Learning Path Compliance and Privacy

Addressing Compliance and Privacy - Technical

Daniel von Büren; Technical Specialist Security & Compliance

29.10.2021

Agenda

- Compliance Management
- Data Protection – Technology

Compliance Management

Simplify compliance and reduce risk

Shared responsibility model

■ Customer management of risk

Data classification and data accountability

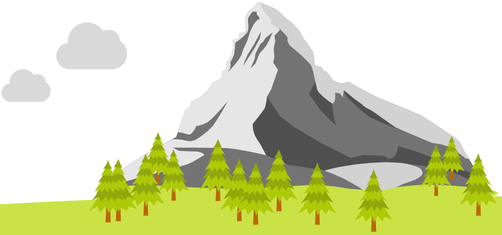
◩ Shared management of risk

Identity & access management | End point devices

□ Provider management of risk

Physical | Networking

■ Cloud customer □ Cloud provider



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	■	■	■	■
Client & end-point protection	■	■	■	◩
Identity & access management	■	■	◩	◩
Application level controls	■	■	◩	□
Network controls	■	◩	□	□
Host infrastructure	■	◩	□	□
Physical security	■	□	□	□

Microsoft Compliance Manager use cases

Data protection baseline

Implement baseline technical, procedural, and people controls to protect your data

IT risk management

Assess and monitor risks in Office 365 and Intune

Regulatory compliance

Assess and maintain controls for data protection regulations (e.g. GDPR, CCPA)

Audits and control assessments

Demonstrate control effectiveness to internal and external auditors

Microsoft Compliance Score

Simplify compliance and reduce risk

Intuitive management

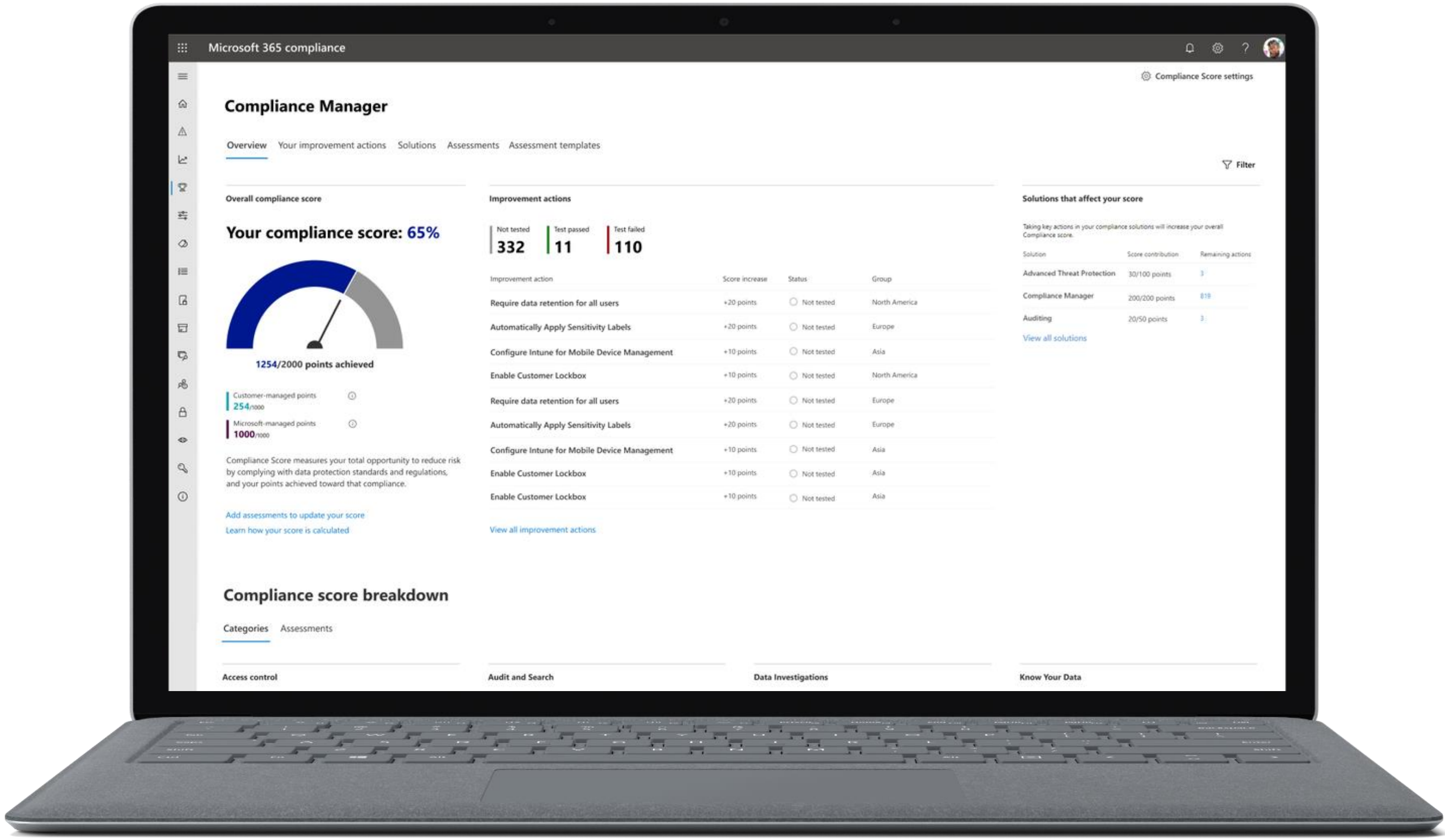
Intuitive end-to-end compliance management from easy onboarding to control implementation

Scalable assessments

Leverage vast out of the box assessment library to meet your unique requirements

Built-in automation

Intelligent automation to reduce risk: compliance score, control mapping and continuous assessments



Microsoft 365 compliance

Compliance Score settings

Compliance Manager

Overview | Your improvement actions | Solutions | Assessments | Assessment templates

Filter

Overall compliance score

Your compliance score: 65%

1254/2000 points achieved

Customer-managed points 254/1000

Microsoft-managed points 1000/1000

Compliance Score measures your total opportunity to reduce risk by complying with data protection standards and regulations, and your points achieved toward that compliance.

Add assessments to update your score

Learn how your score is calculated

Improvement actions

Not tested	Test passed	Test failed
332	11	110

Improvement action	Score increase	Status	Group
Require data retention for all users	+20 points	○ Not tested	North America
Automatically Apply Sensitivity Labels	+20 points	○ Not tested	Europe
Configure Intune for Mobile Device Management	+10 points	○ Not tested	Asia
Enable Customer Lockbox	+10 points	○ Not tested	North America
Require data retention for all users	+20 points	○ Not tested	Europe
Automatically Apply Sensitivity Labels	+20 points	○ Not tested	Europe
Configure Intune for Mobile Device Management	+10 points	○ Not tested	Asia
Enable Customer Lockbox	+10 points	○ Not tested	Asia
Enable Customer Lockbox	+10 points	○ Not tested	Asia

View all improvement actions

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall Compliance score.

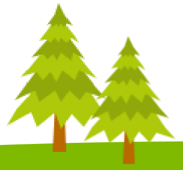
Solution	Score contribution	Remaining actions
Advanced Threat Protection	30/100 points	3
Compliance Manager	200/200 points	819
Auditing	20/50 points	3

View all solutions

Compliance score breakdown

Categories | Assessments

Access control | Audit and Search | Data Investigations | Know Your Data

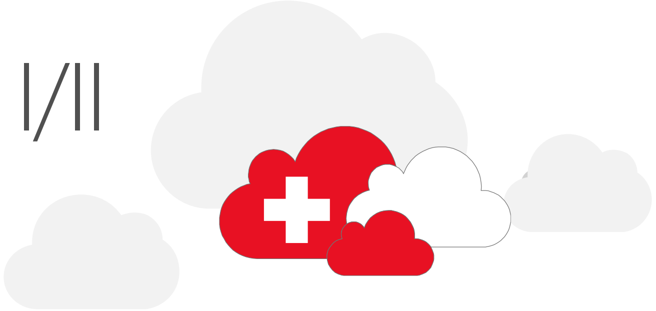


Source: https://compliance.microsoft.com

Data Protection - Technology

How Microsoft supports Data Protection

Data Protection Addendum (DPA) – Encryption I/II



Disclosure of Processed Data

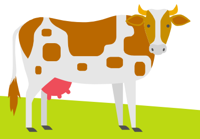
Microsoft will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Professional Services Data; (c) Personal Data; and (d) any other data processed by Microsoft in connection with the Products and Services that is Customer's confidential information under the volume license agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the volume license agreement.

Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

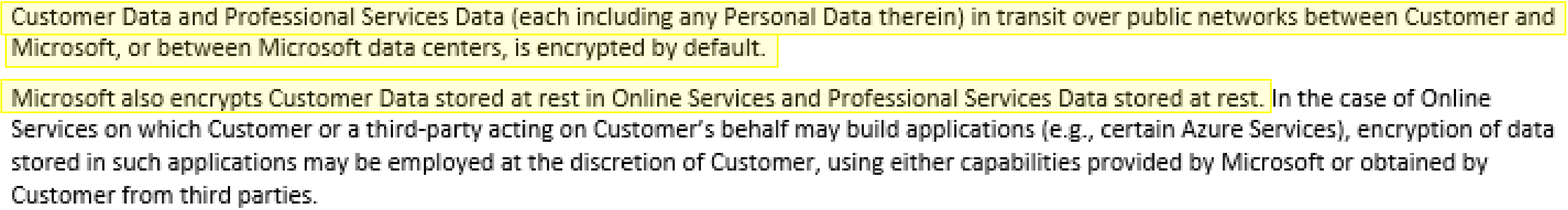
Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.



Data Protection Addendum (DPA) – Encryption II/II

Data Security- Data Encryption



Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

Data Encryption Families

Data Encryption in Transit

Data in transit (in motion) is any data transmitted over the network. This includes data transmitted over an internal network using wired or wireless methods and data transmitted over public networks such as the internet.

Microsoft implementation:

- Transport Layer Security (TLS)
- Message and File Encryption

Data Encryption at Rest

Data at rest is any data stored on media such as system hard drives, external USB drives, storage are networks (SANs), and backup tapes.

Microsoft implementation:

- Disk Encryption (BitLocker/DMCrypt)
- Service Encryption
- Message and File Encryption

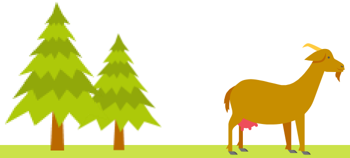
Data Encryption in Use

Data in use refers to data in memory or temporary storage buffers, while an application is using it. Because an application can't process encrypted data, it must decrypt it in memory.

Microsoft implementation:

- Database Encryption
- Azure Confidential Computing
- Homographic Encryption (experimental)

Source: https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption



Types 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.

There is no impact on our services and all functions work as expected.

Bring Your Own Key (BYOK)

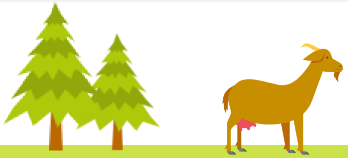
Customer manages its own cloud keys, but shares access with Microsoft to permit malware scanning, indexing, compliance (e.g., eDiscovery), emergency recovery; more expensive, requires more customer tech skills, but can aid compliance with data protection laws (e.g., GDPR, HIPAA).

There is no impact on our services and all functions work as expected.

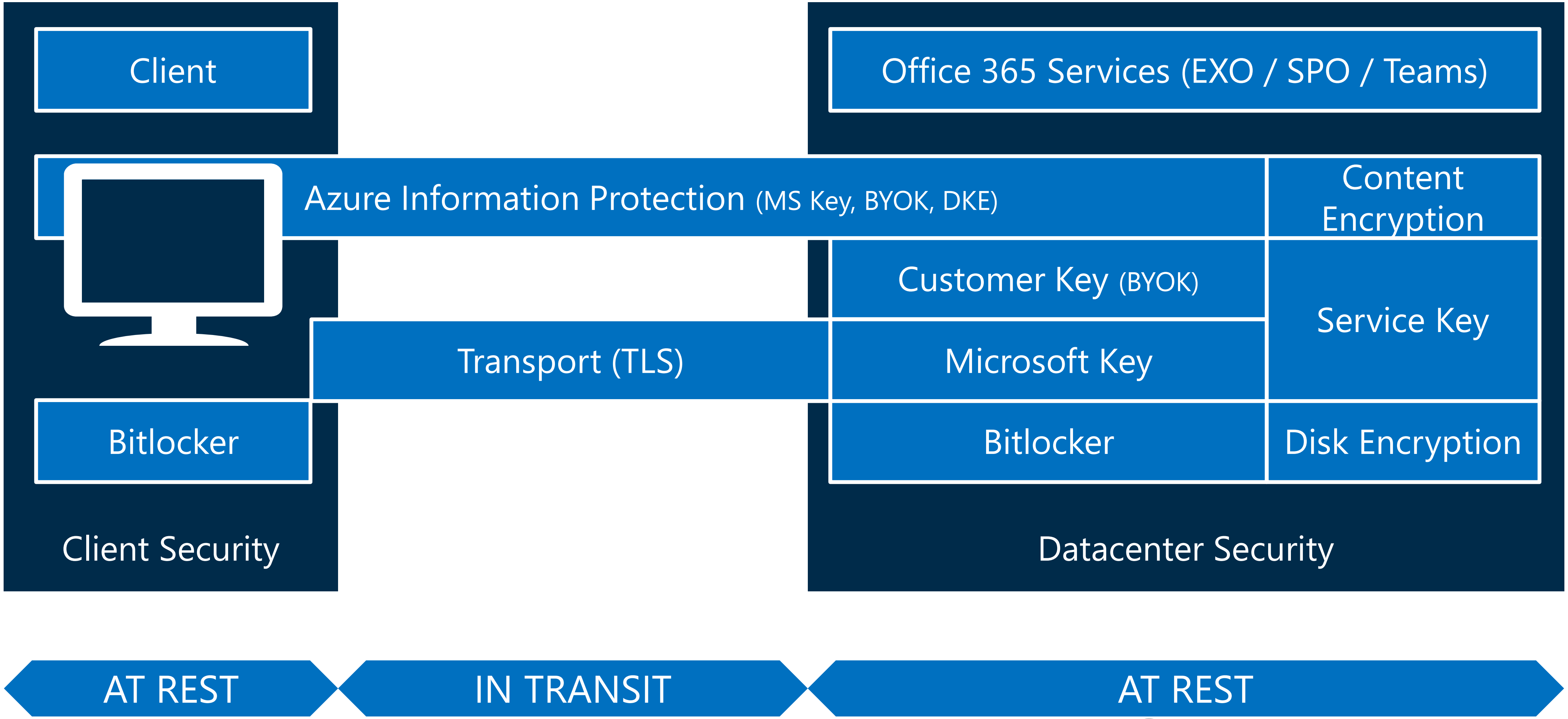
Hold Your Own Key (HYOK)

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.

There is an impact on the services, as data no longer readable (accessible)!



Data Encryption Layers



Client

Office 365 Services (EXO / SPO / Teams)

Azure Information Protection (MS Key, BYOK, DKE)

Content Encryption

Customer Key (BYOK)

Service Key

Transport (TLS)

Microsoft Key

Bitlocker

Bitlocker

Disk Encryption

Client Security

Datacenter Security

AT REST

IN TRANSIT

AT REST

Protect Your Data: Information Protection

Customize protection policies based on data sensitivity

Built-in experiences

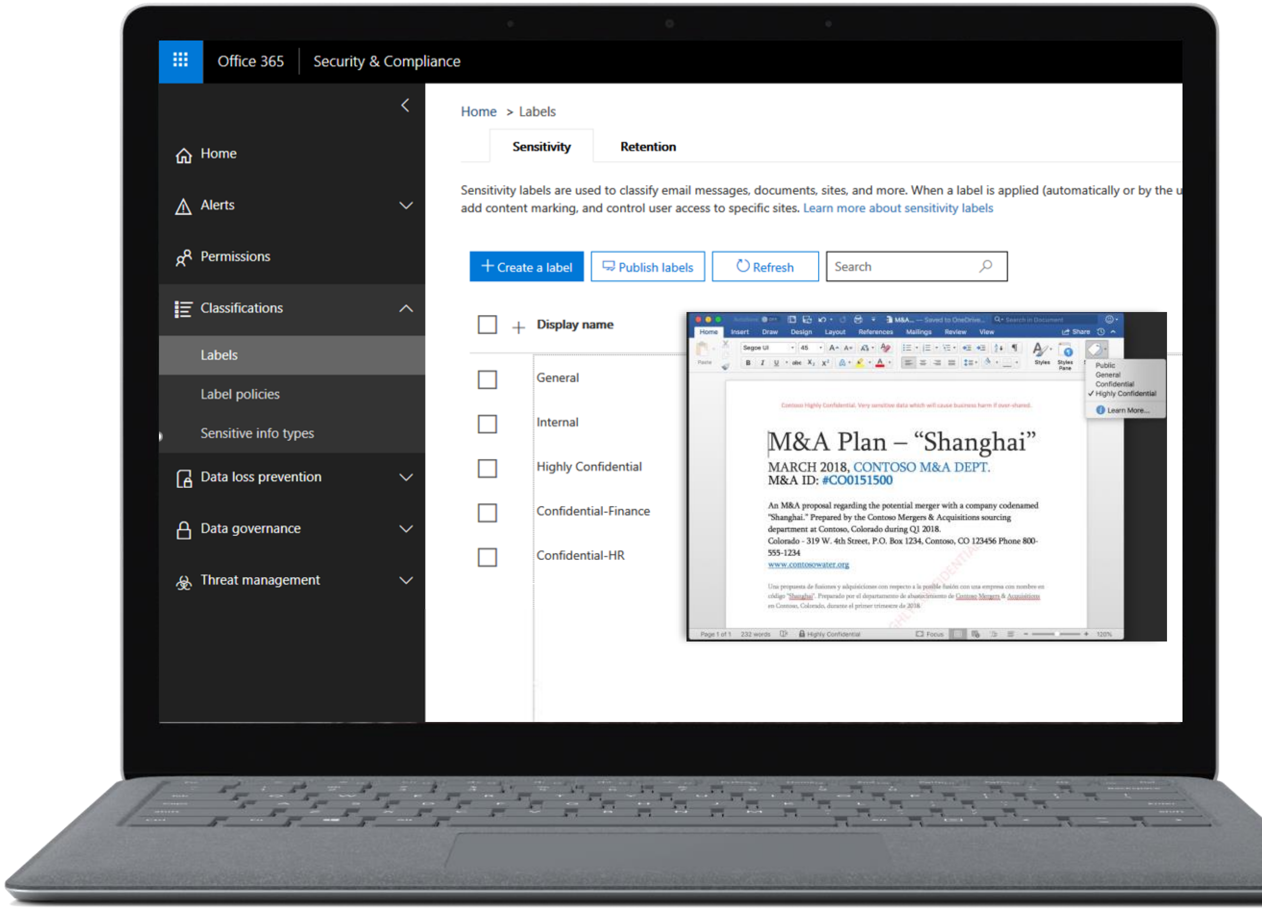
Integrated natively into Office apps, Office 365 services and 3rd-party services

Broad coverage

Protect sensitive information across devices, apps, on-premises file repositories and cloud services

Flexible labeling options

Choose between automatic labeling, manual end-user driven labeling or recommended labeling



Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the u add content marking, and control user access to specific sites. Learn more about sensitivity labels

	Display name
□	General
□	Internal
□	Highly Confidential
□	Confidential-Finance
□	Confidential-HR

Contoso Highly Confidential. Very sensitive data which will cause business harm if over-shared.

M&A Plan – "Shanghai"

MARCH 2018, CONTOSO M&A DEPT.
M&A ID: #CO0151500

An M&A proposal regarding the potential merger with a company codenamed "Shanghai." Prepared by the Contoso Mergers & Acquisitions sourcing department at Contoso, Colorado during Q1 2018.
Colorado - 319 W. 4th Street, P.O. Box 1234, Contoso, CO 123456 Phone 800-555-1234
www.contosowater.org

Una propuesta de fusiones y adquisiciones con respecto a la posible fusión con una empresa con nombre en código "Shanghai". Preparado por el departamento de abastecimiento de Contoso Mergers & Acquisitions en Contoso, Colorado, durante el primer trimestre de 2018.

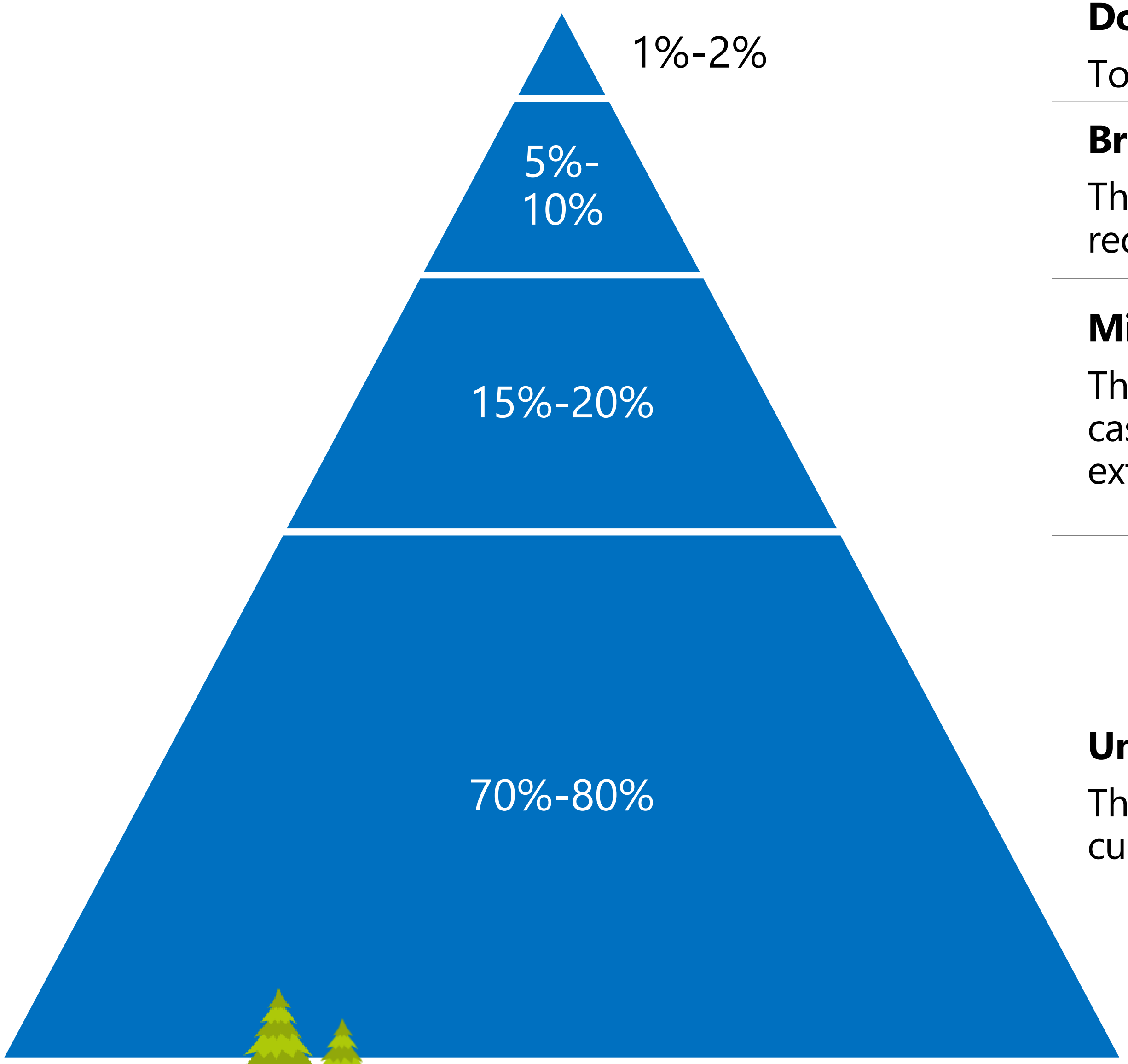
Protect

Apply labels to identify sensitive or proprietary data

- ✓ Customizable
- ✓ Persists as container meta-data or file metadata
- ✓ Enables protection policies like DLP based on labels

- Manual or Automated Labels ✓
- Label data at rest, data in use, or data in transit ✓
- Extensible: readable by other systems ✓

Typical Data Encryption Needs



Double Key Encryption

Top secret data where you can’t trust the provider.

Bring Your Own Key

There are specific internal or external (e.g. regulation) requirements to control data access.

Microsoft Key

There is a need to encrypt data to support specific use cases (e.g. control internal access, collaboration with external partners…).

Unencrypted Data

There is no internal or external regulation require a customer to encrypt those data at rest or even in transit.

Encryption on Dynamics 365 / SQL Databases

Data in Transit

- TLS 1.2 from Client to Service; inside the Microsoft datacenters

Data at Rest

- Field-level data encryption
  Standard Microsoft SQL Server cell level encryption for a set of default entity attributes that contain sensitive information (e.g. usernames, email passwords,…)
- Microsoft SQL Server Transparent Data Encryption (TDE)
  Real-time encryption of data when written to disk (at rest). By default, Microsoft stores and manages the database encryption keys. The manage keys feature in the Dynamics 365 Administration Center gives administrators the ability to self-manage the database encryption keys that are associated with instances of Dynamics 365 (BYOK).

Source: [Encryption in Microsoft Dynamics 365 - Microsoft 365 Compliance | Microsoft Docs]

Servers

Azure Disk Encryption

- Windows Servers
  - BitLocker (full volume encryption)
- Linux
  - DMCrypt (full volume encryption)

Encryption keys and secrets are safeguarded in Azure KeyVault.

Source: [Azure encryption overview | Microsoft Docs]()

Microsoft