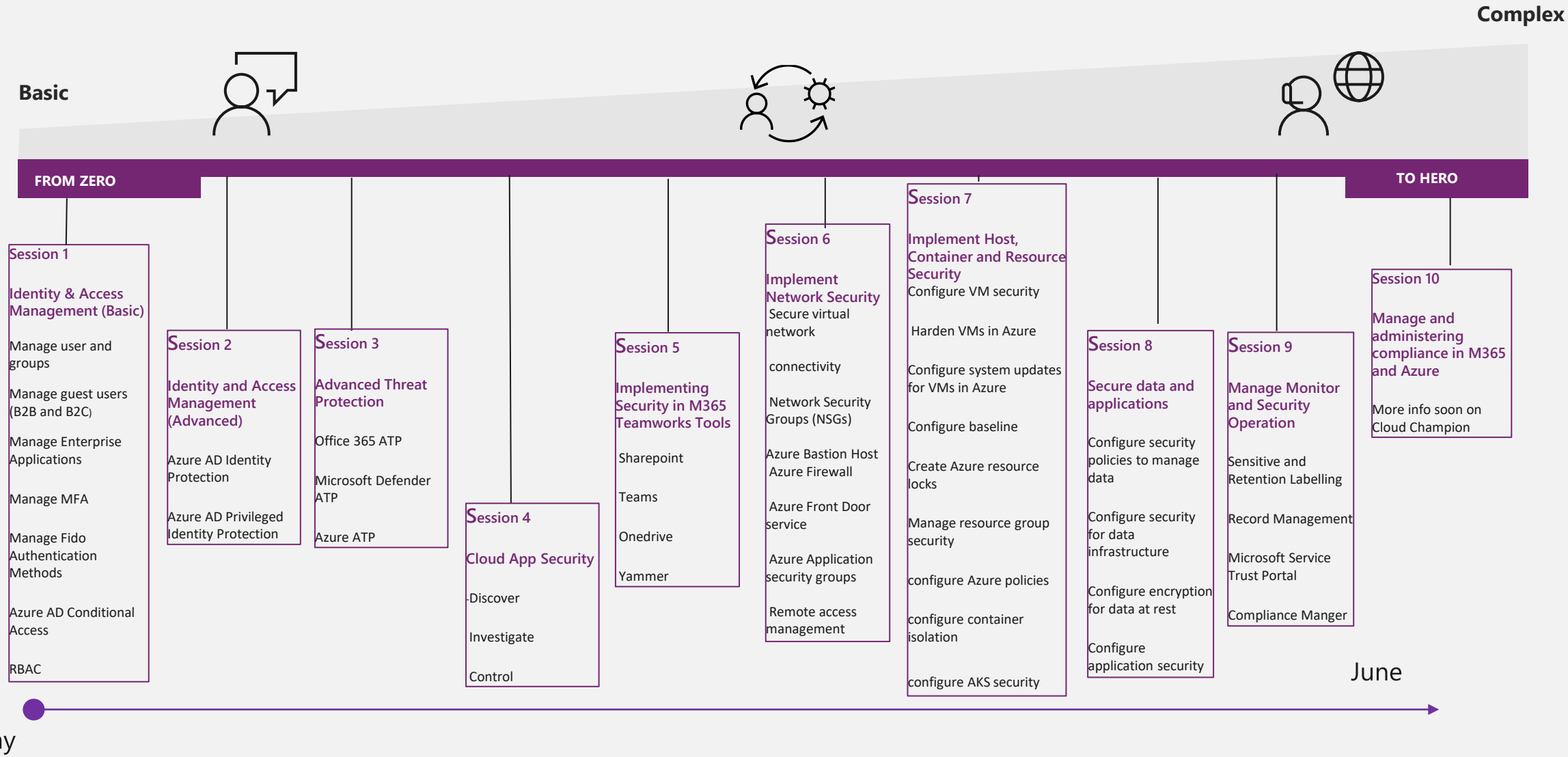
Security Sailing

Session 5 – Implementing Security in M365 Teamworks Tools

Michele

- Senior Consultant – Speaker – Trainer (22 anni)
- Dipendente 50% su tecnologie Microsoft Dipartimento di Informatica – Università degli Studi di Milano
- Freelance 50/70%
- Mi occupo di: AD, SCCM, W10, Win Server, AzureAD, O365, M365, Azure, Enterprise Mobility & Security
- Speaker da 12 anni di WPC e da 5 responsabile agenda ITPRO e Security
- Certificato MCT, MCSE, MCSA, MCITP
- Contatti:
  - michele@sensalari.com
  - michele.sensalari@overneteducation.it
  - Twitter: @ilsensa7
  - Linkedin: https://www.linkedin.com/in/michele-sensalari-4988b7/

Content and Timeline Details



Agenda

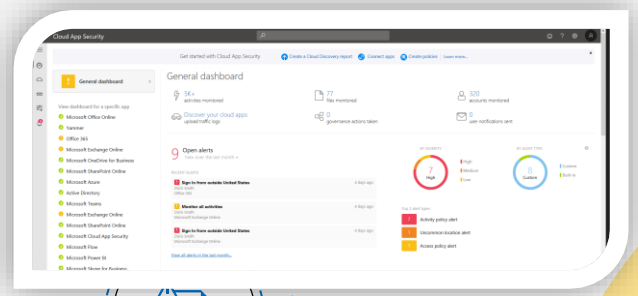
Protection Across the Attack Chain

Office 365 E5
Office 365 ATP
Malware detection, safe links, and safe attachments

EMS E5
Azure AD Identity Protection
Identity protection & conditional access for SSO Applications

EMS E5
Cloud App Security
Extends protection & conditional access to other cloud apps

Unified Portal



Account Compromise in cloud application or VPN

Phishing mail

Opens attachment

Clicks on a URL

User browses to a website

Exploitation & Installation

Command & Control

Attacker collects **reconnaissance and configuration data**

User account **compromise & persistence**

Attacker attempts **lateral movement**

Privileged account **compromised**

Domain **compromise & persistence**

Exfiltrate data

EMS E3/E5
Microsoft Information Protection

Attacker **accesses** sensitive data

Windows E5
Microsoft Defender ATP
Endpoint Detection and Response (EDR) & End-point Protection (EPP)

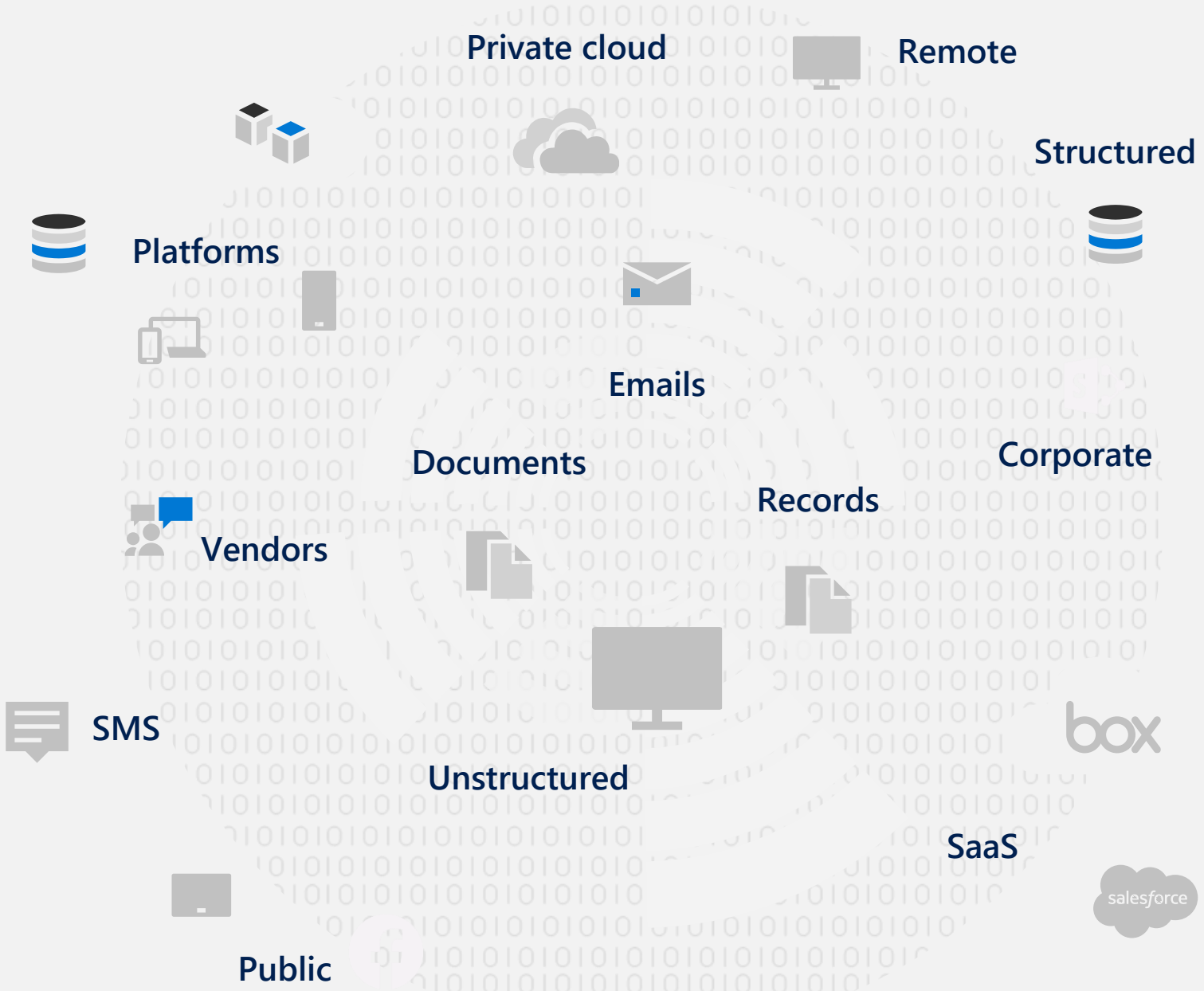
EMS E5
Azure ATP
On Premises Identity protection

"Intrusion Detection for Active Directory"

Information Protection

Data is exploding

It's Created, Stored, and Shared Everywhere



Discovering and managing data is challenging

88%

of organizations no longer have confidence to detect and prevent loss of sensitive data[1]

>80%

of corporate data is "dark" – it's not classified, protected or governed[2]

#1

Protecting and governing sensitive data is biggest concern in complying with regulations

1. Forrester. Security Concerns, Approaches and Technology Adoption. December 2018
2. IBM. Future of Cognitive Computing. November 2015
3. Microsoft GDPR research, 2017

What's your strategy for protecting and governing sensitive and business critical data?

Do you know where your business critical and sensitive data resides and what is being done with it?

Do you have control of this data as it travels inside and outside of your organization?

Are you using solutions to classify, label, and protect this data?

Information Protection & Governance

Protect and govern data – **wherever** it lives

Understand your data landscape and identify important data across your hybrid environment

Apply flexible protection actions including encryption, access restrictions and visual markings and DLP

Automatically retain, delete, and store data and records in compliant manner

Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs

Your information protection needs

DATA PROTECTION

Protect data when device is lost or stolen

Protect data when is in transit.

DATA SEPARATION

Containment

Data separation

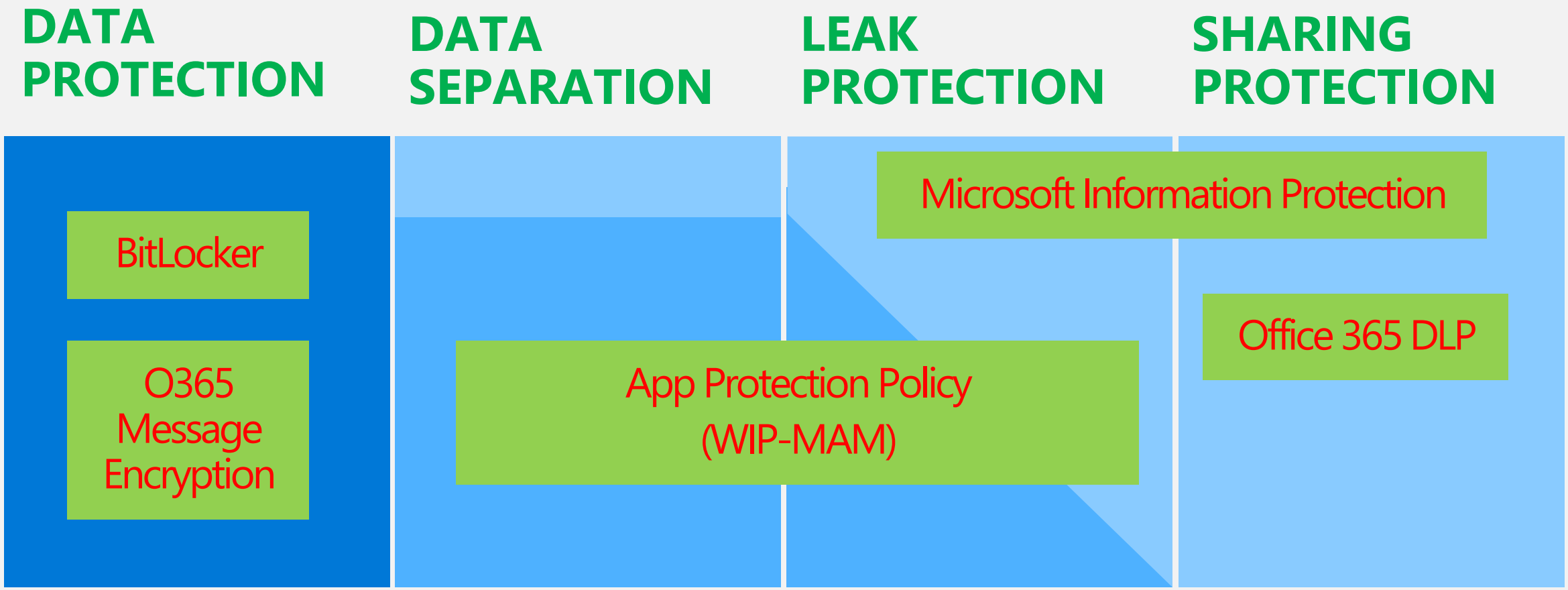
LEAK PROTECTION

Prevent unauthorized users and apps from accessing and leaking data

SHARING PROTECTION

Protect data when shared with others, or shared outside of organizational devices and control

Your information protection needs



Information Protection & Governance

Protect and govern data – **wherever** it lives

Understand your data landscape and identify important data across your hybrid environment

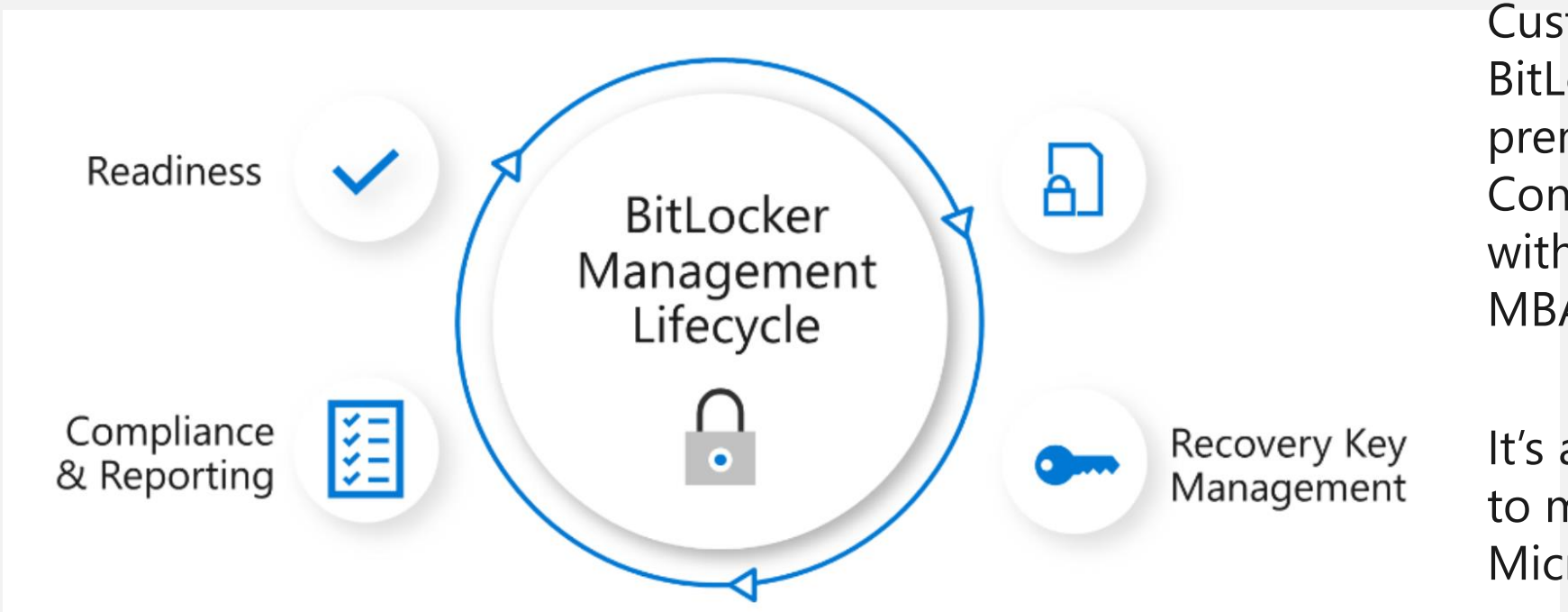
Apply flexible protection actions including encryption, access restrictions and visual markings

Automatically retain, delete, and store data and records in compliant manner

Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs

Bitlocker



Customers who wish to deploy BitLocker management on-premises may do so using Configuration Manager without the need to deploy MBAM.

It's also supported who prefer to manage BitLocker using Microsoft Intune cloud services without maintaining an on-premises infrastructure.

Cloud-based BitLocker management using Microsoft Intune

Managing BitLocker via Intune gives organizations the confidence their Windows data is stored encrypted, without the need to manage an on-premises infrastructure. Here are some of the features you'll get when using Intune for BitLocker management:

✓Silently enable BitLocker allowing BitLocker to be enforced and enabled without user interaction.

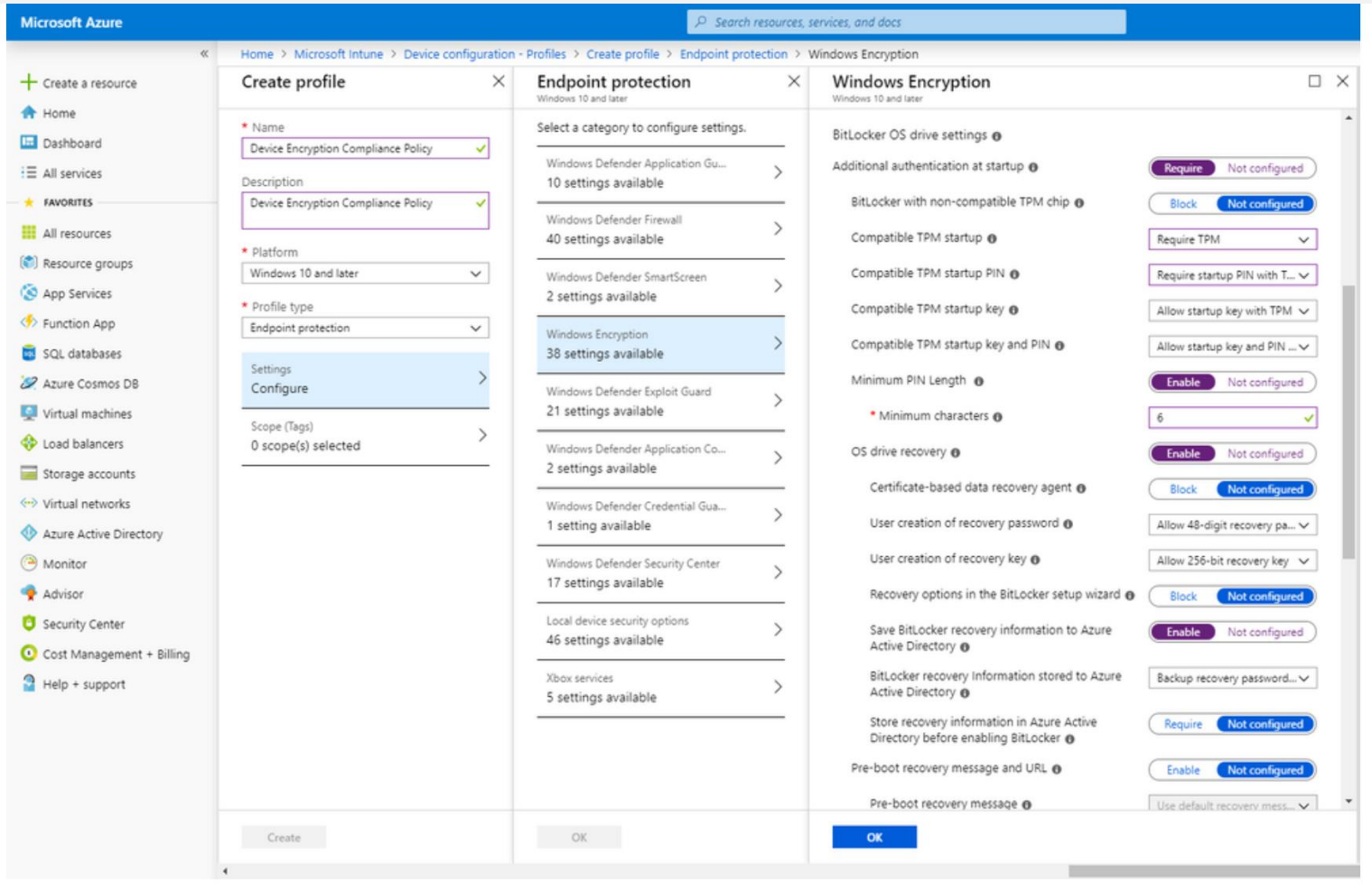
✓Ability for encryption to be enabled by non-administrator users.

✓New BitLocker readiness and compliance reports.

✓IT Pro recovery key access experience.

✓Recovery key rotation, both triggered at the client and the service.

✓Migration from MBAM to Intune can be performed by triggering a BitLocker key rotation and removing redundant BitLocker management agents.



Office 365 Message Encryption

Office 365 Message Encryption

Secure email that works across devices and with anyone

Inside your organization

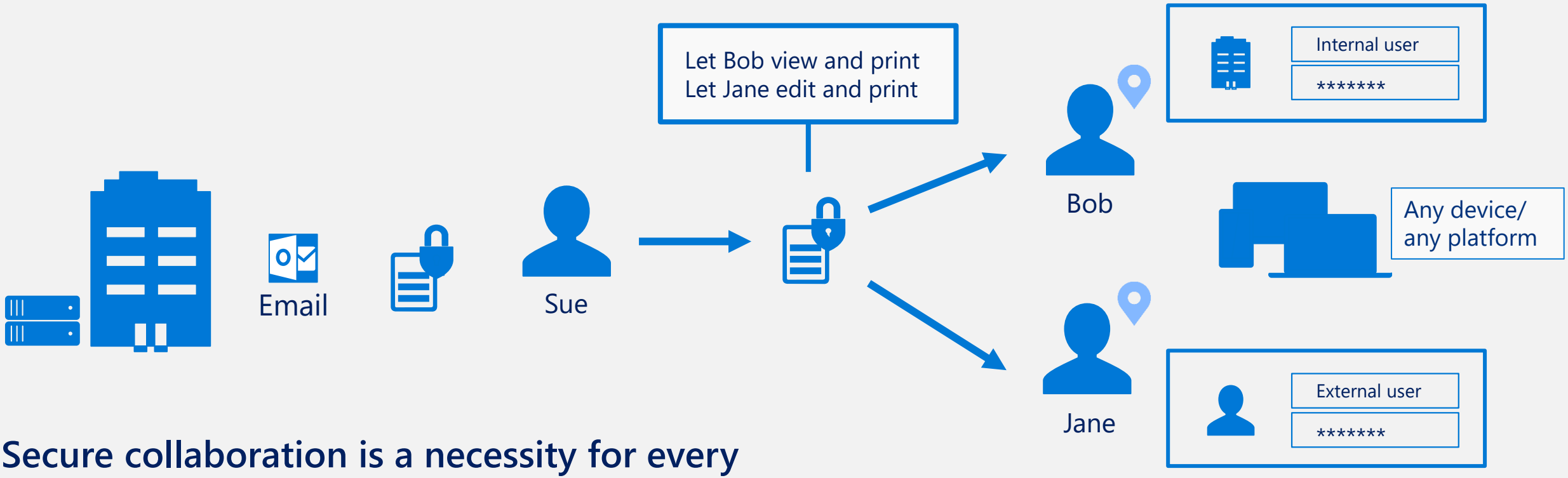
Between your business partners

With any of your customers

Office 365 Message Encryption (OME)

- With Office 365 Message Encryption, an organization can send and receive encrypted email messages between people **inside** and **outside** the organization.
- Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services.
- Email message encryption helps ensure that only intended recipients can view message content.
- Office 365 Message Encryption is built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection

Secure Email collaboration



Secure collaboration is a necessity for every organization.

Office 365 message encryption

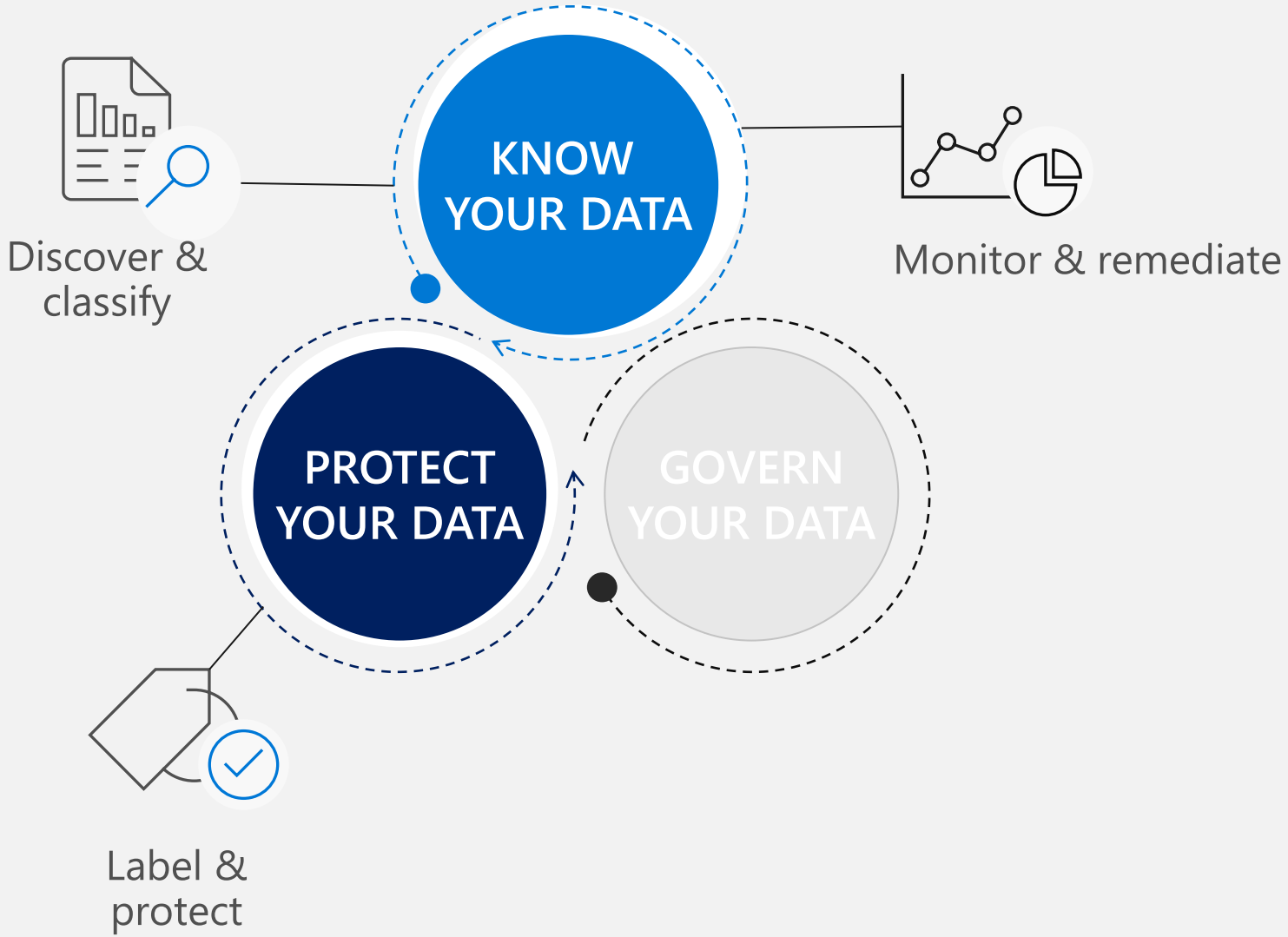
How do recipients sign in to view messages? Three ways:

- Microsoft account–used for sign-in to Microsoft services like OneDrive, XBOX Live, etc.
  - Microsoft account for hotmail.com, outlook.com, live.com already exists
  - User can create Microsoft account for any SMTP address, like gmail.com, mycustomdomain.com–address verification done
    as part of account creation process
  - If recipient does not have a Microsoft account, recipients are navigated through the process of creating one
  - For a given email address, a single Microsoft account is used to access all Microsoft services and view future encrypted emails
- Organizational account–used for sign-in to workloads like Exchange Online, SharePoint Online, etc.
- One time passcode

Microsoft 365 Information Protection

Information Protection & Governance

Protect and govern data – **anywhere** it lives



Know your Data

What methods can I use to classify my data?

Where can I classify my data?

How can I see what happens to my data over its lifecycle?

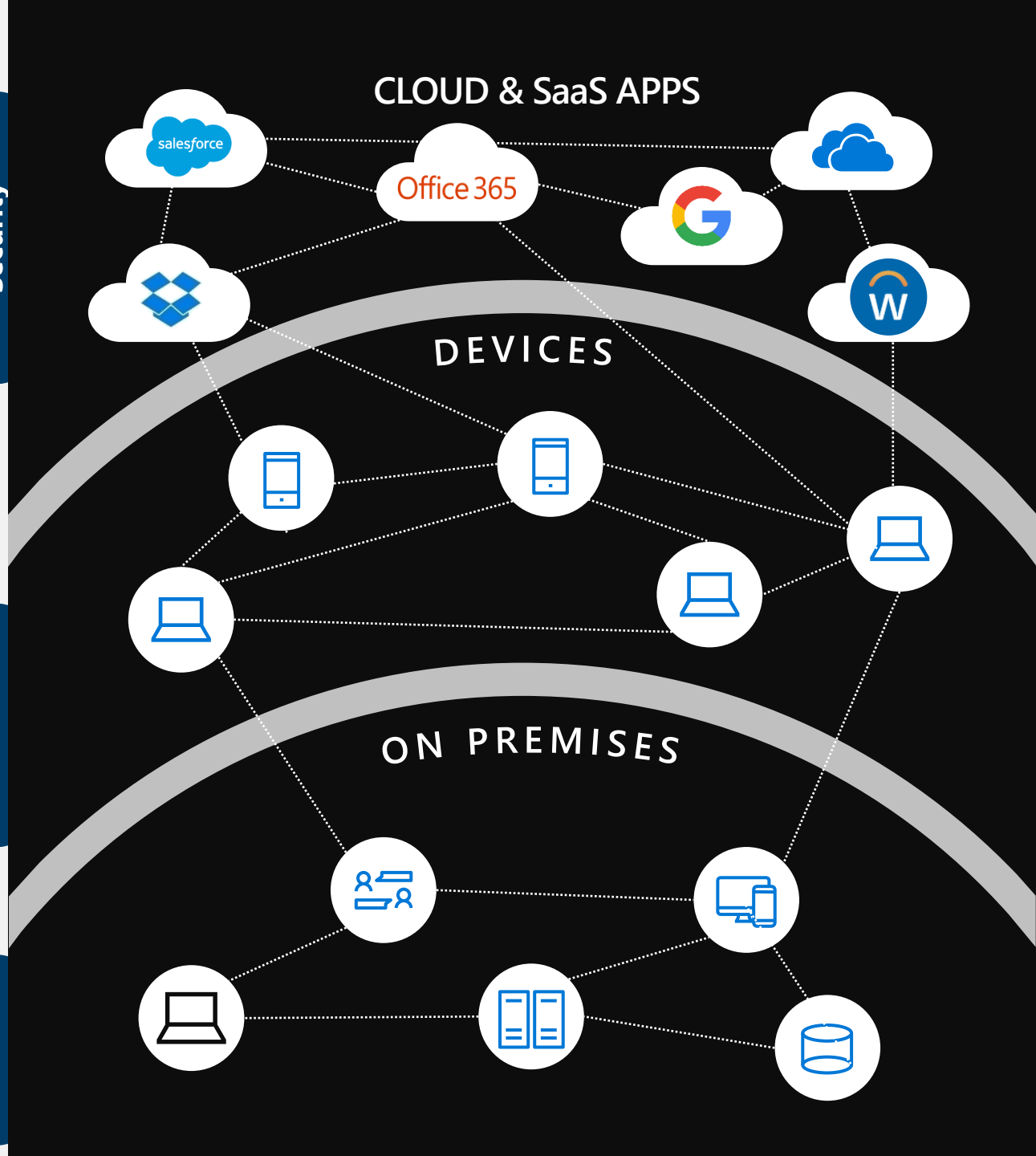
SPANNING ON-PREMISES TO CLOUD

No matter where it's created, modified or shared

Office 365, Microsoft Cloud App Security

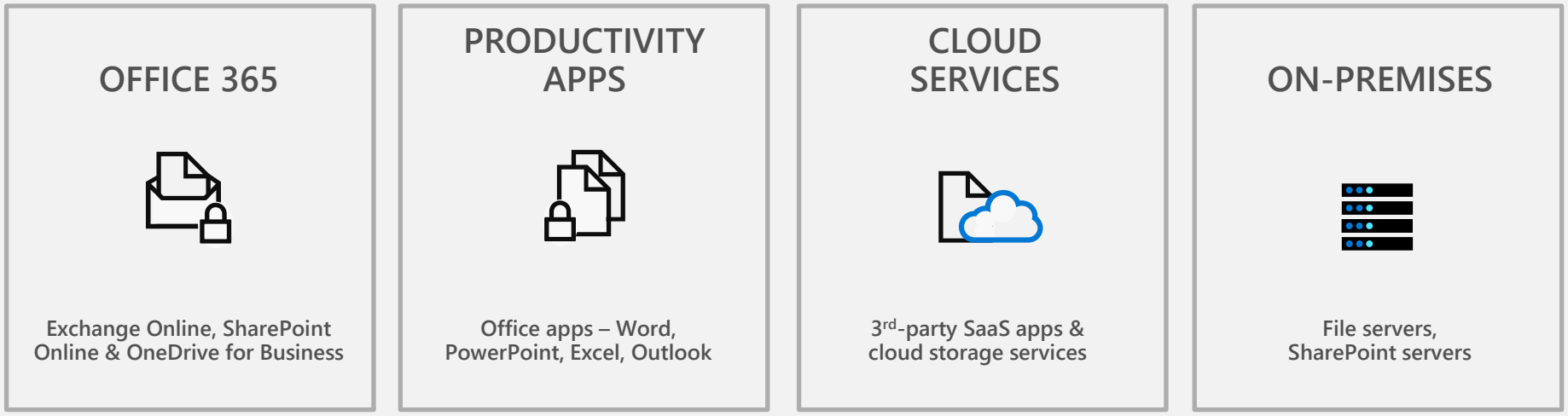
Office apps, Endpoints

AIP scanner



Unified approach to data discovery & classification

- **Consistent auto classification** across devices, apps, services
- **Native integration** in content pipeline and substrate
- **Deep content scanning** with 90+ built-in sensitive information types
- **Fully extensible** scanning with support for custom sensitive information types



Multiple classification methods

Built-in

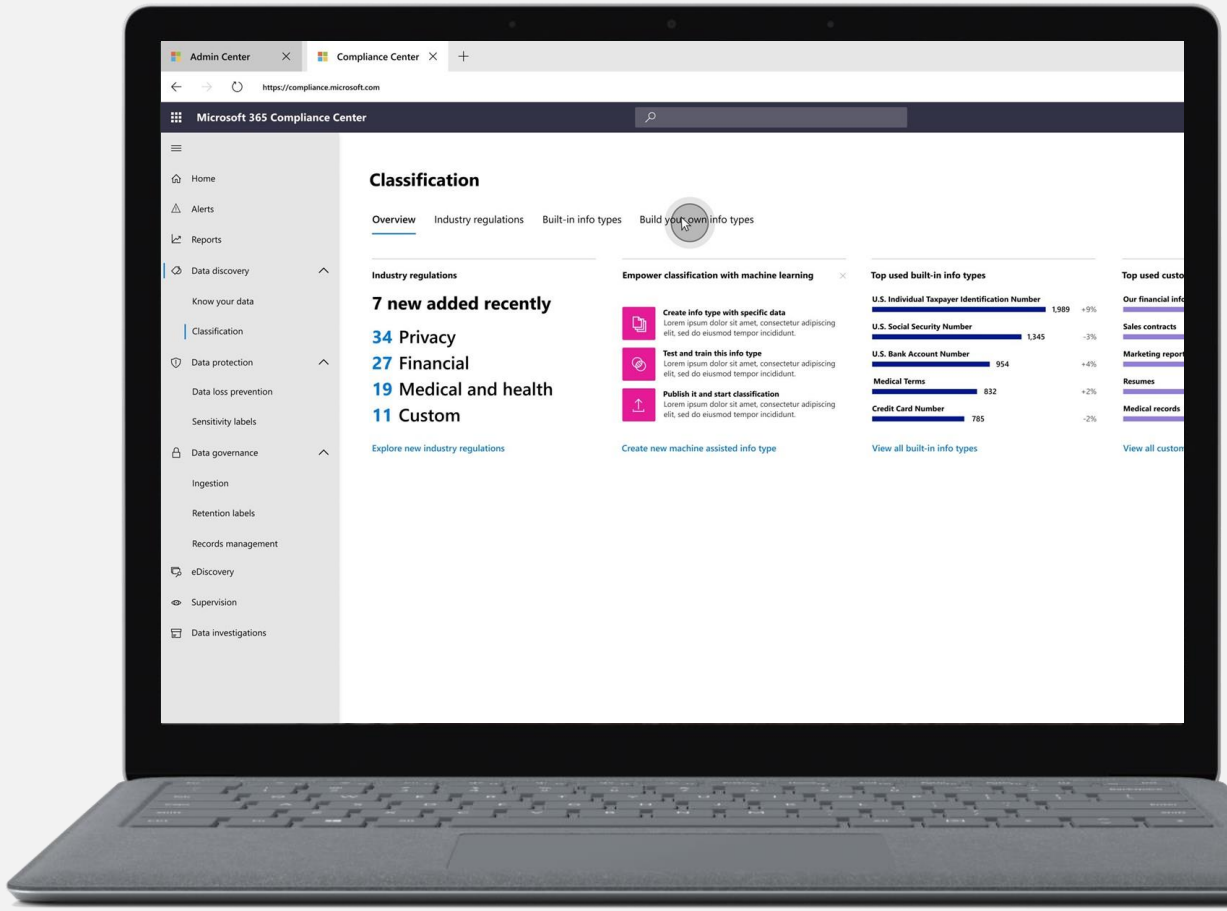
90+ information types provided out of the box to get started

Flexible

Use regex, keywords, and exact data match for data identification

Organized

Mapped to different industry regulations



Discover and classify on-premises files

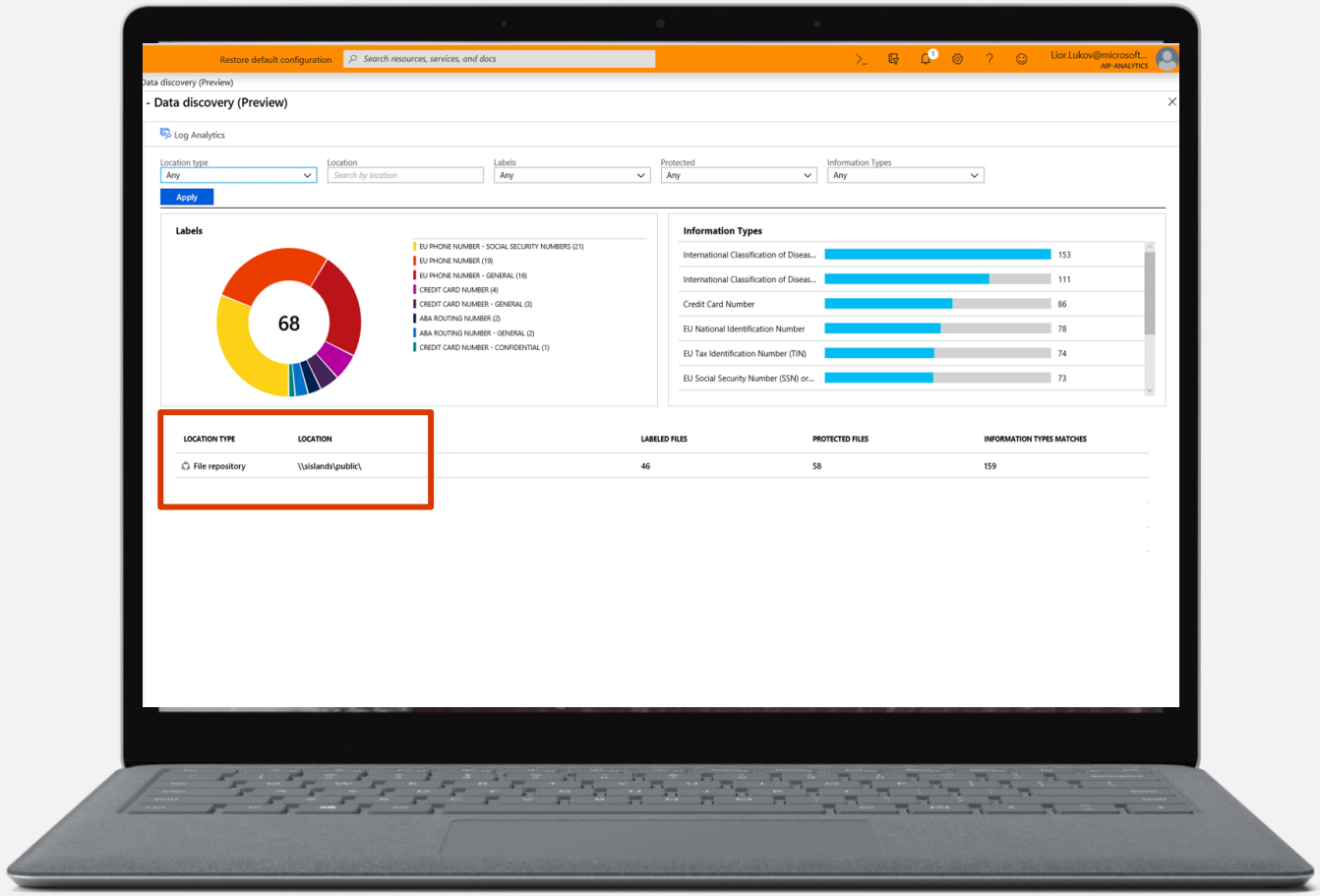
Helps you manage sensitive data prior to migrating to Office 365 or other cloud services

Use **discover** mode to identify and report on files containing sensitive data

Use **enforce** mode to automatically classify, label and protect files with sensitive data

Can be configured to scan:

- CIFS file shares
- SharePoint Server 2016
- SharePoint Server 2013



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

Protect your data across environments

On-prem

Classify and label data in on-prem repositories, including file servers and SharePoint

Office Apps Across Platforms

Label and protect Office files natively across Windows, Mac, iOS, Android and Web Clients

SharePoint, Teams, Groups, PowerBI

Label and protect sensitive data manually and automatically across content and container

Exchange Online

Automatically label and protect sensitive emails in Exchange Online

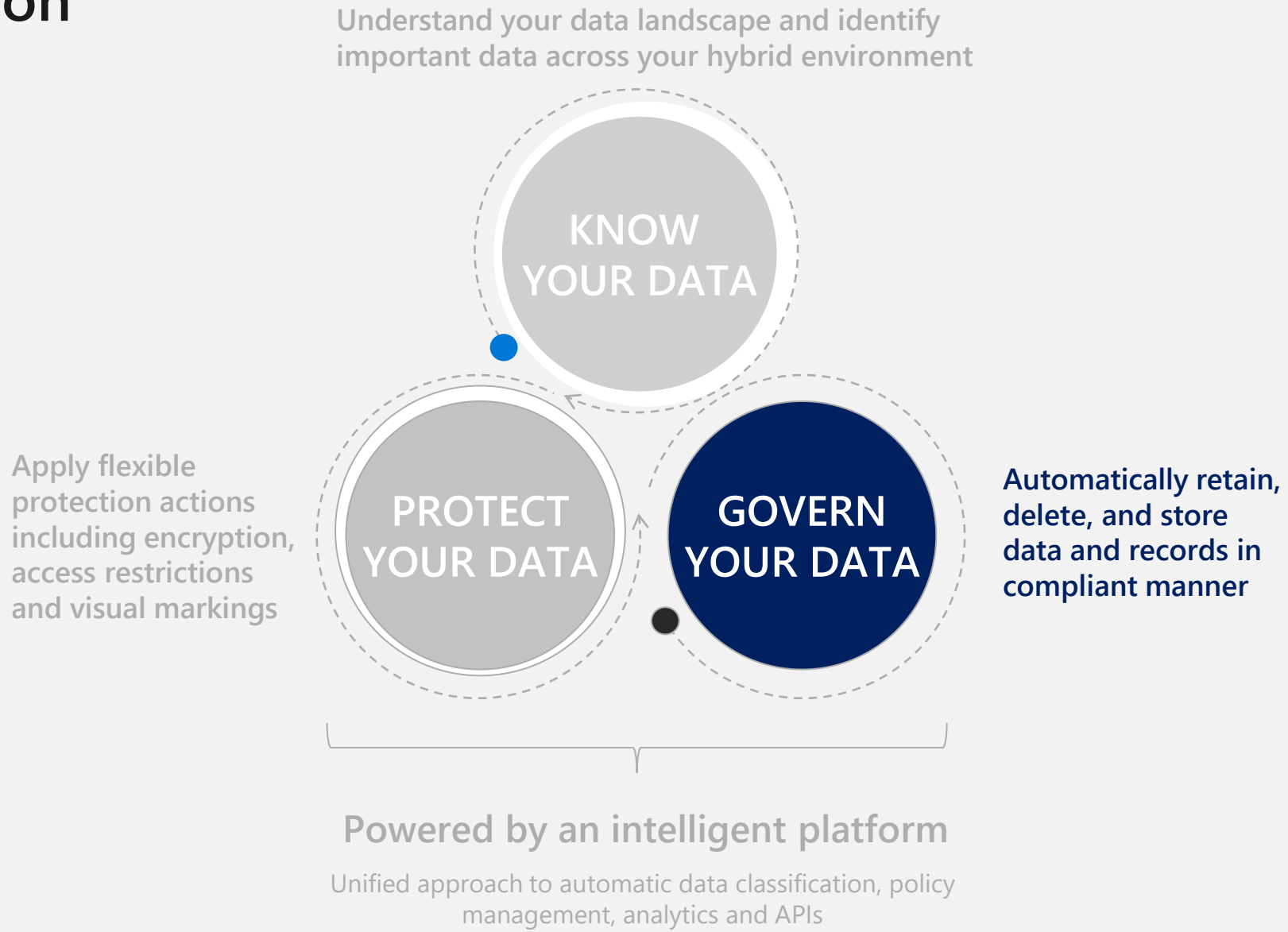
Non-Microsoft Clouds and SaaS apps

Extend protection through Microsoft Cloud App Security to third party clouds and SaaS apps

Unified Label Management in Microsoft 365 Compliance center

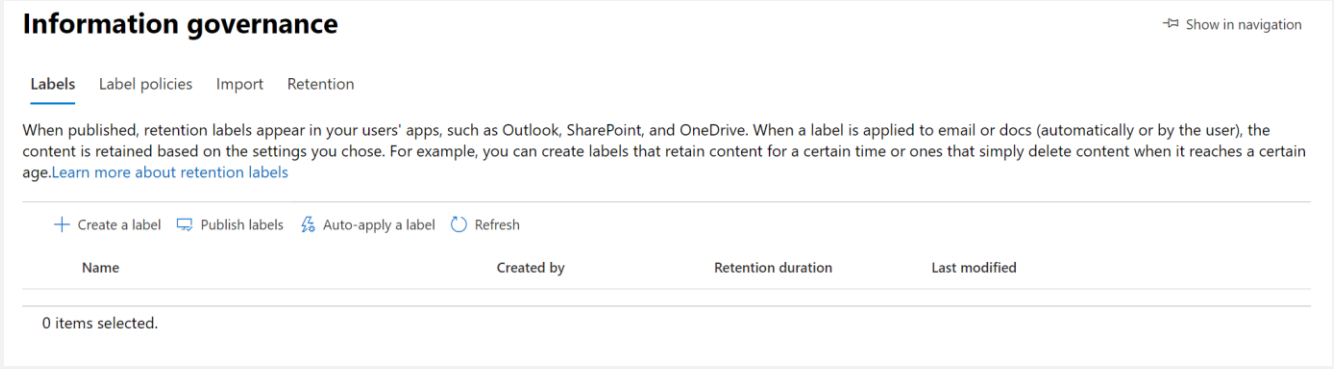
Information Protection & Governance

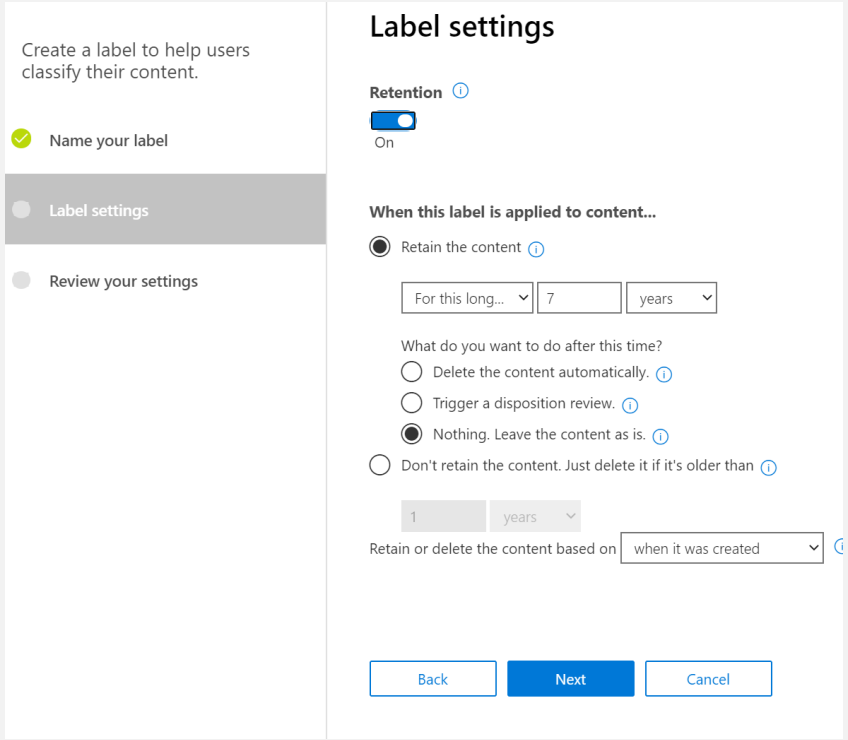
Protect and govern data – **wherever** it lives



Govern Your Data - Information governance

Information governance helps you manage the end-to-end lifecycle of all content across your organization's digital estate, including Microsoft 365 and third-party cloud locations, complex hybrid deployments, and any physical content you bring into Microsoft 365. Trainable classification and automated retention help ensure your data is defensible and retained, and tailored workflows (like disposition review) coupled with deep insights provide greater visibility into remediation.





Office 365 Data Loss Prevention

Why do organizations need DLP?

Prevent Data Loss

Identify and monitor risky sharing activities

Educate users with in-context guidance to make the right decisions

Enforce data use policies upon content without inhibiting productivity

Integrates with classification & labeling to detect and protect data @ egress

Prevent accidental or inappropriate sharing with data loss prevention in Office 365

Microsoft Teams

- Chat messages
- Channel conversations

Exchange Online

- Email in transport
- Email body
- Attachments
- Include or exclude groups

SharePoint Online

- Any file that can be crawled
- Files used in Teams sites
- Include or exclude sites

OneDrive for Business

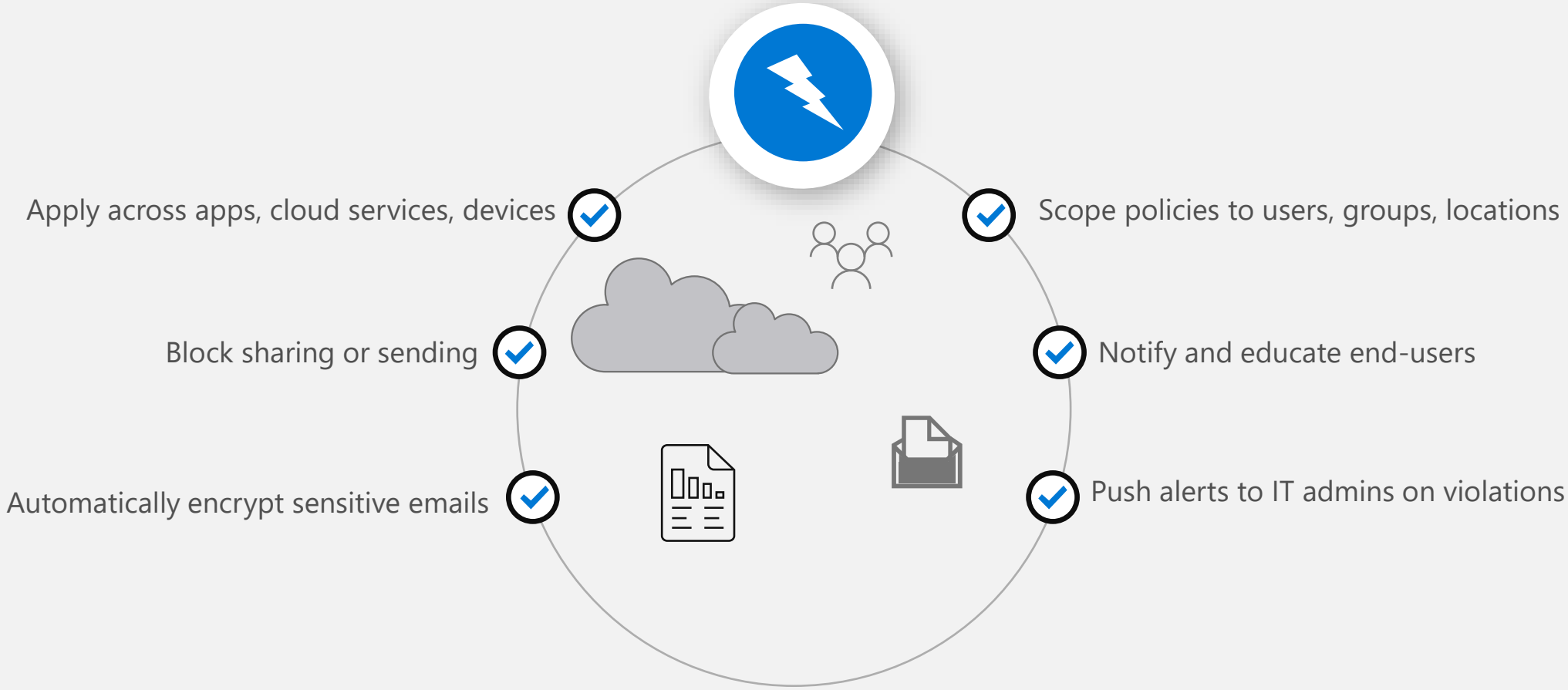
- Same file types as SharePoint
- Include or exclude accounts

Office desktop apps

- In-app policy tips
- Word
- PowerPoint
- Excel
- Outlook

- Policy tips
- Block sharing
- User overrides
- Notification emails

Flexible DLP enforcement options

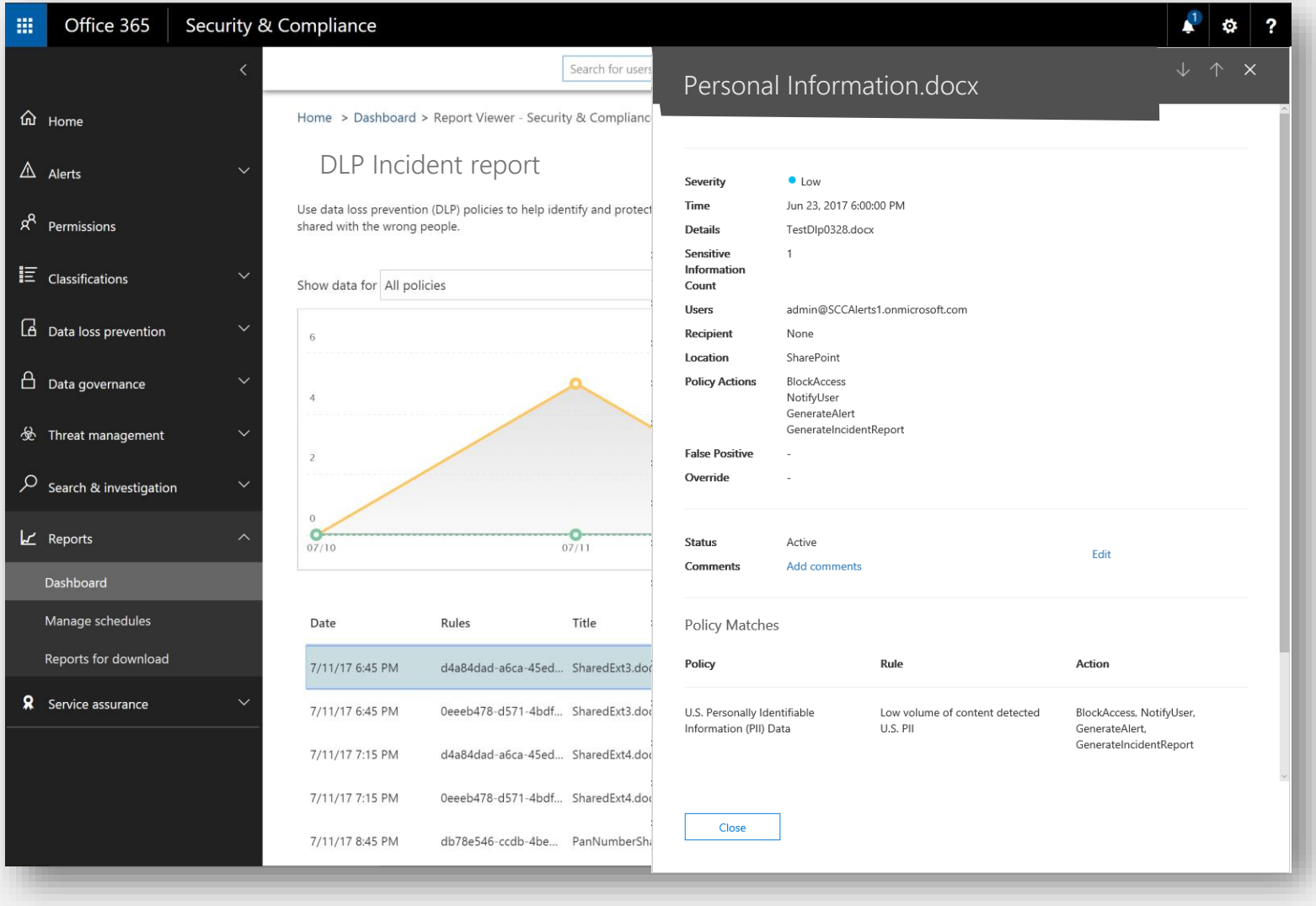


Reporting, Alerts & GIR

Smart report insights provide information on data abnormalities

Enable admins to continue their investigation through the explorer

Complete view of DLP detection for quick assessment of impact



Microsoft

OverNet EDUCATION

Contatti

OverNet Education
+39 02 365738
info@overneteducation.it
www.overneteducation.it

ROZZANO - MILANO
BOLOGNA
ROMA
GENOVA
TORINO

Grazie! – Q&A