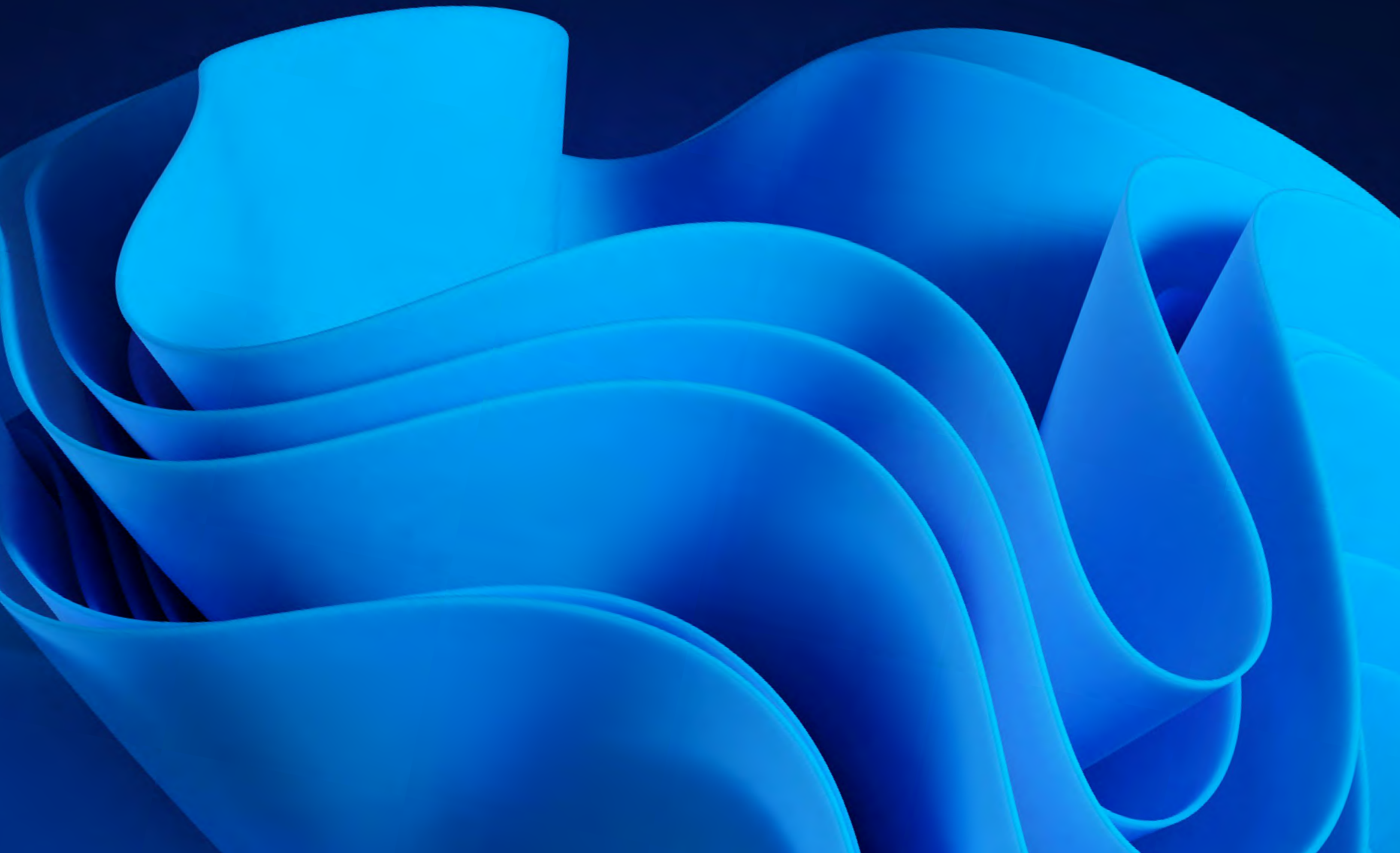
Windows

Securing Today’s Workplace

Modern endpoint strategies

Contents



Introduction

Today’s rapid pace of innovation and evolving work models give rise to both obstacles and opportunities.

To overcome the challenges and embrace the possibilities, enterprises must prioritize three key initiatives:

- Securing their infrastructure against a growing threat landscape across multiple flexible work models
- Streamlining their endpoint management tools and processes so IT administrators can shift their focus from routine tasks to complex problem-solving
- Modernizing their IT and end-user environments to prepare for seamless AI adoption

Endpoints are the entry and exit points for data and communication in a network. Most organizations use a range of endpoints like laptops, desktops, smartphones, tablets, printers, scanners, and IoT devices to perform their day-to-day tasks and collaborate on projects.

However, managing and securing all of these endpoints is getting more difficult as the types of endpoints and applications continue to increase in diversity and complexity.

The past few years have seen several key developments contributing to endpoint security and management hurdles. Most notably, work models have evolved to accommodate hybrid workers using various physical and virtual endpoints.

Meanwhile, organizations are focused on driving innovation and business strategies by incorporating advanced technologies like AI into everyday workflows. These developments mean that organizations must focus on securing their infrastructure across diverse work models, simplifying their endpoint management tools and practices, and modernizing their IT and end-user environments to make them more efficient and AI-ready.

Securing and simplifying your endpoints to make them more productive and future-proof can be a seamless process—with the right practices and solutions. **This e-book offers strategies for modernizing with Windows 11 Enterprise and Microsoft Intune to overcome today’s biggest endpoint security and management hurdles.**

Managing endpoint security is getting harder due to several factors...

Endpoint sprawl

135K

A survey revealed that organizations have an average of 135,000 endpoints.[1]

Poor endpoint visibility

63%

Of organizations reported a lack of endpoint visibility as the top barrier to strong endpoint security.[1]

Lack of security talent

60%

Of companies struggle to recruit cybersecurity talent.[2]

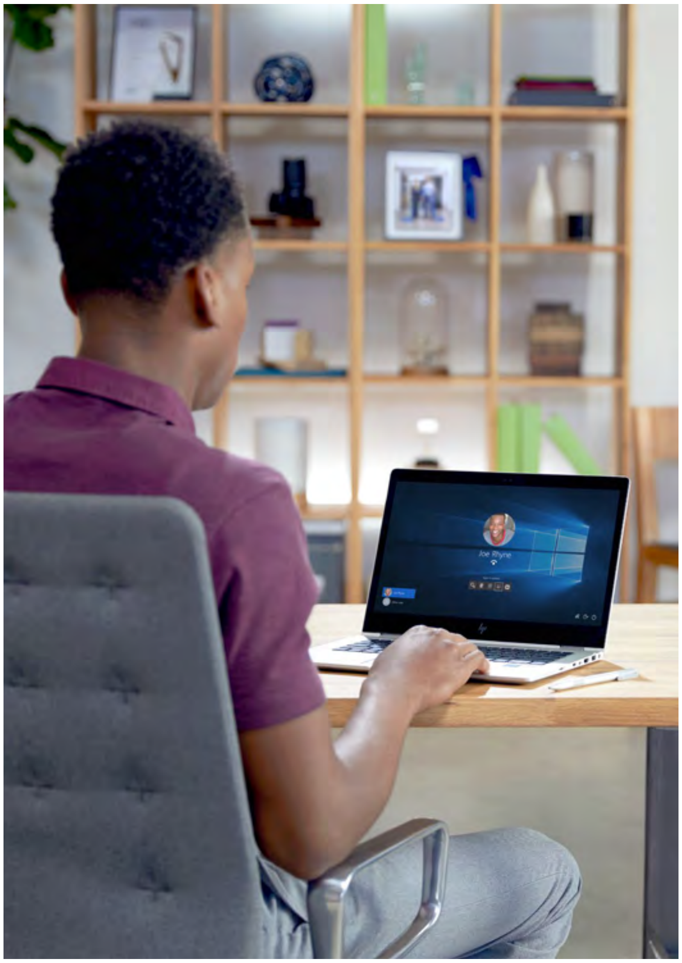
The growing challenges of endpoint management

At a time when every organization is looking to accelerate innovation, the realities of modern work present several key challenges regarding their endpoints.

Challenge #1
The growing threat landscape

Hybrid work models allow employees to work from almost anywhere using a variety of endpoints (personal or company-issued), including laptops, smartphones, tablets, and virtual endpoints to access company resources. These endpoints allow employees to take their work anywhere—but they can also increase an organization's threat surface area.

A larger threat surface area provides more opportunities for bad actors to breach a company's network with phishing, malware, and ransomware. As a result, company data is at higher risk of being compromised, which can disrupt business continuity and cause expensive breaches. With the average breach costing millions of dollars, even one unprotected vulnerability can do a lot of financial damage. Breaches also cause reputational damage, which can't be easily recovered.



$4.4M

The global average cost of a data breach in 2023 was $4.4 million, a 15% increase over three years.[3]

83%

Of organizations have experienced at least one firmware attack in the past two years.[4]

Challenge #2 Managing increasingly diverse physical and virtual endpoints

Modern work includes many physical and virtual endpoints, each requiring unique support and maintenance. This proliferation of tools and solutions can easily overwhelm IT teams with requests and incidents. To handle these requests, IT professionals often use siloed tools that add complexity to their workflows and limit the visibility of their endpoint environment.

The result is increased pressure on IT teams to provide technical support, software updates, patches, backups, and configurations for various endpoints from virtual desktops, Cloud PCs, and mobile devices. On top of that, each siloed tool comes with its own associated cost, making endpoint management more expensive than it would be with only one centralized tool. Without a unified, comprehensive solution for managing a diverse endpoint environment, IT teams spend more time—and more money—constantly mitigating issues rather than focusing on strategy and IT innovation.

41%

Of surveyed CIOs and CISOs surveyed said that transformation and gaining visibility across increasingly complex hybrid ecosystems is their greatest challenge.[5]

Challenge #3 Enabling frictionless productivity

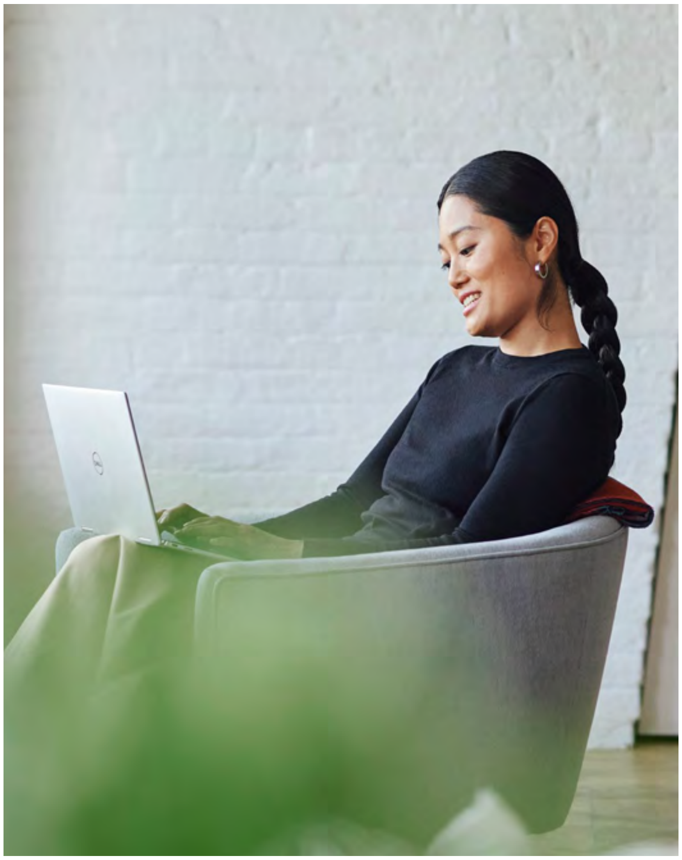
Sometimes, organizations find security and productivity in conflict when strong security policies unintentionally prevent workers from getting the access they need to perform their jobs. When employees encounter security roadblocks trying to use corporate resources, it halts productivity until IT can intervene and resolve the issue.

This challenge doesn't just apply to full-time employees—it also causes friction when onboarding new or temporary workers like contractors, consultants, or workers gained through a merger or acquisition. These workers need access to company resources before they can dig into their tasks. However, with so many endpoints to configure, secure, and deploy, it can take IT teams weeks or even months to set up new employees with the proper access to computing resources and machines—a task that's made even more difficult when those employees are working remotely. Ultimately, these delays can drastically slow down business strategies and limit the organization's vision for growth.

67%

Of IT admins say they struggle to manage flexible work arrangements due to the increased complexity and diversity of physical and virtual endpoints.[6]

Strategies for endpoint modernization



Managing and securing so many devices requires time and attention that could be focused on advancing business goals. Rather than constantly dealing with increased security risks and ballooning IT complexity due to siloed tools, your organization should strive to implement a modern endpoint strategy that secures your infrastructure, simplifies management, and helps power productive experiences.

Strategy #1
Secure your infrastructure with Zero Trust

Goal: Eliminate internal and external vulnerabilities, expand your threat intelligence, and reduce the steps required to access resources.

Steps: Zero Trust is a security model that assumes breach and verifies every request as if it came from an open network. To implement Zero Trust security, ensure your tools of choice include built-in security and automated features for handling encryption, group permissions, and identity checks. You should also bolster your defenses by employing analytics that increase your endpoint visibility to detect and remediate potential threats.

Strategy #2
Simplify endpoint management with an integrated solution

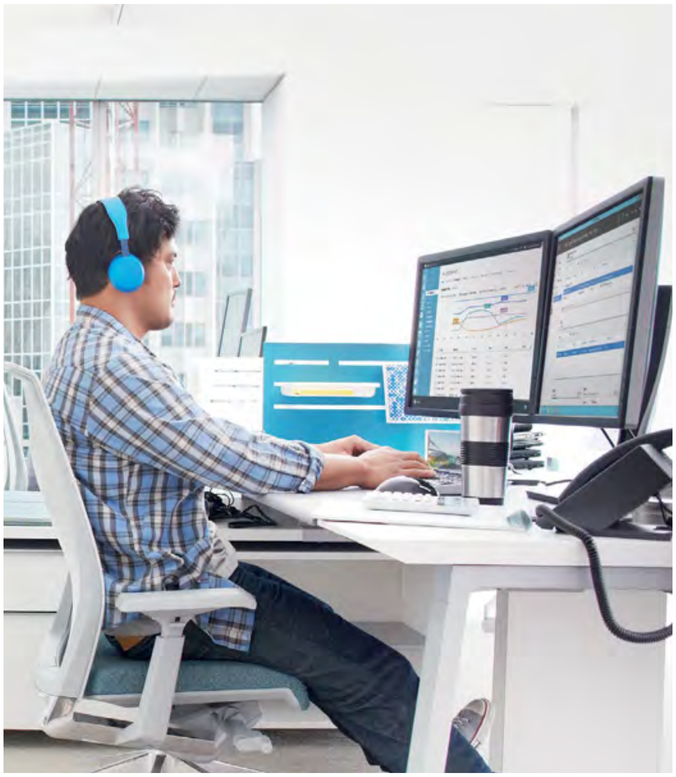
Goal: Reduce the time, support, and licensing costs of managing devices and virtual desktop environments.

Steps: Adopt modern physical and virtual endpoints—that is, those that meet operating system requirements, remain compliant, and adhere to your organization's technical requirements—using a single integrated management solution. If modernizing endpoints isn't in your immediate plan, you can enable modern device capabilities by having everyone use the latest version of your operating system on Cloud PCs. By consolidating management tools into a unified endpoint management solution, IT teams can help employees access apps and programs while freeing up the team's time to focus on innovation initiatives.

Strategy #3
Power productive experiences using AI

Goal: Prepare your infrastructure and endpoints to power AI capabilities in various scenarios.

Steps: Take advantage of productivity tools like Copilot in Windows to extend AI accessibility across all devices and applications using Windows 365 and Windows 11. Copilot in Windows enables enhanced productivity by assisting with troubleshooting issues, getting fast answers to questions, and connecting users with their preferred apps. With the hours freed up using AI assistance, workers have more mental capacity to work on creative problem-solving and collaboration.



Lay the groundwork for effective endpoint management

Migrating to Windows 11 Enterprise—either by adopting new Windows devices or enabling Cloud PCs via Windows 365—is essential to enabling a truly dynamic and secure endpoint environment.

Windows 11 Enterprise: Security and compatibility for the new era of work

Building your efficient-from-anywhere workforce starts with securing your infrastructure with Windows 11 Enterprise, the most secure Microsoft operating system yet. It has built-in security that reduces vulnerabilities across physical and virtual endpoints. With a Zero Trust baseline for security, it protects corporate data, apps, and employees by using enhanced phishing protection, threat intelligence, and multi-factor authentication. On the management side, Windows offers accessibility features, AI tools, and capabilities to help further streamline day-to-day workflows, reduce pressure on IT teams, and drive productivity.

Microsoft Intune and Intune Suite: Consolidated device management

Some Microsoft customers might not know that Microsoft Intune and Windows 11 Enterprise are included in the Microsoft 365 stack of applications, resulting in those customers investing in various third-party applications to manage their endpoints. Using Intune to manage your Windows 11 devices can significantly cut down the number of endpoint management tools you need while providing a centralized, unified console for device management.

Intune helps you simplify management for on-premises, cloud, mobile, desktop, Windows devices, and Windows 365 Cloud PCs with enhanced visibility and Zero Trust security controls. With rapid deployment features, you can set up thousands of PCs with just a few clicks, providing teams with a clearer path to productivity. Additionally, Intune Suite is an add-on to Intune, offering even more sophisticated capabilities like remote help, advanced app management, and advanced endpoint analytics.

Plan your upgrade to Windows 11 today
Windows 10 support ends on October 14, 2025. While that may seem like plenty of runway, modernizing your infrastructure will help keep your organization productive and its data secure by upgrading eligible devices to Windows 11 well ahead of the end of support date.

Modern devices for a modern workforce

Refresh your hardware estate with endpoints that are secure, fast, accessible, and AI-ready.

Operate a native OS on modern devices
Using Windows 11 Enterprise as your native OS on modern devices helps you reduce IT complexity and maintain a more secure infrastructure. It can be activated on two modern endpoints: Windows 11 compatible devices or Windows 365 Cloud PC on any device.

Customers who don't want to buy new hardware can use Windows 365 Cloud PCs, which let workers use Windows 11 Enterprise on any existing device. This enables users to get the same simplified, secure experience as they would using a native Windows 11 device.

Windows 11 Enterprise and M365 time and cost savings
Key findings from commissioned studies conducted by Forrester Consulting on behalf of Microsoft

75%
Reduced setup time for new endpoint by 75%.[7]

30%
Reduced hours to deploy/manage software by 30%.[7]

15%
Up to 15% increased productivity for end users.[8]

109–394%
Projected return on investment of 109 to 394% after three years.[8]

Secure and simplify endpoint management

No matter where your employees are or what devices they're using, Windows 11 Enterprise offers secure, reliable access to apps, personalized settings, and content on native PCs, tablets, and Cloud PCs via Windows 365. From the hardware level to the cloud, Windows 11 Enterprise provides comprehensive protection for your IT infrastructure so workers can manage their tasks efficiently without IT staff worrying that those activities are putting their organization at risk. Plus, with Microsoft Intune and Intune Suite, IT teams can more effectively manage endpoints while minimizing unnecessary costs associated with learning new management tools or dealing with complex deployment processes.

Consider Windows 11 Enterprise for a more secure, reliable, and cost-effective way to manage your endpoints, protect your hybrid workforce, and scale resources as needed now and in the future.

Ready to launch your modern endpoint strategy?

- **Modernize your OS** by migrating to Windows 11 Enterprise.
- **Consolidate and manage device management tools** with Intune plus additional advanced capabilities with Intune Suite.
- **Update your hardware** with secure, accessible Windows devices.

Take the next steps

Simplify your endpoint management.

Learn more

[1] Managing Risks and Costs at the Edge. Ponemon Institute. 2022.
[2] 2022 Cybersecurity Skills Gap Global Research Report. Fortinet.
[3] Cost of a Data Breach 2023. IBM. 2023.
[4] Hypothesis Group 2021. Security Signals. Microsoft 2021.
[5] Deloitte Future of Cyber Survey 2021 | Gaining Visibility into Complexity | Deloitte Global. www.deloitte.com. Accessed December 15, 2023.
[6] IT Trends Report: Remote Work Drives Priorities in 2021. JumpCloud. Accessed December 15, 2023.
[7] The Total Economic Impact™ Of Microsoft 365 E5 Cost Savings And Business Benefits Enabled By Microsoft 365 E5. A commissioned study conducted by Forrester Consulting. August 2023.
[8] New Technology: The Projected Total Economic Impact of Windows 11. Cost Savings and Business Benefits Enabled by Windows 11. A commissioned study conducted by Forrester Consulting. July 2022.