Microsoft's Windows 365 cloud OS hints at shift away from hardware partners

Article

The news: Microsoft announced its **Windows 365** service, a virtual Windows PC running on Microsoft's cloud.

How it works: Subscribers to Windows 365 can access a Windows 10 or Windows 11 desktop using a web browser on virtually any connected device including PCs, Macs, iPads, Android devices, and even Linux PCs, per The Verge. Windows 365 stores information in the cloud, not on the device, and **encryption is used across the board.** All managed disks running cloud PCs are encrypted and data is encrypted at rest, as is all network traffic to and from the cloud PCs.

Why it matters: Moving its operating system to the cloud could obsolete Microsoft's historical **dependence** on specific hardware partners.

- The launch of Windows 11 last month was met with resistance because of new hardware requirements; however, the cloud PC version will not have the same limitations which could put hardware partners like **Intel**, **HP**, **Lenovo**, and **Dell** on notice.

- Microsoft has previously taken the same cloud-based approach to its Office 365 productivity suite, used by more than 1 million companies worldwide, and seems confident it can do the same for Windows.

What's the catch? The processing capabilities of a cloud PC are still unknown, and it remains to be seen whether Windows 365 will work well just for basic productivity apps, or if it can scale to handle more processing-intensive tasks like video editing or 3D rendering. For comparison, **Google's** cloud-based Chrome OS works in a similar way, but is very limited when it comes to running demanding applications.

There's also some concern about storing all of a business's information on Microsoft's cloud. For what it's worth, Microsoft has demonstrated redundancies to keep data safe. Nonetheless, Big Tech outages can have disastrous results for businesses who rely on the cloud to access all their information.

Leading Security Concerns with Microsoft Office 365 According to IT Security Decision-Makers Worldwide, Feb 2021

% of respondents

The risk of compromise of data held in the Microsoft Office 365
48%

The ability of hackers to hide their tracks using legitimate Microsoft tools such as Power Automate and e-Discovery
45%

The risk of credential abuse leading to account takeover by unauthorized users
45%

The difficulty of spotting malicious insiders
39%

Lack of real-time information on threats
35%

Lack of contextualized data to spot unauthorized privilege escalation
25%

I have no security concerns
6%

Note: respondents could select up to three options
Source: Vectra AI, "Office 365 User Survey: IT Security Changes Amidst the Pandemic," conducted by Sapio Research, Mar 17, 2021

264665

eMarketer | InsiderIntelligence.com