What is Secured-core server?

Article • 04/06/2023

> Applies to: Windows Server 2022, Azure Stack HCI version 21H2 and later

Secured-core is a collection of capabilities that offers built-in hardware, firmware, driver and operating system security features. The protection provided by Secured-core systems begins before the operating system boots and continues whilst running. Secured-core server is designed to deliver a secure platform for critical data and applications.

Secured-core server is built on three key security pillars:

- Creating a hardware backed root of trust.
- Defense against firmware level attacks.
- Protecting the OS from the execution of unverified code.

What makes a Secured-core server

The Secured-core initiative started with Windows PCs through a deep collaboration between Microsoft and PC manufacturing partners to provide the most elevated Windows security ever. Microsoft has expanded the partnership further with server manufacturing partners to help ensure Windows Server delivers a secure operating system environment.

Windows Server integrates closely with hardware to provide increasing levels of security:

- Recommended baseline: The recommended minimum for all systems to provide foundational system integrity using TPM 2.0 for a hardware root of trust and Secure Boot. TPM2.0 and Secure boot are required for Windows Server hardware certification. To learn more, see Microsoft raises the security standard for next major Windows Server release
- Secured-core server: Recommended for systems and industries requiring higher levels of assurance. Secured-core server builds on the previous features and uses advanced processor capabilities to provide protection from firmware attacks.

The following table shows how each security concept and feature are used to create a Secured-core server.

Expand table

Concept	Feature	Requirement	Recommended baseline	Secured-Core server
Create a hardware backed root of trust				
	Secure Boot	Secure Boot is enabled in the Unified Extensible Firmware Interface (UEFI) BIOS by default.	✓	✓
	Trusted Platform Module (TPM) 2.0	Meet the latest Microsoft requirements for the Trusted Computing Group (TCG) specification.	✓	✓
	Certified for Windows Server	Demonstrates that a server system meets Microsoft's highest technical bar for security, reliability and manageability.	✓	✓
	Boot DMA protection	Support on devices that have the Input/Output Memory Management Unit (IOMMU). For example, Intel VT-D or AMD-Vi.		✓
Defend against firmware level attacks				
	System Guard Secure Launch	Enabled in the operating system with Dynamic Root of Trust for Measurement (DRTM) compatible Intel and AMD hardware.		✓
Protect the OS from execution of unverified code				

Concept	Feature	Requirement	Recommended baseline	Secured-Core server
	Virtualization-based Security (VBS)	Requires the Windows hypervisor, which is only supported on 64-bit processors with virtualization extensions, including Intel VT-X and AMD-v.	✓	✓
	Hypervisor Enhanced Code Integrity (HVCI)	Hypervisor Code Integrity (HVCI)-compatible drivers plus VBS requirements.	✓	✓

Create a hardware backed root of trust

UEFI Secure boot is a security standard that protects your servers from malicious rootkits by verifying your systems boot components. Secure boot verifies a trusted author has digitally signed the UEFI firmware drivers and applications. When the server is started, the firmware checks the signature of each boot component including firmware drivers and the OS. If the signatures are valid, the server boots and the firmware gives control to the OS.

To learn more about the boot process, see Secure the Windows boot process.

TPM 2.0 provides a secure, hardware-backed storage for sensitive keys and data. Every component loaded during the boot process is measured and the measurements stored in the TPM. By verifying the hardware root-of-trust it elevates the protection provided by capabilities like BitLocker, which uses TPM 2.0 and facilitates the creation of attestation-based workflows. These attestation-based workflows can be incorporated into zero-trust security strategies.

Learn more about Trusted Platform Modules and how Windows uses the TPM.

Along with Secure Boot and TPM 2.0, Windows Server Secured-core uses Boot DMA protection on compatible processors that have the Input/Output Memory Management Unit (IOMMU). For example, Intel VT-D or AMD-Vi. With boot DMA protection, systems are protected from Direct Memory Access (DMA) attacks during boot and during the operating system runtime.

Defend against firmware level attacks

Endpoint protection and detection solutions usually have limited visibility of firmware, given that firmware runs underneath of the operating system. Firmware has a higher level of access and privilege than operating system and hypervisor kernel, making it an attractive target for attackers. Attacks targeting firmware undermine other security measures implemented by the operating system, making it more difficult to identify when a system or user has been compromised.

Beginning with Windows Server 2022, System Guard Secure Launch protects the boot process from firmware attacks by using hardware capabilities from AMD and Intel. With processor support for Dynamic Root of Trust for Measurement (DRTM) technology, Secured-core servers put firmware in a hardware-backed sandbox helping to limit the effects of vulnerabilities in highly privileged firmware code. System Guard uses the DRTM capabilities that are built into compatible processors to launch the operating system, ensuring the system launches into a trusted stated using verified code.

Protect the OS from execution of unverified code

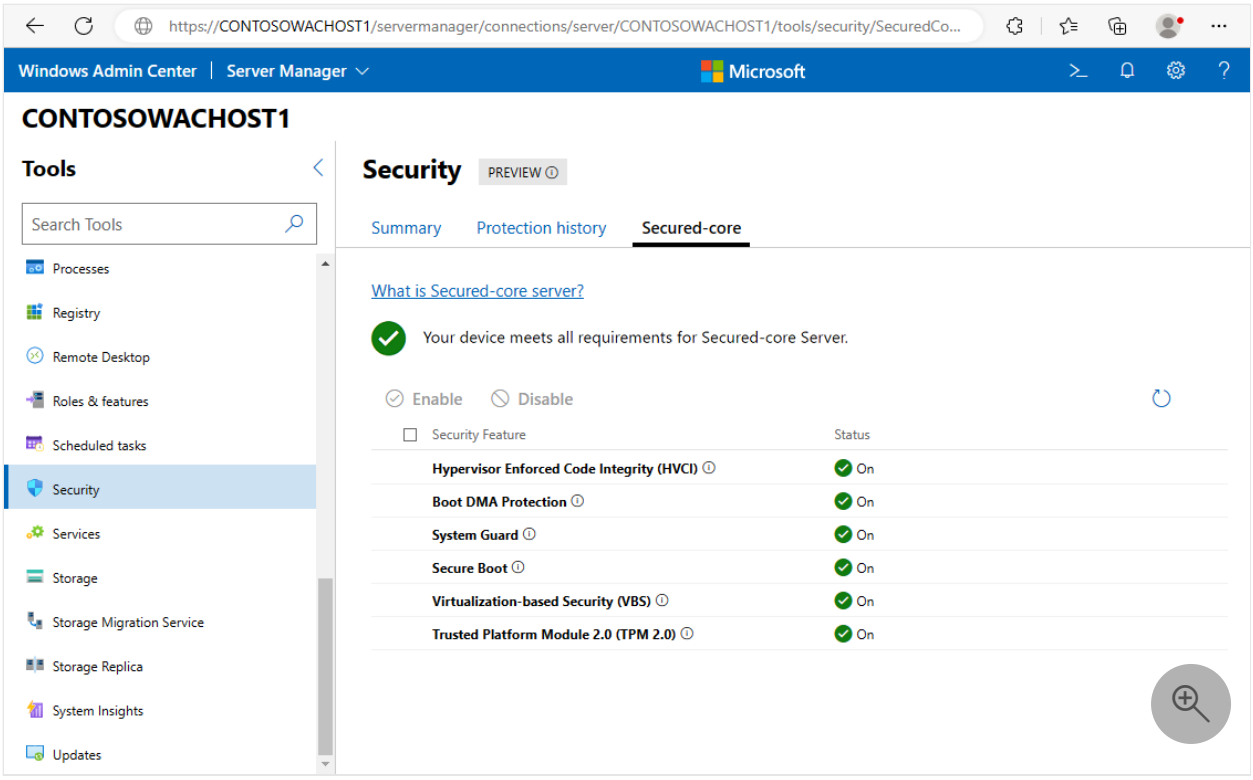
Secured-core server uses Virtualization Based Security (VBS) and hypervisor-protected code integrity (HVCI) to create and isolate a secure region of memory from the normal operating system. VBS uses the Windows hypervisor to create a Virtual Secure Mode (VSM) to offer security boundaries within the operating system, which can be used for other security solutions.

HVCI, commonly referred to as Memory integrity protection, is a security solution that helps ensure that only signed and trusted code is allowed to execute in the kernel. Using only signed and trusted code prevents attacks that attempt to modify the kernel mode code. For example, attacks that modify drivers, or exploits such as WannaCry that attempt to inject malicious code into the kernel.

To learn more about VBS and hardware requirements, see Virtualization-based Security.

Simplified management

You can view and configure the OS security features of Secured-core systems using Windows PowerShell or the security extension in Windows Admin Center. With Azure Stack HCI Integrated Systems, manufacturing partners have further simplified the configuration experience for customers so that Microsoft's best server security is available right out of the box.



Learn more about Windows Admin Center.

Preventative defense

You can proactively defend against and disrupt many of the paths attackers use to exploit systems by enabling Secured-core functionality. Secured-core server enables advanced security features at the bottom layers of the technology stack, protecting the most privileged areas of the system before many security tools are aware of exploits. It also occurs without the need for extra tasks or monitoring by IT and SecOps teams.

Begin your Secured-core journey

You can find hardware certified for Secured-core server from the Windows Server Catalog, and Azure Stack HCI servers in the Azure Stack HCI Catalog. These certified servers come fully equipped with industry-leading security mitigations built into the hardware, firmware, and the operating system to help thwart some of the most advanced attack vectors.

Next steps

Now you understand what Secured-core server is, here are some resources to get you started. Learn about how:

- Configure Secured-core server.

- Microsoft brings advanced hardware security to Server and Edge with Secured-core in the Microsoft Security Blog.
- New Secured-core servers are now available from the Microsoft ecosystem to help secure your infrastructure in the Microsoft Security Blog.
- Building Windows-compatible devices, systems, and filter drivers across all Windows Platforms in Windows Hardware Compatibility Program Specifications and Policies.