Approaches to Managing Insider Risk in a work from anywhere world.

Discover a hub of security excellence and intelligence with Microsoft 365 and insider risk tools.

LIGHTHOUSE

Graham Hosking – Director, Advisory

Intelligent Compliance and Risk Management solutions

Compliance Management

Assess compliance and respond to regulatory requirements.

Information Protection & Governance

Safeguard sensitive data across clouds, apps and endpoints.

Insider Risk Management

Identify and take action on critical insider risks.

Discovery & Response

Quickly investigate and respond with relevant data.

Privacy Management

Safeguard personal data and build a privacy resilient workplace.

How many different types of data risks are out there?

Accidental Sharing

Ransomware

Denial

Fines

Phishing Emails

Overworked Cybersecurity Teams

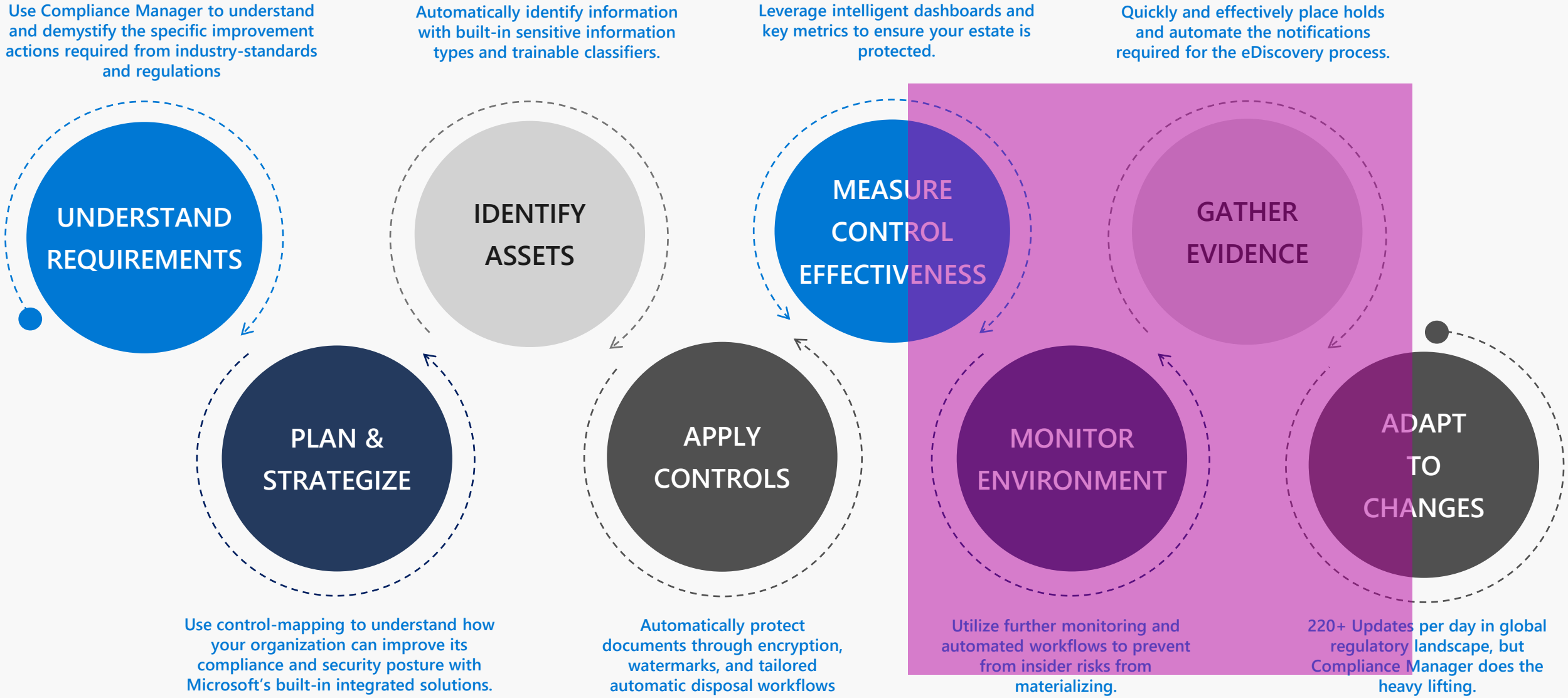
Employee Data Theft

Bribery

Bad Password Hygiene

Too Much Data Access

Fraud



Powered by an intelligent platform

Unified approach to compliance management, data classification/protection/governance, policy management, insider risk management, and eDiscovery

Information Protection & Governance

Protect and govern data wherever it lives

- Auto classification and Retention
- Supervision for monitoring comms
- Event based triggers for IG
- Label analytics
- Trainable ML classifiers
- Regulatory record

Insider Risk Management

Identify and take action on critical insider risks

- Auto classification and Retention
- Supervision for monitoring comms
- Event based triggers for IG
- Label analytics
- Trainable ML classifiers
- Regulatory record

Discover & Respond

Quickly investigate and respond with relevant data

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

Compliance Management | Simplify compliance and reduce risk

The ‘Sly Dog’ gang

Four employees leave their company with more than just branded sweatshirts

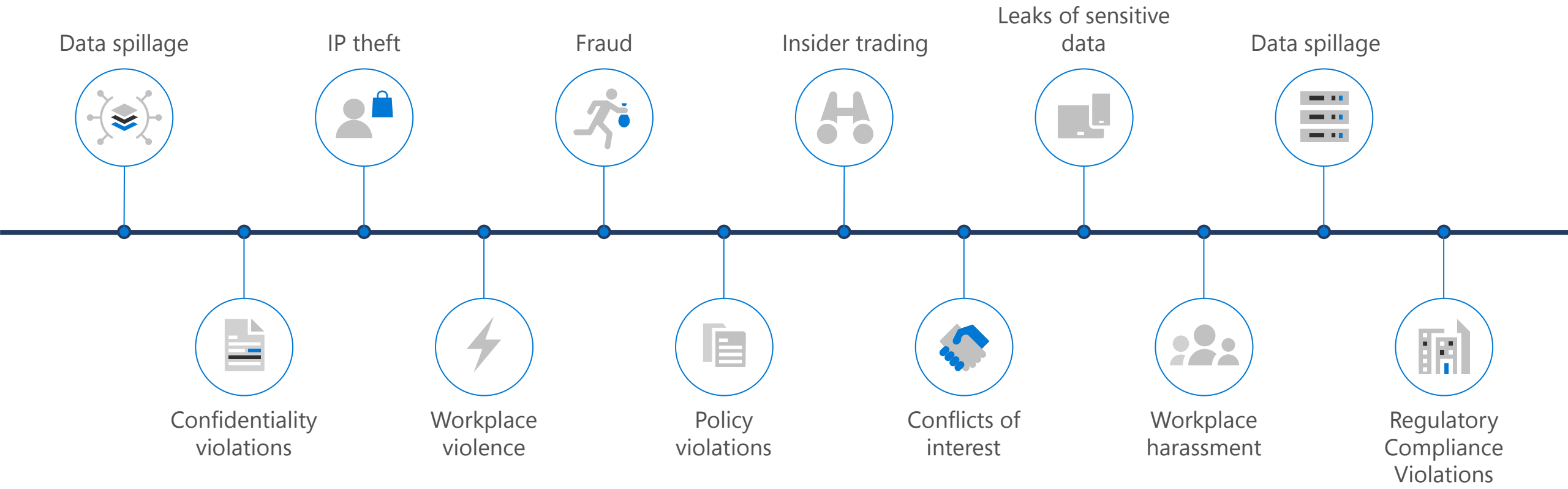
In March of 2019, a large car manufacture with state-of-the-art, proprietary operations and technology filed a lawsuit against four former employees and a competitor for corporate espionage.

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

Organizations face a broad range of risks from insiders



Customers face a broad range of Insider risks

Data spillage
People overshare data and don't remove access rights after valid access.

IP theft
People go to the competition and take data with them for an advantage.

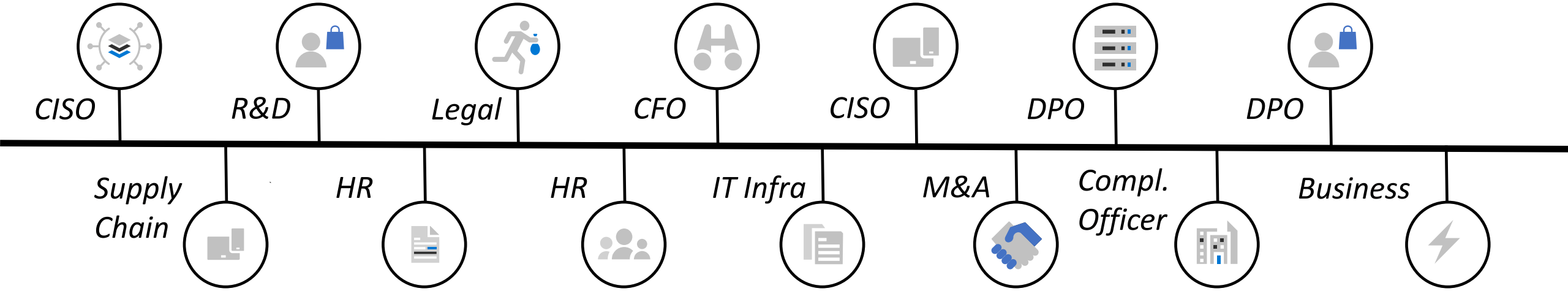
Illicit Activity
Corporate Fraud, Blackmail, and other Illegal activities.

Insider trading
Only the need-to-know should have access to critical financial data.

Leaks of sensitive data
M&A activities, Marketing strategies, Financial results, R&D results.

Data Loss
Mobile devices get stolen, lost and forgotten. Records get deleted without recovery options

"The right to be forgotten"
Registered consumers might request to be removed, as per Privacy regulations.



Leaks of sensitive 3rd party data
Supplier prices, competitor information, etc.

Confidentiality Violations
Unintentional sharing of confidential information.

Workplace violence and harassment
Company culture violations due to bad language and abuse.

Data Proliferation
Many tools can be used on various devices and in multiple locations, companies lose oversight.

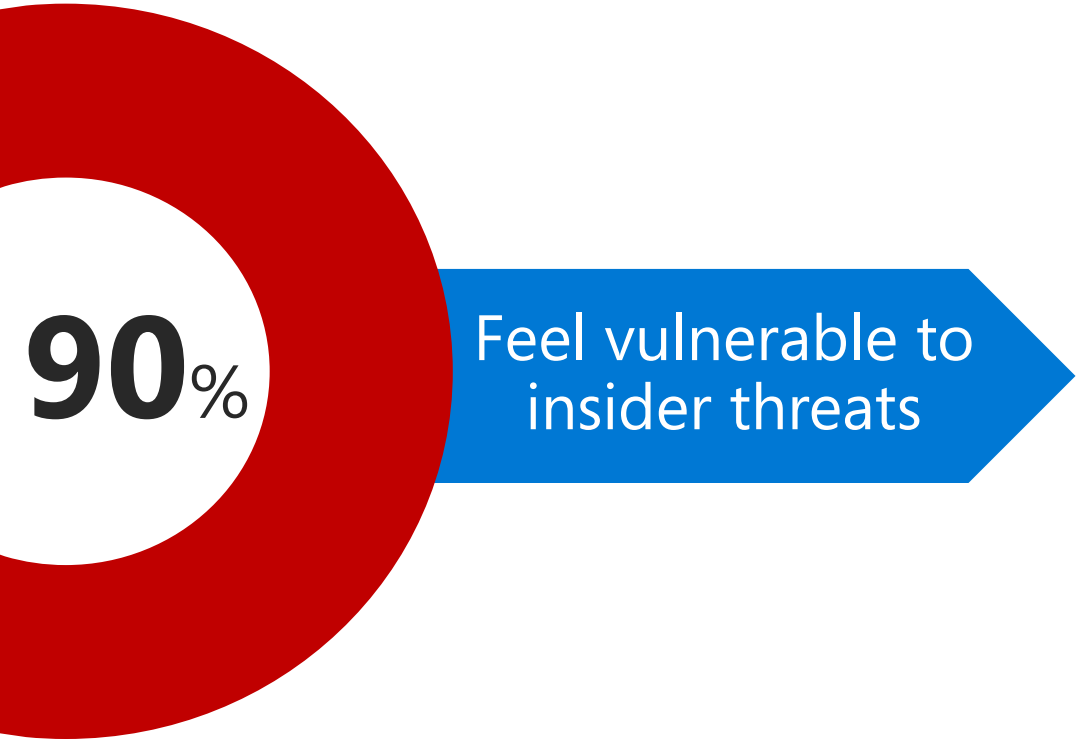
Conflicts of Interest
People act in their own interest rather than in the companies' interest.

Regulatory compliance violations
Many new regulations and updates every day.

Accidental data leakage
Information which is derived through technological functions leads to a breach. (Autocomplete, for example)

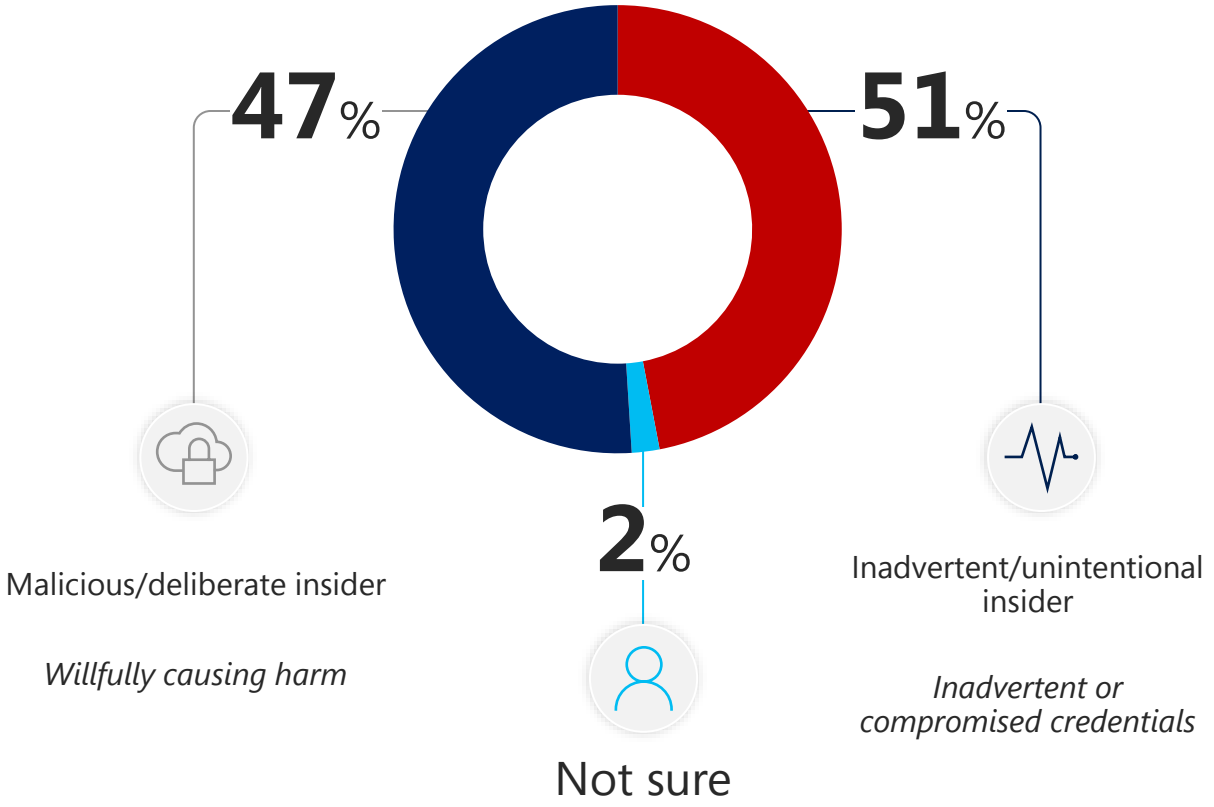
Insider risk is one of your biggest challenges[1]

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

Question:

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

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

Risk

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

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

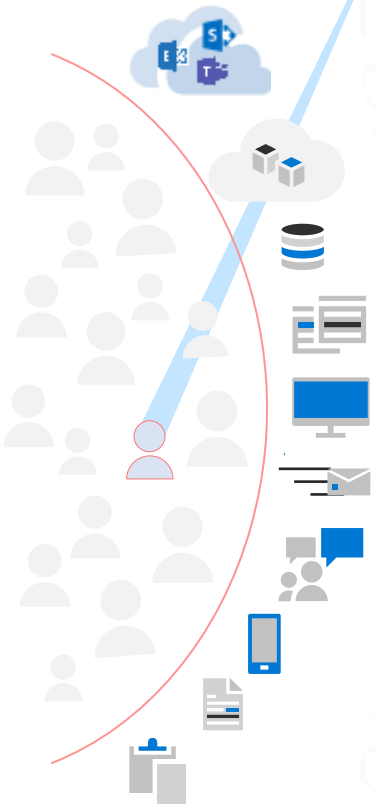
Concerning Behavior

- 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*

A fractured approach for insider risks



Insider risks are difficult to identify & manage

- Data growing, being accessed and shared across multiple devices and apps
- Visibility into location and movement of sensitive data is poor
- Requires analysis of millions of disparate signals and collaboration (security/HR/legal)

Traditional approaches have limitations

	UEBA (user behavior analytics)	**UAM** (user activity monitoring)	**DLP** (data loss prevention)
Complex setup	• Configuration requires scripting (engineering led or managed services) • COGS burden for storage of signals and compute for analytics • Signal curation requires additional solutions (Firewalls, UAM, DLP, EDR) • Events per second are capped • On-prem server-based model	• Requires deployment of endpoint agents and on-prem servers • Management of agents is complex • Scale and performance issues with agent-based model	• Requires deployment of endpoint agents and on-prem servers • Management of agents is complex • Scale and performance issues with agent-based model • Some narrowly focused on email communications
Limited enrichment	• Low visibility into content • Low sentiment analysis • Low understanding of content sensitivity	• Low visibility into content • Low sentiment analysis • Limited signal correlation • Low understanding of content sensitivity	• Low visibility into content • Low sentiment analysis • Limited signal correlation • Prone to high-false positive rate
Narrow workflows	• No integrated workflow beyond SOC	• No integrated workflow beyond SOC	• No integrated workflow beyond SOC

Question:

Who do you believe insider risk is important too?

1. IT dept
2. Legal
3. HR
4. Security team
5. Data protection officer
6. Managers

Answer:

All of them

Compliance is a Cross-Departmental Initiative

Privacy

Though it may not be a defined function in all orgs, privacy typically spearheads the **creation of policy and teaching of privacy best practices** across the org.

Legal

Legal, in partnership with outside counsel, **provide expertise and application on regulations** while simultaneously executing contracts and data sharing agreements.

Information Tech / Security

IT / InfoSec is responsible for **implementing technical solutions dictated by the privacy and compliance teams**. They are tasked with securing and protecting company data.

Risk / Compliance

Compliance, which is **generally a well-established function, especially in regulated orgs**, is tasked with ensuring the solutions and policies in place are sufficient and functional.

HR

HR is not only involved in recruitment, but also measured on **keeping talents in the company**, and connected with the compliance and privacy teams on specific requests like **Data Subject Requests** or **Insider Treat Tracking**.

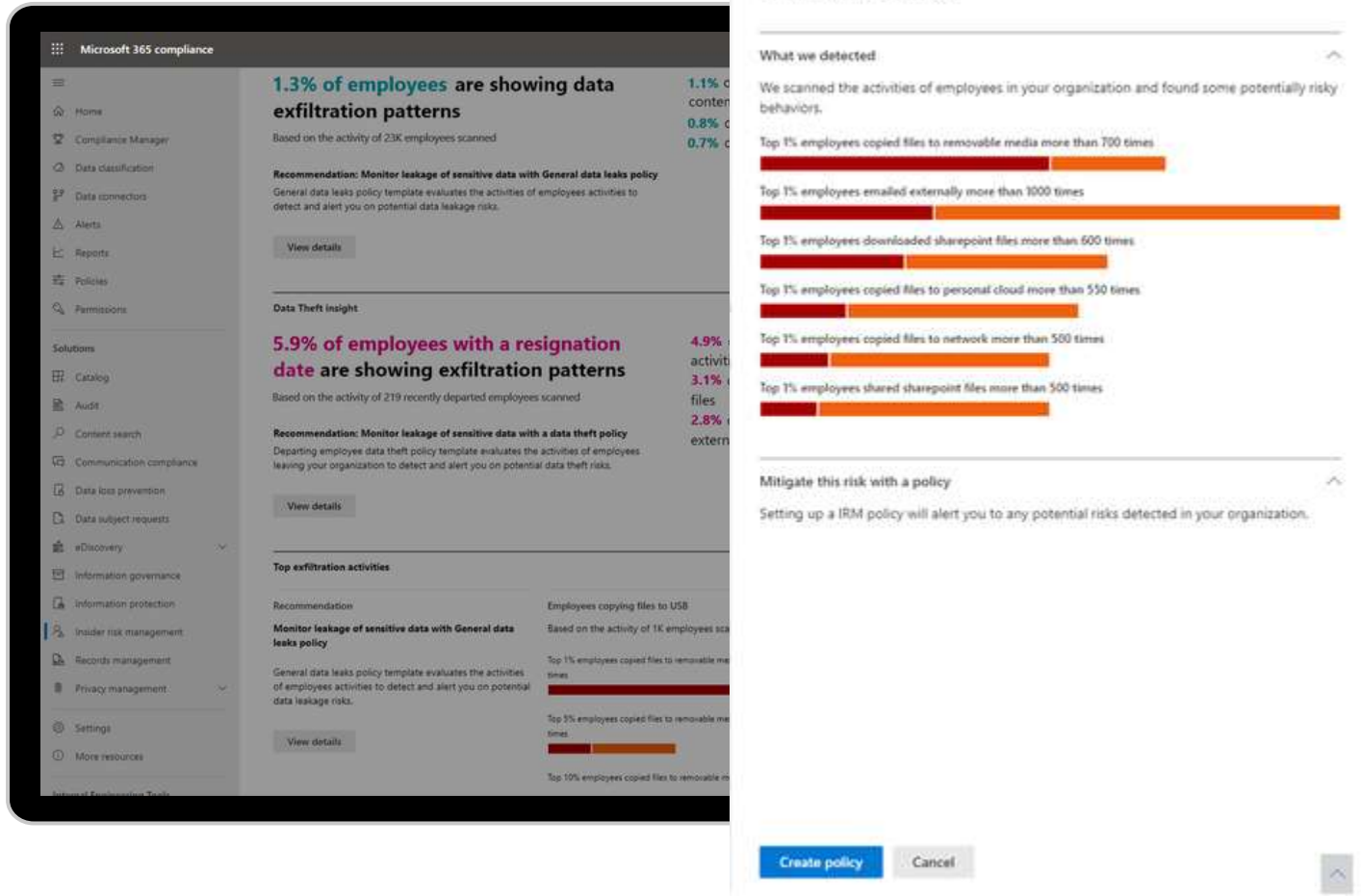
Insider Risk Management

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

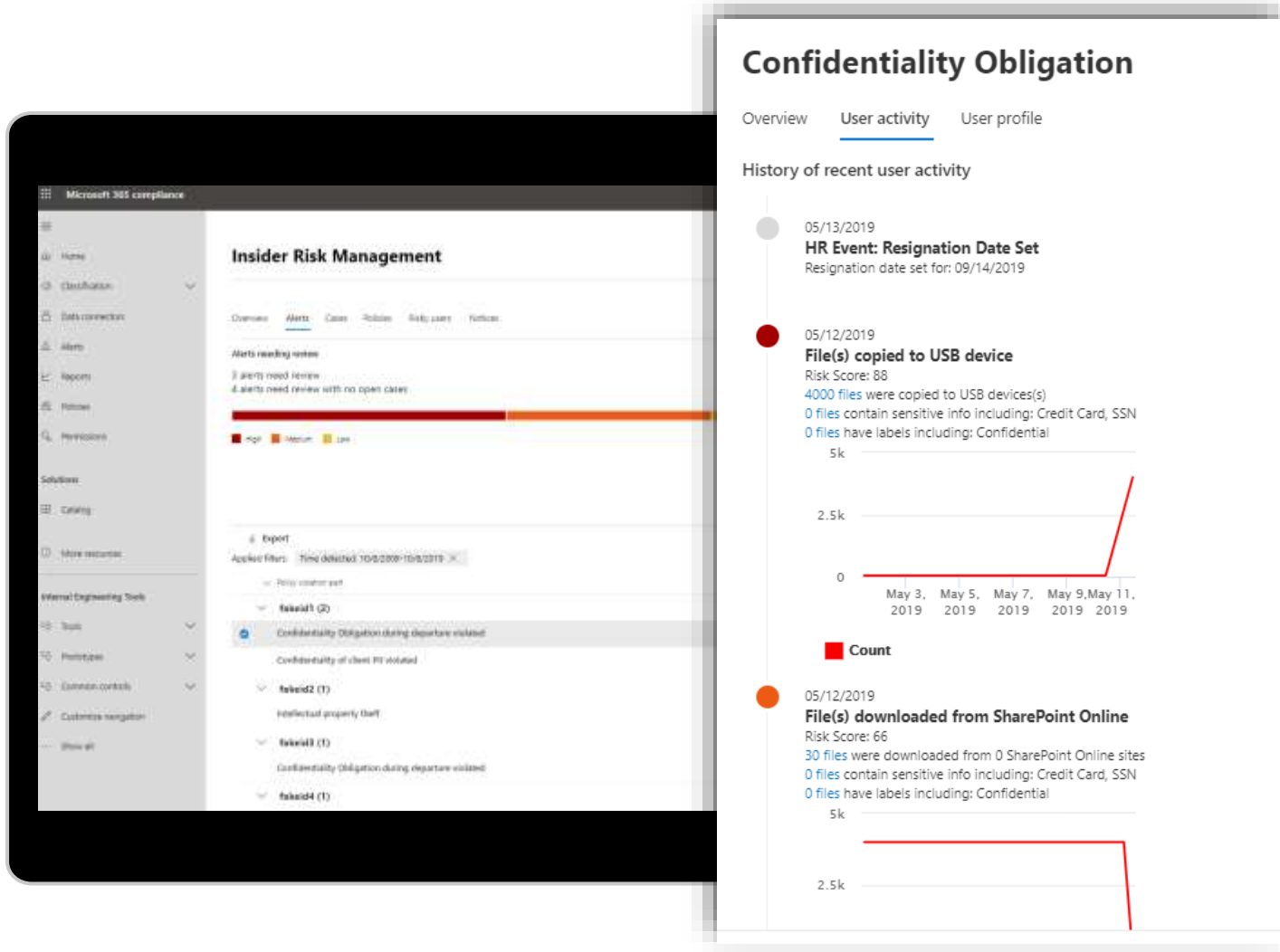
Identify hidden risk patterns with customizable ML templates requiring no end-point agents

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



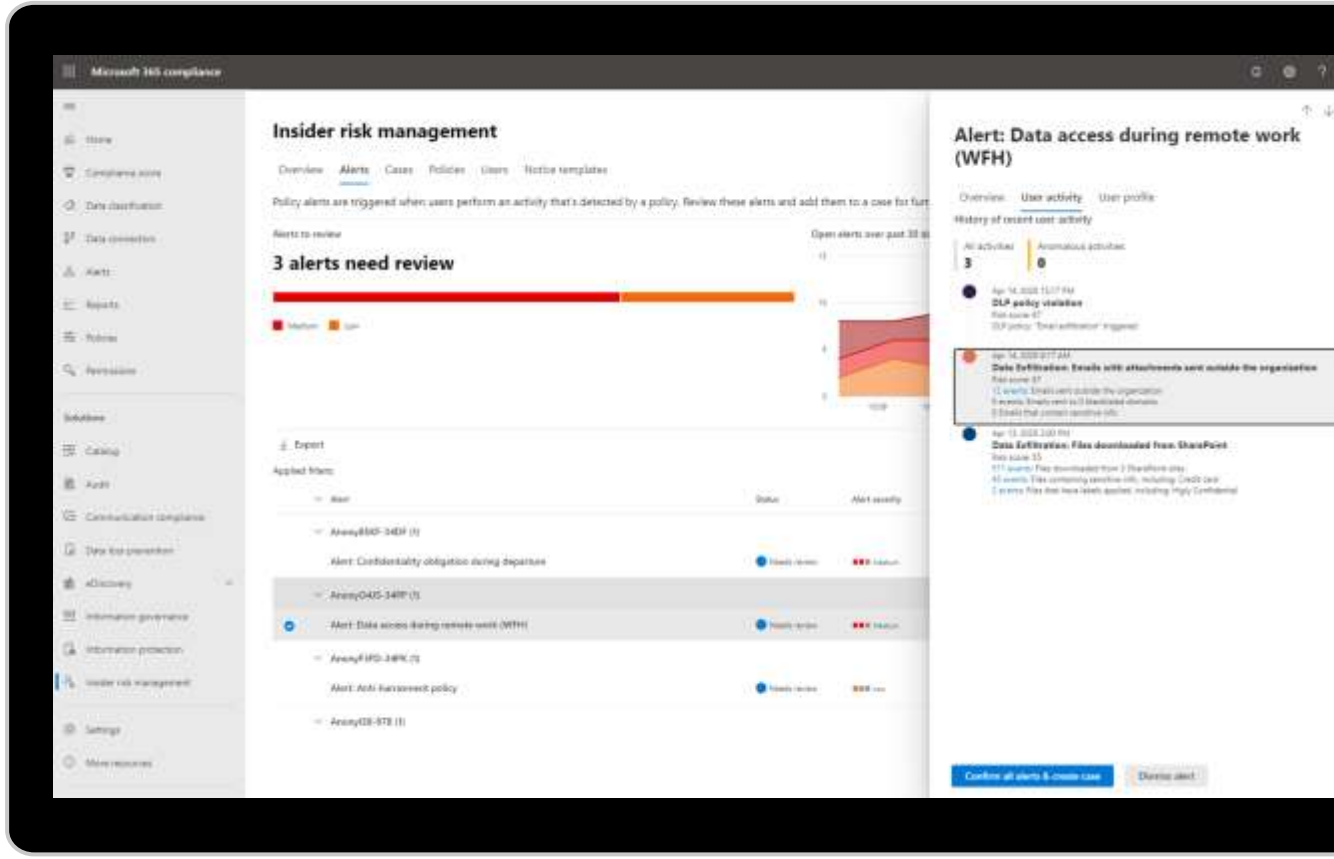
Insider Risk Management

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

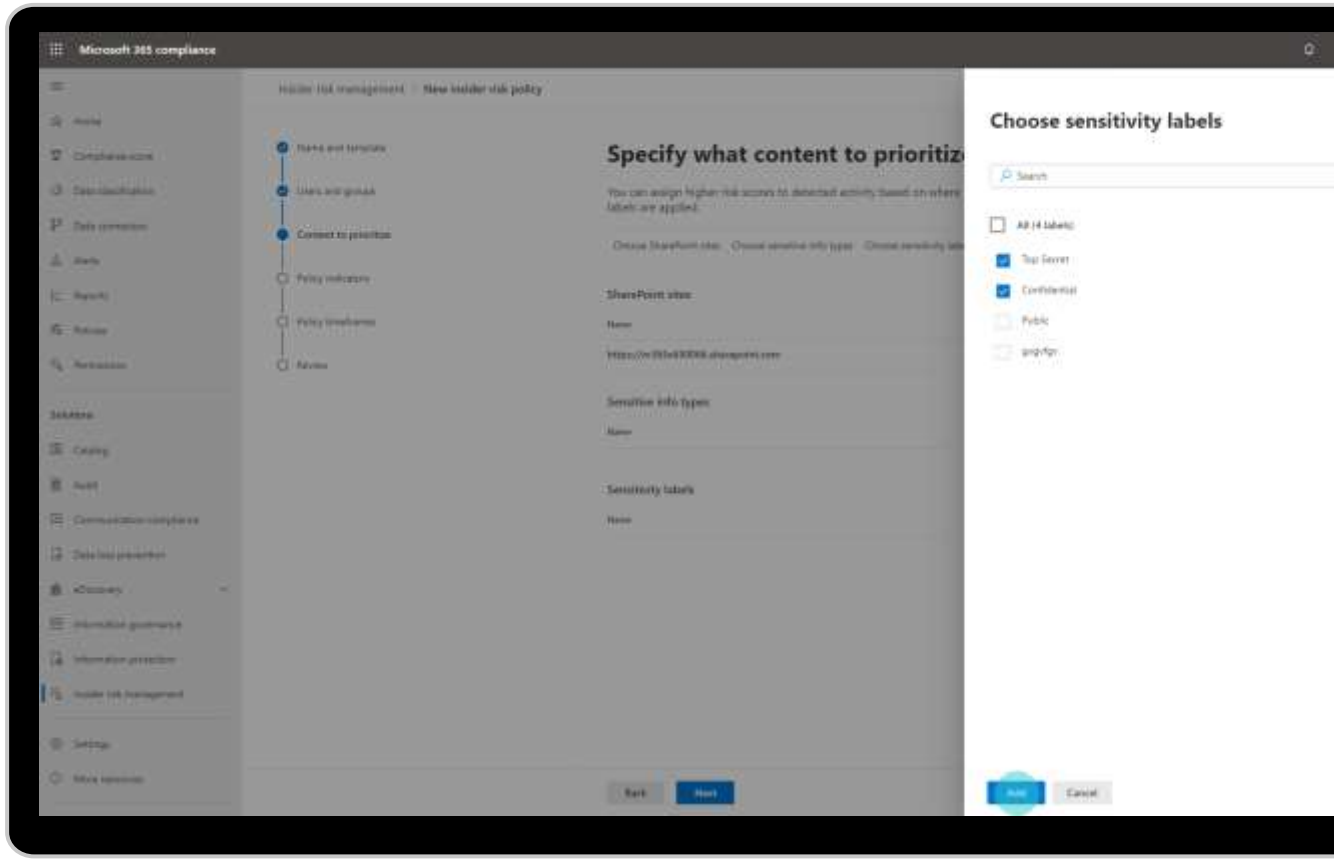
An integrated end-to-end approach for insider risks from Microsoft 365

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 +

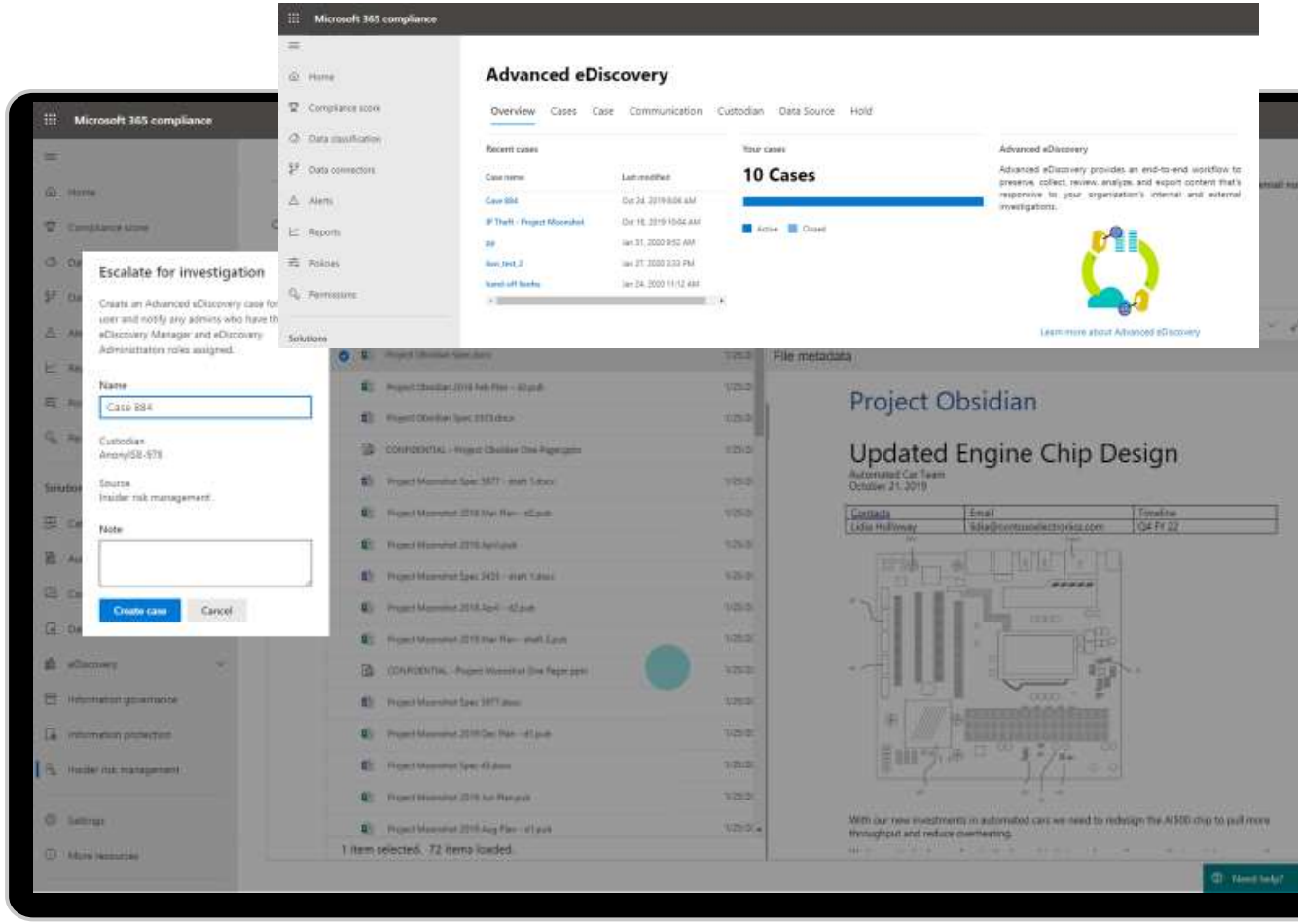
Data Loss Prevention

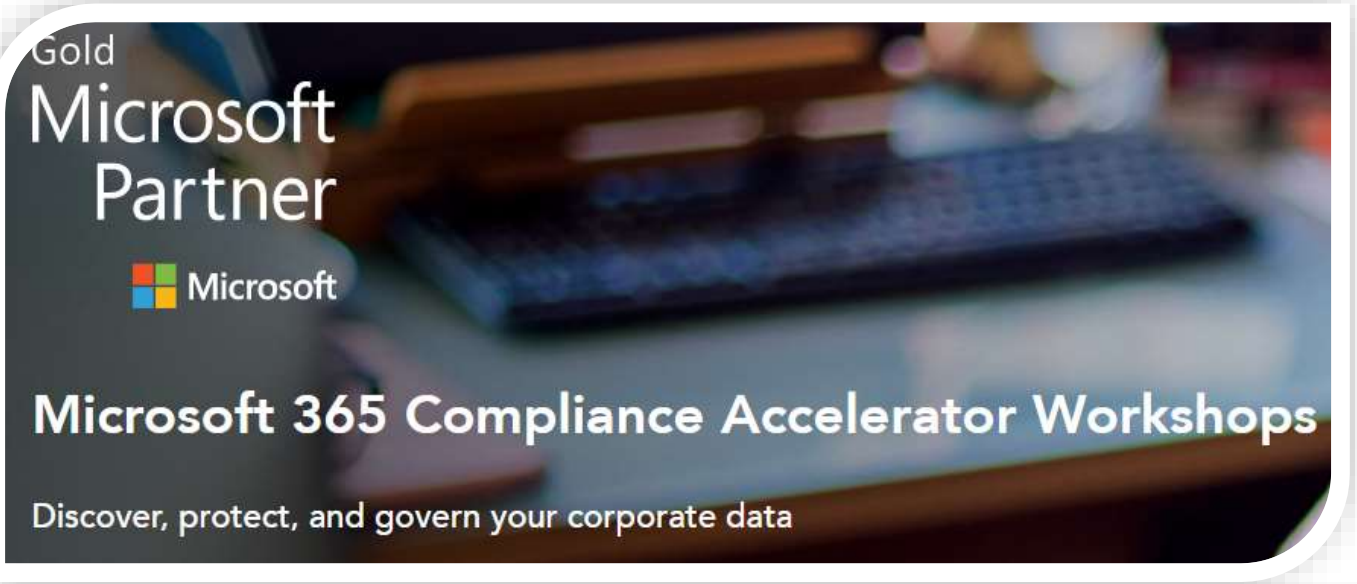
Information Protection

Communication Compliance

Advanced eDiscovery

Legal collaboration
Integrated workflows provide seamless investigation handoff





Discover Sensitive Data Workshop

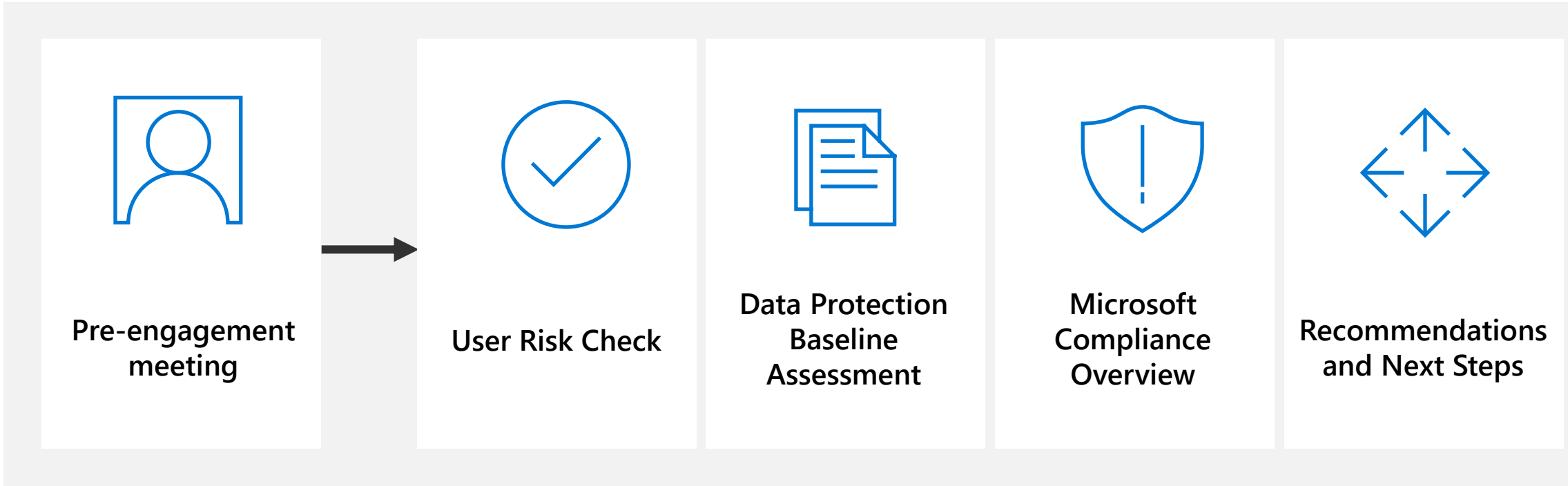
The *Discover Sensitive Data Workshop provides* you with examples of privacy and regulatory risks in the organizational data contained within your own Modern Work environments. This helps you identify compelling ways to remediate the risks through Microsoft 365 E5-associated technologies. Topics include uncovering data risks in your environment and building customer confidence in mitigating risk through data-driven analytics and visualization.

Manage and Investigate Risk Workshop

The *Manage and Investigate Risk Workshop* is designed to provide you with examples of potential data leaks and data theft within your Modern Work environments. Through this workshop, Lighthouse experts help you identify deviations from common corporate policies using Microsoft 365 E5-associated technologies. Topics include uncovering risky user activities, evaluating user communication inside the organization, and understanding how to prioritize and mitigate the identified privacy risks.

https://info.lighthouseglobal.com/2022-m365-compliance-accelerator-workshops

The Manage and Investigate Risk Kick Off



Out-of-box sensitive info types

Microsoft 365 includes 200+ sensitive info types

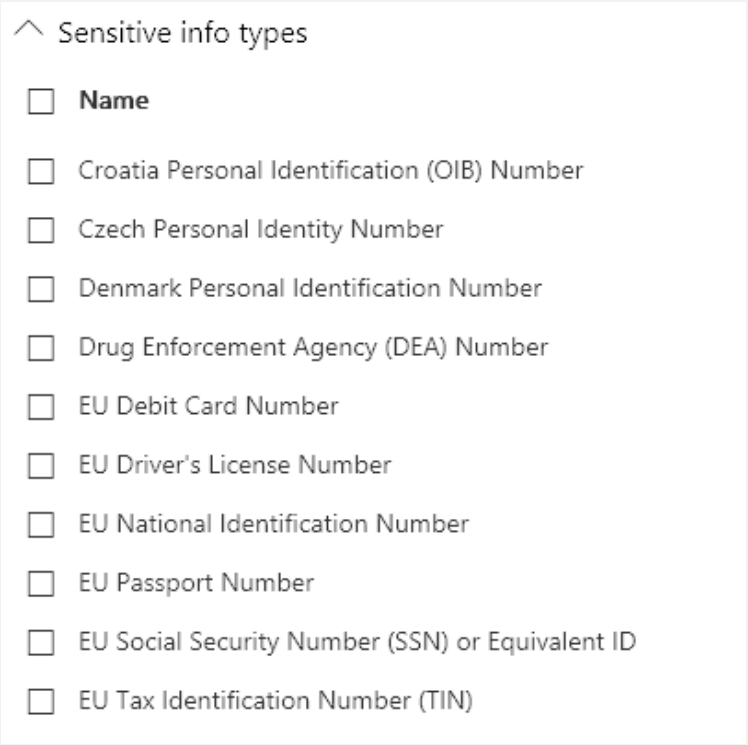
For different countries, industries, or by information type

Sensitive information comes in many forms

Financial data, Personally Identifiable Information (PII)

Examples

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



Customer-specific sensitive info types

Business intellectual property
Business plans, product designs, confidential projects

Employee or customer information
HR Information, resumés, employment records, salary information

Highly confidential information
Mergers and Acquisition, workforce reduction

Examples

- Employee or customer numbers — *Technology: RegEx*
  - <EMP-nnnnn>
  - <CUST-nnnnnn-NL>
- Specific keywords — *Technology: Static Keywords*
  - <Project Enigma>
  - <Highly Confidential>
  - <Internal only>

Module -Insider Risk Discovery

Activity overview

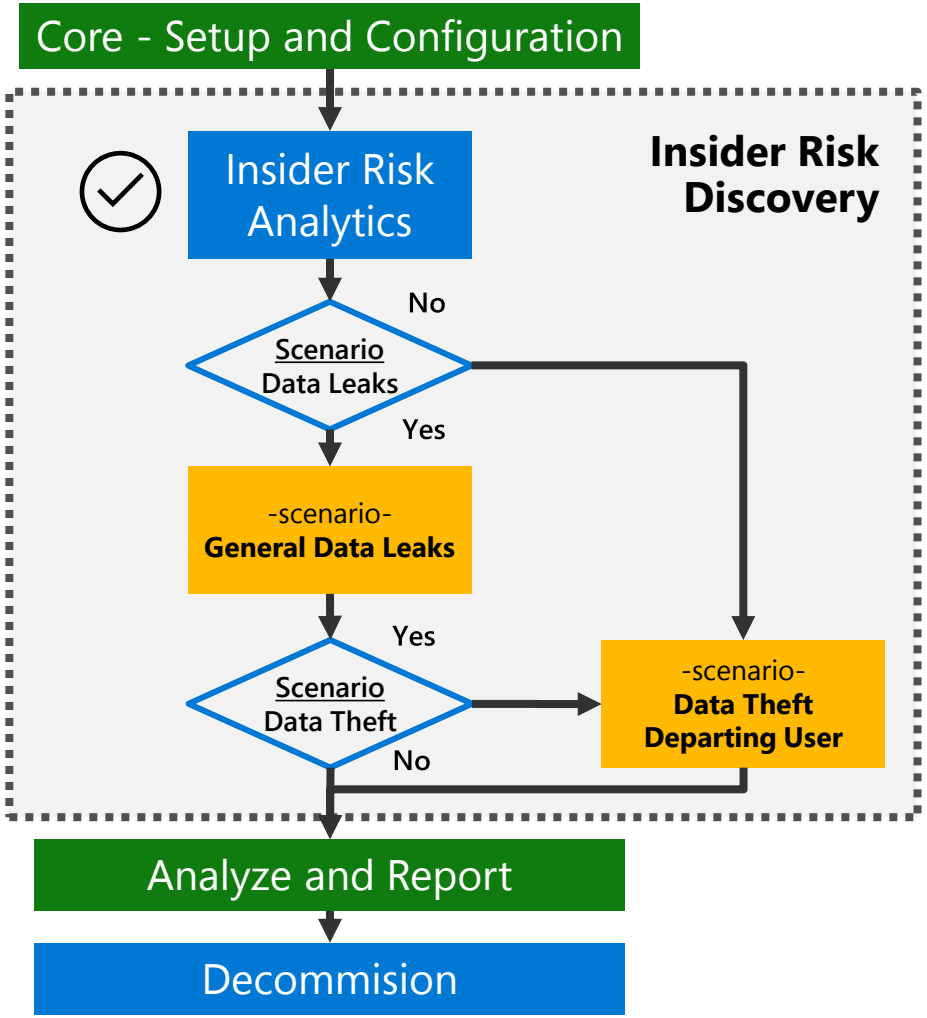
Detect malicious and inadvertent activities in the organization by enabling Insider Risk Management and configuring policies that will define the types of risks to identify and detect.

Insider Risk Analytics

- The first activity for Insider Risk Management

Choose at least one of the additional scenarios:

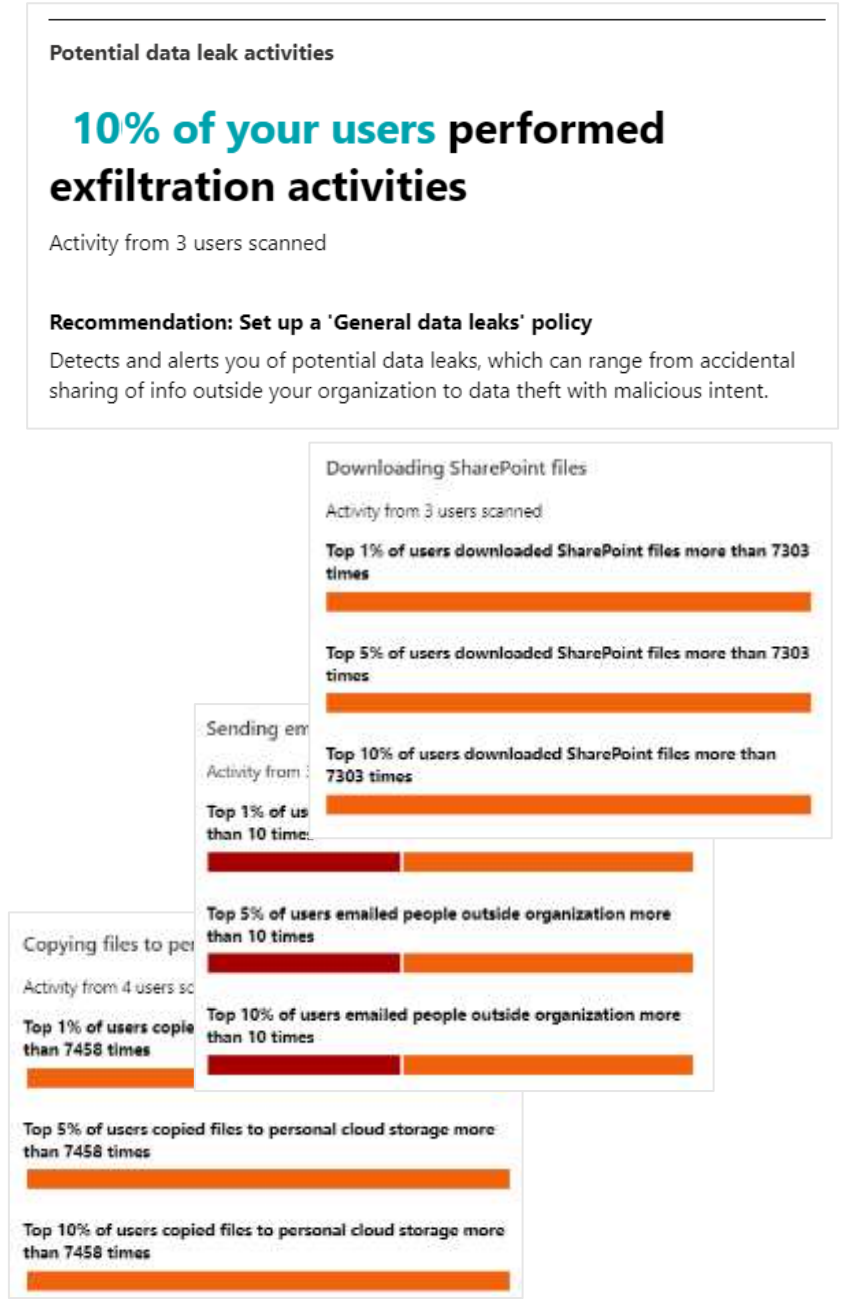
- General data leaks
- Data theft by departing user



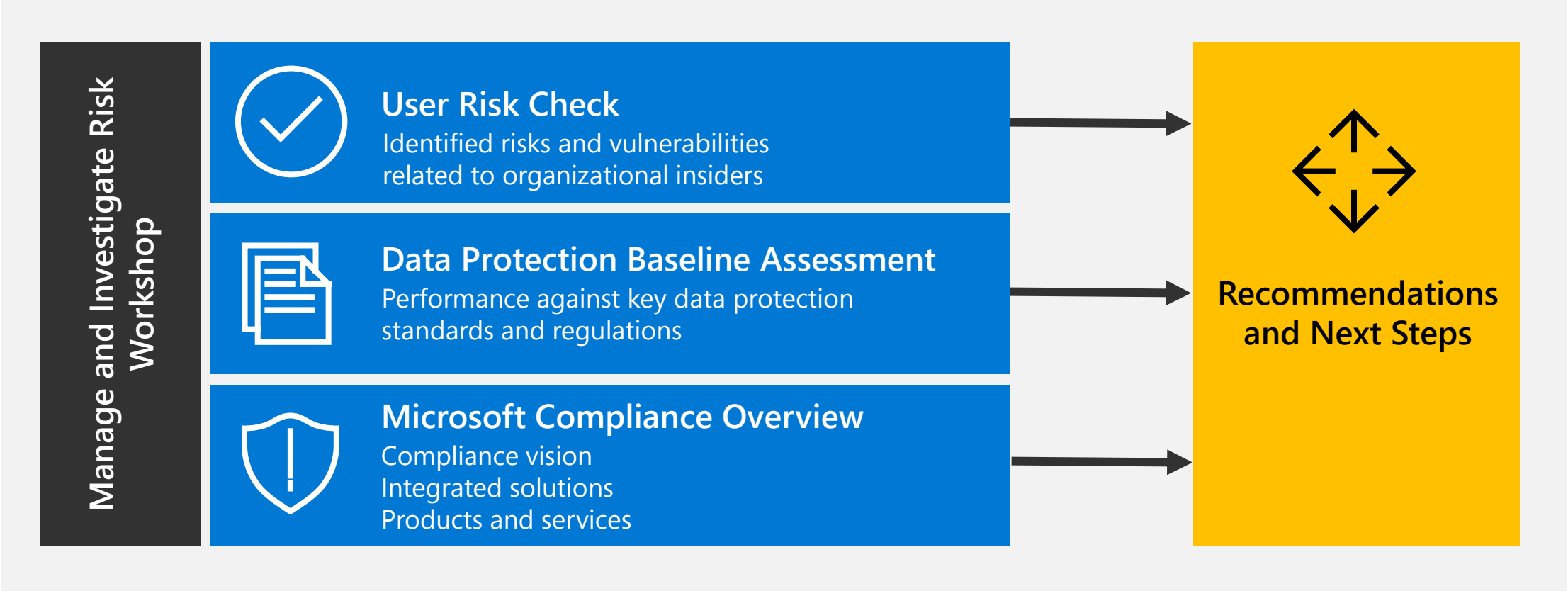
Insider Risk Analytics

Evaluation of potential insider risks

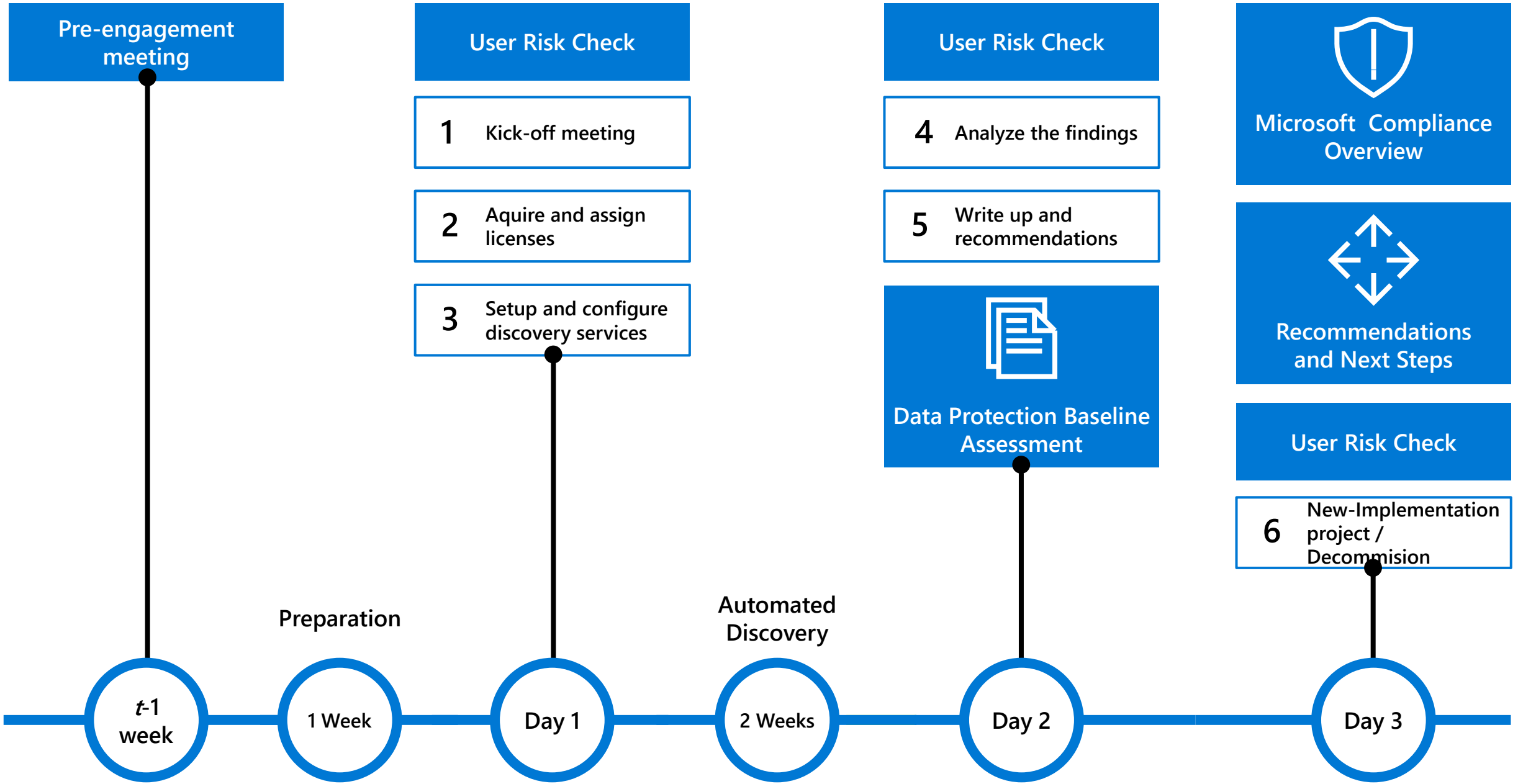
- First activity for Insider Risk Discovery
- Insights based on same signals used by insider risk management
- Works out of the box without configuring policies
- Identify potential areas of high user risk
- Help determine type and scope for policies to consider



Recommendations and next steps



Workshop timeline



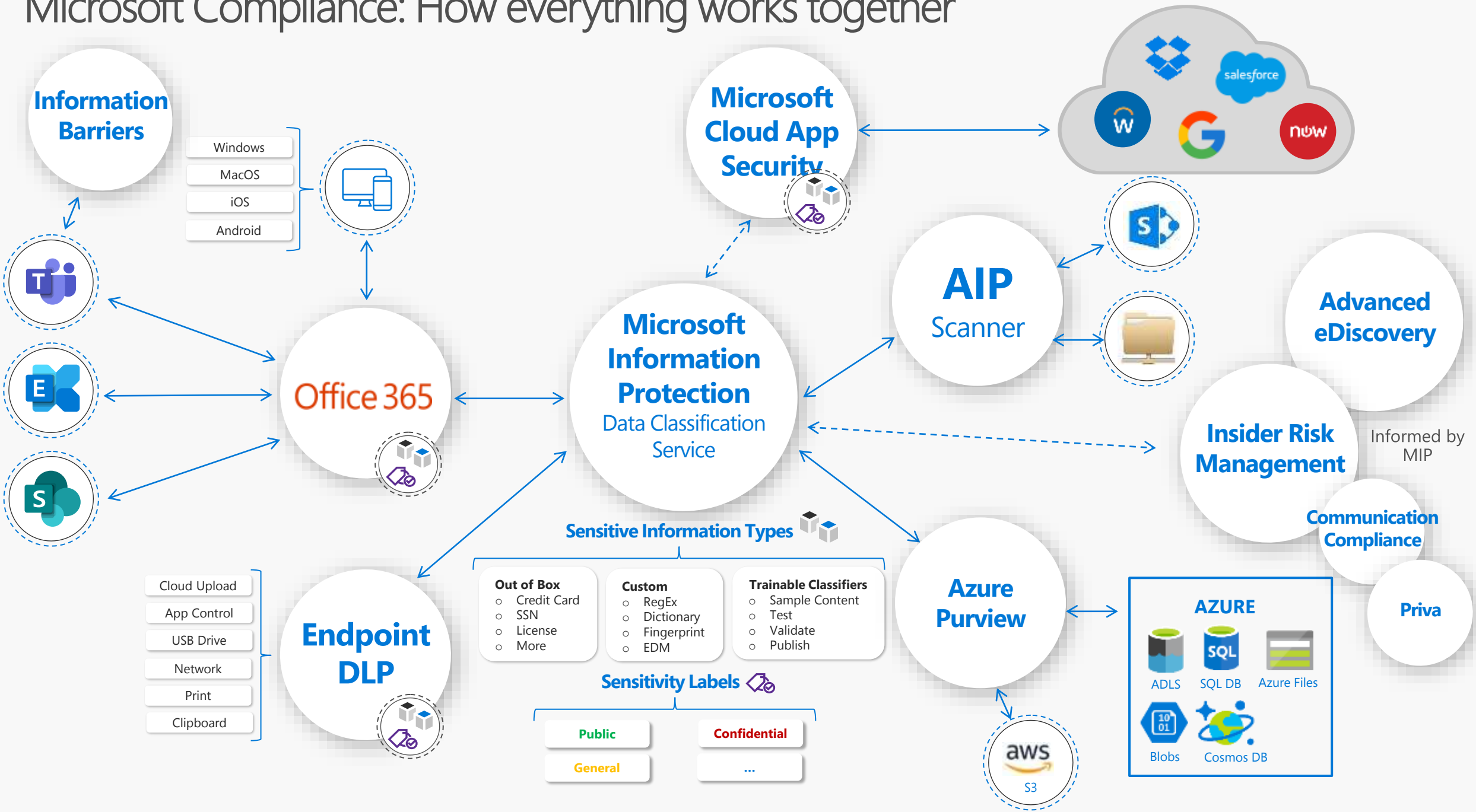
Tailored policy templates

Departing Employee Data Theft	Data Leaks	Security Control Violations
Theft of intellectual property by a departing employee	Intentional or unintentional leak or sensitive or confidential information	Bypassing security controls or violate security policies
• Data Theft – General	• Data Leak – General • Data Leak – Disgruntled • Data Leak – Priority User Groups	• Security Policy Violation – General • Security Policy Violation – Priority User Groups • Security Policy Violation – Departing Employee • Security Policy Violation – Disgruntled Employee

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data[1]

1. 2016 Deloitte Debriefs "Insider threats: What every government agency should know and do"

Microsoft Compliance: How everything works together



Microsoft **Insider Risk Management** : How everything works together

Trainable Classifiers

- Targeted Harassment
- Discrimination
- Offensive Language
- Profanity
- 7- Languages
- Custom Document Models

Sensitive info Types

Out of Box
- Credit Card
- SSN
- License
- More

Custom
- RegEx
- Dictionary
- Fingerprint
- EDM

Connectors

- Human Resources
- Registration date
- Performance
- Physical Badge Access

Cloud App Security

- Mass Download
- Mass Sharing
- Activity After Termination
- Failed Logins

Microsoft Information Protection

- Classified Content
- Protected Content - Decrypt

Defender Sensor

- Cloud Upload
- App Control
- USB Drive
- Network
- Print
- Clipboard
- Defense Evasion
- Unwanted Software

Azure Active Directory

- Activity log – accessed, logon times, locations, risk level etc

365 Audit Log

- Activity log – accessed files, moved, re-named, deleted, etc

Informed by Stack

Insider risk analytics

Logic apps

- Transpose audit logs
- Extract IRM only alerts

365 Audit Log

- Activity log – logs IRM alerts
- O365 Management API

Insider Risk Management Service

Azure Sentinel

- Incident management
- Advanced hunting
- Machine learning analytics

Logic Apps

- Trigger automation
- Automatic remediation
- Alerting & notification
- Auto incident creation for ITSM

Permissions
- RBAC:
- IRM / Sentinel
- Content / Activity Explorer

Policies

Categories
- Data theft
- Data leaks
- Security policy violations

Data leaks/Security templates
- General data leaks
- General security violations
- By priority users
- By disgruntled users
- By departing users

Alerts

- Alert management / Triage
- Review summary/activity
- Create case
- Dismiss alerts

Power Automate

- Add calendar reminders
- Notify manager
- Request info from HR
- Custom flows

Notify User

- **Action**:
- Templated email notices
- Anonymized user entity

Cases

- **Investigation** - User activity
- Activity/content explorers
- Case notes
- Contributors- HR/Legal/Sec
- Close case

Escalation

- **Action**:
- Hand-off to Advanced eDiscovery
- Case creation

Created by G.Hosking 9/2021

Does anyone have a risk solution within their organisation?

Microsoft **Communication Compliance**: How everything works together

1st party communications

- **Chat / Channel messages / Threading**
- **Email / Threading**
- **Chat / Community messages**

Connectors – 3rd party archiving

Microsoft connectors
- Bloomberg msg
- ICE chat
- Instant Bloomberg

Veritas connectors
- Cisco Jabber
- WebEx
- Zoom meetings
- Slack eDiscovery
- Symphony
- +more

TeleMessage connectors
- Android
- WhatsApp
- Signal
- AT&T network
- WeChat
- O2 network
- +more

Data discovery options

Trainable Classifiers

- Targeted Harassment
- Discrimination
- Offensive Language

- Imagine detection – e.g Gory
- 7- Languages
- Custom Document Models

Sensitive info Types

Out of Box
- Credit Card
- SSN
- License
- More

Custom
- RegEx
- Dictionary
- Fingerprint
- EDM

Microsoft Information Protection

- Classified Content
- Protected Content - Decrypt

Data collected

Permissions
- **RBAC**:
- Content / Activity Explorer

Communication Compliance Service

Policies

Policy Templates – Monitor:
- Offensive language
- Sensitive information
- Regulatory compliance
- Conflict of interest – between groups

Custom Policies: Examples:
- Monitor subset or all users
- Reviews/Supervisors
- Comms channel selection
- Direction of comms

Conditions: Examples:
- Data classifiers
- Sensitive info types
- Keywords
- Classification labels
- Optical character recognition

Trainable Classifiers: additions
- Adult images
- Racy images
- Gory images

Escalation for review e.g. Legal / HR

Alerts

- Summary information
- Pending items (to be reviewed)
- Resolved items (reviewed)

- Alert management / Triage
- Review items / history
- Resolve items
- Content explorer / threaded items
- Annotate /redact / translation
- Tag – Compliant/Questionable
- Report false-positive (ML)
- Remove message from Teams

Examples:
- Add calendar reminders
- Notify manager
- Request info from HR
- Custom flows

Power Automate

Notify User

- **Action**:
- Templated email notices
- Anonymized user entity

Escalation for investigation

- **Action**:
- Hand-off to Advanced eDiscovery
- Case creation

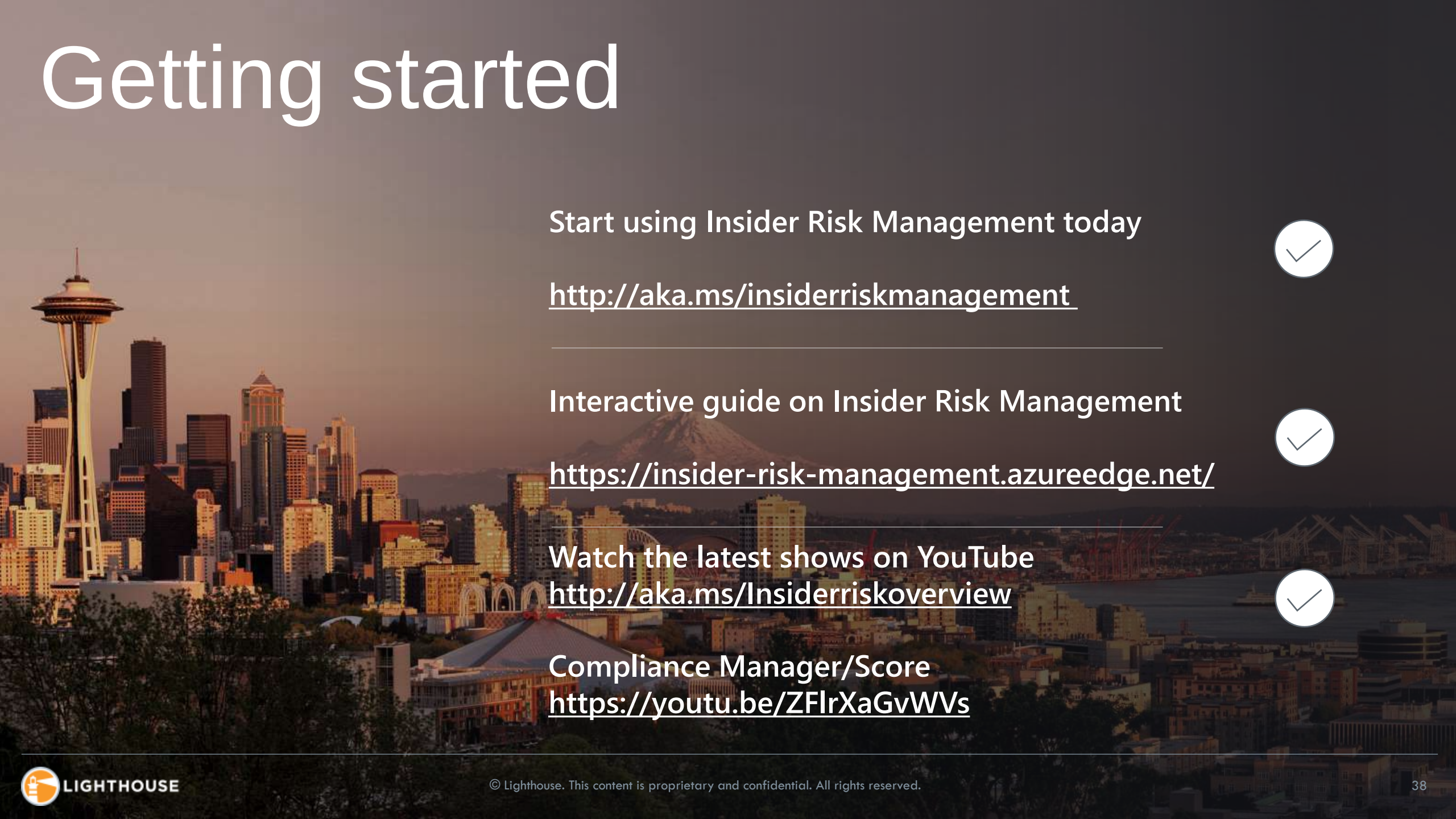
Reports

- **Review**:
- Policy matches
- Items per policy
- Detailed reports e.g. User

Created by G.Hosking 9/2021

DEMO TIME

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/ZFIrXaGvWVs

E5 Compliance gets more value

New categories, new features in existing categories*

2019

- Microsoft Information Protection (MIP)
- Customer Key
- Privileged Access Management
- Customer Lockbox
- Information Governance (IG)
- Advanced eDiscovery (AeD)

2020 Spring

- Advanced Audit
- Insider Risk Management
- Communication Compliance
- Records Management (RM)
- Sensitivity labels in SPO, EXO, OneDrive (preview)
- AeD: Teams private channels

- Microsoft Information Protection
- Customer Key
- Privileged Access Management
- Customer Lockbox
- Information Governance
- Advanced eDiscovery

2020 Summer

- MIP: Endpoint DLP (Preview)
- MIP: Content Explorer/Activity Explorer
- MIP: Exact Data Match
- MIP: Sensitivity labels in Teams, groups, and SPO sites
- MIP: Auto classify with sensitivity labels
- AeD: Yammer

- Advanced Audit
- Insider Risk Management
- Communication Compliance
- Records Management
- Sensitivity labels in SPO, EXO, OneDrive (preview)
- AeD: Teams private channels

- Microsoft Information Protection
- Customer Key
- Privileged Access Management
- Customer Lockbox
- Information Governance
- Advanced eDiscovery

2020 Fall

- Compliance Manager
- Double Key Encryption
- IG: Trainable classifiers/feedback loop (preview)
- 25+ pre-built data connectors (1st and 3rd party)
- RM: Regulatory record label (preview)
- IG: Support for Teams meeting recordings (preview)
- IG and RM: SharePoint Syntex integration
- Insider Risk Management:
  - Integration with Teams, Power Automate, and ServiceNow
  - New policy templates and enhanced customization
  - Increase in signals
  - Push alerts to Management Activity API
  - Physical badge connector, User360
- Graph API for Teams DLP, AeD & Teams Export (preview)
- Advanced Audit: user search, mail sent events

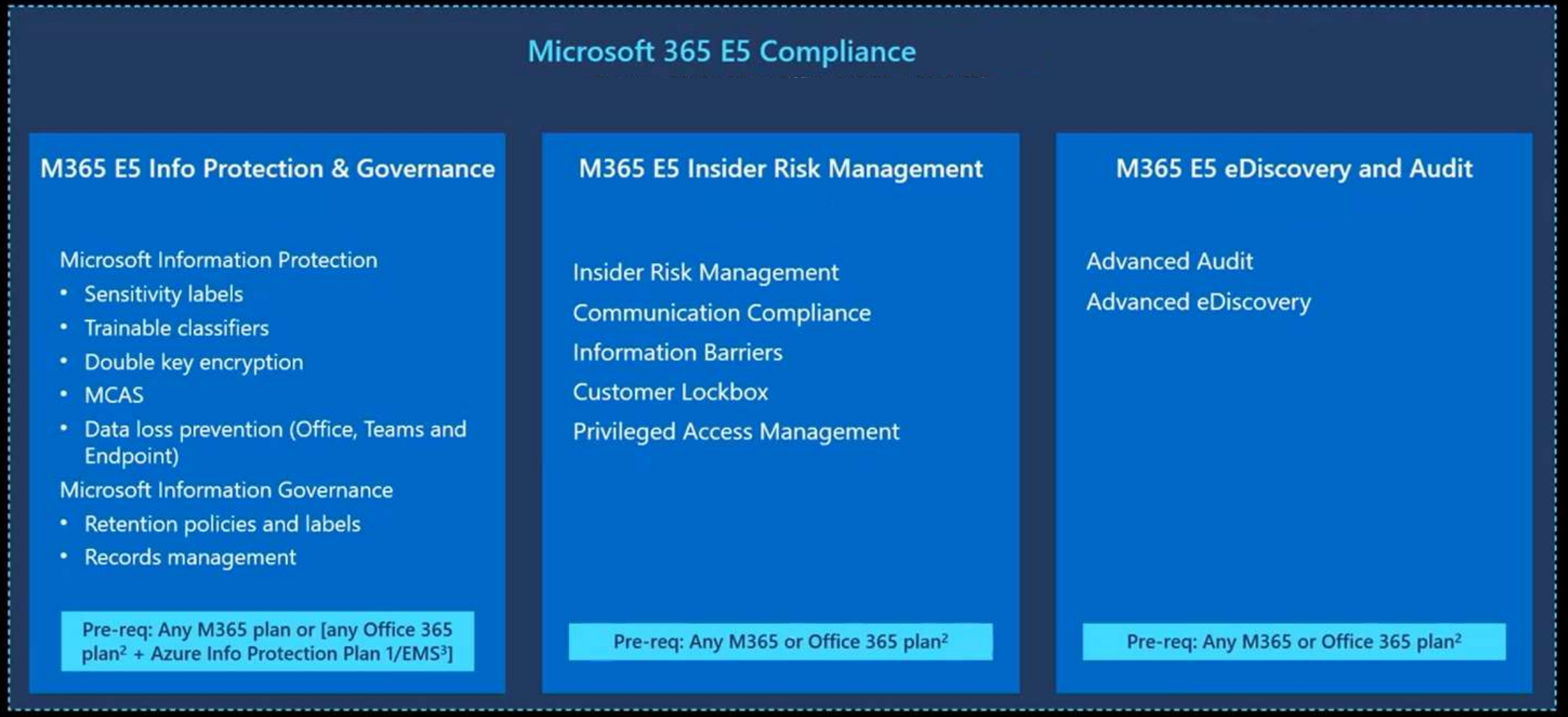
- MIP: Endpoint DLP
- MIP: Content Explorer/Activity Explorer
- MIP: Exact Data Match
- MIP: Sensitivity labels in Teams, groups, and SPO sites
- MIP: Auto classify with sensitivity labels
- Advanced eDiscovery: Yammer

- Advanced Audit
- Insider Risk Management
- Communication Compliance
- Records Management
- Sensitivity labels in SPO, EXO, OneDrive (preview)
- AeD: Teams private channels

- Microsoft Information Protection
- Customer Key
- Privileged Access Management
- Customer Lockbox
- Information Governance
- Advanced eDiscovery

*Not comprehensive; for full list go to service descriptions: https://aka.ms/servicedescriptions

Microsoft 365 E5 Compliance



Microsoft 365 E5 Compliance Add-Ons

Data Connectors

- Enable third party data archiving
- Leverage premium services across on your third-party data

Pre-req: Any M365 E5 plan or any Office 365 E5 plan

Premium Assessments for Compliance Manager

- Purchase one of 150+ out-of-the-box assessments that are kept up-to-date

Pre-req: Any M365 E5 plan or any Office 365 E5 plan

10-Year Audit Log Retention

- Retain audit logs for up to 10 years

Pre-req: M365 E5, M365 E5 Compliance, M365 E5 eDiscovery & Audit or Office 365 E5 plan