Windows 11 Security Guide: Security by design. Security by default.

Windows 11

Introduction

Today's organizations face a world of accelerated change, from marketplace fluctuation and sociopolitical events to the rapid adoption of new AI technologies. However, as organizations and industries innovate, so do increasingly sophisticated cybercriminals. Research shows that employees, including their devices, services, and identities, are at the center of attacks on businesses of all sizes. Some leading threats include identity attacks, ransomware, targeted phishing attempts, and business email compromise.[1]

To address the ever-growing and changing threat landscape, we announced the Secure Future Initiative in November 2023. The SFI endeavors to advance cybersecurity protection across all our company and products.

Microsoft is committed to putting security above all else, with products and services that are secure by design and secure by default. We synthesize more than 65 trillion signals daily to understand digital threats and criminal cyberactivity.[1] Through the SFI initiative we've dedicated the equivalent of 34,000 full-time engineers to the highest priority security tasks. We continuously apply what we learn from incidents to improve our security and privacy models, security architecture, and technical controls.

Security by design. Security by default.

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. Windows 11 is secure by design and secure by default, with layers of defense enabled on day one to enhance your protection without the need to first configure settings. This secure-by-design approach spans the Windows edition range including Pro, Enterprise, Enterprise IoT, and Education editions. Copilot+ PCs are the fastest, most intelligent Windows devices ever, and they are also the most secure. These groundbreaking AI PCs come with Secured-core PC protection and the latest safeguards like Microsoft Pluton and Windows Enhanced Sign-in Security enabled by default.

With the exception of Windows IoT Long-Term Servicing Channel (LTSC) editions, support for Windows 10 is ending soon on October 14, 2025. Upgrading or replacing outdated devices before Windows 10 support ends is a critical priority for building a strong security posture. Discover why organizations of all sizes, including 90% of Fortune 500 companies are relying on Windows 11.

Security priorities and benefits

Windows 11 enables you to 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 62% drop in security incidents, including a 3.0x reduction in firmware attacks.[2]

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,[3] token protection,[3] passkeys, and Microsoft Intune Endpoint Privilege Management[4] are some of the latest capabilities that help protect organizations and individual users against attack. Windows Hello and Windows Hello for Business work with hardware-based features like Trusted Platform Module (TPM) 2.0, biometric scanners, and Windows presence sensing to enable easier, secure sign-on, and protection of your data and credentials.

Existing security features are also continuously enhanced across Windows 11. For example, Bitlocker encryption has been optimized for additional security and performance and is available on more devices.

Identity protection

Attackers are increasingly targeting employees and their devices, so 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, and features like passkeys and secure biometric sign-in virtually eliminate the risk of lost or stolen passwords.[5] Enhanced phishing protection also increases safety; in fact, businesses reported 2.9x fewer instances of identity theft with the hardware-backed protection in Windows 11.[2]

Businesses reported **2.9x fewer instances** of identity theft with the hardware-backed protection in Windows 11.[2]

Application safeguards

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

With Trusted Signing, developers can effortlessly sign their applications. This process ensures the authenticity and integrity of the applications while enhancing security features to prevent and mitigate the impacts of malware on Windows.

Device health and access control

Increase protection and efficiency with Windows 11 and chip-to-cloud security. Microsoft provides the tools needed to attest that the devices connecting to your network, or accessing your data and resources, are trustworthy. You can enforce security policies and conditional access with a cloud-based device management solution such as Microsoft Intune, Microsoft Entra ID, and a comprehensive security baseline. 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 improved productivity for IT and security teams by a reported 25%.[6]

Chip-to-cloud security

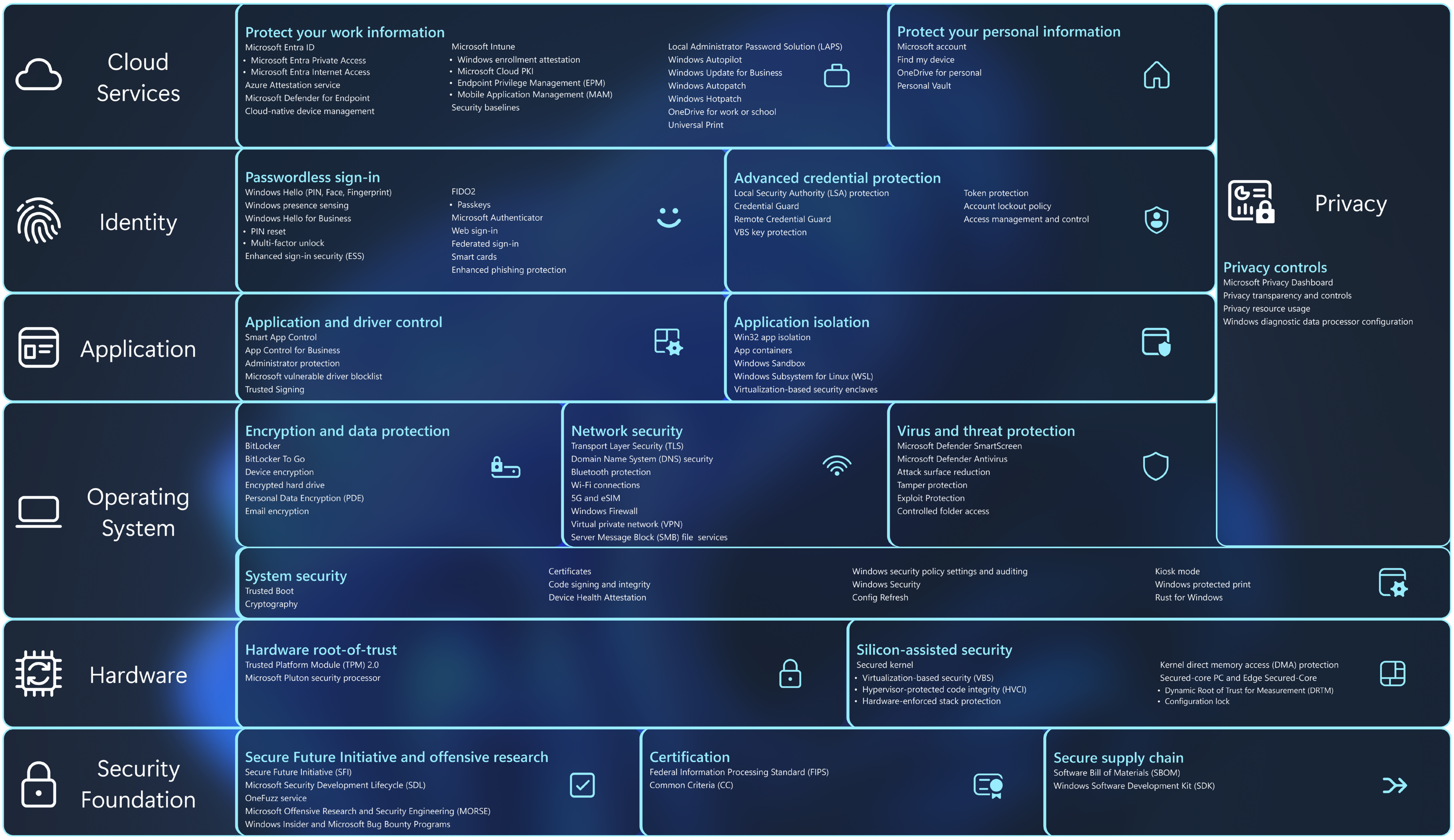
In Windows 11, hardware and software work together to protect sensitive data, from the core of the device all the way to the cloud. Comprehensive protection helps keep organizations secure, no matter where people work.

A streamlined, chip-to-cloud security solution based on Windows 11 improved productivity for IT and security teams by a reported 25%.[6]

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 that our products not only meet, but exceed, the security expectations of our customers by providing robust protection against modern cyber threats while maintaining ease-of-use and performance. By integrating advanced security measures from the ground up, we aim to create a safer digital environment for everyone.

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, demonstrating a layer-by-layer view into features. To explore the feature details thoroughly, refer to the Security Book.



Cloud Services

Protect your work information
Microsoft Entra ID
- Microsoft Entra Private Access
- Microsoft Entra Internet Access

Azure Attestation service
Microsoft Defender for Endpoint
Cloud-native device management
Microsoft Intune
- Windows enrollment attestation
- Microsoft Cloud PKI
- Endpoint Privilege Management (EPM)
- Mobile Application Management (MAM)

Security baselines
Local Administrator Password Solution (LAPS)
Windows Autopilot
Windows Update for Business
Windows Autopatch
Windows Hotpatch
OneDrive for work or school
Universal Print

Protect your personal information
Microsoft account
Find my device
OneDrive for personal
Personal Vault

Identity

Passwordless sign-in
Windows Hello (PIN, Face, Fingerprint)
Windows presence sensing
Windows Hello for Business
- PIN reset
- Multi-factor unlock

Enhanced sign-in security (ESS)
FIDO2
- Passkeys

Microsoft Authenticator
Web sign-in
Federated sign-in
Smart cards
Enhanced phishing protection

Advanced credential protection
Local Security Authority (LSA) protection
Credential Guard
Remote Credential Guard
VBS key protection
Token protection
Account lockout policy
Access management and control

Privacy

Privacy controls
Microsoft Privacy Dashboard
Privacy transparency and controls
Privacy resource usage
Windows diagnostic data processor configuration

Application

Application and driver control
Smart App Control
App Control for Business
Administrator protection
Microsoft vulnerable driver blocklist
Trusted Signing

Application isolation
Win32 app isolation
App containers
Windows Sandbox
Windows Subsystem for Linux (WSL)
Virtualization-based security enclaves

Operating System

Encryption and data protection
BitLocker
BitLocker To Go
Device encryption
Encrypted hard drive
Personal Data Encryption (PDE)
Email encryption

Network security
Transport Layer Security (TLS)
Domain Name System (DNS) security
Bluetooth protection
Wi-Fi connections
5G and eSIM
Windows Firewall
Virtual private network (VPN)
Server Message Block (SMB) file services

Virus and threat protection
Microsoft Defender SmartScreen
Microsoft Defender Antivirus
Attack surface reduction
Tamper protection
Exploit Protection
Controlled folder access

System security
Trusted Boot
Cryptography
Certificates
Code signing and integrity
Device Health Attestation
Windows security policy settings and auditing
Windows Security
Config Refresh
Kiosk mode
Windows protected print
Rust for Windows

Hardware

Hardware root-of-trust
Trusted Platform Module (TPM) 2.0
Microsoft Pluton security processor

Silicon-assisted security
Secured kernel
- Virtualization-based security (VBS)
- Hypervisor-protected code integrity (HVCI)
- Hardware-enforced stack protection

Kernel direct memory access (DMA) protection
Secured-core PC and Edge Secured-Core
- Dynamic Root of Trust for Measurement (DRTM)
- Configuration lock

Security Foundation

Secure Future Initiative and offensive research
Secure Future Initiative (SFI)
Microsoft Security Development Lifecycle (SDL)
OneFuzz service
Microsoft Offensive Research and Security Engineering (MORSE)
Windows Insider and Microsoft Bug Bounty Programs

Certification
Federal Information Processing Standard (FIPS)
Common Criteria (CC)

Secure supply chain
Software Bill of Materials (SBOM)
Windows Software Development Kit (SDK)

▶ **Learn more: https://aka.ms/securitybook**

Thank you

1. Microsoft digital defense report, CISO executive summary, October 2023.
2. Windows 11 Survey Report. Techaisle, September 2024. Windows 11 results are in comparison with Windows 10 devices
3. Requires developer enablement.
4. Sold separately.
5. The Passkey can be saved locally to the Windows device and authenticated via Windows Hello or Windows Hello for Business. Hardware dependent.
6. 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.