

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

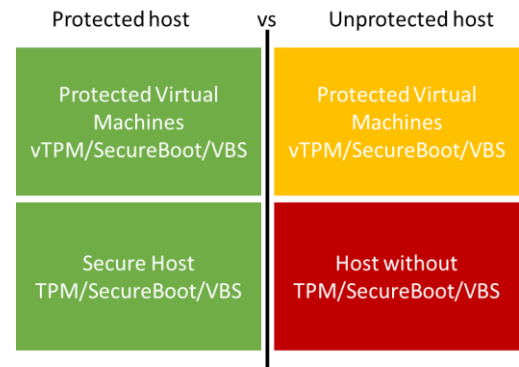
Leverage your Azure Stack HCI investment to run workloads on a highly secure infrastructure by choosing the hardware designed for the Trusted enterprise virtualization scenario, with unparalleled levels of operating system security enabled with virtualization-based security (VBS) and hybrid cloud capabilities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

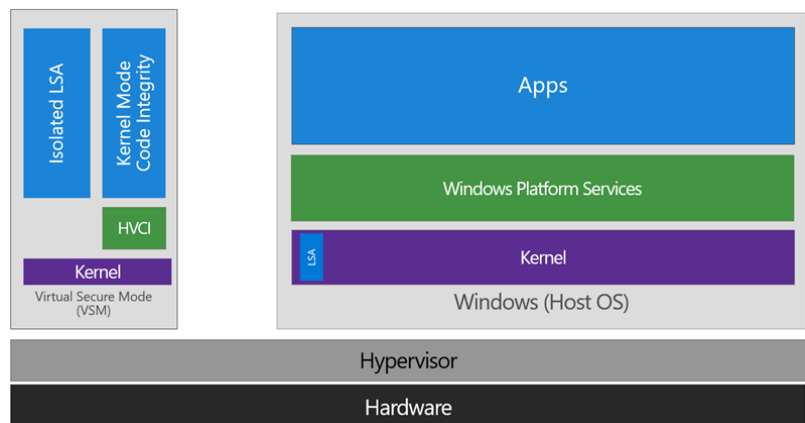
Virtualization-based security (VBS) is a key component of the [security investments in Azure Stack HCI](#) to protect hosts and virtual machines from security threats.

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 permissions across all system memory. Pages are only made executable after code integrity checks inside the virtual

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

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 Kepler Switchless Validated Nodes for Azure Stack HCI

DataON Kepler Switchless solutions 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.

Available in 2- and 3-node versions, DataON Kepler validated nodes for Azure Stack HCI feature switchless back-to-back networking for peak simplicity and affordability. They feature innovative technologies that set Azure Stack HCI apart at the small scale. Nested resiliency protects you from multiple concurrent failures. Cloud quorum technologies can leverage Azure instead of an appliance virtual machine for a quorum. Kepler 3-node (K3N) solutions provide an additional layer of resiliency over Kepler 2-node (K2N) solutions, essential in environments or multiple ROBO and edge deployments that require 3-way mirror fault tolerance.

DataON Kepler validated nodes provide a reference-architecture-like experience, with the broadest choice of hardware components. Validated nodes combine Intel® technology and Azure Stack HCI software to provide a powerful platform for data center modernization. Together they enable organizations to modernize their infrastructure, start or extend their hybrid cloud journey, and consolidate virtualized workloads.

DataON is an exclusive Microsoft partner, with 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 for Windows Admin Center

DataON MUST is included with DataON validated nodes. 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.

How to deploy VBS and HVCI-enabled Azure Stack HCI

1. Plan Hardware Deployment

All 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.

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.

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION




DataON K2N-6104	DataON K2N-6112	DataON K2N-6208	DataON K2N-6212	DataON K2N-6216	DataON K2N-6224
Optimized for size & performance	Optimized for size & performance	Optimized for performance & expansion	Optimized for IOPS & capacity	Optimized for IOPS & performance	Optimized for IOPS & performance
2 to 16 Nodes					
All-NVMe flash storage	All-NVMe flash storage	All-NVMe flash storage	Hybrid storage	All-NVMe flash storage	All-NVMe flash storage
1U / 1-Node rack 4x 2.5" Bays	1U / 1-Node Rack 12x 2.5" Bays	2U / 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 16x 2.5" Bays	2U / 1-Node Rack 24x 2.5" Bays
3rd Generation Intel® Xeon® Scalable processors					
Up to 12TB DDR4					
Intel® NVMe SSDs					
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  **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 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.

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