Cloudflare Response to CMA Invitation to Comment on its Strategic Market Status Investigation into Microsoft's Business Software Ecosystem
June 2026

Cloudflare welcomes the opportunity to respond to the CMA's Invitation To Comment (ITC) on its Strategic Market Status investigation into Microsoft's business software ecosystem.

Executive summary

Cloudflare supports the CMA's goal of achieving a competitive business software market that does not improperly leverage market dominance to affect adjacent markets. This goal requires the CMA's investigation to take into account the interconnection of the business software ecosystem and related cloud services. To assist the CMA in its investigation, this submission identifies factors that will help accomplish a competitive business software market; describes the interconnection between business software markets and adjacent cloud service markets; and gives examples of anti-competitive practices observed by both us and our customers that demonstrate why including relevant cloud services in the proposed scope of investigation and potential interventions is appropriate in this case. We welcome further discussion with the CMA on any of these issues.

1. **Background on Cloudflare**

Cloudflare is a connectivity cloud provider that empowers organisations to make their employees, applications and networks faster, more resilient and more secure everywhere, while reducing complexity and cost. We provide a comprehensive suite of cloud based and cloud related services through our global network, which spans more than 335 cities in over 125 countries. More than 20% of the web sits behind Cloudflare's network. Cloudflare's services include protection of public applications and APIs from exploits and automated bots, safeguarding corporate infrastructure against network-level DDoS attacks, securing employees and corporate data via Zero Trust access controls and advanced email security, and developer platforms that run application code and data storage within a highly secure, serverless environment. Critically, all of these services run on our own infrastructure and not on any other hyperscaler cloud platform, providing architectural independence that allows Cloudflare to bypass hyperscaler markups, optimize power efficiency, and deploy our tailored software for web security, caching, and edge computing.

Given our position within the ecosystem, we interact with Microsoft and other hyperscalers both directly and indirectly through our customers who rely on Microsoft business software and other adjacent products. This perspective allows us to provide unique insights based on our own experience and the experience of our customers.

2. **The scope of the CMA's investigation should remain broad to help encourage the creation of a competitive market**

As we have previously described, Cloudflare strongly feels that businesses and consumers should be able to choose the best cloud services – including services offered and consumed within

hyperscaler cloud infrastructure – for their needs. That means they should be empowered to evaluate offerings and use services from a range of providers. Allowing customers to connect their data between apps, data, devices, networks, and clouds in a fully interoperable and cost effective way provides security, performance, and competition benefits for the entire market.

a. The desired competitive end state for the CMA's investigation and interventions.

To assess the proper scope and proposed remedies for the CMA's investigation, it is useful to lay out what a competitive business software ecosystem would look like. We believe a competitive business software ecosystem has the following characteristics:

- **Customers can unbundle**. A customer who buys productivity software should be able to choose different providers for identity, for security, for storage, and for emerging categories such as AI agents — without giving up the value of the software they have already purchased. The freedom to take pieces of the stack from different providers, on commercially viable terms, is what makes a market work.
- **Interoperability**. Files, identity, classification labels, traffic, and policy state should flow across providers on neutral terms. Where one vendor's design choices determine whether another vendor can connect at all, the market does not function as a market.
- **Customers purchase individual services on their merits**. A company should win the customer because it offers the best service for the customer's problem — not because it was already paid for inside a bundle, or because the credits the customer has already committed only redeem in one direction as a result of marketplace rules.

By contrast, vendor lock-in and uncompetitive bundling practices make it near impossible to mix and match competitive offerings across different organizations. This reduces market availability, competitiveness, and interoperability both for business software products and adjacent activities and services in the cloud.

We welcome that the CMA's own framing of healthy competition in the business software ecosystem captures a similar desired end-state: customers should be able to "negotiate good deals and use the best products for their needs" and "combine products and applications from a range of providers as well as Microsoft to meet their particular needs," so that "a wide range of companies can win customers if they offer a better deal or more innovative product, supporting investment and growth for the UK."[1]

We therefore support the CMA continuing to focus its investigation on enabling this end state for customers and companies, and believe the scope of the investigation should be defined by a primary criterion: whether it effectively assesses if customers have genuine alternatives across their integrated cloud and software stacks to enable this end state.

b. The scope of the investigation must account for the integrated nature of cloud markets and the broader impacts of market dominance in the business software ecosystem

[1] CMA invitation to comment, pg 2, para.3

Where a practice in an adjacent service or activity is the mechanism through which business software dominance is extended or defended, that practice belongs in the scope of this investigation.

Accordingly, we support the proposed broad scope of the CMA's digital activities descriptions, which spans business software, productivity software, operating systems, database management and related identity access and security software. We also strongly agree with the ITC's identification of "preventing the leveraging of market power into adjacent activities, such as cloud services," (concern a) and "ensuring that commercial arrangements like bundling do not distort customer purchasing decisions" (concern c) as key areas of concern that the investigation, and any conduct requirements or other interventions that might result, should address.

A broad scope is particularly vital when evaluating the business software ecosystem. Market status in business software must be understood and evaluated as part of a single intertwined ecosystem, where dominance in one market (such as business software) can be extended to build dominance in the next market (such as cloud computing). Market position and anti-competitive practices in business software inherently extend through an integrated combination of cloud services that are deeply interconnected. We and our customers frequently observe three primary practices that drive expansion into adjacent products and markets:

- **Unfair commercial terms** (such as marketplace rules and committed spend) that unfairly disadvantage third party cloud services vendors;

- **Technical design choices** (such as restricting third-party security tool traffic inspections or locking data tagging behind tier upgrade requirements) that create barriers to third-party cloud service provider interoperability; and

- **Bundling** that forecloses choice in adjacent and emerging areas, including in particular bundling of cloud security tools and emerging agentic AI offerings.

Viewed in isolation, any of these practices has an anti-competitive effect. But together, they can create a compounding dynamic that no single practice would achieve alone. That is why it's necessary to include them in this investigation. If the CMA evaluates these market practices independently – or worse, excludes any of them from the scope of its investigation – it could risk missing the true scale and strategic significance of an entity's market power in the business software ecosystem, including in relation to their market power in adjacent markets.

As a result, the CMA should ensure that digital activities that fall within the three categories mentioned above, including the listing of software within the Azure Marketplace and cloud-based security and identity management offerings, remain within the scope of its investigation.

3. The CMA should consider commercial terms, technical barriers, and bundling in its investigation

The three practices mentioned above - unfair commercial terms, technical barriers, and bundling -- distort competition in business software and adjacent markets. Because of the impacts on business

software lock-in, interoperability, and customer choice, the CMA must target all three practices and the impacted services within the scope of its investigation.

a. Unfair commercial terms (such as marketplace rules and committed spend) that unfairly disadvantage third party cloud services vendors

Distribution channels for business software – like marketplaces – should operate as neutral gateways that allow customers to choose the best solution for their needs regardless of infrastructure. When a company controls the primary marketplace through which complementary products reach customers, it should not be able to use that control to favour its own services and infrastructure over competitors, including through terms that regulate marketplace rules, default settings, or pricing visibility. Otherwise, that dominance can turn a distribution channel into a foreclosure mechanism.

b. Technical design choices (such as restricting third-party security tool traffic inspections or locking data tagging behind tier upgrade requirements) that create barriers to third-party cloud service provider interoperability

One vendor's design choice should not be allowed to preclude another vendor from offering a customer the product it needs. Customers should be able to choose the security tools that best fit their needs, across every layer of their infrastructure. When a dominant vendor uses technical design to prevent third-party tools from inspecting or auditing its traffic or accessing its features, it extends its market power beyond the software itself.

c. Bundling that forecloses choice in adjacent and emerging areas, including in particular bundling of cloud security tools and emerging agentic AI offerings

Security products should be evaluated and purchased on their individual merits — their effectiveness, cost, and fit with a customer's existing set of tools. When a dominant vendor includes security services in a software suite that customers already licence for other purposes, it bypasses that evaluation process entirely, giving it an unfair competitive advantage. While we appreciate accessible security tools that improve cyber resilience, dominant providers shouldn't be able to use bundling to restrict customer choice and engineer vendor lock-in to gain a competitive advantage in other relevant markets. Customers end up using security tools they never chose, while rival providers face competitive barriers regardless of the quality of their products. Customers should always have the freedom to purchase individual cloud security tools that meet their needs, particularly in rapidly evolving fields like agentic AI security, without being forced into less comprehensive or unwanted products simply because they are tied to a bundle.

4. Possible interventions the CMA should consider as part of its investigation

As the CMA considers proportionate, conduct-focused interventions that would respond to the its stated concerns, the CMA should include exploration of the following possible interventions in the scope of this investigation:

- **To address concern (a) - leveraging power in adjacent activities.** Marketplace listings and the redemption of prepaid customer commitments should be infrastructure-neutral. Cloud providers should not be allowed to preference business software partners that only build on their infrastructure, whether through marketplace access or committed spend discounts. The operator of a marketplace tied to its own infrastructure also should not have visibility into independent vendors' commercial terms, especially in a way that places those vendors at a structural disadvantage when competing against the operator's own offerings.

- **To address concern (b) - technical design and interoperability.** Cloud providers should make their security features interoperable with third-party providers. Where a dominant business software provider's technical design choices determine whether third parties can interoperate – including in encrypted traffic inspection, in classification and labelling, in identity routing, or other activities – those design choices should be opened to third-party interoperability on neutral, documented, and stable terms. The aim would not be mandating any particular technical architecture, but instead ensuring technical design choices are not used as an instrument of exclusion. Ultimately, where a customer wants to use an independent third-party tool alongside the business software they purchase, the design of that business software should not, itself, prevent them from doing so.

- **To address concern (c) - bundling.** Security, identity, and emerging-category services bundled into business software suites should also be available as standalone purchases that are transparent and at fair market value, rather than being bundled below cost with existing products in markets where hyperscalers already have a dominant position.

5. Conclusion

To foster healthy competition in the business software ecosystem, and to ensure the CMA appropriately addresses the full scope of how dominance in the business software ecosystem extends into and impacts competition in adjacent markets, including cloud services, we recommend that the CMA:

- Maintain the proposed broad scope of its investigation and proposed definitions of covered activities.

- Account for the interconnected nature of the business software ecosystem and related cloud services and markets by ensuring the investigation includes consideration of related cloud services within its scope.

- Implement the interventions listed above, which are all focused on ensuring the healthy competitive end state we have set out at that start of this submission.

We welcome further discussion with the CMA on any of these issues.