Azure Stack HCI: Secured-Core Server

Leverage your Azure Stack HCI investment to run workloads on a highly secure infrastructure by choosing the hardware designed for Secured-core Server, with unparalleled levels of host security enabled with TPM2.0, Secure boot, virtualization-based security (VBS), boot DMA guard, and DRTM protection. The security extension for Windows Admin Center provides the easiest and simplest way to enable, monitor and maintain the fully protected posture of Secured-core Server hosts. Below, you will find a how-to guide for building an infrastructure for the Secured-core Server on Azure Stack HCI.

Overview of Secured-core Server scenario

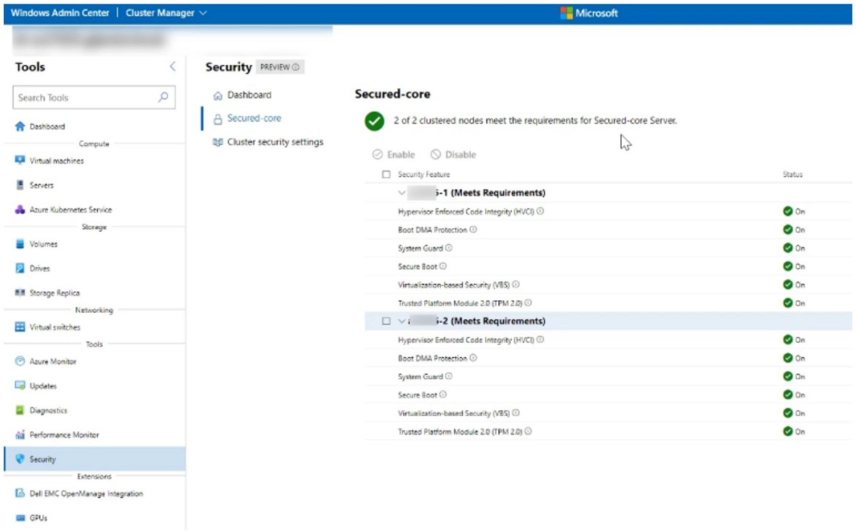
There are two clear trends emerging in the server space today. First, organizations around the world are embracing digital transformation using technologies across cloud and edge computing to better serve their customers and thrive in fast-paced environments. Second, attackers are constantly innovating new attacks as technology changes and targeting these organizations' high-value infrastructure with advanced technical capabilities connected to both cybercrime and espionage. The MagBo marketplace, which sells access to more than 43,000 hacked servers, exemplifies the ever-expanding cybercrime threat. Compromised servers are being exploited to mine cryptocurrency and are being hit with ransomware attacks.

Given these factors, continuing to raise the security bar for critical infrastructure against attackers and make it easy for organizations to hit that higher bar is a clear priority for both customers and Microsoft. Using our learnings from the Secured-core PC initiative, Microsoft is collaborating with partners to expand Secured-core to Azure Stack HCI.

Following Secured-core PC, we are introducing Secured-core Server which 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 new security extension in the Windows Admin Center makes it easy for customers to configure the OS security features of Secured-core for Azure Stack HCI systems. will allow enabling advanced security with a click of the button from a web browser anywhere in the world. 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.



[redacted]

Secured-core

2 of 2 clustered nodes meet the requirements for Secured-core Server.

□ Security Feature	Status
[redacted]-1 (Meets Requirements)	
Hypervisor Enforced Code Integrity (HVCI)	On
Boot DMA Protection	On
System Guard	On
Secure Boot	On
Virtualization-based Security (VBS)	On
Trusted Platform Module 2.0 (TPM 2.0)	On
□ [redacted]-2 (Meets Requirements)	
Hypervisor Enforced Code Integrity (HVCI)	On
Boot DMA Protection	On
System Guard	On
Secure Boot	On
Virtualization-based Security (VBS)	On
Trusted Platform Module 2.0 (TPM 2.0)	On

Advanced protection

Secured-core Servers 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 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 the 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 uptick in firmware vulnerabilities, in large part due to the higher level of privileges that firmware runs combined with limited visibility into firmware by traditional anti-virus solutions. Using processor support for Dynamic Root of Trust of Measurement (DRTM) technology, Secured-core systems put firmware in a hardware-based sandbox helping to limit the impact of vulnerabilities in millions of lines of highly privileged firmware code. Along with pre-boot DMA protection, Secured-core systems provide protection throughout the boot process.
- **Virtualization-based security (VBS):** Secured-core Server support VBS and hypervisor-based code integrity (HVCI). The cryptocurrency mining attack mentioned earlier leveraged the EternalBlue exploit. VBS and HVCI help protect against this entire class of vulnerabilities by isolating privileged parts of the OS, like the kernel, from the rest of the system. This helps to ensure that servers remain devoted to running critical workloads and helps 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. This set of defenses also enables IT and SecOps teams better leverage their time across the many areas that need their attention.

How to deploy Secured-core Server enabled Azure Stack HCI

1. Plan Hardware Deployment

   DataON Integrated Systems for Azure Stack HCI are certified for the Secured-core Server Additional Qualification, which means the products are capable of providing the following functionalities:

   - TPM2.0
   - Secure boot
   - Virtualization based security
   - Hypervisor-protected code integrity
   - Pre-boot DMA protection
   - DRTM protection

2. Deploy Secured-core Server enabled Azure Stack HCI
   - **Step by Step guide** to deploying Azure Stack HCI.
   - Also install Windows Admin Center for managing Azure Stack HCI.

3. Optionally, from Windows Admin Center, you can set up Azure Security Center to add threat protection and quickly assess your security posture of your workloads.
   - You can also setup additional Azure Hybrid Services such as Backup, File Sync, Site Recovery, Point-to-Site VPN, Update Management, and Azure Monitor in WAC.

Summary

With the completion of the Azure Stack HCI Secured-core Server deployment, you have a platform with the highest security standards for protecting security sensitive workloads on both physical and virtual machines.