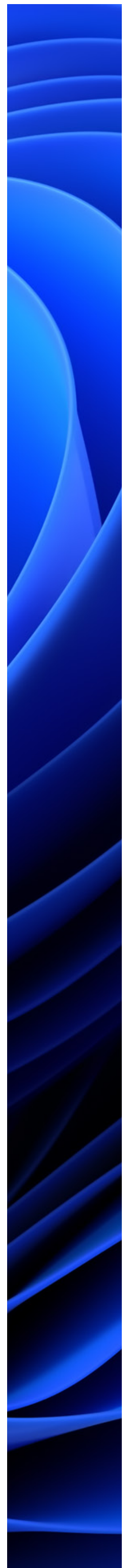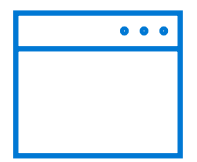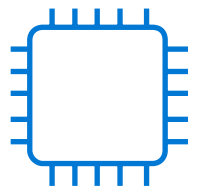# Windows 11 Security Book:
Powerful security from chip to cloud

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 and Privacy | Privacy Controls and Transparency | 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 the new data from the Microsoft commissioned Security Signals report, 75% of security decision-makers at the vice-president level and above feel that the move to hybrid work leaves their organization more vulnerable to security threats.
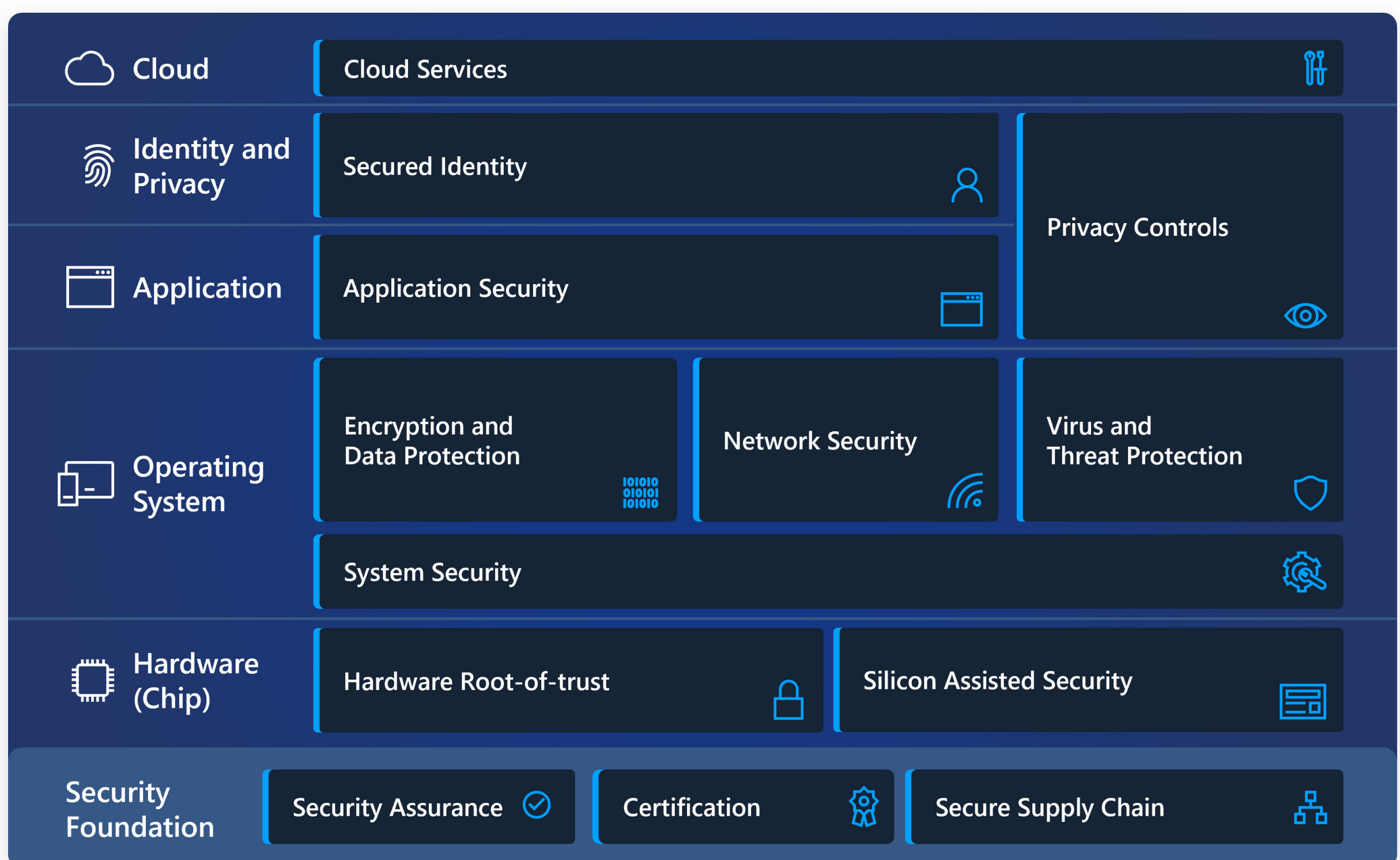
At Microsoft, we work hard to **empower every person and every organization on the planet to achieve more**. We're committed to helping customers get secure—and stay secure. With over $1 billion invested in security each year, more than 3,500 dedicated security professionals, and some 1.3 billion Windows 10 devices used around the world, we have deep insight into the threats our customers face.

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

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

3

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

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

Cloud	Cloud Services		
Identity and Privacy	Secured Identity		Privacy Controls
Application	Application Security		
Operating System	Encryption and Data Protection	Network Security	Virus and Threat Protection
	System Security		
Hardware (Chip)	Hardware Root-of-trust		Silicon Assisted Security
Security Foundation	Security Assurance	Certification	Secure Supply Chain

How Windows 11 enables Zero Trust protection

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

Verify explicitly   **Use least privileged access**   **Assume breach**
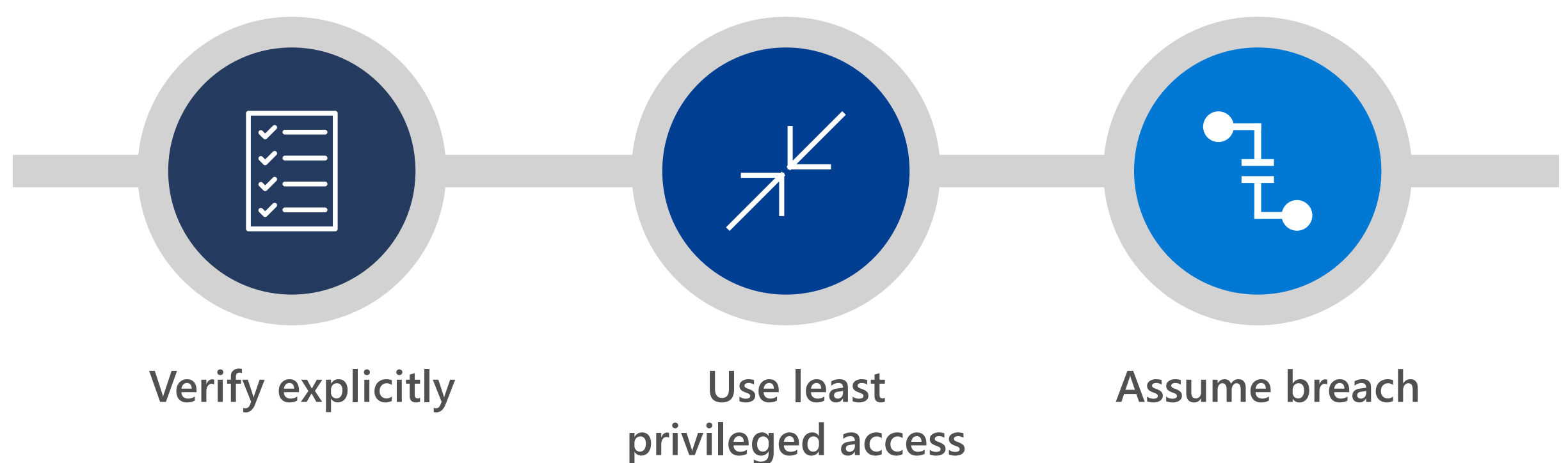
For Windows 11, the Zero Trust principle of verify explicitly applies to the risks introduced by both devices and users. Windows 11 provides chip-to-cloud security, giving IT administrators the attestation and measurements to determine whether a device meets requirements and can be trusted. And Windows 11 works out of the box with Microsoft Intune and Azure Active Directory, so access decisions and enforcement are seamless. Plus, IT Administrators can easily customize Windows 11 to meet specific user and policy requirements for access, privacy, compliance, and more.

Individual users also benefit from powerful safeguards including new standards for hardware-based security and passwordless protection. Now, all users can replace potentially risky passwords by providing secure proof of identity with the Microsoft Authenticator app, signing in with face or fingerprint,[2] a security key, or a verification code sent to a phone or email.

Overview of Windows 11 security priorities

Security, by default

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

Enhanced hardware and operating system security

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

In Windows 11, hardware and software work together to protect the operating system, with virtualization-based security (VBS) and Secure Boot built-in and enabled by default on new CPUs. Even if bad actors get in, they don't get far. VBS uses hardware virtualization features to create and isolate a secure region of memory from the operating system. This isolated environment hosts multiple security solutions, greatly increasing protection from vulnerabilities in the operating system, and preventing the use of malicious exploits. In combination with device health attestation with cloud services Windows 11 is zero trust ready.

Robust application security and privacy controls

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

In Windows 11, [Microsoft Defender Application 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 device location or access resources like camera and microphone.

Secured identities

Passwords are inconvenient to use and prime targets for cybercriminals—and they've been an important part of digital security for years. That changes with the passwordless protection

available with Windows 11. After a secure authorization process, credentials are protected behind layers of hardware and software security, giving users secure, passwordless access to their apps and cloud services.
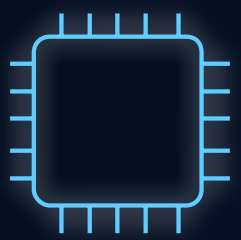
Individual users can remove the password from their Microsoft account and use the Microsoft Authenticator app,[4] Windows Hello,[5] a FIDO2 security key, a smart card, or a verification code sent to their phone or email. IT administrators and consumers can set up Windows 11 devices as passwordless out-of-the-box, taking advantage of technologies such as Windows Hello in alignment with Fast Identity Online (FIDO) standards.

Windows 11 protects credentials with chip-level hardware security including TPM 2.0 combined with VBS and Microsoft Credential Guard.
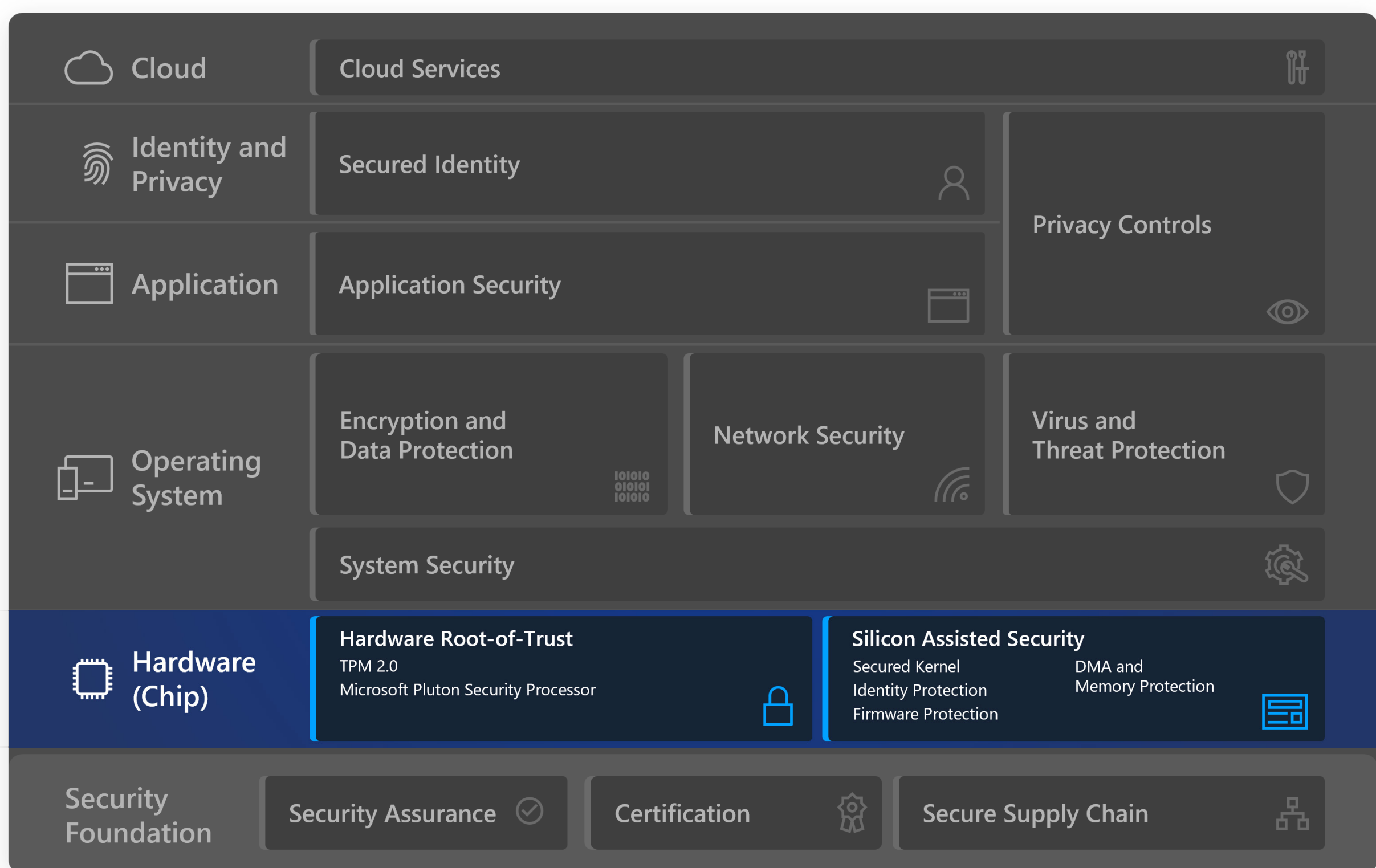
Connecting to cloud services

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

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

Hardware Security

Cloud	Cloud Services		
Identity and Privacy	Secured Identity		Privacy Controls
Application	Application Security		
Operating System	Encryption and Data Protection	Network Security	Virus and Threat Protection
	System Security		
Hardware (Chip)	**Hardware Root-of-Trust** TPM 2.0 Microsoft Pluton Security Processor	**Silicon Assisted Security** Secured Kernel Identity Protection Firmware Protection	DMA and Memory Protection
Security Foundation	Security Assurance	Certification	Secure Supply Chain

Modern threats require modern security with a strong alignment between hardware security and software security techniques 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 inside, intruders can be difficult to detect while engaging in multiple nefarious activities from stealing important data or credentials to implanting malware into low level device firmware that 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. By building security capabilities in hardware we can remove entire classes of vulnerabilities that previously existed in software alone. This also often provides significant performance wins compared to implementing the same security capability in software, thereby increasing the system's overall security without taking a measurable hit to system performance.

With Windows 11, Microsoft has raised the hardware security bar to design the most secure version of Windows ever. We have carefully chosen the hardware requirements and default security features based on threat intelligence and input from leading experts around the globe including the DoD, NSA and UK's NCSC, 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 to create tight integration that protects from the chip to the cloud.

Though 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 hardware turns on, loads firmware, and then launches the operating system. Hardware root-of-trust meets two important security goals for the system. It securely measures the firmware and operating system code that boots the system so that malware cannot infect boot code and hide its presence. Hardware root-of-trust also provides a highly-secure area isolated from the operating system and applications for storing cryptographic keys, data, and code. This protection safeguards critical resources such as the Windows authentication stack, single sign-on tokens, the Windows Hello biometric stack, and BitLocker volume encryption keys.

Trusted Platform Module (TPM)

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

The 2.0 version of the TPM specification includes important enhancements such as the cryptographic algorithm flexibility that enables stronger crypto algorithms and the ability for customers to use preferred alternative algorithms. Starting with Windows 10, Microsoft's hardware certification required 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.

Pluton security processor

Microsoft Pluton security processor, provides security at the chip. Pluton is a hardware root-of-trust designed by Microsoft in partnership with our silicon partners that is intended to provide the robustness and flexibility needed by modern PCs to address the evolving threat landscape. The Pluton design embeds the hardware root-of trust directly into the same silicon substrate as the CPU. This important design principle eliminates a common weakness when the root-of-trust is located in another discrete chip on the motherboard that is separate from the CPU. The weakness is that while the root-of-trust chip itself may be very secure there is a weak link in the communication path between the discrete root-of-trust and the CPU that can be exploited by physical attacks.

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 being a TPM 2.0,

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.

As with other TPMs, credentials, encryption keys, and other sensitive information cannot be 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 emerging attack techniques such as speculative execution cannot access key material. Pluton also includes the unique Secure Hardware Cryptography Key (SHACK) technology. SHACK helps ensure that keys are never exposed outside the protected hardware, even to the Pluton firmware itself, providing an unprecedented level of security for Windows customers.

Pluton also solves the major security challenge of keeping system firmware up to date across the entire PC ecosystem. Today customers receive updates to their security firmware from a variety of different sources than can be difficult to manage, resulting in widespread update issues. Pluton provides a flexible, updateable platform for running firmware that implements end-to-end security functionality authored, maintained, and updated by Microsoft. Pluton is integrated with the Windows Update service benefitting from over a decade of operational experience reliably delivering updates across over a billion endpoint systems.

The Microsoft Pluton security processor will ship with select new Windows PCs starting in 2022.

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 CPUs 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 the CPU's hardware virtualization instructions to create a secure region of memory isolated from the normal operating system. Windows uses this isolated VBS environment to protect security sensitive operating system functions such as the secure kernel and security assets such as authenticated user credentials. Even if malware gains access to the main OS kernel, VBS greatly limits and contains exploits because the hypervisor and virtualization hardware help prevent the malware from executing code or accessing platform secrets running within the VBS secure environment.

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.

Windows 11 Secured-core PCs

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 strengthen protection against advanced threats such as kernel attacks from ransomware. 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, stopping infections in their tracks. Virtualization-based security comes enabled by default. And with built in hypervisor protected code integrity that protects system memory, Secured-core PCs ensure that all operating system code is trustworthy, and executables are signed by known and approved authorities only.

Benefits of a Secured-core Windows 11 PC include:

- Powerful security capabilities integrated across software, hardware, firmware, and identity protection

- Deep integration between Microsoft, device manufacturers, and chip manufacturers to deliver powerful security capabilities that help prevent infections across software, firmware, and hardware

- Security features across the stack are enabled by default by device manufacturers helping ensure customers are secure from the start

Memory protection in Secured-core PCs

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 an experience identical to USB. Because PCI hot plug ports are external and easily-accessible, PCs are susceptible to drive-by Direct Memory Access (DMA) attacks. Memory access protection (also known as Kernel DMA Protection) protects PCs against drive-by DMA attacks that use PCIe hot plug devices by limiting these external peripherals from being able to directly copy memory when the user has locked their PC.

Drive-by DMA attacks typically happen quickly while the system owner isn't present. The attacks are performed with 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 in a USB-like device and walks away with all the secrets on the machine or injects malware that gives the attacker full remote control over the PC, including the ability to bypass the lock screen.

Note, Memory access protection does not protect against DMA attacks via older ports like 1394/FireWire, PCMCIA, CardBus, or ExpressCard.

Learn how to check if your PC supports Kernel DMA protection and about Kernel DMA protection requirements.
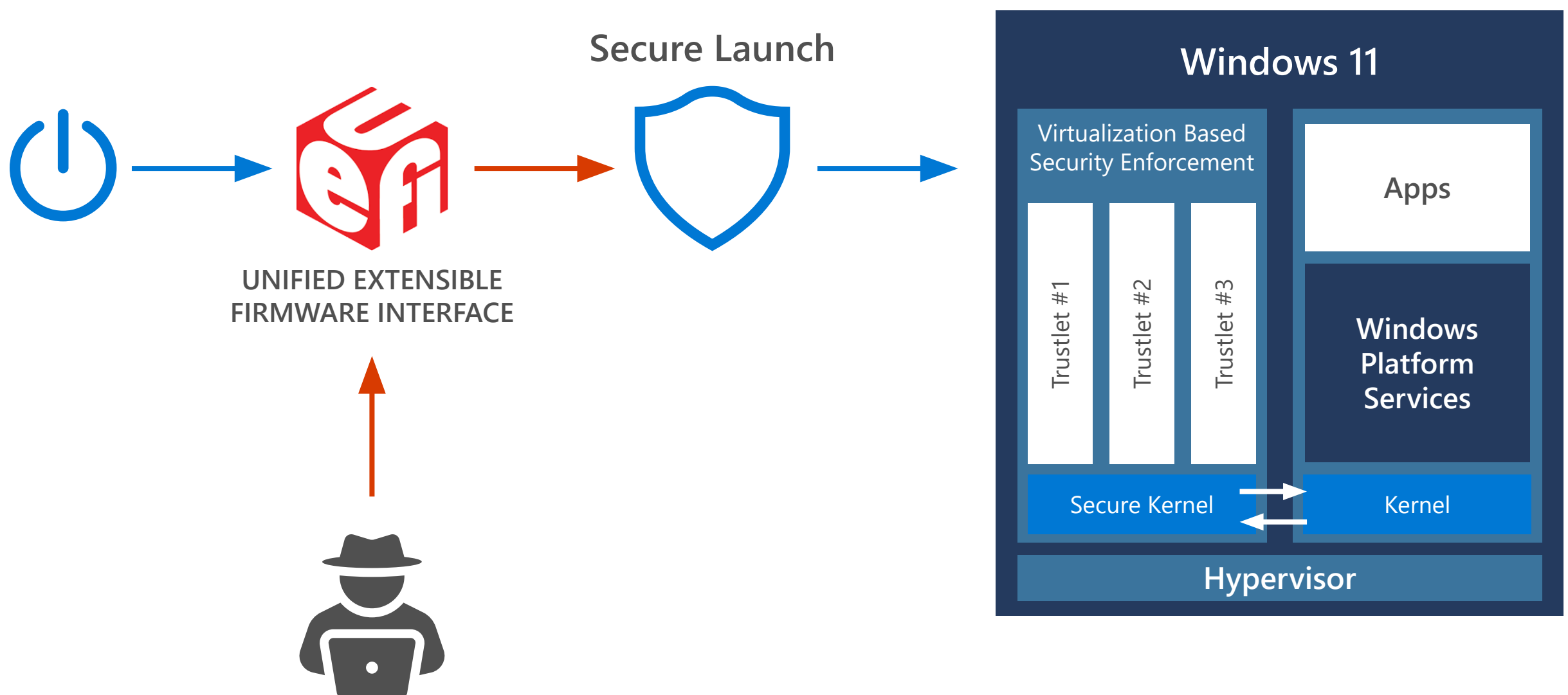
Firmware protection in Secured-core PCs

Secured-core PCs defend at the firmware level with multiple layers of protection enabled, helping ensure that devices launch safely in a hardware-controlled state.

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. 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).

With thousands of PC vendors producing numerous PC models with diverse UEFI firmware components, there becomes an incredibly large number of SRTM signatures and measurements at bootup that are inherently trusted by secure boot, making it more

challenging to constrain trust on any particular device to only what is needed to boot that device. Two techniques exist to constrain trust: either maintain a list of known "bad" SRTM measurements, also called a block list, which suffers from the drawback of being inherently brittle; or maintain a list of known "good" SRTM measurements, or an allow list, which is difficult to keep up-to-date at scale.
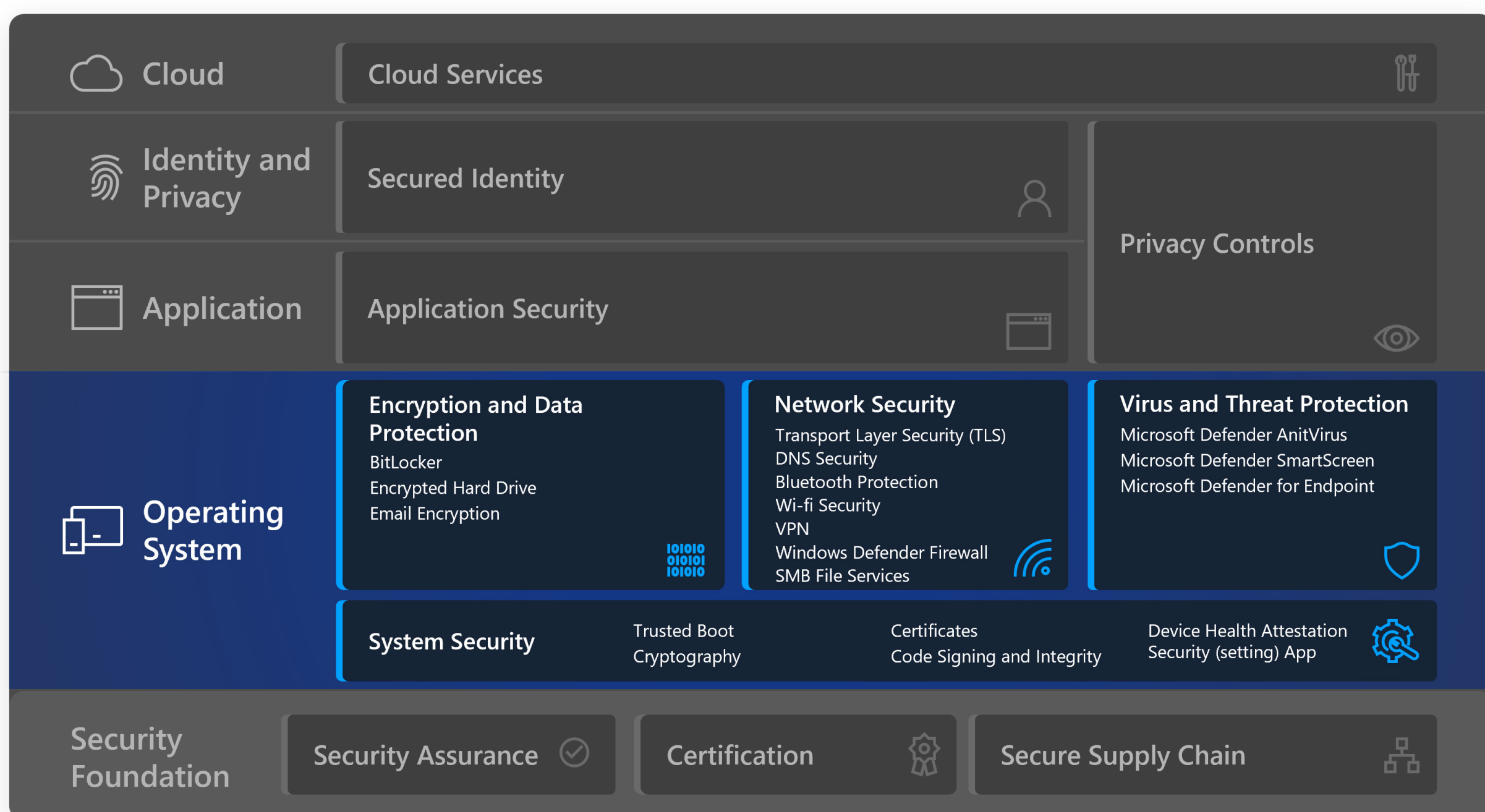
In Secured-core PCs, Windows Defender System Guard Secure Launch addresses these issues with a technology known as the Dynamic Root of Trust for Measurement (DRTM). DRTM lets the system follow the normal UEFI Secure Boot process initially, but before Windows is launched the system enters a hardware controlled trusted state that forces the CPU(s) down hardware secured code path. If a malware rootkit/bootkit bypassed UEFI Secure Boot and had been resident in memory, DRTM will prevent it from accessing secrets and critical code protected by the virtualization-based security environment. System Management Mode (SMM) isolation complements the protections provided by DRTM by helping to reduce the attack surface from SMM, which is an execution mode in x86-based processors that runs at a higher effective privilege than the hypervisor. Relying on capabilities provided by silicon providers like Intel and AMD, SMM isolation enforces policies that enforce restrictions such as preventing SMM code from accessing OS memory. The SMM isolation policy in effect on a system can also be reliably provided to a remote attestation service.

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

Operating System Security

Cloud	Cloud Services		
Identity and Privacy	Secured Identity		Privacy Controls
Application	Application Security		
Operating System	**Encryption and Data Protection** BitLocker Encrypted Hard Drive Email Encryption	**Network Security** Transport Layer Security (TLS) DNS Security Bluetooth Protection Wi-fi Security VPN Windows Defender Firewall SMB File Services	**Virus and Threat Protection** Microsoft Defender AnitVirus Microsoft Defender SmartScreen Microsoft Defender for Endpoint
	System Security Trusted Boot / Cryptography	Certificates / Code Signing and Integrity	Device Health Attestation / Security (setting) App
Security Foundation	Security Assurance	Certification	Secure Supply Chain

Hardware-based protection is only one link in the chain of chip to cloud security. Security and privacy also depend on an OS that guards your information and PC from the moment it starts.

Windows 11 is the most secure Windows yet with extensive security measures in the OS designed to help keep you 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. Windows 11 enhances built-in hardware protection with OS security out-of-the box to help keep your system, identity, and information safe.

System security

Trusted Boot (UEFI Secure Boot + Measured Boot)
The first step in protecting the operating system is to ensure that it boots securely after the initial hardware and firmware boot sequences have safely finished their early boot sequences. 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.

As the PC begins the boot process, it will first verify that the firmware is digitally signed, reducing the risk of firmware rootkits. Secure Boot then checks all code that runs before the operating system and checks the OS bootloader's digital signature to ensure that it is trusted by the Secure Boot policy and hasn't been tampered with.

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

16

Trusted Boot takes over where Secure Boot leaves off. 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 has been tampered with, the bootloader detects the problem and refuses to load the corrupted component. Tampering or malware attacks on the Windows boot sequence are blocked by the signature-enforcement handshakes between the UEFI, bootloader, kernel, and application environments.

Often, Windows can automatically repair the corrupted component, restoring the integrity of Windows and allowing the PC to start normally.

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](#).

Windows 11 requires all PCs to use Unified Extensible Firmware Interface (UEFI)'s Secure Boot feature.

Cryptography

Cryptography is a mathematical process to protect user and system data, by for example, encrypting data so that only a specific recipient can read it by using a key possessed only by that recipient. Cryptography is a basis for privacy to prevent anyone except the intended recipient from reading data, provides integrity checks to ensure data is free of tampering, and authentication that verifies identity to ensure that communication is secure. The cryptography stack in Windows extends from the chip to the cloud enabling Windows, applications, and services to protect system and user secrets.

Cryptography on Windows 11 is subject to Federal Information Processing Standards (FIPS) 140 certification. FIPS 140 certification ensures that US government approved algorithms are correctly implemented (which includes RSA for signing, ECDH with NIST curves for key agreement, AES for symmetric encryption, and SHA2 for hashing), tests module integrity to prove that no tampering has occurred and proves the randomness for entropy sources.

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)

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

These are natively exposed on Windows through the Crypto API (CAPI) and the Cryptography Next Generation API (CNG) which is powered by Microsoft's open-source cryptographic library SymCrypt. Application developers can leverage these APIs to perform low-level cryptographic operations (BCrypt), key storage operations (NCrypt), protect static data (DPAPI), and securely share secrets (DPAPI-NG).

Certificates

Windows offers several APIs to operate and manage certificates. Certificates are crucial to public key infrastructure (PKI) as they provide the means for safeguarding and authenticating information. Certificates are electronic documents, which conform to the X.509v3 formatting standard, used to claim ownership of a public key. Public keys are used to prove server and client identity, validate code integrity, and used in secure emails. Windows 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. Windows validates certificates through an automatic update mechanism that downloads certificate trust lists (CTL) weekly. Trusted root certificates are used by applications as a reference for trustworthy PKI hierarchies and digital certificates. The list of trusted and untrusted certificates is stored in the CTL and can be updated by the Microsoft Third Party Root Program. Roots in the Microsoft Third Party Root Program are governed through annual audits to ensure compliance with industry standards. For certificate revocation, a certificate is added as an untrusted certificate to the disallowed CTL that is downloaded daily causing the untrusted certificate to be revoked globally across user devices immediately.

Windows also offers enterprise certificate pinning 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 or Internet Explorer.

Code signing and integrity

Code signing, while not a security feature by itself, is integral 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. This ensures that the file hasn't been tampered with, 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.

All software written and published by Microsoft is code-signed to establish that Windows and Microsoft code has integrity, authenticity, and positive reputation. Code signing is how Windows can differentiate its own code from code from external creators, and prevents tampering when code is delivered to user devices.

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 produced by Microsoft, external 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 tests externally produced drivers for hardware and Windows compatibility, and ensures that they are malware free. Lastly, user mode code, applications, Appx/MSIX packaged apps, Windows OS component updates, driver install packages, and their signatures, are evaluated by WinVerifyTrust which relies on the Crypto API. These signatures are verified by confirming they are in the Microsoft Third Party Root Program CTL, and thus trusted and not revoked by the certificate authority.

Device health attestation

Device health attestation and conditional access are used to grant access to corporate resources. This helps reinforce a Zero Trust paradigm that moves enterprise defenses from static, network- based perimeters to focus on users, assets, and resources.

Conditional access evaluates identity signals to confirm that users are who they say they are before they are granted access to corporate resources. Windows 11 supports remote attestation to help confirm that devices are in a good state and have not been tampered with. This helps users access corporate resources whether they're in the office, at home, or when they're traveling.

Information about the firmware, boot process, and software, which is cryptographically stored in the security co-processor (TPM), is used to validate the security state of the device. Attestation provides assurance of trust as it can verify the identity and status of essential components and that the device, firmware, and boot process has not been altered. This capability helps organizations to manage access with confidence. Once the device is attested it can be granted access to resources.

Device health attestation determines:

- If the device can be trusted. This is determined with the help of a secure root-of-trust, or TPM. Devices can attest that the TPM is enabled and in the attestation flow.

- If the OS booted correctly. Many security risks can emerge during the boot process as this can be the most privileged component of the whole system.

- If the OS has the right set of security features enabled.

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 was 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 backed with the appropriate hardware configurations that helps keep you safe. [Measured and Trusted boot](#), implemented by bootloaders and BIOS, verifies and cryptographically records each step of the boot in a

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

19

chained manner. These events are bound to the TPM that functions as a hardware root-of-trust. Remote attestation 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. As an example, Microsoft Intune integrates with Microsoft Azure Attestation to review Windows device health comprehensively and connect this information with AAD conditional access. This integration is key for Zero Trust solutions that help bind trust to an untrusted device.

A summary of the steps involved in attestation and Zero Trust on the 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 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.

- 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 safe.

Microsoft Intune integrates with Microsoft Azure Attestation to review Windows device health comprehensively and connect this information with AAD conditional access – [see Microsoft Azure Attestation Service section below](#). This integration is key for Zero Trust solutions that help bind trust to an untrusted device.

Windows security policy settings and auditing

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

- User authentication to a network or device.

- Resources that users are permitted to access.

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

- Membership in a group.

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

20

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 that you consider high value. Auditing can help identify attacks, network vulnerabilities, and attacks against targets that you consider high value. You can specify categories of security-related events to create an audit policy tailored to the needs of your organization.

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

- Identify your most critical resources and activities.

- Identify the audit settings you need to track them.

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

- Test these settings to validate your choices.

- Develop plans for deploying and managing your audit policy.

Learn more about security policy settings and security auditing.

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

21

Windows security app

Visibility and awareness of device security and health is 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 take action 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.
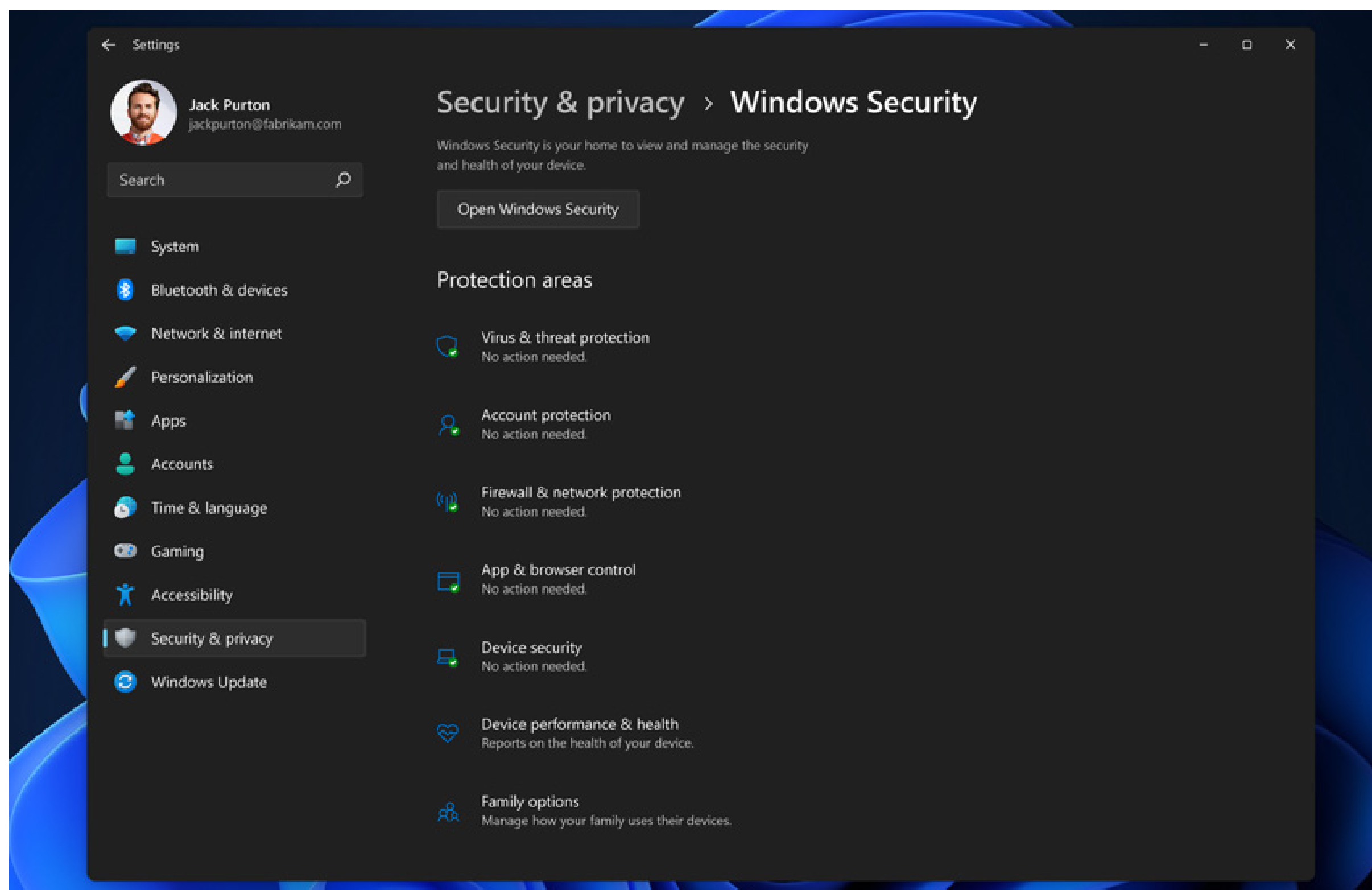
Learn more about the Windows security app.

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

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 Azure6 can be used to save recovery key content. BitLocker

can be managed by any MDM solution such as Microsoft Intune6 using a [configuration service provider (CSP)](#).

BitLocker provides encryption for the OS, fixed data, and removable data drives 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

Encrypted Hard Drive uses the rapid encryption provided by BitLocker Drive Encryption to enhance data security and management.

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 provide:

- Better performance: Encryption hardware, integrated into the drive controller, allows the drive to operate at full data rate with no performance degradation.

- Strong security based in hardware: Encryption is always "on" and the keys for encryption never leave the hard drive. User authentication is performed by the drive before it will unlock, independently of the operating system.

- 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 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.

Encrypted hard drives are a new class of hard drives that are self-encrypted at a hardware level and allow for full disk hardware encryption.

Email encryption

Email encryption (also referred to as [Windows S/MIME](#)), enables users to encrypt outgoing email messages and attachments, so only intended recipients with digital identification (ID)—also called a certificate—can read them. 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 to by a user to people within their organization as well as external contacts if they have their encryption certificates. However, recipients using Windows 10 Mail app can only read encrypted messages if the message is received on their

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

23

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.

Learn more about [configuring S/MIME for Windows](#).

Network security

Windows 11 raises the bar for networking security by bringing a wide array of improvements, helping people work, learn, and play from almost anywhere with confidence. 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 SMB over QUIC as well as new encryption and signing capabilities. Wi-Fi and Bluetooth advancements provide greater trust in connections to other devices. The VPN and Windows Defender Firewall platforms bring new ways to configure easily and debug quickly, ensuring IT administrators and third-party software are more effective.

Transport layer security (TLS)

Transport Layer Security (TLS) is the internet's most deployed security protocol, encrypting data 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 applications 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 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

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 extent existing security models to adopt

new security models such as Zero Trust. DNS over HTTP protocol can be mandated, 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

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 helps 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

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 the 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

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)

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.

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

26

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. The VPN platform also supports classic domain-joined authentication. It's supported by Microsoft Intune 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 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
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 will automatically negotiate this more advanced cipher method when connecting to another computer that requires it and it can also be mandated on clients.

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.

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
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 this 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 on-device prevention is integrated with cloud-delivered protection, which helps ensures near-instant detection and blocking of new and emerging threats.

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

Attack surface reduction
Available in both Windows and Windows Server, 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:

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

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

28

- 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 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.

Lean more about [attack surface reduction](#).

Tamper Protection

Attacks like ransomware attempt to disable security features, such as anti-virus protection, on targeted devices. 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 virus and threat protection

- 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](#).

Network Protection

Network protection in Windows helps prevent users from accessing dangerous IP addresses and domains that may host phishing scams, exploits, and other malicious content on the Internet. Network protection is part of attack surface reduction and helps provide an additional layer of protection for a user. Using reputation-based services, network protection blocks access to potentially harmful, low-reputation based domains and IP addresses. In enterprise environments, network protection works best with Microsoft Defender for Endpoint, which provides detailed reporting into protection events as part of larger investigation scenarios. Learn more about how to [protect your network](#).

Controlled Folder Access

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

Exploit protection automatically applies several exploit mitigation techniques to operating system processes and apps. Exploit protection works best with Microsoft Defender 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 to distribute the XML file to multiple devices simultaneously.

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

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 that 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, Microsoft Defender SmartScreen shows a warning to let the user know that the site might be malicious.

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

30

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 the user that the site might be malicious.

- Checking downloaded files against a list of files that are well known and downloaded by many Windows users. If the file is not on that list, it shows a warning advising caution.

The app and browser control section contains information and settings for Windows Defender SmartScreen. IT administrators and IT pros can get configuration guidance in the Windows Defender SmartScreen documentation library.

Microsoft Defender for Endpoint

Windows E5 customers benefit from Microsoft Defender for Endpoint, an enterprise endpoint detection and response capability that helps enterprise security teams detect, investigate, and respond to advanced threats. Organizations with a dedicated security operations team can use the rich event data and attack insights that 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's threat intelligence is informed by trillions of security signals every day. Combined with our global team of security experts, and cutting-edge artificial intelligence and machine learning, we can see threats that others miss. Our threat intelligence helps provide unparalleled protection for our customers.
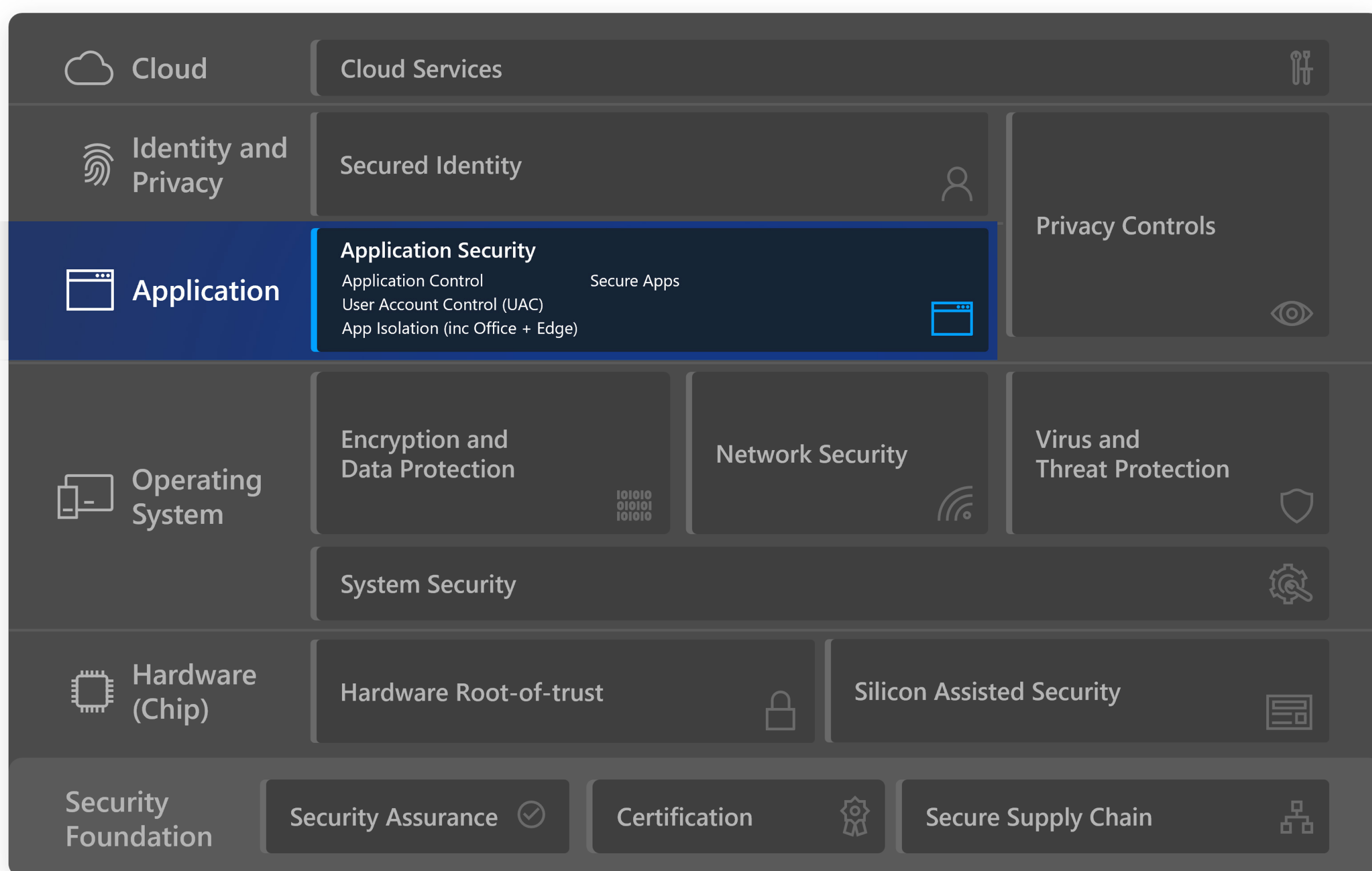
Defender for Endpoint is also part of Microsoft 365 Defender, a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

Learn more about Microsoft Defender for Endpoint and Microsoft 365 Defender.

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

31

Application Security

Cloud	Cloud Services		
Identity and Privacy	Secured Identity		Privacy Controls
Application	**Application Security** Application Control · Secure Apps User Account Control (UAC) App Isolation (inc Office + Edge)		
Operating System	Encryption and Data Protection	Network Security	Virus and Threat Protection
	System Security		
Hardware (Chip)	Hardware Root-of-trust	Silicon Assisted Security	
Security Foundation	Security Assurance	Certification	Secure Supply Chain

Cybercriminals regularly gain access to valuable data by hacking poorly secured applications. Common security failures include "code injection" attacks, in which attackers insert malicious code that can tamper with data, or even destroy it. An application may have its security misconfigured, leaving open doors for hackers. Or vital customer and corporate information may leave sensitive data exposed. Windows 11 protects your valuable data with layers of application security.

A rich application platform, isolation, and code integrity enables developers to build-in security from the ground up to protect against breaches and malware. Running PCs as "least privilege"(aka users not running as admin) is designed to prevent malicious applications getting access they should not. In addition, application controls enable customers to specify what applications run on their devices and only those applications for a comprehensive application security story.

Windows Defender Application Control (WDAC)

Not allowing malicious or potentially unwanted applications on your device is one of the first steps to an effective application security strategy. Windows Defender Application Control (WDAC) enables customers to define their own policy for controlling what is allowed to run

on their devices. Application control is one of the most effective security controls to prevent unwanted or malicious code from running. It moves away from an application trust model where all code is assumed trustworthy to one where apps must earn trust to run. Many organizations cite application control as one of the most effective means for addressing the threat of executable file-based malware (.exe, .dll, etc.).

Windows also includes AppLocker as another solution for application control. While WDAC offers the most robust protection and is regarded by Microsoft as a security feature, AppLocker may be a more appropriate technology for some organizations and can add some defense-in-depth protection. **Use AppLocker when:**

- You have a mixed Windows operating system (OS) environment and need to apply the same policy controls to Windows versions earlier than Windows 10.

- You need to apply different policies for different users or groups on shared computers.

- You do not want to enforce application control on application files such as DLLs or drivers. AppLocker can also be deployed as a complement to WDAC to add user or group-specific rules for shared device scenarios, where it is important to prevent some users from running specific apps. As a best practice you should enforce WDAC at the most restrictive level possible for your organization then use AppLocker to further fine-tune the restrictions.

User Account Control (UAC)

Where possible, PCs should be set up so that the main accounts people use for every day computing are not "admin" accounts. As this helps mitigate the impact of malware should it inadvertently get onto your device. Consumers can change the UAC in settings and enterprises can change the defaults with their MDM such as Intune.

User Account Control (UAC) helps set users up to be productive and with the "least privilege" needed to get their job done. It helps prevent malware from gaining administrative privileges to make unwanted changes to the PC, and from damaging a PC enabling 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.

UAC allows all users to log on to their computers using a standard user account. Processes launched using a standard user token may perform tasks using access rights granted to a standard user. For instance, Windows Explorer automatically inherits standard user level permissions. Additionally, any apps that are started using Windows Explorer (for example, by double-clicking a shortcut) also run with the standard set of user permissions. Many apps,

including those that are included with the operating system itself, are designed to work properly in this way.

Other apps, especially those that were not specifically designed with security settings in mind, often require additional permissions to run successfully. These types of apps are referred to as legacy apps. Additionally, actions such as installing new software and making configuration changes to the Windows Firewall, require more permissions than what is available to a standard user account.

When an app needs to run with more than standard user rights, UAC can restore additional user groups to the token. This enables the user to have explicit control of apps that are making system level changes to their computer or device.
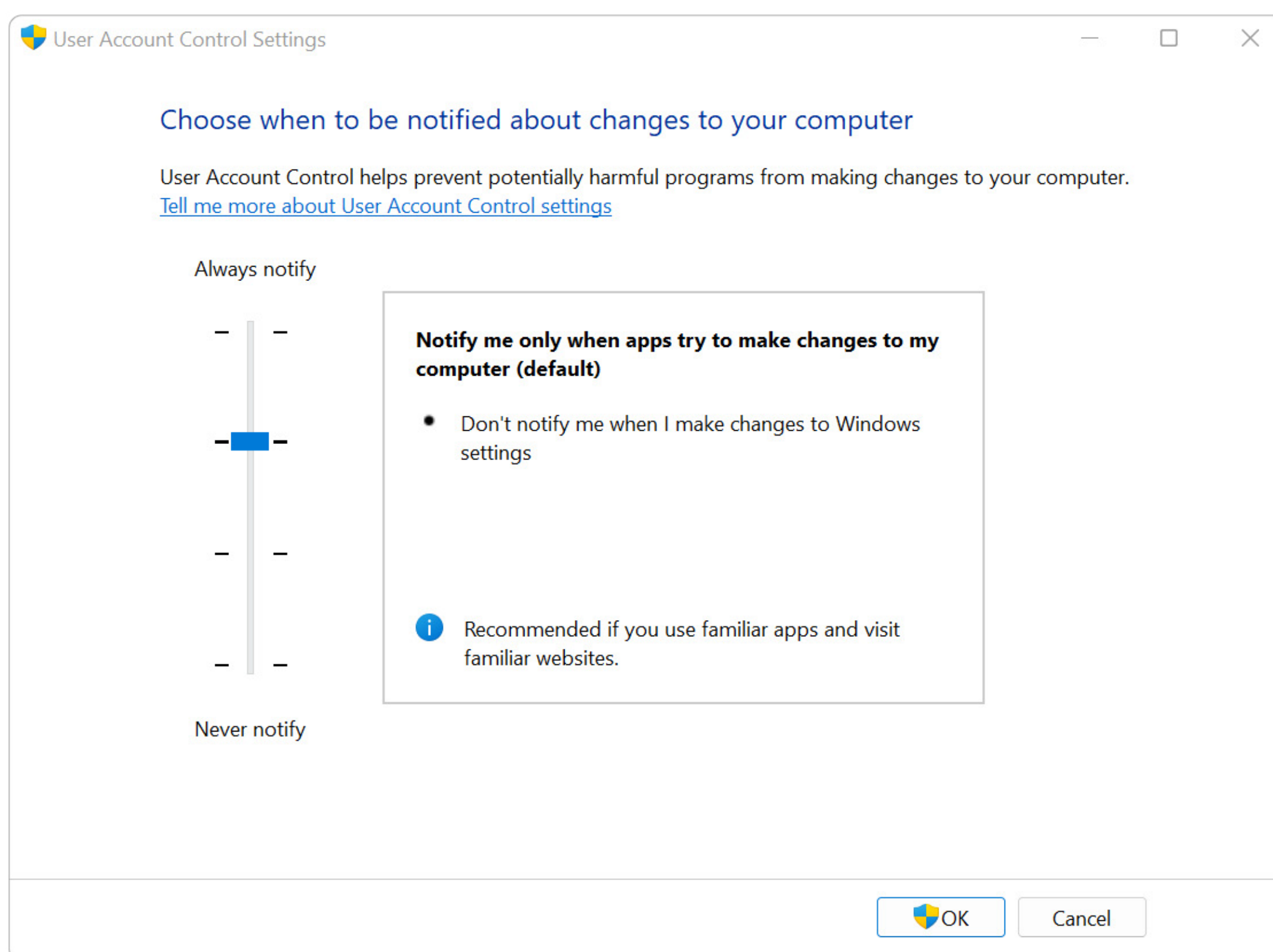
Learn more here about [How User Account Control works](#)

Application isolation

Attackers leverage social engineering tactics to gain users' trust, deceive them and influence their actions – from opening a malicious link attached to an email to visiting a compromised website. The malicious code executes when the application opens the weaponized content, exploiting vulnerabilities and downloading malware on the endpoint. This sophisticated social

engineering attack is a lethal weapon that leverages "the art of deception" allowing attackers to stay undercover while exploiting systems' vulnerabilities.

In such a challenging environment, where application and web browser scans and filters on their own may not be able to stop attackers from tricking users and preventing malicious code to execute, isolation technology is the way forward to defend against 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 users' environments.

Isolation is integral to Windows chip to cloud security posture, enabling applications to apply and run in state-of-the-art virtualization technology such as Windows Defender Application Guard to significantly reduce the blast radius of compatible compromised applications.

Microsoft Defender Application Guard leverages chip-based hardware isolation to run untrusted websites and Office files, seamlessly in an isolated VBS 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 blast radius of the infection is contained and the desktop stays intact. VBS technology also powers other Windows security features like Credential Guard and HVCI.

**Currently Application Guard protects:**

- Word files

- PowerPoint files

- Excel files

- Websites opened inside Edge browser

- Plugin available for other browsers like Google Chrome and Mozilla Firefox

There is a shield added to the icons to the applications that your IT Administrator has enabled Microsoft Defender Application Guard to indicate that there is additional protection when files are opened or websites are browsed.

Learn more about Microsoft Defender Application Guard. Microsoft Defender Application Guard on Windows E3 (Edge) and E5 (Office) is configured using an MDM such as Microsoft Intune. And see blog post Defend against zero-day exploits with isolation technology.

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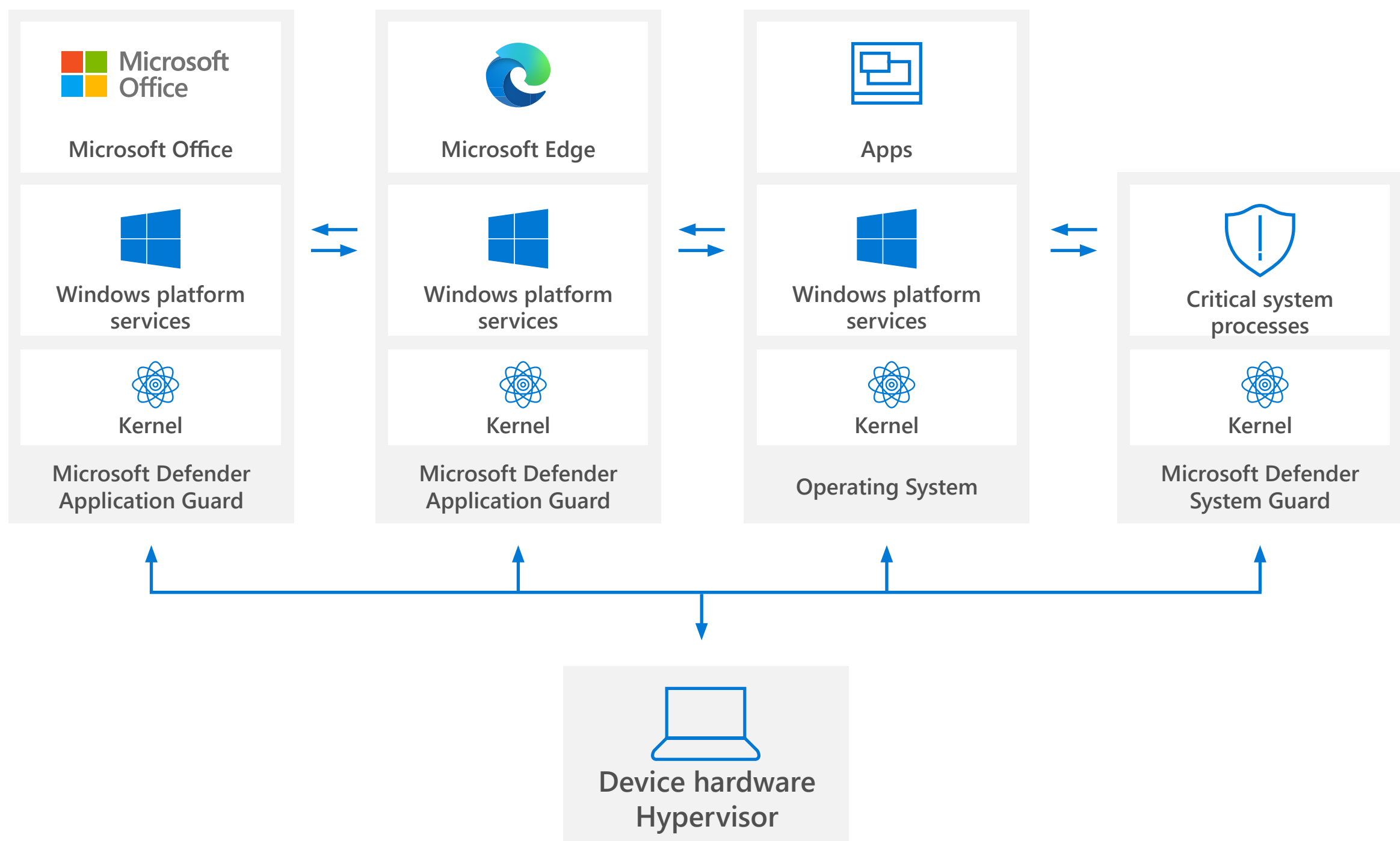
In addition to Application Guard for Office and Edge, Universal Windows Platform (UWP) applications run in Windows containers known as app containers. App containers act as process and resource isolation boundaries, but unlike docker containers, these are special containers designed to run Windows applications.

Processes that run in AppContainer operate with low integrity level, with limited access to resources they do not own. Because the default integrity level of most objects is medium integrity level, the UWP app can access only a limited part of the filesystem, registry, and other resources. The AppContainer 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.

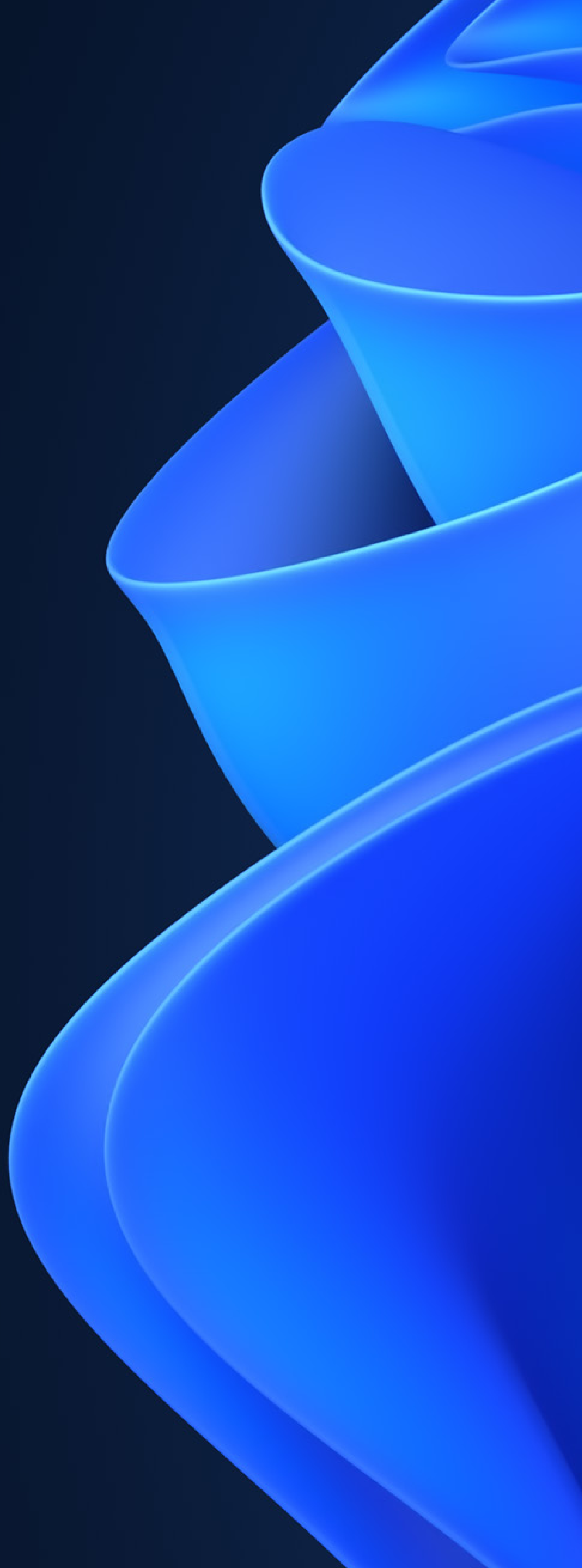Learn more about Windows and app containers.
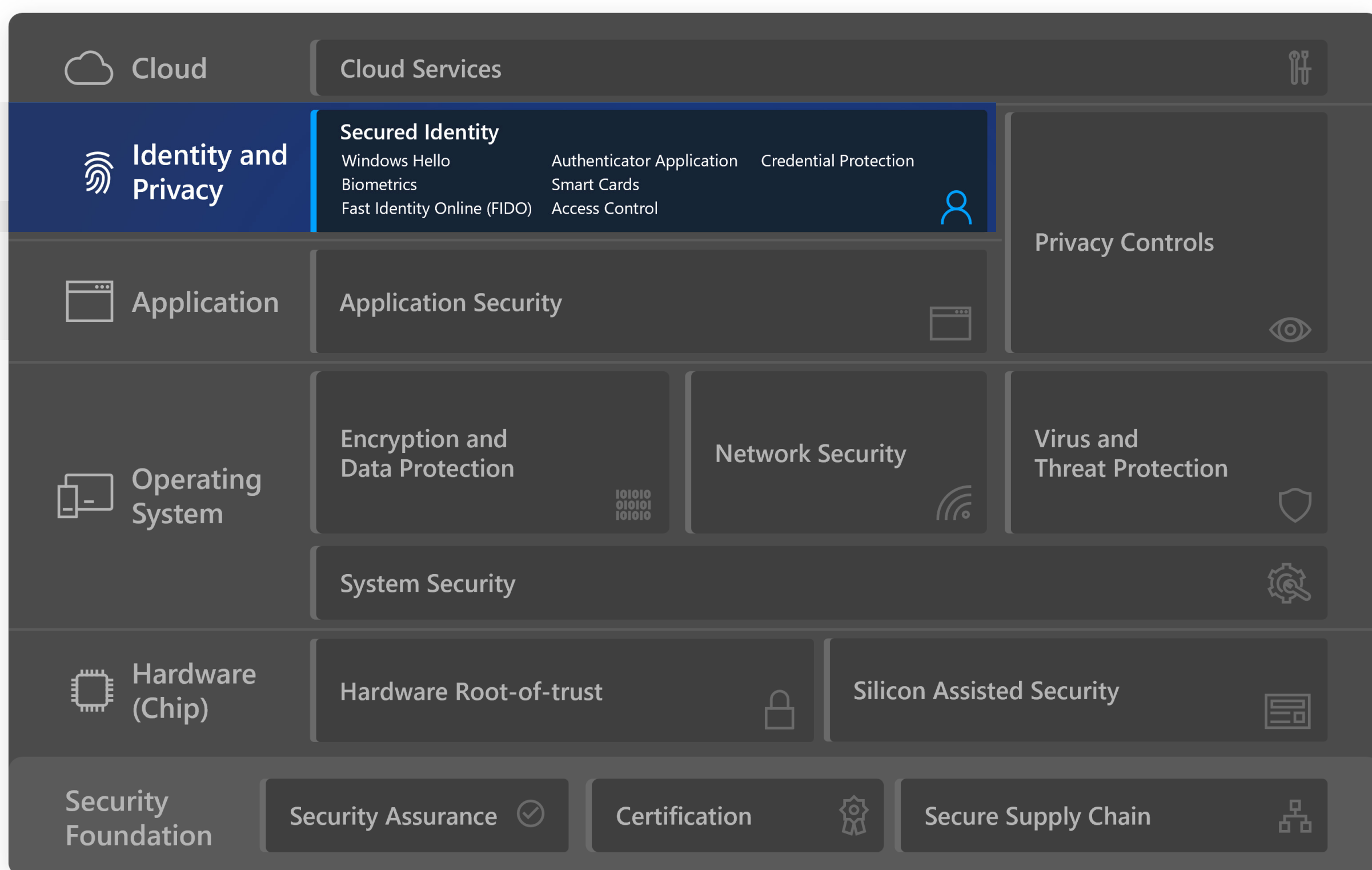
Developing secure applications

Windows App SDK brings a unified set of APIs and tools for developing desktop apps to 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 may find security best practices and information on building Windows desktop and using the SDK at Build desktop apps for Windows | Microsoft Docs. 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.

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

38

Identity
and Privacy

Hybrid work is here to stay, and the security of your business and personal life depends on the right user access the right device and the right data. Weak passwords, password spraying, and phishing are the entry point for many attacks. Malicious actors launch an average of 50 million password attacks every day—579 per second. And phishing attacks have increased, making identity a continuous the battleground for attacks. As Bret Arsenault, Chief Information Security Officer at Microsoft says, "Hackers don't break in, they log in."

The passwordless future is here. Windows 11 devices protect user identities by removing the need to use passwords from day one. With Windows Hello for consumers and Windows Hello for Business, customers can adopt passwordless multifactor authentication (MFA), significantly reducing the risk of compromise. As remote and hybrid work becomes the new normal, Windows 11 provides multiple credential protection options to meet business and consumer needs while complying with ever-evolving regulations.

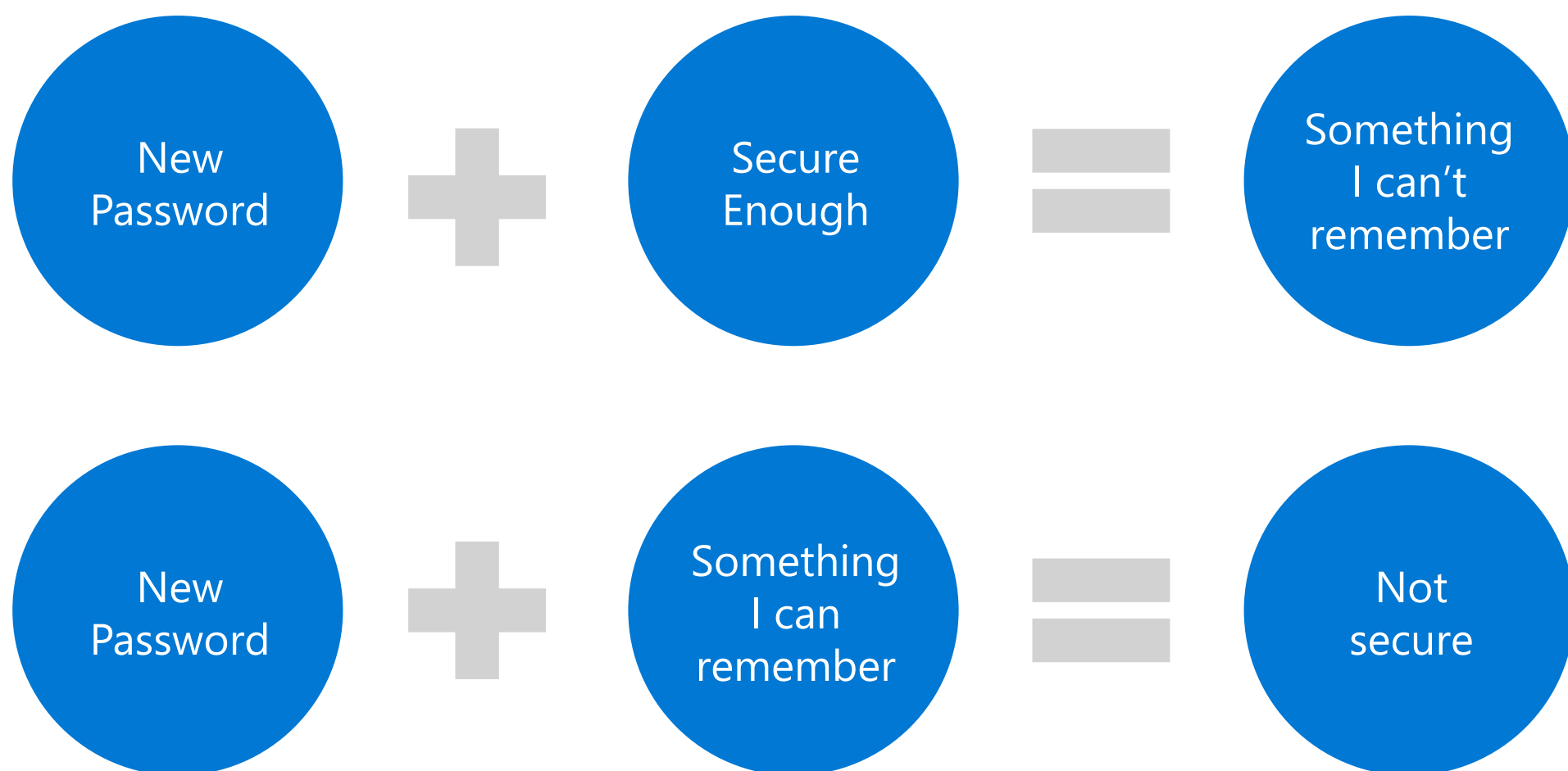# Go Passwordless with Window Hello (PIN and Biometrics)

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

their apps and cloud services.

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

Windows 11 protects credentials with chip-level hardware security including TPM 2.0 combined with VBS and Microsoft Credential Guard

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

[Windows Hello](#) and [Windows Hello for Business](#) replace password-based authentication with a stronger authentication model so that you can sign into your device using a passcode (PIN) or biometric based authentication.[5]

- **Windows Hello** can be used for your personal Microsoft Account (MSA) for accessing your OneDrive and Microsoft email.

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

Windows Hello authentication is only valid on the device that you registered it for and cannot be used on another device, thwarting password phishing attacks.

Using asymmetric keys provisioned in a Trusted Platform Module (TPM), Windows Hello protects user authentication by binding a user's credentials to their device. Windows Hello authentication validates the user based on either PIN or biometrics match and only then releases cryptographic keys bound for that user in the TPM. Because this data never leaves the PC and are never collected by our servers, they cannot be used by anyone that does not have physical access to that device and are protected against typical replay, phishing, spoofing and other network attacks and even password leaks and reuse.

Windows Hello for Business allows IT administrators to set policies to further increase security by disallowing PINs for business users and by enabling 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.

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 [Windows Hello biometric requirements](#).

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 the user authentication processes and data, and secure the pathway by which that data is communicated. These specialized components work to protect against a class of attacks that include biometric sample injection, replay, tampering, and more.

In addition to Windows Hello biometric requirements, 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 it is most typically found supported in Secure-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. Fingerprint authentication is available across all processor types. Please reach out to your OEM for support details.

Fast Identity Online (FIDO)

The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-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 standard and certification is becoming recognized as leading standard for creating secure authentication solutions, across enterprises, governments, and consumer markets.

Windows Hello is a FIDO-certified authenticator and supports the use of device sign-in with FIDO2 security keys, and with Microsoft Edge or other modern browsers, supports the use of secure FIDO-backed credentials to keep user accounts protected. FIDO certified authenticators can immediately protect your organization against the most damaging remote credential stealing and phishing attacks because it inherently requires users to physically act.

Windows 11 can be used as a FIDO authenticator for many popular services.

Learn more about the [FIDO Alliance](#). For more information about Microsoft technologies see [Passwordless security key sign-in - Azure Active Directory](#) and [Azure Active Directory passwordless sign-in](#).

Microsoft Authenticator mobile application

The Microsoft Authenticator app is a perfect companion to help keep secure with Windows 11. It allows easy, secure sign-ins 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 (e.g. the Keychain on iOS and Keystore on Android). You can backup your credentials to the cloud by enabling the encrypted backup option in settings. You can also see your sign-in history and security settings for your Microsoft personal, work, or school accounts. 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.

Learn more about [Microsoft Authenticator](#)

Smart cards

Smart cards are tamper-resistant portable storage devices that can enhance the security of tasks in Windows, such as authenticating clients, signing code, securing e-mail, and signing in with Windows domain accounts.

Smart cards provide:

- Tamper-resistant storage for protecting private keys and other forms of personal information

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

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

Smart cards can be used to sign into domain accounts only, not local accounts. When a password is used to sign in interactively to 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.

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

43

Access control

[Access control](#) in Windows is the process of IT Administrators authorizing users, groups, and computers to access objects and assets on a network or computer. After a user is authenticated, the Windows operating system implements the second phase of protecting resources. Using built-in authorization and access control technologies, Windows determines if an authenticated user has the correct permissions.

IT Administrators can refine the application and management of access to provide the following security:

- 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.

- Enable users to access resources from a variety of devices in numerous locations.

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

- Account for a growing number of use scenarios (such as access from remote locations or from a rapidly expanding variety of devices, such as tablet computers and mobile phones).

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

Access controls ensures that shared resources are available to users and groups other than the resource's owner and are protected from unauthorized use.

Access Control Lists (ACL) describe the permissions available for a specific object, and System Access Control Lists (SACL)s apply to system resources. SACLs provides 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 a part of the operating system is critical to understanding a potential attack.

Learn more about [Access Controls](#).

Other credential protection

Protecting credentials such as domain credentials, NTLM, and Kerberos credentials using virtualization-based security is as important as protecting user credentials with the TPM. Windows Defender Credential Guard helps protect your system from credential theft attack techniques such as pass-the-hash or pass-the-ticket. Tools used in many targeted attacks are blocked. For example, malware running in the operating system with administrative privileges cannot extract secrets.

When Windows Defender Credential Guard is activated:

- NTLM, Kerberos, and Credential Manager take advantage of platform hardware security features, including Secure Boot and virtualization, to protect credentials.

- Windows NTLM, Kerberos credentials, and other secrets run in a VBS protected environment isolated from the running operating system
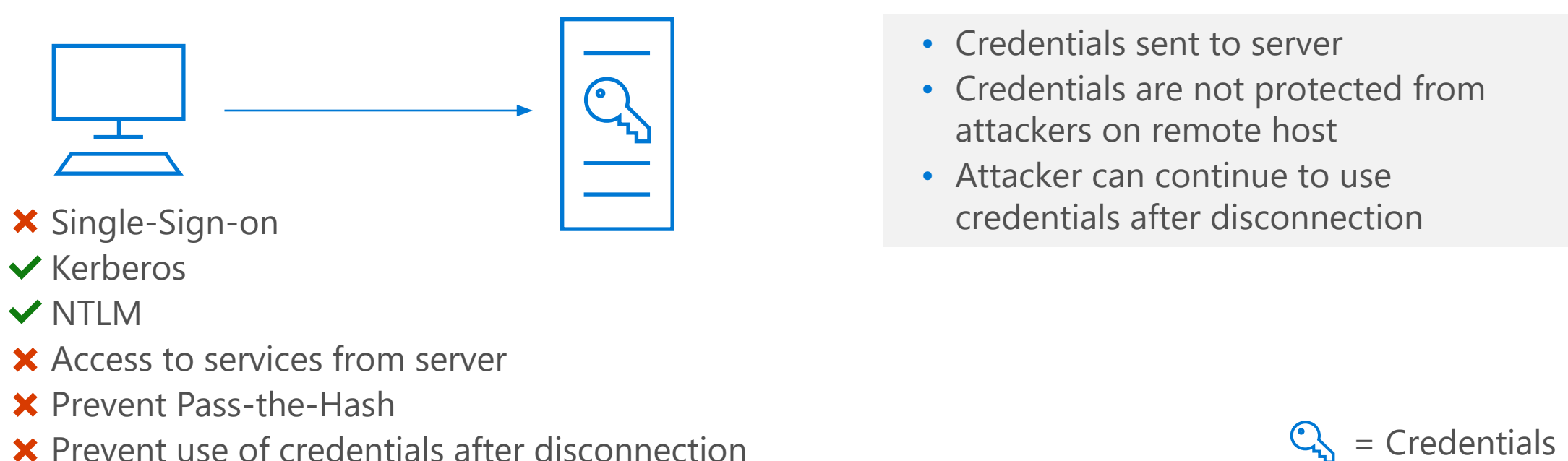
Windows Defender Credential Guard on Windows E3 and E5 is configured using an MDM such as Microsoft Intune.

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
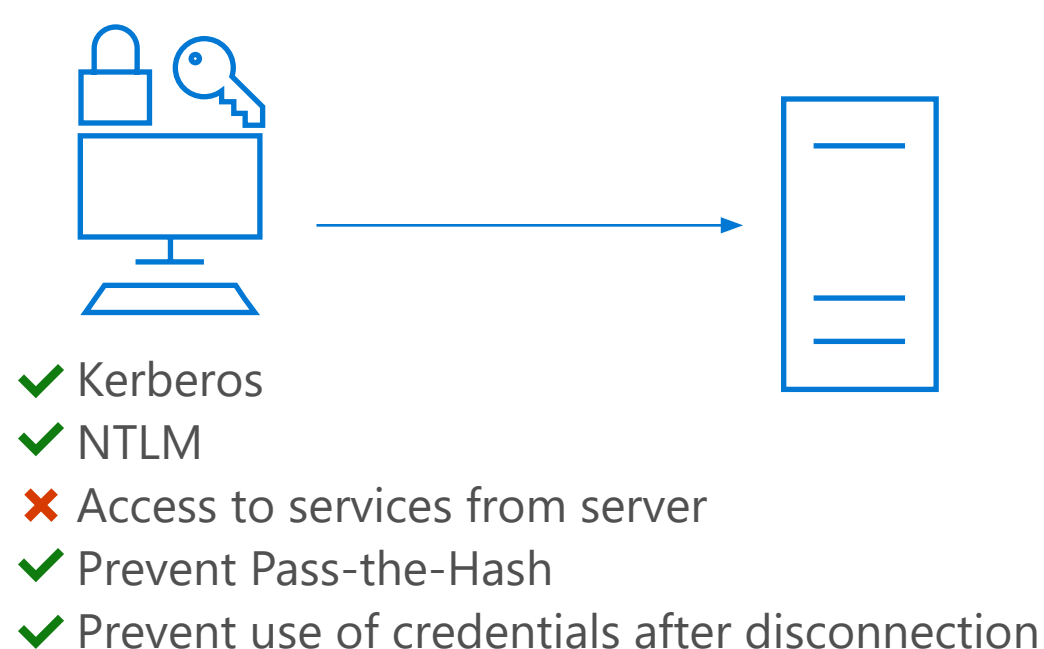
🔑 = Credentials

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

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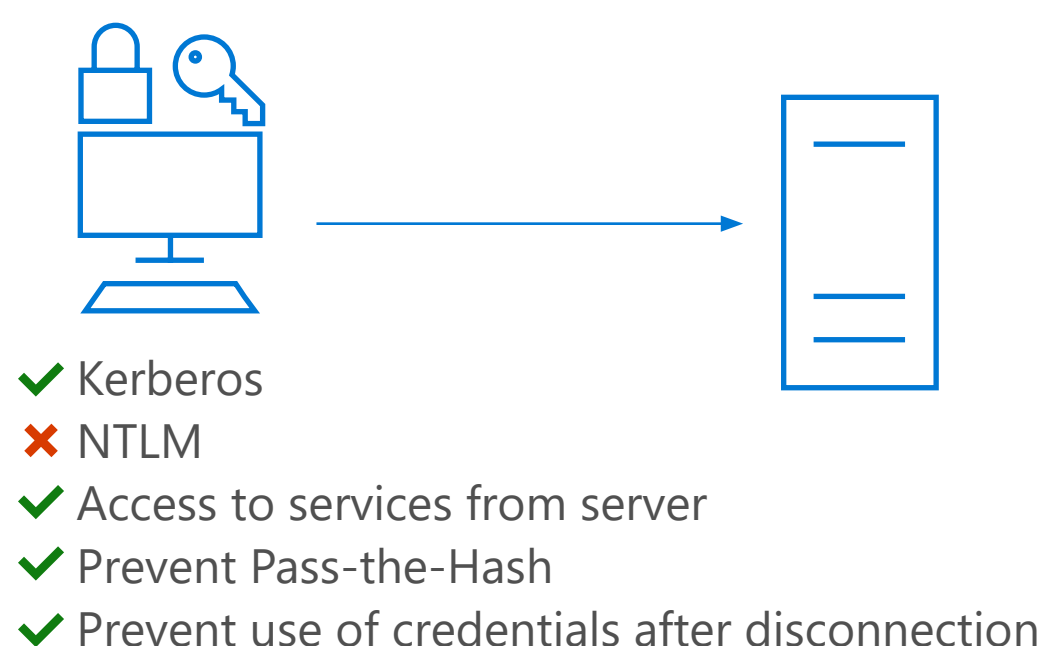
- Credentials protected by Windows Defender Remote Credential Guard
- Connect to other sustems using SSO
- Host must support Windows Defender Remote Credential Guard

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

Restricted Admin Mode

- 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

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

🔒 = Credential protection

🔑 = Credentials

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

Privacy Controls and Transparency
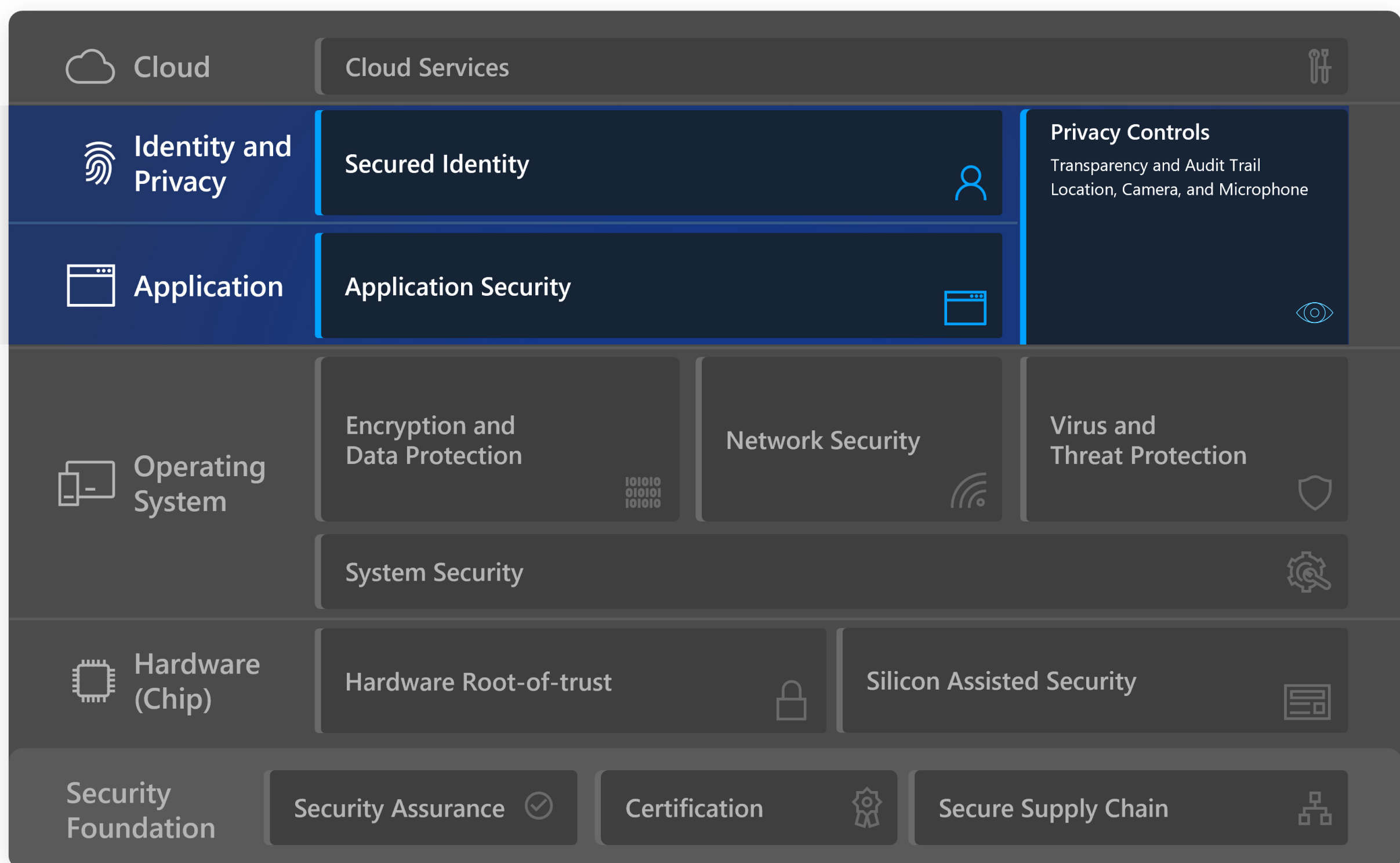
[Privacy: Your data, powering your experiences, controlled by you](#). Privacy is becoming top of mind for customers, who want to know who is using their data and why. They also need to know how to control and manage the data that is being collected—so providing transparency and control over this personal 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's consistent with your expectations. With Windows 11, we provide controls over which apps and features in the OS can collect and use data (such as the device's location) or get access to resources (such as your camera or microphone). Customers can use the Microsoft [Privacy dashboard](#) to view, export, and delete their data, giving them further transparency and control. The [Microsoft Privacy Report](#) provides another resource for customers to learn more about what data Windows collects along with how to manage the data.

Windows 11 is also helping you understand when apps are using or have last used resources such as your camera, microphone, or location. This information helps you make more informed decisions about whether an app is behaving as expected and empowers you to change access given to that app. For resources like microphone or location, we also provide prominent system tray icons to inform users when these are in use. For context, a description

of the app and its activity are presented in a simple tooltip. Apps can also make use of new Windows APIs to support Quick Mute functionality and more.

With Windows 11, enterprise customers have [additional options to manage](#) Windows diagnostic data, allowing them to control this data and use it for services like Update Compliance, a Windows service hosted in Azure.

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

48

Cloud
Services

| Cloud | Cloud Services | OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune) |

Identity and Privacy — Secured Identity — Privacy Controls

Application — Application Security

Operating System — Encryption and Data Protection — Network Security — Virus and Threat Protection — System Security

Hardware (Chip) — Hardware Root-of-trust — Silicon Assisted Security

Security Foundation — Security Assurance — Certification — Secure Supply Chain

Today's workforce has more freedom and mobility than ever before. With the growth of enterprise cloud adoption, increased personal app usage, and proliferation of available apps, the risk of data exposure is at its highest. Enabling Zero Trust protection, Windows 11 works with Microsoft cloud services to help organizations strengthen their multi-cloud security infrastructure, protect hybrid cloud workloads, and safeguard sensitive information while controlling access and mitigating threats.

We are focused on getting customers to the cloud to help keep data and identities safe, and there is continuous monitoring for threat and virus protection through a combination of identity management, device management, and storage options. With the added advantage that if your device is lost or stolen, it is quick to get back up and running with all your data remaining safely in the cloud.

Protecting your work information

Azure Active Directory

Microsoft [Azure Active Directory](#) (Azure AD) is a complete cloud identity and access management solution and a leader in the market for managing identities and directories, enabling access to applications, and protecting identities from security threats. Azure AD empowers organizations to manage and secure identities for employees, partners, and customers to access the applications and services they need. Azure AD provides an identity solution that integrates broadly, from on-premises legacy apps to thousands of top software

as a service (SaaS) applications, while delivering a seamless end-user experience and greater visibility and control. Azure AD offers a robust and granular set of security controls to help protect identities from threats, including single sign-on, multifactor authentication, conditional access policies, identity protection, identity governance, and privileged identity management.

Windows works seamlessly 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 either syncing the device to an Active Directory domain, an Azure Active Directory (Azure AD) domain, or by quickly provisioning corporate owned devices so they meet the policy and security guidelines for the company. Easily configure the devices with the apps and settings the person needs to do their work through management solutions such as Microsoft Intune or Microsoft Endpoint Manager.
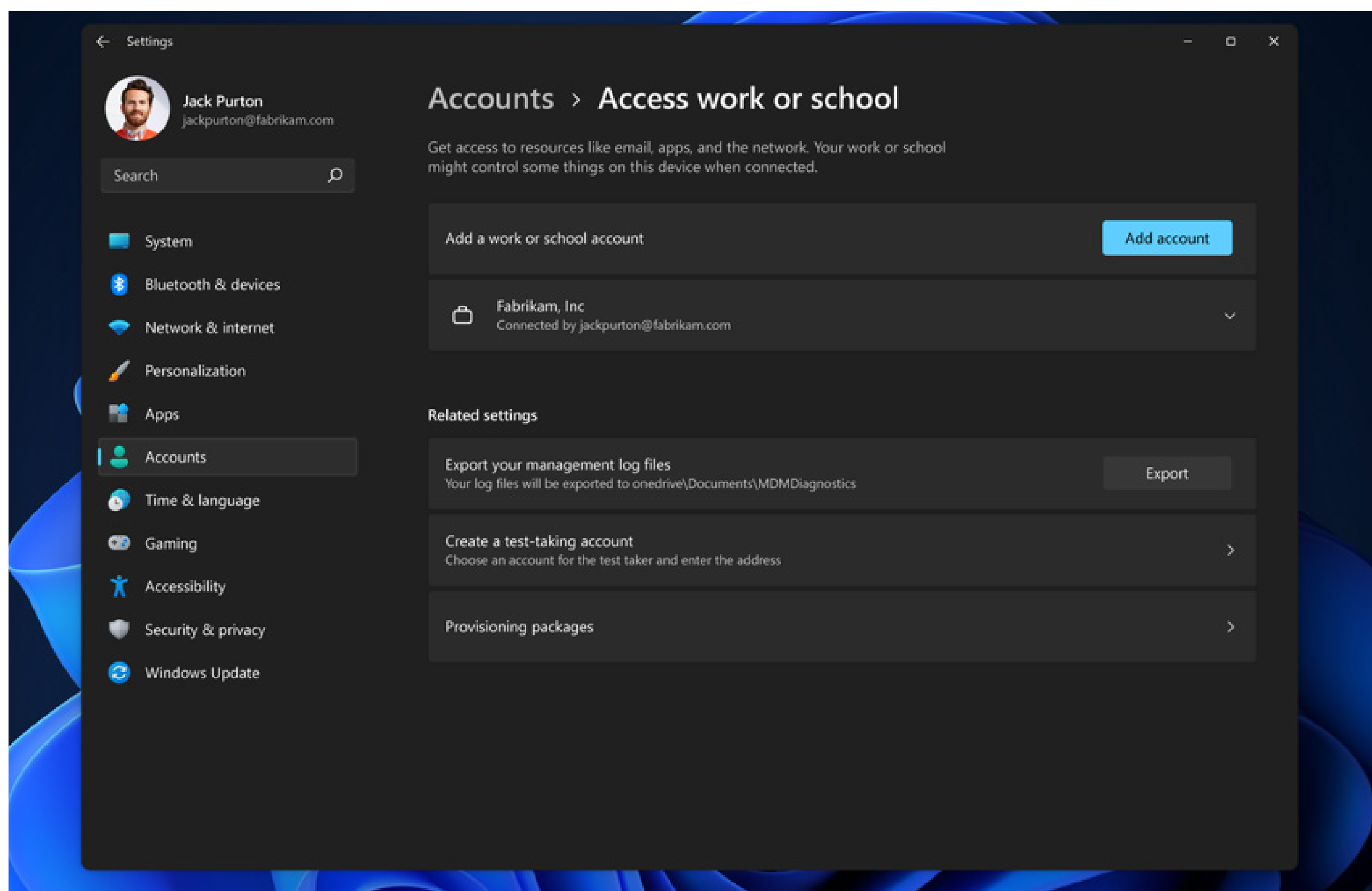
When a device is Azure Active Directory joined and managed with MDM, it will offer the following security benefits:

• Default fully managed user and device settings and policies

• Single sign on to all Microsoft Online Services

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

51

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

- Authentication tokens

- 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 and Microsoft Endpoint Manager

Windows 11 supports modern device management through solutions such as Intune to help IT pros manage company security policies and business applications while avoiding the compromise of the users' privacy on their personal devices. Endpoint Manager combines Microsoft Intune, Configuration Manager, Desktop Analytics, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, and respond and manage risk.

In addition to Intune, solutions from other vendors can be used to manage Windows 11 using industry-standard protocols. MDM-based solutions do not need to create or download a client to manage Windows 11, as the protocol is built into Windows, making it easy for users to get set up.

Windows 11 built-it 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](#).

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

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

52

The MDM security baseline includes policies such as:

- Microsoft inbox security technology – eg BitLocker, Windows Defender SmartScreen, virtualization-based security, Exploit Guard, Defender, and Firewall

- Restricting remote access to devices

- Setting credential requirements for passwords and PINs

- Restricting use of legacy technology

Remote Wipe

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 10 and Windows 11 support the Remote Wipe 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

Config Lock

In an enterprise organization, IT administrators enforce policies on their corporate devices to keep the devices in a compliant state and protect the OS by preventing users from changing configurations and creating config drift.

Config drift occurs when users with local admin rights change settings and put the device out of sync with security policies. Devices in a non-compliant state can be vulnerable until the next sync and configuration reset with the MDM,

Windows 11 with Config Lock enables IT administrators to prevent config drift and keep the OS configuration in the desired state. With config lock, the OS monitors the registry keys that configure each feature and when it detects a drift, reverts to the IT-desired state in seconds.

Windows Autopilot

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.

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

53

- 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).

- 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 here Windows Autopilot.

Microsoft Azure Attestation Service

Microsoft Intune integrates with Microsoft Azure Attestation Service to review Windows device health comprehensively and connect this information with AAD conditional access. This integration is key for Zero Trust solutions that help bind trust to an untrusted device.

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 the security features are in the expected states.

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

54

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 in the cloud to assess the trustworthiness of the platform according to the admin-configured device compliance rules.

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

Protecting your personal information

Microsoft Account

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

[The passwordless future is here for your Microsoft account](#) and built-into Windows is the ability to have a passwordless identity from your device through to the cloud protecting you from phishing or giving away your password by mistake to a nefarious actor.

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 how to set up and [Find and lock a lost Windows device](#) through your Microsoft Account

Family Safety

Microsoft Family Safety empowers you and your family to create healthy habits and protect your loved ones, both online and offline. Get peace of mind that your family is safer while giving your kids independence.

Use your Microsoft account to create a family group on Windows, Xbox, or your mobile devices. Then customize your family settings as your needs change, from the [family.microsoft.com](#) website or the Microsoft Family Safety app on Android and iOS.

Develop healthy digital habits with transparency into your family's activities. View your kids' weekly activity, including web, search, apps and games, and screen time. Balance their time online by setting screen time limits across Windows and Xbox, or set time limits on specific apps or games on Windows, Xbox, or Android to enable kids to be connected for online learning but stay focused.

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

55

Create a safe space for your kids to explore online. Use the content filtering settings to block inappropriate apps and games, and limit browsing to kid-friendly websites using Microsoft Edge on Windows, Xbox, and Android. To avoid surprises, get notified when your kids want to download a more mature app or game from the Microsoft Store on Windows and Xbox with age limits.

Stay connected even when you're apart with family location sharing. Share your location with loved ones, spot them on a map, and save places they visit the most.

Learn more about Microsoft Family Safety.

Microsoft OneDrive—protecting your important files in the cloud

OneDrive provides additional security, backup, and restore options for your important files and photos. With options for both personal and business, 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 including Desktop, Documents, and Pictures on your Windows PC. If your device is lost or stolen, you can quickly recover all your important files and photos.

OneDrive also provides protection for your most sensitive files without losing the convenience of anywhere access. Protect digital copies of your passport, driver's license, and other important documents in OneDrive Personal Vault. Your files will be secured by identity verification, yet 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.

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.

Security Foundation

Microsoft is committed to continuously invest 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 for powerful defense in today's threat environment.

Our strong security foundation leverages Microsoft Security Development Lifecycle (SDL) Bug Bounty, support for product security standards and certifications, and Azure Code signing. As a result, we improve security by producing software with fewer defects and vulnerabilities instead of relying on applying updates after vulnerabilities have been identified.

Built on the principles of Zero Trust, 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, customers get ultimate productivity and intuitive new experiences without compromising security.

Security assurance

Software development lifecycle

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

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, engineers are continuously provided with actionable and up-to-date methods to improve overall product security and development of the product even after the code has been released.

Microsoft stores and manages all Windows source code across all current and past Windows editions and products built on Windows including in a single repository. Security provisions including physical security, minimum privileges, detection, and peer code review process before developers submit any change to Windows further ensures product/code quality, identification of early defects, and ability to check for correctness and issues.

Additionally, our team of Security Assurance and Vulnerability Research experts perform targeted design reviews, audits, and deep penetration testing to some of our Window features that are deemed to contain higher risk attack surface. Microsoft's OneFuzz open

source 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 program 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 the national governments who are participants 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 product 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.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
User Security and Secured Identity | Privacy Controls and Transparency | Cloud Services | Security Foundation | Conclusion

59

Secure Supply Chain

The end to end (E2E) Windows Supply Chain is complex and opaque, extending from developer's check-in to build, chips to firmware, drivers, core OS, 3rd party apps, manufacturing/factory, all the way to secure updates. While we covered the various features as well as components of Windows 11 that enable and drive the security related capabilities, Microsoft also put significant attention and investment to ensure the security of the E2E supply chain for Windows 11. The various cyberattacks like SolarWinds and TSMC WannaCry, and recent Executive Order around enhancing Nation's Cybersecurity, highlighted the criticality and importance of also ensuring the security of products/software supply chain.

Some of the common controls that Microsoft requires the Windows 11 supply chain to comply with are:

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
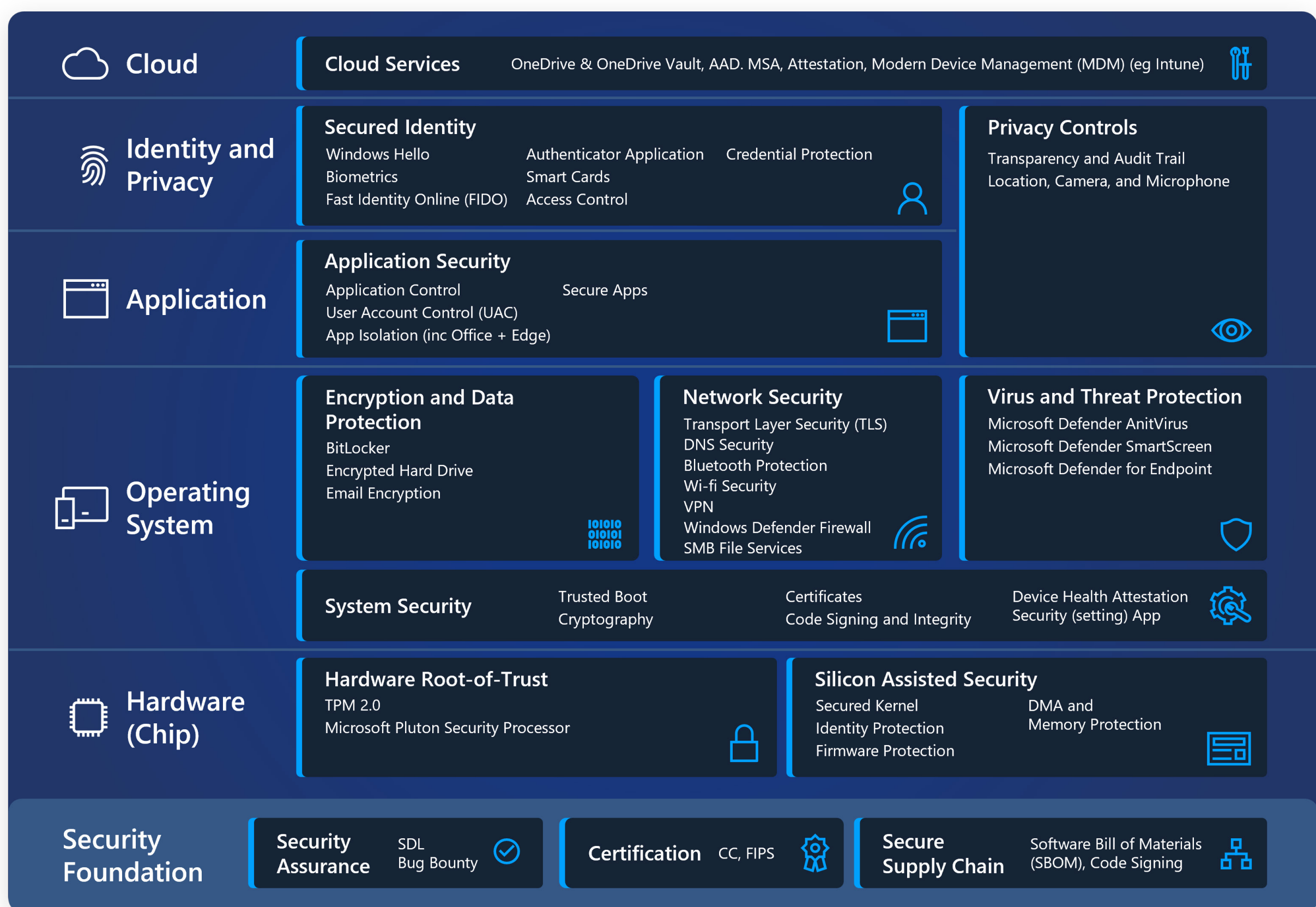Receiving / Shipping / Warehouse & Storage / Logistics Management

Code signing software is the best way to guarantee its integrity and authenticity. Code Signing your 1st and 3rd party applications greatly reduces the complexity associated with crafting and managing application control policies by allowing you to create and deploy 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

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
User Security and Secured Identity | Privacy Controls and Transparency | Cloud Services | Security Foundation | Conclusion

60

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 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. 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 LOB application and IT management scenarios, and test certificates for the development and validation inner loops.

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
User Security and Secured Identity | Privacy Controls and Transparency | Cloud Services | Security Foundation | Conclusion

61

| Cloud | Cloud Services | OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune) |

Identity and Privacy

Secured Identity
Windows Hello
Biometrics
Fast Identity Online (FIDO)

Authenticator Application
Smart Cards
Access Control

Credential Protection

Privacy Controls
Transparency and Audit Trail
Location, Camera, and Microphone

Application

Application Security
Application Control
User Account Control (UAC)
App Isolation (inc Office + Edge)

Secure Apps

Operating System

Encryption and Data Protection
BitLocker
Encrypted Hard Drive
Email Encryption

Network Security
Transport Layer Security (TLS)
DNS Security
Bluetooth Protection
Wi-fi Security
VPN
Windows Defender Firewall
SMB File Services

Virus and Threat Protection
Microsoft Defender AnitVirus
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint

System Security
Trusted Boot
Cryptography

Certificates
Code Signing and Integrity

Device Health Attestation
Security (setting) App

Hardware (Chip)

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

Silicon Assisted Security
Secured Kernel
Identity Protection
Firmware Protection

DMA and
Memory Protection

Security Foundation

Security Assurance
SDL
Bug Bounty

Certification
CC, FIPS

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

Conclusion

Built on the principles of Zero Trust, 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, customers get ultimate productivity and intuitive new experiences without compromising security. Learn how to upgrade to Windows 11 now.

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

Table of Contents | Introduction | Hardware Security | Operating System Security | Application Security
User Security and Secured Identity | Privacy Controls and Transparency | Cloud Services | Security Foundation | Conclusion

62

Appendix

[1]Microsoft Security Signals, September 2021.

[2]Requires compatible hardware with biometric sensors.

[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]Get the free Microsoft Authenticator app for Android or iOS https://www.microsoft.com/en-us/account/authenticator?cmp=h66ftb_42hbak

[5]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.

[6]Subscription sold separately.

[7]Requires TPM 2 or greater for TPM based key protection.

[8]Based on Microsoft telemetry data.