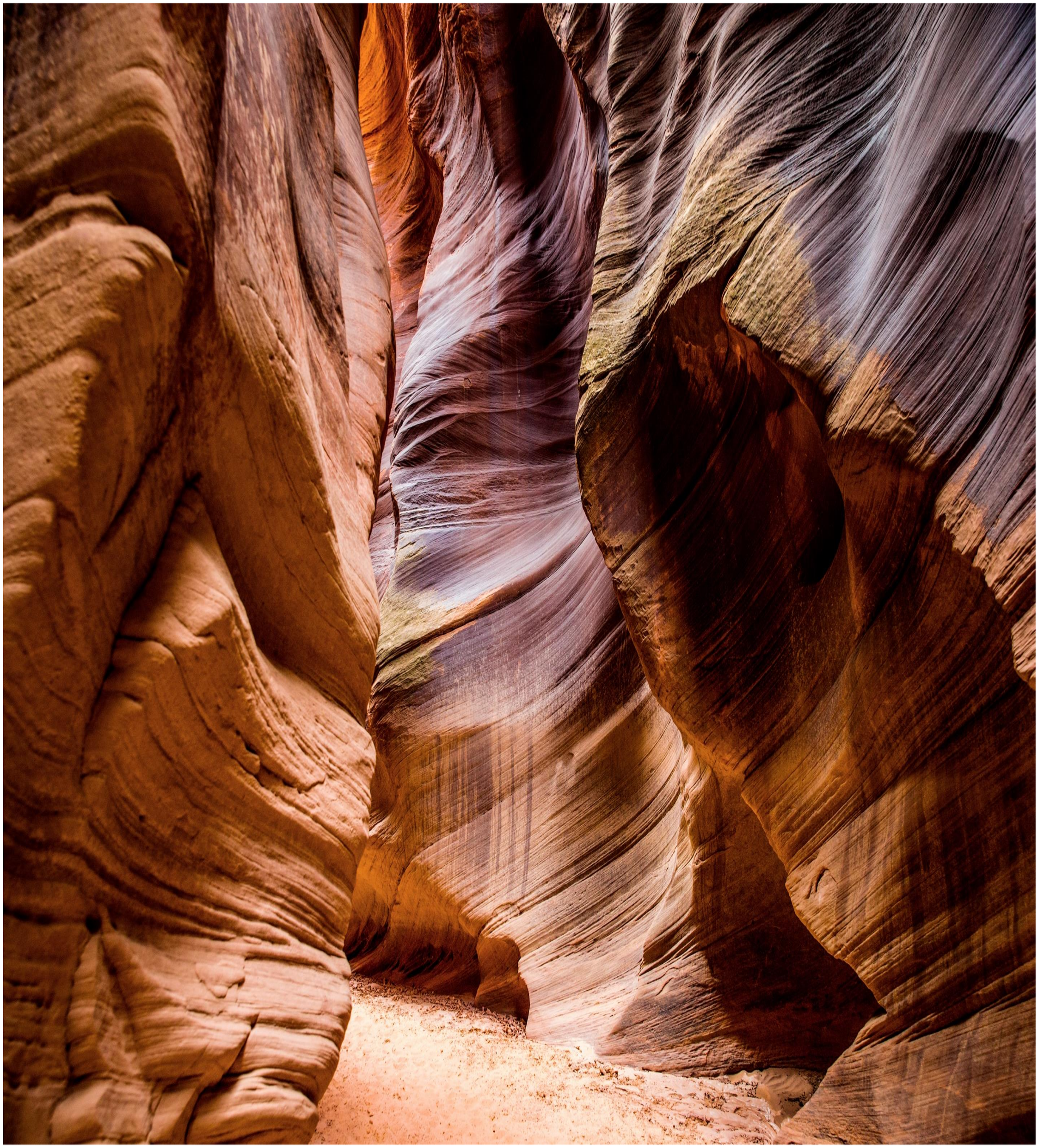


Layered, built-in security from core to cloud

Security threats are evolving in new ways; new kinds of cyberattacks and new vulnerabilities are emerging rapidly, making it imperative for organizations to stay up to date with a trusted operating system to help protect against such threats. Microsoft Windows Server 2025 builds on decades of Microsoft security expertise to deliver security and resiliency for on-premises, hybrid, and cloud-based IT environments. It helps you secure workloads, data, and operations with built-in capabilities and Azure innovations.

Contents

Scope 3

Introduction 4

Trustworthy addition 5

Operational security 11

Workload security 13

Silicon assisted security 14

Security foundation 16

Conclusion 18

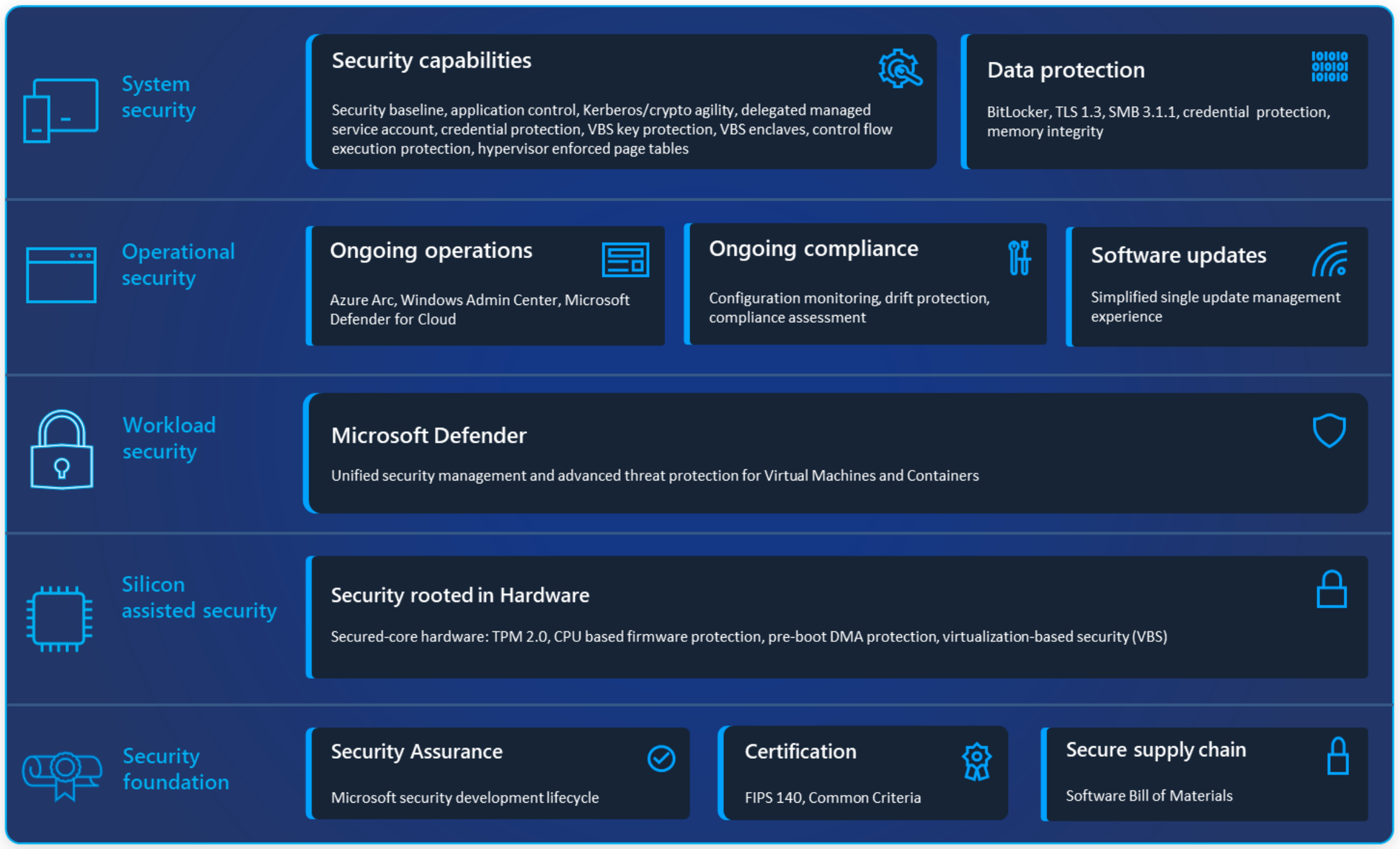
Scope

This security book applies to Windows Server 2025. This book provides an overarching view of security capabilities in Windows Server 2025 including new and improved security features. References to Windows Server refer to Windows Server 2025.

Introduction

Security affects everyone in your organization from upper-level management to the information worker. Inadequate security is a real risk for organizations as a security breach can disrupt all normal business and bring your organization to a halt. Information technology infrastructure is susceptible to a wide variety of attacks. Attackers typically take advantage of vulnerabilities in the hardware, firmware, operating system, or the application layer. Once they gain a foothold, they use techniques such as privilege escalation to move laterally to other systems in the organization. Windows Server supports security capabilities that can help protect, as well as detect and respond to such attacks.

Approximately 80% of security decision makers say that software alone is not enough protection from emerging threats (Microsoft Security Signals). With Windows Server, both hardware and software work together to help protect sensitive data from your server to the cloud. This level of protection helps keep your organization's data and IT infrastructure secure. See the layers of protection in the following diagram to get a brief overview of our security priorities.



Windows Server is designed to help defend against modern threats and is built to meet the requirements of a wide variety of security standards (see Certifications). The security posture of Windows Server is built on the following pillars:

- Security, rooted in hardware – Secured-core certified hardware enables strong security rooted in hardware.
- Security baseline which helps ensure that the system is deployed in a known good state.
- Configuration monitoring and drift protection which help ensure that the system remains in a known good state.

System security

Customers can deploy the system in a known good state in accordance with the Microsoft Cloud Security Benchmark.

Security baseline

Security baseline and best practices

Microsoft provides a tailored security baseline for Windows Server with hundreds of security settings. It supports security best practices based on Microsoft recommended security baselines and industry best practices. Customers can apply the security baseline throughout the device lifecycle starting from initial deployment using Microsoft provided 'PowerShell tooling' or Windows Admin Center, supported by the new security configuration platform, 'OSConfig'. Customers can leverage the 'inbuilt drift control mechanism', one of the salient features of the security configuration platform which helps ensure that the system starts and remains in a known good security state.

This security baseline helps you to meet some of the Center for Internet Security (CIS) Benchmark, Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG), Federal Information Processing Standards (FIPS 140) requirements for the operating system, and Azure Compute Security baselines. The security baseline settings have been verified for compatibility and performance impact. Support of those security baselines is intended to make it easier for customers to help meet their compliance and regulatory requirements.

Use of secure protocols and cryptographic standards

When customers enable the security baseline for Windows Server, only secure versions of protocols will be supported: Transport Layer Security (TLS) versions 1.2 or higher, Datagram Transport Layer Security (DTLS) versions 1.2 or higher, and Server Messaging Block (SMB) 3.0 or higher. Further, the security baseline supports National Institute of Standards and Technology (NIST) guidelines for cryptographic standards.

We have upgraded certificate management – searching or retrieving certificates on Windows now supports SHA-256 hashes, as described in CertFindCertificateInStore function and CertGetCertificateContextProperty function. TLS server authentication is more secure across Windows, and now requires a minimum RSA key length of 2048 bits. For more information, read TLS server authentication: Deprecation of weak RSA certificates.

Application control

Preventing unwanted or malicious applications from running is an important part of an effective security strategy. Application control is an effective means for addressing the threat of executable file-based malware. Application control helps mitigate security threats by restricting applications that users are allowed to run.

While most customers inherently understand the value of application control, the reality is that only some have been able to employ application control solutions in a manageable way. Application Control for Business (previously known as Windows Defender for Application Control or WDAC) provides powerful control over what applications are allowed to run and the code that runs in the OS (kernel).

Microsoft provides WDAC base policies which customers can enable in audit or enforced mode. Customer can also create supplemental policies to augment and extend the base policy. Microsoft provides an Azure Monitor workbook which customers can use for application control insights. Using the workbook will benefit customers by providing at-scale insights on WDAC File Events and Policy Events activity, which will allow them to understand what is being blocked, which policy ran the process and more. Additionally, this data can be filtered and exported to be ingested into WDAC Wizard app to help compose a new application control policy.

Credential protection

Credential Guard uses virtualization-based security (VBS) to help protect against credential theft. With Credential Guard, the Local Security Authority (LSA) stores and protects Active Directory secrets in an isolated environment that is not accessible to the rest of the operating system. By protecting the LSA process with virtualization-based security, Credential Guard helps prevent credential dumping attacks such as pass-the-hash or pass-the-ticket. Credential Guard is now enabled by default on Server machines which meet enablement requirements.

Machine account hardening using Credential Guard

Credential Guard for machine accounts is an opt-in policy managed change that helps secure machine account credentials in AD-joined devices. When enabled, the device's machine account credential becomes bound to the device, to help prevent the manipulation and exfiltration of credentials, even in the face of sophisticated attacks like SolarWinds. This is accomplished by moving the password from the registry and into Credential Guard, while leveraging Virtualization-Based Security (VBS) and TPM cryptography to safeguard it. Additionally, an audit mode is available, allowing customers to evaluate the feature's functionality before full enforcement is implemented.

Delegated Managed Service Account (DMSA)

Service accounts are accounts used to authenticate and authorize services to access resources within a domain. These traditional accounts often rely on manually set, weak, and rarely updated passwords, making them an attractive target for attackers. Despite encryption, the proximity of the encryption key to the passwords poses a huge risk. Once an attacker locates the key, the password can be retrieved, granting unauthorized access to resources, privilege escalation, lateral movement, and other malicious activities.

In Windows Server 2008 R2 and Windows Server 2012, Managed Service Accounts (MSAs) and Group Managed Service Accounts (GMSAs) were introduced. MSAs and GMSAs were designed to isolate domain accounts and enable the automatic generation and rotation of account passwords. Although MSAs and GMSAs are more secure than service accounts, the underlying issue remains – passwords are still used. Eventually, passwords may be leaked due to malicious administrators or inadvertent disclosure, forcing a strong need for a mechanism to eliminate password usage in service accounts.

In Windows Server 2025, a novel account type known as Delegated Managed Service Accounts (DMSA) is set to evolve how domain-joined machines help manage authentication and service account security. Building upon the foundations of GMSAs, DMSAs are designed to facilitate the transition from traditional service accounts to machine-specific accounts that offer enhanced security through managed and fully randomized keys. This shift not only simplifies the management of service accounts but also significantly elevates the security posture of domain environments.

DMSAs inherently limit the scope of account usage by binding service accounts to specific machine identities, to help ensure that only authorized machines can request and use the account. This binding is critical in preventing unauthorized access and usage of the service accounts, thereby mitigating potential security risks. Furthermore, DMSAs incorporate automatic password rotation mechanisms, which help eliminate the need for manual password updates - a common vulnerability in traditional service account management. By automating this process, DMSAs maintain a high level of account security without administrative intervention.

Another significant enhancement introduced with DMSAs is the integration with Credential Guard. This integration binds machine identities and service account tickets to Credential Guard, leveraging its robust security features to further help protect account credentials from exposure and theft. This layered security approach will help ensure that even if attackers penetrate other security barriers, the protection provided by Credential Guard and the inherent features of DMSA will impede unauthorized access to service accounts.

To learn more about DMSA, visit Delegated Managed Service Accounts overview.

Memory integrity protection

Kernel mode code integrity is the Windows process that checks whether all kernel code is properly signed and has not been tampered with before it is allowed to run. Hypervisor-protected code integrity (HVCI), also called memory integrity, uses virtualization-based security (VBS) to run kernel mode code integrity 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.

Memory integrity also restricts kernel memory allocations that could be used to compromise the system, ensuring that kernel memory pages are only made executable after passing code integrity checks inside the secure VBS environment, and executable pages themselves are never writable. That way, even if there are vulnerabilities like buffer overflow that allows malware to attempt to modify memory, executable code pages cannot be modified, and modified memory cannot be made executable. Memory integrity helps protect against attacks that rely on the ability to inject malicious code into the kernel using bugs in kernel-mode software. Customers can enable memory integrity protection to help protect against attacks involving kernel mode code changes.

Data at rest protection

BitLocker Drive Encryption is a data protection feature that addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Data stored on a lost or stolen device is vulnerable to unauthorized access, such as by running a software-attack tool against it, or by transferring the device's hard drive to a different device. BitLocker helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled. Customers can enable BitLocker encryption on OS and data volumes.

Data in transit protection

Transport layer security (TLS)

Transport Layer Security (TLS) is a popular security protocol, encrypting data in transit to help provide a more secure communication channel between two endpoints. Windows enables the latest protocol versions and strong cipher suites by default and offers a full suite of extensions such as client authentication for enhanced server security, or session resumption for improved application performance. TLS 1.3 is the latest version of the protocol and is enabled by default in Windows. This version helps to eliminate obsolete cryptographic algorithms, enhance security over older versions, and aim to encrypt as much of the TLS handshake as possible. The handshake is more performant with one fewer round trip per connection on average and supports only strong cipher suites which provide perfect forward secrecy and less operational risk. Using TLS 1.3 will provide more privacy and lower latencies for encrypted online connections. Note that if the client or server application on either side of the connection does not support TLS 1.3, the connection will fall back to TLS 1.2. Windows uses the latest Datagram Transport Layer Security (DTLS) 1.2 for UDP communications.

Server Messaging Block (SMB) security

Signing is now required by default for all SMB outbound and inbound connections in Windows Server 2025. This changes legacy behavior, where Windows 10 and 11 required SMB signing by default only when connecting to shares named SYSVOL and NETLOGON and where Active Directory domain controllers required SMB signing from their clients. Signing helps prevent data tampering and relay attacks to malicious servers. All the major security industry baselines recommend enabling Server Message Block (SMB) signing. For more information, see Control SMB signing behavior.

The SMB client now supports blocking NTLM authentication for remote outbound connections. Blocking NTLM authentication helps prevent bad actors from tricking clients into sending NTLM requests to malicious servers, counteracting brute force, cracking, and pass-the-hash attacks. NTLM blocking allows organizations to guarantee the use of Kerberos with SMB.

The SMB authentication rate limiter is a feature of SMB server designed to address brute force authentication attacks. Brute force authentication helps attack bombard the SMB server with multiple username and password-guesses and the frequency can range from dozens to thousands of attempts per second. The SMB authentication rate limiter is enabled by default with a 2 second delay between each failed NTLM or Local KDC Kerberos-based authentication attempt. An attack that sends 300 guesses per second for 5 minutes,

for example - 90,000 password guess attempts - would now take 50 hours to complete, increasing the likelihood of detection and diminishing the likelihood of successful guessing. For more information, see Configure SMB authentication rate limiter for Windows.

The SMB over QUIC server is now available in all editions of Windows Server 2025. SMB over QUIC offers an "SMB VPN" for telecommuters, mobile device users, and on highest security internal networks. The server certificate creates a TLS 1.3-encrypted tunnel over a UDP port instead of TCP/445. No SMB traffic - including authentication and authorization - is exposed to the underlying network. SMB behaves normally within the QUIC tunnel, meaning the user experience doesn't change and capabilities like multichannel and compression continue to work. In addition, you can now configure the SMB over QUIC client to allow connection only to specific servers. You can configure the SMB over QUIC server to listen on UDP ports other than 443 for more flexible firewall configuration. For more information, see SMB over QUIC.

SMB over QUIC client access control enables you to restrict which clients can access SMB over QUIC servers. Client access control creates allow and blocklists for devices to connect to the file server based on certificates. Client access control helps give organizations more protection without changing the authentication used when making the SMB connection and does not alter the end user experience. For more information, see Configure SMB over QUIC client access control in Windows Server.

By default, the SMB server and client automatically negotiates the highest matched dialect from SMB 2.0.2 to 3.1.1. You can now specify the SMB protocols used, blocking older, less secure, versions from connecting to the server. For example, you can specify connection to only use SMB 3.1.1, the more secure dialect of the protocol. The minimum and maximum can be set independently on both the SMB client and server, and you can set just a minimum if desired. For more information, see Manage SMB dialects in Windows.

NOTICE. Remote Mailslots are deprecated. The Remote Mailslot protocol is a dated, simple, unreliable, insecure IPC method first introduced in MS DOS. It is now disabled by default for SMB and for DC Locator usage with Active Directory. For more information, see Features removed or no longer developed starting with Windows Server 2025.

Windows Defender Firewall Rules. The built-in Windows defender Firewall rules do not open SMB NetBIOS ports anymore when an administrator configures shares. This change brings SMB firewall rules more in line with the standard behavior for the Windows Server File Server role. Administrators can reconfigure the rules to restore the legacy ports. For more information, see Secure SMB Traffic in Windows Server.

Auditing SMB over QUIC. SMB now supports auditing use of SMB over QUIC, missing third party support for encryption, and missing third party support for signing. These are available at both the SMB server and SMB client logging levels for improved auditing of unsafe or suspicious behaviors.

Requiring encryption for outbound connections. The SMB client now supports requiring encryption of all outbound SMB connections. Encryption of all outbound SMB client connections enforces the highest level of network security and brings management parity to SMB signing, which allows both client and server requirements. When enabled, the SMB client will not connect to an SMB server that doesn't support SMB 3.0 or later, or that doesn't support SMB encryption. For example, a third-party SMB server might support SMB 3.0 but not SMB encryption. Unlike SMB signing, encryption is not required by default. For more information, see Configure the SMB client to require encryption in Windows.

For signing and encryption security, Windows Server supports AES-256-GCM and AES-256-CCM cryptographic suites for the SMB 3.1.1 protocol used by client-server file traffic as well as the intra-cluster data fabric. It continues to support the more broadly compatible AES-128 as well. Windows Server also supports SMB Direct encryption. Data is encrypted before placement, leading to less performance degradation while adding AES-128 and AES-256 protected packet privacy.

Furthermore, Windows Server supports granular control of encrypting intra-node storage communications for Cluster Shared Volumes (CSV) and the storage bus layer (SBL). This means that when using Storage Spaces Direct, you can decide if you want to use encryption or signing on remote file system, CSV, and the SBL traffic separately from each other. And finally, Windows Server supports the accelerated AES-128-GMAC signing option with lower latency and CPU usage. You can use Windows Admin Center (WAC) and PowerShell cmdlets for granular control of SMB signing and encryption. All of these combine to give the maximum flexibility for your threat model and performance requirements. For more information, see SMB security enhancements.

Network security

Software defined networking (SDN) and micro-segmentation

With Windows Server, you can take steps towards ensuring that your applications and workloads are protected from external as well as internal attacks. Through micro-segmentation, you can create granular network policies between applications and services. This essentially reduces the security perimeter to a fence around each application or VM. This fence permits only necessary communication between application tiers or other logical boundaries, thus making it exceedingly more difficult for cyberthreats to spread laterally from one system to another. Micro-segmentation securely isolates networks from each other and reduces the total attack surface of a network security incident.

Micro-segmentation in Windows Server is implemented through Network Security Groups (NSGs), like Azure. With NSGs, you can create allow or deny firewall rules where your rule source and destination are network prefixes. We also support tag-based segmentation, where you can assign any custom tags to classify your VMs, and then apply NSGs based on the tags to restrict communication to/from external as well as internal sources. To prevent your SQL VMs from communicating with your web server VMs, simply tag corresponding VMs with “SQL” and “Web” tags and create a NSG to prevent “Web” tag from communicating with “SQL” tag. These policies are available for VMs on traditional VLAN networks and on SDN overlay networks. Management of NSGs is supported through Windows Admin Center, PowerShell, and REST APIs.

To learn more about NSGs, see Configure network security groups with Windows Admin Center.

To learn more about NSG configuration with tags, see Configure network security groups with tags in Windows Admin Center.

Leveraging Network Security Groups, Windows Admin Center allows you to configure default network policies when you create a virtual machine. With these policies, the virtual machine is protected from unauthorized external as well as internal attacks from the get-go. These policies block all inbound access to virtual machines (except the specified management ports you want enabled) while allowing all outbound access.

To learn more about default network policies, see Enable and assign default network access policies.

Virtualization-based security (VBS) key protection

In Windows Server, applications can now use virtualization-based security to help protect cryptographic keys. With this new capability, keys can be protected from admin-level key theft attacks with negligible effect on performance, reliability, or scale.

VBS uses the virtualization extension capability of the CPU to create an isolated runtime outside of the normal operating system. When in use, VBS keys are isolated in a secure process, allowing key operations to occur without ever exposing the private key material outside of this space. At rest, private key material is encrypted by a TPM key which binds VBS keys to the device. Keys protected in this way cannot be dumped from process memory or exported in plain text from a user’s machine, helping prevent exfiltration attacks by any admin-level attacker.

VBS provides a balanced key protection solution – stronger security than software solutions while still supporting higher scale/performance requirements compared to hardware-based solutions. Applications can also use VBS attestation in combination with Microsoft Azure Attestation SDK to verify that VBS keys are associated with a trusted device.

VBS key protection and attestation is offered as an extension of the NCrypt Cryptographic Next Generation (CNG) framework. .NET support is also available for some VBS functionality.

To learn more, see Advancing key protection in Windows using VBS.

Virtualization-based security (VBS) enclaves

A Virtualization-based security (VBS) enclave is a software-based trusted execution environment (TEE) inside the address space of a host application. VBS enclaves leverage underlying VBS technology to help isolate the sensitive portion of an application in a secure partition of memory. VBS enclaves enable isolation of sensitive workloads from both the host application and the rest of the system. VBS enclaves enable applications to help protect their secrets by removing the need to trust admins and hardening against malicious attackers. For information, read Virtualization-based security (VBS) enclaves.

Hypervisor-enforced Paging Translation

Hypervisor-enforced Paging Translation (HVPT) is a security enhancement to enforce the integrity of guest virtual address to guest physical address translations to help protect critical system data from write-what-where attacks where the attacker can write an arbitrary value to an arbitrary location often as the result of a buffer overflow. HVPT helps to protect page tables that configure critical system data structures. HVPT will protect everything already protected with HVCI today. HVPT is enabled by default where hardware support is available (Intel Alderlake+ vPro enabled hardware) and if VBS and HVCI are enabled. **NOTE.** HVPT is not enabled when Windows Server runs as a guest in a virtual machine.

Control flow execution protection

ROP (return-oriented programming) attacks attempt to redirect and take control of the control flow during execution. Control flow guard (CFG) in Windows helps protect against memory corruption attacks. CFG helps enforce integrity on indirect calls or forward-edge control flow integrity (CFI). Hardware-enforced stack protection (HSP) helps enforce integrity on return addresses on the call stack (backward-edge CFI) via use of hardware-based shadow stack. For more information, read Understanding Hardware-enforced Stack Protection.

Kerberos enhancements

Kerberos in Windows Server now supports crypto agility. As existing cryptographic algorithms become outdated those algorithms can be replaced with new ones. This is important as the industry progressively moves to using post-quantum resilient cryptographic algorithms.

Extended protection for authentication

Man in the middle or relay attacks are when an attacker-controlled server intercepts authentication messages from a client and relay them to a target resource. This is commonly used by attackers to gain access to the resource as the client. Extended protection for authentication (EPA) enhances existing Windows authentication functionality to help protect against these types of attacks using two techniques called channel-binding and service-binding. Channel-binding is used when authentication is done over SSL/TLS and binds the authentication to that specific connection. Service-binding binds authentication to the specific Service Principal Name (SPN) that the client is connecting to. Windows Server now enables EPA by default for the Lightweight Directory Access Protocol (LDAP) and Exchange Server.

Identity management

Active Directory supports several security improvements such as channel binding audit support, DC-location algorithm improvements, improved algorithms for Name/Sid lookups, improved security for confidential attributes, improved security for default machine account passwords, Kerberos related improvements, LDAP encryption by default, LDAP support for TLS 1.3, and legacy SAM RPC password change behavior. For details, you can read Active Directory improvements.

Operational security

Ongoing operations

You can use a service or tool of your choice to operate your Windows Server. This section covers the use of Windows Admin Center and Microsoft Defender for Cloud for operating Windows Server in a more secure manner.

Security management with Windows Admin Center

Windows Admin Center is a locally deployed, browser-based remote management tool that lets you manage your Windows Server running anywhere – physical, virtual, on-premises, in Azure, or in a hosted environment – at no additional cost. Windows Admin Center gives you full control over all aspects of your server infrastructure, providing you with tools to assess the security posture of your Windows Server and proactively take action to help secure and protect it.

Using Windows Admin Center, you can apply the recommended Windows Server security baseline and enable drift protection, without having to remote desktop into the machine or open a PowerShell terminal. From Windows Admin Center, you can view and monitor the security state of your Windows Server security baseline.

You can also gain insights into the security compliance state of your Windows Server machine via the Silicon Assisted Security section of the tool which will display the status of each security requirement for both Secured-core and minimum recommended hardware, allowing you to troubleshoot, enable or disable, and monitor those security requirements.

Continuous monitoring with Microsoft Defender for Cloud

Post deployment, you can leverage Microsoft Defender for Cloud for monitoring the overall security posture of your Azure Arc-enabled Windows Server deployments, like all your hybrid resources across your fleet. Microsoft Defender for Cloud helps improve the security posture of your environment, and helps protect against existing and evolving threats. It provides you with tools to assess the security status of your infrastructure, protect workloads, raise security alerts, and follow specific recommendations to remediate vulnerabilities.

Azure Arc simplifies governance and management by delivering a multi-cloud and on-premises management platform.
It extends management to edge and multi-cloud and provides a single pane of glass management control plane. By Arc-enabling your Windows Server, you can install Azure Monitor agent via Azure Arc. This allows your Windows Server deployment to be monitored through Microsoft Defender for Cloud which continuously monitors the security posture of your entire Windows Server fleet.

Ongoing compliance

Security baseline drift protection

System configuration settings can change over time and drift away from the desired configuration state. This can affect the security posture of your system and make it more vulnerable to attacks. Once you apply the recommended Windows Server security baseline using recommended tools, you can monitor, and perform drift protection from desired state during run time, using the built-in security configuration platform stack in the operating system. This is a new feature which will help protect your ‘desired state’ and protect against any tampering and unintended changes to your declared configuration.

You can enable drift protection during deployment time or after deployment using Windows Admin Center or PowerShell. Once drift protection is applied, the security settings will be refreshed at regular intervals, thus ensuring any change from desired state is remediated. This continuous monitoring and auto-remediation allows your server to have consistent and reliable security posture throughout the lifecycle of the system.

If you need to adjust or update security baseline settings based on your own business requirements, you can modify any of those settings, and use drift protection to maintain your system configuration based on those modified settings. Note, any configuration changes made to settings outside of the security baseline will not be enforced via drift protection.

Azure security baseline compliance assessment

Azure Policy helps to enforce organizational standards and to assess compliance at scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to per-resource and per-policy granularity. You can use Azure Policy to audit Windows Server configuration and perform compliance assessment against the 'security baseline definition' applied during deployment.

In addition to monitoring and reporting compliance, you also have the ability to remediate the security baseline via Azure Policy and Azure Automanage. Security compliance requires strict logging and auditing of security events. With Windows Server, we recommend customers use Microsoft Sentinel security information and event management (SIEM) solution to help uncover sophisticated threats and for proactive threat detection, investigation, and response.

Regulatory compliance

Regulatory Compliance in Azure Policy provides Microsoft created and managed initiative definitions, known as *built-ins*, for the compliance domains and security controls related to different compliance standards. It also provides the compliance domains and security controls for Azure Arc-enabled servers. You can assign the built-ins for a security control individually to help make your resources compliant with specific regulatory standards.

Updates

Software updates

It is important to update your Windows Server and keep it up to date with the latest bug fixes and security updates. This will help address vulnerabilities as and when they are discovered. You can use Windows Update to update the operating system to include the latest bug fixes and security updates. You can use Cluster-Aware Updating (CAU) to update servers in a failover cluster with little or no loss in availability during the update process. You can use Azure Update Manager to help manage and govern updates for your Windows Server machines. You can use Windows Server Update Services (WSUS) especially if your servers are behind a firewall. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network. You can also use 3rd party tools of your choice for update management.

Workload security

Virtual machine security

When creating a new virtual machine through Hyper-V Manager, Generation 2 is now set as the default option in the New Virtual Machine Wizard. Generation 2 virtual machines enable secure boot by default. Secure Boot is a security feature that helps prevent malicious software (malware and corrupted components) from loading when the virtual machine starts. This is done by verifying the digital signature of the components that are loaded during the boot sequence.

Continuous monitoring

You can enable Microsoft Defender for Cloud for your virtual machines running on Windows Server. This enables you to continuously monitor their security posture and take corrective actions. When the virtual machine is Azure Arc-enabled, Microsoft Defender for Cloud can install the Azure Monitor agent inside the virtual machine and correlate events that the agent collects into recommendations (hardening tasks) that you can perform to make your workloads more secure. The hardening tasks are based on security best practices that include managing and enforcing security policies. You can then track the results and manage compliance and governance over time through Defender for Cloud monitoring while reducing the attack surface across all your resources.

Microsoft Defender for Cloud also detects real-time threats such as malware and notifies you by raising security alerts and providing recommendations to remediate attacks. Security alerts are categorized and assigned severity levels to indicate proper responses. Security alerts can be correlated to identify attack patterns and to integrate with Security Information and Event Management (SIEM), Security Orchestration Automated Response (SOAR), and IT Service Management (ITSM) solutions. This allows you to respond to threats and limit the risk to your resources.

You can also use Microsoft Defender for Cloud to protect your workloads such as Azure Arc-enabled SQL Server and Azure Arc-enabled Kubernetes clusters.

Microsoft Sentinel is a security information and event management (SIEM) solution for proactive threat detection, investigation, and response. You can aggregate security data and correlate alerts from virtually any source and modernize your security operations center (SOC) with Microsoft Sentinel. Security alerts from Microsoft Defender for Cloud can be streamed to Microsoft Sentinel, so you can investigate and respond to incidents.

Silicon-assisted security

Secured-core hardware

Secured-core servers take a defense-in-depth approach to basic system security. Using our learnings from the Secured-core PC initiative, Microsoft has teamed up with the ecosystem partners to expand Secured-core to Windows Server. In the Secured-core Server blog you can read examples of how Secured-core servers seamlessly integrate with the broader suite of Microsoft's security offerings to not just identify but also help block real world attacks.

Secured-core Server is built on three key pillars: simplified security, advanced protection, and preventative defense. Secured-core Servers come with the assurance that manufacturing partners have built hardware and firmware that satisfy the requirements of the operating system (OS) security features.

Simplified security

The security extension in Windows Admin Center makes it easy for you to configure the OS security features of Secured-core for Windows Server. The extension provides IT admins with a simplified way to enable and maintain the state of advanced security features provided by Secured-core Server.

Advanced protection

Secured-core Server maximize hardware, firmware, and OS capabilities to help protect against current and future threats. These safeguards create a platform with added security for critical applications and data used on the hosts and/or VMs that run on them. Secured-core functionality spans the following areas:

Hardware root-of-trust: Trusted Platform Module 2.0 (TPM 2.0) comes standard with Secured-core servers, providing a protected store for sensitive keys and data, such as measurements of the components loaded during boot. Being able to verify that firmware that runs during boot is validly signed by the expected author and not tampered with helps improve supply chain security. This hardware root-of-trust elevates the protection provided by capabilities like BitLocker, which uses TPM 2.0 and facilitates the creation of attestation-based workflows that can be incorporated into zero-trust security strategies.

Firmware protection: In the last few years, there has been a significant increase in firmware vulnerabilities, in large part due to the inherently higher level of privileges with which firmware runs combined with the limited visibility into firmware by traditional anti-virus solutions. By using processor support for Dynamic Root of Trust of Measurement (DRTM) technology, Secured-core servers put firmware in a hardware-based sandbox, which helps to limit the impact of vulnerabilities in millions of lines of highly privileged firmware code. Along with pre-boot DMA protection, Secured-core servers provide protection throughout the boot process.

Virtualization-based security (VBS): Secured-core servers support VBS and Hypervisor-protected code integrity (HVCI). VBS and HVCI help enhance the security of Windows Server, offering robust protection against malware that attempts to exploit the Windows kernel. VBS utilizes the Windows hypervisor to establish an isolated virtual environment, forming a root of trust for the operating system under the assumption that the kernel could be compromised. HVCI plays a critical role in helping to safeguard and fortify Windows Server by enforcing kernel mode code integrity within this secure virtual environment. Additionally, HVCI restricts kernel memory allocations that could be exploited to compromise the system, ensuring that kernel memory pages are only made executable following code integrity verification within the secure runtime environment, and that executable pages are never writable. VBS and HVCI works together to help ensure that servers remain devoted to running critical workloads and help protect related applications and data from attack and exfiltration.

Preventative Defense

Enabling Secured-core functionality helps proactively defend against and disrupt many of the paths attackers may use to exploit a system. These defenses also enable IT and SecOps teams to better leverage their time across the many areas that need their attention.

Secured-core certified servers

Secured-core servers help to provide advanced host protection against even the most sophisticated firmware level attacks. Such advanced protection requires deep integration between the operating system and the hardware. This is standardized in the Windows Server certification program via Secured-core Server Additional Qualification (AQ). Secured-core servers can be easily found in the Windows Server catalog by using the Secured-core Server filter in the Additional features section. Windows Server systems supporting Secured-core capabilities are available from a wide variety of industry leading server manufacturers. Thus, customers will benefit from the advanced host protection that is only available with Microsoft operating system platforms, regardless of the hardware manufacturer of their choice.

Security foundation

Security assurance

Microsoft is committed to continuously investing in improving our software development process by building highly secure-by-design software and addressing security compliance requirements. We build in security from the ground up to help defend against existing and emerging threats. Every component of Windows Server, from server core to cloud, is purposefully designed to help ensure ultimate security.

Microsoft Security Development Lifecycle (SDL)

The Microsoft Security Development Lifecycle (SDL) introduces security best practices, tools, and processes throughout all phases of engineering and development. A range of tools and techniques – such as threat modeling, static analysis, fuzzing, and code quality checks – enable continued security value to be embedded into Windows by every engineer on the team from day one. Through the SDL practices, Microsoft engineers are continuously provided with actionable and up-to-date methods to help improve development workflows and overall product security before the code has been released. Additionally, Microsoft Offensive Research and Security Engineering (MORSE) performs targeted design reviews, audits, and deep penetration testing of select Windows features. Microsoft's open source OneFuzz platform allows developers to fuzz features for Windows at scale as part of their development and testing cycle.

Security assessment activities

As part of our SDL, products like Windows Server are reviewed by our Microsoft Offensive Research and Security Engineering (MORSE) team. MORSE works with other Microsoft security teams to perform comprehensive security assessments of the product. The goal of the security assessment activities is to help:

- Confirm security promises the product makes are valid and effective.
- Identify insecure configurations, vulnerabilities, and design flaws in Windows and its dependencies and ensure they are corrected before shipping.
- Review the product against Microsoft's SDL security requirements.
- Confirm the product meets Microsoft's standard of shipping a secure solution from inception.
- Confirm that the product can also be managed to maintain and enhance security during the product's lifecycle.

Product security assessments will be done as new features are included and as the product continues through its lifecycle. This approach to securing edge products, staying current with best practices, customer needs, and regulatory and compliance requirements is the commitment Microsoft is making to developing a security-first product in Windows Server.

Certifications

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 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 in Windows operating systems against FIPS 140-2 since it was first established in 2001.

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

Microsoft publishes the list of FIPS 140 and CC certified products at Federal Information Processing Standard (FIPS) 140 Validation and Common Criteria Certifications.

Secure supply chain

The work to secure the supply chain for software is important to Microsoft and the world. The changing landscape and speed of technology has warranted efforts by governments, organizations, and corporations alike to improve oversight and build in new capabilities. Microsoft is actively involved in developing standards (such as IETF and OpenSSF) and working with others to produce innovative changes. The initial focus is on how we and others produce products but with an eye towards running systems.

Conclusion

Through this book we intend to provide context on how Windows Server and related Azure security capabilities use a multifaceted approach to help protect companies from existing and emerging threats. By describing the different layers of protection (system security, operational security, workload security, silicon assisted security, and security foundation), you can layer your approach to security in a manner that meets your needs. We intend to build on our security foundation with innovations that deliver powerful protection now and in the future.

Of course, a paper of this length does not cover every security topic that you may want to stay informed of, so as a next step we suggest exploring these resources:

Windows Server documentation
What's new in Windows Server 2025
Windows Server Security documentation
Download Windows Server 2025
Microsoft Defender for Cloud
Training for Security Engineers
Training for Security Operations Analysts

Microsoft Azure

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.