4 June 2026

STRATEGIC MARKET STATUS INVESTIGATION INTO MICROSOFT'S BUSINESS SOFTWARE ECOSYSTEM

CFSL SUBMISSION ON INVITATION TO COMMENT

Contents

I. Executive Summary

1. The Coalition for Fair Software Licensing[1] (**CFSL**) welcomes the CMA's decision to assess whether Microsoft should be designated with strategic market status (**SMS**) in relation to its business software ecosystem.

2. Microsoft's market power in the supply of business software is unparalleled, stretching back more than a quarter of a century. The harms arising from Microsoft's conduct are well-understood, well-substantiated, and have been analysed in extensive detail over the course of multiple in-depth investigations, including the CMA's own market investigation into cloud services (the **Cloud MI**). In particular, its discrimination against customer use of 'Listed Providers' – and the corresponding exemption that Microsoft grants its own cloud services via Azure Hybrid Benefit (**AHB**) and other exceptions – was comprehensively found to have an adverse effect on competition in cloud services. Indeed, the harm to competition and customers in the UK is undeniable. The stage is finally set for interventions that will facilitate customer choice and competition on the merits, ultimately to the benefit of the UK's digital economy.

3. At this juncture, timely regulatory intervention is more important than ever. The investigation into Microsoft's anti-competitive practices concerning Teams shows that delayed intervention ultimately leads to ineffective outcomes. The longer interventions are delayed, the more customers will transition from on-premises to cloud computing, and the greater the share of the addressable market that will be locked into both Microsoft's business software ecosystem and its Azure cloud computing service. Technological developments, including the growth of AI and agentic enterprise workflows, will likely accelerate on-premises' customers' desire to migrate to the cloud. These customers will complete their migration without having the opportunity to choose a cloud provider that better suits their needs or which would otherwise succeed on their merits.

4. CFSL therefore urges the CMA to prioritise the imposition of conduct requirements (**CRs**) without delay and publish a roadmap of proposed interventions at the earliest opportunity. These interventions should address Microsoft's licensing restrictions, tying and bundling practices and interoperability barriers, and the use of its substantial and entrenched market power in workplace productivity software to extend and reinforce its position in adjacent

[1] The Coalition launched in September 2022 and is dedicated to protecting fair and transparent software licensing terms, and educating interested parties about the limiting impact that unfair and oblique licensing practices have on growth, opportunity, investment, and security. The Coalition advocates adoption, support, and use of the Principles of Fair Software Licensing, which provide the foundation needed to spur innovation, choice, and growth in the digital economy. 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) Permitted Uses of Software Should Be Reliable and Predictable; and (9) Licenses Should Cover Reasonably Expected Software Uses. Principles of Fair Software Licensing, CFSL, https://www.fairsoftwarelicensing.com/our-principles/.

productivity activities. These practices risk raising barriers to expansion for independent providers, reducing customer choice, and foreclosing effective competition.

5. Ending Microsoft's discrimination against 'Listed Providers' – and, by extension actual and potential customers of those providers – must be a top priority, so that the distortions created by Microsoft's licensing restrictions are addressed. At the very least, the CMA should consult on CRs to address Microsoft's licensing practices in parallel to its SMS investigation of Microsoft's business software ecosystem, given the need for immediate action. And it should be clear that the test for adopting *voluntary* commitments, as opposed to hard-edged conduct requirements, is not met.

6. The CMA should also look swiftly at how Microsoft is increasingly integrating the workflows through which business users create, communicate and collaborate directly into Microsoft 365, Copilot, and other Microsoft-controlled surfaces where it exercises market power. This inhibits opportunities for independent providers to compete on the merits at the point of user choice, and undermines users' ability to mix-and-match a best-in-breed suite of productivity tools; all the more so as Microsoft embeds AI-enabled creation, communication, and collaboration functionality into productivity tools that UK organisations already use every day.

7. In this paper:

   7.1. **Section II** explains that the CMA should consult on the contemplated range of interventions during the SMS investigation itself. Provided measures against Microsoft's licensing restrictions (and ending discrimination against Listed Providers and their customers) are adopted swiftly, CFSL supports the Invitation to Comment's (**ITC**) identifying further areas for intervention too. Microsoft's security software restrictions create severe barriers to switching. And there is a strong case for the CMA to require Microsoft to de-bundle certain aspects of its suites, learning from the European Commission's (**EC**) experience to ensure that any separation is operationally meaningful.

   7.2. **Section III** explains that the broad scope of the investigation and candidate activity definitions are necessary, and should explicitly scope-in additional Microsoft products such as Microsoft 365 Copilot, GitHub Visual Studio Code, and GitHub Copilot.

   7.3. **Section IV** notes that it is uncontroversial that Microsoft has a position of strategic significance (**POSS**).

   7.4. **Section V** explains that Microsoft has substantial and entrenched market power (**SEMP**) in each of the activities (not only as a 'grouped' set of activities).

   7.5. **Section VI** explains that Microsoft's market power is indeed entrenched.

   7.6. **Section VII** concludes.

II. CFSL agrees with the contemplated range of interventions

8. Investigations into SMS designations are not abstract exercises. They are a practical step towards CRs or pro-competition interventions that resolve concerns. Accordingly, with this Section II, CFSL begins with its position on the range of contemplated interventions. In the subsequent Sections III-VI, CFSL explains why it agrees with the corresponding scope of activities being considered for SMS designation.

9. The concerns arising from Microsoft's practices in respect of its business software ecosystem are well-understood, well-substantiated, and have been analysed in extensive details over the course of multiple recent in-depth investigations across a number of jurisdictions.

10. CFSL therefore welcomes the ITC's assessment of potential areas for intervention – in particular, Microsoft's leveraging of its market power from business software into cloud services. Cloud services provide vital infrastructure for UK businesses and other organisations,[2] who spent £9 billion on cloud services in 2023.[3] Yet, as ever more businesses move to cloud platforms for the first time, Microsoft improperly forces customers of its business software products into Azure, even when rival cloud services may better meet customers' needs.

11. Nowhere is this more apparent than Microsoft's discriminatory practices that punish customers of its business software who choose to deploy that software on the cloud service of its closest rivals – so-called 'Listed Providers'. These practices restrict customer choice to use Listed Providers, pushing customers to run Microsoft software on Azure through the exemptions Microsoft grants itself such as via AHB. The CMA has already confirmed in the Cloud MI that Microsoft's licensing practices are having an adverse impact on competition for cloud services. As the Cloud MI found:[4]

> "*Microsoft sets a high input price for AWS and Google for hosting Windows Server and SQL Server. AWS and Google, Microsoft's closest competitors, are targeted specifically as Listed Providers […] The price that AWS and Google face for hosting Windows and SQL Server has increased substantially since 2018. The input cost for AWS and Google is higher than the customer-facing price that Microsoft charges its own customers that qualify for AHB to use Windows Server on Azure. For SQL Server, the input cost for AWS and Google is higher than Microsoft's PAYG customer-facing price*"

---

2 TechUK, Cloud computing and the journey to net zero, 24 April 2024. Last accessed 18 May 2026.

3 CMA, CMA independent inquiry group publishes provisional findings in cloud services market investigation, 28 January 2025. Last accessed 18 May 2026.

4 Cloud MI, Final Report of 31 July 2025, paras. 7.760-761 and 7.776. Last accessed 4 June 2026.

and

"*Considering all the evidence in the round, Microsoft's licensing practices are adversely impacting the competitiveness of AWS and Google in the supply of cloud services, particularly in competing for customers that purchase cloud services which use the relevant Microsoft software as an input. As a result, Microsoft faces weaker competitive constraints from AWS and Google, its most significant competitors, which is reducing competition in cloud services markets*."

12. An effective remedy must therefore bring the differential treatment of Azure and 'Listed Providers' to an end. At present, the consistent body of evidence shows that Microsoft restricts open choice, deals with customers unfairly, and degrades trust and transparency. Swift intervention is therefore needed to facilitate competition in the cloud and ensure customers have meaningful choice in cloud providers, alongside interventions to facilitate competition in business software itself.

A. The CMA can and should consult on CRs during the SMS investigation to address Microsoft's restrictive licensing practices, including to end discrimination against 'Listed Providers'

13. CFSL welcomes the proposed scope of designation and the range of potential concerns that the ITC proposes for further investigation. The priority issue for the CMA to address urgently, though, is Microsoft's licensing restrictions – in particular, the discrimination against, and concept of, Listed Providers – which have been investigated in depth and require intervention at pace. The Digital Markets, Competition and Consumers Act 2024 (**DMCCA**) permits the CMA to consult on potential CRs in parallel with the SMS investigation,[5] and it is necessary for the CMA to leverage the agility of the DMCCA in this case.

14. First, Ofcom and the CMA have undertaken extensive investigative work since 2022, establishing clear evidence-based harms. The effect of Microsoft's conduct has been to raise the costs of its closest competitors, while degrading the quality of their offerings. Its actions produce no viable efficiencies or consumer benefits. The Cloud MI found conclusively that Microsoft's restrictive licensing practices have adverse effects on competition.[6] These matters need not be re-litigated in this process.

15. Second, there is a serious risk of irreparable harm to competition. If the CMA takes the full statutory period until February 2027 to designate Microsoft with SMS, Microsoft will have been permitted to restrict competition, damage incentives to invest and innovate, and ultimately undermine customer choice during a period in which (i) Azure has been

---

5 DMCCA, section 24(3). Last accessed 4 June 2026.

6 Cloud MI Final Report, para. 36(c). Last accessed 4 June 2026.

experiencing rapid growth; (ii) ever more customers are moving to the cloud for the first time; and (iii) Microsoft's licensing practices have been under regulatory scrutiny, but with no interventions in place to prevent the market from tipping. Every month that passes is a month in which Microsoft's harmful conduct shapes enterprise procurement decisions that may lock in yet more cloud computing customers for years to come, which also carries a significant risk of distorting competition in new, evolving AI product areas (as explained further below).

16. Third, there are clear, identifiable and well-considered remedies to consult on immediately, each of which has a basis in Cloud MI, namely that Microsoft must:[7]

    16.1. Apply a fair, reasonable and non-discriminatory (**FRAND**) approach in relation to pricing and licensing options for its software products, regardless of which cloud they are hosted on, and restrict Microsoft from applying discriminatory terms, conditions or policies to certain types of users or potential users. For the avoidance of doubt, this remedy must ensure that Microsoft cannot discriminate against the existing Listed Providers or users of Listed Providers, and must end the concept of 'Listed Providers', or any similar arbitrary category of provider, entirely;

    16.2. Publish clear and detailed information on the FRAND-based pricing of its software products across on-premises environments, Azure and non-Azure clouds;

    16.3. Facilitate a consistent experience for customers who use products in Microsoft's business software ecosystem – including Copilot – on Azure or non-Azure products, with no exceptions;

    16.4. Be prevented from degrading the technical performance of any software product when deployed on non-Azure environments relative to Azure, for example by withholding access to product functionality by technological means or by contractual limitations;

    16.5. Allow customers to deploy pre-existing software product licences on the cloud of the customer's choice; and

    16.6. Permit bring-your-own-licence (**BYOL**) for any product in Microsoft's business software ecosystem (and related services which support their deployment on cloud) to any cloud of the customer's choice, and allowing end customers to rely on their on-premises Microsoft software product licences to deploy that product on any public cloud, regardless of which cloud it is hosted on, provided that the end customer has the necessary licences to do so.[8]

---

7 See eg. CMA Cloud MI Final Report, Appendix W, para. 238. Last accessed 21 May 2026.

8 CFSL also notes that any such CR must also address the structure of Software Assurance fees applicable to licence transfers, to ensure that Microsoft cannot accept BYOL in principle while restoring the cost

17. Fourth, there is no need to defer intervention pending the outcome of investigations in other jurisdictions, such as the EU, US or Japan. The CMA has already found that Microsoft's conduct is harmful and designed many of the remedies that should be imposed. The CMA *is* the leading authority on this issue. In any event, remedies ultimately imposed outside of the UK will not address the ongoing harms caused to UK businesses and the public sector.

18. Fifth, consulting on proposed CRs concurrently with the Proposed Decision and then imposing CRs at the earliest opportunity would – in this case – align with the CMA's '4Ps' principles. It would satisfy the need for 'pace' by "*focusing as quickly as possible on key areas of potential concern.*"[9] It would satisfy the need for 'predictability' in circumstances where the Cloud MI has set out clear findings of harm and the interventions in software licensing that ought to be imposed. It would be 'proportionate'[10] in view of the significant ongoing harm arising caused by Microsoft conduct and its impact on the competitiveness and resilience of business enterprises across the UK economy. And it would not contravene the need for 'process', with Microsoft already having been granted extensive opportunities over multiple years to put its case on these issues (and which it could do again under a s.24 DMCCA consultation).

19. Accordingly, CFSL urges the CMA to (i) publish a roadmap of proposed interventions as soon as possible (which should include at a minimum the remedies recommended by the CMA panel in the Cloud MI Final Report), and **before** it publishes any Proposed Decision; (ii) confirm the remedies proposed above at paragraph 16 are listed as priority, 'Category 1' CRs; and (iii) consult on these CRs at the same time as the Proposed Decision.

B. The investigation should review Microsoft's security software restrictions, which create a further barrier to switching

20. CFSL strongly supports the ITC's proposed inclusion of Microsoft's security software – such as Entra ID, Active Directory, Intune and Defender – in the proposed designation

---

barrier through SA uplift charges or other ancillary fees that have the effect of negating the portability that the CR is intended to secure.

9 CMA, Delivering the 4Ps under the digital markets competition regime, 30 April 2026. Last accessed 22 May 2026.

10 CFSL notes that DMCR Guidance sets out conditions for determining whether a CR is effective and proportionate, namely that it must (i) be effective in achieving its intended aim, by addressing a concern identified by the CMA; (ii) be no more than onerous than it needs to be to achieve that aim; (iii) be the least onerous CR, where there are multiple equally effective options; and (iv) not produce disadvantages that are disproportionate to the aim (para 3.33). CFSL's proposed remedies meet all of these criteria, and therefore it is appropriate to consult on them as soon as possible, to remedy the harms caused by Microsoft's conduct: (i) the remedies are targeted as these address specific, well-identified discriminatory practices that need to be addressed; (ii) they are no more than onerous than is needed, as they would be low-compliance remedies (for example, as Microsoft already operates non-discriminatory pricing for its own AHB customers); (iii) there is no suggestion that there alternative remedies are available; and (iv) they do not produce any disadvantages, let alone those that are disproportionate to the aim. Moreover, these interventions would promote consumer welfare as they would impact customer purchasing decisions, and therefore are likely to lead to increased choice and competition.

scope. Microsoft is the largest vendor of security software globally,[11] has had the highest market share in endpoint security since 2023,[12] and has only been able to achieve these positions by leveraging its market power to erect insurmountable barriers to switching to competitors, such as in the form of severe technical dependencies. CFSL recognises that the security and integrity of widely-deployed enterprise software is a legitimate and important objective and does not urge a conduct that would compromise the security of UK organisations. The relevant question is how to distinguish a genuine security measure from self-preferencing conduct presented as one. A measure genuinely explained by security should apply on equivalent terms to Microsoft's own products, and be no more restrictive than necessary to achieve the security objective. Conduct that burdens rivals while exempting Microsoft's own offerings, or that is more restrictive than the objective requires, is not explained by security. Asymmetry between the treatment of Microsoft's own products and that of competitors illustrates this.

20.1. **In relation to identity and access management (IAM)**, Microsoft has built a moat around its position in IAMs and device management through five, cumulative steps.

20.1.1. First, Microsoft bundles Entra ID and Intune with its dominant E3/E5 Microsoft 365 enterprise plans,[13] creating the false impression that these products are 'free' and ensuring that existing customers are never likely to purchase competing IAM products.

20.1.2. Second, Microsoft reinforces this bundling strategy through technical restrictions. It has made Entra ID fully interoperable with Active Directory (e.g., via non-standard Kerberos-based authentication integrations, which are unavailable to third parties) while restricting third-party access to Active Directory's APIs and technical information. This effectively ties Active Directory's customer base into Entra ID upon their migration from on-premises to cloud computing.

20.1.3. Third, Microsoft forces customers of its productivity software or Windows to use Entra ID and Intune to provision and manage devices remotely, whether they want to or not.

20.1.4. Fourth, Microsoft further entrenches this dependency by withholding the APIs needed for third-party IAM products to manage Microsoft 365 or authenticate non-Windows systems.

---

11 Simple Investing, Microsoft: A Deep Dive Into Its Mammoth Cybersecurity Business, 21 March 2023. Last accessed 20 May 2026.

12 Microsoft, Microsoft ranked number one in modern endpoint security market share third year in a row, 27 August 2025. Last accessed 20 May 2026.

13 See this comparison of Microsoft productivity suite prices. Last accessed 20 May 2026.

20.1.5. Fifth, Microsoft even requires third-party IAM vendors seeking API access to sign agreements obliging them to inform customers that (i) they must maintain Entra ID and/or Intune licenses *alongside* competing solutions, and (ii) placing in those agreements non-disclosure provisions preventing vendors from objecting to these practices.[14]

20.1.6. The cumulative effect of these practices is that Microsoft has created a self-reinforcing system from which customers cannot realistically escape and into which competitors cannot realistically enter. This has knock-on effects. IAM controls access to the entire Microsoft ecosystem and, by extension, enterprise customers' systems and data. Entrenching Active Directory and Entra ID's position enables MSFT to dictate how third-party cloud services interoperate with customers' systems, providing Microsoft with a further mechanism to foreclose rivals and strengthen its market power.

20.2. For years, Microsoft refused to support inbound SCIM[15] for Entra ID, departing from industry practice and forcing competitors to build costly custom integrations that increase friction for customer adoption and risk introducing cybersecurity vulnerabilities. Microsoft has recently established support for standard SCIM protocols, but only after years of inquiries from customers and pressure from regulators. It should be noted that, even then, the support requires an additional consumption charge. And, absent regulatory rules, there is nothing to prevent Microsoft withdrawing this support at a later date, or making it subject to unviable fees or terms.

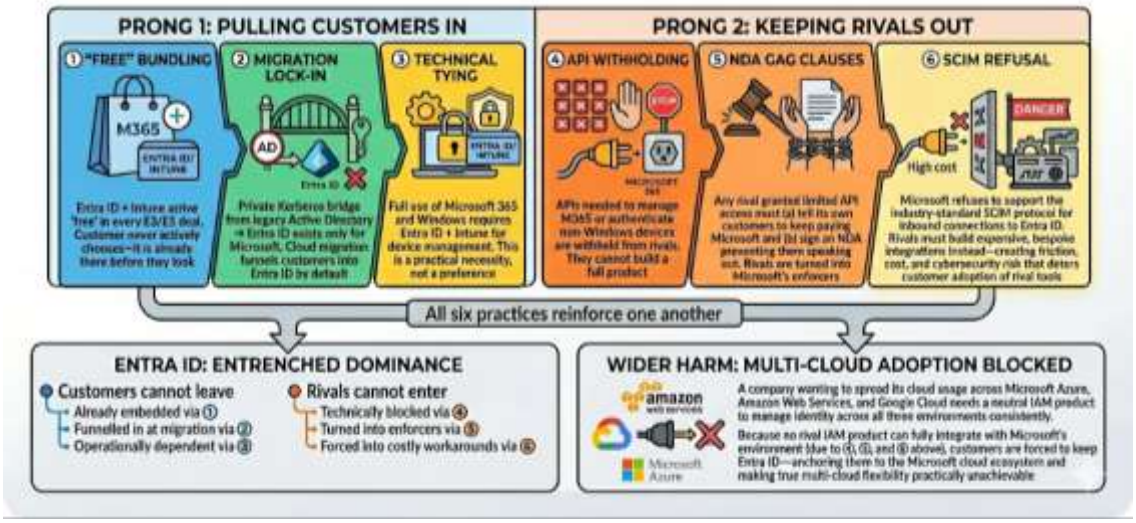
20.3. The cumulative effect of this two-pronged strategy – technically integrating Entra ID and Intune with Microsoft's dominant software, while restricting their interoperability with competing products – has allowed Microsoft to capture a market-leading position in security software. As summarized in Figure 1 below, customers are pulled into Entra ID via the first prong, and prevented from leaving via the second prong. In turn, this creates yet another obstacle to customers seeking to move away from Microsoft products or adopt multi-cloud solutions.

---

14 Companies under these non-disclosure obligations may fear retribution for discussing such API agreements, so the agreements that currently obligate businesses are not public. However, similar language appears in Microsoft's API agreements. See eg. Microsoft's API Terms of Use, section 8. Last accessed 21 May 2026.

15 System for Cross-domain Identity Management. This is an open, industry-wide standard – essentially a universal language that different software systems use to indicate whether a new account (eg. for a new employee) is needed, or that access needs to be revoked (eg. when an employee has left an organisation). Inbound SCIM is the ability for an external system to push user information into another system (eg. using a rival IAM product, such as Okta, to push information into Entra ID).

Figure 1: How Microsoft locks customers in and rivals out



20.4. All of this will have long-term effects on the critical emerging space of AI agents, potentially jeopardising the productivity gains that these AI agents could deliver.

20.4.1. Microsoft's technical documentation confirms that every AI agent operating in a Microsoft environment must have an identity registered and managed within Microsoft's Entra ID. For example, if an agent is to schedule calendar meetings, draft emails, or perform other tasks using Microsoft's ubiquitous productivity software, it must be registered with — and granted access by — Entra ID.

20.4.2. Critically, Microsoft's own documentation states that agent identities can only be issued tokens in the Microsoft Entra tenant where they are created, and cannot access resources or APIs in other tenants.[16] No neutral, third-party IAM system can issue a token that Microsoft's systems will accept — only Microsoft's Entra ID can do that.

20.4.3. This has a direct and damaging consequence for enterprises seeking a multi-cloud strategy. A company running its IT across Microsoft Azure, Amazon Web Services, and Google Cloud might reasonably want a single, independent IAM product to manage all of its AI agent identities centrally, issuing credentials that work across all three environments. The single-tenant rule makes this impossible for the Microsoft slice of that environment: no neutral IAM can issue the tokens Microsoft systems require. The company is therefore

16 See Microsoft, Agent identities in Microsoft Entra Agent ID, last accessed on 2 June 2026. See also e27, A pivot to 'digital seats'? Analyzing Microsoft's alleged AI strategy shift, 20 April 2026, last accessed 4 June 2026.

forced to run Entra ID for its Microsoft environment and something else for the rest — two parallel systems and two sets of costs, which is inefficient.

20.4.4. In principle, Microsoft states that while agent identities are single-tenant, agent identity blueprints can be configured as multitenant, meaning a third-party AI vendor can publish a template that different organisations install into their own Entra ID tenants, creating a local agent identity within each. But this does not resolve the competition concern. The template may come from outside Microsoft, but the actual credential — the token — is always issued by and managed within Microsoft's own system.

20.4.5. Unlike AWS and GCP, which accept federated identity assertions from third-party providers via open standards (OIDC/SAML), Microsoft's agent identity system requires that the operative token be issued exclusively by Entra ID, with no federation path for agent credentials. Moreover, the applications gated by this requirement — email, calendar, productivity tools — are not cloud-infrastructure services but general-purpose business applications with no viable substitute.

20.4.6. This makes Microsoft the unavoidable gatekeeper for enterprise AI agents. And while Microsoft's documentation indicates that it permits third-party providers' AI agents to register, it retains the ability — through its control of Entra — to apply policies, restrict permissions, or disable third-party agents entirely, giving it both the means and incentive to preference its own Copilot-based agents.

20.5. **In relation to endpoint security**, Microsoft has leveraged its market power from its business software ecosystem to become the market leader in endpoint security. Microsoft Defender is automatically bundled with Microsoft 365 plans and comes pre-installed with Windows 10/11,[17] purportedly for free, but in reality with its cost being baked into the price of Microsoft's suites. This cloaks Defender's true cost and shields it from head-to-head competition with rival endpoint security software. Just as in the EC's *Teams* cases, this bundling prevents businesses from assembling best-in-breed suites of software, ultimately softening competition and leading to worse outcomes for customers.[18]

---

17 See eg. CMA Final Report, *Norton/Avast plc*, 2 September 2022, paras. 20-21.

18 See eg. EC Decision of 12 September 2025 in cases AT.40721 (*Microsoft Teams*) and AT. 40872 (*Microsoft Teams II*), para. 146 ("*Additionally, the marginalisation of Teams' rivals, for which customer demand exists, contributes to reduced customer choice. The tie will also lead to increased barriers to entry in the market, as Teams is shielded from competition. This is because Teams has access to a significant part of the installed base in the market and potential Teams' rivals must spend significant resources to offset Teams' advantage*") and paras. 45-47 (*"the SO preliminarily concluded that Microsoft's tying conduct is part of a broader strategy. [...] on defensive leveraging, the SO preliminarily found that Microsoft identified the threat of rival SaaS UCC to the Microsoft Suites, notably because the integration of rival SaaS UCC with other SaaS solutions further enabled customers to adopt a "best-of-breed model"*

20.6. CFSL members have provided direct evidence of these harms.

20.6.1. One CFSL member providing endpoint security solutions for mobile platforms reports that Microsoft's bundling of mobile security within its E5 package creates a 'zero-price anchor' that fundamentally distorts competition: for Microsoft, the bundled product only needs to be "*adequate*", whereas any competitor must be "*dramatically obvious*" in incremental value to justify additional expenditure. This member experiences a 6% annual churn rate, with all of this attrition attributable to customers switching to Microsoft's bundled product. This includes a former major customer with 2024 revenue of over EUR 20 billion, which acknowledged the member's superior security solution but terminated the contract due to a mandate to reduce costs to match Microsoft's effective bundled pricing.[19]

20.6.2. A separate CFSL member providing endpoint and network security solutions reports that Microsoft has leveraged its control over critical system access points to disadvantage competing security products through driver blacklisting and vulnerability mis-categorisation — categorising certain vulnerabilities as "critical" or "severe" when, by the member's assessment, they are routine issues, thereby enabling Microsoft to approach customers claiming there are security issues with the member's products that would not exist if they used Defender instead.[20]

C. The importance of interoperability with elements of Microsoft's business software ecosystem to unlock competition within UK markets and economic growth

21. The ITC correctly identifies technical design and interoperability as a key issue. CFSL strongly endorses this focus. Interoperability 'on paper', such as the publication of API specifications and protocol documentation, does not necessarily produce effective interoperability in practice when access to APIs and customer-generated data is limited in other ways. Interoperability concerns arise at multiple layers of the Microsoft ecosystem simultaneously and must be addressed via formal CRs. Issues that need to be addressed via CRs include:

21.1. **API and integration layer**: The Microsoft Graph API, which provides access to Microsoft 365 data (emails, calendar entries, documents, meeting recordings) is the

whereby customers chose themselves their preferred SaaS solutions from various providers instead of purchasing all the SaaS solutions they need from one single provider. Therefore, Microsoft sought to protect its Microsoft suites [...], reduce the potential for best-of-breed solutions integrating non-Microsoft software [...] [and] the tie would also enable Microsoft to upsell existing customers to a broader range of additional Microsoft software.")

19 Annex B – Case Study 2

20 Annex B – Case Study 3

single most important integration point for enterprise applications. Restrictions on Graph API access - whether through rate limiting, scope limitations, or differential access terms - directly disadvantage rival cloud providers seeking to offer Microsoft 365-integrated services. CFSL members have provided direct evidence of these restrictions in practice.

21.1.1. One CFSL member providing cloud and network security solutions to UK customers reports that Microsoft's current API imposes a cap of 50,000 API calls for licensed users regardless of actual company size, such that a customer with 400,000 licensed Microsoft 365 users receives the same API call limit as a 50,000-user customer. When this member exceeds the applicable bandwidth thresholds, Microsoft informs customers that they would not experience these issues if they used Defender instead — yet Microsoft's own solution does not appear to face equivalent limitations, suggesting that Microsoft either uses an unpublished API or is exempt from the limits it imposes on competitors.[21] Microsoft also charges customers additional fees to unblock rate limits and enable deeper API connections, meaning that customers are required to pay additional costs to use a competitor's product while Microsoft's own solution bypasses these restrictions entirely. The API throttling imposed by Microsoft undermines the ability to deliver the full value of their security solutions and weakens competitive pressure on Microsoft to maintain high security standards, potentially weakening the overall security posture of organisations relying on the Microsoft ecosystem.

21.2. **IAM interoperability**: As described above, the Entra ID/Active Directory integration architecture creates switching friction that is experienced as a concrete technical barrier, not merely a theoretical concern.

21.3. **Telemetry and observability**: Microsoft's security products (Sentinel, Defender) consume telemetry from across the Microsoft ecosystem, and Microsoft does not charge for imports of endpoint logs from these products.[22] Rival security providers cannot access equivalent telemetry breadth, creating a compounding disadvantage in threat detection quality that reinforces Defender's market position. And Microsoft

---

21 Annex B – Case Study 1

22 Microsoft, Plan costs and understand Microsoft Sentinel pricing and billing, last accessed on 2 June 2026. This document explains, for example, that pricing for Sentinel is based on the data ingested. However, among other things: (i) "*Hunting graph and blast radius visualizations in the Microsoft Defender portal, along with Insider Risk Management and Data Security Investigations in the Microsoft Purview portal, don't incur any billing or consumption charges*"; (ii) in respect of Office 365 Audit Logs, including all SharePoint activity, Exchange admin activity, and Teams is a free data source; and (iii) in respect of security alerts for various Defender products (e.g., Defender XDR, Defender for Cloud), these are a free data source (raw logs may still be paid).

does charge for endpoint log imports from competing third-party endpoint, detection, and response products.

21.4. **Microsoft's productivity software:** The CMA received evidence in the Cloud MI that customers are unable to switch away from Microsoft 365 because Microsoft is perceived to be the 'default' supplier of productivity software[23] and that, because these products are 'must-have',[24] customers have no choice but to accept Microsoft's licensing restrictions. CFSL therefore urges the CMA to impose a CR that provides appropriate interoperability to competitors with individual products within these suites (eg. Word, Excel, Outlook, Teams, Copilot) as Microsoft currently reserves to itself.

21.5. **Microsoft's developer tooling:** CFSL members have also experienced barriers arising from Microsoft's control of developer tooling that compound the interoperability and technical migration concerns described above. As one example, organizations seeking to migrate away from GitHub face rate limits on API-based data export that make large-scale migrations operationally disruptive, with secondary limits that are inconsistently documented and disproportionately affect migration workloads. One CFSL member noted an instance in which an enterprise migration of a single 17GB repository with over 80,000 pull requests required months of trial and error, custom scripting to rotate multiple access tokens when hitting rate limits, and manual intervention to resolve cryptic errors and silent failures from GitHub's API. Such barriers compound the effect of other API restrictions and default placement practices such that even where a customer wishes to adopt a competing developer tool, the accumulated technical cost of migration functions as a structural disincentive to doing so.

D. The CMA should impose CRs requiring Microsoft to de-bundle certain aspects of its suites

22. The EC's Teams commitments demonstrate that formal product separation, without accompanying measures to address the go-to-market mechanism through which Microsoft steers customers towards the bundle, does not produce meaningful competitive outcomes. The CMA should learn from this precedent and ensure that any de-bundling CRs imposed on Microsoft address both the product configuration and the sales practices that give effect to the bundle. The CMA should also ensure that any interventions to address Microsoft's bundling practices are future-proofed, taking account for the dynamic nature of this market, as well as to account for the continuously-evolving nature of Microsoft's product suites. In particular, the CMA should impose CRs in respect of the following:

---

23 Cloud MI Final Report, Appendix R, para 127 to 128. Last accessed 4 June 2026.

24 Cloud MI Final Report, Appendix R, para 138. Last accessed 4 June 2026.

22.1. **Microsoft 365 Copilot and AI agents**: The CMA should impose a CR requiring Microsoft to offer Copilot and AI agent functionality as standalone products, available for purchase independently of Microsoft 365 and E5/E7 enterprise plans. Microsoft's launch of the E7 bundle in April 2026 - which integrates Copilot, AI agents and expanded identity services into a single suite of products - represents an acceleration of the bundling strategy that led to the anticompetitive outcomes identified in the EC's Teams investigation. Unless Copilot is required to be offered and priced independently, Microsoft is likely to replicate the Teams playbook by embedding Copilot so deeply into the Microsoft 365 suite that customers will not be able to perceive any viable alternative, foreclosing competition from rival AI providers while the market is still continuing to develop and evolve.

22.2. **Anti-Circumvention Obligations**: Any de-bundling CR should also include a robust anti-circumvention obligation. Microsoft should not be able to comply formally by separating a named product, while reintroducing materially equivalent functionality through another Microsoft-controlled surface, bundle, add-on, agent or default workflow. This is particularly important in AI-enabled productivity software, where the same underlying functionality can be moved rapidly between Microsoft 365 apps, Copilot, PowerPoint, Teams, Windows and future AI agent experiences. The Teams unbundling experience demonstrates that formal product separation without operational separation of sales, CRM and quoting functions produces nominal compliance without competitive effect: Microsoft's sales teams continue to promote the integrated bundle as the default option, and the pricing differential between bundled and unbundled plans is insufficient to overcome the integration costs and administrative friction of adopting competing products.

22.2.1. The CMA should therefore define any relevant obligation by reference to the competitive function performed and the route to market; not merely by reference to current Microsoft product names.

22.2.2. Further, where a de-bundling CR is imposed, the CMA should require Microsoft to: (i) ensure that its sales organisation does not preference the bundled offering over the unbundled alternative in customer-facing communications, pricing proposals, renewal processes or enterprise agreement negotiations; (ii) maintain separate quoting and CRM workflows for bundled and unbundled product configurations, so that sales representatives are not incentivised - whether through compensation structures, default system settings or management direction - to steer customers towards the bundled option; and (iii) provide the CMA or an independent monitor with access to internal CRM data, sales performance metrics and quoting records sufficient to verify compliance with these obligations on an ongoing basis.

E. Microsoft's conduct has harmed UK consumers and UK businesses

23. There are widespread concerns that Microsoft's conduct has harmed – and continues to harm – the UK. The CMA itself confirmed that the adverse effect on competition found in the Cloud MI is unlikely to have been time-limited,[25] and concerns have been raised in Parliament that Microsoft's conduct harms UK organisations, including by *"ripping off"* the NHS.[26]

    23.1. First, the CMA has already confirmed that outcomes for customers are worse due to Microsoft's anticompetitive practices, as evidenced by the elevated costs that Microsoft imposes on AWS and Google Cloud, with the result being that "*customers generally perceive them to be more expensive than Microsoft.*"[27] Preventing these practices will make outcomes better for customers, and by extension, UK consumers.

    23.2. Second, Microsoft has restricted cloud choice and reduced innovation, and therefore investment, by ensuring that Azure adoption is closely and deeply linked to pre-existing Microsoft product use. Microsoft has engineered a scenario where customers are unlikely to switch to rival clouds or indeed to providers that rival any aspect of its business software ecosystem. This dampens incentives to innovate and invest in the UK for Microsoft's rivals, and is likely to suppress new entrants to these markets.

    23.3. Third, customers are no longer able to buy and deploy Microsoft licences from independent managed service providers, if those providers host their services on Listed Providers' clouds, and hosted service providers cannot run their solutions on the cloud infrastructure of their choice, or supply customers with SPLA licences for Microsoft software to be used with their hosted solutions. This restricts customers' ability to select the IT provider of their choice, resulting in continued and sustained harm to UK consumers.

    23.4. Fourth, similar harms arise within productivity software itself. This is particularly significant in the current enterprise procurement environment. Independent providers do not compete with Microsoft only on product quality. They also compete against Microsoft's distribution advantage, default positioning and procurement baseline. Microsoft can place its own functionality inside the products that organisational users already use every day, while independent providers must overcome separate budget approval, procurement review, security review, vendor onboarding and change-management processes.

---

25 Cloud MI Final Report, Appendix W, para 264. Last accessed 4 June 2026.

26 See eg. The Guardian, Microsoft has 'ripped off the NHS', says MP amid call for contracts with British firms, 19 November 2025. Last accessed 21 May 2026.

27 Cloud MI Final Report, para 31. Last accessed 4 June 2026.

23.4.1. CFSL members' evidence confirms the harm in concrete terms. One CFSL member operating R&D expenditure at 25% of revenue reports that its entire 6% annual customer churn — all of which is attributable to customers switching to Microsoft's bundled product — comes directly out of its R&D budget, creating a downward cycle in which Microsoft's impairment of the member's ability to generate revenue directly impairs its ability to innovate and invest in product development.[28] This member reports that a former major customer with 2024 revenue of over EUR 23 billion acknowledged the member's superior security solution to Microsoft's but cut the contract due to a cost-reduction mandate — a decision driven not by product quality but by the commercial pressure created by Microsoft's zero-price bundling strategy. The mobile security component is just one element of the E5 bundle, meaning multiple vendors across different security categories are experiencing similar competitive harm, with the bundling strategy effectively setting a "minimally viable standard" that becomes the baseline for many customers regardless of whether superior alternatives exist.

23.4.2. As another CFSL member noted, productivity workflows increasingly include visual, branded and multimedia work outputs, Microsoft's bundling and default distribution practices can impair competition by making Microsoft's own creation tools appear "already included" or "good enough" within existing Microsoft 365 or Copilot commercial arrangements.

23.5. Fifth, the July 2026 global price and packaging updates[29] heighten this concern. Microsoft is increasing prices across selected commercial suites and government equivalents, while also expanding the functionality included in Microsoft 365, including Copilot Chat enhancements and Copilot Chat Analytics across a range of enterprise, frontline and business suites. Microsoft is also introducing Microsoft 365 Business Standard with Copilot and Microsoft 365 Business Premium with Copilot, with Copilot built into Word, Excel, PowerPoint, Outlook and Teams.

24. This combination of higher suite pricing and broader AI functionality may increase procurement pressure on customers to rely on what is already included in Microsoft 365 and their dependencies on the broader Microsoft business software ecosystem, rather than separately procuring independent tools and providers. In practice, Microsoft can raise the prices while expanding the scope of their products and services, making alternatives / competitors appear incremental, duplicative or harder to justify — even where they offer superior or more specialised functionality. This reduces the likelihood that customers meaningfully evaluate rival products on their merits, thereby weakening competitive constraints that would otherwise discipline Microsoft.

---

28 Annex B – Case Study 2

29 Microsoft, Microsoft 365 Pricing and Packing Updates, effective 1 July 2026. Last accessed 2 June 2026.

25. These harms are severe, are borne by UK organisations across the economy, including the public sector, and will require clear and focused CRs. Nevertheless, the benefits of these remedies for the UK are likely to outweigh any cost to Microsoft[30] in the form of greater choice and stronger incentives to innovate across all sectors, and will fulfil the DMCCA's aim of "*protecting [...] UK consumers*."[31]

F. Microsoft's conduct confirms that the criteria for accepting voluntary commitments are not met

26. The Mobile SMS investigations established criteria for accepting voluntary commitments.[32] The CMA confirmed that is "*unlikely to pursue commitments"* where (i) there is significant divergence between the CMA and SMS firm on what the CMA is looking to achieve; (ii) where the firm has little incentive to change its conduct; (iii) where compliance is difficult to determine, observe or monitor; (iv) where measures can be easily circumvented; or (v) where the firm's historical conduct does not give the CMA confidence that the firm will work constructively with the CMA.

27. Voluntary commitments are *not* appropriate to resolve the issues set out in paragraph 13-19, with mandatory CRs being the only viable remedy. This is for the following reasons:

    27.1. **There is a significant divergence between Microsoft's harmful conduct and what is needed to remedy the various harms.** It is a matter of public record that Microsoft has sought to avoid previous interventions, including by offering voluntary concessions to affected cloud providers without serious intent to comply or deliver genuine improvement to market outcomes.[33] Critically, Microsoft has taken no such measures to terminate its restrictive licensing practices against Listed Providers, necessitating the launch of the present proceedings.[34] This is despite facing multiple

---

30 DMCCA, section 19(5). Last accessed 4 June 2026.

31 DMCCA, Explanatory Note 92. Last accessed 4 June 2026.

32 CMA, Call for Evidence in relation to potential interventions, 10 February 2026, para. 9. Last accessed 21 May 2026.

33 Examples include Microsoft's 2022 licensing changes to avoid an EC investigation (but deliberately excluding Listed Providers) and the 2024 CISPE settlement (where it failed to deliver many of the agreed changes). Microsoft's recent voluntary concessions to the CMA purportedly sought to facilitate cross-cloud management for customers. However, these measures fail to address IAM interoperability, which remains the most significant technical barrier to multi-cloud deployments.

34 CMA, CMA announces package of actions on business software and cloud services, 31 March 2026. Last accessed 21 May 2026. ("*An SMS designation would allow the CMA to act on a major concern from the CMA's cloud market investigation – Microsoft's use of software licensing reducing competition in cloud. It would also provide a route to ensuring a level playing field among providers at a critical moment, as AI-driven innovation reshapes competition in productivity software*.")

investigations globally into the same harms.[35] In short, Microsoft has not *offered* a voluntary solution.

27.2. **Absent formal CRs, Microsoft has little to no incentive to change its conduct.** It is clear that Microsoft is benefiting from delaying the end of its harmful practices. As the Cloud MI found, Microsoft has consistently held the largest share of revenue growth[36], enabling it to further entrench its position. Imposing CRs on Microsoft and formalising its duty of care[37] is the only way to procure that Microsoft refrains from continuing to harm competition and customers in the UK.

27.3. **The CMA confirmed in the Cloud MI that Microsoft can easily circumvent remedies,** citing that the "*nature of [Microsoft's] practices [...] and connections to wider elements of Microsoft's business"*[38] meant that it would have been "*challenging*" to impose remedies. While CFSL maintains that the CMA could – and should – have imposed remedies following the Cloud MI, CFSL agrees that formal remedies under the DMCCA are needed to end Microsoft's harmful conduct and ensure that Microsoft is not permitted to backslide in the future.

27.4. **Microsoft's historical conduct confirms it is unlikely to work constructively or willingly in relation to these issues.** As regards Microsoft's historical conduct, CFSL notes that Microsoft was reported to have "*repeatedly failed to meet the terms of the settlement with CISPE"* reached in July 2024,[39] so much so that a new agreement was reached just 12 months later, but which still failed to remove the tie between Entra ID and Microsoft 365.[40] This piecemeal approach confirms that until Microsoft is subject to formal remedies, these issues will simply not be solved.

---

35 For example, the JFTC raided Microsoft Japan in February 2026 as part of an investigation of its licensing practices, the FTC is investigating similar practices in the US, and CADE is investigating in Brazil.

36 See eg. Cloud MI Final Report, para. 3.243. Last accessed 4 June 2026.

37 DMCCA, section 101(1). Last accessed 4 June 2026.

38 Cloud MI Final Report, Appendix W, para 266. Last accessed 4 June 2026.

39 See eg. Data Center Dynamics, Microsoft and CISPE agree to new commercial terms after failure of Azure Local, 18 July 2025. Last accessed 21 May 2026.

40 See eg. The Register, EU cloud gang wins Microsoft concessions, but fair software licensing group brands them 'stalling tactic', last accessed 18 July 2025. Last accessed 21 July 2026. ("*However, the agreement [between Microsoft and CISPE] has failed to remove the technical tie-in between Entra ID (formerly Azure Active Directory) and Microsoft 365, restricting users in their choice of ID management when deploying Microsoft software in the cloud.*")

III. CFSL agrees with the proposed investigation scope and candidate descriptions

28. CFSL agrees that each of the five proposed sub-activities relate to digital activities pursuant to the DMCCA.[41]

29. Moreover, each digital activity is linked to the UK, as (i) each activity has a significant number of UK users, (ii) Microsoft carries on business in the UK in relation to these activities and, given the global nature of Microsoft's business ecosystem, the way Microsoft carries on these activities is likely to have an immediate, substantial and foreseeable effect on trade in the UK.[42]

30. Finally, CFSL considers that it is possible and reasonable for the CMA to 'group' these activities. Not only can they be (and indeed, are) carried out in combination to fulfil a specific purpose; they are fundamentally architected by Microsoft to be consumed as a single, integrated package.

A. Microsoft 365 Copilot should be scoped into designation

31. CFSL notes that the CMA intends to investigate the extent to which Copilot forms part of the proposed designation scope. CFSL agrees that the CMA should conduct a thorough analysis of Microsoft's integration of its AI products into its business software ecosystem. Moreover, CFSL considers that the evidence already shows that Copilot should be designated with SMS as the dynamism of the AI-assistant layer does not cut against a finding of entrenchment, it confirms it. Based on the CMA's own guidance,[43] Copilot meets the test for designation.

    31.1. On the supply side, Microsoft offers Copilot as part of its productivity software suites and specifically advertises the inclusion of Copilot as being useful for work and productivity, even on its personal subscription plans.[44] Moreover, Copilot is not distinct from other productivity software in terms of (i) access points and branding, as it is branded as part of Microsoft 365[45] and primarily accessed via integration into Word, Excel, Outlook and Teams, or via Windows, or (ii) business models as Copilot

---

41 DMCCA, section 3(1). Last accessed 4 June 2026.

42 DMCCA, section 4. Last accessed 4 June 2026. CFSL notes that only one of these criteria need to be satisfied to prove a link to the UK.

43 DMCR Guidance at para. 2.10 (*"in identifying a digital activity and consider which of the firm's products it may comprise, the CMA will typically* ***look at how these products are offered and consumed****. For example, the CMA may consider* ***how the potential SMS structures itself and its business model, how businesses and consumers use and access its products*** *and any interlinkages among them*").

44 See Annex A.

45 For example, Microsoft brands Copilot as 'Microsoft 365 Copilot'. See eg. Microsoft, Organisations, What is Copilot, last accessed 21 May 2026.

is monetised the same way as other parts of Microsoft's business software ecosystem – ie. via subscriptions. Moreover, Microsoft itself confirms that Copilot enhances – and is enhanced by – its position within Microsoft's business software ecosystem, confirming that "*Microsoft 365 Copilot's accuracy and latency powered by Work IQ is unmatched, delivering faster and more accurate work-grounded results than competition.*"[46] Microsoft has also confirmed that Copilot's performance advantage derives from the Microsoft 365 data estate, which is itself the core of the Productivity Software Suite digital activity.

31.2. On the demand side, Microsoft confirms that Copilot is used by customers for "*boosting productivity*", "*document creation*", "*data analysis*", "*project management*" and "*communication*,"[47] all of which falls squarely within the scope of 'productivity'. Microsoft also describes the benefits of Copilot as "*business benefits*" and it is a power tool that "*redefines productivity by* "*streamlining tasks*"[48]– confirmation that Microsoft predominantly intends for Copilot to be used for business and productivity tasks.

31.3. Copilot should also be assessed by reference to the way productivity is evolving in modern workplaces. Business users increasingly use productivity software to create visual, branded and multimedia work outputs, including presentations, documents, internal communications, images, videos, campaign materials and other business content. These use cases fall within the ordinary meaning of 'productivity software' because they are used by organisations to communicate, collaborate, explain complex topics and produce commercial work products.

31.4. Finally, as Copilot becomes a primary interface through which organisational users discover, access, and use software functionality,[49] Microsoft will increasingly be able to influence how third-party providers conduct themselves and reach customers, reinforcing its position of strategic significance.

---

46 See comments by Satya Nadella, Microsoft CEO, on 28 January 2026. CFSL notes that the CMA has noted this evidence and that it may suggest that AI developments are likely to further entrench Microsoft's market power. See CMA Microsoft SMS Investigation Notice, para 27, last accessed 4 June 2026.

47 See eg. Microsoft Copilot, What is a copilot?, last accessed 21 May 2026.

48 Ibid.

49 See eg. AI Magazine, Is Microsoft AI the Ultimate Enterprise Trojan Horse?, 2 June 2026. Last accessed 3 June 2026. (*"Microsoft has been quietly pursuing a different strategy [to model development] - turning AI into an invisible layer that sits across the operating system, productivity suite and enterprise stack. [...] [Microsoft] is embedding intelligence so deeply into existing workflows that businesses may adopt an AI-first operating model without ever making a conscious platform switch. [...] Far from simply answering questions, the widely adopted Copilot can now perform multi-step actions inside Word, Excel and PowerPoint - acting more like a colleague than a digital assistant.*")

31.4.1. This is reflected in Microsoft's own product positioning. Microsoft describes Microsoft 365 Copilot as "AI built for work" and says it turns data into insights "in the apps you already know."[50] Microsoft also describes Work IQ as the intelligence layer behind Microsoft 365 Copilot and agents, using emails, files, meetings, chats and transactions to support the "flow of work."[51] Microsoft's Create experience within Copilot allows users to turn ideas into "designed content, videos, podcasts, or surveys", or edit existing content, using a prompt, template or company brand kit.

31.4.2. Microsoft's latest Copilot design materials further demonstrate that Copilot is being embedded directly into Microsoft 365 productivity workflows. Microsoft says the redesigned Copilot experience creates a single, flexible entry point across Microsoft 365 apps and surfaces relevant actions to help users in their work. Microsoft also says Copilot is evolving from a tool that responds to prompts within a single document into an experience that can take action, draw on broader work context and operate inside the apps where users already spend their time. It expressly refers to capability-focused agents including Designer, Researcher, Word, Excel and PowerPoint.

32. Copilot is therefore not merely an optional chatbot or peripheral AI service. It is increasingly positioned as the AI layer through which Microsoft users create, analyse, communicate and complete work inside the Microsoft 365 productivity suite. Copilot's integration into Microsoft 365 is therefore capable of extending Microsoft's market power across a broader set of productivity workflows. The CMA should treat Copilot as, first and foremost, a Microsoft-controlled productivity layer that can determine whether users remain within Microsoft surfaces or discover independent alternatives.

B. The CMA should confirm that GitHub, Visual Studio Code and GitHub Copilot form part of the relevant activities

33. CFSL supports the CMA including GitHub, Visual Studio, Visual Studio Code (**VS Code**) and GitHub Copilot as part of the digital activities designated with SMS, making the following points explicit:

33.1. First, the CMA should confirm that GitHub falls within the Productivity Software Suite digital activity, and consequently within the scope of any SMS designation. The ITC's definition of that activity is framed broadly around software that "*enables users to work and collaborate in an organisation, including to create, record, communicate and manage information*." GitHub satisfies each element of that definition in an enterprise context. Developers use it to create software, to collaborate through pull requests and code reviews, to record decisions and track how they work through issues

50 Microsoft, Microsoft 365 Copilot. Last accessed 2 June 2026.

51 Microsoft Tech Community, A closer look at Work IQ. Last accessed 2 June 2026.

and audit trails, to communicate through structured review and comment workflows, and to manage information through project planning tools. The case for inclusion is reinforced by GitHub's deep commercial and technical integration with the other products the CMA has already identified as within scope. All GitHub workloads are being migrated to Azure; GitHub Enterprise is bundled with Visual Studio subscriptions; and Azure DevOps usage rights are included within GitHub Enterprise licenses. Beyond these formal arrangements, CFSL members have documented a consistent pattern of Microsoft sales representatives offering GitHub at zero or heavily discounted prices within broader enterprise negotiations spanning Azure, Microsoft 365, and Copilot. As with other components of the Microsoft Productivity Suite, these commercial arrangements mean that the competitive dynamics of the developer and AI tools market cannot be adequately assessed, and conduct requirements in relation to them may be precluded or complicated if GitHub sits outside the scope of designation. Microsoft itself even confirms the critical role that GitHub plays within its ecosystem, and will continue to play in the future.[52]

33.2. Second, the CMA should also make clear that VS Code forms part of the 'Productivity Software Suite' sub-activity. VS Code is used by developer teams to 'create' software, collaborate on code and 'manage information' (eg. repositories). It therefore satisfies the functional definition for this sub-activity. Moreover, the definition of 'productivity software suite' is not confined – and must not be confined – to merely Microsoft 365 or O365 suites and the products contained within them. In fact, Microsoft bundles Microsoft 365 apps and the Microsoft 365 E5 suite into its VS Code suite subscriptions too.[53]

33.3. Third, GitHub Copilot is a product that is explicitly branded as Copilot, and is the most commercially significant 'Copilot product' for developers, with ~20 million users by July 2025 and Microsoft reporting in FY2024 that it had 1.8 million paid subscribers and over 77,000 enterprise customers. It is undeniably 'productivity software',[54] and is included within VS Code suite subscriptions. It should therefore be scoped into designation too.

34. Other authorities have recognised the competitive significance of Microsoft's ownership of GitHub in affording it privileged and lower-effort access to public source code repository

---

52 See eg, this speech by Satya Nadella at Microsoft Build 2026. ("*GitHub is not just about the code repo, it's becoming the control plane for all the [AI] agents [too]*)."

53 See eg. the Visual Studio Enterprise standard and Professional standard suites include Microsoft 365 E5 subscriptions. Last accessed 21 May 2026.

54 See letter from Satya Nadella to Microsoft shareholders dated 18 October 2024. Last accessed 21 May 2026.

data underpinning the development of GitHub Copilot.[55] Importantly, designation of these products would enable the CMA to assess CRs to address potential harms that CFSL sees as being likely to arise (and, indeed, may have already arisen); namely (i) Microsoft giving its own products an advantage versus rival AI coding assistants, including by giving GitHub Copilot privileged API access to VS Code; and (ii) deep integration with Microsoft's IAM tools, further strengthening Microsoft's gatekeeper role in authentication.

34.1. Microsoft gives GitHub Copilot privileged API access to VS Code that competing AI coding assistants cannot replicate. Microsoft's documentation explicitly states that third-party developers "*are not able to publish extensions using the proposed API on the Marketplace*." Nevertheless, the GitHub Copilot Chat extension uses these restricted APIs in production. Microsoft is therefore using control of one of its dominant software platforms (VS Code, which has over 70% market share in integrated development environments)[56] to advantage its own AI product (GitHub Copilot). This is no different to how it uses its control of Windows Server to unfairly advantage Azure, and requires a similar CR to be imposed.

34.2. Potential measures to resolve this harm could include (i) making available to competing AI coding assistants the same APIs, extension points and context window access that GitHub Copilot receives within VS Code, on equivalent terms and without delay relative to GitHub Copilot's own access; (ii) refraining from using its control of the VS Code marketplace to preference GitHub Copilot in search rankings, default settings or pre-installation; and (iii) publishing and maintaining documentation of all APIs available to AI coding assistant extensions, including any APIs currently designated as 'proposed' or otherwise restricted, so that competitors can develop functionally equivalent integrations.

IV. Microsoft has a position of strategic significance in each of the sub-activities

35. Given the evidence that the CMA cites in the Annex to the Investigation Notice,[57] it is uncontroversial that Microsoft has POSS in relation to each of the activities. It is beyond doubt, for example, that in respect of the digital activity (however it is ultimately defined), Microsoft has "*achieved a position of significant size or scale in respect of the digital activity*" or "*a significant number of other undertakings use the digital activity as carried out by [Microsoft] in carrying on their business*" (DMCCA, ss.6(a) and (b)). And while CFSL acknowledges that the CMA cannot pre-judge whether Microsoft has POSS, CFSL

55 See Bundeskartellamt, Decision under Section 19a(1) of the German Competition Act (GWB), Microsoft / Paramount Significance for Competition Across Markets, B6-26/23, 27 September 2024, paras 593–594.

56 See eg. Stack Overflow Survey 2025, which confirms that Visual Studio Code had ~75.9% market share in 2024. Last accessed 21 May 2026.

57 See CMA Microsoft SMS Investigation Notice, paras. 18 and 28. Last accessed 4 June 2026.

submits that the evidence from the Cloud MI confirms that this requirement for SMS is satisfied.

V. Microsoft has substantial and entrenched market power in each of the sub-activities; not just the grouped activity.

36. CFSL notes that the Investigation Notice confirms that the CMA considers that there are reasons to consider that Microsoft has substantial market power in relation to "*each of the digital activities*", in addition to the grouped activity.[58] CFSL is confident that an analysis of Microsoft's market power in each of the sub-activities will confirm that Microsoft has SEMP in these activities, and collectively the grouped activity.

37. The breadth of international findings against Microsoft, a selection of which the Investigation Notice references,[59] confirms its substantial market power, which has been entrenched and persisted over a long period of time. These findings span multiple jurisdictions, multiple legal frameworks, and multiple years. They confirm that Microsoft's market power is not a transient phenomenon produced by a temporarily successful product cycle — it is a structural feature of these activities that has persisted across different jurisdictions.

38. Over and above the evidence the CMA already cites as suggesting substantial market power, CFSL also notes that Microsoft cannot point to intense innovation as evidence that it faces competitive constraints – for example, in relation to the productivity software suite activity, Microsoft currently lists just 25 'changes' across the entirety of Microsoft 365 in 2026.[60] By contrast, Google Workspace lists 169 recent releases in 2026.[61] In relation to developer tooling, GitHub has publicly announced that it will prioritise migrating its infrastructure to Azure over new feature development, a strategic choice that reflects Microsoft's incentive to deepen GitHub's integration with Azure rather than invest in GitHub as a standalone competitive product.[62]

---

58 See CMA Microsoft SMS Investigation Notice, para. 22. Last accessed 4 June 2026.

59 See CMA Microsoft SMS Investigation Notice, para. 25. Last accessed 4 June 2026.

60 Microsoft 365, Microsoft 365 Roadmap. Last accessed 21 May 2026.

61 Google Workspace, What's new in Google Workspace (recent releases). Last accessed 21 May 2026.

62 The New Stack, GitHub Will Prioritize Migrating to Azure Over Feature Development, 8 October 2025. Last accessed 4 June 2026.

VI. The evidence confirms that Microsoft's position in the relevant activity is entrenched

39. CFSL agrees that CMA already has reasonable grounds to consider that Microsoft's position in relation to the digital activities is entrenched.

40. The CMA rightly acknowledges that Microsoft is well-placed to tie its AI capabilities to other products within its business software ecosystem, not least because Microsoft itself has confirmed "*the most important database underneath for any company that uses Microsoft today is the data underneath Microsoft 365*"[63]. The competitive significance of Copilot is not limited to the functionality Microsoft provides directly. As Copilot increasingly becomes the interface through which users discover, access, and execute workplace tasks, Microsoft gains the ability to influence whether users are directed toward Microsoft-native functionality or independent alternatives. This creates a risk of self-preferencing at the workflow-discovery layer, even where rival products remain technically available. This is a new, AI-specific switching barrier that compounds existing barriers.

40.1. Microsoft's AI capabilities are likely to reinforce existing switching barriers and further entrench Microsoft's position in workplace productivity software by extending its ecosystem into adjacent productivity activities. This risks raising barriers to expansion for independent providers, weakening competitive constraints and reducing customer choice. Copilot is not merely enhancing existing Office functions. It is increasingly becoming a Microsoft-controlled productivity layer through which users create, communicate, collaborate, analyse information and generate work outputs from within Microsoft 365.

40.2. This risk is particularly acute because Microsoft can combine AI functionality with its existing control over Microsoft 365 apps, work data, identity, permissions, SharePoint assets, Teams collaboration and enterprise administration. Indeed, Microsoft has confirmed that it intends to operate these all as a single system.[64] Microsoft's own materials position Copilot as operating in the flow of work and increasingly across Microsoft 365 apps.

40.3. Microsoft's own usage data illustrates the power of embedding Copilot directly into core productivity applications. Microsoft reports that, after rolling out new in-app Copilot experiences, Copilot usage increased by 27% in Word, 33% in Excel, 43% in

---

63 See CMA Microsoft SMS Investigation Notice, para. 27.

64 Microsoft, AI alone won't change your business. The system running it will, 2 June 2026. Last accessed 3 June 2026. ("*"Enterprises can't afford to assemble their agent strategy one piece at a time.* ***Disconnected tools stitched together after the fact can slow teams down and introduce unnecessary risk.*** *Building, contextualizing, running, governing, and improving agents should happen within one coherent system.* ***That's why we're bringing together Azure, GitHub, Microsoft IQ, Fabric, Foundry, Windows, Microsoft Security, and Microsoft 365 to operate as a single system*** *you can use to deploy agents at enterprise scale. Enterprises also need the flexibility to choose the right model for the task, balancing quality, speed, and cost — including Microsoft models, partner models, and open models"*)

PowerPoint and 30% in Outlook.[65] Microsoft notes that these figures reflect short-term usage changes and may not indicate long-term trends, but they nevertheless show how quickly usage can shift when Microsoft places AI functionality inside the apps where business users already work. This supports the need for the CMA to examine not only whether Copilot is bundled with Microsoft 365, but also how Microsoft's in-app defaults and workflow placement can expand Copilot adoption and reduce opportunities for independent providers to compete at the point of user choice.

40.4. Microsoft has also described Copilot functionality that supports PowerPoint presentation generation, branded templates, approved images, AI-generated images, designs, videos and other workplace outputs. The effect is that users may be able to perform a growing range of productivity tasks without leaving Microsoft-controlled surfaces. Where Copilot can generate documents, presentations, visual assets, branded content, videos and marketing materials from within Microsoft 365, independent providers may be excluded before users or organisations reach a meaningful point of choice.

40.5. This creates a new AI-specific switching barrier that compounds Microsoft's existing distribution advantages. Microsoft can make its own AI-enabled productivity and creation tools appear more convenient, more integrated and lower-friction than independent alternatives, regardless of whether those alternatives are more specialised or offer superior functionality.

41. Far from Microsoft market power in product areas like productivity software being *disrupted* by AI, Microsoft is actually well-positioned to *benefit* from the shift to AI. It has the ability to gatekeep which AI agents can interact with Microsoft's must-have business software, as described above at para. 20.4. It controls Agent 365, which will provide the future platform interface for choosing AI models. It has confirmed that GitHub[66] and Teams[67] are poised to become the critical layers for interaction with AI agents. As has been suggested in the specialist press, Microsoft may even require AI agents to have paid Microsoft 365 'seats', which would generate *more* revenue for Microsoft in the proposed designated activity area with the shift to agentic AI.[68] And Microsoft Azure AI Foundry

---

65 Microsoft, Introducing a new design for Microsoft 365, 28 May 2026. Last accessed 2 June 2026.

66 See eg, this speech by Satya Nadella at Microsoft Build 2026. ("*GitHub is not just about the code repo, it's becoming the control plane for all the [AI] agents [too].*"

67 See eg, this speech by Satya Nadella at Microsoft Build 2026. ("*Teams, in some sense, has become this destination for multi-player human-to-agent interaction. We want you to be able to find agents and interact with agents, right in Teams.*"

68 See eg. Business Insider, Microsoft exec suggests AI agents will need to buy software licenses, just like employees, 10 April 2026. Last accessed 4 June 2026.

(which features over 11,000 models)[69] vastly outnumbers Google Cloud (200+ models)[70] and AWS (100+ models)[71] in terms of model quantity, in effect acting as an aggregator for the entire industry. In other words, all the relevant indicia suggest that Microsoft's position in the relevant digital activity will be strengthened by the move to AI; not disrupted by it.

42. Independent analyst research further confirms the structural and self-reinforcing nature of Microsoft's market power. For example, AllianceBernstein has estimated that Microsoft's Desktop-as-a-Service offerings (Windows 365 and Azure Virtual Desktop) could generate an additional USD 14 to 38 billion in Azure annual revenue over the next three to five years, growing to USD 75 to 100 billion over the long term — potentially increasing Azure's long-term revenue opportunity by over 50%, excluding any upside from AI. Critically, customers moving to Desktop-as-a-Service cannot use OEM Windows licences obtained with a PC and must instead purchase packaged Windows licences, which are on average more expensive, and through cross-discounting practices incentives customers to purchase Microsoft 365.[72]

43. Finally, CFSL anticipates that Microsoft may argue that emerging AI-assisted coding tools are disrupting incumbent software architectures, reducing the relevance of traditional enterprise OS and RDBMS products. This argument would be misguided.

    43.1. First, AI-assisted coding tools accelerate new development but do not re-engineer existing enterprise applications. The lift-and-shift installed base of Windows Server and SQL Server workloads is not likely disrupted by AI coding tools, let alone within a five-year horizon. Even with the AI tools on the market, it remains a complex manual exercise to modernise applications, such that the emergence of AI tools will not erode Microsoft's SEMP any time in the foreseeable future.

    43.2. Second, GitHub, GitHub Copilot and VS Code are themselves Microsoft products. As described above, they are tightly integrated, with Github Copilot's market position being the result of an unearned advantage from privileged integration with Github and VSC. The growth of these products reinforces, not disrupts, Microsoft's developer ecosystem position. The growth in popularity of AI-assisted coding tools is likely to

---

69 Microsoft Azure, Foundry Models. Last accessed 21 May 2026.

70 Google Cloud, Model Garden on Gemini Enterprise Agent Platform. Last accessed 21 May 2026.

71 AWS, Supported foundation models in Amazon Bedrock. Last accessed 21 May 2026.

72 AllianceBernstein, Microsoft: The Windows desktop windfall for Azure, 13 September 2023, page 7. ("*To use any on-premise virtual desktop (eg. from Citrix or VMWare) or any Desktop-as-a-Service (from Microsoft or a 3rd party) one can not use an OEM license of Windows obtained with a PC. They need a packaged Windows licence plus they need to put that licence under some form of support (which they would get directly or with Microsoft 365*"), ("*While we do not know the blended price for Windows it is on average significantly lower [than] the packaged price of Windows*"), and ("*Thus, while companies that may be switching from either an on-premise virtual desktop solution or already have Windows via a commercial agreement will not pay more, companies that are moving from PCs with OEM Windows licenses (and do not own Microsoft 365) to Desktop-as-a-Service will likely pay more for their Windows*.")

increase, not reduce, dependence on the surrounding DevSecOps and infrastructure ecosystem. As AI increases code output, the bottlenecks move downstream into later stages of the software development lifecycle. This makes the platform that governs those downstream functions more important, not less.[73] Where one firm controls the coding surface, source code host, CI/CD workflow, security tooling and cloud environment, AI-assisted development can therefore deepen ecosystem dependence and raise switching costs rather than disrupt incumbent infrastructure.

43.3. Third, agentic AI systems operate on top of data and application infrastructure - they do not replace it. An AI agent that orchestrates enterprise workflows still depends on the underlying Microsoft business software applications as its data source and action environment. And the platform for building, deploying and scaling those agents will likely depend on which models are available to developers to use – as explained above, Microsoft's Azure AI Foundry contains a far greater quantity of models than its rivals.

VII. Conclusion

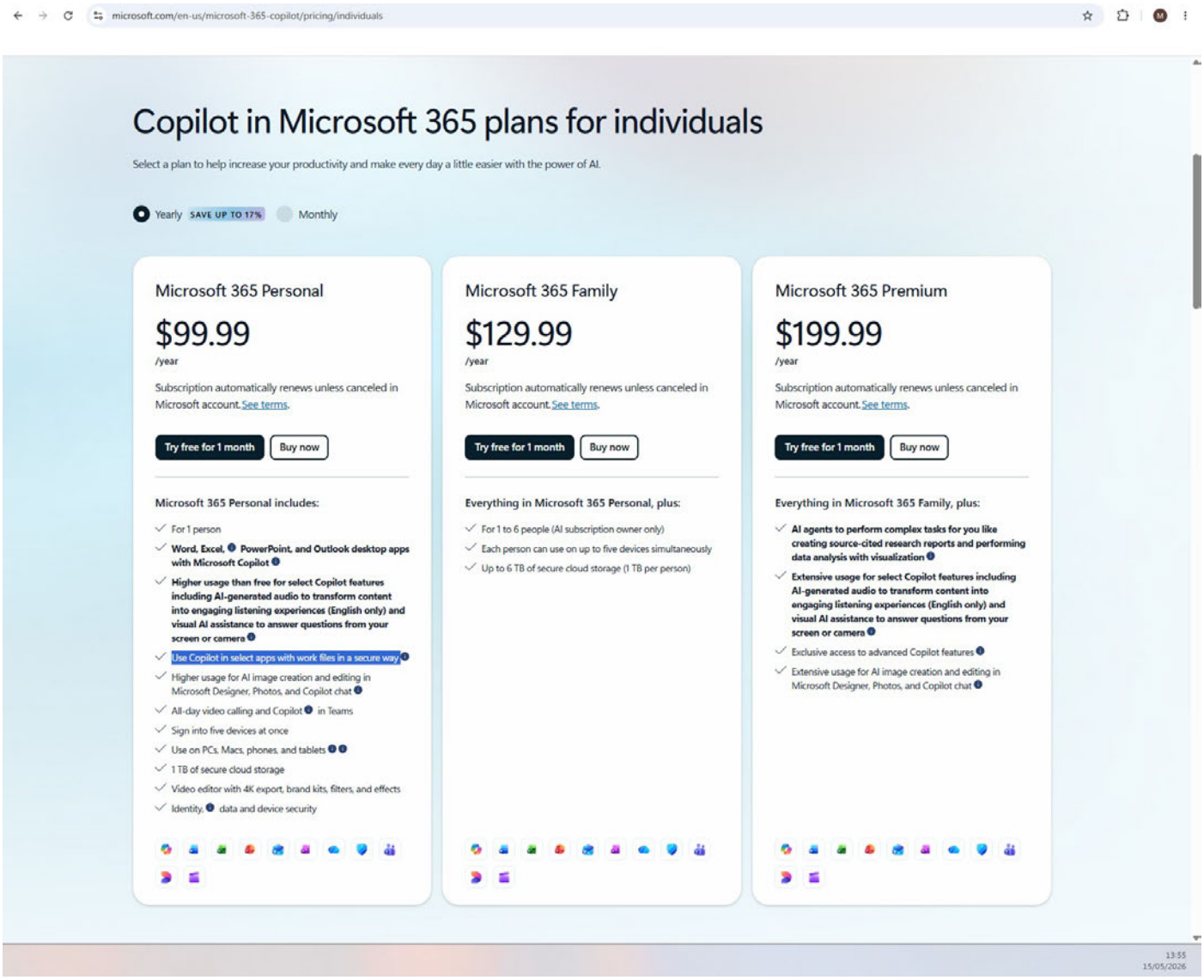
44. CFSL urges the CMA to designate Microsoft with SMS in relation to its business software ecosystem and to prioritise the imposition of mandatory CRs addressing Microsoft's licensing restrictions (including discrimination against 'Listed Providers'), bundling practices and interoperability barriers without delay.

45. The evidence – drawn from the Cloud MI, CFSL members' direct experience, and regulatory findings – confirms that Microsoft has SEMP in relation to its business software ecosystem, and that voluntary commitments are insufficient to remedy the identified harms. Swift and decisive intervention under the DMCCA is essential to maintain competition, protect UK customers, and ensure that the rapid growth of cloud and AI markets is not foreclosed by Microsoft's anticompetitive conduct.

---

73 See eg. AI Magazine, Is Microsoft AI the Ultimate Enterprise Trojan Horse?, 2 June 2026. Last accessed 3 June 2026. (*"Microsoft has been quietly pursuing a different strategy [to model development] - turning AI into an invisible layer that sits across the operating system, productivity suite and enterprise stack."* [...] *[Microsoft] is betting that enterprises will ultimately value governance, security and workflow integration more than the underlying model itself. In other words, Microsoft doesn't need to own the best model* ***if it owns the platform where AI work happens. Most enterprises already rely on Windows, Microsoft 365, Teams, Azure and Entra.***")

Annex A to CFSL's response dated 4 June 2026 to the Microsoft SMS ITC



Annex B to CFSL's response dated 4 June 2026 to the Microsoft SMS ITC

Coalition for Fair Software Licensing: Member Case Studies

Coalition members report facing significant barriers from Microsoft's control over both product bundling and technical integration. Companies describe arbitrary API restrictions and throttling limits that Microsoft's own products do not face. Members also highlight loss of major customers not due to inferior product quality, but due to Microsoft's bundled strategies creating cost pressures.

By eliminating competition, these practices weaken Microsoft's incentive to deliver high-quality security. This ultimately weakens security protection and diminishes economic gains for UK organisations despite technically superior alternatives being available.

Case Study: Company 1

Company background

This company provides cloud and network security solutions to UK customers, requiring API integration with Microsoft's products and infrastructure to deliver their security services.

Nature of the competitive harm

Microsoft's control over API access creates significant barriers to this company's ability to compete effectively:

Forced Migration to restrictive API: The company's cloud and network security products require API access into Microsoft's products and estate. Microsoft set an end-of-life date for the old API interface, forcing all customers to migrate by this date with no alternative. The new API imposes strict bandwidth thresholds and caps API call limits at 50,000 for licensed users, regardless of actual company size, disadvantaging larger customers. This company cited an example of a customer with 400,000 licensed M365 users receiving the same API call limit as a 50,000-user customer, despite paying for 400,000 licenses.

These APIs have specific bandwidth thresholds for traffic volume. This company quickly finds itself exceeding these bandwidth limits, at which point Microsoft tells customers they wouldn't experience these issues if they were using Defender instead. Microsoft's own solution does not appear to face such limitation, suggesting Microsoft either uses an unpublished API or is exempt from the limits it imposes on competitors.

Inadequate support and additional fees: This company was required to develop against an unstable interface that changed daily, with documentation issues requiring reverse engineering of functionalities. Progress on mitigating performance issues only occurred after directly connecting with a Microsoft software development engineer to rectify the issue - signalling that the company appeared to be stalling on addressing such issues without prompting. Additionally, Microsoft charges customers extra fees to unblock rate limits and enable deeper API connections. This means that customers are essentially required to pay additional costs to use a competitor's product while Microsoft's own solution bypasses these restrictions and feeds entirely.

Delayed fixes and security vulnerabilities: Microsoft acknowledged a critical bug in the new API, preventing the sending of collaboration actions for OneDrive and SharePoint, which is a core security feature. The estimated fix timeline of two to three months is an unacceptably long period for a security vulnerability in an advertised feature, and Microsoft's own CASB solution most likely does not face the same issue or delay.

Limited data access and opaque integration roadmap: This company cited that Microsoft restricted the types of API data provided and maintains an opaque roadmap for their integration into the Microsoft environment. This forces the company's teams to remain behind the

development of Microsoft's own solution in order to feed in most effectively, representing a covert means of keeping competition at arm's length.

Risk of complete access denial: If Microsoft were to take an even more aggressive position and shut off API access entirely, it would put this company's customers at immediate risk and create massive operational challenges.

Comparative experiences with competitor tools: This company noted that it experienced no product problems similar to the above with other providers' collaboration tools, such as Google's, suggesting a deliberate approach from Microsoft rather than technical limitations.

Main concerns

Performance degradation: Microsoft's API throttling undermines the company's ability to deliver the full value of its security solutions to customers, creating a competitive disadvantage stemming from Microsoft's gatekeeping rather than product quality.

Customer churn from bundling and throttling: Microsoft eliminated enterprise licensing discounts and forced migration to cloud agreements, driving up E5 prices and pushing customers toward Microsoft's bundled security. As a result, this company lost major accounts, including several Fortune 500 companies, which were forced to consolidate to Microsoft for budgetary reasons.

Customer vulnerability: Current and potential customers face reduced security protection due to Microsoft's artificial limitations on the third-party security tools' ability to function optimally within the Microsoft ecosystem. This company pointed to critical security features remaining broken for months while Microsoft prioritises its own competing solution.

Market consolidation risk: The erosion of third-party security tools reduces competitive pressure on Microsoft to maintain high security standards, potentially weakening the overall security posture of organisations relying on the Microsoft ecosystem.

Case Study: Company 2

Company background

This cybersecurity company provides endpoint security solutions for mobile platforms to customers in the UK, protecting against malware, human-factor (e.g. phishing, credential threats) and non-human factor vulnerabilities (e.g. agentic AI applications). The company serves 3,500 enterprise customers on subscription contracts, with the top 100 customers generating 80% of revenue.

Nature of the competitive harm

Microsoft's bundling and marketing strategy through its E3 and E5 licenses creates a ‘zero-price anchor’ that fundamentally distorts competition:

Zero-price bundling: Mobile security is included in Microsoft's E5 package, which many customers already possess. This creates the perception of a "free" product, making it extremely difficult for the company to compete even when its product is superior. For Microsoft, the bundled product only needs to be "adequate," whereas any competitor must be "dramatically obvious" in incremental value to justify additional expenditure.

Renewal pressure: While the company can successfully compete for net new business through RFP processes where they can demonstrate superior security capabilities, renewal decisions increasingly come from CFOs making top-down decisions based on cost savings rather than security performance. At renewal time, customers face pressure to simply save money by using what is already included in their Microsoft bundle, making it harder to justify the value proposition than during the original detailed RFP process.

Pattern of partner displacement: Microsoft appears to partner with companies when it lacks capability, builds basic-level features, then competes directly whilst edging out relevant partners.

Public sector mandates: Microsoft has aggressively marketed this bundling strategy to government customers, including in the US Department of Defense, which created an edict stating that if Microsoft sells a capability, agencies cannot purchase it from other vendors.

Main concerns

Customer churn from bundling: This company experiences a 6% annual churn rate, with all of this attrition attributable to customers switching to Microsoft's "free" bundled product. An example of this churn includes a former major customer for the company (with a 2024 revenue of over €23 bn), that acknowledged its superior security solution to Microsoft but cut the contract due to a mandate to reduce costs by 20%.

This approach has also forced the company to privately offer a ‘free’ version of its product with reduced capabilities at time of renewal to counter Microsoft, with the hopes of upselling in future, which customers have not adopted due to having product approval with a single vendor.

Innovation investment impact: This company operates R&D at 25% of revenue. All of the 6% annual loss, therefore comes out of the 25% spent on R&D. Microsoft's impairment of its ability to generate revenue directly impairs its ability to innovate and invest in product development, creating a downward cycle that undermines its competitive position over time.

Market-wide implications: The mobile security component is just one element of the E5 bundle, meaning multiple vendors across different security categories are experiencing similar competitive harm. The bundling strategy effectively sets a "minimally viable standard" that becomes the baseline for many customers, regardless of whether superior alternatives exist. Consequently, this creates vulnerabilities across the digital ecosystem.

Vendor consolidation pressure: Beyond the direct cost savings, Microsoft is able to quantify additional savings from vendor consolidation (reducing multiple contracts, simplified legal processes, administrative efficiency), which creates further pressure on customers to adopt Microsoft's bundled offerings even when third-party solutions are technically superior.

Case Study: Company 3

Company background

This cybersecurity company provides endpoint and network security solutions to customers in the UK. Their products operate through drivers that function within Microsoft systems.

Nature of the competitive harm

Microsoft is leveraging its control over critical system access points to disadvantage this company's security products in several ways:

Driver blacklisting and vulnerability categorisation: The company's drivers require Microsoft's permission to access and enable functionality within Microsoft's own systems. Microsoft has categorised certain vulnerabilities as "critical" or "severe" when by this company's assessment, they are routine issues. This disconnect between Microsoft's categorisation and the actual severity allows Microsoft to approach customers, claiming there are security issues with this company's products that wouldn't exist if they used Microsoft Defender instead.

Procedural opacity: Microsoft makes decisions about access and functionality in a vacuum and informs affected parties only after the fact, contrary to Microsoft's own published policies and procedures. There is no contractually binding language in these policies, preventing this company from seeking legal recourse.

Main concerns

Operational risk: If Microsoft were to take a more aggressive position and shut off access overnight, it would put customers at significant risk. Unlike cloud-based tools, endpoint-level solutions cannot be updated wholesale overnight or within a short timeframe, creating massive operational challenges.

Customer impact: This company tracks the speeds customers are experiencing and receives complaints, with the root cause traceable to Microsoft's practices. This degraded performance undermines the company's competitive position despite its superior security capabilities.

Market-wide security implications: The erosion of third-party security tools reduces Microsoft's incentive to remain at the forefront of security protection, making the entire ecosystem less secure. This is particularly concerning given current cybersecurity threats and the need for defence-in-depth strategies.

Bundling pressure: Budget-conscious customers are increasingly viewing Microsoft's bundled security offerings as "good enough" despite this company's winning on technical security features. Customers are foregoing third-party protection layers in favour of what's included in their Microsoft licenses.

Case Study: Company 4

Company background

The company is a cloud-based digital workspace platform that helps organizations in the UK deliver secure virtual desktops and applications to employees on any device, from anywhere. It hosts desktops and apps in public clouds, including Microsoft Azure and Google Cloud.

Nature of Competitive Harm

Microsoft's licensing restrictions have created significant competitive disadvantages for the company's cloud PC solution, limiting its ability to compete effectively against Microsoft's Azure virtualization offerings despite operating in the relative market longer than Microsoft.

When Microsoft revised its licensing terms in 2019 to restrict where its software could be deployed, it didn't merely update contract language—it materially reduced customers' freedom to choose where and how to run the software they had already purchased. Under the new framework, customers using on-premises licenses could no longer move those workloads to dedicated hosted cloud services operated by "Listed Providers" such as Amazon Web Services, Google Cloud, or AliCloud without paying for additional Software Assurance and mobility rights. In 2022,

In effect, Microsoft imposed a financial penalty on running its software anywhere but Azure.

These restrictions also function as anti-competitive barriers to the broader cloud market. By limiting where Windows and Office can be economically deployed, Microsoft constrains rival cloud providers' ability to offer competitive alternatives. Demand is redirected toward Azure not because it wins on the merits, but because Microsoft's licensing rules make moving to competitors structurally more expensive or less viable.

Main Concerns

Customer lock-in: The 2019 software policy change transformed licensing into a mechanism for steering customer behaviour. Rather than competing on price, performance, or security, Microsoft embedded provider preferences directly into its contracts and customers are now no longer free to select the best infrastructure for their needs; they are pushed toward Azure to avoid added costs and complexity.

The company noted that their largest customer was brought to them originally by Google Cloud, but because of the limitations of running M365 on Google Cloud, the company was forced to run the customer's workload on Azure.

Stifling Competition and Innovation: Competitors are effectively prevented from offering equivalent services for Microsoft workloads on shared or multi-tenant infrastructure. Even when rivals can match or exceed Azure on performance or price, customers face licensing penalties that neutralize those advantages.

The result is a market shaped by contract terms rather than competition. The company noted that 90+% of their customers run M365 today, which cannot be run on Google Cloud. As such, these customers are being filtered out as potential new customers for the company by Google Cloud field teams.

Case Study: Company 5

Company Background

A software company providing an AI-assisted software development product suite that competes directly with Microsoft's GitHub and GitHub Copilot. The company's products integrate with Visual Studio Code, the dominant developer environment globally, through the VS Code extension marketplace.

Nature of the competitive harm

Microsoft maintains over 150 internal "Proposed APIs" within VS Code, advanced programming interfaces that provide powerful functionality but that it restricts from use by third-party Marketplace extensions. Microsoft's documentation explicitly states that third-party developers "are not able to publish extensions using the proposed API on the Marketplace." Nevertheless, the GitHub Copilot Chat extension, available in the Marketplace, uses these restricted APIs in production. This constitutes a structural asymmetry that systematically advantages Microsoft's own AI coding assistant over competing products.

"Streaming" example. As one example of a specific technical challenge created by this API access restriction, the company's AI-assistant VS Code extension was initially able to achieve real-time streaming of AI responses through an engineering workaround. When you ask an AI coding assistant for help, instead of waiting for the complete answer, streaming shows you the response as it is being generated.] However, when Microsoft updated VS Code's underlying system, the workaround broke. Because the company does not have access to the relevant API, it could not justify rebuilding the workaround and had to drop the feature. VS Code users of the company's AI offering now have a noticeably degraded experience relative to users of GitHub Copilot. As a mid-sized company with limited engineering resources, the company cannot indefinitely invest in workarounds for APIs that Microsoft denies to third parties while granting access to its own products.

Beyond API access restrictions, Microsoft leverages its control of VS Code to steer user behaviour toward Copilot adoption through default UI placement. VS Code contains easily accessible Copilot buttons embedded directly in its interface and actively prompts users to adopt Copilot features, while competing extensions must be independently discovered, installed, and manually configured. This default placement advantage operates independently of API access restrictions. Even where third-party integrations are technically possible, Microsoft's control over onboarding flows and UI prominence in VS Code materially skews developer adoption toward Copilot.

In October 2025, GitHub announced 'Agent HQ,' framed as a platform broadening third-party coding agent choice within GitHub. However, the announcement simultaneously disclosed that Copilot Pro+ users would be able to work with select partner agents directly within the VS Code editor itself, making Copilot the first and privileged entry point for in-editor agentic

workflows. Here again, an announced interoperability measure preserves Copilot's structural advantages within the VS Code environment.

Main concerns

Platform control used to advantage a first-party product. The API restrictions fundamentally advantage Microsoft's own products operating in its own, widely-adopted Integrated Development Environment. Microsoft's stated justifications for proposed API restrictions and other technical barriers typically invoke stability concerns and the need to preserve flexibility for future changes. However, Microsoft's own products appear to use these APIs in production environments serving millions of users, which indicates the barrier is a policy choice rather than a genuine engineering constraint.

Fragility of workaround-dependent competition; resource asymmetry falling disproportionately on mid-sized competitors. In order to approach technical parity operating in the VS Code environment, competitors must invest time and resources in engineering workable solutions. These solutions may be deprecated or "broken" without warning when VS Code updates, putting smaller competitors at a consistent disadvantage in their ability to offer competing products within the VS Code environment.

Limiting consumer choice. Developers using VS Code may face a meaningfully skewed choice of coding assistants because competitors cannot access foundational APIs that make GitHub Copilot work seamlessly. Even where third-party integrations are technically possible, Microsoft's control over default placement, onboarding flows, and UI prominence in VS Code materially skews developer adoption toward Copilot, effectively skewing user choice in their favour.