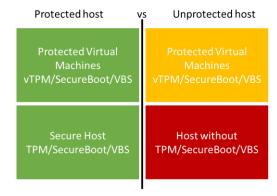# AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

Leverage your Azure Stack HCI investment to run workloads on a highly secure infrastructure by choosing the hardware designed for the Trusted enterprise virtualization scenario, with unparalleled levels of operating system security enabled with virtualization-based security (VBS) and hybrid cloud capabilities made easy through Windows Admin Center and Azure portal.

Below, you will find a how-to guide for building an infrastructure for the Trusted enterprise virtualization scenario on Azure Stack HCI.

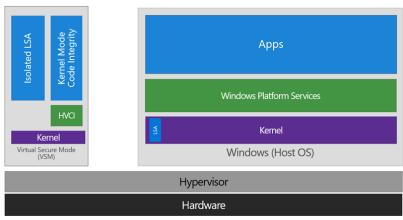## Overview of Trusted enterprise virtualization scenario

Virtualization-based security (VBS) is a key component of the security investments in Azure Stack HCI to protect hosts and virtual machines from security threats.

For example, the Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems, and lists VBS and hypervisor-protected-code-integrity (HVCI) as general security requirements. It is imperative to use host hardware that is VBS and HVCI enabled, in order for the protected workloads on virtual machines to fulfil their security promise because protection of virtual machines is not guaranteed on a compromised host.

VBS uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system. Windows can use this "virtual secure mode" to host a number of security solutions, providing them with greatly increased protection from vulnerabilities in the operating system, and preventing the use of malicious exploits which attempt to defeat protections.

VBS uses the Windows hypervisor to create this "virtual secure mode", and to enforce restrictions which protect vital system and operating system resources, or to protect security assets such as authenticated user credentials. With the increased protections offered by VBS, even if malware gains access to the operating system kernel the possible exploits can be greatly limited and contained, because the hypervisor can prevent the malware from executing code or accessing platform secrets.

One such security solution example is HVCI, which uses VBS to significantly strengthen code integrity policy enforcement. Kernel mode code integrity checks all kernel mode drivers and binaries before they are started and prevents unsigned drivers or system files from being loaded into system memory.

HVCI leverages VBS to run the code integrity service inside a virtual secure mode, providing stronger protections against kernel viruses and malware. The hypervisor, the most privileged level of system software, sets and enforces page

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

permissions across all system memory. Pages are only made executable after code integrity checks inside the virtual secure mode have passed, and executable pages are not writable. That way, even if there are vulnerabilities like buffer overflow that allow malware to attempt to modify memory, code pages cannot be modified, and modified memory cannot be made executable.

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 and firmware for network cards, host bust 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 VBS and HVCI-enabled Azure Stack HCI

1. Plan Hardware Deployment

    DataON AZS-6112 Integrated Systems for Azure Stack HCI are optimized for size & performance, with 3rd Generation Intel® Xeon® Scalable processors and all-NVMe flash storage.

    All the Azure Stack HCI solutions from DataON are certified for the Hardware Assurance Additional Qualification, which tests for all the functionality needed for VBS. However, VBS and HVCI are not automatically enabled in Azure Stack HCI and Step 2 will guide you on how to enable them.

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

Warning: Hypervisor-protected code integrity (HVCI) may be incompatible with devices not listed in the Azure Stack HCI catalog. Microsoft strongly recommends using an Azure Stack HCI validated solution from our hardware partners for the Trusted enterprise virtualization scenario.

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
3rd Generation Intel® Xeon® Scalable processors				2nd Generation 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		

2. Deploy VBS-Enabled Azure Stack HCI

   Step by Step guide to deploy Azure Stack HCI. Also install Windows Admin Center (WAC) for managing Azure Stack HCI.
   Enable virtualization-based protection of code integrity

3. From Windows Admin Center (WAC), set up Azure Security Center to add threat protection and quickly assess your security posture of your workloads.

   - You can also setup additional 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 Trusted enterprise virtualization deployment and the configuration of VBS / HVCI, you now have a platform with the highest security standards for protecting security sensitive workloads on both physical and virtual machines.

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

www.dataonstorage.com | 1-888-725-8588 | sales@dataonstorage.com

04/22

DataON | Microsoft Azure