Windows 11 Security Guide: Powerful security by design

Windows

Introduction

Emerging technologies and evolving business trends bring new opportunities and challenges for organizations of all sizes. As technology and workstyles transform, so does the threat landscape with growing numbers of increasingly sophisticated attacks on organizations and employees.

To thrive, organizations need security to work anywhere. Microsoft's 2022 Work Trend Index shows "cybersecurity issues and risks" are top concerns for business decision-makers, who worry about issues like malware, stolen credentials, devices that lack security updates, and physical attacks on lost or stolen devices.

In the past, a corporate network and software-based security were the first lines of defense. With an increasingly distributed and mobile workforce, attention has shifted to hardware-based endpoint security. People are now the top target for cybercriminals, with 74% of all breaches due to human error, privilege misuses, stolen credentials, or social engineering. Most attacks are financially motivated, and credential theft, phishing, and exploitation of vulnerabilities are the primary attack vectors. Credential theft is the most prevalent attack vector, accounting for 50% of breaches.[1]

At Microsoft, we work hard to help organizations evolve and stay agile while protecting against modern threats. We're committed to helping businesses and their employees get secure—and stay secure. We synthesize 43 trillion signals daily to understand and protect against digital threats. We have more than 8,500 dedicated security professionals across 77 countries and over 15,000 partners in our security ecosystem striving to increase resilience for our customers.[2]

Businesses worldwide are moving toward secure-by-design and secure-by-default strategies. With these models, organizations choose products from manufacturers that consider security as a business requirement, not just a technical feature. With a secure-by-default strategy, businesses can proactively reduce risk and exposure to threats across their organization because products are shipped with security features already built in and enabled.

To help businesses transform and thrive in a new era, we built Windows 11 to be secure by design and secure by default. Windows 11 devices arrive with more security features enabled out of the box. In contrast, Windows 10 devices came with many safeguards turned off unless enabled by IT or employees. The default security provided by Windows 11 elevates protection without needing to configure settings. In addition, Windows 11 devices have been shown to increase malware resistance without impacting performance.[3]

Windows 11 is the most secure Windows ever, built in deep partnership with original equipment manufacturers (OEMs) and silicon manufacturers. Discover why organizations of all sizes, including 90% of Fortune 500 companies, are taking advantage of the powerful default protection of Windows 11.[4]

Security priorities and benefits

Security by design and security by default

Windows 11 is designed with layers of security enabled by default, so you can focus on your work, not your security settings. Out-of-the-box features such as credential safeguards, malware shields, and application protection led to a reported 58% drop in security incidents, including a 3.1x reduction in firmware attacks.[5]

Out-of-the-box features such as credential safeguards, malware shields, and application protection led to a reported 58% drop in security incidents, including a 3.1x reduction in firmware attacks.

In Windows 11, hardware and software work together to shrink the attack surface, protect system integrity, and shield valuable data. New and enhanced features are designed for security by default. For example, Win32 apps in isolation (public preview)[6], token protection (public preview)[6], and Microsoft Intune Endpoint Privilege Management[7] are some of the latest capabilities that help protect your organization and employees against attack. Windows Hello and Windows Hello for Business work with hardware-based features like TPM 2.0 and biometric scanners for credential protection and easier, secure sign-on. Existing security features like BitLocker encryption have also been enhanced to optimize both security and performance.

Protect employees against evolving threats

With attackers targeting employees and their devices, organizations need stronger security against increasingly sophisticated cyberthreats. Windows 11 provides proactive protection against credential theft. Windows Hello and TPM 2.0 work together to shield identities. Secure biometric sign-in virtually eliminates the risk of lost or stolen passwords. And enhanced phishing protection increases safety. In fact, businesses reported 2.8x fewer instances of identity theft with the hardware-backed protection in Windows 11.[5]

Businesses reported 2.8x fewer instances of identity theft with the hardware-backed protection in Windows 11.[5]

Gain mission-critical application safeguards

Help keep business data secure and employees productive with robust safeguards and control for applications. Windows 11 has multiple layers of application security that shield critical data and code integrity. Application protection, privacy controls, and least-privilege principles enable developers to build in security by design. This integrated security protects against breaches and malware, helps keep data private, and gives IT administrators the controls they need. As a result, organizations and regulators can be confident that critical data is protected.

End-to-end protection with modern management

Increase protection and efficiency with Windows 11 and chip-to-cloud security. Microsoft offers comprehensive cloud services for identity, storage, and access management. In addition, Microsoft also provides the tools needed to attest that Windows 11 devices connecting to your network or accessing your data and resources are trustworthy. You can also enforce compliance and conditional access with modern device management (MDM) solutions such as Microsoft Intune[9] and Microsoft Entra ID (formerly known as Azure Active Directory).

Security by default not only enables people to work securely anywhere, but it also simplifies IT. A streamlined, chip-to-cloud security solution based on Windows 11 has improved productivity for IT and security teams by a reported 25%.[8]

Security by design and default

In Windows 11, 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. This simple diagram shows the layers of protection in Windows 11, while each chapter provides a layer-by-layer deep dive into features.

Learn more: Windows security features licensing and edition requirements

Thank you

1. “2023 Data Breach Investigations Report,” Verizon, 2023.
2. “Microsoft Digital Defense Report 2022,” Microsoft, 2022.
3. Compared to Windows 10 devices. “Improve your day-to-day experience with Windows 11 Pro laptops,” Principled Technologies, February 2023.
4. Based on Monthly Active Device data. “Earnings Release FY23 Q3,” Microsoft, April 2023.
5. Windows 11 results are in comparison with Windows 10 devices. “Windows 11 Survey Report,” Techaisle, February 2022.
6. Requires developer enablement.
7. Requires Microsoft Entra ID (formerly AAD) and Microsoft Intune or other modern device management solution product required; sold separately.
8. Commissioned study delivered by Forrester Consulting. “The Total Economic Impact™ of Windows 11 Pro Devices”, December 2022. Note, quantified benefits reflect results over three years combined into a single composite organization that generates $1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices.
9. Sold separately

Part No. September 2023