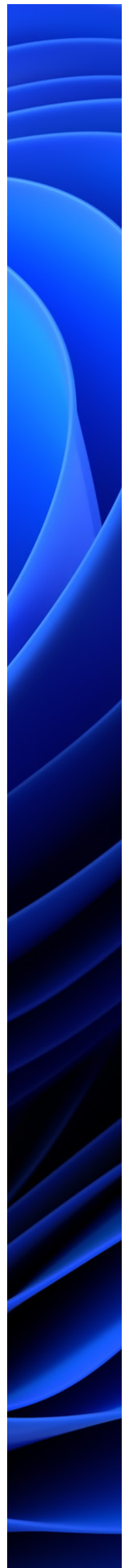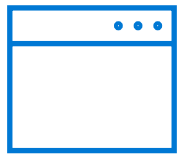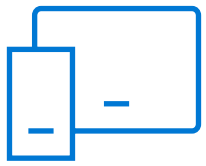# Windows 11 Security Book:
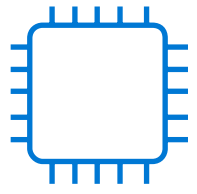# Powerful security from chip to cloud

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

:: Windows

Table of contents

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

2

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.

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	Code Signing and Integrity	Windows Security Policy Setting and Auditing
Cryptography	Device Health Attestation	Windows Security App
Certificates		

Hardware (Chip)

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

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

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**
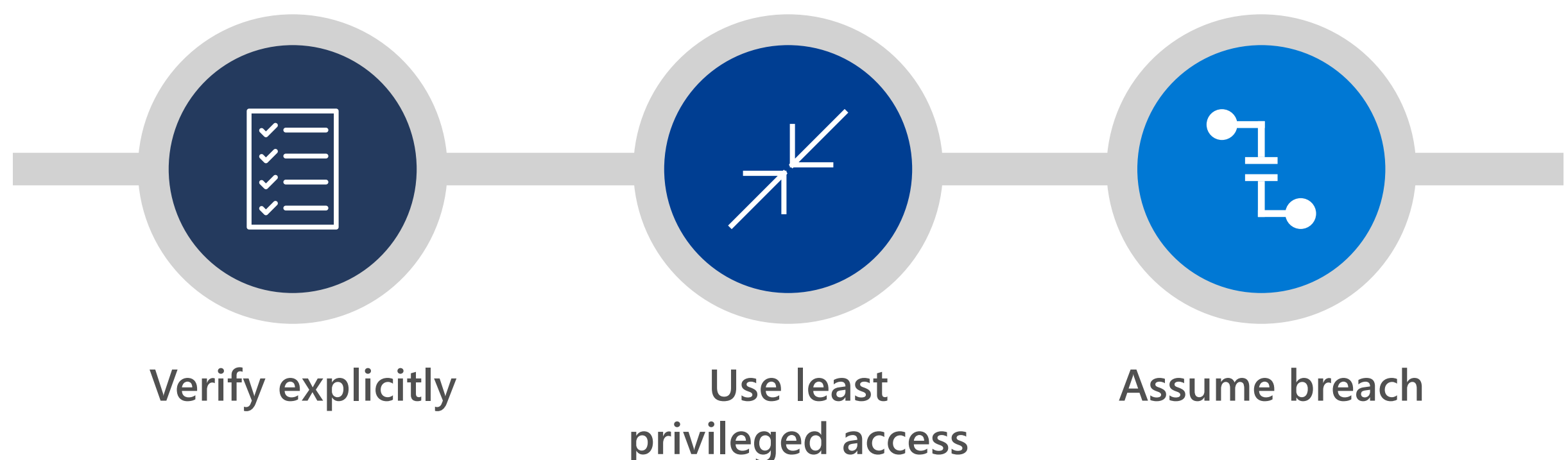
For Windows 11, the zero-trust principle of "verify explicitly" applies to risks introduced by both devices and people. Windows 11 provides chip-to-cloud security, enabling IT administrators to implement strong authorization and authentication processes with tools such as our premier solution Windows 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.

Overview of Windows 11 security priorities

Security, by default

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

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

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.
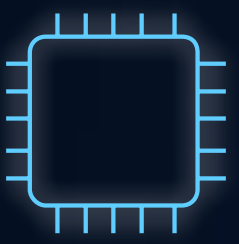
Secured identities

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

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]

Hardware
Security

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

Today's ever-evolving threats require strong alignment between hardware and software technologies to keep users, data, and devices protected. The operating system alone cannot protect from the wide range of tools and techniques cybercriminals use to compromise a computer. Once they gain a foothold, intruders can be difficult to detect while engaging in multiple nefarious activities that range from stealing important data and credentials to implanting malware into low-level device firmware. Once malware is installed in firmware, it becomes difficult to identify and remove. These new threats call for computing hardware that is secure down to the very core, including hardware chips and processors which store sensitive business information. With hardware-based protection, we can enable strong mitigation against entire classes of vulnerabilities that are difficult to thwart with software alone. Hardware-based protection can also increase the system's overall security without measurably slowing performance, compared to implementing the same capability in software.

With Windows 11, Microsoft has raised the hardware security bar to design the most secure version of Windows ever from chip to cloud. We have carefully chosen the hardware requirements and default security features based on threat intelligence, global regulatory requirements, and our own Microsoft Security team. We have worked with our chip and device manufacturing partners to integrate advanced security capabilities across software, firmware, and hardware.

Through a powerful combination of hardware root-of-trust and silicon-assisted security, Windows 11 delivers built-in hardware protection out of the box.

Hardware root-of-trust

A hardware root-of-trust helps protect and maintain the integrity of the system as the device powers on, loads firmware, and then launches the operating system. Hardware root-of-trust meets multiple important security goals for the system. For example, the Secure Boot process provides a secure start up environment that only allows devices to boot with software trusted by the OEM. When the PC starts, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as Option ROMs), EFI applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system. Rollback protection also prevents the system from rolling back to older versions of firmware.

In addition, hardware root-of-trust provides a highly secure area isolated from the operating system and applications for storing cryptographic keys, data, and code. This protection helps mitigate attacks against the Windows authentication stack, single sign-on tokens, the Windows Hello biometric stack, and BitLocker volume encryption keys.

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. TPMs provide security and privacy benefits for system hardware, platform owners, and users. Windows Hello, BitLocker, Windows Defender System Guard, and other Windows features rely on the TPM for capabilities such as key generation, secure storage, encryption, boot integrity measurements, and attestation. These capabilities in turn help customers strengthen protection of their identities and data.

The 2.0 version of the specification includes support for newer algorithms, which can improve driver signing and key generation performance. Starting with Windows 10, Microsoft's hardware certification requires all new Windows PCs to include TPM 2.0 built in and enabled by default. With Windows 11, both new and upgraded devices must have TPM 2.0. The requirement strengthens the security posture across all Windows 11 devices and helps ensure that these devices can benefit from future security capabilities that depend on a hardware root-of-trust.

Learn more about the [Windows 11 TPM specifications](#) and [enabling TPM 2.0 on your PC](#).

Microsoft Pluton

Note: This section applies to all Windows 11 editions, including Home, Pro, Enterprise, and Education.

The Microsoft Pluton security processor is designed by Microsoft in partnership with silicon partners. Pluton enhances the protection of Windows 11 devices, including Secured-core PCs, with a hardware root-of-trust that provides additional protection for cryptographic keys and other secrets. Pluton is designed to reduce the attack surface as it integrates

the security chip directly into the processor. It can be used with a discreet TPM 2.0 or as a standalone security processor.

When root of trust is located on a separate, discrete chip on the motherboard, the communication path between the root-of-trust and the CPU can be vulnerable to physical attack. Embedding Pluton into the CPU makes it harder to target the communication path for exploitation.

Pluton supports the TPM 2.0 industry standard allowing customers to immediately benefit from the enhanced security in Windows features that rely on TPMs including BitLocker, Windows Hello, and Windows Defender System Guard. In addition to providing root-of-trust, Pluton also supports other security functionality beyond what is possible with the TPM 2.0 specification, and this extensibility allows for additional Pluton firmware and OS features to be delivered over time via Windows Update. The first example of such a scenario was developed in close partnership with multiple OEMs. Windows will use Pluton to securely integrate with other hardware security components on the system to provide greater visibility into the state of the platform to the Windows end user and eventually to IT administrators, who will have new platform resiliency signals that can be used for zero-trust conditional access workflows.

As with other TPMs, credentials, encryption keys, and other sensitive information cannot be easily extracted from Pluton even if an attacker has installed malware or has complete physical possession of the PC. Storing sensitive data like encryption keys securely within the Pluton processor, which is isolated from the rest of the system, helps ensure that attackers cannot access sensitive data—even if attackers use emerging techniques like speculative execution.

Pluton also solves the major security challenge of keeping its own root-of-trust firmware up to date across the entire PC ecosystem. Today customers receive updates to their security firmware from a variety of different sources, which may make it difficult for customers to get alerts about security updates resulting in systems remaining in a vulnerable state. Pluton provides a flexible, updateable platform for its firmware that implements end-to-end security functionality authored, maintained, and updated by Microsoft. Pluton is integrated with the Windows Update service, benefiting from over a decade of operational experience reliably delivering updates across over a billion endpoint systems.

Microsoft Pluton is available with select new Windows PCs.

Learn more: [Meet the Microsoft Pluton processor – The security chip designed for the future of Windows PCs | Microsoft Security Blog](#)

Silicon assisted security

In addition to a modern hardware root-of-trust, there are numerous other capabilities in the latest chips that harden the operating system against threats such as by protecting the boot process, safeguarding the integrity of memory, isolating security sensitive compute logic, and more.

Secured kernel

Virtualization-based security (VBS), also known as core isolation, is a critical building block in a secure system. VBS uses hardware virtualization features to host a secure kernel separated from the operating system. This means that even if the operating system is compromised, the secure kernel is still protected.

The isolated VBS environment protects processes, such as security solutions and credential managers, from other processes running in memory. Even if malware gains access to the main OS kernel, the hypervisor and virtualization hardware help prevent the malware from executing unauthorized code or accessing platform secrets in the VBS environment. VBS implements virtual trust level 1 (VTL1), which has higher privilege than the virtual trust level 0 (VTL0) implemented in the main kernel.

Since more privileged VTLs can enforce their own memory protections, higher VTLs can effectively protect areas of memory from lower VTLs. In practice, this allows a lower VTL to protect isolated memory regions by securing them with a higher VTL. For example, VTL0 could store a secret in VTL1, at which point only VTL1 could access it. Even if VTL0 is compromised, the secret would be safe.

Hypervisor-protected code integrity (HVCI), also called memory integrity, uses VBS to run Kernel Mode Code Integrity (KMCI) inside the secure VBS environment instead of the main Windows kernel. This helps prevent attacks that attempt to modify kernel mode code such as drivers. The KMCI role is to check that all kernel code is properly signed and hasn't been tampered with before it is allowed to run.

HVCI ensures that only validated code can be executed in kernel-mode. The hypervisor leverages processor virtualization extensions to enforce memory protections that prevent kernel-mode software from executing code that has not been first validated by the code integrity subsystem. HVCI protects against common attacks like WannaCry that rely on the ability to inject malicious code into the kernel. HVCI can prevent injection of malicious kernel-mode code even when drivers and other kernel-mode software have bugs.

All Windows 11 devices will support HVCI and most new devices will come with VBS and HVCI protection turned on by default.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

12

Hardware-enforced stack protection

Note: This section applies to all Windows 11 editions:Home, Pro, Pro Workstation, Enterprise, Pro Education and Education and OEM Specific.

Hardware-enforced stack protection integrates software and hardware for a modern defense against cyberthreats such as memory corruption and zero-day exploits. Based on Control-flow Enforcement Technology (CET) from Intel and AMD Shadow Stacks, hardware-enforced stack protection is designed to protect against exploit techniques that try to hijack return addresses on the stack.

Application code includes a program processing stack that hackers seek to corrupt or disrupt in a type of attack called stack smashing. When defenses like executable space protection began thwarting such attacks, hackers turned to new methods like return oriented programming. Return oriented programming, a form of advanced stack smashing, can be used to bypass defenses, hijack the data stack, and ultimately force a device to perform harmful operations.

To guard against these control-flow hijacking attacks, the Windows kernel creates a separate "shadow stack" for return addresses. Windows 11 extends stack protection capabilities to provide both user mode and kernel mode support.

Windows 11 Secured-core PCs

Note: This section applies to all Windows 11 edition: Home, Pro, Pro Workstation, Enterprise, Pro Education and Education.

The March 2021 Security Signals report shows that more than 80% of enterprises have experienced at least one firmware attack in the past two years. For customers in data sensitive industries like financial services, government, and healthcare, Microsoft has worked with OEM partners to offer a special category of devices called Secured-core PCs. The devices ship with additional security measures enabled at the firmware layer, or device core, that underpins Windows.

Secured-core PCs help prevent malware attacks and minimize firmware vulnerabilities by launching into a clean and trusted state at startup with a hardware-enforced root of trust. Virtualization-based security comes enabled by default. And with built-in hypervisor-protected code integrity (HVCI) shielding system memory, Secured-core PCs ensure that all executables are signed by known and approved authorities only.

Secured-core PC protection against physical attacks

Secured-core PCs also protect against physical threats such as drive-by Direct Memory Access (DMA) attacks. PCIe hot plug devices such as Thunderbolt, USB4, and CFexpress allow users to attach new classes of external peripherals, including graphics cards or other

PCI devices, to their PCs with the plug-and-play ease of USB. Because PCI hot plug ports are external and easily accessible, PCs are susceptible to drive-by DMA attacks. Memory access protection (also known as Kernel DMA Protection) protects against these attacks by preventing external peripherals from gaining unauthorized access to memory.

Drive-by DMA attacks typically happen quickly while the system owner isn't present. The attacks are performed using simple to moderate attacking tools created with affordable, off-the-shelf hardware and software that do not require the disassembly of the PC. For example, a PC owner might leave a device for a quick coffee break. Meanwhile, an attacker plugs an external tool into a port to steal information or inject code that gives the attacker remote control over the PCs, including the ability to bypass the lock screen.

With memory access protection built in and enabled, Secured-core PCs protect against physical attack wherever people work.

Firmware protection in Secured-core PCs

Secured-core PCs provide multiple layers of robust protections against hardware and firmware attacks.

Sophisticated malware attacks may commonly attempt to install "bootkits" or "rootkits" on the system to evade detection and achieve persistence. This malicious software may run at the firmware level prior to Windows being loaded, or during the Windows boot process itself, enabling the system to start with the highest level of privilege. Because critical subsystems in Windows leverage virtualization-based security, protecting the hypervisor becomes increasingly important. To ensure that no unauthorized firmware or software can start before the Windows bootloader, Windows PCs rely on the Unified Extensible Firmware Interface (UEFI) Secure Boot standard, a baseline security feature of all Windows 11 PCs. Secure boot helps ensure that only authorized firmware and software with trusted digital signatures can execute. In addition, measurements of all boot components are securely stored in the TPM to help establish a non-repudiable audit log of the boot called the Static Root of Trust for Measurement (SRTM).
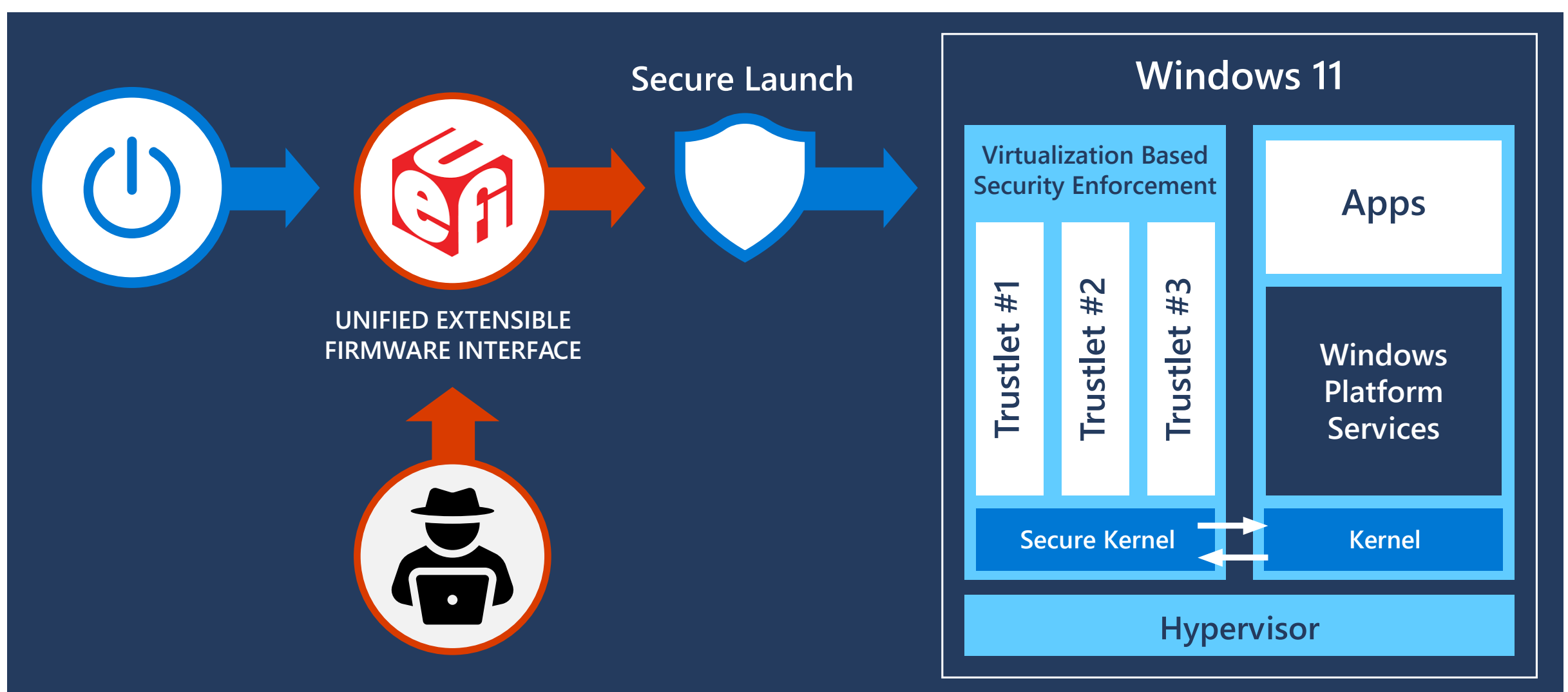
Thousands of PC vendors produce numerous device models with diverse UEFI firmware components, which in turn creates an incredibly large number of SRTM signatures and measurements at bootup. Because these signatures and measurements are inherently trusted by secure boot, it can be challenging to constrain trust to only what is needed to boot on any specific device. Traditionally, block lists and allow lists have been the two main techniques used to constrain trust, and they continue to expand if devices rely only on SRTM measurements.

In Secured-core PCs, Windows Defender System Guard Secure Launch protects bootup with a technology known as the Dynamic Root of Trust for Measurement (DRTM). With DRTM, the system initially follows the normal UEFI Secure Boot process. However, before launching, the system enters a hardware-controlled trusted state that forces the CPU(s) down a hardware-secured code path. If a malware rootkit/bootkit has bypassed UEFI Secure Boot and resides

in memory, DRTM will prevent it from accessing secrets and critical code protected by the virtualization-based security environment. Firmware Attack Surface Reduction technology can be used instead of DRTM on supporting devices such as Microsoft Surface.

System Management Mode (SMM) isolation is an execution mode in x86-based processors that runs at a higher effective privilege than the hypervisor. SSM complements the protections provided by DRTM by helping to reduce the attack surface. Relying on capabilities provided by silicon providers like Intel and AMD, SMM isolation enforces policies that implement restrictions such as preventing SMM code from accessing OS memory. The SMM isolation policy is included as part of the DRTM measurements that can be sent to a verifier like Microsoft Azure Remote Attestation.

Learn more about Dynamic Root of Trust Measurement and SMM isolation.

Table of Contents | Introduction | **Hardware Security** | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

15

Operating System Security

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

Windows 11 is the most secure Windows yet with extensive security measures in the operating system designed to help keep devices, identities, and information safe. These measures include built-in advanced encryption and data protection, robust network and system security, and intelligent safeguards against ever evolving viruses and threats.

System security

Trusted Boot (Secure Boot + Measured Boot)

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

Windows 11 requires all PCs to use Unified Extensible Firmware Interface (UEFI)'s Secure Boot feature. When a Windows 11 device starts, Secure Boot and Trusted Boot work together to prevent malware and corrupted components from loading. Secure Boot provides initial protection then Trusted Boot picks up the process.

Secure Boot makes a safe and trusted path from the Unified Extensible Firmware Interface (UEFI) through the Windows kernel's Trusted Boot sequence. Malware attacks on the Windows boot sequence are blocked by the signature-enforcement handshakes throughout the boot sequence between the UEFI, bootloader, kernel, and application environments.

To reduce the risk of firmware rootkits, the PC verifies that firmware is digitally signed as it begins the boot process. Then Secure Boot checks the OS bootloader's digital signature as well as all code that runs prior to the operating system starting to ensure the signature and code are uncompromised and trusted by the Secure Boot policy.

Trusted Boot picks up the process that began with Secure Boot. The Windows bootloader verifies the digital signature of the Windows kernel before loading it. The Windows kernel, in turn, verifies every other component of the Windows startup process, including boot drivers, startup files, and your antimalware product's early-launch antimalware (ELAM) driver. If any of these files have been tampered with, the bootloader detects the problem and refuses to load the corrupted component. Often, Windows can automatically repair the corrupted component, restoring the integrity of Windows and allowing the PC to start normally.

Tampering or malware attacks on the Windows boot sequence are blocked by the signature enforcement handshakes between the UEFI, bootloader, kernel, and application environments.

For more information about these features and how they help prevent root kits and boot kits from loading during the startup process, see Secure the Windows boot process.

Cryptography

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

Cryptography is designed to protect user and system data. The cryptography stack in Windows extends from the chip to the cloud, enabling Windows, applications, and services to protect system and user secrets. For example, data can be encrypted so that only a specific reader with a unique key can read it. As a basis for data security, cryptography helps prevent anyone except the intended recipient from reading data, performs integrity checks to ensure data is free of tampering, and authenticates identity to ensure that communication is secure.

Windows 11 cryptography is certified to meet the Federal Information Processing Standard (FIPS) 140. FIPS 140 certification ensures that US government approved algorithms are correctly implemented. Learn more about FIPS 140 validation.

Windows cryptographic modules provide low-level primitives such as:

- Random number generators (RNG)

- Support for AES 128/256 with XTS, ECB, CBC, CFB, CCM, GCM modes of operation; RSA and DSA 2048, 3072, and 4096 key sizes; ECDSA over curves P-256, P-384, P-521

- Hashing (support for SHA1, SHA-256, SHA-384, and SHA-512)

- Signing and verification (padding support for OAEP, PSS, PKCS1)

Table of Contents | Introduction | Hardware Security | **Operating System Security** | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

18

- Key agreement and key derivation (support for ECDH over NIST-standard prime curves P-256, P-384, P-521 and HKDF)

Application developers can use these cryptographic modules to perform low-level cryptographic operations (BCrypt), key storage operations (NCrypt), protect static data (DPAPI), and securely share secrets (DPAPI-NG).

Developers can access the modules on Windows through the Crypto API (CAPI) and the Cryptography Next Generation API (CNG), which are both powered by Microsoft's open-source cryptographic library SymCrypt. SymCrypt supports complete transparency through its open-source code. In addition, SymCrypt offers performance optimization for cryptographic operations by taking advantage of assembly and hardware acceleration when available.

SymCrypt is part of Microsoft's commitment to transparency, which includes the global Microsoft Government Security Program that aims to provide confidential security information and resources people need to trust Microsoft's products and services. The program offers controlled access to source code and exchange threat and vulnerability information, opportunities to engage on technical content about Microsoft's products and services, and access to five globally-distributed Transparency Centers.

Certificates

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

To help safeguard and authenticate information, Windows provides comprehensive support for certificates and certificate management.

The built-in certificate management command-line utility (certmgr.exe) or MMC snap-in (certmgr.msc) can be used to view and manage certificates, certificate trust lists (CTLs), and certificate revocation lists (CRLs). Whenever a certificate is used in Windows, we validate that the leaf certificate and all the certificates in its chain of trust have not been revoked or compromised. The CTLs and CRLs on the machine are used as a reference for PKI trust and are updated weekly by the Microsoft Third Party Root program via Windows update. If a trusted certificate or root is revoked, all global devices will be updated, meaning users can trust that Windows will automatically protect against vulnerabilities in public key infrastructure.

For cloud and enterprise deployments, Windows also offers users the ability to auto-enroll and renew certificates in Active Directory with Group Policy to reduce the risk of potential outages due to certificate expiration or misconfiguration. Additionally, enterprise certificate pinning can be used to help reduce man-in-the-middle attacks by enabling users to protect their internal domain names from chaining to unwanted certificates. A web application's server authentication certificate chain is checked to ensure it matches a restricted set of certificates. Any web application triggering a name mismatch will start event logging and prevent user access from Microsoft Edge.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

19

Code signing and integrity

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

To ensure that Windows files have not been tampered with, the Windows code integrity process verifies the signature of each file in Windows. Code signing is core to establishing the integrity of firmware, drivers, and software across the Windows platform. Code signing creates a digital signature by encrypting the hash of the file with the private key portion of a code signing certificate and embedding the signature into the file. The Windows code integrity process verifies the signed file by decrypting the signature to check the integrity of the file and confirm that it is from a reputable publisher, ensuring that the file hasn't been tampered with.

The digital signature is evaluated across the Windows environment on Windows boot code, Windows kernel code, and Windows user mode applications. Secure Boot and Code Integrity verify the signature on bootloaders, Option ROMs, and other boot components, to ensure that it is trusted and from reputable publishers. For drivers not published by Microsoft, Kernel Code Integrity verifies the signature on kernel drivers and requires that drivers be signed by Windows or certified by the [Windows Hardware Compatibility Program](#) (WHCP). This program ensures that third party drivers are compatible with various hardware and Windows, and that the drivers are from vetted driver developers.

Device health attestation

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

The Windows device health attestation process supports a [zero-trust](#) paradigm that shifts the focus from static, network-based perimeters to users, assets, and resources.

The attestation process confirms the device, firmware, and boot process are in a good state and have not been tampered with before they can access corporate resources. These determinations are made with data stored in the TPM which provides a secure root of trust. The information is sent to an attestation service, such as Azure Attestation, to verify the device is in a trusted state. Then, an MDM tool like Microsoft Endpoint Manager reviews device health and connects this information with Azure Active Directory for conditional access.

Windows includes many security features to help protect users from malware and attacks. However, security components are trustworthy only if the platform boots as expected and is not tampered with. As noted above, Windows relies on Unified Extensible Firmware Interface (UEFI) Secure Boot, ELAM, DRTM, Trusted Boot, and other low-level hardware and firmware security features to protect your PC from attacks. From the moment you power on your PC until your anti-malware starts, Windows is backed with the appropriate hardware configurations that help keep you safe. [Measured boot](#), implemented by bootloaders and BIOS, verifies and cryptographically records each step of the boot in a chained manner. These events are bound to the TPM that functions as a hardware root-of-trust. Remote attestation

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

20

is the mechanism by which these events are read and verified by a service to provide a verifiable, unbiased, and tamper resilient report. Remote attestation is the trusted auditor of your systems boot, allowing relying parties to bind trust to the device and its security.

A summary of the steps involved in attestation and zero-trust on a Windows device are as follows:

- During each step of the boot process, such as a file load, update of special variables, and more, information such as file hashes and signature(s) are measured in the TPM Platform Configuration Register (PCRs). The measurements are bound by a [Trusted Computing Group specification](#) that dictates what events can be recorded and the format of each event. The data provides important information about device security from the moment it powers on.

- Once Windows has booted, the attestor (or verifier) requests the TPM to get the measurements stored in its PCRs alongside the measured boot log. Together these form the attestation evidence that's sent to the Microsoft Azure Attestation Service.

- The TPM is verified by using the keys/cryptographic material available on the chipset with an [Azure Certificate Service](#).

- The above information is sent to the [Azure Attestation service](#) to verify that the device is in a trusted state.

Windows security policy settings and auditing

Note: This section applies to all Windows 11 editions, including Home, Pro, Enterprise, Pro Education and Education.

Security policy settings are a critical part of your overall security strategy. Windows provides a robust set of security setting policies IT administrators can use to help protect Windows devices and other resources in your organization. Security settings policies are rules you can configure on a device, or multiple devices, to control:

- User authentication to a network or device.

- Resources users are permitted to access.

- Whether to record a user's or group's actions in the event log.

- Membership in a group.

Security auditing is one of the most powerful tools that you can use to maintain the integrity of your network and assets. Auditing can help identify attacks, network vulnerabilities, and attacks against targets you consider high value. You can specify categories of security-related events to create an audit policy tailored to the needs of your organization.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

21

All auditing categories are disabled when Windows is first installed. Before enabling them, follow these steps to create an effective security auditing policy:

1. Identify your most critical resources and activities.

2. Identify the audit settings you need to track them.

3. Assess the advantages and potential costs associated with each resource or setting.

4. Test these settings to validate your choices.

5. Develop plans for deploying and managing your audit policy.

Learn more about security policy settings and security auditing.

Windows security app

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

Visibility and awareness of device security and health are key to any action taken. The Windows built-in security application found in settings provides an at-a-glance view of the security status and health of your device. These insights help you identify issues and act to make sure you're protected. You can quickly see the status of your virus and threat protection, firewall and network security, device security controls, and more.

Learn more about the Windows security app.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

22

Encryption and data protection

When people travel with their PCs, their confidential information travels with them. Wherever confidential data is stored, it must be protected against unauthorized access, whether through physical device theft or from malicious applications.

BitLocker

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

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. BitLocker uses AES algorithm in XTS or CBC mode of operation with 128-bit or 256-bit key length to encrypt data on the volume. Cloud storage on Microsoft OneDrive or Azure[6] can be used to save recovery key content. BitLocker can be managed by any MDM solution such as Microsoft Intune[6] using a configuration service provider (CSP).

BitLocker provides encryption for the OS, fixed data, and removable data drives (BitLocker to go) leveraging technologies like hardware security test interface (HSTI), Modern Standby, UEFI Secure Boot and TPM. Windows consistently improves data protection by improving existing options and providing new strategies.

Encrypted hard drive

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

Encrypted hard drives are a class of hard drives that are self-encrypted at the hardware level and allow for full disk hardware encryption while being transparent to the device user. These drives combine the security and management benefits provided by BitLocker Drive Encryption with the power of self-encrypting drives.

By offloading the cryptographic operations to hardware, encrypted hard drives increase BitLocker performance and reduce CPU usage and power consumption. Because encrypted hard drives encrypt data quickly, BitLocker deployment can be expanded across enterprise devices with little to no impact on productivity.

Encrypted hard drives enable:

- Smooth performance: Encryption hardware, integrated into the drive controller, allows the drive to operate at full data rate without performance degradation.

- Strong security based in hardware: Encryption is always "on" and the keys for encryption never leave the hard drive. The drive authenticates users independently from the operating system before it unlocks.

- Ease of use: Encryption is transparent to the user and the user does not need to enable it. Encrypted hard drives are easily erased using an on-board encryption key; there is no need to re-encrypt data on the drive.

- Lower cost of ownership: There is no need for new infrastructure to manage encryption keys since BitLocker leverages your existing infrastructure to store recovery information. Your device operates more efficiently because processor cycles do not need to be used for the encryption process.

Personal data encryption

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

Personal data encryption works with BitLocker and Windows Hello for Business, either with PIN or biometrics (Face or Fingerprint), is used to protect the container which houses the Encryption keys used by PDE. When the user logs in (either after bootup or unlocking after a lock screen), the container gets authenticated to release the keys in the container to decrypt user content.

Email encryption

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

Email encryption enables users to encrypt outgoing email messages and attachments, so only intended recipients with a digital identification (ID)—also called a certificate—can read them.[7] Users can digitally sign a message, which verifies the identity of the sender and ensures the message has not been tampered with.

These encrypted messages can be sent by a user to people within their organization as well as external contacts if they have proper encryption certificates.

However, recipients using Windows 10 Mail app can only read encrypted messages if the message is received on their Exchange account and they have corresponding decryption keys. Encrypted messages can be read only by recipients who have a certificate. If an encrypted message is sent to recipient(s) whose encryption certificate are not available, the app will prompt you to remove these recipients before sending the email.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

24

Network security

Windows 11 raises the bar for network security, offering comprehensive protection to help people work with confidence from almost anywhere. To help reduce an organization's attack surface, network protection in Windows prevents people from accessing dangerous IP addresses and domains that may host phishing scams, exploits, and other malicious content. Using reputation-based services, network protection blocks access to potentially harmful, low-reputation based domains and IP addresses.

New DNS and TLS protocol versions strengthen the end-to-end protections needed for applications, web services, and zero-trust networking. File access adds an untrusted network scenario with Server Message Block over QUIC as well as new encryption and signing capabilities. Wi-Fi and Bluetooth advancements also provide greater trust in connections to other devices. In addition, VPN and Windows Defender Firewall platforms offer new ways to easily configure and debug software.

In enterprise environments, network protection works best with Microsoft Defender for Endpoint, which provides detailed reporting on protection events as part of larger investigation scenarios. Learn more about how to protect your network.

Transport layer security (TLS)

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

Transport Layer Security (TLS) is the internet's most deployed security protocol, encrypting data in transit to provide a secure communication channel between two endpoints. Windows prefers the latest protocol versions and strong cipher suites by default and offers a full suite of extensions such as client authentication for enhanced server security, or session resumption for improved application performance.

TLS 1.3 is the latest version of the protocol and is enabled by default in Windows 11. This version eliminates obsolete cryptographic algorithms, enhances security over older versions, and aims to encrypt as much of the TLS handshake as possible. The handshake is more performant with one fewer round trip per connection on average and supports only five strong cipher suites which provide perfect forward secrecy and less operational risk. Customers using TLS 1.3 (or Windows components that support it, including HTTP.SYS, WinInet, .NET, MsQUIC, and more) on Windows 11 will get more privacy and lower latencies for their encrypted online connections. Note that if the client or server application on either side of the connection does not support TLS 1.3, Windows will fall back to TLS 1.2.

DNS security

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

In Windows 11, the Windows DNS client supports DNS over HTTPS, an encrypted DNS protocol. This allows administrators to ensure their devices protect their name queries from on-path attackers, whether they are passive observers logging browsing behavior or active attackers trying to redirect clients to malicious sites. In a zero-trust model where there is no trust placed in a network boundary, having a secure connection to a trusted name resolver is required.

Windows 11 provides Group Policy as well as programmatic controls to configure DNS over HTTP behavior. As a result, IT administrators can extend existing security to adopt new models such as zero trust. IT administrators can mandate DNS over HTTP protocol, ensuring that devices that use insecure DNS will fail to connect to network resources. IT administrators also have the option not to use DNS over HTTP for legacy deployments where network edge appliances are trusted to inspect plain-text DNS traffic. By default, Windows 11 will defer to the local administrator on which resolvers should use DNS over HTTP.

Support for DNS encryption integrates with existing Windows DNS configurations such as the Name Resolution Policy Table (NRPT), the system HOSTS file, as well as resolvers specified per network adapter or network profile. The integration helps Windows 11 ensure that the benefits of greater DNS security do not regress existing DNS control mechanisms.

Bluetooth protection

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

The number of Bluetooth devices connected to Windows continues to increase. Windows users connect their Bluetooth headsets, mice, keyboard, and other accessories and improve their day-to-day PC experience by enjoying streaming, productivity, and gaming. Windows supports all standard Bluetooth pairing protocols, including classic and LE Secure connections, secure simple pairing, and classic and LE legacy pairing. Windows also implements host based LE privacy. Windows updates help users stay current with OS and driver security features in accordance with the Bluetooth Special Interest Group (SIG), Standard Vulnerability Reports, as well as issues beyond those required by the Bluetooth core industry standards. Microsoft strongly recommends that you also ensure your firmware and/ or software of your Bluetooth accessories are kept up to date.

IT-managed environments have a number of Bluetooth policies (MDM, Group Policy and PowerShell) that can be managed through MDM tools such as Microsoft Intune. You can configure Windows to use Bluetooth technology while supporting the security needs of your organization. For example, you can allow input and audio while blocking file transfer, force encryption standards, limit Windows discoverability, or even disable Bluetooth entirely for the most sensitive environments.

Securing Wi-Fi connections

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

Windows Wi-Fi supports industry standardized authentication and encryption methods when connecting to Wi-Fi networks. WPA (Wi-Fi Protected Access) is a security standard developed by the Wi-Fi Alliance to provide sophisticated data encryption and better user authentication The current security standard for Wi-Fi Authentication is WPA3 which provides a more secure and reliable connection method and replaces WPA2 and older security protocols. Opportunistic Wireless Encryption (OWE) is a technology that allows wireless devices to establish encrypted connections to public Wi-Fi hotspots.

WPA3 is supported in Windows 11 (WPA3 Personal and WPA3 Enterprise 192-bit Suite B) as well as OWE implementation for more security while connecting to Wi-Fi hotspots.

Windows 11 enhances Wi-Fi security by enabling additional elements of WPA3 security such as the new H2E protocol and WPA3 Enterprise Support which includes enhanced Server Cert validation and the TLS1.3 for authentication using EAP-TLS Authentication. Windows 11 provides Microsoft partners the ability to bring the best platform security on new devices.

WPA3 is now a mandatory requirement by WFA for any Wi-Fi Certification.

Windows Defender Firewall

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

Windows Defender Firewall with Advanced Security is an important part of a layered security model. It provides host-based, two-way network traffic filtering, blocking unauthorized traffic flowing into or out of the local device based on the types of networks to which the device is connected.

Windows Defender Firewall in Windows 11 offers the following benefits:

- Reduces the risk of network security threats: Windows Defender Firewall reduces the attack surface of a device with rules to restrict or allow traffic by many properties such as IP addresses, ports, or program paths. Reducing the attack surface of a device increases manageability and decreases the likelihood of a successful attack.

- Safeguards sensitive data and intellectual property: With its integration with Internet Protocol Security (IPsec), Windows Defender Firewall provides a simple way to enforce authenticated, end-to-end network communications. It provides scalable, tiered access to trusted network resources, helping to enforce integrity of the data, and optionally helping to protect the confidentiality of the data.

- Extends the value of existing investments: Because Windows Defender Firewall is a host-based firewall that is included with the operating system, there is no additional hardware or software required. Windows Defender Firewall is also designed to complement existing non-Microsoft network security solutions through a documented application programming interface (API).

Windows 11 makes the Windows Defender Firewall easier to analyze and debug. IPsec behavior has been integrated with Packet Monitor (pktmon), an in-box cross-component network diagnostic tool for Windows. Additionally, the Windows Defender Firewall event logs have been enhanced to ensure an audit can identify the specific filter that was responsible for any given event. This enables analysis of firewall behavior and rich packet capture without relying on third-party tools.

Virtual private networks (VPN)

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

Organizations have long relied on Windows to provide reliable, secured, and manageable virtual private network (VPN) solutions. The Windows VPN client platform includes built-in VPN protocols, configuration support, a common VPN user interface, and programming support for custom VPN protocols. VPN apps are available in the Microsoft Store for both enterprise and consumer VPNs, including apps for the most popular enterprise VPN gateways.

In Windows 11 we've integrated the most commonly used VPN controls right into the Windows 11 Quick Actions pane. From the Quick Actions pane users can see the status of their VPN, start and stop the VPN tunnels, and with one click can go to the modern Settings app for more control.

The Windows VPN platform connects to Azure Active Directory (Azure AD) and Conditional Access for single sign-on, including multi-factor authentication (MFA) through Azure AD.[6] The VPN platform also supports classic domain-joined authentication. It's supported by Microsoft Endpoint Manager and other mobile device management (MDM) providers. The flexible VPN profile supports both built-in protocols and custom protocols, can configure multiple authentication methods, can be automatically started as needed or manually started by the end-user, and supports split-tunnel VPN and exclusive VPN with exceptions for trusted external sites.

With Universal Windows Platform (UWP) VPN apps, end users never get stuck on an old version of their VPN client. VPN apps from the store will be automatically updated as needed. Naturally, the updates are in the control of your IT admins.

The Windows VPN platform has been tuned and hardened for cloud-based VPN providers like Azure VPN. Features like AAD auth, Windows user interface integration, plumbing

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

28

IKE traffic selectors, and server support are all built into the Windows VPN platform. The integration into the Windows VPN platform leads to a simpler IT admin experience; user authentication is more consistent, and users can easily find and control their VPN.

SMB file services

Note: This section applies to the following Windows 11 editions: Home, Pro, Pro Workstation, Enterprise, Pro Education, and Education. Except when noted differently.

SMB and file services are the most common Windows workload in the commercial and public sector ecosystem. Users and applications rely on SMB to access the files that run organizations large and small. In Windows 11, the SMB protocol has significant security updates to meet today's threats, including AES-256 bits encryption, accelerated SMB signing, Remote Directory Memory Access (RDMA) network encryption, and entirely new scenario, SMB over QUIC for untrusted networks.

SMB Encryption provides end-to-end encryption of SMB data and protects data from eavesdropping occurrences on internal networks. Windows 11 introduces AES-256-GCM and AES-256-CCM cryptographic suites for SMB 3.1.1 encryption. Windows administrators can mandate the use of this more advanced security or continue to use the more compatible and still-safe AES-128 encryption.

In Windows 11 Enterprise, Education, and Pro Workstation, SMB Direct now supports encryption. For demanding workloads like video rendering, data science, or extremely large files, you can now operate with the same safety as traditional TCP and the performance of RDMA. Previously, enabling SMB encryption disabled direct data placement, making RDMA as slow as TCP. Now data is encrypted before placement, leading to relatively minor performance degradation while adding AES-128 and AES-256 protected packet privacy.

Windows 11 introduces AES-128-GMAC for SMB signing. Windows will automatically negotiate this better-performing cipher method when connecting to another computer that supports it. Signing prevents common attacks like relay, spoofing, and is required by default when clients communicate with Active Directory domain controllers.

Finally, Windows 11 introduces SMB over QUIC (Preview), an alternative to the TCP network transport, providing secure, reliable connectivity to edge file servers over untrusted networks like the Internet as well as highly secure communications on internal networks. QUIC is an IETF-standardized protocol with many benefits when compared with TCP, but most importantly it always requires TLS 1.3 and encryption. SMB over QUIC offers an "SMB VPN" for telecommuters, mobile device users, and high security organizations. All SMB traffic, including authentication and authorization within the tunnel is never exposed to the underlying network. SMB behaves normally within the QUIC tunnel, meaning the user experience doesn't change. SMB over QUIC will be a game changing feature for Windows 11 accessing Windows file servers and eventually Azure Files and third parties.

Table of Contents | Introduction | Hardware Security | **Operating System Security** | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

29

Virus and threat protection

Today's cyber threat landscape is more complex than ever. This new world requires a new approach to threat prevention, detection, and response. Microsoft Defender Antivirus, along with many other features that are built into Windows 11, are at the frontlines to protect customers against current and emerging threats.

Microsoft Defender Antivirus

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

Microsoft Defender Antivirus is a next-generation protection solution included in all versions of Windows 10 and Windows 11. From the moment you boot Windows, Microsoft Defender Antivirus continually monitors for malware, viruses, and security threats. In addition to real-time protection, updates are downloaded automatically to help keep your device safe and protect it from threats. If you have another antivirus app installed and turned on, Microsoft Defender Antivirus will turn off automatically. If you uninstall the other app, Microsoft Defender Antivirus will turn back on.

Microsoft Defender Antivirus, includes real-time, behavior-based, and heuristic antivirus protection. This combination of always-on content scanning, file and process behavior monitoring, and other heuristics effectively prevents security threats. Microsoft Defender Antivirus continually scans for malware and threats and also detects and blocks potentially unwanted applications (PUA) which are applications that are deemed to negatively impact your device but are not considered malware.

Microsoft Defender Antivirus always-on protection is integrated with cloud-delivered protection, which helps ensure near instant detection and blocking of new and emerging threats. This combination of local and cloud-delivered technologies provides award-winning protection at home and at work.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

30

Learn more about [next generation protection with Microsoft Defender Antivirus](#).

Local Security Authority Protection

Note: This section applies to all Windows 11 editions, Home, Pro, Enterprise, Education and IoT.

Windows has several critical processes to verify a user's identity. Verification processes include Local Security Authority (LSA) which is responsible for authenticating users and verifying Windows logins. LSA handles tokens and credentials such as passwords that are used for single sign-on to a Microsoft account and Azure services. To help protect these credentials, additional LSA protection will be enabled by default on new, enterprise-joined Windows 11 devices. By loading only trusted, signed code, LSA provides significant protection against credential theft.

Attack surface reduction

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

Attack surface reduction rules help prevent software behaviors that are often abused to compromise your device or network. By reducing the number of attack surfaces, you can reduce the overall vulnerability of your organization. Administrators can configure specific attack surface reduction rules to help block certain behaviors, such as:

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

31

- Launching executable files and scripts that attempt to download or run files

- Running obfuscated or otherwise suspicious scripts

- Performing behaviors that apps don't usually initiate during normal day-to-day work

For example, an attacker might try to run an unsigned script from a USB drive or have a macro in an Office document make calls directly to the Win32 API. Attack surface reduction rules can constrain these kinds of risky behaviors and improve the defensive posture of the device. For comprehensive protection, follow steps for enabling hardware-based isolation for Microsoft Edge and reducing the attack surface across applications, folders, device, network, and firewall.

Learn more about attack surface reduction.

Tamper protection

Note: This section applies to the following Windows 11 editions: Home, Pro, Pro Workstation, Enterprise, Pro Education, and Education.[8]

Attacks like ransomware attempt to disable security features, such as anti-virus protection. Bad actors like to disable security features to get easier access to user's data, to install malware, or to otherwise exploit user's data, identity, and devices without fear of being blocked. Tamper protection helps prevent these kinds of activities.
With tamper protection, malware is prevented from taking actions such as:

- Disabling real-time protection

- Turning off behavior monitoring

- Disabling antivirus (such as IOfficeAntivirus (IOAV))

- Disabling cloud-delivered protection

- Removing security intelligence updates

Learn more about tamper protection.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

32

Microsoft vulnerable driver blocklist

Note: This section applies to the following Windows 11 editions: Home, Pro, Pro Workstation, Enterprise, Pro Education, and Education.[8]

The Windows kernel is the most privileged software and is therefore a compelling target for malware authors. Since Windows has strict requirements for code running in the kernel, cybercriminals commonly exploit vulnerabilities in kernel drivers to get access. Microsoft works with the ecosystem partners to constantly identify and respond to potentially vulnerable kernel drivers. Prior to Windows 11 2022 Update, Windows enforced a block policy when HVCI is enabled to prevent vulnerable versions of drivers from running. Beginning with Windows 11 2022 Update, the block policy is now on by default for all new Windows PCs and users can opt-in to enforce the policy from the Windows Security app.

Controlled folder access

Note: This section applies to the following Windows 11 editions: Home, Pro, Pro Workstation, Enterprise, Pro Education, and Education.[9]

You can protect your valuable information in specific folders by managing app access to specific folders. Only trusted apps can access protected folders, which are specified when controlled folder access is configured. Typically, commonly used folders, such as those used for documents, pictures, downloads, are included in the list of controlled folders.

Controlled folder access works with a list of trusted apps. Apps that are included in the list of trusted software work as expected. Apps that are not included in the trusted list are prevented from making any changes to files inside protected folders.

Controlled folder access helps protect user's valuable data from malicious apps and threats, such as ransomware. Learn more about controlled folder access.

Exploit protection

Note: This section applies to the following Windows 11 editions: Home, Pro, Pro Workstation, Enterprise, Pro Education and, Education.[9]

Exploit protection automatically applies several exploit mitigation techniques to operating system processes and apps. Exploit protection works best with Microsoft Defender[6] for Endpoint, which gives organizations detailed reporting into exploit protection events and blocks as part of typical alert investigation scenarios. You can enable exploit protection on an individual device, and then use Group Policy in Azure Active Directory to distribute the XML file to multiple devices simultaneously.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

33

When a mitigation is encountered on the device, a notification will be displayed from the Action Center. You can customize the notification with your company details and contact information. You can also enable the rules individually to customize which techniques the feature monitors.

You can use audit mode to evaluate how exploit protection would impact your organization if it were enabled.

Windows 11 provides configuration options for exploit protection. You can prevent users from modifying these specific options with Group Policy. Learn more about [protecting devices from exploits](#).

Microsoft Defender SmartScreen

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

Microsoft Defender SmartScreen protects against phishing, malware websites and applications, and the downloading of potentially malicious files.

SmartScreen determines whether a site is potentially malicious by:

- Analyzing visited webpages looking for indications of suspicious behavior. If it determines a page is suspicious, it will show a warning page to advise caution.

- Checking the visited sites against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen warns that that the site might be malicious.

SmartScreen also determines whether a downloaded app or app installer is potentially malicious by:

- Checking downloaded files against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen warns that the site might be malicious.

- Checking downloaded files against a list of well-known downloaded files. If the file is not on that list, Smartscreen displays a caution alert.

For enhanced phishing protection, **SmartScreen also alerts people when they are entering their Microsoft credentials into a potentially risky location**. IT can customize which notifications appear through Microsoft Endpoint Manager. This protection runs in audit mode by default, giving IT admins full control to make decisions around policy creation and enforcement.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

34

Because Windows 11 comes with these enhancements already built-in and enabled, users have extra security from the moment they turn on their device.

The app and browser control section contains information and settings for Microsoft Defender SmartScreen. IT administrators and IT pros can get configuration guidance in the [Microsoft Defender SmartScreen documentation library](#).

Microsoft Defender for Endpoint

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

Microsoft Defender for Endpoint is an enterprise endpoint detection and response solution that helps security teams detect, investigate, and respond to advanced threats.[10] Organizations can use the rich event data and attack insights Defender for Endpoint provides to investigate incidents. Defender for Endpoint brings together the following elements to provide a more complete picture of security incidents:

- Endpoint behavioral sensors: Embedded in Windows, these sensors collect and process behavioral signals from the operating system and send this sensor data to your private, isolated, cloud instance of Microsoft Defender for Endpoint.

- Cloud security analytics: Leveraging big-data, device-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products such as Microsoft 365[6] and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.

- Threat intelligence: Microsoft processes over 43 trillion security signals every 24 hours yielding a deep and broad view into the evolving threat landscape. Combined with our global team of security experts, and cutting-edge artificial intelligence and machine learning, we can see threats that others miss. This threat intelligence helps provide unparalleled protection for our customers. The protections built into our platforms and products blocked attacks that include 31 billion identity threats and 32 billion email threats.

- Rich response capabilities: Empowering SecOps teams to isolate, remediate, and remote into machines to further investigate and stop active threats in their environment, as well as block files, network destinations, and create alerts for them. In addition, Automated Investigation and Remediation can help reduce the load on the SOC by already performing these normally manual steps towards remediation and providing detailed investigation outcomes.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

35

Defender for Endpoint is also part of Microsoft 365 Defender, our end-to-end cloud native XDR solution that combines best of breed endpoint, email, and identity security products enabling organizations to prevent, detect, investigate, and remediate attacks by delivering deep visibility, granular context, and actionable insights generated from raw signals harnessed across the Microsoft 365 environment and other platforms, all synthesized into a single dashboard. This solution offers tremendous value to organizations of any size, especially those that are looking to break away from the added complexity of multiple point solutions, not only by keeping them protected from sophisticated attacks but by saving IT and security teams time and resources that could have been better used elsewhere.

Learn more about [Microsoft Defender for Endpoint](#) and [Microsoft 365 Defender](#).

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

36

Application Security

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

Cybercriminals can take advantage of poorly secured applications to access valuable resources. With Windows 11, IT admins can combat common application attacks from the moment a device is provisioned. For example, IT can remove local admin rights from user accounts, so that PCs run with least privilege to prevent malicious applications from accessing sensitive resources.

In addition, organizations can control which applications run on their devices with Windows Defender Application Control.

Windows 11 offers a rich application platform with layers of security like isolation and code integrity that help protect your valuable data. Developers can also take advantage of these capabilities to build in security from the ground up to protect against breaches and malware.

User Account Control

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

User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

Organizations can use a modern device management (MDM) solution like Microsoft Endpoint Manager to remotely configure UAC settings. Organizations without MDM can change settings directly on the device.

Enabling UAC helps prevent malware from altering PC settings and potentially gaining access to networks and sensitive data. UAC can also block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

Users with standard accounts, or those using administrative accounts with UAC enabled, run most programs with limited access rights. This includes the Windows shell and any apps started from the shell such as Windows Explorer, a web browser, productivity suite, graphics programs, or games.

Some apps require additional permissions and will not work properly (or at all) when running with limited permissions. When an app needs to run with more than standard user rights, UAC allows users to run apps with a "full" administrator token (with administrative groups and privileges) instead of their default user access token. Users continue to operate in the standard user security context, while enabling certain executables to run with elevated privileges, if needed.
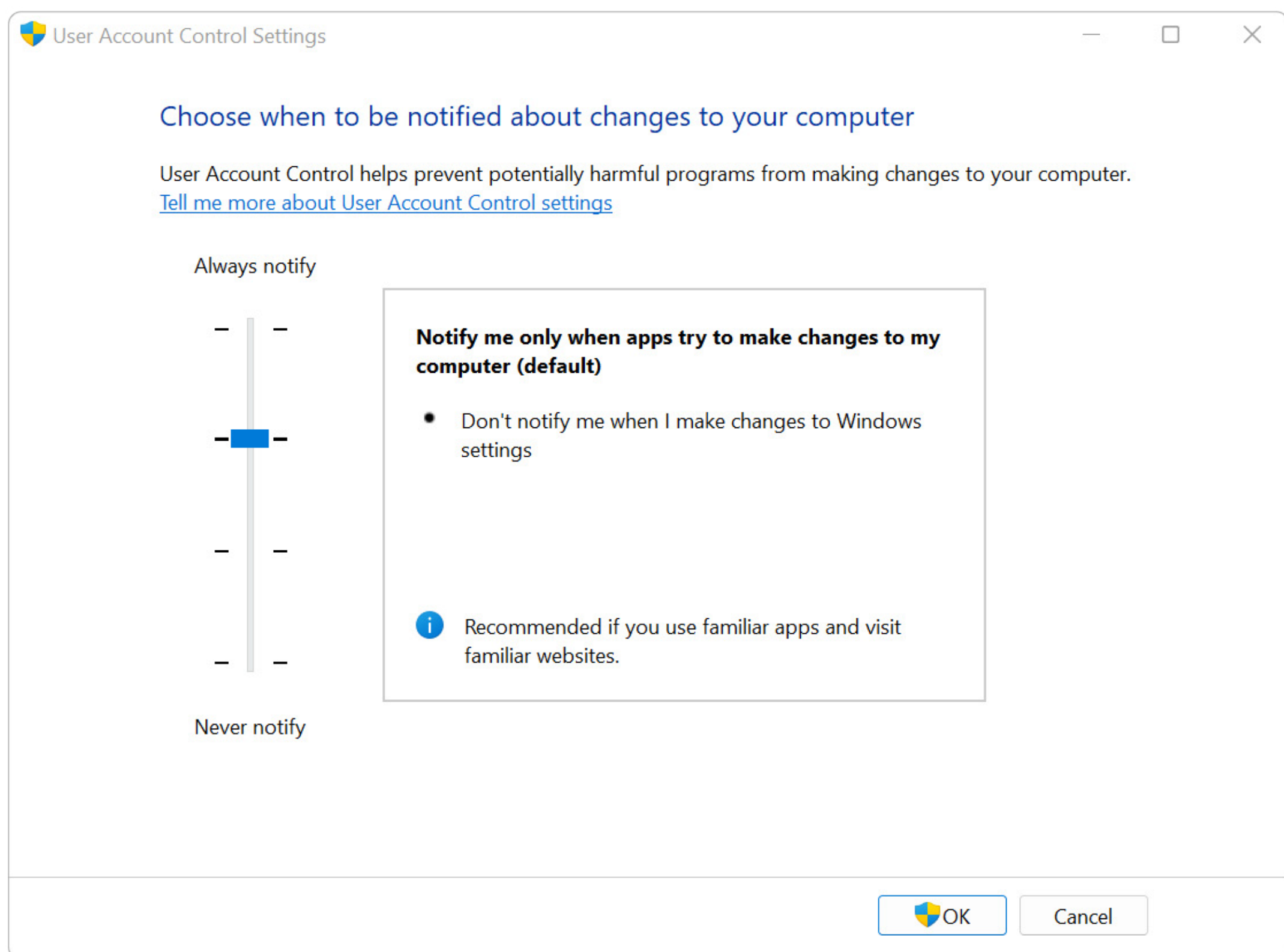
Learn more about How User Account Control works.

Windows Defender Application Control (WDAC)

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

Your organization is only as secure as the applications that run on your devices. With application control, apps must earn trust to run, in contrast to an application trust model where all code is assumed trustworthy. By helping prevent unwanted or malicious code from running, application control is an important part of an effective security strategy. Many organizations cite application control as one of the most effective means for addressing the threat of executable file-based malware.

Windows 10 and above include Windows Defender Application Control (WDAC) as well as AppLocker. WDAC is the next generation app control solution for Windows and provides powerful control over what runs in your environment. Customers who were using AppLocker on previous versions of Windows can continue to use the feature as they consider whether to switch to WDAC for the stronger protection. Learn more about WDAC and AppLocker.

To simplify WDAC enablement, organizations can take advantage of Azure Code Signing, a secure and fully-managed service for signing WDAC policies and apps.

Smart App Control

Note: This section applies to the following Windows 11 editions: Home, Pro, Pro Workstation, Enterprise, Pro Education, and Education. Smart App Control availability may vary by market and user profile.

Smart App Control prevents users from running malicious applications on Windows devices by blocking untrusted or unsigned applications. Smart App Control goes beyond previous built-in browser protections, by adding another layer of security that is woven directly into the core of the OS at the process level. Using AI, our new Smart App Control only allows processes to run that are predicted to be safe based on existing and new intelligence processed daily. Smart App Control builds on top of the same cloud-based AI used in Windows Defender Application Control (WDAC) to predict the safety of an application, so people can be confident they are using safe and reliable applications on their new Windows devices. Additionally, unknown script files and macros from the web are blocked when Smart App Control is active, greatly improving security for everyday users while using the internet. Designed for consumers and information workers that use known and signed applications in their daily work, Smart App Control will ship with new devices with Windows 11, version 22H2 installed. Devices running previous versions of Windows 11 will have to be reset with a clean installation of Windows 11, version 22H2 to take advantage of this feature. Smart App Control will be disabled on devices enrolled in enterprise management. We suggest enterprises running line of business applications continue to leverage Windows Defender Application Control (WDAC).

Application Guard for Microsoft Office and Application Guard for Microsoft Edge

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

Application Guard is designed to help keep employees productive by protecting against current and emerging threats.[11]

Attackers take advantage of social engineering tactics to deceive users and influence their actions—from opening a malicious link in an email to directing them to a compromised website. Malicious code executes when the content is opened, exploits vulnerabilities, and downloads malware to the device.

Scans and filters might not provide enough protection when users voluntarily execute malicious code. Hardware isolation can help defend against such exploits. Based on the zero-trust principles of explicit verification, least privilege access, and assumption of breach, isolation treats any application and browsing session as untrustworthy by default, adding multiple roadblocks for attackers attempting to get into user environments.

Integral to the Windows 11 chip-to-cloud security posture, isolation enables applications to run in a virtualized environment to reduce the potential impact of malicious code.

Application Guard uses chip-based hardware isolation to seamlessly run untrusted websites and Office files in a Hyper-V-based container separated from the host operating system. As a result, anything that happens in the container stays isolated from the desktop operating system. If malicious code originates from a document or website running inside the container, the infection is contained and the desktop stays intact.

Application Guard protects Office files including Word, PowerPoint, and Excel. It also protects websites opened in Edge browser, and a plugin is available for browsers such as Google Chrome and Mozilla Firefox. Application icons will have a small shield if Application Guard has been enabled and they are under protection.

Learn more about Application Guard. Application Guard for Microsoft Edge and Application Guard for Microsoft Office E5 are configured using an MDM such as Microsoft Endpoint Manager. Also see blog post Defend against zero-day exploits with isolation technology.

## Hardware isolation of Microsoft Edge & Microsoft Office
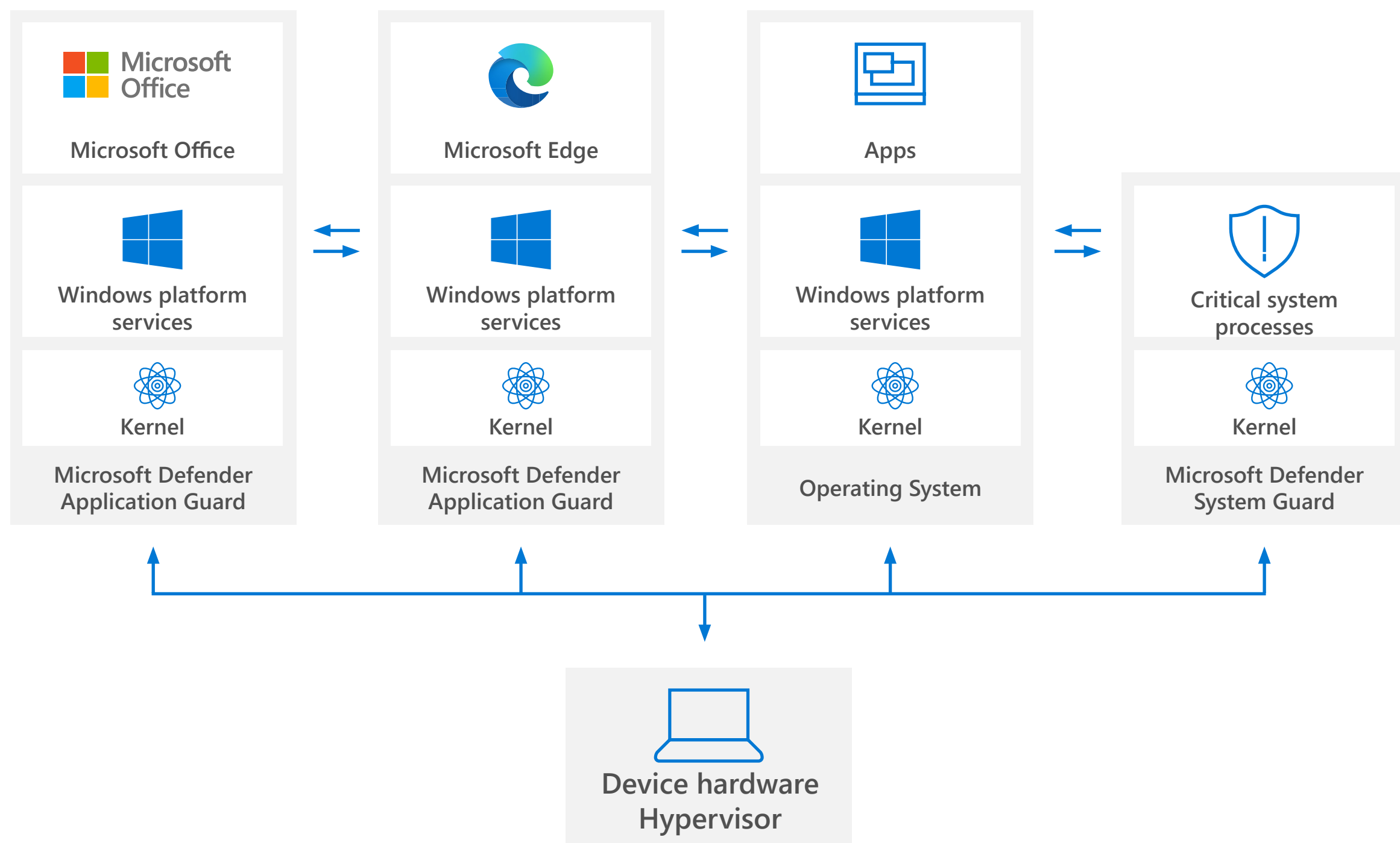
App containers

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

In addition to Application Guard for Office and Edge, Universal Windows Platform (UWP) applications run in Windows containers known as app containers. App containers act as process and resource isolation boundaries, but unlike docker containers, these are special containers designed to run Windows applications.

Processes that run in app containers operate with low integrity level, meaning they have limited access to resources they do not own. Because the default integrity level of most resources is medium integrity level, the UWP app can access only a subset of the filesystem, registry, and other resources. The app container also enforces restrictions on network connectivity; for example, access to a local host is not allowed. As a result, malware or infected apps have limited footprint for escape.

Learn more about Windows and app containers.

Developing secure applications

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

Developers have an opportunity to design highly secure applications that benefit from the latest Windows 11 safeguards. The Windows App SDK provides a unified set of APIs and tools for developing desktop apps for Windows 11 and Windows 10. To help create apps that are up-to-date and protected, the SDK follows the same security standards, protocols, and compliance as the core Windows operating system.

If you are a developer, you can find security best practices and information at Windows application development—best practices. You can get started with Windows App SDK Samples on GitHub. For an example of the continuous security process in action with the Windows App SDK, see the most recent release.

Identity
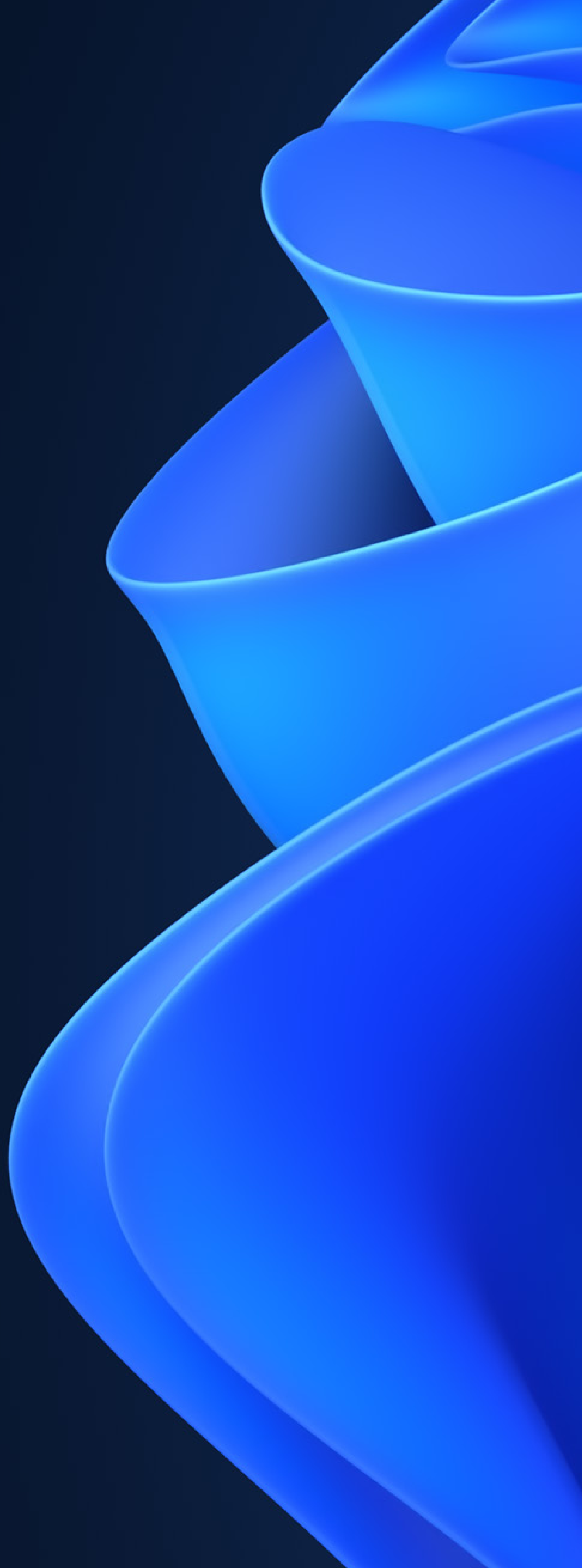
Secured Identity

Hybrid work is here to stay, and the security of your organization depends on the right user access, the right device, and the right data. Weak passwords, password reuse, password spraying, and phishing are the entry points for many attacks. Hackers launch more than 800 password attacks per second worldwide. And phishing attacks have increased, making identity a continuous battleground for attacks. As Bret Arsenault, Chief Information Security Officer at Microsoft says, "Hackers don't break in, they log in."

Hardware and software technologies work together in Windows to deliver powerful, ongoing protection of identity and privacy from the moment you sign onto your device.

To significantly reduce the risk of compromise in today's hybrid workplace, Windows 11 provides identity and credential protection options to meet business needs while helping organizations comply with ever-evolving regulations.

Enabling passwordless sign in

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

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.

New Password + Secure Enough = Something I can't remember

New Password + Something I can remember = Not secure
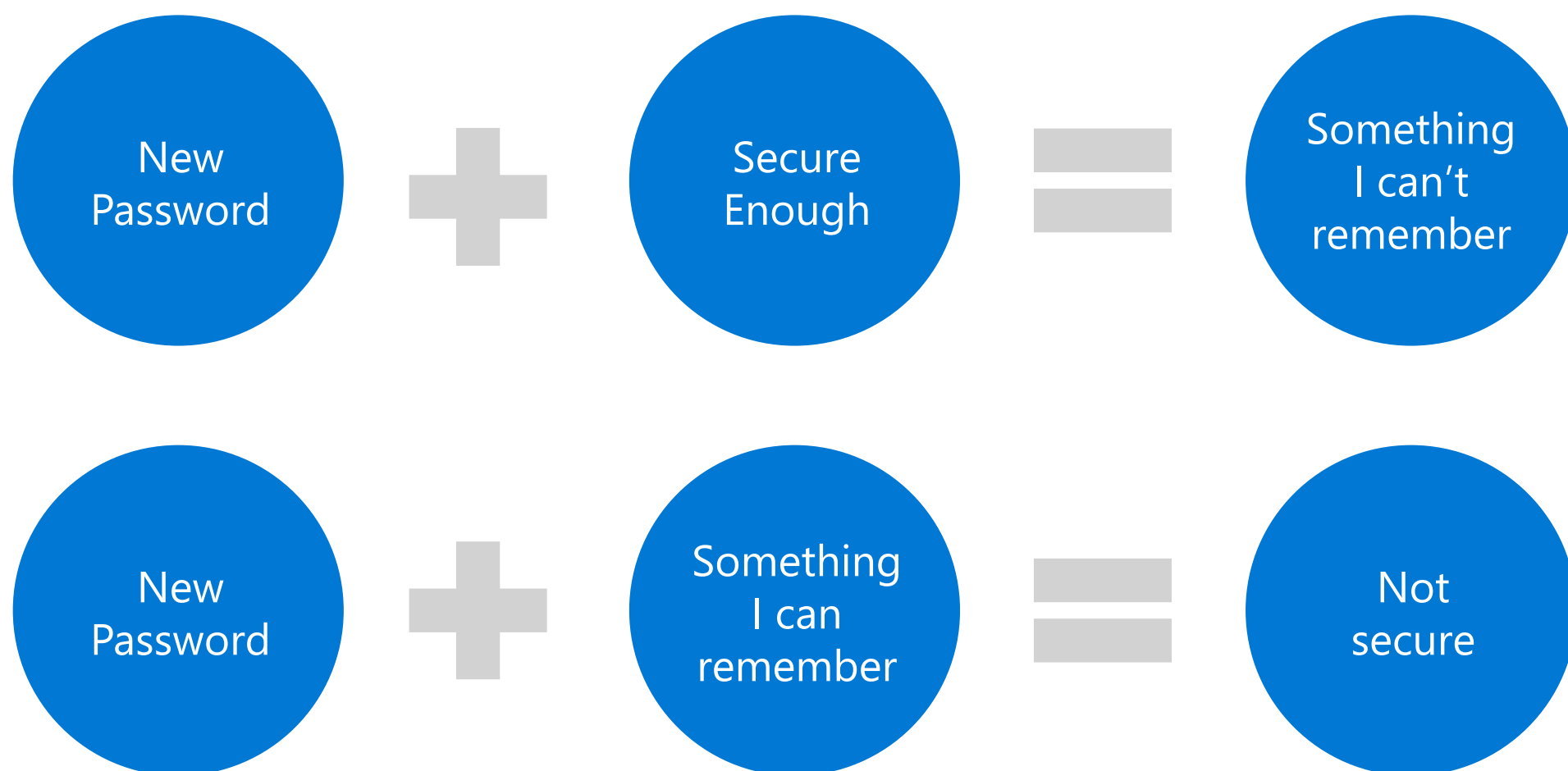
Windows Hello—a key to your passwordless future

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

The premier built-in passwordless solution for Windows is Windows Hello which provides built-in support for the Fast ID Online v2.0 (FIDO2) passwordless industry standard without the hassle of extra security keys. Windows Hello provides a secure, convenient sign-in experience by augmenting or replacing passwords with a stronger authentication model based on a PIN or biometric sign in such as facial or fingerprint recognition all secured by the Trusted Platform Module (TPM).[5] Step by step guidance makes set up easy.

Using asymmetric keys provisioned in the TPM, Windows Hello protects authentication by binding a user's credentials to their device. Windows Hello validates the user based on either a PIN or biometrics match and only then releases cryptographic keys bound to that user in the TPM.

PIN and biometric data stays on the device and cannot be stored or accessed externally. Since the data cannot be accessed by anyone without physical access to the device, credentials are protected against replay attacks, phishing, and spoofing as well as password reuse and leaks.

Windows Hello can authenticate users to a Microsoft account (MSA), Active Directory (AD), Azure Active Directory (AAD), identity provider services, or relying parties that also meets the FIDO2 standards.

- **Windows Hello** can be used with your personal MSA to access your OneDrive, Microsoft email, and other apps.

- **Windows Hello for Business** works with your organization's Active Directory and Azure Active Directory accounts giving you access to work or school resources.

Unlocking credentials with Windows Hello for Business

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

Windows 11 devices can protect user identities by removing the need to use passwords from day one. It's easy to get started with the method that's right for your organization.

A password may only need to be used once during the provisioning process, after which people use a PIN, face, or fingerprint to unlock credentials and sign into the device.

Provisioning methods include:

- Temporary Access Pass (TAP), a time-limited passcode with strong authentication requirements issued through Azure Active Directory.

- Existing multi-factor authentication with Azure Active Directory, including authentication methods like the Microsoft Authenticator app.

Windows Hello for Business replaces the username and password by combining a security key or certificate with a PIN or biometrics data, and then mapping the credentials to a user account during setup. There are multiple ways to deploy Windows Hello for Business, depending on your organization's needs. Organizations that rely on certificates typically use on-premises public key infrastructure (PKI) to support authentication through Certificate Trust. Organizations using key trust deployment require root-of-trust provided by certificates on domain controllers.

Now, organizations with hybrid scenarios can eliminate the need for on-premises domain controllers and simplify passwordless adoption by using Windows Hello for Business cloud Kerberos trust.[12] Running on Azure Active Directory Kerberos, this solution uses security keys and replaces on-premises domain controllers with a cloud-based root-of-trust. As a result, organizations can take advantage of Windows Hello for Business and deploy passwordless security keys with minimal additional setup or infrastructure. Users will authenticate directly with Azure Active Directory, helping speed access to on-premises applications and other resources.

Windows Hello PIN

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

The Windows Hello PIN, which can only be entered by someone with physical access to the device, can be used for strong multifactor authentication. The PIN is protected by the TPM— and like biometric data—never leaves the device. When you enter your PIN, an authentication key is unlocked and used to sign a request sent to the authenticating server. The TPM protects against threats including PIN brute-force attacks on lost or stolen devices. After too many incorrect guesses, the device locks. IT admins can set security policies for PINs such as complexity, length, and expiration.

Windows Hello biometric sign in

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

Windows Hello biometric sign in enhances both security and productivity with a quick, convenient sign on experience. And there's no need to enter a password each time when your face or fingerprint is your credential.

Windows devices that support biometric hardware such as fingerprint or facial recognition cameras integrate directly with Windows Hello, enabling access to Windows client resources and services. Biometric readers for both face and fingerprint must comply with Microsoft Microsoft Windows Hello biometric requirements. Windows Hello facial recognition is designed to only authenticate from trusted cameras used at the time of enrollment.

If a peripheral camera is attached to the device after enrollment, that camera will only be allowed for facial authentication after it has been validated by signing in with the internal camera. For additional security, external cameras can be disabled for use with Windows Hello facial recognition.

Windows presence sensing[13]

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

Windows presence sensing provides another layer of data security protection for hybrid workers. Windows 11 devices can intelligently adapt to your presence to help you stay secure and productive, whether you're working at home, the office, or a public environment. Windows presence sensing combines presence detection sensors with Windows Hello facial recognition to sign you in hands-free, and automatically locks your device when you leave.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

48

Windows Hello enhanced sign-in security

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

Windows Hello biometrics also supports enhanced sign-in security, which uses specialized hardware and software components to raise the security bar even higher for biometric sign in.

Enhanced sign-in security biometrics uses VBS and the TPM to isolate user authentication processes and data and secure the pathway by which the information is communicated. These specialized components protect against a class of attacks that include biometric sample injection, replay, tampering, and more. For example, fingerprint readers must implement Secure Device Connection Protocol, which uses key negotiation and a Microsoft-issued certificate to protect and securely store user authentication data. For facial recognition, components such as the Secure Devices (SDEV) table and process isolation with trustlets help prevent additional class of attacks.

Enhanced Sign-in Security is configured by device manufacturers during the manufacturing process and is most typically supported in Secured-core PC. For facial recognition, Enhanced Sign-in Security is supported by Intel USB and AMD USB processor/camera combinations including specific modules from manufacturers. Intel MIPI will also be supported starting with version Windows 11 2022 Update. Fingerprint authentication is available across all processor types. Please reach out to your OEM for support details.

Microsoft Authenticator

Note: This section applies to all Windows 11 editions, including Home, Pro, Enterprise, Pro Education, and Education.

The Microsoft Authenticator app, which runs on iOS and Android devices, is a perfect companion to help keep you secure and productive when using Windows 11. Microsoft Authenticator can be used to bootstrap Windows Hello for Business, so you never need to have a password to get started on Windows 11.

Microsoft Authenticator also enables easy, secure sign-in for all your online accounts using multifactor authentication, passwordless phone sign-in, or password autofill. The Authenticator app is secured with a public/private key pair in hardware-backed storage such as the Keychain in iOS and Keystore on Android. IT admins can ensure employees are actively using Microsoft Authenticator, and that it's set up correctly to back up credentials.

Individual users can back up their credentials to the cloud by enabling the encrypted backup option in settings. They can also see their sign-in history and security settings for Microsoft personal, work, or school accounts.

Using this secure app for authentication and authorization enables people to be in control of how, where, and when their credentials are used. Adopting this approach benefits both organizations and individual users, who can secure both work and personal accounts.

Learn more about [Microsoft Authenticator](#).

Fast Identity Online (FIDO) support

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

The open industry FIDO Alliance was established to promote authentication standards that reduce reliance on passwords. Fast Identity Online (FIDO) defined CTAP and WebAuthN specifications are becoming the open standard for providing strong authentication that is non-phishable, user-friendly, and privacy-respecting with implementations from major platform providers and relying parties. FIDO standards and certifications are becoming recognized as the leading standard for creating secure authentication solutions across enterprises, governments, and consumer markets.

Windows 11 can also use external FIDO2 security keys for authentication alongside or in addition to Windows Hello which is also a FIDO2 certified passwordless solution. As a result, Windows 11 can be used as a FIDO authenticator for many popular identity management services.

Simplified sign in for education

Note: This section applies to Windows 11 Pro for Education and Education edition.

Windows 11 supports federated sign in with external education identity management services. For students unable to type easily or remember complex passwords, this capability enables secure sign in through methods like QR codes or pictures.

Smart cards

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

Organizations also have the option of using smart cards, an authentication method that pre-dates biometric sign in. Smart cards are tamper-resistant, portable storage devices that can enhance Windows security when authenticating clients, signing code, securing e-mail, and signing in with Windows domain accounts.

Smart cards provide:

- Ease of use in scenarios such as healthcare where employees need to sign in and out quickly and/or without using their hands, or when sharing a workstation.

- Isolation of security-critical computations that involve authentication, digital signatures, and key exchange from other parts of the computer. These computations are performed

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security | Identity | Privacy | Cloud Services | Security Foundation | Conclusion

50

on the smart card.

- Portability of credentials and other private information between computers at work, home, or on the road

Smart cards can only be used to sign into domain accounts, not local accounts. When a password is used to sign into a domain account, Windows uses the Kerberos version 5 (v5) protocol for authentication. If you use a smart card, the operating system uses Kerberos v5 authentication with X.509 v3 certificates.

Account lockout secure defaults

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

New devices with Windows 11 2022 Update installed will have account lockout polices that are secure by default. These policies will mitigate brute-force attacks, such as hackers attempting to access Windows devices via the Remote Desktop Protocol (RDP).

Enhanced phishing protection in Microsoft Defender SmartScreen

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

As malware protection and other safeguards evolve, cybercriminals look for new ways to circumvent security measures. Phishing has emerged as a leading threat, with apps and websites designed to steal credentials by tricking people into voluntarily entering passwords. As a result, many organizations are transitioning to the ease and security of passwordless sign in with Windows Hello or Windows Hello for Business.

However, people who are still using passwords can also benefit from powerful credential protection in Windows 11. Microsoft Defender SmartScreen now includes enhanced phishing protection to automatically detect when you enter your Microsoft password into any app or website. Windows then identifies if the app or site is securely authenticating to Microsoft and warns if your credentials are at risk. Because you are alerted at the moment of potential credential theft, you can take pre-emptive action before your password is used against you or your organization.

Access management

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

Windows Hello for Business is configured by Group Policy in Active Directory or a mobile device management (MDM) policy in Microsoft Endpoint Manager and other MDM solutions. IT administrators can set policies that strengthen security and also enable group setup of multifactor authentication for a single sign-in experience. With Windows Hello for Business,

IT administrators can also create conditional access policies, such as allowing users to only access approved networks.

Access control in Windows ensures that shared resources are available to users and groups other than the resource's owner and are protected from unauthorized use. IT administrators can manage users', groups', and computers' access to objects and assets on a network or computer. After a user is authenticated, the Windows operating system implements the second phase of protecting resources by using built-in authorization and access control technologies to determine if an authenticated user has the correct permissions.

Access Control Lists (ACL) describe the permissions for a specific object and can also contain System Access Control Lists (SACL). SACLs provide a way to audit specific system level events, such as when a user attempt to access file system objects. These events are essential for tracking activity for objects that are sensitive or valuable and require extra monitoring. Being able to audit when a resource attempts to read or write part of the operating system is critical to understanding a potential attack.

IT administrators can refine the application and management of access to:

- Protect a greater number and variety of network resources from misuse.

- Provision users to access resources in a manner that is consistent with organizational policies and the requirements of their jobs. Organizations can implement the principle of least privileged access, which asserts that users should be granted access only to the data and operations they require to perform their jobs.

- Update users' ability to access resources on a regular basis as an organization's policies change or as users' jobs change.

- Support evolving workplace needs, including access from hybrid or remote locations, or from a rapidly expanding array of devices including tablets and mobile phones.

- Identify and resolve access issues when legitimate users are unable to access resources that they need to perform their jobs.

Learn more about [Access Control](#).

Advanced credential protection

In addition to adopting passwordless sign in, organizations can strengthen security for user

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

52

and domain credentials with Windows Credential Guard and Windows Defender Remote Credential Guard.

Windows Credential Guard

Note: This section applies to Windows 11 Enterprise.

Enabled by default in Windows 11 Enterprise, Windows Credential Guard uses hardware-backed, virtualization-based security (VBS) to protect against credential theft. With Windows Credential Guard, the Local Security Authority (LSA) stores and protects secrets in an isolated environment that is not accessible to the rest of the operating system. LSA uses remote procedure calls to communicate with the isolated LSA process.

By protecting the LSA process with virtualization-based security, Windows Credential Guard shields systems from credential theft attack techniques like pass-the-hash or pass-the-ticket. It also helps prevent malware from accessing system secrets even if the process is running with admin privileges.
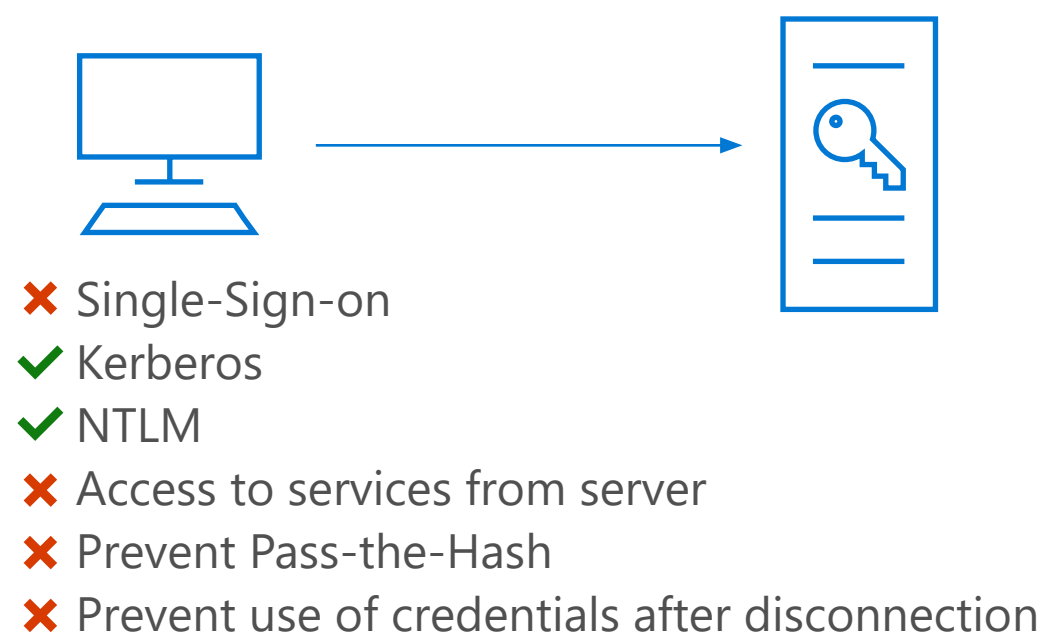
[Window Defender Remote Credential Guard](#) helps you protect your credentials over a Remote Desktop connection by redirecting the Kerberos requests back to the device that is requesting the connection. It also provides single sign-on experiences for Remote Desktop sessions.

Administrator credentials are highly privileged and must be protected. When you use Windows Defender Remote Credential Guard to connect during Remote Desktop sessions your credential and credential derivatives are never passed over the network to the target device. If the target device is compromised, your credentials are not exposed.

The following diagram shows how a standard Remote Desktop session to a server without Windows Defender Remote Credential Guard works:

Remote Desktop connection to a server without Windows Defender Remote Credential Guard

- Credentials sent to server
- Credentials are not protected from attackers on remote host
- Attacker can continue to use credentials after disconnection

✖ Single-Sign-on
✔ Kerberos
✔ NTLM
✖ Access to services from server
✖ Prevent Pass-the-Hash
✖ Prevent use of credentials after disconnection

= Credentials

The following diagrams help understand how Windows Defender Remote Credential Guard works, what it helps to protect against, and compares it with the Restricted Admin mode option:

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

54

Privacy
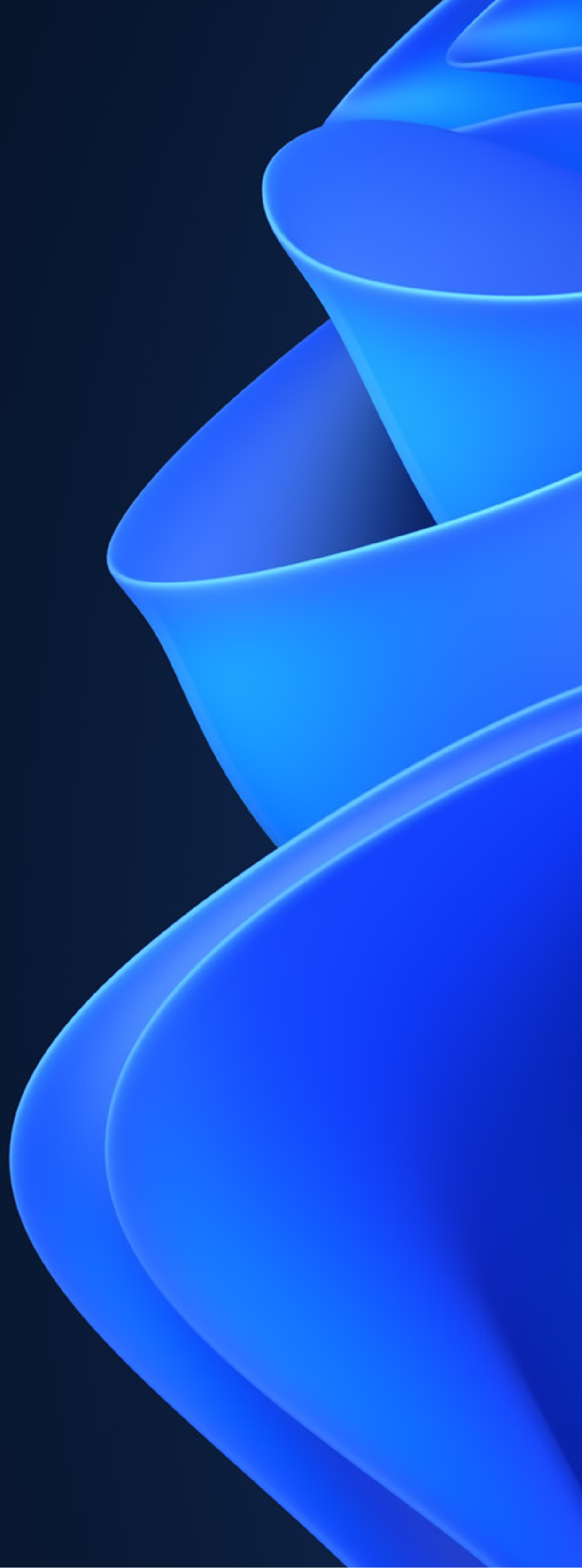
Remote Desktop connection to a server with Windows Defender Remote Credential Guard

- ✔ Kerberos
- ✖ NTLM
- ✔ Access to services from server
- ✔ Prevent Pass-the-Hash
- ✔ Prevent use of credentials after disconnection

- • Credentials protected by Windows Defender Remote Credential Guard
- • Connect to other systems using SSO
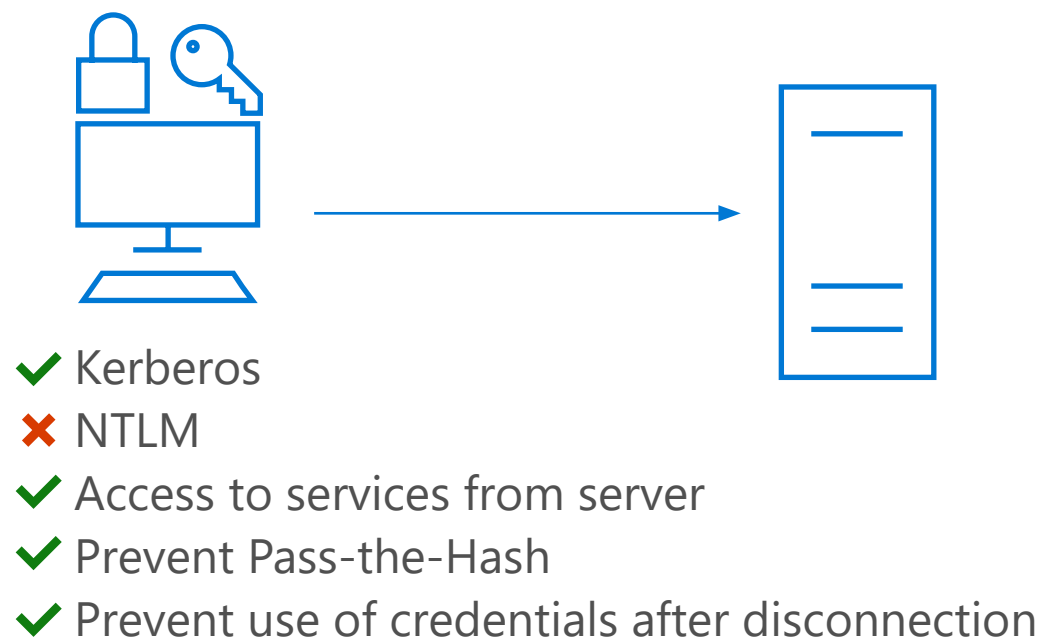- • Host must support Windows Defender Remote Credential Guard

Restricted admin mode

- ✔ Kerberos
- ✔ NTLM
- ✖ Access to services from server
- ✔ Prevent Pass-the-Hash
- ✔ Prevent use of credentials after disconnection
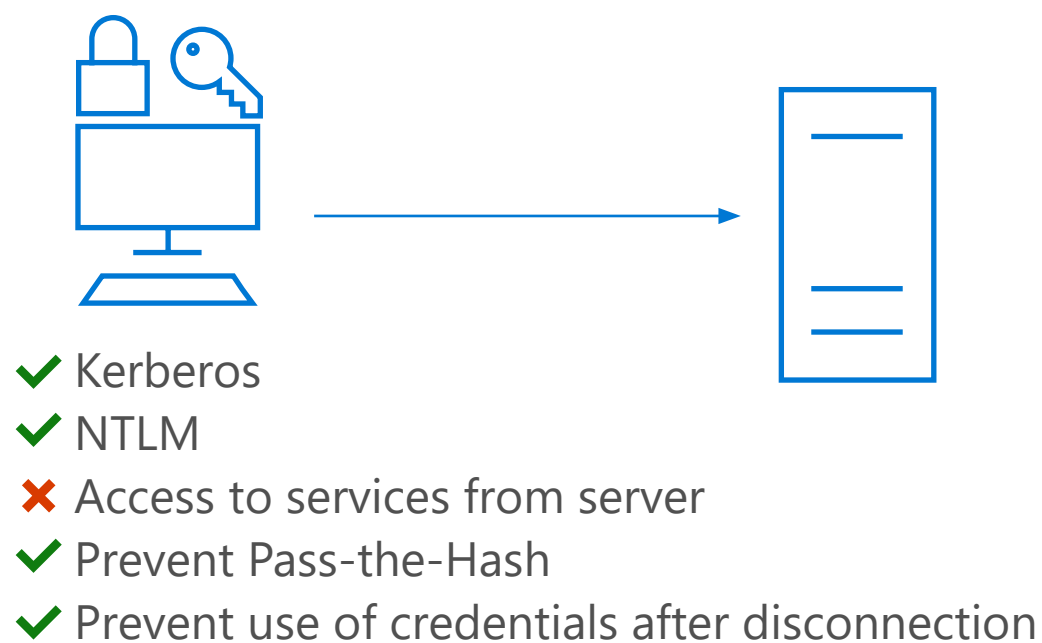
- • Credentials used are remote server local admin credentials
- • Connect to other systems using the host's identity
- • Host must support Restricted Admin mode
- • Highest protection level
- • Requires user account administrator rights

🔒 = Credential protection
🔑 = Credentials

As illustrated, Windows Defender Remote Credential Guard blocks NTLM (allowing only Kerberos), helping to prevent pass-the-hash attacks and malicious use of credentials after disconnection.

Privacy controls

[Privacy: Your data, powering your experiences, controlled by you](#). Privacy is becoming top of mind for customers, who want to know who is using their data and why. They also need to know how to control and manage the data that is being collected—so providing transparency and control over this personal data is essential. At Microsoft we are focused on protecting the privacy and confidentiality of your data and will only use it in a way that is consistent with your expectations.

Customers can use the Microsoft [Microsoft Privacy dashboard](#) to view, export, and delete their information, giving them further transparency and control. They can also use the [Microsoft Privacy Report](#) to learn more about Windows data collection and how to manage it. For enterprises we provide a guide for Windows Privacy Compliance that provides additional details on the available controls and transparency.

Track app usage

Prominent system tray icons show users when resources and apps like microphones and location are in use. A description of the app and its activity are presented in a simple tooltip that appears when you hover over an icon with your cursor. Apps can also make use of new Windows APIs to support Quick Mute functionality and more.

Every Microsoft customer should be able to use our products secure in the knowledge that we will protect their privacy and give them the information and tools they need to easily make privacy decisions with confidence. Accessed in Settings, the new app usage history feature gives users a seven-day history of resource access for Location, Camera, Microphone, Phone Calls, Messaging, Contacts, Pictures, Videos, Music library, Screenshots, and other apps.

This information helps you determine if an app is behaving as expected, so that you can change the app's access to resources as desired.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security | Identity | Privacy | Cloud Services | Security Foundation | Conclusion

57

Cloud
Services

Cloud

Cloud Services

Protecting your work information			Protecting with Microsoft Accounts
Azure Active Directory	Microsoft Endpoint Manager	Universal Print	Microsoft Account
Modern Device Management	Remote Wipe	Microsoft Azure Attestation Service	Find my Device
MDM Security Baseline	Secured-core Configuration Lock	Azure Code Signing	OneDrive Personal Vault
Windows Autopatch	Windows Autopilot and Zero-Touch Deployment	Microsoft OneDrive	

Identity

Secured Identity

	Windows Hello	Advanced Credential Protection	**Privacy**
Enabling Passwordless Sign In	PIN	Windows Credential Guard	Transparency and Audit Trail location, camera, and microphone
Windows Hello (for Business)	Windows Presence Sensing	Windows Defender Remote	Use of diagnostic data
Temporary Access Pass	Enhanced Sign in Security	Credential Guard	
Cloud Trust	Simplified Sign in for EDU	Smart Cards	
Microsoft Authenticator	Enhanced Phishing Detection/Protection	Access Management	
Fast Identity Online (FIDO)			

Application

Application Security

Smart App Control	App isolation
User Account Control (UAC)	App containers
Windows Defender Application Control (WDAC)	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	Code Signing and Integrity	Windows Security Policy Setting and Auditing
Cryptography	Device Health Attestation	Windows Security App
Certificates		

Hardware (Chip)

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

Silicon Assisted Security

Secured Kernel (HVCI enabled by default)	Secured-Core PCs
Hardware Enforced Stack Protection	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

Today's workforce has more freedom and mobility than ever before, and the risk of data exposure is also at its highest. We are focused on getting customers to the cloud to benefit from modern hybrid workstyles while improving security management. Built on zero-trust principles, Windows 11 works with Microsoft cloud services to safeguard sensitive information while controlling access and mitigating threats.

From identity and device management to Office apps and data storage, Windows 11 and integrated cloud services can help improve productivity, security, and resilience anywhere.

Protecting your work information

Azure Active Directory

Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education. AAD is sold separately.
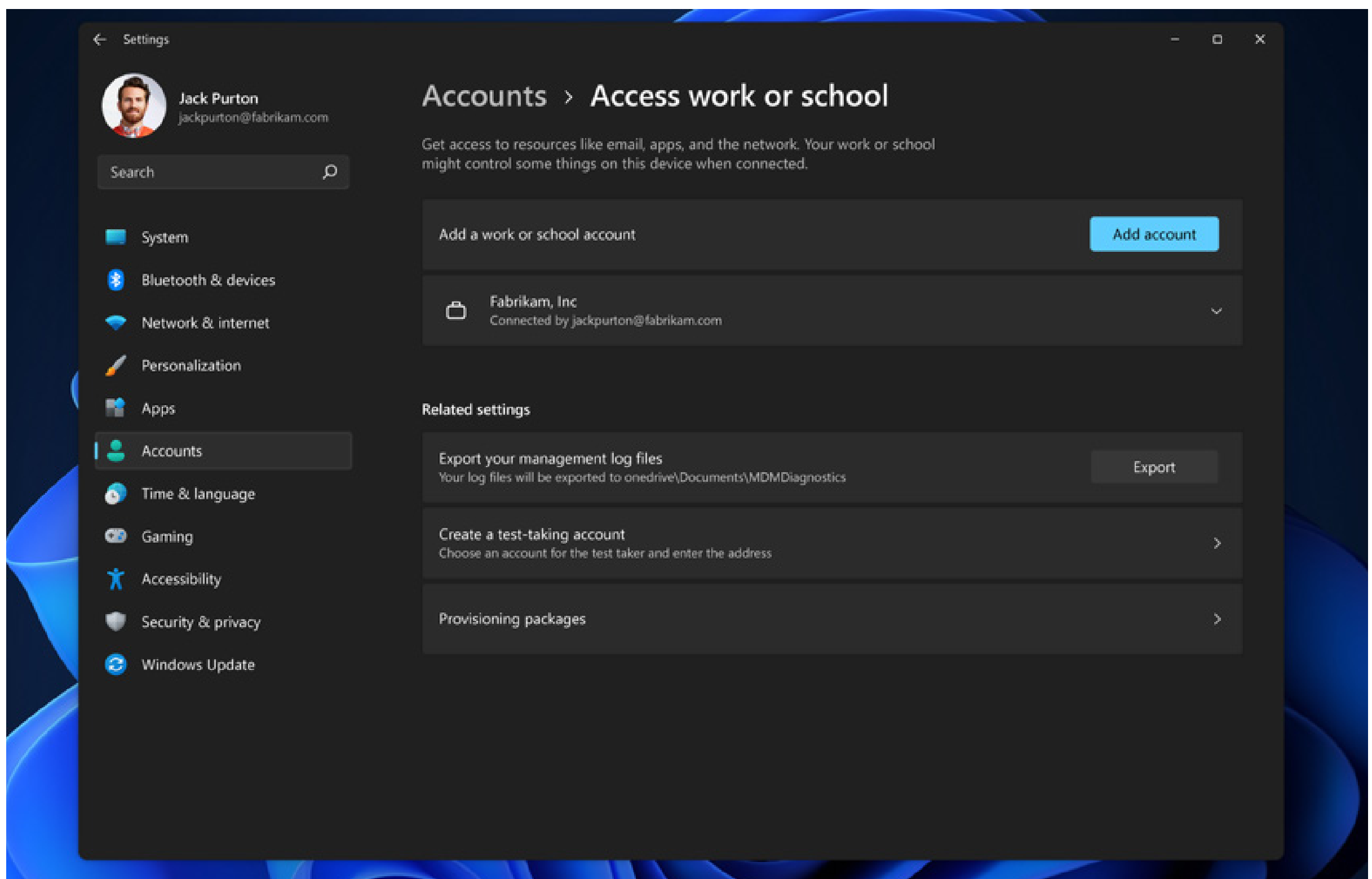
Microsoft Azure Active Directory is a comprehensive cloud-based identity management solution that helps enable secure access to applications, networks, and other resources and guard against threats. Azure Active Directory can also be used with Windows Autopilot for zero-touch provisioning of devices preconfigured with corporate security policies.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

59

Organizations can deploy Azure Active Directory joined devices to enable access to both cloud and on-premises apps and resources. Access to resources can be controlled based on Azure AD account and Conditional Access policies applied to the device. By registering devices with Azure Active Directory—also called Workplace joined—you can also support users in bring your own device (BYOD) or mobile device scenarios. Credentials are authenticated and bound to the joined device and cannot be transferred to another.

To provide more security and control for IT and a seamless experience for end users, Azure Active Directory works with apps and services including on-premises software and thousands of software-as-a-service (SaaS) applications. Azure Active Directory protections include single sign-on, multifactor authentication, conditional access policies, identity protection, identity governance, and privileged identity management.

Windows 11 works with Azure Active Directory to provide secure access, identity management, and single sign-on to apps and services from anywhere. Windows has built-in settings to add work or school accounts by syncing the device configuration to an Active Directory or Azure Active Directory domain.

When a device is Azure Active Directory joined and managed with Microsoft Endpoint Manager[6], it will offer the following security benefits:

- Default managed user and device settings and policies

- Single sign-on to all Microsoft Online Services

- Full suite of authentication management capabilities using Windows Hello for Business

- Single sign-on (SSO) to enterprise and SaaS applications

- No use of consumer Microsoft Account identity

Organizations and users can join or register their Windows devices with Azure AD to get a seamless experience to both native and web applications. In addition, users can setup Windows Hello for Business or FIDO2 security keys with Azure AD and benefit from greater security with passwordless authentication. In combination with Microsoft Endpoint Manager, Azure AD offers a powerful security control through Conditional Access to protect access to organizational resources to healthy and compliant devices. Note that Azure Active Directory is only supported on Windows Pro and Enterprise editions.

Learn more about the available subscriptions and pricing for Azure Active Directory.

Modern device management (MDM)

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

Windows 11 supports modern device management so that IT pros can manage company security policies and business applications without compromising user privacy on corporate or employee-owned devices. With MDM solutions, IT can manage Windows 11 using industry-standard protocols. To simplify setup for users, management features are built directly into Windows, eliminating the need for a separate MDM client.

Windows 11 built-in management features include:

- The enrollment client, which enrolls and configures the device to communicate with the enterprise management server.

- The management client, which periodically synchronizes with the management server to check for updates and apply the latest policies set by IT.

Learn more about the MDM protocols: [MS-MDM]: Mobile Device Management Protocol and [MS-MDE2]: Mobile Device Enrollment Protocol Version 2.

MDM security baseline

Windows 11 can be configured with Microsoft's [MDM security baseline](#) backed by ADMX policies, which functions like the Microsoft GP-based security baseline. The security baseline enables IT administrators to easily address security concerns and compliance needs for modern cloud-managed devices.

The MDM security baseline includes policies for:

- Microsoft inbox security technology such as BitLocker, Windows Defender for SmartScreen, virtualization-based security, Windows Defender Exploit Guard, Microsoft Defender Antivirus, and Windows Firewall.

- Restricting remote access to devices.

- Setting credential requirements for passwords and PINs.

- Restricting use of legacy technology.

Microsoft Endpoint Manager[14]

Microsoft Endpoint Manager is sold separately. Note: This section applies to the following Windows 11 editions: Pro, Pro Workstation, Enterprise, Pro Education, and Education.

Microsoft Endpoint Manager is a comprehensive endpoint management solution that helps secure, deploy, and manage users, apps, and devices. Endpoint Manager brings together technologies like Microsoft Intune, Microsoft Configuration Manager and Windows Autopilot to simplify provisioning, configuration management, and software updates across your organization.

Endpoint Manager works with Azure Active Directory to manage security features and processes including multifactor authentication.

You can cut costs while securing and managing remote PCs through the cloud in compliance with your company's policies.[15] For example, you save time and money by provisioning preconfigured devices to remote employees using Windows Autopilot for zero-touch deployment.

Windows 11 enables IT professionals move to the cloud while consistently enforcing security policies. Windows 11 provides expanded support for Group Policy administrative templates (ADMX-backed policies) in MDM solutions like Microsoft Endpoint Manager, enabling IT professionals to easily apply the same security policies to both on-premises and remote devices.

Learn more about [Microsoft Endpoint Manager](#).

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | **Cloud Services** | Security Foundation | Conclusion

62

Remote Wipe

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

When a device is lost or stolen, IT administrators might want to remotely wipe data stored in memory and hard disks. A help desk agent might also want to reset devices to fix issues encountered by remote workers.

Windows 11 supports the Remote Wipe configuration service provider (CSP) so that MDM solutions can remotely initiate any of the following operations:

- Reset the device and remove user accounts and data.

- Reset the device and clean the drive.

- Reset the device but persist user accounts and data.

Windows Autopatch

Note: This section applies to the following Windows 11 editions: Enterprise with an E3 or E5 plan (or subscription).

Updating software and resolving vulnerabilities is an ongoing process, and IT administrators anticipate software updates on the second Tuesday of the month with some trepidation. The fear that an update may introduce new issues into the system must be weighed against the benefits of closing potential gaps in protection and realizing gains from new features.

With the Autopatch service, IT teams can delegate management of updates to Windows 10/11, Microsoft Edge, and Microsoft 365 apps to Microsoft. Under the hood, Autopatch takes over configuration of the policies and deployment service of Windows Update for Business. What the customer gets are endpoints that are up to date, thanks to dynamically generated rings for progressive deployment that will pause and/or roll back updates (where possible) when issues arise.

The goal is to provide peace of mind to IT pros, encourage rapid adoption of updates, and to reduce bandwidth required to deploy them successfully, thereby closing gaps in protection that may have been open to exploitation by malicious actors.

Learn more about [Windows AutoPatch](#).

Secured-core configuration lock (config lock)

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

In an enterprise organization, IT administrators enforce policies on their corporate devices to protect the OS and keep devices in a compliant state by preventing users from changing configurations and creating configuration drift. Configuration drift occurs when users with local admin rights change settings and put the device out of sync with security policies.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | **Cloud Services** | Security Foundation | Conclusion

63

Devices in a non-compliant state can be vulnerable until the next sync and configuration reset with the MDM.

Secured-core configuration lock (config lock) is a Secured-core PC (SCPC) feature that prevents users from making unwanted changes to security settings. With config lock, the OS monitors the registry keys that configure each feature and when it detects a drift, reverts to the IT-desired SCPC state in seconds.

Learn more about [Windows 11 with config lock](#).

Windows Autopilot and zero-touch deployment

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

Traditionally, IT pros spend significant time building and customizing images that will later be deployed to devices. Windows Autopilot introduces a new approach with a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use and ensuring they are delivered locked down and compliant with corporate security policies.

- From a user perspective, it only takes a few simple operations to get their device ready for use.

- From an IT pro perspective, the only interaction required from the end user is to connect to a network and verify their credentials. After that point setup is automated.

Windows Autopilot enables you to:

- Automatically join devices to Azure Active Directory (Azure AD) or Active Directory via Hybrid Azure AD Join. For more information about the differences between these two join options, see [Introduction to device management in Azure Active Directory](#).

- Auto-enroll devices into MDM services, such as Microsoft Intune (Requires an Azure AD Premium subscription for configuration).

- Automatic upgrade to Enterprise Edition if required.

- Restrict the Administrator account creation.

- Create and auto-assign devices to configuration groups based on a device's profile.

- Customize OOBE content specific to the organization.

Existing devices can also be quickly prepared for a new user with [Windows Autopilot Reset](#). The reset capability is also useful in break/fix scenarios to quickly bring a device back to a business-ready state.

Learn more about [Windows Autopilot](#).

Universal Print

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

Unlike traditional print solutions that rely on Windows print servers, Universal Print is a Microsoft hosted cloud subscription service that supports a zero-trust security model by enabling network isolation of printers, including the Universal Print connector software, from the rest of the organization's resources.[16] Client devices do not need to be on the same local network as the printers.

Universal Print supports zero-trust security by requiring that:

- Each connection to Universal Print cloud service requires authentication that has been validated by Azure AD. A hacker would have to have knowledge of the right credentials to successfully connect to the Universal Print service.

- Every connection established by the client, the printer, or another cloud services to the Universal Print cloud service uses TLS 1.2 protection. This protects network snooping of traffic to gain access to sensitive data.

- Each acting client app must register with Azure AD and specify the set of permission scopes it requires. Microsoft's own acting client apps—for example the Universal Print connector—are registered with the Azure AD service and customers consent to the required permission scopes as part of onboarding the app.

- Each authentication with Azure AD from an acting client app cannot extend the permission scope as defined by the acting client app. This prevents the app from requesting additional permissions if the app is breached.

Additionally, Windows 11 includes MDM support to simplify printer setup for user. With initial support from Microsoft Endpoint Manager, admins can now configure policies to provision specific printers onto the user's Windows devices.

Learn more about Universal Print.

Microsoft Azure Attestation Service

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

Remote attestation helps ensure that devices are compliant with security policies and operating in a trusted state before they are allowed access to resources. Microsoft Intune integrates with Microsoft Azure Attestation Service to review Windows device health comprehensively and connect this information with AAD conditional access.

Attestation policies are configured in the Microsoft Azure Attestation Service which can then:

- Verify the integrity of evidence provided by the Windows Attestation component by validating the signature and ensuring the Platform Configuration Registers (PCRs) match the values recomputed by replaying the measured boot log.

- Verify that the TPM has a valid Attestation Identity Key issued by the authenticated TPM.

- Verify that security features are in the expected states.

Once this verification is complete the attestation service returns a signed report with the security features states to the relying party—such as Microsoft Intune—to assess the trustworthiness of the platform relative to the admin-configured device compliance specifications.

Conditional access is then granted or denied based on the device's compliance.

Azure Code Signing

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

Windows Defender Application Control (WDAC) in Windows 11 enables customers to define policies for controlling what is allowed to run on their devices. WDAC policies can be remotely applied to devices using an MDM solution like Microsoft Endpoint Manager.

To simplify WDAC enablement, organizations can take advantage of Azure Code Signing, a secure and fully managed service for signing WDAC policies and apps.

Microsoft OneDrive

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

OneDrive provides additional security, backup, and restore options for your important files. OneDrive stores and protects your files in the cloud, allowing you to access them from your laptop, desktop, and mobile devices. Plus, OneDrive provides an excellent solution for backing up your folders. If your device is lost or stolen, you can quickly recover all your important files from the cloud.

Learn more about OneDrive.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | **Cloud Services** | Security Foundation | Conclusion

66

In the event of a ransomware attack, OneDrive can enable recovery. And if you've configured backups in OneDrive, you have additional options to mitigate and recover from a ransomware attack. Learn more about how to recover from a ransomware attack using Office 365 and how to restore from your OneDrive.

Protecting your personal information

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

Microsoft Account

When you add your Microsoft Account to Windows 11, you can bring all your Windows, Microsoft Edge, web page favorites, files, photos, and a whole lot more. Your Microsoft Account lets you manage everything all in one place. Keep tabs on your subscriptions and order history, update your privacy and security settings, track the health and safety of your devices, and get rewards. Everything stays with you in the cloud, across devices, and between OS ecosystems, including iOS and Android.

You can even go passwordless with your Microsoft Account by removing the password from your MSA and using the Microsoft Authenticator app on your mobile Android or iOS phone.

Find my Device

When location services are turned on, basic system services like time zone and Find my Device will be allowed to use location. When enabled, Find my Device can be used to help recover lost or stolen hardware to reduce security threats that rely on physical access to devices.

Learn more about how to set up, find, and lock a lost Windows device through your Microsoft Account.

OneDrive Personal Vault

OneDrive Personal Vault also provides protection for your most important or sensitive files and photos without sacrificing the convenience of anywhere access. Protect digital copies of your important documents in OneDrive Personal Vault. Your files will be secured by identity verification, yet still easily accessible to you across your devices.

Learn how to set up your Personal Vault with a strong authentication method or a second step of identity verification, such as your fingerprint, face, PIN, or a code sent to you via email or SMS.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security | Identity | Privacy | **Cloud Services** | Security Foundation | Conclusion

67

Security
Foundation

Microsoft is committed to continuously investing in improving our software development process, building highly secure-by-design software, and addressing security compliance requirements. At Microsoft, we embed security and privacy considerations from the earliest life-cycle phases of all our software development processes. We build in security from the ground up for powerful defense in today's threat environment.

Every component of the Windows 11 technology stack, from chip-to-cloud, is purposefully designed to help ensure ultimate security. Windows 11 meets the modern threats of today's hybrid work environments by delivering hardware-based isolation, end-to-end encryption, and advanced malware protection.

With Windows 11, organizations can improve productivity and gain intuitive new experiences without compromising security.

Security foundation

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

Software development lifecycle

The Microsoft Security Development Lifecycle (SDL) introduces security best practices, tools, and processes throughout all phases of engineering and development.

A range of tools and techniques—such as threat modeling, static analysis, fuzzing, and code quality checks—enable continued security value to be embedded into Windows by every engineer on the team from day one. Through the SDL practices, Microsoft engineers are continuously provided with actionable and up-to-date methods to improve development workflows and overall product security before the code has been released.

Additionally, Microsoft Offensive Research and Security Engineering performs targeted design reviews, audits, and deep penetration testing of select Windows features. Microsoft's open source OneFuzz platform allows developers to fuzz features for Windows at scale as part of their development and testing cycle.

Windows Insiders and bug bounty program

As part of our secure development process, the Microsoft Windows Insider Preview bounty program invites eligible researchers across the globe to find and submit vulnerabilities that reproduce in the latest Windows Insider Preview (WIP) Dev Channel.

The goal of the Windows Insider Preview bounty program is to uncover significant vulnerabilities that have a direct and demonstrable impact on the security of customers using the latest version of Windows.

Through this collaboration with researchers across the globe, our teams identify critical vulnerabilities that were not previously found during development and quicky fix the issues before releasing our final Windows.

Learn more about the [Windows Insider Program](#).

Certification

Microsoft is committed to supporting product security standards and certifications, including FIPS 140 and Common Criteria as an external validation of security assurance.

The Federal Information Processing Standard (FIPS) Publication 140 is a U.S. government standard that defines the minimum security requirements for cryptographic modules in IT products. Microsoft maintains an active commitment to meeting the requirements of the FIPS 140 standard, having validated cryptographic modules against FIPS 140-2 since it was first established in 2001. Multiple Microsoft products, including Windows 11, Windows 10, Windows Server, and many cloud services, use these cryptographic modules.

Common Criteria (CC) is an international standard currently maintained by national governments who participate in the Common Criteria Recognition Arrangement. CC defines a common taxonomy for security functional requirements, security assurance requirements, and an evaluation methodology used to ensure products undergoing evaluation satisfy the functional and assurance requirements. Microsoft ensures that products incorporate the features and functions required by relevant Common Criteria Protection Profiles and completes Common Criteria certifications of Microsoft Windows products.

Microsoft publishes the list of FIPS 140 and CC certified products at [Federal Information Processing Standard (FIPS) 140 Validation—Windows security | Microsoft Docs](#) and [Common Criteria Certifications—Windows security | Microsoft Docs](#).

Secure supply chain

The end-to-end Windows supply chain is complex, extending from the entire development process to components such as chips, firmware, drivers, operating system, and apps from other organizations, manufacturing, and security updates. Microsoft invests significantly in Windows 11 supply chain security, as well as the security of features and components. In 2021 the United States issued an executive order on enhancing the nation's cybersecurity. The executive order, along with various attacks like SolarWinds and WannaCry, elevated the urgency and importance of ensuring a secure supply chain.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

70

Microsoft requires the Windows 11 supply chain to comply with controls including:

Identity Management and User Access Control
Access Control / Principles of least privilege / RBAC / Segregation of Duties / MFAs /
Account Management / Physical Access Control

Information Security
Information Handling / Cryptography / Vulnerability Scanning / Encryption / Integrity and Attestation / Confidentiality

Operational Controls
Code of Repo Ownership / Config & Change Management / Asset ownership / Manufacturing Standards

Security Monitoring & Event Logging
Network / Host / Application / Services / DevOps / Manufacturing Security / Physical Security Monitoring

Supplier Security Control
SSPA / Supplier Screening / Supplier Inventory

Logistics Security Control
Receiving / Shipping / Warehouse & Storage / Logistics Management

In addition to following the above supply chain security controls, SBOMs are leveraged to provide the transparency and provenance of the content as it moves through various stages of the Windows supply chain. This enables trust between each supply chain segment, ensures that tampering has not taken place during ingestion and along the way, and provides a provable chain of custody for the product that we ship to customers.

Code signing software is the best way to guarantee application integrity and authenticity. Code signing proprietary applications and software from other organizations greatly reduces the complexity of creating and managing application control policies. Code signing enables the creation and deployment of certificate chain-based application control policies which can then be cryptographically enforced.

Traditionally, code signing has been a difficult undertaking due to the complexities involved in obtaining certificates, securely managing those certificates, and integrating a proper signing process into the development and continuous integration and continuous deployment (CI/CD) pipelines.

Azure Code Signing (currently in private preview) minimizes the complexity of code signing with a turnkey service backed by a Microsoft managed certificate authority, eliminating the need to procure and self-manage any signing certificates. The service is managed just as any other Azure resource and integrates easily with the leading development and CI/CD toolsets.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
Identity | Privacy | Cloud Services | Security Foundation | Conclusion

71

Cloud	**Cloud Services**	**Protecting your work information**		**Protecting with Microsoft Accounts**
		Azure Active Directory	Microsoft Endpoint Manager	Universal Print	Microsoft Account
		Modern Device Management	Remote Wipe	Microsoft Azure Attestation Service	Find my Device
		MDM Security Baseline	Secured-core Configuration Lock	Azure Code Signing	OneDrive Personal Vault
		Windows Autopatch	Windows Autopilot and Zero-Touch Deployment	Microsoft OneDrive	

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

Various trust levels are supported to enable code signing in the end-to-end development to deployment pipeline—Public trust for publicly released software, Private trust for line-of-business applications and IT management scenarios, and test certificates for the development and validation of inner loops.

Conclusion

Designed for hybrid work, Windows 11 is the most secure Windows yet with hardware and software working together to provide powerful protection across the device, operating system, identities, applications, and cloud services. We will continue to build on our security foundations with innovations that deliver powerful protection now and in the future.

Learn how to upgrade to Windows 11 now.

For the latest information and version of this document see windows.com/business/windows-11-security.

What's new

New

Azure Code Signing
Enhanced phishing protection with Microsoft Defender SmartScreen
Hardware-enforced stack protection
Secured-core configuration lock
Simplified sign-in for education
Smart App Control
Windows presence sensing

Enhanced

Cryptopgraphy
Microsoft Pluton
Microsoft vulnerable driver blocklist
Secured kernel (HVCI enabled by default)
Firmware protection in Secured-core PCs
Windows Defender Credential Guard
Microsoft Defender Application Guard (MDAG)
Windows Defender Firewall

Document revision history

Date	Summary
November 2021	Link updates and formatting
February 2022	Revisions to Hardware root-of-trust, Virus and threat protection, and Windows Hello for Business content.
April 2022	Added Upcoming features section
September 2022	Updates with Windows 11 2022 Update features and enhancements. See [What's New](#).
April 2023	Minor edits and updates to edition availability

Appendix

Endnotes

1   Microsoft Security Signals, September 2021.
2   Hypervisor-protected coder integrity, which activates virtualization-based security, is enabled by default on clean installations only.
3   Windows 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.
4   Windows 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.
5   Microsoft Endpoint Manager and Microsoft Azure Active Directory subscriptions sold separately.
6   Sold separately.
7   Email encryption is supported on products such as Microsoft Exchange Server and Microsoft Exchange Online.
8   [Microsoft Defender for Endpoint Plan 1](#) and [Microsoft Defender for Endpoint Plan 2](#)
9   [Microsoft Defender for Endpoint Plan 2](#) and [Microsoft 365 Defender](#)
10   Available with a standalone license for Windows 11 Pro, and as part of Windows 11 E5.
11   Microsoft Application Guard for Microsoft Edge is available with Windows 11 E3. Microsoft Application Guard for Microsoft Office is available with Microsoft 365 E5.
12   Requires Azure Active Directory Premium; sold separately.
13   Hardware dependent feature available in a future release.
14   Microsoft 365 E3 or E5 required; sold separately.
15   The Total Economic Impact™ of Windows Pro Device, Forrester study commissioned by Microsoft, June 2020.
16   Universal print is available with Windows 11 Enterprise E3.