Azure security baseline for Azure Resource Manager

Article • 02/25/2025

This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Azure Resource Manager. 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 Azure Resource Manager.

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 Azure Resource Manager have been excluded. To see how Azure Resource Manager completely maps to the Microsoft cloud security benchmark, see the full Azure Resource Manager security baseline mapping file .

Security profile

The security profile summarizes high-impact behaviors of Azure Resource Manager, which may result in increased security considerations.

Expand table

Service Behavior Attribute	Value
Product Category	MGMT/Governance
Customer can access HOST / OS	No Access
Service can be deployed into customer's virtual network	False
Stores customer content at rest	False

Network security

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

NS-2: Secure cloud services with network controls

Features

Azure Private Link

Description: Service native IP filtering capability for filtering network traffic (not to be confused with NSG or Azure Firewall). Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Deploy private endpoints to establish a private access point for managing the resources under the root management group (tenant).

Note: Resource Management Private Link resources can be connected to a private endpoint to enable secure, private access for managing Azure resources.

Reference: Create a private link for managing Azure resources

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
False	Not Applicable	Not Applicable

Feature notes: Azure Resource Manager supports private connectivity through Azure private endpoints and the Resource Management Private Links resource. However, the ability to disable public network access is not yet available.

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

Privileged access

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

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
False	Not Applicable	Not Applicable

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

Data protection

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

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	True	Microsoft

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

Reference: Migrating to TLS 1.2 for Azure Resource Manager

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

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

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

Reference: Azure Policy built-in definitions for Azure Resource Manager

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: Microsoft Defender for Resource Manager monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity.

Reference: Overview of Microsoft Defender for Resource Manager

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Resources:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for App Service should be enabled	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3

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: Enable resource logs for Azure Resource Manager. When you create and manage resources in Azure, your requests are orchestrated through Azure's control plane, Azure Resource Manager. With resource logging you can monitor the volume and latency of control plane requests made to Azure. With these metrics, you can observe traffic and latency for control plane requests throughout your subscriptions. For example, you can now figure out when your requests have been throttled or failed by filtering for specific status codes.

Reference: Azure Resource Manager metrics in Azure Monitor

Backup and recovery

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

BR-1: Ensure regular automated backups

Features

Service Native Backup Capability

Description: Service supports its own native backup capability (if not using Azure Backup). Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: Azure Resource Manager template export can't be used to capture data at rest. For resource configurations, we recommend that you create infrastructure from source templates and that when required, you redeploy from that source of truth. Template Export can help bootstrap that process, but it is not robust enough to account for disaster recovery.

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

Next steps

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