

# Compliance @ Speed - 20<sup>th</sup> April, 2021

Join the Microsoft Protectors for a 3.5 hour event, where you will be taken on a deeper journey into our Compliance Platform across Microsoft 365 and Azure + learn how to automate using Power Platform integrations



Illustrations by Becky Cholerton



Graham Hosking



Leon Butler



Dan Cousineau



Ally Turnbull



Taygan Rifat



Mark Oburoh



Ana Demeny



# Meet the Team!

# Housekeeping



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



This will be recorded and links sent within 7 days



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



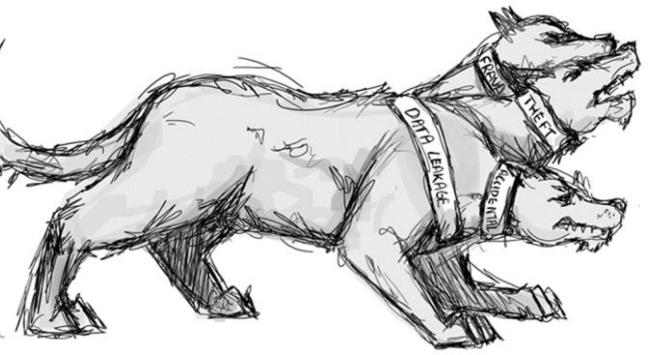
This is a one way speaker to attendees audio, so please ask any questions in the Q&A



Feedback –  
[aka.ms/complianceatspeedfeed](http://aka.ms/complianceatspeedfeed)



**All content is under your partnership NDA**



# Agenda (UK GMT)



- 09:30 - Intro and Housekeeping – Ally Turnbull
- 09:40 - Opening Keynote - Compliance Story – Dan Cousineau
- 10:00 - Compliance Score – Graham Hosking
- 10:15 - Teams DLP – Ally Turnbull
- 10:30 - **Break 10 mins**
- 10:40 - Insider Risk / Communications Compliance – Graham Hosking
- 11:15 - Power Automate and Insider Risk – Ally Turnbull + Ana Demeny
- 11:40 - **Break 10 mins**
- 11:50 - Power Virtual Agents – Ally Turnbull + Mark O
- 12:10 - Advanced DLP monitoring with Azure Sentinel – Leon Butler
- 12:25 - Azure Purview – Taygan Rifat
- 12:50 – Wrap Up
- 13:00 – Event ends



# Microsoft Compliance

Protect & govern sensitive data | Manage & investigate risk

**Dan Cousineau**

Compliance Product Marketing Manager

 /dancousineau



# Enterprise Governance, Risk & Compliance Market

Organisations face surge in DSAR's since 2018.

220+ regulatory updates issued every day.

Compliance marketing content is top download for Jan, Feb, March.

ICO now over 821 incidents being considered  
by Investigations Department.

90% organizations feel vulnerable to insider threats.

"The number of incidents has increased by a staggering 47% in just two years".

# Enterprise Governance, Risk & Compliance Market

**\$60bn**

*Projected size of Global eGRC  
market in 2025*

**13.5%**

*CAGR of global eGRC market*

**\$17.7bn**

*Size of Europe's GRC market in  
2025*

**14%**

*CAGR of Europe's eGRC market*

# Europe's eGRC software market vs services Market

**Post COVID-19**

**\$10.4bn**

*Projected size of eGRC **Software**  
market in Europe by 2025*

**\$7.3bn**

*Projected size of eGRC **Services**  
market in Europe by 2025*

*Post COVID-19: Europe eGRC market size, by service, 2021-2025 (USD MILLION)*

Service	2021 - e	2025 - p	CAGR (2020 -2025)
Training & Consulting	1,814	2,928	13.0%
Integration	945	1,234	9.0%
Support	1,641	3,139	15.2%
<b>Total</b>	<b>4,400</b>	<b>7,302</b>	<b>13.1%</b>

e: estimated; p: projected

Source: Secondary Research, Expert Interviews and MarketandMarkets Analysis

# Post COVID-19: Europe eGRC market size, by software, 2021-2025 (USD MILLION)

\$10.4bn

*Projected size of eGRC **Software** market in Europe by 2025*

Software Type	2021 - e	2025 - p	CAGR (2020 -2025)
Policy Management	616	781	6.2%
Compliance Management	593	754	6.1%
Audit Management	378	531	8.4%
Incident Management	1,656	2,074	5.7%
Risk Management	2,013	4,994	24.8%
Others*	641	1,316	17.5%
<b>Total</b>	<b>5,915</b>	<b>10,450</b>	<b>14.6%</b>

e: estimated; p: projected

\*Others includes business continuity management, financial control management and issue management

**Source:** Secondary Research, Expert Interviews and MarketandMarkets Analysis

# Intelligent compliance and risk management solutions



## Information Protection & Governance

Protect and govern data anywhere it lives

Policy Management  
Audit Management



## Insider Risk Management

Identify and remediate critical insider risks

Incident Management  
Risk Management  
Others  
Audit Management



## Discover & Respond

Quickly investigate and respond with relevant data

Incident Management  
Others  
Audit Management



## Compliance Management

Simplify and automate risk assessments

Compliance Management  
Audit Management

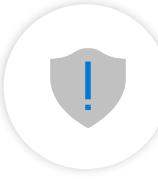
# Protect & govern sensitive data | Manage & investigate risk



## 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 Templates

# Different rooms in the house

## FUNCTION KEY

- |                                       |            |                                       |             |
|---------------------------------------|------------|---------------------------------------|-------------|
| <span style="color: green;">●</span>  | Privacy    | <span style="color: red;">●</span>    | IT          |
| <span style="color: blue;">●</span>   | Compliance | <span style="color: grey;">●</span>   | LOB         |
| <span style="color: yellow;">●</span> | Legal      | <span style="color: yellow;">●</span> | Procurement |
| <span style="color: purple;">●</span> | HR         |                                       |             |



## 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

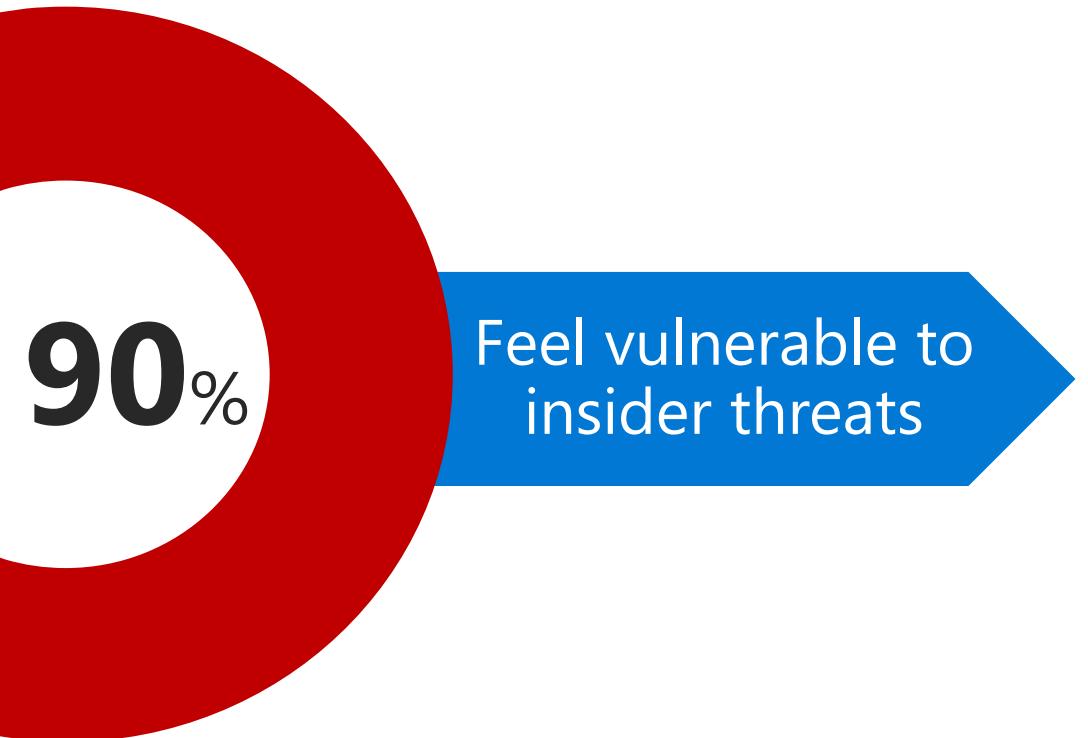
Simplify and automate risk assessments

Compliance Score  
Compliance Manager  
Long-Term Auditing  
Assessment template

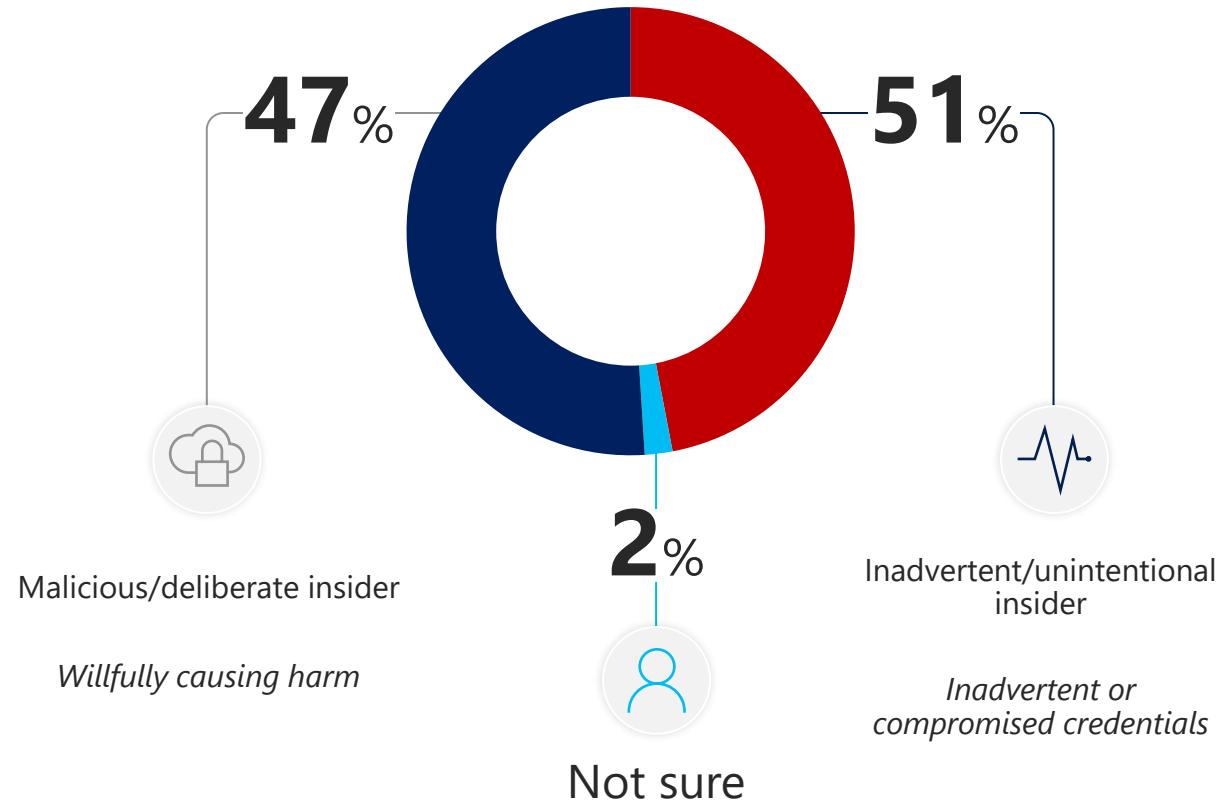


# Insider risk is one of your biggest challenges<sup>1</sup>

How vulnerable is your organization  
to insider threats?



What type of insider are you most  
concerned about?



[Home](#)[Compliance Manager](#)[Data classification](#)[Data connectors](#)[Alerts](#)[Reports](#)[Policies](#)[Permissions](#)[Solutions](#)[Catalog](#)[Application protection and gover...](#)[Audit](#)[Content search](#)[Communication compliance](#)[Data loss prevention](#)[Data subject requests](#)[eDiscovery](#)[Information governance](#)[Information protection](#)[Insider risk management](#)[Records management](#)

Insider risk management &gt; Cases &gt; IRM005

## IRM005

[Resolve case](#)[Case actions](#)[Case overview](#)[Alerts](#)[User activity](#)[Activity explorer \(preview\)](#)[Content explorer](#)[Case notes](#)[Contributors](#)

### Deletion: Files deleted

Mar 19, 2021 (UTC) | Risk score: 5/100  
16 events: Files deleted from Windows 10 Machine

### Collection: Sensitive files moved to new location

Mar 19, 2021 (UTC) | Risk score: 15/100  
34 events: Sensitive files moved to new location  
34 events: Files containing sensitive info, including: Project Codenames, Pharma Data, EU Social Security Number (SSN) or Equivalent ID, EU National Identification Number, Slovakia Personal Number  
0 Files with labels applied  
0 Files that are hidden

### Deletion: Files deleted

Mar 18, 2021 (UTC) | Risk score: 5/100  
19 events: Files deleted from Windows 10 Machine

### Collection: Sensitive files moved to new location

Mar 18, 2021 (UTC) | Risk score: 15/100  
43 events: Sensitive files moved to new location  
43 events: Files containing sensitive info, including: Slovakia Personal Number, Defence Terms, EU Social Security Number (SSN) or Equivalent ID, Bulgaria Uniform Civil Number, EU National Identification Number  
0 Files with labels applied  
0 Files that are hidden

### Collection: Files downloaded from SharePoint

Mar 18, 2021 (UTC) | Risk score: 75/100  
940 events: Files downloaded from 1 SharePoint site (Explore content)

[6 Months](#)[3 Months](#)[1 Month](#)

Risk score

100

90

80

70

60

50

40

30

20

10

0

11/1/2020

12/1/2020

1/1/2021

2/1/2021

3/1/2021

4/1/2021

Access Deletion Collection Exfiltration Infiltration Obfuscation Security

DLP policy

violation 10 annotations

59 annotations

# Results from the last scan for risk activities

X

The insights below provide a summary of anonymized user activities detected. Activities scanned are the same ones detected by insider risk policies. After reviewing the insights, view their details to drill down further and set up a recommended policy to address potential risks.

Insights from April 14 - April 18

## Potential data leak activities

### 25% of your users performed exfiltration activities

Activity from 4 users scanned

#### Recommendation: Set up a 'General data leaks' policy

Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

[View details](#)

## Top exfiltration activities

### Recommendation

#### Set up a 'General data leaks' policy

Create a policy that detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

[View details](#)

### Downloading SharePoint files

Activity from 1 users scanned

Top 1% of users downloaded SharePoint files more than 181 times

Top 5% of users downloaded SharePoint files more than 181 times

Top 10% of users downloaded SharePoint files more than 181 times

### Sending email to people outside yo

Activity from 4 users scanned

Top 1% of users emailed people outside 10 times

Top 5% of users emailed people outside 10 times

Top 10% of users emailed people outside 10 times

[Create policy](#)

[Close](#)

## Exfiltration insights

After reviewing the exfiltration activities we detected below, consider setting up the recommended policy to help address potential risks.

### What we detected

The following is recent exfiltration activity from users in your organization.

Top 1% of users downloaded SharePoint files more than 181 times

Top 1% of users emailed people outside organization more than 10 times

### Recommendation

Create a 'General data leaks' policy that detects and alerts you of potential data leaks by users, which can range from accidental sharing of info outside your organization to data theft with malicious intent.



# Thank You!



# Compliance Manager/Score

Graham Hosking – Security and compliance specialist

# Intelligent compliance and risk management solutions



## Information Protection & Governance

Protect and govern data wherever it lives



## Insider Risk Management

Identify and take action on critical insider risks



## Discover & Respond

Quickly investigate and respond with relevant data



## Compliance Management

Simplify compliance and reduce risk

# Microsoft 365 compliance offerings

Microsoft offers the most comprehensive set of compliance offerings to help you comply with national, regional, and industry-specific requirements.

## GLOBAL



ISO 27001



ISO 27018



ISO 27017



ISO 22301<sup>1</sup>



ISO 20000-1<sup>1</sup>



SOC 1  
Type 2



SOC 2  
Type 2



SOC 3



CSA STAR  
Self-Assessment



CSA CCM



WCAG 2.0  
AA



CIS Benchmark

## US GOV



FedRAMP  
Moderate



DoD DISA  
SRG Level 2<sup>2</sup>



DoD DISA  
SRG Level 4<sup>2</sup>



DoD DISA  
SRG Level 5<sup>2</sup>



SP 800-171<sup>2</sup>



NIST CSF



FIPS 140-2



Section 508 VPAT



ITAR<sup>2</sup>



CJIS<sup>2</sup>



IRS 1075<sup>2</sup>



DFARS<sup>2</sup>



FERPA

## INDUSTRY



GLBA



FFIEC



Japan  
FISC



GxP  
21 CFR Part 11



HITRUST  
CSF



Netherlands  
NEN 7510



23 NYCRR 500



PCI DSS



SOX



APRA



HIPAA/HITECH Act



TISAX

## REGIONAL



Argentina PDPA



Australia  
IRAP/CCSL



Australia  
IRAP PROTECTED



EU  
Model Clauses



EU  
GDPR



EU  
EN 301 549



EU  
ENISA IAF



EU-US  
Privacy Shield



GOV.UK  
G-Cloud



Japan  
My Number Act



Japan  
CS Mark Gold



Canada  
Privacy Laws



Netherlands  
BIR 2012



Spain  
ENS



New Zealand  
GCIO



Singapore  
MTCS



USA  
CCPA



China  
DJCP<sup>1</sup>



China  
GB 18030<sup>1</sup>



China  
TRUCS<sup>1</sup>



Germany

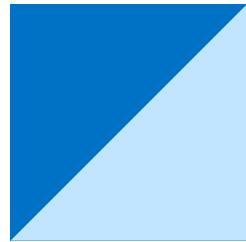
IDW PS 951

<sup>1</sup> Only for Office 365 operated by 21 Vianet | <sup>2</sup> Only for GCC/GCC High

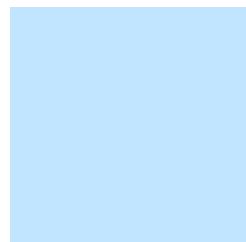
# Shared Responsibility Model



Customer management of risk  
Data Classification and data accountability



Shared management of risk  
Identity & access management | End Point Devices



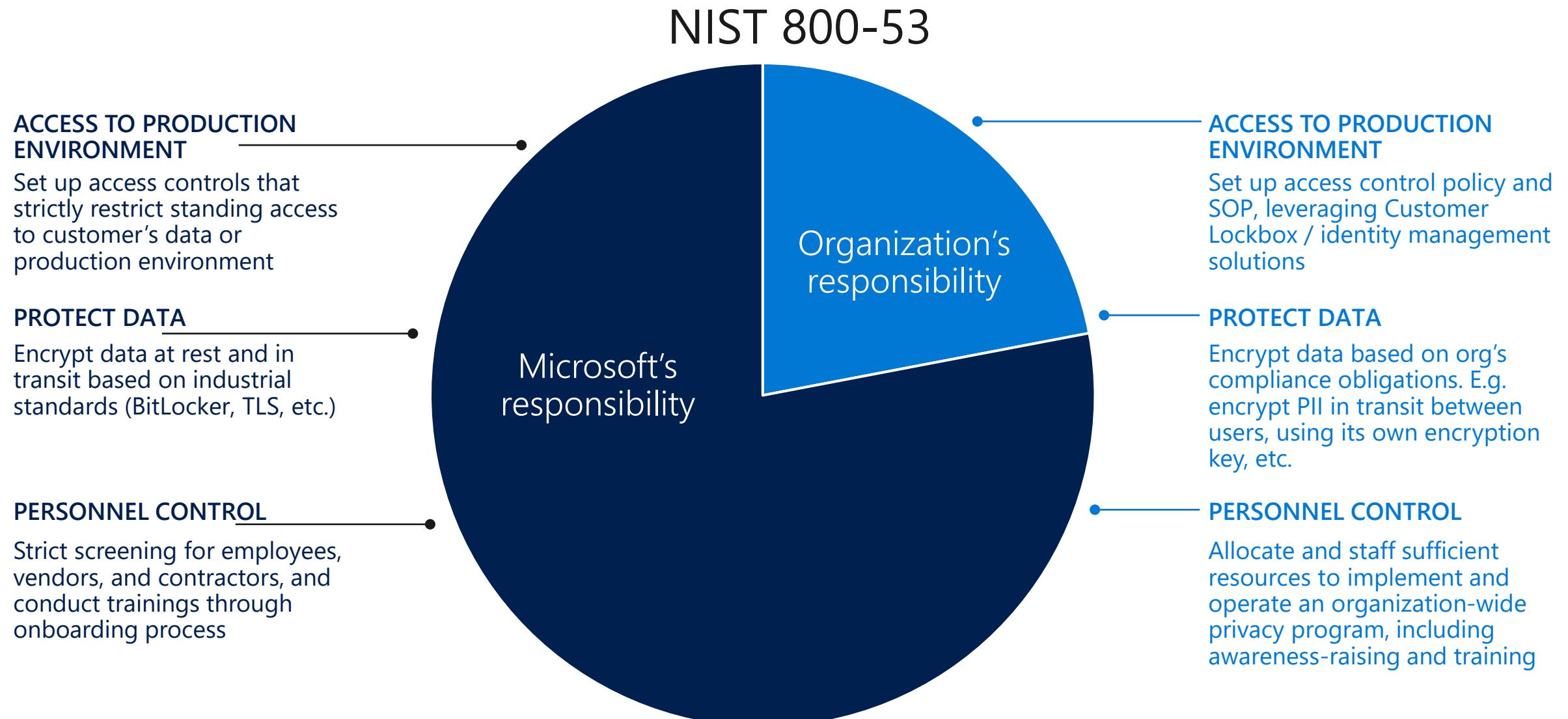
Provider management of risk  
Physical | Networking

Cloud Customer

Cloud Provider

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	Dark Blue	Dark Blue	Dark Blue	Dark Blue
Client & end-point protection	Dark Blue	Dark Blue	Dark Blue	Light Blue
Identity & access management	Dark Blue	Dark Blue	Light Blue	Light Blue
Application level controls	Dark Blue	Dark Blue	Dark Blue	Light Blue
Network controls	Dark Blue	Light Blue	Light Blue	Light Blue
Host Infrastructure	Dark Blue	Light Blue	Light Blue	Light Blue
Physical Security	Dark Blue	Light Blue	Light Blue	Light Blue

# Shared Responsibility

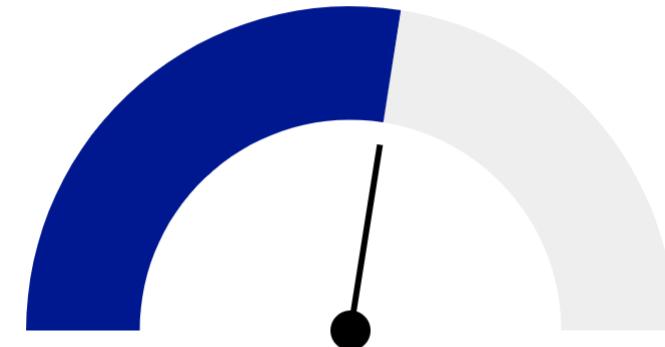




# DEMO

Overall compliance score

**Your compliance  
score: 55%**



**1173/2124 points achieved**

Your points achieved ⓘ

**108**/1059

Microsoft managed points achieved ⓘ

**1065**/1065

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

# How is your compliance score calculated?



Preventative



Detective



Corrective

► Mandatory

+27 points

+3 points

+3 points

👁️ Discretionary

+9 points

+1 points

+1 points

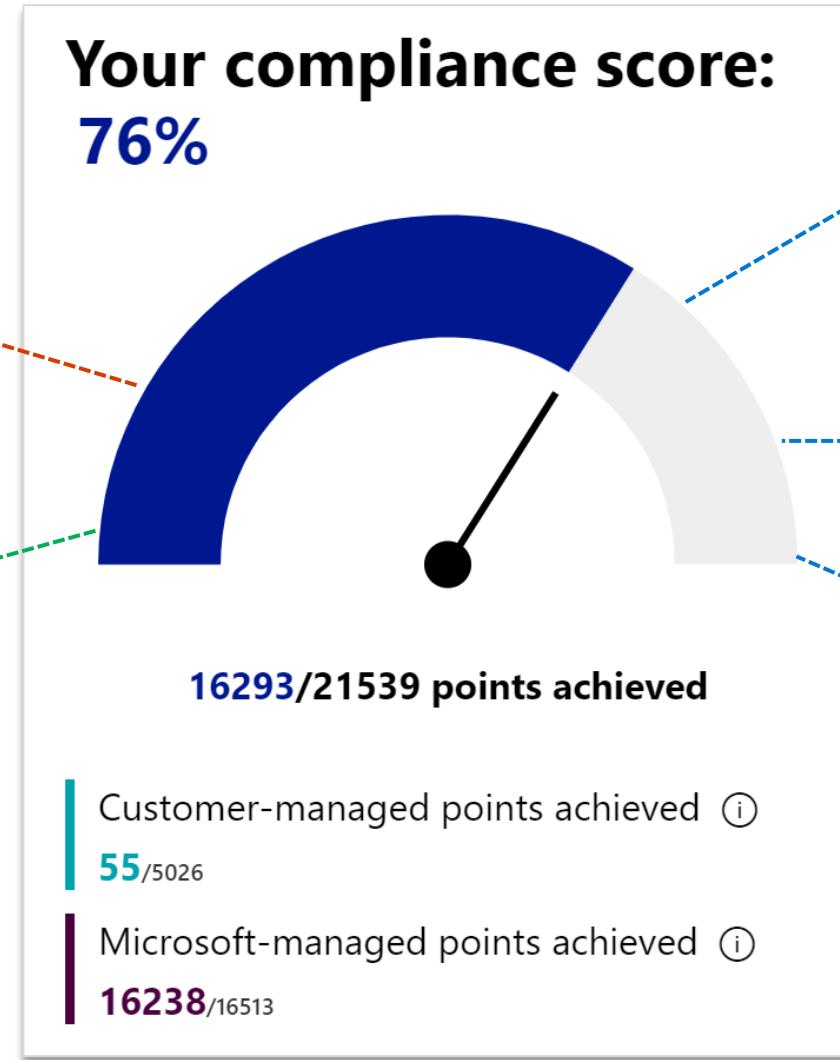
# How is your compliance score calculated?



Mandatory



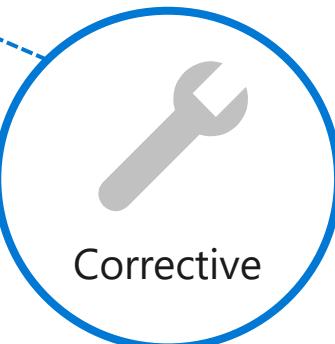
Discretionary



Preventative



Detective



Corrective

# Compliance Manager

Simplify compliance and reduce risk

## Intuitive management

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

## Scalable assessments

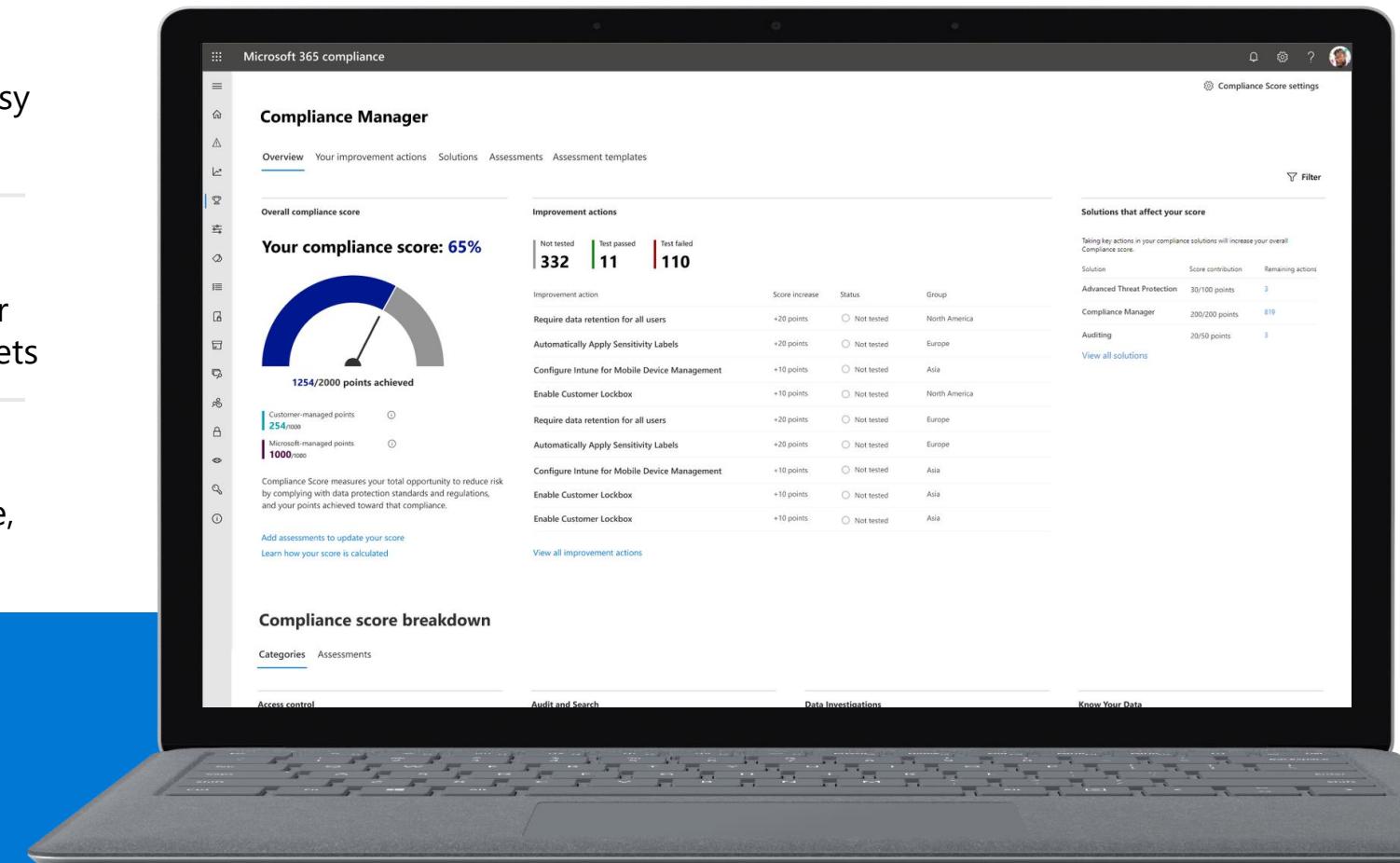
Leverage vast out of the box assessments to meet your unique compliance requirements across all of your assets

## Built-in automation

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

### Key Partner Opportunities:

- Custom Templates / Intellectual Property
- Compliance Assessments
- Managed GRC / Record Keeping



# Next Steps



Review technical documentation and public assets  
[aka.ms/compliancemanager/techdocs](https://aka.ms/compliancemanager/techdocs)

---

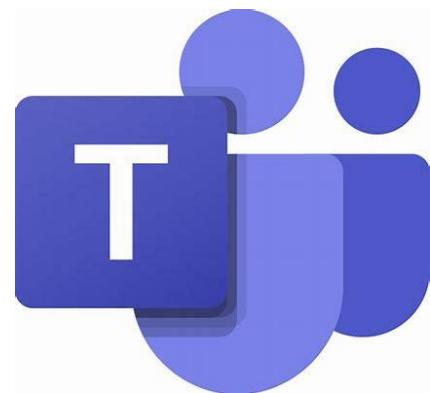
View our latest announcement and videos:  
[aka.ms/compliancemanager/Gablog](https://aka.ms/compliancemanager/Gablog)  
[aka.ms/VideoHub/ComplianceManagement](https://aka.ms/VideoHub/ComplianceManagement)

---

Get started today:  
[aka.ms/compliancemanager](https://aka.ms/compliancemanager)

Try it out:  
[Aka.Ms/E5Trial](https://Aka.Ms/E5Trial)

# Teams Data Loss Protection (DLP)



# Why Teams Data Loss Prevention?



## Microsoft Teams and Compliance

With **115 million** daily active users on Teams, compliance solutions are top of mind to help protect & manage risk

The number of Teams daily active users is ever increasing

- >115 Million daily active users (October 2020)

Teams is helping users to:

- Work from everywhere
- Share data with everybody
- Connect and communicate with everyone

But how do you control your corporate data?

- Do you know what is being shared?
- Do you know who is sharing what and with who?
- Can you control the risk of sending sensitive information?

*"Teams Data Loss Prevention will identify and stop inadvertently sharing of sensitive information, it will help to qualify, quantify and mitigate the risks"*

# Security and Compliance in Microsoft Teams



Safeguarding privacy



Meetings and conference controls



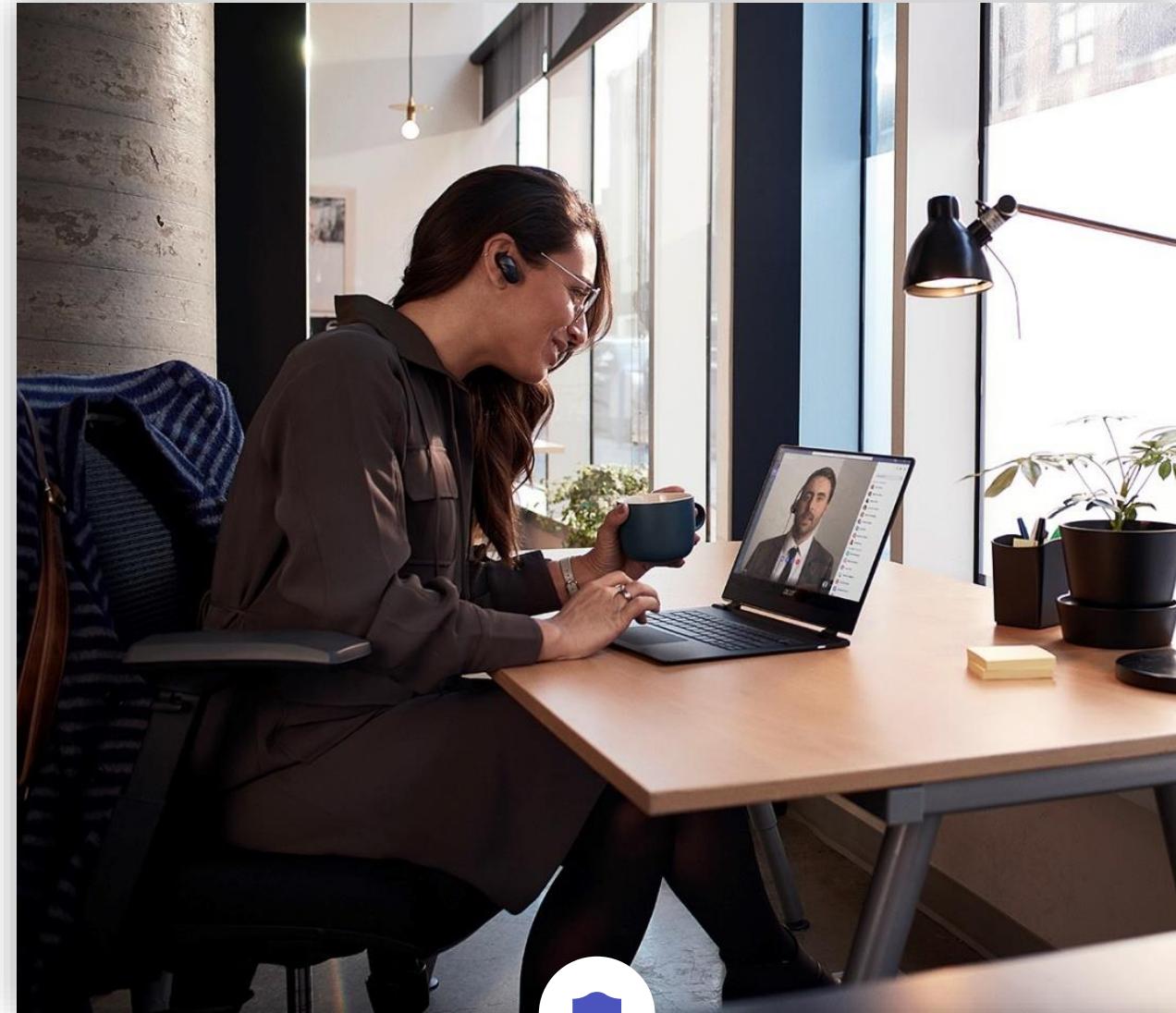
Identity and account protection



Data protection against  
cybersecurity threats



Support for 90+ regulations and  
internal compliance



Built on Microsoft 365 Security

# Microsoft Information Protection in Teams

Sensitive data protection is provided at three levels in Microsoft 365 services with granular controls to cover various scenarios and risks



Protection at the service level  
(e.g. Teams/SP site)



Protection at a document level



Prevention of data loss

Azure Active Directory + Microsoft 365 Defender + Azure Defender

# Protection of Teams and SharePoint sites

## Control who can join a Team

- Privacy – ‘Public’ vs ‘Private’
- Choose ‘public’ for anyone in your organization to join the team, or ‘private’ for only selective members can join the team
- Control whether the Team owner can add guests to the team.

## Control access to Teams sites from unmanaged devices

- For unmanaged devices, allow full access, web only access, or block access completely

## Protect with Sensitivity Labels

- Regulate access to sensitive Office documents stored in Teams with sensitivity labels
- Control access from unmanaged devices

## Granular control to external sharing of files in Teams sites

- Choose the level of external sharing: anonymous, secure external sharing, or block external access completely

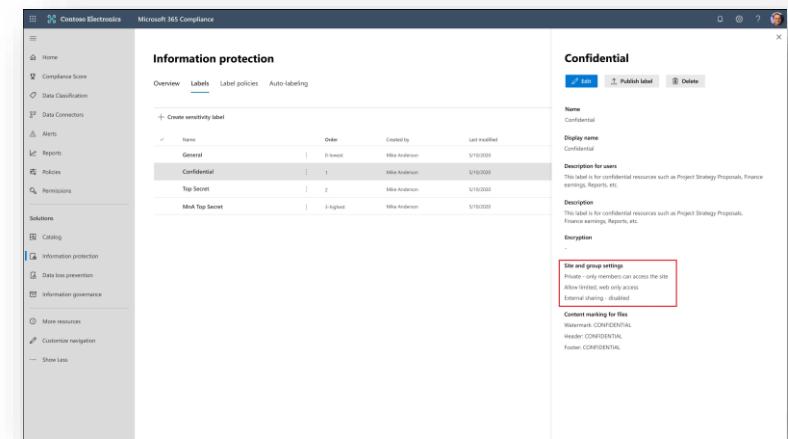


Figure: Admin experience on M365 compliance center. Labeling to protect at Teams site level

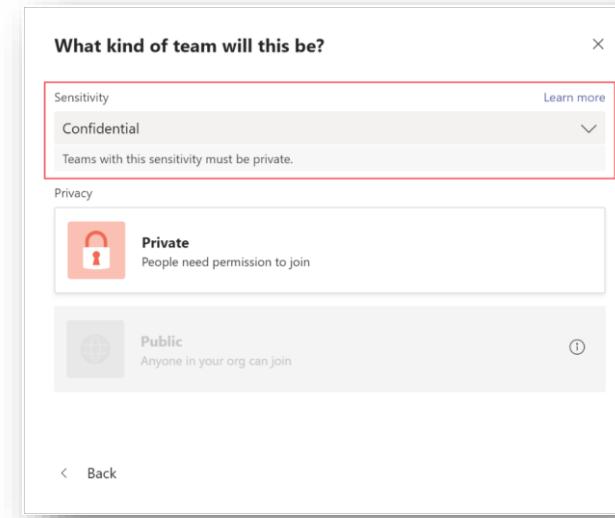


Figure: Team creation user experience – Select sensitivity label for the new team



Microsoft Teams  
and Compliance

# Teams DLP DEMO

# Data Loss Prevention for Microsoft Teams

Prevent sharing sensitive information in a channel or chat session

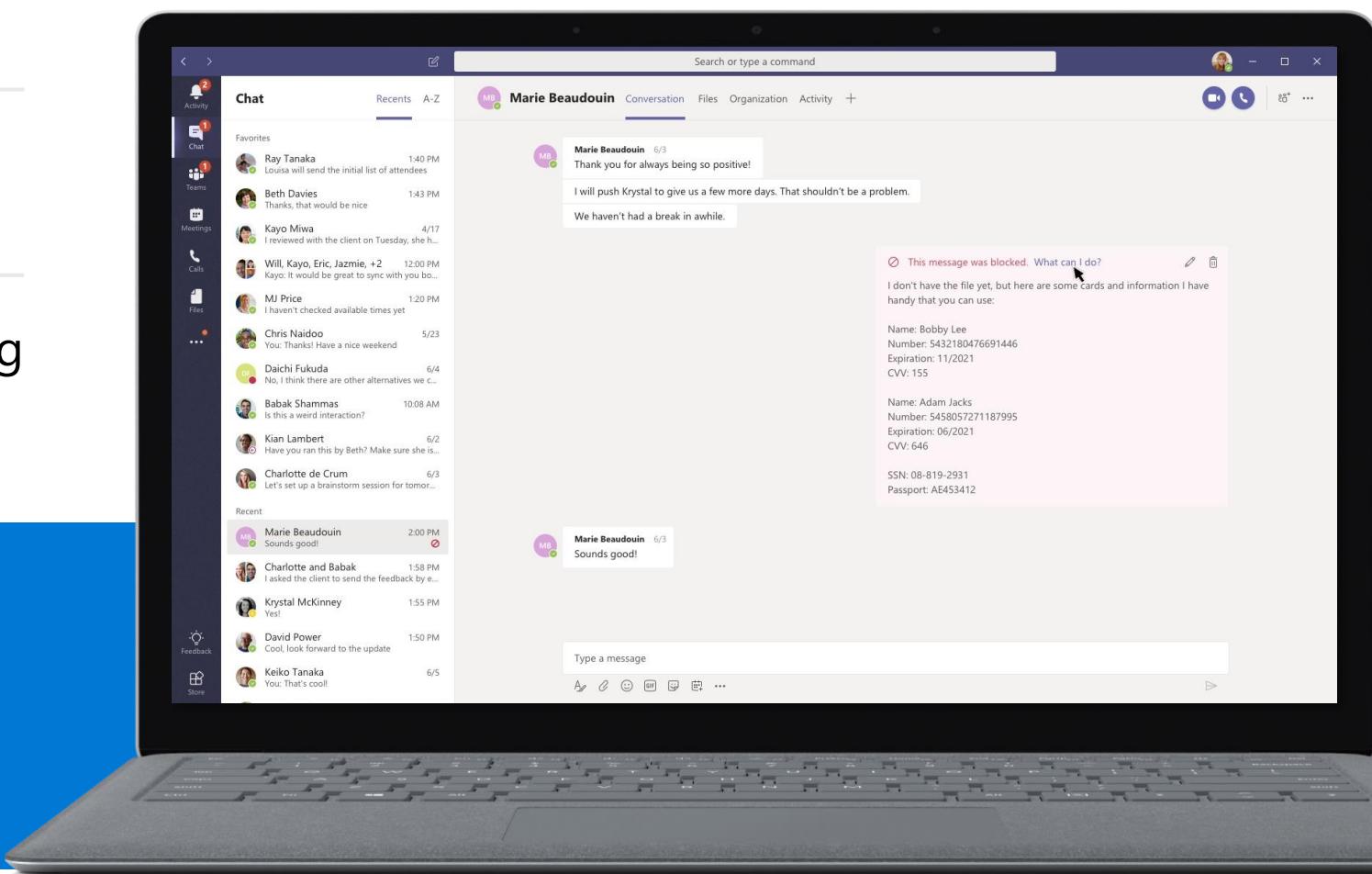
**Automatically block messages** which contain sensitive information

**Educate and guide end-users** with notifications and “policy tips”

**Unified classification engine** supporting 90+ sensitive information types and custom sensitive info type creation

## Key Partner Opportunities:

- Collaboration compliance assessment
- Remote Work Transformation
- Policy Implementation and Management
- Data Loss Mitigation
- Managed Information Protection Services



Break 1  
Please return at  
10:40am BST  
(British Summer  
Time)

---





# Insider Risk Management

Graham Hosking – Security and compliance specialist

*Illustrations by Becky Cholerton*



# Intelligent compliance and risk management solutions



## Information Protection & Governance

Protect and govern data wherever it lives



## Insider Risk Management

Identify and take action on critical insider risks



## Discover & Respond

Quickly investigate and respond with relevant data



## Compliance Management

Simplify compliance and reduce risk

# The 'Sly Dog' gang

Four employees leave their company with more than just branded sweatshirts



In March of 2019, a large car manufacture with state-of-the-art, proprietary operations and technology filed a lawsuit against four former employees and a competitor for corporate espionage.



Ringleader emailed himself proprietary warehouse schematics and operational procedures with the subject "**you sly dog you...**" Goes on to recruit three more conspirators...



The others then transferred confidential documents from work email to personal with the comment "**good stuff**"

The **theft was discovered** only when one of them mistakenly sent an email to an old work email address, attaching a version of a proprietary document, freshly-emblazoned with the competitor's logo

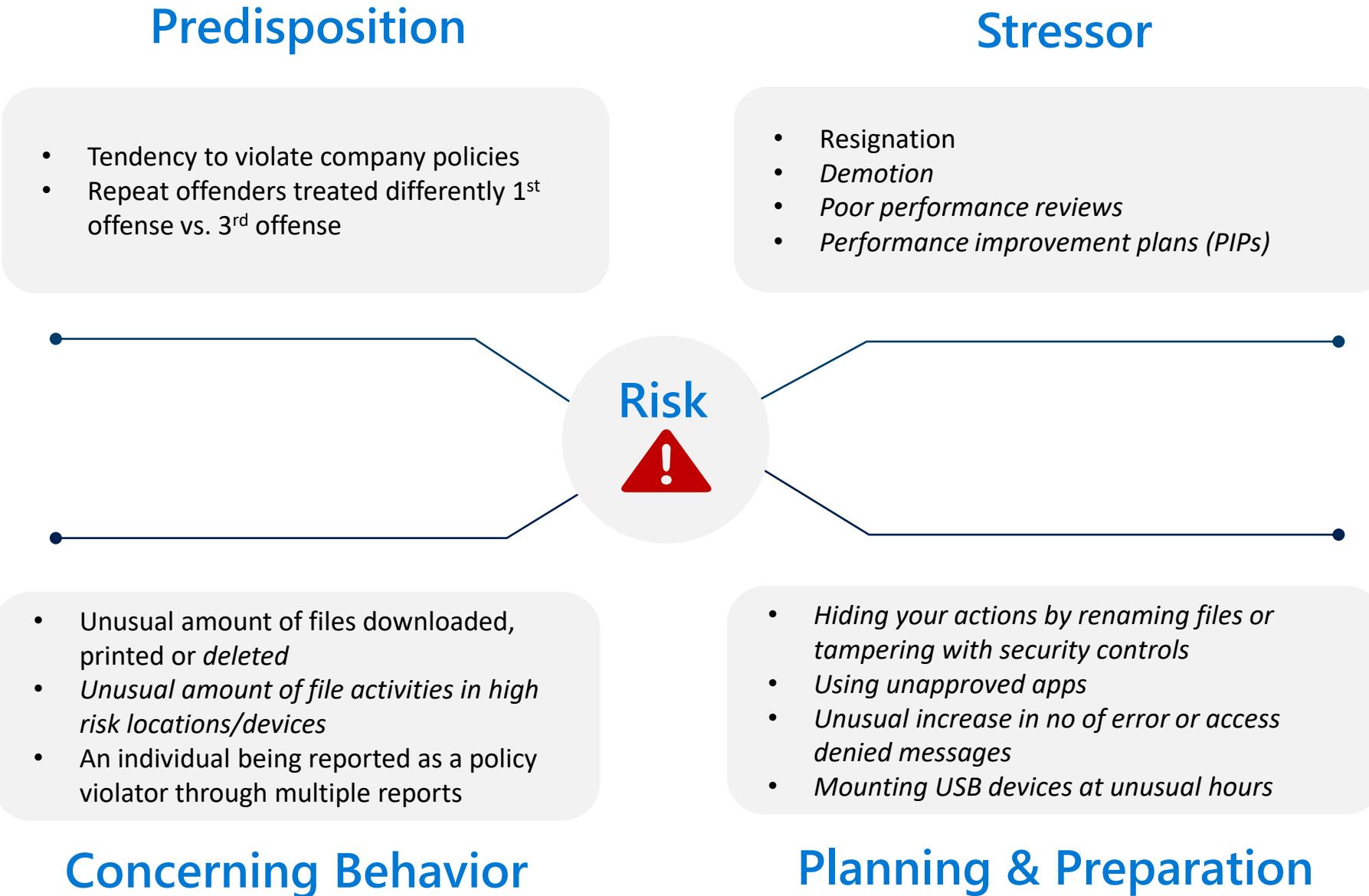
## Question:

Have you ever taken data from a previous company  
that you believed would help in a new role?

<http://pollev.com/compatspeed>

# The path leading to a malicious insider risk

Identifying indicators across phases of the critical-path can help to enable higher fidelity detections



# The path leading to a malicious insider risk

Identifying indicators across phases of the critical-path can help to enable higher fidelity detections

## Predisposition

51% of employees involved in an insider threat incident had a history of violating IT security policies leading up to the incident [Deloitte Metastudy](#)

## Stressor

92% of Insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor [Carnegie Mellon CERT](#)



97% of insider threat cases studied by Stanford University involved an employee whose behavior a supervisor had flagged, but the organization failed to follow up on [Deloitte Metastudy](#)

## Concerning Behavior

## Planning & Preparation

# Designing an intelligent insider risk solution

## Transparent

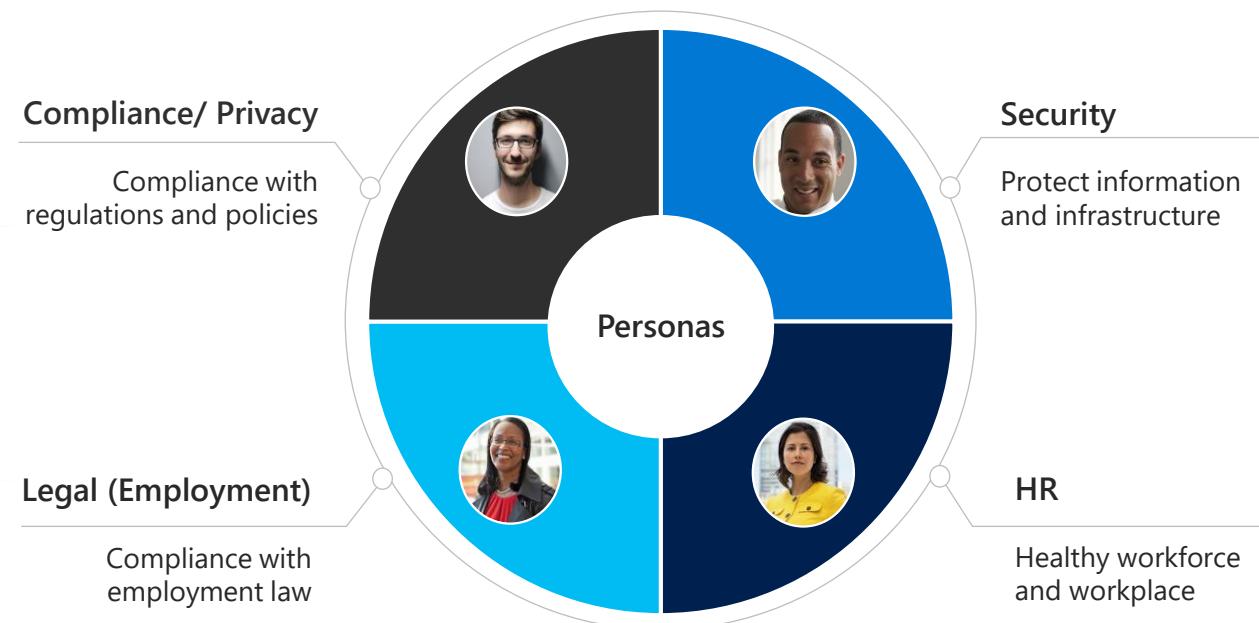
 Balance employee privacy versus the organization's risk

## Intelligent

 Leverage machine learning to identify hidden patterns

## Integrated

 Integrated workflows to support collaboration to address risks



# Insider Risk Management

Analytics provide breadth of risk in your environment

## Hidden Risks

Even before your policies are setup

## Aggregated data

Anonymity data across your organisation

## Place to start

Determine which polies to setup to start taking action.

The screenshot displays the Microsoft 365 Compliance portal. On the left, a sidebar lists various compliance management features: Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, and Permissions. Below this is a Solutions section with Catalog, Audit, Content search, Communication compliance, Data loss prevention, Data subject requests, eDiscovery, Information governance, Information protection, Insider risk management (which is selected), Records management, Privacy management, Settings, and More resources.

The main content area is divided into three sections:

- Exfiltration insights:** Shows that 1.3% of employees are showing data exfiltration patterns. A recommendation to "Monitor leakage of sensitive data with General data leaks policy" is provided. It also highlights top activities: Top 1% employees copied files to removable media more than 700 times, Top 1% employees emailed externally more than 1000 times, Top 1% employees downloaded sharepoint files more than 600 times, Top 1% employees copied files to personal cloud more than 550 times, Top 1% employees copied files to network more than 500 times, and Top 1% employees shared sharepoint files more than 500 times.
- Data Theft insight:** Shows that 5.9% of employees with a resignation date are showing exfiltration patterns. A recommendation to "Monitor leakage of sensitive data with a data theft policy" is provided. It highlights top activities: Employees copying files to USB, Top 1% employees copied files to removable media more than 1000 times, Top 5% employees copied files to removable media more than 500 times, and Top 10% employees copied files to removable media more than 100 times.
- Mitigate this risk with a policy:** A call-to-action button labeled "Create policy" is present.

At the bottom right, there are "Create policy" and "Cancel" buttons.

# Insider Risk Management

An integrated end-to-end approach for insider risks

## Hidden Risks

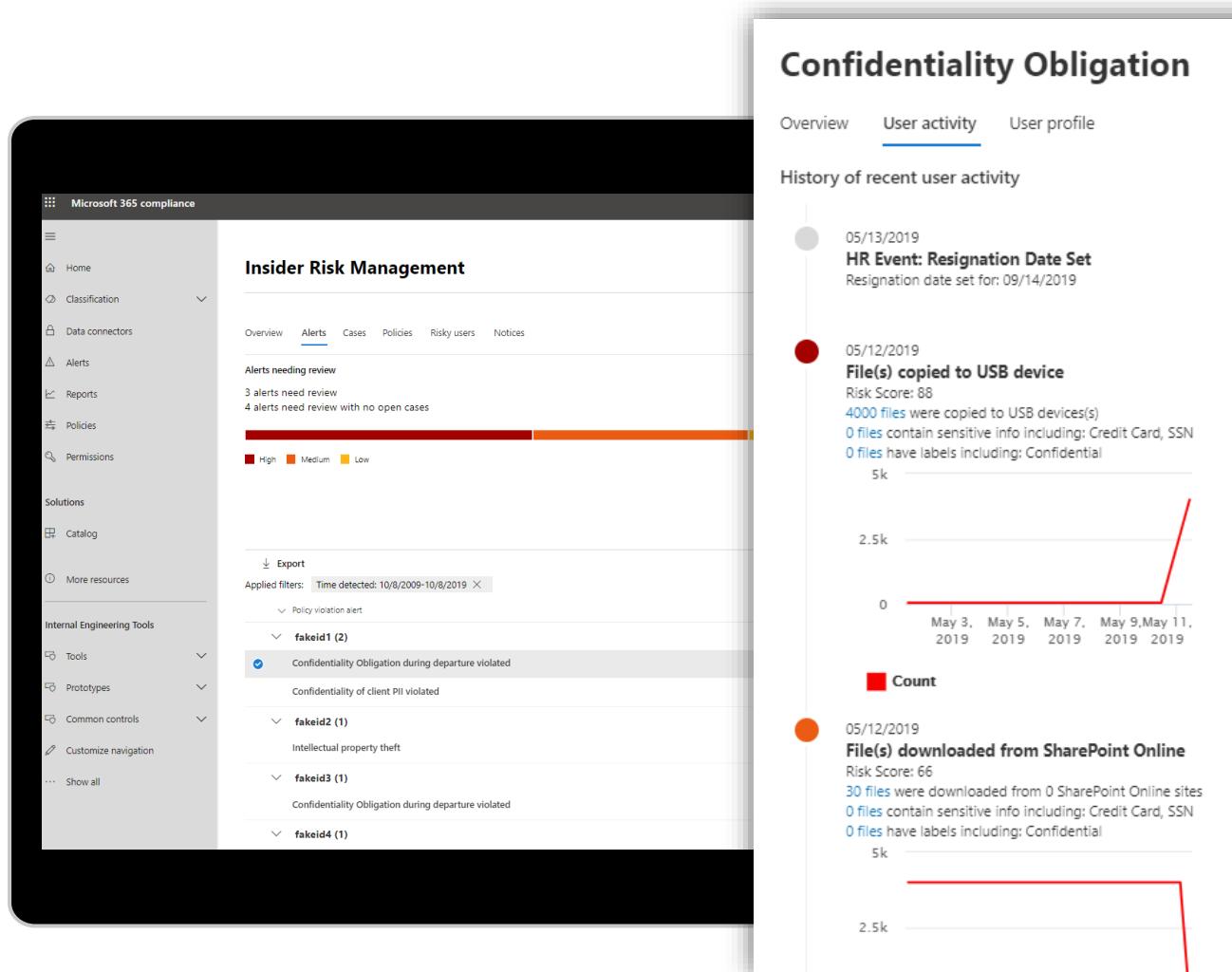
Identify hidden risk patterns with customizable ML templates requiring no end-point agents

## Privacy built-in

Anonymity controls ensure data about risks is appropriately managed

## End-to-end investigations

Integrated investigation workflows allow for collaboration across Security, HR and legal



# Insider Risk Management

An integrated end-to-end approach for insider risks from Microsoft 365

## Insider Risk Management +



### Data Loss Prevention

#### Alerts

Leverage DLP alerts to activate Insider Risk Management policies

**Insider risk management**

Overview Alerts Cases Policies Users Notice templates

Policy alerts are triggered when users perform an activity that's detected by a policy. Review these alerts and add them to a case for further investigation.

Alerts to review

3 alerts need review

Open alerts over past 30 days

Medium Low

Alert: Data access during remote work (WFH)

Overview User activity User profile

History of recent user activity

All activities Anomalous activities

3 0

Apr 14, 2020 12:17 PM DLP policy violation Risk score: 67 DLP policy: "Email exfiltration" triggered

Apr 14, 2020 8:17 AM Data Exfiltration: Emails with attachments sent outside the organization Risk score: 67 12 events: Emails sent outside the organization 0 events: Emails sent to 0 blacklisted domains 0 emails that contain sensitive info

Apr 13, 2020 2:00 PM Data Exfiltration: Files downloaded from SharePoint Risk score: 55 511 events: Files downloaded from 2 SharePoint sites 45 events: Files containing sensitive info, including: Credit card 2 events: Files that have labels applied, including: Highly Confidential

Confirm all alerts & create case Dismiss alert

# Insider Risk Management

An integrated end-to-end approach for insider risks from Microsoft 365

## Insider Risk Management +



Data Loss Prevention

Information Protection

### Enrichment

Understand context with Information Protection labels and built in sensitive data types

Microsoft 365 compliance

Insider risk management > New insider risk policy

Name and template

Users and groups

Content to prioritize

Policy indicators

Policy timeframes

Review

Specify what content to prioritize

You can assign higher risk scores to detected activity based on where labels are applied.

Choose SharePoint sites Choose sensitive info types Choose sensitivity labels

SharePoint sites

Name

https://m365x65006.sharepoint.com

Sensitive info types

Name

Sensitivity labels

Name

Choose sensitivity labels

Search

All (4 labels)

Top Secret

Confidential

Public

gvgvfgv

Back Next Add Cancel

# Insider Risk Management

An integrated end-to-end approach for insider risks from Microsoft 365

Insider Risk Management +



Data Loss Prevention

Information Protection

Communication Compliance

Advanced eDiscovery

## Legal collaboration

Integrated workflows provide  
seamless investigation handoff

Microsoft 365 compliance

Advanced eDiscovery

Recent cases

Case name	Last modified
Case 884	Oct 24, 2019 8:06 AM
IP Theft - Project Moonshot	Oct 18, 2019 10:04 AM
pp	Jan 31, 2020 9:52 AM
lives, test, 2	Jan 27, 2020 2:33 PM
hand off luke	Jan 24, 2020 11:12 AM

10 Cases

File metadata

Project Obsidian

Updated Engine Chip Design

Automated Car Team  
October 21, 2019

Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 22

With our new investments in automated cars we need to redesign the AI500 chip to pull more throughput and reduce overheating.

# Insider Risk Management

Identify and take action on critical insider risks

## Rich insights via tailored templates

Machine learning correlates native and third-party signals to identify insider risks

## Privacy built-in

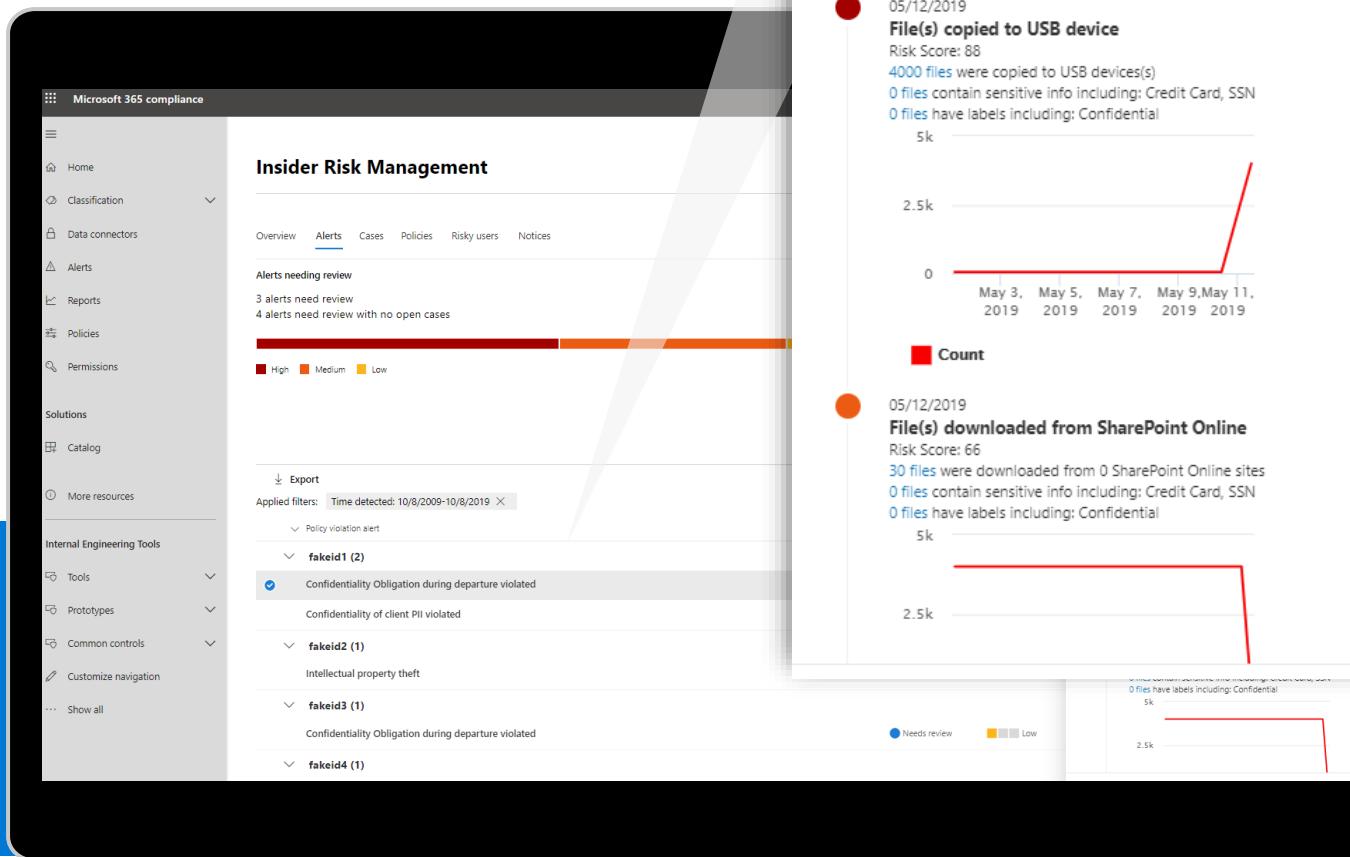
Anonymity controls ensure data about risks is appropriately managed

## End-to-end investigations

Integrated investigation workflows allow for collaboration across IT, HR, and legal

## Key Partner Opportunities:

- Insider Risk Assessment
- Policy Implementation and Administration
- Managed Insider Risk L1 / Alert Review
- Managed Insider Risk L2 / Investigations
- Managed Insider Risk (End to End Service)





# DEMO

Lets get stuck in!  
Insider Risk Management

# Data Connectors

Bring in non-Microsoft data and benefit from M365 Compliance value

## One catalog for all connectors

Discover all supported connectors built by Microsoft and partners (Telemessage and Globanet) in one place

## Simplified deployment and monitoring

Few clicks to setup data import for most connectors \*\*

## Data available for all compliance solutions

Hi-fidelity data ingestion available for all compliance solutions

## Built-in connectors for various categories

25 built-in connectors including Bloomberg Message, Slack eDiscovery, Zoom Meetings, Webex, Twitter etc.

The screenshot displays the Microsoft 365 Data Connectors interface. On the left is a dark sidebar with white text and icons, listing various features: Home, Compliance score, Data classification, Data connectors (which is the active tab, indicated by a blue underline), Alerts, Reports, Policies, and Permissions. Below this is a 'Solutions' section with 'Catalog' selected. At the bottom of the sidebar are links for 'More resources', 'Customize navigation', and 'Show all'. The main content area has a black header with the title 'Data connectors'. Underneath is a navigation bar with 'Overview' (underlined) and 'Connectors'. A green feedback bar at the top says 'Is there a specific connector you are looking for? Please let us know what you are looking for through this feedback.' Below this is a section titled 'Connect to your data sources' featuring a card for 'Instant Bloomberg' by Microsoft. The card includes a brief description: 'Connecting to your Instant Bloomberg data is valuable for communication compliance, records management, and eDiscovery solutions.', a 'Learn more' link, and a 'View' button. Another card for 'Facebook business pages' is partially visible below it, also with a 'View' button.

\*\* Connectors by 3<sup>rd</sup> party vendors requires purchasing the subscription directly with the vendor before deployment.

# 25 pre-built connectors available in Microsoft 365 compliance center

2019

Instant Bloomberg Facebook

LinkedIn Twitter

Our connector partners

Globanet

TeleMessage

Social

Facebook

Twitter

LinkedIn

Finance

Instant Bloomberg

Bloomberg Message

ICE Chat

Symphony

FX Connect

Thomson Reuters Eikon

IM/  
Collaboration

Slack

Zoom Meetings

Facebook Workplace

Webex Teams

Mobile/Text

WhatsApp Archiver

Android Archiver

AT&T

Verizon

Bell Network

O<sub>2</sub> Telephonica

Telus

Enterprise Number Archiver

Other

HR Connector

Physical badging systems

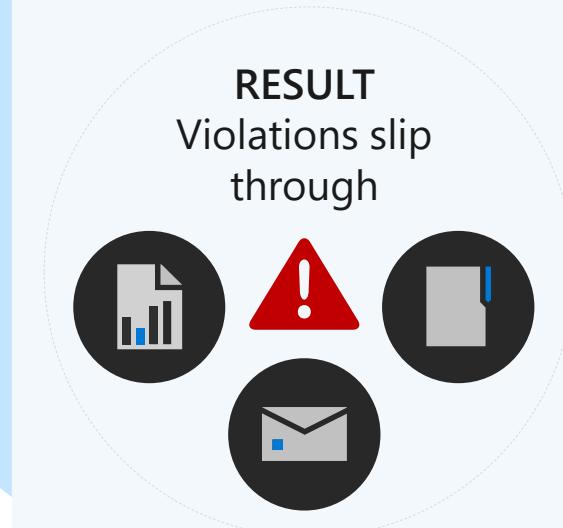
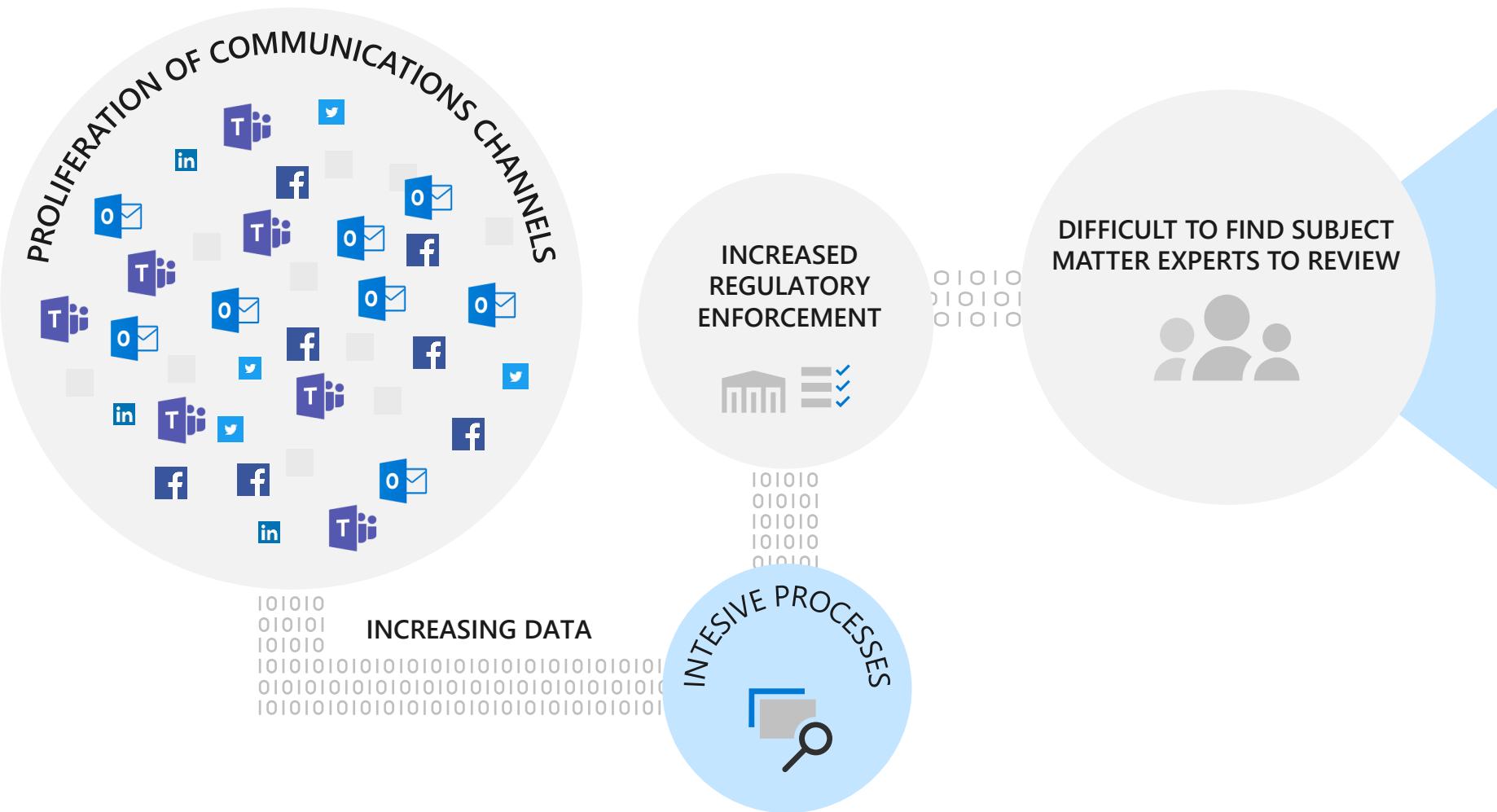
Generic Text delimited importer

Generic email importer

2020

\*Pre-built data connectors include connectors built by Microsoft and by partners - TeleMessage and Globanet. Except for TeleMessage and Globanet, Microsoft does not have direct relationships with the data source companies in bringing these data connectors to the platform.

# Typical workflow and customers pain points



# Communication Compliance

Quickly identify and remediate corporate code-of-conduct policy violations



## Intelligent customizable playbooks

Leverage machine learning to detect violations across Teams, Exchange and 3rd party content



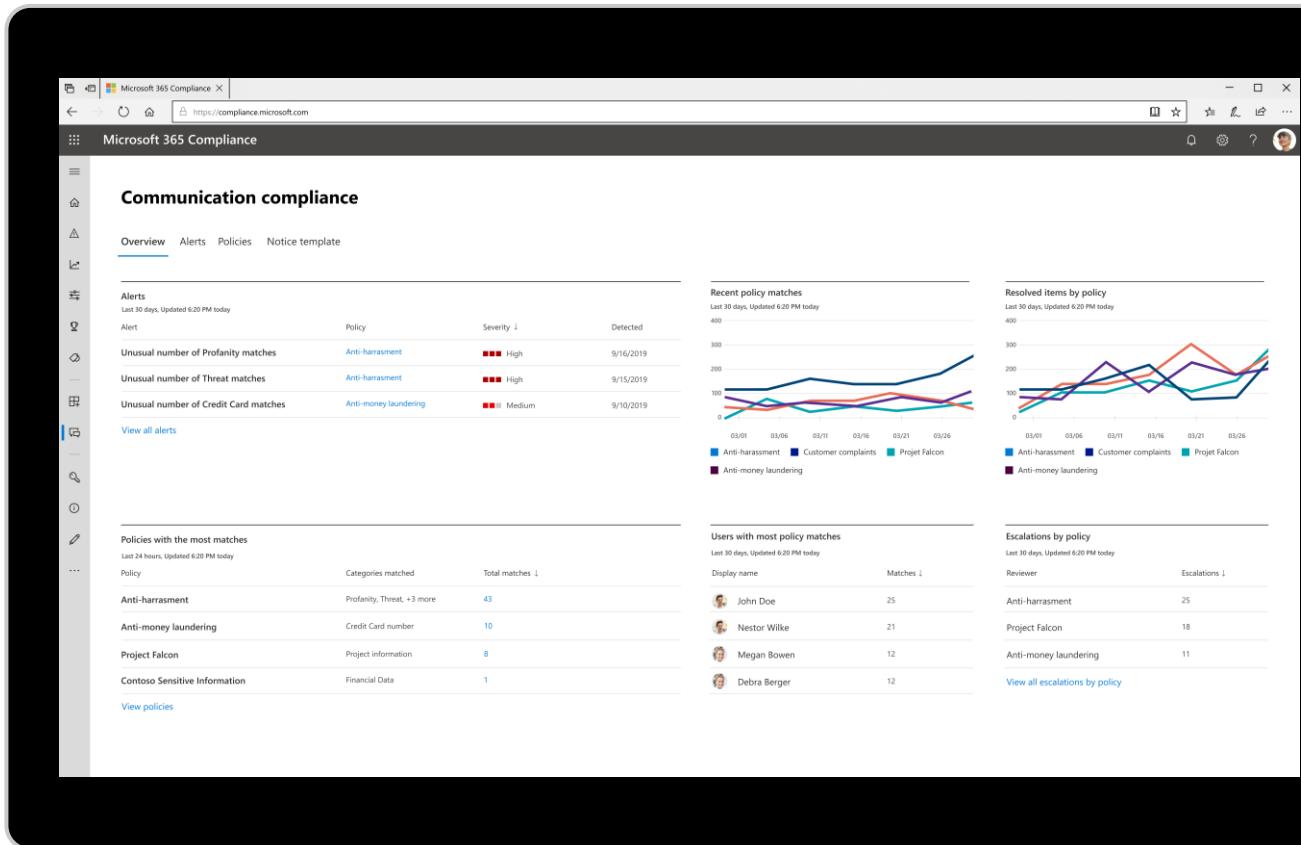
## Flexible remediation workflows

Remediation workflows to quickly act on violations and remove incriminating messages on Teams



## Actionable insights

Gain insight into policy violations by detecting threatening language in a timely manner



# Intelligent customizable playbooks



Leverage machine learning to intelligently reduce false positives



Customizable pre-configured templates to address common communications risks



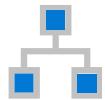
Build your own machine learning model to detect violations unique to your organization

The screenshot shows a web browser window titled "Microsoft 365 Compliance" with the URL "https://compliance.microsoft.com". The page is titled "Communication compliance > Create policy". On the left, there's a navigation sidebar with options like "Name", "Users and reviewers", "Locations", "Conditions and percentage", and "Finish". The main content area is titled "Choose conditions and review percentage". It includes sections for "Communication direction" (Inbound, Outbound, Internal) and "Conditions" (Content matches any of these classifiers, Classifiers, Threat, Profanity, Harassment). A "Review percentage" slider is set to 100. At the bottom, there are "Back", "Next", and "Cancel" buttons.

# Flexible remediation workflows



Conversation threading, keyword highlighting, exact & near duplicates, filters for efficient review



Built-in remediation workflows to quickly act on violations, ability to remove Teams message



Historical user context on past violations and remediation actions

The screenshot shows the Microsoft 365 Compliance interface with the 'Anti-harassment' policy selected. On the left, there's a list of violations under 'Pending (3)' and 'Resolved (57)'. The 'Resolved' section includes items like 'Hi team, quick reminder ...' from Bob Anderson to Jane Doe, 'Post analysis' from John Doe to Maria Cameron, and 'Re: What about tomorrow?' from Kim Klose to Katie James. On the right, a 'Send a notice' dialog box is open, allowing users to send an email notification to the violator. The dialog includes fields for 'Send notification to', 'Send from', 'Cc', 'Bcc', 'Subject', 'Message body', and buttons for 'Resolve', 'Tag as', 'Send notice', and 'Cancel'.

# Actionable insights



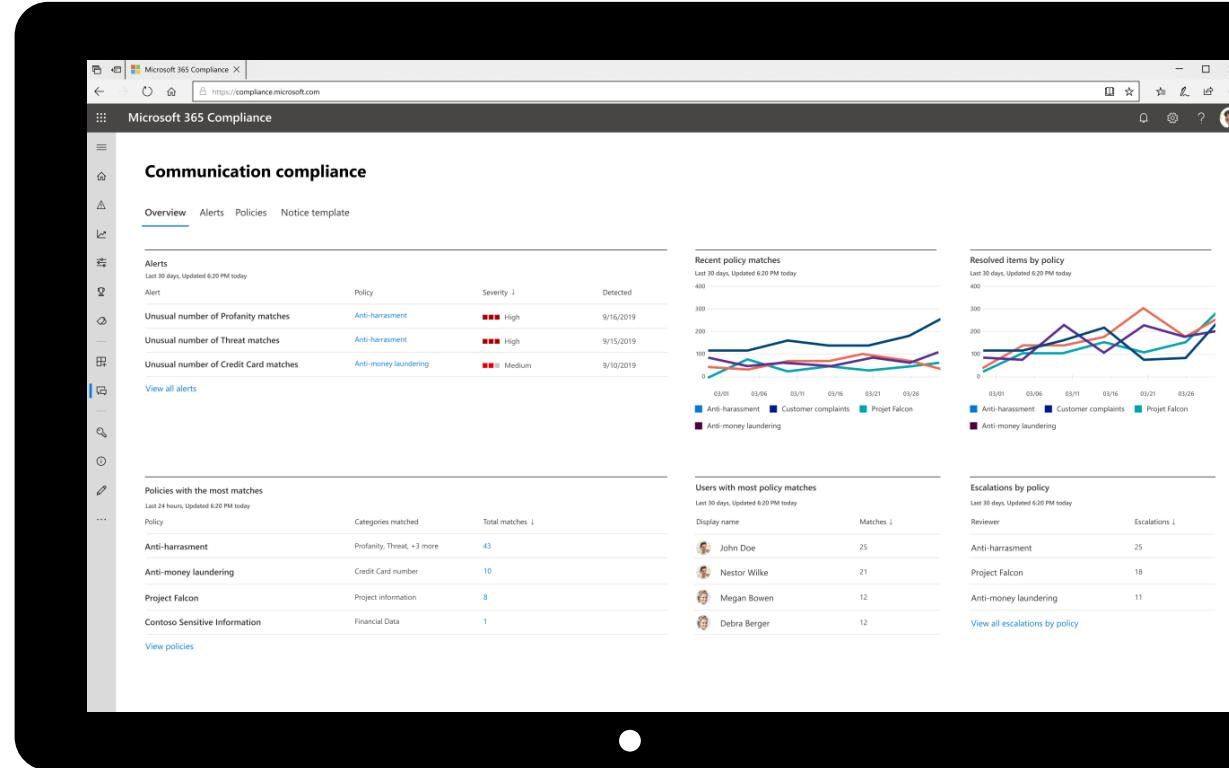
Proactive intelligent alerts on policy violations requiring immediate attention



Interactive dashboard showing violations, actions and trends by policy



Full audit of review activities and tracking of policy implementation





# DEMO

Lets get stuck in!  
Communication Compliance

# Communication Compliance

Quickly identify and remediate corporate code-of-conduct policy violations

## Intelligent customizable playbooks

Leverage machine learning to detect violations across Teams, Exchange and third-party party content

## Flexible remediation workflows

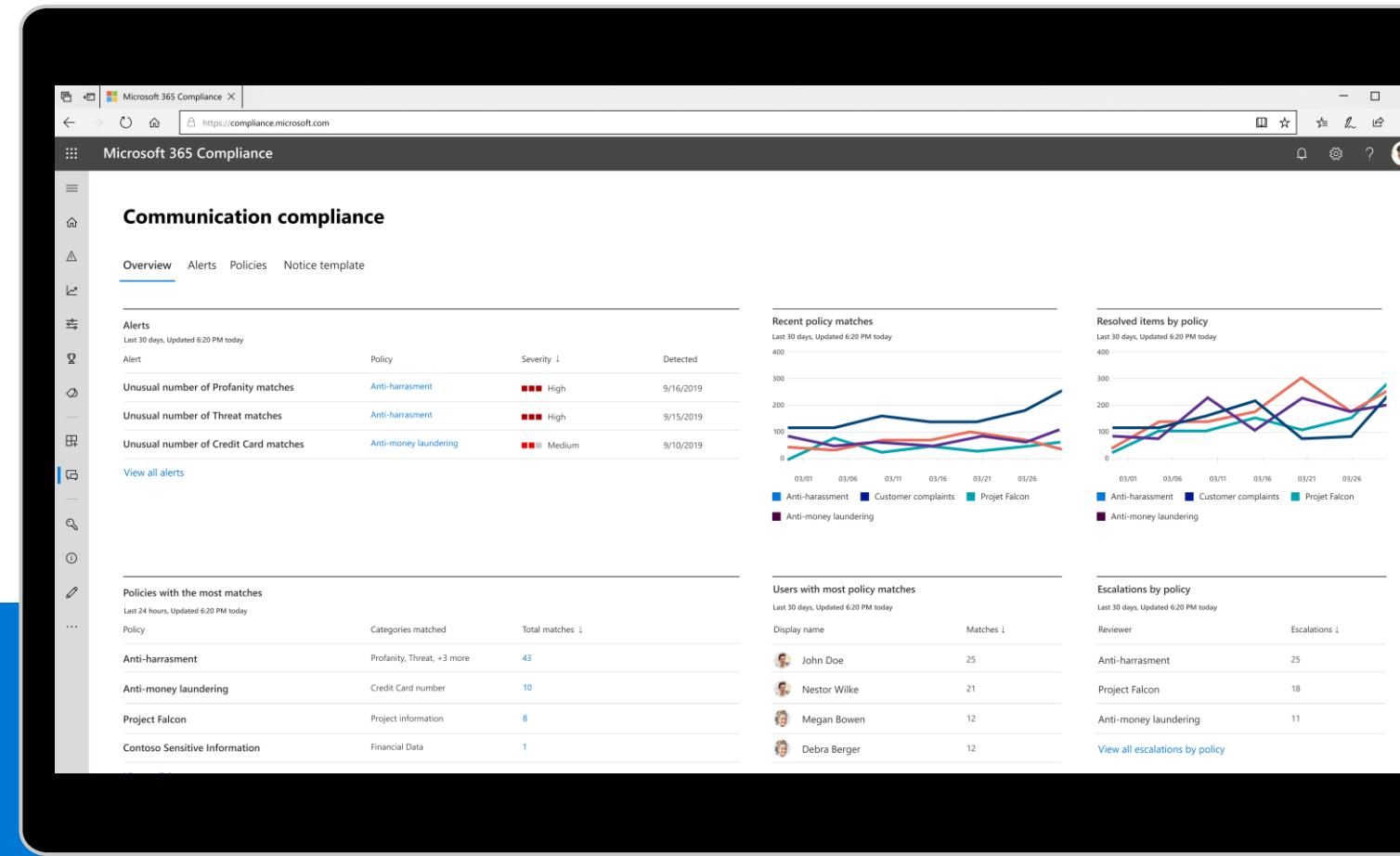
Remediation workflows to quickly act on violations

## Actionable insights

Interactive dashboard with policy violations, actions, and trends

### Key Partner Opportunities:

- Policy implementation and management
- Managed Case Review
- Managed Compliance (including HR Integration)



# Getting started



Start using Insider Risk Management today

<http://aka.ms/insiderriskmanagement>



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/ZFlrXaGvWVs>



 @AnaDemeny

 /anademeny

 Partner Technical Architect  
(INTEGRATION & RPA)



# Power Automate

## Digital Transformation ++



Ally Turnbull

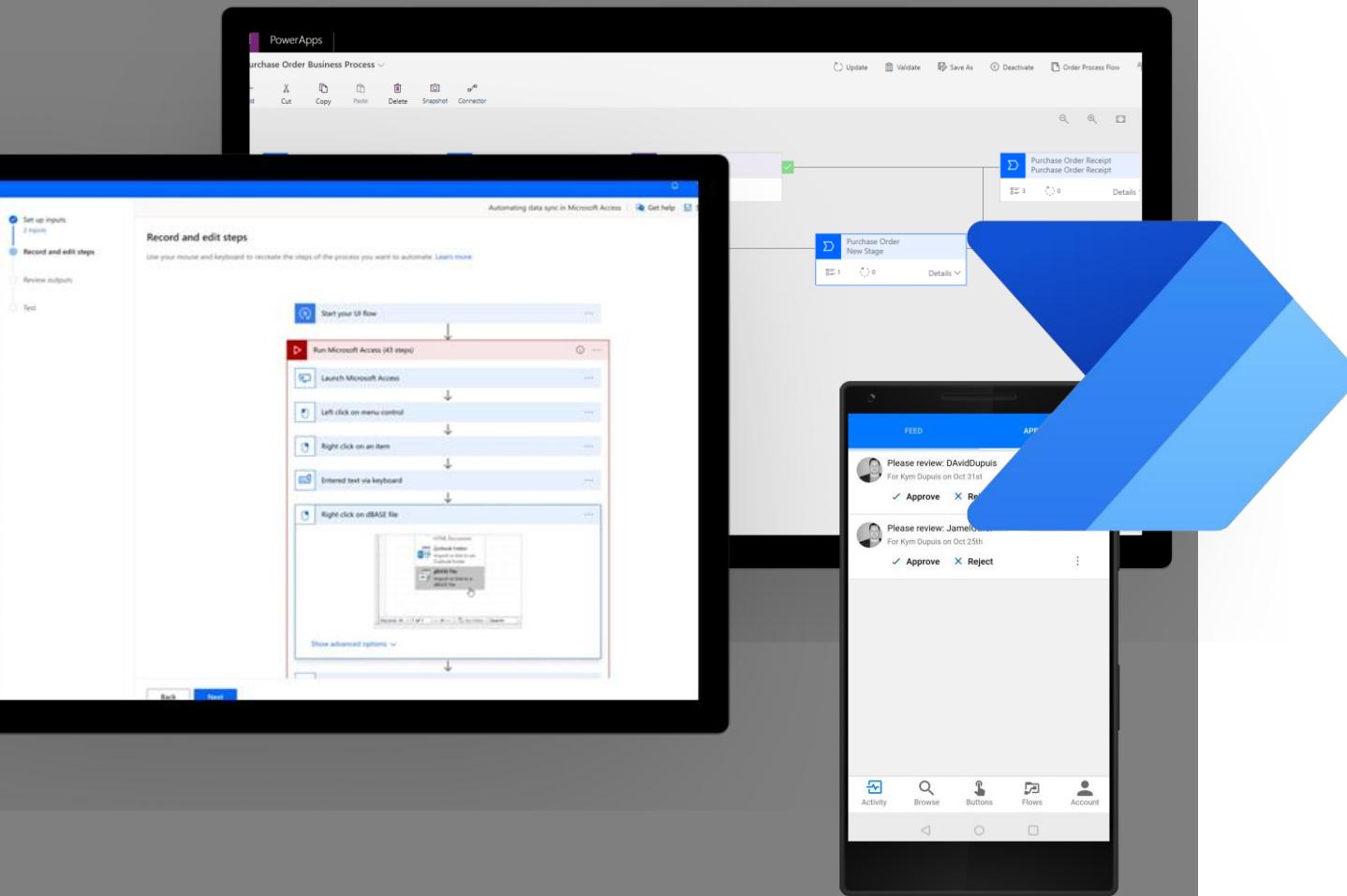
 /turnvirtual

 Cloud Solution Architect  
(Security, Compliance and Identity)

# Low-code tools and what they are good for

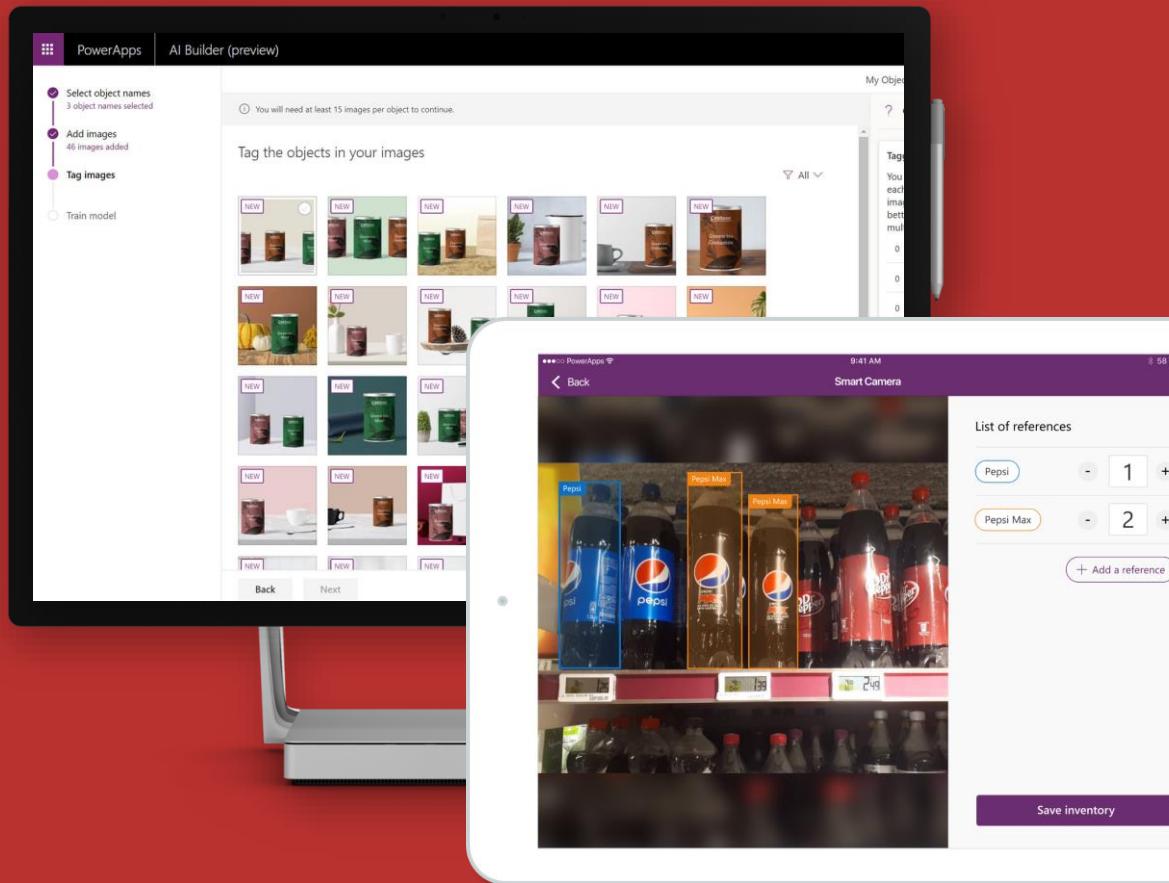


# Automate tasks and business processes workflows with Power Automate



- 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

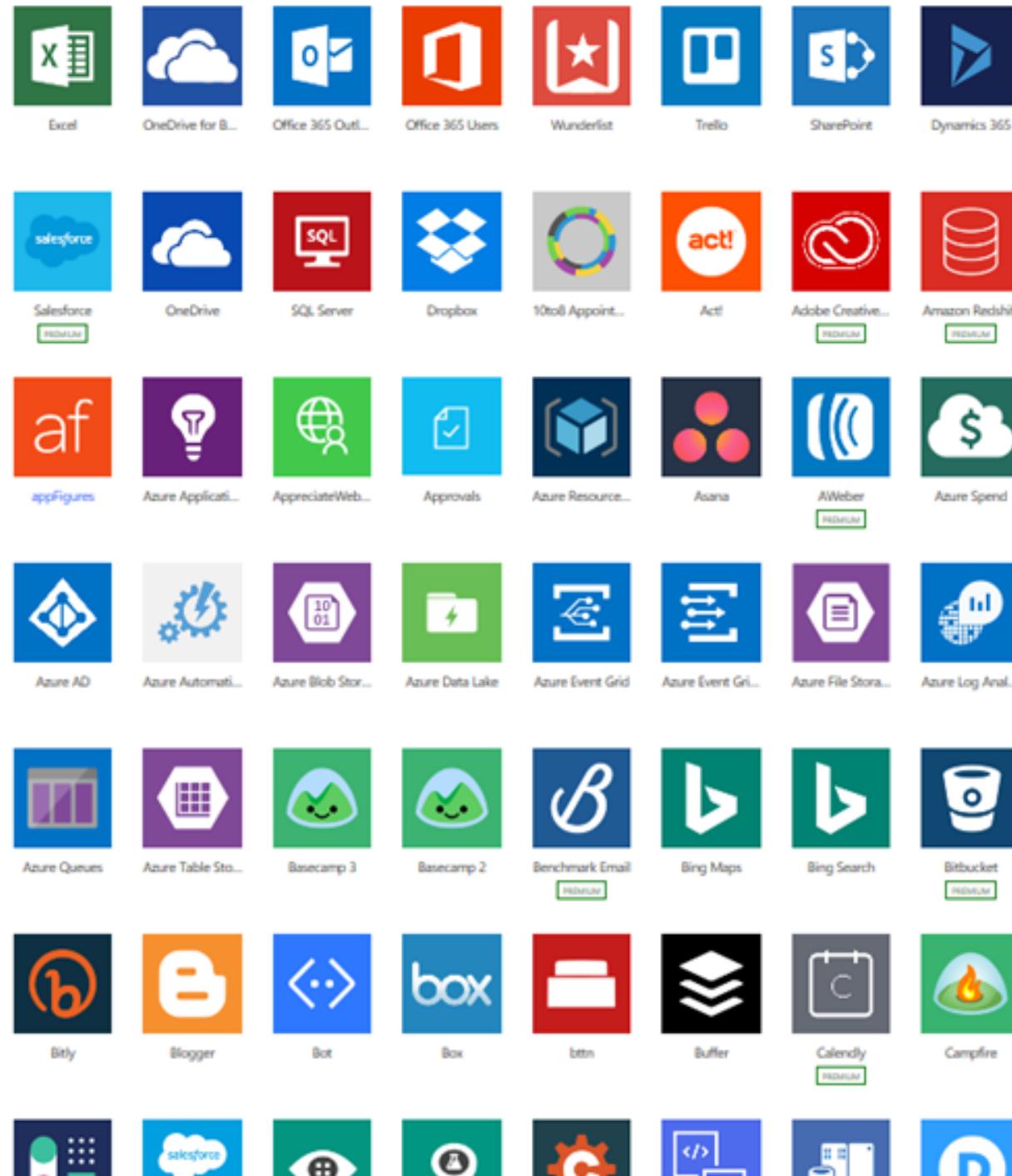
# Infuse artificial intelligence in your business solution with AI Builder



- 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**

# Connect to your company data and services with connectors

- Built-in connectivity to **400+ cloud services**, content services, databases, APIs, etc.
- Seamless hybrid connectivity to on-premises systems via the **On-Premises Data Gateway**
- **Custom Connector** support allows developer / IT systems to register as a building block for citizen developers
- Multiple data sources in a single application for processes that span systems
- **Standard connectors** are included in Office 365 and **Premium and Custom Connectors** are included in Power Apps, Dynamics 365 and Flow Licenses
- **Data Loss Prevention** policies controlled by IT security and platform admins



# Seamless automation across Microsoft 365



A laptop screen displaying a SharePoint document library titled 'Costoso'. The library contains several PDF files named 'invoice-[number].pdf'. A 'Create a flow' overlay is visible, prompting the user to start with a template and create automated tasks between SharePoint data and other apps. It lists options like 'Send a customized email when a new file is added', 'Request manager approval for a selected file', and 'Request approval in Teams for a selected item in SharePoint'.

A laptop screen showing an Excel spreadsheet with columns for First Name, Last Name, Company, Email Address, and ID. A Microsoft Flow overlay is displayed over the spreadsheet, showing actions such as 'Copy data from selected row to Dynamics 365', 'Send an email to a data source', and 'Add a new item to a data source'.

A laptop screen showing a Microsoft Teams chat window. The conversation is between 'Matt Hildinger' and 'Finance Department'. It includes a screenshot of a Microsoft Flow card, a message from Matt Hildinger, and a reply from the Finance Department. The message from Matt includes a link to a GitHub repository for a 'reference documentation'.



Microsoft  
Power Automate

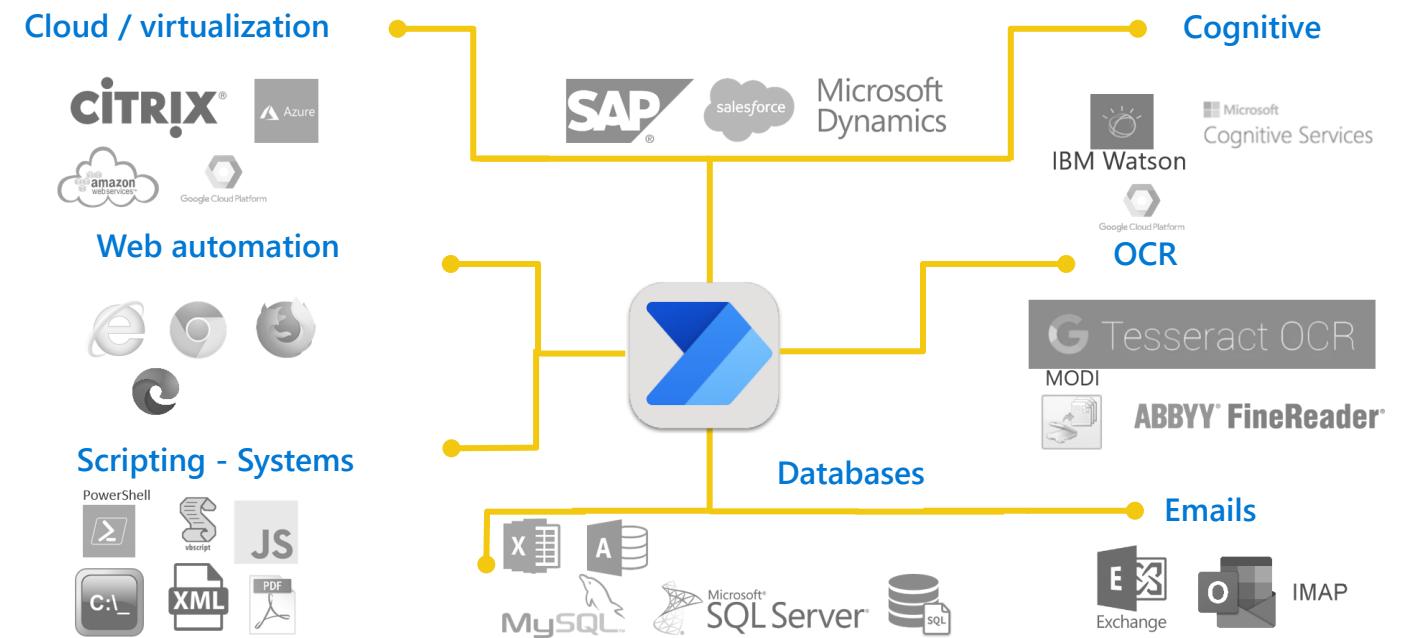
# Bridging automation between the old and new

Robotic process automation (RPA) automates repetitive tasks by recording the user actions in the application and repeating those actions directly in the application user interface



# 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



# Microsoft Ignite RPA Highlight

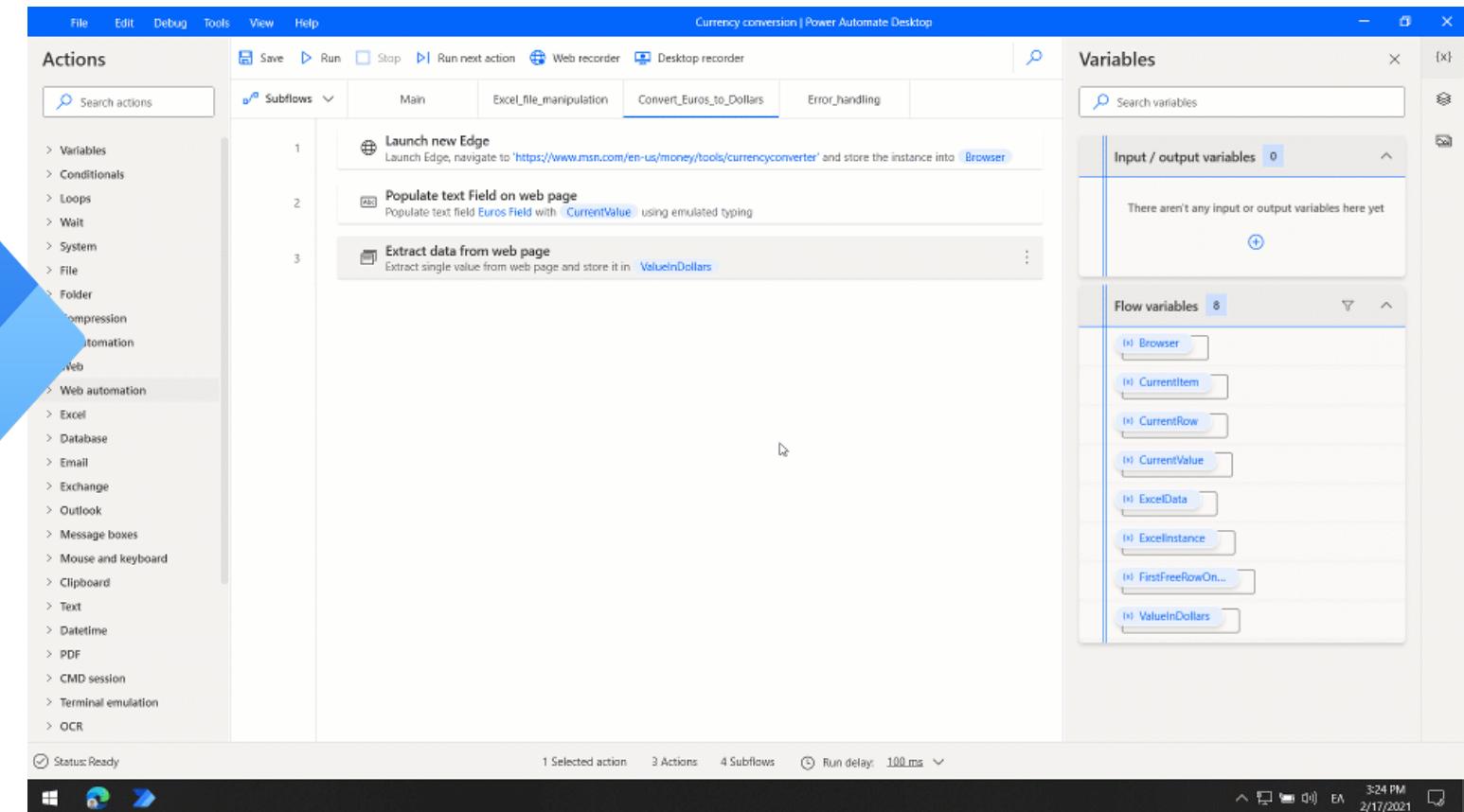
[Power Automate Desktop](#) will be available to Windows 10 users **at no additional cost**

Use Cloud Flows to extend automation even further and access 400+ custom connectors

[Get started with Power Automate Desktop](#)

[Download the Power Automate, Power Apps and Power Virtual Agents Licensing Guides](#)

[Watch the "Automating benefits for the Communications sector" video](#)



# Insider Risk Power Automate Templates (Public Preview)

Insider risk management > Settings

Privacy Policy indicators Policy timeframes Intelligent detections Export alerts (preview) Priority user groups (preview) Priority physical assets (previe

Use Power Automate flows to automatically manage insider risk management processes and tasks. You can create flows here using built-in insider risk management templates, or use the Power Automate console to create custom flows. [Learn more](#)

The screenshot shows the Microsoft Power Automate interface for Insider Risk Management. At the top, there's a navigation bar with links for Privacy, Policy indicators, Policy timeframes, Intelligent detections, Export alerts (preview), Priority user groups (preview), and Priority physical assets (preview). Below the navigation is a section titled "Use Power Automate flows to automatically manage insider risk management processes and tasks. You can create flows here using built-in insider risk management templates, or use the Power Automate console to create custom flows. [Learn more](#)". A "New" button with a plus sign is on the left, and "Install" and "Search" buttons are on the right. The main area displays a list of templates:

- Notify manager of insider risk alerts for user** (Instant, 1 wk ago, By Microsoft)
- Notify manager (CC)** (Instant, 82, By Microsoft)
- Notify manager of insider risk alerts for user** (Instant, 81, By Microsoft)
- Notify users when they're added to an insider risk policy** (Instant, 61, By Microsoft)
- Request info from HR or business about a user in an insider risk case** (Instant, 50, By Microsoft)
- Add a calendar reminder to follow-up on an insider risk case** (Instant, 22, By Microsoft)
- Add a calendar reminder to follow-up on a privacy management case** (Instant, 15, By Microsoft Power Automate Community)
- Create record for insider risk case in ServiceNow** (Instant, 7, By Microsoft)

**LICENCE** - Microsoft 365 subscriptions that **include** insider risk management **do not need additional Power Automate licenses** to use the recommended insider risk management Power Automate templates



# Demo



# RPA Early Adopter Program



# What we need from you

## Our asks

### **Enroll & Learn:** Pass all Power Automate MS Learn Modules

- Pre-sales: [Catalyst Partner Learning Module](#)
- Business Training: [Introduction to Power Automate - Learn | Microsoft Docs](#)
- Technical Training: [RPA/PartnershipLearn \(aka.ms\)](#)
- Fundamentals & Expert Technical Training: Early CY 2021

### **Prove Expertise:** Proof of Power Automate product experience or past deployment

- FlowIDs, EnvironmentIDs, PAL association
- Publish AppSource Consulting Offers for Power Automate

### **Engage Customer:** Proof of upcoming/ ongoing customer deployment

- SoW, MSX (or PC Opp), Customer Contact

### **Celebrate Success:** Present deployment story

- Get customer permission for sharing within Microsoft

# What we give you in return

Your “gets”!

## Microsoft Assets

- [Microsoft Partner Community](#)
- Bill of Materials
- 1:Many RPA in a Day - Presales Activities  
<https://aka.ms/RPAinaDayPackage>
- NDA Community – early disclosures
- Technical assets
- Internal Production License for RPA for 6 months (deploy, test, train)  
*\*Once proof of completing the learning and proving expertise, production license will be provided*
- Monthly Tech-syncs with SI Success & Buddy to De-risk Deployments
- Publish RPA Partner Success Story
- Recommended as a Deployment partner to the Microsoft field (only top 10)

Join us  
10 am – 12 pm  
3<sup>rd</sup>, 4<sup>th</sup> & 5<sup>th</sup> May

# What you can offer your customer

## What we offer together

### Microsoft Assets

- [Microsoft Partner Community](#)
- Free RPA in a Day
  - Live, lab-led training
  - All Train-the-Trainer and lab assets
- Self-service search for RPA offers on AppSource (when co-sell ready)
- Expert partner engaged
- Monthly Tech-syncs with CAT Buddy to De-risk Deployments
- Direct connection with Engineering
- Future customers get qualified partner recommendations



 @AnaDemeny

 /anademeny

 Partner Technical Architect  
(INTEGRATION & RPA)

Thank  
you!  
△ !



Ally Turnbull

 /turnvirtual

 Cloud Solution Architect  
(Security, Compliance and Identity)

Break 1  
Please return at  
**12:00pm BST**  
(British Summer  
Time)

---



# Power Virtual Agents

Partner Technical Architect

**Mark Oburoh**

@thatguymarko 

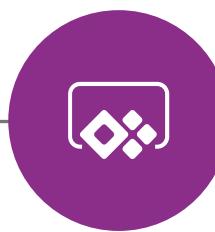


# Microsoft Power Platform

The low-code platform that spans Office 365, Azure, Dynamics 365, and standalone applications  
**Innovation anywhere. Unlocks value everywhere.**



**Power BI**  
Business analytics



**Power Apps**  
Application development



**Power Automate**  
Process automation



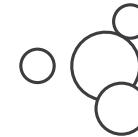
**Power Virtual Agents**  
Intelligent virtual agents



**Data connectors**



**Portals**



**AI Builder**



**Dataverse**

# Efficient and secure data integration and storage

Power virtual agents is built on the Microsoft Dataverse \*formally Common Data Service (CDS)

Microsoft Dataverse lets you securely store  
and manage data that's used by business applications.

Dynamics 365

Office 365

Mobile Apps

Web Apps



Power Apps



Power Automate



Power BI



Power Virtual Agents



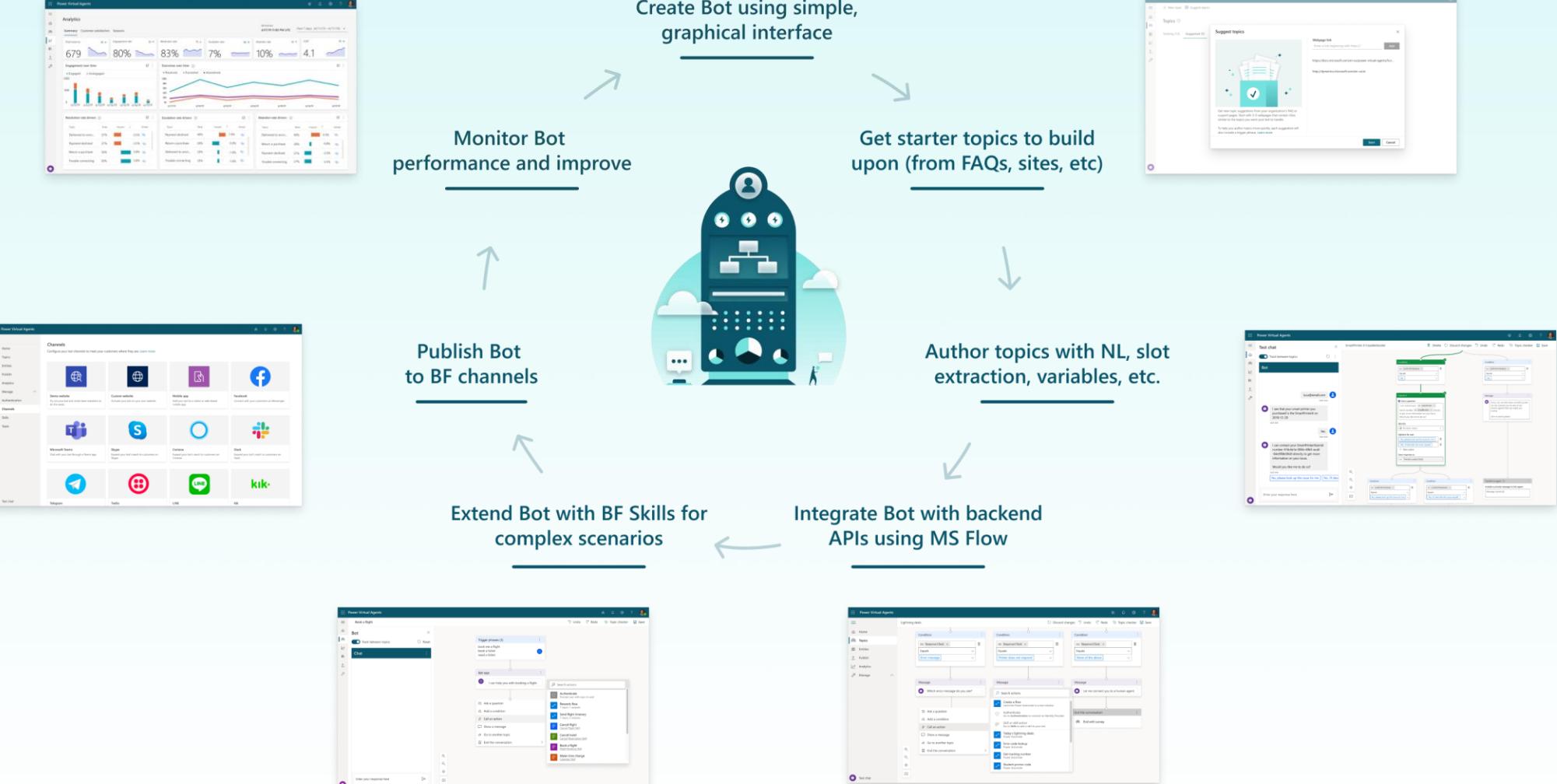
Dataverse



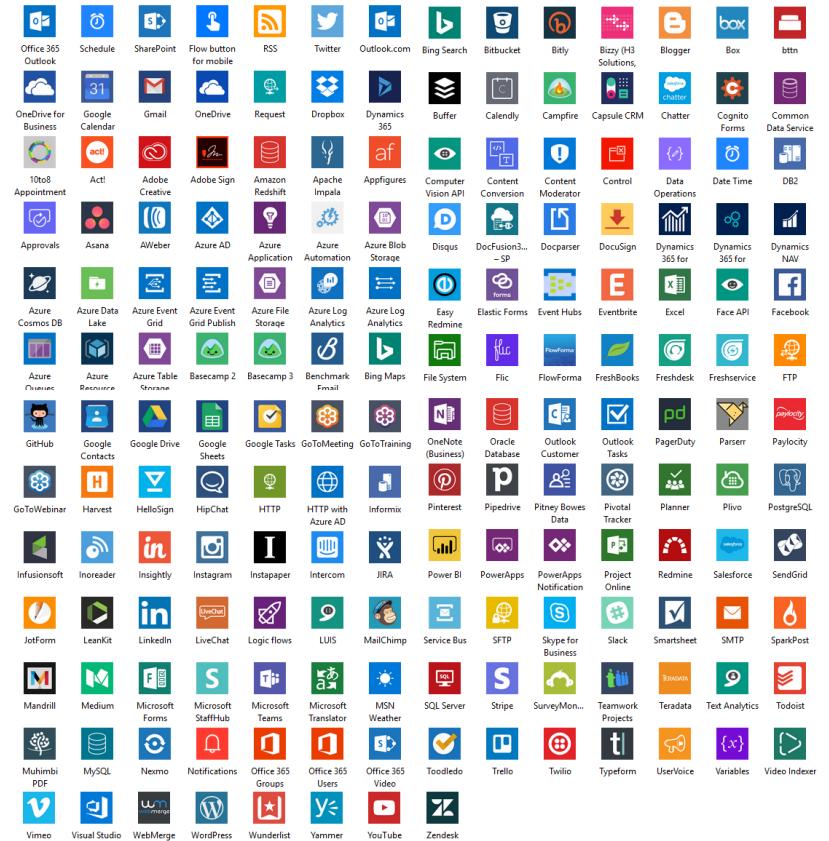
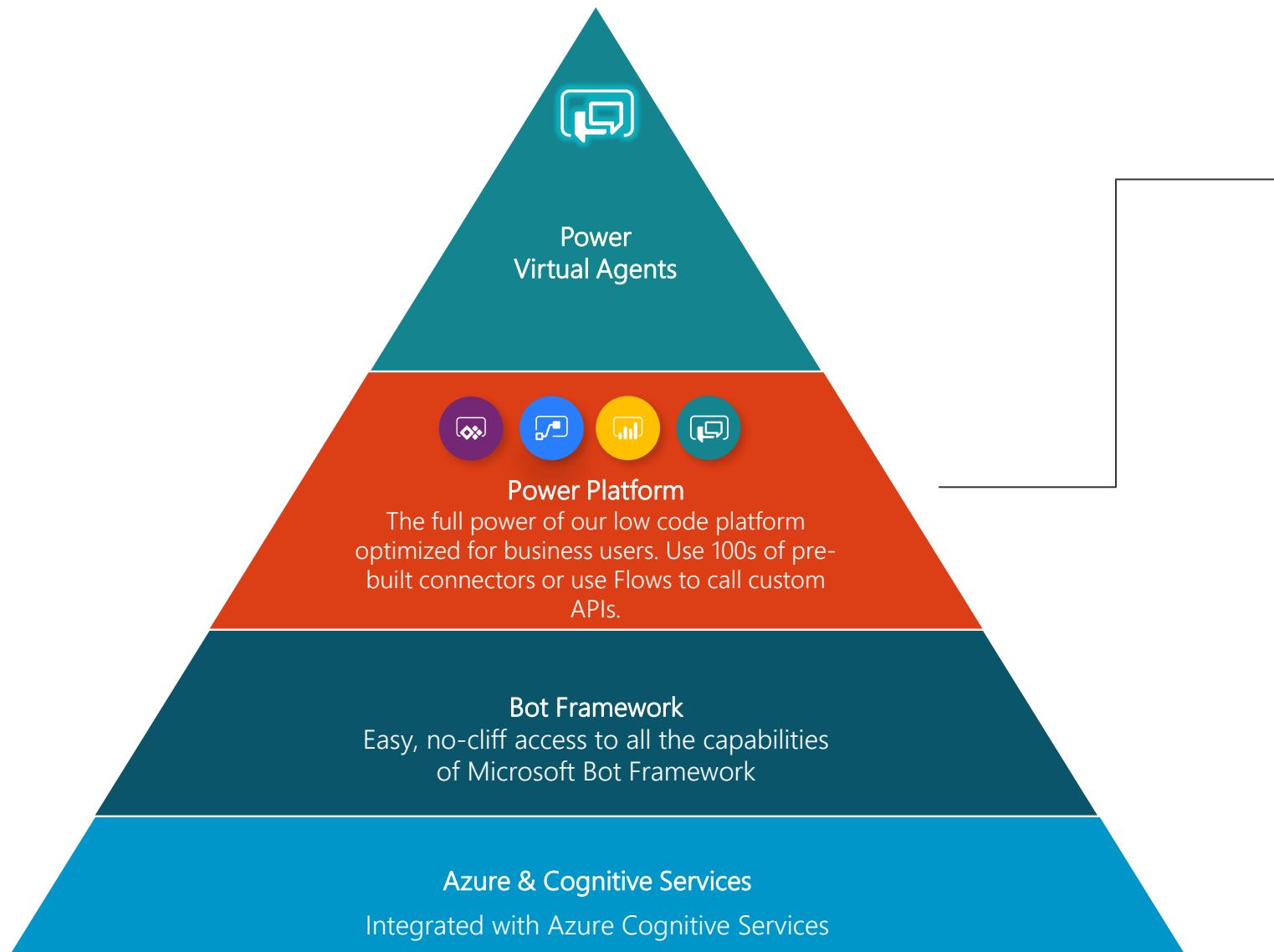
Data connectors

Azure

# Power Virtual Agents Lifecycle



# Built on Power Platform & Bot Framework



# Making Bots Easy

## Simple, graphical bot creation

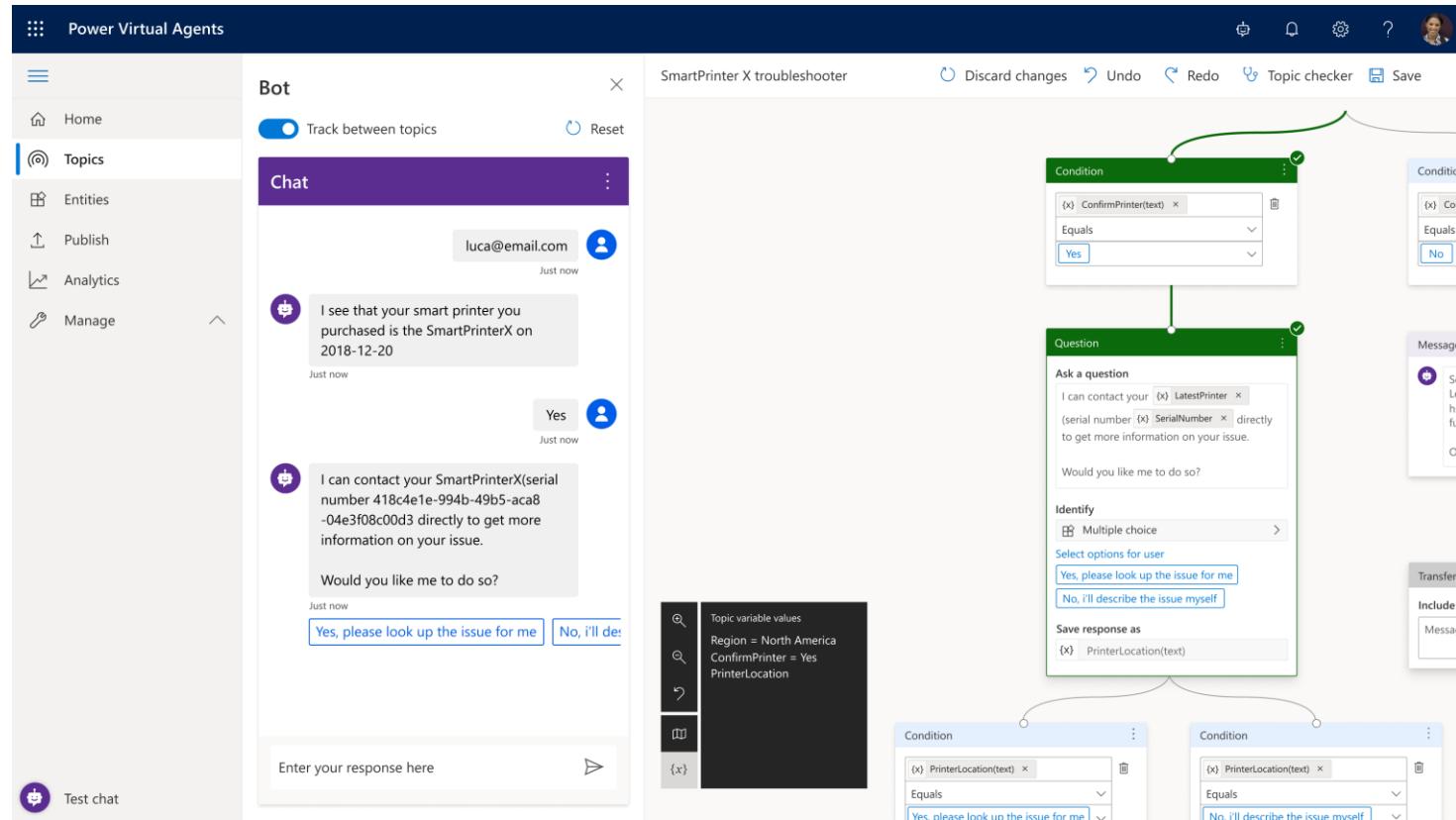
Easily test and maintain bots through a simple, easy to use graphical interface

## Extract information from user responses

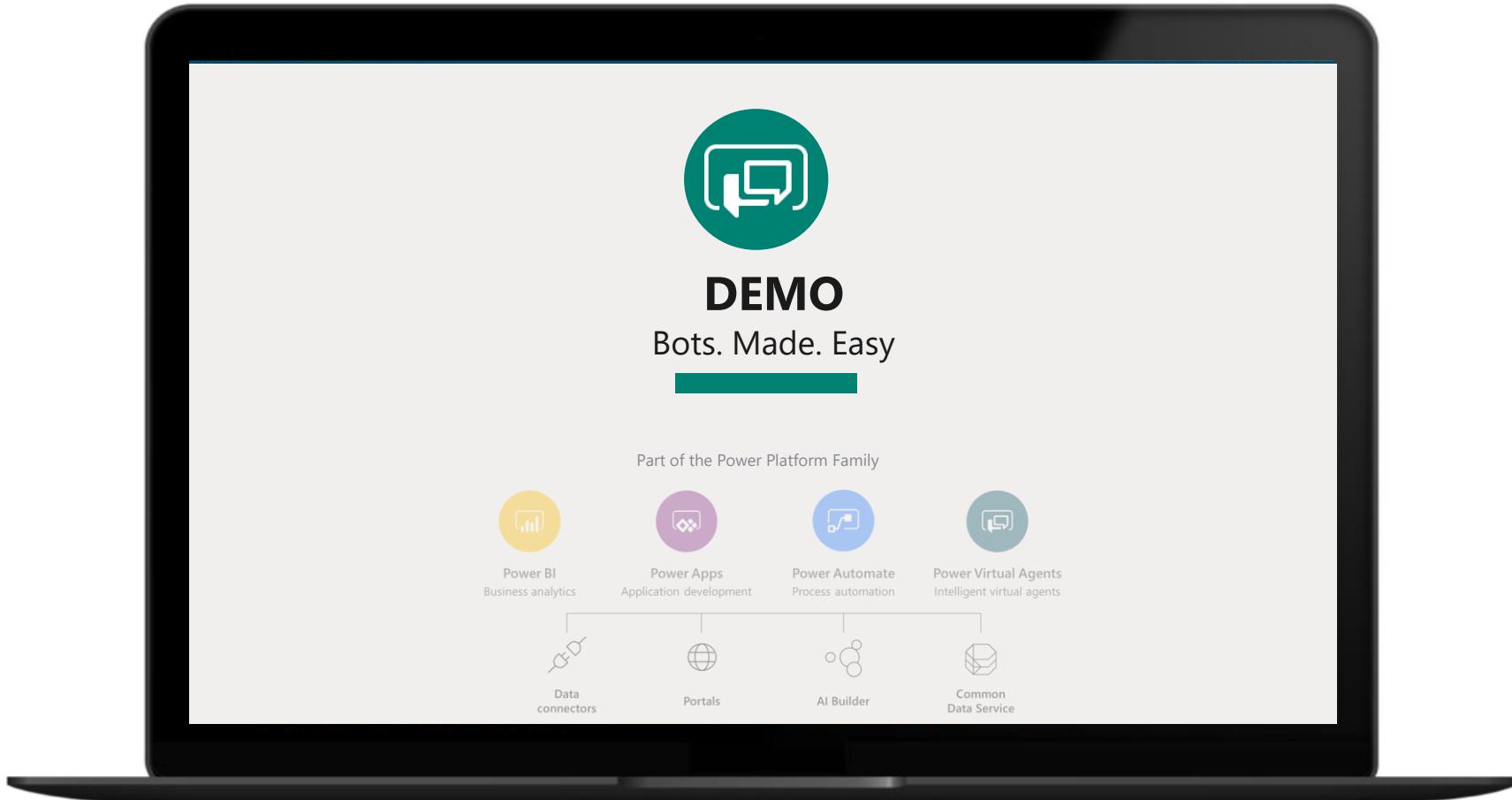
Recognize, extract, and act on dozens of common entities in a user's responses. For example, colors, currencies, ages, dates and times. Or create your own custom entities, e.g. model numbers

## Remember user responses

Store user information for use later in variables and use them to branch or create complex conversations



# Making Bots Easy - DEMO



# Building chatbots with Power Virtual Agents

- **Democratize AI** Empower your business users to easily create powerful bots using a guided, no-code graphical interface. No need for developers or data scientists.
- **Faster, Better Bot Building**  
Make building and keeping a bot up-to-date bot faster. No need for IT or dev teams to maintain the bot lifecycle
- **SaaS - No Infrastructure Complexity & Cost**  
No need to deal with hosting or complex, costly infrastructure. Build, deploy, host and manage your bot – all using our intuitive web interface
- **Available everywhere**  
Add your bot anywhere you engage with customers: website, mobile app, Facebook, Teams or more.
- **Engage Naturally**  
Engage with customers and employees conversationally. Resolve routine issues easily, freeing up staff to focus on complex matters
- **Get Started Easily**  
Point the AI to your website, and automatically build topics to get started with a few clicks using Microsoft Q&A Maker technology
- **Continuously Improve**  
As the bot gets used, powerful metrics and insights help tell you what topics to build next.
- **Take Action**  
Connect to your backend with a few clicks using the 100s of Power Platform connectors – or call APIs and custom workflows using Flow.
- **Access to the full power of Bot Framework**  
Built in access to the full power of Microsoft Bot Framework's Skills, Adaptive Dialogs and Cognitive Services.
- **No need to train custom models**  
Semantic embedding eliminates the need for data scientists or complex model tuning

# Multi Channel

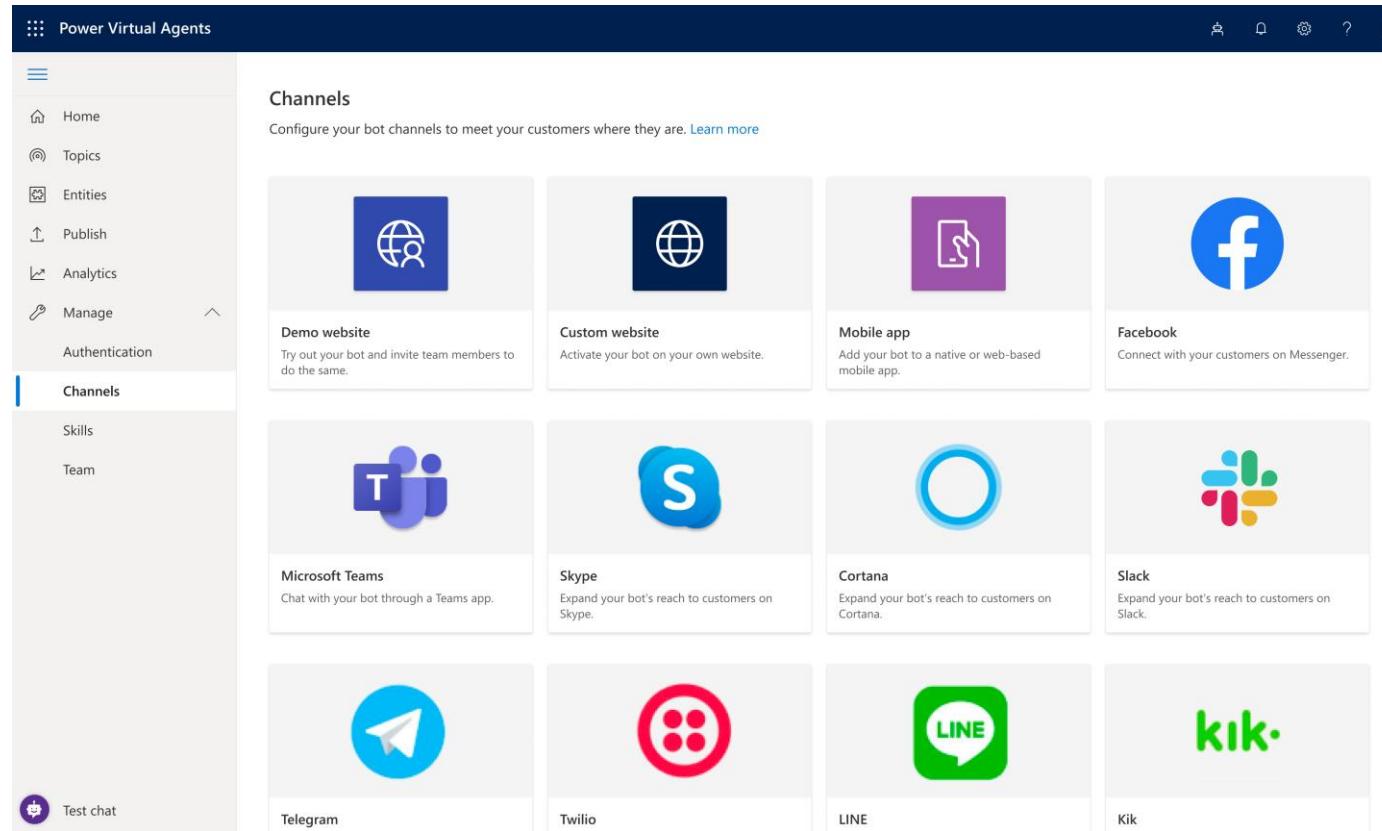
Use bots wherever you need them:

## Configure and deploy to multiple channels

Easily embed your bot wherever your organization engages with customers: websites, mobile apps, Facebook, Teams or any of the dozens of channels supported by Bot Framework

## Deploy to demo sites with a single click

Test and gain feedback by deploying your bot to a demo website and sharing it internally with colleagues, before embedding it to your own website when ready



# Power Virtual Agents for Teams vs Power Virtual Agents Standalone



## PVA for Teams (seeded)

Only seeded in Teams (not Office 365). Can only build, publish and use the Teams native experience with no restriction to number of sessions.

## PVA standalone

Access premium connectors for flows and host intelligent bots externally from Teams, through other channels including web.

The screenshot shows the Power Virtual Agents web application. On the left, a sidebar includes icons for Activity, Chat, Teams, Calendar, Calls, Files, and Power Virtual Agents. The main content area has a header "Power Virtual Agents" with tabs for Home, Chatbots, and About. Below the header, there's a section titled "Build collaboration, one chat at a time" with a "Start now" button. To the right, there are four cards: "Learn more" (Power Virtual Agents quickstart), "Publish your bot" (Configure the bot to your preferred channels), "Improve with analytics" (Monitor bot performance), and "Find new topics with AI" (Scan documentation or support assets for suggestions). A large screenshot of the bot builder interface is visible on the far right.

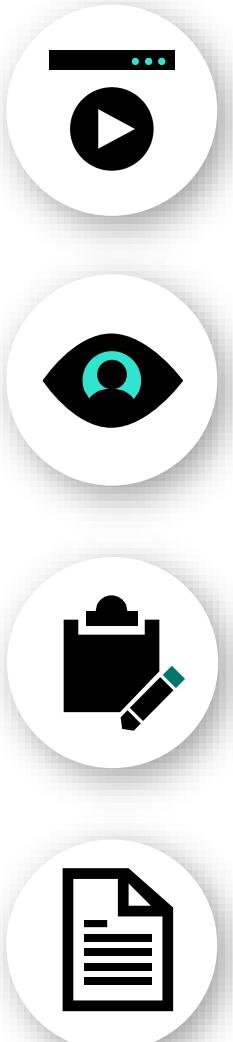
# Learn more about Microsoft Power Virtual Agents

Visit [Power Virtual Agents](#) page  
to learn more and request a demo

Technical details about the  
application are available in our  
[help documentation](#)

For questions please engage in  
our [Community forum](#)

Power Virtual Agents Product  
[Blog](#) and [Yammer group](#)

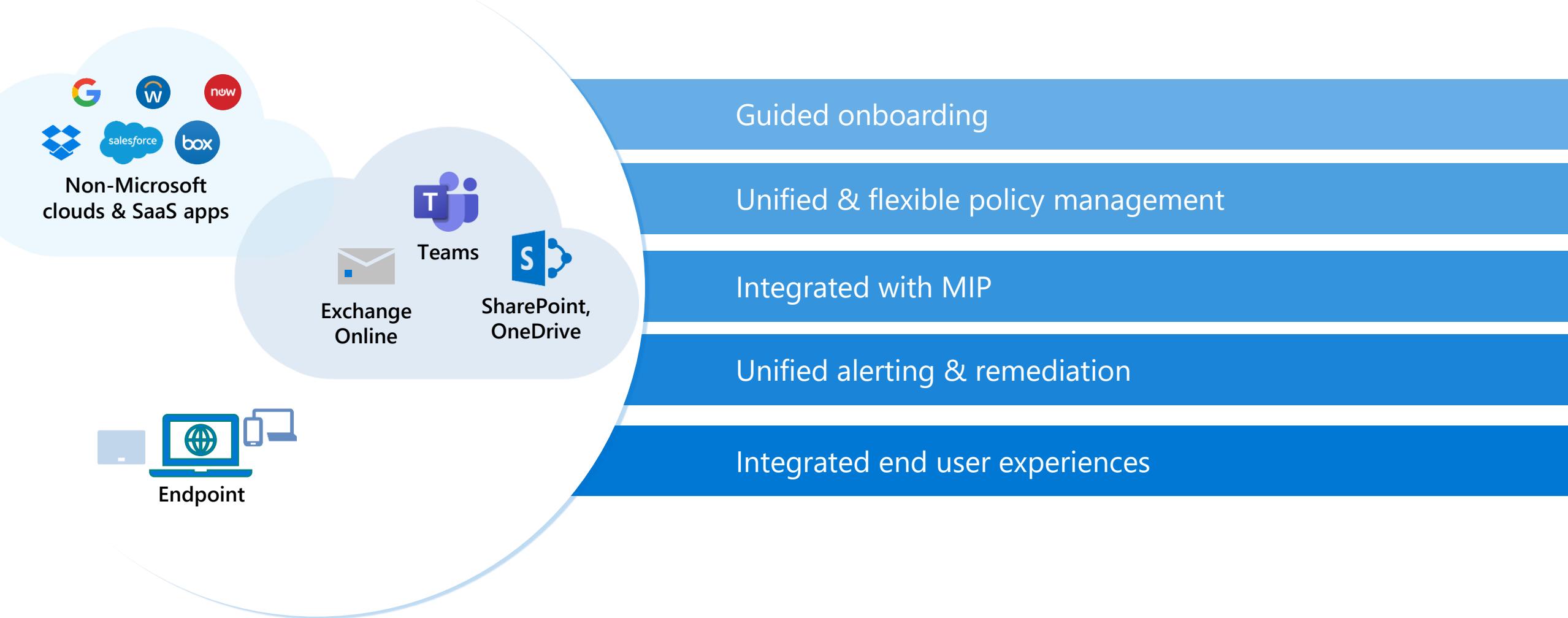


# Advanced DLP Monitoring with Sentinel



# Data Loss Prevention

Comprehensive support across workloads with unified and integrated experiences



What reporting is available?

Can reporting be customised?

How do I investigate an incident?

Can I integrate with XYZ data?

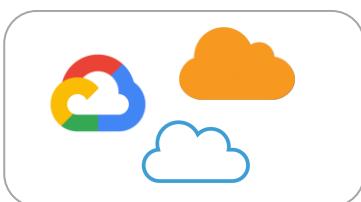
## Data sources



SecurityEvent, DNS,  
Windows FW, DHCP



Alerts, Events



API



REST API



CEF 514



Syslog



Azure Log Analytics Agent

# Azure Sentinel

View      Detect      Manage      Investigate      Respond      Hunt



Dashboards



Custom  
security alerts



Custom dashboards



Automation  
&  
orchestration



Machine learning, notebooks,  
bookmarks, community



Community



ActivityFeed-AzureFunction

https://github.com/OfficeDev/O365-ActivityFeed-AzureFunction/tree/master/Sentinel/EndPointDLP\_preview

Why GitHub? Team Enterprise Explore Marketplace Pricing

Search / Sign in Sign up

OfficeDev / O365-ActivityFeed-AzureFunction

Code Issues 1 Pull requests Discussions Actions Projects Security Insights

master Go to file

jonnords Update BlobtoSPO.json ... ✓ 9deba0a on 8 Mar History

..

Analytics Delete DLPToAnalyticsRuleEndpoint.ps1 6 months ago

DocumentCopy Update BlobtoSPO.json last month

Report Added Device pivoted view 7 months ago

QueueDLPEvents.ps1 Updated cursor handling 2 months ago

SensitiveInfoType.ps1 Create SensitiveInfoType.ps1 8 months ago

StoreEndpointDLPEvents.ps1 Update StoreEndpointDLPEvents.ps1 6 months ago

deploysentinelfunction.json Update deploysentinelfunction.json 7 months ago

enablesubscription.ps1 Update enablesubscription.ps1 7 months ago

endpointdlpservice.zip Updated function to handle incorrect timestamp 2 months ago

readme.md Update readme.md 6 months ago

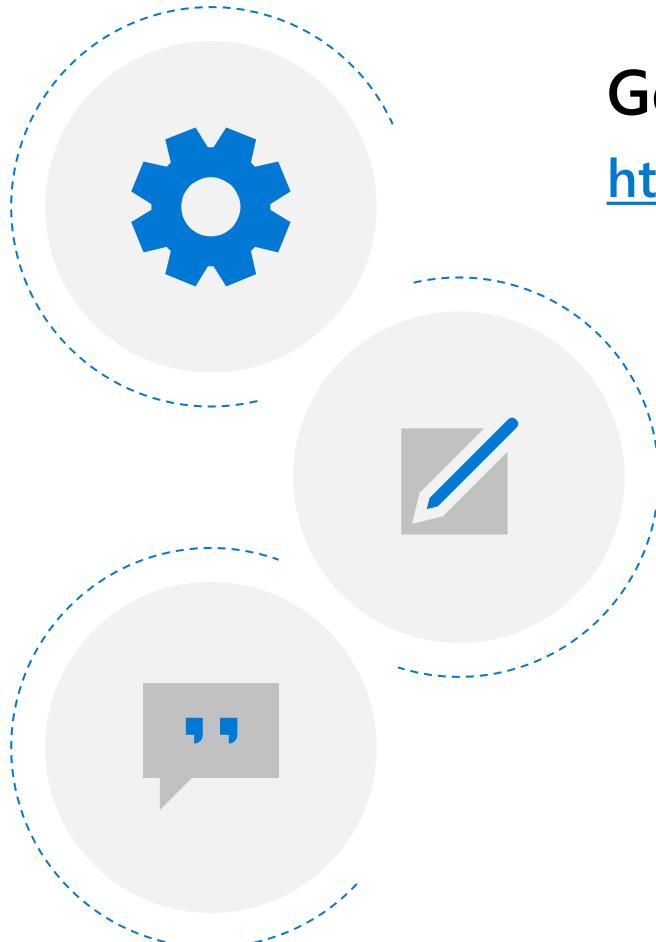
readme.md

Deploy to Azure

page\_type: sample products:

- office-365

# Next Steps



## Getting Started with Azure Sentinel

<https://azure.microsoft.com/en-gb/services/azure-sentinel>

## DLP Reporting Sample GitHub Repository

[https://github.com/OfficeDev/O365-ActivityFeed-AzureFunction/tree/master/Sentinel/EndPointDLP\\_preview](https://github.com/OfficeDev/O365-ActivityFeed-AzureFunction/tree/master/Sentinel/EndPointDLP_preview)



# Azure Purview

UNIFIED DATA GOVERNANCE TO MAXIMIZE  
THE BUSINESS VALUE OF DATA





Watch @ [aka.ms/purview/L100](https://aka.ms/purview/L100)

Now Available On-Demand

# Data Governance with Azure Purview

Register & Scan

Search & Browse

Lineage

Glossary

Insights

Classifications

Integration with Synapse Analytics



[aka.ms/purview/L100](https://aka.ms/purview/L100)

# Data is your most strategic asset

90%

Of corporate strategies will  
cite information as a critical  
enterprise asset by 2022

GARTNER

*Why Data and Analytics are key to digital transformation. Christy Pettey. Mar, 2019*

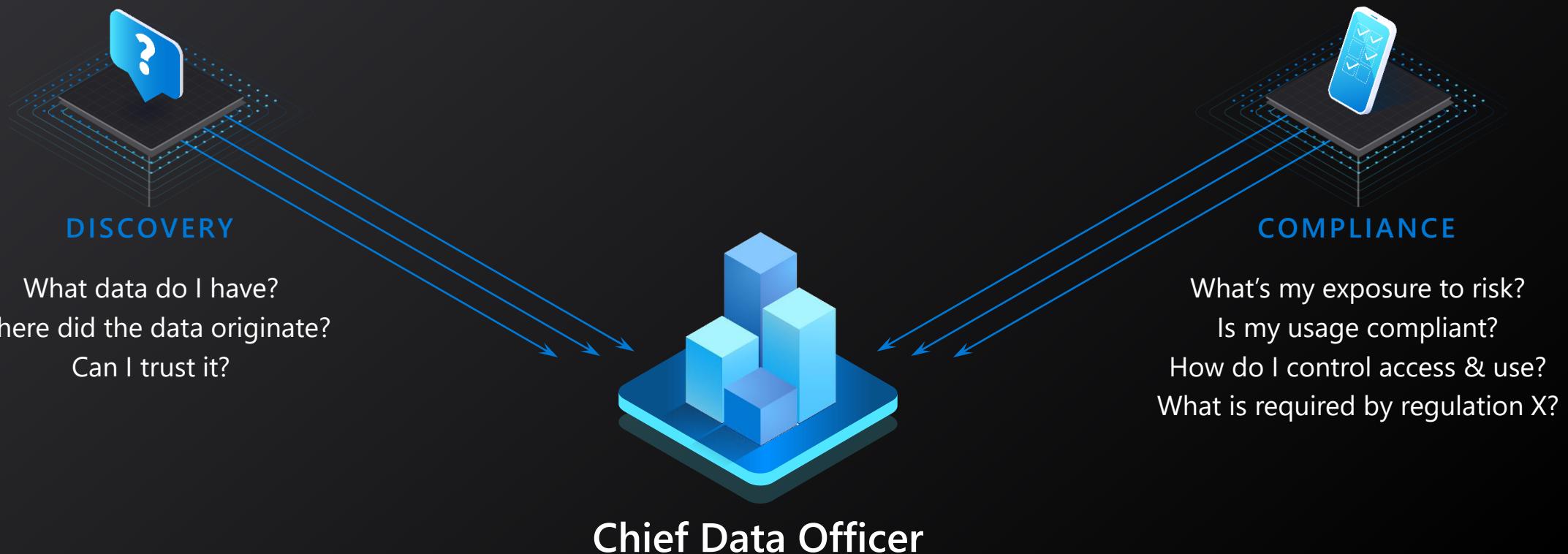
175 ZB

Expected global volume of  
data generated annually  
by 2025

IDC

*IDC Data Age 2025, Dave Reinsel,*

# Data governance is becoming increasingly interdisciplinary



# Azure Purview

## UNIFIED DATA GOVERNANCE

### Data Map

- Automate and manage metadata at scale

---

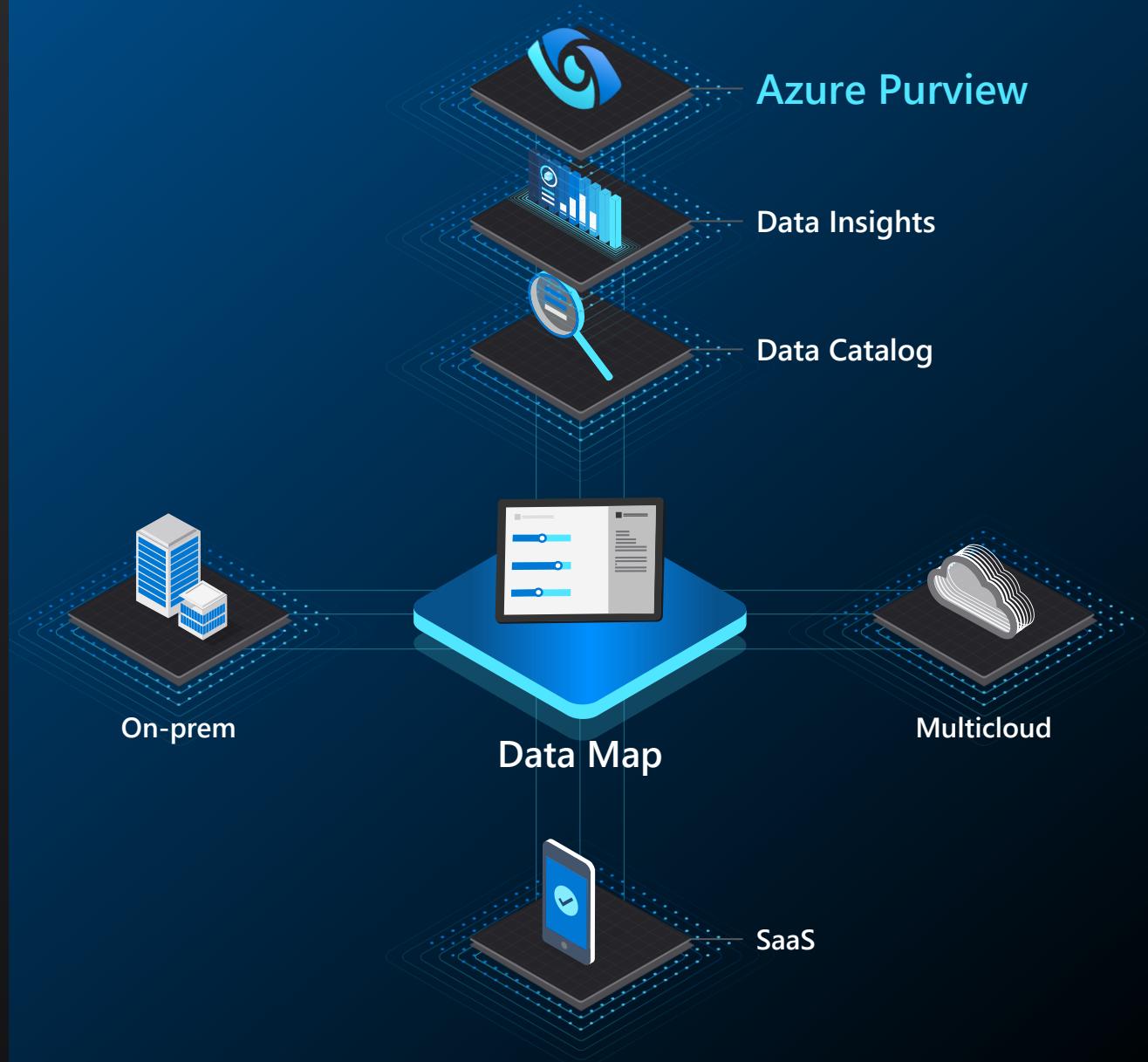
### Data Catalog

- Enable effortless discovery for data consumers

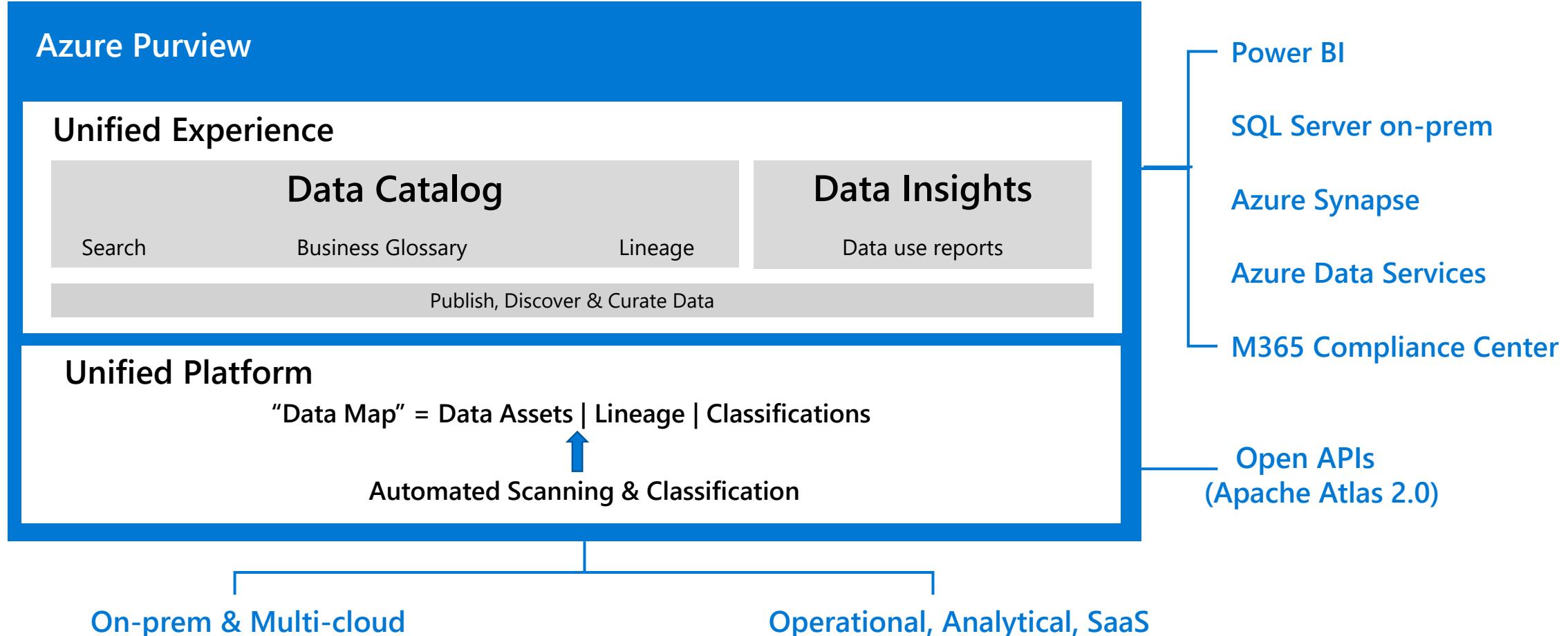
---

### Data Insights

- Assess data usage across your organization



# Azure Purview: Unified Data Governance





# Azure Purview

## Demo



# Sensitivity Labels

## Security & Compliance Center

- » General
- Account information
- Scan rule sets
- Integration runtimes
- Metrics
- Metadata management
- Classifications**
- Classification rules
- Resource sets
- Scoped resource sets
- External connections
- Data Factory
- Data Share
- Security and access
- Access control
- Credentials

## Classifications

New Edit Delete Refresh

System Custom

These are the system provided classifications.

Filter by name...

Display name	Formal name	Description
ABA Routing Number	MICROSOFT.FINANCIAL.US.ABA_ROUTING_NUMB...	ABA Routing Number
Age of an individual	MICROSOFT.PERSONAL.AGE	Age of an individual
Argentina National Identity (DNI) Number	MICROSOFT.GOVERNMENT.ARGENITNA.DNI_NU...	Argentina National Identity (DNI) Number
Australia Bank Account Number	MICROSOFT.FINANCIAL.AUSTRALIA.BANK_ACCOU...	Australia Bank Account Number
Australia Driver's License Number	MICROSOFT.GOVERNMENT.AUSTRALIA.DRIVERS_L...	Australia Driver's License Number
Australia Medical Account Number	MICROSOFT.GOVERNMENT.AUSTRALIA.MEDICAL_...	Australia Medical Account Number
Australia Passport Number	MICROSOFT.GOVERNMENT.AUSTRALIA.PASSPORT...	Australia Passport Number
Australia Tax File Number	MICROSOFT.GOVERNMENT.AUSTRALIA.TAX_FILE_...	Australia Tax File Number
Belgium National Number	MICROSOFT.GOVERNMENT.BELGIUM.NATIONAL_...	Belgium National Number
Brazil Individual Taxpayer Identification Number (C...	MICROSOFT.GOVERNMENT.BRAZIL.CPF_NUMBER	Brazil Individual Taxpayer Identification Number (CPF)

[Home](#)[Compliance Manager](#)[Data classification](#)[Data connectors](#)[Alerts](#)[Reports](#)[Policies](#)[Permissions](#)

#### Solutions

[Catalog](#)[Application protection and gover...](#)[Audit](#)[Content search](#)[Communication compliance](#)

## Data classification

[Overview](#)   [Trainable classifiers](#)   [Sensitive info types](#)   [Exact data matches](#)   [Content explorer](#)   [Activity explo](#)

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we

[+ Create sensitive info type](#)   [⟳ Refresh](#)

Name ↑	Type	Publisher
ABA Routing Number	Entity	Microsoft Corporation
Argentina National Identity (DNI) Number	Entity	Microsoft Corporation
Argentina Unique Tax Identification Key (CUIT/CUIL)	Entity	Microsoft Corporation
Australia Bank Account Number	Entity	Microsoft Corporation
Australia Driver's License Number	Entity	Microsoft Corporation
Australia Medical Account Number	Entity	Microsoft Corporation
Australia Passport Number	Entity	Microsoft Corporation
Australia Tax File Number	Entity	Microsoft Corporation

[Home](#)[Compliance Manager](#)[Data classification](#)[Data connectors](#)[Alerts](#)[Reports](#)[Policies](#)[Permissions](#)

## Solutions

[Catalog](#)[Application protection and gover...](#)

# Information protection

[Labels](#)   [Label policies](#)   [Auto-labeling](#)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected according to the label's settings. You can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

(i) Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn on here, but no changes will be made until you do.

(i) You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first [complete these steps](#) to enable the feature.

[+ Create a label](#)   [Publish labels](#)   [Refresh](#)

Name	Order	Scope	Created by
Highly Confidential	... 0 - highest	File, Email, PurviewAssets	Taygan Rifat

- >> Insights
- Assets
- Scans
- Glossary
- Classification
- Sensitivity labels
- File extensions

## Sensitivity label insights

View information about how sources, files, and tables have been labeled.

### Overview of sources with sensitivity labels

Subscriptions

2

Unique labels found

3

Sources labeled

6

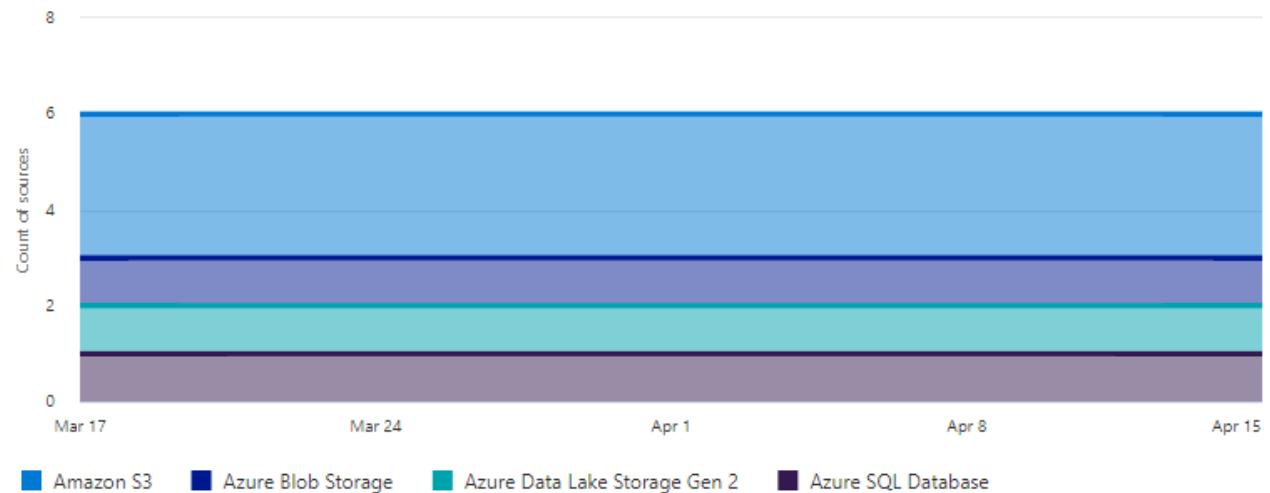
Files labeled

50

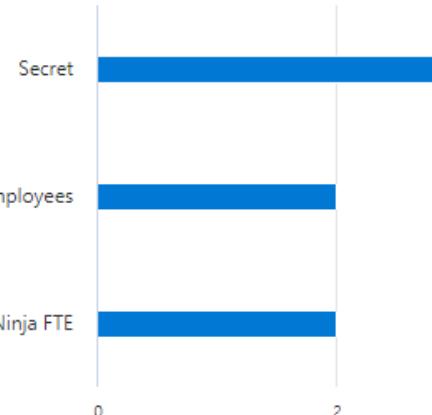
Tables labeled

1

### Top sources with labeled data (last 30 days)



### Top labels applied across sources



[View more](#)

## Supported data types for sensitivity labels in Azure Purview

Sensitivity labels are supported in Azure Purview for the following data types:

Data type	Sources
Automatic labeling for files	<ul style="list-style-type: none"><li>- Azure Blob Storage</li><li>- Azure Data Lake Storage Gen 1 and Gen 2</li></ul>
Automatic labeling for database columns	<ul style="list-style-type: none"><li>- SQL server</li><li>- Azure SQL database</li><li>- Azure SQL Database Managed Instance</li><li>- Azure Synapse</li><li>- Azure Cosmos DB</li></ul> <p>For more information, see <a href="#">Labeling for SQL database columns</a> below.</p>

Information protection - Microsoft

.compliance.microsoft.com/informationprotection?viewid=sensitivityla...

Contoso Electronics Microsoft 365 compliance Diagnostics

Data loss prevention Data subject requests eDiscovery Information governance Information protection Insider risk management Records management Privacy management Settings

# Information protection

Labels Label policies Auto-labeling

New feature in preview

## Extend labeling to assets in Azure Purview

When you turn on labeling for Azure Purview, you'll be able to apply your Microsoft 365 sensitivity labels to assets such as SQL columns, files in Azure Blob Storage, and more. [Learn more about labeling for Azure Purview](#)

Turn on

Microsoft 365 Compliance Center > Information Protection > Labels

## New sensitivity label

### Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

### Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name \* ⓘ

General

Display name \* ⓘ

General

Description for users \* ⓘ

Business data that is not intended for public consumption. However, this can be shared with external partners, as required. Examples include a company internal telephone directory, organizational charts, internal standards, and most internal communication.

Description for admins ⓘ

Enter a description that's helpful for admins who will manage this label

## New sensitivity label

Name & description

**Scope**

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

### Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

**Files & emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

(i) To set up auto-labeling for files in Azure, make sure you also scope this label to 'Azure Purview assets' below.

**Groups & sites**

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

(i) To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first [complete these steps](#) to enable the feature.

**Azure Purview assets (preview)**

Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

## New sensitivity label

- Name & description
- Scope
- Files & emails**
- Groups & sites
- Azure Purview assets (preview)
- Finish

### Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

**Encrypt files and emails**

Control who can access files and emails that have this label applied.

**Mark the content of files**

Add custom headers, footers, and watermarks to files and emails that have this label applied.

## New sensitivity label

Name & description

Scope

Files & emails

Auto-labeling

Groups & sites

Azure Purview assets (preview)

Finish

### Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. [Learn more about auto-labeling for Microsoft 365](#)

Because this label is scoped to assets in Azure Purview, we'll also apply it to files in Azure Blob Storage that match the same conditions. [Learn more about auto-labeling in Azure Purview](#)

(i) To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. [Learn more about auto-labeling policies](#)

### Auto-labeling for files and emails



#### detect content that matches these conditions

##### Content contains

Default

All of these



##### Sensitive info types

Credit Card Number

High confidence



Instance count

1

to Any



Add

Create group

## New sensitivity label

Name & description

Scope

Files & emails

Groups & sites

Azure Purview assets (preview)

Finish

### Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers.  
[Learn more about these settings](#)

**Privacy and external user access settings**

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

**External sharing and Conditional Access settings**

Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.

## New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- Finish

### Auto-labeling for database columns

Automatically apply this label to Azure database columns (such as SQL, Synapse, and more) that contain the sensitive info types you choose here. [Learn more about auto-labeling for database columns](#)

#### Auto-labeling for database columns



Content contains any of these sensitive info types  
Credit Card Number

[Edit](#)

## New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Azure Purview assets (preview)
- 



### Review your settings and finish

#### Name

General

[Edit](#)

#### Display name

General

[Edit](#)

#### Description for users

Business data that is not intended for public consumption. However, this can be shared with external partners, such as customers, suppliers, and business partners. This includes internal telephone directory, organizational charts, internal standards, and most internal business documents.

[Edit](#)

#### Scope

File,Email,PurviewAssets

[Edit](#)

#### Content marking

[Edit](#)

#### Auto-labeling

Automatically apply the label

[Edit](#)

#### Group settings

[Edit](#)

#### Site settings

[Edit](#)

#### Auto-labeling for database columns

Automatically apply

[Edit](#)

[Back](#)

[Create label](#)

# Make the most of your Microsoft investments



Multi-cloud,  
Hybrid, and SaaS



Operational and  
Analytical data



# 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.



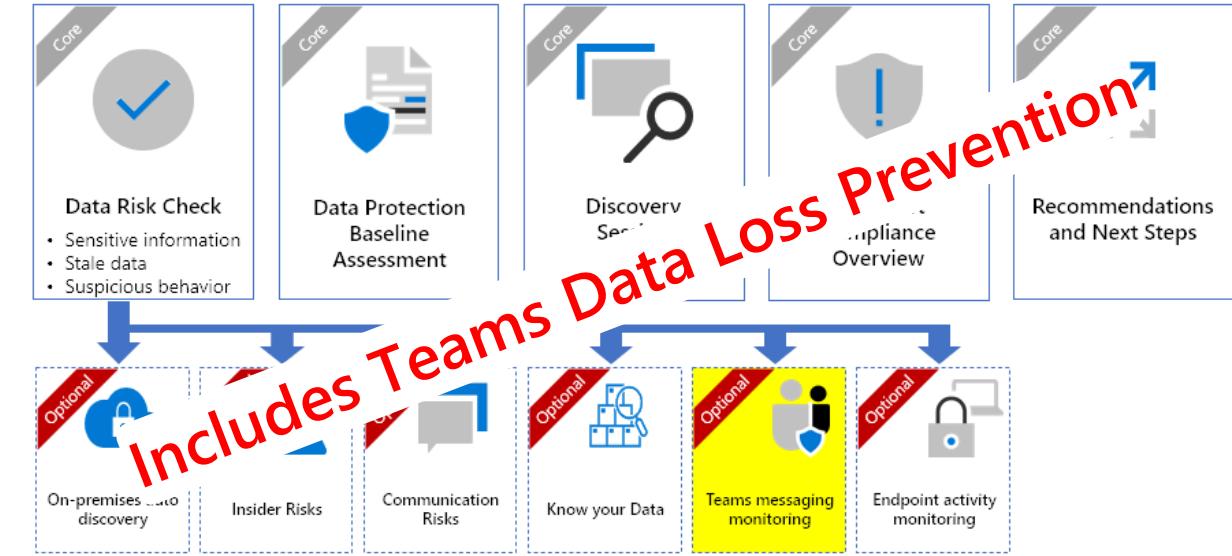
## Learn about Microsoft's Compliance Portfolio

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](#)

## Associate

### M365 Security Administrator Associate

- [MS-500: Microsoft 365 Security Administration](#)

### Microsoft Security Operations Analyst

- [SC-200: Microsoft Security Operations Analyst](#)

### Microsoft Identity and Access Administrator

- [SC-300: Microsoft Identity and Access Administrator](#)

### Microsoft Information Protection Administrator

- [SC-400: Microsoft Information Protection Administrator](#)

### Azure Security Engineer

- [AZ-500: Microsoft Azure Security Technologies](#)

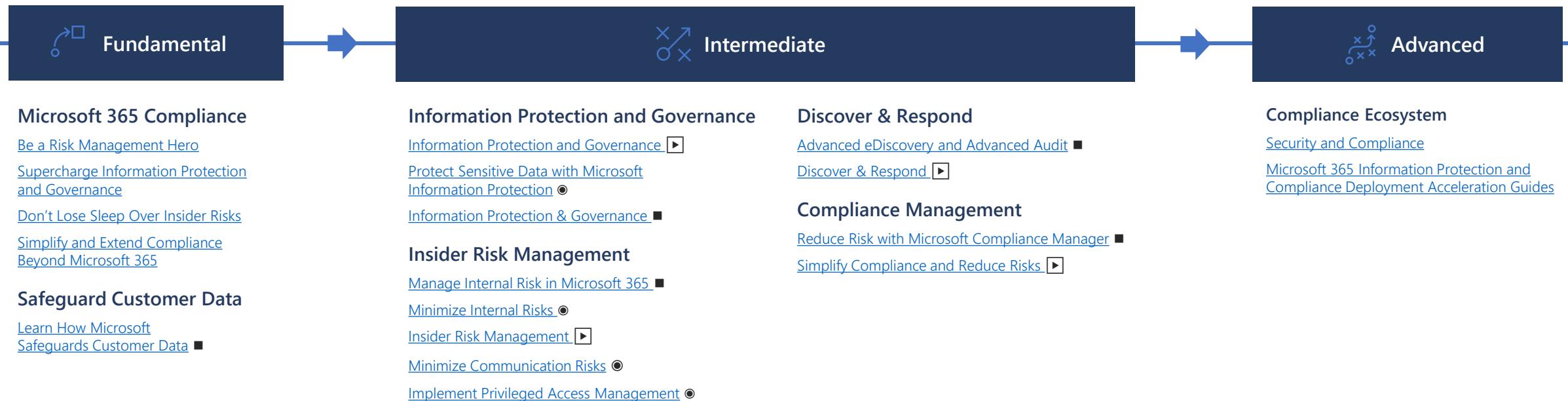
## Expert

### 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



Legend



Microsoft Learning Path



YouTube Playlist



Interactive Guide



# 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.

# Teams DLP Links

- **Blogs:**
  - What's New and What's Coming in Information Protection:  
<https://techcommunity.microsoft.com/t5/microsoft-security-and/what-s-new-and-what-s-coming-in-information-protection/ba-p/1797438>
  - Unified approach to data loss prevention from Microsoft:  
<https://techcommunity.microsoft.com/t5/microsoft-security-and/a-unified-approach-to-data-loss-prevention-from-microsoft/ba-p/1694492>
  - Sensitivity labels in Teams/SharePoint sites: <https://aka.ms/M365SitesLabelsGA>
  - Automatic classification in Microsoft 365 services: <https://aka.ms/M365AutoClassificationGA>
  - Sensitivity labels in Files: <https://aka.ms/M365FilesLabelsGA>
- **Documentation:**
  - [Microsoft Teams DLP Playbook!!! - Microsoft Tech Community](#)
  - Data loss prevention and Microsoft Teams: <https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide>
  - Sensitivity labels in Teams/SharePoint sites: <https://aka.ms/M365SitesLabels>
  - Automatic classification in Microsoft 365 services: <https://aka.ms/M365AutoClassification>
  - Sensitivity labels in Files: <https://aka.ms/M365FilesLabels>

# Upcoming Security, Compliance & Identity Partner Events

- **Compliance@Speed – Part 2 & 3**
  - <https://aka.ms/complianceatspeed-reg>
  - [Part 2 – 26<sup>th</sup> May](#) and [Part 3 – 23<sup>rd</sup> June](#)
- **Microsoft Defender Masterclass III**
  - 19<sup>th</sup> May – 9am to 1pm
  - <https://aka.ms/defendermasterclass3-reg>
- **Microsoft Defender Masterclass IV – Capture the Flag**
  - 17<sup>th</sup> June – 9am to 1pm
  - <https://aka.ms/defendermasterclass4-reg>

Compliance @ Speed - 9:30am - 1pm (British Summer Time)

Join the Microsoft Protectors for a 3.5 hour event, where you will be taken on a deeper journey into our Compliance Platform across Microsoft 365 and Azure + learn how to automate using Power Platform integrations



Protectors... Register your bravery at [aka.ms/complianceatspeed-reg](https://aka.ms/complianceatspeed-reg)

Illustrations by [Rocky Chertok](#)



# Power Platform Events from Microsoft UK

## RPA In A Day

### Power Automate Desktop - Train the Partner event

If you're a Power Platform, Dynamics, Modern Work or Azure partner and you're looking to expand your practice to include automation, or indeed if you're already an automation partner considering Power Automate for Desktop, this **free** event the event for you.

The hands-on, step-by-step lab exercises will guide you through building a modern end to end enterprise-style RPA scenario to process incoming invoices. Whilst working through the labs, you will use Power Automate capabilities such as: Power Automate Desktop, API connectors to automate a business process and form processing models developed in AI Builder.

**Join us**  
**10 am – 12 pm**  
**3<sup>rd</sup>, 4<sup>th</sup> & 5<sup>th</sup> May**

[aka.ms/RPAInADay\\_May](http://aka.ms/RPAInADay_May)



Get in touch to build a compliance practice!  
Email - Alison.Turnbull@microsoft.com



# Feedback –

<https://aka.ms/complianceatspeedfeed>

