200 XP

Encryption

10 minutes

Data is an organization's most valuable and irreplaceable asset, and encryption serves as the last and strongest line of defense in a layered security strategy. Being a healthcare provider, Lamna Healthcare stores large amounts of sensitive data. They recently experienced a breach that exposed the unencrypted sensitive data of patients, and are now fully aware that they have gaps in their data protection capabilities. They want to understand how they could have better used encryption to protect themselves and their patients from this type of incident. Here, we'll take a look at what encryption is, how to approach the encryption of data, and what encryption capabilities are available on Azure.

What is encryption?

Encryption is the process of making data unreadable and unusable. To use or read the encrypted data, it must be *decrypted*, which requires the use of a secret key. There are two top-level types of encryption: **Symmetric** and **Asymmetric**.

Symmetric encryption uses the same key to encrypt and decrypt the data. Consider a desktop password manager application. You enter your passwords and they are encrypted with your own personal key (your key is often derived from your master password). When the data needs to be retrieved, the same key is used and the data is decrypted.

Asymmetric encryption uses a public key and private key pair. Either key can encrypt but cannot decrypt its own encrypted data. To decrypt, you need the paired key. Asymmetric encryption is used for things like TLS (used in https), and data signing.

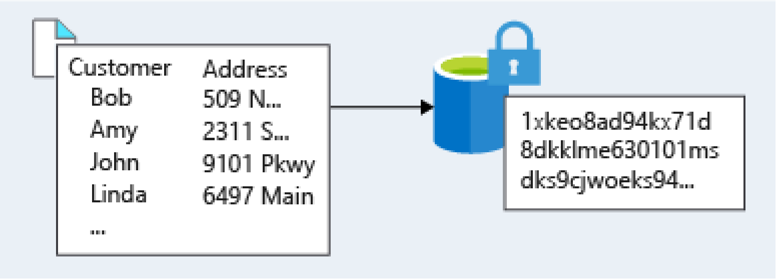
Both symmetric and asymmetric encryption play a role in properly securing your data.

Encryption is typically approached in two ways: encryption at rest and encryption in transit.

Encryption at rest

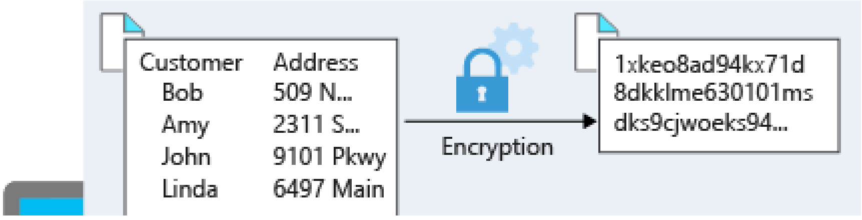
Data at rest is the data that has been stored on a physical medium. This could be data stored on the disk of a server, data stored in a database, or data stored in a storage account. Regardless of the storage mechanism, encryption of data at rest ensures that the stored data is unreadable without the keys and secrets needed to decrypt it. If an attacker were to obtain a hard drive with encrypted data and did not have access to the encryption keys, the attacker would not compromise the data without great difficulty. In such a scenario, an attacker would have to attempt attacks against encrypted data, which are much more complex and resource consuming than accessing unencrypted data on a hard drive.

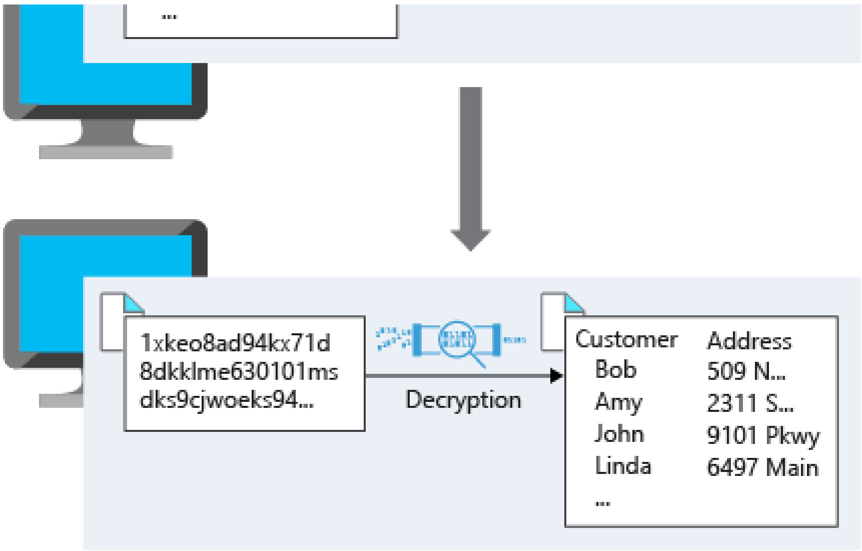
The actual data that is encrypted could vary in its content, usage, and importance to the organization. This could be financial information critical to the business, intellectual property that has been developed by the business, personal data that the business stores about customers or employees, and even the keys and secrets used for the encryption of the data itself.



Encryption in transit

Data in transit is the data actively moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by encrypting the data prior to sending it over a network, or setting up a secure channel to transmit unencrypted data between two systems. Encrypting data in transit protects the data from outside observers and provides a mechanism to transmit data while limiting risk of exposure.





Identify and classify data

Let's revisit the problem Lamna Healthcare is attempting to solve. They have had previous incidents that exposed sensitive data, so there's a gap between what they are encrypting and what they should be encrypting. They need to start by identifying and classifying the types of data they are storing, and align this with the business and regulatory requirements surrounding the storage of data. It's beneficial to classify this data as it relates to the impact of exposure to the organization, its customers, or partners. An example classification could be as follows:

Data classification	Explanation	Examples
Restricted	Data classified as restricted poses significant risk if exposed, altered, or deleted. Strong levels of protection are required for this data.	Data containing Social Security numbers, credit card numbers, personal health records
Private	Data classified as private poses moderate risk if exposed, altered, or deleted. Reasonable levels of protection are required for this data. Data that is not classified as restricted or public will be classified as private.	Personal records containing information such as address, phone number, academic records, customer purchase records
Public	Data classified as public poses no risk if exposed,	Public financial reports,

Data classification	Explanation	Examples
	altered, or deleted. No protection is required for this data.	public policies, product documentation for customers

By taking an inventory of the types of data being stored, they can get a better picture of where sensitive data may be stored and where existing encryption may or may not be happening.

A thorough understanding of the regulatory and business requirements that apply to data the organization stores is also important. The regulatory requirements an organization must adhere to will often drive a large part of the data encryption requirements. For Lamna Healthcare, they are storing sensitive data that falls under the Health Insurance Portability and Accountability Act (HIPAA), which contains requirements on how to handle and store patient data. Other industries may fall under different regulatory requirements. A financial institution may store account information that falls within Payment Card Industry (PCI) standards. An organization doing business in the EU may fall under the General Data Protection Regulation (GDPR), which defines the handling of personal data in the EU. Business requirements may also dictate that any data that could put the organization at financial risk containing competitive information needs to be encrypted.

Once you have the data classified and your requirements defined, you can then take advantage of various tools and technologies to implement and enforce encryption in your architecture.

Encryption on Azure

Let's take a look at some ways that Azure enables you to encrypt data across services.

Encrypting raw storage

Azure Storage Service Encryption for data at rest helps you protect your data to meet your organizational security and compliance commitments. With this feature, the Azure storage platform automatically encrypts your data before persisting it to Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage, and decrypts the data before retrieval. The handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is transparent to applications using the services.

For Lamna Healthcare, this means that whenever they are using services that support storage service encryption, their data is encrypted on the physical medium of storage. In the highly unlikely event that access to the physical disk is obtained, data will be unreadable since it has been encrypted as written to the physical disk.

Encrypting virtual machines

Storage Service encryption provides low-level encryption protection for data written to physical disk, but how do you protect the virtual hard disks (VHD) of virtual machines? If a malicious attacker gained access to your Azure subscription and exfiltrated the VHDs of your virtual machines, how would you ensure they would be unable to access data stored on the VHD?

Azure Disk Encryption (ADE) is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks. ADE leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets (and you can use managed identity for Azure services for accessing the key vault).

Lamna Healthcare can apply ADE to their virtual machines to be sure any data stored on VHDs is secured to their organizational and compliance requirements. Because boot disks are also encrypted, they can control and audit usage.

Encrypting databases

Lamna Healthcare has several databases deployed that store data that needs additional protection. They've moved many databases to Azure SQL Database and want to ensure that their data is encrypted within their database. If the data files, log files, or backup files were stolen, they want to ensure they are unreadable without access to the encryption keys.

Transparent data encryption (TDE) helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. By default, TDE is enabled for all newly deployed Azure SQL Databases.

TDE encrypts the storage of an entire database by using a symmetric key called the database encryption key. By default, Azure provides a unique encryption key per logical SQL Server and handles all the details. Bring-your-own-key is also supported with keys stored in Azure Key Vault.

Since TDE is enabled by default, Lamna Healthcare can be confident they have the proper protections in place for data stored in their databases.

Encrypting secrets

We've seen that the encryption services all use keys to encrypt and decrypt data, so how do we ensure that the keys themselves are secure? Lamna Healthcare may also have passwords, connection strings, or other sensitive pieces of information that they need to securely store connection strings, or other sensitive pieces of information that they need to securely store.

Azure Key Vault is a cloud service that works as a secure secrets store. Key Vault allows you to create multiple secure containers, called vaults. These vaults are backed by hardware security modules (HSMs). Vaults help reduce the chances of accidental loss of security information by centralizing the storage of application secrets. Key Vaults also control and log the access to anything stored in them. Azure Key Vault can handle requesting and renewing Transport Layer Security (TLS) certificates, providing the features required for a robust certificate lifecycle management solution. Key Vault is designed to support any type of secret. These secrets could be passwords, database credentials, API keys and, certificates.

Because Azure AD identities can be granted access to use Azure Key Vault secrets, applications using managed identities for Azure services can automatically and seamlessly acquire the secrets they need.

Lamna Healthcare can use Key Vault for the storage of all their sensitive application information, including the TLS certificates they use to secure communication between systems.

Encryption at Lamna Healthcare

Lamna Healthcare has gone through the identification and classification process for all the data they are storing. They've aligned these classifications with the regulatory and business requirements, and realized they have far more data they have to encrypt. They have encrypted all virtual machines that are storing sensitive data, and are encrypting all sensitive patient information they are storing on blob storage. TDE is enabled on all of their databases, so their relational databases meet their encryption requirements regardless of classification. They have also worked across the organization use Key Vault to store all certificates and credential information that applications may need for operation.

Summary

Encryption is often the last layer of defense from attackers, and is an important piece of a layered approach to securing your architecture. Azure provides built-in capabilities and services to encrypt and protect data from unintended exposure. Protection of customer data stored within Azure Services is of paramount importance to Microsoft and should be included in any architecture design. Foundational services such as Azure Storage, Azure Virtual Machines, Azure SQL Database, and Azure Key Vault can help secure your environment through encryption.

Check your knowledge

1. True or false: only Windows virtual machines can use Azure Disk Encryption

○ True

○ False

2. When classifying data, which of the following is a factor?

○ Level of risk posed to customers if exposed

○ Method of data transport

○ Whether the data is stored on virtual machines or in a database

○ The amount of data stored

Check your answers