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.
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 the new data from the Microsoft commissioned Security Signals report, 75% of security decision-makers at the vice-president level and above feel that the move to hybrid work leaves their organization more vulnerable to security threats.

At Microsoft, we work hard to empower every person and every organization on the planet to achieve more. We’re committed to helping customers get secure—and stay secure. With over $1 billion invested in security each year, more than 3,500 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.

Our customers need modern security solutions that deliver end-to-end protection anywhere. Windows 11 is a build with Zero Trust principles for the new era of hybrid work. Zero Trust is a security model based on the premise that no user or device anywhere can have access until safety and integrity is proven. Windows 11 raises the security baselines with new requirements built into both hardware and software for advanced protection from chip to cloud. With Windows 11, our customers can enable hybrid productivity and new experiences without compromising security.

In Windows 11, hardware and software work together for protection from the CPU all the way to the cloud. See the layers of protection in this simple diagram and get a brief overview of our security priorities below.

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 for protection from the CPU all the way to the cloud. See the layers of protection in this simple diagram and get a brief overview of our security priorities below.
How Windows 11 enables Zero Trust protection

The Zero Trust principles are threefold. First, verify explicitly. That means always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies. The second uses least-privileged access, which limits user access with just-in-time and just-enough-access, risk-based adaptive polices, and data protection to help secure both data and productivity. And lastly, assume breach. Assume breach operates in a manner that minimizes blast radius and segments access. Verify end-to-end encryption and use analytics to gain visibility to improve threat detection and defenses.

For Windows 11, the Zero Trust principle of verify explicitly applies to the risks introduced by both devices and users. Windows 11 provides chip-to-cloud security, giving IT administrators the attestation and measurements to determine whether a device meets requirements and can be trusted. And Windows 11 works out of the box with Microsoft Intune 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. Now, all users can replace potentially risky passwords by providing secure proof of identity with the Microsoft Authenticator app, signing in with face or fingerprint,² a security key, or a verification code sent to a phone or email.
Overview of Windows 11 security priorities

Security, by default

Nearly 90% of security decision makers surveyed say that outdated hardware leaves organizations more open to attacks, and that more 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 more hybrid work and learning. The new set of hardware security requirements that comes with Windows 11 is designed to build a foundation that is even stronger and more resilient to attacks.

Enhanced hardware and operating system security

With hardware-based isolation security that begins at the chip, Windows 11 stores sensitive data behind additional security 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, with virtualization-based security (VBS) and Secure Boot built-in and enabled by default on new CPUs. Even if bad actors get in, they don’t get far. VBS uses hardware virtualization features to create and isolate a secure region of memory from the operating system. This isolated environment hosts multiple security solutions, greatly increasing protection from vulnerabilities in the operating system, and preventing the use of malicious exploits. In combination with device health attestation with cloud services Windows 11 is zero trust ready.
Overview of Windows 11 security priorities

Robust application security and privacy controls

To help keep personal and business information protected and private, Windows 11 has multiple layers of application security to 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 Guard³ 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 provide more controls over which apps and features can collect and use data such as device location or access resources like camera and microphone.

Secured identities

Passwords are inconvenient to use and prime targets for cybercriminals—and they’ve been an important part of digital security for years. That changes with the passwordless protection available with Windows 11. After a secure authorization process, credentials are protected behind layers of hardware and software security, giving users secure, passwordless access to their apps and cloud services.

Individual users can remove the password from their Microsoft account and use the Microsoft Authenticator app,⁴ Windows Hello,⁵ a FIDO2 security key, a smart card, or a verification code sent to their phone or email. IT administrators and consumers can set up Windows 11 devices as passwordless out-of-the-box, taking advantage of technologies such as Windows Hello in alignment with Fast Identity Online (FIDO) standards.

Windows 11 protects credentials with chip-level hardware security including TPM 2.0 combined with VBS and Windows Defender Credential Guard.
Overview of Windows 11 security priorities

Connecting to cloud services

Windows 11 security extends zero-trust all the way to the cloud, enabling policies, controls, procedures, and technologies that work together to protect your devices, data, applications, and identities from anywhere.

Microsoft offers comprehensive cloud services for identity, storage and access management in addition to the tools to attest that any Windows device connecting to your network is trustworthy. You can also enforce compliance and conditional access with a modern device management (MDM) service such as Microsoft Intune that works with Azure Active Directory to control access to applications and data through the cloud.⁶
Thank you

²Requires compatible hardware with biometric sensors.
³Windows 10 Pro and above support Application Guard protection for Microsoft Edge. Microsoft Defender Application Guard for Office requires Windows 10 Enterprise, and Microsoft 365 E5 or Microsoft 365 E5 Security.
⁴Get the free Microsoft Authenticator app for Android or iOS https://www.microsoft.com/en-us/account/authenticator?cmp=h66ftb_42hbak
⁵Windows Hello supports multi-factor authentication including facial recognition, fingerprint, and PIN. Requires specialized hardware such as fingerprint reader, illuminated IT sensor or other biometric sensors and capable devices.
⁶Subscription sold separately.