



By: Tomorrow's Affairs Staff

# Microsoft sells both Windows and its security, and the UK regulator is now investigating it



On 16 October, the UK Competition and Markets Authority (CMA) proposed granting **Microsoft** the status of a company with strategic market power in business software. The proposal covers Windows, Office programmes, Windows Server, SQL Server and cybersecurity software.

More than a million British businesses and public institutions rely on Microsoft products, with around 20 million monthly users. The **public consultation** runs until 13 November, and the regulator must decide on the status no later than 13 February 2027.

Media attention has focused on the possibility that Microsoft is tying Copilot to programmes that customers already use, but the October document also raises a serious question about the position of competing cyber-protection providers.

Microsoft develops the operating system, determines how other programmes access its core components and simultaneously sells its own protection. Its advantage in that market may come from a high-quality product, favourable contracts or technical rules that it sets for itself as the platform owner.

The British regulator is gathering evidence on how bundling Microsoft's products and setting terms of access to its systems may restrict competition. If the CMA confirms that status, Microsoft will be treated in Britain as a company so powerful in the market that special rules apply to it.

The regulator could order it, for example, to sell security software separately from the office suite at a transparent price, or to give competing security providers the same access to Windows as Defender has.

If Microsoft breaches such obligations, fines can reach 10 per cent of its worldwide turnover. The status itself is not a punishment and does not mean that Microsoft has broken the law to date.

## The Office contract already

## includes protection

Microsoft 365 E5 is a package for large organisations that adds security services alongside Office programmes. Defender detects attacks and malware, Entra manages access to data and Intune enables monitoring of office computers and phones.

From 18 November 2025, Microsoft gradually began including Security Copilot, its artificial intelligence programme for security teams, with a monthly usage limit for E5 users. It benefits an organisation to obtain email, computers, employee accounts and their protection from a single supplier.

The price list shows why customers cannot easily calculate how much they are paying for this protection. As of 1 July 2026, the **E5 package with Teams** in the US costs \$60 per user per month, and the cheaper E3 package costs \$39. The \$21 difference covers security services as well as other extras, and Microsoft does not say how much of that relates specifically to protection.

### The CMA concluded that Microsoft's licensing terms made it difficult for users to switch to competing providers

A business that already pays for E5 and wants protection from CrowdStrike or SentinelOne would effectively be paying for protection twice, with the added cost of connecting the new programme to the existing system. The CMA is investigating whether such package ties customers to Microsoft's protection.

The procedure has a long history. In July 2025, following an investigation into the cloud services market, the CMA concluded that **Microsoft's licensing terms** made it difficult for users to switch to competing providers.

In March 2026, it announced a broader **investigation** into Microsoft's business software, which formally began on 14 May 2026.

In the October document, the CMA also lists specific complaints from competitors. They claim they receive the data needed to detect attacks later and to a lesser extent than Microsoft's programmes do. They also complain that Microsoft limits how often their programmes can download data from its systems.

In addition, many Microsoft services rely on Entra ID, a system for managing employee accounts, so a business that uses it can hardly entrust its protection to someone else. The regulator has yet to verify these claims.

## CrowdStrike has shown how deep those rules go

In July 2024, a faulty update to the CrowdStrike Falcon security programme brought down approximately 8.5 million **Windows PCs**, according to Microsoft's estimates. Passenger check-in systems at airports, banking services and healthcare operations were disrupted.

The bug originated in a third-party programme that had access to the Windows core, the part of the operating system that manages the computer's most important functions. A programme with such privileges can detect a dangerous process very early, but a serious error in it can stop the entire computer.

After the incident, Microsoft pointed in the media to a 2009 competition agreement with the European Commission. The company argued that it had accepted an obligation to allow security software manufacturers access to certain parts of Windows under conditions comparable to those applying to its own products.

Microsoft's October 2009 announcement lists the availability of software interfaces used by its security products. The European Commission rejected the claim that the agreement was responsible for the outage.

## After the CrowdStrike crash, Microsoft began changing how security programmes work on Windows

A Commission spokesperson told Euronews that it was up to Microsoft to adapt its **protection** to new threats while respecting competition rules. They added that Microsoft had never raised any security objections to the 2009 agreement with the Commission, either before or after the system crash.

The dispute over how the agreement should be interpreted remains important today. The 2009 documents oblige Microsoft to give competitors access to parts of Windows used by its Defender, but they do not make clear whether this includes permanent access to the core of the system itself.

After the CrowdStrike crash, Microsoft began changing how security programmes work on Windows. In November 2024 it launched the Windows Resiliency Initiative, and on 18 November 2025 it announced that a new security programme platform, called **WESP**, was already being tested with selected partners and would be more widely available in 2026.

Security programmes would run on it outside the Windows core, so their errors would be less likely to bring down the entire computer.

This would reduce the risk of another crash like the one in 2024. It remains to be seen, however, whether competitors on the new platform will be able to detect and stop attacks as effectively as Microsoft Defender.

Microsoft itself determines what security programmes on Windows are allowed to do, so any such change affects its competitors as well.

The British regulator has not opened a separate investigation into Microsoft's new platform for security programmes.

To date, there is no evidence that Microsoft

gives its competitors fewer options than it gives its own Defender.

## Microsoft also failed to protect its own systems

Relying on a single supplier carries significant risk. In April 2024, the **US Cyber Safety Review Board** released a report on how the Chinese group Storm-0558 hacked the emails of US government officials in 2023, including then Commerce Secretary Gina Raimondo.

The attackers obtained a Microsoft digital key and used it to create fake credentials that Microsoft's system accepted as genuine. The board identified multiple security failures and concluded that the company's security culture was inadequate.

**The intrusion was discovered by the State Department because it was paying for Microsoft's more expensive G5 licence**

The intrusion was discovered by the State Department because it was paying for Microsoft's more expensive G5 licence, which records who accessed mail and when, and has its own alert system.

The Department of Commerce did not have those records, so it could not easily determine what the attackers had accessed. Following this, on 19 July 2023, Microsoft announced that it would provide such records free of charge to more users.

The case shows that the ability to detect the attack in the first place depended on how much the customer was paying Microsoft. It does not prove that a competing security programme would have prevented the intrusion.

It does show, however, why independent protection must receive complete data in time, especially when the failure is caused by the provider itself.

## The European dispute over Teams offers a model solution

In September 2025, the **European Commission** accepted Microsoft's commitments in the dispute over Teams, which the company had sold together with its Office programmes.

Microsoft has undertaken to offer bundles without Teams to customers in the EU, Norway, Iceland and Liechtenstein, with a larger price difference between bundles with and without Teams than before.

Microsoft has also promised to make it easier for competing business communication programmes to connect to its services. Customers who do not want Teams can now finally see how much they are paying for it.

The same approach could be applied in Britain to protection in the E5 package. Microsoft already sells a set of Defender Suite security programmes as an add-on to the cheaper E3 package, as well as some security programmes separately.



*CMA chief executive Sarah Cardell (right) highlighted Microsoft's long-standing, strong position in the UK market and the need for organisations to be able to combine products from different suppliers freely*

It does not help the E5 buyer, though, because they would have to keep everything else in the package, exclude Microsoft's protection, buy another provider's product and pay less.

Competitors' access to Windows and security data is harder to manage, because each such

change must be assessed from the point of view of the security of the system itself.

Microsoft responded that it disagreed with the CMA's assessment and that its products, including Copilot, can be connected to competing services.

CMA chief executive Sarah Cardell highlighted Microsoft's long-standing, strong position in the UK market and the need for organisations to be able to combine products from different suppliers freely.

The CMA will now examine whether a business that chooses third-party protection actually receives all the data and functions it requires.

## Status decision by February, measures not yet chosen

The CMA must decide on Microsoft's status by 13 February 2027. The regulator is still gathering evidence on security software. In its October plan, the CMA mentioned possible changes to how packages are sold and to equal access to data, but it has not yet chosen any measures.

Each obligation would undergo further assessment and public consultation after the status decision, so the first changes are unlikely to take effect before the second half of 2027.

**If it decides to intervene, the CMA will most likely start with pricing and packages**

If it decides to intervene, the CMA will most likely start with pricing and packages, where it already has the precedent of Teams. It will leave access to Windows and security data for later, as that requires technical checks.

Microsoft will probably try to pre-empt formal measures with its own offer, as it did in Brussels.

What will be crucial for customers is how much they can save if they buy protection from another supplier and whether that supplier will receive the same data as Defender.

That will determine whether they choose protection based on its quality or based on the contract they already have with Microsoft.