Microsoft

What enterprise Legal and Compliance leaders need to know about encryption in Microsoft cloud

Encryption fundamentals

Every organization has legitimate secrets it needs to protect

These secrets fall into three categories:

1. Confidential business information
2. Highly regulated personal data (GDPR, HIPAA, etc.)
3. Genuinely top secret information (national security and similar)

Encryption comes in many varieties suited for different purposes, Legal and Compliance leaders in the enterprise must understand their policy implications.

There are good reasons why in most circumstances you should share control of your encryption keys with your cloud provider: you have the option not to, but if you do our cloud will conduct AI-powered scans of your content for dangerous malware and phishing attacks, and also perform indexing and compliance checks for you.

Six Microsoft encryption families

In transit (minimum)

1. Transport Layer encryption: for data pipes

At rest (standard)

2. Disk encryption: protect against device theft or tampering
3. Service encryption: protect customer data in cloud services (Office 365, etc.) from hackers and malicious insiders, comply with data protection laws

In transit and at rest (advanced)

4. Message & file encryption: not only encrypt individual files, but also control what recipients can do with them, audit who sees them (Azure Information Protection, Office Message Encryption)

In use (advanced and experimental)

5. Database encryption: protect data even while database is operating on it; now available with Azure SQL Server
6. Homomorphic encryption: active area of research, may one day allow cloud to scan data for malware and compliance without decrypting it, also train AI while guaranteeing privacy of personal data

Three kinds of encryption keys

Microsoft-managed keys:

Microsoft manages cloud keys on customers behalf; easiest to set up, but still highly secure, suitable for most small and medium organizations.

Customer Key and Bring Your Own Key (BYOK):

Customer manages its own cloud keys, but shares access with Microsoft to permit malware scanning, indexing, compliance (e.g., eDiscovery), emergency recovery; more expensive, requires more customer tech skills, but can aid compliance with data protection laws (e.g., GDPR, HIPAA).

Hold Your Own Key (HYOK):

Customer retains exclusive control on its own premises of keys used for top secret subset of its information (1% or 2%), while continuing to use cloud keys for other sensitive information; imposes extra cost and extra risk (because blocks cloud scanning for malware and compliance), but may be required by some customers.

Encryption requires balancing risks and trust in your cloud partner

Our senior leaders Satya Nadella and Brad Smith have made it unmistakably clear that Microsoft's most fundamental commitment as a company is to earn the trust of our customers.

That's why we are building cybersecurity and privacy into the very foundations of our cloud platform.

When choosing an approach to encryption and the cloud, you should always conduct a reasoned, evidence-based effort to measure and make a realistic comparison of the risks you face.

When you evaluate the potential risk of entrusting your sensitive data to the Microsoft cloud, you should ask **"does the evidence really suggest it could be safer somewhere else?"** We believe the answer is "not likely."

Microsoft

How to choose the right encryption solutions in the Microsoft cloud

All scenarios assume Transport encryption and Disk encryption as minimum defaults

BYOK = Bring Your Own Key

HYOK = Hold Your Own Key

TDE = Transparent Data Encryption

What kinds of information need to be protected?

Standard confidential business information

(IP, strategies, financial data ...)

Service-level encryption:

Microsoft-managed keys (Office 365, Dynamics) or Customer Key (Office 365), TDE (SQL Server)

File and message encryption:

Microsoft-managed keys with Azure Information Protection or Office Message Encryption

Highly regulated information

(GDPR, HIPPA ...)

Service-level encryption:

Customer Key (Office 365), BYOK (Dynamics), TDE (SQL Server)

File and message encryption:

BYOK with Azure Information Protection or Office Message Encryption

Database in use encryption

Always Encrypted

“Top secret” information

(Defense, litigation ... 1% or 2% of all information)

Service-level encryption:

Customer Key (Office 365), BYOK (Dynamics), TDE (SQL Server)

File and message encryption:

HYOK or S/MIME with Azure Information Protection

Database in use encryption

Azure Confidential Computing (Always Encrypted with Secure Enclaves)

Revised 10/30/19

Microsoft

The six kinds of Microsoft encryption

Where encryption happens	What is encrypted	Microsoft products	Comments
In transit	Data pipes	Transport Layer Security protocol & others	TLS and other standard protocols encrypt data as it moves between client sites and our cloud and between our own data centers
At rest	Disk	BitLocker and others	Encryption of storage devices in Azure data centers protects customer data in the event that devices are stolen or tampered with; also helps comply with data protection laws
	Service	Service-level encryption for Office 365, Dynamics 365, Power BI, Azure SQL Database	Goes beyond disk encryption to encrypt all customer data associated with a cloud service; protects data against access by malicious insiders or outside hackers; helps comply with data protection and data residency laws Service-level encryption can use Microsoft-managed keys, or Customer Key/BYOK
In transit & at rest	Documents	Azure Information Protection (AIP) & Office 365 Message Encryption (OME)	AIP and OME use Azure Rights Management to embed "allowable use policies" into encrypted messages and files; senders use these policies to control what recipients can do with documents AIP can be used with Microsoft-managed keys, BYOK, or HYOK OME can be used with Microsoft-managed keys or BYOK
In use	Database	Azure Confidential Computing, Always Encrypted (Database)	Even while being processed by database servers in Azure, customer data can be protected by encryption software or hardware
	Anything	Homomorphic encryption	Microsoft Research is developing new methods that may one day make it feasible to encrypt any kind of data while it is being computed on, thus allowing data to remain encrypted at all times

Microsoft

Advanced encryption options in Microsoft 365 E5

Name	Available	Function	Purpose		
Bring Your Own Key (BYOK)	E3, E5, and E5 Compliance	Customer-controlled encryption and enforcement of access restrictions for Office 365 documents in transit protected with Azure Information Protection	Regulatory compliance	Can Microsoft access data for malware scanning, emergency recovery or law enforcement order?	Yes
Customer Key	E5, or E5 Compliance only	Customer-controlled encryption for Office 365 documents at rest on Microsoft cloud servers	Regulatory compliance		Yes (but not after customer revokes availability key)
Hold Your Own Key (HOYK)	E5, or E5 Compliance only (reguires additional Active Directory Rights Management Services server on premises)	Customer-controlled encryption for Azure data and Office 365 documents at rest and in transit circulating between members of the same organization	Regulatory compliance and protection for top secret information		No

Revised 10/30/19