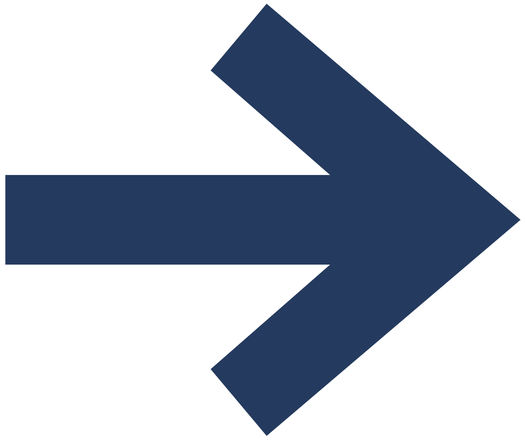
Windows 11

Starting at the Endpoint

A new approach to modernizing devices, systems, and teamwork



The endpoint is the new workplace

This e-book is not going to tell you that the world has changed, that workers want more flexibility, that customers want more convenience, that cybercriminals want your data, or that you can use technology to meet these challenges—IT and business leaders already know all that.

What may be less familiar is the concept of focusing on endpoints, like PCs and mobile devices, as a starting point to drive large-scale modernization projects. Traditionally, to enable remote work, implement new security measures, or simplify IT management, an organization needed to deploy and manage a separate solution for each objective. Plus, redeploy some solutions multiple times to run on multiple devices.

But widespread remote work has inspired (or necessitated, depending on your point of view) a new approach in which all of these capabilities are incorporated into the operating system itself. The potential benefits and ROI are significant. Employees enjoy smoother, more secure experiences with less downtime—even when working on personal devices—and IT departments can better govern devices, infrastructure, and security from a single management tool.

Modernizing endpoints is a practical way to realize these benefits. It's a foundational investment that simplifies operations, safeguards data, and sets your organization up for resiliency and growth.

Definition / modernizing endpoints:

The practice of improving the ease-of-use, hardware and software performance, cross-functionality, and security of workers' desktop, tablet, and mobile devices. This includes personal devices that run work applications.

Chapter

/ 01

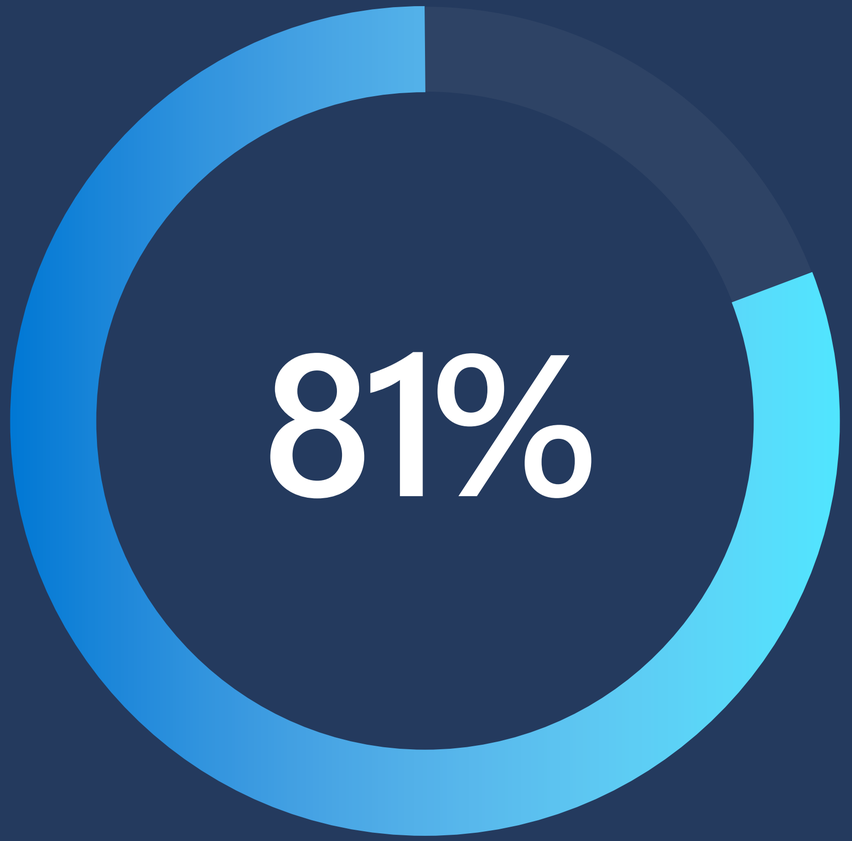
Increase flexibility by modernizing endpoints

Working whenever, wherever, on any device, used to be a perk. Today, it's fundamental for most people and enterprises.[1] In fact, in a Forrester study commissioned by Microsoft, employers expressed that allowing people to use their personal devices for work—and to work with more flexibility between home and the office— improves employee satisfaction and reduces turnover.[2]

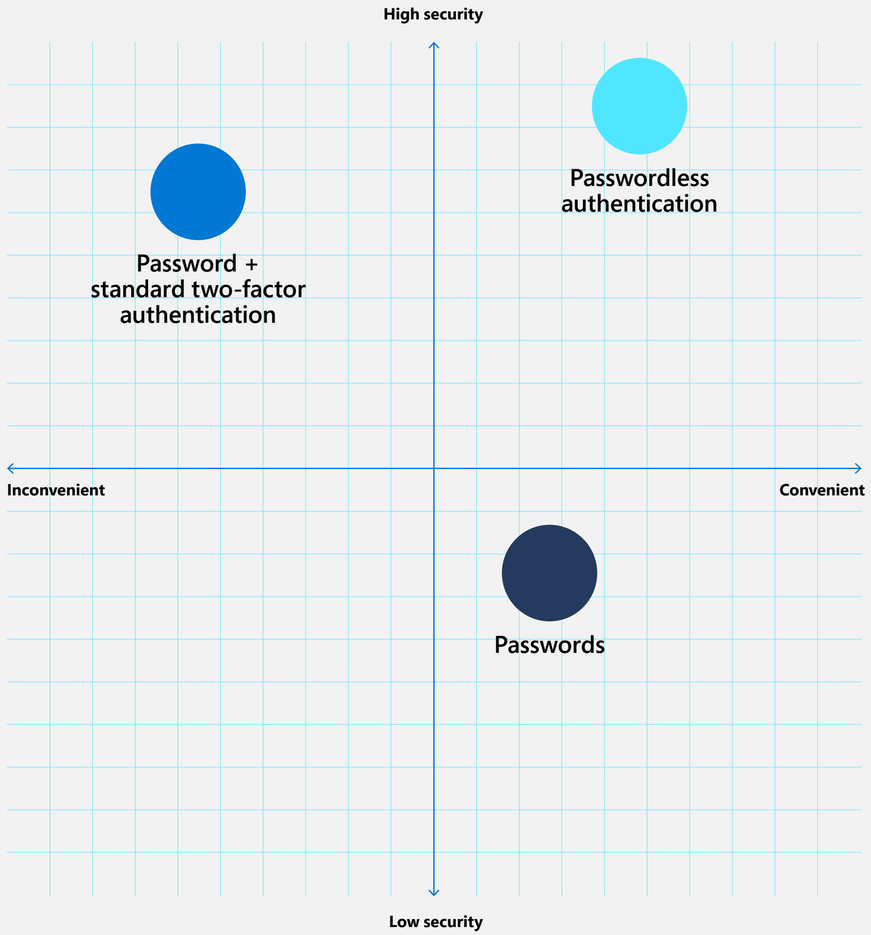
Switching between devices shouldn't just be possible, it should be easy, with a consistent look and feel. People should be able to create a presentation on their laptop, edit it on their phone, and present it with their tablet, all without having to troubleshoot their devices. The whole experience should be intuitive and seamless so people can stay in the flow of work. To meet these requirements, IT departments are increasingly focusing on the operating system on employees' endpoints as a key modernization strategy.

[1] "The winner by a long stretch," The WorkLab Year in Review, Microsoft, 2021.
[2] The Total Economic Impact™ Of Modernizing Endpoints, Forrester Consulting study commissioned by Microsoft, September 2021.

Percentage of business leaders adjusting their workplace flexibility policies



Passwordless authentication is more secure and more convenient than other options



Flexibility starts in IT

Giving employees flexibility starts in the IT department by equipping IT and security workers with the tools they need to save budget and support endpoints remotely.

To make that possible without requiring a heavy time commitment, IT leaders should consider deploying solutions like endpoint management apps that support both cloud-based and on-premises device management.

Another way to offer flexibility is by switching to passwordless authentication. Windows 11 is specifically designed to streamline this process and simplify deployment so people can start signing in with a tap or look sooner. It's faster and easier for employees—and much harder to hack. And deploying multifactor authentication—a key part of passwordless authentication—can thwart 99.9 percent of cyberattacks.[3]

Modernizing operating systems is key

Giving employees more flexibility isn't necessarily about providing the latest phone or laptop. It's about adopting an IT strategy that allows people to use any device they choose, with security built in. To implement that strategy broadly and achieve your flexibility goals, consider upgrading your operating system and, as needed, any endpoint devices that are unable to support a newer OS.

[3]Passwordless Protection: Reduce your risk exposure with passwordless authentication, Microsoft Security, 2021.

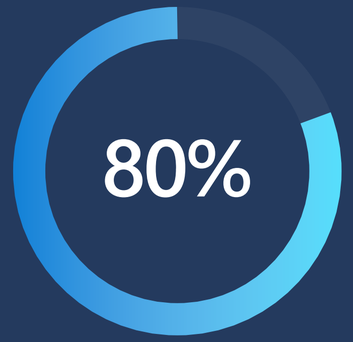
Chapter

/ 02

Deliver amazing employee experiences

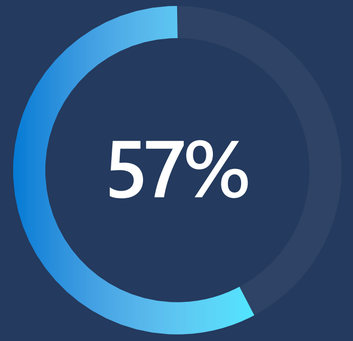
In the 2022 Work Trend Index from Microsoft, 80 percent of employees said they were just as productive—or more—in their jobs since going hybrid. 57 percent of remote employees are considering a shift to hybrid, while 51 percent of hybrid employees are considering a shift to remote. Plus, remote jobs on LinkedIn attract 2.6 times more views and nearly 3 times more applicants compared to on-site roles.[4] Enterprises that deliver this flexibility with a modernized endpoint environment will stand out in a competitive talent market.

To be successful, everyone—including frontline workers, executives, and information workers—needs to seamlessly collaborate, access information quickly, and carve out time for focused work and their own wellbeing. And employees who can easily complete their tasks, no matter where they are, are happier and more productive.[5] A modernized endpoint environment helps them stay in control of their day, and it shapes their perceptions of your organization.

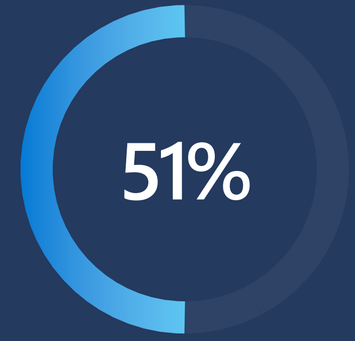


of employees say they're as productive—or more—working hybrid

as many applicants for remote than on-site jobs



of remote employees are considering a shift to hybrid work



of hybrid employees are considering a shift to remote work

[4]2022 Work Trend Index: Annual Report: Great Expectations: Making Hybrid Work *Work*, Microsoft, March 16, 2022.
[5]The Total Economic Impact™ Of Modernizing Endpoints, Forrester Consulting study commissioned by Microsoft, September 2021.

Build a thriving workplace

Improving employees' experiences with their devices isn't just about helping them work faster—it's also about empowering them to contribute more meaningfully to the enterprise. According to a report by Forbes Insights, "Employees benefit from a simple and consistent experience that improves their efficiency, collaboration, and communication with customers and each other."[6]

Key to this is eliminating the friction of toggling between endpoints so that employees don't have to divert focus away from their work in order to start using another device. For example, an operating system that delivers curated content can help them plan their day and easily access people and files, regardless of which device they're using. Passwordless methods like fingerprint scans, PINs, and facial recognition streamline app sign-up and sign-in. And voice typing and support for gestures and styluses make it simple to work on any device.

Create an inclusive culture

IT departments can help foster a positive, thriving culture across hybrid teams by implementing technology that supports participation from people with different communication styles and backgrounds. A unified endpoint environment fosters collaboration across devices, locations, and documents. Adopting tools that use intuitive design principles makes it effortless to start and participate in meetings and chats with people inside the office and across the world.

An inclusive workplace that empowers employees to be themselves and get things done is a powerful differentiator for enterprise organizations. Modernizing your endpoints will help you deliver a digital experience that makes your workplace more productive and fun.

[6]"Section IV: Endpoint Modernization," Reimagining Endpoints: Productive and Secure Computing in Today's Hybrid, Front-Line and Edge Environments, Forbes Insights in association with Microsoft, 2021.

Chapter

/ 03

Protect people, data, and services

As employees expand the number and variety of devices that they use to do their work—including their personal devices—IT departments are scrambling to keep endpoints compliant and up to date. A study of enterprise IT leaders revealed some common challenges[7]:

- Stitched-together security solutions that are disparate and outdated.
- Overdependence on VPNs, outdated identity management, and inadequate device management controls.
- Increased risks of data breaches, restrictive authentication policies that degrade the employee experience, and obstacles to onboarding new technology and employees.

To address these challenges, organizations are increasingly adopting **Zero-Trust architecture** as a holistic approach to securing bring-your-own-device environments, cloud-based assets, and remote users.[8]

Endpoint security starts with a holistic Zero-Trust approach

The principles of Zero Trust are:

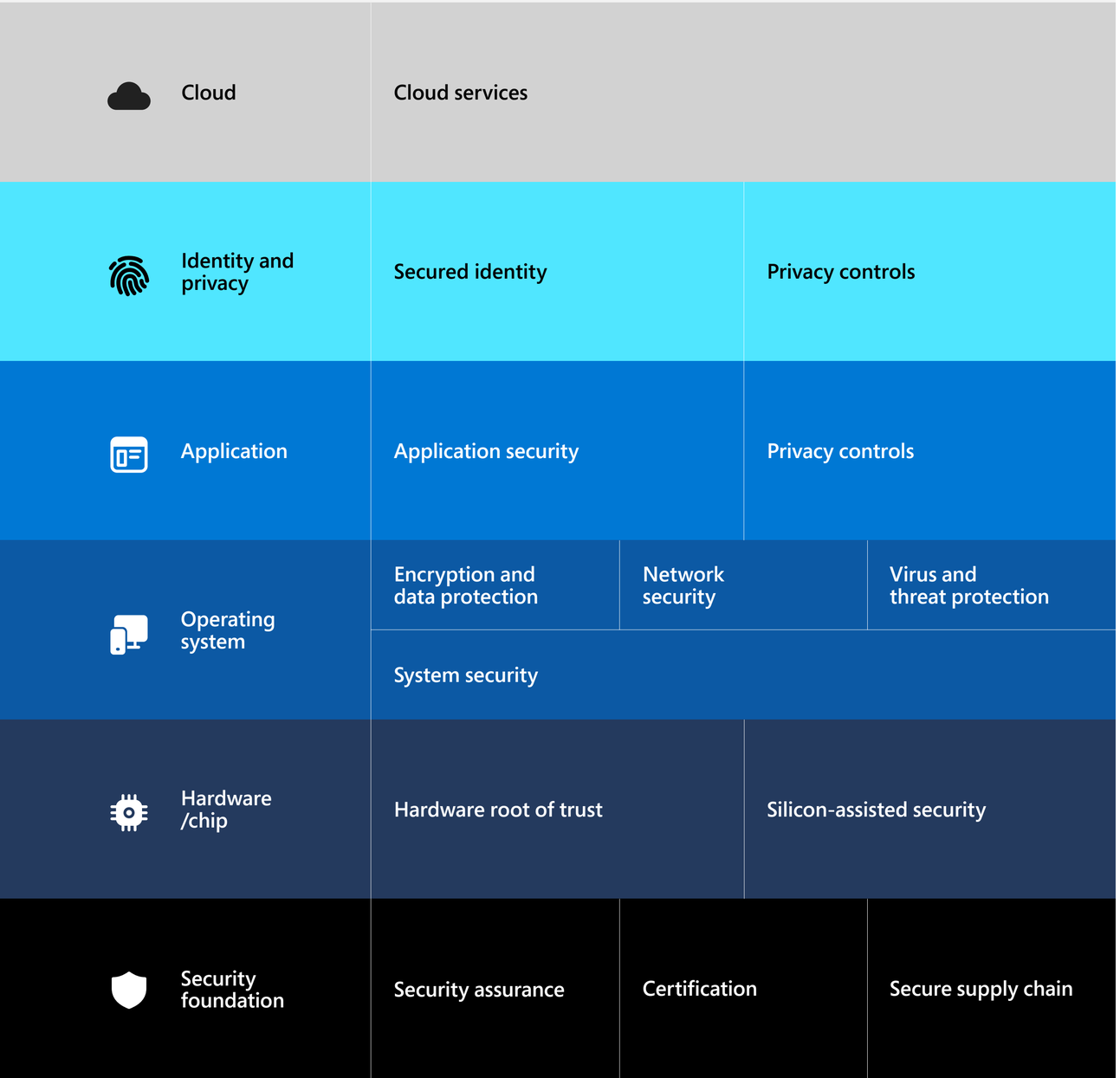
1. **Verify explicitly**. Always authenticate and authorize based on all available data points.
2. **Use the least privileged access**. Limit user access with just-in-time and just-enough access, risk-based adaptive policies, and data protection.
3. **Assume breach**. Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to improve visibility, threat detection, and defenses.

Microsoft encourages the use of Zero-Trust controls to provide visibility, automation, and orchestration across identities, endpoints, applications, network, infrastructure, and data.

Zero Trust across the digital estate

[7]The Total Economic Impact™ of Zero Trust Solutions from Microsoft: Cost Savings and Business Benefits Enabled by Microsoft's Zero Trust Solutions. A commissioned study conducted by Forrester Consulting on behalf of Microsoft. December 2021.
[8]McKendrick, Joe. Reimagining Endpoints: Productive and Secure Computing in Today's Hybrid, Frontline, and Edge Environments.

The six layers of Zero-Trust security



Zero Trust extends from the chip to the cloud

Robust end-to-end security strategies should:

- **Separate hardware from software** to protect against threats—the endpoint device is protected before it's even booted up.
- **Protect the operating system** against unauthorized access to critical data.
- **Prioritize application** security and prevent access to unverified code.
- **Protect user identities** with passwordless security.
- **Extend security to the cloud** to help protect devices, data, apps, and identities remotely.

Zero-Trust endpoint security begins with hardware-based isolation at the chip level. Sensitive data is stored behind security barriers and kept separate from the operating system, so encryption keys and user credentials are protected from unauthorized access.

Organizations should implement security features for hardware and operating systems that:

- **Protect and maintain system integrity** as the firmware loads, preventing unauthorized firmware or software from starting before the operating system launches.
- **Use a trusted platform module** (TPM) 2.0 for features like Windows Hello and BitLocker.
- **Create virtualization-based security** using CPU hardware virtualization to secure a region of memory isolated from the host operating system to protect information and code integrity.

An exciting development in hardware root-of-trust technology is Pluton, a security processor designed by Microsoft to foil sophisticated attacks. The chip can be configured as the device TPM or as a security processor in non-TMP scenarios, such as platform resilience.


Chart
Sales Goal
67%
Junk
Yesterday
Wanda Howard
Tomorrow's Sync
12:55 PM
Let's make sure that we come prepared to
Elvia Atikins
Team Pictures
12:55 PM
We look forward to meeting our fall intervi
Tomorrow, 11:00 AM (30m
RSVP
Alpine Ski House
Opportunity
South Africa Coffee
Opportunity
People
Aadi Kapoor
Files
Trade financing proposal
South African deck
Aida Proposal estimates
12:40

Chapter

/ 04

Mitigate risks and vulnerabilities

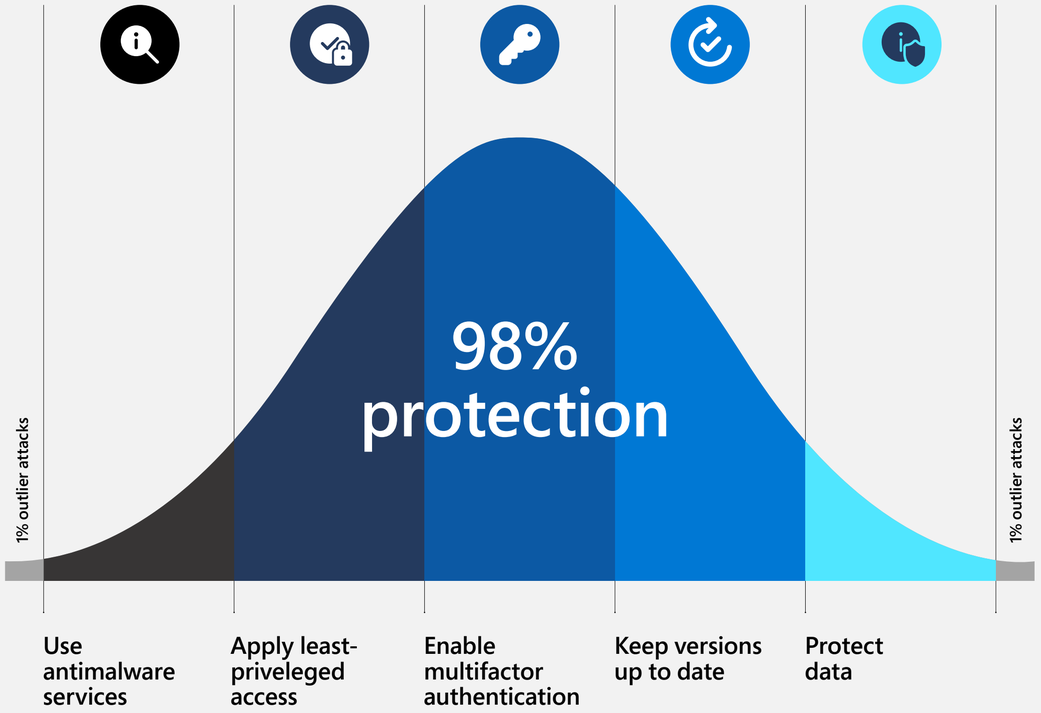
Common perception is that cyberattacks are complex, difficult-to-stop operations. But the reality is that most attacks stem from employee resistance to following basic security best practices for creating passwords and identifying phishing attempts. In fact, stolen passwords are by far the most common way enterprise accounts and data get compromised. Even attacks by nation-state actors typically rely on simple tactics like password sprays, which capitalize on employees using weak passwords.[9]

In 2021 alone, Microsoft detected and blocked more than 25 billion attempts to hijack enterprise accounts.[10] These weren't sophisticated attacks. They were simple, brute-force login attempts and stolen passwords.

Why, then, do so many IT departments struggle to prevent these breaches? The explanation is simple: It's more of a people problem than a technology problem. So, while IT departments need to continue to educate employees on basic security practices, there are two endpoint modernization solutions that help mitigate the "people" part of the problem and therefore the vast majority of attacks: multifactor authentication and patching.

[9]"Identity is the New Battleground," Cyber Signals, December – January 2021.
[10]Ibid.

The cybersecurity bell curve: Basic hygiene still protects against 98 percent of attacks



Fewer than 20 percent of Microsoft customers employ multifactor authentication.[11]

[11]Microsoft Digital Defense Report, October 2021.

Basic security hygiene essentials

- **A Zero-Trust approach** to authentication. Zero Trust assumes your operating system security has already been breached and requires that employees consistently verify their identities using multifactor authentication.
- **Multifactor authentication.** Employees provide multiple forms of identification, such as a hardware token and biometric, to access their accounts and data.
- **Passwordless authentication** eliminates the need for employee-generated passwords, which are usually the weakest link of an organization's security.
- **Updating and patching software** is a simple but effective way of preventing attacks. IT departments should implement automatic updates to harden security across the organization.

Advanced threat protection

Next to basic security hygiene, implementing advanced threat protection that detects and responds to attacks before they can cause harm is critical. Organizations should use:

- **A host firewall,** such as Windows Defender Firewall, to limit which devices can enter the network and the data that can be sent from within and to require authentication from any device that attempts to communicate with devices on the network.
- **Multifaceted antivirus software** which unifies machine learning, big-data analysis, and in-depth resilience research to provide comprehensive protection for endpoint devices—Microsoft Defender Antivirus is a well-known example.

Chapter

/ 05

Enable unified management

A key advantage of modernizing endpoints is the opportunity to simultaneously unify your IT management tools, save your IT team time, and minimize administration costs. Besides boosting efficiency, using a single control center to manage your organization's endpoints increases the speed, scale, and consistency of your network security efforts.

Having a unified administrative control pane that's built into your operating system, such as in Windows 11, allows you to:

- Manage endpoint devices, security, and cloud resources from a single place.
- Secure, deploy, and manage corporate and personal devices without disrupting work.
- Simplify IT with tools that allow different vendors and solutions to work together.
- More easily implement security updates, patches, and policies throughout your organization.
- Quickly assess the compliance of individual PCs and devices, or of your entire enterprise.
- More effectively protect against data breaches by encrypting all data in the system.

Advanced security management

Here's a closer look at two unified security management features that organizations running Windows should make full use of: **advanced group policy management** and **modern BitLocker administration management**.

Advanced group policy management

Using advanced group policy management to keep your user and desktop configurations up to date enables your network administrators to work faster and on a larger scale. In addition, it helps to reduce machine downtime for employees throughout your organization.

Rather than having to configure each computer in a Windows Server Active Directory environment one by one, you can use one central console to configure all sites, domains, and organizational units. Besides reducing your total cost of ownership, this gives your IT team more granular control over key endpoint updates.

Modern BitLocker administration management

Using modern BitLocker administration management streamlines your deployment and monitoring of BitLocker-protected devices and allows you to safeguard network endpoints more efficiently against data loss and theft.

This enables your IT team to automate volume encryption on client computers across your entire organization, centralize compliance monitoring and reporting, and simplify key recovery. It also allows your employees to take advantage of self-service tools to recover encrypted devices themselves—without having to contact the help desk. All of this helps to scale device deployment and reduce the cost of provisioning and supporting encrypted drives.

Chapter

/ 06

Increase IT productivity

IT teams see two types of business benefits from endpoint modernization: **rote task simplification or automation** and **redundant solution consolidation or elimination**.

Rote task simplification or automation

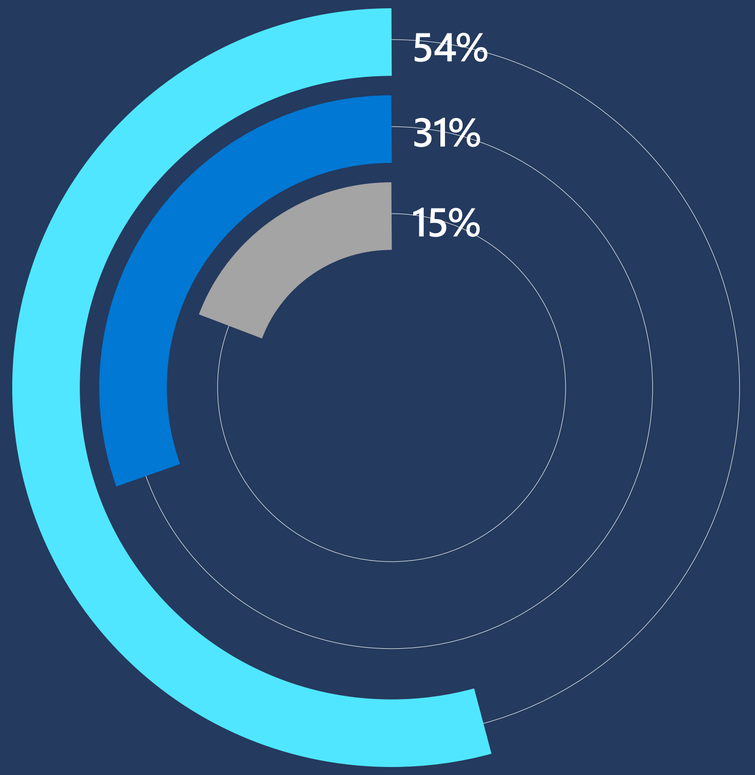
We know modernized operating systems provide endpoint users with smoother experiences, increased security and flexibility, and built-in risk mitigation. But for the IT teams that manage endpoint technology, these benefits also translate to increased productivity. Time previously taken by repeatable, day-to-day tasks is freed up for higher-value work. This is especially beneficial for lean IT departments with limited headcount and resources.

Potential efficiency gains include:

- **Reduced help desk calls.** By using tools like BitLocker PIN or a self-service portal, endpoint users are empowered to resolve more technology challenges on their own. When employees own taking care of tasks like updating apps or login credentials, help desks get time back to apply to other projects.
- **Solution and update deployments at scale.** Most IT teams still provision and update endpoint devices on site.[12] Modernized endpoints enable easy deployments with remote and automated roll-out capabilities.
- **Global policy management.** Modernized endpoint management systems allow IT teams to manage most tasks—like compliance and security—from a single control center. Centrally managed policies make it easier to keep enterprise-wide desktop configurations up to date and reduce downtime for employees.

[12]The Total Economic Impact™ Of Modernizing Endpoints, Forrester Consulting study commissioned by Microsoft, September 2021.
[13]Ibid.

Most enterprise IT departments provision, update, and secure endpoints on site



Done on-site by IT

Done remotely by IT

Done remotely by end users

Base: 301 global IT decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2021.[13]

I only want to buy one license for things. I don't want to buy two licenses for the same capability.[14]

—Director of user services and security operations at a pharmaceutical organization

Redundant solution consolidation or elimination

Modernized endpoints also afford IT teams the opportunity to consolidate—or even eliminate—disparate or redundant services and solutions. This frees up budget, time, and resources for other projects.

Disparate software solutions incur both quantified and unquantified expenses. **Quantified expenses** are costs measured with a monetary figure, like licensing fee agreements and vendor support costs. **Unquantified expenses** include harder-to-measure investments, like the time and effort of an employee to learn how to operate a new software solution and implement it within an existing software ecosystem.

Modernized endpoints don't just have the latest software, but also a wealth of integrated solutions built into the operating system. With a suite of solutions designed to work together from the start, IT teams can shed redundant services and free up time and resources that were previously devoted to solution maintenance. From a cost optimization standpoint, opportunities abound. The Forrester Consulting Total Economic Impact™ Of Modernizing Endpoints study commissioned by Microsoft estimates that eliminating redundant software solutions results in more than USD607,000 in reduced costs over three years for a composite organization of 4,000 people.[15]

[14]Ibid.
[15]Ibid.

Evaluate and develop your organization's endpoint strategy

It may surprise you that an e-book that recommends modernizing endpoints would also recommend that some enterprises maintain their current endpoint strategies. The fact is, many organizations have successfully enabled remote work, improved their workplace collaboration tools, implemented advanced security measures, and unified their IT management by deploying separate, complementary solutions. After all, Microsoft has been helping organizations to do this for a long time.

But the reality is that it now makes more sense for Windows to treat work and personal devices, workplace tools, cloud resources, and security as if they're interoperable by default—because for most employees and IT departments, they now are. And while Windows 10 will continue to be a platform of innovation for many successful organizations, Windows 11—which can be deployed in the same environment as Windows 10—is specifically designed to meet those needs more holistically.

Wherever you are in your endpoint modernization plans, we hope the guidance in this e-book provides you with a useful framework for evaluating and developing your organization's endpoint strategy.

Learn more about Windows 11
Or explore the deployment documentation