Windows 11 Security Guide:
Powerful security from chip to cloud

Built with zero-trust principles at the core to safeguard data and access anywhere, keeping you protected and productive.

Windows

Introduction

The acceleration of digital transformation and the expansion of both remote and hybrid workplaces brings new opportunities to organizations, communities, and individuals. Our work styles have transformed. And now more than ever, employees need simple, intuitive user experiences to collaborate and stay productive, wherever work happens. But the expansion of access and ability to work anywhere has also introduced new threats and risks. According to data from the Microsoft commissioned Security Signals report, 75% of security decision-makers at the vice-president level and above feel the move to hybrid work leaves their organization more vulnerable to security threats. And Microsoft's 2022 Work Trend Index shows "cybersecurity issues and risks" are top concerns for business decisions makers, who worry about issues like malware, stolen credentials, devices that lack security updates, and physical attacks on lost or stolen devices.

At Microsoft, we work hard to help organizations adapt to hybrid work while protecting against modern threats. We're committed to helping customers get secure—and stay secure. With over $20 billion invested in security over five years, more than 8,500 dedicated security professionals, and some 1.3 billion Windows 10 devices used around the world, we have deep insight into the threats our customers face and the steps they need to take to address them.

Organizations worldwide are adopting a zero-trust security model based on the premise that no person or device anywhere can have access until safety and integrity is proven. We know that our customers need modern security solutions, so we built Windows 11 on zero-trust principles for the new era of hybrid work. Windows 11 raises the security baselines with new requirements for advanced hardware and software protection that extends from chip to cloud. With Windows 11, our customers can enable hybrid productivity and new experiences anywhere without compromising security.
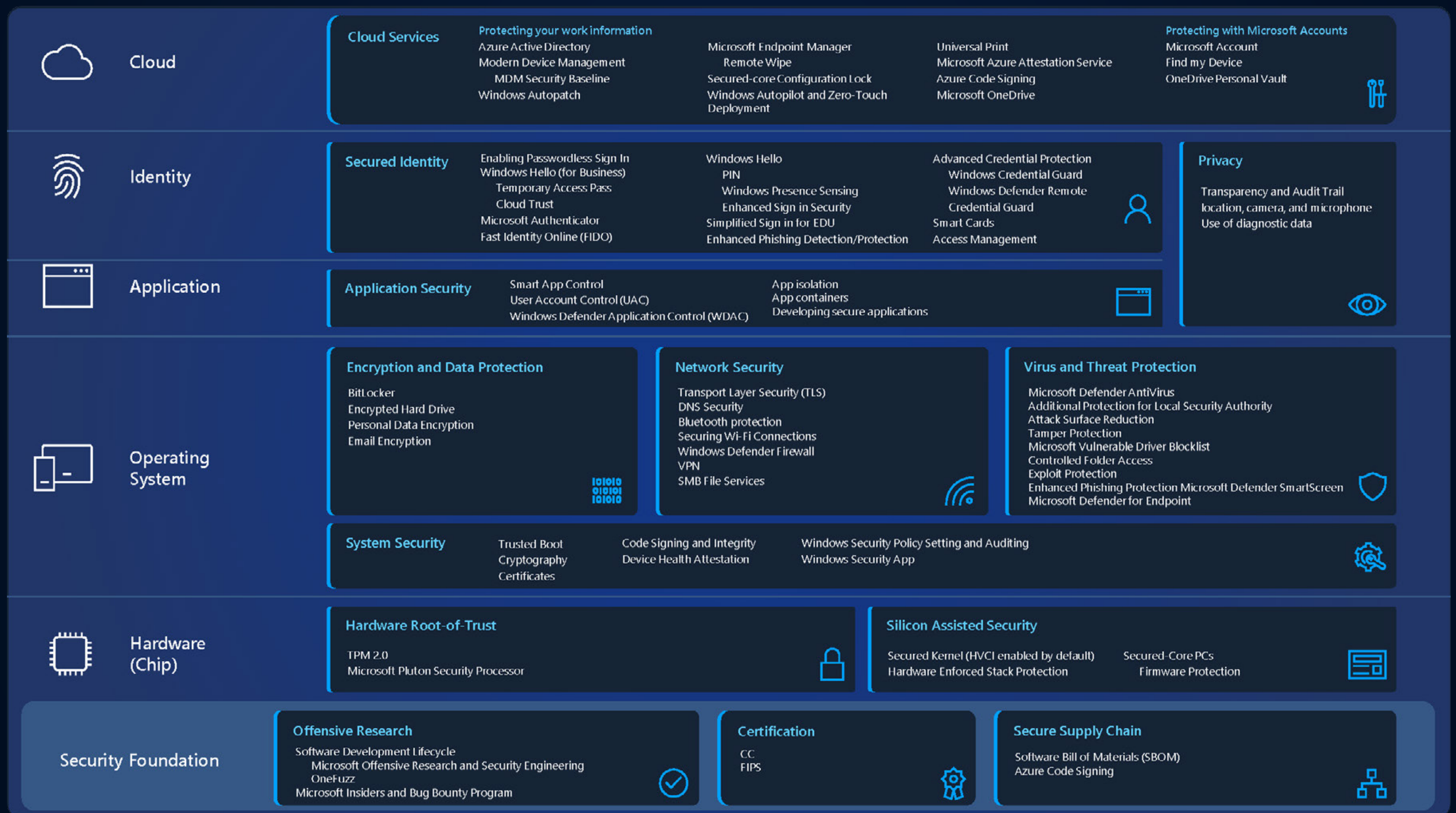
> **Keep reading for a brief intro on Windows 11 security.**
>
> For a deep dive into security features download **Windows 11: Powerful security from chip to cloud** from our website.

Approximately 80% of security decision makers say that software alone is not enough protection from emerging threats.[1]

In Windows 11, hardware and software work together to protect sensitive data from the core of your PC all the way to the cloud. The comprehensive protection helps keep your organization secure, no matter where people work. See the layers of protection in this simple diagram and get a brief overview of our security priorities below.

Cloud

Cloud Services

Protecting your work information
- Azure Active Directory
- Modern Device Management
  - MDM Security Baseline
- Windows Autopatch

- Microsoft Endpoint Manager
- Remote Wipe
- Secured-core Configuration Lock
- Windows Autopilot and Zero-Touch Deployment

- Universal Print
- Microsoft Azure Attestation Service
- Azure Code Signing
- Microsoft OneDrive

Protecting with Microsoft Accounts
- Microsoft Account
- Find my Device
- OneDrive Personal Vault

Identity

Secured Identity

- Enabling Passwordless Sign In
- Windows Hello (for Business)
  - Temporary Access Pass
  - Cloud Trust
- Microsoft Authenticator
- Fast Identity Online (FIDO)

- Windows Hello
  - PIN
- Windows Presence Sensing
- Enhanced Sign in Security
- Simplified Sign in for EDU
- Enhanced Phishing Detection/Protection

- Advanced Credential Protection
  - Windows Credential Guard
  - Windows Defender Remote Credential Guard
- Smart Cards
- Access Management

Privacy
- Transparency and Audit Trail location, camera, and microphone
- Use of diagnostic data

Application

Application Security

- Smart App Control
- User Account Control (UAC)
- Windows Defender Application Control (WDAC)

- App isolation
- App containers
- Developing secure applications

Operating System

Encryption and Data Protection
- BitLocker
- Encrypted Hard Drive
- Personal Data Encryption
- Email Encryption

Network Security
- Transport Layer Security (TLS)
- DNS Security
- Bluetooth protection
- Securing Wi-Fi Connections
- Windows Defender Firewall
- VPN
- SMB File Services

Virus and Threat Protection
- Microsoft Defender AntiVirus
- Additional Protection for Local Security Authority
- Attack Surface Reduction
- Tamper Protection
- Microsoft Vulnerable Driver Blocklist
- Controlled Folder Access
- Exploit Protection
- Enhanced Phishing Protection Microsoft Defender SmartScreen
- Microsoft Defender for Endpoint

System Security
- Trusted Boot
- Cryptography Certificates
- Code Signing and Integrity
- Device Health Attestation
- Windows Security Policy Setting and Auditing
- Windows Security App

Hardware (Chip)

Hardware Root-of-Trust
- TPM 2.0
- Microsoft Pluton Security Processor

Silicon Assisted Security
- Secured Kernel (HVCI enabled by default)
- Hardware Enforced Stack Protection
- Secured-Core PCs
- Firmware Protection

Security Foundation

Offensive Research
- Software Development Lifecycle
  - Microsoft Offensive Research and Security Engineering
  - OneFuzz
- Microsoft Insiders and Bug Bounty Program

Certification
- CC
- FIPS

Secure Supply Chain
- Software Bill of Materials (SBOM)
- Azure Code Signing

How Windows 11 enables zero-trust protection

Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education.

A zero-trust security model gives the right people the right access at the right time. Zero-trust security is based on three principles:

1. Reduce risk by explicitly verifying data points such as user identity, location, and device health for every access request, without exception.

2. When verified, give people and devices access to only necessary resources for the necessary amount of time.

3. Use continuous analytics to drive threat detection and improve defenses.

You should continue to strengthen your zero-trust posture as well. To improve threat detection and defenses, verify end-to-end encryption and use analytics to gain visibility.

Verify explicitly   **Use least privileged access**   **Assume breach**

For Windows 11, the zero-trust principle of "verify explicitly" applies to risks introduced by both devices and people. Windows 11 provides chip-to-cloud security, enabling IT administrators to implement strong authorization and authentication processes with tools such as our premier solution Windows Hello for Business. IT administrators also gain attestation and measurements for determining if a device meets requirements and can be trusted. In addition, Windows 11 works out-of-the-box with Microsoft Endpoint Manager and Azure Active Directory, so access decisions and enforcement are seamless. Plus, IT administrators can easily customize Windows 11 to meet specific user and policy requirements for access, privacy, compliance, and more.

Individual users also benefit from powerful safeguards including new standards for hardware-based security and passwordless protection that help safeguard data and privacy.

Security, by default

Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education.

Nearly 90% of security decision makers surveyed say outdated hardware leaves organizations more open to attacks and using modern hardware would help protect against future threats.[1] Building on the innovations of Windows 10, we've worked with our manufacturer and silicon partners to provide additional hardware security capabilities to meet the evolving threat landscape and enable hybrid work and learning. The new set of hardware security requirements that comes with Windows 11 supports new ways of working with a foundation that is even stronger and more resilient to attacks.

Enhanced hardware and operating system security

Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education.

With hardware-based isolation security that begins at the chip, Windows 11 stores sensitive data behind additional barriers separated from the operating system. As a result, information including encryption keys and user credentials are protected from unauthorized access and tampering.

In Windows 11, hardware and software work together to protect the operating system. For example, new devices come with virtualization-based security (VBS) and Secure Boot built-in and enabled by default to contain and limit malware exploits.[2]

Robust application security and privacy controls

Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education.

To help keep personal and business information protected and private, Windows 11 has multiple layers of application security that safeguard critical data and code integrity. Application isolation and controls, code integrity, privacy controls, and least-privilege principles enable developers to build in security and privacy from the ground up. This integrated security protects against breaches and malware, helps keep data private, and gives IT administrators the controls they need.

In Windows 11, Microsoft Defender Application Guard[3] uses Hyper-V virtualization technology to isolate untrusted websites and Microsoft Office files in containers, separate from and unable to access the host operating system and enterprise data. To protect privacy, Windows 11 also provides more controls over which apps and features can collect and use data such as the device's location, or access resources like camera and microphone.

Secured identities

Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education.

Passwords have been an important part of digital security for a long time, and they're also a top target for cybercriminals. Windows 11 provides powerful protection against credential theft with chip-level hardware security. Credentials are protected by layers of hardware and software security such as TPM 2.0, VBS, and/or Windows Defender Credential Guard, making it harder for attackers to steal credentials from a device. And with Windows Hello, users can quickly sign in with face, fingerprint, or PIN for passwordless protection.[4]

Connecting to cloud services

Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education.

Microsoft offers comprehensive cloud services for identity, storage, and access management in addition to the tools needed to attest that Windows 11 devices connecting to your network are trustworthy. You can also enforce compliance and conditional access with a modern device management (MDM) service such as Microsoft Endpoint Manager, which works with Azure Active Directory and Microsoft Azure Attestation to control access to applications and data through the cloud.[5]

Thank you