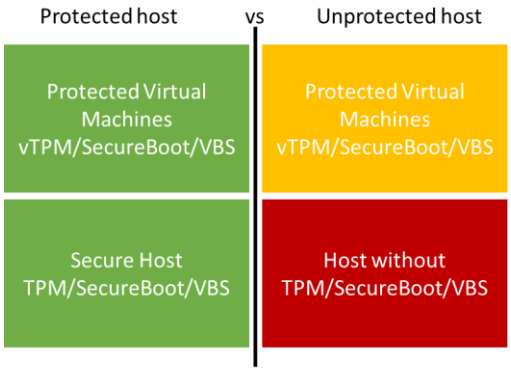
AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

Nutzen Sie Ihre Azure Stack HCI-Investitionen, um Workloads in einer hochsicheren Infrastruktur laufen lassen, indem Sie die Hardware aussähen, die für das Virtualisierungsszenario "Vertrauenswürdiges Unternehmen" entwickelt wurde, wobei die Betriebssystemsicherheit mit VIRTUALisierungsbasierter Sicherheit (VBS) und Hybrid-Cloud-Funktionen, die über Windows Admin Center und das Azure-Portal erleichtert sind.
Nachfolgend finden Sie eine Anleitung zur Erstellung einer Infrastruktur in Azure Stack HCI.

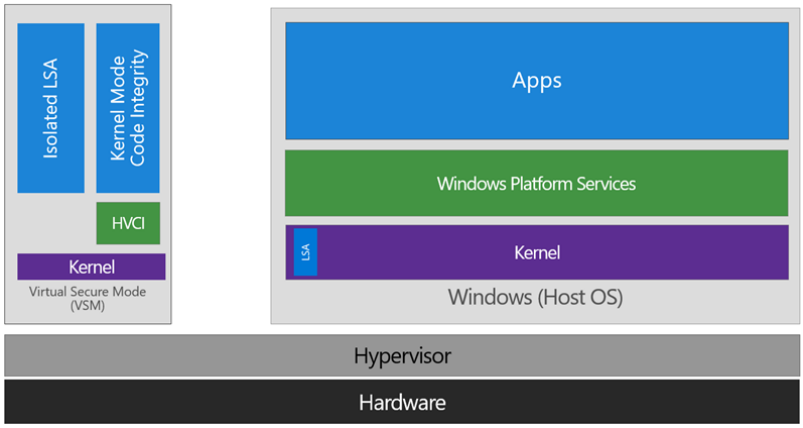
Überblick über das Virtualisierungsszenario

Virtualisierungsbasierte Security (VBS) ist eine wichtige Komponente der Sicherheitsinvestitionen in Azure Stack HCI, um Hosts und virtuelle Maschinen vor Sicherheitsbedrohungen zu schützen.
Beispielsweise wird der Security Technical Implementation Guide (STIG) als Tool zur Verbesserung der Sicherheit von DoD-Informationssystemen (Department of Defense) veröffentlicht und listet VBS und Hypervisor-protected-code-integrity (HVCI) als allgemeine Sicherheitsanforderungen auf. Es ist notwendig, Hosthardware zu verwenden, die VBS- und HVCI-fähig ist, damit die geschützten Workloads auf virtuellen Maschinen ihr Sicherheitsversprechen erfüllen, da der Schutz virtueller Maschinen auf einem kompromittierten Host nicht gewährleistet ist.



VBS verwendet Hardwarevirtualisierungsfunktionen, um einen sicheren Speicherbereich vom normalen Betriebssystem zu erstellen und zu isolieren. Windows kann diesen "virtuellen sicheren Modus" verwenden, um eine Reihe von Sicherheitslösungen zu hosten, ihnen einen stark erhöhten Schutz vor Sicherheitslücken im Betriebssystem zu bieten und die Verwendung böswilliger Exploits zu verhindern, die versuchen Schutzmaßnahmen zu verhindern.

VBS verwendet den Windows-Hypervisor um diesen "virtuellensicheren Modus" zu erstellen und Einschränkungen zu erzwingen, die wichtige System- und Betriebssystemressourcen schützen, oder um Sicherheitsressourcen wie authentifizierte Benutzeranmeldeinformationen zu schützen. Mit dem erhöhten Schutz durch VBS, auch wenn eine Malware einen Zugriff auf das Betriebssystem-Kernel hat, die möglichen Exploits können stark eingeschränkt und enthalten sein, weil der Hypervisor kann die Malware von der Ausführung von Code oder Zugriff auf Plattform Geheimnisse zu verhindern.



Ein Beispiel für eine solche Sicherheitslösung ist HVCI, das VBS verwendet, um die Durchsetzung von Richtlinien für die Codeintegrität erheblich zu stärken. Die Codeintegrität des Kernelmodus überprüft alle Kernelmodustreiber und Binärdateien, bevor sie gestartet werden, und verhindert, dass nicht signierte Treiber oder Systemdateien in den Systemspeicher geladen werden.

primeLine SOLUTIONS
primeLine Solutions GmbH, Zur Bauernwiese 25, 32549 Bad Oeynhausen
Telefon: +49 5731 8694-450 E-Mail: vertrieb@primeline.org

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

HVCI nutzt VBS, um den Codeintegritätsdienst in einem virtuellen sicheren Modusauszuführen und bietet einen stärkeren Schutz vor Kernelviren und Malware. Der Hypervisor, die privilegiertesten Ebene der Systemsoftware, legt Seitenberechtigungen für den gesamten Systemspeicher fest und erzwingt diese. Seiten werden erst ausführbar gemacht, nachdem Codeintegritätsprüfungen im virtuellen sicheren Modus bestanden wurden und ausführbare Seiten nicht beschreibbar sind. Auf diese Weise können Codepages nicht geändert werden, und geänderter Speicher kann nicht ausführbar gemacht werden, selbst wenn es Sicherheitslücken wie Pufferüberlauf gibt, die Malware versuchen, den Arbeitsspeicher zu ändern.

Bereitstellen von VBS- und HVCI-fähigen Azure Stack HCI

1. Hardwarebereitstellung planen

   Alle Azure Stack HCI-Lösungen von primeLine sind für die Hardware Assurance-Zusatzqualifizierung zertifiziert, die alle für VBS erforderlichen Funktionen testet. VBS und HVCI sind jedoch nicht automatisch in Azure Stack HCI aktiviert, und Schritt 2 führt Sie zur Aktivierung.

   Warnung: Die Hypervisor-geschützte Codeintegrität (HVCI) ist möglicherweise nicht kompatibel mit Geräten, die nicht im Azure Stack HCI-Katalog aufgeführt sind. Microsoft empfiehlt dringend die Verwendung einer von Azure Stack HCI validierten Lösung von unseren Hardwarepartnern für das Virtualisierungsszenario vertrauenswürdiger Unternehmen.

1. Die primeLine egino HCI Series A1 SoC Familie unterstützt das Trusted Enterprise Virtualization mit folgenden Modellen:

egino HCI Series A1 12121a-SoC-XN1
egino HCI Series A1 12121a-SoC-XA1

Jeder primeLine egino HCI Server hat Azure Stack HCI, sowie getestete Firmware und Treiber vorinstalliert, eine Konfigurationsanleitung liegt den Systemen bei.

2. Bereitstellen von VBS-aktivierten Azure Stack HCI
   Schritt für Schritt Anleitung zum Bereitstellen von Azure Stack HCI. Installieren Sie auch Windows Admin Center (WAC) für die Verwaltung von Azure Stack HCI.
   Virtualisierungs-basierte minaden Schutz der Codeintegrität ermöglichen

3. Richten Sie von Windows Admin Center (WAC) aus Azure Security Center ein, um Bedrohungsschutz hinzuzufügen und Ihre Sicherheitsposition Ihrer Workloads schnell zu bewerten.

primeLine SOLUTIONS
primeLine Solutions GmbH, Zur Bauernwiese 25, 32549 Bad Oeynhausen
Telefon: +49 5731 8694-450 E-Mail: vertrieb@primeline.org

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

- Sie können auch zusätzliche Azure hybrid services Einrichtungen einrichten, z. B. Backup, Dateisynchronisierung, Standortwiederherstellung, Punkt-zu-Standort-VPN, Updateverwaltung und Azure Monitor in WAC.

Zusammenfassung

Mit dem Abschluss der Azure Stack HCI Trusted Enterprise Virtualization-Bereitstellung und der Konfiguration von VBS / HVCI verfügen Sie jetzt eine Plattform mit den höchsten Sicherheitsstandards zum Schutz sicherheitsrelevanter Workloads auf physischen und virtuellen Maschinen.