enterprise Exchange servers.** • New Microsoft Exchange zero-days actively exploited in attacks. (Source)
October 2022	**548,000+ Users Exposed in BlueBleed Data Leak.** **Over 2.4 terabytes of exposed data identified on a misconfiguration Microsoft endpoint.** • The data pertained to over 65,000 companies and 548,000 users, including customer emails, project information, and signed documents. • Microsoft Confirms Server Misconfiguration Led to 65,000+ Companies' Data Leak (Source)
October 2022	**Lazarus Group Attack.** **North Korean group Lazarus used social engineering and open-source software installers to access Windows operating systems.** • Hackers use Microsoft IIS web server logs to control malware (Source) • Unofficial Patch Released for New Actively Exploited Windows MotW Vulnerability (Source)
October – November 2022	**Threat Actors Gain Access to Military Facility's IT System Through Widely Known Microsoft Exchange Vulnerabilities.** **In October, NSA, FBI, and CISA release joint advisory admitting threat actors maintained long-term access to a military industrial facility's IT environment.** • "From November 2021 through January 2022, the Cybersecurity and Infrastructure Security Agency (CISA) responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network…Some APT actors gained initial access to the organization's Microsoft Exchange Server as early as mid-January 2021." (Source) **In November, Microsoft releases its 2022 Digital Defense Report, again emphasizing how consumers should take further security precautions.** • "Good cyber hygiene practices remain the best defense while the cloud provides the best physical and logical security against cyberattacks. This year's report includes even more recommendations for how people and organizations can protect themselves from attacks. The biggest thing people can do is pay attention to the basics." (Source)

Date	Events

2023	**Total Zero Days: 22**
	
	Relevant Reporting:
	• **Generally**
	  ○ March 30 - *The Verge:* Huge Microsoft exploit allowed users to manipulate Bing search results and access Outlook email accounts
	  ○ April 20 - *TechRadar:* Microsoft SQL servers hacked to spread ransomware
	  ○ April 20 - *TechRadar:* Bing and Cortana source code reportedly stolen by Medusa ransomware crew
	  ○ June 17 - *Associated Press:* Microsoft says early June disruptions to Outlook, cloud platform, were cyberattacks
	  ○ July 10 - *SC Magazine:* 'Big Head' malware threat looms, warn researchers
	• **Azure**
	• March 31 - *Infosecurity Magazine:* New Azure Flaw "Super FabriXss" Enables Remote Code Execution Attacks
	  ○ April 11 - *The Hacker News:* Newly Discovered "By-Design" Flaw in Microsoft Azure Could Expose Storage Accounts to Hackers
	  ○ May 6 - *SC Magazine:* Microsoft Azure API Management service impacted by flaws
	  ○ May 18 - *Dark Reading:* Microsoft Azure VMs Hijacked in Cloud Cyberattack
	  ○ June 21 - *The Hacker News:* Critical 'nOAuth' Flaw in Microsoft Azure AD Enabled Complete Account Takeover
	  ○ August 3 - *Bleeping Computer:* New Microsoft Azure AD CTS feature can be abused for lateral movement
	• **Windows**
	  ○ January 10 - *CRN:* Microsoft Seeing Exploits Of Windows Zero Day Vulnerability
	  ○ March 15 - *ITPro:* Windows admins plagued with issues after installing Outlook zero day patch
	  ○ March 22 - *Ars Technica:* "Acropalypse" Android screenshot bug turns into a 0-day Windows vulnerability
	  ○ July 13 - *Forbes:* Windows Users Urged To Update As Microsoft Confirms New Zero-Day Exploits
	  ○ October 5 - *The Hacker News:* CISA Warns of Active Exploitation of JetBrains and Windows Vulnerabilities
	• **Office**
	  ○ May 25 - *Bleeping Computer:* Microsoft 365 phishing attacks use encrypted RPMSG messages
	  ○ July 13 - *SC Magazine:* Malicious Microsoft Office docs drop LokiBot malware
	  ○ September 12 - *The Record:* CISA warns of attacks using Microsoft Word, Adobe bugs
	  ○ November 23 - *Cybersecurity News:* Hackers using Weaponized Office Document to Exploit Windows Search RCE
	• **Exchange**
	  ○ January 12 - *Bleeping Computer:* Microsoft: Cuba ransomware hacking Exchange servers via OWASSRF flaw
	  ○ January 26 - *CRN:* Microsoft Really Wants People To Patch Their Exchange Servers
	• **Teams**
	  ○ June 22 - *Bleeping Computer:* Microsoft Teams bug allows malware delivery from external accounts
	  ○ September 9 - *Bleeping Computer:* Microsoft Teams phishing attack pushes DarkGate malware

Date	Events
July 2023	**Chinese Hackers Spy on U.S. Gov. Agencies (Depts. of State, Commerce) via Vulnerability in Microsoft Cloud.** **In a blog post, Microsoft acknowledges that 25 organizations were involved in the hack, including government agencies.** • "**Accountability starts with us.** The accountability starts right here at Microsoft. We remain steadfast in our commitment to keep our customers safe. We are continually self-evaluating, learning from incidents, and hardening our identity/access platforms to manage evolving risks around keys and tokens. We need to continue to push the envelope on security so we're prepared for whatever might come our way. We will continue to work with our customers and community to share information and strengthen our collective defenses." (Source) **Media reports reference Brad Smith's 2021 remarks, noting this time the company "left its own keys on the table."** • "In 2021, for example, Microsoft President Brad Smith said in testimony before the U.S. House of Representatives that not doing so was like "leaving your keys on the kitchen table." If we extend Smith's metaphor to the most recent operation against the company, it seems that Microsoft left its own keys on the table inside its own house only to have them swiped and used against 25 different customers." (Source)
July 2023	**Sen. Ron Wyden (D-OR) to Demand U.S. Agencies Demand Accountability from Microsoft Over Latest Hacks.** **Wyden demanded that the Department of Justice, CISA, and the FTC hold Microsoft responsible for the recent hack.** • "I write to request that your agencies take action to hold Microsoft responsible for its negligent cybersecurity practices, which enabled a successful Chinese espionage campaign against the United States government." (Source) • "… Microsoft bears significant responsibility for this new incident… as Microsoft pointed out after the SolarWinds incident, high-value encryption keys should be stored in an HSM, whose sole function is to prevent the theft of encryption keys. But Microsoft's admission that they have now moved consumer encryption keys to a 'hardened key store used for our enterprise systems' **raises serious questions** about whether Microsoft followed its own security advice and stored such keys in an HSM." (Source) **Wyden said Microsoft never properly took accountability for the 2020 SolarWinds hack.** • "Microsoft never took responsibility for its role in the SolarWinds hacking campaign. It blamed federal agencies for not pushing it to prioritize defending against the encryption key theft technique used by Russia, which Microsoft had known about since 2017. It blamed its customers for using the default logging settings chosen by Microsoft, and then blamed them for not storing the high-value encryption keys in a hardware vault, known as a Hardware Security Module (HSM)." (Source)
August 2023	**Independent Government Cyber Review Board Announces Investigation into Microsoft.** "Today, Secretary of Homeland Security Alejandro N. Mayorkas announced that the Cyber Safety Review Board (CSRB) will conduct its next review on the malicious targeting of cloud computing environments. The review will focus on approaches government, industry, and Cloud Service Providers (CSPs) should employ to strengthen identity management and authentication in the cloud. The CSRB will assess the recent Microsoft Exchange Online intrusion, initially reported in July 2023, and conduct a broader review of issues relating to cloud-based identity and authentication infrastructure affecting applicable CSPs and their customers." (Source)

Date	Events
August 2023	**Microsoft Teams Compromised by Russia's Cozy Bear.** **The Russian gang known as Cozy Bear has been using Microsoft Teams to phish marks in governments, NGOs, and IT businesses.** • How an unpatched Microsoft Exchange 0-day likely caused one of the UK's biggest hacks ever (Source) • Microsoft addresses Office vulnerability attacked by Russian spooks in latest update (Source)
November 2023 - January 2024	**Midnight Blizzard Steals Emails & Other Documents from Key Microsoft Executives Through Password Spray.** **In a late Friday news dump, Microsoft publicly disclosed that Midnight Blizzard accessed senior leaders' emails, with the first attack occurring as far back as November 2023.** • Russian hackers exploited an Outlook bug to hijack Exchange accounts and targeted entities including government, energy, transportation, and other key organizations in the U.S., Europe, and Middle East. • "The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024…Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium…Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents. The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed." (Source) **Several days later, Microsoft says the company is "shifting the balance we need to strike between security and business risk."** • " As stated in the MSRC blog, given the reality of threat actors that are well resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk – the traditional sort of calculus is simply no longer sufficient. For Microsoft, this incident has highlighted the urgent need to move even faster…If the same team were to deploy the legacy tenant today, mandatory Microsoft policy and workflows would ensure MFA and our active protections are enabled to comply with current policies and guidance, resulting in better protection against these sorts of attacks." (Source) **Microsoft CEO Satya Nadella avoids commenting on Microsoft's security lapses in NBC interview.** • "I'm glad that we have the capability we have to even detect what they are doing … If this is about two nation states attacking each other and especially civilian targets, then we are in a very new world order. It is a breakdown of world order that we have not seen before." (Source)

2024	**Total Zero Days: 8 [as of May 20, 2024]**
	
	Relevant Reporting:
	• **Generally**
	  ○ March 1 - *Windows Central*: Microsoft's GitHub is under siege as security experts claim over 100,000 Github repositories are infected
	  ○ March 11 - *Bleeping Computer*: Researchers expose Microsoft SCCM misconfigs usable in cyberattacks [ActiveDirectory]
	  ○ March 21 - *The Hac`ker News*: Russia Hackers Using TinyTurla-NG to Breach European NGO's Systems

Date	Events

	• **Azure**
	  ○ February 6 - *Dark Reading:* Microsoft Azure HDInsight Bugs Expose Big Data to Breaches
	  ○ February 29 - *SC Magazine:* Azure-connected IoT devices at risk of RCE due to critical vulnerability
	• **Windows**
	  ○ January 15 - *Bleeping Computer:* Windows SmartScreen flaw exploited to drop Phemedrone malware
	  ○ February 13 - *Bleeping Computer:* Hackers used new Windows Defender zero-day to drop DarkMe malware
	  ○ February 29 - *SecurityWeek:* Windows Zero-Day Exploited by North Korean Hackers in Rootkit Attack
	  ○ March 1 - *SecurityWeek:* CISA Warns of Windows Streaming Service Vulnerability Exploitation
	  ○ March 5 - *Security Affairs:* CISA Adds Microsoft Windows Kernel Bug Used by Lazarus APT to its Known Exploited Vulnerabilities Catalog
	  ○ March 14 - *TechRadar:* Hackers exploit another Windows security flaw to drop DarkGate malware
	• **Exchange**
	  ○ February 19 - *Bleeping Computer:* Over 28,500 Exchange servers vulnerable to actively exploited bug
	• **Teams**
	  ○ January 30 - *Bleeping Computer:* Microsoft Teams phishing pushes DarkGate malware via group chats
	• **SharePoint**
	  ○ January 12 - *The Register:* Exploit for under-siege SharePoint vuln reportedly in hands of ransomware crew
	  ○ March 27 - *Security Week:* CISA: Second SharePoint Flaw Disclosed at Pwn2Own Exploited in Attacks

April 2024	**Independent Government Cyber Review Board Faults Microsoft for "Cascade of Security Failures" Related to the Preventable Summer 2023 China Hack.**
	
	On March 20, 2024, the Cyber Safety Review Board ("The Board") issued a report titled, "Review of the Summer 2023 Microsoft Exchange Online Intrusion," which faulted Microsoft for a "corporate culture that deprioritized enterprise security investments…"
	• "The CSRB's review found that the intrusion by Storm-0558, a hacking group assessed to be affiliated with the People's Republic of China, was preventable. It identified a series of Microsoft operational and strategic decisions that collectively pointed to a corporate culture that deprioritized enterprise security investments and rigorous risk management, at odds with the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations. The Board recommends that Microsoft develop and publicly share a plan with specific timelines to make fundamental, security-focused reforms across the company and its suite of products. Microsoft fully cooperated with the Board's review." (Source)
	
	The Board also found that Microsoft's "security culture was inadequate and requires an overhaul…"
	• "The Board finds that this intrusion was preventable and should never have occurred. The Board also concludes that Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations. The Board reaches this conclusion based on:
	  ○ 1. the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed;
	  ○ 2. Microsoft's failure to detect the compromise of its cryptographic crown jewels on its own, relying instead on a customer to reach out to identify anomalies the customer had observed;

Date	Events
	○ 3. the Board's assessment of security practices at other cloud service providers, which maintained security controls that Microsoft did not; ○ 4. Microsoft's failure to detect a compromise of an employee's laptop from a recently acquired company prior to allowing it to connect to Microsoft's corporate network in 2021; ○ 5. Microsoft's decision not to correct, in a timely manner, its inaccurate public statements about this incident, including a corporate statement that Microsoft believed it had determined the likely root cause of the intrusion when in fact, it still has not; even though Microsoft acknowledged to the Board in November 2023 that its September 6, 2023 blog post about the root cause was inaccurate, it did not update that post until March 12, 2024, as the Board was concluding its review and only after the Board's repeated questioning about Microsoft's plans to issue a correction; ○ 6. the Board's observation of a separate incident, disclosed by Microsoft in January 2024, the investigation of which was not in the purview of the Board's review, which revealed a compromise that allowed a different nation-state actor to access highly-sensitive Microsoft corporate email accounts, source code repositories, and internal systems; and ○ 7. how Microsoft's ubiquitous and critical products, which underpin essential services that support national security, the foundations of our economy, and public health and safety, require the company to demonstrate the highest standards of security, accountability, and transparency." (Source)
May 2024	**Microsoft announced in a blog post that the company is making security a top priority for every employee—including Executives.** **On May 3 2024, Microsoft announced making security a top priority above all else.** • "Last November, we launched the Secure Future Initiative (SFI) to prepare for the increasing scale and high stakes of cyberattacks. SFI brings together every part of Microsoft to advance cybersecurity protection across our company and products. Since then, the threat landscape has continued to rapidly evolve, and we have learned a lot. The recent findings by the Department of Homeland Security's Cyber Safety Review Board (CSRB) regarding the Storm-0558 cyberattack from last July, and the Midnight Blizzard attack we reported in January, underscore the severity of the threats facing our company and our customers. Microsoft plays a central role in the world's digital ecosystem, and this comes with a critical responsibility to earn and maintain trust. We must and will do more." **Satya Nadella released a memo detailing the new security overhaul for the company and "how to learn from attackers to improve its security processes." (Source)** • "If you're faced with the tradeoff between security and another priority, your answer is clear: Do security. In some cases, this will mean prioritizing security above other things we do, such as releasing new features or providing ongoing support for legacy systems. This is key to advancing both our platform quality and capability such that we can protect the digital estates of our customers and build a safer world for all."
May 2024	**Senator Vance (R-OH), Senator Scott (R-FL), and Congressman LaTurner (KS-02) expressed their concerns about the cybersecurity practices of the federal government in letters to Jen Easterly, Head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA).**

Date	Events
	On May 8, 2024, Senator Scott sends a letter to Easterly regarding the ongoing hacks by Russian state actors and exposed sensitive federal communications. Scott's letter specifically mentions the CSRB report and Microsoft's operational and strategic decisions that collectively pointed to deprioritized security investments and risk management. • "It is worrying that the administration's cybersecurity efforts appear to be more focused on colluding with Big Tech to censor the speech of law-abiding Americans, than it has been on preventing cyberattacks. The continued politicization of CISA represents a serious and dangerous misuse of government resources that should be 100% focused on its obligation to protect the cybersecurity of the U.S. government from foreign actors and holding commercial partners that have failed to meet our security standards accountable." **On May 10, 2024, Senator Vance sends a letter to Easterly expressing concern that U.S. critical infrastructure appears to be under attack from the PRC state-sponsored hacker group known as Volt Typhoon** • "According to reports, Volt Typhoon has compromised hundreds of thousands of devices since it was publicly identified by Microsoft in May 2023. Indeed, experts believe the group has targeted U.S. critical infrastructure since mid-2021 using malicious software that penetrates internetconnected systems. On January 31, 2024, the FBI reported that it had disrupted some of Volt Typhoon's operations by removing the group's malware from some small office routers. However, on February 7, 2024, CISA, the FBI, and other U.S. agencies along with the Five Eyes partners released a major advisory in which they warned that Volt Typhoon was pre-positioning on critical infrastructure networks to "enable disruption or destruction of critical services in the event of increased geopolitical tensions." According to the agencies, "this is a critical business risk for every organization in the United States and allied countries." **On May 13, 2024, Congressman LaTurner (KS-02) sends a letter to Easterly expressing concerns about the cybersecurity practices of Microsoft as the largest vendor to the federal government.** • "Microsoft is a leading provider of productivity software, cloud services, and security technology to the federal government, but I am concerned about recent vulnerabilities exposed during cyber- attacks against the company and the potential impact on our national security. In just the past few years, it has been reported that Microsoft's security posture has failed numerous times - exposing data and information for millions of records. These security failures include the 60,000 emails stolen from the State Department exposing cabinet level communications that the CSRB report looked into, thousands of Microsoft Azure customer database and accounts being exposed, an estimated 30,000 United States companies using Microsoft Exchange Servers being breached, and thousands of customers impacted by the SolarWinds security failures. Most recently, it was reported that Microsoft's company systems were breached, exposing emails of senior company executives containing unknown customer, government, or national security related information."
May 2024	**Leaders on the U.S. House Homeland Security Committee wrote to Brad Smith, the vice chair and president of Microsoft, asking him to testify on May 22.** **On May 9, 2024, the two top leaders on the House Homeland Security Committee want to put Microsoft on the hot seat about its cybersecurity practices. Committee Chairman Mark Green (R-Tenn.) and Ranking Member Bennie Thompson (D-Texas) wrote to Brad Smith, the vice chairman and president of Microsoft, asking him to testify on May 22.** • "As a trusted provider of operating systems, cloud platforms, and productivity software for U.S. government agencies, including those within the U.S. intelligence community, Microsoft bears a profound responsibility to prioritize and implement effective cybersecurity measures. However, the CSRB

Date	Events
	report revealed that Microsoft has repeatedly failed to prevent substantial cyber intrusions, causing grave implications for the security and integrity of U.S. government data, networks, and information, and putting Americans—including U.S. government officials—at risk. The CSRB's report further revealed that a "cascade of Microsoft's avoidable errors" may have allowed the 2023 Microsoft Exchange Online cyber intrusion by the People's Republic of China (PRC) cyber espionage group, Storm-0558, to succeed. These findings underscore the critical importance of immediate and decisive action." (**Source**)
June 2024	**Brad Smith, the vice chair and president of Microsoft, testifies before the U.S. House Homeland Security Committee at a hearing regarding, "A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and Implications for Homeland Security."** **On June 13, 2024, Brad Smith, the vice chairman and president of Microsoft, testifies before the U.S. House Homeland Security Committee regarding cybersecurity failures in Storm-0558 and other foreign-based hacks to assess whether the steps taken by Microsoft are sufficient to address security concerns raised in April Cyber Safety Review Board report.** • "Transparency is a foundation of trust and Microsoft needs to be more transparent. In 2002, Bill Gates said, "when we face a choice between adding features and resolving security issues, we need to choose security." The CSRB found at Microsoft had "drifted away from this ethos….Last November, Microsoft announced a secure future initiative touting a reinvigorated approach to security. But in January, Microsoft itself was compromised by Russian threat actors who used unsophisticated tactics to assess emails of high level employees. Unfortunately, those emails included correspondence with government officials and put the security federal networks at risk, once again, basic cyber security tools that were not enabled would have thought that this intrusion." (Source) • "Multiple lawmakers on the House Homeland Security Committee pressed Smith about whether he was being transparent about the company's response to the breach, other recent security lapses, and its continued business in China. … 'I'm sorry, I just for some reason, I just don't trust what you're saying to me,' Rep. Carlos Gimenez (R-Fla) said Thursday to Smith, during a heated exchange about whether Microsoft's work in China leaves it more vulnerable to the country's intelligence services. … At one point, Rep. Clay Higgins (R-La) pressed Smith about why Microsoft was indecisive in correcting information it had published on the hack but later determined was misleading — a key finding of the report. When Smith said the company hesitated because it didn't consider the new information 'actionable,' Higgins shot back: 'That answer does not encourage trust.'" (Source)