

# 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

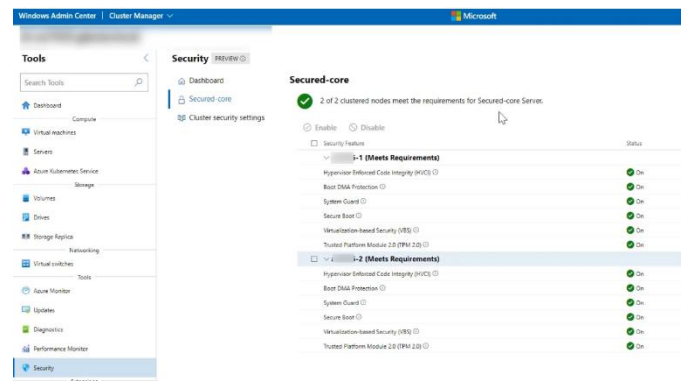
There are two clear trends emerging in the server space today. First, organizations around the world are embracing digital transformation using technologies across cloud and edge computing to better serve their customers and thrive in fast-paced environments. Second, attackers are constantly innovating 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, and it 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.



## 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

# AZURE STACK HCI: SECURED-CORE SERVER

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.

## DataON Integrated Systems for Azure Stack HCI

DataON Integrated Systems for Azure Stack HCI are designed for remote office/branch offices, edge, and IoT deployments. These deployments can present a challenge for IT departments because of constrained budgets, space and power footprints, and limited IT resources.

Integrated Systems provide a fully integrated appliance-like hybrid cloud experience, delivering the fastest time-to-value through the convenience of pre-installed software, integrated drivers, and firmware updates. Simple to deploy and procure, they're ideal for customers who require turnkey solutions with little deployment effort from IT staff.

DataON Integrated Systems can be optimized for high performance with all-NVMe storage or balanced capacity and storage with flexible hybrid NVMe cache and SSD/HDD storage. With Azure Stack HCI, customers can get great resiliency with nested two-way mirroring.

DataON is an exclusive Microsoft partner, with over 100 Integrated Systems and validated nodes in the Microsoft Azure Stack HCI Catalog, as well as over 1000 HCI clusters and 150PB of storage deployed. DataON is a Microsoft Gold Partner, Microsoft Cloud Service Provider (CSP), and an Intel Strategic OEM Partner.

## DataON MUST and MUST Pro for Windows Admin Center

DataON MUST and MUST Pro are included with DataON Integrated Systems. DataON MUST provides real-time monitoring & alerts for Azure Stack HCI. It features a centralized dashboard, historic data reporting, enhanced disk mapping, email alerts, and call home services. MUST Pro integrates with Microsoft's cluster aware updating (CAU) functionality to simplify deployment and updates to Azure Stack HCI, with minimal disruptions to your infrastructure. It checks and ensures that servers have the same OS version, drivers, firmware, BIOS, and BMC. It also checks the drivers

# AZURE STACK HCI: SECURED-CORE SERVER

and firmware for network cards, host bus adapters, and SSD and HDD drives. With a single click, your entire cluster can be updated, helping to you secure against the latest server exploits.

## How to deploy Secured-core Server enabled Azure Stack HCI

### 1. Plan Hardware Deployment

DataON AZS-108 Integrated Systems for Azure Stack HCI are optimized for size & performance, with 2nd Generation Intel® Xeon® Scalable processors and all-NVMe flash storage.


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

1. TPM2.0
2. Secure boot
3. Virtualization Based Security
4. Hypervisor-protected Code Integrity
5. Pre-boot DMA protection
6. DRTM protection



DataON AZS-6112	DataON AZS-6212	DataON AZS-6224	DataON AZS-108	DataON AZS-212	DataON AZS-216
Optimized for size & performance	Optimized for IOPS & capacity	Optimized for IOPS & performance	Optimized for size & performance	Optimized for IOPS & capacity	Optimized for IOPS & performance
2 to 16 Nodes			2 to 16 Nodes		
All-NVMe flash storage	Hybrid storage	All-NVMe flash storage	All-NVMe flash storage	Hybrid storage	All-NVMe flash storage
1U / 1-Node Rack 12x 2.5" Bays	2U / 1-Node Rack 2x 2.5"/3.5" NVMe + 10x 3.5" SAS/SATA	2U / 1-Node Rack 24x 2.5" Bays	1U / 1-Node Rack 8x 2.5" Bays	2U / 1-Node Rack 12x 3.5" Bays	2U / 1-Node Rack 16x 2.5" Bays
<b>3rd Generation</b> Intel® Xeon® Scalable processors			<b>2nd Generation</b> Intel® Xeon® Scalable processors		
Up to 12TB DDR4			128GB to 1.5TB DDR4		
Intel® NVMe SSDs			Intel® NVMe SSDs		
25GbE RDMA networking			25GbE RDMA networking		

# AZURE STACK HCI: SECURED-CORE SERVER

2. Deploy Secured-core Server enabled Azure Stack HCI
  - **Step by Step guide** to [deploy Azure Stack HCI](#). Also install [Windows Admin Center \(WAC\)](#) for managing Azure Stack HCI.
3. Optionally, from Windows Admin Center (WAC), 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.

[www.dataonstorage.com](http://www.dataonstorage.com) | 1-888-725-8588 | [sales@dataonstorage.com](mailto:sales@dataonstorage.com)

Copyright © 2022 DataON. All Rights Reserved. Specifications may change without notice. DataON is not responsible for photographic or typographical errors. DataON, the DataON logo, MUST, and the MUST logo are trademarks of DataON in the United States and certain other countries. Other company, product, or services names may be trademarks or service marks of others.

04/22