Azure security baseline for Key Vault

Article • 02/25/2025

This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Key Vault. 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 Key Vault.

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

Security profile

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

Expand table

Service Behavior Attribute	Value
Product Category	Security

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
True	False	Customer

Configuration Guidance: Azure Key Vault supports virtual network service endpoints which allows you to restrict the key vault access to a specified virtual network.

Reference: Azure Key Vault Network Security

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.

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 Key Vault to establish a private access point for the resources.

Reference: Azure Key Vault Private Link

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 using the Azure Key Vault firewall IP filtering rules.

Reference: Azure Key Vault network security

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.KeyVault:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Key Vault should have firewall enabled	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: https://docs.microsoft.com/azure/key-vault/general/network-security	Audit, Deny, Disabled	3.2.1

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

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

Reference: Azure Key Vault authentication

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
False	Not Applicable	Not Applicable

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

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: Azure Key Vault authentication

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: It is recommended to use managed identities instead of service principals. When service principals have to be used, limit the usage to use case scenarios where non-user-based access is required and managed identities are not supported, such as automation flows or 3rd party system integrations.

Reference: Azure Key Vault authentication

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: Azure Key Vault 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: About Azure Key Vault secrets

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: 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: Azure Key Vault RBAC support

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.

Additional Guidance: No Additional configurations are required as this is managed by Azure Platform

Reference: Azure Key Vault security features

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 Key Vault secure store of secrets and keys

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: Azure Key Vault is where you store your keys for customer-managed key (CMK) encryption. You have the option to use either software-protected keys or HSM (hardware security module)-protected keys for your CMK solution.

Note: For customer-managed key and HSM details, please refer to: https://techcommunity.microsoft.com/t5/azure-confidential-computing/azure-key-vault-managed-hsm-control-your-data-in-the-cloud/ba-p/3359310

Reference: Azure Key Vault secure store of secrets and keys

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: Follow the Azure Key Vault best practices to securely manage your key lifecycle in key vault. This includes the key generation, distribution, storage, rotation, and revocation.

Reference: Azure Key Vault key management

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.KeyVault:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Key Vault keys should have an expiration date	Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It is a recommended security practice to set expiration dates on cryptographic keys.	Audit, Deny, Disabled	1.0.2

DP-7: Use a secure certificate management process

Features

Certificate Management in Azure Key Vault

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

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Follow the Azure Key Vault best practice to securely manage your certificate lifecycle in the key vault. This includes the key creation/import, rotation, revocation, storage, and purge of the certificate.

Reference: Azure Key Vault certificate management

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.KeyVault:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Certificates should have the specified maximum validity period	Manage your organizational compliance requirements by specifying the maximum amount of time that a certificate can be valid within your key vault.	audit, Audit, deny, Deny, disabled, Disabled	2.2.1

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: Use Microsoft Defender for Cloud to configure Azure Policy to audit and enforce configurations of your Azure Key Vault. Use Azure Monitor to create alerts when there is a configuration deviation detected on the resources. Use Azure Policy [deny] and [deploy if not exists] effects to enforce secure configuration across Azure resources.

Reference: Azure Key Vault policy

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: Enable Microsoft Defender for Key Vault, when you get an alert from Microsoft Defender for Key Vault, investigate and respond to the alert.

Reference: Microsoft Defender for Azure Key Vault

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 your key vault. Resource logs for Azure Key Vault can log key operation activities such as key creation, retrieve, and deletion.

Reference: Azure Key Vault logging

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
False	Not Applicable	Not Applicable

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

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: Use Azure Key Vault native backup feature to backup your secrets, keys, and certificates and ensure the service is recoverable using the backup data.

Reference: Azure Key Vault backup

Next steps

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