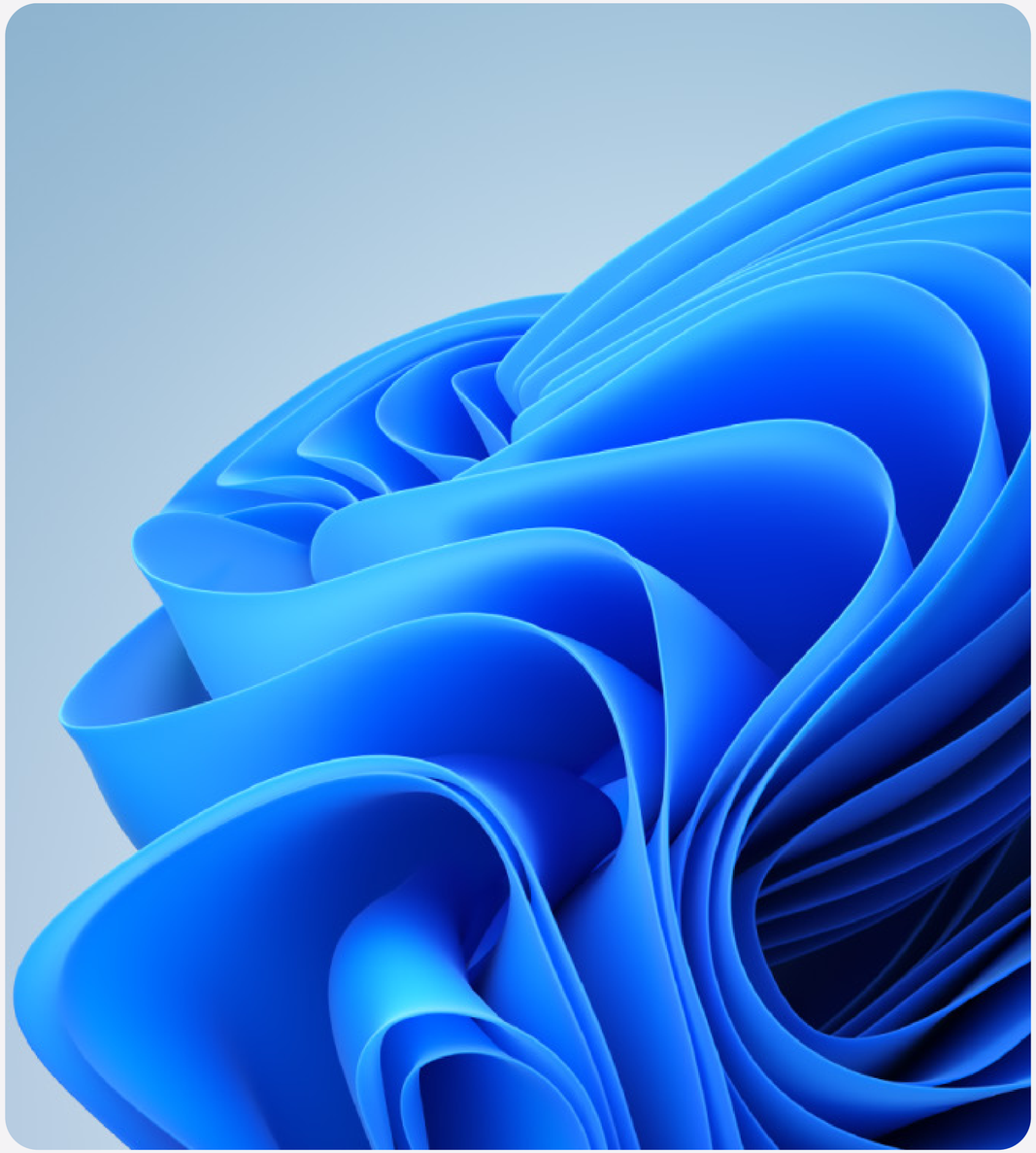
Microsoft

Build a foundation for modern digital resilience

Leadership strategies for preventing, responding to, and recovering from endpoint disruptions.



E-book

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 AI-powered solutions at unprecedented speeds, fundamentally changing both their software infrastructure and 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.

This challenge requires both new preventive and protective measures against incidents and innovative approaches to rapid disaster recovery.

This modern threat landscape demands that every organization face 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 maintaining smooth operations. Think of it as your organization's immune system—constantly monitoring, detecting, protecting against, and managing threats and evolving to protect against new challenges.

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 also 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 Windows is committed to helping organizations be more resilient.

"Microsoft runs on trust, and trust must be earned and maintained."

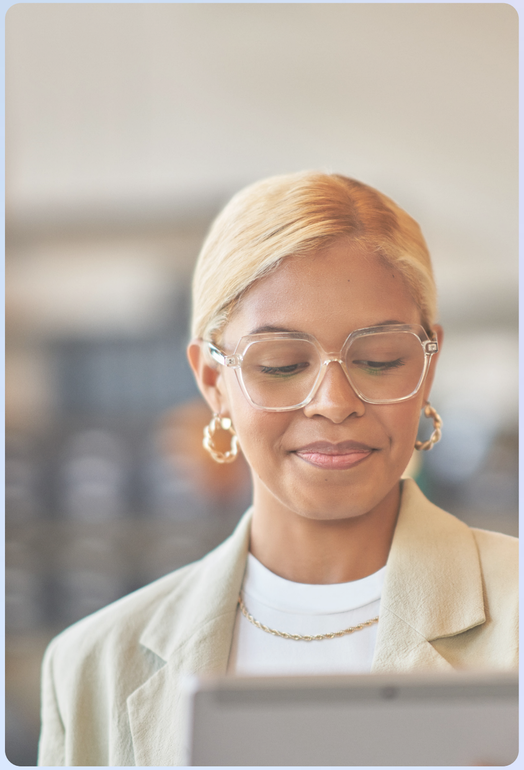
Charlie Bell, EVP Security, Microsoft

Windows Resiliency Initiative: prevention, management and recovery from incidents

Let's dive into how Microsoft enables organizations to be more resilient, starting with the foundation of the Windows ecosystem. So that Windows acts as a reliable core, the Windows Resiliency Initiative focuses on three key areas of enhancement:

1. **Evolving the open ecosystem of solutions and partnerships.**
2. **Investing in the Windows platform to elevate system reliability.**
3. **Improving system availability to recover quickly when endpoints are blocked.**

Each of these areas is designed to address the evolving reliability challenges in our interconnected world.



Evolving the Windows open ecosystem of resilient security solutions

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

The Windows Resiliency Initiative fosters strategic partnerships throughout the entire value chain, enabling companies to respond to disruptions and emerge with enhanced 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 adhere to Safe Deployment Practices when updating their customers' Windows endpoints. Updates to security products should be rolled out gradually, using deployment rings, and accompanied by proactive monitoring to minimize potential disruptions. These practices complement our platform investments, shifting security functionality from kernel to user mode—together delivering greater stability, 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

“Bitdefender is pleased to collaborate with Microsoft to redefine how security is delivered to Windows users. Through the Windows Resiliency Initiative and development of the Windows endpoint security platform, our teams have worked together to modernize the security architecture—creating a resilient, forward-looking foundation that enhances protection against evolving threats while maintaining a seamless user experience. This initiative reflects our shared commitment to advancing industry standards and delivering secure, high-performing Windows environments for customers everywhere.”

Florin Virlan, SVP, Product and Engineering at Bitdefender Customer Solutions Group

Investing in the Windows platform elevates system reliability

Strengthening collaboration across the technology ecosystem is essential to improving resilience. Preventing drivers from bringing down PCs is a priority for the Windows Resiliency initiative, focused on preventing, managing and recovering from PC incidents.

Today, security software on Windows typically runs in kernel mode. This brings with it a reliability risk, as mistakes made in kernel mode code can crash the operating system, causing an immediate reboot. The Windows endpoint security platform (WESP) offers a new alternative design for developing security software that can run in user mode. Microsoft and a number of security partners are collaborating to define these new capabilities, which are intended to improve the stability and reliability of Windows devices.

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, such as 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.

Ecosystem collaboration does not end with the Microsoft Virus Initiative focused on security partners, but extends to all partners developing drivers for all kinds of applications and peripherals.

Preventing drivers from disrupting PCs is a priority for the Windows Resiliency Initiative, focusing on preventing, managing, and recovering from PC downtime incidents. In addition to security partners, the Windows ecosystem also includes a large number of partners that commercialize solutions that extend the functionality of your digital workplace. Microsoft partners with more than 4,000 vendors that develop and deliver drivers, such as audio, networking, and many other classes. We are working on a change to reduce risk in the larger Windows driver ecosystem, using new and evolved Microsoft-authored “class drivers” as well as user mode drivers from partners.

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 numerous improvements for reliability, leading to a decrease in crashes and downtime. While most users no longer frequently experience blue screens, recovery tools have remained essentially unchanged highlighting 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 processes and tools to prepare for and manage endpoint incidents.

Microsoft is transforming the Windows Recovery Environment (WinRE) with powerful new features and recovery tools. Opening up WinRE to be a networked and managed OS with the addition of enterprise ethernet and Wi-Fi.

Quick Machine Recovery (QMR) is a solution that can execute targeted fixes from Windows Update on machines when Windows is unable to boot. Targeted at large-scale outages, when a machine enters and remains in the Windows Recovery Environment, 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.

We are introducing additional modern recovery capability designed to minimize downtime and simplify remediation. These tools help recover individual machines as well as groups of devices that are impacted. Windows users and IT admins face significant frustration when a PC stops functioning due to flawed updates, configuration errors, or other outages. Traditional recovery

methods are often slow, require manual intervention, and disrupt productivity—sometimes taking hours or even days to resolve.

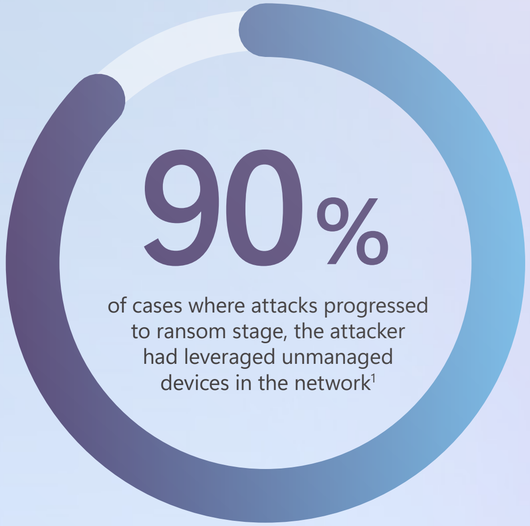
Microsoft Intune will become the single and scalable cross-recovery-tool management plane (announcing), with WinRE becoming the key element of the recovery framework and an Intune-managed client OS. As such, it allows IT professionals to choose the right tool for the job, as Intune will be able to initiate and report on these tools and orchestrate an enterprise endpoint recovery strategy.

In addition, point-in-time restore (Preview) helps PC-users and IT Pros recover individual or groups of devices without the need for technical expertise or lengthy troubleshooting. It offers comprehensive rollback within minutes to the exact state of the system at a previous point in time, including the OS, apps, settings, and local files. It features fast (minutes) and predictable recovery from a broad range of issues without needing extensive troubleshooting. It is also easy to use with built-in guardrails (short retention period, disk space limits) that prioritize reliability.

Cloud rebuild (announcing) enables IT Professionals to completely rebuild an existing PC that is experiencing erratic behaviors or has become inoperative to the user, and where the undesired behavior is difficult or time-consuming to diagnose and remediate. Cloud rebuild reinstalls a completely new Windows 11 OS with the appropriate drivers, making the device usable and reliable. In combination with OneDrive, the user's files remain available, and with support from Windows Autopilot and Backup for Organizations, further device settings can be restored as well. Integration with Microsoft Intune allows for additional configuration and app installation, as well as restoration of PC settings. It will take time to do a rebuild, but the outcome is a reliable user experience, higher user satisfaction, and saved time compared to lengthy diagnostics and costly helpdesk calls.

To manage kiosks in public places that run Windows, we are introducing digital signage mode in preview, so you can protect your public displays from system messages. Digital signage mode operates in parallel to Kiosk mode and enables you to set policies to control what the next steps are once a kiosk enters an error state.

And finally, we have also launched Windows in Mission Critical Services for Microsoft 365, that can prioritize connection to product teams when you are dealing with a major outage.



[1] IBM Cost of a Data Breach Report 2024

Strategies to act on today to build a resiliency program

Modern organizations must prioritize IT resiliency and crisis management integration or risk consequences.

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

These four strategies can help strengthen prevention, response, and recovery efforts:

1 Invest in hardware and software that contain integrated capabilities to support a strategy.

When a disruption's impact exceeds the acceptable level 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, enabling the organization to manage unforeseen disruptions, continue delivering its strategic aims, and return to a viable operating state in conditions of extreme uncertainty.

2 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, 80-90% used unmanaged devices as their initial access point.[1]

3 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]

4 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] Microsoft Digital Defense Report 2024

[2] Windows Security best practices for integrating and managing security tools

For additional reading

1

"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

2

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

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

3

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


Microsoft