Microsoft 365 Information Protection

شركة التزامـــــــن الرقمي
للاتصالات وتقنية المعلومات

AGENDA

1 **Introduction**

2 **Data Lifecycle**

3 **Information Protection**

4 **App Protection**

Microsoft 365 Business Premium

One solution to run your business securely, from anywhere

- Microsoft 365 Business Standard (Office apps and services, Teams)

+

- Microsoft Defender for Office 365
- Intune
- Azure AD Premium Plan 1
- Azure Information Protection Premium P1
- Device Antivirus
- Autopilot
- Windows Virtual Desktop license
- Windows Upgrade rights

Collaborate in real time

Enable secure access to work apps

Protect against cyberthreats and data loss

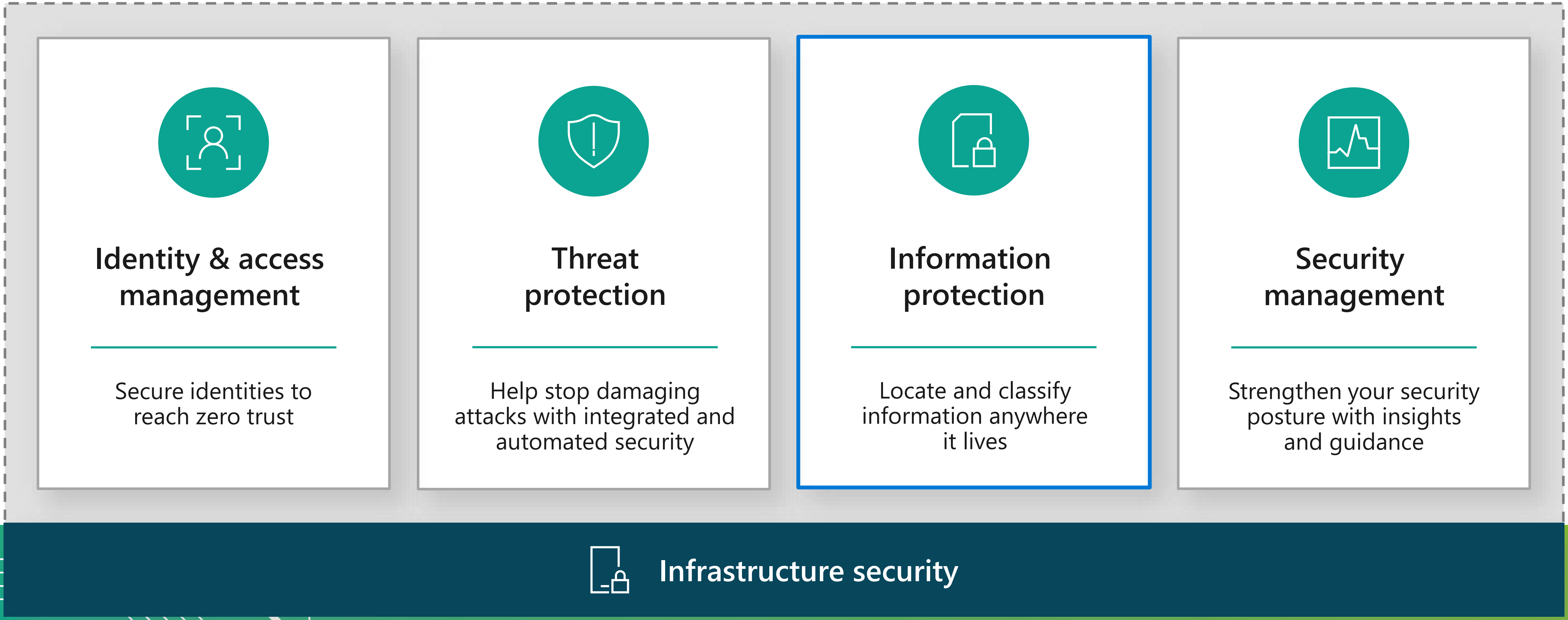
Secure devices that connect to your data

Defender for Business brings enterprise grade information security to Microsoft 365 Business Premium

PRE MDB WITH MDB

		Microsoft 365 Business Premium	Microsoft Defender for Business (MDB)
eDiscovery and Audits	eDiscovery	•	
	Litigation Hold	•	
Information Protection	Email Archiving	•	
	Information Rights Management	•	
	File classification/labeling	•	
	File tracking and revocation	•	
	Message Encryption	•	
Data Loss Prevention	Data Loss Prevention	•	
	Data App Security	•	
Email and Collaboration Security	Safe links	•	
	Safe Attachments	•	
	Anti-phishing	•	
Device management	Windows device setup & management	•[1]	
	Device health analytics	•	
	Mobile Device Management	•	
	Mobile App Management	•	
Identity and Access Management and Security	Risk based Conditional access	•	
	Multi-factor authentication	•	
Device Security	Centralized management	•	•
	Simplified client configuration	•	•
	Next-gen protection	•	•
	Attack Surface Reduction	•	•
	Network Protection	•	•
	Web Category blocking	•	•
	Endpoint detection and response	•	•
	Cross platform support (iOS/Android/Mac)	•[3]	•[3]
	Automated investigation and response	•[2]	•[2]
	Threat and vulnerability	•	•
	Threat intelligence	•[2]	•[2]

Enterprise-class technology



Identity & access management

Secure identities to reach zero trust

Threat protection

Help stop damaging attacks with integrated and automated security

Information protection

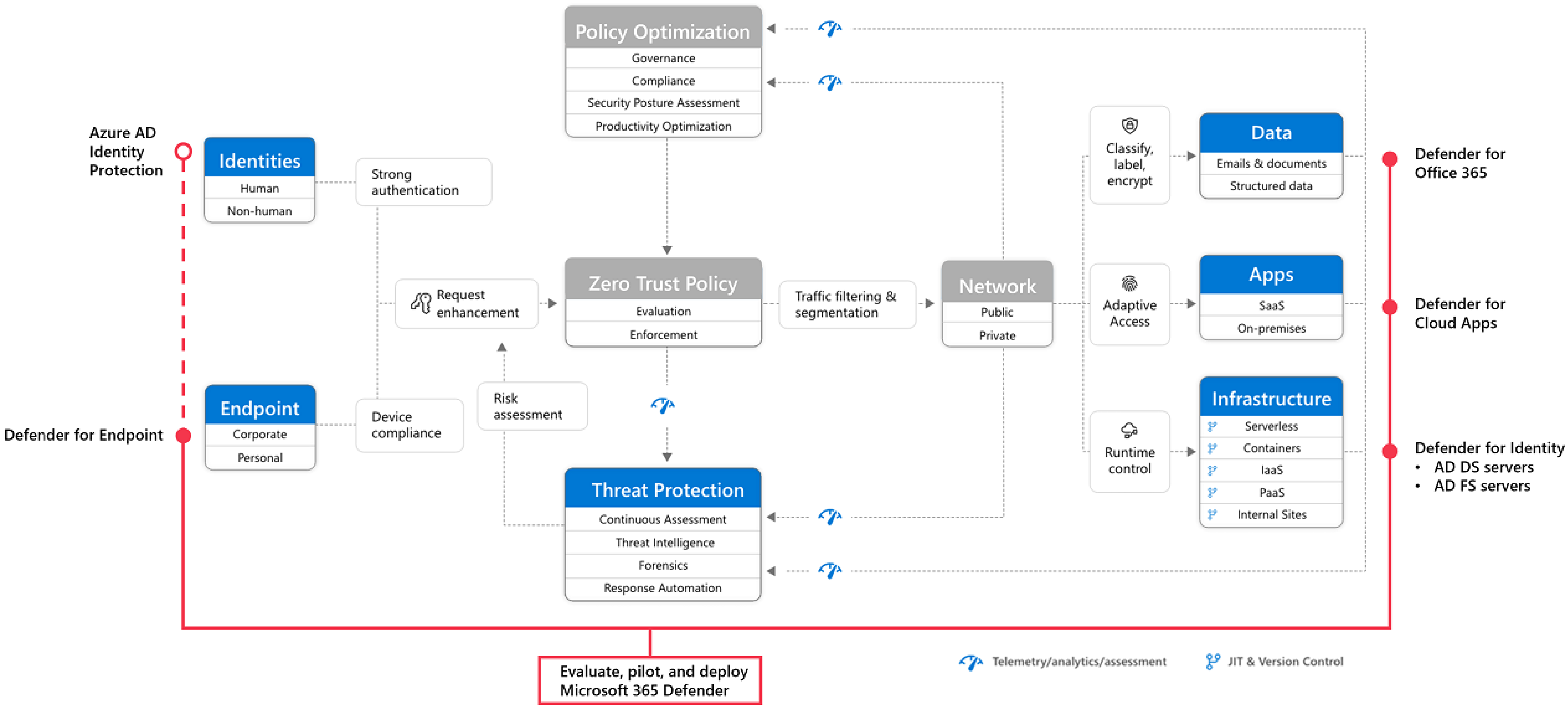
Locate and classify information anywhere it lives

Security management

Strengthen your security posture with insights and guidance

Infrastructure security

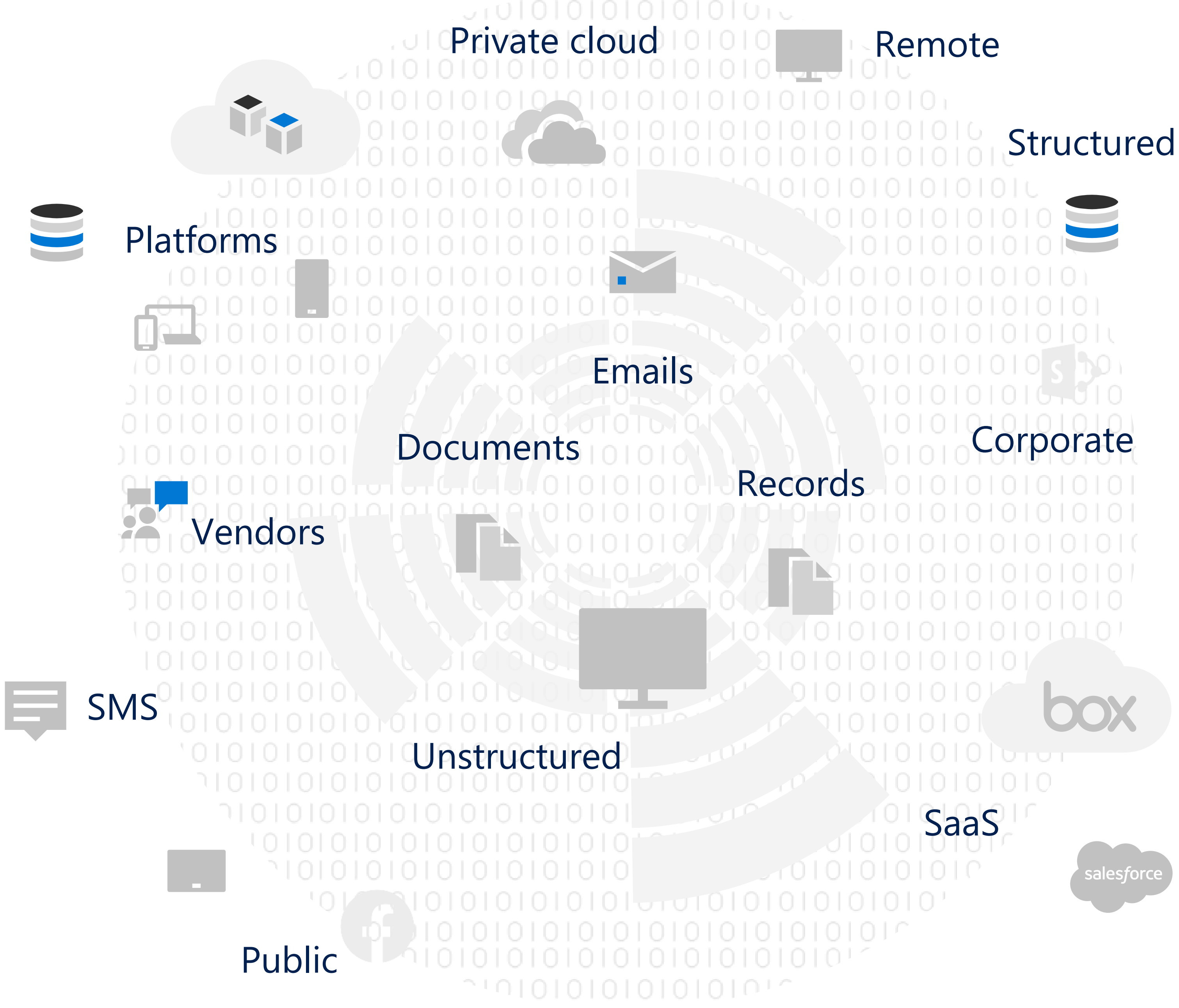
Zero Trust security architecture



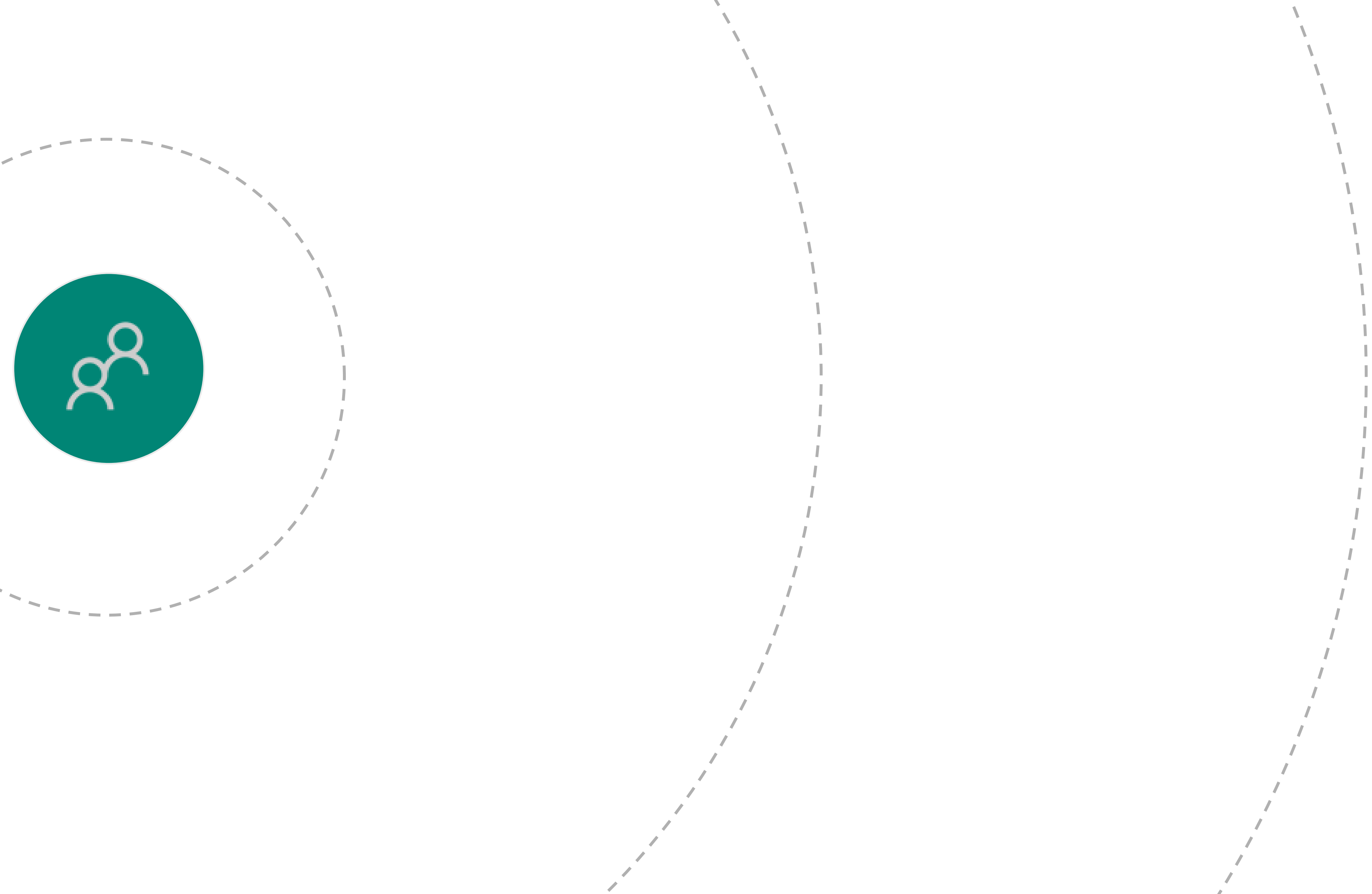
Data Lifecycle

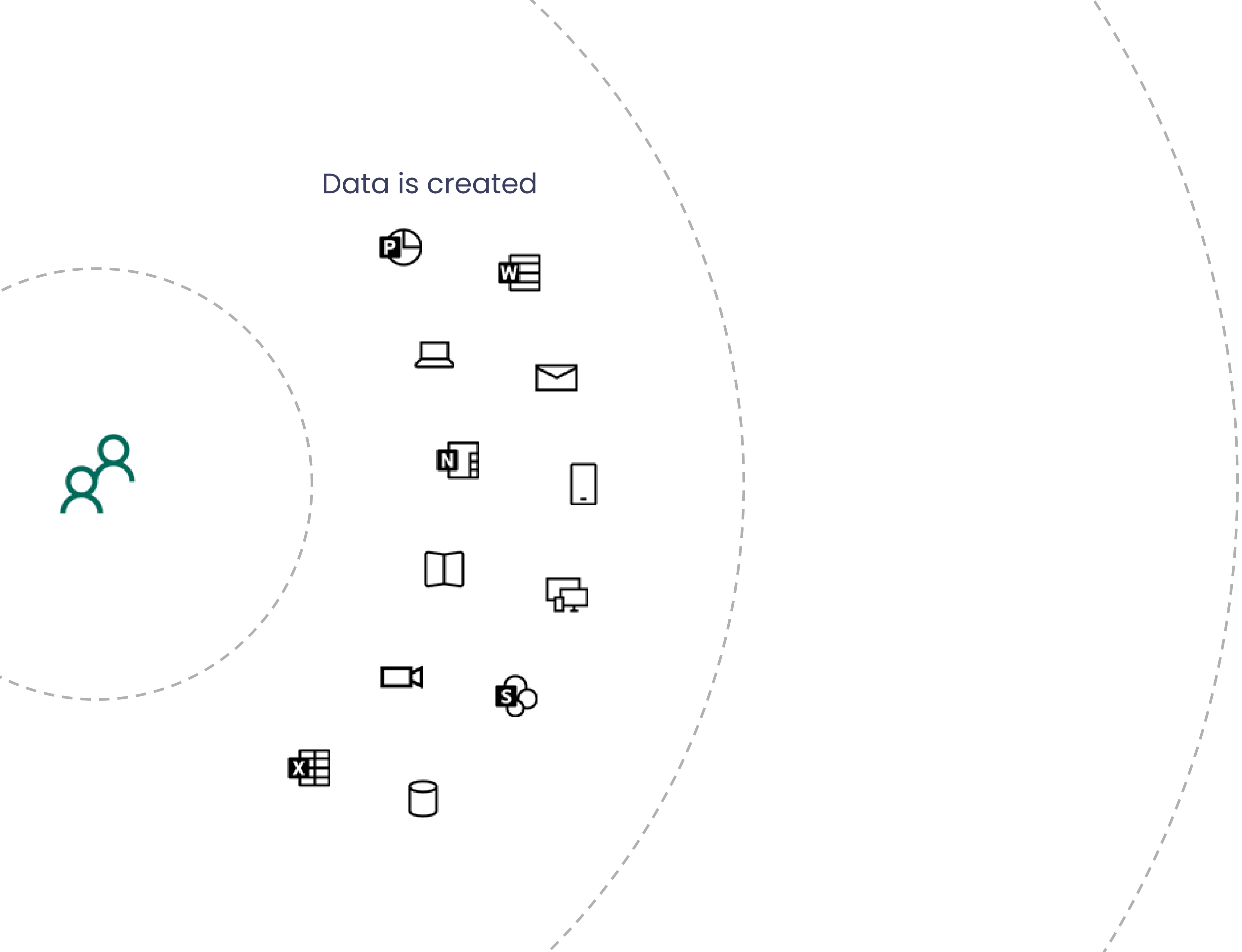
DATA IS EXPLODING

It’s created, stored, and shared EVERYWHERE

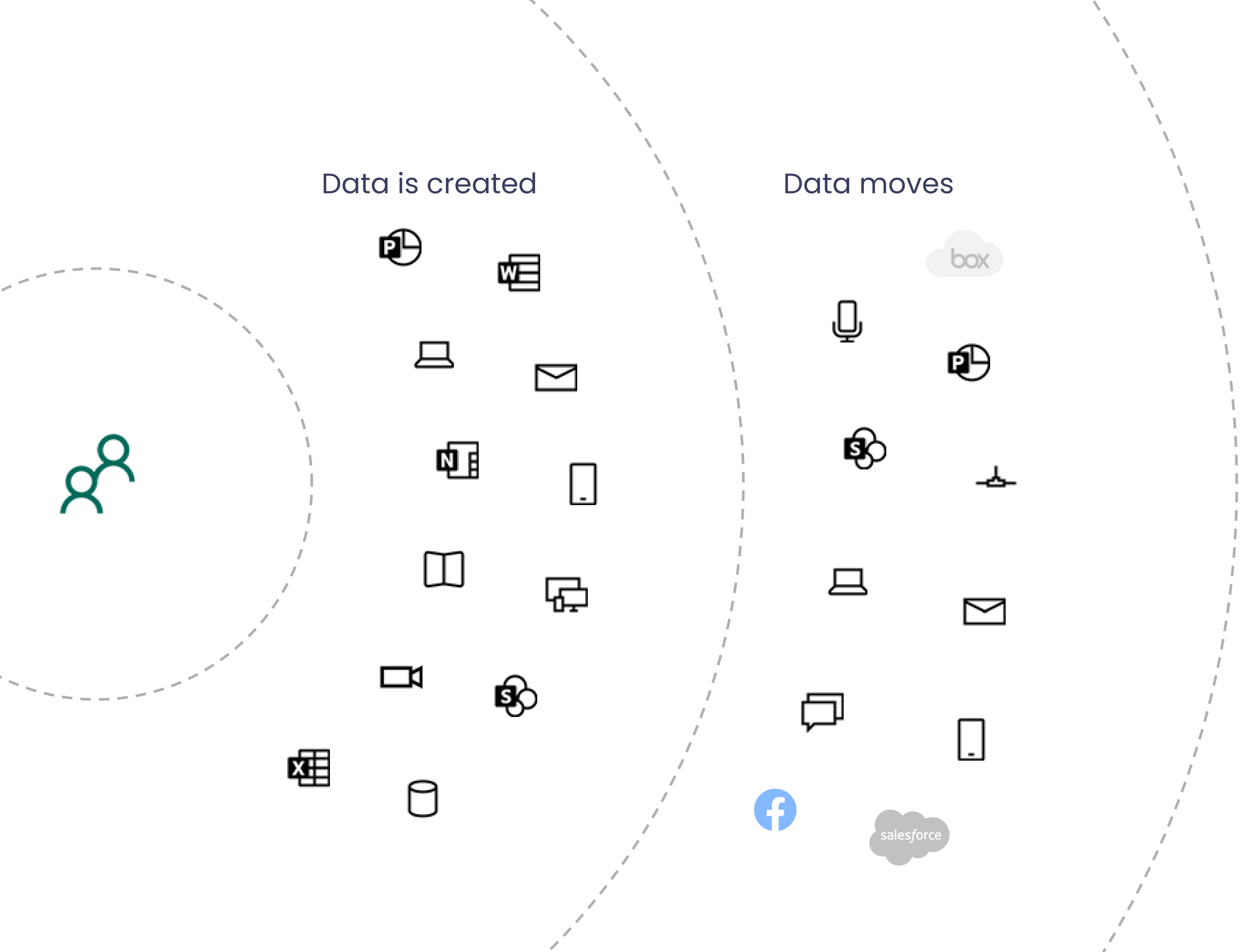


The Data Lifecycle



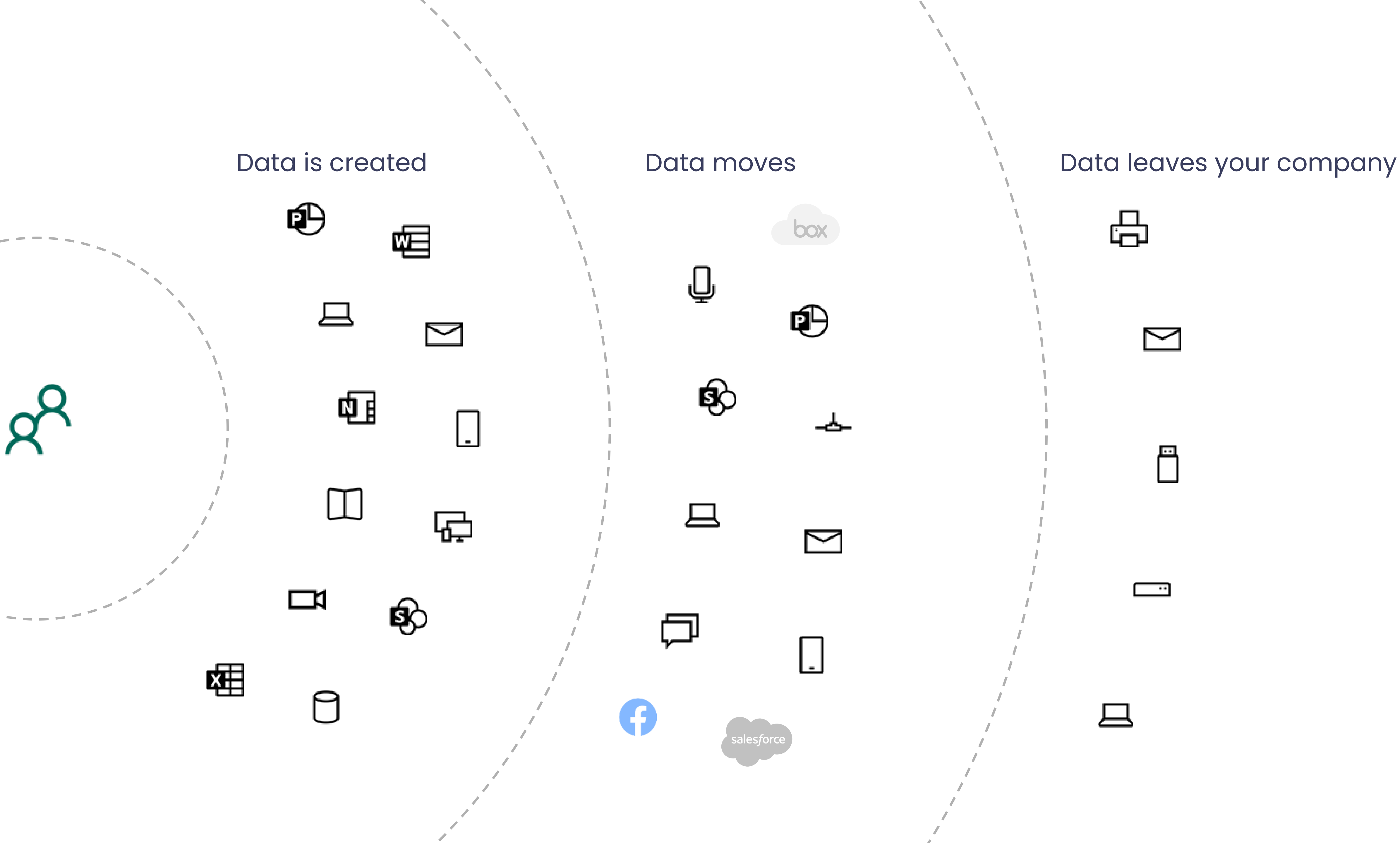


Data is created



Data is created

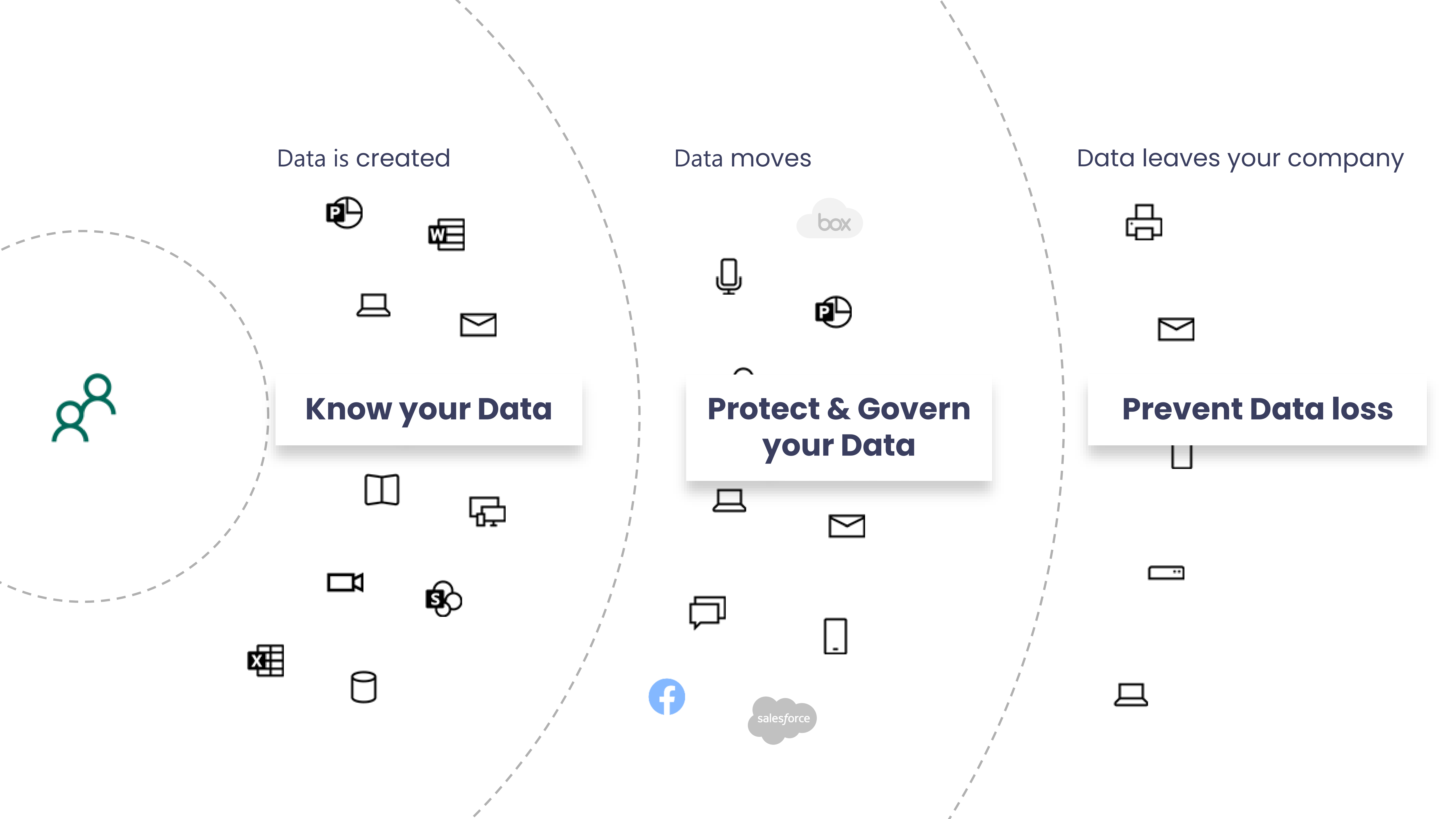
Data moves



Data is created

Data moves

Data leaves your company



Data is created

Know your Data

Data moves

Protect & Govern your Data

Data leaves your company

Prevent Data loss

Know your Data

What kinds of sensitive data do I have in my organization?

Where is it located?

What methods can I use to identify and classify it?

Data Classification Matrix

	Public data	Sensitive data	Confidential data
Risk degree	Low	Medium	High
Description	Data that can be either freely disclosed to the public or has does not have an impact on the company if it is published.	Information of medium importance, typically created for internal use only, not meant for public disclosure.	Highly sensitive data concerning either customers or corporate individuals, absolutely not meant for public disclosure.
Access rights	Low or nonexistent limitations	Moderate access, mostly available to people on a need-to-know basis (in case someone needs this data to do their job properly)	Highly selective case-by-case approved access under an NDA
Potential impact	The negative impact from this data type getting into the wrong hands or being published publicly ranges from non-existent to inconvenient at most.	The negative impact from this data type getting into the wrong hands or being published is on a moderate rate, meaning concerning, but not business-critical.	The negative impact from this data type getting into the wrong hands or being published is highly destructive, capable of creating both financial and lawful problems to the company.

Data Sensitivity Levels

Data classification helps an organization understand the value of its data, determine whether the data is at risk, and implement controls to mitigate risks.

Data classification also helps an organization comply with relevant industry-specific regulatory mandates such as SOX, HIPAA, PCI DSS, and GDPR.

Low Sensitivity	Medium Sensitivity	High Sensitivity
Public website content, press releases	Emails and documents with no confidential data	Financial records, intellectual property, authentication data

Data Sensitivity Best Practices

Since the high, medium, and low labels are somewhat generic, a best practice is to use labels for each sensitivity level that make sense for your organization. Two widely-used models are shown below.

Sensitivity	MODEL 1	MODEL 2
High	Confidential	Restricted
Medium	Internal Use Only	Sensitive
Low	Public	Unrestricted

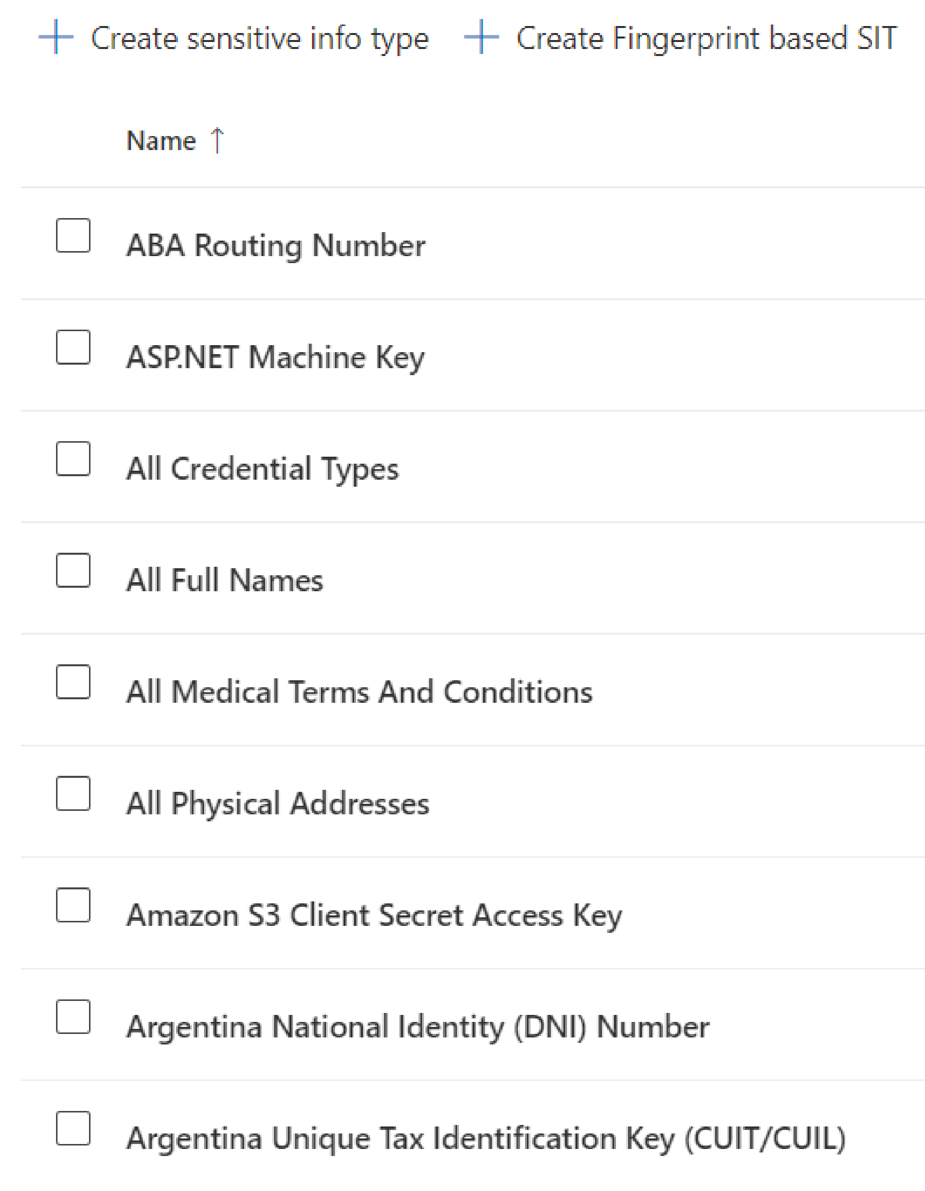
Out-of-box sensitive info types

Microsoft 365 includes 200+ sensitive info types
For different countries, industries, or by information type

Sensitive information comes in many forms
Financial data, Personally Identifiable Information (PII)

Examples

- Croatia Personal Identification (OIB) Number
- EU Debit Card Number
- EU Passport Number
- US Drivers License Number
- Social Security Number



	Name ↑
□	ABA Routing Number
□	ASP.NET Machine Key
□	All Credential Types
□	All Full Names
□	All Medical Terms And Conditions
□	All Physical Addresses
□	Amazon S3 Client Secret Access Key
□	Argentina National Identity (DNI) Number
□	Argentina Unique Tax Identification Key (CUIT/CUIL)

Customer-specific sensitive info types

Business intellectual property

Business plans, product designs, confidential projects

Employee or customer information

HR Information, resumés, employment records, salary information

Highly confidential information

Mergers and Acquisition, workforce reduction

Examples

- Employee or customer numbers *Technology: RegEx*

  <EMP-nnnnn>

  <CUST-nnnnnn-NL>

- Specific keywords *Technology: Static Keywords*

  <Project Enigma>

  <Highly Confidential>

  <Internal only>

Classifiers - Microsoft Purview

Flexible options to know your data

Understand what’s sensitive, what’s business critical & across your environment

Scanner: Spanning on-premises to cloud

Content explorer

Use built-in classification methods

Activity explorer

Auto-classification using trainable classifiers

Protect your Data

How can I protect my sensitive data?

Where can I protect my sensitive data?

How can I balance data security and productivity?

Protect your data using sensitivity labels

- ✓ Customizable
- ✓ Persists as container metadata or file metadata
- ✓ Readable by other systems
- ✓ Determines DLP policy based on labels
- ✓ Extensible to partner solutions

- Manual or Automated Labels ✓
- Apply to content or containers ✓
- Label data at rest, data in use, or data in transit ✓
- Enable protection actions based on labels ✓
- Seamless end user experience across productivity applications ✓

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels

Discover

Scan & detect sensitive data based on policy

Classify

Classify and label data based on sensitivity

Protect

Apply protection actions, including encryption, access restrictions

Monitor

Reporting, alerts, remediations

Comprehensive

Devices

Apps

Cloud services

On-premises

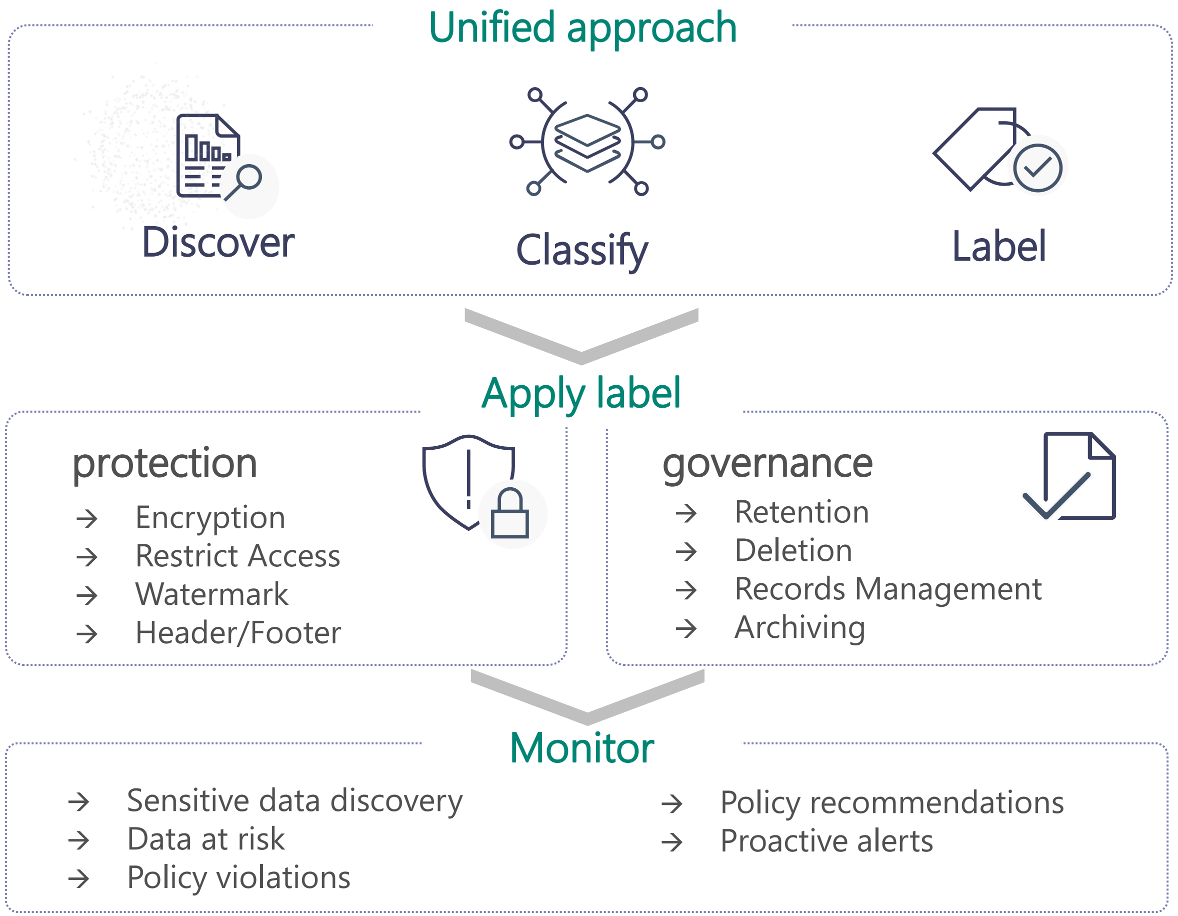
Data protection & data governance go hand-in-hand

Unified approach to discover, classify & label

Automatically apply policy-based actions

Proactive monitoring to identify risks

Broad coverage across locations



Unified approach

Discover

Classify

Label

Apply label

protection

- → Encryption
- → Restrict Access
- → Watermark
- → Header/Footer

governance

- → Retention
- → Deletion
- → Records Management
- → Archiving

Monitor

- → Sensitive data discovery
- → Data at risk
- → Policy violations
- → Policy recommendations
- → Proactive alerts

[SharePoint online - labels]()

Prevent data loss

How can I prevent accidental sharing of sensitive data?

How can I ensure my employees get timely guidance?

Office 365 Data Loss Prevention

Detect, protect & monitor your sensitive information

Detect

Easily create policies that find sensitive content wherever it lies in Office 365

Protect

Stop accidental sharing and educate users

Monitor

Get visibility into how your data is being protected

Unified policy configuration & management

Centralized

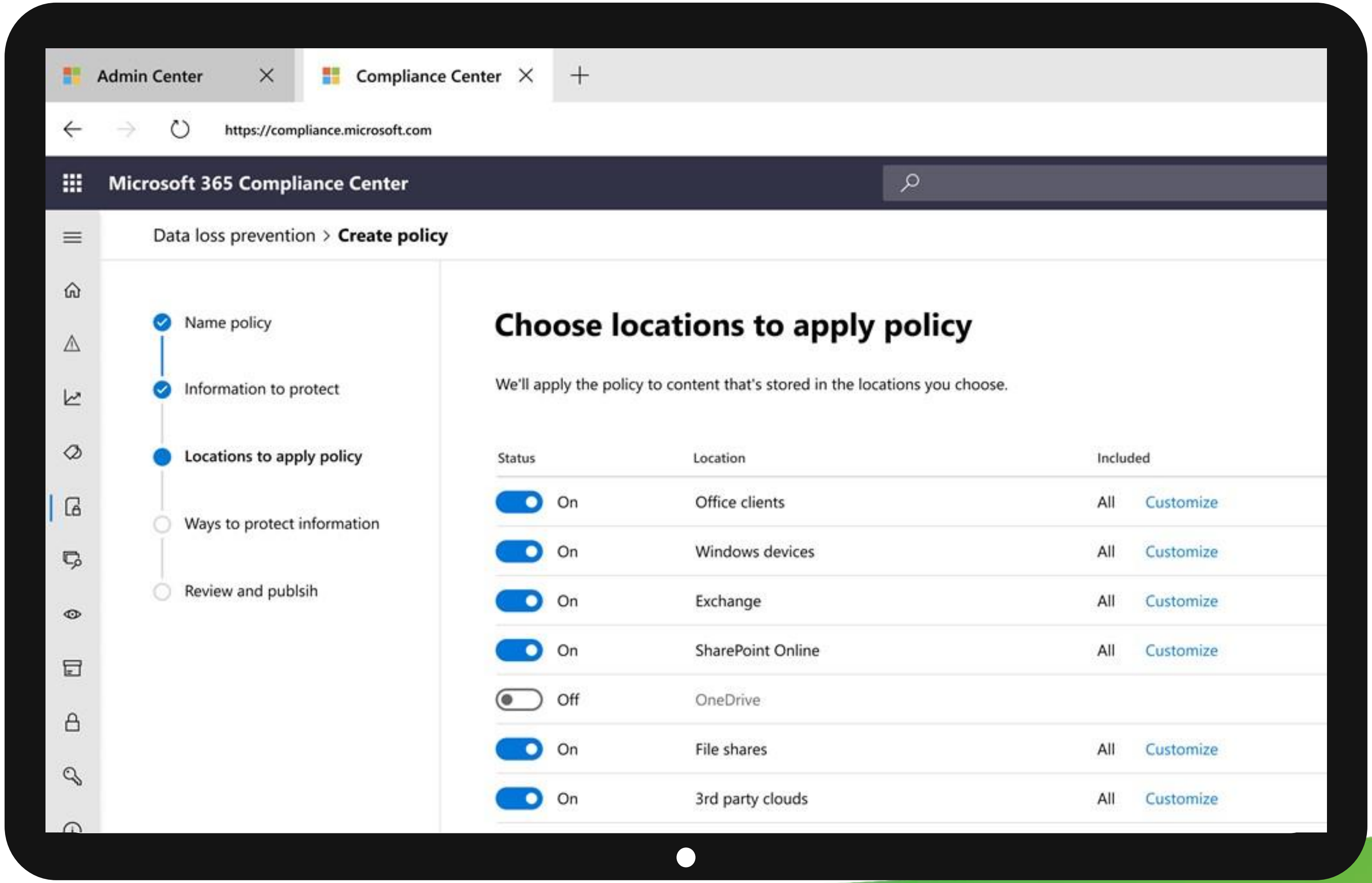
Single destination to configure policies for data protection and data governance, across locations

Customized

Customize conditions, rules and exceptions to granularly define policy actions

Consistent

Consistent enforcement using common policy engine


Admin Center
Compliance Center
https://compliance.microsoft.com
Microsoft 365 Compliance Center

Data loss prevention > **Create policy**

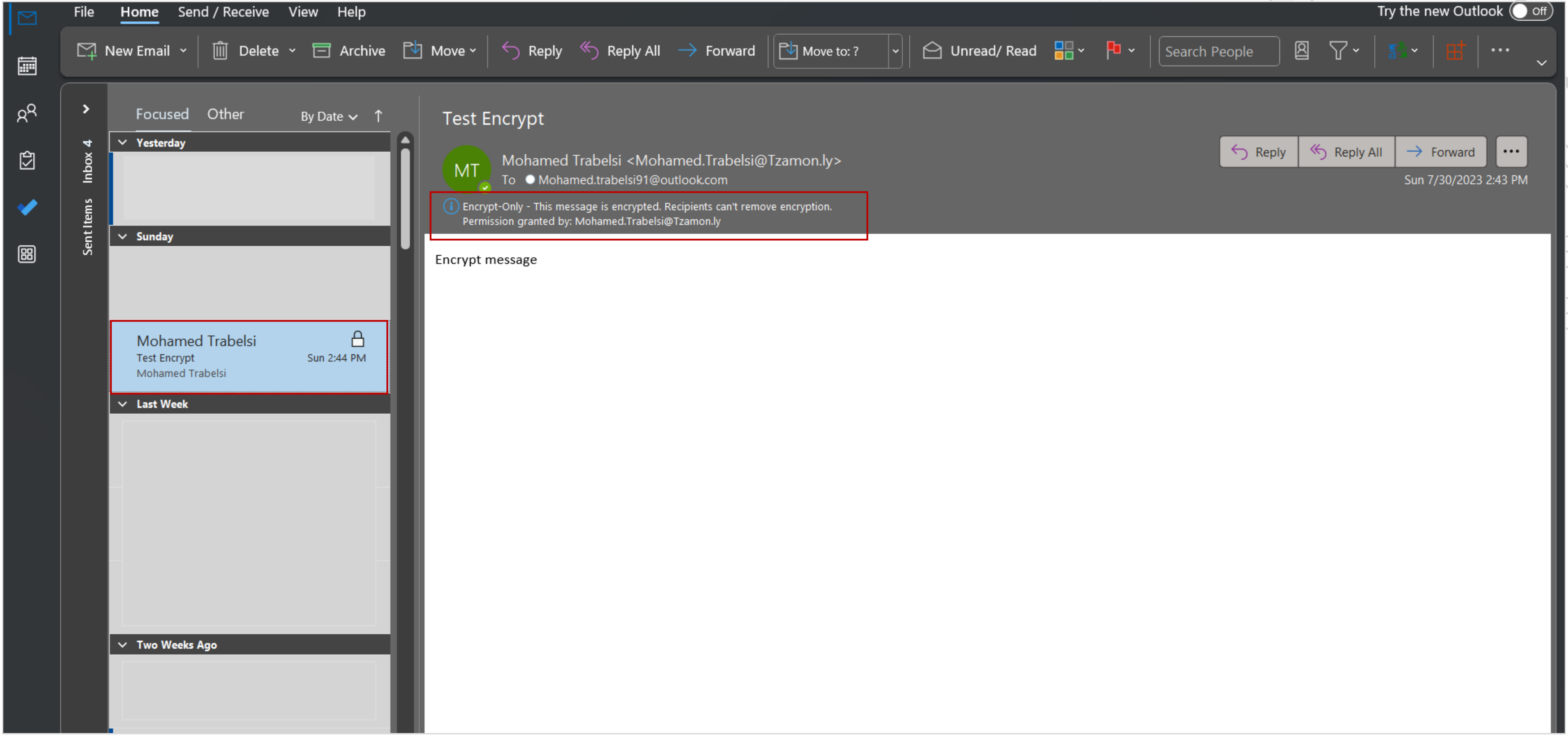
- Name policy
- Information to protect
- **Locations to apply policy**
- Ways to protect information
- Review and publsih

Choose locations to apply policy

We'll apply the policy to content that's stored in the locations you choose.

Status	Location	Included	
On	Office clients	All	Customize
On	Windows devices	All	Customize
On	Exchange	All	Customize
On	SharePoint Online	All	Customize
Off	OneDrive		
On	File shares	All	Customize
On	3rd party clouds	All	Customize

Message Encryption



Test Encrypt

Mohamed Trabelsi <Mohamed.Trabelsi@Tzamon.ly>

To Mohamed.trabelsi91@outlook.com

Sun 7/30/2023 2:43 PM

Encrypt-Only - This message is encrypted. Recipients can't remove encryption.
Permission granted by: Mohamed.Trabelsi@Tzamon.ly

Encrypt message

Challenge

Accidental data loss or data breach

Northwind uses occasionally use a password on an excel spreadsheet to guard sensitive info like salaries.

But these security measures are used inconsistently. Lots of documents are emailed around or saved on USB keys without any protections. **Anyone can download a confidential document and leave the company.**

Over 80%

of small and medium businesses handle PII data.[1]

[1]Source: Microsoft Internal Research of SMBs (2-299 employees)

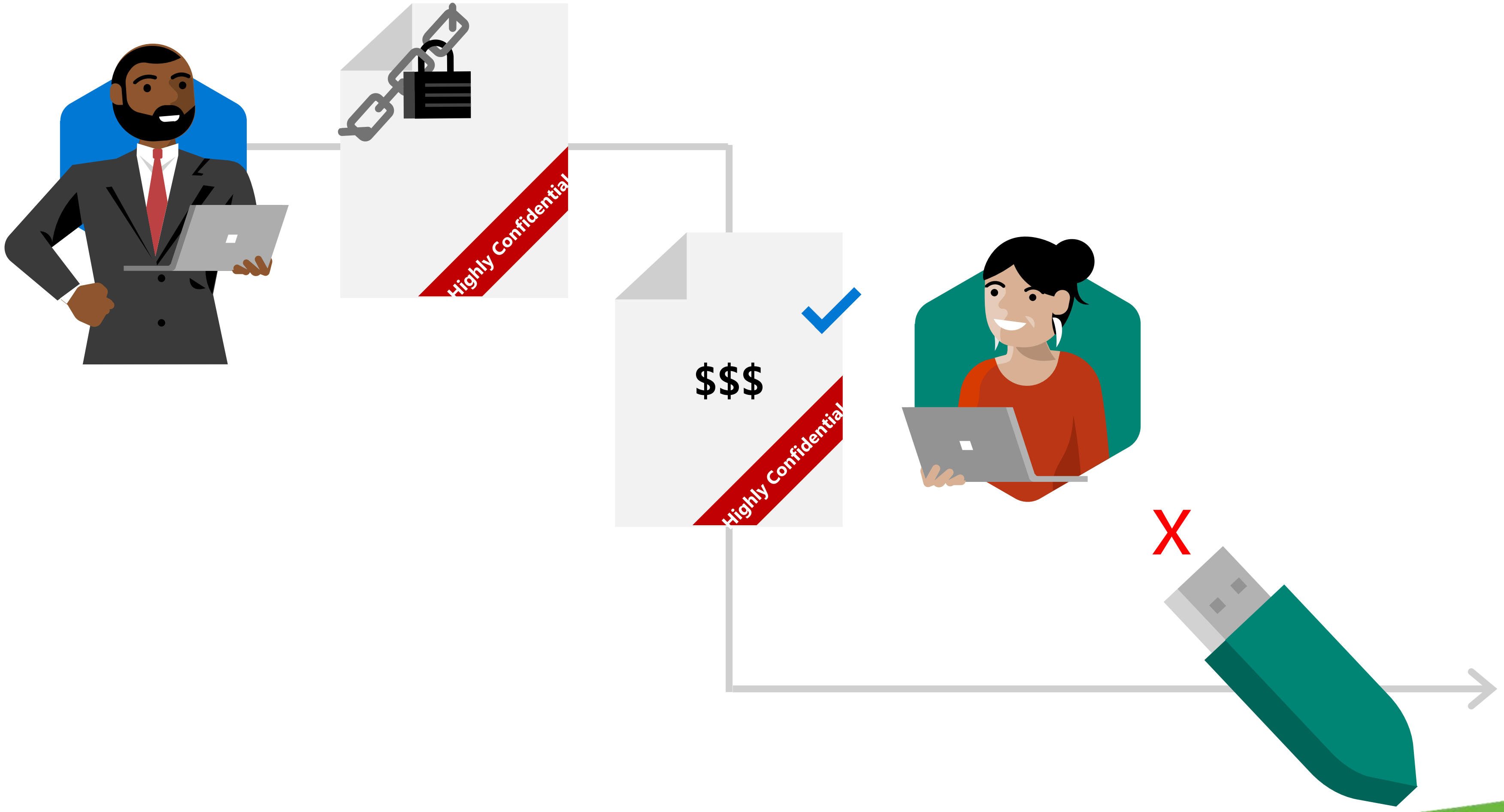
Solution

Secure sensitive data

Adrian creates the company's sales forecast and classifies it as "Highly Confidential." As Northwind Traders is now using **Microsoft 365 Business Premium, "Highly Confidential" files are automatically encrypted,** and only accessible to company employees.

Laura, a Northwind Traders salesperson, attempts to open the file. Microsoft 365 Business Premium verifies that she is a Northwind Traders employee and decrypts the file for her.

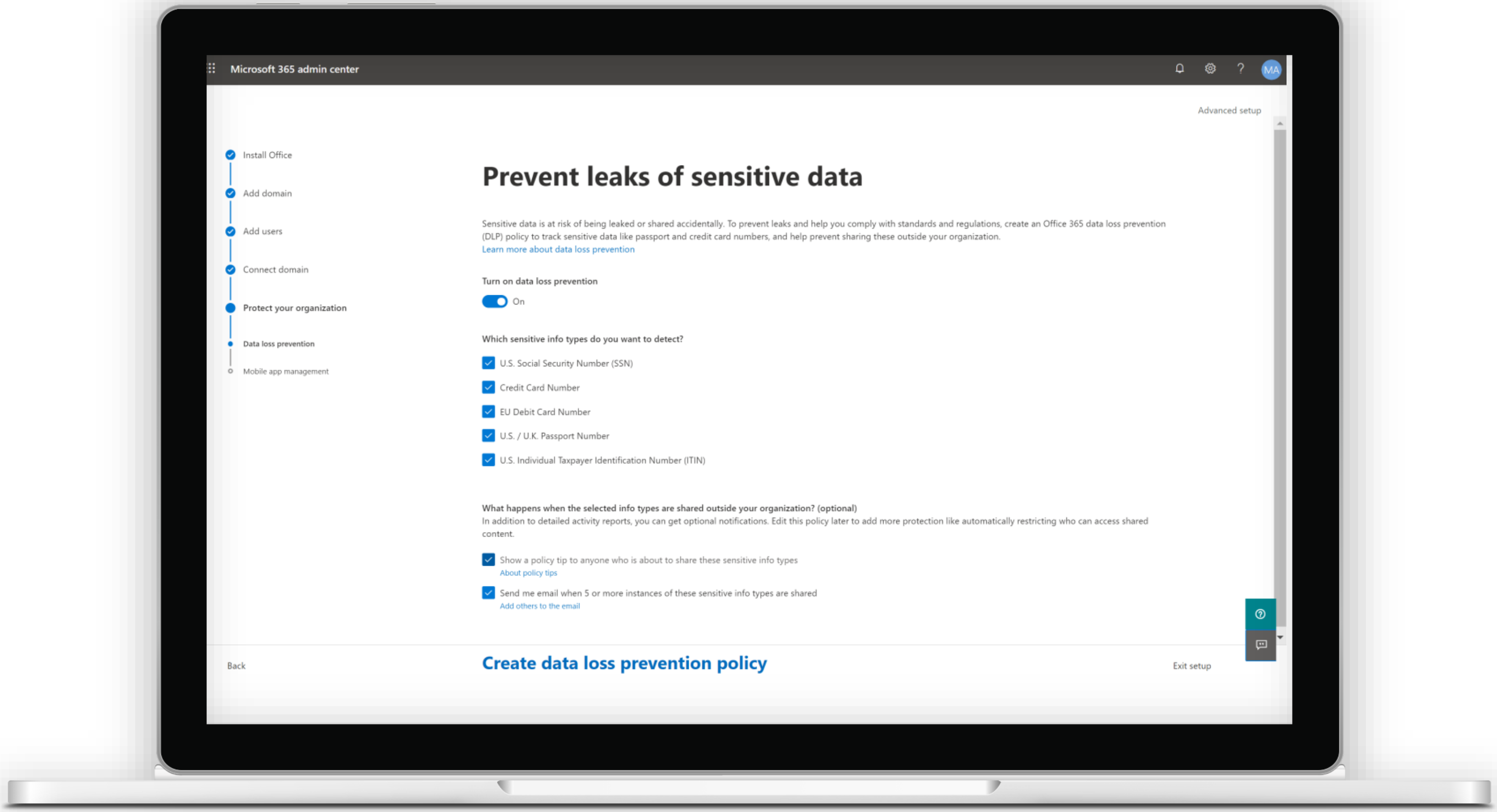
Even if any employee leaves the company, and stores the document on a personal device, they cannot access it because the document access is tied to their work credentials.



Solution

Secure sensitive data

With **Microsoft 365 Business Premium, you get advanced capabilities like Data Loss Prevention and Azure Information Protection,** to help classify and protect sensitive data like customer or employee information, confidential business data, social security numbers, credit card numbers and more.



Prevent leaks of sensitive data

Sensitive data is at risk of being leaked or shared accidentally. To prevent leaks and help you comply with standards and regulations, create an Office 365 data loss prevention (DLP) policy to track sensitive data like passport and credit card numbers, and help prevent sharing these outside your organization.
Learn more about data loss prevention

Turn on data loss prevention
On

Which sensitive info types do you want to detect?

☑ U.S. Social Security Number (SSN)
☑ Credit Card Number
☑ EU Debit Card Number
☑ U.S. / U.K. Passport Number
☑ U.S. Individual Taxpayer Identification Number (ITIN)

What happens when the selected info types are shared outside your organization? (optional)
In addition to detailed activity reports, you can get optional notifications. Edit this policy later to add more protection like automatically restricting who can access shared content.

☑ Show a policy tip to anyone who is about to share these sensitive info types
About policy tips
☑ Send me email when 5 or more instances of these sensitive info types are shared
Add others to the email

Create data loss prevention policy

Over 55%

SMBs say they are concerned about employees leaving their company with data on personal devices.[1]

Source: Underserved and Unprepared: The State of SMB Cybersecurity in 2019, survey data collected by 850 global SMBs in 2019

Managing Mobile Devices

Managing mobile devices – two approaches

Phones

Tablets

Mobile Application Management (MAM)

- Commonly used for personal devices or BYOD (Bring Your Own Device scenario)
- No Device Enrollment required
- Company manages the security of only those applications that are enrolled

Key capabilities

Secure corporate data within apps

Report app inventory & usage

Remove corporate data

Administration

Managed via setup wizard and simplified UI

Mobile Device Management (MDM)

- Commonly used for total management of company-owned devices
- **Device Enrollment Required**
- Company manages the security of the entire device

Key capabilities

Provision settings, certs, profiles

Advanced policy controls

Report & measure device compliance

Administration

Managed via Intune admin center
Additional steps to set up (provision certificates, etc)

https://docs.microsoft.com/en-us/intune/ios-enroll
https://docs.microsoft.com/en-us/intune/android-enroll

App Protection Policies (APP)

Multi-identity awareness

Targets corporate
accounts, not
personal and
unmanaged

Conditional launch

Device health
OS version
App version/SDK
Device model or manufacturer

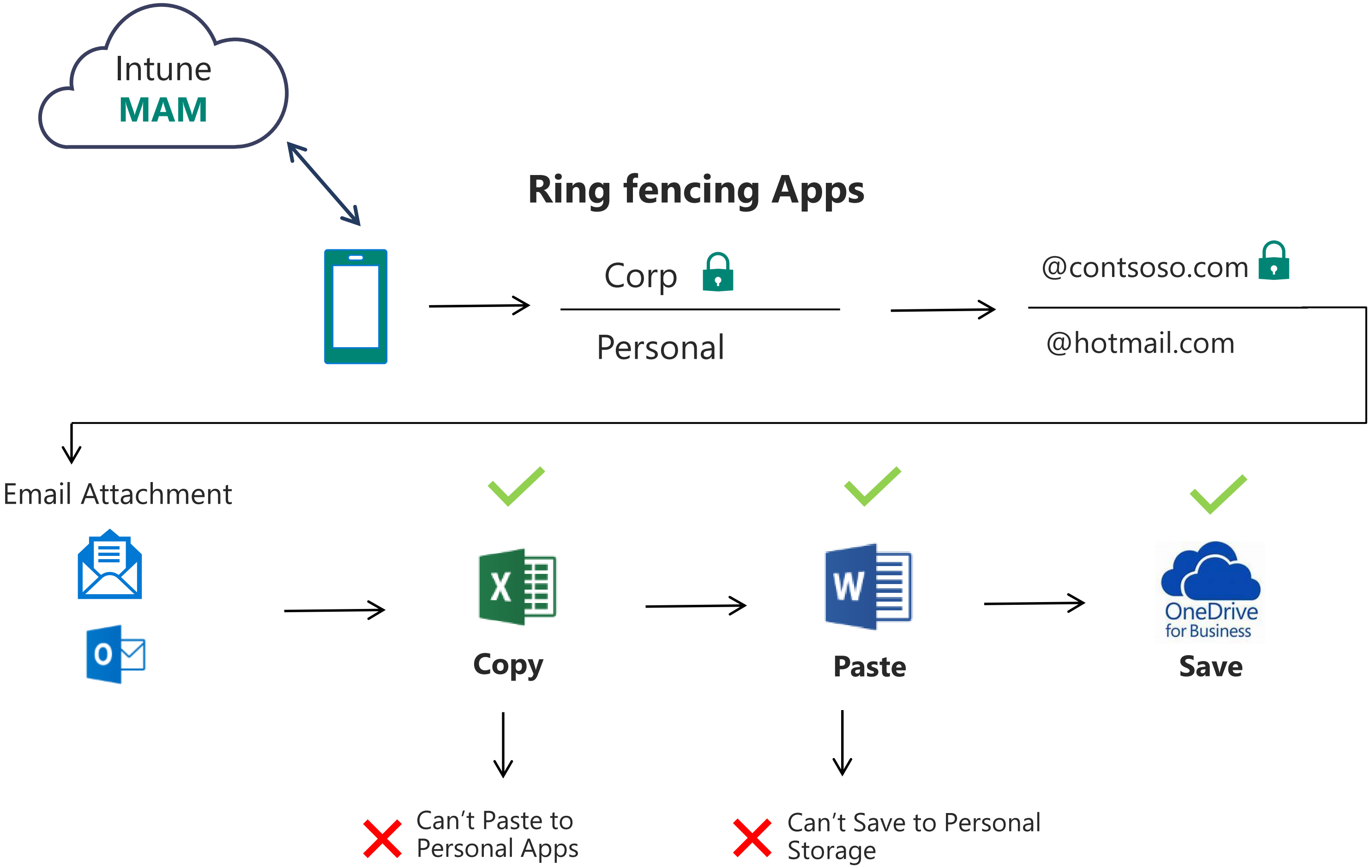
Access requirements

PIN
Biometrics
Credentials
Inactivity timers

Data protection

Between apps
Encryption
Transfer web data
Selective wipe

Mobile Application Management (MAM) for Personal or BYOD devices



Intune MAM does two things without requiring Device Enrollment

- **Separates company managed apps from personal apps**, and set policies on how data is accessed from managed apps
- **Ensures corporate data can't be copied** and pasted to personal apps within the device

Challenge

Work data on personal devices

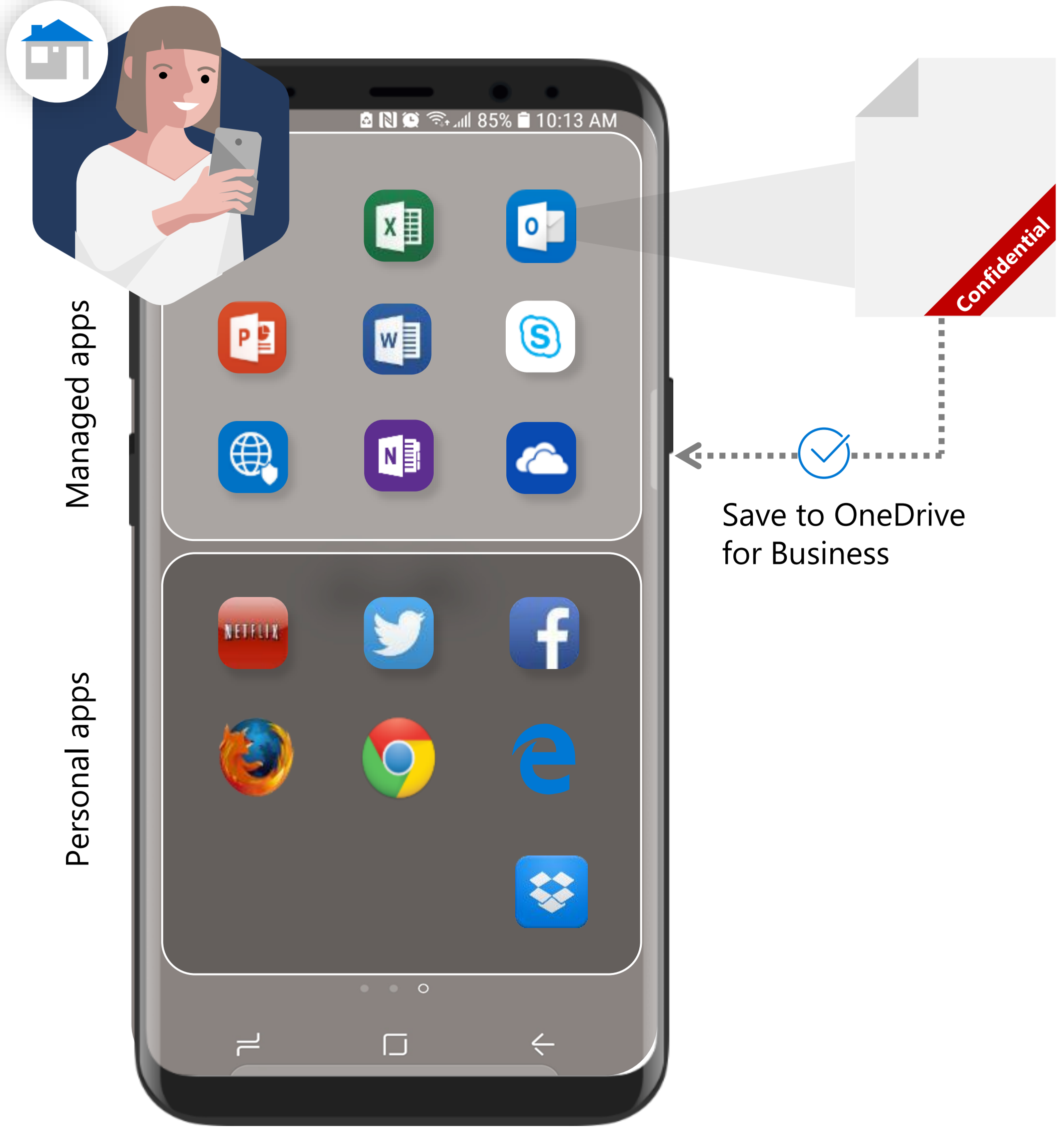
85% 10:13 AM
Confidential
Save to
personal storage

A Northwind Traders marketing manager is using her personal phone to check company email. She receives a confidential business plan and saves it for later reference. **She accidently saves to a personal share which is not secure.**

64% of SMBs allow employees to access work data on personal phones and computers.[1]

[1] *Source: Microsoft Internal Research of SMBs (2-299 employees)*

Protect work data on personal devices



Save to OneDrive for Business

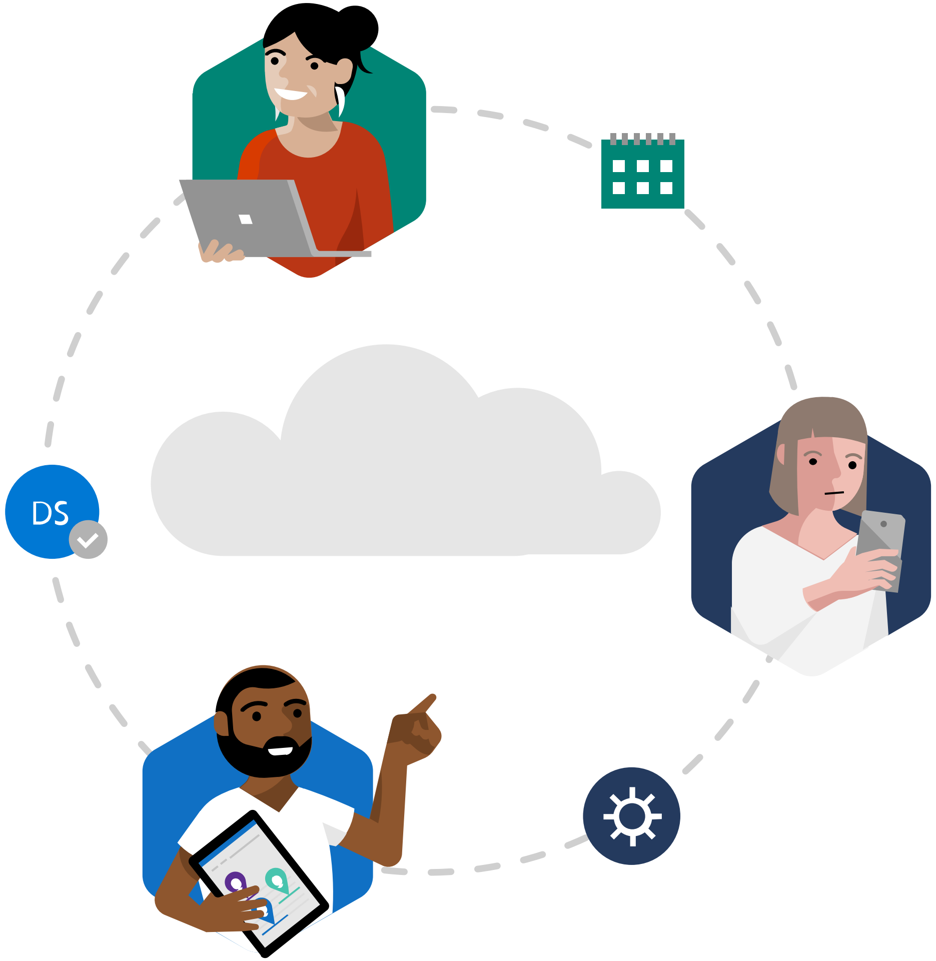
With Microsoft 365 Business Premium, you can set up Intune App Protection Policies, so work apps can be separated from personal apps. Administrators can specify that work documents and attachments are only saved on authorized and secure work share like OneDrive for Business, safeguarding sensitive work information.

58% of employee devices on average are configured with proper security protocols and fewer than **1 in 5** saying that all employees undergo security training.[1]

[1] *Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2019 survey of SMBs (1-499 employees)*

Challenge

Unauthorized access to work data



Company employees need access to work data as they work from home or on the go. However, bad actors outside the circle of trust may try to gain access to work information, for example by stealing passwords and trying to gain access to the work data from another country.

Thank You