Windows

Build a foundation for modern digital resilience

Leadership strategies for preventing, responding to, and recovering from digital disruption.

Resiliency in the face of an evolving digital landscape

The cybersecurity threats faced by every organization today have never been more serious, with new threats emerging faster than ever before. Organizations are implementing security resilience and AI-powered solutions at unprecedented speeds, fundamentally changing both their software infrastructure and security protocols. This rapid pace of change, surpassing even the Internet and smartphone revolutions, creates significant challenges in maintaining the reliability of and access to systems that end users depend on.

The dual challenges of security and system resilience require both new protective measures against incidents and innovative approaches to rapid disaster recovery.

In today's digital landscape, every organization faces the critical question: How quickly can our organization recover when a disruption occurs? Rapid recovery isn't just beneficial in our interconnected digital world; it's essential for survival. As technology advances, it brings exciting opportunities and significant risks that organizations must navigate.

At its core, resilience means an organization can anticipate, prepare for, respond to, and recover from disruptions while running operations smoothly. Think of it as your organization's immune system - constantly monitoring, detecting, protecting against and managing threats and evolving to protect against new challenges.

89%

of business leaders say resilience is now a top strategic priority.

The result of resiliency programs? "Improved risk management, better financial performance, competitive advantage in the marketplace, a protected reputation and stakeholder trust."

PwC's Global Crisis and Resilience Survey 2023

A resilient first approach

This eBook can help IT decision makers discover how Windows platform innovations support their journey toward a more secure and reliable endpoint infrastructure, enabling a resilience-first approach.

Organizational resilience is crucial for thriving amidst challenges. Organizations that invest in resilience can gain a competitive advantage. They not only withstand disruptions but emerge stronger, better positioned for enduring success in our quickly changing digital world. By prioritizing and investing in resilience, organizations create frameworks that support long-term success.

Let's explore how Microsoft Windows is committed to helping organizations be more resilient.

"Microsoft runs on trust, and trust must be earned and maintained. Our pledge to our customers and our community is to prioritize your cyber safety above all else."

Charlie Bell, EVP Security,
Microsoft: Secure Future Initiative

Secure Future Initiative

Satya Nadella announced Microsoft's Secure Future Initiative with the goal to prioritize security across all aspects of the company. In his May 3, 2024, company-wide memo, Nadella emphasized this commitment, stating: "If you're faced with the tradeoff between security and another priority, your answer is clear: Do security." Making security priority number one for Microsoft, he also made it everyone's responsibility stating: "Security is a team sport, and accelerating SFI isn't just job number one for our security teams – it's everyone's top priority and our customers' greatest need."[1]

Born from the urgent need to defend against sophisticated cyberattacks, the Secure Future Initiative has led Microsoft to remove 730,000 non-compliant apps and 5.75 million inactive cloud tenants, significantly reducing potential attack surfaces in 2024.

Microsoft's Secure Future Initiative (SFI) rests on three core principles that work together to create a durable chain of security.

Secure by Design: Built in security from day one. Rather than treating security as an afterthought, we weave protective measures into products and services from the earliest stages of development. This proactive approach means security is part of our DNA, not a patch added later.

Secure by default: Protection without complexity. Your security shouldn't depend on complex configurations or expert knowledge. That is why we activate robust security features automatically, helping to ensure organizations are protected from the moment they start using our products.

Secure Operations: End-to-end protection you can trust. Security isn't just about features; it's about maintaining the highest standards throughout our operations. Our process is designed to protect your business and data from development to deployment.

Together, these principles create a security framework that comprehensively safeguards your organization, delivering robust security without sacrificing performance or usability.

We've built Windows 11 to reflect this core belief, helping to ensure our partners, developers, and you have the most secure foundation possible for your digital future.

Read the latest Secure Future Initiative progress report.

The Microsoft Windows Resiliency Initiative is focused at helping to prevent, manage and remediate incidents that make employee endpoints unavailable. It is a broad Windows-focused set of workstreams to elevate the reliability of Windows endpoints, including Windows Client, Cloud and Server.

USD 4.81M

The average cost of a breach when attackers used compromised credentials, which happened in 16% of the breach cases studied.[1]

1. Cost of a Data Breach Report 2024

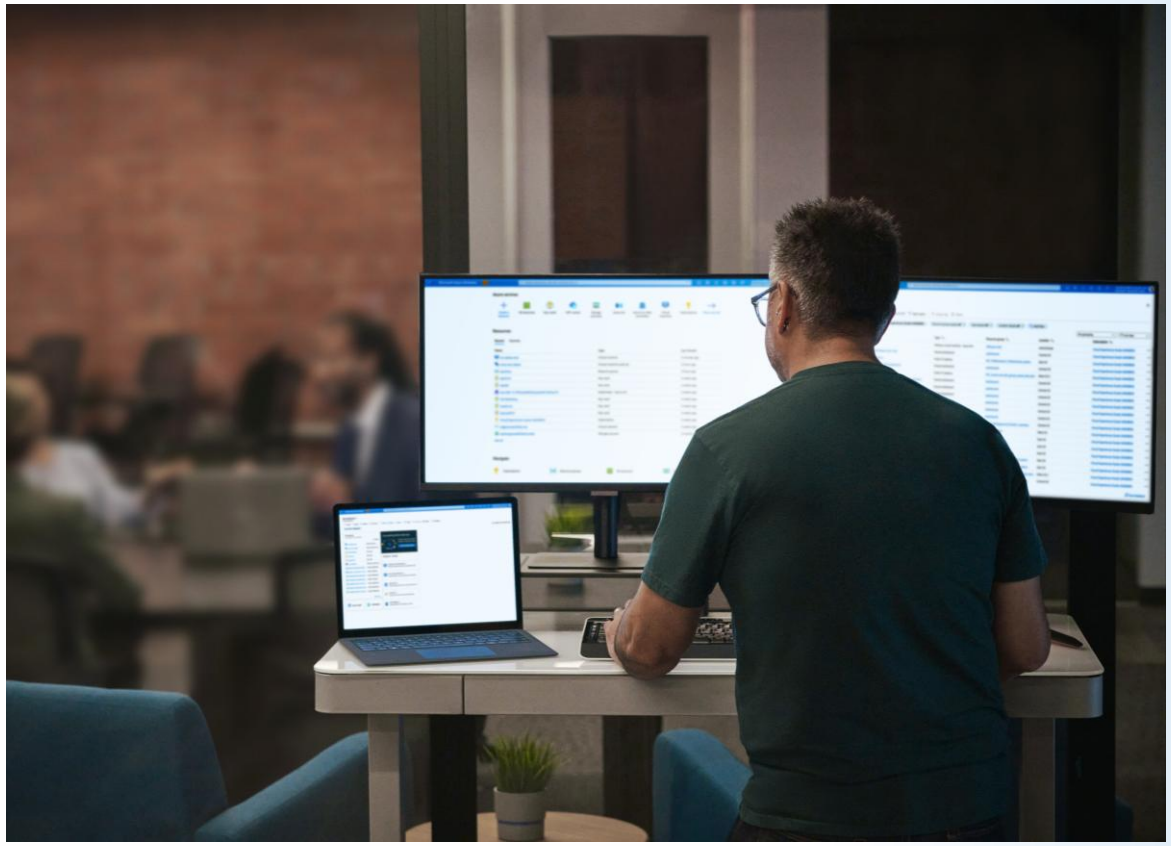
Windows Resiliency Initiative: prevention, management and recovery from incidents

Let's explore how Microsoft Windows helps organizations be more resilient, starting with the Windows security investments.

The Windows Resiliency Initiative (WRI) focuses on four foundational areas:

1. Enhancing security functionality to prevent incidents.
2. Improving system availability by recovering quickly when endpoints are blocked.
3. Investing in the Windows platform elevating system reliability.
4. Evolving the open ecosystem of solutions and partnerships.

Each area addresses the evolving security and reliability challenges in our interconnected world.



Enhancing security functionality to prevent incidents.

With Windows, supported by the principles of WRI, we've fundamentally reimagined our approach to security, delivering our most secure Windows product to date. Let's explore more detail about three of the improved features that enhance security functionality to prevent incidents in Windows.

Layering hardware and software for transformative security.

At the heart of Windows 11's security architecture lies a powerful combination of hardware-enforced security, working seamlessly with advanced software protection. This creates multiple layers of defense that safeguard identities, data, and systems while enabling innovation to flourish.

It is a security ecosystem that evolves alongside emerging threats, continuously adapting, learning, and strengthening its defenses. This isn't merely an improvement over Windows 10; it's a transformative leap forward in protecting organizations and employees.

This helps ensure our partners, developers, and you have the most secure foundation possible for their digital future. In today's rapidly evolving threat landscape, this commitment to security is not just about protection, it's about enabling organizations to advance with assurance.

Application and driver control

Windows 11 asserts stronger controls for apps and drivers allowed to run on the operating system.

Apps and drivers that are not reputable often lead to malware and script-based attacks. Attacks are getting more sophisticated. They are becoming more targeted.[1]

To help employees obtain reputable apps, smaller organizations can use *App Control for Business* policies to help ensure that only verified apps can run on devices. These policies leverage AI to simplify deployment and management, providing peace of mind that only signed apps or apps predicted to be safe by Microsoft cloud-based AI can run on a device.

This means fewer disruptions, reduced security incidents, and more confidence in your system's integrity.

1. Microsoft Digital Defense Report 2024

Printers and print infrastructure have been a new and underreported vector for cybersecurity attacks. Windows recently introduced *Windows Protected Print Mode (WPP)*, one of the largest changes to the Windows print stack in over 20 years with the modernization of the Windows Print System. *Print Support Apps* allow printer OEMs and IHVs to extend the WPP for a tailored user-experience without compromising security with kernel-mode printer drivers.

The new platform maximizes compatibility and puts users first, while supporting a large ecosystem of partners and devices.

Windows Protected Print works with Mopria certified printers. Learn more at: https://mopria.org/print-with-windows

Identity Protection

Phishing remains a significant threat. By adding additional hardening to *Windows Hello*, the built-in multifactor authentication (MFA) solution in Windows, users benefit from enhanced protection against phishing attacks. This improvement makes signing in more secure and convenient than ever before, providing a more seamless user experience.

Windows Hello offers significant benefits by allowing users to sign in using biometrics (face or fingerprint) or a device PIN, which is unique to the device. This multifactor authentication (MFA) solution is a cornerstone of Windows 11 security, providing enhanced security and convenience.

Enabled by default with Entra-join, Windows Hello enables a smooth single sign-on (SSO) both on-premises and to the cloud, making it suitable both for hybrid and pure cloud environments. Additionally, Windows Hello has been extended to support *passkeys*, offering robust protection across much of the web.

MFA has evolved from an optional security measure to an essential component of modern security architecture, eliminating the need to remember complex passwords and significantly enhancing overall security.

While multifactor authentication adoption is rising to 41%, attackers are shifting tactics, targeting infrastructure and employing adversary-in-the-middle (AiTM) phishing attacks and token theft.[1]

600M

identity attacks occurred daily in 2024.[1]

1. Microsoft Digital Defense Report 2024

The Windows Resiliency Initiative strengthens security while maintaining user flexibility through *administrator protection*.[2] Windows will introduce significant changes by removing admin privileges by default on new PCs. With this feature, employees have standard user permissions by default but can still make system changes, including app installation, when necessary. Instead of maintaining constant administrator access, users gain enhanced protection and operate in a standard account and use Windows Hello to temporarily authorize administrator actions.

This streamlined process significantly reduces the risk of attacks that exploit admin privileges, including unauthorized software installations and system modifications. By putting control firmly in users' hands, not malware's, organizations can significantly reduce their vulnerability to privilege-based attacks without sacrificing productivity.

Despite a 2.75x increase in ransomware-linked encounters in 2024, attacks reaching the encryption stage have decreased threefold over two years due to automatic attack disruption. Of those attacks that did progress to the ransom stage, over 90% used unmanaged devices as their initial access point or for remote encryption.[1]

99%

of the 600M identity attacks per day in 2024 were password based.[1]

1. Microsoft Digital Defense Report 2024

Improving system availability by recovering quickly when endpoints are blocked.

One of the most significant areas of improvement in the Windows Resiliency Initiative is recovery.

In the past 20 years, Windows has undergone various improvements for reliability, leading to a decrease in crashes. While most users no longer frequently experience blue screens, recovery tools have remained essentially unchanged. There is a need for more robust recovery solutions. Organizations have expressed the desire for more comprehensive measures to prevent and manage incidents, and the Windows Resiliency Initiative aims to meet these demands.

The Windows Resiliency Initiative enhances the platform's reliability through incident prevention, the development of rapid recovery tools, and best practice documentation.

Microsoft is transforming the Windows Recovery Environment (WinRE) with powerful new features. *Quick Machine Recovery* (QMR) is a solution that can execute targeted fixes from Windows Update on machines when Windows is unable to boot. When a machine enters the Windows Recovery Environment (WinRE), it will contact Windows Update to download and run fixes. This helps ensure that recovery is swift and effective, maintaining the system's reliability.

Learn more about administrator protection at: Quick machine recovery.

Investing in the Windows platform, elevating reliability

We are developing new *Windows capabilities for security-product developers to build their products outside of kernel mode*. Security products, like anti-virus and endpoint protection solutions, will be able to run in user mode just like regular applications. Running outside the kernel not only helps reduce the risk of system crashes but also simplifies recovery when issues occur. Ultimately, this evolution enables developers to deliver strong protection while improving the overall stability and resilience of Windows devices.

90%

of cases where attacks progressed to ransom stage, the attacker had leveraged unmanaged devices in the network

Microsoft Digital Defense Report 2024

Evolving an open ecosystem of resilient security solutions

> We appreciated the opportunity to join these important discussions with Microsoft and industry peers on how best to collaborate in building a more resilient and open Windows endpoint security ecosystem that strengthens security for our mutual customers.[1]
>
> **— Drew Bagley, VP & Counsel, Privacy and Cyber Policy, CrowdStrike**

Strengthening collaboration across the technology ecosystem is essential to improving security and resilience.

The Windows Resiliency Initiative builds strategic partnerships along every step of the value chain, helping companies respond to disruption and emerge with improved solutions that propel businesses forward.

To further improve resilience, we are evolving our partnership with endpoint security providers through the *Microsoft Virus Initiative* (MVI). These partners' software has extensive integration with the Windows platform and plays a significant role in safeguarding your environment. As part of this evolution, MVI partners are now required to implement new processes in collaboration with Microsoft engineering teams to improve reliability.

In addition to increased testing and strengthened incident response processes, these partners must follow *Safe Deployment Practices* for updates to their customers' Windows endpoints. Updates to security products must be gradual, using deployment rings, as well as proactive monitoring to minimize potential disruptions. These practices complement our platform investments to shift security functionality from kernel to user mode—together delivering greater stability, faster recovery, and reduced operational risk for enterprise customers who depend on a secure and reliable Windows environment.

Microsoft convened the *Windows Endpoint Security Ecosystem Summit* in September 2024[1] bringing together a diverse group of MVI security partners representing a worldwide partner ecosystem as well as the US *Cybersecurity and Infrastructure Security Agency* (CISA).

The summit aimed to define new ways to increase resilience across the ecosystem and ensure Windows remains an open platform, enabling user choice and innovation while maintaining the highest quality standards for security. MVI partners from around the globe, including Microsoft Defender, committed to adopting safe deployment practices and conducting additional security and compatibility testing for components like security kernel drivers.

CISA participated in the summit and expressed its commitment[2] to ongoing collaboration with Microsoft to help ensure the delivery of safe, secure, and resilient software. They highlighted the importance of safe software deployments and provided guidelines for producing software secure by design, by default, and through delivery.

1. Taking steps that drive resiliency and security for Windows customers
2. CISA Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers

Eight strategies to act on today, to build a resilient program

In today's rapidly evolving digital landscape, organizations must prioritize IT resiliency and crisis management integration.

Organizations are encouraged to take proactive steps now to build an information technology resiliency program capable of effectively managing disruptions with minimal impact on their strategic goals.

These eight strategies can help strengthen prevention, response, and recovery efforts.

1 **Invest in hardware and software that contain integrated capabilities to support a security strategy.** When a disruption-impact exceeds the acceptable level of impact for an organization, it becomes a crisis. In a crisis, resilience plans may be overwhelmed, and the tolerable levels of impact may be breached. A crisis management capability built into your own organizational system should provide a flexible and dynamic approach to enable an organization to manage unforeseen disruptions, continue to deliver its strategic aims, and return to a viable operating state in these conditions of extreme uncertainty.

2 **Embrace Zero Trust principles and maintain a comprehensive asset inventory.** Adopt proactive measures by regularly auditing your endpoint estate as well as eliminating unused or non-compliant applications and tenants. Of attacks that progressed to the ransom stage, 80 to 90% used unmanaged devices as their initial access point, or used them for remote encryption.[1]

3 **Practice consistent security hygiene.** Apply Windows Security best practices[2] for integrating and managing security tools and Incident response.[3] Basic security hygiene includes patching regularly, rotating or replacing passwords with biometrics, finding trusted sources for threat intelligence, and maintaining a regular security detection routing.

1. Microsoft Digital Defense Report 2024
2. https://www.microsoft.com/security/blog/2024/07/27/windows-security-best-practices-for-integrating-and-managing-security-tools
3. https://learn.microsoft.com/security/operations/incident-response-overview

4 **Transition to phishing-resistant, passwordless authentication methods** like Windows Hello and passkeys. Enhance monitoring with AI-driven threat detection and ensure access only from managed devices. Secure your identity infrastructure by governing permissions and retiring unused applications.[1]

5 **Implement blocklists for known malicious domains and apps.** Stay ahead of evolving scam tactics with blocklists. Leverage AI detection models used in App Control and Microsoft Edge with SmartScreen enabled. Client-side signals can improve the speed and efficiency of identifying and neutralizing tech-scams.

6 **Strengthen your posture with Microsoft Intune and Windows Autopatch.** Windows Autopatch automatically updates Windows endpoints with the latest security and quality updates, and updates drivers, Microsoft 365 apps, Microsoft Edge and Teams. Windows Autopatch supports hot patches that don't interrupt the device-user when Windows is in use.[2]

7 **Collaborate with government bodies and industry partners to strengthen cybersecurity measures.** Participate in collective defense initiatives[3] and adhere to international standards, to enhance resilience against evolving cyber threats and contribute to global stability.

8 **Incorporate Cloud PCs into your recovery strategy for enhanced flexibility.** Cloud PCs are resilient. Point-in-time restore administrators can quickly revert a Cloud PC to an earlier desirable state. With configuration and cross region disaster recovery options from Windows 365, Cloud PCs can be restored quickly with snapshots backed up to different zones.

1. 4 ways to protect you from phishing. & Securing the sign-in process
2. Use safe deployment practices to safeguard and manage your environment
3. CISA Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers

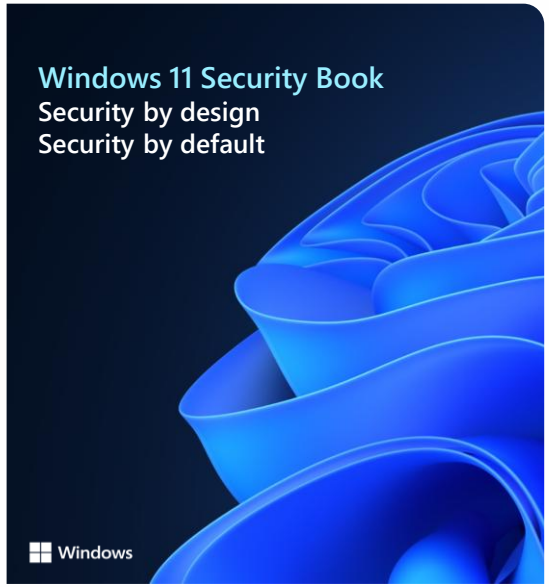
For additional reading

"Microsoft runs on trust, and trust must be earned and maintained. Our pledge to our customers and our community is to prioritize your cyber safety above all else."
Charlie Bell, EVP Security, Microsoft

To learn more about the **Secure Future Initiative**, read the SFI Progress Report

With Windows 11, we've fundamentally reimagined our approach to security, delivering our most secure Windows yet.

To learn more about the **Windows Security** and how Windows can help you implement Zero Trust, read the Windows 11 Security Book



We are entering a new reality—one in which AI can reason and solve problems in remarkable ways. This intelligence on tap will rewrite the rules of business and transform knowledge work as we know it.

To learn how you can adapt, read the 2025 Work Trend Index Annual Report