Response to the Competition and Markets Authority (CMA) Strategic Market Status Investigation into Microsoft's Business Software Ecosystem

Submitted by: Mosaic Island Ltd

Version 1

15th May 2026

Mosaic Island Business Context

Mosaic Island is a UK-based boutique technology consultancy supporting clients with their technology architecture and digital transformation needs. Our current and past clients include:

In our last Financial Year ending 31 July 2025, our turnover was £14.1m, with a net margin of £0.5m.

Our organisation has 26 employees. For our client facing technology professional services in addition to our employees, we engage associates (contractors) for specialist architecture related services (~60 associates currently engaged.)

Our IT must meet the needs our business (enterprise functions), and the needs of our clients and adapt to consultancy delivery to the business productivity tooling of their

choice. We also hold Cyber Essentials and ISO 27001 certification – so our IT must support the security controls of our Information Security Management System.

Our Experience / View on Microsoft Business products

From our experience both as a Microsoft customer and as Consultancy advising our clients, we believe there are significant interoperability and customer lock-in concerns within the ecosystem.

The Microsoft ecosystem increasingly creates technical, financial and operational barriers that make it difficult for organisations, particularly SMEs, to adopt alternative products, operate mixed environments, and optimise costs.

The following observations reflect our direct operational experience.

1. Customers are Locked into a Microsoft-Controlled Operating Model

A significant concern is that Microsoft forces customers down specific architectural and operational paths with limited practical alternatives.

For example:

- Device management and compliance workflows strongly favour full Microsoft Intune enrolment and Microsoft-native controls.
- Alternative approaches (such as lighter-touch BYOD controls, third-party security tooling, or application protection-only models) are either poorly supported or operationally unreliable.
- Microsoft's ecosystem often appears technically capable of supporting interoperability, but functionality is intentionally restricted unless customers adopt Microsoft's preferred stack end-to-end.

In practice, organisations are frequently faced with a choice:

- adopt Microsoft's full ecosystem "the Microsoft way", or
- accept degraded functionality, reduced visibility, and operational friction.

This creates substantial barriers, increased costs, and operational setup and maintenance overhead.

2. Microsoft's Licensing Structure Has Become Increasingly Complex, Fragmented and Anti-Competitive

We have observed increasing fragmentation and unpredictability in Microsoft licensing.

Examples include:

- functionality unexpectedly requiring additional standalone licences;
- overlapping licence entitlements that do not behave consistently;
- licensing changes impacting existing deployments without adequate notice;
- products bundled in ways that encourage customers to expand Microsoft dependency rather than evaluate alternatives.

A practical example from our operations involved Microsoft Intune/device compliance functionality behaving inconsistently across devices unless additional standalone Intune licensing was purchased, despite core functionality ostensibly being included within existing Microsoft 365 licences.

This creates:

- unnecessary additional cost;
- increased administrative overhead;
- confusion for SMEs without dedicated Microsoft licensing specialists.

The complexity of Microsoft licensing increasingly disadvantages SMEs that lack enterprise resources and budget to scale their deployment to Microsoft's ecosystem complexity.

3. Interoperability with Non-Microsoft Security and Productivity Tools Is Poor

Microsoft's ecosystem frequently favours Microsoft-native tooling and creates operational friction when organisations attempt to use alternative vendors.

For example:

- Microsoft security tooling is optimised for Microsoft Defender and Microsoft-native identity/security services.
- Organisations using third-party tools (such as Bitdefender or alternative endpoint/security platforms) encounter reduced integration capability and inconsistent management experiences)
- We operate both Windows and OSX laptops. We have recently decommissioned our JAMF MDM tooling for OSX laptops and moved it to Microsoft Intune MDM because of Microsoft led restrictions
- Reporting and compliance data are often siloed or difficult to access unless additional Microsoft tooling is purchased.

This creates a commercially coercive environment where customers are encouraged to consolidate further into Microsoft products, even where alternative tools may be better suited, more cost-effective or preferred.

4. AI Capabilities Risk Reinforcing Existing Market Dominance

The integration of Copilot into Teams, Outlook, Microsoft 365 and other collaboration platforms creates a strong ecosystem lock-in effect because:

- competing AI providers cannot access equivalent native integration points;
- Microsoft benefits from privileged access to workplace context, collaboration metadata and productivity workflows;
- organisations may be forced into duplicate spending on AI platforms.

As an example:

- our business currently uses both ChatGPT and Microsoft Copilot; Microsoft-native capabilities such as Teams meeting integration are only available effectively through Copilot
- ChatGPT deliver equivalent functionality despite offering superior AI capability in other areas. We are forced to procure CoPilot and ChatGPT. The additional cost our business is £3k per annum (and rising) due to overlapping AI capabilities.

This creates an uneven competitive environment where platform ownership determines AI capability access.

We believe interoperability requirements should ensure that:

- customers can use alternative AI assistants across Microsoft collaboration platforms;
- meeting recordings, productivity context and workplace data can be securely accessed by competing AI providers where customers choose;
- AI functionality is not unfairly tied to Microsoft productivity subscriptions.

5. Operational Transparency and Change Management Are Poor

Microsoft frequently introduces changes that materially impact customers without sufficient transparency or operational communication.

Examples include:

- licensing changes;
- changes to application behaviour;
- modifications to management tooling.

While software evolution is expected, the issue is the lack of proactive impact communication and the operational burden placed on customers and IT teams.

For SMEs this creates disproportionate operational overhead because:

- IT teams must continually investigate unexpected behavioural changes;
- reporting and compliance baselines become unreliable;
- significant time is spent diagnosing ecosystem inconsistencies rather than delivering business value.

6. Reporting and Administrative Tooling Are Fragmented and Inefficient

Microsoft's reporting ecosystem is fragmented across multiple admin centres, APIs and licensing layers.

We have experienced:

- inconsistent reporting data;
- stale or delayed device/compliance information;
- limited out-of-the-box operational reporting appropriate to SMEs

Even relatively straightforward operational reporting often requires:

- specialist expertise;
- additional licences;
- custom integration work.

This creates unnecessary operational complexity and disadvantages SMEs that lack dedicated / sufficient engineering resources across the Microsoft stack

7. Mid-Sized Organisations Are Particularly Disadvantaged

In our view, Microsoft's ecosystem works relatively effectively:

- for very small businesses using mostly default settings; and
- for very large enterprises with specialist Microsoft engineering teams and substantial budgets.

However, mid-sized organisations are disproportionately impacted because they:

- require enterprise-grade governance and security;
- lack the budget and internal resource of large enterprises;
- must absorb increasing licensing and administrative complexity.

This creates a “middle market gap” where organisations are operationally dependent on Microsoft, have complex IT needs, but lack realistic flexibility or negotiating leverage.

Our Recommendations to the CMA

We encourage the CMA to consider remedies focused on:

1. Interoperability obligations - Require Microsoft to support equivalent interoperability for third-party AI, security and management tooling.

2. Licensing transparency - Prevent anti-competitive bundling and require clearer disclosure of licensing dependencies and functional limitations.

3. AI platform neutrality - Ensure customers can use competing AI providers within Microsoft collaboration and productivity environments.

4. Administrative and reporting openness - Improve access to operational and compliance data through standardised APIs and reporting interfaces.

5. Fair BYOD and device management support - Prevent Microsoft from technically disadvantaging non-Microsoft or mixed-management approaches.

Closing Statement

Microsoft products are deeply embedded across UK businesses and public sector organisations.

For many businesses, Microsoft is mission critical.

This makes interoperability, openness and fair competition critically important.

From our experience, the Microsoft ecosystem increasingly creates technical, operational and commercial incentives that encourage customers toward deeper dependency on Microsoft products and services (the gravity draw of the “Microsoft” black hole towards increasing dependence and cost), while making alternative approaches more difficult, costly and operationally risky.