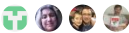


Encryption decision guide

02/11/2019 • 7 minutes to read • Contributors 

In this article

- Key management
- Data encryption
- Learn more
- Next steps

Encrypting data protects it against unauthorized access. Properly implemented encryption policy provides additional layers of security for your cloud-based workloads and guards against attackers and other unauthorized users from both inside and outside your organization and networks.

Jump to: [Key management](#) | [Data encryption](#) | [Learn more](#)

Cloud encryption strategy focuses on corporate policy and compliance mandates. Encrypting resources is desirable, and many Azure services such as Azure Storage and Azure SQL Database enable encryption by default. However, encryption has costs that can increase latency and overall resource usage.

For demanding workloads, striking the correct balance between encryption and performance, and determining how data and traffic is encrypted can be essential. Encryption mechanisms can vary in cost and complexity, and both technical and policy requirements can influence your decisions on how encryption is applied and how you store and manage critical secrets and keys.

Corporate policy and third-party compliance are the biggest drivers when planning an encryption strategy. Azure provides multiple standard mechanisms that can meet common requirements for encrypting data, whether at rest or in transit. However, for policies and compliance requirements that demand tighter controls, such as standardized secrets and key management, encryption in-use, or data-specific encryption, you will need to develop a more sophisticated encryption strategy to support these requirements.

Key management

Encryption of data in the cloud depends on the secure storage, management, and operational use of encryption keys. A key management system is critical to your organization's ability to create, store, and manage cryptographic keys, as well important passwords, connection strings, and other IT confidential information.

Modern key management systems such as Azure Key Vault support storage and management of software protected keys for dev and test usage and hardware security module (HSM) protected keys for maximum protection of production workloads or sensitive data.

When planning a cloud migration, the following table can help you decide how to store and manage encryption keys, certificates, and secrets, which are critical for creating secure and manageable cloud deployments:

Question	Cloud-native	Bring your own key	Hold your own key
Does your organization lack centralized key and secret management?	Yes	No	No
Will you need to limit the creation of keys and secrets to devices to your on-premises hardware, while using these keys in the cloud?	No	Yes	No

Question	Cloud-native	Bring your own key	Hold your own key
Does your organization have rules or policies in place that would prevent keys from being stored offsite?	No	No	Yes

Cloud-native

With cloud-native key management, all keys and secrets are generated, managed, and stored in a cloud-based vault such as Azure Key Vault. This approach simplifies many IT tasks related to key management, such as key backup, storage, and renewal.

Using a cloud-native key management system includes these assumptions:

- You trust the cloud key management solution with creating, managing, and hosting your organization's secrets and keys.
- You enable all on-premises applications and services that rely on accessing encryption services or secrets to access the cloud key management system.

Bring your own key

With a bring your own key approach, you generate keys on dedicated HSM hardware within your on-premises environment, then securely transferring these keys to a cloud-based management system such as Azure Key Vault for use with your cloud-hosted resources.

Bring your own key assumptions: Generating keys on-premises and using them with a cloud-based key management system includes these assumptions:

- You trust the underlying security and access control infrastructure of the cloud platform for hosting and using your keys and secrets.
- Your cloud-hosted applications or services are able to access and use keys and secrets in a robust and secure way.
- You are required by regulatory or organizational policy to keep the creation and management of your organization's secrets and keys on-premises.

On-premises (hold your own key)

In certain scenarios, there may be regulatory, policy, or technical reasons why you can't store keys on a cloud-based key management system. In these cases, you must generate keys using on-premises hardware, store and manage them using an on-premises key management system, and provision a mechanism to allow cloud-based resource to access these keys for encryption purposes. Note that holding your own key may not be compatible with all Azure-based services.

On-premises key management assumptions: Using an on-premises key management system includes these assumptions:

- You are required by regulatory or organizational policy to keep the creation, management, and hosting of your organization's secrets and keys on-premises.
- Any cloud-based applications or services that rely on accessing encryption services or secrets can access the on-premises key management system.

Data encryption

There are several different states of data with different encryption needs to consider when planning your encryption policy:

Data state	Data
Data in transit	Internal network traffic, internet connections, connections between datacenters or virtual networks
Data at rest	Databases, files, virtual drives, PaaS storage
Data in use	Data loaded in RAM or in CPU caches

Data in transit

Data in transit is data moving between resources on the internal, between datacenters or external networks, or over the internet.

Encrypting data in transit is usually done by requiring SSL/TLS protocols for traffic. Traffic transiting between your cloud-hosted resources to external network or the public internet should always be encrypted. PaaS resources generally also enforce SSL/TLS encryption to traffic by default. Whether you enforce encryption for traffic between IaaS resources hosted inside your virtual networks is a decision for your cloud adoption teams and workload owners and is generally recommended.

Assumptions about encrypting data in transit: Implementing proper encryption policy for data in transit assumes the following:

- All publicly accessible endpoints in your cloud environment will communicate with the public internet using SSL/TLS protocols.
- When connecting cloud networks with on-premises or other external network over the public internet, use encrypted VPN protocols.
- When connecting cloud networks with on-premises or other external network using a dedicated WAN connection such as ExpressRoute, you will use a VPN or other encryption appliance on-premises paired with a corresponding virtual VPN or encryption appliance deployed to your cloud network.
- If you have sensitive data that shouldn't be included in traffic logs or other diagnostics reports visible to IT staff, you will encrypt all traffic between resources in your virtual network.

Data at rest

Data at rest represents any data not being actively moved or processed, including files, databases, virtual machine drives, PaaS storage accounts, or similar assets. Encrypting stored data protects virtual devices or files against unauthorized access either from external network penetration, rogue internal users, or accidental releases.

PaaS storage and database resources generally enforce encryption by default. IaaS resources can be secured by encrypting data at the virtual disk level or by encrypting the entire storage account hosting your virtual drives. All of these assets can make use of either Microsoft-managed or customer-managed keys stored in Azure Key Vault.

Encryption for data at rest also encompasses more advanced database encryption techniques, such as column-level and row level encryption, providing much more control over exactly what data is being secured.

Your overall policy and compliance requirements, the sensitivity of the data being stored, and the performance requirements of your workloads should determine which assets require encryption.

Assumptions about encrypting data at rest. Encrypting data at rest assumes the following:

- You are storing data that is not meant for public consumption.
- Your workloads can accept the added latency cost of disk encryption.

Data in use

Encryption for data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. Use of technologies such as full memory encryption, enclave technologies, such as Intel's Secure Guard Extensions (SGX). This also includes cryptographic techniques, such as homomorphic encryption that can be used to create secure, trusted execution environments.

Assumptions about encrypting data in use: Encrypting data in use assumes the following:

- You are required to maintain data ownership separate from the underlying cloud platform at all times, even at the RAM and CPU level.

Learn more

For more information about encryption and key management in Azure, see:

- [Azure encryption overview](#). A detailed description of how Azure uses encryption to secure both data at rest and data in transit.
- [Azure Key Vault](#). Key Vault is the primary key management system for storing and managing cryptographic keys, secrets, and certificates within Azure.
- [Azure Data Security and Encryption Best Practices](#). A discussion of Azure data security and encryption best practices.
- [Confidential computing in Azure](#). Azure's confidential computing initiative provides tools and technology to create trusted execution environments or other encryption mechanisms to secure data in use.

Next steps

Encryption is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the [decision guides overview](#) to learn about alternative patterns or models used when making design decisions for other types of infrastructure.

Architectural decision guides