Compliance @ Speed – 20th 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

Microsoft

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 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

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

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.

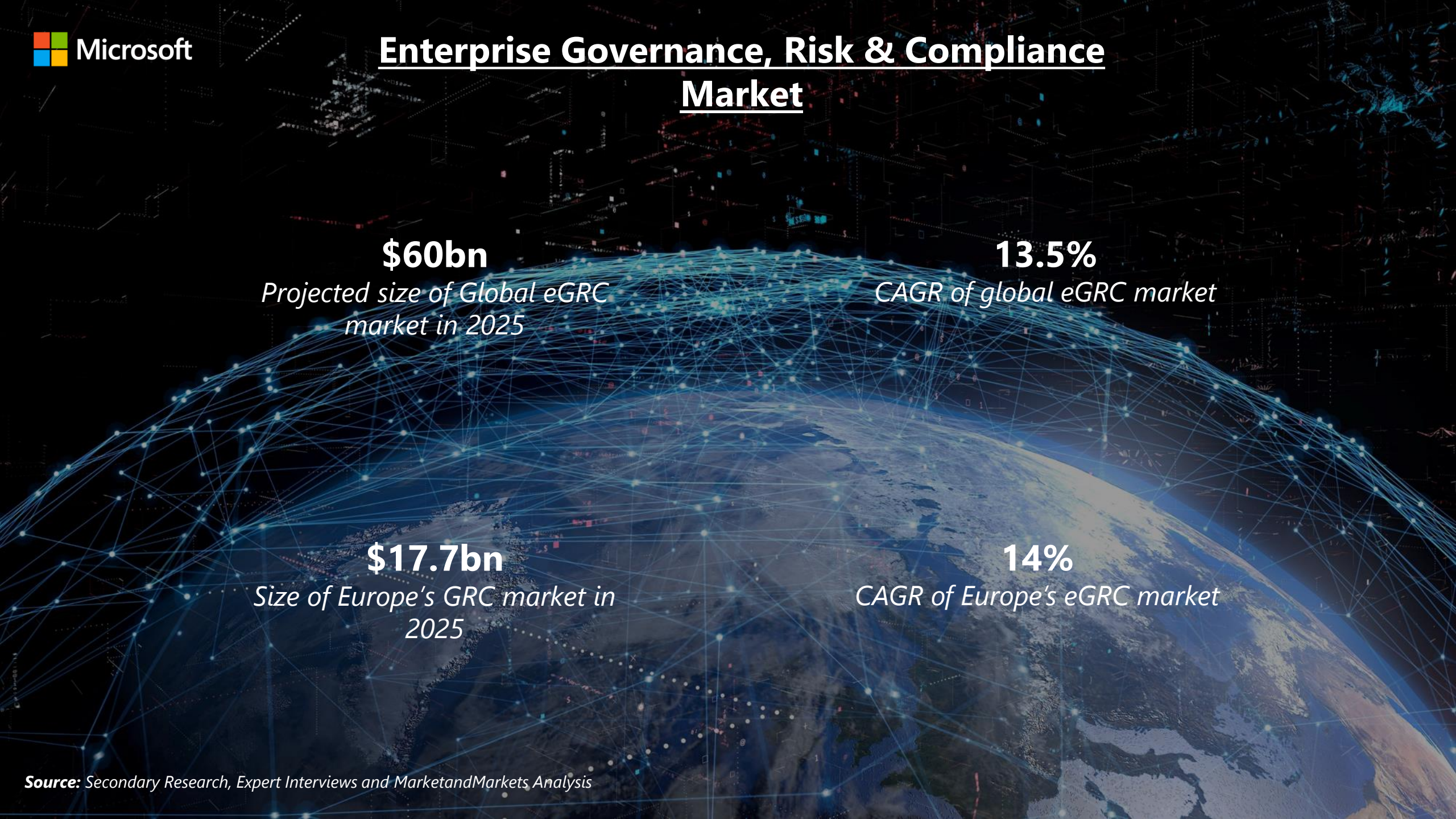
ICO now over 821 incidents being considered by Investigations Department.

90% organizations feel vulnerable to insider threats.

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

Sources: *Microsoft Research, FOI request ICO, crowdresearchpartners.com, gartner.com* - Market Guide for Insider Risk Management Solutions

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

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

Microsoft

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%
Total	**4,400**	**7,302**	**13.1%**

e: estimated; p: projected

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

Microsoft

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%
Total	**5,915**	**10,450**	**14.6%**

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

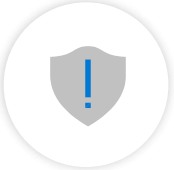
Compliance Management
Audit Management

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

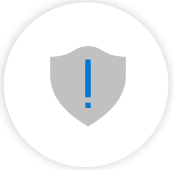
FUNCTION KEY

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

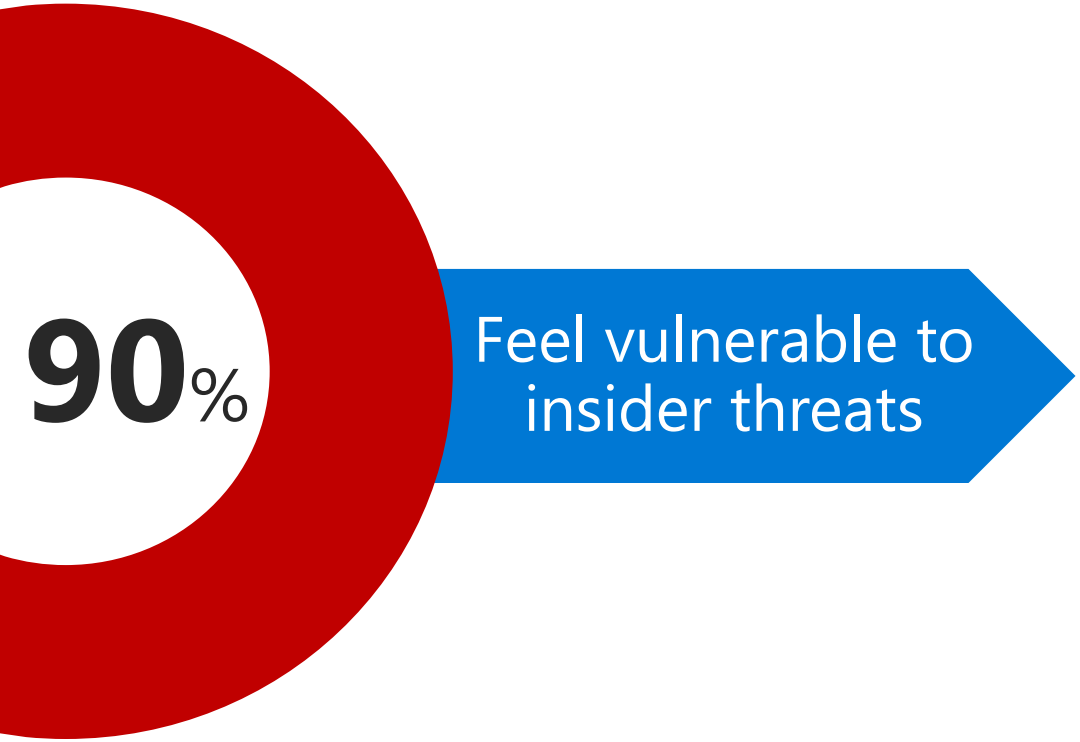
Compliance Management

Simplify and automate risk assessments

Compliance Score
Compliance Manager
Long-Term Auditing
Assessment template

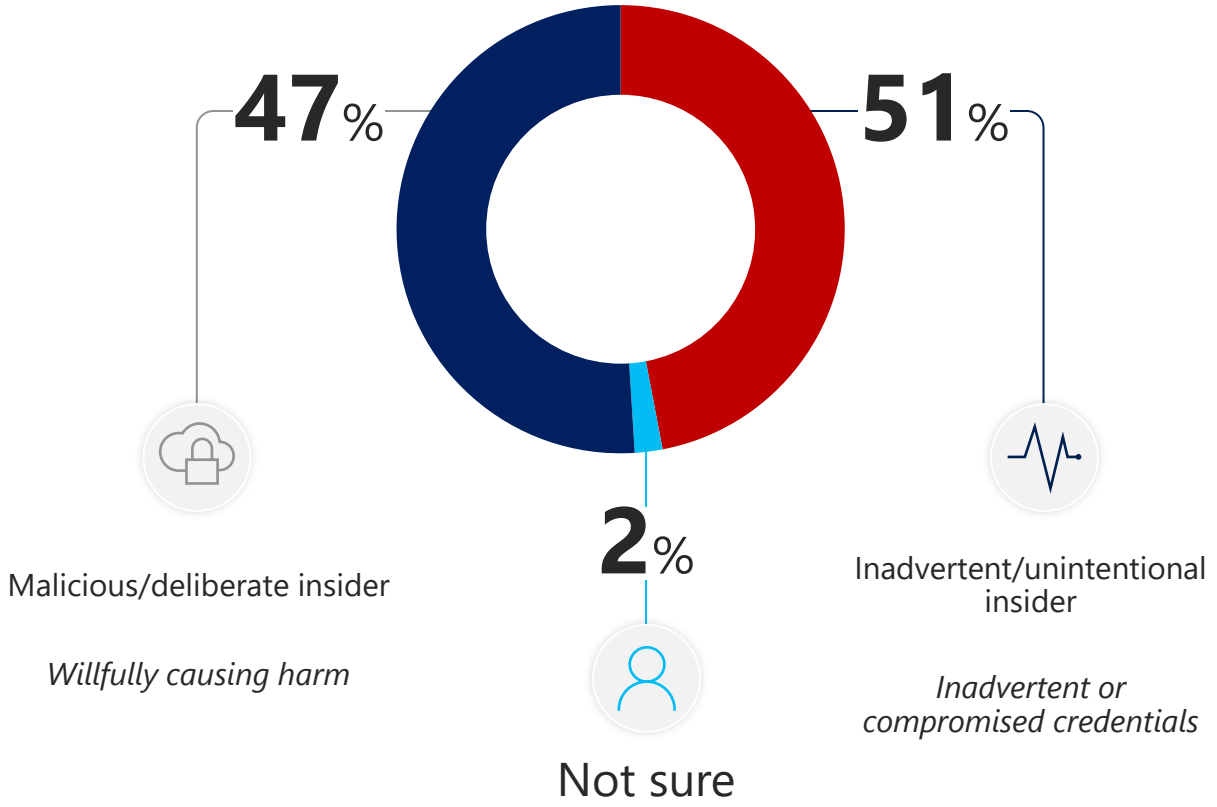
Insider risk is one of your biggest challenges[1]

How vulnerable is your organization to insider threats?



Feel vulnerable to insider threats

What type of insider are you most concerned about?



https://crowdresearchpartners.com/portfolio/insider-threat-report/

1. 95% of organizations surveyed were 100+ seats

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

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

Results from the last scan for risk activities

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

25% of users performed activities involving ser
25% of users downloaded SharePoint files

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 outsid than 10 times

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.

Create policy

Close

Microsoft

Thank You!

Compliance Manager/Score

Graham Hosking – Security and compliance specialist

Illustrations by Becky Cholerton

Microsoft

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.

[1] Only for Office 365 operated by 21 Vianet | [2] Only for GCC/GCC High

Shared Responsibility Model

Customer management of risk

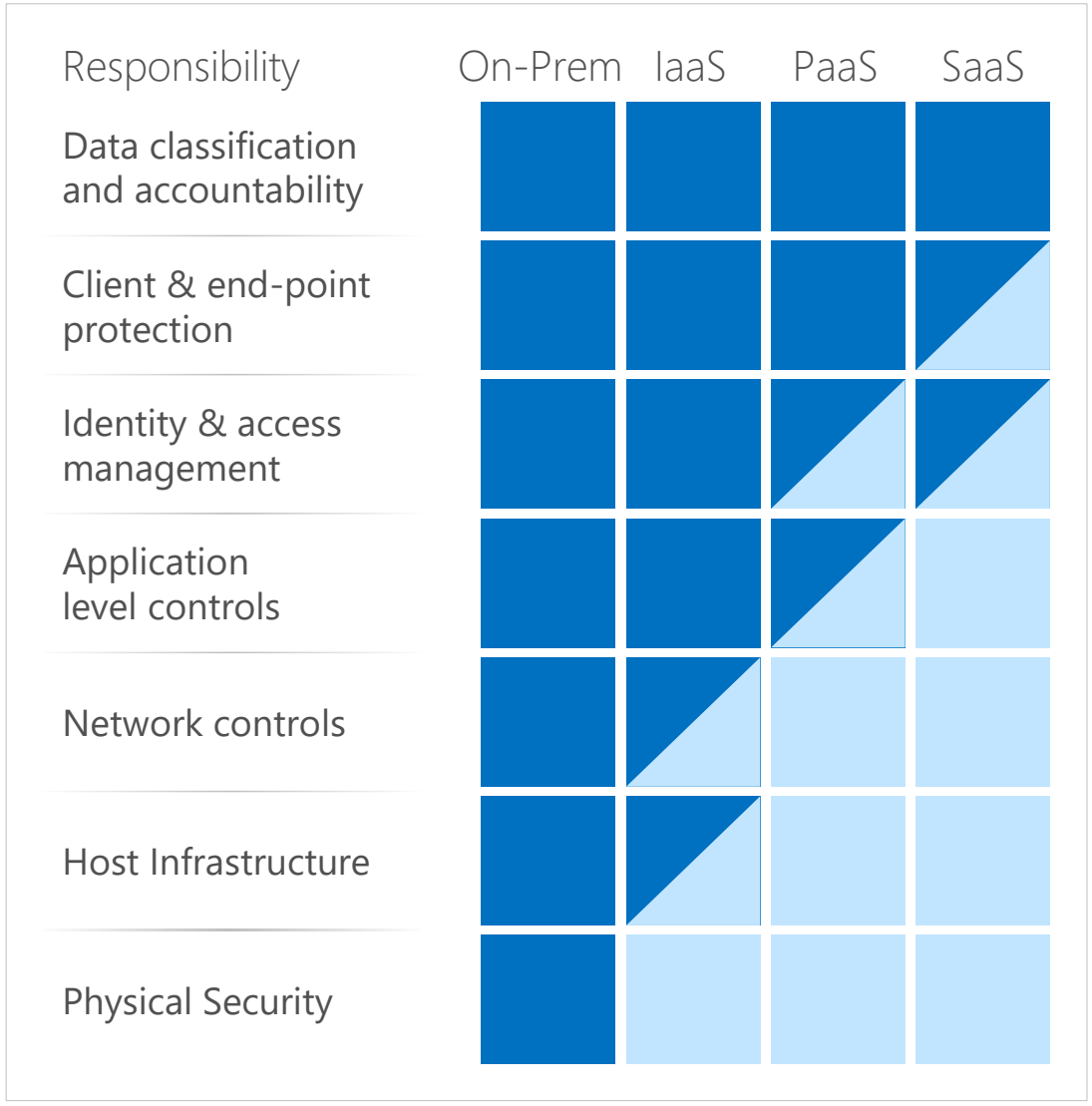
Data Classification and data accountability

Shared management of risk

Identity & access management | End Point Devices

Provider management of risk

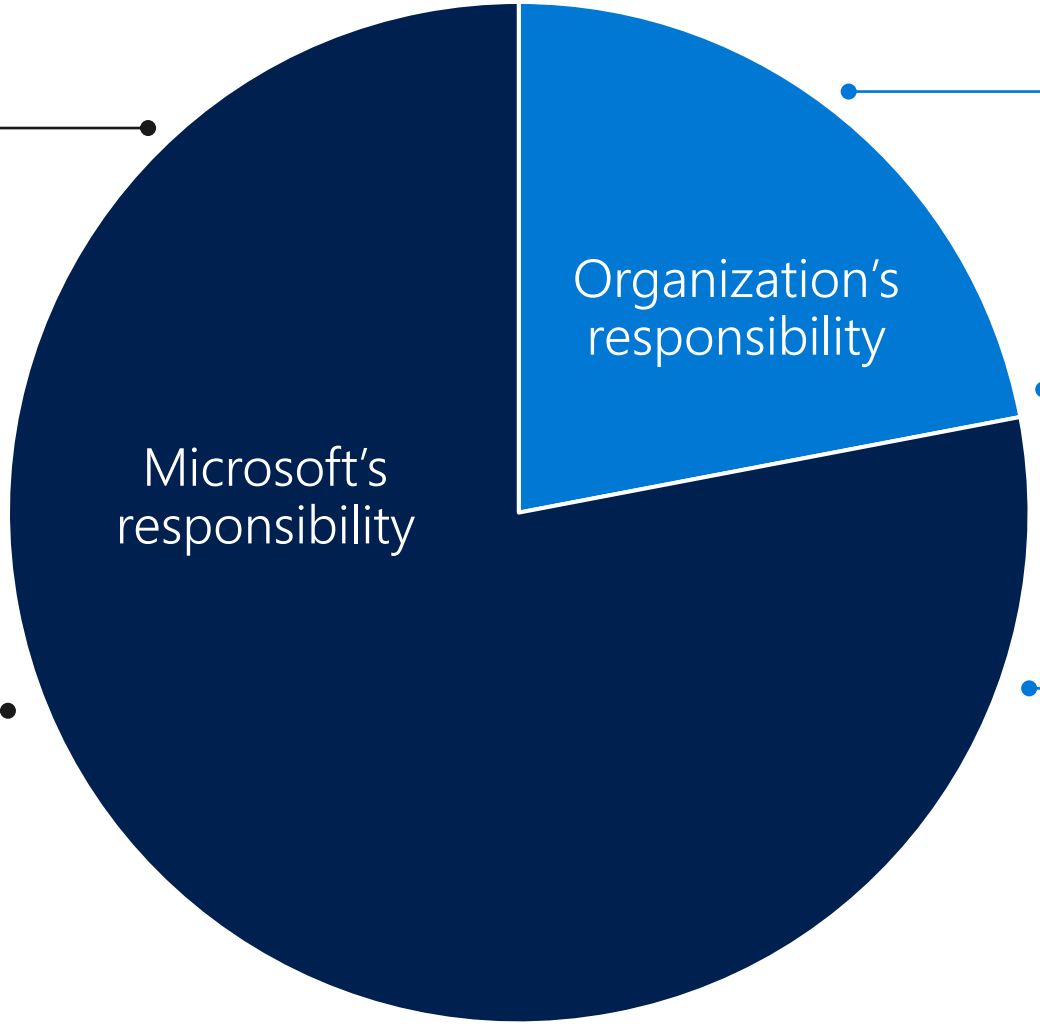
Physical | Networking



Cloud Customer **Cloud Provider**

Shared Responsibility

NIST 800-53



ACCESS TO PRODUCTION ENVIRONMENT

Set up access controls that strictly restrict standing access to customer's data or production environment

PROTECT DATA

Encrypt data at rest and in transit based on industrial standards (BitLocker, TLS, etc.)

PERSONNEL CONTROL

Strict screening for employees, vendors, and contractors, and conduct trainings through onboarding process

ACCESS TO PRODUCTION ENVIRONMENT

Set up access control policy and SOP, leveraging Customer Lockbox / identity management solutions

PROTECT DATA

Encrypt data based on org's compliance obligations. E.g. encrypt PII in transit between users, using its own encryption key, etc.

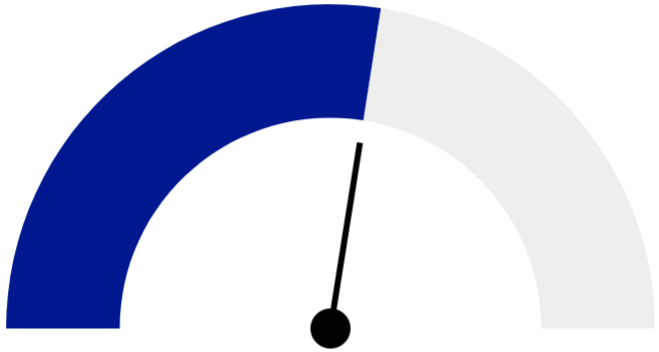
PERSONNEL CONTROL

Allocate and staff sufficient resources to implement and operate an organization-wide privacy program, including awareness-raising and training

DEMO

Overall compliance score

Your compliance score: 55%



1173/2124 points achieved

Your points achieved ⓘ

108/1059

Microsoft managed points achieved ⓘ

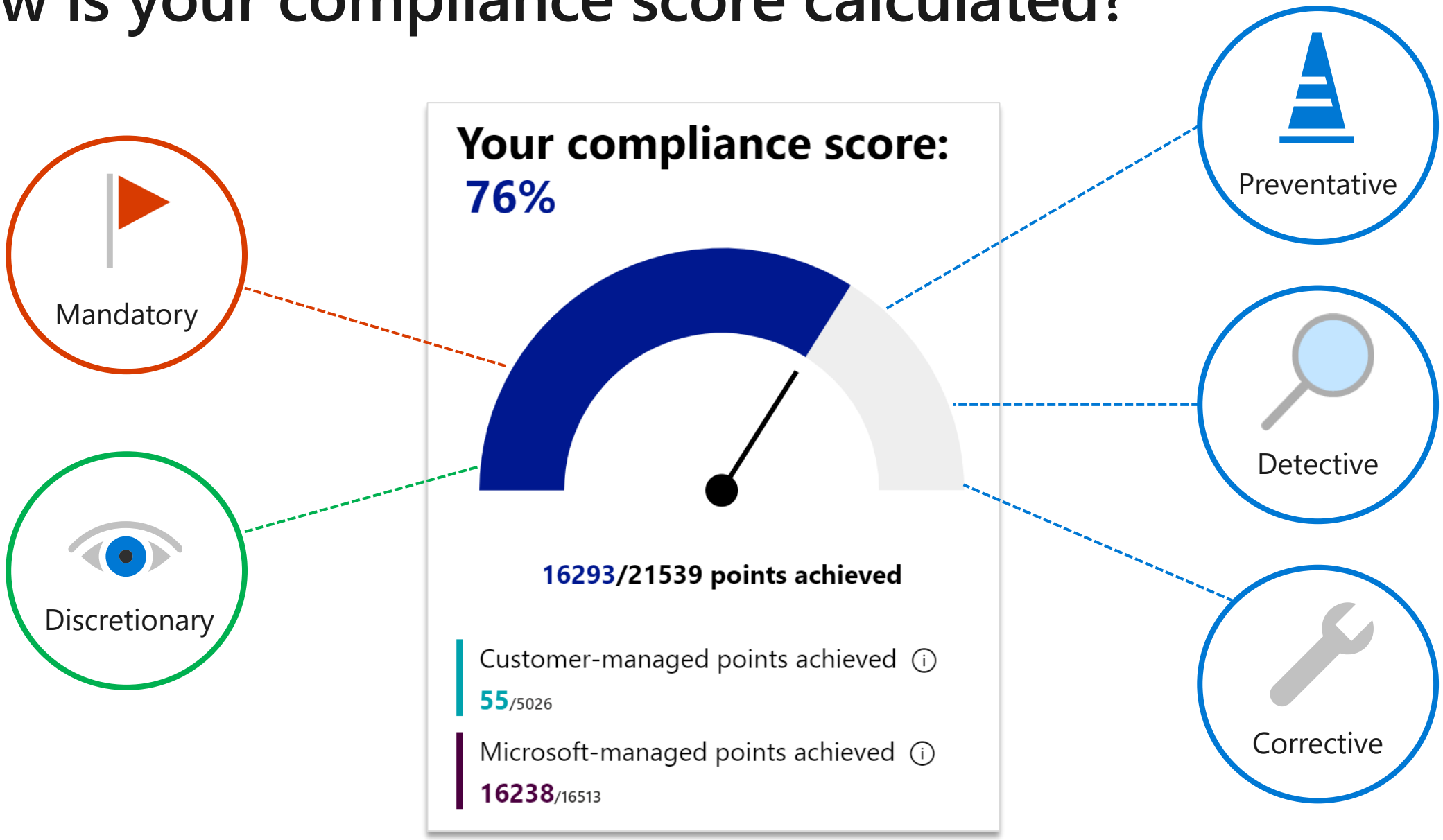
1065/1065

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?



Compliance Manager

Simplify compliance and reduce risk

Intuitive management

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

Scalable assessments

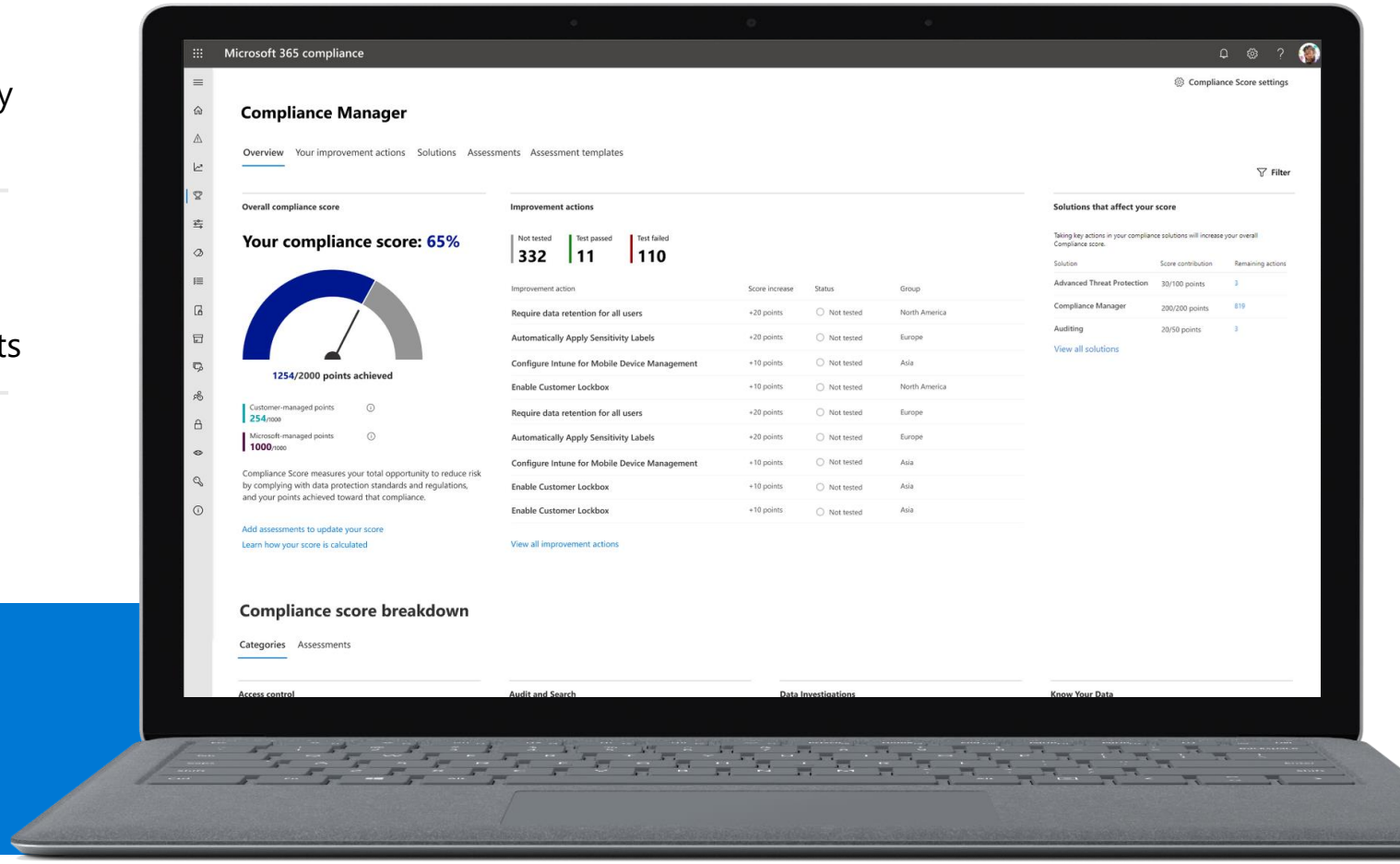
Leverage vast out of the box assessments to meet your unique compliance requirements across all of your assets

Built-in automation

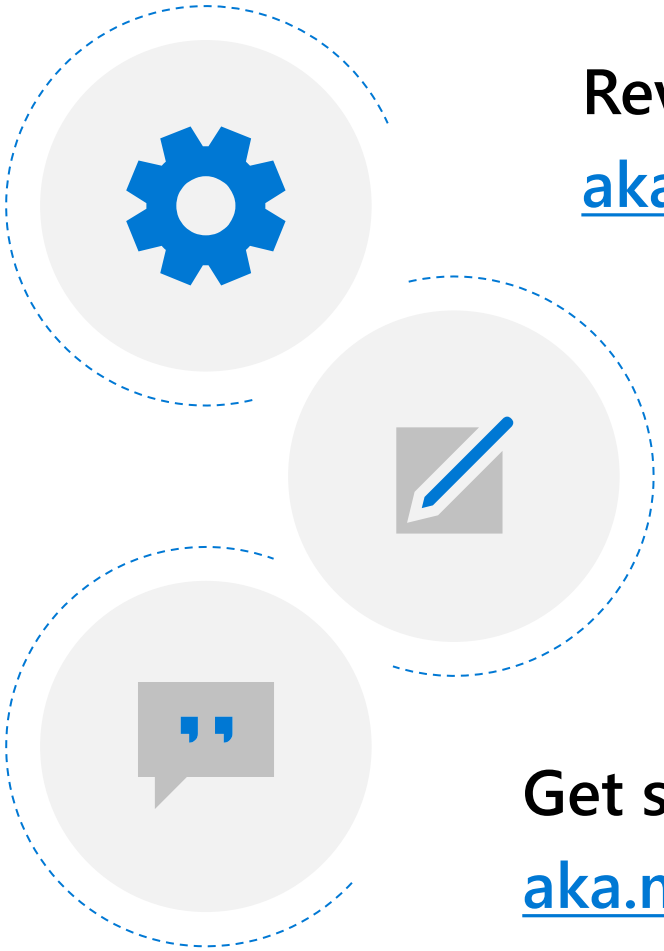
Intelligent automation to reduce risk: compliance score, control mapping and continuous assessments

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

View our latest announcement and videos:

aka.ms/compliancemanager/Gablog

aka.ms/VideoHub/ComplianceManagement

Get started today:

aka.ms/compliancemanager

Try it out:

Aka.Ms/E5Trial

Teams Data Loss Protection (DLP)

Illustrations by Becky Cholerton

Microsoft

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

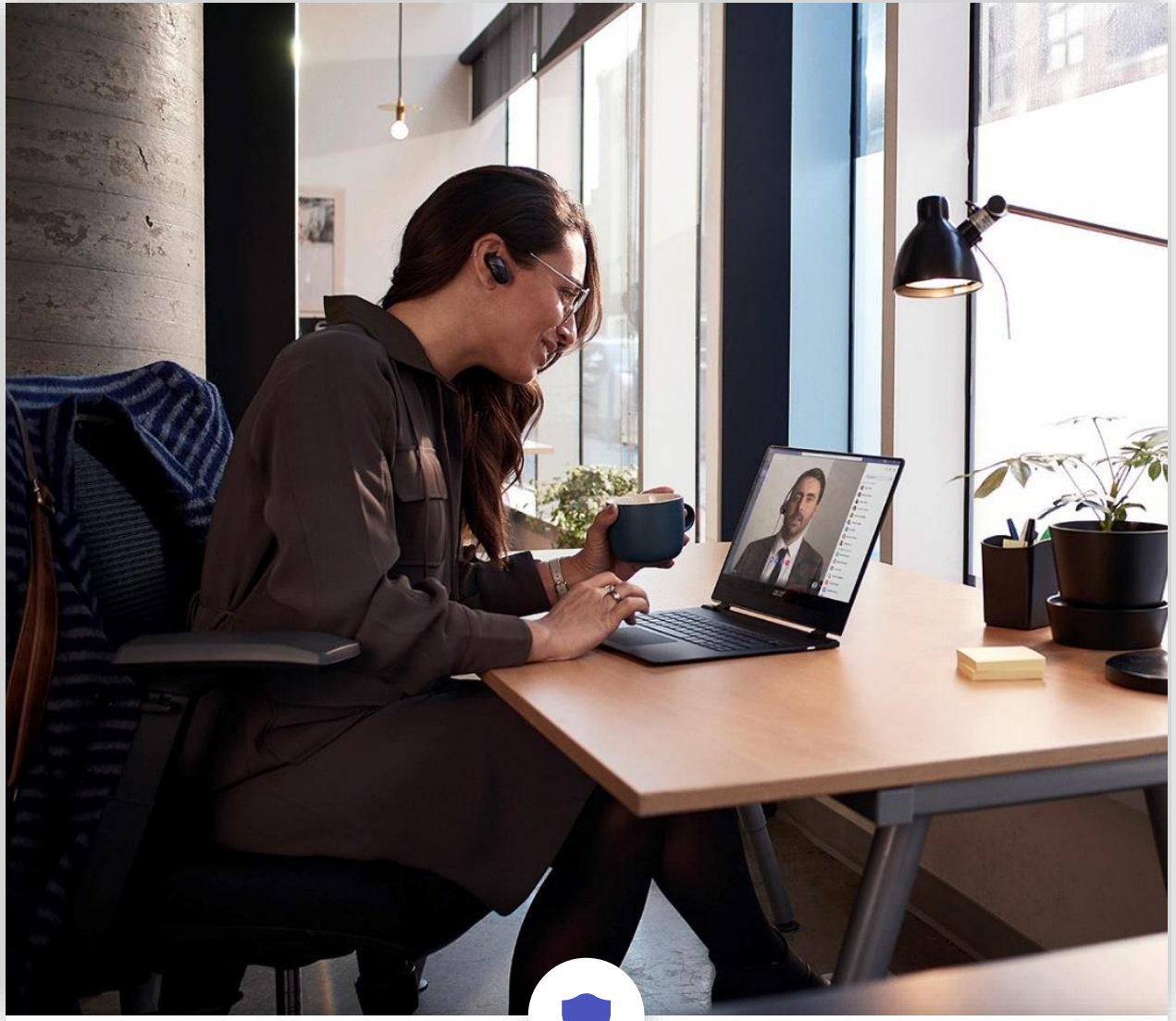
But how do you control your corporate data?

- 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

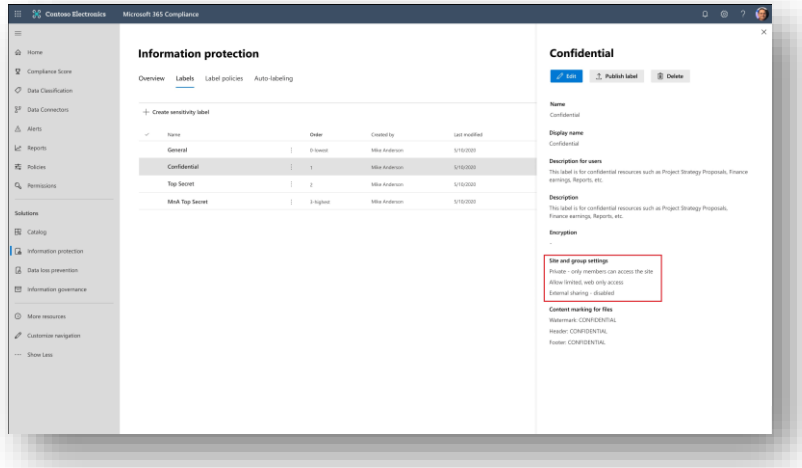


Figure: Admin experience on M365 compliance center. Labeling to protect at Teams site level

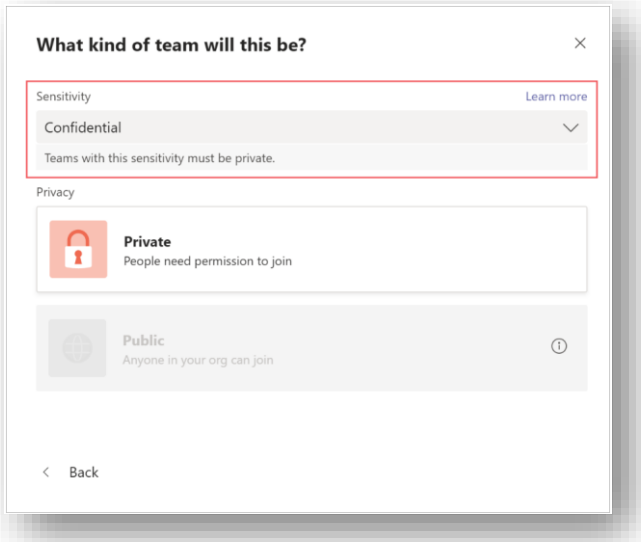


Figure: Team creation user experience – Select sensitivity label for the new team

Microsoft Teams and Compliance

Teams DLP DEMO

Data Loss Prevention for Microsoft Teams

Prevent sharing sensitive information in a channel or chat session

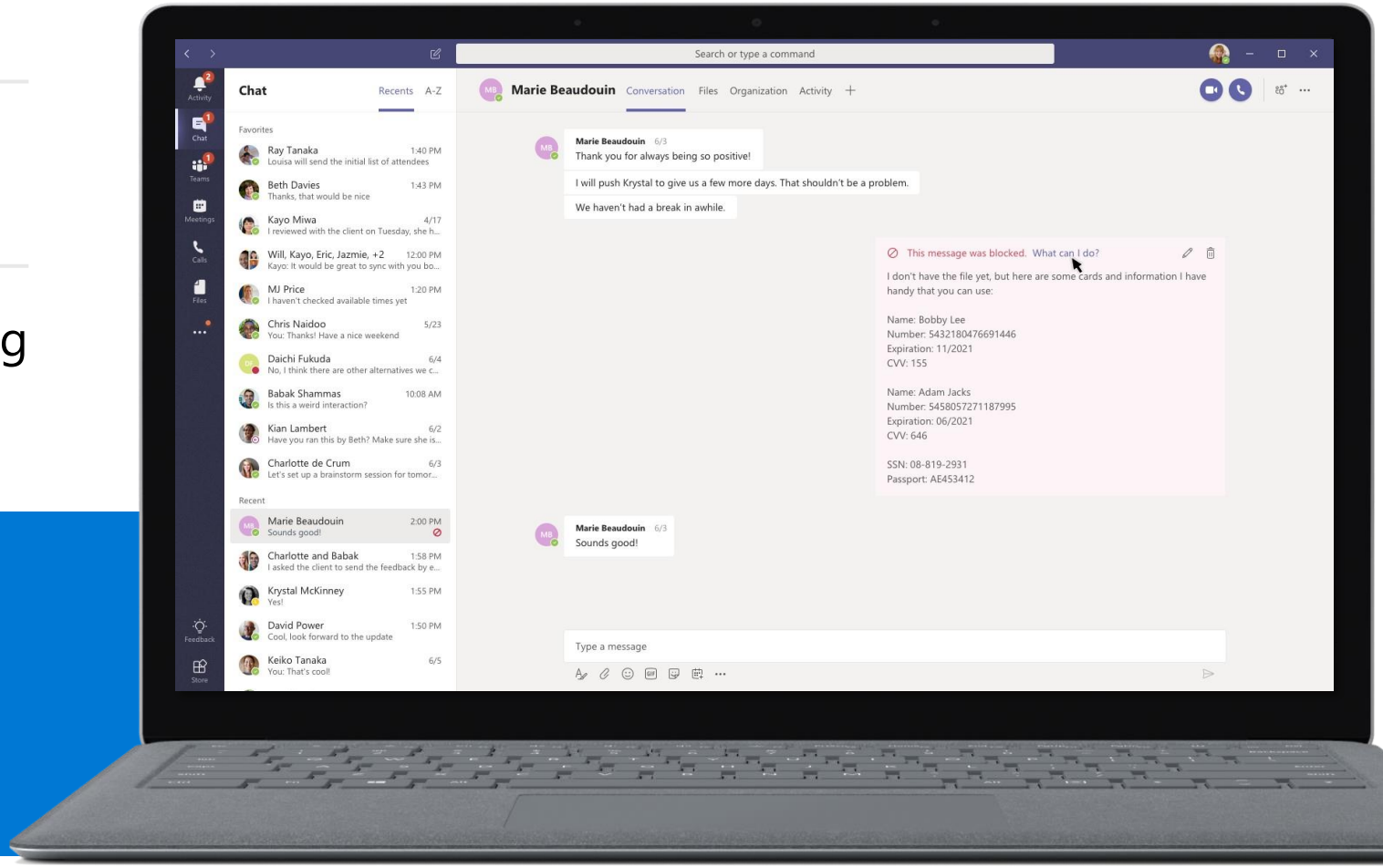
Automatically block messages which contain sensitive information

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

Microsoft

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 competitors 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

Predisposition

- Tendency to violate company policies
- Repeat offenders treated differently 1st offense vs. 3rd offense

Stressor

- Resignation
- *Demotion*
- *Poor performance reviews*
- *Performance improvement plans (PIPs)*

Risk

Concerning Behavior

- Unusual amount of files downloaded, printed or *deleted*
- *Unusual amount of file activities in high risk locations/devices*
- An individual being reported as a policy violator through multiple reports

Planning & Preparation

- *Hiding your actions by renaming files or tampering with security controls*
- *Using unapproved apps*
- *Unusual increase in no of error or access denied messages*
- *Mounting USB devices at unusual hours*

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

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them Deloitte Metastudy

Planning & Preparation

Designing an intelligent insider risk solution

Transparent

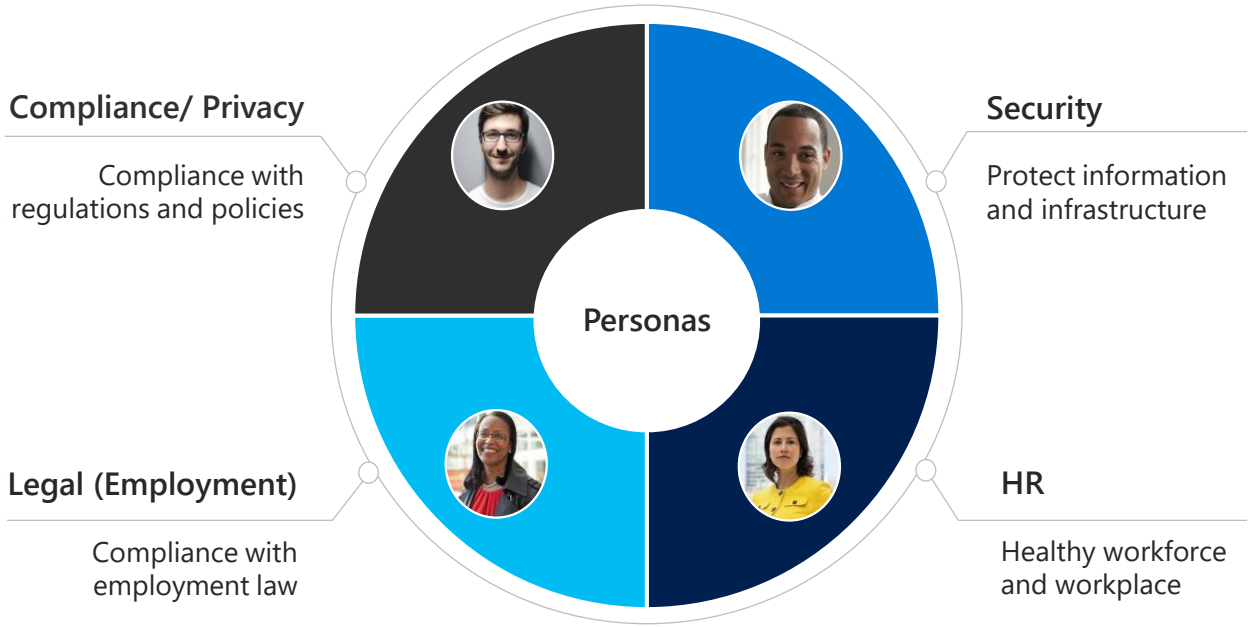
Balance employee privacy versus the organization's risk

Intelligent

Leverage machine learning to identify hidden patterns

Integrated

Integrated workflows to support collaboration to address risks



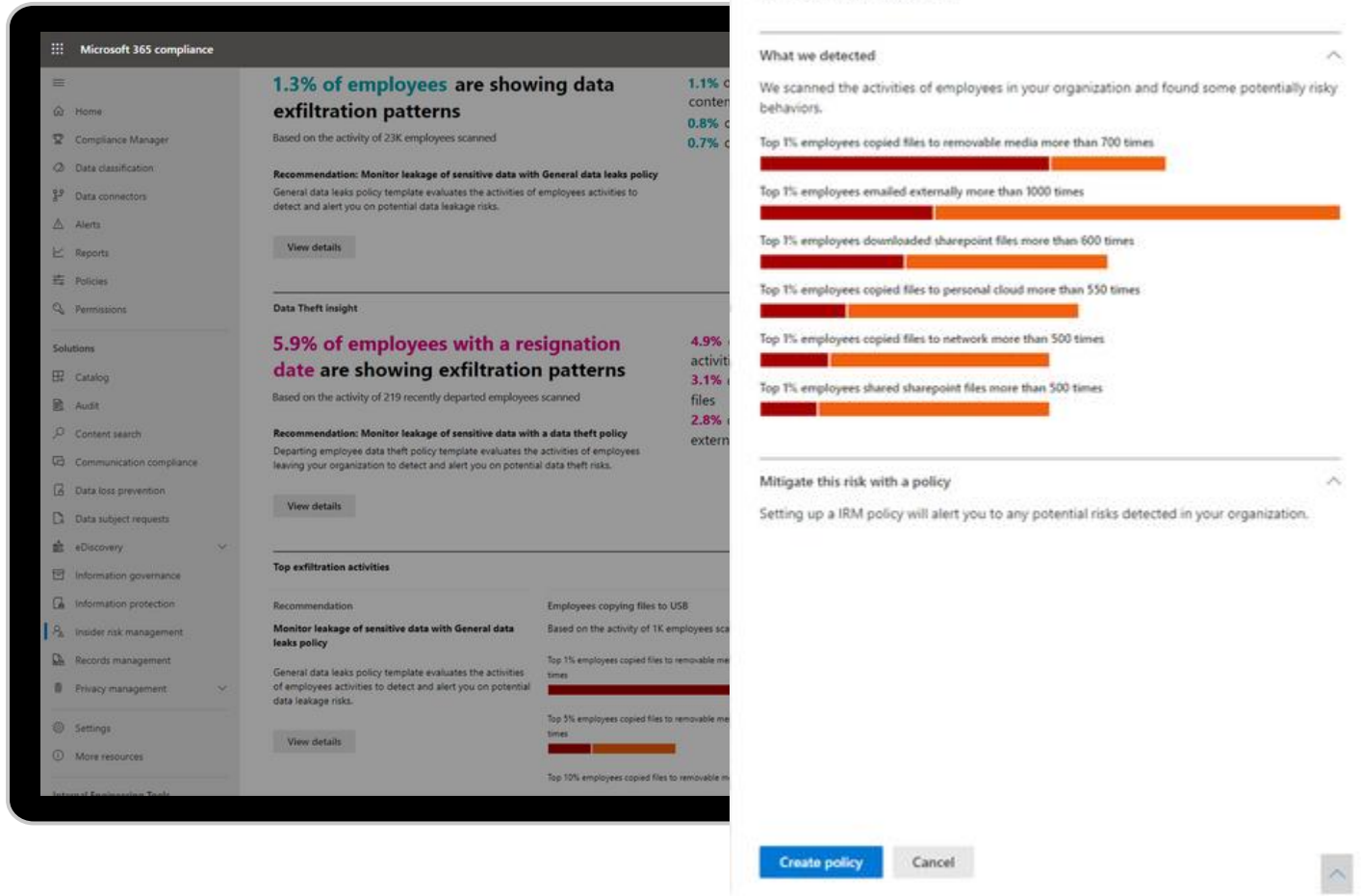
Insider Risk Management

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.



Insider Risk Management

An integrated end-to-end approach for insider risks

Hidden Risks

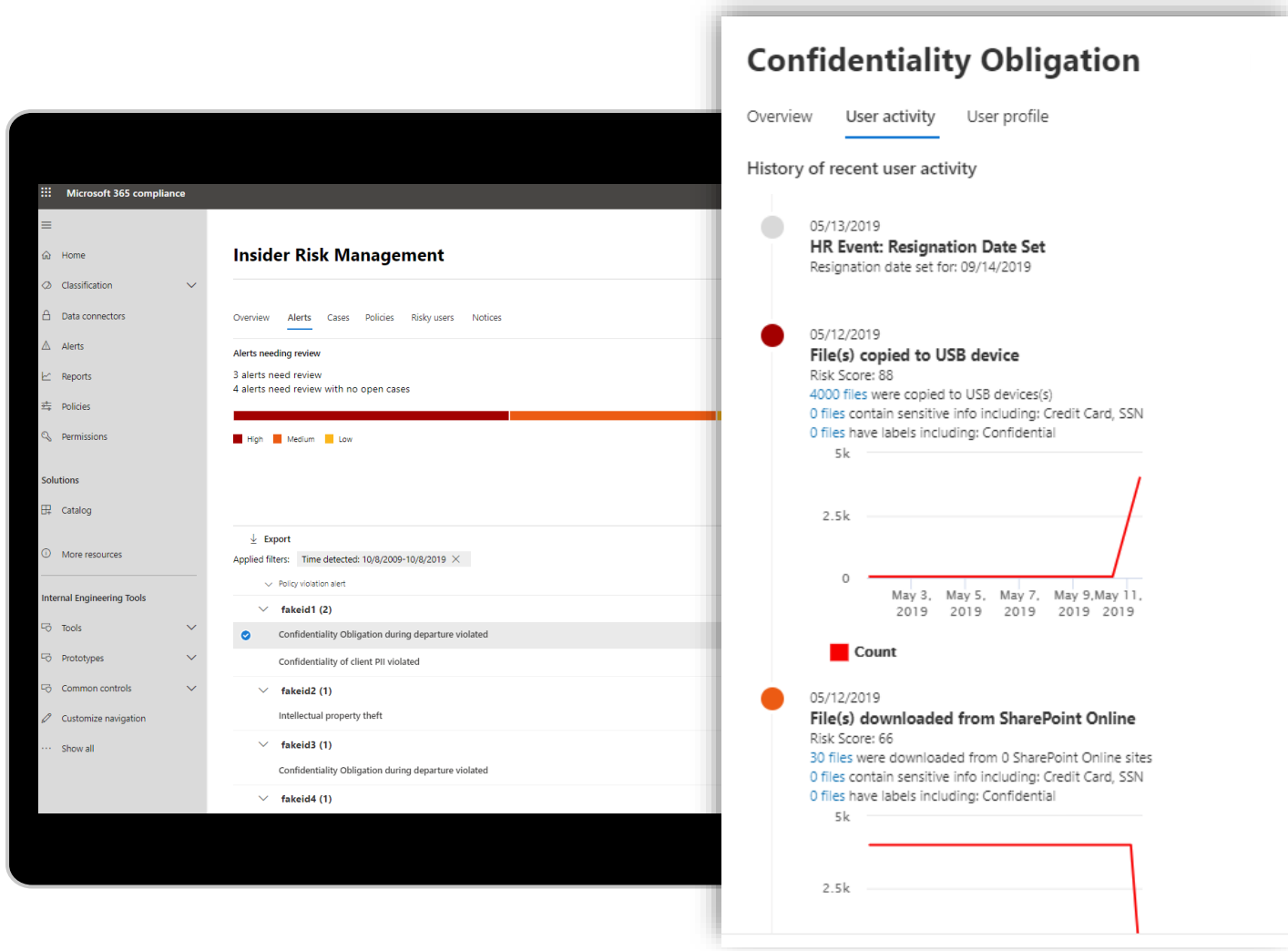
Identify hidden risk patterns with customizable ML templates requiring no end-point agents

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



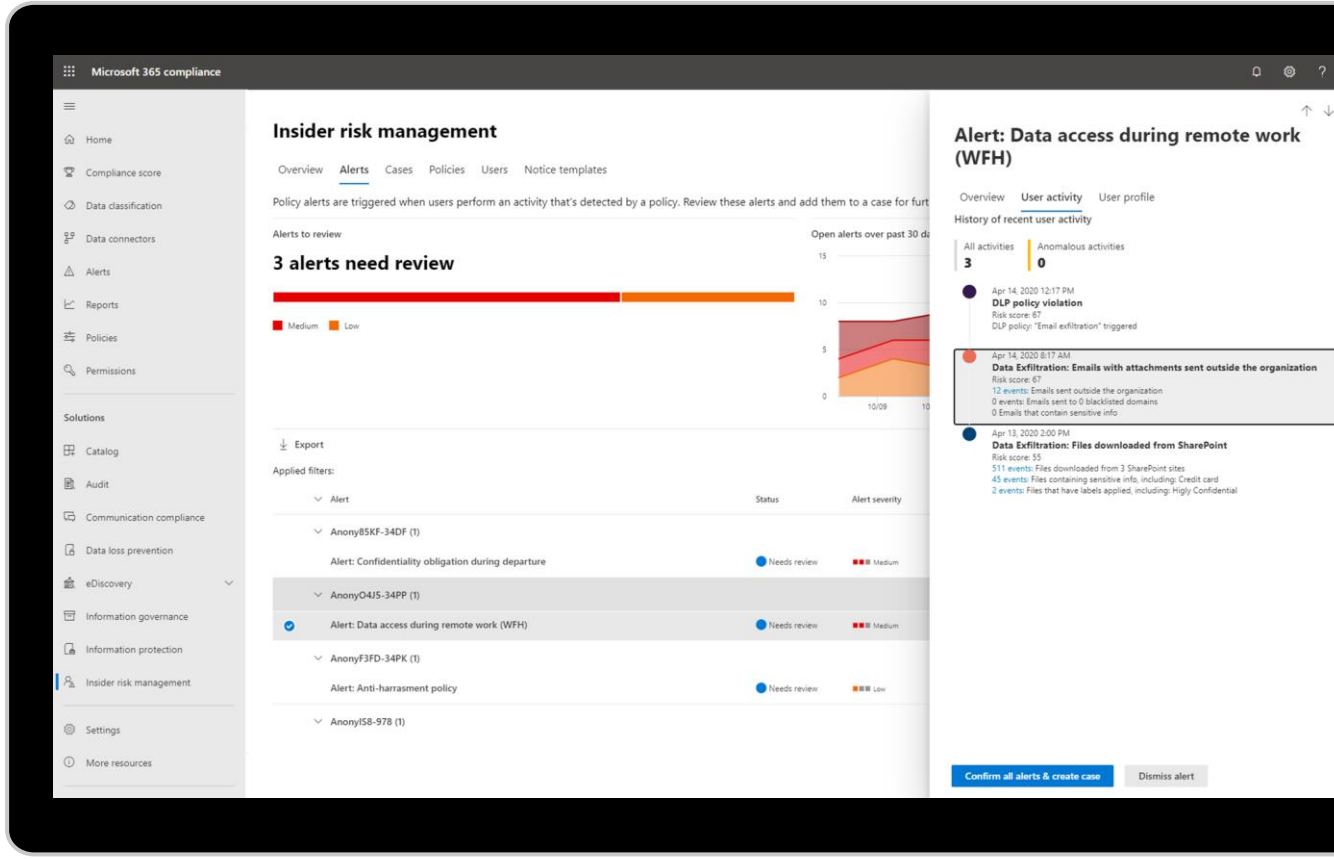
Insider Risk Management

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

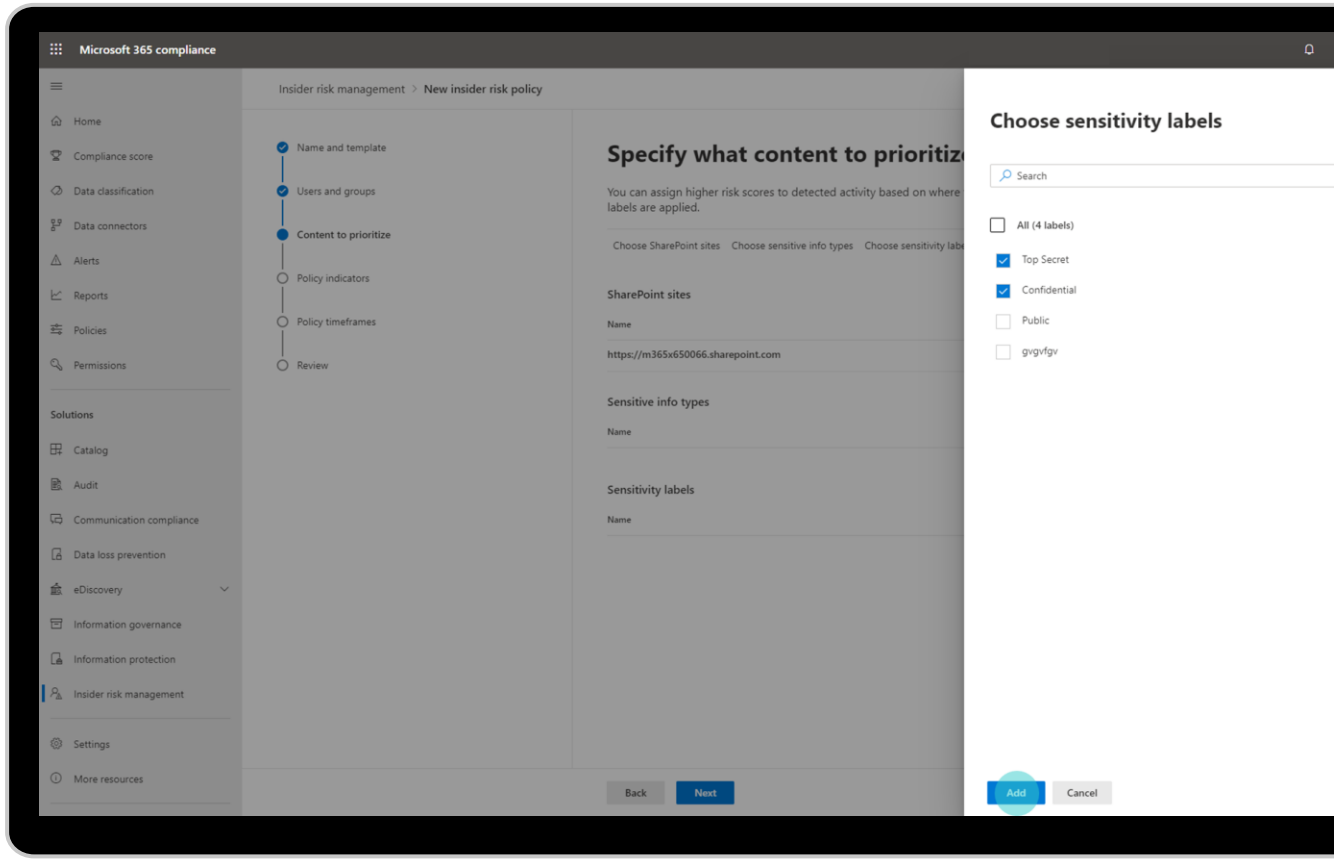
An integrated end-to-end approach for insider risks from Microsoft 365

Insider Risk Management +

Data Loss Prevention

Information Protection

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



Insider Risk Management

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

Insider Risk Management +

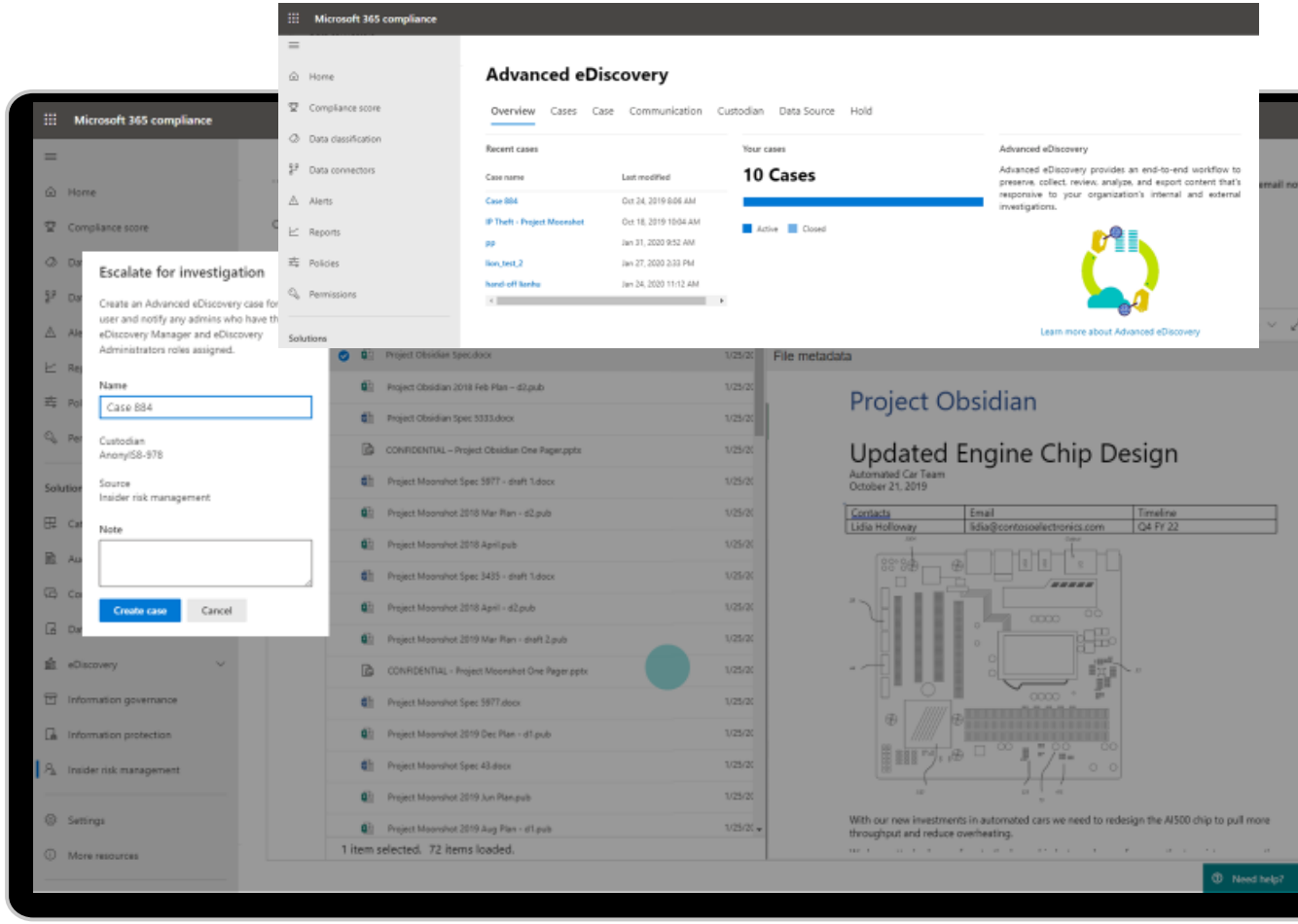
Data Loss Prevention

Information Protection

Communication Compliance

Advanced eDiscovery

Legal collaboration
Integrated workflows provide seamless investigation handoff



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

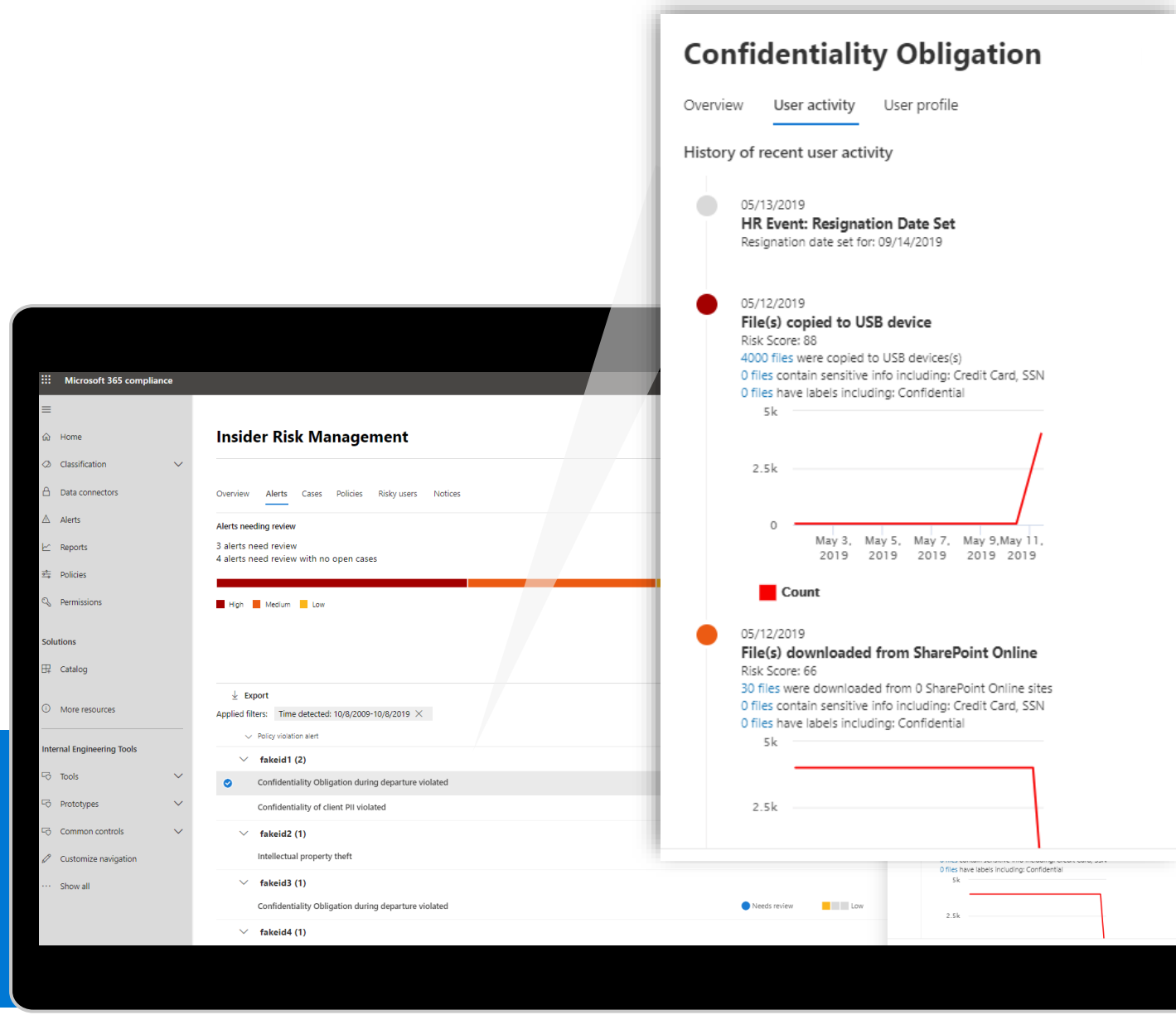
Anonymity controls ensure data about risks is appropriately managed

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

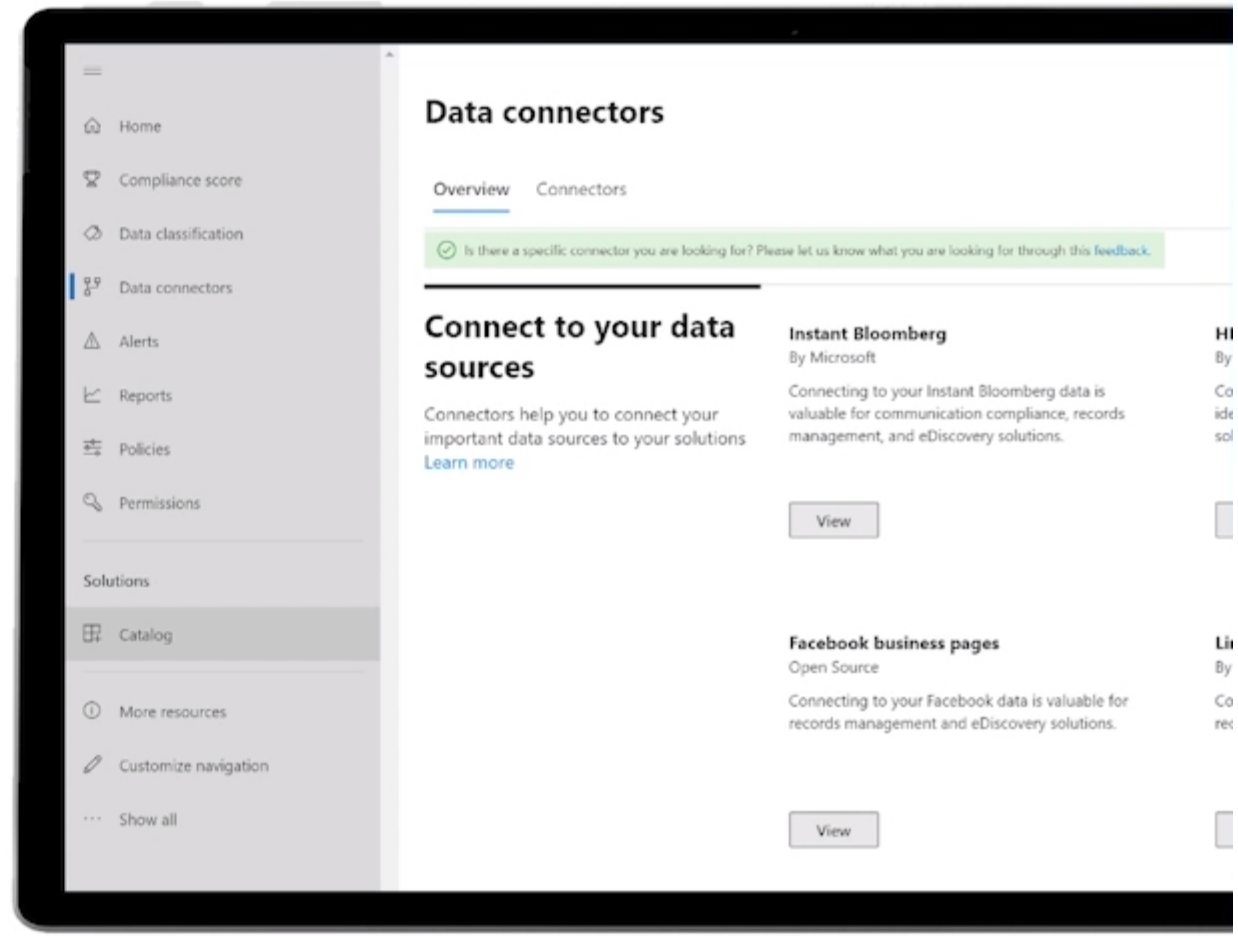
Few clicks to setup data import for most connectors **

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.



*** Connectors by 3rd 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

2020

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

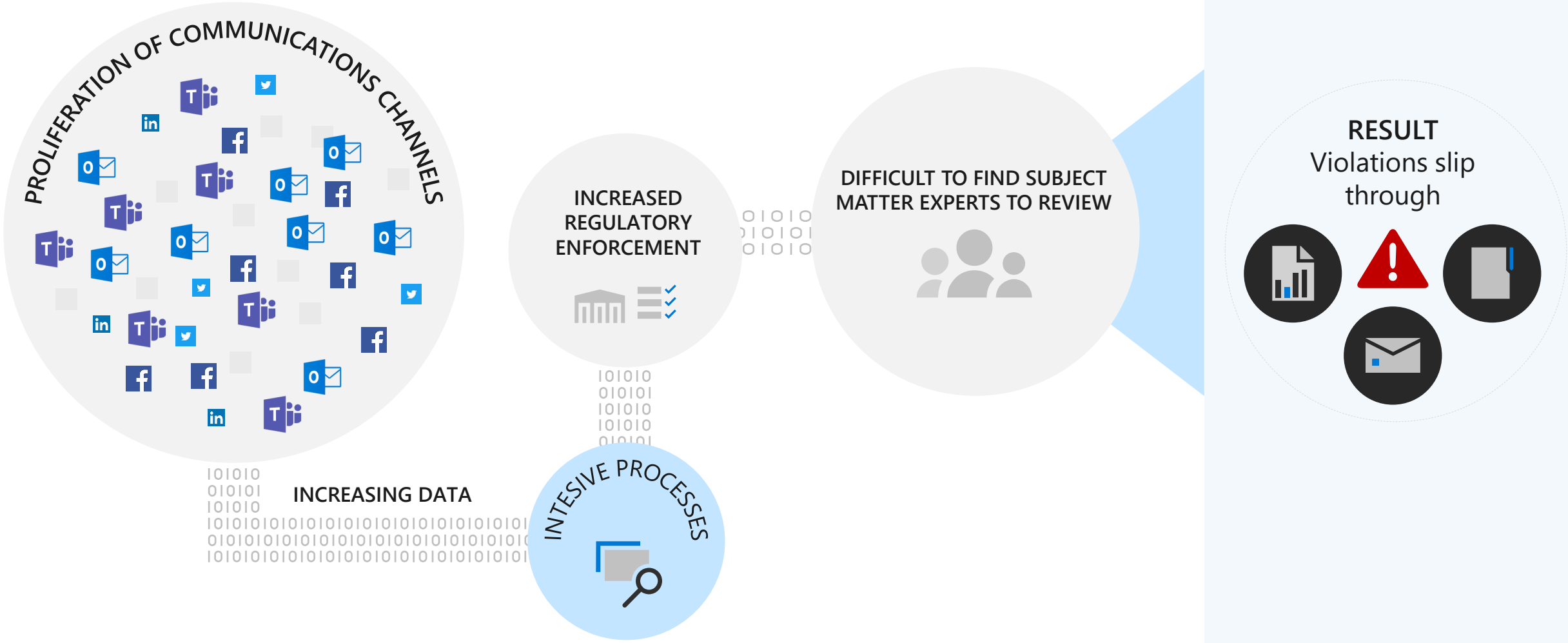
- WhatsApp Archiver
- Android Archiver
- AT&T
- Verizon
- Bell Network
- O_2 Telephonica
- Telus
- Enterprise Number Archiver

Other

- HR Connector
- Physical badging systems
- Generic Text delimited importer
- Generic email importer

*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

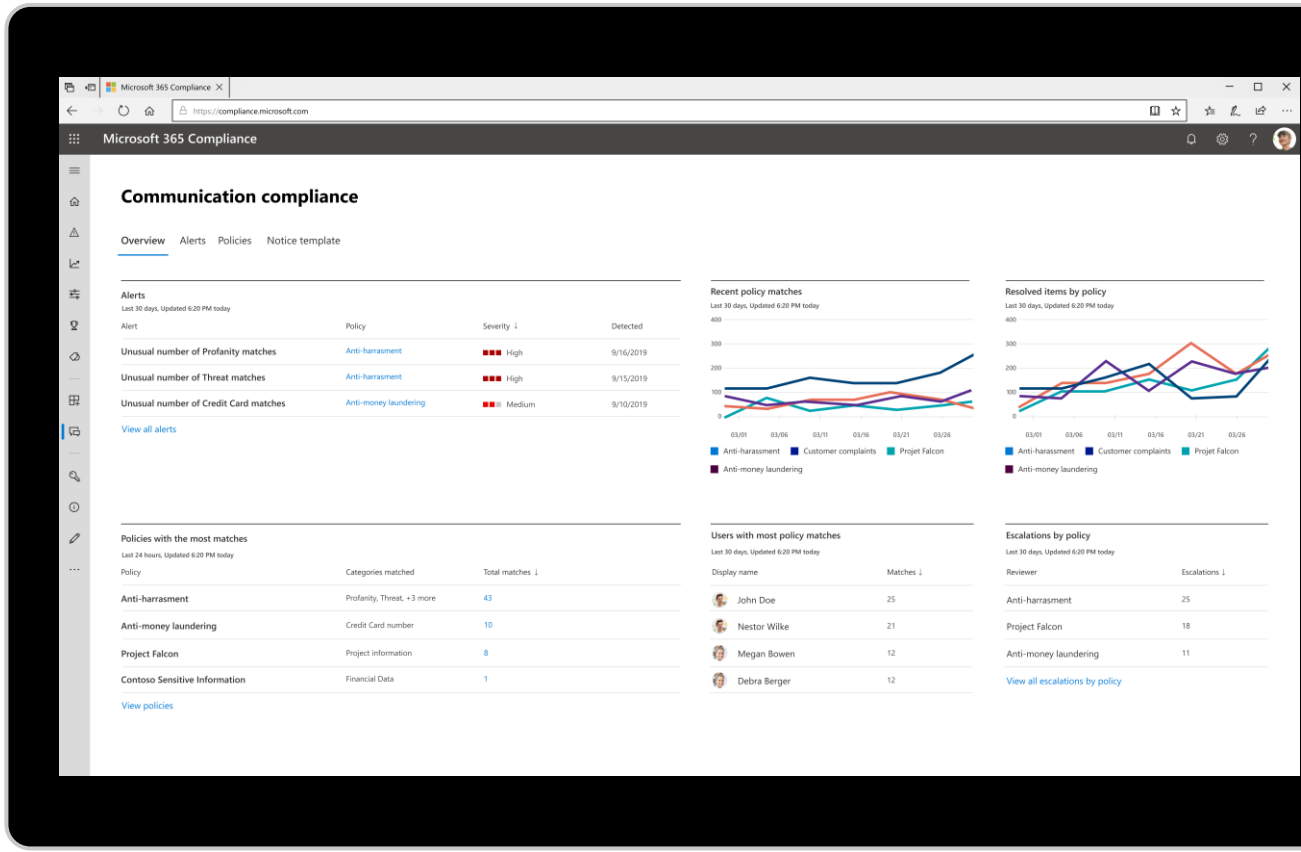
Leverage machine learning to detect violations across Teams, Exchange and 3rd party content

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

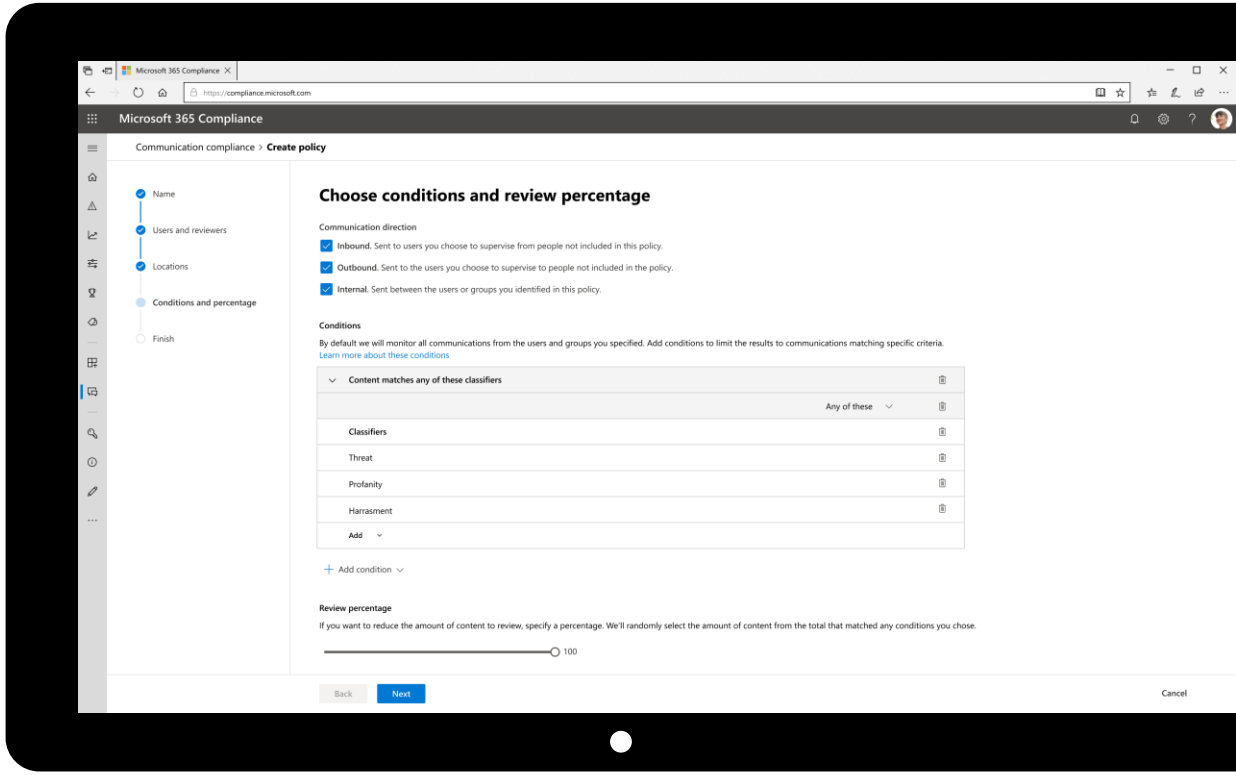


Intelligent customizable playbooks

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

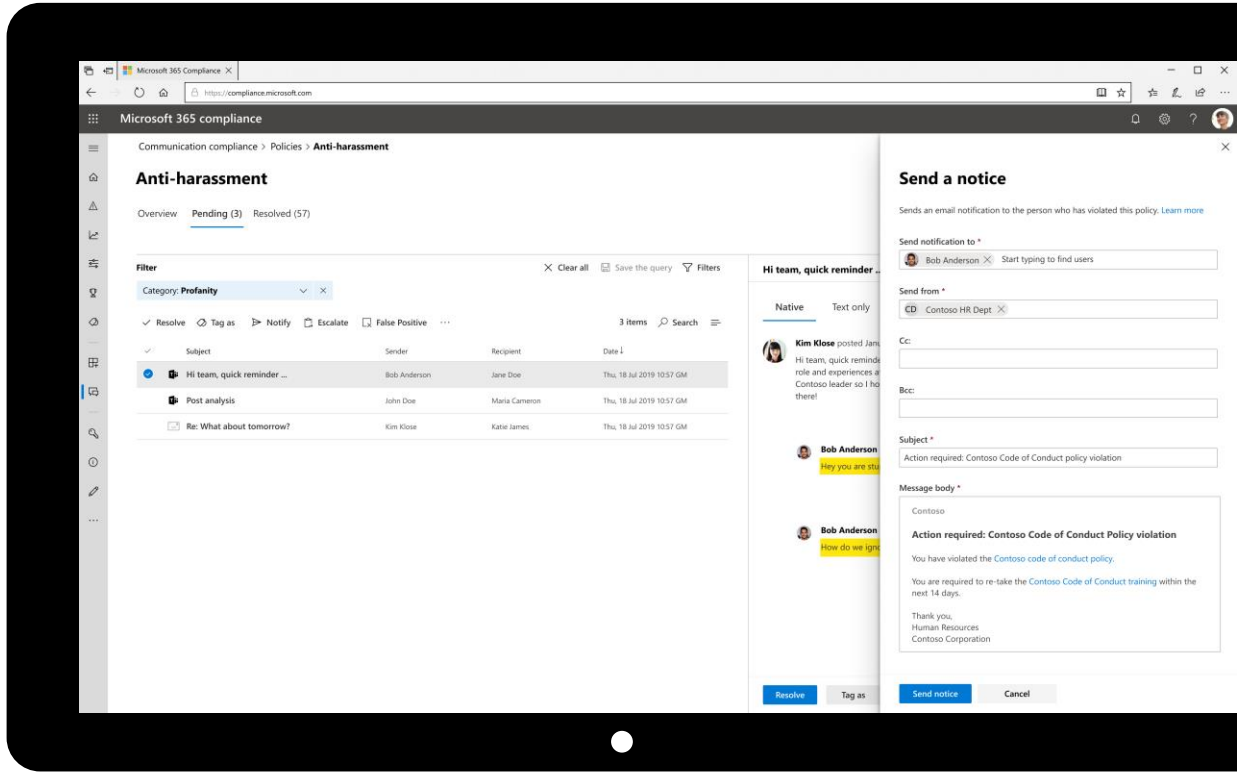


Flexible remediation workflows

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

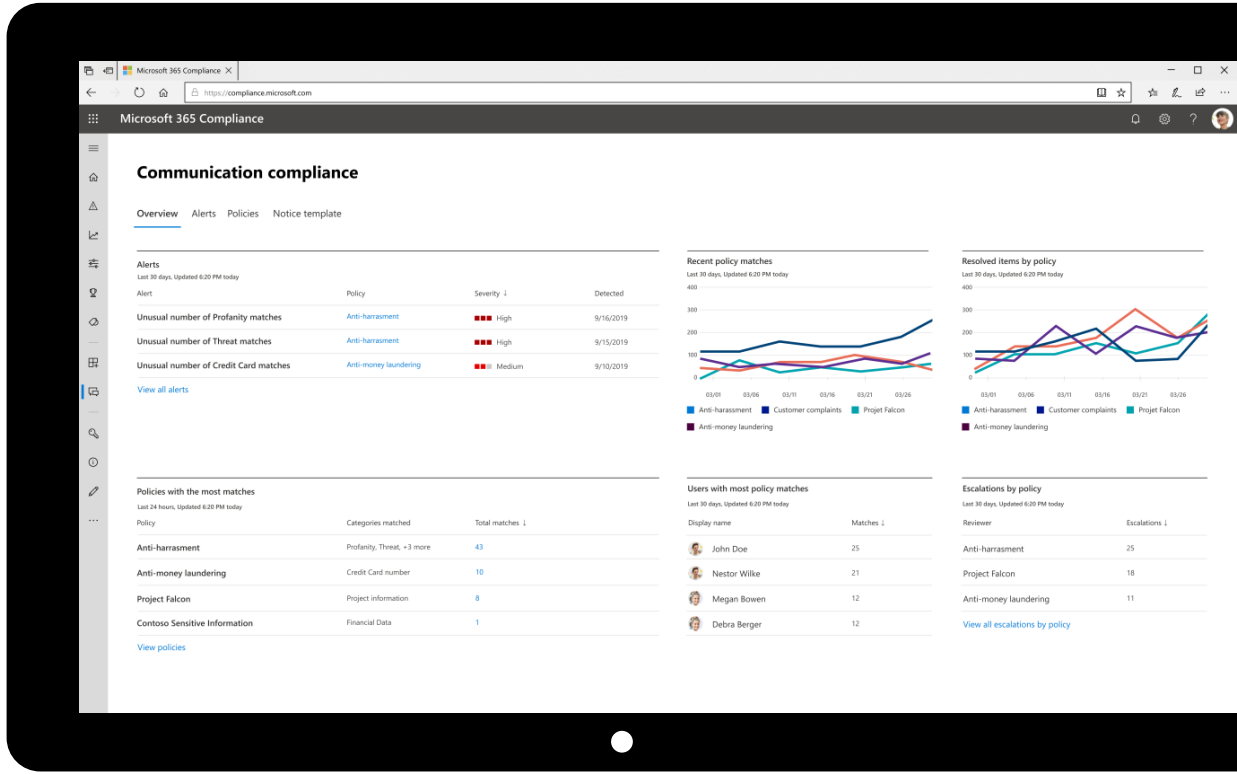


Actionable insights

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

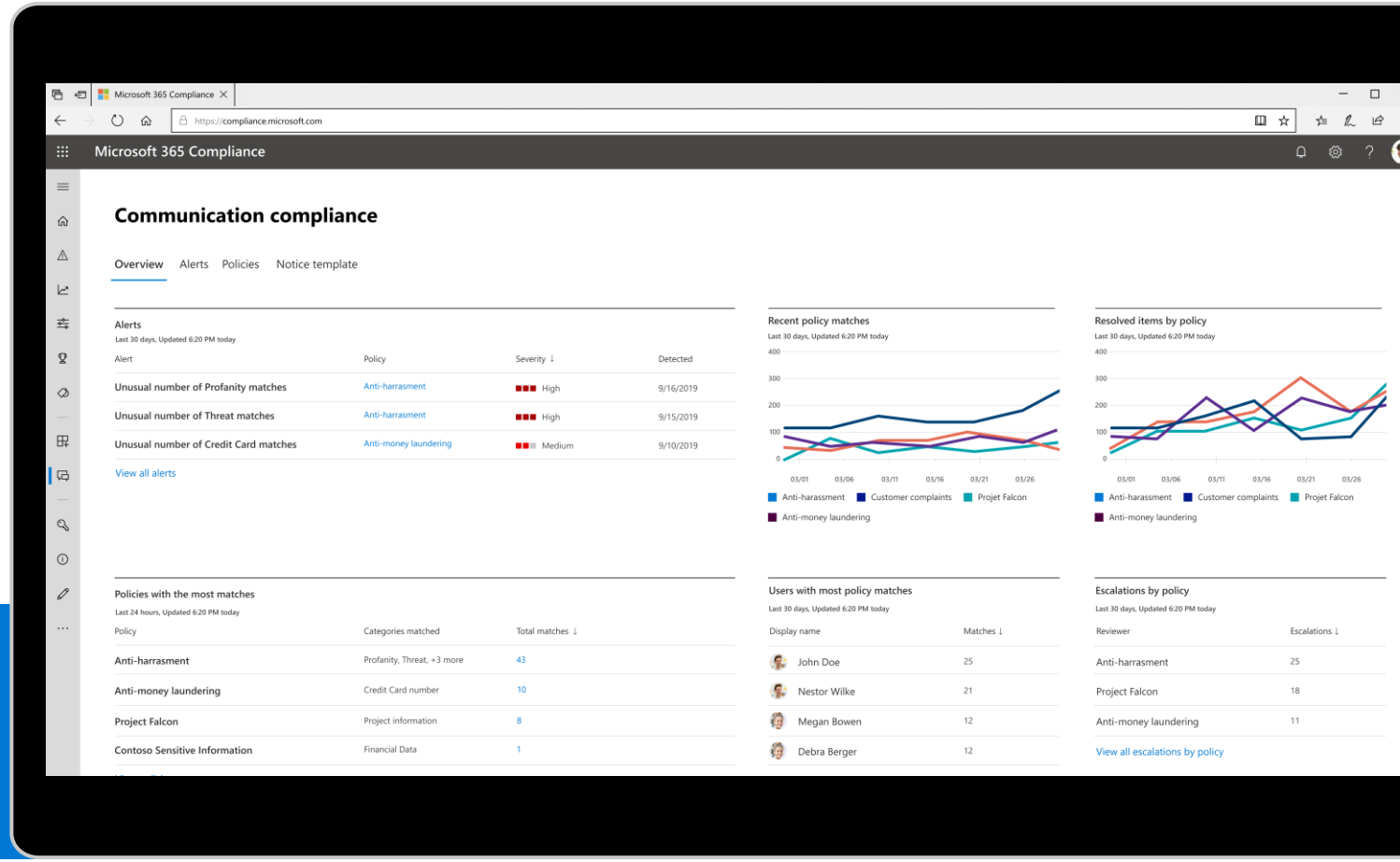
Leverage machine learning to detect violations across Teams, Exchange and third-party party content

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

Power Automate

Digital Transformation ++

@AnaDemeny

/anademeny

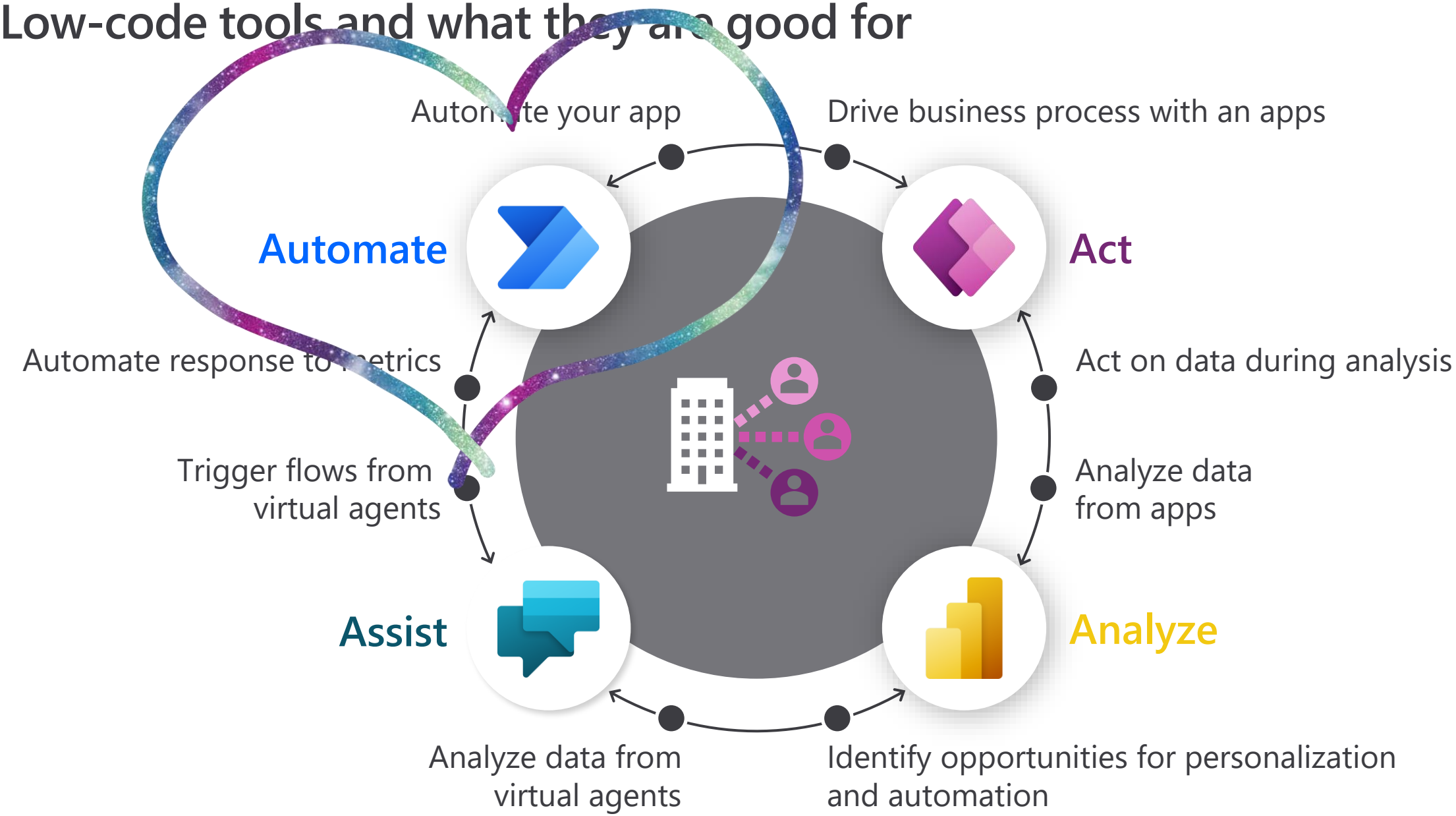
Partner Technical Architect
(INTEGRATION & RPA)

Ally Turnbull

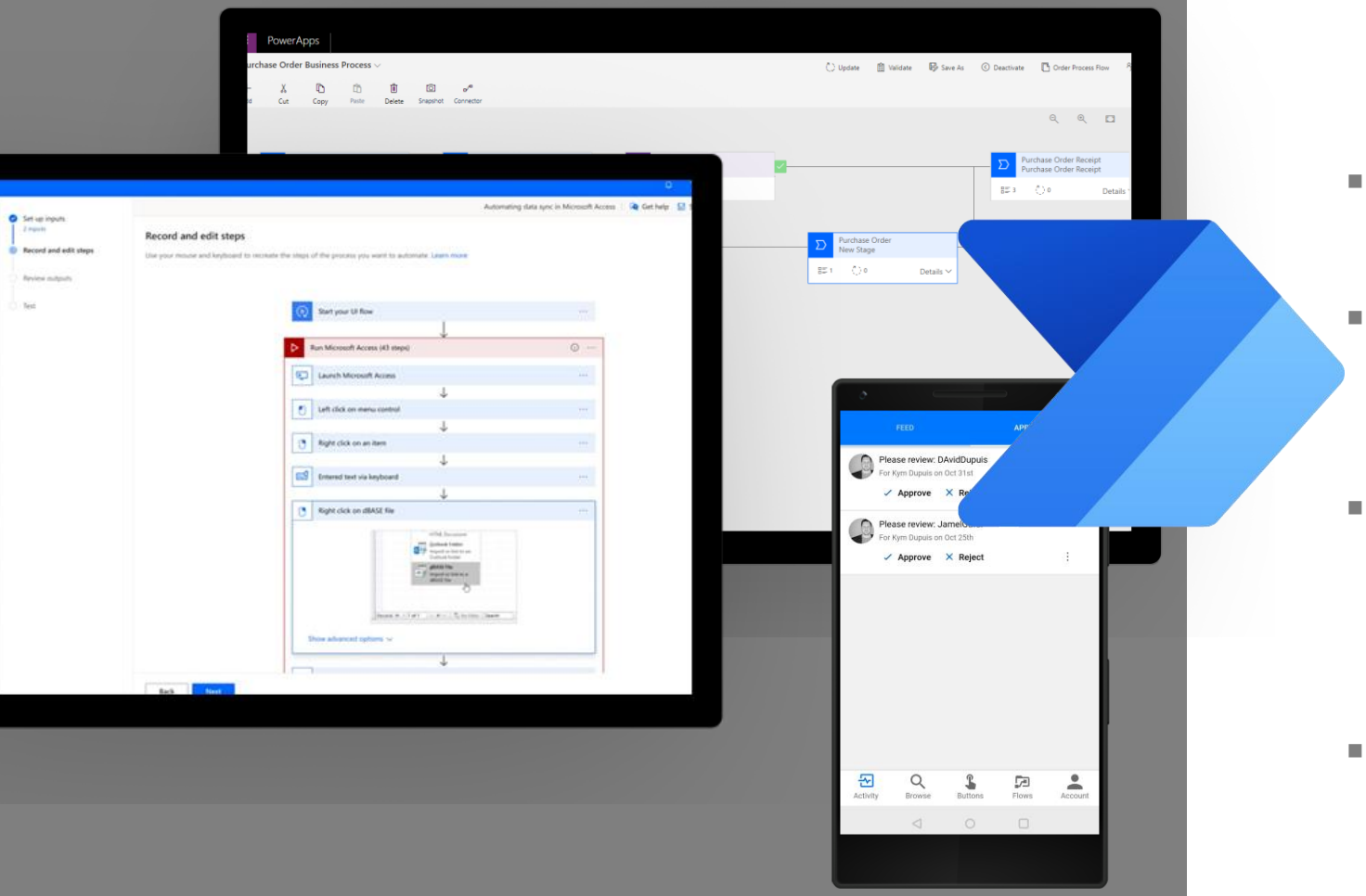
/turnvirtual

Cloud Solution Architect
(Security, Compliance and Identity)

Low-code tools and what they are good for

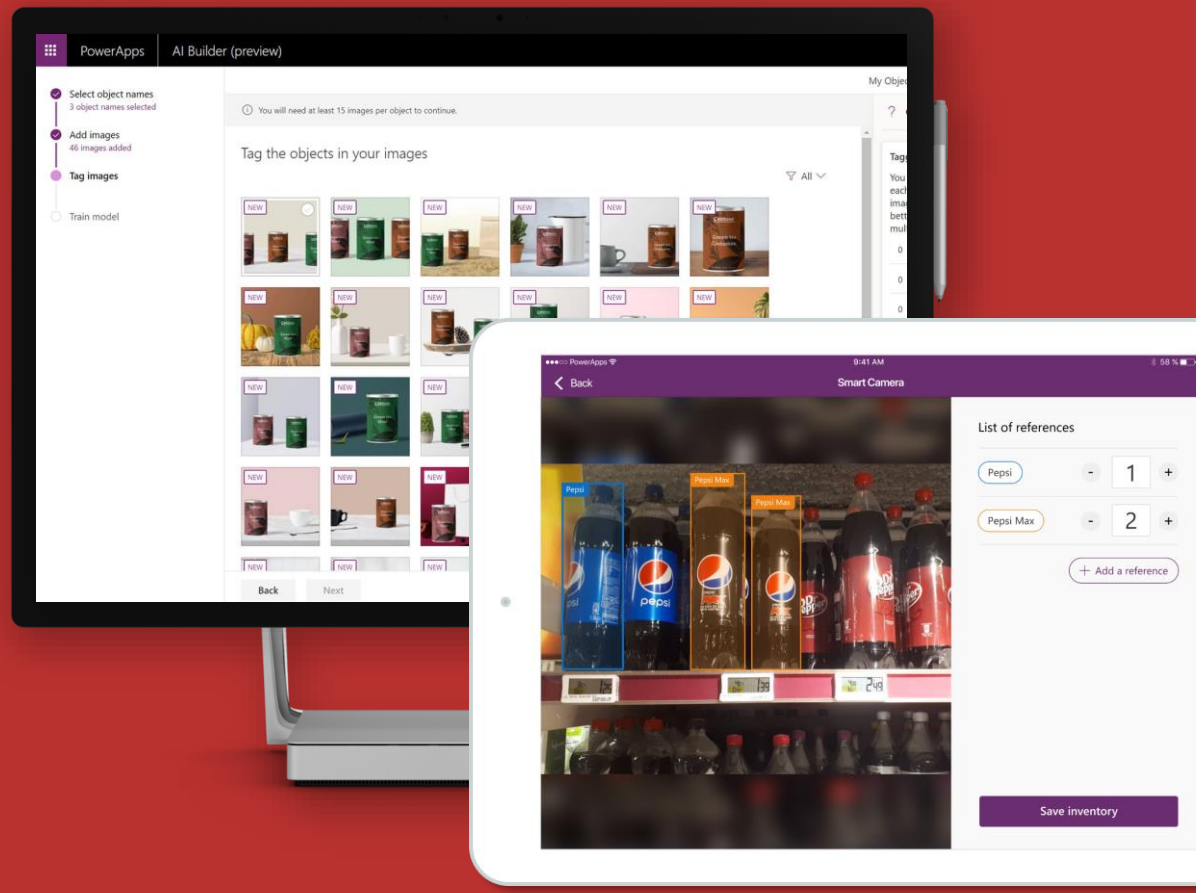


Automate tasks and business processes workflows with Power Automate



- 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

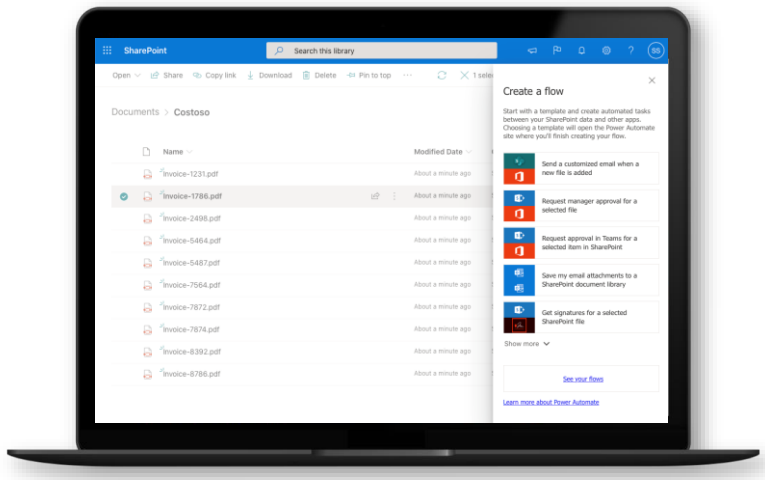


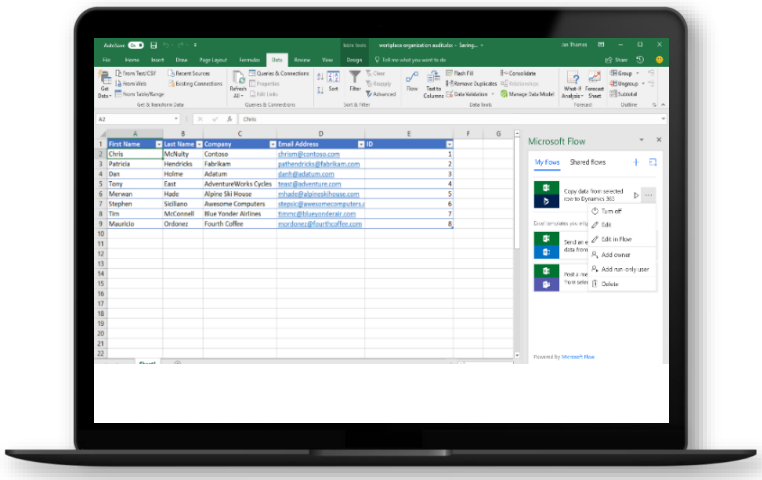
- Every citizen developer is now an AI expert and can easily build, train, deploy and use **AI Builder**
- Create and organize contact and account data more efficiently with **business card scanner**
- Predict outcomes directly from historical business data patterns with **Prediction**
- Spend less time 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**

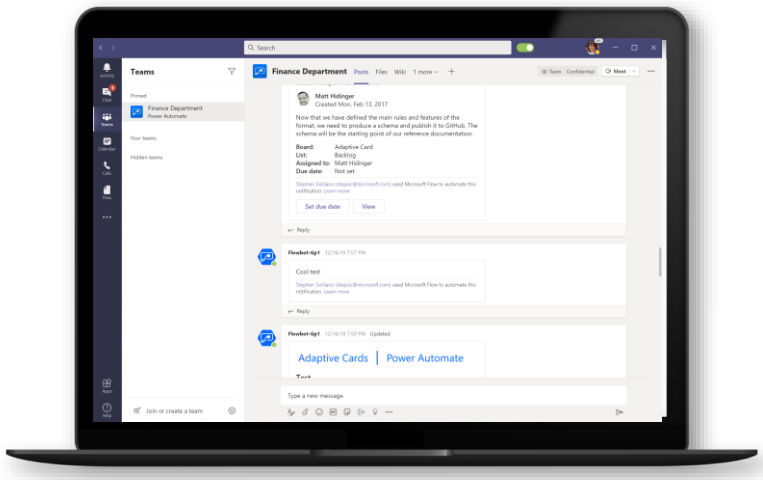
Connect to your company data and services with connectors

- 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





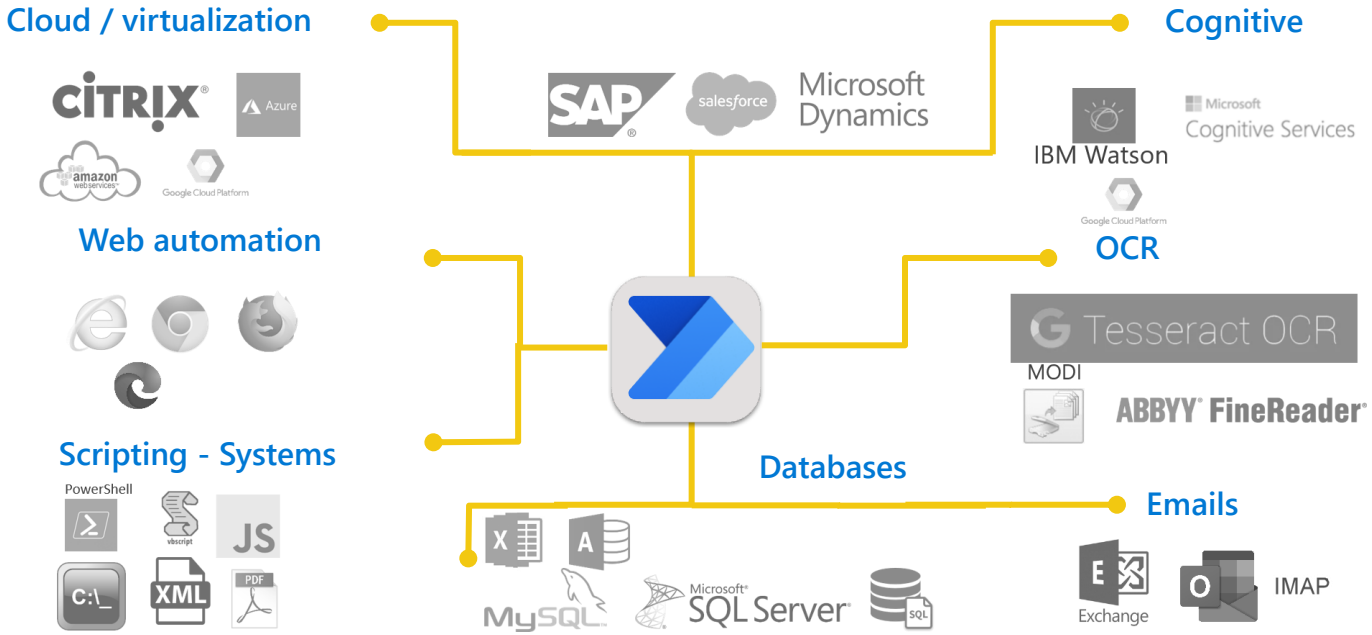


Bridging automation between the old and new

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

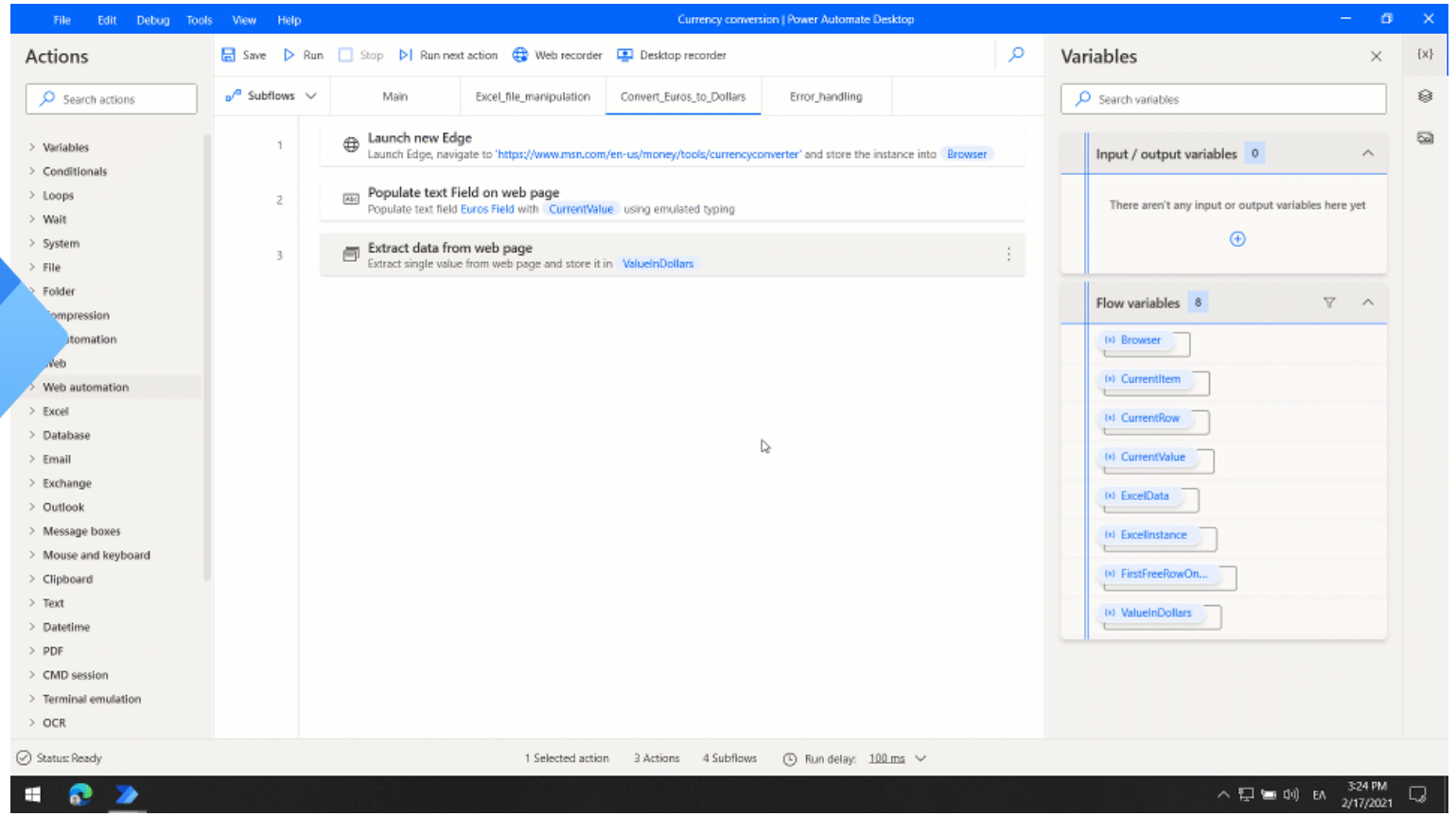
Power Automate Desktop will be available to Windows 10 users **at no additional cost**

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

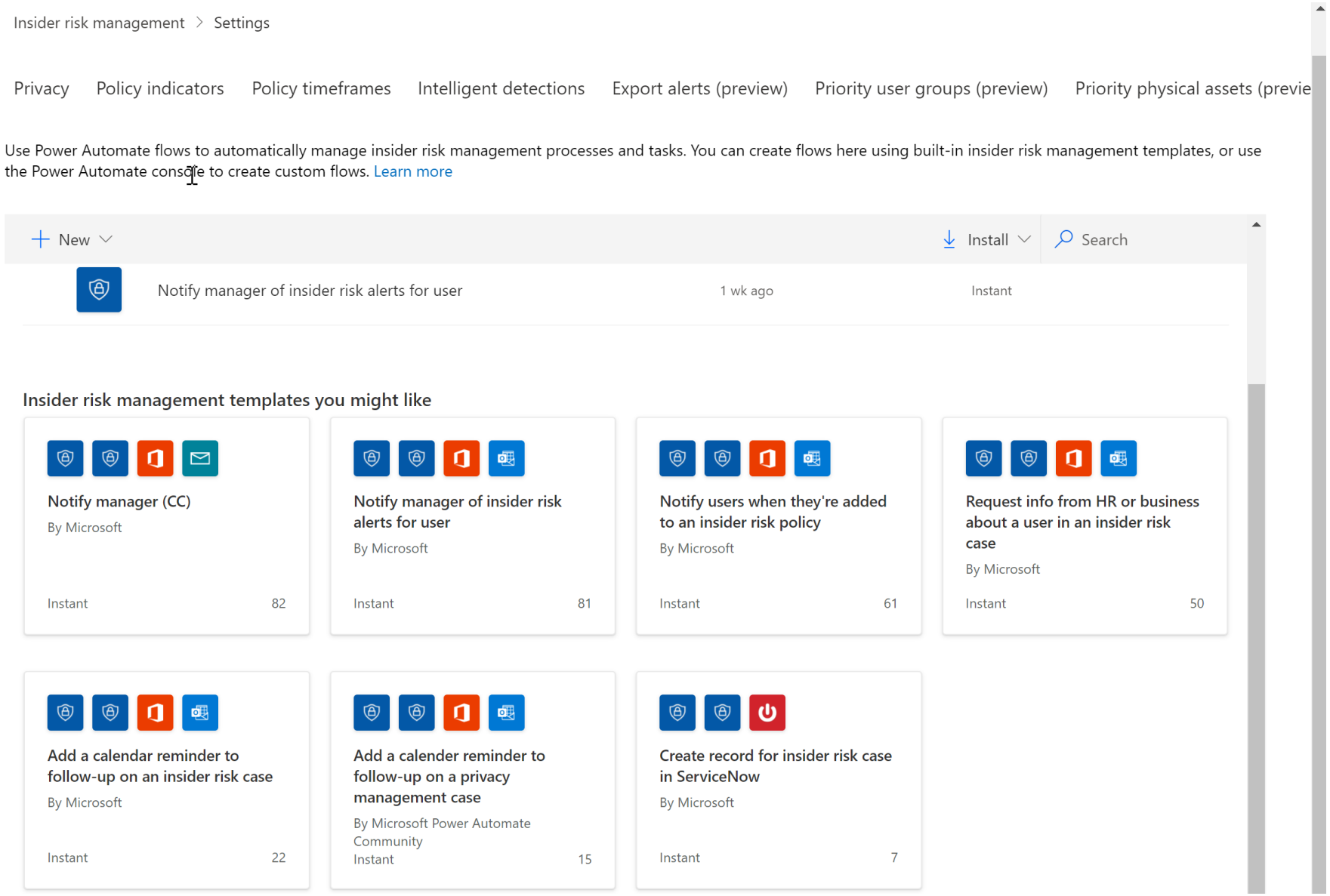
Get started with Power Automate Desktop

Download the Power Automate, Power Apps and Power Virtual Agents Licensing Guides

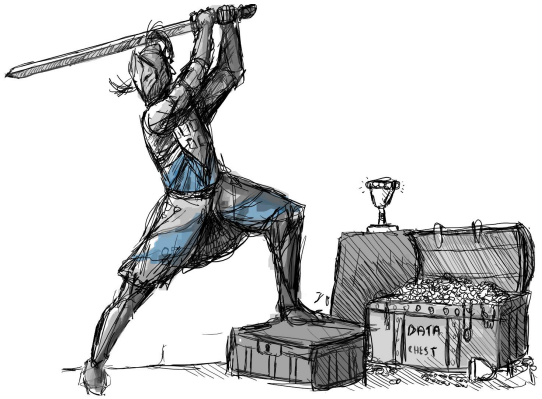
Watch the “Automating benefits for the Communications sector” video



Insider Risk Power Automate Templates (Public Preview)



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

Microsoft

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
3rd, 4th & 5th May

aka.ms/RPAInADay_May

Microsoft
Power Automate

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

Thank you!

@AnaDemeny

/anademeny

Partner Technical Architect
(INTEGRATION & RPA)

Ally Turnbull

/turnvirtual

Cloud Solution Architect
(Security, Compliance and Identity)

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

Microsoft Power Platform

Power Virtual Agents

Partner Technical Architect

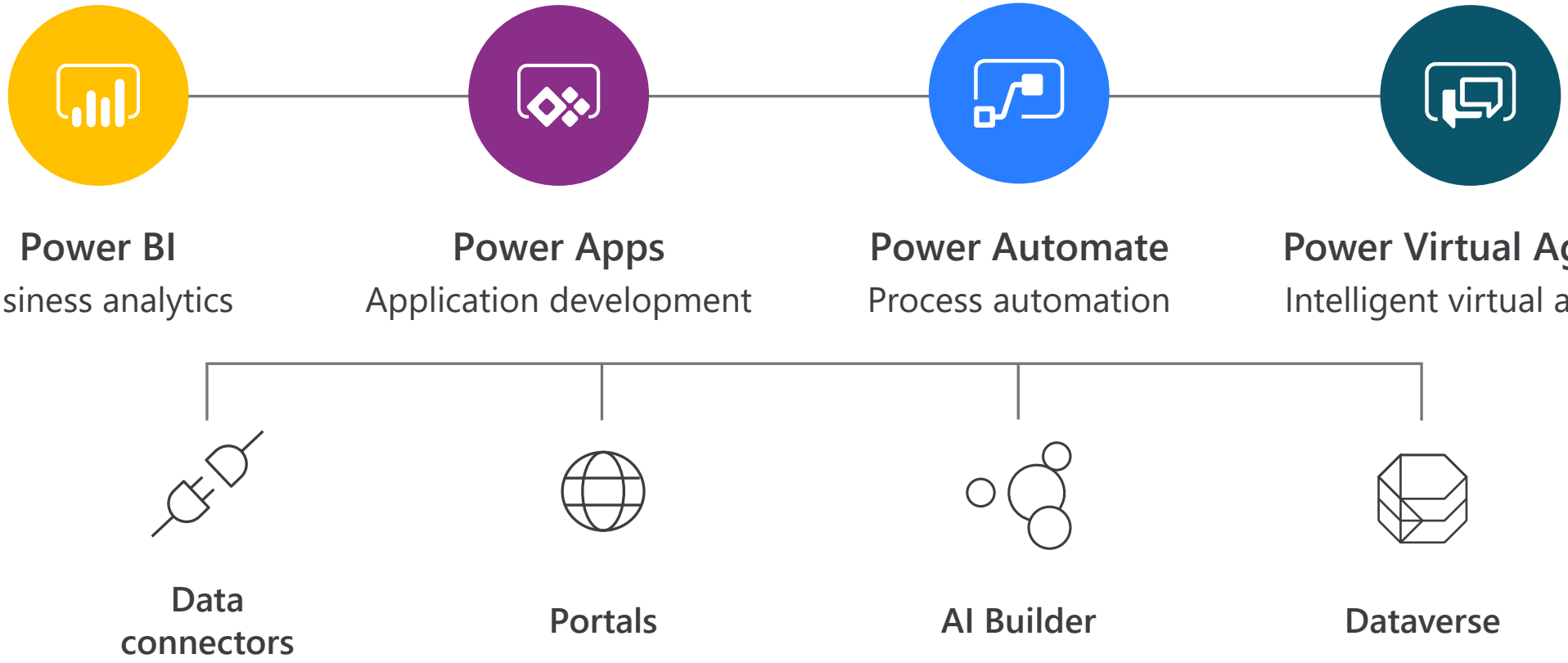
Mark Oburoh

@thatguymarko

Microsoft Power Platform

The low-code platform that spans Office 365, Azure, Dynamics 365, and standalone applications

Innovation anywhere. Unlocks value everywhere.



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

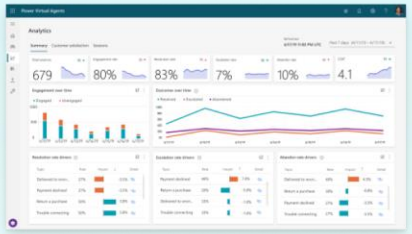
Dataverse

Data connectors

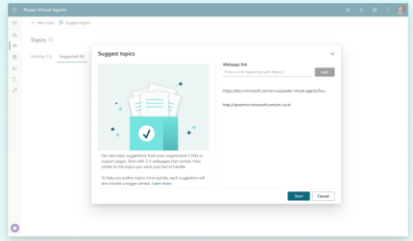
Azure

Power Virtual Agents Lifecycle

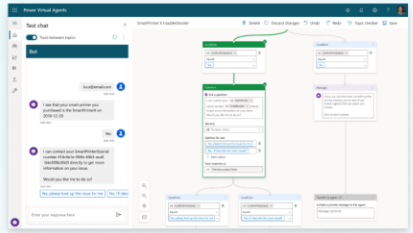
Create Bot using simple, graphical interface



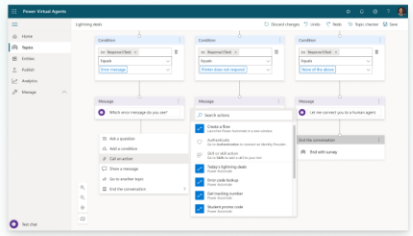
Get starter topics to build upon (from FAQs, sites, etc)



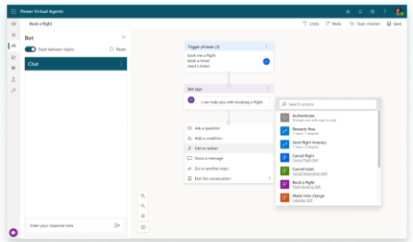
Author topics with NL, slot extraction, variables, etc.



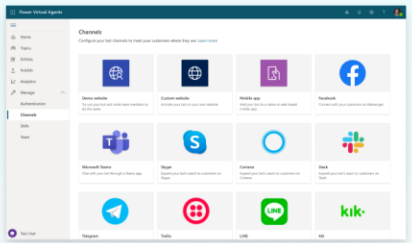
Integrate Bot with backend APIs using MS Flow



Extend Bot with BF Skills for complex scenarios

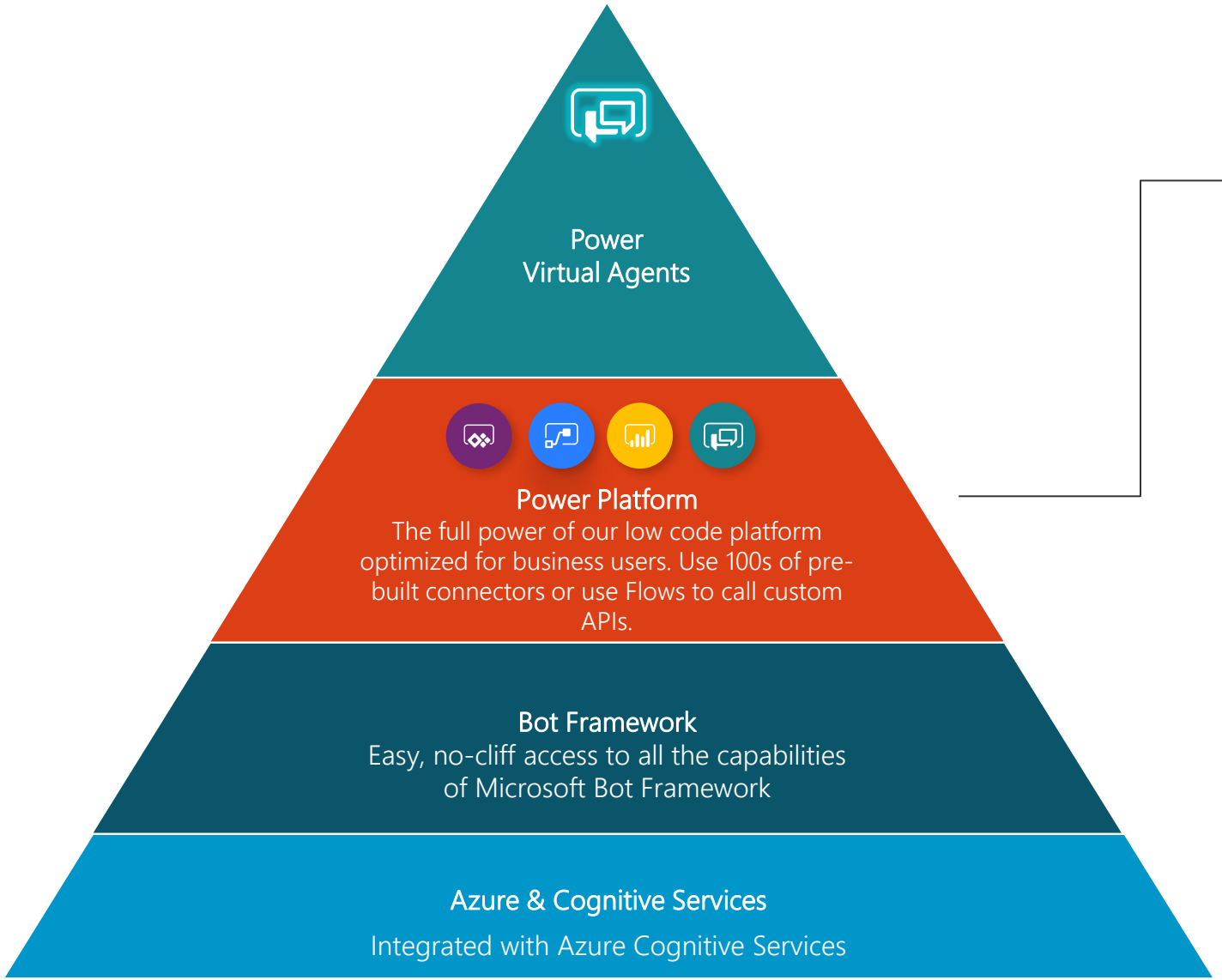


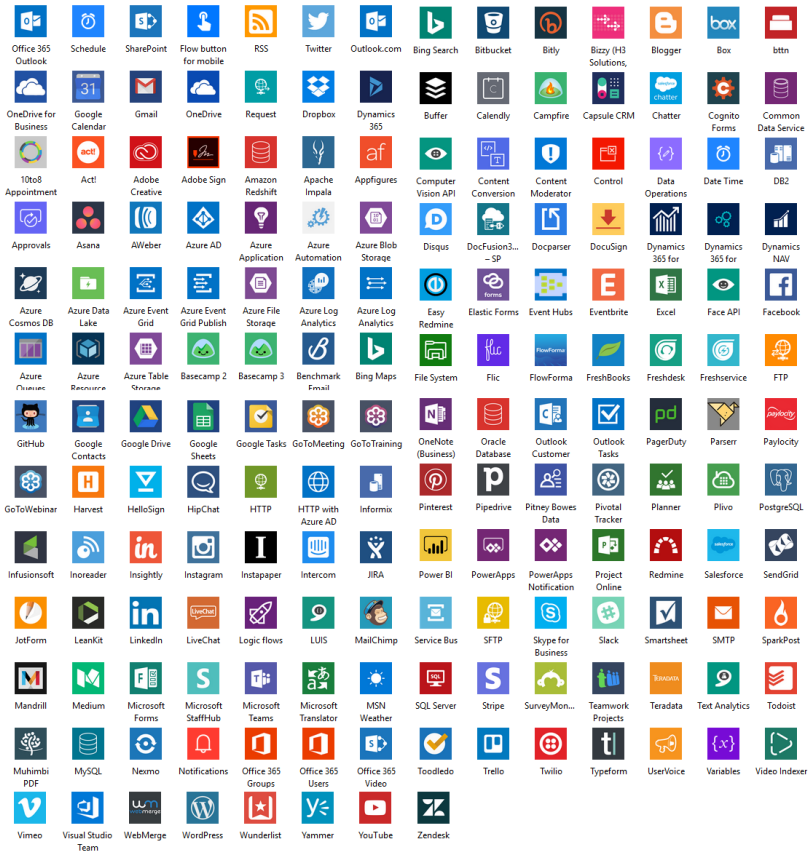
Publish Bot to BF channels



Monitor Bot performance and improve

Built on Power Platform & Bot Framework





Making Bots Easy

Simple, graphical bot creation

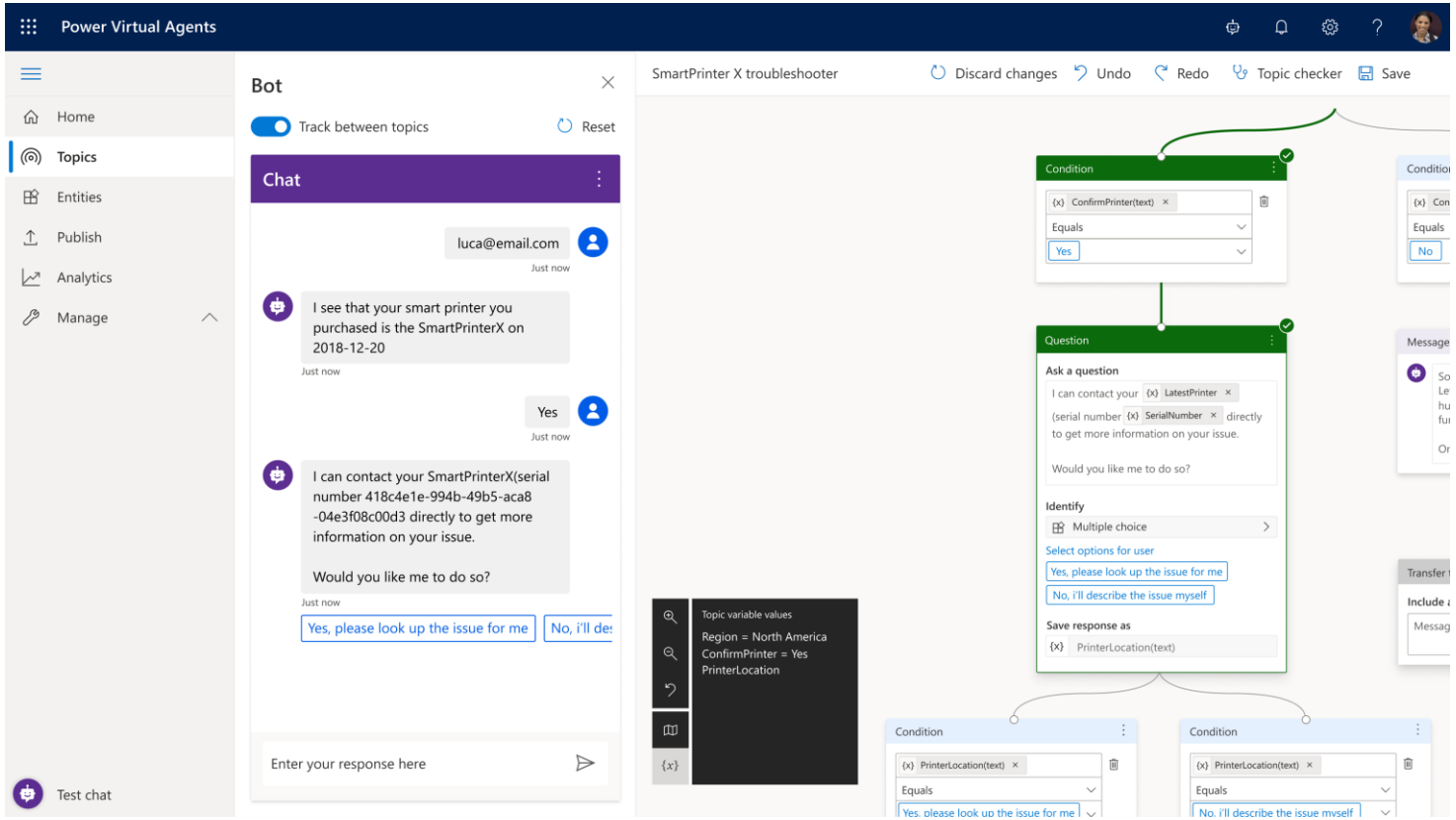
Easily test and maintain bots through a simple, easy to use graphical interface

Extract information from user responses

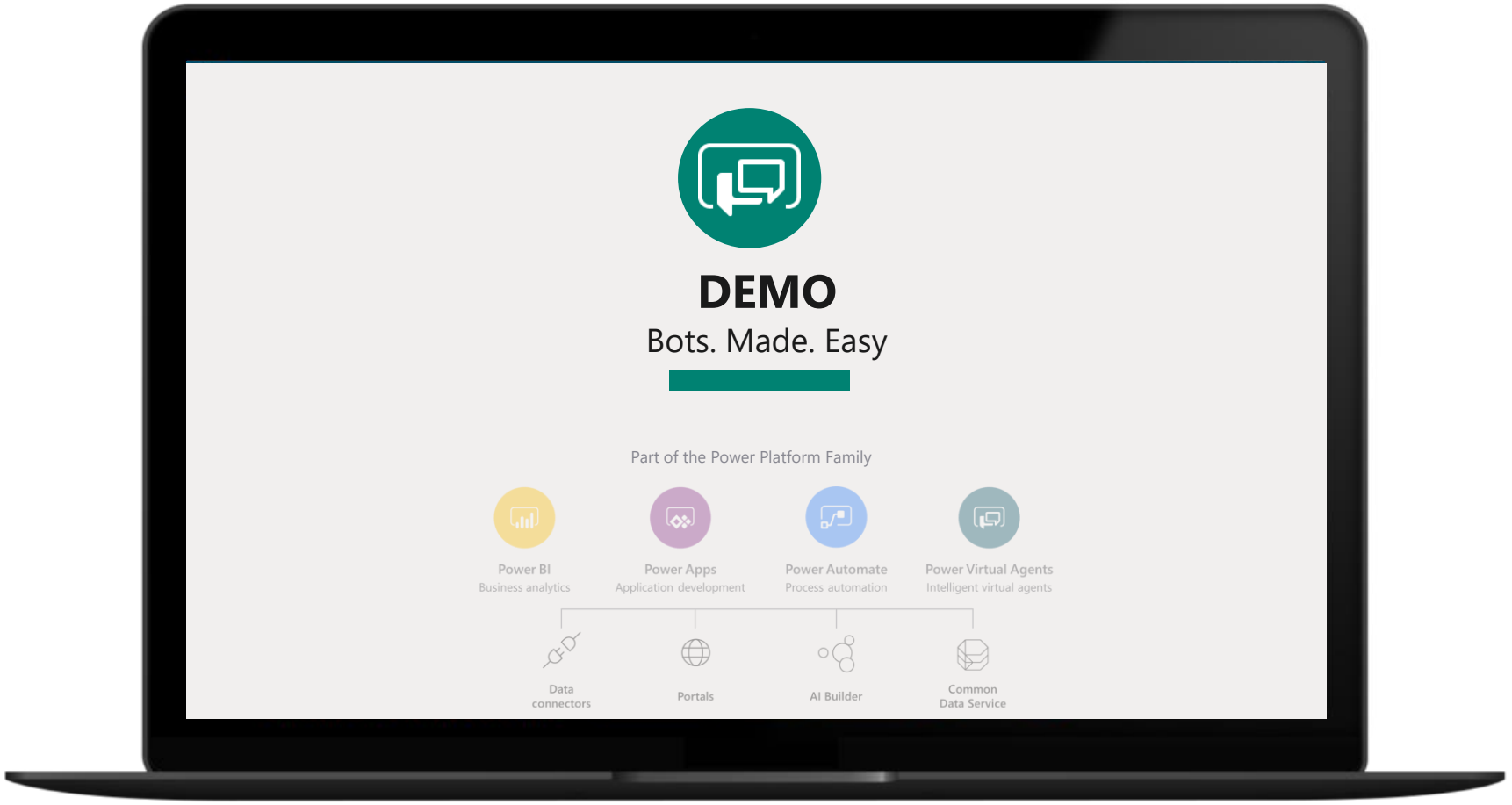
Recognize, extract, and act on dozens of common entities in a user's responses. For example, colors, currencies, ages, dates and times. Or create your own custom entities, e.g. model numbers

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

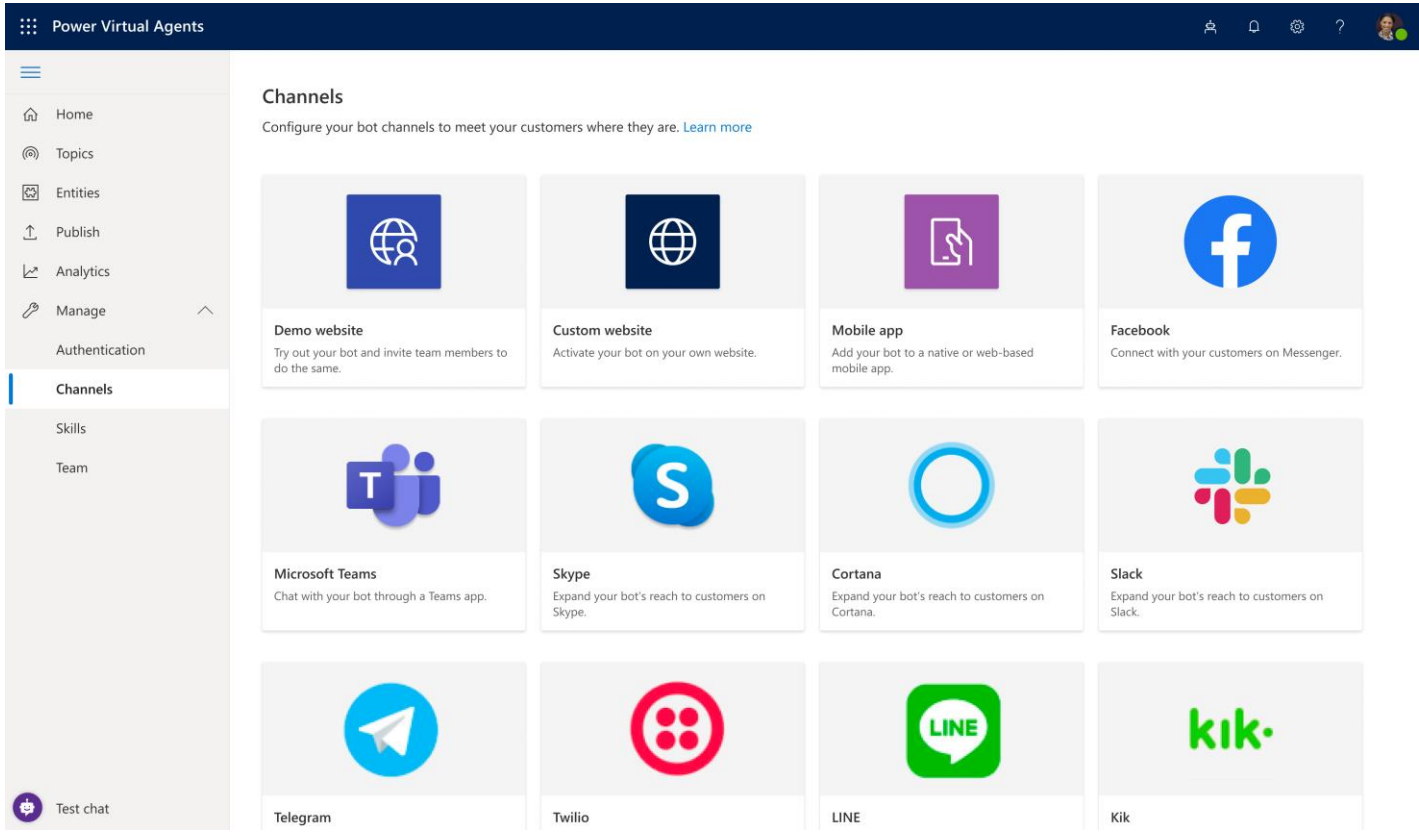
Use bots wherever you need them:

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



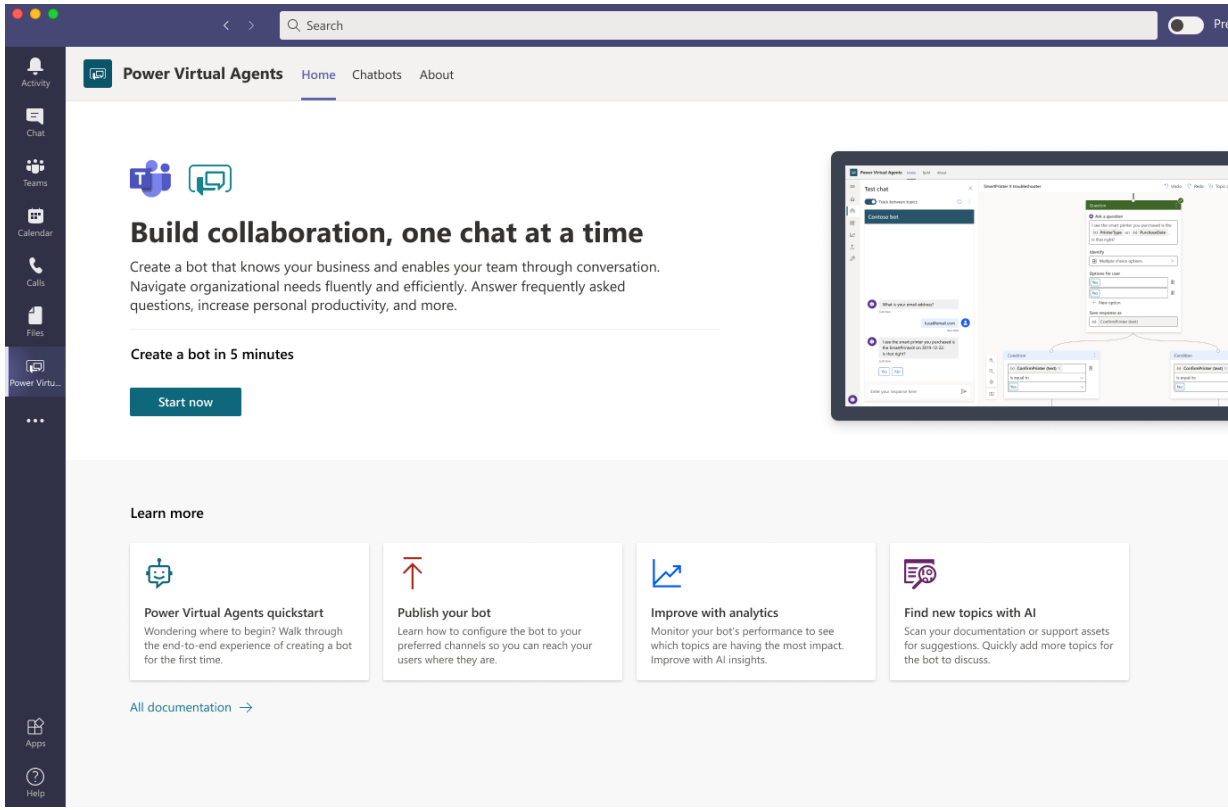
Power Virtual Agents for Teams vs Power Virtual Agents Standalone

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.



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

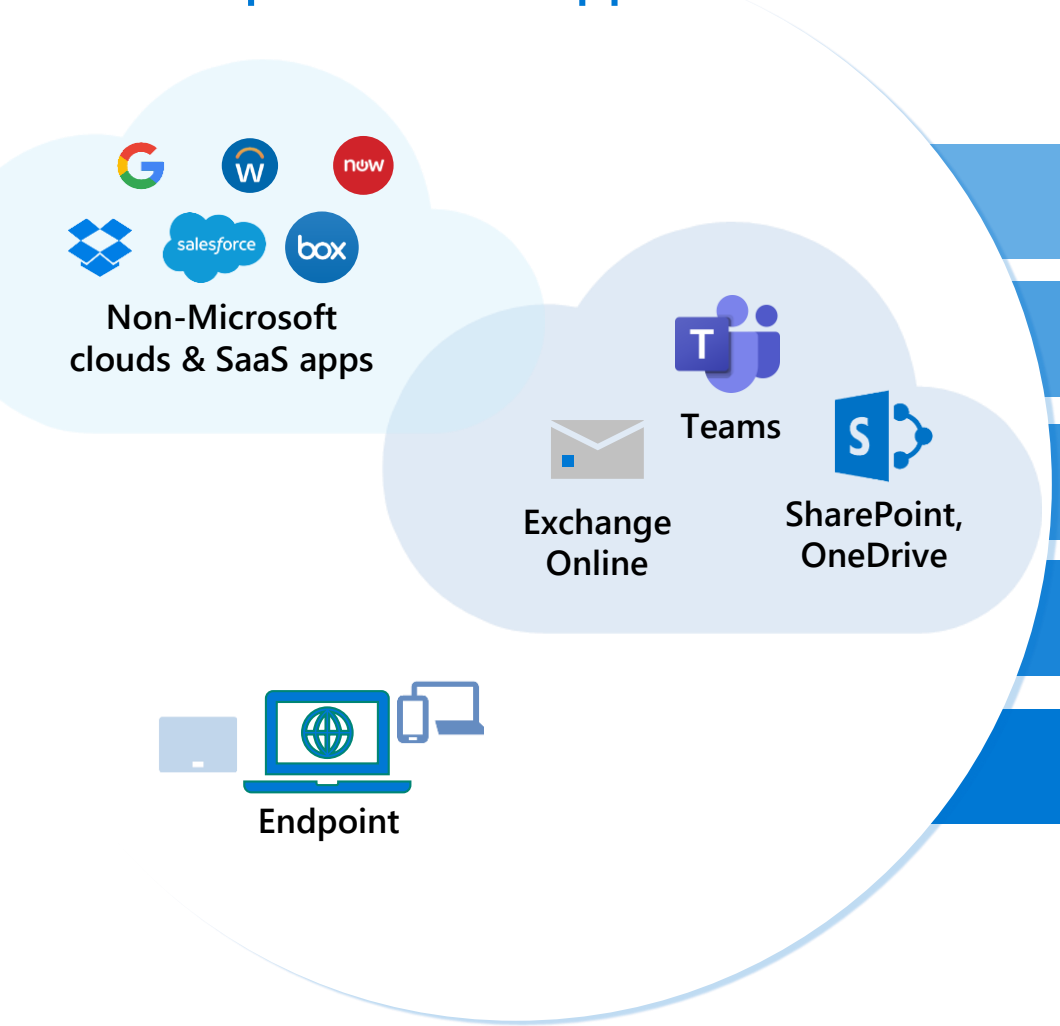
Power Virtual Agents Product Blog and Yammer group

Advanced DLP Monitoring with Sentinel

Microsoft

Data Loss Prevention

Comprehensive support across workloads with unified and integrated experiences



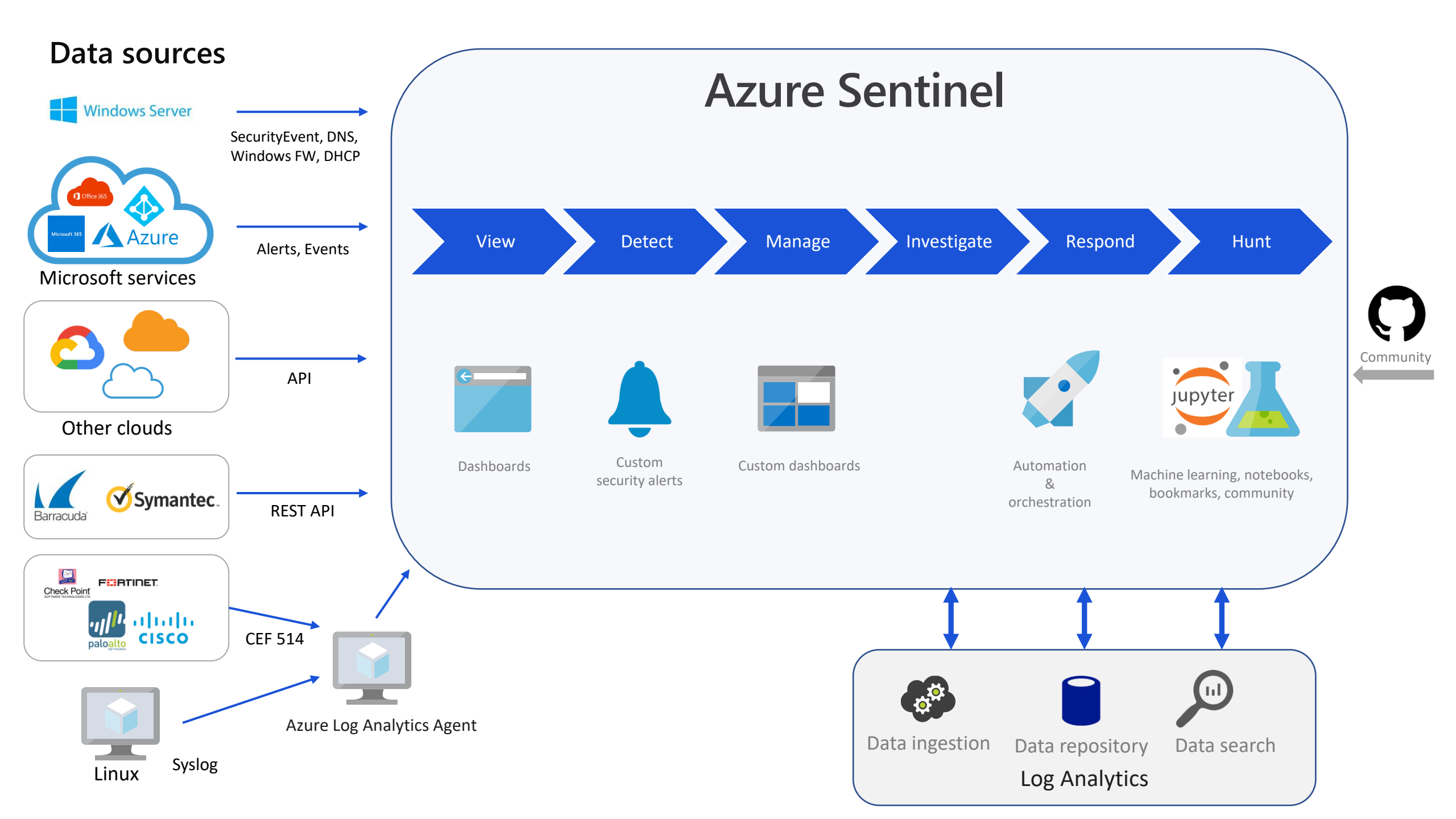
- Guided onboarding
- Unified & flexible policy management
- Integrated with MIP
- Unified alerting & remediation
- Integrated end user experiences

What reporting is available?

Can reporting be customised?

How do I investigate an incident?

Can I integrate with XYZ data?


Data sources
Windows Server
SecurityEvent, DNS, Windows FW, DHCP
Office 365
Microsoft 365
Azure
Alerts, Events
Microsoft services
API
Other clouds
Barracuda
Symantec
REST API
Check Point
FORTINET
paloalto
cisco
CEF 514
Azure Log Analytics Agent
Linux
Syslog
Azure Sentinel
View
Detect
Manage
Investigate
Respond
Hunt
Dashboards
Custom security alerts
Custom dashboards
Automation & orchestration
jupyter
Machine learning, notebooks, bookmarks, community
Community
Data ingestion
Data repository
Data search
Log Analytics

OfficeDev / O365-ActivityFeed-AzureFunction

master O365-ActivityFeed-AzureFunction / Sentinel / EndPointDLP_preview / 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

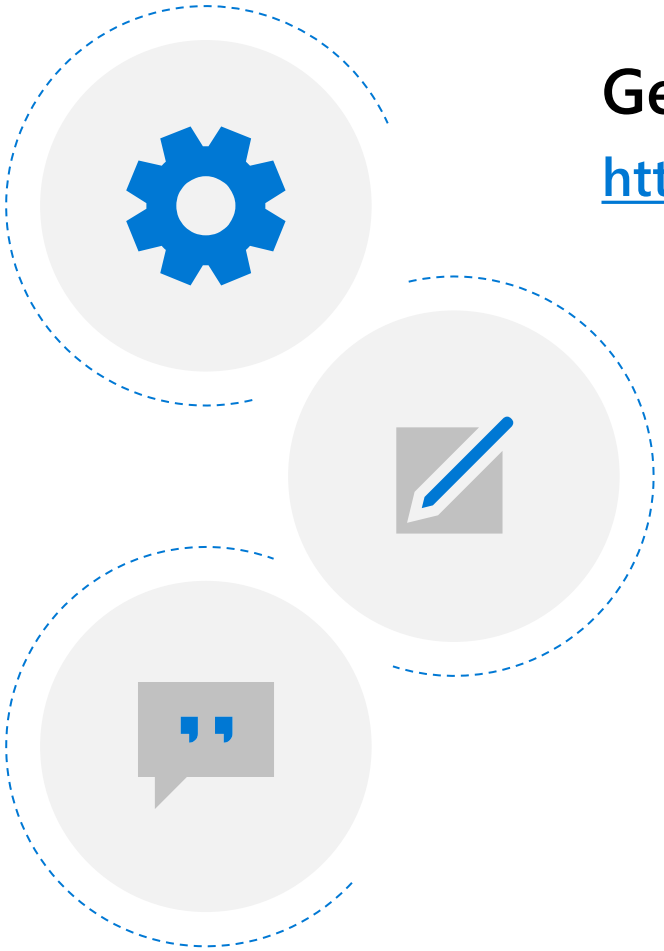
readme.md

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

Microsoft

Azure Purview

UNIFIED DATA GOVERNANCE TO MAXIMIZE
THE BUSINESS VALUE OF DATA

Microsoft

Watch @ 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

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,

Microsoft

Data governance is becoming increasingly interdisciplinary

DISCOVERY

What data do I have?
Where did the data originate?
Can I trust it?

COMPLIANCE

What's my exposure to risk?
Is my usage compliant?
How do I control access & use?
What is required by regulation X?

Chief Data Officer

Azure Purview

UNIFIED DATA GOVERNANCE

Data Map

- Automate and manage metadata at scale

Data Catalog

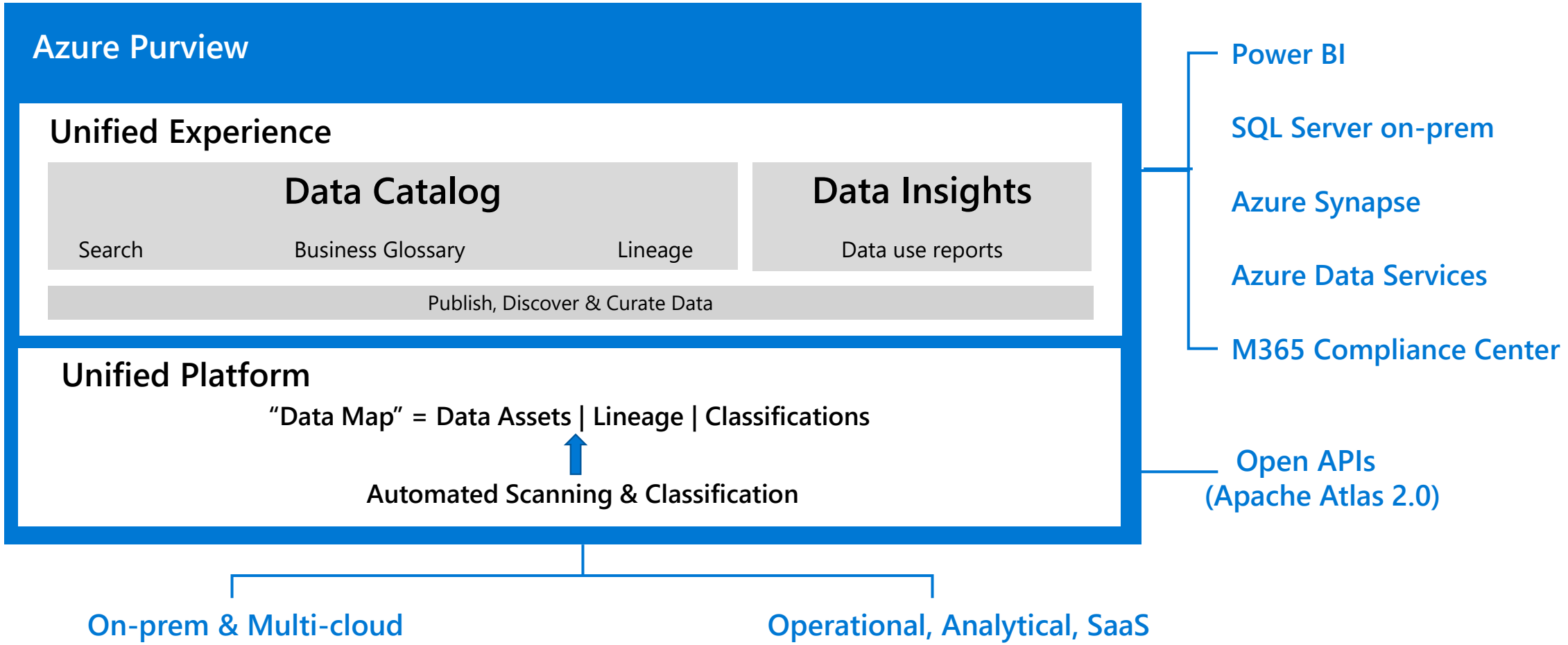
- Enable effortless discovery for data consumers

Data Insights

- Assess data usage across your organization

Microsoft

Azure Purview: Unified Data Governance

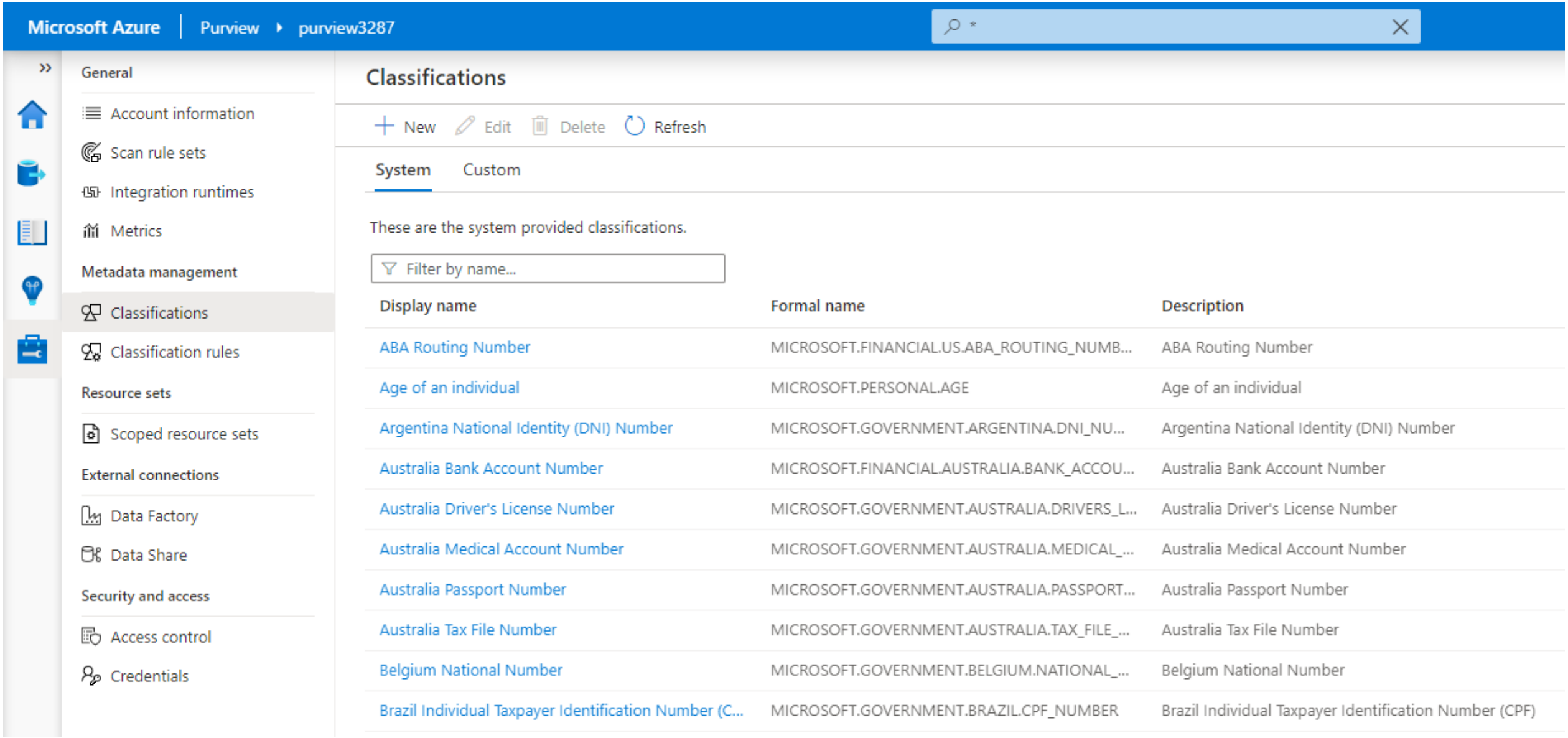


Microsoft

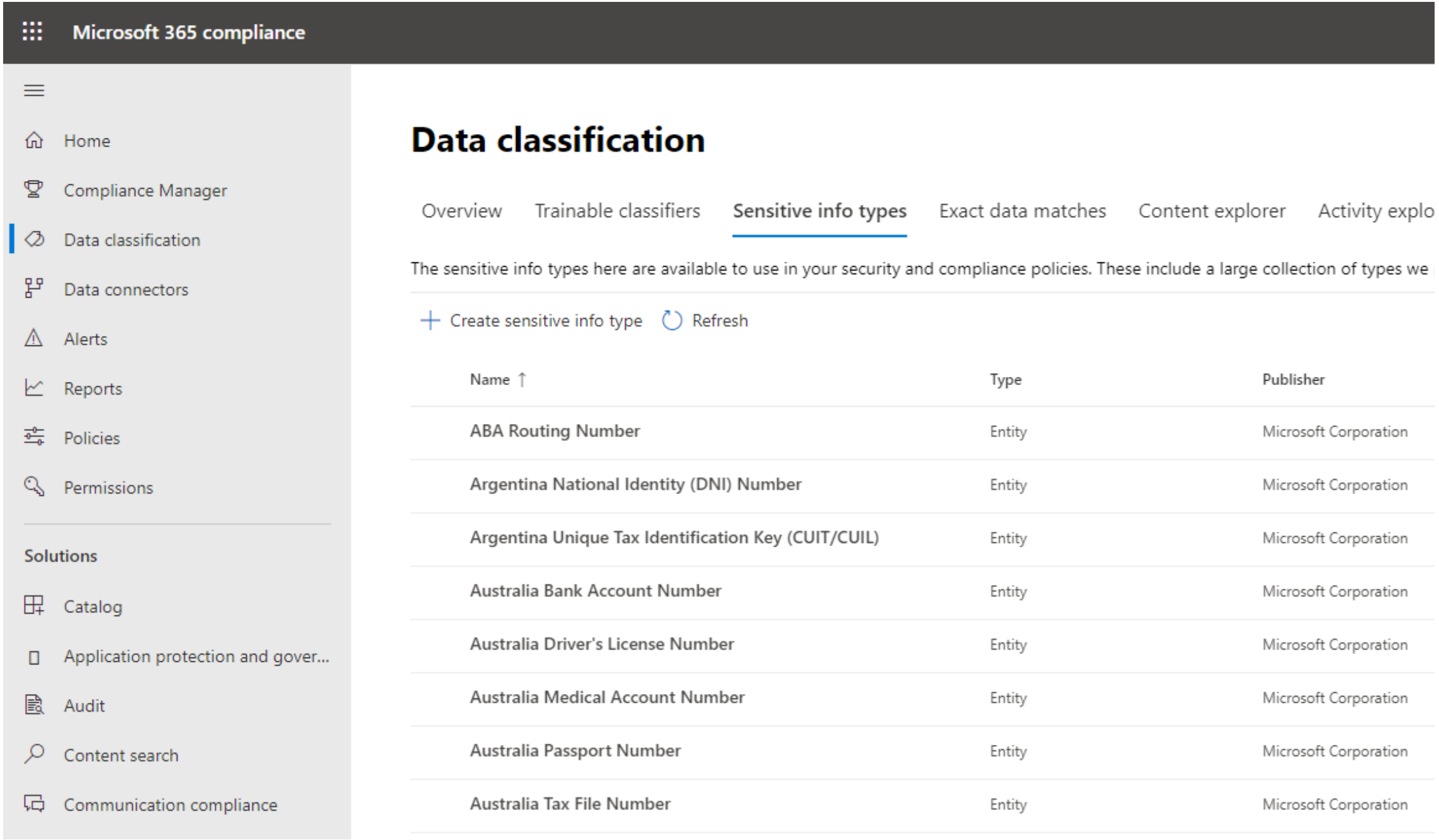
Azure Purview

Demo

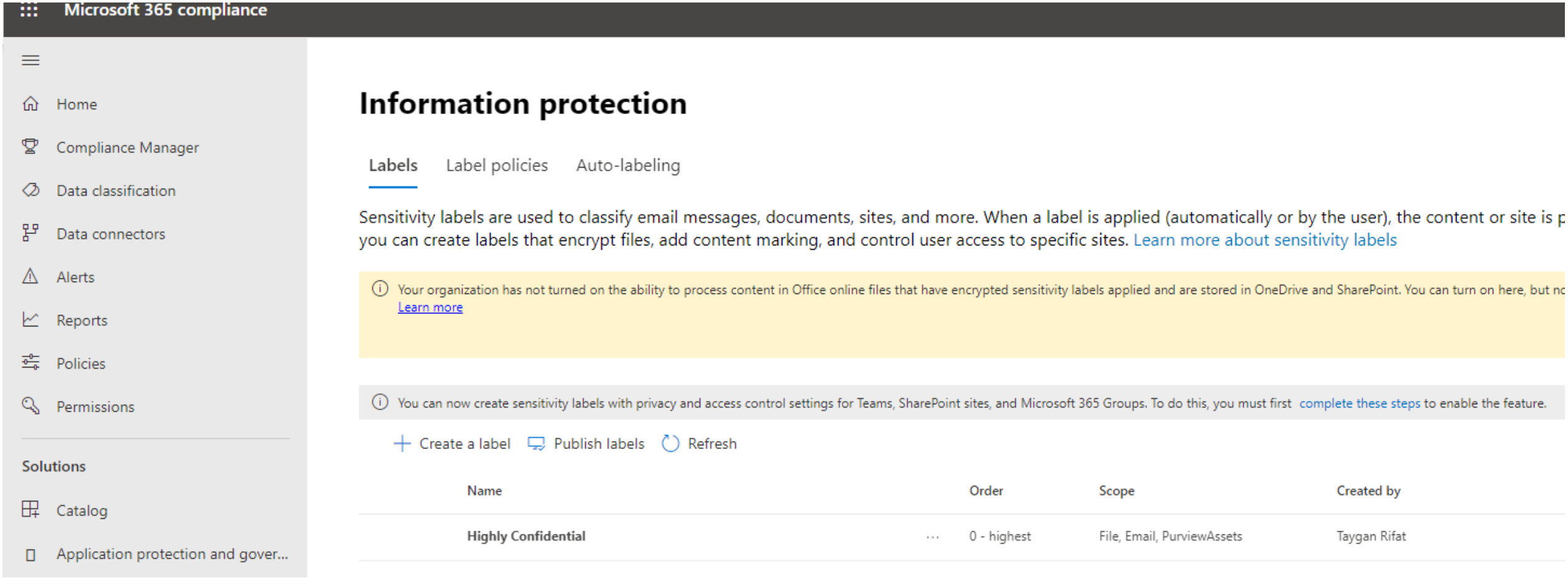
Sensitivity Labels
Security & Compliance Center



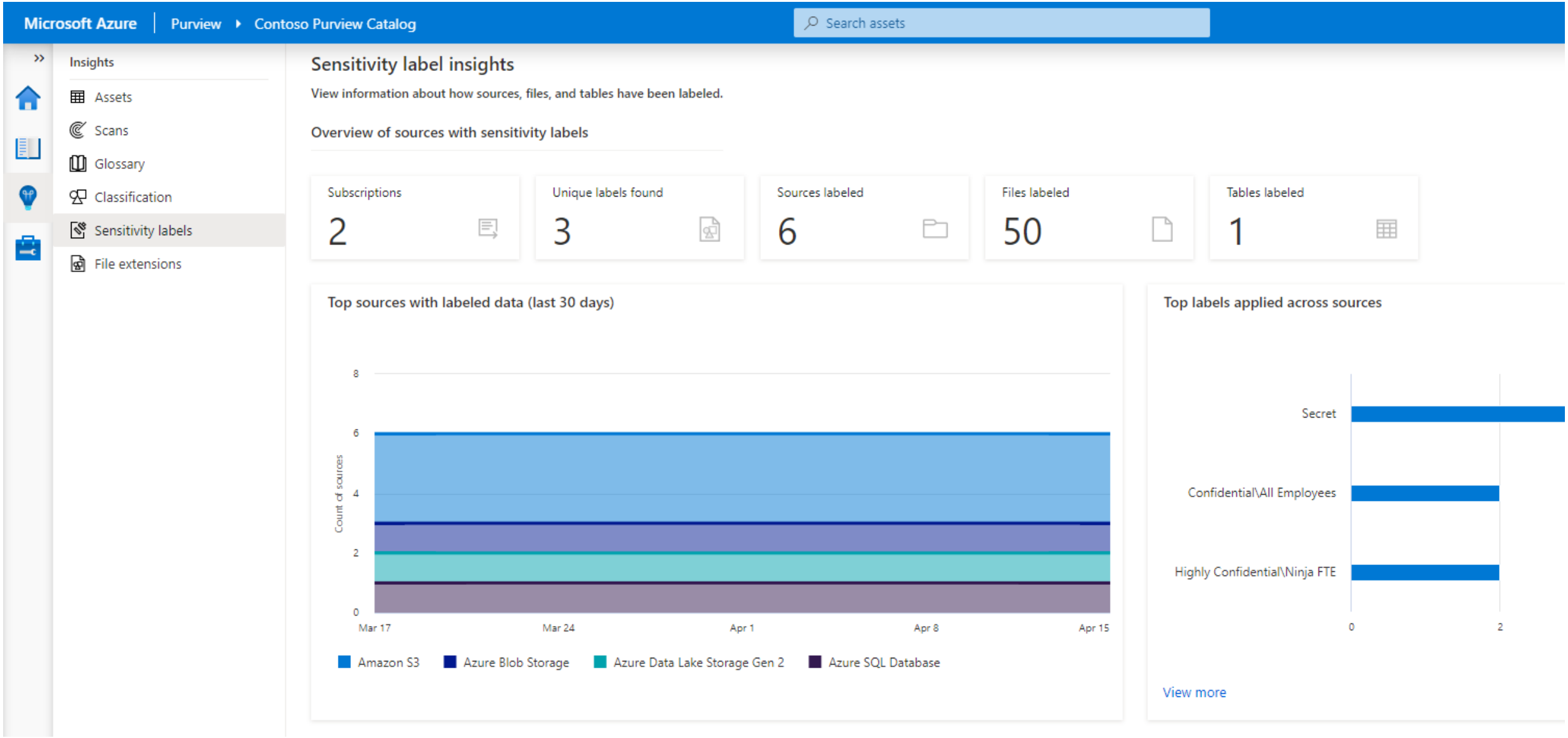
Azure Purview Studio > Management Center > Classifications



Microsoft 365 Compliance Center > Data Classification > Sensitive Info Types



Microsoft 365 Compliance Center > Information Protection > Sensitivity Labels

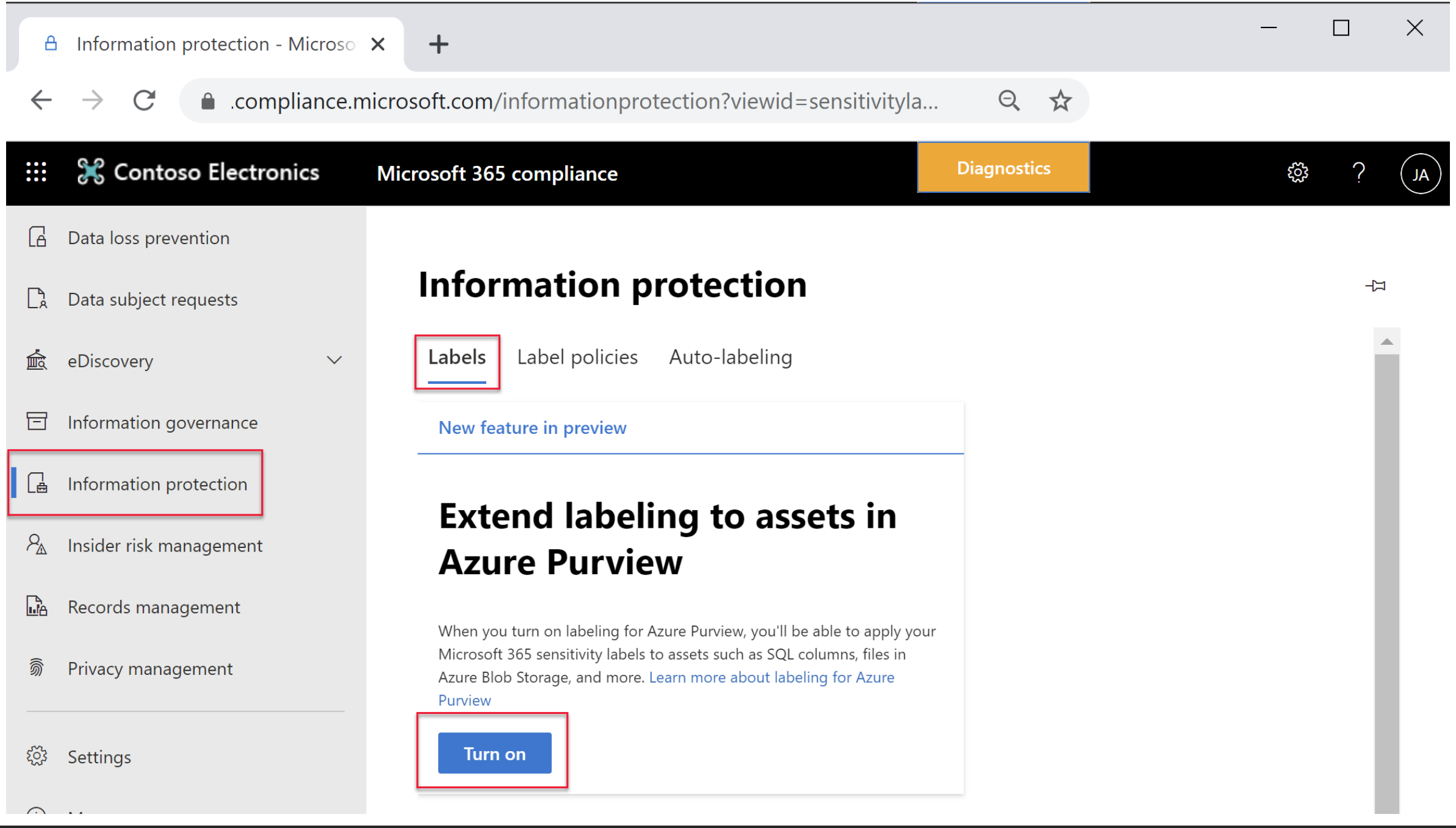


Azure Purview Studio > Insights > Sensitivity Labels

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	- Azure Blob Storage - Azure Data Lake Storage Gen 1 and Gen 2
Automatic labeling for database columns	- SQL server - Azure SQL database - Azure SQL Database Managed Instance - Azure Synapse - Azure Cosmos DB For more information, see Labeling for SQL database columns below.



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 *

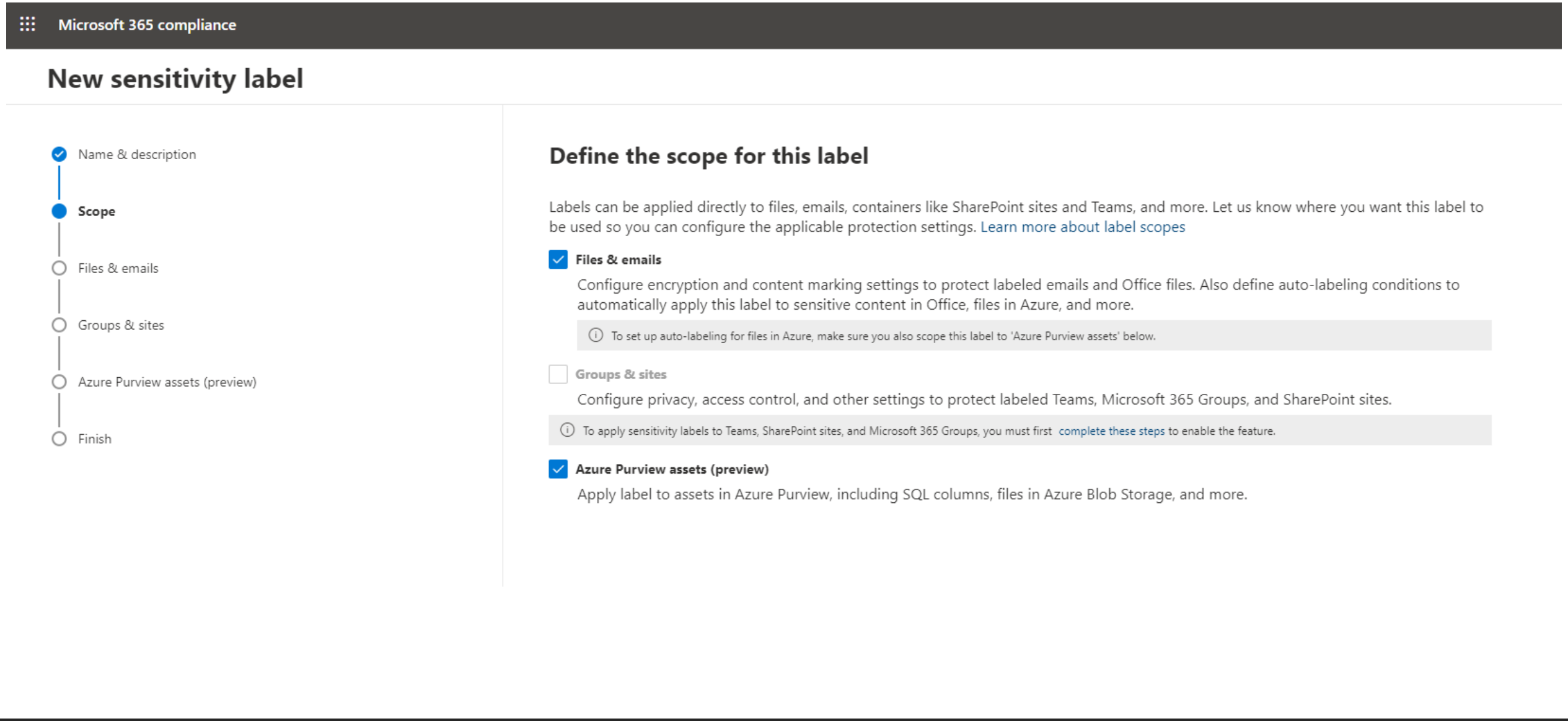
General

Description for users *

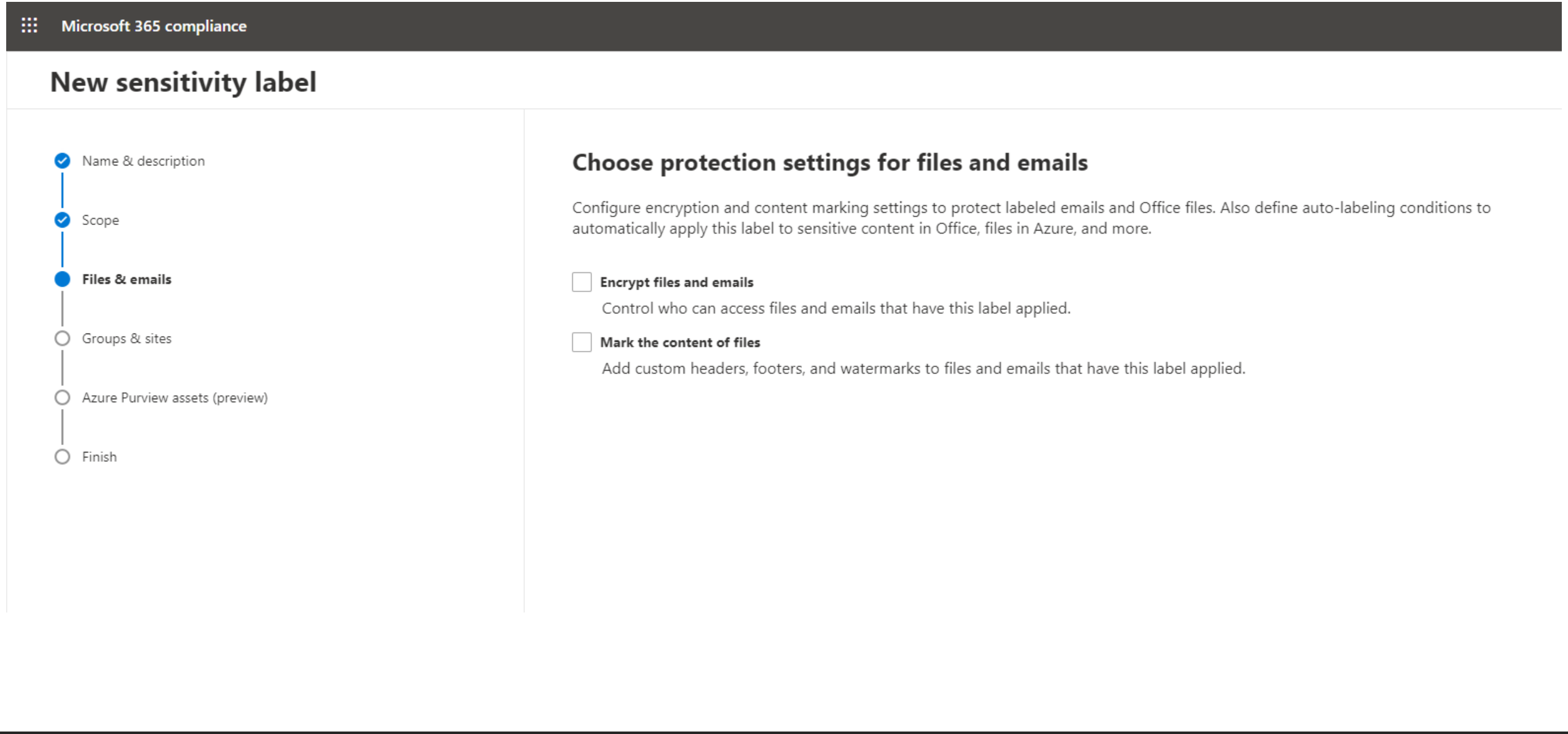
Business data that is not intended for public consumption. However, this can be shared with external partners, as required. Examples include a company internal telephone directory, organizational charts, internal standards, and most internal communication.

Description for admins

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



New Sensitivity Label > Scope



New Sensitivity Label > Files & Emails

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

ⓘ 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

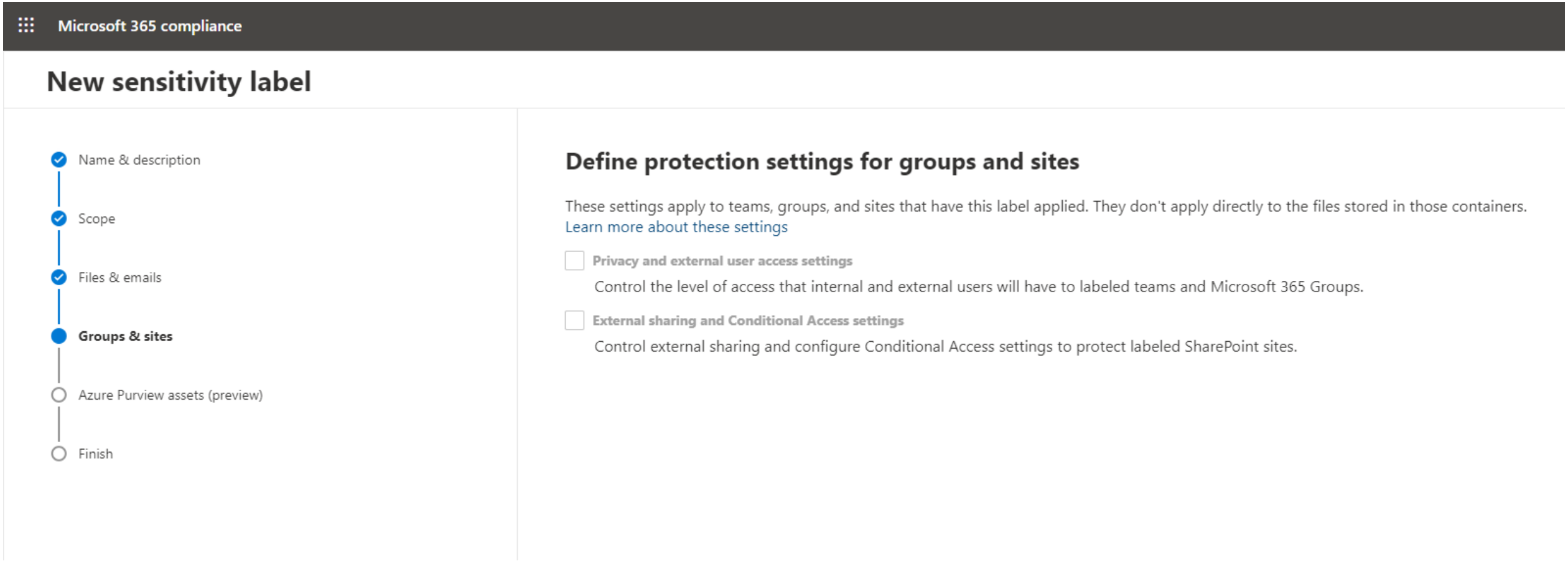
Default — All of these

Sensitive info types

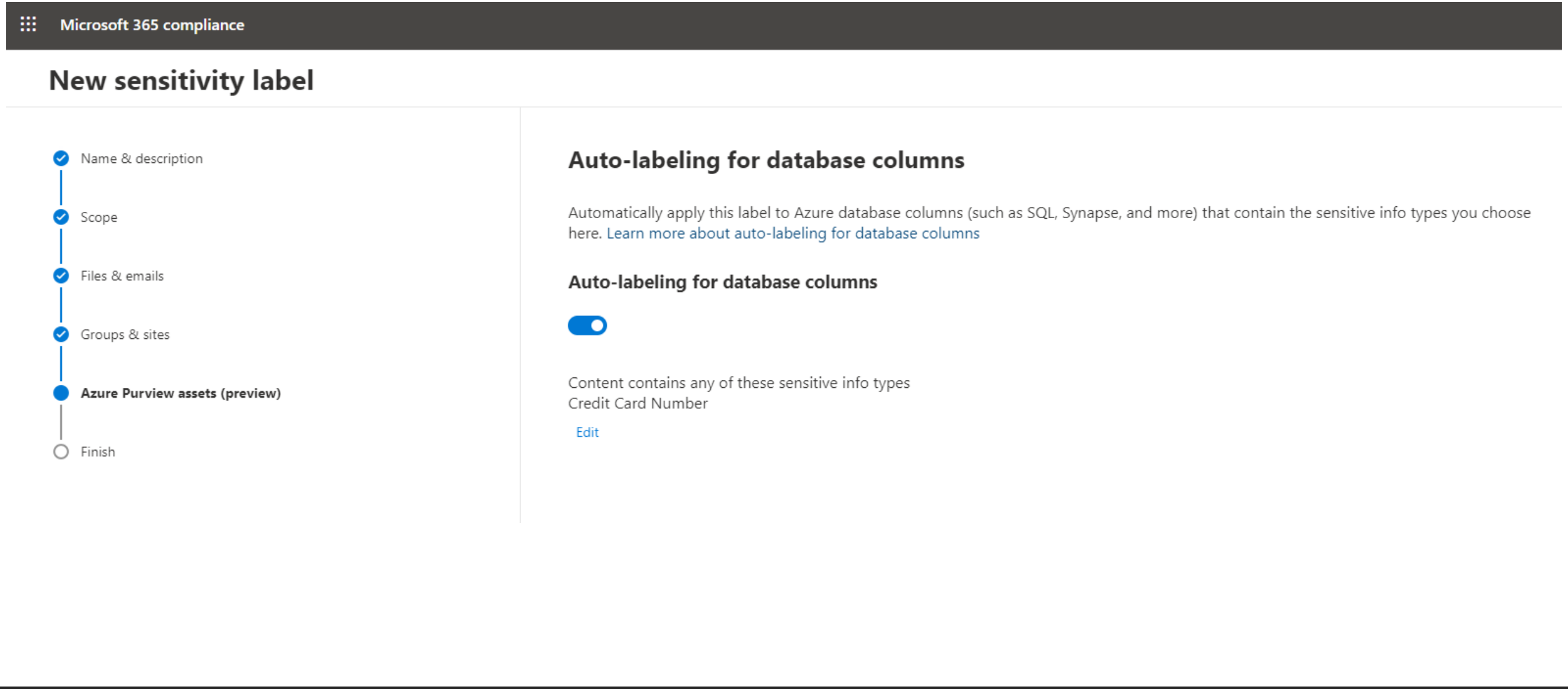
Credit Card Number — High confidence — Instance count 1 to Any

Add

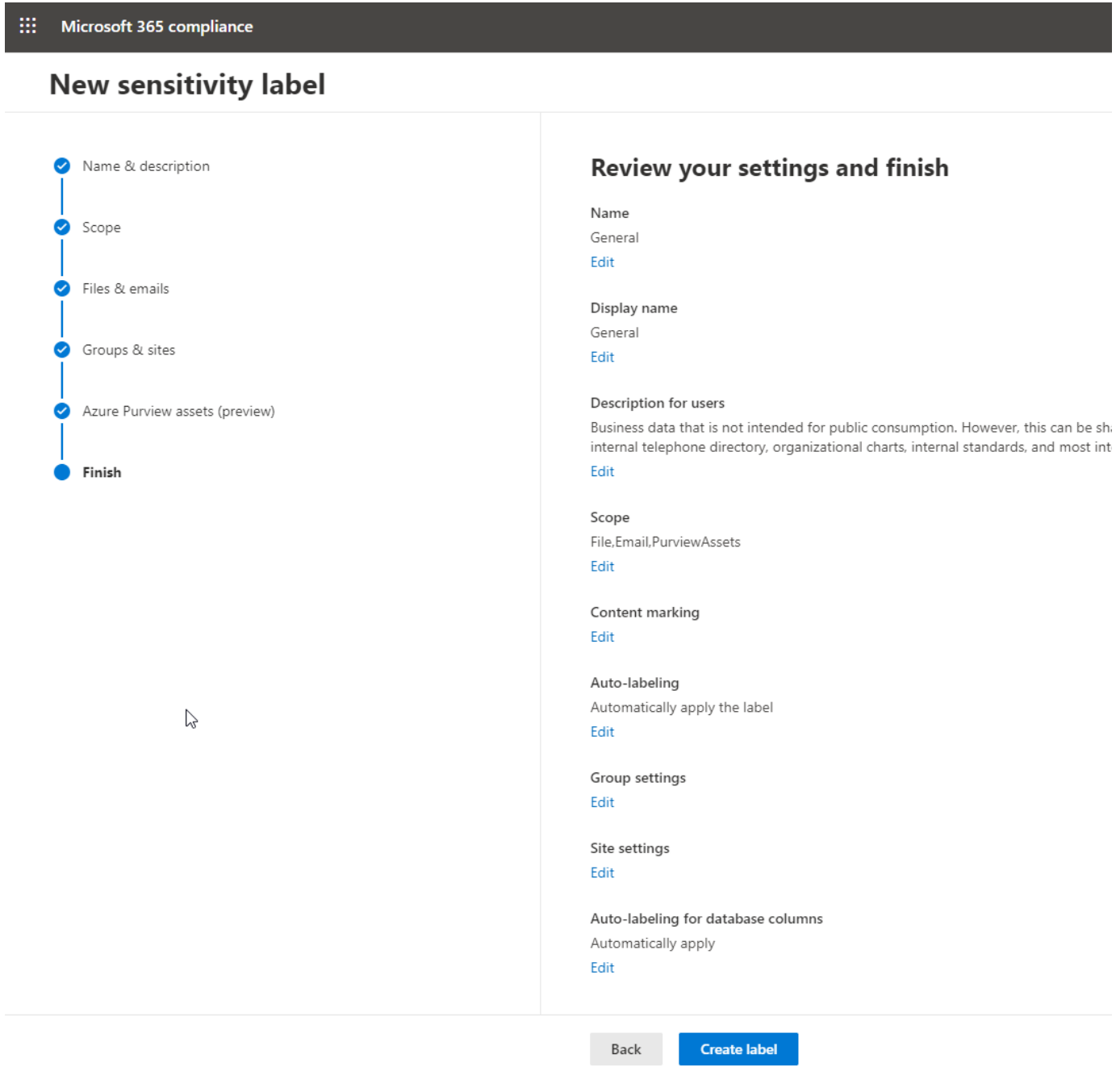
Create group



New Sensitivity Label > Groups & sites

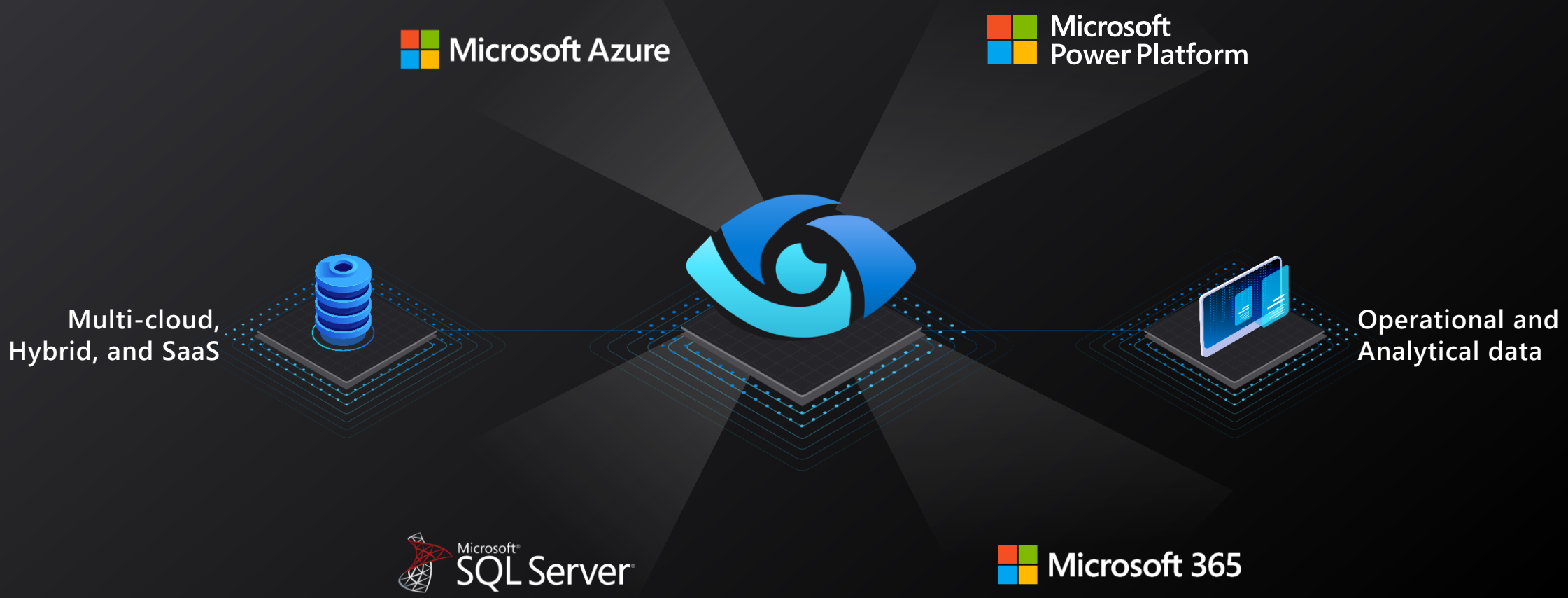


New Sensitivity Label > Azure Purview assets (preview)



New Sensitivity Label > Finish

Make the most of your Microsoft investments



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

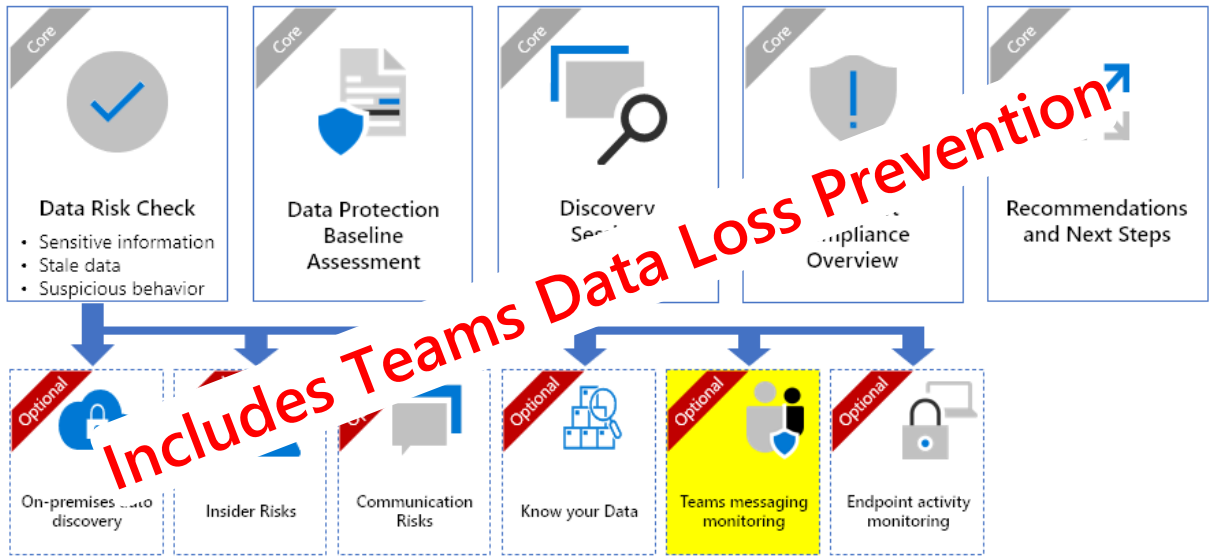
Discover compliance risks of existing data
Insight in the organizations data across the organization

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

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

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 – 26th May and Part 3 – 23rd June

- **Microsoft Defender Masterclass III**
  - 19th May – 9am to 1pm
  - https://aka.ms/defendermasterclass3-reg

- **Microsoft Defender Masterclass IV – Capture the Flag**
  - 17th June – 9am to 1pm
  - https://aka.ms/defendermasterclass4-reg

Power Platform Events from Microsoft UK

RPA In A Day

Power Automate Desktop - Train the Partner event

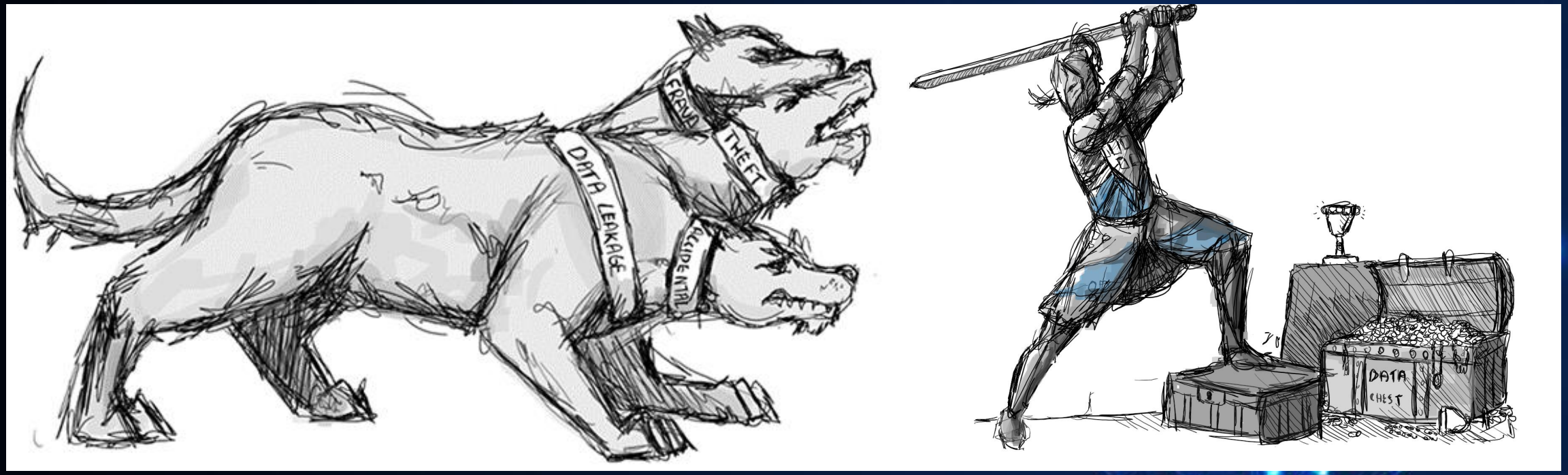
If you're a Power Platform, Dynamics, Modern Work or Azure partner and you're looking to expand your practice to include automation, or indeed if you're already an automation partner considering Power Automate for Desktop, this **free** event the event for you.

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
3rd, 4th & 5th May

aka.ms/RPAInADay_May

Microsoft



Get in touch to build a compliance practice!

Email - Alison.Turnbull@microsoft.com

Microsoft

Feedback –

https//aka.ms/complianceatspeedfeed