

November 9, 2023

VIA Electronic Submission

To: cloudmi@cma.gov.uk

Re: Response to CMA Cloud Services Market Investigation Issues Statement

The Coalition for Fair Software Licensing (the "<u>CFSL</u>" or the "<u>Coalition</u>") appreciates the opportunity to submit this letter to the Competition and Markets Authority (CMA) in response to the Issues Statement outlining a framework for an independent market investigation into Cloud Market Services following referral from Ofcom. Although the Issues Statement outlines a number of hypotheses and theories of harm potentially resulting in an "adverse effect on competition (AEC)," our comments focus on "software licensing practices by cloud service providers (that) restrict customer choice and prevent effective competition;" specifically, those of Microsoft and the impact of those practices on customer choice, competition, and cybersecurity.

The Coalition is a global initiative that brings together information technology providers, customers and users, including businesses and government organisations, from the UK, Europe, North America and APAC. The Coalition engaged with Ofcom throughout their market study where our members expressed profound concerns with the software licensing restrictions and bundling practices by Microsoft and other legacy vendors. The damages of these practices are reflected in Ofcom's final cloud market study report (Chapter 9). Our members care deeply about competition and call for the adoption of the *Principles of Fair Software Licensing*¹ to ensure that the IT services market (including cloud) is vibrant, transparent, and fair.

We submit this letter to summarize some of the considerations that we have previously discussed with Ofcom and in response to their findings in the final report. Our members greatly appreciate the inclusion of software licensing practices in the Issues Statement and believe that the software licensing restrictions adopted by Microsoft and described by Ofcom in Chapter 9 of their report should take a prominent place in the forthcoming market investigation. We understand that the CMA will be working to further define the exact scope of the market investigation reference (MIR) and are at your disposal to provide further evidence and discuss this submission with participation of our members.

Executive Summary

Virtually every business in the UK 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

¹ The principles are: (1) Licensing Terms Should Be Clear and Intelligible; (2) Freedom to Bring Previously Purchased Software to the Cloud; (3) Customers Should Be Free to Run their On-Premises Software on the Cloud of their Choice; (4) Reducing Costs through Efficient Use of Hardware; (5) Freedom from Retaliation for Cloud Choices; (6) Avoiding Customer Lock-In Through Interoperable Directory Software; (7) Equal Treatment for Software Licensing Fees in the Cloud; (8) Equal Treatment for Software Licensing Fees in the Cloud; and (9) Licenses Should Cover Reasonably Expected Software Uses. Our Principles, available at: https://www.fairsoftwarelicensing.com/our-principles/.

embraced BYOL with the emerging cloud, and most continue this practice today.

Microsoft, however, which has long dominated operating (Windows 10/11, Windows Server 2019/2023) and productivity software (Office 365),² 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 made a monumental change to its licensing practices and policies. This change presented existing software customers with a Hobson's choice:

(a) forego their previously purchased (often perpetual) software licenses and incur the additional cost of purchasing a second license to run legacy Office software with gaps in capabilities on the cloud provider of their choice;

(b) not have the ability to run Office 365 on their cloud provider of choice; or

(c) migrate to Azure 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.

² Frederic Jenny, Unfair Software Licensing Practices: A quantification of costs for cloud customers, at 13 available at:

https://cispe.cloud/website_cispe/wp-content/uploads/2023/06/Quantification-of-Cost-of-U nfair-Software-Licensing_Prof-Jenny_June-2023_web.pdf) [CISPE English Report] (June 2023).

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 agrees that the CMA should investigate them as part of the forthcoming cloud computing services MIR as the CMA has indicated it will in its Issues Statement. Further, while the Coalition continues to receive input from members regarding specific remedies, we are generally supportive of the proposed remedies to software licensing practices included in the Issues Statement and believe they are consistent with the *Principles for Fair Software Licensing*.

The Coalition and Cloud Computing

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. First launched in France in April 2021 as a collaboration of CISPE (the Association of Cloud Infrastructure Service Providers in Europe) and CIGREF (a CIOs' association representing over 150 French organizations, mostly the largest listed companies on the Euronext Paris Stock Exchange), the *Principles of Fair Software Licensing* provide the foundation needed to spur innovation, choice, and growth in the digital economy.³ The *Principles* have since gathered the support of organizations representing interests ranging from cloud service startups and their venture funders to CIOs and customer companies in the United Kingdom, throughout the European Union (including Italy, Spain, Netherlands, Germany, and Denmark), and Israel.

The European-based allies of the Coalition have worked tirelessly to bring fair competition to and customer choice in the cloud in Europe, including by filing complaints with European antitrust authorities.⁴

³ Our Principles, available at: <u>https://www.fairsoftwarelicensing.com/our-principles/</u>.

⁴ Paul Kunert, *Euro clouds lodge another complaint against Microsoft over anti-competitive licenses,* The Register, available at:

https://www.theregister.com/2022/11/09/cispe_ec_microsoft_complaint/ (Nov. 9, 2022).

As with the efforts of CISPE and others in Europe, the Coalition has worked to accomplish real change—but the restrictive licensing practices that limit customer choice and hinder competition persist.⁵

1. Brief Background on Licensing and the Cloud

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. There are three key elements to this definition⁶:

- <u>Computing Resources</u>: these include hardware (servers and network equipment) and software (applications) that are used to process workloads and store data.
- <u>On Demand</u>: 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.
- <u>Via a Network</u>: 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.

For many customers, cloud computing is more efficient than "do it yourself" IT solutions. Demand for cloud computing services has exploded in recent years. For example, Gartner forecasts worldwide end-user spending on public cloud services to grow 20.7% to total \$591.8 (~ £484.35) billion in 2023,

⁵ While Microsoft is not alone in its cloud-related anticompetitive licensing, Microsoft's monopoly position in multiple critical upstream software markets makes it a powerful example of the ways in which competition is being substantially lessened, to the detriment of software and IT service customers. That being said, it is worth noting that one study showed that Oracle licenses its software in its own cloud on an "actual" CPU basis, while in a competitors' cloud, it licenses on an "available" CPU basis. Michael Garland, *Vendor Locking in the Cloud*, FCW, https://fcw.com/comment/2022/04/vendor-locking-cloud/365665/, (Apr. 14, 2022).

⁶ *The NIST Definition of Cloud Computing,* U.S. Department of Commerce National Institutes of Standards and Technology, available at:

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

up from \$490.3 (~ \pm 401.28) billion in 2022, with the highest end-user spending growth in IaaS (29.8%).⁷

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. In particular, entities were generally able to bring their on-premises software with them into the cloud.⁸ This ability to take on-premises software into the cloud not only proved efficient for cloud customers, it also facilitated competition by lowering switching costs between cloud and 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 ("<u>BYOL</u>") for any software license that you owned.⁹ As described below, however, 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.

2. Anticompetitive Conduct in Information Technology

A set of distinct yet interrelated practices threaten competition throughout the cloud stack and in information technology. As outlined below, Microsoft uses its dominance in desktop operating, server, and productivity software to impose additional costs on or outright prohibit customers from licensing software for use on competing cloud providers and tie adjacent

⁷ Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \$600 Billion in 2023, available at:

https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwi de-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023 (Oct. 31, 2022). ⁸ One exception to this was Microsoft, as discussed *infra*.

⁹ See MetrixData360, Bring Your Own License (BYOL) on Third Party Cloud Providers, available at <u>https://metrixdata360.com/uncategorized/19158-2/;</u> Gregg Keizer, Microsoft set to close licensing loopholes, leave cloud rivals high and dry, Computer World, available at:

https://www.computerworld.com/article/3435104/microsoft-set-to-close-licensing-loopholes-leave-cloud-rivals-high-and-dry.html (September 3, 2019).

product market offerings together, preventing customers from picking only their preferred or best services. 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.

A. Leveraging Microsoft's Dominance to Skew Competition

Broadly speaking, Microsoft's anticompetitive practices involve leveraging its longstanding dominant positions in desktop operating, server, and productivity software, in which customers purchase licenses for Microsoft "must-have" products like Windows, Word, Excel and PowerPoint, to promote Azure, its cloud computing product, and other Microsoft products like Teams and Defender. As noted below, while they have invited complaints from customers and scrutiny from regulators, these practices have proven remarkably successful in driving business to Azure and expanding the reach of other Microsoft products.

Microsoft holds a dominant position in: (1) operating systems (OSs) for personal computers and servers (*i.e.*, Windows (desktop) 10 and 11; Windows Server);¹⁰ (2) productivity software for PCs (*i.e.*, Office and Microsoft 365 (cloud-based));¹¹ and (3) enterprise mail server software and services (*i.e.*, Exchange Server).¹² As the CMA is aware, in the late 1990s and early 2000s, Microsoft faced a series of legal challenges, including in the US and EU, to prevent the company from continuing to implement a set of exclusionary practices that protected Microsoft's OS monopoly from competition in the

¹⁰ Case COMP/C-3/39.530 – Microsoft (Tying), Comm'n Decision (Dec. 16, 2009),

https://ec.europa.eu/competition/antitrust/cases/dec_docs/39530/39530_2671_5.pdf (client PC operating systems); COMP/C-3/37.792 – Microsoft, Comm'n Decision (Mar. 24, 2004), https://your.caselex.eu/storage/announcement/37792_4177_3.pdf (client PC operating systems and work group server operating systems). See also CMA, Anticipated acquisition by Microsoft of Activision Blizzard, Inc. Final Report (Apr. 26, 2023),

https://assets.publishing.service.gov.uk/media/644939aa529eda000c3b0525/Microsoft_Activis ion_Final_Report_.pdf (findings on Microsoft's position in PC operating systems).

¹¹ <u>https://ec.europa.eu/competition/mergers/cases1/202231/M_10290_8431645_854_3.pdf;</u> Case M.8124 – Microsoft/LinkedIn, Comm'n Decision (Dec. 6, 2016),

https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf (findings on Microsoft's market shares in productivity software).

¹² Ioana Patringenaru, *Who's got your mail? Google and Microsoft, mostly*, UC San Diego Today, available at: <u>https://today.ucsd.edu/story/IMC2021_savage</u>. The research was funded by the National Science Foundation, the University of California San Diego, the EU H2020 CONCORDIA project and Google.

nascent "middleware" market.¹³ Though the governments prevailed and the historical practices in question ceased, the company maintained its OS dominance and developed a new set of exclusionary practices to capture customers seeking to benefit from the cloud-based technologies that have emerged in the intervening years.¹⁴

Now, a quarter century later, the company is once again leveraging its dominance and using similar conduct to imperil competition across a broad range of cloud services.

i. Licensing

Microsoft's licensing terms restrict customers from using licenses they have already purchased to run Windows, Office, and the like on competing cloud services, but not on Azure. The company has never justified this conduct; and, after years of cloud customers and competitors drawing attention to the issue in Europe, Microsoft President Brad Smith last year conceded that "[t]here definitely are some valid concerns.... It's very important for us to learn more and then make some changes."¹⁵

As set out in further detail below, recent licensing changes made by Microsoft that purport to address antitrust concerns not only fall far short of that promise, but skew competition further. As CISPE observed, "[o]n the contrary, the new contractual terms ... add[ed] new unfair practices to the list."¹⁶

¹³ United States v. Microsoft, No. 98-1232 (filed May 18, 1998); T-201/04, Microsoft v Commission, Judgement of 17 September 2007.

¹⁴ Jordan Novet and Erin Black, *How Microsoft Windows Came to Dominate PC Operating* Systems, CNBC, available at:

https://www.cnbc.com/video/2021/07/10/how-windows-came-to-dominate-pc-operating-sys tems.html (Jul. 10, 2021).

¹⁵ Dina Bass, *Microsoft Customers Decry Cloud Contracts That Sideline Rivals*, Bloomberg, available at:

https://www.bloomberg.com/news/articles/2022-04-12/microsoft-customers-decry-cloud-co ntracts-that-sideline-rivals#xj4y7vzkg (Apr. 11, 2022)

¹⁶ CISPE, CISPE files complaint against Microsoft in European Commission, available at: https://cispe.cloud/cispe-files-complaint-against-microsoft-with-european-commission/. Paul Kunert, Top cloud players reject Microsoft's attempt to settle EU licensing complaint, The Register, available at:

https://www.theregister.com/2023/05/30/microsoft_cispe_settlement_rejected/?td=rt-4a (May 30, 2023).

Enterprise License Agreements

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, as Microsoft has moved from Office 365 to Microsoft 365 enterprise licenses and related tiers, the packages have included an increasing number of products from their vertical stack to drive adoption and dependence on the Microsoft ecosystem.¹⁷ 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,¹⁸ 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.

Restricting BYOL

¹⁷ Arif Bacchus, *What's the Difference Between Office 365 and Microsoft 365?*, ONMSFT.com – The Tech News Site, available at:

https://www.onmsft.com/feature/whats-the-difference-between-office-365-and-microsoft-3 65/ (Oct. 8, 2019). Note that both the "E" and "M" level Microsoft licensing nomenclature continues to be used in spite of a transition toward the sale of Microsoft 365 (or "M") packages. ¹⁸ Mary Jo Foley, *Microsoft makes changes in its field sales, support groups as FY'21 begins,* ZDNet, available at:

https://www.zdnet.com/article/microsoft-makes-changes-in-its-field-sales-support-groups-a s-fy21-begins/ (Jul. 6, 2020).

As noted above, BYOL was a well-established norm in the software business before cloud computing and allowed customers to run purchased software in the hardware environment of their choice, be it on-premises or on cloud provider(s) of choice. It has predominated software use in cloud computing from its launch in 2006, with one notable exception. Since 2019, Microsoft has made a series of changes to their licensing terms that restrict BYOL; limiting customer use of non-Azure infrastructure to deploy Microsoft software and forcing legacy customers to move from flexible perpetual licenses purchased for on-premises use to subscription arrangements run on Azure.

At the outset of the cloud, Microsoft's software license terms required the licensed software to be housed on a server that was "fully dedicated" to the license-holder, something that was not possible for early cloud services customers. In response to this license term however, in 2008–2009, cloud service providers began offering "dedicated hosts," individualized servers that were dedicated to a single cloud customer, as a service to permit Microsoft's software customers to comply with the license terms while still leveraging the benefits of the cloud. This sapped cloud efficiency, as providers were required to dedicate whole servers to customers, as opposed to allowing servers to be used simultaneously by multiple customers and better utilizing available capacity. The whole service was more expensive.¹⁹

Microsoft's Azure was announced in October 2008 and launched commercially in 2010. In 2011, the company introduced License Mobility, which permitted customers to bring Microsoft licenses to the cloud. License Mobility also did not permit the use of key products, such as Windows Server and Windows Desktop, although a customer that moved to Azure was permitted use of the desired products.²⁰

In 2014, in response to competitive pressures and to grow the company's share price, Microsoft pivoted to embrace the cloud. Just 52 days into Satya Nadella's tenure as Microsoft's CEO, he publicly announced his

¹⁹ Christopher Mims, Everything that's wrong with Microsoft, as told by veterans who abandoned the company, Quartz, available at:

https://qz.com/118513/the-long-hard-road-back-for-microsoft (Aug. 26, 2013).

²⁰ Saul Hansell, *Steve Ballmer Maps Microsoft's Cloud-y Future*, New York Times, available at: <u>https://archive.nytimes.com/bits.blogs.nytimes.com/2009/03/20/steve-ballmer-maps-microsofts-cloud-y-future/</u> (Mar. 20, 2009).

"Mobile-First, Cloud-First" initiative, focusing on developing Azure into "a cloud for everyone and every device".²¹

During this period, customer demand for cloud services boomed. Numerous cloud providers entered the market, and thousands upon thousands of customers moved to the cloud. Prices went down.²² Services flourished.

By 2018, Azure was driving Microsoft's share price, and pressure to grow Azure share was immense.²³ Azure had grown aggressively from the first quarter of 2017 until the third quarter of 2018, reaching revenue growth greater than 90% year over year in each quarter.²⁴ However, Azure's growth began to fall in the fourth quarter of 2018.²⁵ After two quarters of decelerated growth, Wall Street analysts reduced Azure's global growth expectations.²⁶

https://www.wsj.com/articles/microsofts-cloud-continues-to-fuel-growth-1532032095 (July 19, 2018).

²⁵ Id.

²¹ Satya Nadella, Microsoft Press Briefing, available at:

https://news.microsoft.com/2014/03/27/satya-nadella-mobile-first-cloud-first-press-briefing/ (Mar. 27, 2014).

²² Kurt Mackie, *Microsoft Cuts Prices on Some Azure Services*, Redmond Magazine, available at: <u>https://redmondmag.com/articles/2014/09/25/azure-price-cuts.aspx?admgarea=BDNA&m=1</u> (Sep. 25, 2014).

²³ "Microsoft's success in building out its cloud business has driven up shares of the company more than 40% in the past year ... The performance of Microsoft's Azure cloud-computing services, as well as its Office 365 online-productivity service for businesses, has pushed Microsoft shares to record highs over the past two weeks. ... After hours, shares touched record highs above \$108 following Ms. Hood's guidance for segments that include Azure and Windows. The projections topped Wall Street's expectations.... Azure revenue increased 89%, compared with 93% three months ago—the first time the business has grown slower than 90% since Microsoft began reporting the metric in October 2015." Jay Greene, *Microsoft's Revenue Gets Lift From Cloud*, The Wall Street Journal, available at:

²⁴ Jay Greene, *Microsoft's Cloud Strategy Pays Off*, The Wall Street Journal, available at: <u>https://www.wsj.com/articles/microsofts-profit-revenue-rise-even-as-cloud-business-growth</u> <u>-slows-1540413172</u> (Oct. 24, 2018).

²⁶ Jay Greene, *In Microsoft's Earnings, Watch the Pace of Cloud Growth*, The Wall Street Journal, available at:

https://www.wsj.com/articles/in-microsofts-earnings-watch-the-pace-of-cloud-growth-15403 73401 (Oct. 24, 2018). "[E]xpects growth eased to 72.5% in the just-ended quarter." Jay Greene, *Microsoft's Expanding Cloud Is Likely to Limit Growth*, The Wall Street Journal, available at: https://www.wsj.com/articles/microsofts-expanding-cloud-is-likely-to-limit-growth-115488442 00 (Jan. 30, 2019) <u>compare with</u> "In the just-ended quarter, Azure grew 76%, a strong showing as the pace of growth has been decelerating as Azure gets bigger." Jay Greene, *Microsoft's Gain Tempered by Chip*, The Wall Street Journal, available at:

By July 2019, the stock market still had lofty expectations of continued double-digit topline revenue growth for Azure.²⁷ In spite of Microsoft coming under pressure for a series of Azure-related outages,²⁸ Microsoft hit those analyst projections and offered guidance of double digit revenue growth into the next fiscal year. This was despite Azure revenue growth falling to 64% by that point.²⁹ But Microsoft recognized that Azure was having trouble competing on the merits, beset among other things by insufficient redundancy and a lack of capacity (ultimately resulting in a 2020 Teams blackout that required the company to put resource limits on Azure subscribers).³⁰

In August 2019, Microsoft announced a change to its licensing terms. Beginning in October of that year, it wrote: "on-premises licenses purchased without Software Assurance and mobility rights cannot be deployed with dedicated hosted cloud services offered by the following public cloud providers: Microsoft, Alibaba, Amazon (including VMware Cloud on AWS), and Google."³¹ As a practical matter, that meant that customers would need to

https://www.wsj.com/articles/microsoft-results-to-hinge-on-cloud-computing-growth-115560 98203 (Apr. 24, 2019) compare with "Azure . . . saw revenue surge 73% year over year." Dan Gallagher, *Microsoft Resists Gravity's Pull*, The Wall Street Journal, available at:

https://www.wsj.com/articles/microsoft-expected-to-report-earnings-boost-what-to-watch-11 563442202 (July 18, 2019).

²⁸ See, e.g., M. Van Horenbeeck, Office 365 Monitoring: 5/2/19 Office 365 and Azure Global Outage Recap, ENow, available at:

https://www.enowsoftware.com/office-365-monitoring-outages/sharepoint-outage-2019-offic e365-monitoring (May 2019).

³⁰ The Economist, *How Satya Nadella turned Microsoft around*, available at:

https://www.economist.com/briefing/2020/10/22/how-satya-nadella-turned-microsoft-aroun d (Oct. 22, 2020).

https://www.microsoft.com/en-us/licensing/news/updated-licensing-rights-for-dedicated-clo ud (Aug. 1, 2019).

https://www.wsj.com/articles/microsoft-reports-slower-sales-in-some-product-lines-despitecloud-strength-11548885062 (Jan 30. 2019); "Analysts at UBS estimate Azure revenue grew 66% in the fiscal third quarter" Asa Fitch, *Microsoft Results to Hinge on Cloud-Computing Growth*, The Wall Street Journal, available at:

https://www.wsj.com/articles/microsoft-resists-gravitys-pull-11556192166 (Apr. 25, 2019).

²⁷ Asa Fitch, *Microsoft Expected to Report Earnings Boost: What to Watch*, The Wall Street Journal, available at:

²⁹ Asa Fitch, *Microsoft's Cloud Business Drives Record Sales*, The Wall Street Journal, available at: <u>https://www.wsj.com/articles/microsofts-cloud-business-drives-record-sales-11563481232</u> (July 18, 2019).

³¹ Microsoft, Updated Microsoft Licensing Terms for Dedicated Hosted Cloud Services, available at:

repurchase their existing licenses to operate software on these other cloud providers, dubbed "Listed Providers."³²

On-Premises/Traditional outsourcing services		Cloud services	
On-premises	Traditional outsourcing	Dedicated hosted cloud services by Listed Providers	Multitenant cloud services
On-premises use rights		License Mobility through Software Assurance where applicable Azure Hybrid Benefit for Azure only Cloud services with licenses included	

The inclusion of Microsoft on the list was illusory: for customers of Azure, the "Azure Hybrid Benefit" enabled "costs savings" relative to using other, competing providers.³³ As the Economist observed, "Not to offend antitrust rules Microsoft put Azure on its list alongside AWS, GCP, and Alibaba Cloud. But it separately offered customers a better deal to move to Azure, offsetting the extra cost."³⁴ In short, Azure Hybrid Benefits provides Microsoft with a way to bypass the limitations that it imposes on other "Listed Providers." Under the program, customers can access the same software but have to forfeit their existing licenses in return for cloud-based subscriptions that only apply to Azure.

If a customer wished to use another cloud provider, they would need to purchase a new license in addition to the Microsoft license they already had for the same software, often at a significant cost, even if the non-Azure cloud provider was willing to dedicate servers solely to the customer. For some software, there was no option but to run Microsoft architecture.³⁵

- https://azure.microsoft.com/en-us/pricing/hybrid-benefit/#features (advertising that "AWS is up to 5 times more expensive than Azure for Windows Server and SQL Server").
- ³⁴ The Economist, *How Satya Nadella turned Microsoft around*, available at:

³² Id.

³³ Microsoft, Azure Hybrid Benefit, available at:

https://www.economist.com/briefing/2020/10/22/how-satya-nadella-turned-microsoft-aroun d (Oct. 22, 2020).

³⁵ One version of the Office suite—the one used in cloud-computing environments—is no longer allowed for use on rival cloud providers. And newer versions of the traditional Office product have similar limitations," *Microsoft Customers Decry Cloud Contracts That Sideline Rivals*, Bloomberg, available at:

https://www.bloomberg.com/news/articles/2022-04-12/microsoft-customers-decry-cloud-co ntracts-that-sideline-rivals#xj4y7vzkg (Apr. 11, 2022).

For Microsoft, this policy change accelerated the growth of Azure's infrastructure offering.³⁶ As the cloud computing industry continues to grow, Azure is growing at a faster pace than any of its competitors.³⁷ As Raj Bala of Gartner told the Economist in 2020, "Microsoft is taking its arsenal of Windows Server, a massive software installed base, and using it punitively against its competitors."³⁸ Azure has continued to grow despite offering little practical advantage to customers. As Gartner observed, "2021 was a relatively unremarkable year for Microsoft Azure as it relates to novel innovations..."³⁹

In 2021 and 2022, many customers were coming up to the end of their Microsoft contracts. The new licensing rules coerced customer migration to the Azure architecture, from competitors large and small alike, which accelerated growth for Azure. Indeed, according to Flexera's 2022 State of the Cloud Report, by 2022, Microsoft Azure usage met or exceeded that of cloud first-mover AWS for the first time.⁴⁰ These new rules also led some smaller cloud providers in Europe to bring confidential complaints to the European Commission, including France's OVHCloud, Italy's Aruba, several Danish cloud providers and CISPE.⁴¹

Even Microsoft was compelled to concede the problematic nature of its policy change. In Spring 2022, recognizing the impact on competing cloud providers and touting support for a "healthy competitive environment,"

³⁶ CloudZero, *55 Cloud Computing Statistics That Will Blow Your Mind* at 23; *see* F. Jenny, CISPE Deck, Slide 4. Indeed, the data show that Microsoft's growth has come at the expense of smaller cloud service providers. *Id*.

³⁷ CloudZero, 55 Cloud Computing Statistics That Will Blow Your Mind at 23.

³⁸ The Economist, *How Satya Nadella turned Microsoft around*, available at:

https://www.economist.com/briefing/2020/10/22/how-satya-nadella-turned-microsoft-aroun d (Oct. 22, 2020).

³⁹ Gartner Research, CIP Magic Quadrant (2022) at 10.

⁴⁰ Flexera, State of the Cloud Report (2022) at 8.

⁴¹ Foo Young Chee, Microsoft Faces New EU Antitrust Complaint on Cloud Computing Practices, Reuters, available at:

https://www.reuters.com/technology/microsoft-faces-new-eu-antitrust-complaint-cloud-co mputing-practices-2022-11-08/ (November 9, 2022). The complaint filed by OVH, Aruba, and Danish Cloud Providers has since been reportedly privately settled with Microsoft. However, the terms of any such settlement have not been publicly disclosed. Paul Kunert, *Euro cloud providers react to MS potentially cutting deal on antitrust*, The Register, available at: https://www.theregister.com/2023/03/30/microsoft_euro_complaints/ (Mar. 30, 2023).

Microsoft President Brad Smith acknowledged the validity of (at least some of) the concerns.⁴²

In August 2022, Microsoft offered a reprieve from the additional licensing requirements for certain EU-based cloud providers, but who would qualify, whether they would be required to agree to Microsoft Software Assurance Programs,⁴³ or other additional obligations remained unclear. Most of the changes were added ways for other companies to resell access to Azure architecture. In addition, 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 largest 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.

In addition, Microsoft used this opportunity to introduce yet another restriction: partners⁴⁴ will no longer be able to supply Microsoft software if the software will ultimately be deployed on infrastructure supplied by Listed Providers, preventing customers from choosing any infrastructure that is not Azure.⁴⁵ While these new restrictions do not take effect until 1 October 2025,

https://www.theregister.com/2022/05/18/microsoft

⁴² Dina Bass, *Microsoft Customers Decry Cloud Contracts That Sideline Rivals*, Bloomberg, available at:

https://www.bloomberg.com/news/articles/2022-04-12/microsoft-customers-decry-cloud-co ntracts-that-sideline-rivals#xj4y7vzkg (Apr. 11, 2022); *EU Policy Blog*, Microsoft responds to European Cloud Provider feedback with new programs and principles, *available at*: https://blogs.microsoft.com/eupolicy/

^{2022/05/18/}microsoft-responds-to-european-cloud-provider-feedback-with-new-programsand-principles/ (May 18, 2022); Paul Kunert, *Microsoft revises software licensing, cloud policies amid EU regulator scrutiny*, The Register, available at:

<u>_cloud_concessions/</u> (May 18, 2022).

⁴³ Software Assurance programs provide the opportunity for Microsoft to create and develop further direct links to customers, enabling greater data transfer to the company, and increasing the risk of the anticompetitive use of such data. See Microsoft, Software Assurance, available at: <u>https://www.microsoft.com/en-us/licensing/licensing-programs/software-assurance-default</u>. ⁴⁴ See SoftwareOne, Guide: Microsoft Cloud Partner Program, available at:

https://www.softwareone.com/en-ch/blog/articles/2023/06/19/guide-microsoft-cloud-partner -programm (June 20, 2023).

⁴⁵ See Foo Yun Chee, Amazon, Google slam Microsoft's cloud computing changes, Reuters, available at:

https://www.reuters.com/technology/amazon-google-slam-microsofts-cloud-computing-cha nges-2022-08-30/ (Aug. 30, 2022); Ananya Bhattacharya, *Microsoft's cloud computing changes stir up a storm*, Quartz, *available at*:

customers are already grappling with how to manage their ongoing and future digital transformation and cloud migration strategies, many of which were agreed to contractually prior to the 1 October 2022 licensing changes.⁴⁶ For example, customers adopting multi-cloud solutions, which combine offerings from multiple cloud service providers, including Listed Providers, could be forced to abandon the Listed Provider's cloud infrastructure services if they wish to use Microsoft applications for which they had already paid.

What had been an anticompetitive policy was now also anticompetitive and facially discriminatory. Or, as one customer member of the Coalition noted:

> These business practices have resulted in little to no competition.... As a result of the licensing restrictions, the Company was forced to choose between additional cost and poor user experiences on the one hand, or make the transition to Microsoft's Cloud, all at significantly more cost in the end. No ability to negotiate can overcome the licensing restrictions that hamper cloud provider choice by the Company.⁴⁷

Azure's growth in cloud computing would, meanwhile, accelerate.⁴⁸

Discriminatory Provider Licensing

Microsoft offers two types of license agreements directly to cloud service providers. Through the Cloud Solution Provider Program ("CSPP"), a provider can resell Microsoft cloud products. These products must be hosted on Microsoft's cloud servers (Azure), so the cloud service provider is forced to bring its customers (and its data) to Microsoft's servers. CSPP licensees risk

https://finance.yahoo.com/news/microsofts-cloud-computing-changes-stir-070300853.html (August 31, 2022); Kurt Mackie, Microsoft To Ease Cloud Services Options for Partners and Customers in October, Redmond Magazine, available at:

https://redmondmag.com/articles/2022/08/31/microsoft-cloud-services-options.aspx (Aug. 31, 2022).

⁴⁶ See SAMExpert, *Microsoft SPLA / CSP-Hosting / BYOL Changes and Updates*, available at: <u>https://samexpert.com/microsoft-spla-changes-and-updates/</u> (Apr. 2, 2023).

⁴⁷ Note that the Company asked to keep their comment anonymized out of concern that retaliatory measures will be taken against them for expressing discontent with these business practices.

⁴⁸ CloudZero, 55 Cloud Computing Statistics That Will Blow Your Mind at 23.

losing their customers, due to the absence of value-added services and the fact that Microsoft establishes direct relationships with their customers.

The other option is to enter into a Services Provider License Agreement ("SPLA"), whereby the cloud service providers can offer cloud solutions directly hosted on their servers that integrate Microsoft products. Instead of the customer supplying the license to operate the Microsoft software on the cloud, the cloud provider is the licensee. The SPLA is a commercial agreement between Microsoft and a partner (cloud service provider), which pays for a license for the use of a Microsoft product, which is then used on the partner's servers. There is a direct relationship between the cloud service provider (using Microsoft's software) and its customers.

As Microsoft increased the restriction on BYOL licenses and ensured that certain dominant products such as Windows Server were unavailable for BYOL, customers were increasingly required to repurchase licenses or access software under a SPLA or CSPP-unless, of course, they chose to move to Azure. Around the same time that Microsoft was ending BYOL for its customers, it was increasing the price of the SPLA—but not the CSPP. That is, Microsoft began to charge more to cloud providers who were in direct competition with Azure. The distinction was substantial. In January 2018 and again in January 2019, the company increased SPLA prices 10-15%, while leaving CSPP prices unchanged.⁴⁹ In addition, certain Listed Providers have experienced even more significant cost increases in recent years—more than 60% increases in costs as compared to previous SPLAs—which often leaves the Listed Provider with no choice but to pass the cost onto customers. These price increases by Microsoft reflect not only the company's market power in the licensed products, but also its effort to hamstring competing cloud providers and drive business to Azure without having to compete on the merits.

Moreover, the SPLA does not allow competing cloud providers to offer their customers the full Microsoft productivity suite (Office 365 or Microsoft 365) that Microsoft offers on Azure. Cloud service providers are therefore unable to offer the full Microsoft 365 experience, which is required by many businesses and organizations, despite paying a higher license fee. Because Office 365 and Microsoft 365 are not available on SPLA and because there are restrictions on the licenses, customers are not able to purchase or bring

⁴⁹ Digital Edge Ventures, Inc., *Microsoft SPLA Price Increases*, available at: <u>https://knowledge.digitaledge.net/newsletters/microsoft-spla-price-increases/</u> (Oct. 2017).

Microsoft's most popular and core products – which also happen to be central to the enterprise license – with them to a competing cloud.⁵⁰

Customers want access to the best set of software and the best cloud providers, but the terms of the SPLA are structured to drive their business to Azure. This discriminatory licensing program exacerbates the problems that Microsoft's restriction of BYOL created.

In Europe, meanwhile, CSPPs have blossomed:, Microsoft cited the fact that 75 companies had signed up for the program. The critical point, however, is that CSPPs are resellers of Azure. While purporting to support European cloud providers, Microsoft continued to implement a scheme to corral customers to the Azure infrastructure.

ii. Tying

As noted above, 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. To wit, Microsoft ties several software products to its Microsoft 365 cloud-based office product, the net result of which is vendor lock-in and a less secure cloud experience for users.⁵¹

 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. That means that unless they agree to use Microsoft's file hosting product and upload data to Microsoft's servers, cloud providers serving customers using the Microsoft Office suite of products cannot offer their customers default saving to another, better file

⁵⁰ Moreover, security updates of Microsoft Office licensed under the SPLA are limited compared to the security updates provided to those with CSPP licenses. *See* Microsoft, SPLA Program, available at: <u>https://www.microsoft.com/en-us/licensing/licensing-programs/spla-program</u>; *See* Microsoft, Cloud Storage Partner Program, available at:

https://learn.microsoft.com/en-us/microsoft-365/cloud-storage-partner-program/. Support for mobile devices, and other technical support are also more limited under SPLA than CSPP—despite the higher prices charged. *Id.*

⁵¹ Microsoft's tying of "Azure credits" with Microsoft 365 exacerbates its leveraging of its dominant Office product suite to drive customers to Azure. These credits can only be used to acquire Azure cloud services, and are not available when access to the Office product suite is purchased from a cloud service provider other than Microsoft.

hosting service or the ability to utilize the Autosave function. For example, if a customer wished to use DropBox or Box, they would still be required to pay for 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. As Defender is widely-regarded as an inferior cybersecurity tool to others products in the security market,⁵² Microsoft's decision to tie Defender with the Microsoft 365 Office suite has raised cybersecurity rankles.⁵³ As one commentator explained: "Microsoft . . . is looking to cash-in by offering to protect everyone from the vulnerabilities they introduce into the market".⁵⁴ The net result of this tying has been expanded adoption of Defender and foreclosed competition for far superior products. As one commentator noted, Microsoft is getting paid as the "the arsonist, the fire department, and the building inspector," despite providing inferior cybersecurity for its customers.⁵⁵
- Azure Active Directory and Intune, user identity, authentication, and device management: Microsoft does not provide sufficient Application Programming Interfaces ("APIs") needed to allow

⁵² Sergiu Gatlan, *Microsoft Defender Mistakenly Tagging URLs as Malicious*, Bleeping Computer, available at:

https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-mistakenly-taggingurls-as-malicious/ (Mar. 29, 2023).

⁵³ Anthony M. Freed, *Microsoft's Failure to Prioritize Security Puts Everyone at Risk*, Cybereason Blog, available at:

https://www.cybereason.com/blog/microsofts-failure-to-prioritize-security-puts-everyone-at-<u>risk</u> (Oct. 14, 2021); Ryan Kalember, *The Microsoft Paradox: Contributing to Cyber Threats and Monetizing the Cure*, Fortune, available at:

https://fortune.com/2021/12/06/microsoft-paradox-cybersecurity-solarwinds-exchange-nation al/ (Dec. 6, 2021).

⁵⁴ Anthony M. Freed, *Microsoft's Failure to Prioritize Security Puts Everyone at Risk*, Cybereason Blog, available at:

https://www.cybereason.com/blog/microsofts-failure-to-prioritize-security-puts-everyone-atrisk (Oct. 14, 2021).

⁵⁵ Ryan Kalember, *The Microsoft Paradox: Contributing to Cyber Threats and Monetizing the Cure*, Fortune, available at:

https://fortune.com/2021/12/06/microsoft-paradox-cybersecurity-solarwinds-exchange-nation al/ (Dec. 6, 2021).

interoperability between Microsoft products ActiveDirectory, Azure Active Directory, Intune and third-party identity and device management products. Microsoft has long tied its Active Directory and Azure Active Directory services to the license for its dominant offerings, including for Windows OS and Office productivity suite. This not only 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 Active Directory historically and now Azure Active Directory. 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 Active Directory or Azure Active Directory. As Microsoft has moved to Microsoft 365 enterprise agreements, customers are now required to use an Azure Active Directory identity – and for some licenses, Microsoft Intune endpoint management – to access Microsoft 365 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.⁵⁶ For example, if you want to leverage an Azure Active Directory identity - which as noted above is required if you use Microsoft 365 – to authenticate a Mac, it is difficult to do so using an alternative operating system to Windows and creates a significant disincentive for customers to use competing operating systems. Similarly, if you want to use a third-party identity solution, you will not have all of the APIs required for equivalent services on Windows and Azure Active Directory. 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

⁵⁶ See Microsoft, High level architecture for Windows 365, available at: <u>https://learn.microsoft.com/en-us/windows-365/enterprise/high-level-architecture</u> (Jun. 15, 2023) (high level overview of interdependence of products within the Windows 365 ecosystem, noting the default versus optional settings and services).

infrastructure, in particular, in hybrid and/or multi-cloud environments where Microsoft products run alongside other applications. As the U.K. Office of Communications ("Ofcom") found in its report on cloud ("Ofcom Report"), "Limitations to Interoperability are especially relevant in regard to Microsoft – limitations are not strictly imposed but stem from the difficulties of making the Microsoft stack work with a non-Azure cloud."⁵⁷

• Teams, communication and collaboration: nearly every Microsoft 365 subscription plan includes Teams by default. However, as outlined above, Microsoft does not price individual products within its ELAs. As a result, customers cannot either discern the price of Teams or avoid having it, even if they prefer another communication and collaboration product. Teams also limits integration capabilities with third party communication and collaboration solutions to the frustration of customers and despite the fact that other communication industry players ensure such functionality (*e.g.*, Slack, Zoom).⁵⁸ Specifically, while Microsoft allows third parties to develop APIs that enable third-party platform customers to increase their engagement with Teams, these offered solutions are one directional. APIs that would enable third party services to integrate natively within Teams are not similarly supported. As a result, Teams has grown to a dominant collaboration product, despite users uniformly rating Teams below its competitors in virtually every major category - including usability, reliability and functionality except price.⁵⁹ By leveraging its dominant desktop and

⁵⁷ Ofcom, Cloud Services Market Report, available at

https://www.ofcom.org.uk/consultations-and-statements/category-2/cloud-services-marketstudy (Oct. 2023).

⁵⁸ Slack, Slack Files EU Competition Complaint Against Microsoft (July 22, 2020). Hoping to head off an investigation by EU competition authorities based on this complaint, Microsoft recently announced that they would unbundle Teams from Office, effective October 1, 2023. See Javier Espinoza, Microsoft Agrees to Stop Bundling Teams with Office, Financial Times, available at: <u>https://www.ft.com/content/be838956-7038-4179-8a1c-851b83048d5d</u> (April 23, 2023). This remedy was met with skepticism from the communications collaboration sector and came too late for Slack, which sold to Salesforce soon after filing its complaint.

⁵⁹ Daniel Rubino, *Microsoft Teams gets trashed by Wirecutter, highlights lingering issues with consumer push*, Windows Central, *available at*:

<u>https://www.windowscentral.com/microsoft-teams-personal-use-needs-help</u> (March 9, 2021); Melanie Pinola, *The Best Team Messaging App Is Slack,* WireCutter (New York Times), *available*

productivity products to compel the adoption of Teams and limiting integration capabilities with competing products, Microsoft not only inhibits the ability of alternative communication and collaboration providers to effectively compete but also harms its own customers.⁶⁰ That harm is evident in Microsoft's February 2023 release of Teams Premium. The add-on license for separate purchase provides access to not only sets of advanced features but previously "free" features that "will move from Teams licenses to Teams Premium Licenses."⁶¹ The monetization of Teams via Teams Premium - an expenditure over and above existing licenses that already make Teams available to clients - demonstrates how Microsoft leverages its dominance in adjacent product markets to drive adoption, and then raises prices. Then, Microsoft monetizes the product at issue (here, Teams) only after customer adoption is sticky enough that paying for what used to be "free" is more appealing than the friction of switching providers.

In August 2023, Microsoft announced changes to Microsoft 365 and Office 365 to "unbundle Teams" in Europe "to address [...]concerns" raised by the European Commission's investigation stemming from Slack's 2020 formal complaint.⁶² Microsoft also stated that it would "enhance [its] existing resources on interoperability with Microsoft 365 and Office 365" as well as "create new mechanisms to enable third-party solutions to host Office web applications."⁶³ Despite the global nature of the anticompetitive practices that the proposed changes are ostensibly intended to address, not only are they limited in

at: <u>https://www.nytimes.com/wirecutter/reviews/best-team-messaging-app/#how-we-tested</u> (March 26, 2021).

⁶⁰ Jason Aten, *Microsoft is Trying to Force You to Use its Software Like it's 1998 all over again,* Inc., available at:

https://www.inc.com/jason-aten/microsoft-is-trying-to-force-you-to-use-its-software-like-its -1998-all-over-again.html (Jan. 4, 2022).

⁶¹ Nicole Herskowitz, *Microsoft Teams Premium: Cut costs and add AI-powered productivity*, Microsoft, available at:

https://www.microsoft.com/en-us/microsoft-365/blog/2023/02/01/microsoft-teams-premium -cut-costs-and-add-ai-powered-productivity/ (Feb 1, 2023).

 ⁶² Microsoft, New subscription structure for Microsoft 365 in Europe, available at: <u>https://www.microsoft.com/en-us/licensing/news/Microsoft365-Teams-EEA</u> (August 31, 2023).
⁶³ Id. application to a subset of EEA-based users, but also fall short of addressing underlying concerns. Specifically, the changes: 1) are available only to net new users, significantly limiting their practical utility and availability; 2) are offered at a paltry discount that falls short of a reasonable market value for Teams or comparable communications and collaboration products; and, 3) provide no accountability for the limited interoperability concessions Microsoft has offered.

Fundamentally, what these changes do is constitute an admission that a core element of its business model (*i.e.*, tying/bundling products to its broader, popular business suites) limits customer choice and competition both in the communication and collaboration space and in other markets in which Microsoft competes.

B. Anticompetitive Effects

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 the UK and globally are considering the use of cloud services for the security, flexibility, and other benefits they can deliver.

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.⁶⁴ 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

⁶⁴ Frederic Jenny, Cloud Infrastructure Services: An Analysis of Potentially Anti-Competitive Practices, available at: <u>35b77d_4490e58b3da3490590cf55d15f561e4b.pdf (usrfiles.com)</u> [CISPE English Report] (Oct. 2021).

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.

Meanwhile, Microsoft has benefitted handsomely from these practices, supporting the growth in several Microsoft products, including Azure, Defender, and Teams, even against products widely regarded as superior. Microsoft's share of the global cloud infrastructure services segment jumped in recent years,⁶⁵ including 30-40% share [IaaS and PaaS] in the UK in 2022 per Ofcom's report.⁶⁶

i. Increased Cost

As a result of the anticompetitive practices set out above, all of Microsoft's licensed products, which are integral to the workloads of many American 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."⁶⁷

A customer selecting a cloud service provider other than Microsoft faces higher costs for reasons unrelated to efficiency or competition on the merits. The licensing changes and discriminatory treatment of SPLA have led to increased prices—sometimes more than \$100 (~ \pm 82) million for a single customer⁶⁸—for Microsoft software customers that wished to use the cloud

⁶⁵ Synergy Research Group, Cloud Spending Growth Rate Slows But Q4 Still Up by 10 Billion from 2021, available at:

https://www.srgresearch.com/articles/cloud-spending-growth-rate-slows-but-q4-still-up-by-10-billion-from-2021-microsoft-gains-market-share (Feb. 6, 2023): Statista, Worldwide Market Share of Leading Cloud Infrastructure Service Providers, available at:

https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructur e-service-providers/ (Apr. 28, 2023).

⁶⁶ Ofcom, Cloud Services Market Study: Final Report, at p. 74, available at

https://www.ofcom.org.uk/ data/assets/pdf_file/0027/269127/Cloud-services-market-studyfinal-report.pdf (Oct. 5, 2023).

⁶⁷ Richard Waters, *Microsoft's Tactics to Win Cloud Battle Lead to New Antitrust Scrutiny*, Financial Times, available at:

https://www.ft.com/content/350e7fed-cd52-4a0a-9902-5f2d9ebc3fe7 (Apr. 12, 2022).

⁶⁸ The Economist, *How Satya Nadella turned Microsoft around*, available at:

https://www.economist.com/briefing/2020/10/22/how-satya-nadella-turned-microsoft-aroun d (Oct. 22, 2020).

services of the Listed Providers. Frederic Jenny estimates that Microsoft's licensing practices have cost customers choosing non-Microsoft cloud services over €1.5 (~ £1.296) billion in Europe.⁶⁹

There is no rational explanation or objective justification for why Microsoft engages such a complex license and price differentiation. The cost of supply is not affected. It is simply a means to make their competitors' offers less attractive.

Microsoft has made proposals in 2022 that it suggests resolves these concerns.⁷⁰ 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 and customers both in the UK and globally 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.

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

⁶⁹ Frederic Jenny, Unfair Software Licensing Practices: A quantification of costs for cloud customers, available at:

https://cispe.cloud/website_cispe/wp-content/uploads/2023/06/Quantification-of-Cost-of-U nfair-Software-Licensing_Prof-Jenny_June-2023_web.pdf) [CISPE English Report] (June 2023).

⁷⁰ Microsoft Blog, New Licensing Benefits Make Bringing Workloads and Licences to Partners' Clouds Easier, available at:

https://blogs.partner.microsoft.com/partner/new-licensing-benefits-make-bringing-workloads -and-licenses-to-partners-clouds-easier/ (Aug. 29, 2022).

expensive but explaining to you why it's cheaper because it includes things.⁷¹

The Ofcom Market Research Report found that Azure customers are less likely to pay the price quoted by Microsoft than Google and AWS customers.⁷² Among those that experienced a price increase when renewing their contract, the mean reported increase was around 20%.⁷³ Gartner's research confirms this: "Many Gartner clients report frustration with watching their Azure costs increase over time without knowing why."⁷⁴

Microsoft's customers recognize the harm of Microsoft's ties and increase on their budget spend. Some customers feel they are "paying Microsoft for dozens of features [they] don't use". One customer explained to Ofcom: "It's why you pay what you pay sometimes, because they will tell us there's thousands of features and like, yeah, I need about four of them." Others feel that they should not consider other cloud-based software, because Microsoft's programs have "no cost".⁷⁵

ii. Less Choice for the End-User

This is not just a question of price but also of customer choice. It is vital that the customer has the choice of which services and IT service providers to use so that they may achieve the best solution for their IT needs. Microsoft's practices inhibit that choice, weaken existing competition, and discourage potential competitors from innovating and entering the market.

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

⁷¹ Ofcom, Cloud Services Market Research - Summary of Findings at 58, available at: <u>https://www.ofcom.org.uk/___data/assets/pdf__file/0031/256459/context-consulting-cloud-ser_vices-market-research-summary-of-findings.pdf</u> (April 2023).

 ⁷² Ofcom, Cloud Services Market Research - Summary of Findings at 13, available at: https://www.ofcom.org.uk/___data/assets/pdf_file/0031/256459/context-consulting-cloud-ser
<u>vices-market-research-summary-of-findings.pdf</u> (April 2023).
⁷³ Id.

⁷⁴ Gartner Research, CIP Magic Quadrant (2022) at 10.

⁷⁵ Ofcom, Cloud Services Market Research - Summary of Findings at 59, available at: <u>https://www.ofcom.org.uk/___data/assets/pdf_file/0031/256459/context-consulting-cloud-ser</u> <u>vices-market-research-summary-of-findings.pdf</u> (April 2023).

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.⁷⁶

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.

Once again, recognizing a competition problem of its own creation, last summer Microsoft promised to remove the requirement for additional licenses to offer virtual desktop functions.⁷⁷ However, to date, the only changes we have

⁷⁶ Omdia, Monoculture and Market Share: The State of Communications and Collaboration Software in the US Government (Sept. 21, 2021) ("Bundling can also be used as an effective strategy in the procurement process because vendors that combine products—or throw in ancillary products for free—can be more difficult for rivals that have smaller subsets of products to compete against. While it may still be possible to compete effectively by offering an alternate bundle, those vendors with a firstcomer advantage can significantly lower their costs or effectively commoditize entire categories of software and further entrench legacy systems even if they offer new or additional services as free or discounted add-ons. This can hurt the customer.)

⁷⁷ Microsoft Blog, New Licensing Benefits Make Bringing Workloads and Licences to Partners' Clouds Easier, available at:

https://blogs.partner.microsoft.com/partner/new-licensing-benefits-make-bringing-workloads -and-licenses-to-partners-clouds-easier/ (Aug. 29, 2022).

seen have been to within the Azure Hybrid Benefit program⁷⁸ and these do not do anything to address competition concerns.⁷⁹

iii. Cybersecurity

One of the less discussed and increasingly concerning consequences of Microsoft's anticompetitive restrictive licensing and tying practices is that of increased cybersecurity risk. Prescient Comply LLC, a US-based cybersecurity and corporate investigations firm, recently released a report commissioned by the Coalition on the impact of restrictive software licensing practices on cybersecurity. While that report is included as an appendix to our comments, we would like to include a brief summary of the cybersecurity concerns raised by these software licensing practices.

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.⁸⁰

Microsoft has been implicated in a number of security related concerns in recent years, including on a few occasions a disturbing lack of transparency. These have included issues in connection with the Microsoft operating system, Microsoft software, and Microsoft's Azure cloud solutions.⁸¹

⁷⁸ Microsoft, Explore Azure Hybrid Benefit for Windows VMs, available at:

https://learn.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licens ing (Apr. 19, 2023).

⁷⁹ Simon Sharwood, *Microsoft makes Windows Server 2022 licenses a little less cynical,* The Register, available at:

https://www.theregister.com/2023/04/26/windows_server_license_changes/ (Apr. 26, 2023). ⁸⁰ Omdia, Monoculture and Market Share: The State of Communications and Collaboration Software in the US Government (Sept. 21, 2021); Dan Gouré, *DoD's Software Acquisition Strategy Could Result In Dangerous Security Vulnerabilities*, RealClearDefense, available at:

https://www.realcleardefense.com/articles/2023/03/22/dods_software_acquisition_strategy_ could_result_in_dangerous_security_vulnerabilities_888706.html (Mar. 22, 2023).

⁸¹ See, e.g., Ryan Kalember, The Microsoft Paradox: Contributing to Cyber Threats and Monetizing the Cure, Fortune, available

at: https://fortune.com/2021/12/06/microsoft-paradox-cybersecurity-solarwinds-exchange-nat

Commentators have raised this concern in a number of contexts. Generally, some have asked, "Far from a cybersecurity savior, is Microsoft effectively setting the house on fire and leaving organizations with the bill for putting it out?"⁸² More specifically others have noted the implications of the federal government's contracts with Microsoft, particularly those related to the military.⁸³ As senior researcher at IDC and former Director of US Defense Information at the Department of Defense Paul Strassman stated, "Finding a crack through which one could induce mayhem with only a few keystrokes would be worth a great deal of money, especially when supporting an act of terrorism."⁸⁴ This is especially true for any governmental entities, companies, and organizations that are a target of Chinese-based advanced persistent threats (APTs), as Microsoft shares their source code with the Chinese government⁸⁵ and has identified at least one zero-day attack on its own

at: <u>https://fortune.com/2021/12/06/microsoft-paradox-cybersecurity-solarwinds-exchange-nat</u> <u>ional/</u> (Dec. 6, 2021).

Cybersecurity Ecosystem is Critical for Network Security, C4ISRNews, available at:

ional/ (Dec. 6, 2021); Ionut Arghire, *Microsoft Azure Users Warned of Potential Shared Key Authorization Abuse*, Security Week, available at:

https://www.securityweek.com/microsoft-azure-users-warned-of-potential-shared-key-autho rization-abuse/ (April 11, 2023); Anthony M. Freed, *Microsoft's Failure to Prioritize Security Puts Everyone at Risk*, Cybereason Blog, available

at: <u>https://www.cybereason.com/blog/microsofts-failure-to-prioritize-security-puts-everyone-at-risk</u> (Oct. 14, 2021).

⁸² Ryan Kalember, *The Microsoft Paradox: Contributing to Cyber Threats and Monetizing the Cure*, Fortune, available

⁸³ Shaun Waterman, *Pentagon Hacking Fears Fueled by Microsoft's Monopoly on Military IT*, Newsweek, available at:

https://www.newsweek.com/pentagon-hacking-fears-raised-microsoft-military-software-it-a ntivirus-monopoly-cybersecurity-1794369 (May 16, 2023); John Zangardi, A Diverse

https://www.c4isrnet.com/opinion/2021/11/09/a-diverse-cybersecurity-ecosystem-is-critical-fo r-network-security/ (Nov. 9, 2021); Dan Gouré, DoD's Software Acquisition Strategy Could Result In Dangerous Security Vulnerabilities, RealClearDefense, available at:

https://www.realcleardefense.com/articles/2023/03/22/dods_software_acquisition_strategy_ could_result_in_dangerous_security_vulnerabilities_888706.html (Mar. 22, 2023).

⁸⁴ Paul Strassman, *The Pernicious Characteristics of Monocultures*, PBS, available at: <u>https://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/threat.html</u>

⁸⁵ Microsoft, China Information Technology Security Certification Center Source Code Review Lab Opened, available at:

https://news.microsoft.com/2003/09/26/china-information-technology-security-certificationcenter-source-code-review-lab-opened/ (September 26, 2003) ("Microsoft is the first commercial software company that provides the Chinese government with access to its source code.")

products (CVE-2021-42321⁸⁶) that was likely known by Chinese APTs before it was known by Microsoft.⁸⁷

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.⁸⁸

Further, the implications for cybersecurity and impact on the associated sector is not limited to Defender or even other security products currently tied to the Microsoft 365 suites (*e.g.* Active Directory, Azure Active Directory, Intune). Rather, this is a practice that is developing in real-time with the potential to include a growing number of security products. To that end, it is worth noting that Microsoft announced in July 2023 that it would be adding two Zero Trust products to its Entra suite of security products: Entra Internet Access to protect against malicious Internet traffic, and Entra Private Access to permit greater identity management.⁸⁹ Given the stated intent to integrate these products into the Microsoft 365 productivity suite⁹⁰ and above outlined practice of tying adjacent products to these licenses, there is a concern that this will be yet another product offering included in their productivity bundles. Doing so not only raises concerns about internet security with an expanded

⁸⁶ National Institute of Standards and Technology, *CVE-2021-42321: Microsoft Exchange Server Remote Code Execution Vulnerability*, available at:

https://nvd.nist.gov/vuln/detail/CVE-2021-42321 (August 29, 2022).

⁸⁷ Microsoft, *Digital Defense Report 2022*, available at:

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country <u>=us#page=40</u> (December 6, 2022) ("The vulnerabilities described below were first developed and deployed by China-based nation state actors in attacks, before being discovered and spread among other actors in the larger threat ecosystem.")

⁸⁸ Shaun Waterman, *Pentagon Hacking Fears Fueled by Microsoft's Monopoly on Military IT,* Newsweek, available at:

https://www.newsweek.com/pentagon-hacking-fears-raised-microsoft-military-software-it-a ntivirus-monopoly-cybersecurity-1794369 (May 16, 2023).

⁸⁹ Microsoft Blog, *Microsoft Entra expands into Security Service Edge and Azure AD becomes Microsoft Entra ID,* available at:

https://www.microsoft.com/en-us/security/blog/2023/07/11/microsoft-entra-expands-into-sec urity-service-edge-and-azure-ad-becomes-microsoft-entra-id/ (July 11, 2023).

single vendor attack surface, but would also further entrench Microsoft's dominant position to the detriment of both customers of and competition in network security services.

As the Atlantic asked in 2021, "Is Windows as good a product as it would be if it faced more robust competition? When Windows has major security flaws, for example, billions of customers and companies are impacted, because of its market share. If we're wondering whether crappy airline experiences are a competition problem, should the same question apply to crappy computer security?"⁹¹ 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.⁹²

C. Proposed Remedies

The Coalition is supportive of any action that is consistent with the *Principles for Fair Software Licensing Principles*. While we are generally supportive of the proposed remedies included in the software licensing practices section of the CMA's Issues Statement, we are continuing to receive input from members as to how these would be specifically applied to Microsoft's current licensing policies and practices. The Coalition intends to share these recommendations and positions with the CMA once it is finalized in the coming weeks.

3. Conclusion

While the cloud computing industry is expected to continue to grow at a fast clip, Microsoft's share has jumped in recent years and continues to outpace its rivals due to its ability to foreclose other rivals and boost its own market share via unfair and harmful practices⁹³ This conduct harms consumers and also the competition among cloud providers and other

⁹¹ Molly Wood, *The Invisible Tech Behemoth*, The Atlantic, available at:

https://www.theatlantic.com/ideas/archive/2021/07/microsofts-antitrust/619599/ (July 29, 2021).

⁹² John Zangardi, A Diverse Cybersecurity Ecosystem is Critical for Network Security, C4ISRNews, available at:

https://www.c4isrnet.com/opinion/2021/11/09/a-diverse-cybersecurity-ecosystem-is-critical-fo r-network-security/ (Nov. 9, 2021).

⁹³ CloudZero, 55 Cloud Computing Statistics That Will Blow Your Mind at 23.

participants in the technology stack. Once Microsoft locks its customers into the Azure/Office 365/Windows Server environment, Microsoft leverages its position to raise prices, with prices increasing on average about 20% and many customers not understanding why prices are increasing.⁹⁴

Microsoft is leveraging its monopoly power in software markets to distort and avoid the competitive process for its own gain. This is firmly within Microsoft's playbook and has served it well in the past, to the detriment of consumers. And the impact is happening now.

We urge the CMA to treat with urgency and attention this problematic matter and duly investigate it in the course of the MIR.

* * *

The CFSL appreciates the opportunity to engage further with the CMA inquiry team to address any questions that you may have, either about our comments, the impact of restrictive software licensing practices on cloud choice and adoption, or potential remedies to these practices. We stand ready to present to you, both as a collective Coalition and individual member meetings, and are happy to respond to any RFIs, as needed.

Respectfully submitted,

Ryan Triplette Executive Director Coalition for Fair Software Licensing

Attachment: Report Impact of Software Licensing Practices on Cybersecurity by Prescient Comply, LLC and commissioned by the Coalition for Fair Software Licensing (November 2023)

⁹⁴ Ofcom, Cloud Services Market Research - Summary of Findings at 58, available at: <u>https://www.ofcom.org.uk/______data/assets/pdf__file/0031/256459/context-consulting-cloud-ser______vices-market-research-summary-of-findings.pdf</u> (April 2023).



180 N Stetson Ave. • Ste. 2625 • Chicago, IL 60601
T: 312-667-0667 • E: info@prescient.com
W: www.prescient.com

Impact of Software Licensing Practices on Cybersecurity

Business practices and outsized vulnerabilities can lead to a "Cyber Tax" on small- and medium-sized businesses of up to 500%.

In collaboration with:



November 2023

NOTE ON AUTHORSHIP

Prescient Comply LLC ("Prescient"), a cybersecurity and corporate investigations firm headquartered in Chicago, IL, was tasked with preparing a cybersecurity industry analysis of the impact, if any, of restrictive software licensing practices on behalf of the **Coalition for Fair Software Licensing** ("CFSL").

This report, prepared in October and November 2023, represents research-backed analysis and industry expertise gained from our digital forensics, incident response, and cybersecurity experience.

Sources included public records, news media, social media, and other publicly available information. Studies published by subject matter experts were screened for potential bias or other relevant ownership information whenever possible. Prescient experts often testify regarding the quality of products and software from security providers mentioned throughout this report.

SUMMARY OF FINDINGS

The severity of a cyberattack can be determined by examining the vulnerability under exploit and the breadth of the vulnerable software's deployment. History has shown that many severe cyberattacks - SolarWinds, the Microsoft Exchange Server hacks, and others - were especially damaging due to uniform information technology ("IT") architecture that spread vulnerable software across an entire business, industry, or government agency. This uniformity creates systemic risk in the form of a single attack surface and single point of failure in which attackers replicate the same attack within or across organizations.

Restrictive licensing is one of the most common ways technology vendors create uniform IT environments that span businesses, industries, and governments. They do so for good reason – it's great for their business, but not necessarily best for customers' overall security. Market-leading vendors like Microsoft may erect barriers to interoperability and / or implement other restrictions to limit choice.¹

Our research and experience find that there is a connection between restrictive licensing and cybersecurity risk and cost. This "cyber tax" manifests itself in the form of incident costs, legal and regulatory expenses, additional security spend due to tiered pricing structures, added insurance costs, and security consultation, which come because of reliance on legacy software vendors, like Microsoft. According to a recent study by NetDiligence, when an incident occurs, small to medium-sized enterprises ("SMEs") spent on average an additional \$103,000 on crisis services, \$156,000 on legal and regulatory expenses, and \$175,000 on incident costs.² For governments, the cyber tax also extracts an opportunity cost, as often limited resources are pulled away from public services.

We examined this "cyber tax" being levied on SMEs, which are the bedrock of the United States' economy and often rely on Microsoft Office 365 and other legacy software.³ Our research found that SMEs who largely use Office 365 and Azure can end up paying a "tax" of up to \$434,000 per incident - nearly 5x (498%) the cost of their annual spend on Office 365 and Azure (\$87,120

¹ Dina Bass, Microsoft Customers Decry Cloud Contracts That Sideline Rivals, *Bloomberg*, available at: <u>https://www.bloomberg.com/news/articles/2022-04-12/microsoft-customers-decry-cloud-contracts-that-sideline-rivals#xj4y7vzkg</u> (Apr. 11, 2022).

² NetDiligence, *Cyber Claims Study: 2023 Report*, available at: <u>https://netdiligence.com/cyber-claims-study-2023-report/</u>.

³ For the purposes of this report, we define SMEs as independent businesses with approximately 50-500 employees with less than \$500 million in annual revenue.

annually on average).^{4 5} Combined with outsized vulnerabilities associated with Microsoft products and the restrictive licensing practices mentioned above, this "tax" is only likely to increase over time.

Ransomware and business email compromise ("BEC") were the two leading causes of cyberattacks, accounting for 46% of insurance claims and 72% of total incident cost during the five-year period between 2018 and 2022.⁶ Research suggests that Microsoft "leads the pack" with most vulnerabilities associated with ransomware.⁷ In fact, studies indicate that Office 365 users were more than twice as likely to experience a claim compared to Google Workspace users. Furthermore, on-premises Microsoft Exchange users were nearly three times more likely to experience a claim compared to businesses using Google Workspace.⁸ Other studies underscore the disproportionately high vulnerability of Microsoft products, even when adjusted against their relatively smaller competitors: one study identified Microsoft as the vendor with the largest number of zero-day vulnerabilities,⁹ while another concluded that nearly 30% of the known exploited vulnerabilities are attributable to Microsoft—more than the next five providers combined.¹⁰

These findings closely mirror our own experience. Prescient's team has conducted numerous ransomware, business email compromise, and other topically relevant cybersecurity investigations for clients, large, small, and in between. We provide digital forensics and incident response services, virtual Chief Information Security Office (CISO) consultation, cybersecurity audits and risk assessments, and other related services.

Prescient has observed that most of the cybersecurity incidents we encounter involve Microsoftrelated technologies.

⁴ Average annual Office 365 and related product spend calculated after extensive consultation with one of the United States' largely and fastest-growing IT managed service providers.

⁵ For the purposes of this study, we focused on SMEs, though it is certainly possible that a similar "tax" exists for larger enterprises and government agencies with wider attack surfaces and who hold more sensitive data.

⁶NetDiligence, *Cyber Claims Study: 2023 Report*, available at: <u>https://netdiligence.com/cyber-claims-study-2023-report/</u>.

⁷ Invanti, *Ransomware Research Reveals 12 Vulnerabilities Have Become Newly Associated with Ransomware in Q1 2023*, available at: <u>https://www.ivanti.com/company/press-releases/2023/ransomware-research-reveals-12-vulnerabilities-have-become-newly-associated-with-ransomware-in-q1-2023</u> (May 18, 2023).

⁸ Coalition, 2023 Cyber Claims Report: Mid-Year Update, available at: <u>https://info.coalitioninc.com/rs/566-KWJ-784/images/Coalition_2023-Claims-Mid-Year-Update.pdf</u>.

⁹ ZeroDay.CZ Tracking Project, Zero Day Vulnerability Statistics, available at: <u>https://www.zero-day.cz/research/</u>.

¹⁰ Cybersecurity & Infrastructure Security Agency, *Known Vulnerabilities Catalog*, available at: <u>https://www.cisa.gov/known-exploited-vulnerabilities-catalog</u>.

Contents

Our research is structured as follows:

Part I provides a glimpse into the changing cybersecurity landscape, why these changes increase risk from breaches and other cybersecurity incidents, and why the current cybersecurity market dynamic leads to increased costs for customers.

Part II details our experience with one common element of cyber tax: tiered pricing of cybersecurity products, its risks and ultimate costs imposed on customers.

Part III discusses additional restrictive licensing practices and provides examples of their costs to customers.

While international terrorism dominated the rankings of national threats for a full decade after 9/11, by 2013, cybersecurity firmly took the number one spot among a ranking of global threats and has been the focus among non-nation-state-specific threats ever since.

From the moment cybersecurity became a buzzword, the only constant in this wide-ranging field has been its ever-changing nature. Some of the trends and challenges of recent years were predictable, such as the increased use and dependence on technologies. Some new challenges perhaps less so, such as business practices that would evolve around those technologies. Nevertheless, the rate of change is rapidly accelerating, putting pressure on the leaders in both the public and private sectors to scrutinize their current software, infrastructure, and cybersecurity assets and procedures.¹¹

The increased cybersecurity challenges are the price for the economic benefits and convenience of being online. Unfortunately, the real costs of falling behind these rapid changes are also increasing. Multiple reports suggest that damages from ransomware, the fastest growing type of cybercrime, are increasing every year.¹² ¹³ In addition to ransomware payments, victims suffer losses because of downtime, reputational damage, legal costs, and further investments in new security solutions.¹⁴ Moreover, the increasing dependency on interconnected networks leads to additional, hidden costs that reach far beyond the primary victim of the attack.

Cyber Incidents on the Rise

The ongoing and measurable consequence of the rapidly changing cybersecurity landscape is the increase of breaches and other cybersecurity incidents.

Although specific figures tend to vary due to measurement methods and the impossibility of comprehensive coverage, outlets tend to agree on one fact: throughout the last two decades, the

¹¹ Jim Boehm, Charlie Lewis, Kathleen Li, Daniel Wallance, and Dennis Dias, *Cybersecurity Trends: Looking Over the Horizon*, McKinsey & Company, available at: <u>https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/trends-looking-over-the-horizon</u> (Mar. 10, 2022).

¹² Steve Morgan, *Global Ransomware Damage Costs Predicted to Exceed \$256 Billion by 2031*, Cybercrime Magazine, available at: <u>https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/</u> (Jul. 7, 2023).

¹³ Blackfog, *Beyond the Ransom: The True Cost of Ransomware Attacks*, available at: <u>https://www.blackfog.com/the-true-cost-of-ransomware-attacks/</u>. 14 *Id*.

number of data breaches has regularly increased exponentially.¹⁵ Statista reports a 500% increase in the decade leading to 2014,¹⁶ while Forbes observed that the same decade had seen over 300 data breaches involving the theft of 100,000 or more records.¹⁷ Even so, multiple sources report nine of the ten biggest breaches in history occurring after 2014.¹⁸

In the simplest of senses, a global increase in data breaches can be correlated with an increase in the amount of data organizations and consumers store, generally. One figure estimates that global data production in 2020 was 44 times greater than it was in 2009.²⁰

More recently, studies point to an increasing complexity and sophistication of ransomware attacks specifically. Cybersecurity firm Sophos conducts an annual, vendor-agnostic survey of thousands of IT professionals in mid-sized organizations. Their 2022 report revealed "an ever more challenging attack environment," finding that the complexity and sophistication of ransomware attacks had increased, and that the proportion of organizations directly impacted by ransomware had nearly doubled over the prior twelve months.²¹ The firm's 2023 report found that ransomware had affected the same proportion of respondents, 66%, but noted that adversaries were more able to "consistently execute attacks at scale."²² In early 2022, the U.S. Cybersecurity & Infrastructure Security Agency ("CISA") likewise issued a Cybersecurity Advisory regarding the increased globalized threat of ransomware.²³

Likewise, more data means an increase in software and its complexity, which in turn becomes that much more subject to vulnerabilities that go unnoticed by developers prior to public release. A study by Mandiant analyzing 200 zero-day vulnerabilities between 2012 to 2021 found that these exploits are expected to continue to grow from year to year, partially because of "the continued move toward cloud hosting, mobile, and Internet-of-Things technologies [that] increases the

16 Statista, Cyber crime: Number of compromises and impacted individuals 2005-2022, available at:

17 Niall McCarthy, *Chart: The Biggest Data Breaches in US* History, Forbes, available at: <u>https://www.forbes.com/sites/niallmccarthy/2014/08/26/chart-the-biggest-data-breaches-in-u-s-history/?sh=4004981d7735</u> (Aug. 29, 2014).

21 Sophos, State of Ransomware 2022, available at:

¹⁵ Juliana De Groot, *The History of Data Bridges*, DataInsider (Digital Guardian Blog), available at: <u>https://www.digitalguardian.com/blog/history-data-breaches</u> (Aug. 22, 2022).

https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (Aug. 29, 2023).

¹⁸ Abi Tyas Tunggal, *The 72 Biggest Data Breaches of All* Time, Upguard Blog, available at: <u>https://www.upguard.com/blog/biggest-data-breaches</u> (Aug. 3, 2023).

¹⁹ Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st* Century, CSO Online, available at: <u>https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html</u> (Nov. 8, 2022). 20 De Groot *supra* note 15.

https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf. 22 Sophos, State of Ransomware 2023, available at:

https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf. 23 Cybersecurity & Infrastructure Security Agency, 2021 Trends Show Increased Globalized Threat of

Ransomware, available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a (Feb. 10, 2022).

volume and complexity of systems and devices connected to the internet—put simply, more software leads to more software flaws."²⁴

A Data Breach Chronology Database from the nonprofit Privacy Rights Clearinghouse includes information on more than 20,000 data breaches dated between 2005 and February 2022.²⁵

Breaches can be sorted by the number of reported records impacted; firms such as Epsilon and Marriot / Starwood, for example, have suffered breaches affecting over 200 million customers.

"Customers are often at the mercy of service providers to inform them of vulnerabilities in the service providers' software or platform."

However, such breach statistics which are regularly limited to the U.S.,

and which most often focus only on the entities affected and the magnitude or sensitivity of their breached records—belie the fact that breaches regularly occur due to the involvement of an organization's vendors, partners, and other service providers, particularly those which interface with IT functions such as data storage. Indeed, the 2022 CISA advisory observes a recent increase in "malicious cyber activity targeting managed service providers."²⁶

Based upon research on vulnerabilities between 2006 and 2016, Cybersecurity Help ("CH") reported Microsoft as the vendor with the largest number of zero-day vulnerabilities, 46% of those reported. (The second-closest vendor was Adobe, with 18.26%).²⁷ Similarly, data from 2020 through 2023 reveal Microsoft as the vendor with the most vulnerabilities (25.63%), followed by Apple Inc (18.49%), and then Google (16.81%).²⁸ Vendor software can be further subcategorized; for instance, Microsoft Windows represents 68.85% of the vendor's 2020-2023 vulnerabilities, followed by Microsoft Exchange Server (11.48%), and so on.

Other databases compiling vulnerabilities confirm the findings from CH's database. Since 2021, CISA has reported more than 930 known vulnerabilities, with nearly 30% of which are attributable to Microsoft—more than the next five providers combined.²⁹

25 Privacy Rights Clearinghouse, Data Breach Chronology, available at: <u>https://privacyrights.org/data-breaches</u>. 26 Cybersecurity & Infrastructure Security Agency, *Protecting Against Cyber Threats to Managed Service*

²⁴ James Sadowski, Zero Tolerance: More Zero-Days Exploited in 2021 than Ever Before, Mandiant Blog, available at: <u>https://www.mandiant.com/resources/blog/zero-days-exploited-2021</u> (Aug. 10, 2023).

Providers and Their Customers, available at: <u>https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a</u> (May 11, 2022).

²⁷ Zero-Day.CZ Tracking Project supra note 10.

²⁸ Id.

²⁹ Cybersecurity & Infrastructure Security Agency supra note 10.

This disproportionate share of vulnerabilities might be most readily attributed to a similar disproportionate market share. Indeed, according to aggregate data collection firm StatCounter Global Stats, Windows accounts for 69.51% of the desktop operating system market share worldwide. The second-highest market share belongs to Mac OS X, with 20.43%.³⁰ As such, it is reasonable to assume that unknown software vulnerabilities and related breaches will affect Microsoft and other software market leaders at comparably proportionate rates.

However, certain sources draw attention to disproportionately high instances of ransomware, malware, and other breach incidents for market leaders even when adjusted relatively against their smaller competitors. According to Datto's 2020 Global State of the Channel Ransomware Report, for instance, 91% of Windows desktops, 76% of Windows servers, and 8% of Windows tablets were reported by 1,000+ managed service providers as targets of ransomware attacks. The desktop and server numbers were significantly higher than the 7% infection rate reported for MacOS X.³¹ Similarly, a study by Mandiant analyzing zero-days from a dozen software vendors in 2021 found that 75% of those reported were attributed to products from only three providers: Microsoft, Google, and Apple (the study was conducted prior to Mandiant's subsequent acquisition by Google).^{32 33}

The Cybersecurity Market is Evolving, But Not Fast Enough

Of course, the cybersecurity market is evolving as well. Indeed, in the first quarter of 2023, spending on cybersecurity increased by 12.5% compared to the same period a year earlier, outpacing the rest of the tech sector.³⁴ However, the increase in breaches and other cybersecurity incidents suggests that cybercriminals are outpacing and outmaneuvering their pursuers.

A closer look at the players in the field indicates that some of this growth has not necessarily led to innovation or effective solutions to the emerging challenges. The largest cybersecurity player in the market, Microsoft, grew its security-focused business by approximately 33% in 2022, generating approximately \$20 billion.³⁵ However, some of Microsoft's business practices that

³⁰ StatCounter, Desltop Operating System Market Share Worldwide, available at: <u>https://gs.statcounter.com/os-market-share/desktop/worldwide</u>.

³¹ Datto, Datto's Global State of the Channel Ransomware Report, available at: <u>https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf</u>.

³² Sadowski supra note 24.

³³ Thomas Kurian, *Google + Mandiant: Transforming Security Operations and Incident* Response, available at: <u>https://cloud.google.com/blog/products/identity-security/google-completes-acquisition-of-mandiant</u> (Sept. 12, 2022).

³⁴ Stephen Weigand, *Cybersecurity market grew 12.5% in first quarter, outpacing overall tech* market, SC Media, available at: <u>https://www.scmagazine.com/news/cybersecurity-market-grew-12-5-in-first-quarter-outpacing-overall-tech-market</u> (June 20, 2023).

³⁵ Sam Boughedda, *Microsoft the largest cybersecurity player in the market – CFRA* Research, Investing, available at: <u>https://www.investing.com/news/stock-market-news/microsoft-the-largest-cybersecurity-player-in-the-market-cfra-research-432SI-3080399</u> (May 11, 2023).

contributed to this growth and position in the market have been criticized as anti-competitive and stifling innovation. For example, Microsoft's vendor lock-in and bundling of products has been a thorn in the eye of some of its competitors and the subject of legal battles for more than a decade.³⁶ ^{37 38} Of course, using a single vendor can have benefits, including better integration of single-vendor solutions.³⁹ However, single vendor lock-in presents significant risks to customers when the vendor is in the position of assessing and reporting the vulnerabilities in its own software and operating system. This creates a conflict of interest and misaligned incentives for the vendor; and, ultimately increasing cybersecurity risk borne by the customer. In addition, restricting interoperability and services to those allowed only by the service provider may ultimately prevent the agility necessary to tackle the everchanging cybersecurity challenges.

Another trend that is prevalent today and directly affects the customers has emerged with the advent of hybrid and cloud-based IT infrastructure. Providers of hybrid and cloud-based services began to offer tailored services and features to consumers. This pricing strategy is commonly referred to as **tiered pricing**. Tiered pricing allows providers to sell their products or services at different price points by restricting or expanding certain features of their products. This allows consumers to select the services they want at a price they can afford. However, this tiered pricing may lead to hidden vulnerabilities, leave the customers with inadequate protection, and ultimately lead to greater direct and indirect damages and costs.

³⁶ Matt Ashare, *Cloud tensions flare as Google accuses Microsoft of vendor lock-in*, CIO Dive, available at: <u>https://www.ciodive.com/news/Google-battles-Microsoft-cloud-SaaS-Federal-Trade-Commission/653816/</u> (June 26, 2023).

³⁷ Melanie Chernoff, *The European Commission Stands Against Vendor Lock*-In, OpenSource Blog, available at: https://opensource.com/government/09/12/european-commission-stands-against-vendor-lock (Dec. 23, 2009). 38 Kyle Rankin, *Vendor Lock-In: Now in the* Cloud, Linux Journal, available at: https://www.linuxjournal.com/content/vendor-lock (Dec. 23, 2009).

³⁹ Peter Zaitsev, *Understanding the Potential Impact of Vendor-Lock on Your* Business, Forbes, available at: https://www.forbes.com/sites/forbestechcouncil/2021/03/30/understanding-the-potential-impact-of-vendor-lock-inon-your-business/?sh=5956cb0d5455 (Mar.30, 2021).

Tiered offerings are typically sold as prepackaged software bundles and often include different levels of security features, with more enhanced security features at the higher priced tiers. Unfortunately, the lower-level tiers are significantly more susceptible to data breaches and/or incident response hindrances due to cybersecurity gaps and limited response features. During a cyber-attack, some customers may feel the need to remain with their current software vendor but upgrade into a higher tier with more security features. With the lion's share of this industry's market, we will use Microsoft's tiered pricing strategy for this discussion. It is important to note, however, that most hybrid and cloud-based IT providers also offer tiered pricing models, though key differences exist between each.

Cybersecurity Gaps

Limiting cybersecurity options to tiered pricing models contribute to greater occurrence of cybersecurity gaps that expose businesses to risk and potential exploitation. Naturally, companies are primarily focused on generating revenue and reducing costs. Because of this, customers may be more inclined to choose a lower tier that includes fewer and more basic security features. Although most tiers provide standard security features (e.g., email filtering, password policies, multifactor authentication, etc.), advanced cybersecurity features (e.g., endpoint security, data loss prevention, auditing, etc.) are often only available in the higher tiered packages. Customers who either 1) choose a lower tier, or 2) have security needs that fall in between two tiers and opt for a lower tier will find themselves under-protected from cybersecurity risk and subsequently vulnerable to risk and exploitation. Unfortunately, many customers do not realize the extent to which they are under-protected until a cybersecurity incident occurs.

This tiered pricing strategy is akin to a scenario in which an individual purchases a vehicle with brakes and a seatbelt but learns they need to pay an additional cost for items such as anti-lock brakes and airbags. Allowing a customer to choose between different safety devices rather than standardizing features across all vehicles could have detrimental effects as the absence of anti-lock brakes and airbags during an accident could impact whether passengers survive a collision. United States Senator Ron Wyden of Oregon used the same car analogy when he criticized Microsoft in a *Wall Street Journal* ("WSJ") article.⁴⁰ Specifically, Senator Wyden noted that customers who had not purchased Microsoft's premium tiered service were unable to detect a state sponsor attack.

⁴⁰ Robert McMillan and Dustin Volz, *China Hacking Was Undetectable for Some Who Had Less Expensive Microsoft Services*, Wall Street Journal, available at: <u>https://www.wsj.com/articles/china-hacking-was-undetectable-for-some-who-had-less-expensive-microsoft-services-58730629</u> (July 13, 2023).

"Service providers foster insecure environments when they fail to provide critical cybersecurity features across all tiers or allow customers to opt out of cybersecurity features." Senator Wyden stated that "Offering insecure products and then charging people for premium features necessary to not get hacked is like selling a car and then charging extra for seatbelts and airbags."⁴¹ The WSJ article also quoted an anonymous Senior CISA official who advocated for standardizing cybersecurity features across product

offerings: "Every organization using a technology service like Microsoft 365 should have access to logging and other security data out of the box to reasonably detect malicious cyber activity."⁴² Indeed, under the leadership of Jen Easterly, CISA has been pushing for making software secure-by-design and putting the liability on the vendors to sell better products:^{43 44}

"Technology providers and software developers must take ownership of their customers' security outcomes rather than treating each product as if it carries an implicit caveat emptor. To achieve this, every technology provider must begin by creating products that are both 'secure by default' and 'secure by design."⁴⁵

Service providers using tiered packaging strategies foster insecure environments when they fail to provide critical cybersecurity features across all tiers or allow customers to opt out of essential cybersecurity features via purchase of a lower tier package.

In addition to tiered security features, legacy software providers often present customers with a complex array of choices that can be difficult for customers to understand and make informed decisions to select the right tier to protect their business. As such, customers often need to spend a considerable amount of time researching the different features in each tiered package and mapping these offerings to fit their cybersecurity needs. For example, Microsoft has several 365 offerings for business customers. There are basic, standard, and premium, as well as apps for business tiers. For enterprise-level customers, there are enterprise levels 1, 3, and 5, as well as apps for enterprise tiers. In addition, there are frontline workforce (e.g., M365 F1 and F3), government (e.g., O365 G3, O365 G5, M365 G3, and M365), and nonprofit (basic, standard, and premium) tiers.

43 CISA Director Jen Easterly and Executive Assistant Director Eric Goldstein, *Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products*, Foreign Affairs, available at: https://www.cisa.gov/sites/default/files/2023-04/foreign-affairs_stop-passing-buck-on-cybersecurity_508.pdf and https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity (Feb. 1, 2023).

45 Easterly and Goldstein supra note 45.

⁴¹ *Id*.

⁴² Id.

⁴⁴ Jessica Lyons Hardcastle, US Cybersecurity Chief: Software makers shouldn't lawyer their way out of security responsibilities, The Register, available at: <u>https://www.theregister.com/2023/02/28/cisa_easterly_secure_software/</u> (Feb. 28, 2023).

Reviewing the different tiers and features can be a daunting task. This is especially true for novice or non-cybersecurity personnel (i.e., CEOs, CFOs, procurement officers, etc.) who are tasked with tier selection on behalf of their organization.

These tiers can be confusing to understand and often provide ambiguous information about their security features. The wrong selection could have catastrophic results, affecting the confidentiality, integrity, and/or availability (commonly referred to as the CIA Triad by information security professionals) of the customer's data. Customers who select a tier that does not meet their cybersecurity needs may learn they do not have the capabilities within their tier to address a cybersecurity incident and are forced to upgrade to a more expensive tier or find another solution to address the issue. Moreover, alternative solutions may be limited or restricted to only services or vendors approved by the service provider, thus limiting the customer's options and reducing competitive opportunities for outside, or non-approved, vendors to address security flaws.

Lastly, some of the cybersecurity features offered in tiered packages require setup, configuration, and training. Many features are not "plug and play" nor are they turned on by default. Expert assistance (either internally or externally) may be required to implement these security features or controls. Customers who lack the knowledge or personnel to configure these features often need to purchase additional services from the service provider or authorized partner. In addition, these support packages are often presented in the form of tiered pricing levels.

"Alternative solutions may be limited or restricted to only services or vendors approved by the service provider, thus limiting the customer's options and reducing competitive opportunities for outside, or non-approved, vendors to address security flaws."

Data Breaches, Incident Response, & Hindrances

Tiered pricing models can contribute to hybrid and cloud-based breaches because customers cannot pick and choose which security and auditing features they need. Security features are often sold in prepackaged tiers and do not allow customers to select features from higher tier packages or tiers that do not include upgrading.

One such feature is Microsoft's "Impossible Travel." Impossible travel is an anomaly detection tool used to identify account compromises. It detects when a user connects from two different countries (e.g., New York and Montenegro) and determines if the time between connections (e.g., 1:00 PM EST and 9:00 PM CET) is possible. If the time between those connections cannot be

made through conventional air travel, the account is flagged as "impossible travel". This would be an important and helpful feature to be included in all tiers. However, if a customer has a Microsoft Business Standard license, they will need to upgrade to a higher tier product (e.g., Microsoft 365 Business Premium, Microsoft 365 Enterprise 5, Azure, etc.) that includes Impossible Travel. As a result of a forced upgrade, the customer further binds or ties their IT security to Microsoft and possibly extends their licensing period. It is worth mentioning that Prescient has observed that a large percentage of its business email compromise (BEC) clients, including those that were breached using Microsoft's MFA, upgraded their license immediately after the incident to a package that includes Impossible Travel. Consequently, if these clients had Impossible Travel embedded in the lower tier or if they had the ability to add it at the time of purchase, many of the BECs may not have occurred.

A second feature often overlooked by tiered customers is logfile retention. Most of Prescient's Microsoft breach clients were unaware that their logs were retained for 90 days for lower tier users (i.e., non-E5 users and/or guest users).⁴⁶ According to an IBM report, it may take approximately 197 days to discover a breach. As such, 90-day retention period was grossly inadequate to assist victims of data breaches.⁴⁷ Facing pressure from policymakers, customers, and industry, Microsoft recently announced changes to their audit log retention policies to extend the retention period from 90 to 180 days for audit logs generated after October 17, 2023.⁴⁸ However, as the extension falls short of the average time to discover a breach, it is unclear how much this extension will help. Tiered customers who identify a breach after the logs have been purged find themselves in a guessing game as to how long the threat actors were in their system and what data was accessed or exfiltrated. This is a nightmare scenario for companies that fall under breach reporting guidelines as they often need to spend considerable amounts of money and resources to answer these two questions for regulators and their customers. These victims will often upgrade to a higher tier during a data breach in the hopes that they can recover the missing or purged logs. It is important to note that this log retention tier issue applies to other vendors and not just Microsoft.

Data loss prevention ("DLP") is a third feature that is not often available at lower tiers offered by hybrid and cloud-based service providers. DLP features are tools used to 1) detect potential data breaches and data exfiltration, and 2) prevent sensitive data loss. These are typically available to customers who select higher tier options. DLP features can help customers monitor which users are accessing and transmitting sensitive information in an organization. They are also designed to prevent access to sensitive data while in use, in transit, or at rest. Deploying tools of this nature could help reduce the number of data breaches in the United States. Unfortunately, service providers require their customers to pay an additional cost for these features.

⁴⁶ Microsoft, *Manage audit log retention* policies, available at: <u>https://learn.microsoft.com/en-us/purview/audit-log-retention-policies</u> (Oct. 24, 2023).

⁴⁷ IBM, Cost of Data Breach Report 2023, available at: <u>https://www.ibm.com/reports/data-breach</u>.

⁴⁸ Microsoft *supra* note 46.

PART III RESTRICTIVE LICENSING PRACTICES & HIDDEN COSTS

The restrictive licensing practices of legacy vendors often lead to locking customers into their uniform ecosystem. While a uniform or identical IT architecture allows service providers to efficiently manage and maintain their clients' cloud-based infrastructure, it also provides a roadmap or single attack vector for hackers to exploit all of the service provider's customers en masse each time a vulnerability is discovered. Additionally, it puts the service provider in a position of assessing and reporting the vulnerabilities in its own software and operating system rather than relying on a third-party vendor to provide objective feedback. Of note, this threat is amplified exponentially when segments considered critical infrastructure (e.g., healthcare, transportation and logistics, energy, defense, and financial services) rely on a limited number of cloud service providers. This was demonstrated in a recent attack on U.S. government agencies by nation-state actors.

In July 2023, the email accounts of several U.S. government agencies were breached by a hacker group affiliated with the Chinese government, stealing 60,000 emails.⁴⁹ The Chinese hacker group, Storm-0558, was able to exploit Microsoft's "GetAccessTokenForResourceAPI", which allowed the group to forge signed access tokens, impersonate customer accounts, and gain access to 25 organizations and government agencies.^{50 51} The threat actors discovered this security flaw after successfully compromising a Microsoft engineer's corporate account.⁵² Once the flaw was discovered, the threat actors were able to compromise several U.S. government agencies that used Microsoft's Exchange Online and Azure Active Directory services. As demonstrated in this example, the government's reliance on a single vendor created a weakness and a single point of failure that diminished the government's cyber-resiliency against a cyber-attack.

"Uniform IT architecture also provides a roadmap or single attack vector for hackers to exploit all of the service provider's customers en masse each time a vulnerability is discovered."

⁴⁹ Karoun Demirjian, *Chinese Hackers Stole 60,000 State Department Emails in Breach Reported in July*, New York Times, available at: <u>https://www.nytimes.com/2023/09/27/us/politics/chinese-hackers-state-department.html</u> 50 Sergiu Gatlan, *Stolen Microsoft key offered widespread access to Microsoft cloud* services, Bleeping Computer, available at: <u>https://www.bleepingcomputer.com/news/security/stolen-microsoft-key-offered-widespread-access-to-microsoft-cloud-services/</u> (July 21, 2023).

⁵¹ Demirjian supra note 50.

⁵² Phil Muncaster, *Microsoft Breach Exposed 60,000 State Department Emails*, InfoSecurity Magazine, available at: <u>https://www.infosecurity-magazine.com/news/microsoft-breach-60000-state</u> (Sept. 29, 2023).

Limited Integration Capabilities

In our experience, legacy software providers often prohibit integration of "non-authorized" external security solutions (presumably those offered by competing service providers) into their platforms. This restriction is in direct opposition to the "defense in depth" strategy, which is a best

"The closed software environment forces the customer to use the service providers' tools that are often hard to interpret, produce false positives, and do not work as well as some industry standard tools." practice in cybersecurity. Defense in depth is a multi-layered approach to cybersecurity that incorporates different defense mechanisms at varying layers to protect systems and the data contained therein. These different defense mechanisms increase the efficacy of blocking an attack at a deeper layer of security should the previous security layer fail. Restricting integration of external solutions creates more vulnerable environments because threat actors can apply what they have learned from the environment of one service provider's customer to the environments of that

provider's other customers. There have been a few limited instances where legacy providers have allowed some "authorized" external solutions (e.g., Endpoint Detection and Response systems) to be integrated into their environment. However, several of these external solutions have been proven to be ineffective in blocking cyber-attacks or they conflicted with the provider's operating system or solutions (e.g., Microsoft's Defender, etc.) and subsequently did not perform as expected.

Ultimately, the uniform architecture and limited integration capabilities contribute to the cyber tax as they create more vulnerable environments that are more easily exploited, increasing the likelihood of devastating breaches and contributing to increasing breach remediation costs.

Tool Dependency

Legacy software providers boast about available tools for customers to manage and address their cybersecurity needs when subscribing to their tiered service. However, there is little information about the expertise needed to properly implement and utilize these tools. In addition, the closed software environment forces the customer to use the service providers' tools that are often hard to interpret, produce false positives, and do not work as well as some industry standard tools. For instance, in a recent court case, a Special Master determined that Microsoft Purview tool did not

"satisfy the duty of reasonable inquiry under Federal Rule of Civil Procedure 26(g)(1)."⁵³ The Special Master stated that Microsoft's 365 Purview tool does not 1) "fully index" documents in its cloud environment, 2) does not accommodate complex Boolean searches, and 3) does not allow users to validate their search and production results. As a result of these flaws, customers that rely on Microsoft's Purview tool for eDiscovery might miss critical data needed for a legal matter, which can adversely affect their case.

Forced Upgrades & Vendor Lock-In

As previously mentioned, most breach victims upgrade their tier during a cyber incident in the hope that it will help them respond to and/or mitigate the incident. In addition, on-premises victims typically opt to move their entire infrastructure to the cloud service offered by the legacy software vendor. This transfer to the cloud results in the customer shifting more control and data to the same service provider and operating systems involved in the cyber incident. This is especially true for Microsoft victims in Prescient's DFIR practice who have often moved their entire on-premises Active Directory (AD) to Microsoft's Azure Active Directory (also known as Microsoft Entra).⁵⁴ Unfortunately, this move often transfers (or syncs) the same settings that caused the original breach. Additionally, Azure Active Directory features new settings that create new vulnerabilities, as noted by discoveries from cloud security providers Wiz and Tenable.^{55 56}

While these forced upgrades are perceived as necessary to restore security and operations, many customers fail to understand that the shift does not protect the customer from future hacks or breaches. According to Palo Alto's *Cloud Threat Report*, the "fast evolution and growth of cloud workloads—as well as the complexity of managing hybrid and multi-cloud environments—cause many organizations to fall behind the curve and inadvertently introduce security weaknesses into their environments, as evidenced by the many legacy resources, vulnerabilities, and insecure configurations [they've] witnessed. These gaps give adversaries significant opportunities to gain a foothold in the cloud."⁵⁷

55 Rob Wright, Wiz warns of exposed multi-tenant apps in Azure AD, TechTarget, available at:

https://www.techtarget.com/searchsecurity/news/366547696/Wiz-warns-of-exposed-multi-tenant-apps-in-Azure-AD (Aug. 9, 2023).

⁵³ John Patzakis, Special Master Determines Microsoft Purview Does Not Comply with FRCP 26(g) Due to Unreliable and Incomplete Search Results, X1: NextGen GRC & EDiscovery Law Blog, available at: https://www.x1.com/2023/08/01/special-master-determines-microsoft-purview-does-not-comply-with-frcp-26g-due-

<u>https://www.x1.com/2023/08/01/special-master-determines-microsoft-purview-does-not-comply-with-frcp-26g-due-to-unreliable-and-incomplete-search-results/</u> (Aug. 1, 2023).

⁵⁴ Active Directory (AD) authenticates and authorizes all users and computers in a Windows computer network. It assigns and enforces security policies for all computers. Visit the following link for more information about AD: https://en.wikipedia.org/wiki/Active_Directory

⁵⁶ Ernestas Naprys, *Expert voices pile up on Microsoft's "negligent" security* management, Cyber News, available at: <u>https://cybernews.com/news/microsoft-azure-negligent-security-management/</u> (Sept. 22, 2023).

⁵⁷ Palo Alto Networks, Cloud Threat Report: Navigating the Expanding Attack Surface, available at: https://start.paloaltonetworks.com/rs/531-OCS-018/images/4.13PM_unit42-cloud-threat-report-volume7-final.pdf.

Unfortunately, these forced upgrades during a time of a cyber incident further enmesh these customers with service providers, and, in essence, lock them into their services, which makes it difficult and expensive for customers to shift to a new service provider. This dynamic also reduces the opportunity for non-legacy providers to break into the market and introduce newer, and possibly more secure, solutions. Once customers transition their operation to the cloud, they often learn of additional fees and/or hidden costs related to networking, processing, and storage. As such, customers can quickly exceed their anticipated costs.

Cyber Insurance Premiums

The increase in cyber incidents has led to an increase in demand for cyber insurance. At the same time, the growing costs of these incidents are driving up the premiums. Indeed, between 2020 and 2022, premiums increased by a median of 50%.⁵⁸ In addition to the increasing premiums, insurance companies are increasing their requirements and list of exclusions. In some cases, this leads to more time and effort spent by the companies to obtain insurance. According to Delinea's 2023 State of Cyber Insurance report, "the percentage of respondents reporting that the process to get cyber insurance took more than six months increased from 0.46% in 2022 to 7% in 2023."⁵⁹

In much worse cases, rising premiums and restrictive coverage leave many companies uninsured.⁶⁰ A 2022 BlackBerry and Corvus Insurance study found that nearly half of the surveyed companies

"These forced upgrades further enmesh customers with service providers, and, in essence, lock them into their services, which makes it difficult and expensive for customers to shift to a new service provider. This dynamic also reduces the opportunity for non-legacy providers to break into the market and introduce newer, and possibly more secure, solutions."

⁵⁸ Judy Greenwald, *Company cyber budgets jump 70% in four years: Moody's*, Business Insurance, available at: https://www.businessinsurance.com/article/20230929/NEWS06/912360168/Company-cyber-budgets-jump-70-in-four-years-Moody%E2%80%99s- (Sept. 29, 2023).

⁵⁹ Michael Hill, *Time and effort to obtain cyber insurance increasing for US* businesses, CSO Online, available at: <u>https://www.csoonline.com/article/650609/time-and-effort-to-obtain-cyber-insurance-increasing-for-us-businesses.html</u> (Aug. 29, 2023).

⁶⁰ Bob Ackerman, *Making Cyber Risk Insurable: Cyber Insurance Industry in 2023*, Forbes, available at: <u>https://www.forbes.com/sites/forbesfinancecouncil/2023/04/27/making-cyber-risk-insurable-disrupting-the-cyber-insurance-industry-in-2023/?sh=36c6c44958eb</u> (Apr. 27, 2023).

did not have insurance and of those insured, over one third were not covered for ransomware payments.⁶¹ The same study found that more than one third of respondents were denied cyber coverage specifically for not meeting the requirement of deploying Endpoint Detection and Response ("EDR") solutions.⁶² Notably, Microsoft's endpoint security solution Defender for Business is offered in its Microsoft 365 Business Premium package but has to be purchased separately in its more basic tiers.⁶³

⁶¹ Bruce Sussman, The State of Cyber Insurance, Blackberry Blog, available at:

https://blogs.blackberry.com/en/2022/11/the-state-of-cyber-insurance-2022-research (Nov. 21, 2022). 62 *Id.*

⁶³ Microsoft, *Find the Best Microsoft 365 Plan for Your* Business, available at: <u>https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products?tab=2</u>.

CONCLUSION

The changing cybersecurity landscape is putting pressure on the leaders in both the public and private sectors to scrutinize their current cybersecurity infrastructure and procedures and look for new solutions. The landscape of cybersecurity challenges has grown even more complex with the collective shift away from traditional on-premises security infrastructure into hybrid or fully cloud-based solutions from external providers.

Legacy software providers, taking advantage of their dominant market share, engage in practices that may ultimately expose their customers to greater cybersecurity risks and costs over time. The costs – direct breach remediation, security upgrades, legal fees, loss of time, reputational and IP damages – associated with these practices can be thought of as a "cyber tax."

These practices can especially affect small and medium-sized businesses, who collectively form the foundation of the U.S. economy. While legacy providers strengthen their market share, their expanded control and handling of financial, medical, and other critical data only further incentivizes the malicious actors behind an increasingly complex and prevalent landscape of ransomware and other cybersecurity incidents.

The tradeoff is seasonal returns for a minority of tech shareholders at the cost of mass data exposure, personal and corporate, from a larger majority of affected individuals, both directly (through their own firsthand organizational involvement) and indirectly (when their own customer data, interpolated into the larger landscape of vendors and organizations that make up the U.S. economy, is breached). This is a shortsighted exchange, compromising personal and organizational security for marginal gains of "too-big-to-fail" legacy software providers, who will in turn likely face stricter regulations in the years to come, when governmental incentives have more closely aligned against these factors.