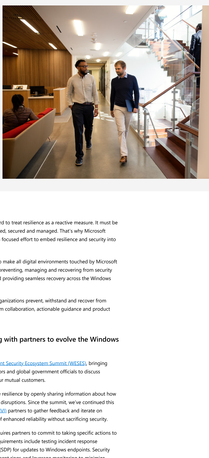
Windows for Business

June 26, 2025

The Windows Resiliency Initiative: Building resilience for a future-ready enterprise

By David Weston, Vice President Enterprise and OS Security at Microsoft



Resilience isn't optional—it's a strategic imperative.

In today's threat landscape, organizations can't afford to treat resilience as a reactive measure. It must be built into the foundation of how systems are designed, secured and managed. That's why Microsoft launched the Windows Resiliency Initiative (WRI)—a focused effort to embed resilience and security into the Windows platform itself.

Announced at Ignite, WRI is an initiative designed to make all digital environments touched by Microsoft products more secure and resilient. WRI prioritizes preventing, managing and recovering from security and reliability incidents, mitigating issues swiftly and providing seamless recovery across the Windows platform.

WRI outlines Microsoft's commitment to helping organizations prevent, withstand and recover from disruptions. This includes three core areas: ecosystem collaboration, actionable guidance and product innovation.

Ecosystem collaboration and learning with partners to evolve the Windows ecosystem

In September 2024, we hosted the Windows Endpoint Security Ecosystem Summit (WESES), bringing together a diverse group of endpoint security vendors and global government officials to discuss strategies for improving resiliency and protecting our mutual customers.

We recognized our shared responsibility to enhance resilience by openly sharing information about how our products function, handle updates and manage disruptions. Since the summit, we've continued this close collaboration with Microsoft Virus Initiative (MVI) partners to gather feedback and insights on Windows platform capabilities to achieve the goal of enhanced reliability without sacrificing security.

As a part of this evolution, our MVI 3.0 program requires partners to commit to taking specific actions to improve the security and reliability of Windows. Requirements include testing incident response processes and following safe deployment practices (SDP) for updates to Windows endpoints. Security product updates must be gradual, leverage deployment rings and leverage monitoring to minimize negative impacts. These practices complement our platform investments, enabling us to deliver greater stability, faster recovery and reduced operational risk for enterprise customers who rely on a secure and reliable Windows environment.

Next month, we will deliver a private preview of the Windows endpoint security platform to a set of MVI partners. The new Windows capabilities will allow them to test building their solutions to run outside the Windows kernel. This means security products like anti-virus and endpoint protection solutions can run in user mode just as apps do. This change will help security developers provide a better reliability and easier recovery resulting in less impact on Windows devices in the event of unexpected issues. We will continue to collaborate deeply with our MVI partners throughout the private preview.

Here are some insights from MVI partners that provide further perspective:

> ***Bitdefender:*** *"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.**
>
> ***CrowdStrike:*** *"We spoke at WESES last year to emphasize the importance of our industry coming together and, since then, have seen significant customer interest in the progress toward greater platform resiliency. Through this collaboration, we've driven substantial improvements to the planned capabilities for the Windows endpoint security platform, paving the way for a more integrated high-performing security solution. With the introduction of MVI 3.0, we've successfully met all the new standards and recognize how these rigorous requirements strengthen the overall ecosystem. We remain fully committed to developing a Windows endpoint security platform-ready product and look forward to leveraging these new capabilities as Microsoft releases them."* **— Alex Ionescu, Chief Technology Innovation Officer, CrowdStrike.**
>
> ***ESET:*** *"The collaboration between ESET and Microsoft technology teams on the proposed Windows endpoint security platform changes continue to be productive with open and ongoing dialogue. Delivering a stable and resilient operating system environment is extremely important for our joint customers, and the ESET team continue to provide detailed feedback to help ensure there is no degradation in the security or performance currently enjoyed by our customers. The increased requirements to maintain MVI membership complement the Windows endpoint security platform, requiring the documentation and adoption of resilient processes to help ensure any incident is either avoided or managed both efficiently and expediently. ESET are committed to the important evolution of both the MVI partnership and the engineering collaboration with Microsoft; something we have valued for several decades."* **—Juraj Malcho, Chief Technology Officer, ESET**
>
> ***SentinelOne:*** *"SentinelOne is pleased to be collaborating with Microsoft to drive a more resilient approach to delivering endpoint protection products on Windows. As a security-first company, we understand that every vendor must live up to stringent engineering, testing and deployment standards and follow software development and deployment best practices. SentinelOne has followed these processes for years and we appreciate the opportunity to provide input to Microsoft and shape changes that can drive better outcomes for our shared customers."* **— Stefan Krantz, SVP and Head of Engineering, SentinelOne**
>
> ***Sophos:*** *"Sophos has been a close collaborator with Microsoft on the Windows endpoint security platform since the Windows Endpoint Security Ecosystem Summit last September, and we're enthusiastic about the advancements introduced with MVI 3.0. This evolution underscores Microsoft's thoughtful approach to equally among its security partners and its ongoing commitment to a resilient and secure ecosystem, aligned with Sophos' dedication to responsible multi-stage software release practices. By establishing MVI 3.0 as a standard for the Windows security ecosystem, we believe the entire industry, vendors and customers alike, will benefit from stronger, more stable protection. We look forward to deepening our partnership with Microsoft and continuing to deliver advanced endpoint security capabilities to protect our shared customers."* **— John Peterson, Chief Development Officer, Sophos**
>
> ***Trellix:*** *"We have a long and trusted partnership with Microsoft, and will keep working closely with the Windows endpoint security platform program as it is nurtured and scaled. Over the last year, we have worked with Microsoft to ensure that our processes and products continue to meet stringent requirements and have engaged with feedback and recommendations to improve operational resilience. Safe deployment practices and transparency advance our entire industry and strengthen cybersecurity outcomes for all."* **— Jim Treinen, SVP, Engineering, Trellix**
>
> ***Trend Micro:*** *"Our collaboration with Microsoft on the Windows endpoint security platform reflects a shared commitment to more resilient enterprise security. We've contributed across technical validation and MVI 3.0 alignment, ensuring the platform is ready for real-world deployment. Just as important, we see the Windows endpoint security platform supporting a more integrated and resilient security model, where platform and protection work together to meet the evolving needs of modern enterprise."* **— Rachel Jin, Chief Enterprise Platform Officer, Trend Micro**
>
> ***WithSecure:*** *"WithSecure is proud to be part of Microsoft's Windows Resiliency Initiative, a collaborative effort to strengthen the Windows ecosystem. Our team has worked diligently to help meet the MVI 3.0 requirements, including improving our safe deployment practices resulting in reduced risk for our customers and partners. Through deep technical collaboration with Microsoft, we're making Windows more secure, resilient and easier for security vendors to work with. As new Windows endpoint security platform capabilities emerge, WithSecure is excited to leverage them to help our customers stay ahead of evolving threats. We look forward to the many security-enhancing opportunities this collaboration will bring."* **— Johannes Rave, Lead Architect of XDR at WithSecure**

Actionable guidance to build organizational resilience: Introducing the Windows Resiliency Initiative e-book

Today, we are happy to introduce the Windows Resiliency Initiative e-book, one result of our commitment to provide guidance for others building organizational resiliency. The e-book is a resource that helps organizations understand how Windows provides foundational practices, strategies and tools to build resilience and embrace a resilience-focused strategy across their IT platform.

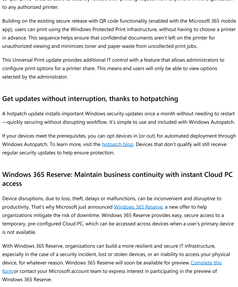
Product innovation to support resiliency on the Windows platform

As an outcome of WRI, organizations can look forward to several new Windows product innovations to support them in their journeys to build infrastructures that can rapidly adapt as needed while maintaining a foundation of resilience. Consider adding these capabilities to your digital repertoire.

Now it's easier than ever to navigate unexpected restarts and recover faster

A key trait of a resilient organization is the ability to maintain productivity and minimize disruptions. But when unexpected restarts occur, they can cause delays and impact business continuity. This is why we are streamlining the unexpected restart experience. We are also adding quick machine recovery, a recovery mechanism for PCs that cannot restart successfully. This change is part of a larger continued effort to reduce disruption in the event of an unexpected restart.

The Windows 11 24H2 release included improvements to crash dump collection which reduced downtime during an unexpected restart to about two seconds for most users. We're introducing a simplified user interface (UI) that pairs with the shortened experience. The updated UI improves readability and aligns better with Windows 11 design principles, while preserving the technical information on the screen for when it is needed.



The new Windows 11 unexpected restart screen

The simplified UI for unexpected restarts will be available starting later this summer on all Windows 11, version 24H2 devices.

In the case of consecutive unexpected restarts, devices can get stuck in the Windows Recovery Environment (Windows RE), impacting productivity and often requiring IT teams to spend significant time troubleshooting and restoring affected devices. This is where quick machine recovery (QMR) can help. When a widespread outage affects devices from starting properly, Microsoft can broadly deploy targeted remediations to affected devices via Windows RE—automating fixes with QMR and quickly getting users to a productive state without requiring complex manual intervention from IT.

We are excited to announce QMR will be generally available later this summer together with the renewed unexpected restart functionality. QMR supports all editions of Windows 11, version 24H2 devices. It is enabled by default for Windows 11 Home devices; IT admins will be in full control and can enable it on devices running Windows 11 Pro and Enterprise. Later this year, Microsoft will release additional capabilities for IT teams to customize QMR.

Microsoft Connected Cache saves internet bandwidth

With today's interconnected work ecosystems, reliable internet bandwidth has become essential for organizations seeking resiliency through a cloud-native approach to device management. Case in point: When all devices in a system simultaneously attempt to download updates, an organization's network bandwidth, especially in branch offices, can be negatively impacted.

Microsoft Connected Cache can help organizations improve their bandwidth when performing upgrades to Windows 11. Windows Autopilot device provisioning, Microsoft Intune application installations and Windows Autopatch monthly updates. Connected Cache will be generally available in the coming weeks.

Internet bandwidth is saved when Connected Cache nodes transparently and dynamically cache the Microsoft-published content that downstream Windows devices need to download. Using this solution, content requests from Delivery Optimization can be served by the locally deployed Connected Cache node instead of the cloud. This results in fast, bandwidth-efficient delivery across devices.

Introducing Universal Print anywhere: Print securely, flexibly and confidentially

Organizational resilience is a holistic concept that extends to printer systems, including third-party drivers that, while often essential to operations, can be an exposure point. Universal Print anywhere, also known as "pull print," enables users to securely release their printing request from anywhere in the organization to any authorized printer.

Building on the existing secure release with QR code functionality (enabled with the Microsoft 365 mobile app), users can print using the Windows Protected Print infrastructure, without having to choose a printer in advance. This sequence helps ensure that confidential documents aren't left on the printer for unauthorized viewing and minimizes toner and paper waste from uncollected print jobs.

This Universal Print update provides additional IT control with a feature that allows administrators to configure print options for a printer share. This means end users will only be able to view options selected by the administrator.

Get updates without interruption, thanks to hotpatching

A hotpatch update installs important Windows security updates once a month without needing to restart—quickly securing without disrupting workflow. It's simple to use and included with Windows Autopatch.

If your devices meet the prerequisites, you can opt devices in (or out) for automated deployment through Windows Autopatch. To learn more, visit the hotpatch blog. Devices that don't qualify will still receive regular security updates to help ensure protection.

Windows 365 Reserve: Maintain business continuity with instant Cloud PC access

Device disruptions, due to loss, theft, delays or malfunctions, can be inconvenient and disruptive to productivity. That's why Microsoft just announced Windows 365 Reserve, a new offer to help organizations mitigate the risk of downtime. Windows 365 Reserve provides easy, secure access to a temporary, pre-configured Cloud PC, which can be accessed across devices when a user's primary device is not available.

With Windows 365 Reserve, organizations can build a more resilient and secure IT infrastructure, especially in the case of a security incident, lost or stolen devices, or an inability to access your physical device, for whatever reason. Windows 365 Reserve will soon be available for preview. Complete this form now to contact your Microsoft account team to express interest in participating in the preview of Windows 365 Reserve.

Prepare for a digital future with resiliency as the foundation

Building organizational resilience is a necessary strategic imperative as we move into a new age of digital capabilities—and risk. Organizations equipped with strategies, best practices and tools that will support their ability to maintain operations as they anticipate, prepare for, respond to and recover from disruptions are more likely to thrive and remain competitive within today's complex and interconnected digital ecosystems.

Microsoft is here to support you as you build resilience in your security strategy with our WRI commitment to helping organizations prepare for uncertainty, minimize risk and emerge stronger from any challenge.

Consider these helpful links:

- Windows Resiliency Initiative e-book
- Microsoft Connected Cache for Enterprise
- Universal Print secure cloud-print infrastructure
- Quick machine recovery
- Upgrading to Windows 11 24H2, the most secure and resilient Windows yet

Disclaimer:
This blog post is for informational purposes only and outlines Microsoft's current product direction and plans. Product availability, licensing terms and capabilities may vary by region and are subject to change. All third-party trademarks are the property of their respective owners.

Editor's note – June 27, 2025 – A quote from Sophos was added.