Windows 11 Security Guide: Raising the security bar for everyone

Introduction

The Security Book not only provides valuable technical information, it also shows how we think about elevating security and resiliency for every organization.

Each Windows release brings new capabilities, stronger defenses, and relentless innovation—because the stakes have never been higher. Today, digital transformation and AI adoption are accelerating at breakneck speed. But so are the tactics of cybercriminals. Leading threats include identity attacks, ransomware, targeted phishing attempts, and business email compromise.[1]

Attackers don't always break in—they sign in, targeting people, applications, and devices at the heart of every organization. That's why security isn't just a feature in Windows; it's our foundation and our future. Even if you don't have a squad of security specialists, Windows is designed to help you defend against the most common and damaging attacks—like phishing, malware, and credential theft—right out of the box.

Microsoft's commitment: security by design; security by default

Microsoft prioritizes security over all else. Announced in 2023, the Microsoft Secure Future Initiative (SFI) is dedicated to advancing cybersecurity in everything we create and provide. Products and services are secure by design and secure by default. For secure operations, we continuously apply what we learn from incidents to improve our security and privacy models, security architecture, and technical controls.

Through the SFI we have mobilized the equivalent of 35,000 full-time engineers committed to the highest security standards into how we design, build, test, and operate our products and services. We synthesize more than 100 trillion signals daily to understand digital threats and criminal cyberactivity.[1] And we thwarted US$4 billion in fraud attempts in one year with new policies, detection models, and investigation methods.[2]

Working together with a shared focus is key to improving global security, from individuals and organizations to governments and industries. The world is moving toward a secure by design and secure by default approach, where technology producers are tasked with incorporating security during the initial design phase, and offering products that deliver protection right out of the box. As part of our commitment to making the world a safer place, we build security into every innovation, including Windows 11.

This secure by design approach spans the Windows edition range including Home, Pro, Enterprise, Enterprise IoT, and Education editions. Hardware and software work together to optimize security, and Copilot+ PCs offer the highest level of Windows protection. Copilot+ PCs are the fastest, most intelligent, and secure Windows devices ever. These groundbreaking PCs come with Secured-core PC protection and the latest safeguards like the Microsoft Pluton security processor and Windows Enhanced Sign-in Security enabled by default.

Better together protection for a modern security landscape

Windows 11 can strengthen security while reducing costs through simpler management and greater flexibility. Windows PCs are easily managed at scale with your modern device management solution like Microsoft Intune, with hundreds of configuration possibilities to meet unique business needs.

Seamless integration with solutions like Microsoft Defender, Entra ID, and Intune[3] opens to the door to multiple benefits, including passwordless authentication, granular management of security policies across endpoints, and ability to leverage new time-saving technologies that increase efficiency and protection.

For example, Windows backup for organizations strengthens identity-based recovery and protection with automated backup from PC to cloud, including user data and personalized settings. Windows Autopatch and hotpatch automate upgrades and updates for Windows PCs and Microsoft 365 apps—covering security and productivity features, drivers, and firmware—with hotpatch enabling faster security and compliance by applying critical updates without a restart.[4] Organizations can also take advantage of new Microsoft Security Copilot agents in Intune to save significant time investigating, identifying, and remediating threats.

With Windows at the center, organizations benefit from layers of security and intelligent management solutions. As a result, they can increase resilience and adopt the latest technologies with confidence, including advanced AI.

Security priorities and benefits

Windows 11 enables you to focus on your work, not your security settings. Hardware and software work together to shrink the attack surface, protect system integrity, and shield valuable data.

Out-of-the-box features such as credential safeguards, malware shields, and application protection led to a reported 62% drop in security incidents, including a 3x reduction in firmware attacks.[5]

Businesses reported a 62% drop in security incidents, including a 3x reduction in firmware attacks.[5]

Identity and data protection

Attackers increasingly target employees and their devices. Windows 11 provides proactive protection against credential theft, with Windows Hello and TPM 2.0 shielding identities, and features like passkeys and secure biometric sign-in virtually eliminating the risk of lost or stolen passwords. Enhanced phishing protection means businesses report 2.9x fewer instances of identity theft with hardware-backed protection.[5,6]

Looking ahead, Windows 11 is already integrating post-quantum cryptography algorithms to safeguard sensitive information against emerging threats from quantum computing.

A streamlined, chip-to-cloud security solution based on Windows 11 improved productivity for IT and security teams by a reported 25%.[7]

Application safeguards

Robust application controls keep business data secure and employees productive. Windows App Control for Business ensures only trusted code runs, while Trusted Signing enables developers to effortlessly sign their applications, supporting authenticity and integrity. Integrated privacy controls and least-privilege principles help organizations and regulators trust that critical data is protected.

Device health and access control

Windows 11 and chip-to-cloud security provide the tools to attest that devices connecting to your network are trustworthy. Enforce security policies and conditional access with cloud-based device management solutions like Intune and Entra ID, plus comprehensive security baselines. Security by default enables secure work anywhere and simplifies IT—businesses with Copilot+ PCs anticipate up to 30% drop in device management time due to improved reliability and support for proactive diagnostics.[7]

Chip-to-cloud security

With Windows 11 devices, hardware and software work together to protect sensitive data from the core of your PC all the way to the cloud. Comprehensive protection helps keep your organization secure, no matter where people work. Microsoft cloud offerings include Windows 365 Cloud PCs, which are accessible from any device and provide Windows security with the power and scalability of the cloud.

Conclusion

We will continue to innovate with security by design and security by default at the heart of every new Windows 11 PC and Windows 11 IoT device. This commitment ensures our products not only meet but exceed the security expectations of our customers—providing robust protection against modern cyber threats while maintaining ease of use and performance.

With intelligent solutions based on Windows, you can innovate with confidence, equipped with enterprise-grade security by default, granular policy management, and device-to-cloud resilience.

Explore the full Security Book for a deep dive into features and best practices: aka.ms/securitybook

Thank you

1. Microsoft Digital Defense Report 2025. In response to growing cyber threats, Microsoft reassigned the equivalent of approximately 34,000 full-time engineers to security initiatives.
2. Microsoft Secure Future Initiative executive summary, April 2025.
3. Sold separately.
4. Eligible Windows 11 Enterprise license required.
5. Windows 11 Survey Report. Techaisle LLC, September 2024. Commissioned by Microsoft. Windows 11 results are in comparison with Windows 10 devices
6. Biometric authentication requires an on-device camera configured for near infrared imaging or fingerprint reader.
7. New Tech: The Projected Total Economic Impact™ of Microsoft Copilot+ PCs. Microsoft-commissioned study by Forrester Consulting, July 2025. Projected benefits for a single composite organization that has US$1 billion annual revenue and 2,000 employees with 80% using Copilot+ PCs. In comparison to a mixed environment of conventional Windows 11 and Windows 10 PCs.

Published November 2025