Microsoft Azure

Azure Stack HCI Security Book

Layered, built-in security from core to cloud

Security threats are evolving in new ways, new vulnerabilities are emerging for organizations all the time, making it imperative to choose an infrastructure that is protected from these threats. Azure Stack HCI, a Microsoft Azure Arc-enabled infrastructure, is designed and built to help secure workloads, data, and operations with built-in capabilities inspired by Azure hyper scaled security.

Contents

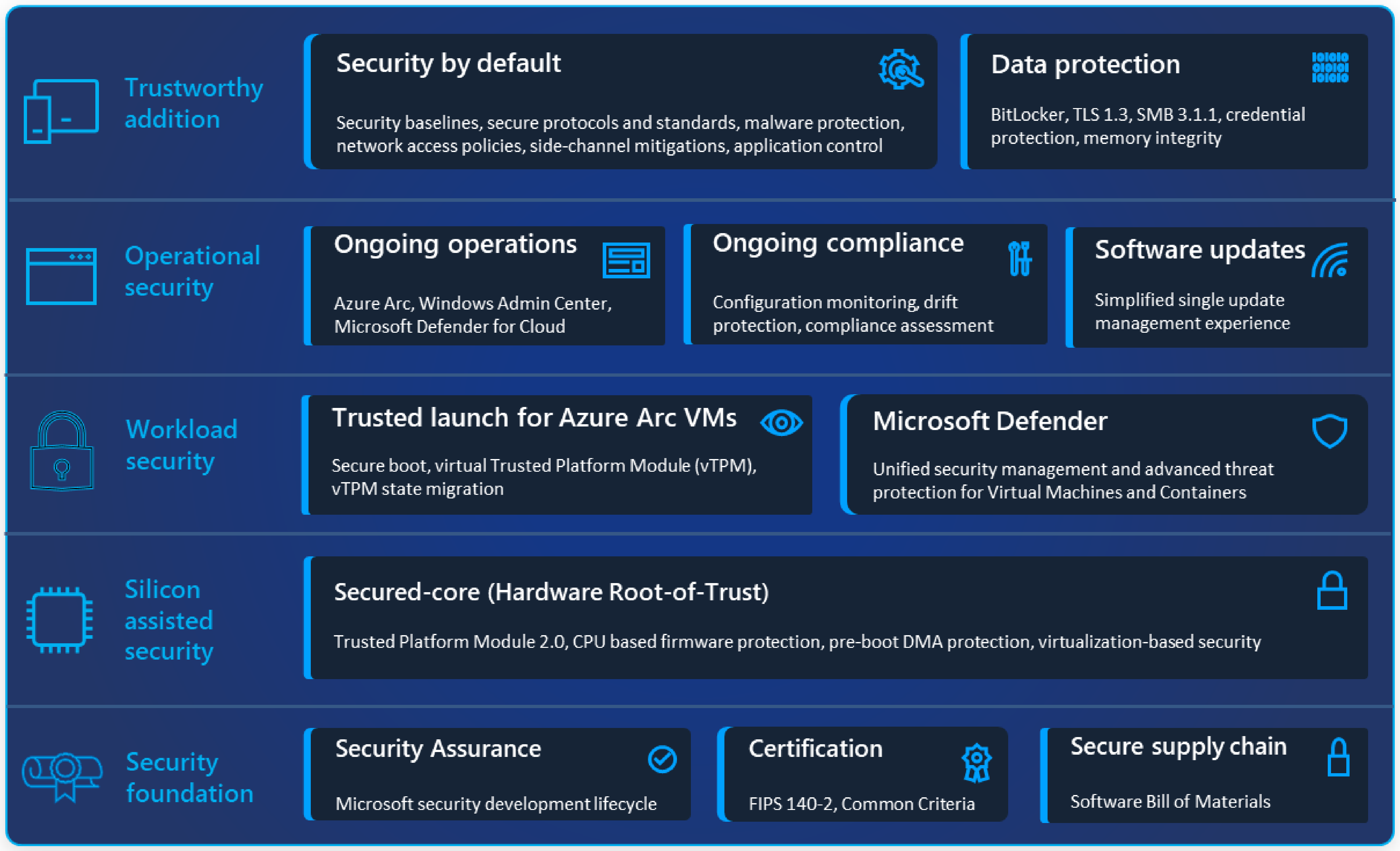
Scope

This security book applies to the new feature version of Azure Stack HCI (generally available on Feb 1, 2024) and above.

Introduction

Security affects everyone in your organization from upper-level management to the information worker. Inadequate security is a real risk for organizations as a security breach can disrupt all normal business and bring your organization to a halt. Information technology infrastructure is susceptible to a wide variety of attacks. Attackers typically take advantage of vulnerabilities in the hardware, firmware, operating system, or the application layer. Once they gain a foothold, they use techniques such as privilege escalation to move laterally to other systems in the organization. Azure Stack HCI supports security capabilities that can help protect as well as detect and respond to such attacks as quickly as possible.

Approximately 80% of security decision makers say that software alone is not enough protection from emerging threats (Microsoft Security Signals). With Azure Stack HCI, both hardware and software work together to help protect sensitive data from the core of your server all the way to the cloud. This level of protection helps keep your organization's data and IT infrastructure secure. See the layers of protection in the following diagram to get a brief overview of our security priorities.



Trustworthy addition

Security by default

Security baselines, secure protocols and standards, malware protection, network access policies, side-channel mitigations, application control

Data protection

BitLocker, TLS 1.3, SMB 3.1.1, credential protection, memory integrity

Operational security

Ongoing operations

Azure Arc, Windows Admin Center, Microsoft Defender for Cloud

Ongoing compliance

Configuration monitoring, drift protection, compliance assessment

Software updates

Simplified single update management experience

Workload security

Trusted launch for Azure Arc VMs

Secure boot, virtual Trusted Platform Module (vTPM), vTPM state migration

Microsoft Defender

Unified security management and advanced threat protection for Virtual Machines and Containers

Silicon assisted security

Secured-core (Hardware Root-of-Trust)

Trusted Platform Module 2.0, CPU based firmware protection, pre-boot DMA protection, virtualization-based security

Security foundation

Security Assurance

Microsoft security development lifecycle

Certification

FIPS 140-2, Common Criteria

Secure supply chain

Software Bill of Materials

Azure Stack HCI is designed to help defend against modern threats and was built to meet the requirements of a wide variety of security standards (see Certifications). The security posture of the Azure Stack HCI infrastructure is built on the following pillars:

- Security, rooted in hardware – Secured-core certified hardware enables strong security rooted in hardware.
- Security, by default – Security baselines and essential security features are enabled by default, right from the start. This ensures that the system is deployed in a known good state.
- Security posture, continuously monitored – Verify that the system remains in a known good state. This is achieved through a protect, detect, and respond framework that allows for continuous monitoring of system security state and remediation of configuration drifts.

Trustworthy addition

Our customers face the significant burden of getting their infrastructure to meet a wide variety of security standards and be compliant with industry specific compliance requirements. They may spend several millions of dollars on external tools to get their infrastructure to meet those requirements. This is a tall order for many customers as they need to identify and enable various security capabilities. Even when they do, how those various security capabilities work together is yet another challenge to deal with.

Our goal is to empower customers to achieve their security requirements, regardless of industry regulations or compliance, more easily and in a flexible manner. Azure Stack HCI builds on industry-leading security features such as Windows Defender Application Control and BitLocker. With Azure Stack HCI, we have enabled security right from the start, where the system is by default deployed in a known good state in accordance with the Microsoft Cloud Security Benchmark.

With this change, customers do not have to burden themselves with the mechanics of enabling the various security capabilities, at least not for most of the well-known security requirements. From a customer standpoint, security "just works".

Security by default

Security baselines and best practices enabled by default

By default, Azure Stack HCI enables security baseline settings and security best practices based on Microsoft recommended security baselines and industry best practices. A tailored security baseline with over 300 security settings is enforced with a drift control mechanism which ensures that the system starts and remains in a known good security state.

This security baseline enables you to closely meet the Center for Internet Security (CIS) Benchmark, Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG), and Federal Information Processing Standards (FIPS 140-2) requirements for the operating system (OS), and Azure Compute Security baselines. The security baseline settings have been verified for compatibility and performance impact. The default enablement of those security baselines is intended to make it easier for customers to meet their compliance and regulatory requirements.

Insecure protocols disabled by default

Insecure protocols such as TLS versions less than 1.2, DTLS versions less than 1.2, SMB 1.0, and WDigest which have inherent vulnerabilities are disabled by default in Azure Stack HCI.

Use of secure protocols and cryptographic standards

Azure Stack HCI uses secure protocols such as Transport Layer Security (TLS) versions 1.2 or higher, Datagram Transport Layer Security (DTLS) versions 1.2 or higher, and Server Messaging Blok (SMB) 2.0 or higher. It supports National Institute of Standards and Technology (NIST) guidelines for cryptographic standards.

Mitigations for speculative side-channel hardware vulnerabilities

Modern CPUs achieve performance by using idle CPU cycles to perform speculative and out of order execution of instructions. For instance, the CPU may predict the target of a branch instruction and speculatively execute the instructions at the predicted branch target.

If the CPU later discovers that the branch prediction was incorrect, all the machine state that was computed speculatively is discarded. However, this operation can leave residual traces in various caches that are used by the CPU. These residual traces can leave observable side effects (side channel) which attackers may be able to use to extract information about private data using a timing attack. Spectre and Meltdown are some of the original transient execution CPU vulnerabilities. Azure Stack HCI enables mitigations for known speculative execution side channel hardware vulnerabilities by default.

Application control

Preventing unwanted or malicious applications from running is an important part of an effective security strategy. Application control is one of the most effective means for addressing the threat of executable file-based malware. Application control helps mitigate security threats by restricting the applications that users are allowed to run.

While most customers inherently understand the value of application control, the reality is that only some have been able to employ application control solutions in a manageable way. Windows Defender Application Control (WDAC) provides powerful control over what applications are allowed to run and the code that runs in the OS (kernel).

WDAC is enabled by default on Azure Stack HCI, and out of the box it includes a set of base policies to ensure that only known platform components and applications are allowed to run. You can extend and customize this application control policy. For more information on base policies included in Azure Stack HCI and how to create supplemental policies, see Windows Defender Application Control for Azure Stack HCI.

Credential protection

Windows Defender Credential Guard uses virtualization-based security (VBS) to protect against credential theft. With Windows Credential Guard, the Local Security Authority (LSA) stores and protects Active Directory secrets in an isolated environment that is not accessible to the rest of the operating system. By protecting the LSA process with virtualization-based security, Windows Defender Credential Guard shields systems from credential theft attack techniques like pass-the-hash or pass-the-ticket. It also helps prevent malware from accessing system secrets even if the process is running with admin privileges. Windows Defender Credential Guard is enabled by default in Azure Stack HCI.

Memory integrity protection

Kernel Mode Code Integrity is the Windows process that checks whether all kernel code is properly signed and has not been tampered with before it is allowed to run. Hypervisor-protected code integrity (HVCI), also called memory integrity, uses virtualization-based security (VBS) to run Kernel Mode Code Integrity inside the secure VBS environment instead of the main Windows kernel. This helps prevent attacks that attempt to modify kernel mode code such as drivers.

Memory integrity also restricts kernel memory allocations that could be used to compromise the system, ensuring that kernel memory pages are only made executable after passing code integrity checks inside the secure VBS environment, and executable pages themselves are never writable. That way, even if there are vulnerabilities like buffer overflow that allows malware to attempt to modify memory, executable code pages cannot be modified, and modified memory cannot be made executable. Memory integrity helps protect against attacks that rely on the ability to inject malicious code into the kernel using bugs in kernel-mode software. Memory integrity protection is enabled by default in Azure Stack HCI.

Data at rest protection

BitLocker Drive Encryption is a data protection feature that addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers or storage components. With Azure Stack HCI, all infrastructure and tenant data is encrypted at rest using BitLocker. Both OS volumes (or system volumes containing the OS VHDX in boot from VHDX scenarios) and Cluster Shared Volumes are by default encrypted with BitLocker using XTS-AES 256-bit encryption algorithm. In situations where BitLocker is unable to unlock a local OS volume or data volume, it will deny access to the encrypted data. To learn more about BitLocker protection, see BitLocker encryption on Azure Stack HCI.

Data in transit protection

Transport layer security (TLS)

Transport Layer Security (TLS) is the internet's most deployed security protocol, encrypting data in transit to provide a secure communication channel between two endpoints. Azure Stack HCI enables the latest protocol versions and strong cipher suites by default and offers a full suite of extensions such as client authentication for enhanced server security, or session resumption for improved application performance. TLS 1.3 is the latest version of the protocol and is enabled by default in Azure Stack HCI. This version eliminates obsolete cryptographic algorithms, enhances security over older versions, and aims to encrypt as much of the TLS handshake as possible. The handshake is more performant with one fewer round trip per connection on average and supports only strong cipher suites which provide perfect forward secrecy and less operational risk. Using TLS 1.3 will provide more privacy and lower latencies for encrypted online connections. Note that if the client or server application on either side of the connection does not support TLS 1.3, Azure Stack HCI will fall back to TLS 1.2. Azure Stack HCI uses the latest Datagram Transport Layer Security (DTLS) 1.2 for UDP communications.

Server Messaging Block (SMB) signing and encryption

All the major security industry baselines recommend enabling Server Message Block (SMB) signing. To make it easier for you to get your infrastructure to be compliant with those baselines and best practices, we are enabling SMB signing requirement for client connections by default in Azure Stack HCI. SMB encryption of intra-cluster traffic is not enabled by default but is an option you can enable during or after deployment. SMB encryption can impact performance depending on the system configuration.

For signing and encryption security, Azure Stack HCI now supports AES-256-GCM and AES-256-CCM cryptographic suites for the SMB 3.1.1 protocol used by client-server file traffic as well as the intra-cluster data fabric. It continues to support the more broadly compatible AES-128 as well. Azure Stack HCI also supports SMB Direct encryption, an option that was previously unavailable without significant performance impact. Data is encrypted before placement, leading to less performance degradation while adding AES-128 and AES-256 protected packet privacy.

Furthermore, Azure Stack HCI now supports granular control of encrypting intra-node storage communications for Cluster Shared Volumes (CSV) and the storage bus layer (SBL). This means that when using Storage Spaces Direct, you can decide if you wish to use encryption or signing on remote file system, CSV, and the SBL traffic separately from each other. And finally, Azure Stack HCI supports the accelerated AES-128-GMAC signing option with lower latency and CPU usage. You can use Windows Admin Center (WAC) and PowerShell cmdlets for granular control of SMB signing and encryption. All of these combine to give the maximum flexibility for your threat model and performance requirements. For more information, see SMB security enhancements.

Network security

Software defined networking (SDN) and micro-segmentation

With Azure Stack HCI, you can take steps towards ensuring that your applications and workloads are protected from external as well as internal attacks. Through micro-segmentation, you can create granular network policies between applications and services. This essentially reduces the security perimeter to a fence around each application or VM. This fence permits only necessary communication between application tiers or other logical boundaries, thus making it exceedingly difficult for cyberthreats to spread laterally from one system to another. Micro-segmentation securely isolates networks from each other and reduces the total attack surface of a network security incident.

Micro-segmentation in Azure Stack HCI is implemented through Network Security Groups (NSGs), like Azure. With NSGs, you can create allow or deny firewall rules where your rule source and destination are network prefixes. We also support tag-based segmentation, where you can assign any custom tags to classify your VMs, and then apply NSGs based on the tags to restrict communication to/from external as well as internal sources. So, to prevent your SQL VMs from communicating with your web server VMs, simply tag corresponding VMs with “SQL” and “Web” tags and create a NSG to prevent “Web” tag from communicating with “SQL” tag. These policies are available for VMs on traditional VLAN networks and on SDN overlay networks. Management of NSGs is supported through Windows Admin Center, PowerShell, and REST APIs. To learn more about NSGs, see Configure network security groups with tags in Windows Admin Center.

Finally, we also support default network access policies. Default network access policies help ensure that all virtual machines (VMs) in your Azure Stack HCI cluster are secure by default from external threats. If you choose to enable default policies for a virtual machine (VM), we will block inbound access to the VM by default, while giving the option to enable specific selective inbound management ports and thus securing the VM from external attacks. To learn more about default network access policies, see Manage default network access policies on your Azure Stack HCI.

Malware protection

Microsoft Defender Antivirus is real-time, behavior-based, and heuristic antivirus protection. It helps protect the operating system against viruses, malware, spyware, and other threats. In addition to real-time protection, updates are downloaded automatically to help keep your device safe and protect it from threats.

The combination of always-on content scanning, file and process behavior monitoring, and other heuristics effectively prevents security threats. Microsoft Defender Antivirus continually scans for malware and threats, and it detects and blocks potentially unwanted applications (PUA) which are applications that are deemed to negatively impact your device but are not considered malware. Microsoft Defender Antivirus always-on protection is integrated with cloud-delivered protection, which helps ensure near instant detection and blocking of new and emerging threats. To learn more, see Microsoft Defender Antivirus. By default, Microsoft Defender Antivirus is enabled in Azure Stack HCI.

Privacy

Azure Stack HCI collects the minimum data required to keep the system current, secure, and operating properly. This includes telemetry event data and diagnostics data. Telemetry pipeline transmits a steady stream of curated events to Azure. The diagnostics pipeline emits an episodic set of diagnostic data to Azure only when allowed by the customer. Data collection is enabled by default in Azure Stack HCI. However, you can disable data collection by changing the service health data setting via the Azure portal. For more information, see Azure Stack HCI data collection.

Operational security

Ongoing operations

Windows Admin Center in Azure

Traditional server administration requires on-premises identities, roles, and groups to manage the server. With Azure Stack HCI, you can manage your cluster through Windows Admin Center in Azure using your Microsoft Entra identities. This allows you to use Azure capabilities such as Microsoft Entra for additional security. Windows Admin Center in Azure has many capabilities that make your management platform more secure.

No inbound connectivity
You can securely manage your cluster from anywhere without needing a VPN, public IP address, or other inbound connectivity to your machine.

With the Windows Admin Center extension in Azure, you get the management, configuration, troubleshooting, and maintenance functionality for managing your Azure Stack HCI cluster in the Azure portal. Azure Stack HCI cluster and workload management no longer requires you to establish line-of-sight or Remote Desktop Protocol (RDP) - this can all be done natively from the Azure portal. Windows Admin Center provides tools and experiences that you would normally find in Failover Cluster Manager, Device Manager, Task Manager, Hyper-V Manager, and most other Microsoft Management Console (MMC) tools.

Azure Active Directory authentication
Authentication to Windows Admin Center is provided via a single sign-on experience that uses your Microsoft Entra credentials to authenticate you to your cluster. You no longer need to manage or share credentials for your cluster to provide your cluster administrators with access to your cluster. Windows Admin Center can authenticate you to your cluster using your Azure AD credentials, regardless of whether the device is Azure AD joined or not.

Role-based access control
Access to Windows Admin Center is controlled by an Azure role-based access control (RBAC) role named Windows Admin Center Administrator Login. Customers must be a part of this role to gain access to Windows Admin Center. To further enhance security, customers can leverage Azure AD Privileged Identity Management (PIM) to enable customers to get just-in-time (JIT) RBAC access to Windows Admin Center.

Two-factor authentication
With Windows Admin Center integrated in Azure portal, you can configure Azure AD multi-factor authentication (MFA) settings to control access to Windows Admin Center. To customize the end-user experience for Azure AD multi-factor authentication, you can configure options for settings like account lockout thresholds or fraud alerts and notifications. Some settings are available directly in the Azure portal for Microsoft Entra, and some are in a separate Azure AD Multi-Factor Authentication portal.

Logging
Windows Admin Center writes event logs to give you insight into management activities being performed on their servers, and to help you troubleshoot any Windows Admin Center issues.

Always up to date
Windows Admin Center, just like any other Azure service, is always up to date with the latest and greatest management experiences. Unlike previous on-premises tools that had long release cycles, Windows Admin Center in Azure updates often and automatically.

Security tool
The built-in security tool within Windows Admin Center gives you the ability to monitor and toggle Azure Stack HCI security settings. This tool lets you monitor and change your Secured-core, Windows Defender Application Control, and many other settings, all from within the Azure portal.

Lost Azure connectivity
In the event you lose connectivity to Azure, you can use an on-premises deployment of Windows Admin Center to troubleshoot issues and continue to manage your cluster with a familiar experience, until connectivity to Azure has been restored.

Continuous monitoring with Microsoft Defender for Cloud

Microsoft Defender for Cloud is a security posture management solution with advanced threat protection capabilities. It provides you with tools to assess the security status of your infrastructure, protect workloads, raise security alerts, and follow specific recommendations to remediate attacks and address future threats. It performs all these services at high speed in the cloud through auto-provisioning and protection with Azure services.

You can use Microsoft Defender for Cloud to assess both the individual and overall security posture of all your hybrid resources across your entire fleet. Microsoft Defender for Cloud helps improve the security posture of your environment, and can protect against existing and evolving threats. You can use Microsoft Defender for Cloud to monitor the security posture of your Azure Stack HCI infrastructure. This requires connectivity to Azure.

Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform. It extends management to edge and multi-cloud and provides a single pane of glass management control plane. Azure Stack HCI is Arc-enabled by default and has Azure Monitor agent installed via Azure Arc on each node in the cluster. This allows Azure Stack HCI to be monitored through Microsoft Defender for Cloud along with other resources. This enables you to manage and continuously monitor the security posture of your entire Azure Stack HCI fleet through Microsoft Defender for Cloud.

Ongoing compliance

Configuration monitoring and drift protection

With Azure Stack HCI, you can apply the recommended Azure Stack HCI security baseline and Secured-core settings, monitor, and perform drift protection from desired state during both deployment and run-time, using the built-in configuration management stack in the operating system. You can choose if you want drift protection to be turned on or off during deployment time or after deployment using Windows Admin Center or PowerShell.

Once drift protection is applied, the security settings will be refreshed at regular intervals, thus ensuring any change from desired state is remediated. This continuous monitoring and auto-remediation allows you to have consistent and reliable security posture throughout the lifecycle of the system.

For those who need to adjust or update security settings based on their own business requirements, in addition to keeping a balanced security posture based on Microsoft's recommendation, you can still leverage the initial security baseline, stop the drift control, and make any modification over any of the 300+ settings initially defined. To learn more, see Security baseline and drift control.

Azure security baseline compliance assessment

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity.

During run-time, you can use Azure Policy to audit Azure Stack HCI host machine configuration and perform compliance assessments based on Azure security baseline policies. In the future, we will also have the capability to remediate the security settings via Azure Policy and Azure Automanage.

SIEM integration

Security compliance requires strict logging and auditing of security events. In Azure Stack HCI, we recommend customers to use our Cloud SIEM Azure Sentinel service. For those organizations that use their own SIEM, Azure Stack HCI comes with an integrated syslog forwarder mechanism which can be used to forward security related events to a SIEM.

The integrated syslog forwarder, once configured, emits syslog messages as defined in RFC 3164, with the payload in Common Event Format (CEF). All audits and security events are collected on each host and exported via syslog with CEF payload to a Syslog Server endpoint.

Microsoft Defender for Cloud regulatory compliance

Microsoft Defender for Cloud streamlines the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard. Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in the regulatory standards that you have applied to your subscriptions. The dashboard reflects the status of your compliance with those standards. The regulatory compliance dashboard provides insights into your compliance posture based on how you are meeting specific compliance requirements such as ISO 27001:2013, PCI DSS v4, and NIST SP 800-53 R5.

Updates

Software updates

Azure Stack HCI contains many individual features and components, such as OS, agents and services, drivers, and firmware. Staying up to date with recent security fixes and feature improvements is important and essential for proper operation. The update feature in Azure Stack HCI uses an orchestrator (Lifecycle Manager) which centrally manages the deployment experience for the entire cluster.

The update feature offers many benefits:

- Provides a simplified, consolidated, single update management experience.
- Provides a well-tested configuration.
- Helps avoid downtime with health checks before and during an update.
- Improves reliability with automatic retry and remediation of known issues.
- Provides a common backend experience irrespective of whether the updates are managed locally or via Azure portal.

Azure Stack HCI solutions are designed to have a predictable update experience:

- Microsoft releases monthly patch (quality and reliability) updates, quarterly baseline (features and improvements) updates, hotfixes (for critical or security issues) as needed, and solution builder extension updates (driver, firmware, and other partner content specific to the system solution used) as needed.
- To keep your Azure Stack HCI cluster in a supported state, you must install updates regularly and stay current within six months of the most recent release. We recommend installing updates as and when they are released.

You can update your Azure Stack HCI cluster either via Azure portal using Azure Update Manager or via PowerShell command line interface. For more information on how to keep your Azure Stack HCI cluster up to date, read about updates for Azure Stack HCI. The Cluster-Aware Updating feature orchestrates update install on each server in the cluster so that your applications continue to run during the cluster upgrade.

To regularly update virtual machines running on your Azure Stack HCI, you can use Windows Update, Windows Server Update Services, and Azure Update Management to update VMs.

Workload security

Trusted launch for Azure Arc VMs

Trusted launch for Azure Arc VMs on Azure Stack HCI supports secure boot, virtual Trusted Platform Module (vTPM), and vTPM state transfer when a VM migrates or fails over within a cluster. You can choose Trusted launch as a security type when creating Azure Arc VMs on Azure Stack HCI via Azure portal or Azure CLI. For more information on Trusted launch, you can read Trusted launch for Azure Arc VMs.

With standard VMs, vTPM state is not preserved when a VM migrates or fails over to another node. This limits functionality and availability of applications that rely on the vTPM and its state. With Trusted launch, vTPM state is automatically moved along with the VM, when a VM migrates or fails over to another node within a cluster. This allows applications that rely on the vTPM state to continue to function normally even as the VM migrates or fails over. Applications use TPM in a variety of ways. In general, any application that relies on the TPM will benefit from Trusted launch capabilities. For more information, you can read the blog about Trusted launch for Arc VMs on Azure Stack HCI.

Continuous monitoring

You can enable Microsoft Defender for Cloud for your virtual machines running on Azure Stack HCI hosts. This enables you to continuously monitor their security posture and take corrective actions. With Azure Stack HCI, all virtual machines are automatically Arc-enabled. Microsoft Defender for Cloud protects virtual machines by installing the Azure Monitor agent inside the virtual machine and correlating events that the agent collects into recommendations (hardening tasks) that you can perform to make your workloads secure. The hardening tasks are based on security best practices that include managing and enforcing security policies. You can then track the results and manage compliance and governance over time through Defender for Cloud monitoring while reducing the attack surface across all your resources.

Microsoft Defender for Cloud also detects real-time threats such as malware and responds quickly by raising security alerts and providing recommendations to remediate attacks. Security alerts are categorized and assigned severity levels to indicate proper responses. Security alerts can be correlated to identify attack patterns and to integrate with Security Information and Event Management (SIEM), Security Orchestration Automated Response (SOAR), and IT Service Management (ITSM) solutions. This allows you to respond to threats quickly and limit the risk to your resources.

You can also use Microsoft Defender for Cloud to protect your workloads such as Azure Arc-enabled SQL Server and Azure Arc-enabled Kubernetes clusters.

Microsoft Sentinel is a comprehensive security information and event management (SIEM) solution for proactive threat detection, investigation, and response. You can aggregate security data and correlate alerts from virtually any source and modernize your security operations center (SOC) with Microsoft Sentinel. Security alerts from Microsoft Defender for Cloud can be streamed to Microsoft Sentinel, so you can investigate and respond to incidents.

Silicon assisted security

Secured-core hardware

There are two clear trends emerging in the server space today. First, organizations around the world are embracing digital transformation using technologies across cloud and edge to better serve their customers and thrive in fast-paced environments. Second, attackers are constantly evolving their attack strategies and targeting these organizations' high-value infrastructure with advanced technical capabilities connected to both cybercrime and espionage.

The MagBo marketplace, which sells access to more than 43,000 hacked servers, exemplifies the ever-expanding cybercrime threat. Compromised servers are being exploited to mine cryptocurrency and are being hit with ransomware attacks. The Security Signals report shows that more than 80% of enterprises have experienced at least one firmware attack in the past two years.

Given these factors, continuing to raise the security bar for critical infrastructure against attackers and making it easy for organizations to meet that higher bar is a clear priority for both customers and Microsoft. Using our learnings from the Secured-core PC initiative, Microsoft has teamed up with the ecosystem partners to expand Secured-core to Azure Stack HCI.

Following Secured-core PC, we are introducing Secured-core Server which is built on three key pillars: simplified security, advanced protection, and preventative defense. Secured-core Servers come with the assurance that manufacturing partners have built hardware and firmware that satisfy the requirements of the operating system (OS) security features.

Simplified security

The security extension in Windows Admin Center makes it easy for you to configure the OS security features of Secured-core for Azure Stack HCI. The extension enables advanced security with a click of the button from a web browser anywhere in the world. With Azure Stack HCI Integrated Systems, manufacturing partners have further simplified the configuration experience for you so that Microsoft's best server security is available right out of the box.

Advanced protection

Secured-core Servers maximize hardware, firmware, and OS capabilities to help protect against current and future threats. These safeguards create a platform with added security for critical applications and data used on the hosts and VMs that run on them. Secured-core functionality spans the following areas:

Hardware root-of-trust: Trusted Platform Module 2.0 (TPM 2.0) comes standard with Secured-core Servers, providing a protected store for sensitive keys and data, such as measurements of the components loaded during boot. Being able to verify that firmware that runs during boot is validly signed by the expected author and not tampered with helps improve supply chain security. This hardware root-of-trust elevates the protection provided by capabilities like BitLocker, which uses TPM 2.0 and facilitates the creation of attestation-based workflows that can be incorporated into zero-trust security strategies.

Firmware protection: In the last few years, there has been a significant uptick in firmware vulnerabilities, in large part due to the inherently higher level of privileges with which firmware runs combined with the limited visibility into firmware by traditional anti-virus solutions. Using processor support for Dynamic Root of Trust of Measurement (DRTM) technology, Secured-core systems put firmware in a hardware-based sandbox helping to limit the impact of vulnerabilities in millions of lines of highly privileged firmware code. Along with pre-boot DMA protection, Secured-core systems provide protection throughout the boot process.

Virtualization-based security (VBS): Secured-core servers support VBS and hypervisor-based code integrity (HVCI). The cryptocurrency mining attack mentioned earlier leveraged the EternalBlue exploit. VBS and HVCI help protect against this entire class of vulnerabilities by isolating privileged parts of the OS, like the kernel, from the rest of the system. This helps to ensure that servers remain devoted to running critical workloads and helps protect related applications and data from attack and exfiltration.

Enabling Secured-core functionality helps proactively defend against and disrupt many of the paths attackers may use to exploit a system. These defenses also enable IT and SecOps teams to better leverage their time across the many areas that need their attention.

Azure Stack HCI solutions

Secured-core servers can be easily identified in the Azure Stack HCI catalog as well as in the Windows Server catalog. Azure Stack HCI solutions supporting Secured-core capabilities are available from industry leading solution builders today. Furthermore, starting with Azure Stack HCI, version 22H2, Secured-core support is required on all new solutions based on Gen 3 or newer CPU. Thus, customers will benefit from host protection that is available with Microsoft OS platforms.

Microsoft Hardware Solution Partners provide Azure Stack HCI solution categories (Premier Solutions, Integrated Systems and Validated Nodes) with hardware service, support, and security updates for at least five years.

Security foundation

Security assurance

Microsoft is committed to continuously investing in improving our software development process, building highly secure-by-design software, and addressing security compliance requirements. We build in security from the ground up for powerful defense in today's threat environment. Every component of Azure Stack HCI, from server core to cloud, is purposefully designed to help ensure ultimate security.

Microsoft Security Development Lifecycle (SDL)

The Microsoft Security Development Lifecycle (SDL) introduces security best practices, tools, and processes throughout all phases of engineering and development. A range of tools and techniques - such as threat modeling, static analysis, fuzzing, and code quality checks—enable continued security value to be embedded into Windows by every engineer on the team from day one. Through the SDL practices, Microsoft engineers are continuously provided with actionable and up-to-date methods to improve development workflows and overall product security before the code has been released. Additionally, Microsoft Offensive Research and Security Engineering (MORSE) performs targeted design reviews, audits, and deep penetration testing of select Windows features. Microsoft's open source OneFuzz platform allows developers to fuzz features for Windows at scale as part of their development and testing cycle.

Security assessment activities

As part of our SDL, products like Azure Stack HCI are reviewed by our Microsoft Offensive Research and Security Engineering (MORSE) Edge team. MORSE works with other Microsoft security teams to perform comprehensive security assessments of the product. The goal of the security assessment activities is to:

- Ensure security promises the product makes are valid and effective.
- Identify insecure configurations, vulnerabilities, and design flaws in the Azure Stack HCI platform and its dependencies and ensure they are corrected before shipping.
- Review the product against Microsoft's SDL security requirements.
- Ensure the product meets Microsoft's standard of shipping a secure solution from inception.
- Ensure that the product can also be managed to maintain and enhance security during the product's lifecycle.

Comprehensive product security assessments will be done as new features are included and as the product continues through its lifecycle. The consistency in a comprehensive approach to securing edge products, staying current with best practices, customer needs, and regulatory and compliance requirements is the strongest indicator of the commitment Microsoft has made to developing a security-first product in Azure Stack HCI.

Certifications

Microsoft is committed to supporting product security standards and certifications, including FIPS 140 and Common Criteria as an external validation of security assurance. The Federal Information Processing Standard (FIPS) Publication 140 is a U.S. government standard that defines minimum security requirements for cryptographic modules in IT products. Microsoft maintains an active commitment to meeting the requirements of the FIPS 140 standard, having validated cryptographic modules in Windows operating systems against FIPS 140-2 since it was first established in 2001.

Common Criteria (CC) is an international standard currently maintained by national governments who participate in the Common Criteria Recognition Arrangement. CC defines a common taxonomy for security functional requirements, security assurance requirements, and an evaluation methodology used to ensure products undergoing evaluation satisfy the functional and assurance requirements. Microsoft ensures that products incorporate the features and functions required by relevant Common Criteria Protection Profiles and completes Common Criteria certifications of Microsoft Windows products.

Microsoft publishes the list of FIPS 140 and CC certified products at Federal Information Processing Standard (FIPS) 140 Validation and Common Criteria Certifications.

Microsoft provides Azure Stack HCI as a commercial-off-the-shelf hybrid infrastructure platform that not only has a comprehensive set of industry-recognized certifications and audits but also gives you an array of platform capabilities to help you fulfill the stringent compliance requirements in both on-premises and cloud settings. Below are some certifications and compliance guidance we provide for Azure Stack HCI platform:

- Federal Information Processing Standard (FIPS) 140
- Common Criteria for Information Technology Security Evaluation (CC)
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- U.S. Federal Risk and Authorization Management Program (FedRAMP)
- International Organization for Standardization (ISO) 27001:2022.

Secure supply chain

The work to secure the supply chain for software is important to Microsoft and the world. The changing landscape and speed of technology has warranted efforts by Governments, organizations, and corporations alike to improve oversight and build in new capabilities. Microsoft is actively involved in developing standards (such as IETF and OpenSSF) and working with others to produce innovative changes. The initial focus is on how we and others produce products but with an eye towards running systems.

Work started with the development of Software Bill of Materials (SBOM) from which the third-party dependencies (ingredients) must be listed. This includes binding of evidence claims and Common Vulnerabilities and Exposure (CVE) reports. The latter will enable a broader ability to assess risk and issues in dependent products.

Conclusion

We designed the Azure Stack HCI system so it is secure right out of the box. Further, we have provided mechanisms to help the system remain secure over time. We will continue to build on our security foundations with innovations that deliver powerful protection now and in the future.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft, Azure, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

© 2024 Microsoft Corporation. All rights reserved.