Azure security baseline for Virtual Machine Scale Sets

Article • 02/25/2025

This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Virtual Machine Scale Sets. The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Virtual Machine Scale Sets.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud portal page.

When a feature has relevant Azure Policy Definitions, they are listed in this baseline to help you measure compliance with the Microsoft cloud security benchmark controls and recommendations. Some recommendations may require a paid Microsoft Defender plan to enable certain security scenarios.

> ⓘ **Note**
>
> **Features** not applicable to Virtual Machine Scale Sets have been excluded. To see how Virtual Machine Scale Sets completely maps to the Microsoft cloud security benchmark, see the full Virtual Machine Scale Sets security baseline mapping file .

Security profile

The security profile summarizes high-impact behaviors of Virtual Machine Scale Sets, which may result in increased security considerations.

Expand table

Service Behavior Attribute	Value
Product Category	Compute
Customer can access HOST / OS	Full Access
Service can be deployed into customer's virtual network	True
Stores customer content at rest	True

Network security

For more information, see the Microsoft cloud security benchmark: Network security.

NS-1: Establish network segmentation boundaries

Features

Virtual Network Integration

Description: Service supports deployment into customer's private Virtual Network (VNet). Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

Configuration Guidance: No additional configurations are required as this is enabled on a default deployment.

Reference: Virtual networks and virtual machines in Azure

Network Security Group Support

Description: Service network traffic respects Network Security Groups rule assignment on its subnets. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use network security groups (NSG) to restrict or monitor traffic by port, protocol, source IP address, or destination IP address. Create NSG rules to restrict your service's open ports (such as preventing management ports from being accessed from untrusted networks). Be aware that by default, NSGs deny all inbound traffic but allow traffic from virtual network and Azure Load Balancers.

When you create an Azure virtual machine (VM), you must create a virtual network or use an existing virtual network and configure the VM with a subnet. Ensure that all deployed subnets have a Network Security Group applied with network access controls specific to your applications trusted ports and sources.

Reference: Network security groups

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive network hardening recommendations should be applied on internet facing virtual machines	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	3.0.0

NS-2: Secure cloud services with network controls

Features

Disable Public Network Access

Description: Service supports disabling public network access either through using service-level IP ACL filtering rule (not NSG or Azure Firewall) or using a 'Disable Public Network Access' toggle switch. Learn more.

⛶ Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature notes: Services installed with the operating system may be used to provide network filtering to disabled public network access.

Configuration Guidance: There is no current Microsoft guidance for this feature configuration. Please review and determine if your organization wants to configure this security feature.

Identity management

For more information, see the Microsoft cloud security benchmark: Identity management.

IM-1: Use centralized identity and authentication system

Features

Azure AD Authentication Required for Data Plane Access

Description: Service supports using Azure AD authentication for data plane access. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Azure Active Directory (Azure AD) as the default authentication method to control your data plane access. Azure AD protects data by using strong encryption for data at rest and in transit. Azure AD also salts, hashes, and securely stores user credentials. You can use managed identities to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code. Your code that's running on a virtual machine, can use its managed identity to request access tokens for services that support Azure AD authentication.

Reference: Azure AD join implementation

Local Authentication Methods for Data Plane Access

Description: Local authentications methods supported for data plane access, such as a local username and password. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

Feature notes: Avoid the usage of local authentication methods or accounts, these should be disabled wherever possible. Instead use Azure AD to authenticate where possible.

Configuration Guidance: No additional configurations are required as this is enabled on a default deployment.

IM-3: Manage application identities securely and automatically

Features

Managed Identities

Description: Data plane actions support authentication using managed identities. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Azure managed identities instead of service principals when possible, which can authenticate to Azure services and resources that support Azure Active Directory (Azure AD) authentication. Managed identity credentials are fully managed, rotated, and protected by the platform, avoiding hard-coded credentials in source code or configuration files.

Reference: Managed identities for Azure resources

Service Principals

Description: Data plane supports authentication using service principals. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature notes: Service principals may be used by applications running in Virtual Machine Scale Sets.

Configuration Guidance: There is no current Microsoft guidance for this feature configuration. Please review and determine if your organization wants to configure this security feature.

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name **(Azure portal)**	**Description**	**Effect(s)**	**Version** **(GitHub)**
Virtual machines' Guest Configuration extension should be	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do	AuditIfNotExists, Disabled	1.0.1

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
deployed with system-assigned managed identity	not have a system assigned managed identity. Learn more at https://aka.ms/gcpol		

IM-8: Restrict the exposure of credential and secrets

Features

Service Credential and Secrets Support Integration and Storage in Azure Key Vault

Description: Data plane supports native use of Azure Key Vault for credential and secrets store. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature notes: Within the data plane or operating system, services may call Azure Key Vault for credentials or secrets.

Configuration Guidance: Ensure that secrets and credentials are stored in secure locations such as Azure Key Vault, instead of embedding them into code or configuration files.

Privileged access

For more information, see the Microsoft cloud security benchmark: Privileged access.

PA-1: Separate and limit highly privileged/administrative users

Features

Local Admin Accounts

Description: Service has the concept of a local administrative account. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

Feature notes: Avoid the usage of local authentication methods or accounts, these should be disabled wherever possible. Instead use Azure AD to authenticate where possible.

Configuration Guidance: No additional configurations are required as this is enabled on a default deployment.

Reference: Create virtual machines in a scale set using Azure portal

PA-7: Follow just enough administration (least privilege) principle

Features

Azure RBAC for Data Plane

Description: Azure Role-Based Access Control (Azure RBAC) can be used to managed access to service's data plane actions. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Azure role-based access control (Azure RBAC) to manage Azure resource access through built-in role assignments. Azure RBAC roles can be assigned to users, groups, service principals, and managed identities.

Reference: Built-in Role for Virtual Machine Contributor

PA-8: Determine access process for cloud provider support

Features

Customer Lockbox

Description: Customer Lockbox can be used for Microsoft support access. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: In support scenarios where Microsoft needs to access your data, use Customer Lockbox to review, then approve or reject each of Microsoft's data access requests.

Data protection

For more information, see the Microsoft cloud security benchmark: Data protection.

DP-1: Discover, classify, and label sensitive data

Features

Sensitive Data Discovery and Classification

Description: Tools (such as Azure Purview or Azure Information Protection) can be used for data discovery and classification in the service. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

DP-2: Monitor anomalies and threats targeting sensitive data

Features

Data Leakage/Loss Prevention

Description: Service supports DLP solution to monitor sensitive data movement (in customer's content). Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

DP-3: Encrypt sensitive data in transit

Features

Data in Transit Encryption

Description: Service supports data in-transit encryption for data plane. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature notes: Certain communication protocols such as SSH are encrypted by default. However, services such as RDP or HTTP must be configured to use TLS for encryption.

Configuration Guidance: Enable secure transfer in services where there is a native data in transit encryption feature built in. Enforce HTTPS on any web applications and services and ensure TLS v1.2 or later is used. Legacy versions such as SSL 3.0, TLS v1.0 should be disabled. For remote management of Virtual Machines, use SSH (for Linux) or RDP/TLS (for Windows) instead of an unencrypted protocol.

Reference: In-transit encryption in VMs

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name **(Azure portal)**	**Description**	**Effect(s)**	**Version** **(GitHub)**
Windows machines should be configured to use secure communication protocols	To protect the privacy of information communicated over the Internet, your machines should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by encrypting a connection between machines.	AuditIfNotExists, Disabled	4.1.1

DP-4: Enable data at rest encryption by default

Features

Data at Rest Encryption Using Platform Keys

Description: Data at-rest encryption using platform keys is supported, any customer content at rest is encrypted with these Microsoft managed keys. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

Feature notes: In addition to the standard encryption with platform managed keys, high security sensitive customers who are concerned of the risk associated with any particular encryption algorithm, implementation, or key being compromised can now opt for additional layer of encryption using a different encryption algorithm/mode at the infrastructure layer using platform managed encryption keys and customer managed keys. This new layer can be applied to persisted OS and data disks, snapshots, and images, all of which will be encrypted at rest with double encryption.

For more information, please visit: Double encryption at rest.

Configuration Guidance: No additional configurations are required as this is enabled on a default deployment.

Reference: Azure Disk Encryption for Virtual Machine Scale Sets

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys; temp disks and data caches aren't encrypted, and data isn't encrypted when flowing between compute and storage resources. Use Azure Disk Encryption or EncryptionAtHost to encrypt all this data.Visit https://aka.ms/diskencryptioncomparison to compare encryption offerings. This	AuditIfNotExists, Disabled	1.2.0-preview

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	policy requires two prerequisites to be deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol .		

DP-5: Use customer-managed key option in data at rest encryption when required

Features

Data at Rest Encryption Using CMK

Description: Data at-rest encryption using customer-managed keys is supported for customer content stored by the service. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: If required for regulatory compliance, define the use case and service scope where encryption using customer-managed keys are needed. Enable and implement data at rest encryption using customer-managed key for those services.

Virtual disks on Virtual Machines (VM) are encrypted at rest using either Server-side encryption or Azure disk encryption (ADE). Azure Disk Encryption leverages the DM-Crypt feature of Linux to encrypt managed disks with customer-managed keys within the guest VM. Server-side encryption with customer-managed keys improves on ADE by enabling you to use any OS types and images for your VMs by encrypting data in the Storage service.

When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls. You must use either Azure Key Vault or Azure Key Vault Managed Hardware Security Module (HSM) to store your customer-managed keys.

You can either import your RSA keys to your Key Vault or generate new RSA keys in Azure Key Vault. Azure managed disks handles the encryption and decryption in a fully transparent fashion using envelope encryption. It encrypts data using an AES 256 based data encryption key (DEK), which is, in turn, protected using your keys. The Storage service generates data encryption keys and encrypts them with customer-managed keys using RSA encryption. The envelope encryption allows you to rotate (change) your keys periodically as per your compliance policies without impacting your VMs. When you rotate your keys, the Storage service re-encrypts the data encryption keys with the new customer-managed keys.

Managed Disks and the Key Vault or managed HSM must be in the same Azure region, but they can be in different subscriptions. They must also be in the same Azure Active Directory (Azure AD) tenant, unless you're encrypting managed disks with cross-tenant customer-managed keys.

Reference: Creating and configuring a key vault for Azure Disk Encryption

DP-6: Use a secure key management process

Features

Key Management in Azure Key Vault

Description: The service supports Azure Key Vault integration for any customer keys, secrets, or certificates. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Azure Key Vault to create and control the life cycle of your encryption keys, including key generation, distribution, and storage. Rotate and revoke your keys in Azure Key Vault and your service based on a defined schedule or when there is a key retirement or compromise. When there is a need to use customer-managed key (CMK) in the workload, service, or application level, ensure you follow the best practices for key management: Use a key hierarchy to generate a separate data encryption key (DEK) with your key encryption key (KEK) in your key vault. Ensure keys are registered with Azure Key Vault and referenced via key IDs from the service or application. If you need to bring your own key (BYOK) to the service (such as importing HSM-protected keys from your on-premises HSMs into Azure Key Vault), follow recommended guidelines to perform initial key generation and key transfer.

Reference: Creating and configuring a key vault for Azure Disk Encryption

Asset management

For more information, see the Microsoft cloud security benchmark: Asset management.

AM-2: Use only approved services

Features

Azure Policy Support

Description: Service configurations can be monitored and enforced via Azure Policy. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Azure Policy can be used to define the desired behavior for your organization's Windows VMs and Linux VMs. By using policies, an organization can enforce various conventions and rules throughout the enterprise and define and implement standard security configurations for Azure Virtual Machine Scale Sets. Enforcement of the desired behavior can help mitigate risk while contributing to the success of the organization.

Reference: Built-in Azure Policy Definitions for Virtual Machine Scale Sets

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name **(Azure portal)**	**Description**	**Effect(s)**	**Version** **(GitHub)**
Virtual machines should be migrated to new Azure Resource Manager resources	Use new Azure Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	1.0.0

AM-5: Use only approved applications in virtual machine

Features

Microsoft Defender for Cloud - Adaptive Application Controls

Description: Service can limit what customer applications run on the virtual machine using Adaptive Application Controls in Microsoft Defender for Cloud. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Microsoft Defender for Cloud adaptive application controls to discover applications running on virtual machines (VMs) and generate an application allow list to mandate which approved applications can run in the VM environment.

Reference: Use adaptive application controls to reduce your machines' attack surfaces

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive application controls for defining safe applications should be enabled on your machines	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining	AuditIfNotExists, Disabled	3.0.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.		

Logging and threat detection

For more information, see the Microsoft cloud security benchmark: Logging and threat detection.

LT-1: Enable threat detection capabilities

Features

Microsoft Defender for Service / Product Offering

Description: Service has an offering-specific Microsoft Defender solution to monitor and alert on security issues. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Defender for Servers extends protection to your Windows and Linux machines running in Azure. Defender for Servers integrates with Microsoft Defender for Endpoint to provide endpoint detection and response (EDR), and also provides a host of additional threat protection features, such as security baselines and OS level assessments, vulnerability assessment scanning, adaptive application controls (AAC), file integrity monitoring (FIM), and more.

Reference: Overview of Microsoft Defender for Servers

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name **(Azure portal)**	**Description**	**Effect(s)**	**Version** **(GitHub)**
Windows Defender Exploit Guard should be enabled on your machines	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).	AuditIfNotExists, Disabled	2.0.0

LT-4: Enable logging for security investigation

Features

Azure Resource Logs

Description: Service produces resource logs that can provide enhanced service-specific metrics and logging. The customer can configure these resource logs and send them to their own data sink like a storage account or log analytics workspace. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Azure Monitor starts automatically collecting metric data for your virtual machine host when you create the VM. To collect logs and performance data from the guest operating system of the virtual machine, though, you must install the Azure Monitor agent. You can install the agent and configure collection using either VM insights or by creating a data collection rule.

Reference: Log Analytics agent overview

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview

Posture and vulnerability management

For more information, see the Microsoft cloud security benchmark: Posture and vulnerability management.

PV-3: Define and establish secure configurations for compute resources

Features

Azure Automation State Configuration

Description: Azure Automation State Configuration can be used to maintain the security configuration of the operating system. Learn more.

Expand table

Supported	**Enabled By Default**	**Configuration Responsibility**
True	False	Customer

Configuration Guidance: Use Azure Automation State Configuration to maintain the security configuration of the operating system. Azure Automation State Configuration is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations for nodes.

Azure Automation State Configuration provides several advantages over the use of DSC outside of Azure. This service enables scalability across thousands of machines quickly and easily from a central, secure location. You can easily enable machines, assign them declarative configurations, and view reports showing each machine's compliance with the desired state you specify.

Reference: Using Virtual Machine Scale Sets with the Azure DSC Extension

Azure Policy Guest Configuration Agent

Description: Azure Policy guest configuration agent can be installed or deployed as an extension to compute resources. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Microsoft Defender for Cloud and Azure Policy guest configuration agent to regularly assess and remediate configuration deviations on your virtual machines.

Reference: Understand the guest configuration feature of Azure Policy

Custom VM Images

Description: Service supports using user-supplied VM images or pre-built images from the marketplace with certain baseline configurations pre-applied. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use a pre-configured hardened image from a trusted supplier such as Microsoft or build a desired secure configuration baseline into the VM image template

Reference: Create and use a custom image for virtual machine scale sets with Azure PowerShell

PV-4: Audit and enforce secure configurations for compute resources

Features

Trusted Launch Virtual Machine

Description: Trusted Launch protects against advanced and persistent attack techniques by combining infrastructure technologies like secure boot, vTPM, and integrity monitoring. Each technology provides another layer of defense against sophisticated threats. Trusted launch allows the secure deployment of virtual machines with verified boot loaders, OS kernels, and drivers, and securely protects keys, certificates, and secrets in the virtual machines. Trusted launch also provides insights and confidents of the entire boot chain's integrity and ensures workloads are trusted and verifiable. Trusted launch is integrated with Microsoft Defender for Cloud to ensure VMs are properly configured, by remotely attesting VM is booted in a healthy way. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature note: Trusted launch is available for generation 2 VMs. Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were initially created without it.

Configuration Guidance: Trusted launch may be enabled during the deployment of the VM. Enable all three - Secure Boot, vTPM, and integrity boot monitoring to ensure the best security posture for the virtual machine. Please note that there are a few prerequisites including onboarding your subscription to Microsoft Defender for Cloud, assigning certain Azure Policy initiatives, and configuring firewall policies.

Reference: Deploy a VM with trusted launch enabled

PV-5: Perform vulnerability assessments

Features

Vulnerability Assessment using Microsoft Defender

Description: Service can be scanned for vulnerability scan using Microsoft Defender for Cloud or other Microsoft Defender services embedded vulnerability assessment capability (including Microsoft Defender for server, container registry, App Service, SQL, and DNS). Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Follow recommendations from Microsoft Defender for Cloud for performing vulnerability assessments on your Azure virtual machines.

Reference: Overview of Microsoft Defender for Servers

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A vulnerability assessment solution should be enabled on your virtual machines	Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you.	AuditIfNotExists, Disabled	3.0.0

PV-6: Rapidly and automatically remediate vulnerabilities

Features

Azure Automation Update Management

Description: Service can use Azure Automation Update Management to deploy patches and updates automatically. Learn more.

⛶ Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: Microsoft offers other capabilities to help you manage updates for your Azure VMs or Azure virtual machine scale sets that you should consider as part of your overall update management strategy.

If you are interested in automatically assessing and updating your Azure virtual machines to maintain security compliance with Critical and Security updates released each month, review Automatic VM guest patching. This is an alternative update management solution for your Azure VMs to auto-update them during off-peak hours, including VMs within an availability set, compared to managing update deployments to those VMs from Update Management in Azure Automation.

If you manage Azure virtual machine scale sets, review how to perform automatic OS image upgrades to safely and automatically upgrade the OS disk for all instances in the scale set.

For more information, please visit: Azure Virtual Machine Scale Set automatic OS image upgrades.

Configuration Guidance: This feature is not supported to secure this service.

Azure Guest Patching Service

Description: Service can use Azure Guest Patching to deploy patches and updates automatically. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Services can leverage the different update mechanisms such as Auto OS Image Upgrades and Auto Guest Patching. The capabilities are recommended to apply the latest security and critical updates to your Virtual Machine's Guest OS by following the Safe Deployment Principles.

Auto Guest Patching allows you to automatically assess and update your Azure virtual machines to maintain security compliance with Critical and Security updates released each month. Updates are applied during off-peak hours, including VMs within an availability set. This capability is available for VMSS Flexible Orchestration, with future support on the roadmap for Uniform Orchestration.

If you run a stateless workload, Auto OS Image Upgrades are ideal to apply the latest update for your VMSS Uniform. With rollback capability, these updates are compatible with Marketplace or Custom images. Future rolling upgrade support on the roadmap for Flexible Orchestration.

Reference: Automatic VM Guest Patching for Azure VMs

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name **(Azure portal)**	**Description**	**Effect(s)**	**Version** **(GitHub)**
[Preview]: System updates should be installed on your machines (powered by Update Center)	Your machines are missing system, security, and critical updates. Software updates often include critical patches to security holes. Such holes are frequently exploited in malware attacks so it's vital to keep your software updated. To install all outstanding patches and secure your machines, follow the remediation steps.	AuditIfNotExists, Disabled	1.0.0-preview

Endpoint security

For more information, see the Microsoft cloud security benchmark: Endpoint security.

ES-1: Use Endpoint Detection and Response (EDR)

Features

EDR Solution

Description: Endpoint Detection and Response (EDR) feature such as Azure Defender for servers can be deployed into the endpoint. Learn more.

Expand table

Supported	**Enabled By Default**	**Configuration Responsibility**
True	False	Customer

Configuration Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats. Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.

Reference: Integrated license for Microsoft Defender for Endpoint

ES-2: Use modern anti-malware software

Features

Anti-Malware Solution

Description: Anti-malware feature such as Microsoft Defender Antivirus, Microsoft Defender for Endpoint can be deployed on the endpoint. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: For Windows Server 2016 and above, Microsoft Defender for Antivirus is installed by default. For Windows Server 2012 R2 and above, customers can install SCEP (System Center Endpoint Protection). For Linux, customers can have the choice of installing Microsoft Defender for Linux. Alternatively, customers also have the choice of installing third-party anti-malware products.

Reference: Microsoft Antimalware for Azure Cloud Services and Virtual Machines

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Endpoint protection health issues should be resolved on your machines	Resolve endpoint protection health issues on your virtual machines to protect them from latest threats and vulnerabilities. Azure Security Center supported endpoint protection solutions are documented here - https://docs.microsoft.com/azure/security-center/security-center-services?tabs=features-windows#supported-endpoint-protection-solutions. Endpoint protection assessment is documented here - https://docs.microsoft.com/azure/security-center/security-center-endpoint-protection.	AuditIfNotExists, Disabled	1.0.0

ES-3: Ensure anti-malware software and signatures are updated

Features

Anti-Malware Solution Health Monitoring

Description: Anti-malware solution provides health status monitoring for platform, engine, and automatic signature updates. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Configure your anti-malware solution to ensure the platform, engine and signatures are updated rapidly and consistently and their status can be monitored.

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name **(Azure portal)**	**Description**	**Effect(s)**	**Version** **(GitHub)**
Endpoint protection health issues should be resolved on your machines	Resolve endpoint protection health issues on your virtual machines to protect them from latest threats and vulnerabilities. Azure Security Center supported endpoint protection solutions are documented here - https://docs.microsoft.com/azure/security-center/security-center-services?tabs=features-windows#supported-endpoint-protection-solutions. Endpoint protection assessment is documented here - https://docs.microsoft.com/azure/security-center/security-center-endpoint-protection.	AuditIfNotExists, Disabled	1.0.0

Backup and recovery

For more information, see the Microsoft cloud security benchmark: Backup and recovery.

BR-1: Ensure regular automated backups

Features

Azure Backup

Description: The service can be backed up by the Azure Backup service. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature notes: Supported for VMSS Flex and not VMSS Uniform

Configuration Guidance: Enable Azure Backup and target Azure Virtual Machines (VM), as well as the desired frequency and retention periods. This includes complete system state backup. If you are using Azure disk encryption, Azure VM backup automatically handles the backup of customer-managed keys. For Azure Virtual Machines, you can use Azure Policy to enable automatic backups.

Reference: How to take a snapshot of a virtual machine scale set instance and managed disk

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Compute:

Expand table

Name **(Azure portal)**	**Description**	**Effect(s)**	**Version** **(GitHub)**
Azure Backup should be enabled for Virtual Machines	Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a secure and cost effective data protection solution for Azure.	AuditIfNotExists, Disabled	3.0.0

Next steps

- See the Microsoft cloud security benchmark overview
- Learn more about Azure security baselines