

# AZURE HYBRID EXPERIENCE DAY 2024

Sicherheit in allen Ebenen, von der Hardware bis zur App



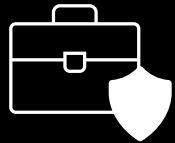
Thomas Roettinger, Principal Program Manager Lead

**MEDIALINE**  
**GROUP**

# Hybrid Security Strategy

- Microsoft Hybrid Security strategy is a security solution that provides a comprehensive approach to security for organizations that have a hybrid infrastructure.
- It is designed to protect against cyber threats and attacks by providing a unified security management experience across on-premises, cloud, and hybrid environments.
- The strategy includes a range of security solutions such as Microsoft Defender for Cloud, which protects workloads running in Azure, hybrid, and other cloud platforms.
- It also includes adopting a Zero Trust security strategy which protects your digital estate by applying a “never trust, always verify” approach.

# Hybrid Security – Customer value pillars



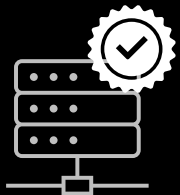
Secure your workloads



Securely operate the infrastructure



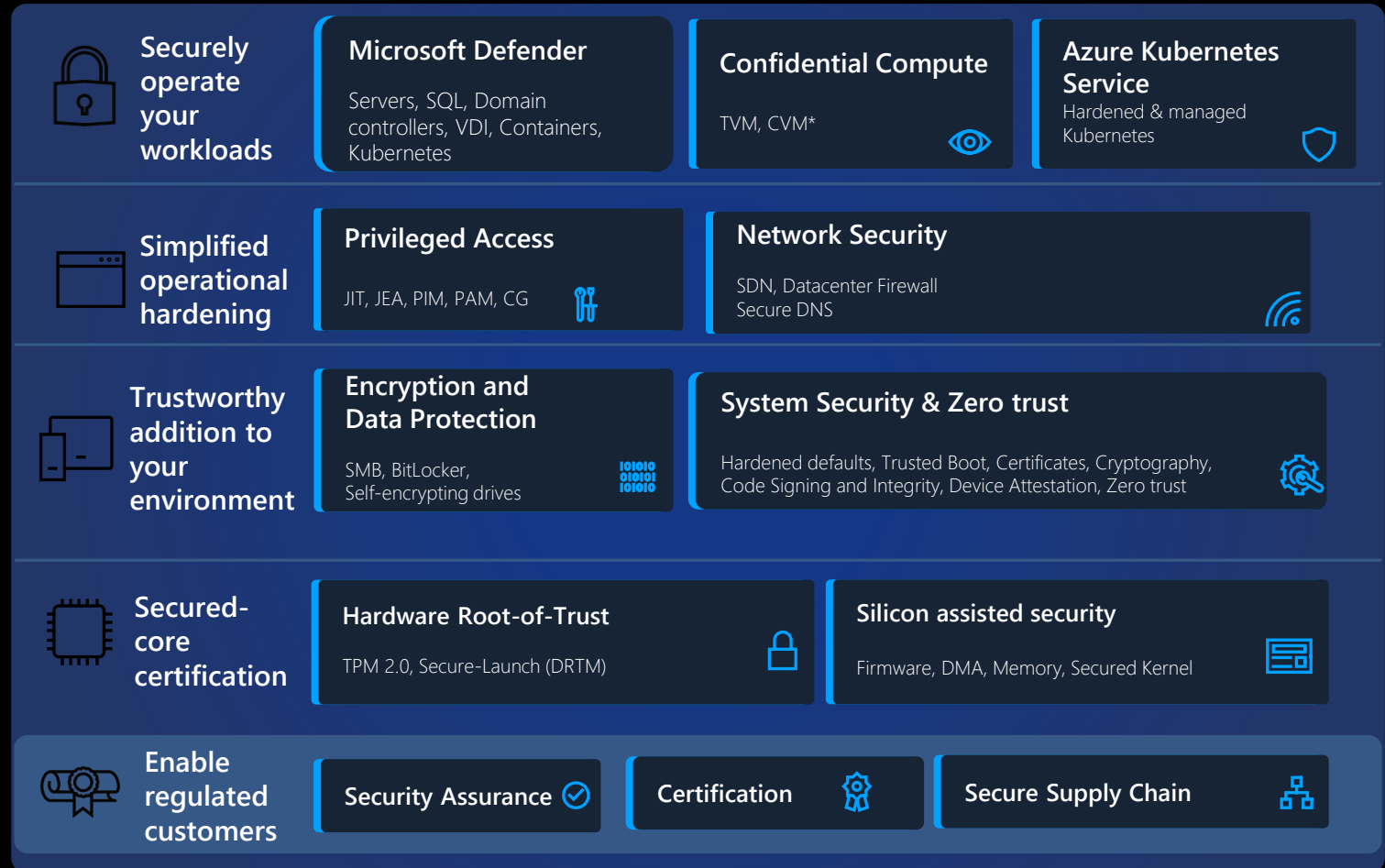
Ensure infrastructure is a trustworthy addition to your secure environment



Purchase hardware with the right security capabilities



Begin journey to meet regulatory requirements



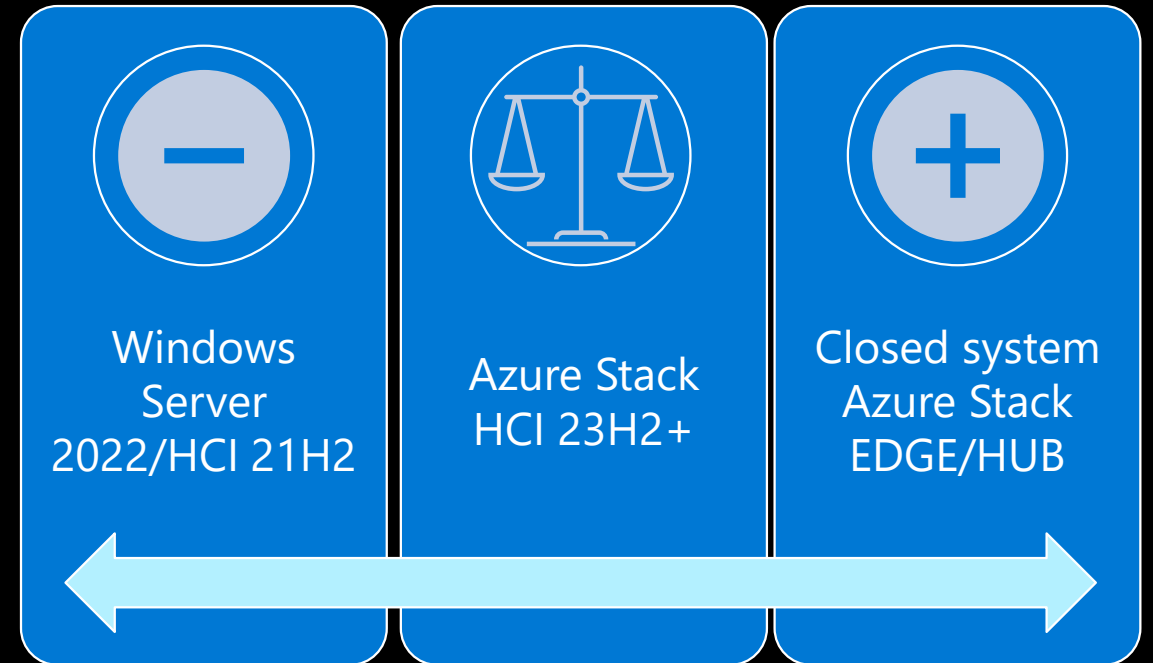
# Security Defaults

Overview of Azure Stack HCI Security

# Security Defaults strategy for 23H2

Provides a set of gold standards aligned with industry best practices to increase the security posture which includes:

- Hardened by Default
- Enabled by default security features consistently (cluster wide)
- Baseline aligned with Industry standards (ASB, CIS)
- Compliance certifications (FIPS – Common Criteria)



# High Level Overview Baseline (taxonomy)



## **Protocols/Ciphers/Hash**

Provides stronger by default system cipher suite.  
Limits unsecure protocols



## **Provides Silicon-based protections**

Secured-Core , Hardware Enforced Stack Protection\*



## **Host-Hardening**

Side-Channel mitigations, NetBIOS NR, WDIGEST, MDAV



## **Compliance**

Certs: FIPS, Common Criteria  
Controls: Azure Security baselines alignment,  
SIEM Integration: SYSLOG forwarder



## **Governance**

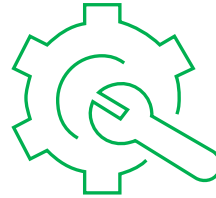
Maintains Security Settings (Drift control) and  
Secrets Management

# High Level Overview Features (taxonomy)



## **Credential Guard**

Protection for OS credentials secrets (Kerberos, NTLM, Tokens)



## **Windows Defender Application Control**

Protection for drivers and applications



## **Data at-rest Encryption**

Bitlocker protection for OS and CSV volumes



## **Data in-transit Protection**

Node, Cluster and VMs network protections



## **Microsoft Defender for the Cloud**

Native resource, Easy onboarding, Endpoint Protection

# We are listening

## Customer needs

**Hardware:** I am unsure how to enable Secured-Core, impact and the reboots needed for it

**Network:** I need to secure my external communications with strong and compliant set of protocols

**Operating System:** I don't know how to configure the multiple security related settings that might have side-effects on the solution (performance, stability, usability)

**Apps:** I need to implement a trusted app environment with whitelisting to protect from unknown, apps, rogue admins or ransomware

## HCI with LCM provides



Zero-touch enablement of Secured-Core features with safe net validations



Sets stronger by default system cipher suite. Limits unsecure protocols in a reliable and tested way



Built-in Microsoft proven security baseline with strong initial secure posture, mitigations, enabled by default security features, compliance alignment and drift control protection with no Group policy dependency



Out-of-box Application control with smart OEM signals or customer override with proven policy for MS components and workloads and ready to expand with simple experiences

# What else is turned ON when I deploy it?

Default Data-in-transit protection with SMB Signing

Default Data-at-rest encryption for OS Volume

Data-in-transit encryption for intra-cluster with a single toggle

Default Data-at-rest encryption for Cluster Share Volume

Micro-architectural side-channel mitigations enabled

Default credential protections with MS Defender Credential Guard

FIPS mode enabled by default

Default protections /exclusions with MS Defender AV

PowerShell and Windows Admin center experiences for all Security Settings

Host and Cluster Security UI view with enforced consistency experience

Application control cmdlets and reboot-less addition of new apps

# Security scenarios when using LCM

## Secure-Start

- Deploys recommended security settings (Baseline and features) with one click for my entire cluster security (TLS, FIPS mode, Secure-Core, Side-Channel, Credential Guard, WDAC, BL, SMB Signing & Encryption)
- Allows deployment of security settings customizations
- Default baseline of +300 settings aligned with Azure Security Windows Baseline and close alignment with (CIS/DISA STIG)
- Automated controls to enable Secured-Core with zero OS touch
- Cluster Certificates rotation and LCM account password rotation
- WDAC Enforced by default with easy expansion and automated cluster policy management
- WDAC OEM Integration through Solution Builder Extension (SBE)



## Secure Operate and Monitor

- [illegible]

# Deployment experience – Lifecycle Manager Deployment tool

Overview of Azure Stack HCI Security

# Azure Arc Deployment integrated with Lifecycle Manager

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Azure Arc | Get started >

## Deploy Azure Stack HCI

Basics Configuration Networking Management **Security** Advanced Tags Validation Review + create

Set the security level of your system's infrastructure

Stick with the recommended security settings for the highest security, or customize the settings. You can also change this later, including uninstalling azure services.

Security level \* ⓘ

☐ Recommended security settings

☒ Customized security settings

Security level

Excellent(7/7)

Settings

Recommended Settings 7 of 7

| Setting                                                                   | Description                                                                         |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Maintain security defaults            | Maintains the security defaults on each server, helping to protect against changes  |
| <input checked="" type="checkbox"/> Windows Defender Credential Guard     | Uses virtualisation-based security to isolate secrets from credential-theft attacks |
| <input checked="" type="checkbox"/> Windows Defender Application Control  | Controls which drivers and apps are allowed to run directly on each server          |
| <input checked="" type="checkbox"/> Bitlocker for the OS boot volume      | Encrypts the OS startup volume on each server                                       |
| <input checked="" type="checkbox"/> Bitlocker for data volumes            | Encrypts cluster shared volumes (CSVs) created on this system during deployment     |
| <input checked="" type="checkbox"/> Signing for external SMB traffic      | Signs SMB traffic between this system and others to help prevent relay attacks      |
| <input checked="" type="checkbox"/> SMB encryption for in-cluster traffic | Encrypts traffic between servers in the cluster (on your storage network)           |

# Azure Portal – view security settings

Overview of Azure Stack HCI Security

# Secure core settings

Home > s31r1501-cl

## s31r1501-cl | Security defaults

Azure Stack HCI

Search

- Windows Admin Center (preview)
- Extensions
- Configuration
- Deployments
- Locks

Resources

- Virtual machines
- Kubernetes clusters
- Logical networks
- Disks
- VM images
- Storage paths

Operations

- Disaster recovery (preview)
- Updates

Security (preview)

- Microsoft Defender for Cloud
- Security defaults**
- Application control (WDAC)
- Data protections

Some settings are turned off in your system BIOS. Consult your hardware manufacturer to turn on these settings.

These settings are maintained / enforced by default. To turn off the default settings, [learn more](#).

The following displays the current status of cluster security and Secured core server settings on your cluster.  
[Learn more about Azure Stack HCI security settings](#)

**Not secure**

✖ 1  
settings are off

**Secured core settings**

| Security setting                                          | Status           |
|-----------------------------------------------------------|------------------|
| <a href="#">Hypervisor Enforced Code Integrity (HVCI)</a> | ✔ 2 of 2 servers |
| <a href="#">Boot DMA protection</a>                       | ✖ 0 of 2 servers |
| <a href="#">System guard</a>                              | ✔ 2 of 2 servers |
| <a href="#">Secure Boot</a>                               | ✔ 2 of 2 servers |
| <a href="#">Virtualization-based Security</a>             | ✔ 2 of 2 servers |
| <a href="#">Trusted Platform Module (TPM) 2.0</a>         | ✔ 2 of 2 servers |

# Application control policies

The screenshot displays the 'Application control (WDAC)' page in the Azure Stack HCI management console. The left-hand navigation pane includes sections for 'Windows Admin Center (preview)', 'Extensions', 'Configuration', 'Deployments', 'Locks', 'Resources' (Virtual machines, Kubernetes clusters, Logical networks, Disks, VM images, Storage paths), 'Operations' (Disaster recovery (preview), Updates), 'Security (preview)' (Microsoft Defender for Cloud, Security defaults), and 'Application control (WDAC)' (selected), and 'Data protections'. The main content area features a search bar, a description of WDAC, a summary of 'Enforced' policies (All), and a table of specific policies.

Home > s31r1501-cl

s31r1501-cl | Application control (WDAC) ☆ ...

Azure Stack HCI

Search

Windows Admin Center (preview)

Extensions

Configuration

Deployments

Locks

Resources

- Virtual machines
- Kubernetes clusters
- Logical networks
- Disks
- VM images
- Storage paths

Operations

- Disaster recovery (preview)
- Updates

Security (preview)

- Microsoft Defender for Cloud
- Security defaults
- Application control (WDAC)
- Data protections

Control which drivers and apps are allowed to run on this system by using Windows Defender Application Control (WDAC) policies. [Learn more](#)

Enforced

✓ All

| Policy                                                                  | Status                    |
|-------------------------------------------------------------------------|---------------------------|
| <a href="#">AzCli_Supplemental_Policy</a>                               | ✓ 2 of 2 servers enforced |
| <a href="#">AS_Base_Policy</a>                                          | ✓ 2 of 2 servers enforced |
| <a href="#">SBE HPE ProLiant-Minimal 4.1.2403.2 supplemental policy</a> | ✓ 2 of 2 servers enforced |

# Data protections

The screenshot displays the Microsoft Azure portal interface for an Azure Stack HCI resource named 's31r1501-cl'. The left-hand navigation pane includes sections for Windows Admin Center, Extensions, Configuration, Deployments, Locks, Resources (Virtual machines, Kubernetes clusters, Logical networks, Disks, VM images, Storage paths), Operations (Disaster recovery, Updates), Security (Microsoft Defender for Cloud, Security defaults, Application control), and Data protections (highlighted).

The main content area is titled 's31r1501-cl | Data protections' and features a search bar and two tabs: 'Volume encryption' (selected) and 'Network protection'. Below the tabs, a message states: 'Use BitLocker to encrypt data on your volumes.'.

Two summary cards are shown: 'BitLocker for OS volumes' and 'BitLocker for data volumes', both indicating 'All' volumes are encrypted with a green checkmark.

A table provides a detailed view of the encryption status for various volumes:

| Volume                               | Server         | Encryption status |
|--------------------------------------|----------------|-------------------|
| <strong>OS volumes</strong>          |                |                   |
| C:                                   | ASRR1S31R15U01 | ✓ Configured      |
| C:                                   | ASRR1S31R15U03 | ✓ Configured      |
| <strong>Data volumes (CSVs)</strong> |                |                   |
| C:\ClusterStorage\Infrastructure_1   | ---            | ✓ Configured      |
| C:\ClusterStorage\UserStorage_1      | ---            | ✓ Configured      |
| C:\ClusterStorage\UserStorage_2      | ---            | ✓ Configured      |

# Security cmdlets for Azure Stack HCI

Overview of Azure Stack HCI Security

# Day 2/100 – PowerShell cmdlets

**Security Features** -Module AzureStackOSConfigAgent

Disable-AzsSecurity

Enable-AzsSecurity

Get-AzsSecurity

-Scope: Local | PerNode | AllNodes | Cluster

-FeatureName | CredentialGuard | DriftControl | DRTM | HVCI | SideChannelMitigation | SMBEncryption | SMBSigning | VBS

Local –Provides boolean value (true/False) on local node - do not interact with ECE.

PerNode –Provides boolean value (true/False) per node report - requires CredSSP or Console (RDP)

AllNodes –Provides boolean value (true/False) computed across nodes- requires CredSSP or Console (RDP)

Cluster –Provides boolean value from ECE store. Interacts with ECE and acts to all the nodes in the cluster, requires ECE authorization (PREFIX-ECESG) and CredSSP or Console session (RDP)

**Management layer json documents** –Module AzureStackOSConfigAgent

Get-AsOSConfigSecuredCoreDoc

Get-AsOSConfigSecuritySettingsDoc

# Day 2/100 – PowerShell cmdlets Cont.

**Bitlocker** - Module: AzureStackBitlockerAgent

Disable-ASBitlocker

Enable-ASBitlocker

Get-ASBitlocker

Get-AsRecoveryKeyInfo

-Scope: : Local | PerNode

-VolumeType: BootVolume | ClusterSharedVolume

Local – Provides BL volumes details on local node - do not interact with ECE.

PerNode – Provides BL volumes details per node report - requires CredSSP or Console session (RDP)

**Windows Defender Application Control** – Module Microsoft.AS.Infra.Security.WDAC

Add-ASWDACSupplementalPolicy

Add-ASLocalWDACSupplementalPolicy

Enable-ASLocalWDACPolicy

Enable-ASWDACPolicy

Get-ASLocalWDACPolicyInfo

Invoke-WDACRefreshPolicyTool

Remove-ASLocalWDACSupplementalPolicy

Remove-ASWDACSupplementalPolicy

# Day 2/100 – PowerShell cmdlets Cont.

## **Secured-Core Tests** - Module **Microsoft.AS.Infra.Security.SecuredCoreSystemInfo**

Test-ASVBSCapable | Test-ASVBSEnabled

Test-ASHVCI Capable | Test-ASHVCIEnabled | Test-ASHVCIRunning

Test-ASDRTM Capable | Test-ASDRTMEnabled

Test-ASDMAEnabled

## **Secrets Rotation** - Module: **Microsoft.AS.Infra.Security.SecretRotation**

Start-SecretRotation - requires CredSSP or Console session (RDP)

Set-AzureStackLCMUserPassword - requires CredSSP or Console session (RDP)

## **SySLOG Forwarder** - Module: **Microsoft.AS.Infra.Security.SyslogForwarder**

Disable-AzSSyslogForwarder – Cluster Wide

Enable-AzSSyslogForwarder – Cluster Wide

Set-AzSSyslogForwarder - Cluster Wide -> 4 operation modes (UDP, TCP, TLS, mTLS)

Get-AzSSyslogForwarder

Local – Provides BL volumes details on local node - do not interact with ECE.

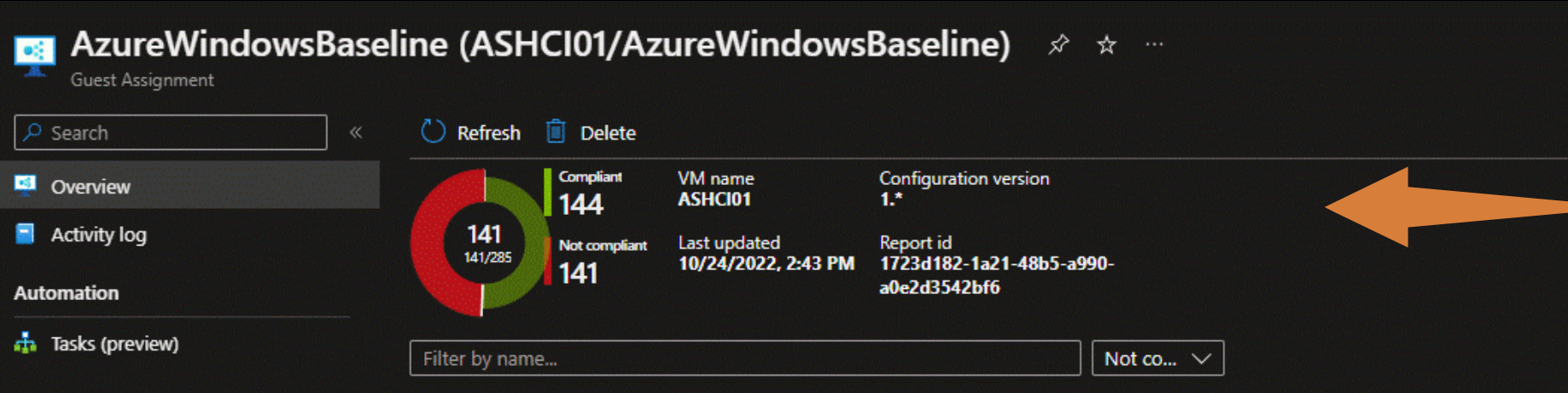
PerNode – Provides BL volumes details per node report - requires CredSSP or Console session (RDP)

Cluster – Provides value from ECE store. Interacts with ECE and acts to all the nodes in the cluster, requires ECE authorization (PREFIX-ECESG) and CredSSP or Console session (RDP)

# Compliance Monitor - Azure Stack HCI

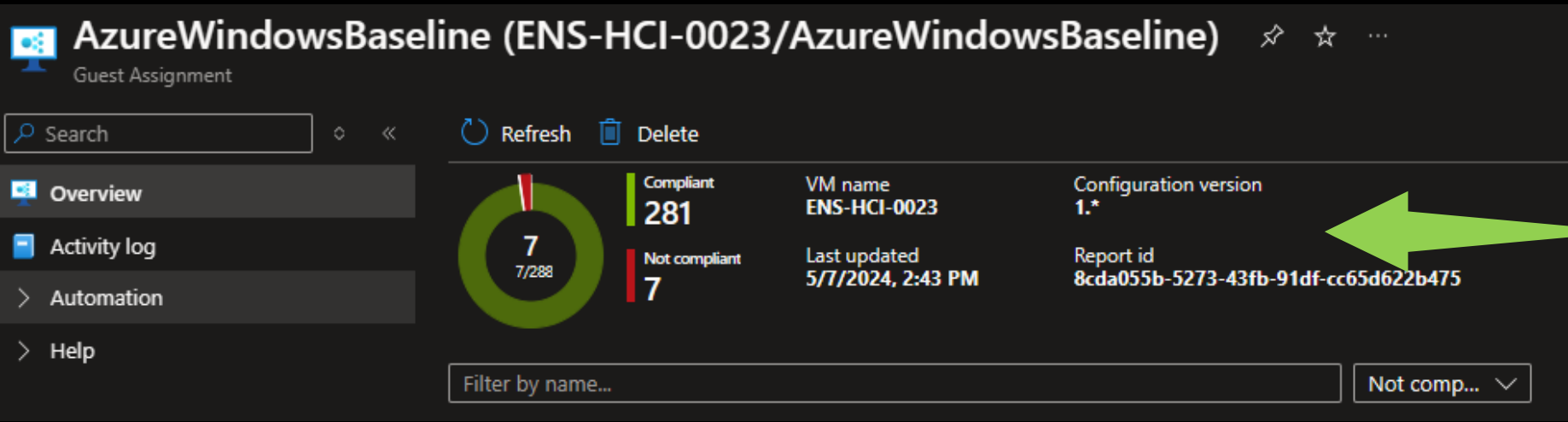
Overview of Azure Stack HCI Security

# Show me the compliance report!



Azure Stack HCI  
22H2 without  
LCM

50% Compliance



Azure Stack HCI  
23H2 Preview  
**with** LCM  
baseline

97.5% Compliance

# Demo

Overview of Azure Stack HCI Security

# Ende!

## Vielen Dank für Ihre Teilnahme!

**Medialine EuroTrade AG**

[sales@medialine.ag](mailto:sales@medialine.ag)  
[www.medialine.com](http://www.medialine.com)

**Breitlerstraße 43**  
**55566 Bad Sobernheim**  
Tel: +49 6751 85378-0  
Fax: +49 6751 85378-11

[www.group.medialine.com](http://www.group.medialine.com)



**MEDIALINE**  
**GROUP**