**Technical Use Cases
For Azure Stack HCI**

| Branch office and edge | Virtual desktop infrastructure | High-performance Microsoft SQL Server | Trusted enterprise virtualization | Scale-out storage |

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.
Below, you will find a how-to guide for building an infrastructure for the Trusted enterprise virtualization scenario on Azure Stack HCI that includes:
-    Overview of Trusted enterprise virtualization scenario
-    Step by step guidance of deploying VBS-enabled Azure Stack HCI and Azure Security Center via Windows Admin Center
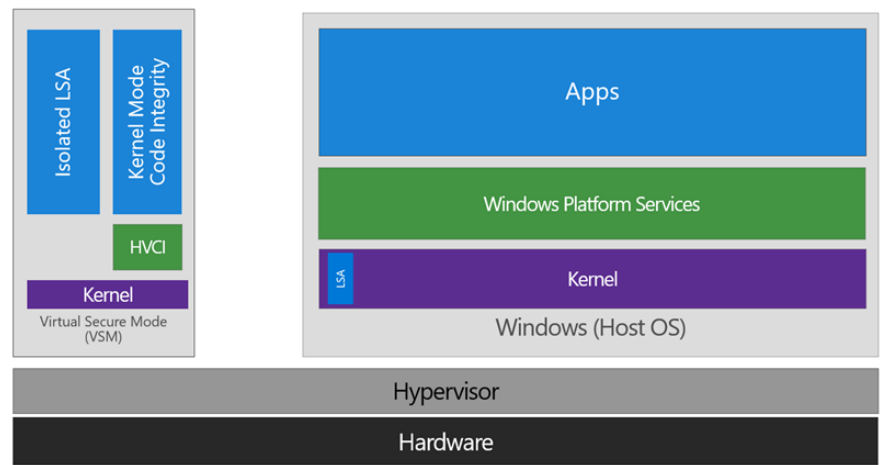
Overview of Trusted enterprise virtualization scenario

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 Windows Server 2019 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.
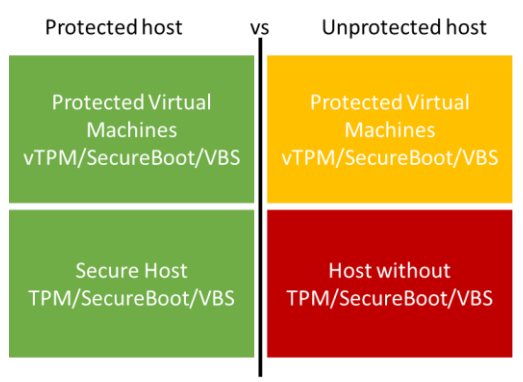
VBS uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system. Windows can use this "virtual secure mode" to host a number of security solutions, providing them with greatly increased protection from vulnerabilities in the operating system, 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.

Stone Computers Ltd.

One such example security solution 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're 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.

How to deploy VBS and HVCI-enabled Azure Stack HCI

1. Plan Hardware Deployment

    All the Elysium SF Azure Stack HCI solutions by Stone Computers Ltd. 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 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 one of our hardware partners at https://www.microsoft.com/en-us/cloud-platform/azure-stack-hci-catalog for the Trusted enterprise virtualization scenario.

    The Elysium SF from Stone Computers as standard is configured with the necessary hardware and UEFI settings to enable Trusted enterprise virtualization, including TPM 2.0, VBS and Secure Boot. You can verify these settings by entering UEFI setting and checking the Advanced > Security menu. All Stone Computers Elysium SF platforms benefit from having the latest approved UEFI firmware installed in our configuration facility prior to shipping, however updates are available here.

2. Deploy VBS-Enabled Azure Stack HCI
    -   Deploy Azure Stack HCI
        Step by Step guide to deploy Azure Stack HCI
        1. Install Windows Server 2019 Datacenter
        2. Add Roles and Features
        3. Setup Failover Clustering and enable a Cluster Witness
        4. Setup Storage Spaces Direct
    -   Enable virtualization-based protection of code integrity

3. Set up Azure Security Center through WAC
    -   Install Windows Admin Center (WAC)
    -   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.

Resources

- [Windows Server Security and Assurance](#)
- [Microsoft Security Compliance Toolkit](#)
- [Windows 10 Enterprise Security](#)
- [Top 10 ways to secure Office 365 and Microsoft 365 Business plans](#)

Stone Computers Elysium SF Product Features

Overview

- Massive scalability with up to 1.6PB of capacity and 704 Physical Processor Cores
- Tailored solution from 4 nodes up to 16 nodes in a single solution
- Datacenter features, performance and reliability
- Rapid deployment – every Elysium is built and tested, fully ready to run out of the box
- Harness the power of the latest generations of processor technology and NVMe acceleration
- Utilize brand new Microsoft Windows Server 2019 features such as CSV level Deduplication, Windows Admin Center and active drive health monitoring
- High bandwidth, low latency interconnect - each node has access to 200Gbit of throughput
- Supports Hardware Encryption with TPM 2.0
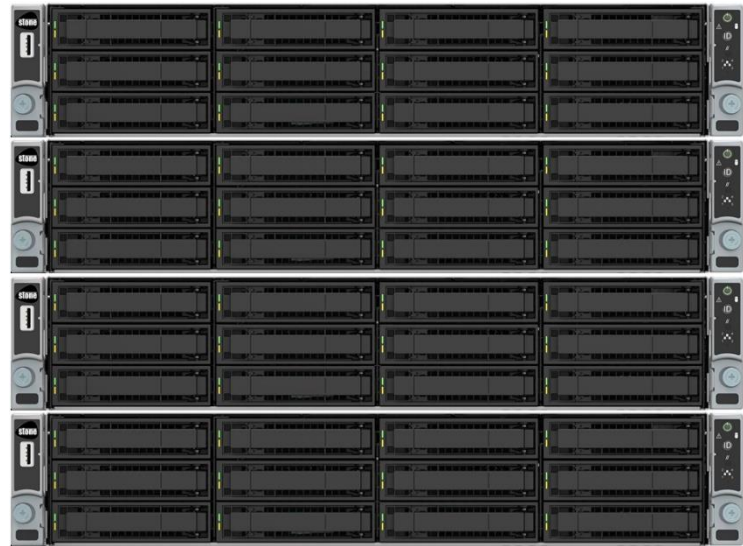
Platform

- 4 to 16 Node Dual-Intel® Xeon® processor platform with the latest processors and features
- Support for up to 1.5TB RAM per node, or 24TB RAM per cluster

Acceleration

- Lighting fast NVMe accelerated storage – typical performance > 3.0M IOPS
- Uses RDMA technology to ensure rapid data flow between nodes, delivering best in class storage system performance

Support

- Factory pre-configuration services
- UK Based technical support with 24/7 access to the Stone support portal
- 5 Years On-site Warranty as standard with options for 7 year and 24x7 helpdesk

For more information, see the [Stone Elysium SF Product Datasheet](#).

Summary

With 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.