

Azure security baseline for Storage

Article • 02/25/2025

This security baseline applies guidance from the [Microsoft cloud security benchmark version 1.0](#) to Storage. 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 Storage.

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 Storage have been excluded. To see how Storage completely maps to the Microsoft cloud security benchmark, see the [full Storage security baseline mapping file](#) .

Security profile

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

 Expand table

Service Behavior Attribute	Value
Product Category	Storage

Service Behavior Attribute	Value
Customer can access HOST / OS	No 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
False	Not Applicable	Not Applicable


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

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 for Azure Storage to establish a private access point for the resources.

Reference: [Use private endpoints for Azure Storage](#)

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

Configuration Guidance: Disable public network access by either using Azure Storage service-level IP ACL filtering or a toggling switch for public network access.

Reference: [Change the default network access rule](#)

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	True	Microsoft

Feature notes: Storage offers multiple ways to authorize to the data plane. Azure provides Azure role-based access control (Azure RBAC) for fine-grained control over a client's access to resources in a storage account. Use Azure AD credentials when possible as a security best practice, rather than using the account key, which can be more easily compromised. When your application design requires shared access signatures for access to Blob storage, use Azure AD credentials to create user delegation shared access signatures (SAS) when possible for superior security.

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

Reference: [Authorize access to data in Azure Storage](#)

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	False	Customer

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: Restrict the use of local authentication methods for data plane access. Instead, use Azure Active Directory (Azure AD) as the default authentication method to control your data plane access.


Reference: [SFTP permission model](#)

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: [Authorize access to blob data with 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

Additional Guidance: With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.

Reference: [Authorize access to blobs using Azure Active Directory](#)

IM-7: Restrict resource access based on conditions

Features

Conditional Access for Data Plane

Description: Data plane access can be controlled using Azure AD Conditional Access Policies. [Learn more.](#)

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Define the applicable conditions and criteria for Azure Active Directory (Azure AD) conditional access in the workload. Consider common use cases such as blocking or granting access from specific locations, blocking risky sign-in behavior, or requiring organization-managed devices for specific applications.

Reference: [Disallow Shared Key authorization to use Azure AD Conditional Access](#)

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

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.

Reference: [Manage storage account keys with Key Vault and the Azure CLI](#)

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
False	Not Applicable	Not Applicable


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

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: Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal.

Authorizing requests against Azure Storage with Azure AD provides superior security and ease of use over Shared Key authorization. Microsoft recommends using Azure AD authorization with your blob applications when possible to assure access with minimum required privileges.

Reference: [Authorize access to blobs using Azure Active Directory](#)

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.

Reference: [Customer Lockbox](#)

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
True	False	Customer

Feature notes: Storage integration with Azure purview is currently in private preview.

Configuration Guidance: Use Azure Purview to scan, classify and label any sensitive data that resides in Azure Storage.

Reference: [Connect to Azure Blob storage in Microsoft Purview](#)

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
True	False	Customer

Configuration Guidance: Defender for Storage continually analyzes the telemetry stream generated by the Azure Blob Storage and Azure Files services. When potentially malicious activities are detected, security alerts are generated. These alerts are displayed in Microsoft Defender for Cloud, together with the details of the suspicious activity along with the relevant investigation steps, remediation actions, and security recommendations.

Microsoft Defender for Storage is built into Microsoft Defender for Cloud. When you enable Microsoft Defender for Cloud's enhanced security features on your subscription, Microsoft Defender for Storage is automatically enabled for all of your storage accounts. You may enable or disable Defender for Storage for individual storage accounts under a specific subscription.

Reference: [Configure Microsoft Defender for Storage](#)

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: [Enforce a minimum required version of Transport Layer Security \(TLS\) for requests to a storage account](#)

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.


Reference: [Azure Storage encryption for data at rest](#)

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 for the in-scope data using customer-managed key for Azure Storage

Reference: [Customer-managed keys for Azure Storage 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: [Manage storage account keys with Key Vault and the Azure CLI](#)

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: Define and implement standard security configurations for network resources associated with your Azure Storage Account with Azure Policy. Use Azure Policy aliases in the "Microsoft.Storage" and "Microsoft.Network" namespaces to create custom policies to audit or enforce the network configuration of your Storage account resources.

You may also make use of built-in policy definitions related to Storage account, such as: Storage Accounts should use a virtual network service endpoint

Reference: [Azure Policy built-in definitions for Azure Storage](#)

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: Use Microsoft Defender for Storage to provide an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit storage accounts. It uses advanced threat detection capabilities and Microsoft Threat Intelligence data to provide contextual security alerts. Those alerts also include steps to mitigate the detected threats and prevent future attacks.

Reference: [Introduction to Microsoft Defender for Storage](#)

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: Ingest logs via Azure Monitor to aggregate security data generated by endpoints devices, network resources, and other security systems. Within Azure Monitor, use Log Analytics Workspace(s) to query and perform analytics, and use Azure Storage Accounts for long-term/archival storage, optionally with security features such as immutable storage and enforced retention holds.

Reference: [Monitoring Azure Blob Storage](#)

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: Azure Backup is currently only supported for Azure Blob storage. Queue and table data can be backed up by using the AzCopy command line tool.

Configuration Guidance: Enable Azure Backup and configure the backup source on a desired frequency and with a desired retention period. Azure Backup lets you easily configure operational backup for protecting block blobs in your storage accounts. Backup of blobs is configured at the storage account level. So, all blobs in the storage account are protected with operational backup.

You can configure backup for multiple storage accounts using the Backup Center. You can also configure backup for a storage account using the storage account’s Data Protection properties.

Reference: [Overview of operational backup for Azure Blobs](#)

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
True	False	Customer

Additional Guidance: Operational backup of blobs is a local backup solution. So the backup data isn't transferred to the Backup vault, but is stored in the source storage account itself. However, the Backup vault still serves as the unit of managing backups. Also, this is a continuous backup solution, which means that you don't need to schedule any backups and all changes will be retained and restorable from the state at a selected point in time.

Reference: [Overview of operational backup for Azure Blobs](#)

Next steps

- See the [Microsoft cloud security benchmark overview](#)
- Learn more about [Azure security baselines](#)