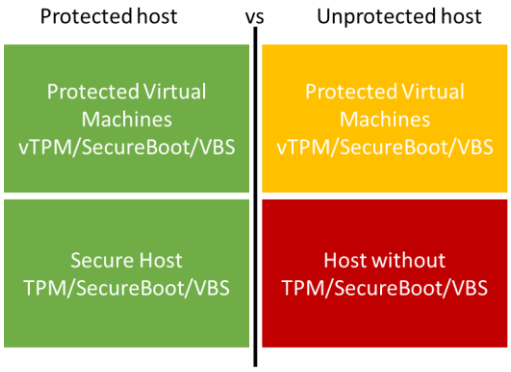
AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

Leverage your Azure Stack HCI investment to run workloads on a highly secure infrastructure by choosing the Lenovo 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

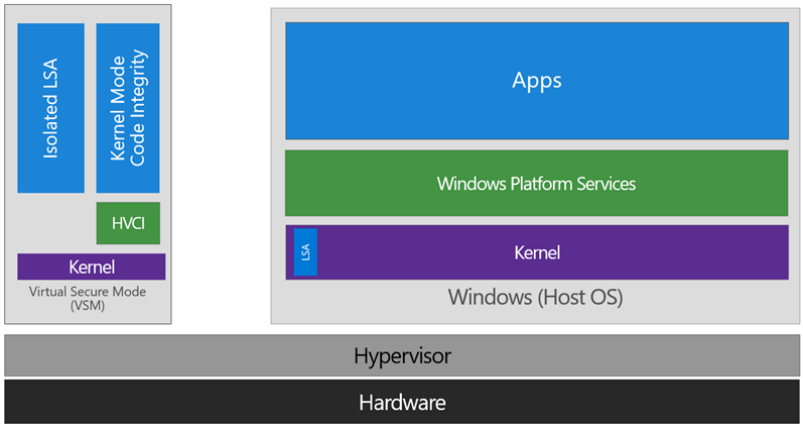
Virtualization-based security (VBS) is a key component of the security investments in Azure Stack HCI to protect hosts and virtual machines from security threats.

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 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.

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

How to deploy VBS and HVCI-enabled Azure Stack HCI

1. Plan Hardware Deployment

All the Azure Stack HCI solutions by Lenovo 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.

Lenovo certified Azure Stack HCI solutions can be found at this link – ThinkAgile MX.

The following Lenovo servers have been certified for Microsoft Azure Stack HCI and are shipped with TPM (Trusted Platform Module) by default making them ideal candidates for Azure Stack HCI trusted enterprise virtualization solutions:

- Lenovo ThinkSystem SR650
  - Lenovo ThinkAgile MX3520 appliances also referred to as Integrated systems are built using SR650 and are preloaded with Microsoft Azure Stack HCI operating system. Lenovo ThinkAgile appliances offer ThinkAgile Advantage Single Point of Support for quick 24/7 problem reporting and resolution.
  - Lenovo ThinkAgile MX certified nodes also referred to as validated nodes are built using SR650 and are available to be preloaded with Azure Stack HCI operating system.
- Lenovo ThinkSystem SR650 V2
  - Lenovo ThinkAgile MX3530 appliances also referred to as Integrated systems are built using SR650 V2 and are preloaded with Microsoft Azure Stack HCI operating system. Lenovo ThinkAgile appliances offer ThinkAgile Advantage Single Point of Support for quick 24/7 problem reporting and resolution.
  - Lenovo ThinkAgile MX3531 certified nodes also referred to as validated nodes are built using SR650 V2 and are available to be preloaded with Azure Stack HCI operating system.
- Lenovo ThinkSystem SR630 V2
  - Lenovo ThinkAgile MX3330 appliances also referred to as Integrated systems are built using SR630 V2 and are preloaded with Microsoft Azure Stack HCI operating system. Lenovo ThinkAgile appliances offer ThinkAgile Advantage Single Point of Support for quick 24/7 problem reporting and resolution.
  - Lenovo ThinkAgile MX3311 certified nodes also referred to as validated nodes are built using SR630 V2 and are available to be preloaded with Azure Stack HCI operating system.
- Lenovo ThinkSystem SE350
  - Lenovo ThinkAgile MX1020 appliances also referred to as Integrated systems are built using SE350 and are preloaded with Microsoft Azure Stack HCI operating system
  - Lenovo ThinkAgile MX1021 certified nodes also referred to as validated nodes are built using SE350 and are available to be preloaded with Azure Stack HCI operating system.
- Lenovo ThinkSystem SR630
  - Lenovo ThinkSystem SR630 servers are certified for Microsoft Azure Stack HCI with Azure Stack HCI operating system.
- Lenovo ThinkSystem SR665 and SR645
  - Lenovo ThinkSystem SR665 and SR635 2-socket servers are built with AMD EPYC 7003 series processors and are certified for Microsoft Azure Stack HCI with Azure Stack HCI operating system.

- Lenovo ThinkSystem SR655 and SR635
  - Lenovo ThinkSystem SR665 and SR635 1-socket servers are built with AMD EPYC 7003 series processors and are certified for Microsoft Azure Stack HCI with Azure Stack HCI operating system.

The Lenovo Azure Stack HCI solutions are built on ThinkSystem servers that offer the following security features:

- Power-on password
- Administrator's password
- Secure firmware updates
- Onboard Trusted Platform Module (TPM) version 1.2 or 2.0 (configurable UEFI system setting)
- Trusted Cryptographic Module (TCM) (optional; PRC only)
- Nationz Trusted Platform Module v2.0 (optional; PRC only)
- Lockable front bezel (optional)
- Security Key Lifecycle Manager (SKLM) encryption key management for SEDs - FoD upgrade (optional)
- Lenovo Business Vantage security software (optional; PRC only)

Steps to enable TPM and Secure Boot can be found in the maintenance manual starting at page #258.

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 Lenovo ThinkAgile MX for Azure Stack HCI platform with the highest security standards for protecting security sensitive workloads on both physical and virtual machines.