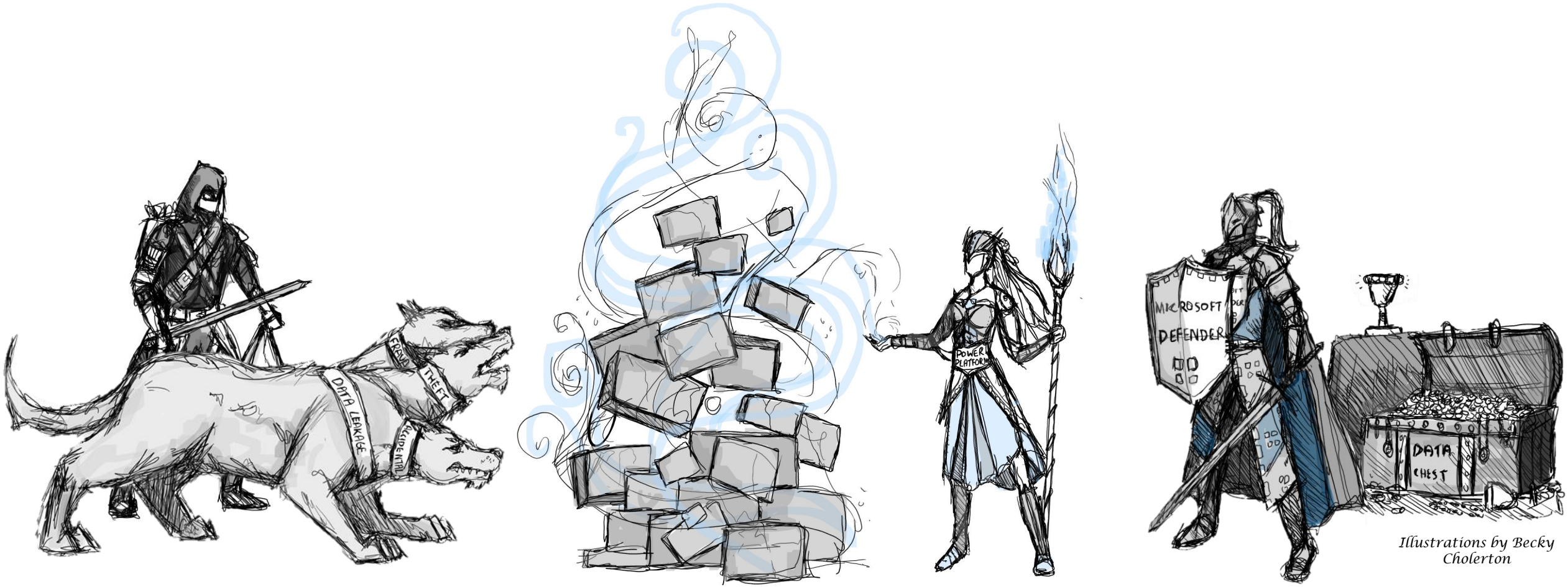
# Compliance @ Speed Part 2 – 26th May, 2021 9:30am – 1pm (British Summer Time)

Join the Microsoft Protectors for Part II at Speed. A 3.5 hour event, where we will build on what you learnt in Part I. More Compliance Platform demos across Microsoft 365 and Azure including:
IRM and Azure Sentinel, MCAS + DLP, more Power Platform integrations+ more Insider Risk Management.




Illustrations by Becky Cholerton

Microsoft

Graham Hosking

Leon Butler

Dan Cousineau

Ally Turnbull

Becky Cholerton

Mark Oburoh

Ana Demeny

# Meet the Team!

# Housekeeping

**There will be breaks & speaker changes throughout**

This is a one way speaker to attendees audio, so please ask any questions in the Q&A

This will be recorded and links sent within 7 days

Feedback – aka.ms/complianceatspeedfeed

These Resources will be shared with you (to share with others at your company)

**All content is under your partnership NDA**

# In case you missed part 1

- **On-Demand Recording** - https://aka.ms/complianceatspeed-reg
- **Slides** - https://aka.ms/complianceatspeed-repo



# Agenda (UK GMT)


09:30 - Intro and Housekeeping – Ally Turnbull

09:40 - Opening Keynote – Customer Journey – Becky Cholerton

10:05 - RPA – Ally Turnbull + Ana Demeny

10:30 - Break 10 mins

10:40 - Insider Risk Deeper Dive– Graham Hosking

11:20 - MCAS DLP – Ally Turnbull

11:40 - Break 10 mins

11:50 - ~~Insider Risk Integration with Azure Sentinel~~ Encryption options in M365 – Leon Butler

12:10 – Advanced Audit – Graham Hosking

12:25 – Project Syntex – Leon Butler

12:50 – Wrap Up

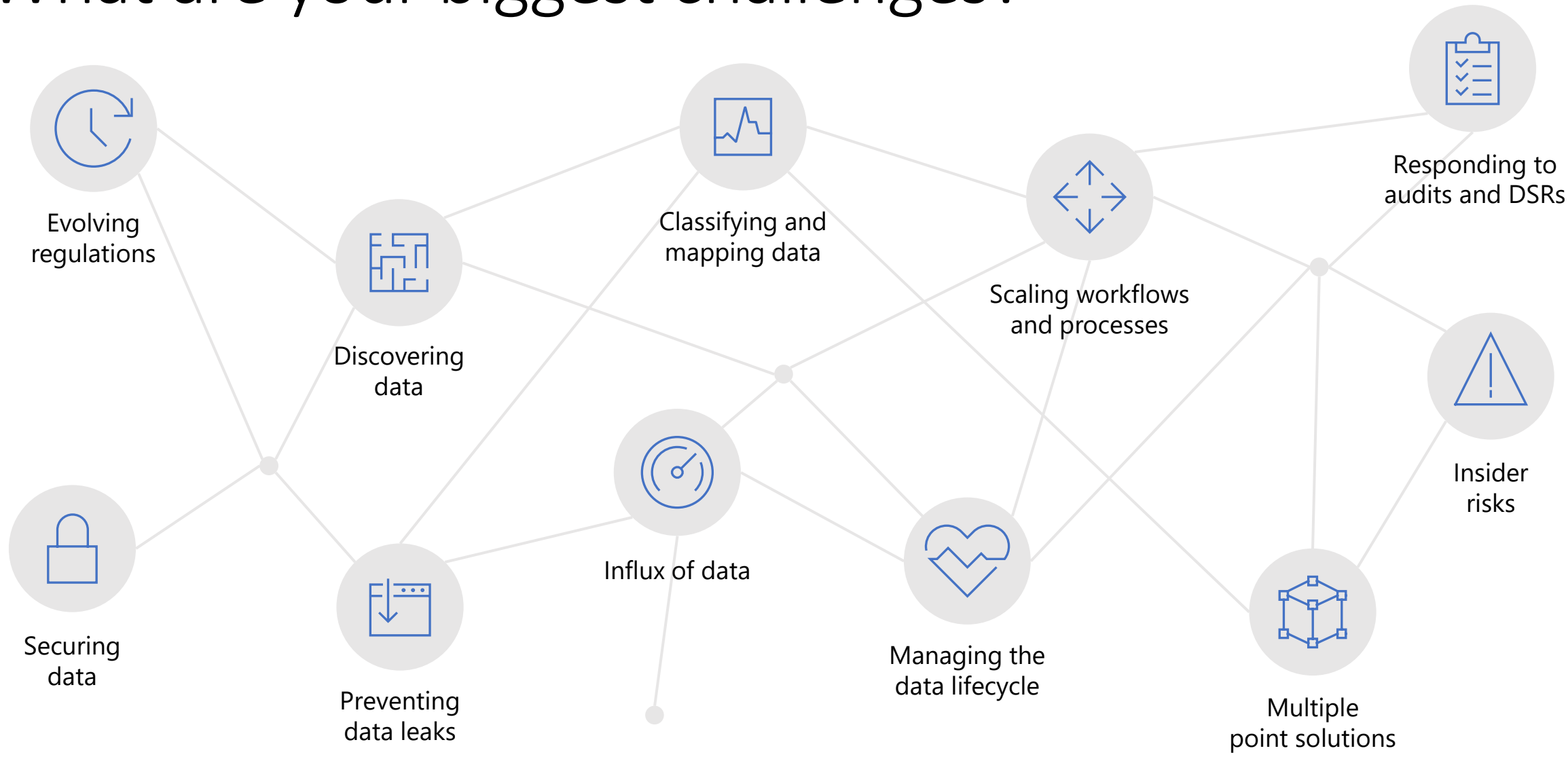
13:00 – Event ends

# Opening Keynote

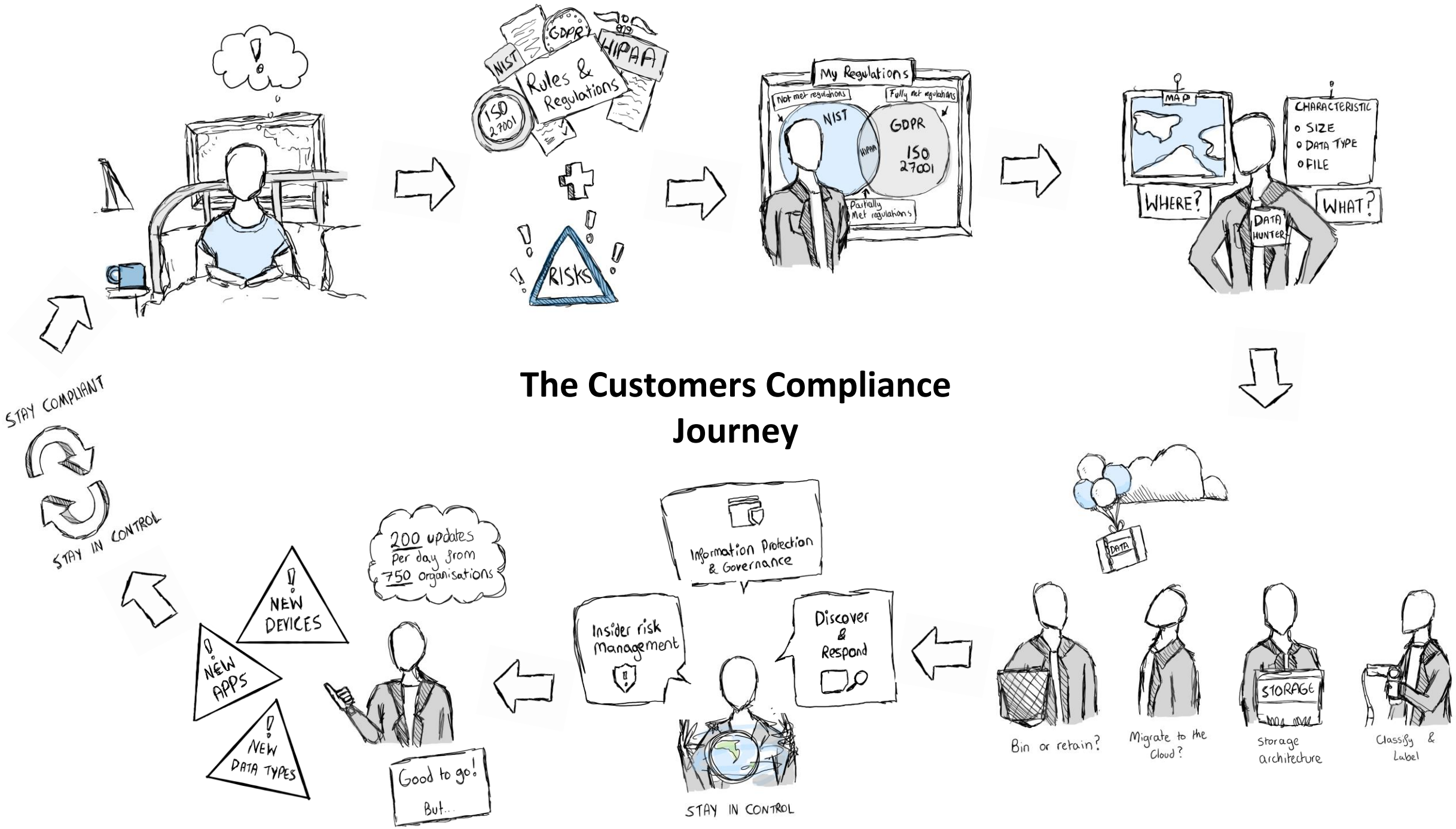
**Compliance @ Speed**

Becky Cholerton
Technical specialist in security & compliance

# What are your biggest challenges?



# The Customers Compliance Journey



# Intelligent compliance and risk management solutions

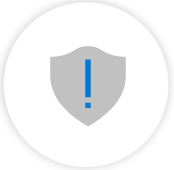
**FUNCTION KEY**

- Privacy
- Compliance
- Legal
- HR
- IT
- LOB
- Procurement

## Information Protection & Governance

Protect and govern data anywhere it lives

Microsoft Information Protection
Advanced Data Governance
Data Loss Prevention
Records Management
Auto classification and Retention



## Insider Risk Management

Identify and remediate critical insider risks

Insider Risk Management
Communications Supervision
Customer Lockbox
Customer Key
Privileged Access Management
Advanced Message Encryption
Label analytics
Trainable ML classifiers
Regulatory record

## Discover & Respond

Quickly investigate and respond with relevant data

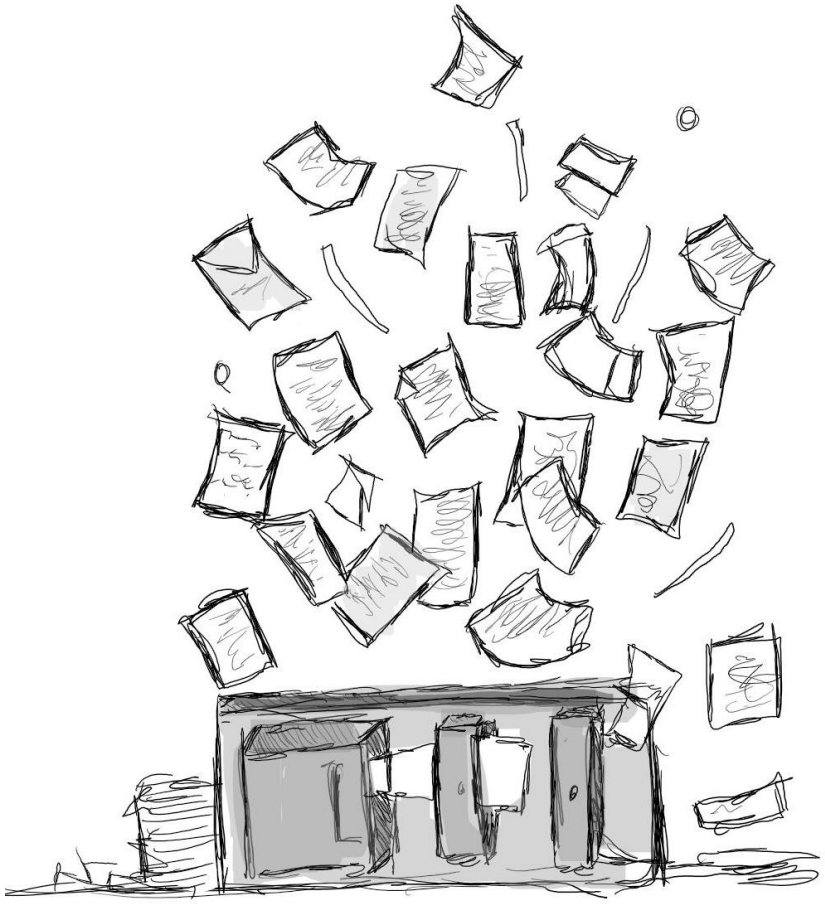
Data Investigations
Advanced eDiscovery
Custodian management
Deep indexing
Redaction
Optical character recognition
Data themes
Near-duplication

## Compliance Management

Simplify and automate risk assessments

Compliance Score
Compliance Manager
Long-Term Auditing
Assessment template

# Data loss prevention (DLP)



# Key customer DLP pain points

## Friction

On-prem infrastructure

Endpoint agent

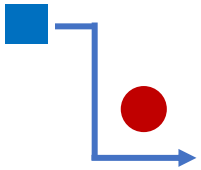
DLP from the ‘outside-in’

Large system footprint

## Difficult to manage

“You can’t protect what you can’t see”

Complicated policies



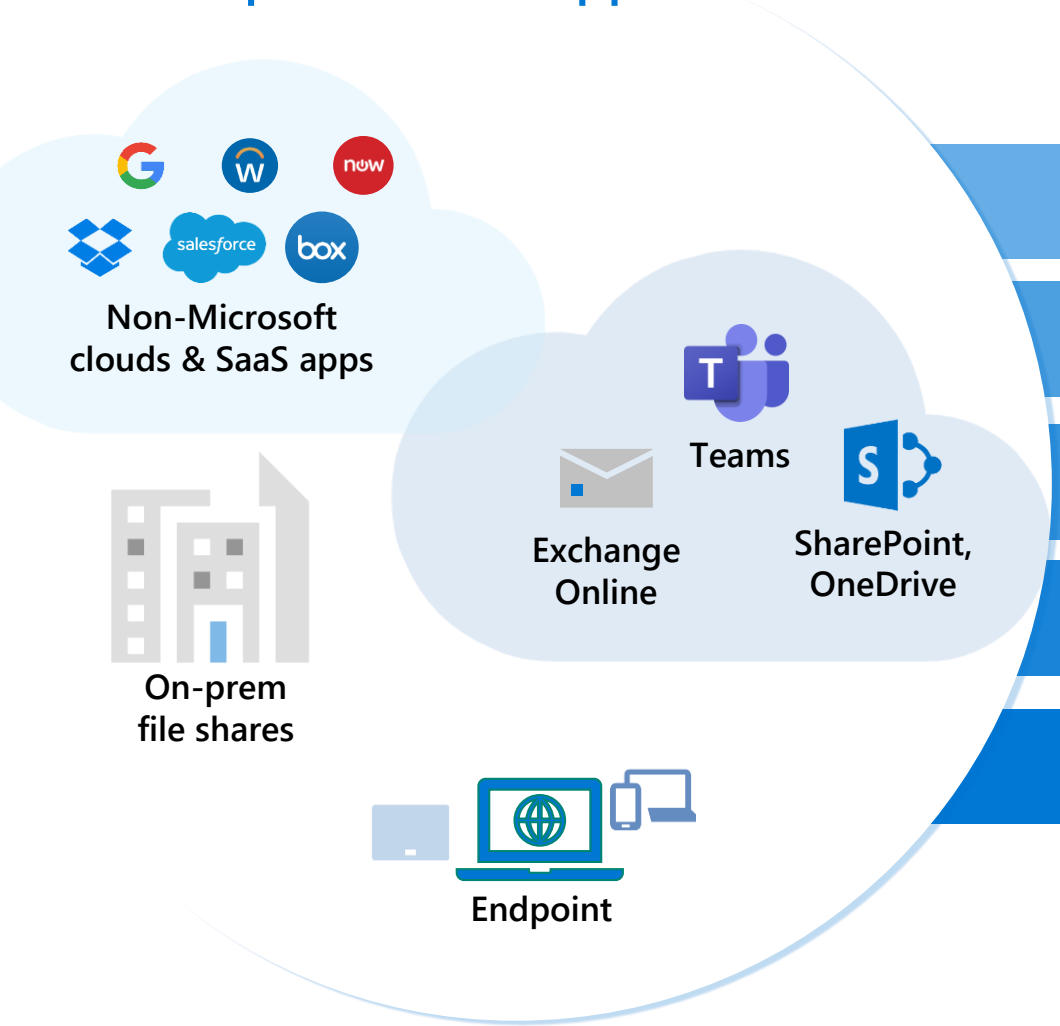
## Effectiveness

Heavy handed lockdown

Siloed solution

# Microsoft DLP solution overview

## Comprehensive support across workloads with unified and integrated experiences




Guided onboarding

Unified & flexible policy management

Integrated with MIP

Integrated end user experiences

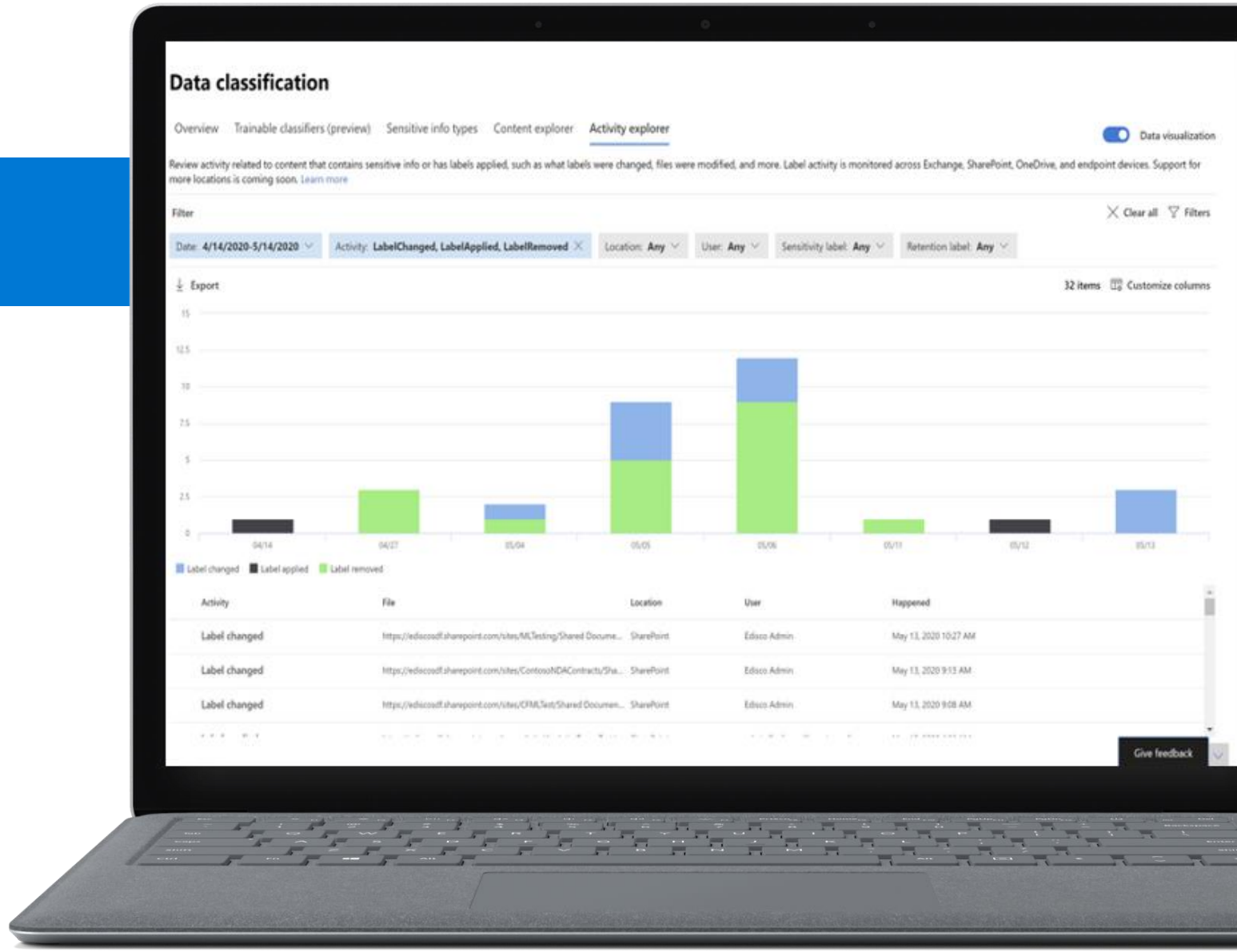
Unified alerting & remediation

# Guided onboarding

Cloud managed and delivered

No on-premise infrastructure required

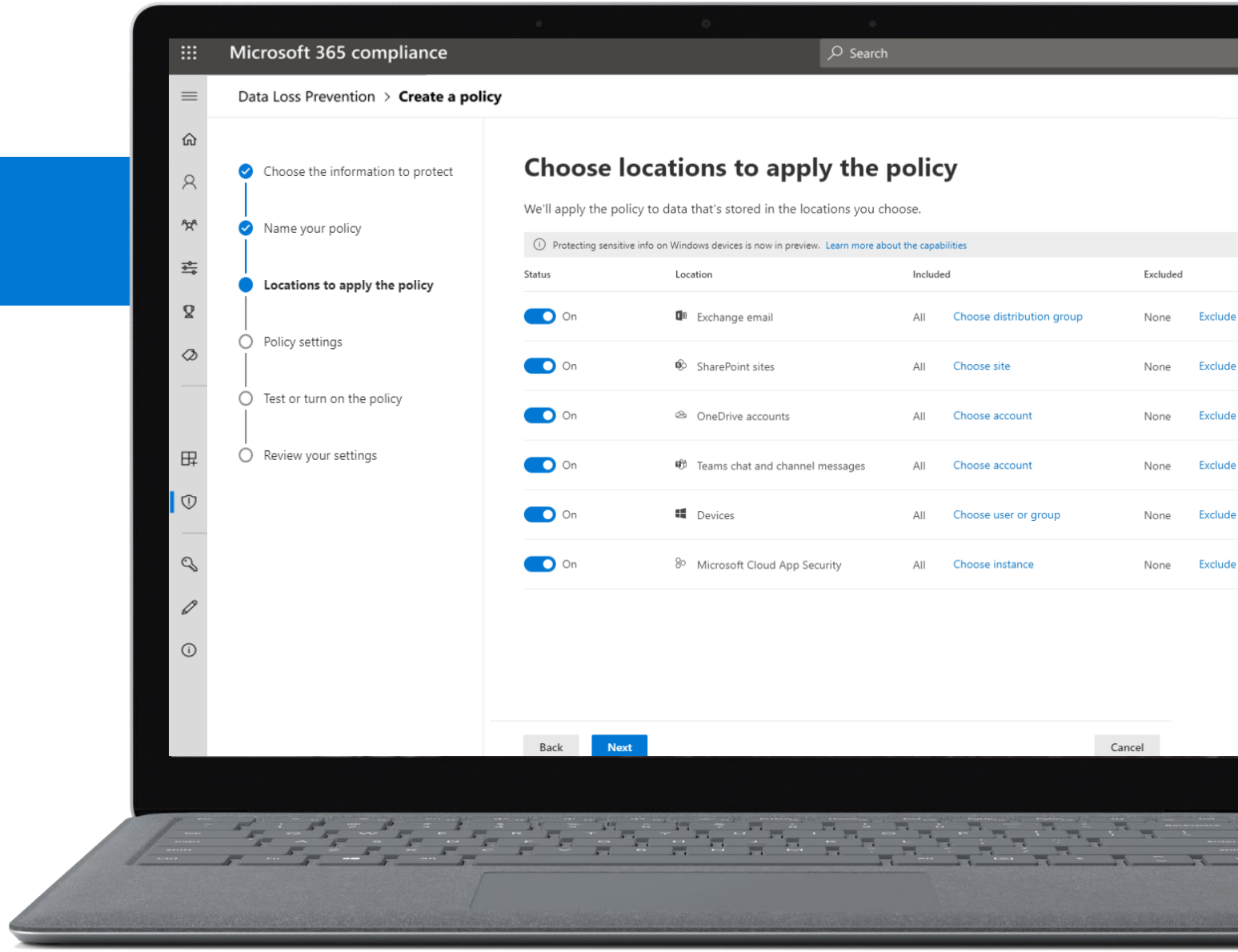
Out-of-the-box analytics, no policy needed



# Unified policy management

Unified, flexible policy management and enforcement across devices, apps and services from Microsoft 365 Compliance Center

Rich flexibility in configuring rules and enforcement actions

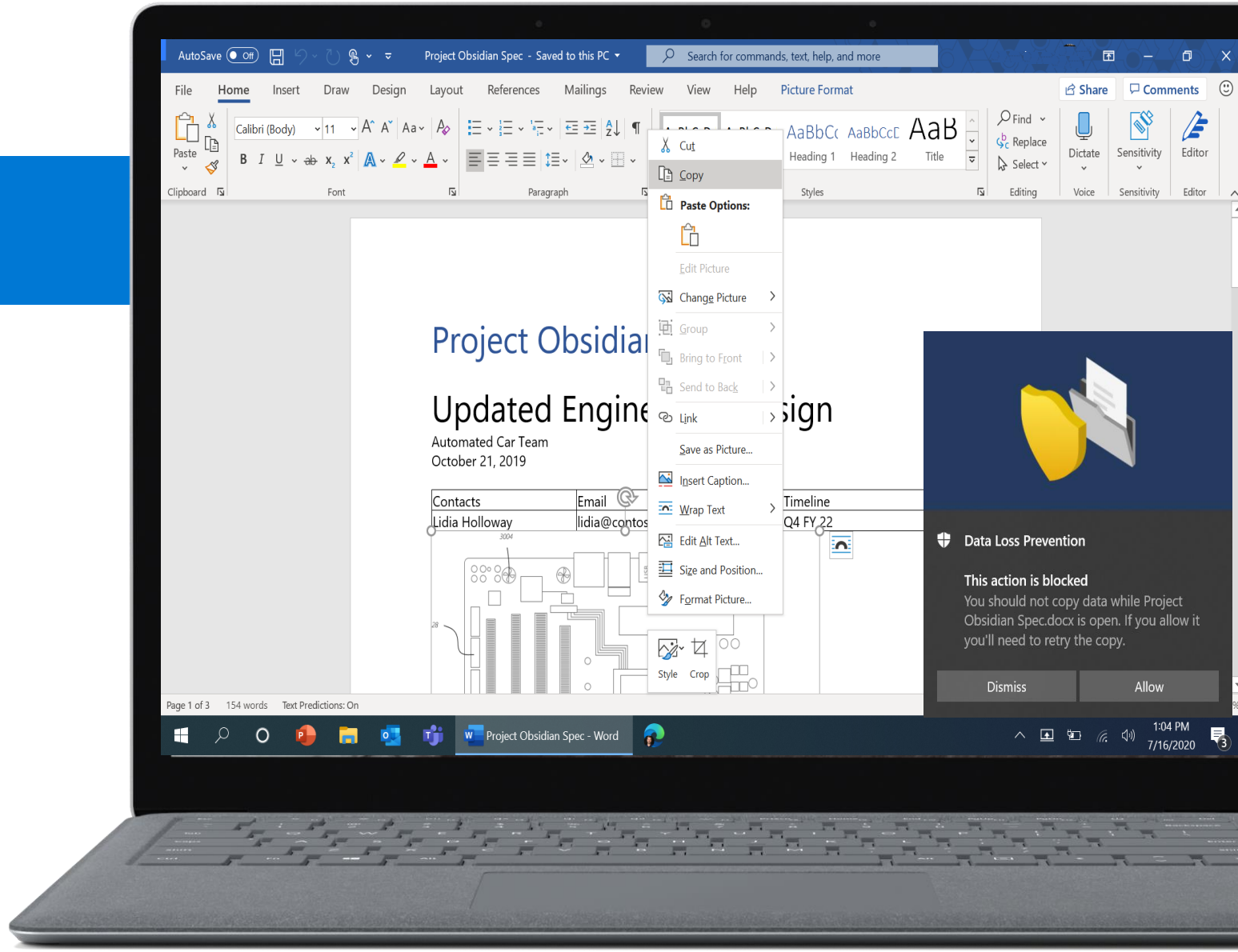


# Integrated end user experience

Built-in experiences in Office, Windows, Edge, and other apps helps preserve user productivity

Policy Tips help educate users when they are about to violate a policy.

Available across platforms: desktop, web, and mobile apps.

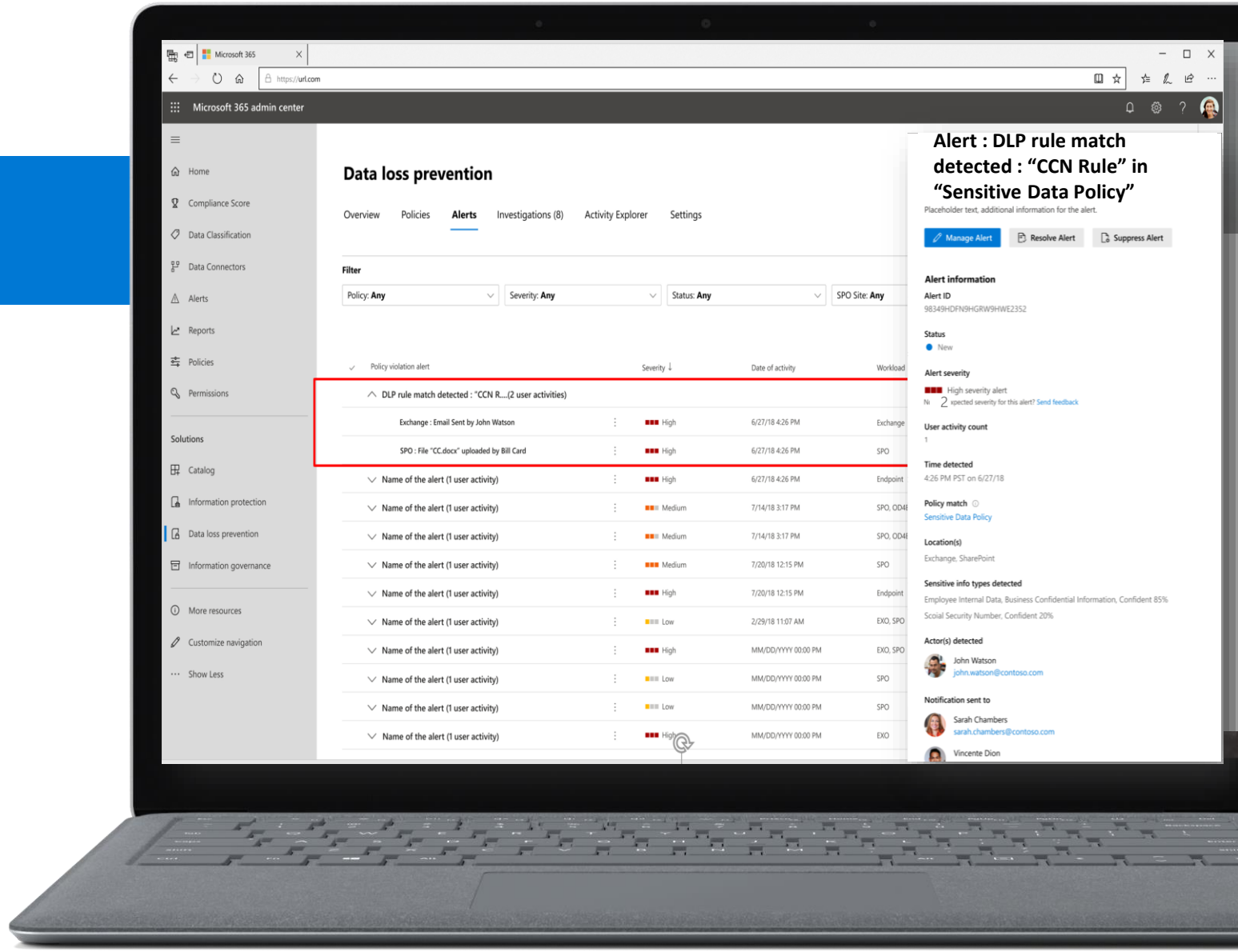


# Unified alerting and remediation

Data-centric protection approach

Rich detail to triage and remediate

API support enabling SIEM integration



# Announcing Endpoint Data Loss Prevention

**Identify and protect information on endpoints**

## Native protection

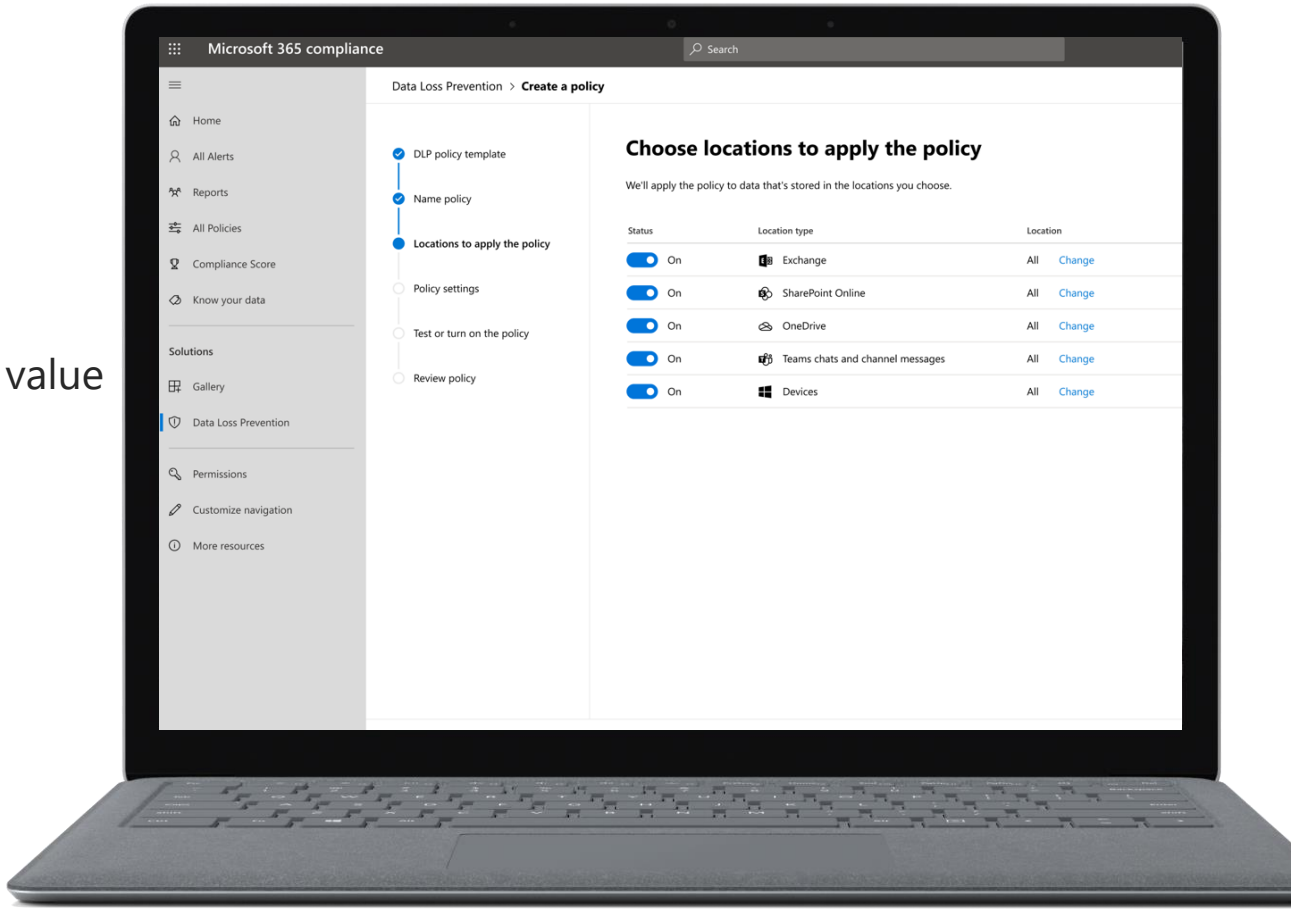
Built-in to Windows 10, Office Apps, Edge – no agent required

## Seamless deployment

Cloud-delivered, lightweight configuration leads to immediate value

## Integrated

Integrations (e.g. with Microsoft Information Protection) build on existing capabilities and focus on risks that matter



# DLP Solution Overview

**Comprehensive support across workloads**

| Exchange Online | Teams | SharePoint, OneDrive | Endpoint | Non-Microsoft Clouds and SaaS apps | On-prem file shares | Expanded to Azure, SQL & non-M365 workloads |
|---|---|---|---|---|---|---|
| | | | | | | Data catalogue |

## Unified and integrated experiences

| Guided onboarding | Unified & flexible policy management | Integrated with MIP | Unified alerting & Remediation | Integrated end-user experiences |
|---|---|---|---|---|
|  |  |  |  |  |

# RPA

## Digital Transformation ++

@AnaDemeny

/anademeny

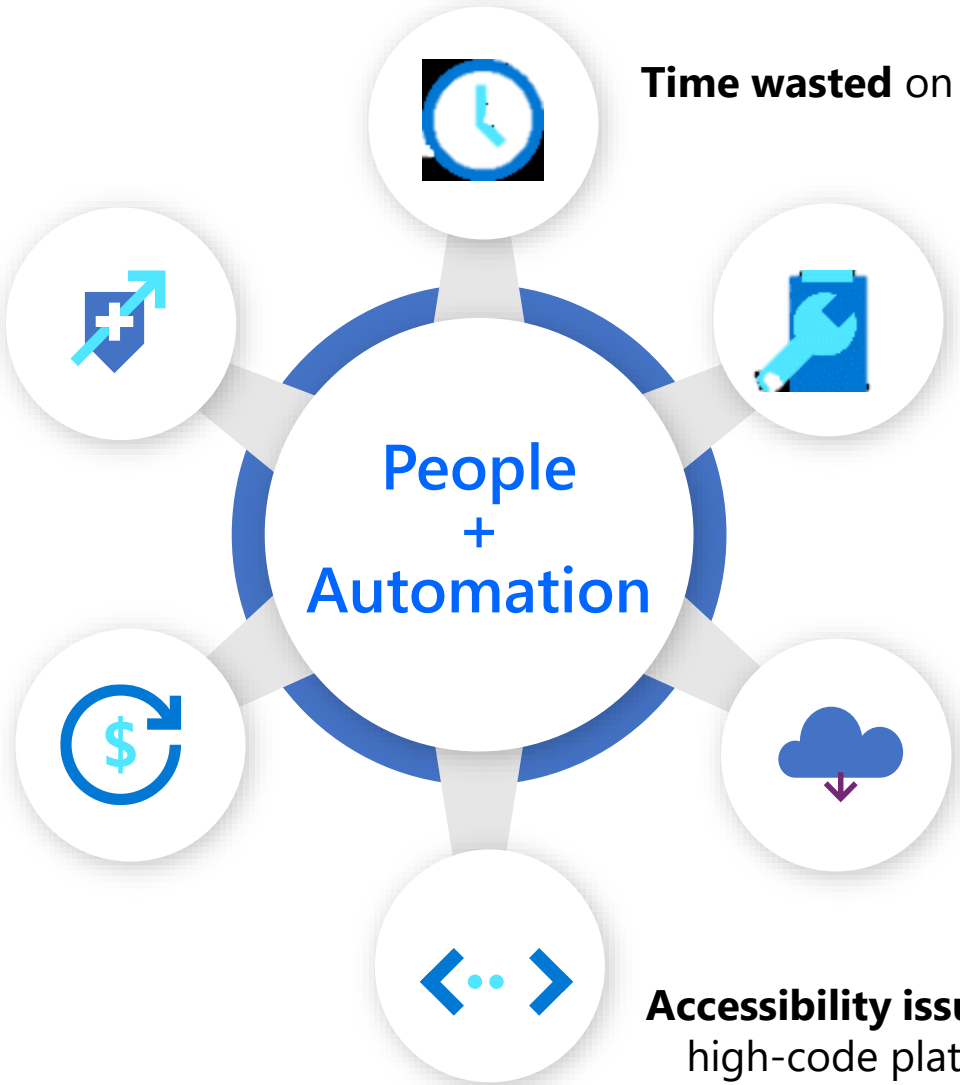
Partner Technical Architect
(INTEGRATION & RPA)

Ally Turnbull

/turnvirtual

Cloud Solution Architect
(Security, Compliance and Identity)

# Key challenges




**Time wasted** on repetitive tasks

Risk of human **error** when conducting repetitive tasks

Difficult to **bridge old and modern** systems with or without **APIs**

**Accessibility issues** with high-code platforms

**High costs** incurred completing repetitive tasks

Hard to manage workflows, while **maintaining security and compliance**

Wave 1

## Changing workforce

**35%** of the workforce are millennials

**75%** of the workforce will be millennials by 2025

**24%** of the workforce are Generation Z

Sources: US Bureau of Labor, Wired

Wave 2

## Surging digital demand

**500m** More apps will be created in the next five years than in the last forty years

**>85%** of organizations struggle to analyze unstructured data

**50%** Half of digital work activities can be automated with current technology

Sources: DORA, Black Duck, ISC, IDC, Forrester, AppAnnie, Microsoft, IDG: Big Data Survey 2017, McKinsey

Wave 3

## Not enough developers


Sources: BLS, NSF, NCES, IDC, Gartner, LinkedIn, C+AI Corp Strat

Wave 4

## The Great Lockdown

**42%** of US employees working from home

**5.1%** contraction in the GDP in 2020

**The most severe recession** since the end of World War II

Sources: World Bank

# Better together with easy scalability

## Power Platform. Innovation anywhere. Unlocks value everywhere.

**Power BI**
Business analytics

**Power Apps**
Application development

**Power Automate**
Workflow automation

**Power Virtual Agents**
Intelligent virtual agents

## Scale with your most used enterprise apps and services in one platform

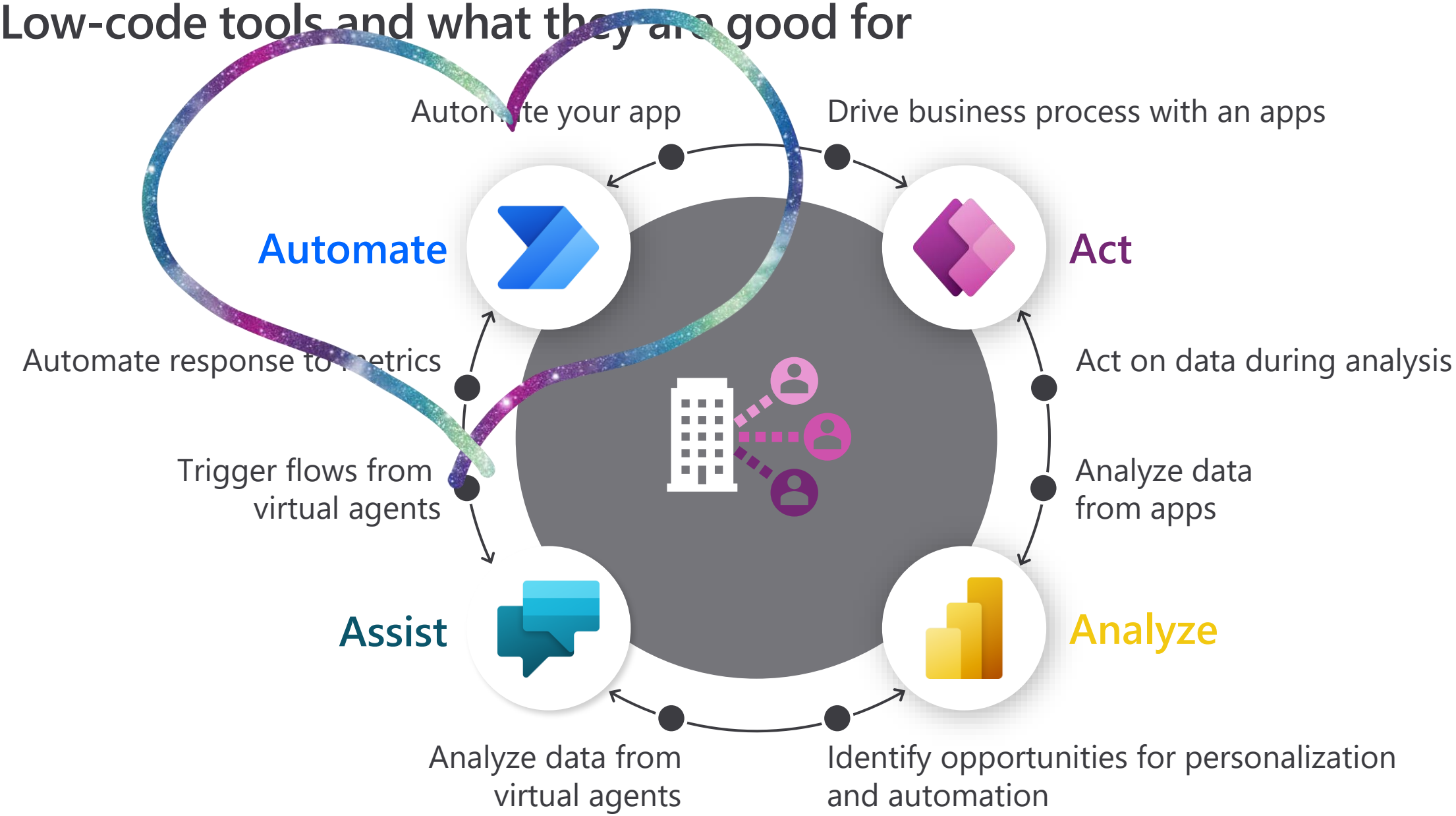
**1st and 3rd party**
Use flows to **bring documents and data from other systems** with other 400+ connectors.

**Microsoft 365**
**Share Excel Spreadsheets data with any system with connectors.**

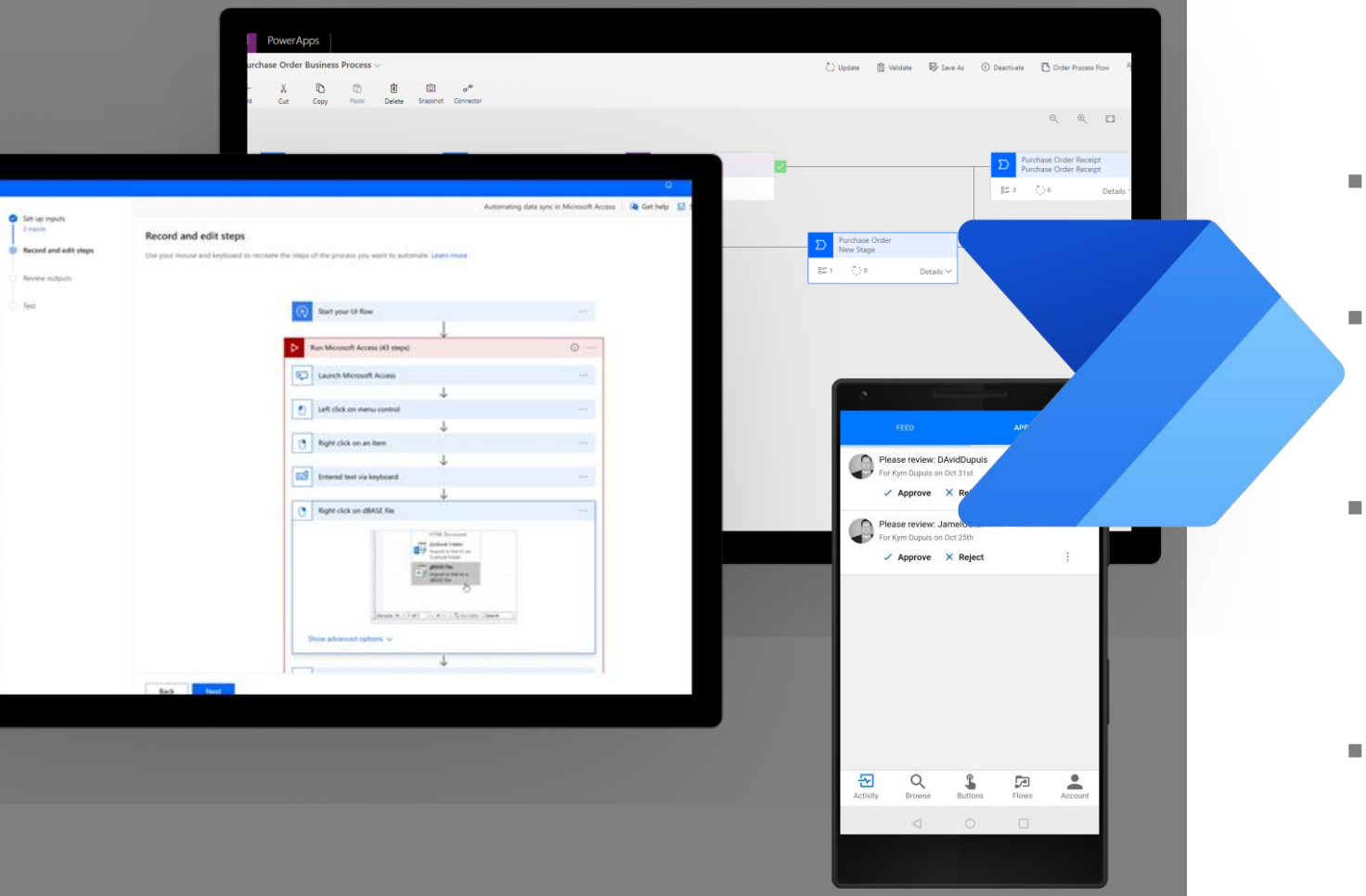
**Microsoft Azure**
**Easily share and reuse Azure solutions with your citizen developers.**

**Dynamics 365**
**Bridge the gaps across all your business applications.**

# Low-code tools and what they are good for

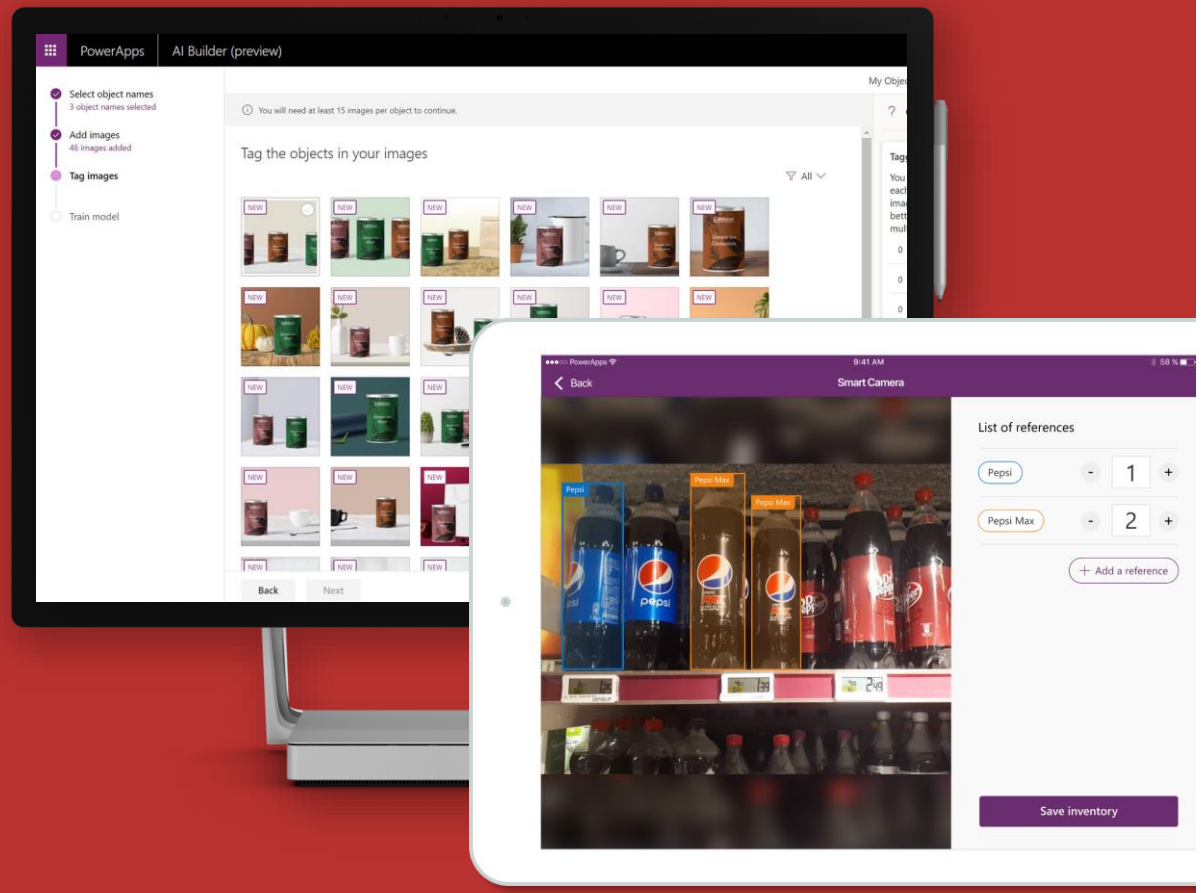


# Automate tasks and business processes workflows with Power Automate




- Processes events from **400+ out-of-the-box triggers to start flows** – plus custom events in external systems through custom connectors
- After the trigger, actions can read and write data in any of the **400+ connectors** in integration workflows
- **Quick modeling of business processes** that span across apps and services
- Integrates with **modern approvals** that can be handled from inside email client or mobile device
- Everything from simple if-this-then-that processes to detailed conditional branching that leverages the Microsoft Cognitive Services for **AI-powered decision making**
- **Robotic Process Automation** delivering end-to-end automation across AI, APIs, and UI on the Microsoft Power Platform

# Infuse artificial intelligence in your business solution with AI Builder




- Every citizen developer is now an AI expert and can easily build, train, deploy and use **AI Builder**
- Create and organize contact and account data more efficiently with **business card scanner**
- Predict outcomes directly from historical business data patterns with **Prediction**
- Spend less time in the field trying to locate, identify and count items with **object recognition**
- Reduce PDF and paper forms data re-entry efforts and errors with OCR **forms processing and receipt scanning**
- Gather insights and trigger actions from natural language processing with **text classification**
- Augment feedback insights with **Sentiment Analysis**

# Recognition in 2020 Gartner MQ reports

Magic Quadrant for Enterprise Low-Code Application Platforms, 2020


Magic Quadrant for Robotic Process Automation, 2020

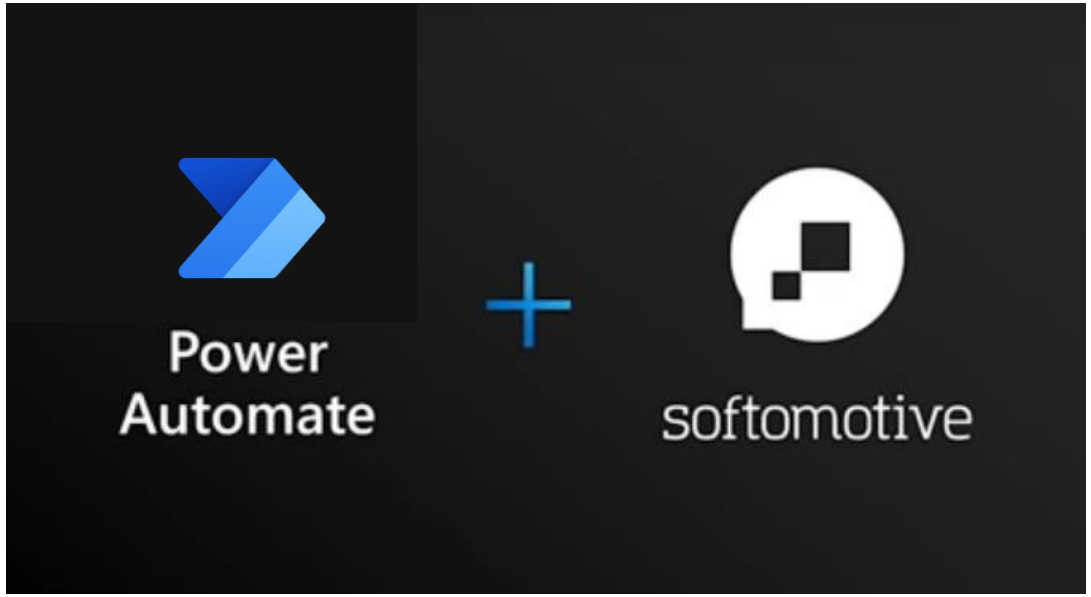

Microsoft Power Automate

# Microsoft acquires Softomotive to expand low-code robotic process automation capabilities in Microsoft Power Automate

Microsoft announced the acquisition of Softomotive, a world-leading provider of robotic process automation (RPA) with over 15 years of experience and the creator of WinAutomation.

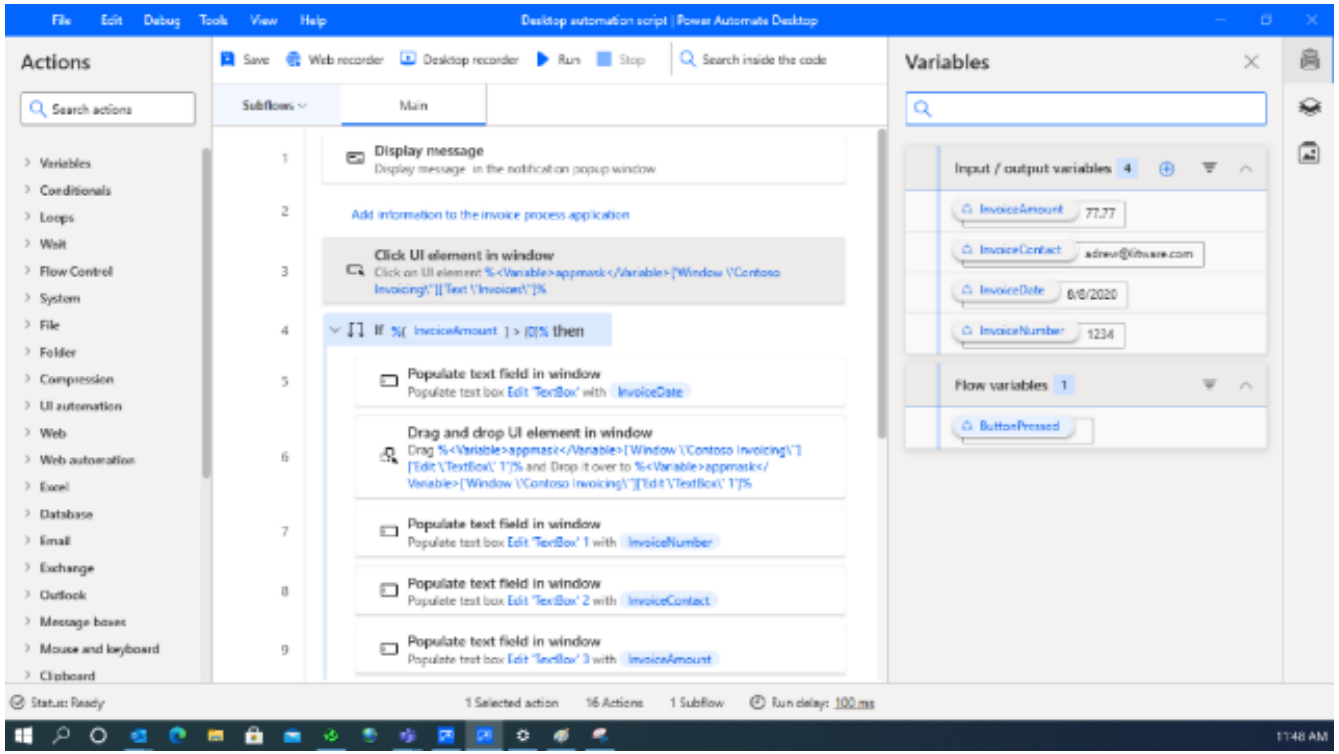
WinAutomation, expands the Microsoft Power Automate capabilities, through it's Web & UI Automation, interaction with Legacy systems and Terminals, Java applications as well as Citrix Automation.

The combination of these two products, addresses all needs in the RPA market, and drives the RPA experience to a completely different level.



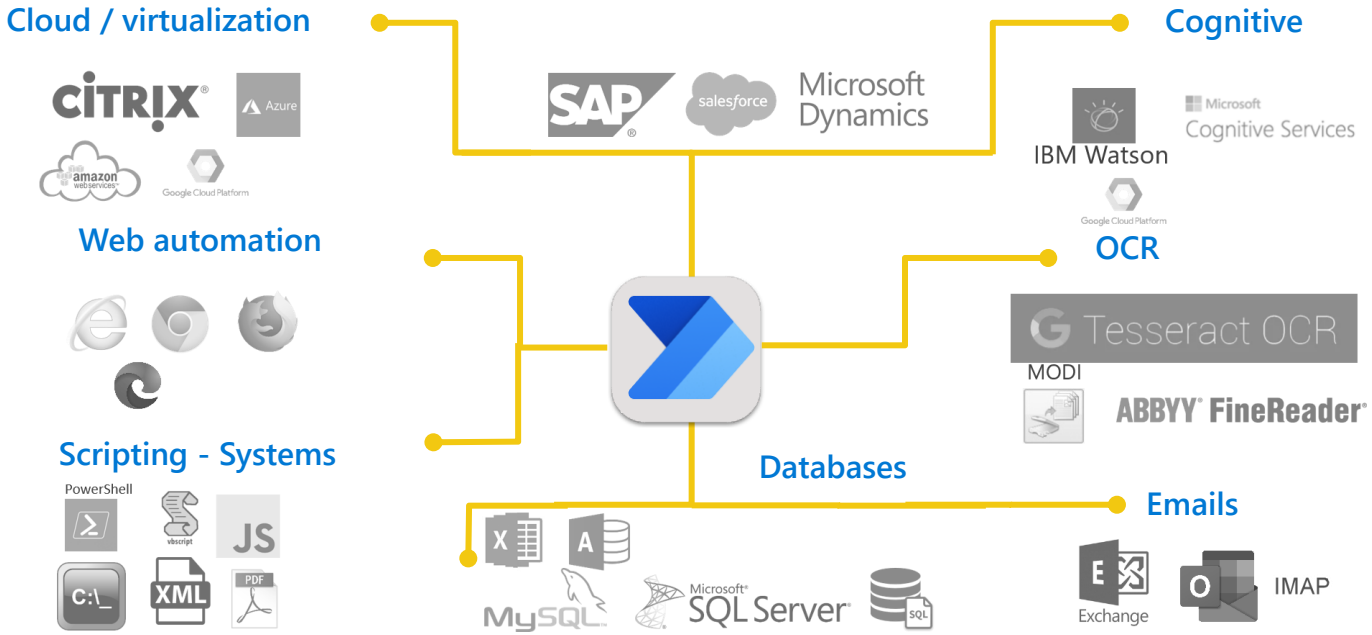
# Introducing Power Automate Desktop

- Technology and intellectual property acquired from Softomotive, now an integrated Power Automate experience.
- Ease of use - Low-code/no-code Drag & drop approach with Recorders (Desktop and Web)
- Advanced Debugging features
- Reusability of Controls, Images and Functions
- User and Process collaboration through message boxes
- Advanced Error handling features
- Support for advanced coding-scripting *(VBScript, JavaScript, Python, PowerShell, Command Line)*
- Attended and Unattended execution mode
- Concurrent process execution



# Bridging automation between the old and new

- Web - desktop applications
- Citrix and VDI Environments
- Cloud automation (Microsoft Azure, Amazon AWS) and Cognitive capabilities (IBM, Google, Microsoft)
- Databases-SQL Excel
- PDF & XML
- Files, folders and mouse-keyboard
- Email (IMAP, smtp, exchange, outlook)
- Computer vision and image recognition
- Encryption – cryptographic actions, CyberArk support
- OCR for structured and unstructured data capturing and handling



# Recognition as Leader in 2021 Forrester Wave report

- **Strong momentum for Power Automate:**

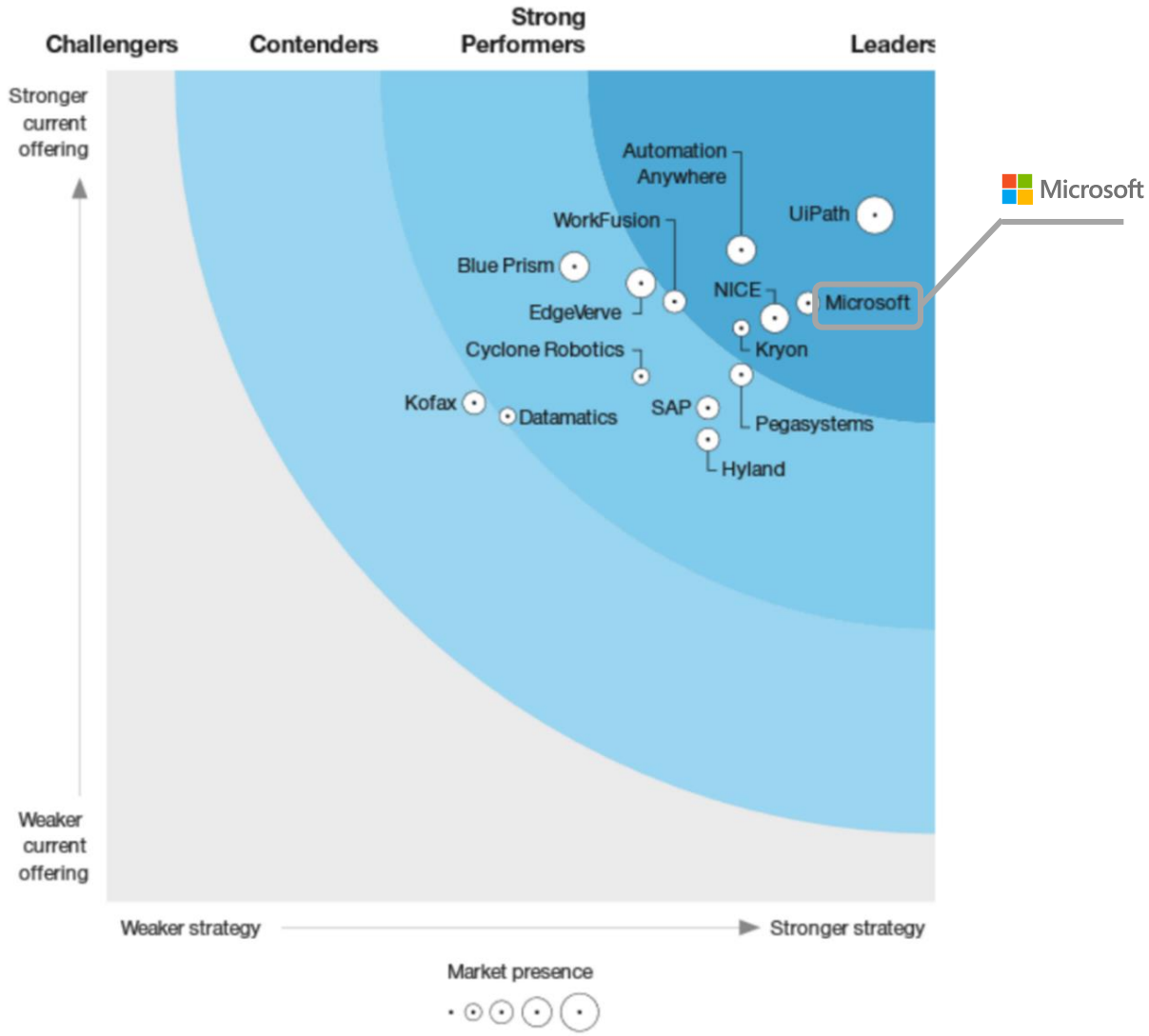
"Microsoft has caught up with the Leaders. The software giant's vision is to deliver the most comprehensive SaaS-based intelligent automation solution; Power Automate is a cloud-native, low-code automation platform that brings together UI- and API-based automation with AI."

- **Customer success is achieved at no cost:**

"[Microsoft offers a] rich set of training and learning resources and community programs, complemented by a broad global partner ecosystem, helps customers succeed at every stage. Microsoft focuses on democratizing RPA by making it accessible to users with a very low entry barrier. Users can start instantly at no cost and can deploy their first automation in minutes."

- **Ease of use and visual appeal:**

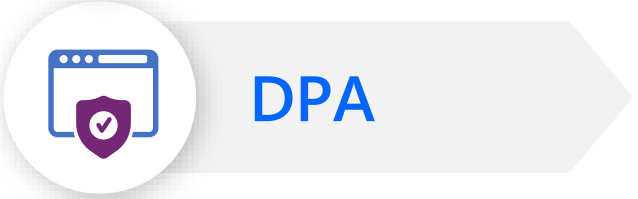
"Microsoft customers seeking RPA get an easy, attractive offering that fits business users, citizen developers and professional developers alike." "The design experience is rich, yet intuitive, and will please citizen and professional developers alike."



# ONE intelligent automation platform

## ...not just an RPA tool


**Robotic process automation –** UI automation in Power Automate through Power Automate Desktop as the platform for desktop authoring. RPA can automate everything from Windows and web applications to legacy systems like mainframes.




**Digital Process Automation –** Cloud flows have access to 400+ built-in, native and 3rd party connectors through no-code APIs – you can even bring your own custom connectors to connect to any system with an API endpoint.

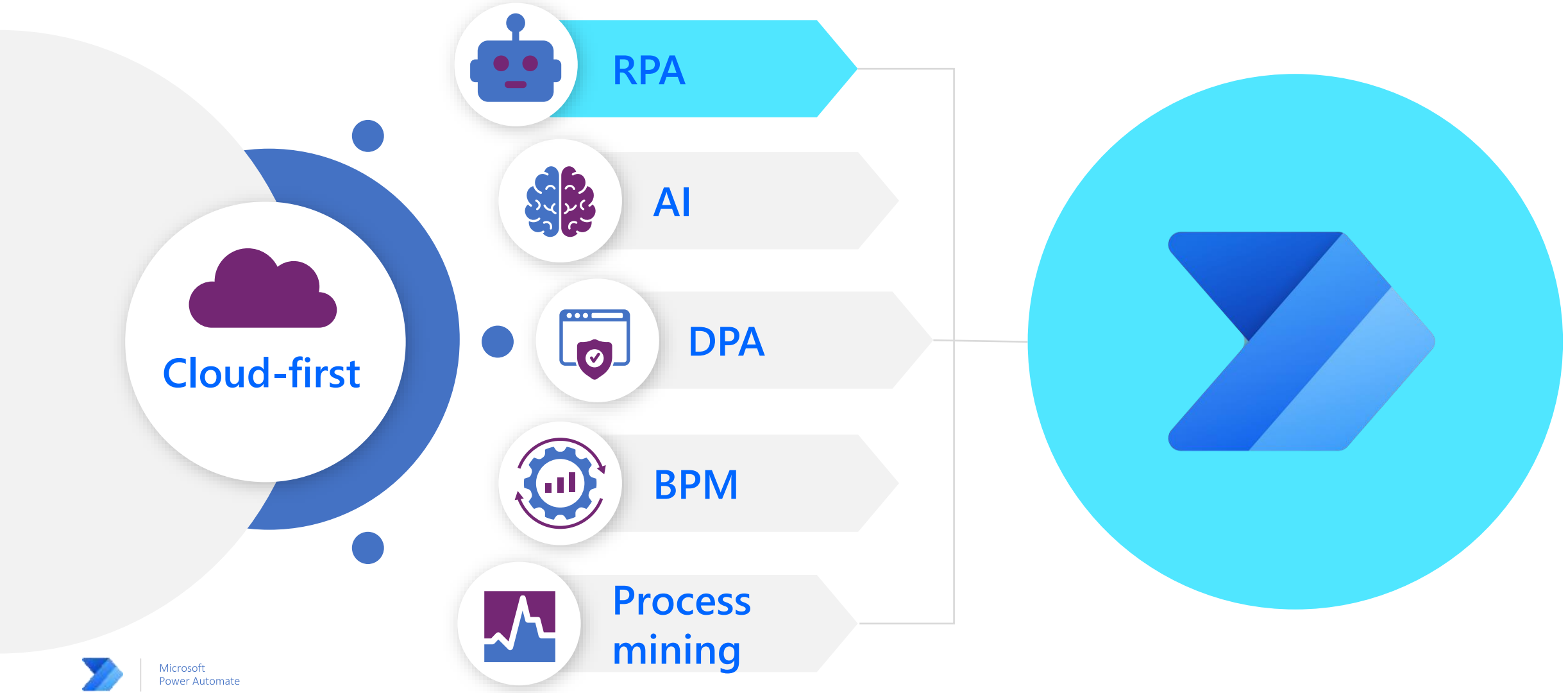

**Artificial intelligence –** AI-driven capabilities like forms processing or intelligent document processing in AI builder, helps automation to understand data from analog sources like paper.


**Business process management –** Automate guided, multistep processes using business process flows. These business process flows can manage everything from basic approval processes to advanced workflows that connect to other systems using DPA or RPA.


**Process advisor (preview) –** Understand how people in your organization are spending time on manual tasks every day. Process advisor lets anyone share their processes so that you can analyze bottlenecks and get recommendations on how to improve using automation.

# Automation is not an island

## One intelligent automation platform



# Top workplace tool

Power Automate takes more than **25 billion** automated actions on behalf of its users every month

**2.8 million** monthly active users

Microsoft

# RPA Early Adopter Program

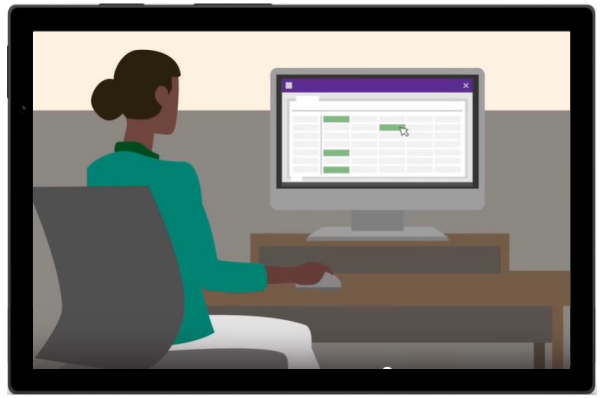
# New: RPA use case videos on Stream


## Invoice Processing

Watch now

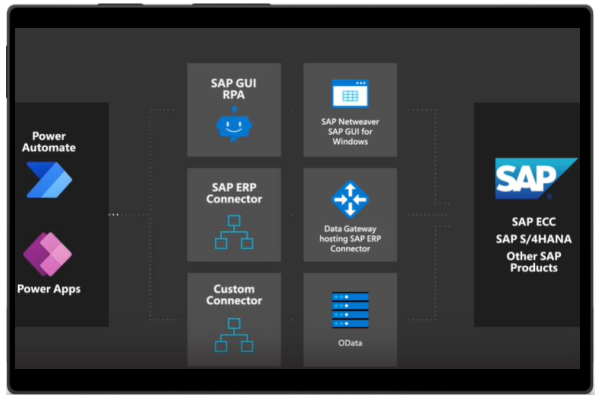

## Loan Processing

Watch now



## Automated Reporting

Watch now




## SAP Use Case

Watch now

# Use Case Decks

## Financial Services

Use Case Deck

## Healthcare

Use Case Deck

## Manufacturing

Use Case Deck

## Retail

Use Case Deck

## Telecommunications

Use Case Deck


# Demo

# Thank you!

@AnaDemeny

/anademeny

Partner Technical Architect
(INTEGRATION & RPA)

Ally Turnbull

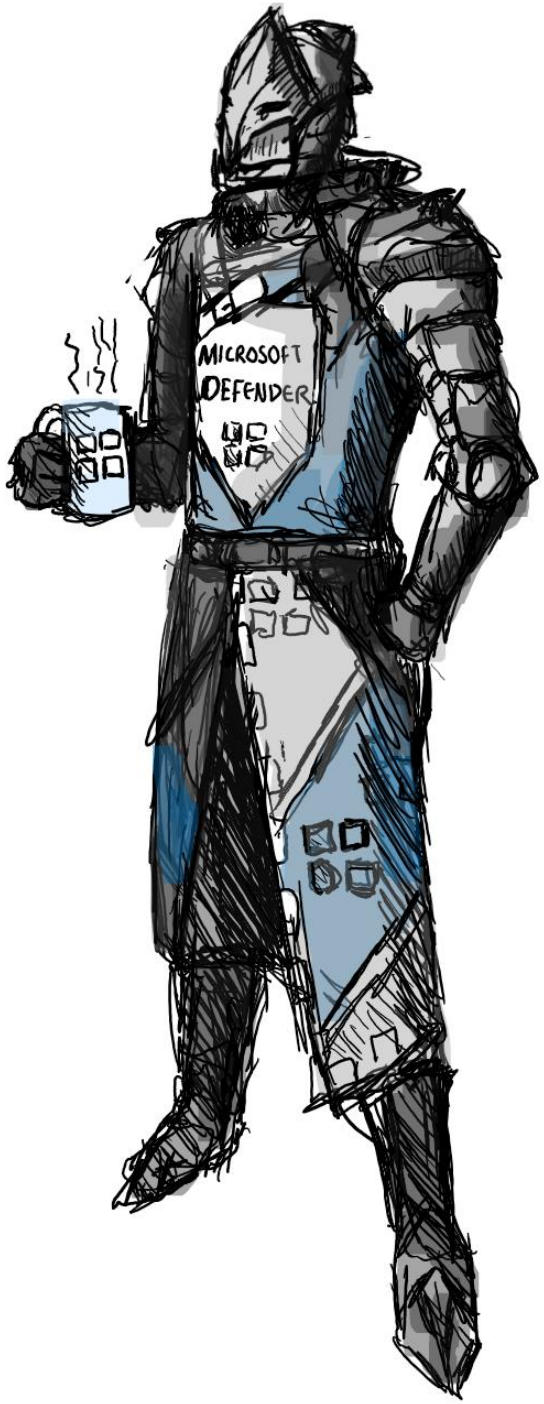
/turnvirtual

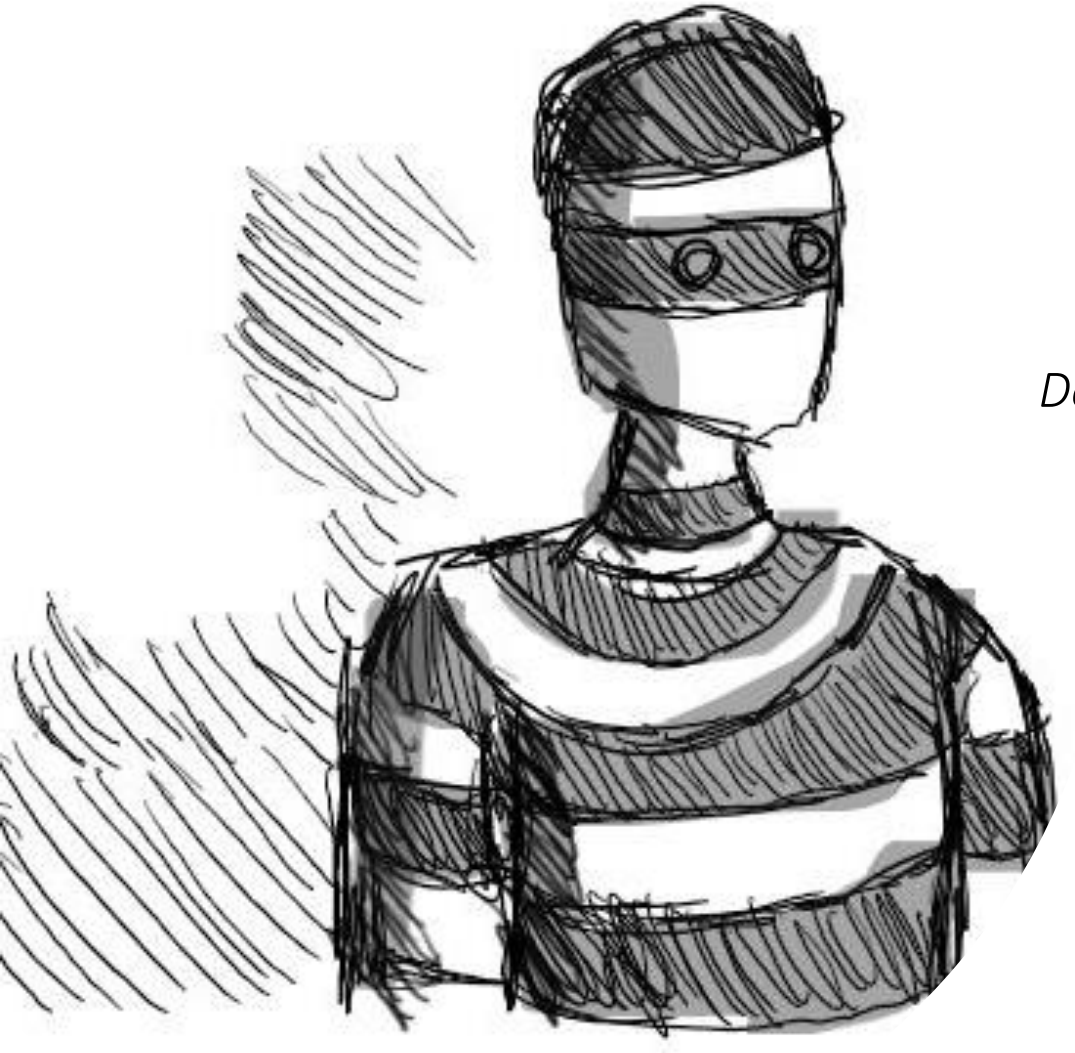
Cloud Solution Architect
(Security, Compliance and Identity)

# Break 1

## Please return at 10:40am BST

**(British Summer Time)**





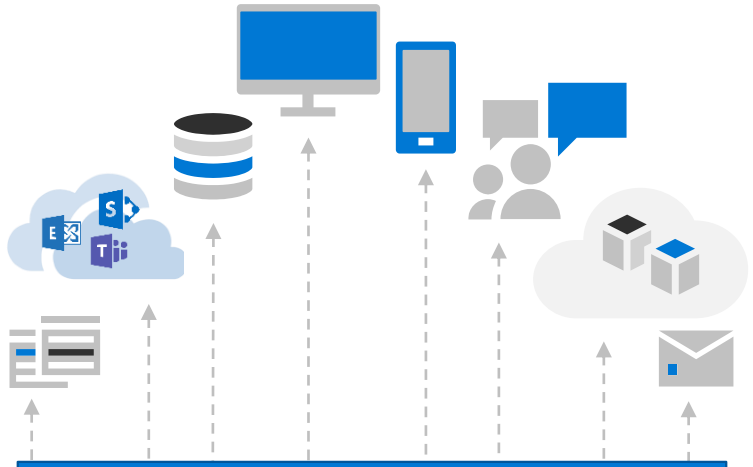
*Deeper into:* # Insider Risk Management

Graham Hosking
Security and Compliance Technical Specialist

*Illustrations by Becky Cholerton*

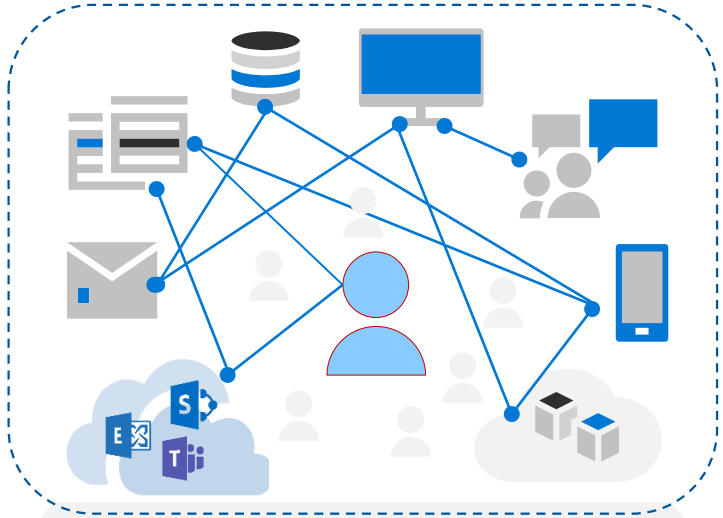
Microsoft

# Addressing risks to your information



## Data Loss Prevention

Enforcing data loss prevention rules across endpoints



## Insider Risk Management

Identify and mitigate risks by a user

| | Data Loss Prevention | Insider Risk Management |
|---|---|---|
| Pivot | Content | User |
| Risk identification | Transactional | Correlated |
| Mitigation of risk | Rule enforcement / User Education | Collaborate across security, HR, legal |
| Examples | • **Block printing** of Word documents with Credit Cards,<br>• **Audit copying** PDF files with label "Confidential" to USB,<br>• **Warn w/ Override** uploading of Office files with label "Sensitive" to Cloud | • Identify **departing employees who are** taking sensitive documents upon departure<br>• Identify **creative insider threat** by correlating activities (collection> obfuscation>exfiltration)<br>• Identify the **vigilant insider threat** involved in careful low-and-slow leak over days |

# Protect against data exfiltration and insider risk

## Insider risk management

**Signals**

**Devices**

Microsoft Defender ATP
- Print
- Copy
- Security signals
- Etc.

**Microsoft 365**

Data loss prevention
Sharing
Download
Etc.

**Human Resources events**

Departures
Retirements
Etc.

**Microsoft Information Protection**

Offensive language
Custom trainable ML classifiers
Etc.

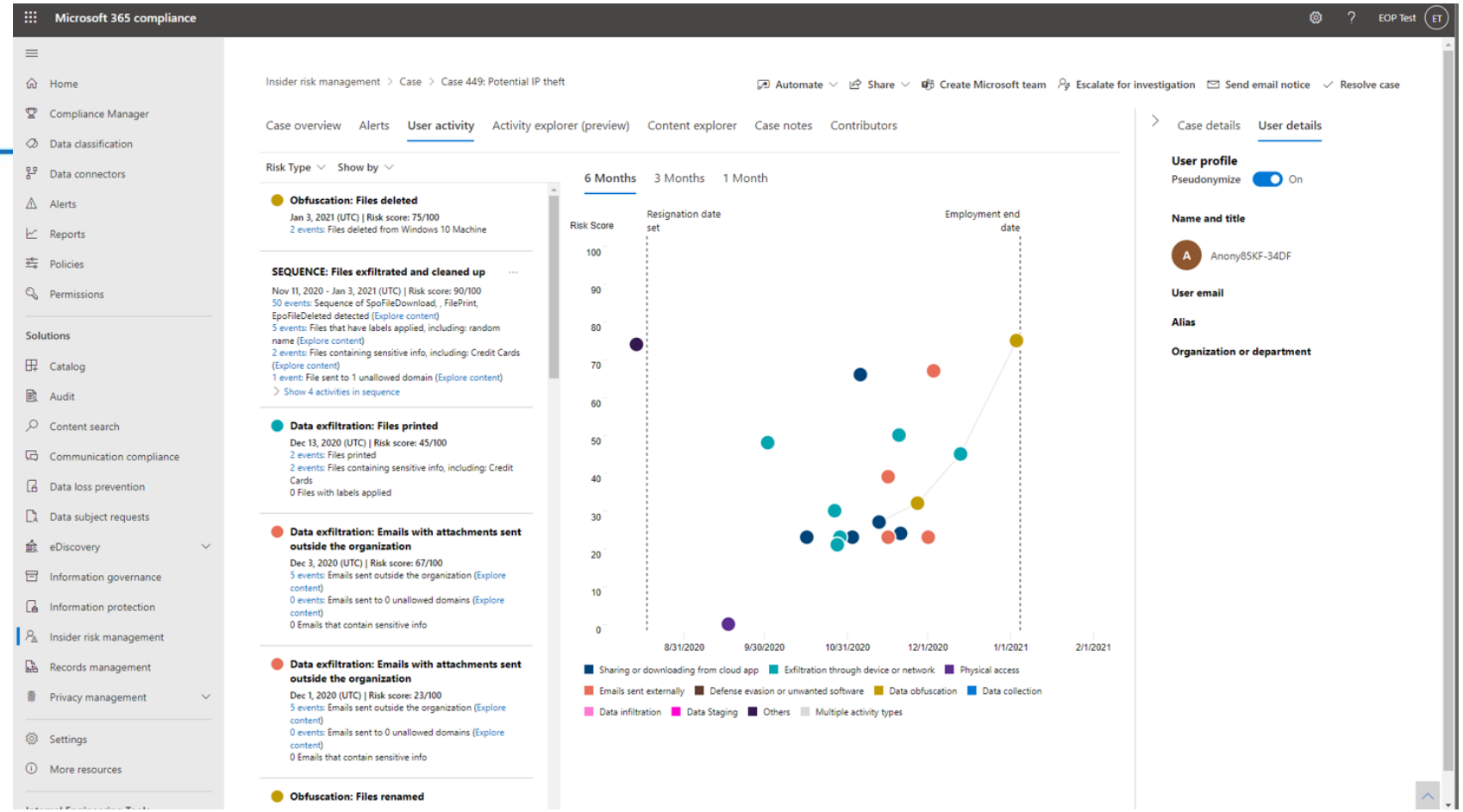
**Other data sources**

**Machine learning**

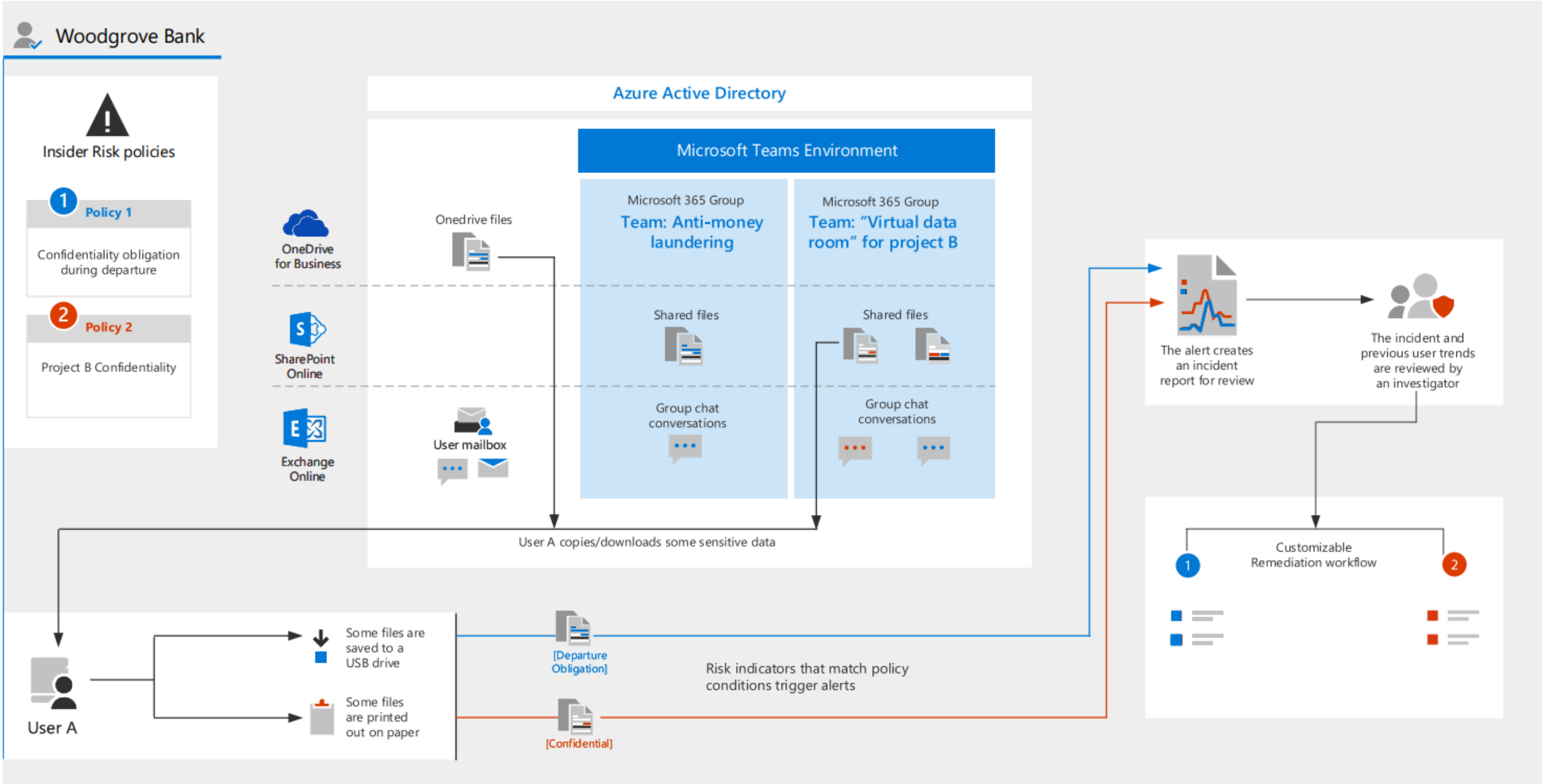
Reasoning across indicators over time

**Risk management**

Alerts
Cases
Investigations
Actions




For a video walkthrough of insider risk management capabilities, see aka.ms/insiderriskguide.


Woodgrove Bank
Insider Risk policies
1
Policy 1
Confidentiality obligation during departure
2
Policy 2
Project B Confidentiality
Azure Active Directory
Microsoft Teams Environment
Microsoft 365 Group
Team: Anti-money laundering
Microsoft 365 Group
Team: "Virtual data room" for project B
OneDrive for Business
Onedrive files
SharePoint Online
Shared files
Shared files
Exchange Online
User mailbox
Group chat conversations
Group chat conversations
User A copies/downloads some sensitive data
The alert creates an incident report for review
The incident and previous user trends are reviewed by an investigator
Customizable Remediation workflow
1
2
User A
Some files are saved to a USB drive
Some files are printed out on paper
[Departure Obligation]
[Confidential]
Risk indicators that match policy conditions trigger alerts

# Steps to Turn on:

Order of switch on:

License dependent :

Assign to each user – Insider Risk Mgmt

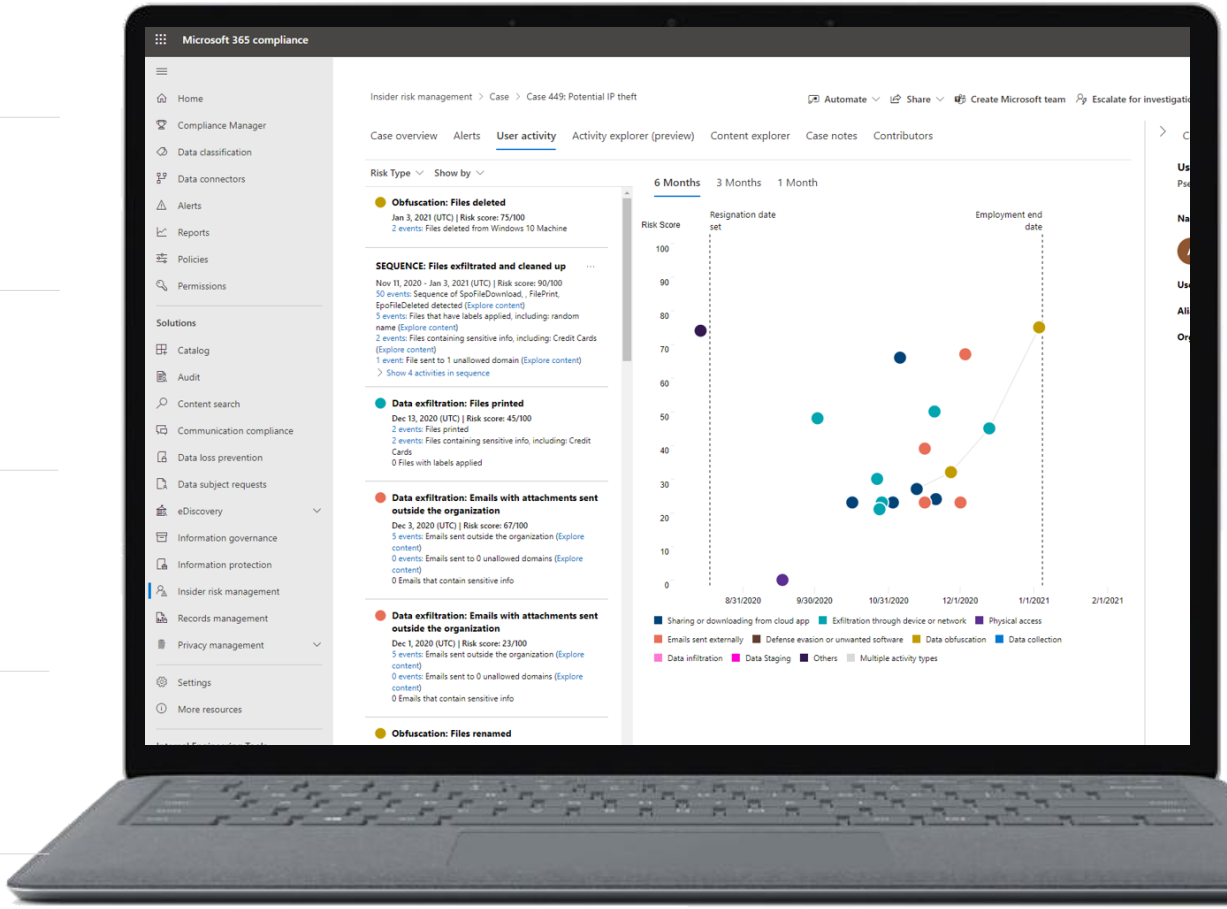
Enable permissions to role assignment

Enable audit log

Enable/evaluate insider risk analytics

DLP Policy – reuse correlated signals

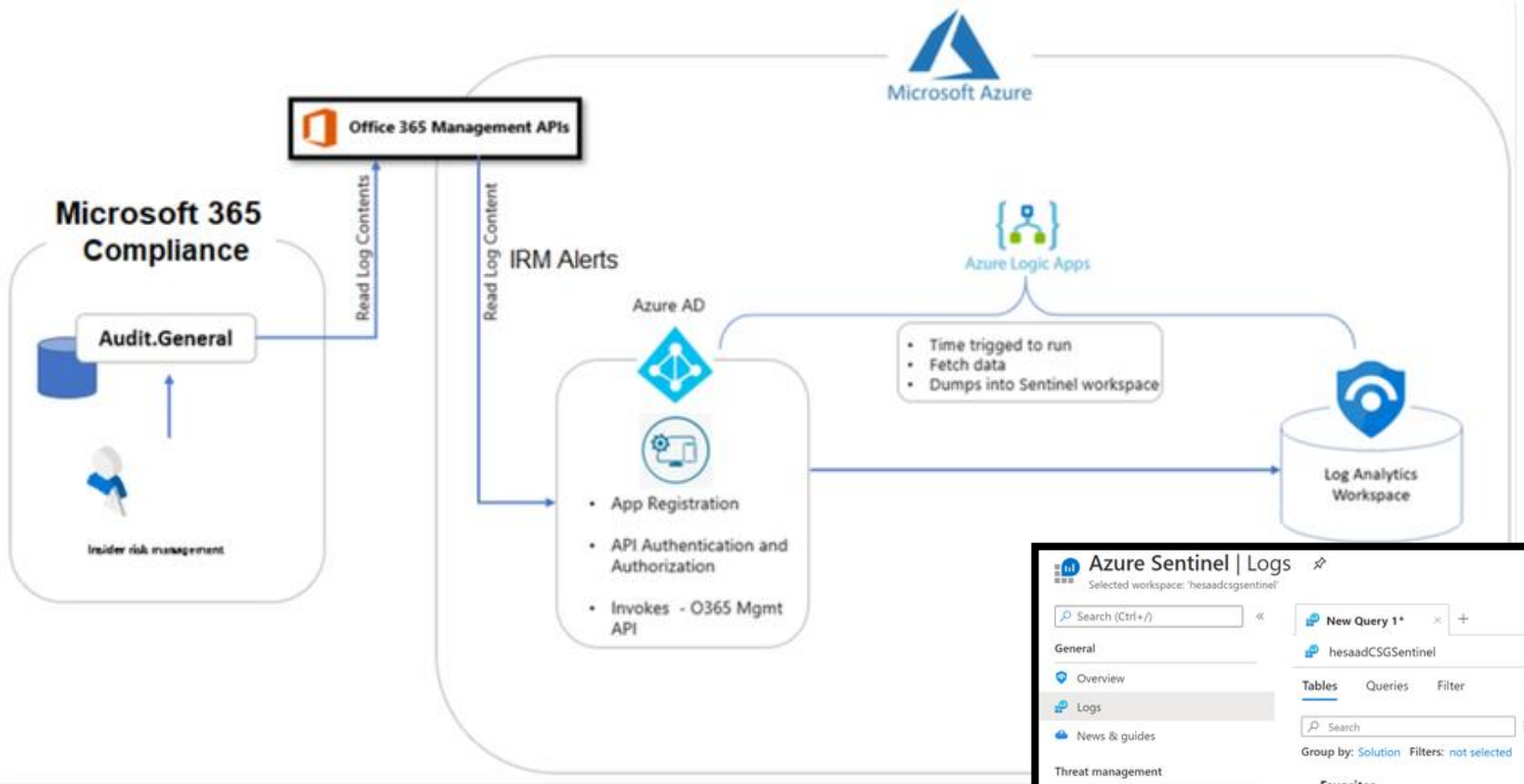
Indicators – Endpoint / HR / MIP Labels / Etc

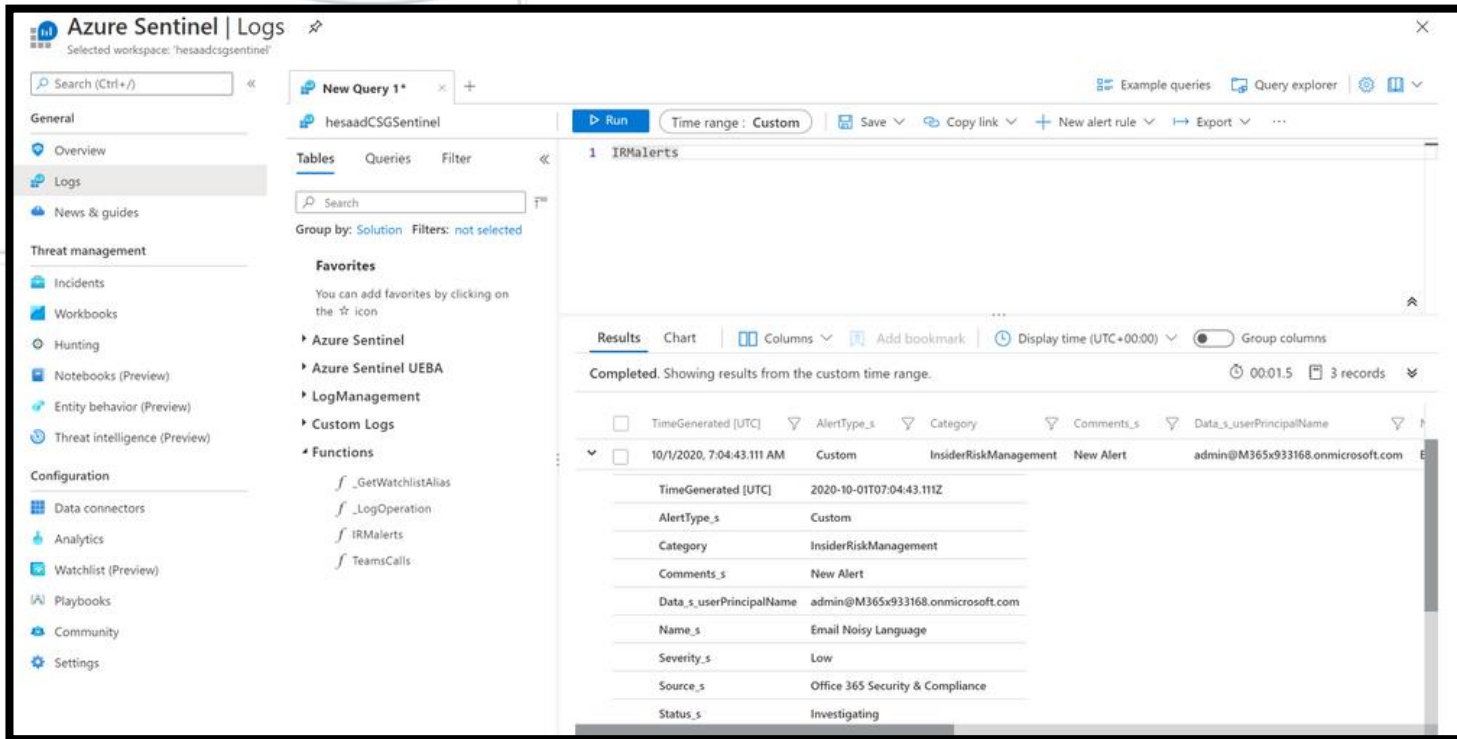


# DEMO

Let’s get stuck in!
Insider Risk Management

# Aggregating Insider Risk Management Information via Azure Sentinel



# Go to Action

Start using Insider Risk Management today

http://aka.ms/insiderriskmanagement

Aggregating IRM into Azure Sentinel
https://techcommunity.microsoft.com/t5/azure-sentinel/aggregating-insider-risk-management-information-via-azure/ba-p/1743211

Interactive guide on Insider Risk Management

https://insider-risk-management.azureedge.net/

Watch the latest shows on YouTube
http://aka.ms/Insiderriskoverview

Compliance Manager/Score
https://youtu.be/ZFIrXaGvWVs




# Information Protection with MCAS

Microsoft

Microsoft Cloud App Security

# Information Protection

## Protecting sensitive information—wherever it lives or travels

**64%**

of organizations report that employees externally share PII and other sensitive business data without encryption.[1]

**34%**

of attacks involve internal actors and 15% are caused by misuse by authorized users such as accidentally leaking sensitive data.[2]

**68%**

of data theft incidents could be prevented with data loss prevention.[3]

# Microsoft Cloud App Security (Cloud Access Security Broker)

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

## Security Operations

- Azure Sentinel (SIEM+SOAR)
- Classic SIEM
- Microsoft 365 Defender

# Microsoft MCAS Architecture (High-Level)

May 2021 v1

## Design & Deployment Guidance

1. Technical Documentation
2. MCAS Ninja Training
3. Top 20 CASB Use Cases
4. MCAS Explainer Series (15mins)
5. aka.ms/MCASBestPractices

## Shadow IT Discovery & Control

### SaaS App Discovery

Discover SaaS apps across the enterprise

Dashboards & reporting on usage & risk

### App Discovery Data Sources

- Microsoft Defender for Endpoint
- Log Collector (Firewall/Proxy)
- REST API
- 3rd Party Secure Web Gateway

### App Risk Scoring

Rates risk for discovered SaaS apps based on regulatory certification, industry standards, and best practices

### Block Unsanctioned Apps via…

- Microsoft Defender for Endpoint
- Firewall Block Script
- 3rd Party Secure Web Gateway

## Secure Access

### Session Monitoring & Control

Identity Provider Integration

Block Activities (Real-Time)

Device State

MDM Signals: Microsoft Endpoint Manager

On-Prem Apps: Azure AD App Proxy, *Beyond User VPN*

### Adaptive Access

Step Up Auth

Outdated Browser/OS

## Security Posture Management

### Security Config Assessments

Multi-cloud security posture + recommended mitigations

Azure Security Center

### Identity Security Posture

Detections & contextual data on known exploitable components & misconfigurations, w/ relevant paths for remediation

Microsoft Defender for Identity

## Threat Protection

### Anomaly Activity Detection

Scans user activity evaluating 90+ risk indicators and factors with machine learning policies

### Malware Detection

Scans connected SaaS apps for malicious files using Microsoft Threat Intelligence and file sandboxing

### Manage OAuth Apps

Visibility and control over extensive attack surface in OAuth apps

## Information Protection

### Files

Visibility to file activity and perform file tasks in connected apps.

### Content Inspection

- Built-In DLP
- Data Classification Service

### Data Loss Prevention Integration

- Microsoft Information Protection
- External DLP Providers

## User & Entity Behavioral Analytics

Detections for anomalous activity across connected SaaS apps, Azure Active Directory and Windows Server Active Directory including compromised users, insider threats, data exfiltration, ransomware activity, etc.

- Windows Server Active Directory
- Azure Active Directory Identity Protection
- Connected SaaS Apps

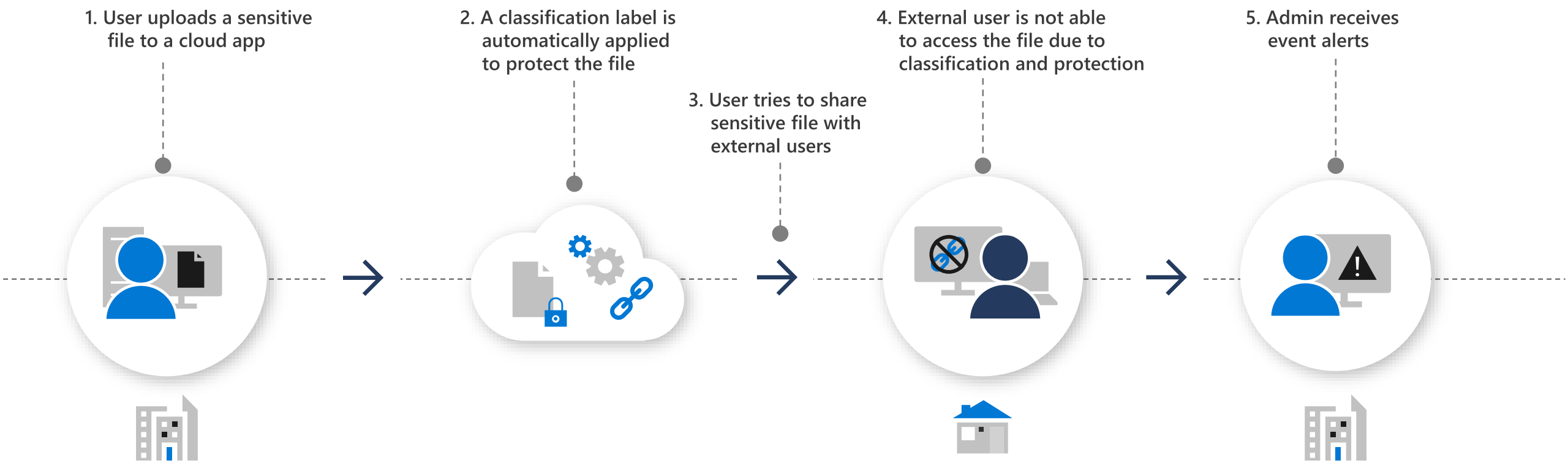
**Discover**

**Manage + Control**

**Investigate + Govern**

**Note**: Product logos indicate integration points

# Lifecycle of protecting sensitive files in the cloud using MCAS



# Which Portal?

| Name | Portal | Colloquial Names | What can you access? (Non-Exhaustive List) |
|---|---|---|---|
| Microsoft 365 Compliance Center | Compliance.microsoft.com | Compliance Center, Compliance Portal | Sensitivity Labels |
| | | | Custom and Built-in Information Types |
| | | | Test Custom Information Types |
| | | | Trainable Classifiers |
| | | | Content Explorer |
| | | | Activity Explorer |
| | | | Endpoint DLP |
| Microsoft Cloud App Security | Portal.cloudappsecurity.com | MCAS, Microsoft CAS, Microsoft CASB | File Policies |
| | | | Threat Detection Policies |
| | | | Information Protection Policies |
| | | | Cloud Discovery Policies |

# MCAS Demo

# MCAS Blogs and Training

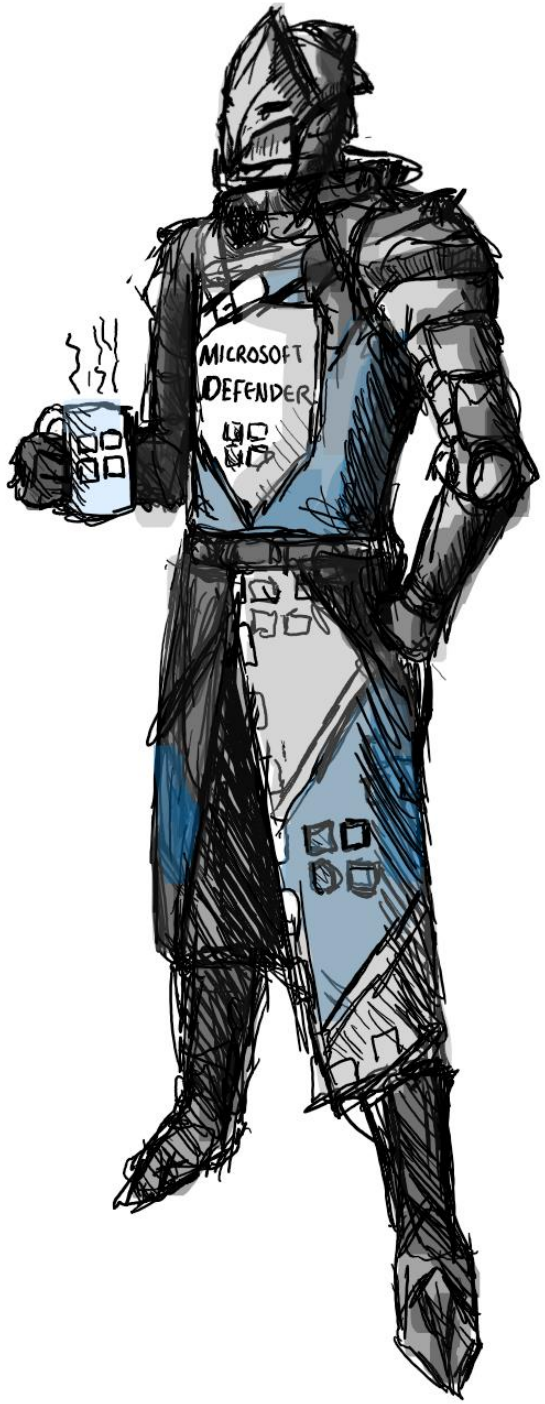
Follow the Microsoft Cloud App Security Ninja blog and learn about Ninja Training.
Go deeper with these interactive guides:

- Discover and manage cloud app usage with Microsoft Cloud App Security
- Protect and control information with Microsoft Cloud App Security
- Detect threats and manage alerts with Microsoft Cloud App Security
- Automate alerts management with Microsoft Power Automate and Cloud App Security

# Break 2

## Please return at 11:45am BST

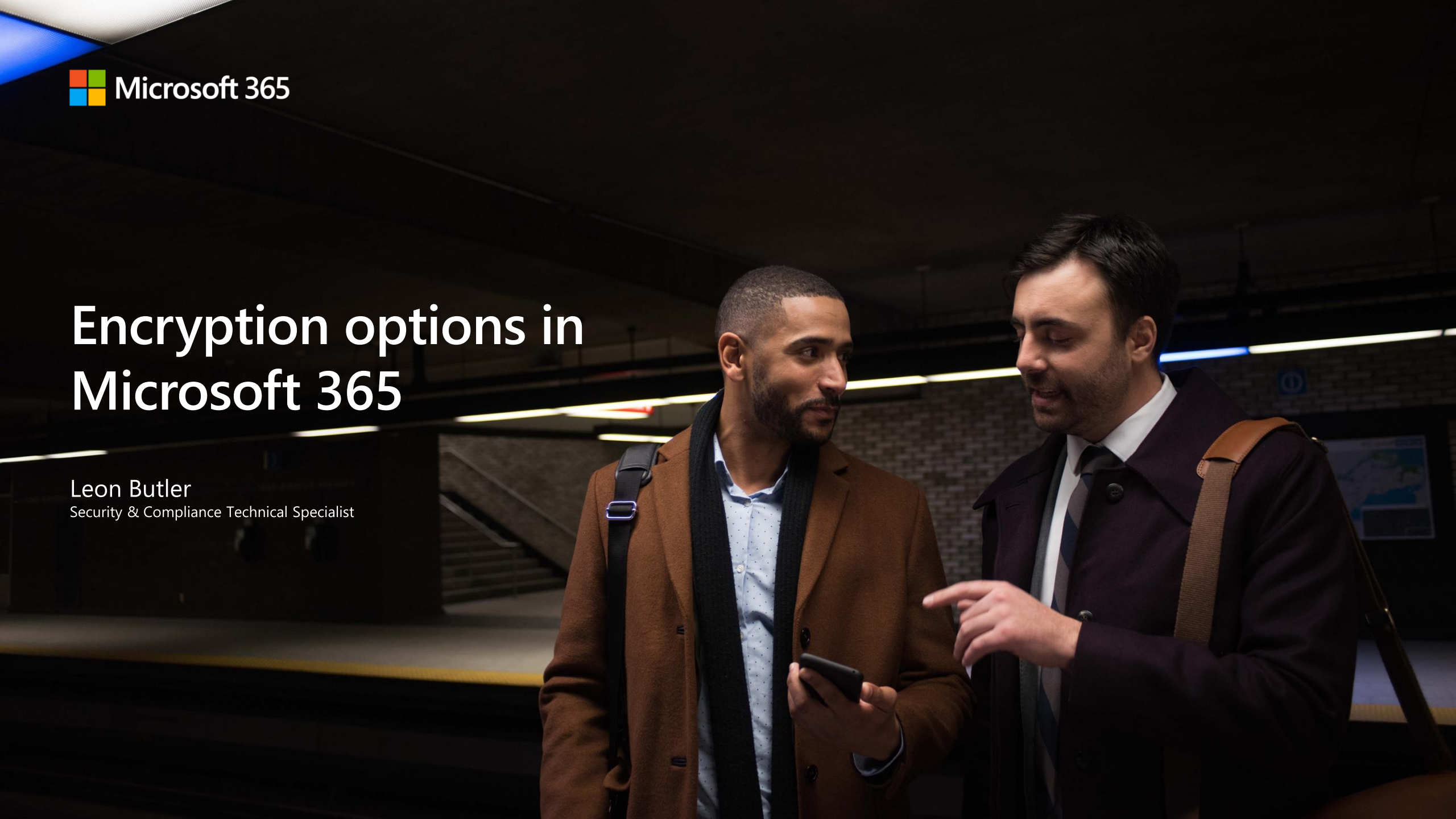
**(British Summer Time)**



Microsoft 365

# Encryption options in Microsoft 365

Leon Butler
Security & Compliance Technical Specialist



# Shared responsibility model

## Customer management of risk

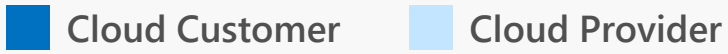
Data Classification and data accountability

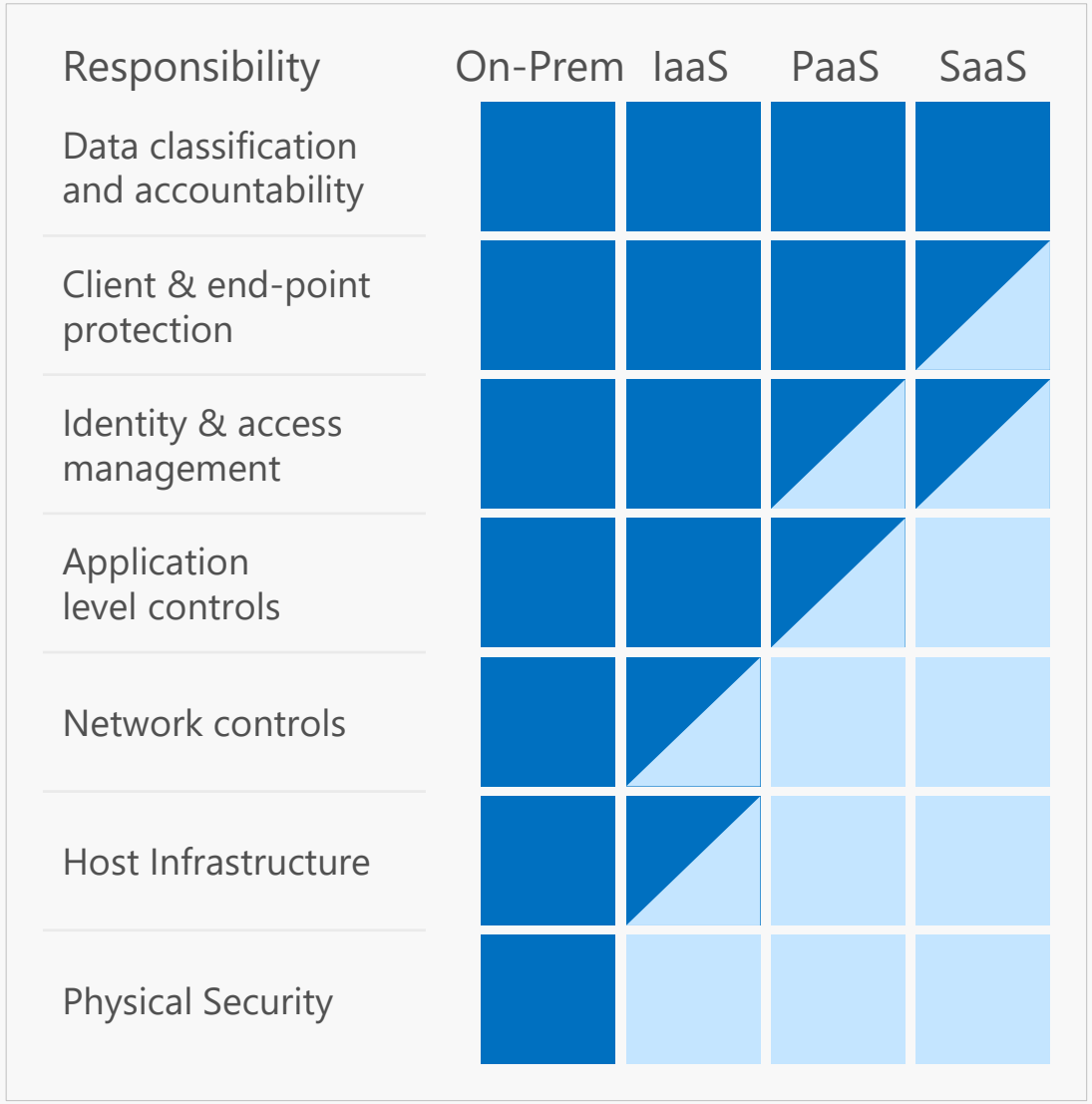
## Shared management of risk

Identity & access management | End Point Devices

## Provider management of risk

Physical | Networking



# Shared responsibility model

NIST 800-53


**Access to production environment**

Implement access controls that prevent standing access to production environment or customer data

**Protect data**

Encrypt data at rest and in transit using industry standard cryptography (BitLocker, Service Encryption, TLS, etc.)

**Personnel control**

Strict screening for employees, vendors, and contractors, and security and privacy training throughout onboarding process

**Access to production environment**

Set up access control policy and SOP, leverage Customer Lockbox and identity management

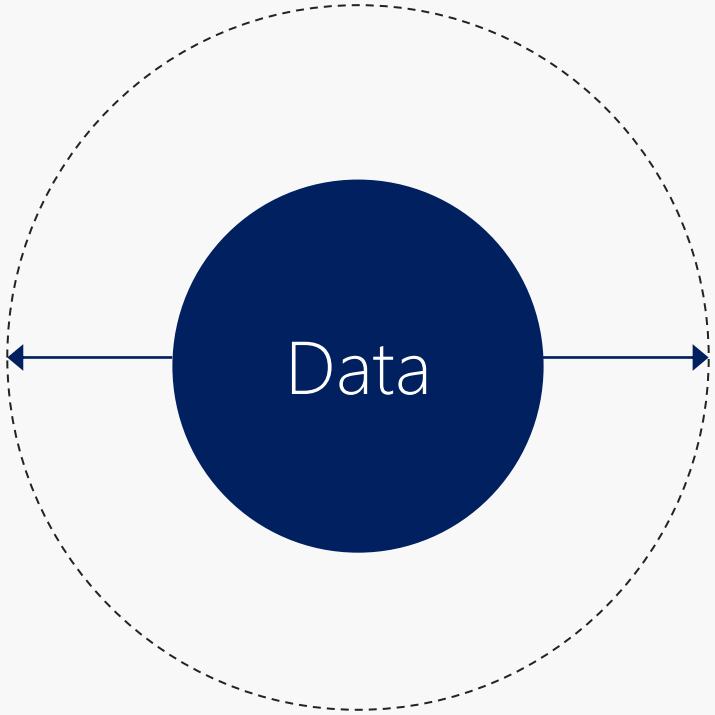
**Protect data**

Encrypt data based on compliance obligations

**Personnel control**

Allocate enough resources to implement an organization-wide privacy program

# Encryption




Encrypt data at rest and in transit

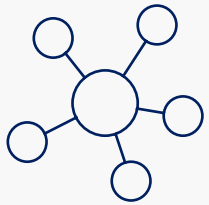
Apply multiple layers of encryption

**Make data unreadable to unauthorized parties**

# Encryption options in Microsoft 365

## Data in-transit

### Network



TLS

### Content

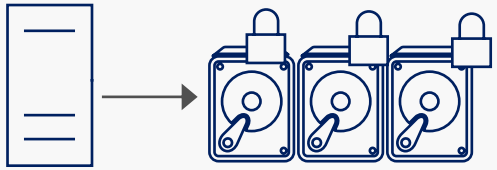
Emails,
Documents

Office 365
Message Encryption

Microsoft
Information Protection

## Data at-rest

### Hardware



Windows
Server

Disk

BitLocker

### Application

Mailboxes

Files

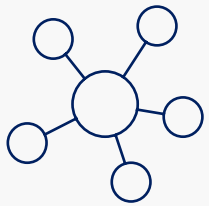
Chat

Service Encryption

# Encryption key management options in Microsoft 365

## Data in-transit

### Network



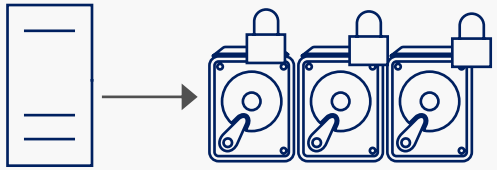
### Content

Emails,
Documents

Bring Your Own Key with MIP
Double Key Encrypt. with MIP
~~(Hold Your Own Key with AIP)~~

## Data at-rest

### Hardware



Windows Server

Disk

### Application

Mailboxes

Files

Chat

Customer key

# Data in-transit

Microsoft Information Protection (MIP)
Office 365 message encryption (OME)

# How do MIP and OME help with compliance?

- Microsoft Information Protection and Office 365 Message Encryption provide **persistent encryption** on documents and emails

- Access to the encrypted document/email is granted based on the user's identity
  - This allows the Admin to enable gated access to sensitive data
  - This allows the Admin to limit access to sensitive data

- Access to the encrypted document/email can also be monitored and revoked
  - This allows the Admin to audit who has access to the document
  - This allows the Admin to audit who has *previously accessed* the document
  - This allows the Admin to control future access to the document

# The decision around keys is important

MIP and OME can act as the means to compliance

Access to your keys == Access to your data

**Therefore,**
Decisions made around key management become critical to compliance.

# Key options in Microsoft Information Protection

There are 3 keys options……

1. Microsoft-managed keys
2. Bring Your Own Key (BYOK)
3. Double Key Encryption (DKE)

~~Hold Your Own Key (HYOK)~~

# Microsoft-managed keys

# What are Microsoft-managed keys?

When the tenant private key is stored and managed by the Microsoft Information Protection service (Microsoft), the key type is referred to as *Microsoft-managed key*.

# Why use Microsoft-managed keys?

## Simple to manage

- No additional subscriptions or configurations needed
- No planning required for capacity, performance, or scale

Handled by Microsoft

## Readily available

- It’s available by default with every tenant that uses AIP
- Great for testing MIP, or for customers that are “pure” Office 365

## Sufficient

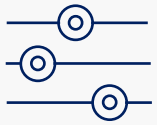
- Security and controls put in place for the keys are adequate for most customers
- Most smaller customers don’t need more than this

# Bring Your Own Key (BYOK)

# What is BYOK?

When you use Azure Key Vault, you can import or generate keys in hardware security modules (HSMs) that never leave the HSM boundary. This scenario is often referred to as *bring your own key*, or BYOK.

# Why use BYOK?



## Better key control

- Show how you have “possession” and “control” over your data via key control

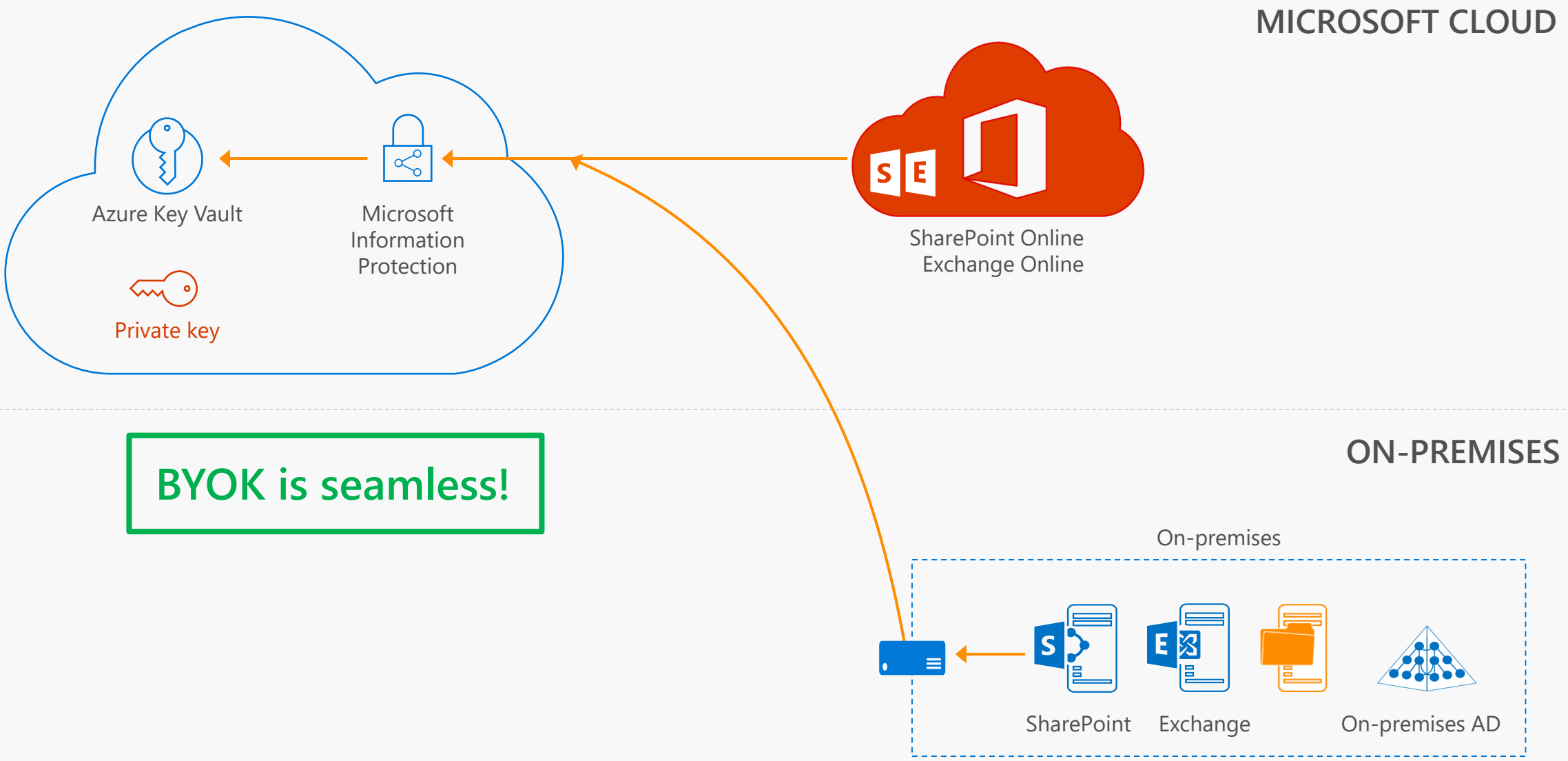
## Compliance requirements

- Data residency requirements and/or crypto regulations make Microsoft-managed keys insufficient for the tenant
- For example: verticals like insurance, health can benefit from use of BYOK

## Organization policies

- Large organizations already have hardware, software, and processes in place to manage their own keys – typically HSM-based. They would like to extend this to the cloud as well

# BYOK topology



# Important points to note

1. Use a vault that is different from the vault used with the customer key
2. Pick a vault location close to your tenant geo location – for performance and latency reasons
3. Follow instructions called out in the documentation: https://docs.microsoft.com/en-us/information-protection/plan-design/plan-implement-tenant-key

**https://channel9.msdn.com/Events/Ignite/Microsoft-Ignite-Orlando-2017/BRK2000**

- 1-hour session on how to configure BYOK
- More drilldown into the protection scenarios
- Understand the implication of each key option on how AIP behaves

# Double Key Encryption (DKE)

# What is DKE?

Uses two keys together to access protected content. Microsoft stores one key in Microsoft Azure, and you hold the other key. You maintain full control of one of your keys using the Double Key Encryption service.

# Why use DKE?

## Secret content

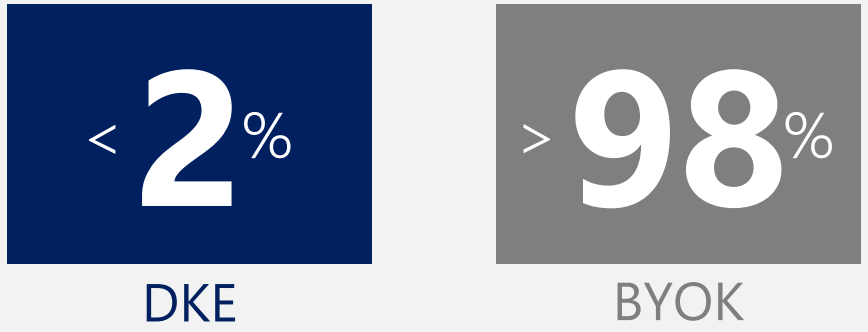
- Certain categories of data cannot be stored on the public cloud. The sensitive nature of the data means that it needs to be stored and protected on-premises

## Compliance requirements

- BYOK doesn't meet the security and audit requirements for certain types of data

## BYOK and DKE are not mutually exclusive

DKE-protected data is typically less than 2% of an organization's protected data. The rest are "cloud-friendly" – can be stored and processed by Office 365 and protected by BYOK keys.



# The DKE value proposition and limitations

| Value proposition | Limitations (by design) |
| --- | --- |
| Data must be opaque to cloud services, even if the data is physically stored in the cloud. | No inter-op with Office 365 services (e.g. Office Web Apps). No indexing, search, web views or any type of "reasoning over data" features will work. |
| Data remains encrypted at all times, inaccessible even to Microsoft services. | Exchange Online transport rules (inc. SPAM/Malware), Office 365 DLP and eDiscovery cannot decrypt content to inspect it. |
| External sharing is possible in a tightly controlled manner with known and named partners. The metadata around this sharing and the access logs are not disclosed to anyone (including Microsoft). | Configuration of external sharing (and DKE by extension) cannot be done through the MIP service and the Azure portal. |
| Companies can prove *physical* access and possession of the private key. | |

# Data at-rest

# BitLocker

# What is BitLocker?

- Data at rest encryption at the disk layer
- Integrate with the operating system
- Prevents data compromise from physical disk theft
- Uses the Trusted Platform Module (TPM) for protection
- Uses AES 256-bit keys

# What is the value proposition of BitLocker?

- Data on a lost or stolen disk is not accessible
- Enhances file and system protections
- Renders data on disks that are decommissioned or recycled inaccessible

# Service Encryption

# What is Service Encryption?

- Application layer encryption in Office 365 for data at rest
- Provides strong separation of Windows Server administrators and customer data
- Additional protection against physical data theft
- Provides an option to customers to use Microsoft-managed or Customer-managed keys, and is effective **regardless of who manages encryption keys**

# What is Service Encryption with Microsoft owned keys?

- Microsoft owned root keys
- Office 365 Customer Data that are not encrypted with Customer Key will be encrypted with Microsoft owned keys
  - SharePoint Online – available today
  - Exchange Online – available today
  - Microsoft Teams – available today
- Root keys stored in Azure Key Vault
- Data Encryption Policies (DEPs) will be created per forest

# What is Service Encryption with Customer Key?

Helps meet compliance and regulatory demands

Customer controlled keys

Enables irrevocable data destruction

Independently audited

Data Encryption Policy flexibility in Exchange Online

Allows for feature rich Office 365 experience while still encrypting data in the service

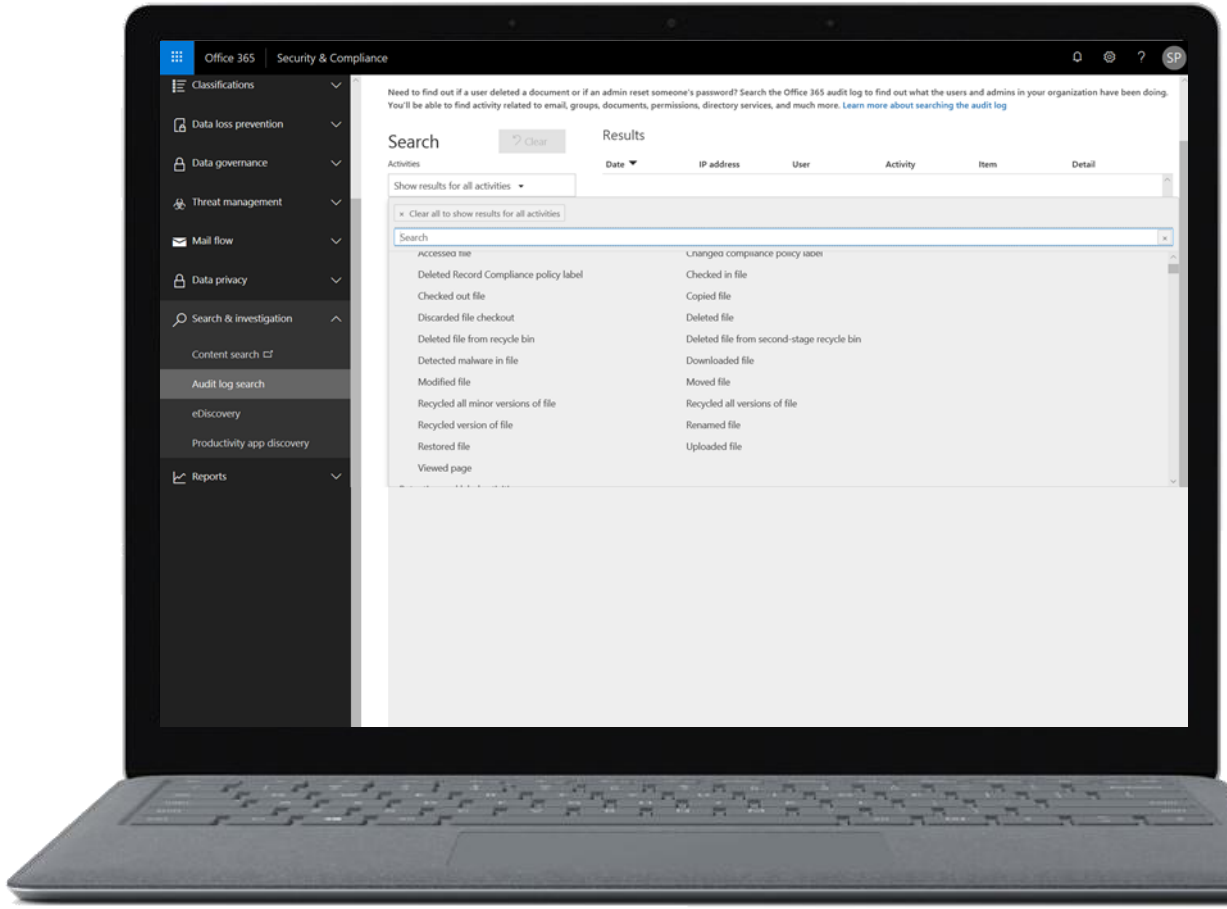
# Advanced Audit for Microsoft 365

Graham Hosking
Security and Compliance Technical Specialist

# Advanced Audit in Microsoft 365

Power your forensic and compliance investigations

- Additional events that are **important for forensic investigations** (e.g. mail items accessed, mail send, user search)
- **Preserve audit logs** for up to a year, with option for 10-year retention add-on
- **High bandwidth access to data** with ~2x the baseline



# Additional events for forensic investigations

## Mail items accessed event

Helps determine scope of messages that may have been compromised by attacker

## Mail send event

Provides insight into either intentional or accidental data leakage

## User search events

Provides insight into searches in Exchange Online or SharePoint online for further data compromise

# Preserving audit log activity

Extending audit log activities beyond 90-days

Average time to detect and contain data breach 208 days

Regulatory obligations indicate audit logs to be retained for longer (e.g. 7-10 years)

- **Audit in M365 90-days**
- **Advanced Audit in Microsoft 365 for 1 year**
- **Advanced Audit with add-on to increase retention for 10-years**

# How Advanced Audit can help

## For your regulatory and legal obligations

- Assess scope of data breach
- Access audit logs to support length of investigation

Forensic investigations

Responding to legal requests

# How Advanced Audit can help

## For your regulatory and legal obligations

- Assess scope of data breach
- Access audit logs to support length of investigation

Forensic investigations

Responding to legal requests

# Fabrikam Hospital data breach – forensic investigation

**HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414,**
Impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity can show there is a low probability the PHI has been compromised

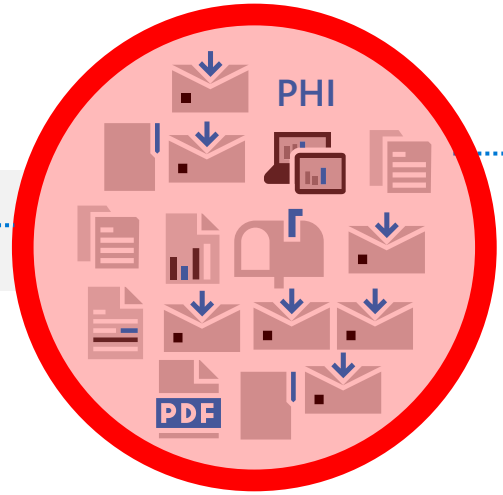
If an attacker gains account access and operates as the user, **the scope of attack can be broad**; and extensive breach must be assumed

**Malicious Attacker**
Phishing attack for account compromise

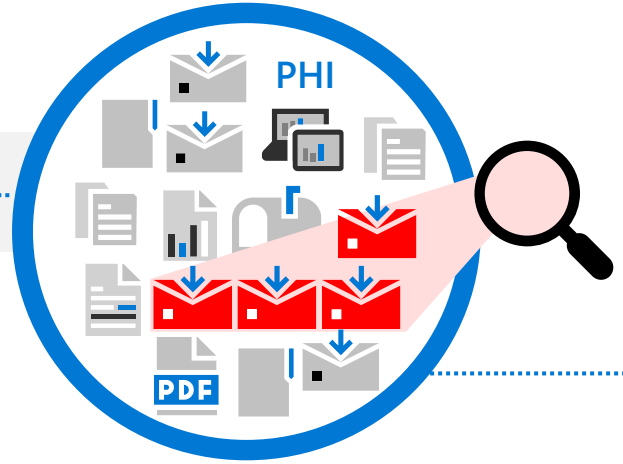
Steals data from email and files

Data breach detected

Regulators seeking information about breach and **defensible proof** that sensitive information was or wasn't exposed




Without tools to scope data breach – presume all data to be breached including PHI




M365 Advanced Audit can provide scope of data compromised in Exchange Online, SharePoint Online and other services

# Audit provides a broad set of user activities for investigations

## User

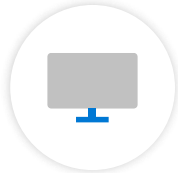
Where did this person login from?

## Email

What emails were read, sent or forwarded?

## Files

Who read or modified confidential documents? Who had access to folders in SharePoint?



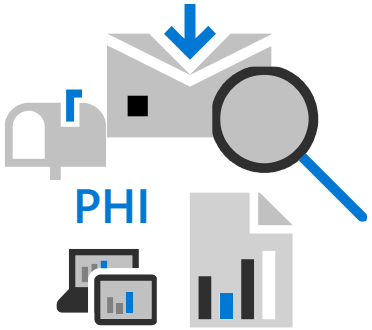
## Searches

What searches were performed in email and SharePoint?

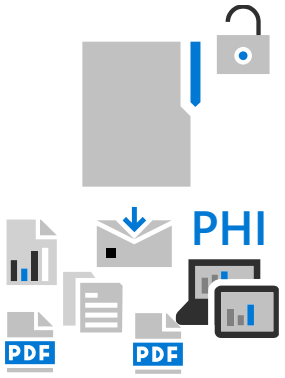
30+ Microsoft Services send user and admin activities to Audit

# Demo – Advanced Audit for Forensic Investigations

An attacker gains access to a user account credentials using a targeted phishing email

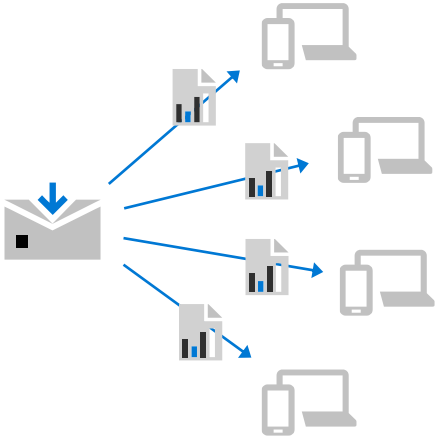



Searches email and SharePoint for PHI data




Accesses SharePoint files containing PHI data

Reads user email



Exfiltrates data by sending email out from that account

➔ *How can Advanced Audit help to uncover what the attacker did?*

# How Advanced Audit can help

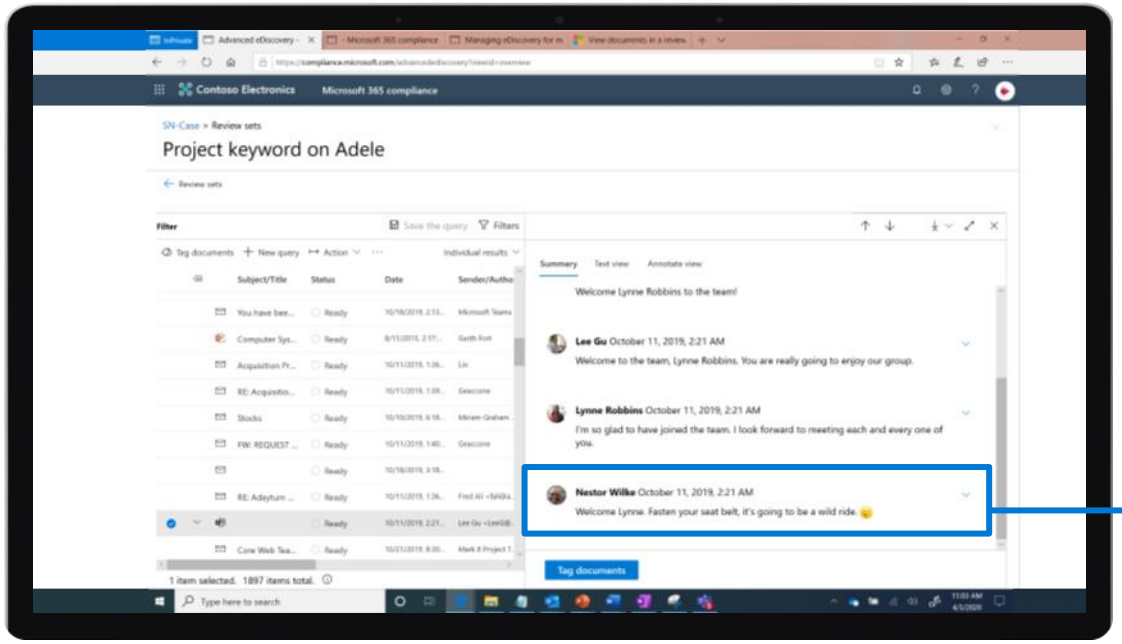
## For your regulatory and legal obligations

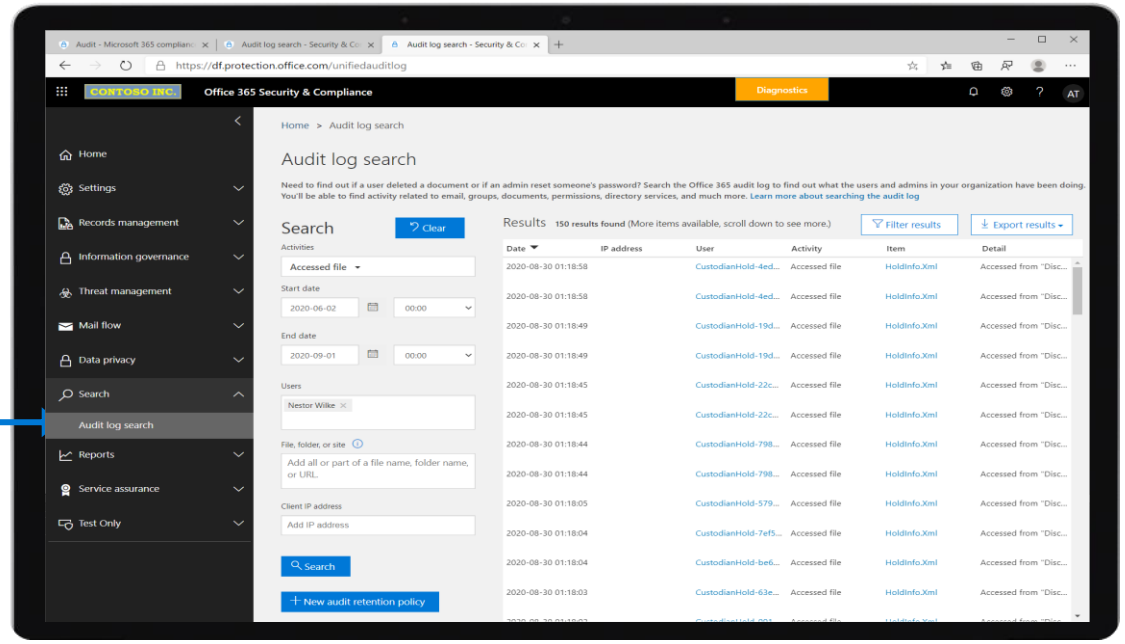
- Assess scope of data breach
- Access audit logs to support length of investigation

Forensic investigations

Responding to legal requests

# Contoso responding to legal request needs historical data that hasn't been put on hold




Long running investigation

Audit provides additional user activity going back a year or optionally to 10 years

# Steps to Turn on:

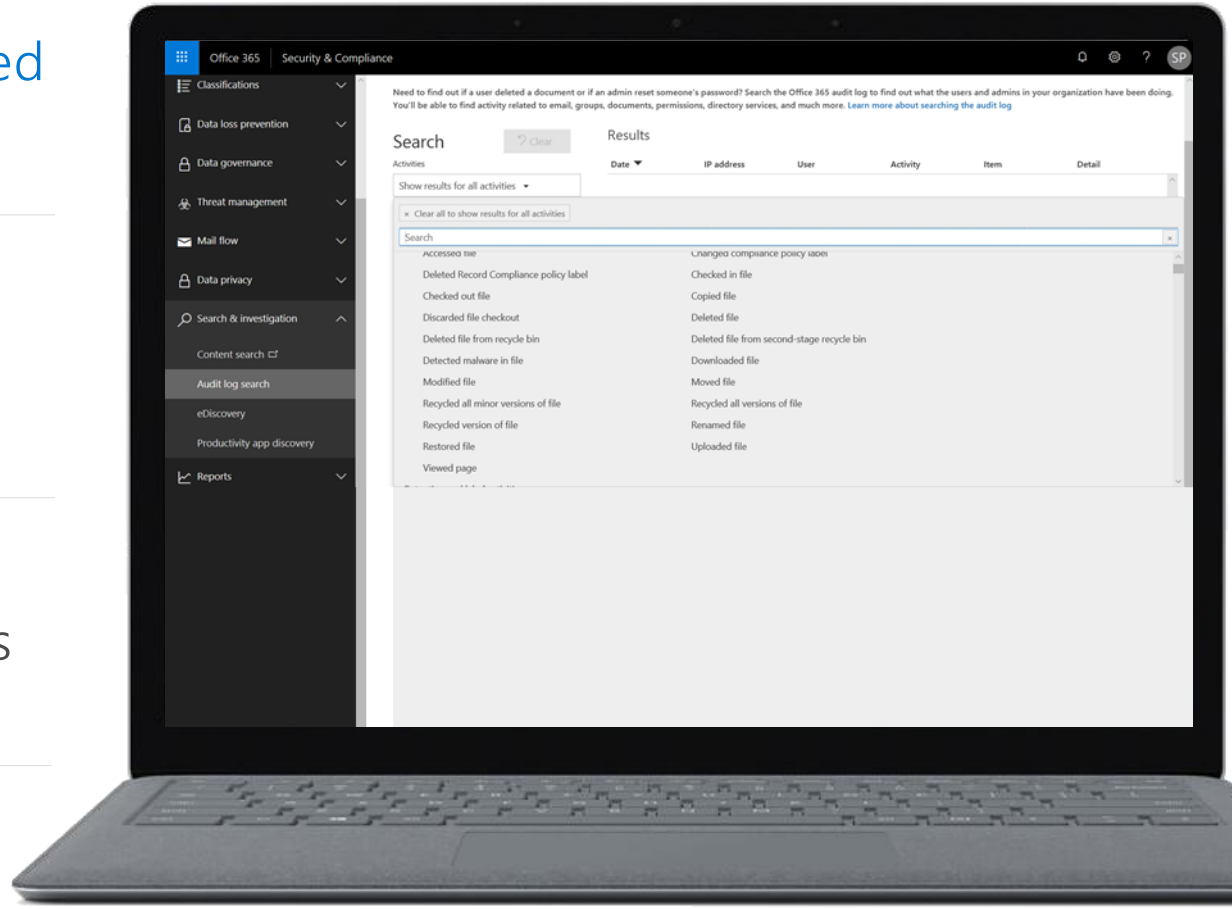
Order of switch on

License dependent : Assign to each user – Advanced Audit

Enable crucial events: Enable for each user

Setup retention policies: Meeting org requirements

Search the log: Four Specific activities….



# DEMO

Let's look inside the audit logs...

# Examples in the log

## Accessed Mailbox Items

**Users**
bert@crossbar.cc

**Activity**
Accessed mailbox items

**Item**

**Detail**
Mail Items Accessed

**Id**
"1b1d1558-143c-4547-931a-b9ecad38a83c"

**Logon Type**
0

**Mailbox Guid**
"f5330d62-6203-4465-bbb9-bcf9dac377bc"

**Mailbox Owner UPN**
"bert@crossbar.cc"

**Mailbox Owner Sid**
"S-1-5-21-2492831211-3977660457-2310828387-25013836"

**Logon User Sid**
"S-1-5-21-2492831211-3977660457-2310828387-25013836"

**Record Type**
50

**External Access**
false

**Client Info String**
"Client=OWA;Action=ViaProxy"

**CreationTime**
2021-05-25T15:23:55

**Id**
1b1d1558-143c-4547-931a-b9ecad38a83c

## Email Search

**Users**
bert@crossbar.cc

**Activity**
Performed email search

**Item**
Email

**Detail**

**Id**
"05e6766f-ff75-4d84-a785-944d9c820d2b"

**Record Type**
101

**Query Source**
"Email"

**Query Text**
"Project McKinley"

**Client User Agent**
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.66"

**QuerySource**
Email

## Sent Message

| User | Activity |
|---|---|
| DebraB@crossbar.cc | Sent message |
| DebraB@crossbar.cc | Sent message |
| alland@crossbar.cc | Sent message |
| alland@crossbar.cc | Sent message |
| alland@crossbar.cc | Sent message |
| alland@crossbar.cc | Sent message |
| alland@crossbar.cc | Sent message |
| alland@crossbar.cc | Sent message |

**LogonUserSid**
S-1-5-21-2492831211-3977660457-2310828387-24142932

**MailboxGuid**
8e451e2a-9196-482f-a9d3-2bc18ab03f58

**MailboxOwnerSid**
S-1-5-21-2492831211-3977660457-2310828387-24142932

**MailboxOwnerUPN**
DebraB@crossbar.cc

**OrganizationName**
M365x764095.onmicrosoft.com

**OriginatingServer**
DB9PR10MB4587 (15.20.4173.020)

**SessionId**
3a3fcf3a-9acd-4f5c-9514-d4ae403f01a2

**Item**


```
"Attachments": "020293.csv.pfile (33884b); 020298.csv.pfile (342
"Id": "Unknown",
"InternetMessageId": "<DB9PR10MB4587ED03C39B751F115246AAC9259@DB
"ParentFolder": {
    "Id": "LgAAAAD08FcHgob7R4jlCNy9UqV+AQA0xnrILoYFQKbb5xdh7oyuA
    "Path": "\\Outbox"
},
"SizeInBytes": 361180,
"Subject": "Bit more"
```

Microsoft

# Get started - Audit

Try thru **E5 trial**

Access thru **Compliance Centre**

**Watch** more https://aka.ms/VideoHub/DiscoverandRespond

**Interactive** Drive-Thu: https://aka.ms/AAcogqe

**Learn more** @aka.ms/AdvancedAudit


Microsoft 365
SharePoint Syntex
Leon Butler
Security & Compliance Technical Specialist

# Modernize content services with Microsoft 365

## What our customers are telling us

Disconnected silos across LOBs & legacy systems

Labor intensive, error prone data entry & interpretation

Managing and applying metadata & taxonomies

Compliance, records & retention management

## Microsoft 365 solves these challenges

Content understanding

Content processing

Content governance

# Project Cortex

Reimagine content and knowledge in Microsoft 365

## Connecting people to knowledge

Tap into shared topics, resources and experts in the context of your work

## Content processing

Intelligently categorize content and automate processes

## Content compliance

Connect and manage content to improve security and compliance

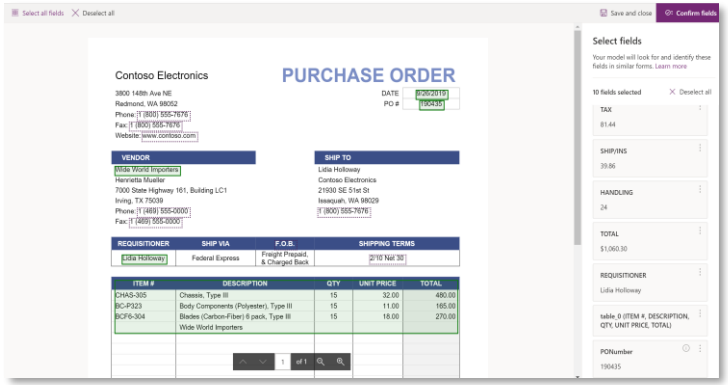
**Microsoft Graph & Microsoft AI**

**Content Services**

# SharePoint Syntex

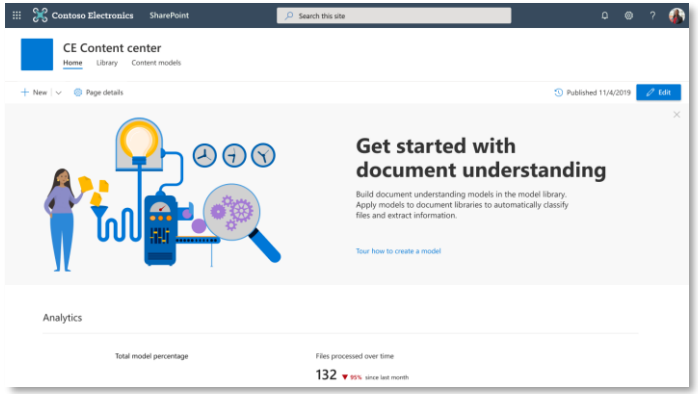
## Content understanding

Create no-code AI models that capture expertise to classify and extract information to automatically apply metadata for knowledge discovery and reuse.



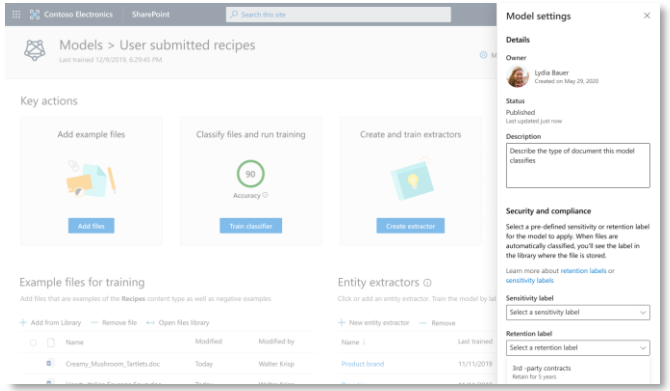

## Content processing

Automate capture, ingestion and categorization of content and streamline content-centric processes using Power Automate.




## Content compliance

Connect and manage content to improve security and governance with integration to Microsoft Information Protection.



# Better together: People + AI

New AI services and capabilities to make it easier to build content understanding and classification apps directly into the content management flow using Microsoft SharePoint Syntex

### Manual

Any content, aided by use of managed terms and content types

### Object detection

Process digital content - photos, scans, receipts, business cards, videos with OCR & text

### Form processing

Capture content types and metadata from purchase orders, applications, other structured documents

### Document understanding

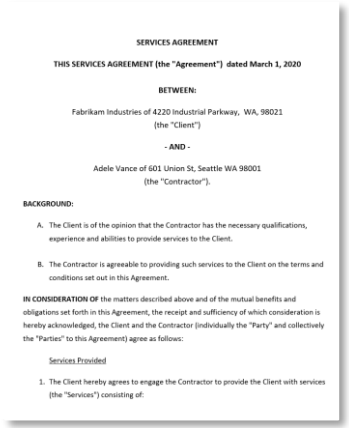
Capture content types and metadata from contracts, resumes, other unstructured documents

**Interactive** → **Pre-built, automated** → **Custom, assisted** → **Custom, compliant**

# Model type based on file format & use case

## Document Understanding

- Created in content center
- Model created in native interface
- Used for unstructured file formats
- Trainable classifier w/ optional extractors
- Can be applied to multiple libraries



SERVICES AGREEMENT

THIS SERVICES AGREEMENT (the "Agreement") dated March 1, 2020

BETWEEN:

Fabrikam Industries of 4220 Industrial Parkway, WA, 98021
(the "Client")

- AND -

Adele Vance of 601 Union St, Seattle WA 98001
(the "Contractor").

BACKGROUND:

A. The Client is of the opinion that the Contractor has the necessary qualifications, experience and abilities to provide services to the Client.

B. The Contractor is agreeable to providing such services to the Client on the terms and conditions set out in this Agreement.

IN CONSIDERATION OF the matters described above and of the mutual benefits and obligations set forth in this Agreement, the receipt and sufficiency of which consideration is hereby acknowledged, the Client and the Contractor (individually the "Party" and collectively the "Parties" to this Agreement) agree as follows:

Services Provided

1. The Client hereby agrees to engage the Contractor to provide the Client with services (the "Services") consisting of:

Train on 5-10 PDF, Office, mail files, including negative examples

## Form Processing

- Created from document library
- Model created in AI Builder
- Used for semi-structured file formats
- Settable classifier
- Restricted to a single library

Contoso Electronics

PURCHASE ORDER

DATE 9/29/2019
PO # 1904574

3800 148th Ave NE
Redmond, WA 98052
Phone: 1 (800) 555-7676
Fax: 1 (800) 555-7676
Website: www.contoso.com

VENDOR
Wide World Importers
Henrietta Mueller
7000 State Highway 161, Building LC1
Irving, TX 75039
Phone: 1 (469) 555-0000
Fax: 1 (469) 555-0000

SHIP TO
Adel Vance
Contoso Electronics
21930 SE 51st St
Issaquah, WA 98029
1 (800) 555-7676

| REQUISITIONER | SHIP VIA | F.O.B. | SHIPPING TERMS |
|---|---|---|---|
| | | | |

| ITEM # | DESCRIPTION | QTY | UNIT PRICE | TOTAL |
|---|---|---|---|---|
| CHAS-511 | Chassis, Type V | 24 | 92.00 | 2,208.00 |
| BC-P503 | Body Components (Polyester), Type V | 25 | 47.00 | 1,175.00 |
| BCF5-502 | Blades (Carbon-Fiber) 5 pack, Type V<br>Wide World Importers | 36 | 33.00 | 1,188.00 |

| | |
|---|---|
| SUBTOTAL | 4,571.00 |
| TAX | 406.82 |
| SHIPPING | 199.11 |
| HANDLING | 24 |
| TOTAL | $5,200.93 |

Comments or Special Instructions
Thank you for your business.

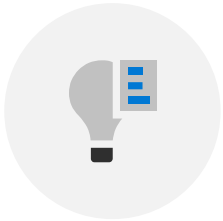
If you have any questions about this purchase order, please contact
Adel Vance, 1 (800) 555-7676, AdelV@Contoso.com

Train on PDF, JPG, PNG format, totaling 50MB/500pp

# Strengthening the metadata foundation

Coherent/consistent across Microsoft 365

Search enrichment find content based on terms



Consistent tagging experience with contextual term suggestions and auto tagging

Improved enterprise content type publishing, discovery, and enforcement with unified taxonomy services

# Demo

# SharePoint Syntex - Compliance integration

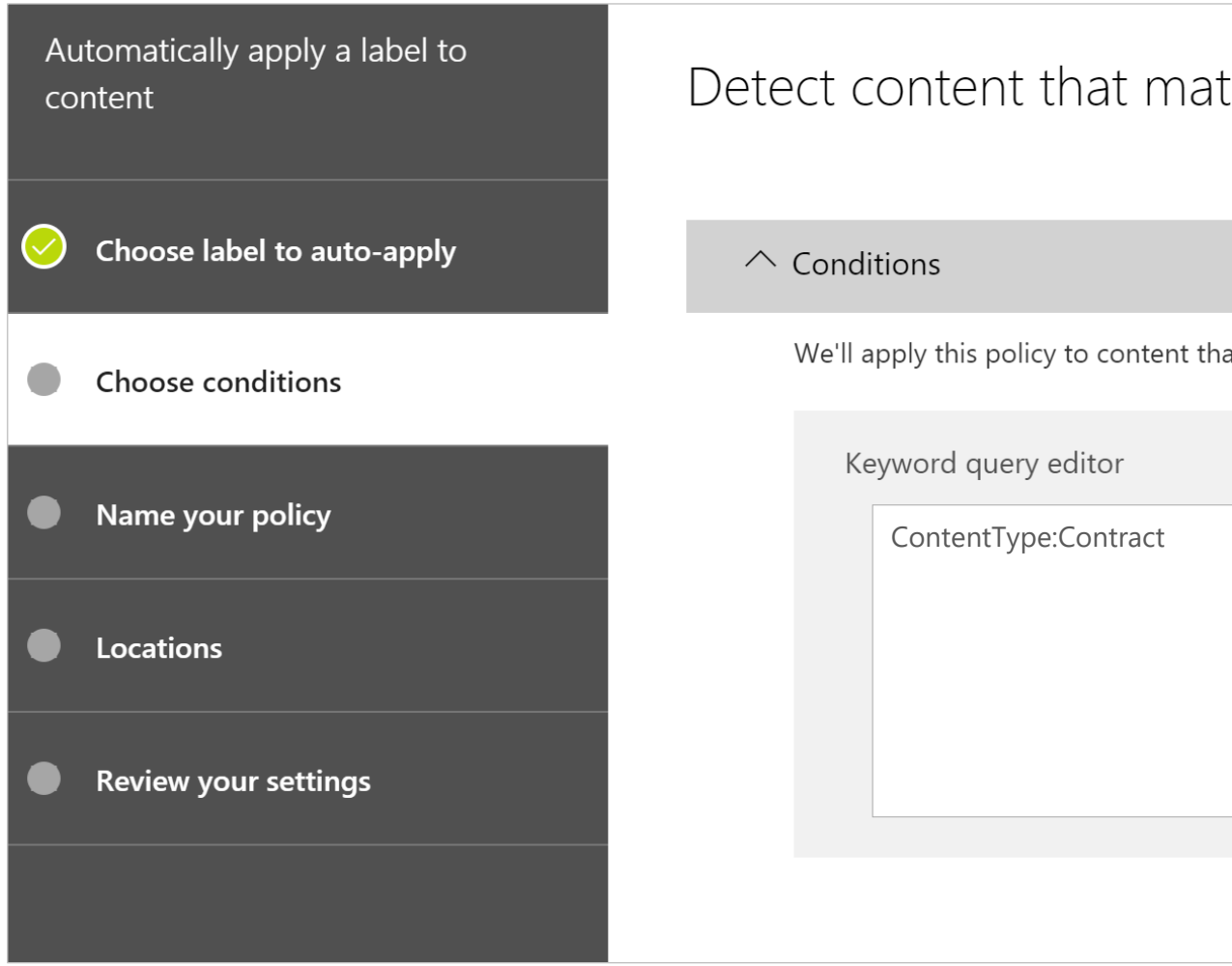
**Retention label** defines record policy based on document **age** or external **event**

**Sensitivity label** sets DLP, encryption, sharing, conditional access policies

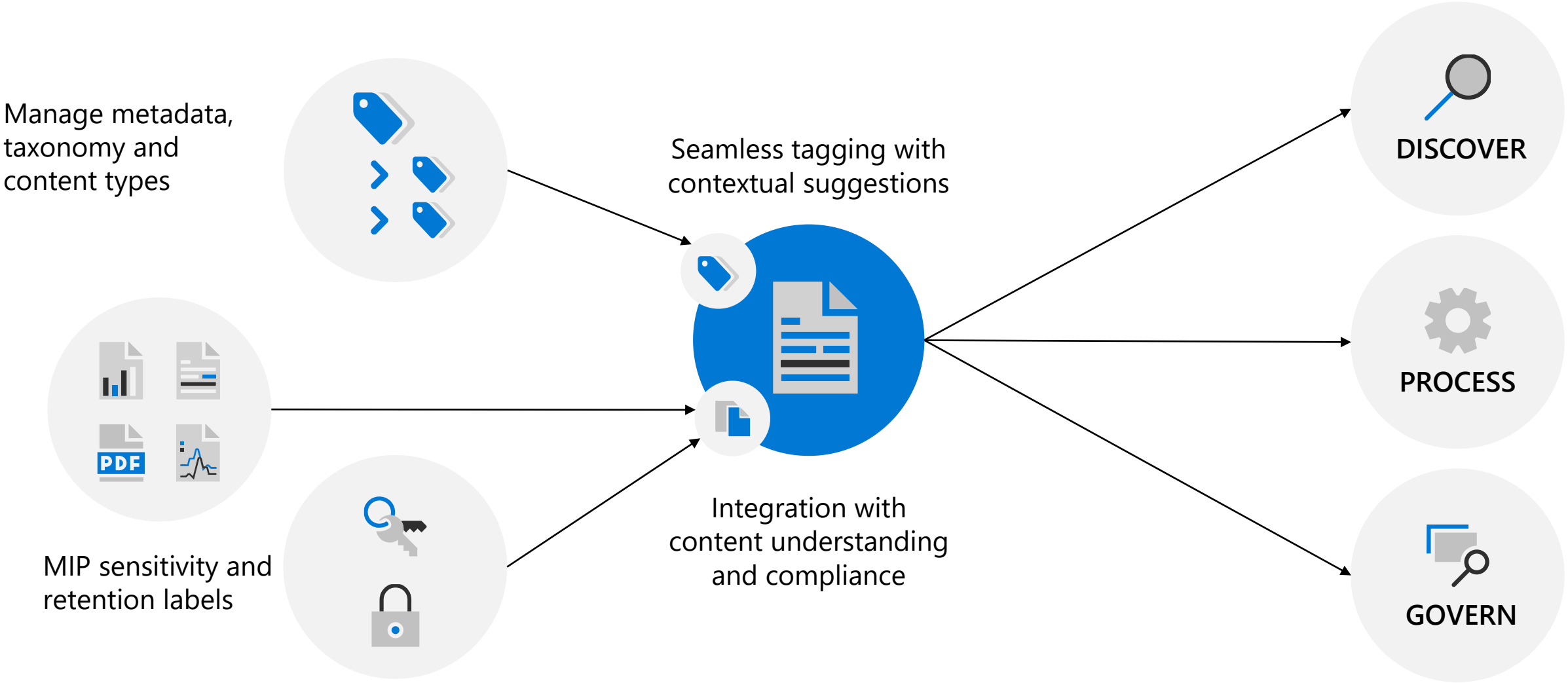
Labels can be applied **interactively** by users

Labels can be applied **automatically** by SharePoint Syntex AI models

**Analytics** and **file plans** provide scaled management of label usage and policies



# RESULTS: Improved precision and consistency



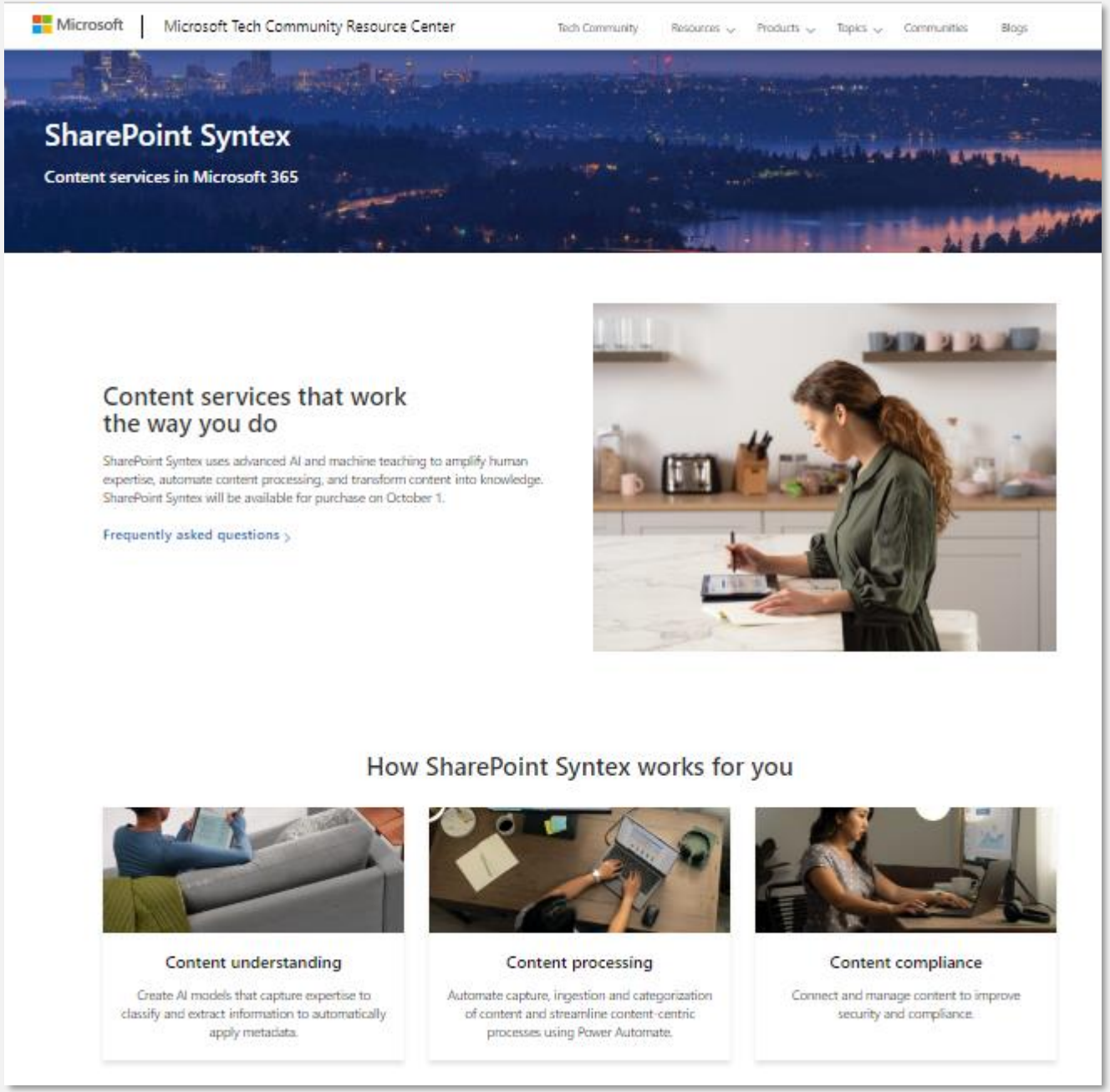
# SharePoint Syntex resources

Blog announcement:
aka.ms/SharePointSyntex/Announce

SharePoint Syntex page:
aka.ms/SharePointSyntex

Video: aka.ms/SharePointSyntex/Video

Demo: aka.ms/SharePointSyntex/Demo



# Get started with the **Compliance Workshop:** Data Risk Management

### Understand the risks of *Dark Data*
Discuss and understand the hidden compliance risks of dark data and how to mitigate

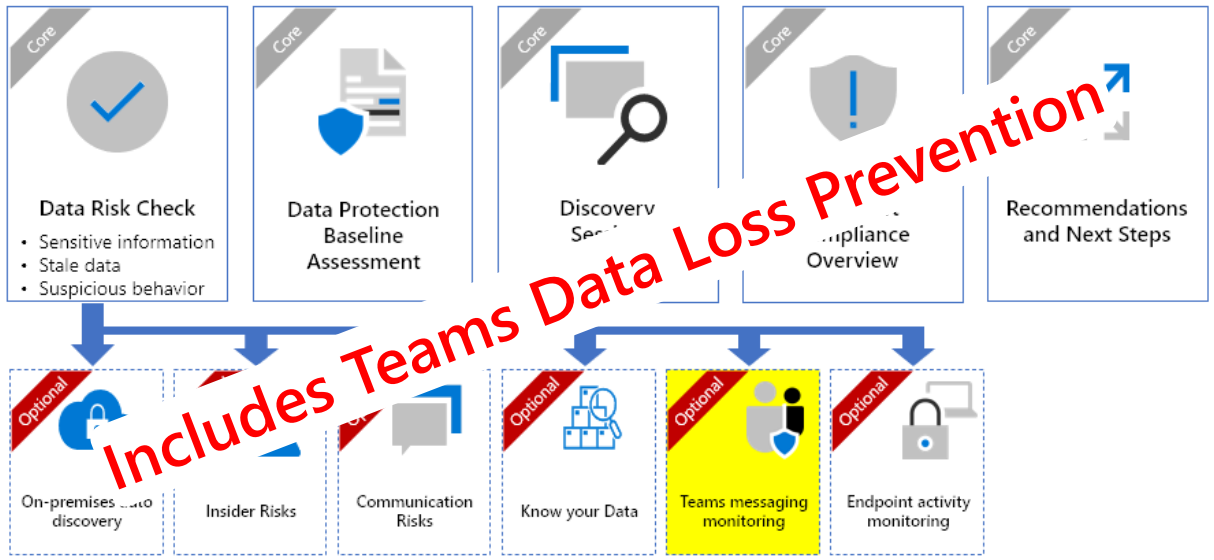
### Discover compliance risks of existing data
Insight in the organizations data across the organization

### Assess the customers Microsoft 365 environment
Assess against a set of controls for key regulations and standards for data protection and general data governance.

### Analyze and report
Analyze the findings and associated compliance risks. Provide insight and highlight most impactful.

### Learn about Microsoft's Compliance Portfolio
How can cloud services help and what does this mean for the end user.

### Recommendations and next steps
Provide recommendations for risk mitigation and define actionable next steps




**Want to know more?**
http://aka.ms/M365PartnerAccelerators

**Download from:**
http://aka.ms/complianceworkshop/download

# Security, Compliance, Identity (SCI) Certifications & Exams

## Fundamental

**Microsoft Security, Compliance, and Identity Fundamentals**

- SC-900: Microsoft Security, Compliance, and Identity Fundamentals **(GA Launch!)**

## Associate

**M365 Security Administrator Associate**

- MS-500: Microsoft 365 Security Administration

**Microsoft Security Operations Analyst**

- SC-200: Microsoft Security Operations Analyst **(GA Launch!)**

**Microsoft Identity and Access Administrator**

- SC-300: Microsoft Identity and Access Administrator **(GA Launch!)**

**Microsoft Information Protection Administrator**

- SC-400: Microsoft Information Protection Administrator **(GA Launch!)**

**Azure Security Engineer**

- AZ-500: Microsoft Azure Security Technologies

## Expert

**M365 Enterprise Administrator Expert**

- MS-100: Microsoft Identity and Services
- MS-101: Microsoft 365 Mobility & Security

- The links for the exams point to learning paths on Microsoft's **Partner Training Center.** These learning paths have modules that send learners to content on Microsoft Learn as well as completed OCP Virtual Training Series for Partners (formerly known as VILT) to help learners on their path to certification with their learning modality of choice.
- Visit the **Partner Training Center** includes learning paths across all Microsoft clouds.
- Go here for the latest certification roadmap **Microsoft training and certifications**.

# Compliance Additional Resources

## Fundamental

### Microsoft 365 Compliance

Be a Risk Management Hero

Supercharge Information Protection and Governance

Don't Lose Sleep Over Insider Risks

Simplify and Extend Compliance Beyond Microsoft 365

### Safeguard Customer Data

Learn How Microsoft Safeguards Customer Data ■

## Intermediate

### Information Protection and Governance

Information Protection and Governance ▶

Protect Sensitive Data with Microsoft Information Protection ◉

Information Protection & Governance ■

### Insider Risk Management

Manage Internal Risk in Microsoft 365 ■

Minimize Internal Risks ◉

Insider Risk Management ▶

Minimize Communication Risks ◉

Implement Privileged Access Management ◉

### Discover & Respond

Advanced eDiscovery and Advanced Audit ■

Discover & Respond ▶

### Compliance Management

Reduce Risk with Microsoft Compliance Manager ■

Simplify Compliance and Reduce Risks ▶

## Advanced

### Compliance Ecosystem

Security and Compliance

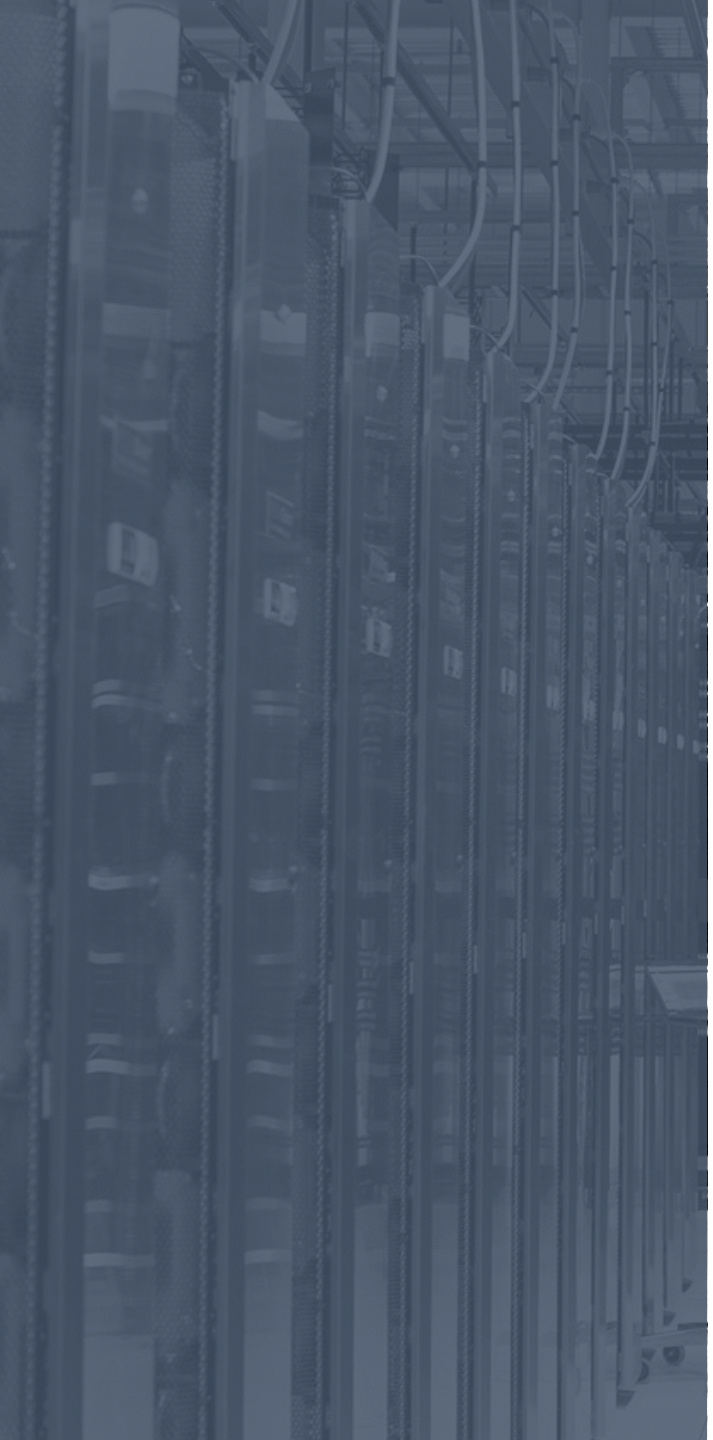
Microsoft 365 Information Protection and Compliance Deployment Acceleration Guides

**Legend**

■ Microsoft Learning Path

▶ YouTube Playlist

◉ Interactive Guide



# Microsoft Information Protection and Governance

- **MIP Website:** https://www.microsoft.com/en-us/microsoft-365/business/data-protection
- **Documentation:** https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-information
- **Blogs**: https://techcommunity.microsoft.com/t5/microsoft-security-and/bg-p/MicrosoftSecurityandCompliance/label-name/Information%20Protection%20&%20Governance
- **Online roadmap tool:** https://aka.ms/mipc/roadmap
- **Licensing**: https://aka.ms/compliancesd
- **Don’t have M365 E5 yet? Sign up for a trial at** aka.ms/M365E5ComplianceTrial
- **Mapping of features to SKUs**: https://aka.ms/MIPLicensing
- **MIP SDK Documentation**: https://aka.ms/MIPSDKDocs
- **MIP SDK Sample**: https://aka.ms/MIPSDKSamples
- **MIP SDK Blog**: https://aka.ms/MIPDevelopers

Microsoft

# Microsoft Security, Compliance, Identity Virtual Hub

At Microsoft, we've reimagined security, identity, and compliance. We provide frictionless security, identity and compliance that you can rely on, so you can be free to go further, faster.

Our intelligent solution is built to empower you and your business, keeping you resilient and agile. It integrates across platforms, clouds, and services, and helps you automate common tasks so you can focus your time on the most important work. Explore the SCI virtual hub learn more about Microsoft's security, identity, and compliance solutions.

## Security

Microsoft's security solutions empower security teams to do more with intelligent capabilities, delivers industry-leading protection, and streamlines integration for comprehensive coverage. Explore these resources to learn how Microsoft can help stop attacks and safeguard your multi-cloud resources.

## Compliance

Explore these resources and learn how to intelligently assess your risks, govern and protect sensitive data, and effectively respond to regulatory requirements.

## Identity

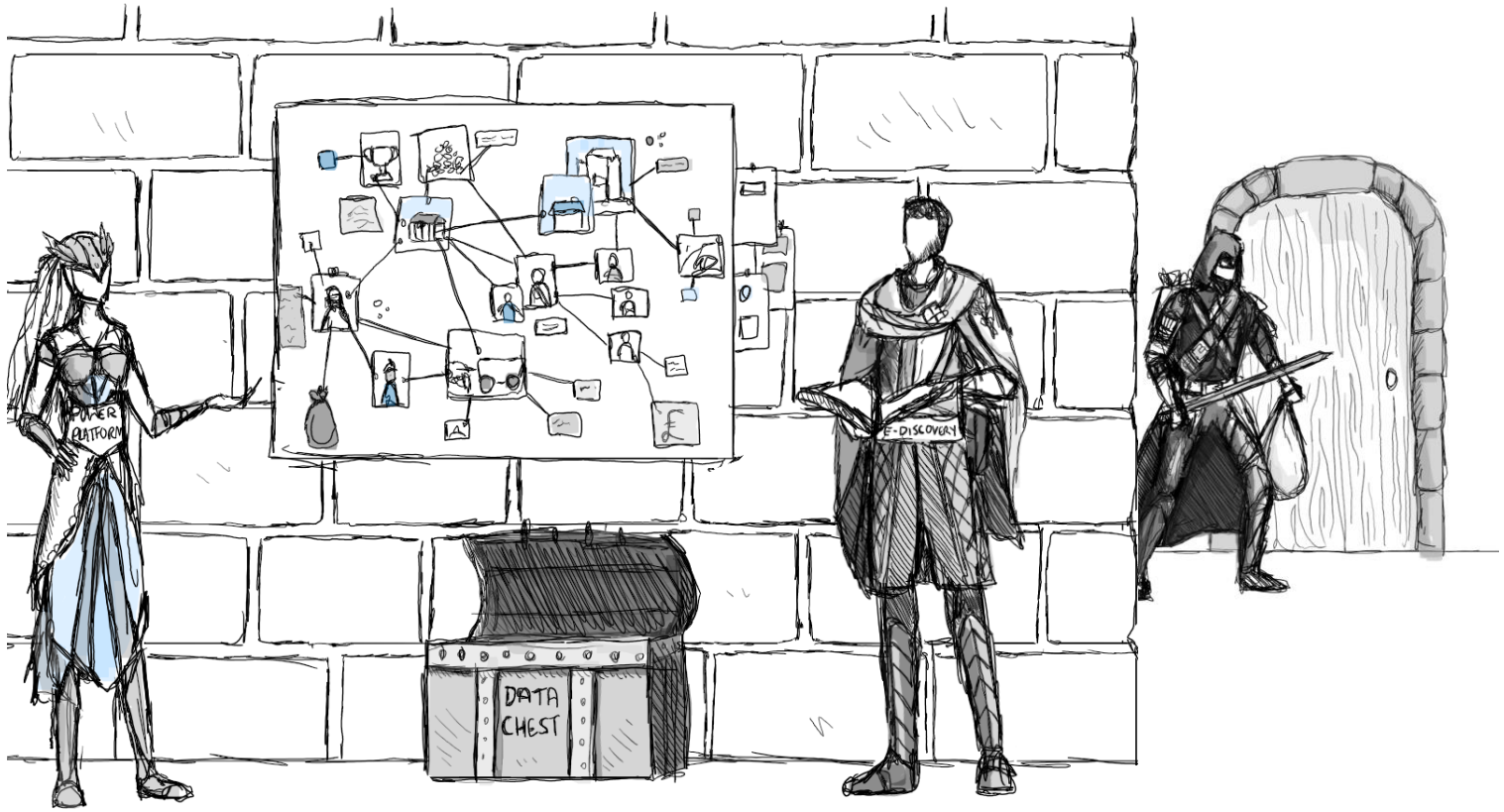
Embrace secure access for a connected world with Microsoft identity and access management services, and build a strong foundation for a Zero Trust security model. Explore these resources to learn how you can secure your workforce, maintain productivity, and protect against threats.

# Upcoming Security, Compliance & Identity Partner Events


- **Microsoft Defender Masterclass III**
  - 17th June – 9am to 1pm
  - https://aka.ms/defendermasterclass3-reg

- **Microsoft Defender Masterclass IV – Capture the Flag**
  - 30th June – 9am to 1pm
  - https://aka.ms/defendermasterclass4-reg

# Compliance @ Speed Part 3 The Finale – 23rd June, 2021 9:30am – 1pm (British Summer Time)




Join the Microsoft Protectors for Part III at Speed. A 3.5 hour event, where we will build on what you learnt in Part I. More Compliance Platform demos across Microsoft 365 and Azure including:

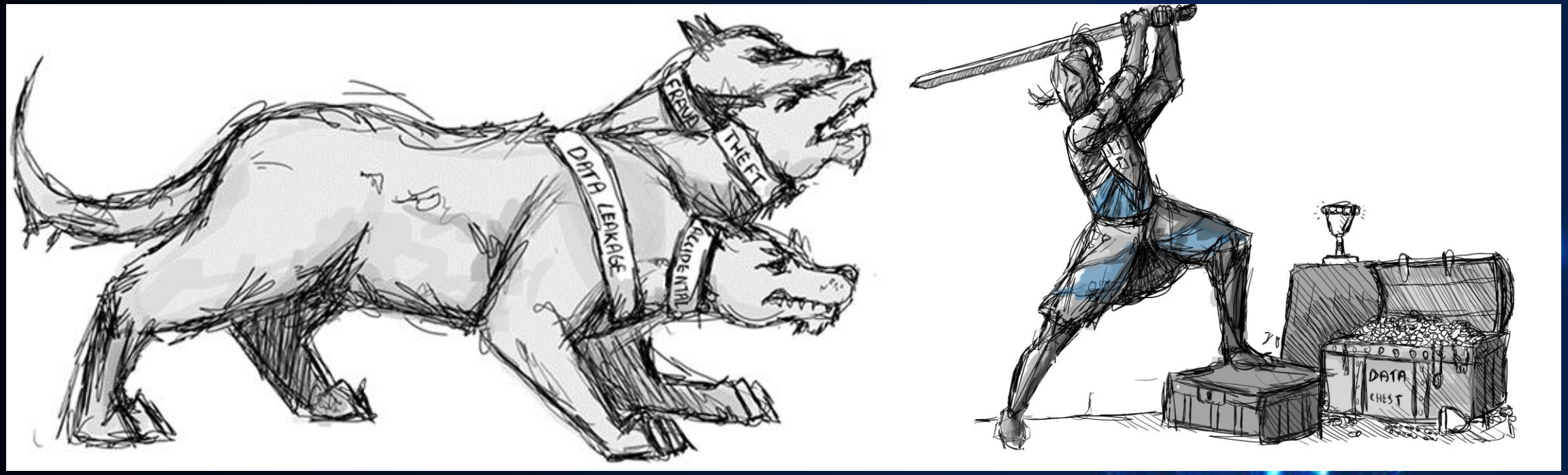
eDiscovery , Azure Sentinel, Conditional Access, AIP Scanner, more Power Platform integrations+ API Intergrations

*Illustrations by Becky Cholerton*

Microsoft

***Protectors.. .Register your bravery at aka.ms/complianceatspeed3-reg***

Microsoft




# Get in touch to build a compliance practice!

Email - Alison.Turnbull@microsoft.com

Microsoft

# Feedback

https//aka.ms/complianceatspeedfeed

# On-Demand Recording Part1

https://aka.ms/complianceatspeed-reg

# Slides

https://aka.ms/complianceatspeed-repo