Windows 365

Security First: Protecting the hybrid workplace

Download the e-book →

Transforming your organization's technology

Modern, flexible work has driven an increase in the diversity of employee endpoints, from desktops to tablets to mobile phones. Security needs to be invulnerable and reliable to ensure data, endpoints, and the business remain protected to avoid the risk and costs of breaches.

What's evolving:

- How and where employees work
- Data sharing and storage processes
- Privacy, compliance, and data security regulations

Prioritize endpoint management and security

The number of global hybrid workers is expected to reach 39% by 2024—meaning the number and diversity of endpoints is only going to continue to increase.[1] Businesses need to mitigate risk and protect data by prioritizing management and security for all users.

68%
of organizations have experienced one or more endpoint attacks that compromised data and/or their IT infrastructure[2]

80-90%
of all successful ransomware compromises originate through unmanaged devices[3]

$4.45M
average global cost per data breach occurrence[4]

Endpoint complexity may pose a challenge for IT teams

Many organizations have added endpoints to accommodate a flexible workplace, often adopting more security and management tools than they need along the way. Now, organizations are challenged with achieving the same or better endpoint management while eliminating redundant tools and saving costs.

Only **10%** of organizations monitor 100% of their endpoints[5]

68% of organizations use more than 10 tools to secure and manage endpoints[5]

The solution: Secure, efficient endpoint management
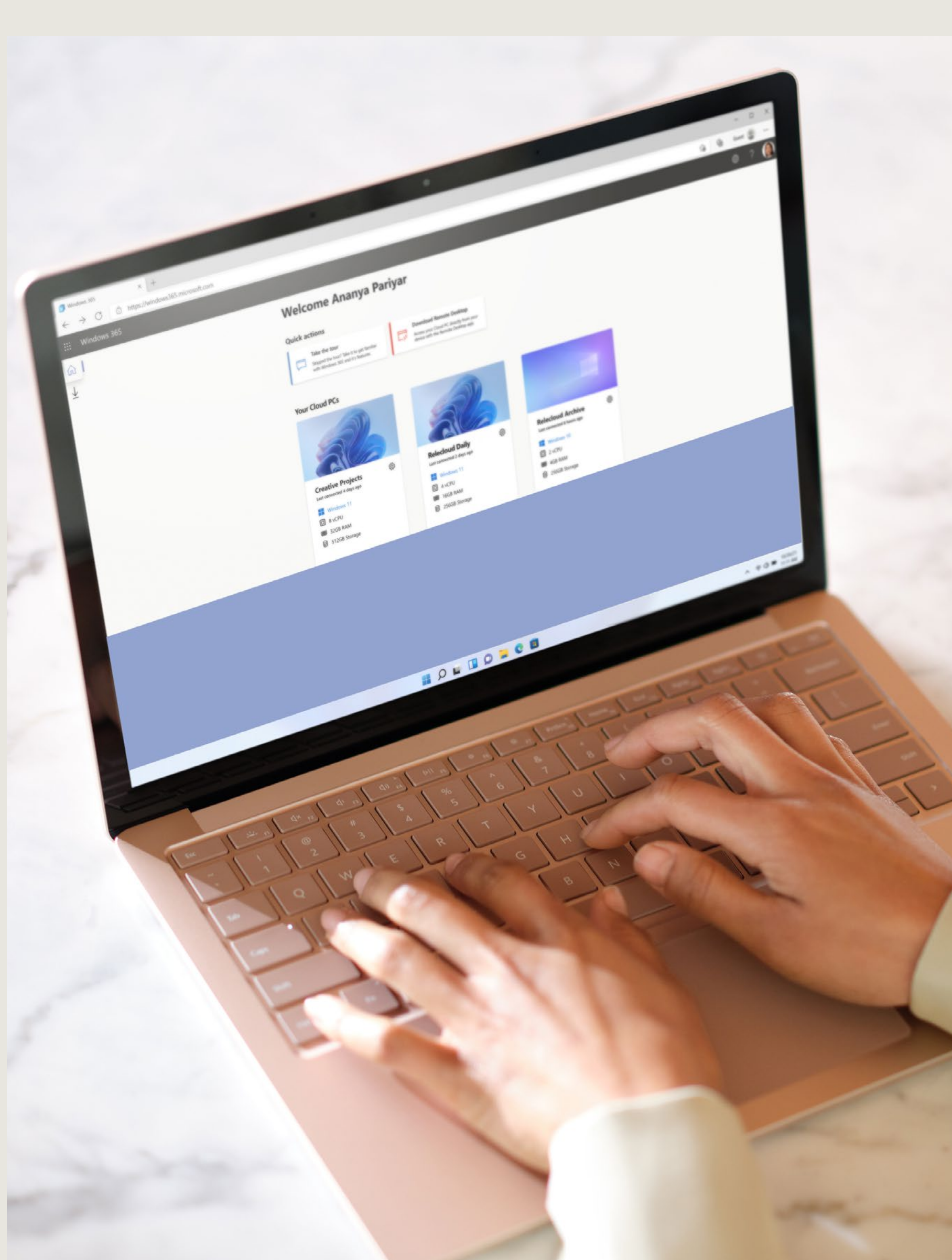
Windows 11 Enterprise, the most secure Windows yet, empowers your organization with built-in endpoint management that protects your data and devices. And because it's accessible from both Windows 11 compatible endpoints or through a Windows 365 Cloud PC, your organization can enjoy the benefits of a modern, flexible Windows experience without the need to upgrade or replace expensive devices.

More than **90%** of clients will use cloud-based endpoint management tools by 2025[6]
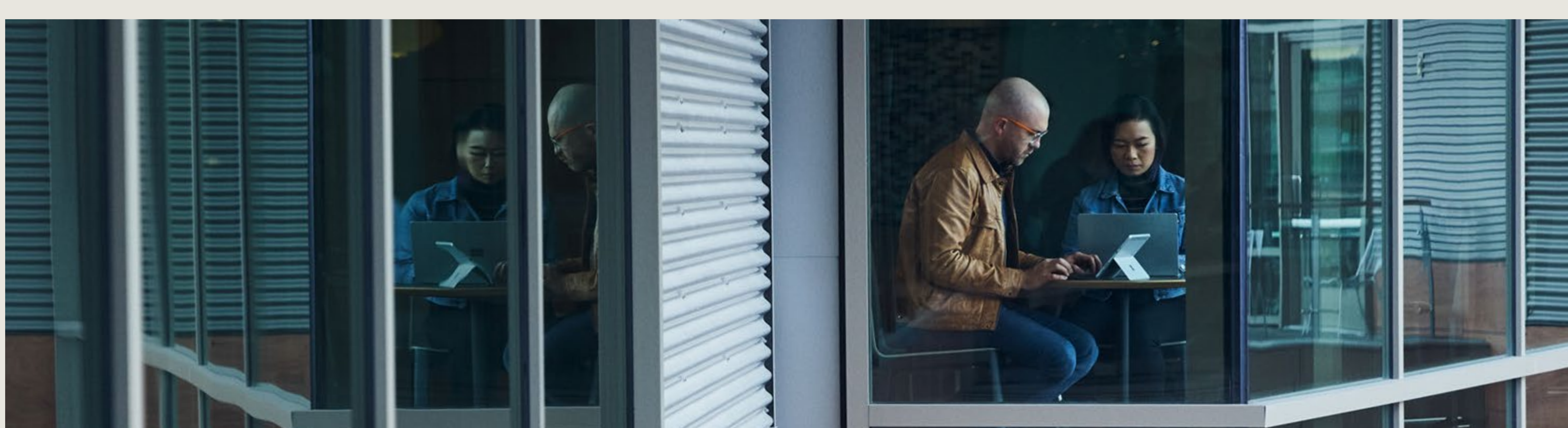
A Zero Trust solution delivers robust, simplified endpoint security and management

Microsoft Intune and Intune Suite are rooted in Zero Trust, a security model that prioritizes verification at the access level to ensure data privacy and protection across endpoints. Intune and Intune Suite can enable faster onboarding, centralized configuration, and advanced protection of all your devices operating Windows 11 Enterprise.

Find ways to enable a more secure IT infrastructure for your flexible workforce

Download the e-book →

Sources:

[1] "How to improve productivity and ensure security for hybrid workforces." Microsoft July 2023.
https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/how-to-improve-productivity-and-ensure-security-for-hybrid-workforces

[2] Ponemon Institute LLC. (2020). The Third Annual Study on the State of Endpoint Security Risk.
https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

[3] Microsoft Threat Intelligence. (2023, October). Microsoft Digital Defense Report 2023.
https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[4] "Average cost of a data breach worldwide from 2014-2023." Statista, October 2023.
https://www.statista.com/statistics/987474/global-average-cost-data-breach/

[5] Knuth, G., & Gruber, D. (2023, February). Managing the Endpoint Vulnerability Gap. Enterprise Strategy Group by Tech Target.
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW9wKT

[6] Wallent, M. (2023, May 16). Microsoft Intune: 5 endpoint management predictions for 2023. Microsoft Security Blog.
https://www.microsoft.com/security/blog/2023/12/01/microsoft-intune-5-endpoint-management-predictions-for-2023/

Windows 365