Microsoft

SUNY THE STATE UNIVERSITY OF NEW YORK

Building a Future-Ready Security Posture

Joshua Klein

Senior Security Specialist

joshuaklein@microsoft.com

Cyberthreats have grown 5x+

Median time for an attacker to access private data from phishing

1h 12mins

SPEED

Password attacks per second

2023	Today
4,000	7,000

SCALE

Threat actors tracked by Microsoft

2023	2024
300	1,500+

SOPHISTICATION

Source: Microsoft

…some specific EDU metrics

3rd

Education was the third most targeted industry in Q2 2024.[1]

3x

More data security incidents occurred in organizations using over 15 tools.[2]

1

single student education record can be worth as much as $350.[3]

43%

of higher education institutions in the UK report a cyber incident at least once a week.[1]

83%

of organizations experience multiple data breaches over time.[2]

1.5x

more likely to succeed with AI by having a mature information management strategy.[4]

1. Cyber Signals Issue 8 | Education under siege: How cybercriminals target our schools
2. Microsoft Digital Defense Report 2024
3. Microsoft Education Blog: Protect educational data with Azure
4. Microsoft and Gartner webinar: Information lifecycle and governance in the age of AI and storage limits

Organizations are facing unprecedented complexity

A disconnected collection of fragmented tools

Source: Microsoft

Cybersecurity pros needed in the world

4.8M

Source: ISC2

New regulatory updates tracked every day

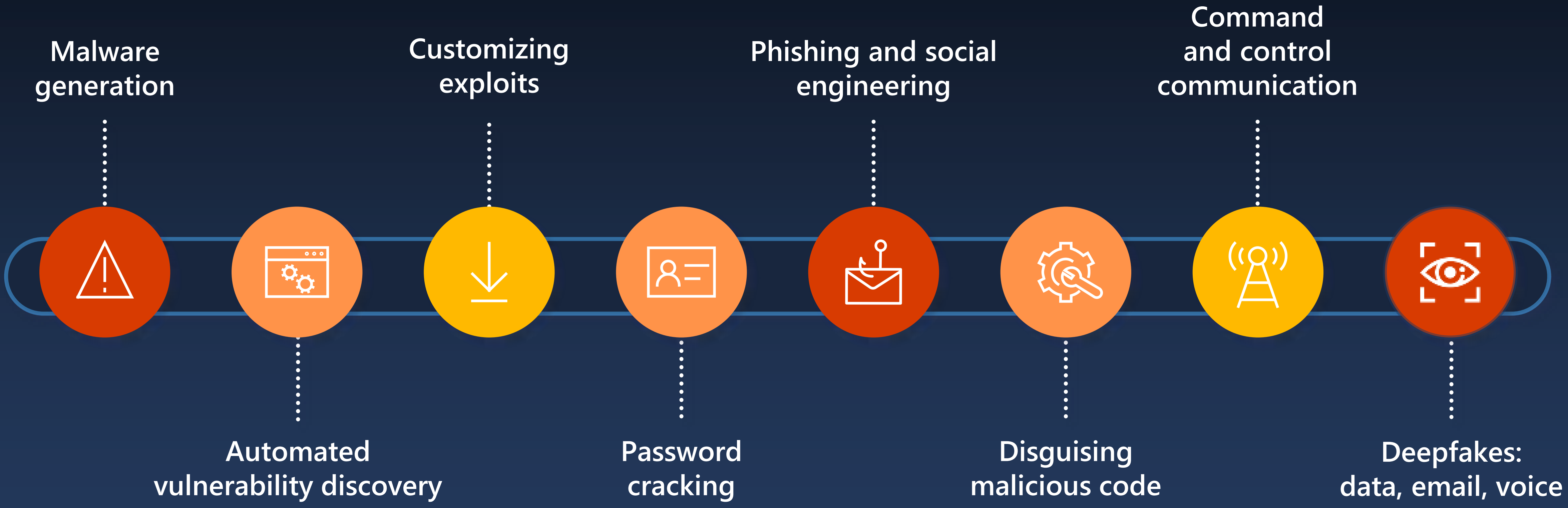
250

every day

Source: IDC

Classified as Microsoft Confidential

Adversaries will use GenAI in creative ways



Malware generation

Automated vulnerability discovery

Customizing exploits

Password cracking

Phishing and social engineering

Disguising malicious code

Command and control communication

Deepfakes: data, email, voice

Classified as Microsoft Confidential

Security teams are forced to defend in silos

Email & collab

Identity

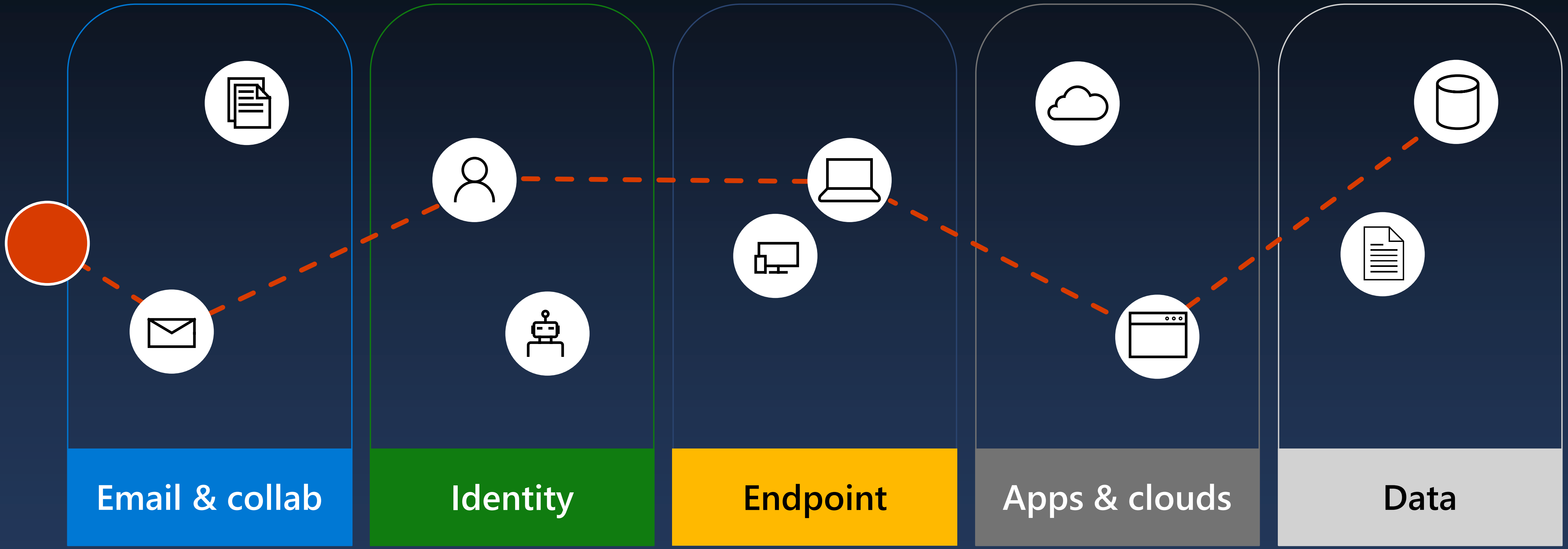
Endpoint

Apps & clouds

Data

...with tools focused on protecting individual domains

Attackers think in graphs



...quietly traversing across the network through the gaps between siloed tools

Classified as Microsoft Confidential

Security teams need better outcomes in the age of AI

Be more secure

Stay compliant

Lower total cost of ownership

What if you could have better outcomes

Lower the risk
of a breach by **72%**

Reduce the time
it takes to respond
to threats by **88%**

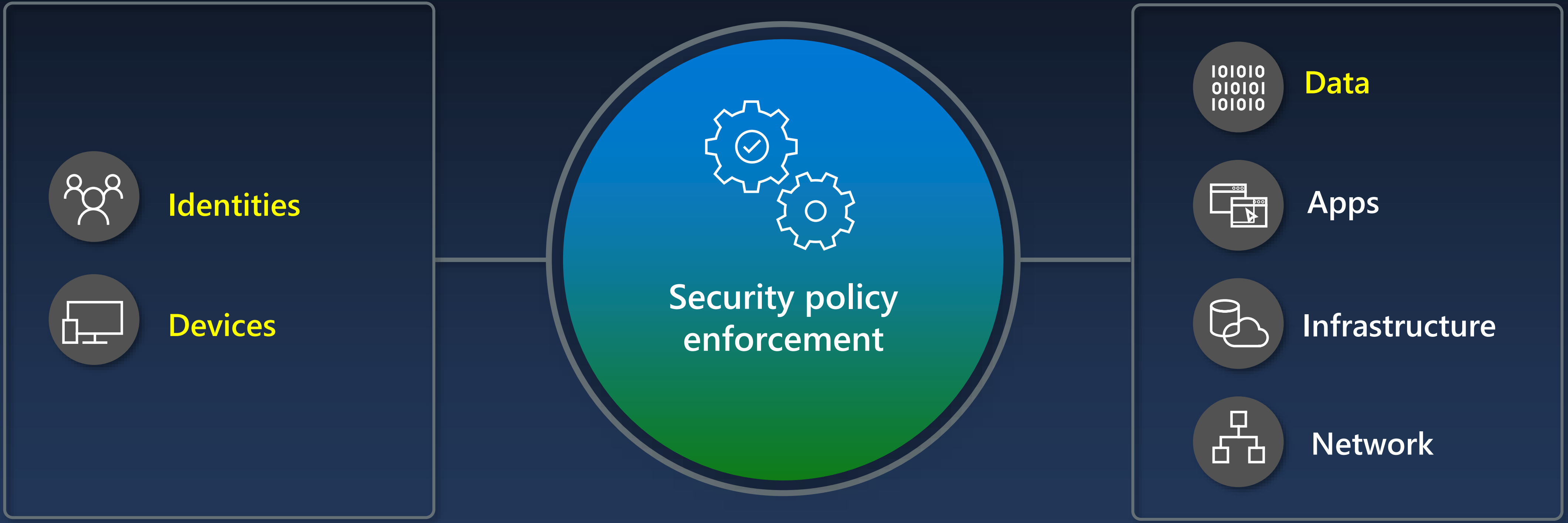
Increase the accuracy
of novice security pros
by **44%**

Sources: Forrester & Microsoft

Classified as Microsoft Confidential

Securing our customers with a Zero Trust approach

Verify explicitly | Use least-privileged access | Assume breach



Identities

Devices

Security policy enforcement

Data

Apps

Infrastructure

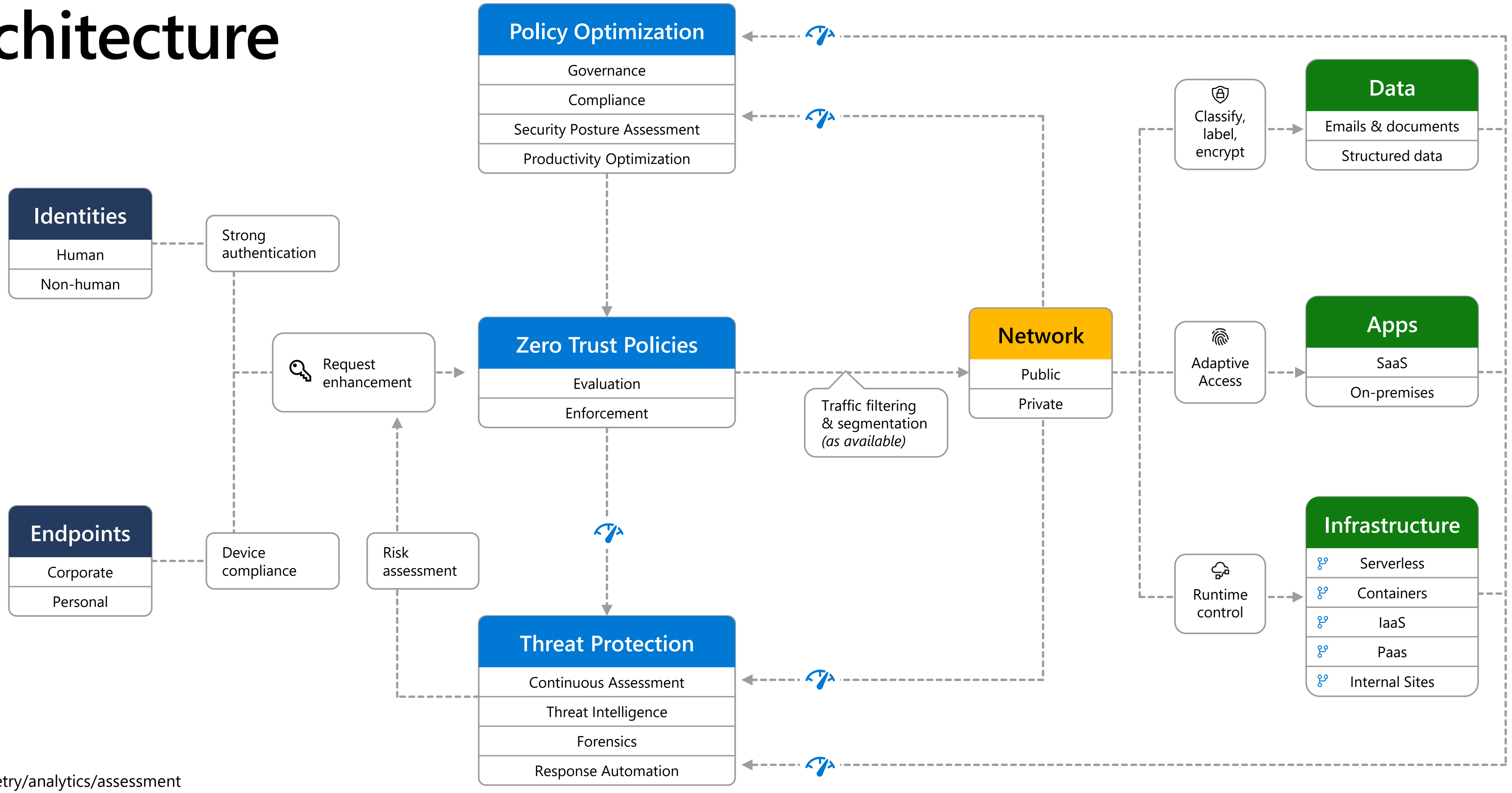
Network

Zero Trust is a proactive mindset that assumes all activity—even by known users—could be an attempt to breach systems.

Classified as Microsoft Confidential

Microsoft Security

Zero Trust architecture



Policy Optimization
- Governance
- Compliance
- Security Posture Assessment
- Productivity Optimization

Identities
- Human
- Non-human

Strong authentication

Request enhancement

Zero Trust Policies
- Evaluation
- Enforcement

Traffic filtering & segmentation *(as available)*

Network
- Public
- Private

Classify, label, encrypt

Data
- Emails & documents
- Structured data

Adaptive Access

Apps
- SaaS
- On-premises

Runtime control

Infrastructure
- Serverless
- Containers
- IaaS
- Paas
- Internal Sites

Endpoints
- Corporate
- Personal

Device compliance

Risk assessment

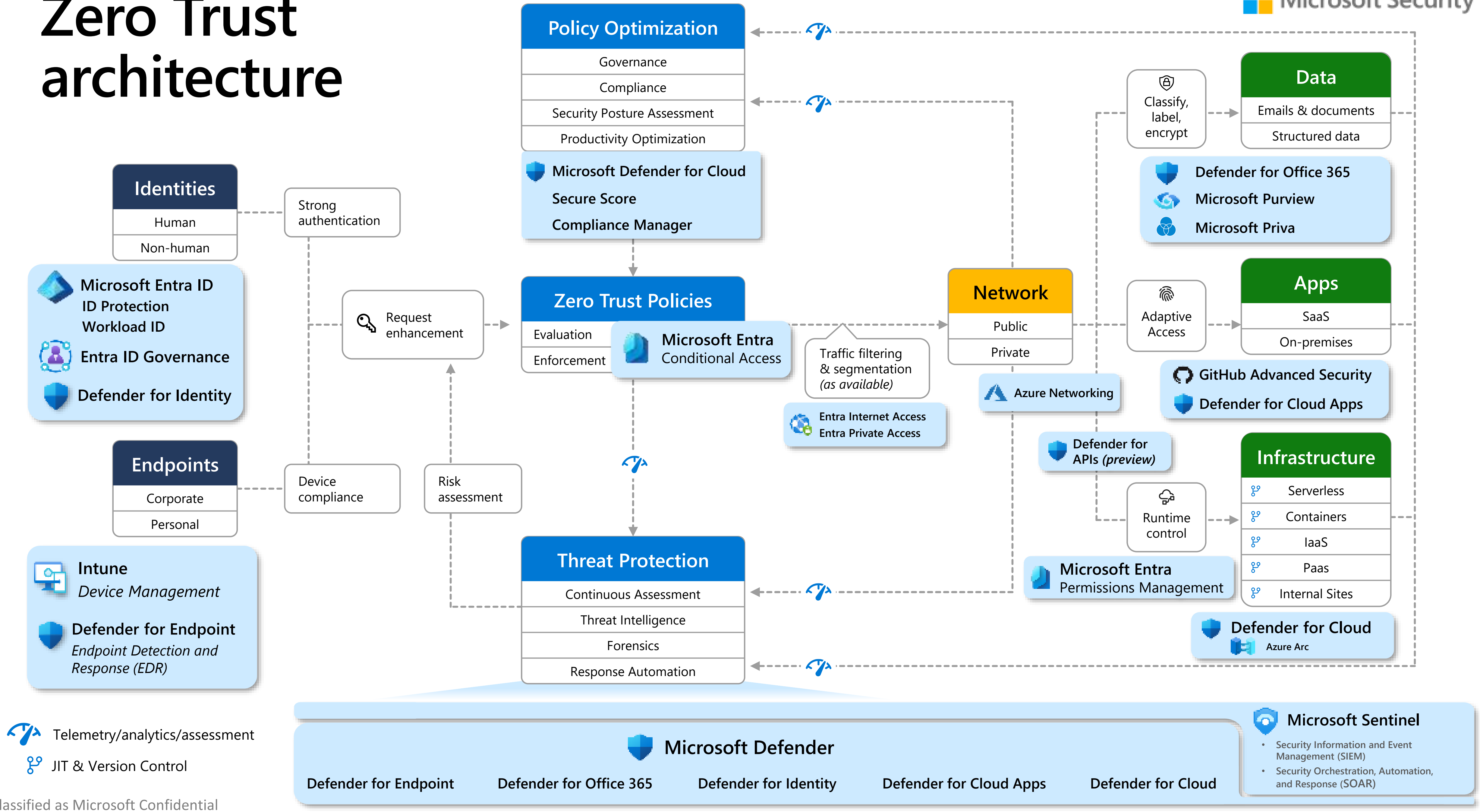
Threat Protection
- Continuous Assessment
- Threat Intelligence
- Forensics
- Response Automation

Telemetry/analytics/assessment

JIT & Version Control

Zero Trust architecture

Microsoft Security



Policy Optimization

- Governance
- Compliance
- Security Posture Assessment
- Productivity Optimization

Microsoft Defender for Cloud
Secure Score
Compliance Manager

Identities

- Human
- Non-human

Strong authentication

Microsoft Entra ID
ID Protection
Workload ID
Entra ID Governance
Defender for Identity

Request enhancement

Zero Trust Policies

- Evaluation
- Enforcement

Microsoft Entra
Conditional Access

Traffic filtering & segmentation *(as available)*

Entra Internet Access
Entra Private Access

Network

- Public
- Private

Azure Networking

Endpoints

- Corporate
- Personal

Device compliance

Risk assessment

Intune
Device Management

Defender for Endpoint
Endpoint Detection and Response (EDR)

Data

Classify, label, encrypt

- Emails & documents
- Structured data

Defender for Office 365
Microsoft Purview
Microsoft Priva

Apps

Adaptive Access

- SaaS
- On-premises

GitHub Advanced Security
Defender for Cloud Apps

Defender for APIs *(preview)*

Infrastructure

Runtime control

- Serverless
- Containers
- IaaS
- Paas
- Internal Sites

Microsoft Entra
Permissions Management

Defender for Cloud
Azure Arc

Threat Protection

- Continuous Assessment
- Threat Intelligence
- Forensics
- Response Automation

Microsoft Defender

Defender for Endpoint | Defender for Office 365 | Defender for Identity | Defender for Cloud Apps | Defender for Cloud

Microsoft Sentinel

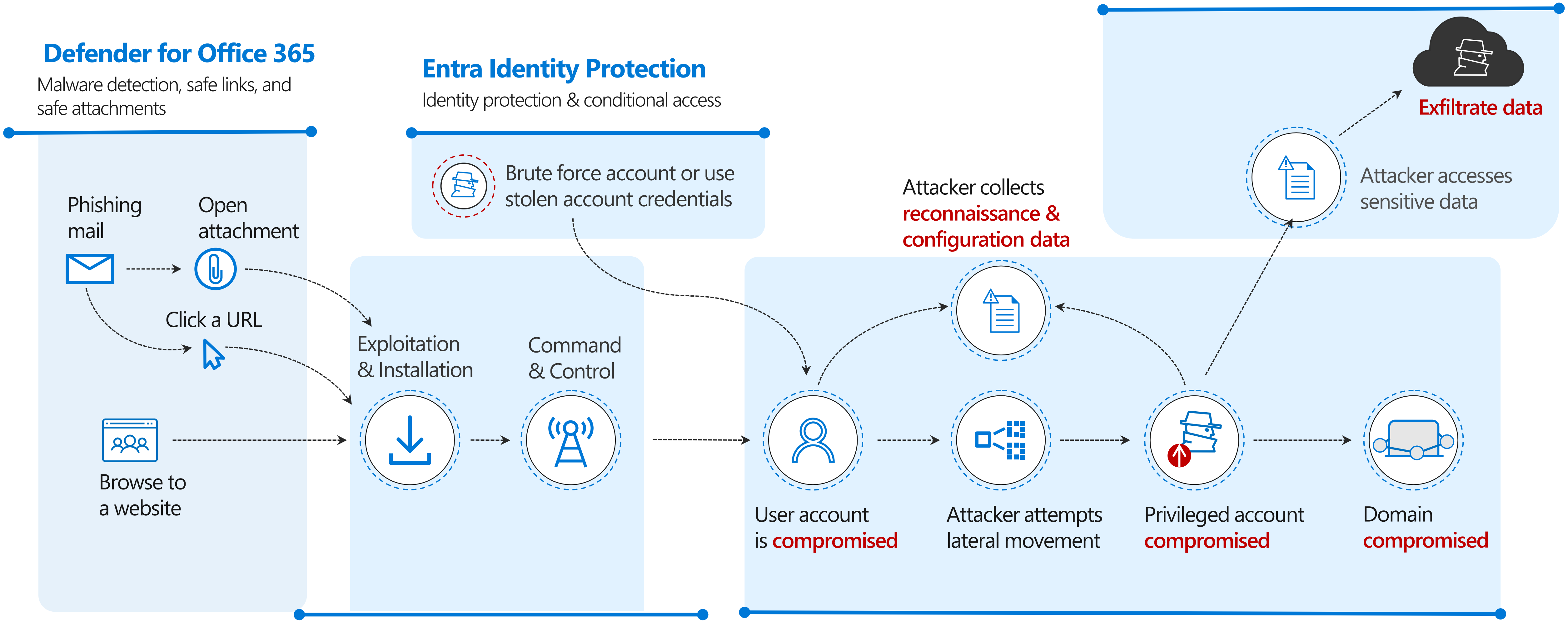
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Telemetry/analytics/assessment
JIT & Version Control

Microsoft Defender XDR

Defender for Cloud Apps

Extends protection & conditional access to other cloud apps



Defender for Office 365

Malware detection, safe links, and safe attachments

Phishing mail

Open attachment

Click a URL

Browse to a website

Entra Identity Protection

Identity protection & conditional access

Brute force account or use stolen account credentials

Exploitation & Installation

Command & Control

Attacker collects **reconnaissance & configuration data**

User account is **compromised**

Attacker attempts lateral movement

Privileged account **compromised**

Domain **compromised**

Attacker accesses sensitive data

Exfiltrate data

Defender for Endpoint

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Defender for Identity

Identity protection

Microsoft Entra ID

Protect your users, apps, workloads, and devices.

Multicloud identity and access management

Users

Apps

Workloads

Devices

Secure
adaptive access

Seamless user
experiences

Unified identity
management

Simplified identity
governance

Microsoft Defender for Identity

Protect on-premises identities with cloud intelligence.

Proactive identity posture assessments highlight misconfigurations or strays from best practice to help bolster defenses.

Risky configurations mean lower security

Built-in detections, mapped to MITRE techniques, enable SecOps to detect threats with high confidence in real time.

Detection breadth: Suspicious activities and behaviour analysis

User investigation priority score combines data from cloud and on-premises to highlight users at the highest risk.

User investigation ranking

Integration with Microsoft Defender XDR delivers **full XDR signal**, enabling advanced hunting and comprehensive automatic remediation.

Automated security workflows

Comprehensive capabilities

Proactive identity security posture assessments

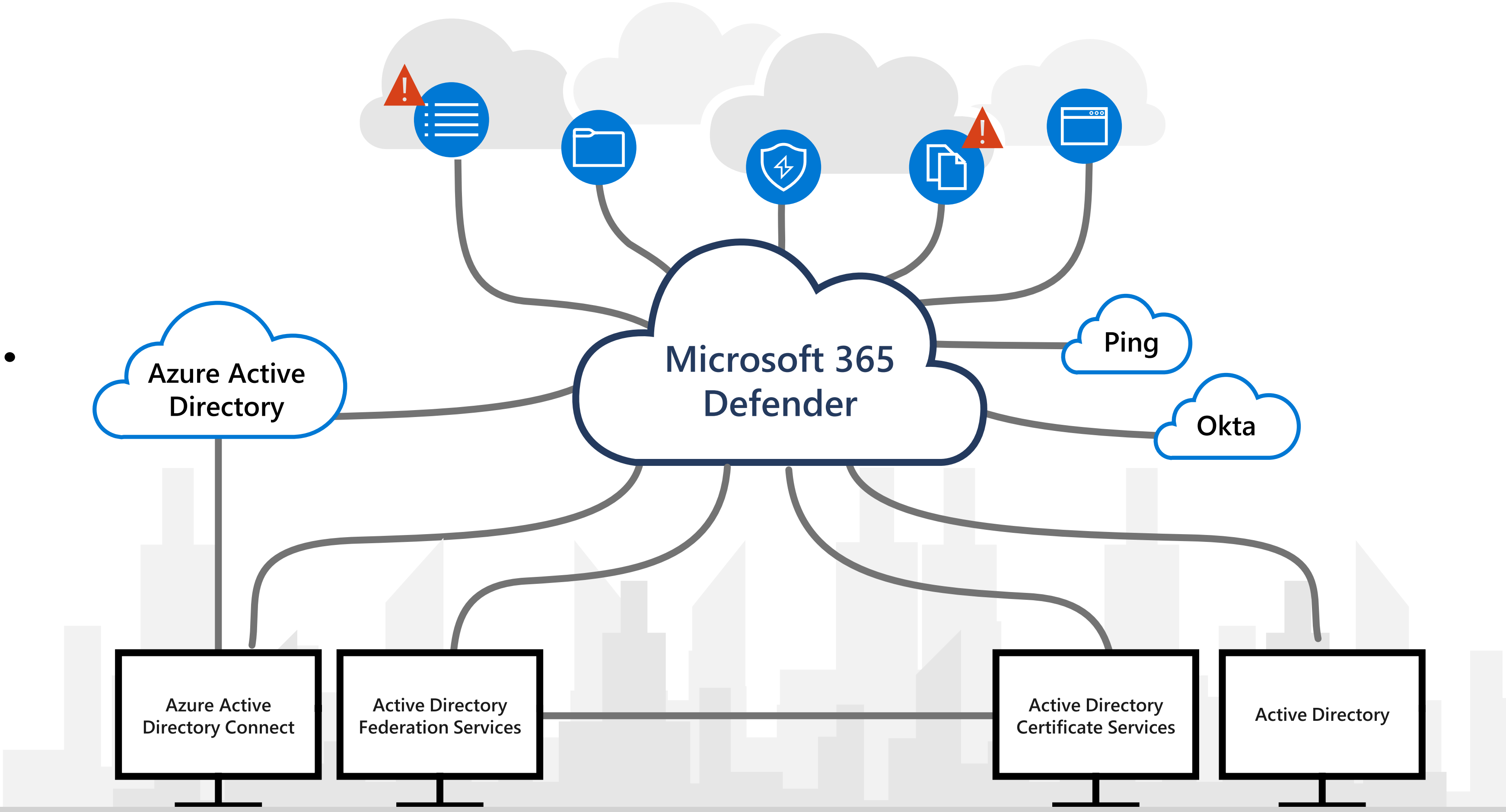
Real-time analytics and data intelligence

User investigation priority

Automatic response to compromised identities

Use advanced identity detections.

Detect attacks across your identities and identity infrastructure.


Microsoft 365 Defender
Azure Active Directory
Ping
Okta
Azure Active Directory Connect
Active Directory Federation Services
Active Directory Certificate Services
Active Directory

Reconnaissance

Security principal enumeration (LDAP)

Users group membership enumeration

Users and IP address enumeration

Credential access

Brute force attempts (now also detected via AD FS)

Suspicious VPN connection

Honeytoken account suspicious activities

Lateral movement

NTLM Relay and NTLM tampering

Pass-the-Ticket

Pass-the-Hash

Overpass-the-Hash

Persistence

Golden Ticket attack

DCShadow, DCSync

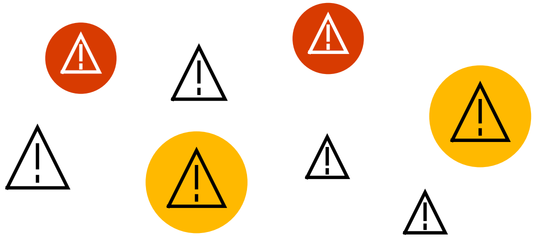
Data exfiltration

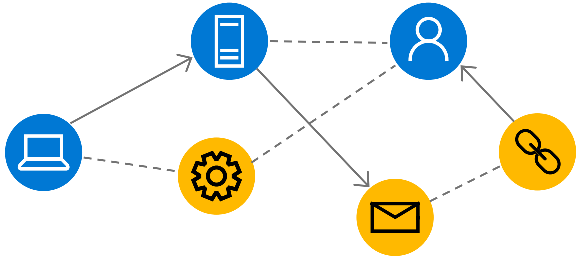
Code execution/service creation on DC & AD FS

SMB packet manipulation

Classified as Microsoft Confidential

Endpoint Detection and Response isn’t enough





vs.

EDR	XDR
Endpoint security only	Holistic security and signal correlation across identity, email, endpoint, cloud app, data loss prevention (DLP) security, and more
Siloed endpoint alerts	Incident-based investigation and response experience
Can only help fend off endpoint-specific attacks and lacks the big picture to help with advanced attacks	Protects against advanced attacks such as ransomware and business email compromise (BEC)

Classified as Microsoft Confidential

Microsoft Defender for Endpoint

Delivering end-to-end protection for all your devices.

Coverage that works **across platforms**—from iOS and Android to Linux and macOS to Windows and network devices.

Industry-leading **threat protection** backed by global threat intelligence, proven with **MITRE attack results**. [1]

Built in AI and **automation** help identify vulnerabilities and threats while enabling rapid response.

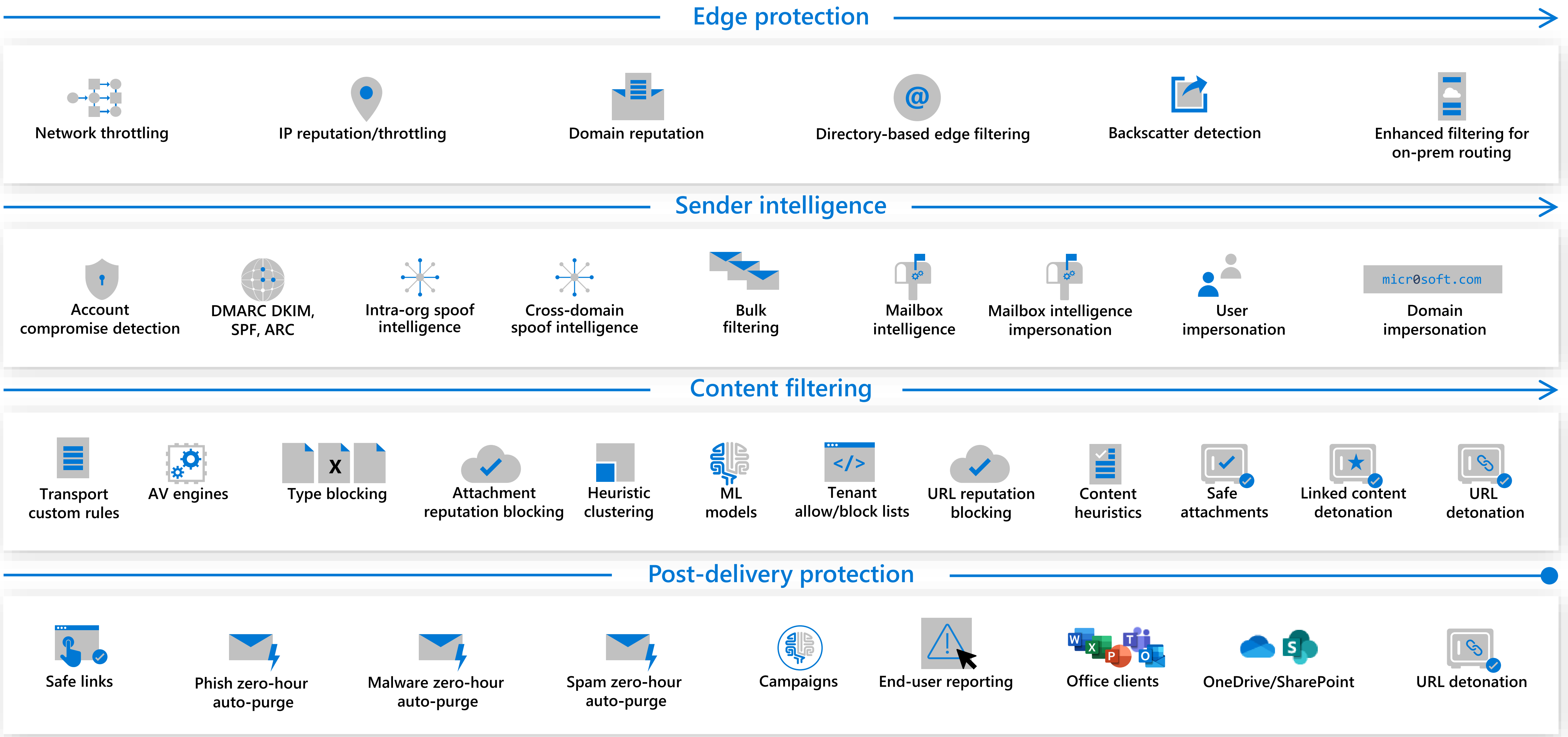
Natively integrates with Microsoft 365 Defender, enabling a **full XDR solution** for more comprehensive protection.

Comprehensive capabilities

- Vulnerability management
- Attack surface reduction
- Next-generation protection
- Endpoint detection and response
- Auto investigation and remediation

[1] Microsoft protects against human-operated ransomware across the full attack chain in the 2022 MITRE Engenuity ATT&CK® Evaluations blog, Rob Lefferts, Corp VP, Microsoft 365 Security

Email - Multi-Layered protection stack



Edge protection

- Network throttling
- IP reputation/throttling
- Domain reputation
- Directory-based edge filtering
- Backscatter detection
- Enhanced filtering for on-prem routing

Sender intelligence

- Account compromise detection
- DMARC DKIM, SPF, ARC
- Intra-org spoof intelligence
- Cross-domain spoof intelligence
- Bulk filtering
- Mailbox intelligence
- Mailbox intelligence impersonation
- User impersonation
- Domain impersonation

Content filtering

- Transport custom rules
- AV engines
- Type blocking
- Attachment reputation blocking
- Heuristic clustering
- ML models
- Tenant allow/block lists
- URL reputation blocking
- Content heuristics
- Safe attachments
- Linked content detonation
- URL detonation

Post-delivery protection

- Safe links
- Phish zero-hour auto-purge
- Malware zero-hour auto-purge
- Spam zero-hour auto-purge
- Campaigns
- End-user reporting
- Office clients
- OneDrive/SharePoint
- URL detonation

Classified as Microsoft Confidential

Microsoft Defender for Cloud Apps

Discover and control the use of shadow IT

Identify, and assess risk of cloud apps and services used by your organization.

Protect your information anywhere in the cloud

Understand, classify, and protect the exposure of sensitive information—across all your cloud apps.

Protect against cyberthreats and anomalies

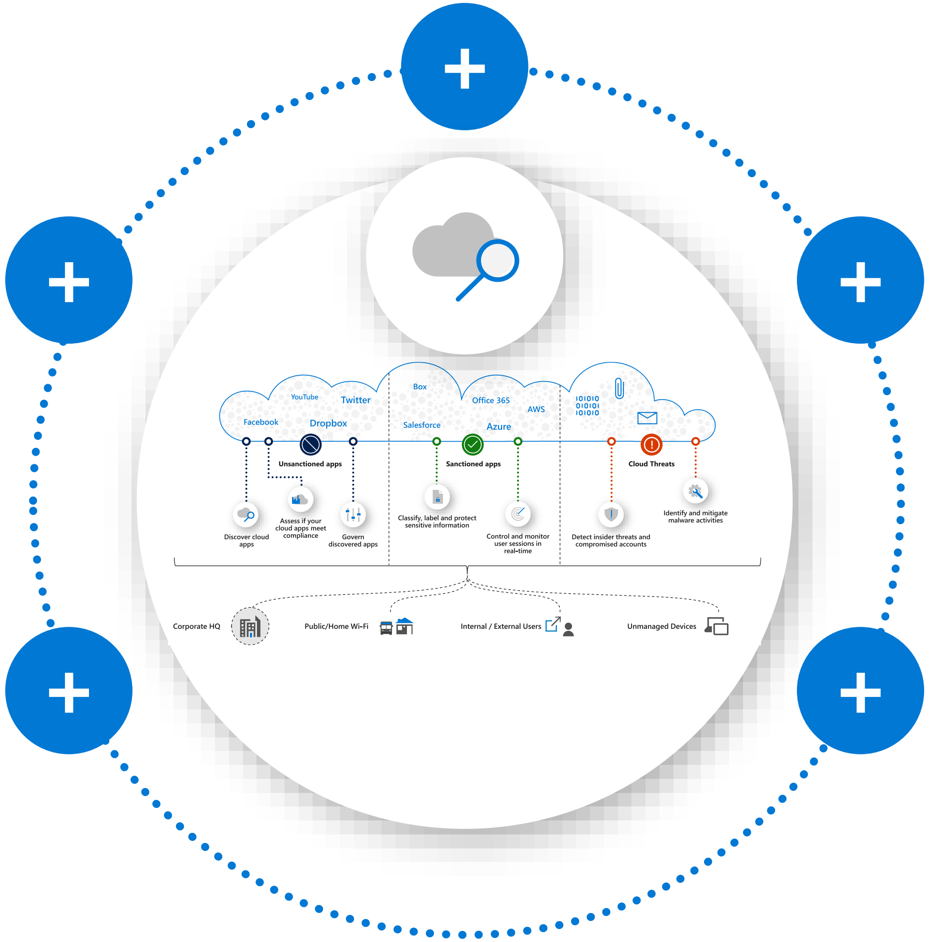
Detect unusual behavior, compromised users, or rogue applications and remediate automatically.

Secure Access

Secure access, without compromising performance, for any user on any device to any resource.

Security Posture Management

Investigate security configuration gaps by viewing all cloud platform security recommendations together.


+
+
+
+
+
Facebook
YouTube
Twitter
Dropbox
Unsanctioned apps
Discover cloud apps
Assess if your cloud apps meet compliance
Govern discovered apps
Box
Salesforce
Office 365
AWS
Azure
Sanctioned apps
Classify, label and protect sensitive information
Control and monitor user sessions in real-time
101010
010101
101010
Cloud Threats
Detect insider threats and compromised accounts
Identify and mitigate malware activities
Corporate HQ
Public/Home Wi-Fi
Internal / External Users
Unmanaged Devices

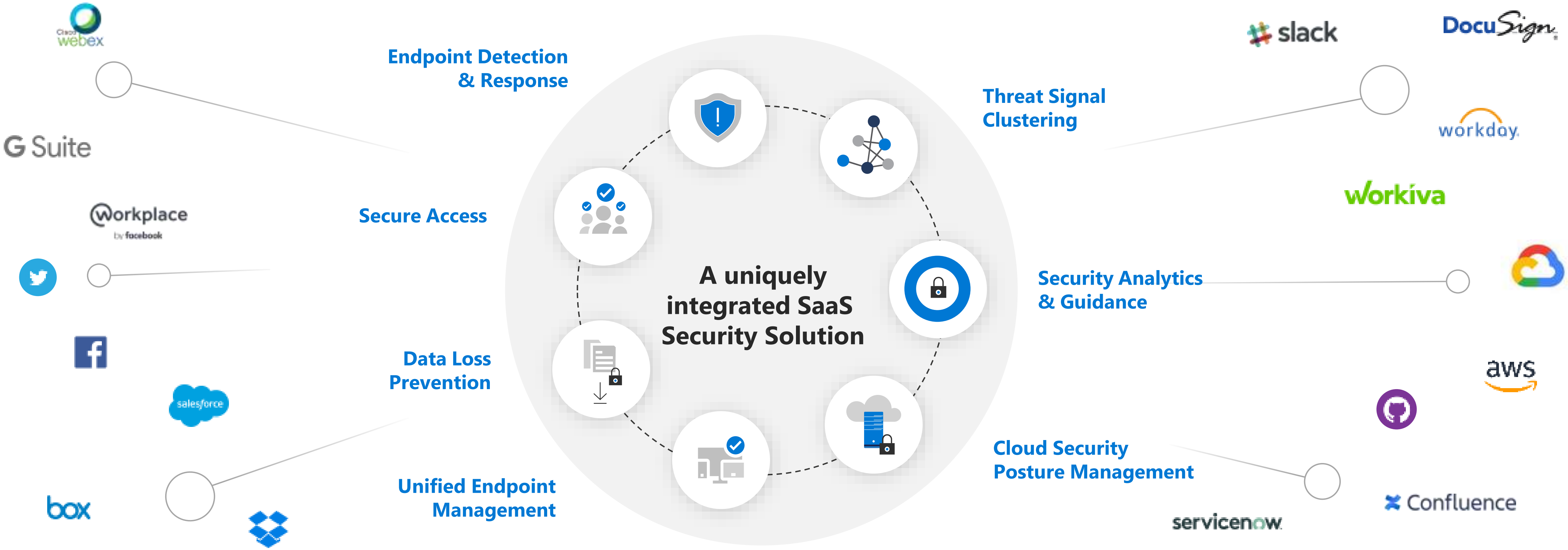
Microsoft Defender for Cloud Apps

SaaS Security Platform

Deep Visibility and Risk Assessment

Natively integrated across the broader Microsoft product stack to deliver unique capabilities

Rooted in supporting any app



A uniquely integrated SaaS Security Solution

Endpoint Detection & Response

Threat Signal Clustering

Secure Access

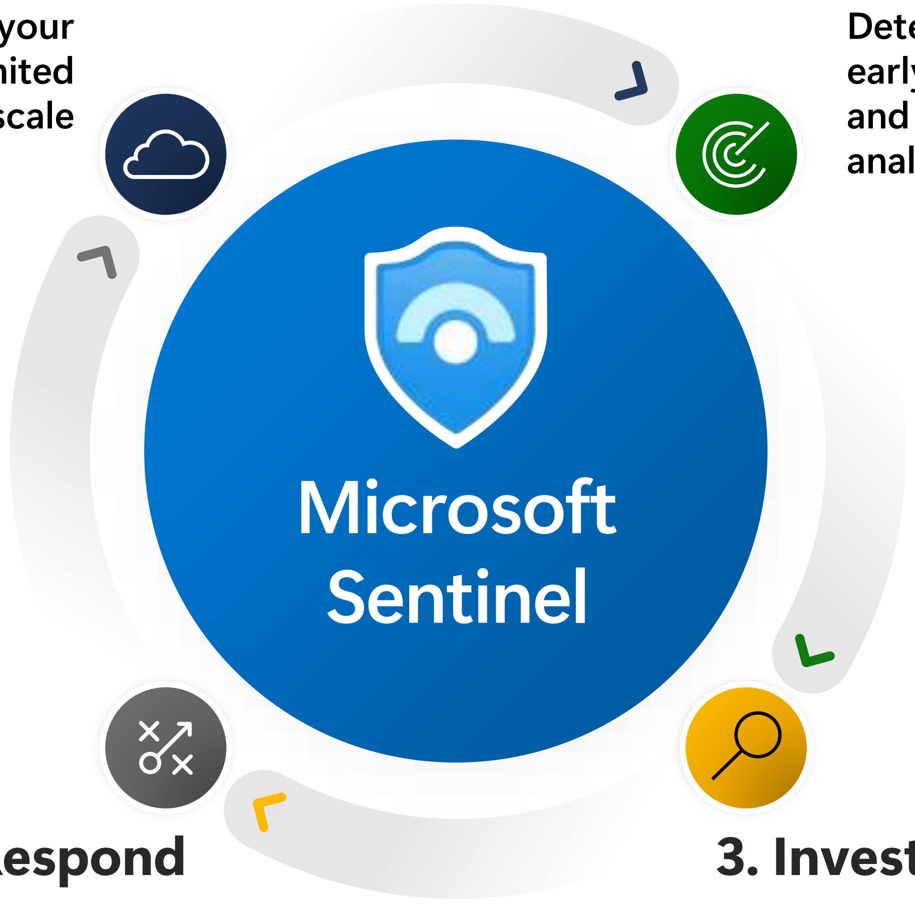
Security Analytics & Guidance

Data Loss Prevention

Cloud Security Posture Management

Unified Endpoint Management

Flexible protection across your multi-cloud, multi-platform environments



1. Collect

Gather data from all your sources with unlimited cloud speed and scale

2. Detect

Detect anomalies early with user entity and behavior analytics

3. Investigate

Correlate alerts into prioritized incidents for a full picture of attacks

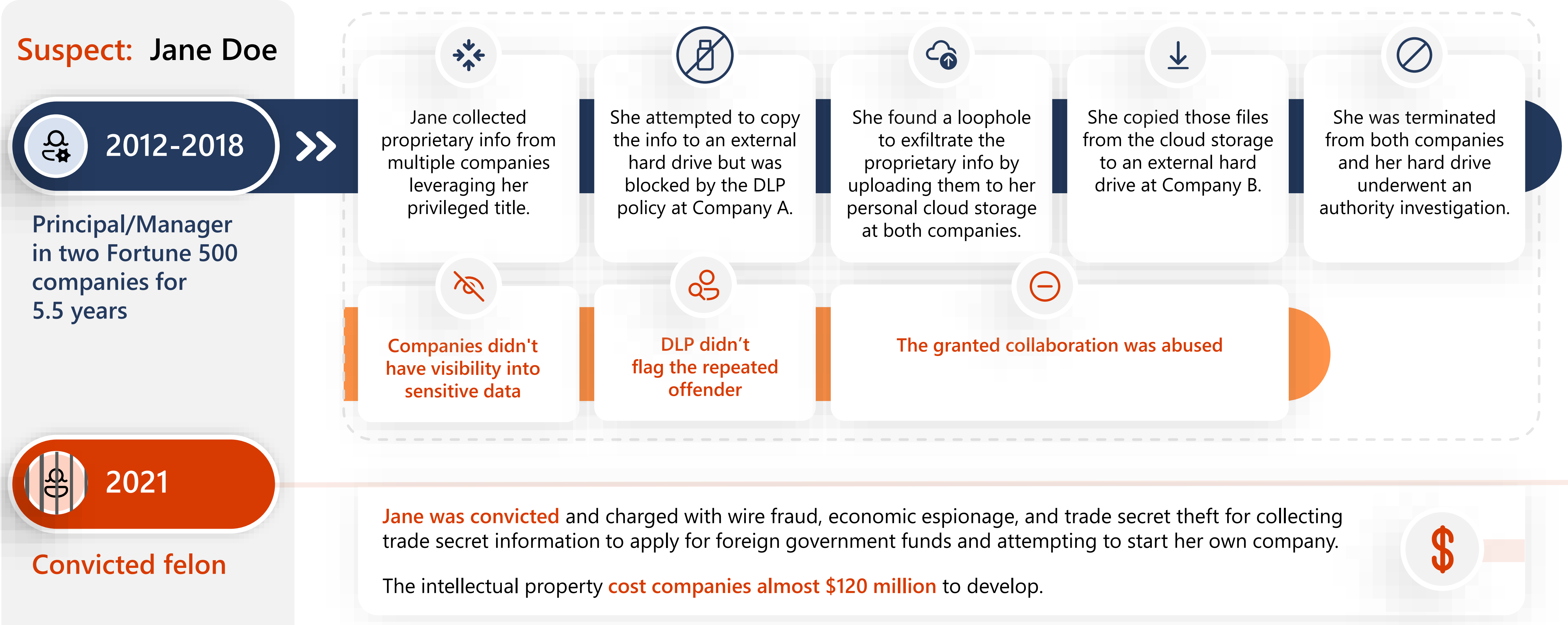
4. Respond

Built in SOAR automation for rapid response

Classified as Microsoft Confidential

A real-world story of corporate espionage

Trusted employee, Jane Doe, used stolen proprietary information to start her own company



Suspect: Jane Doe

2012-2018

Principal/Manager in two Fortune 500 companies for 5.5 years

Jane collected proprietary info from multiple companies leveraging her privileged title.

She attempted to copy the info to an external hard drive but was blocked by the DLP policy at Company A.

She found a loophole to exfiltrate the proprietary info by uploading them to her personal cloud storage at both companies.

She copied those files from the cloud storage to an external hard drive at Company B.

She was terminated from both companies and her hard drive underwent an authority investigation.

Companies didn't have visibility into sensitive data

DLP didn’t flag the repeated offender

The granted collaboration was abused

2021

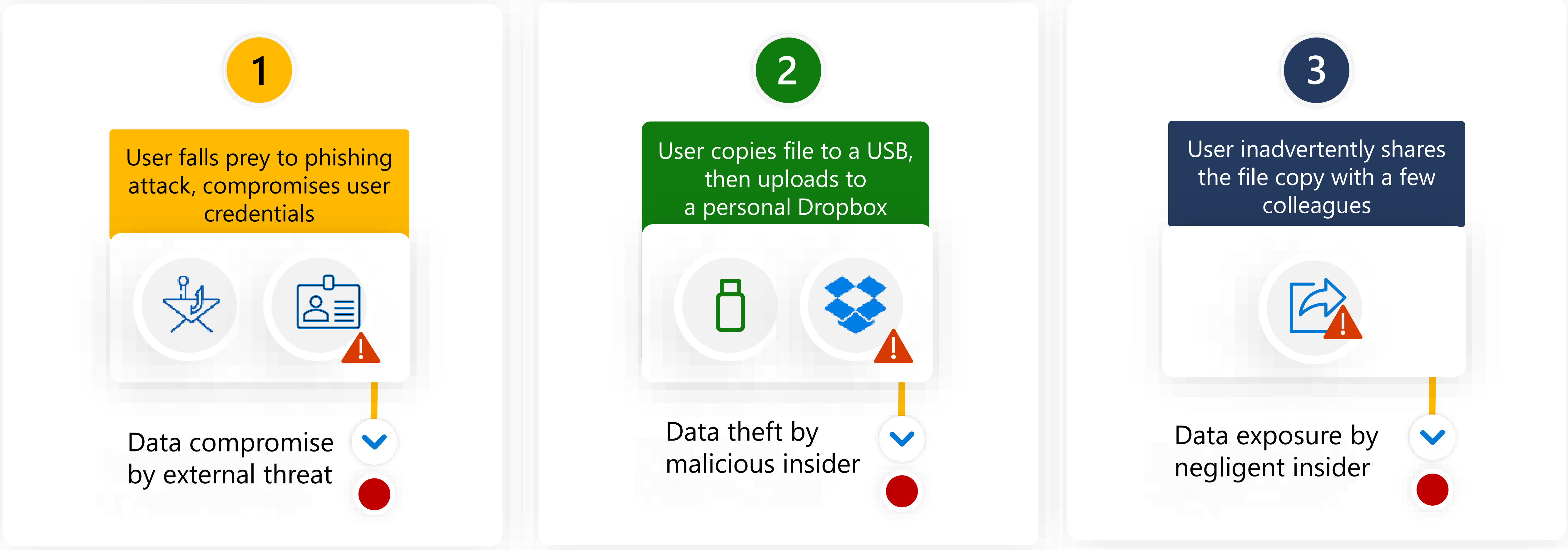
Convicted felon

Jane was convicted and charged with wire fraud, economic espionage, and trade secret theft for collecting trade secret information to apply for foreign government funds and attempting to start her own company.

The intellectual property cost companies almost $120 million to develop.

Data security incidents can happen anytime, anywhere

Data at risk of misuse if organization has no visibility into their data estate



1

User falls prey to phishing attack, compromises user credentials

Data compromise by external threat

2

User copies file to a USB, then uploads to a personal Dropbox

Data theft by malicious insider

3

User inadvertently shares the file copy with a few colleagues

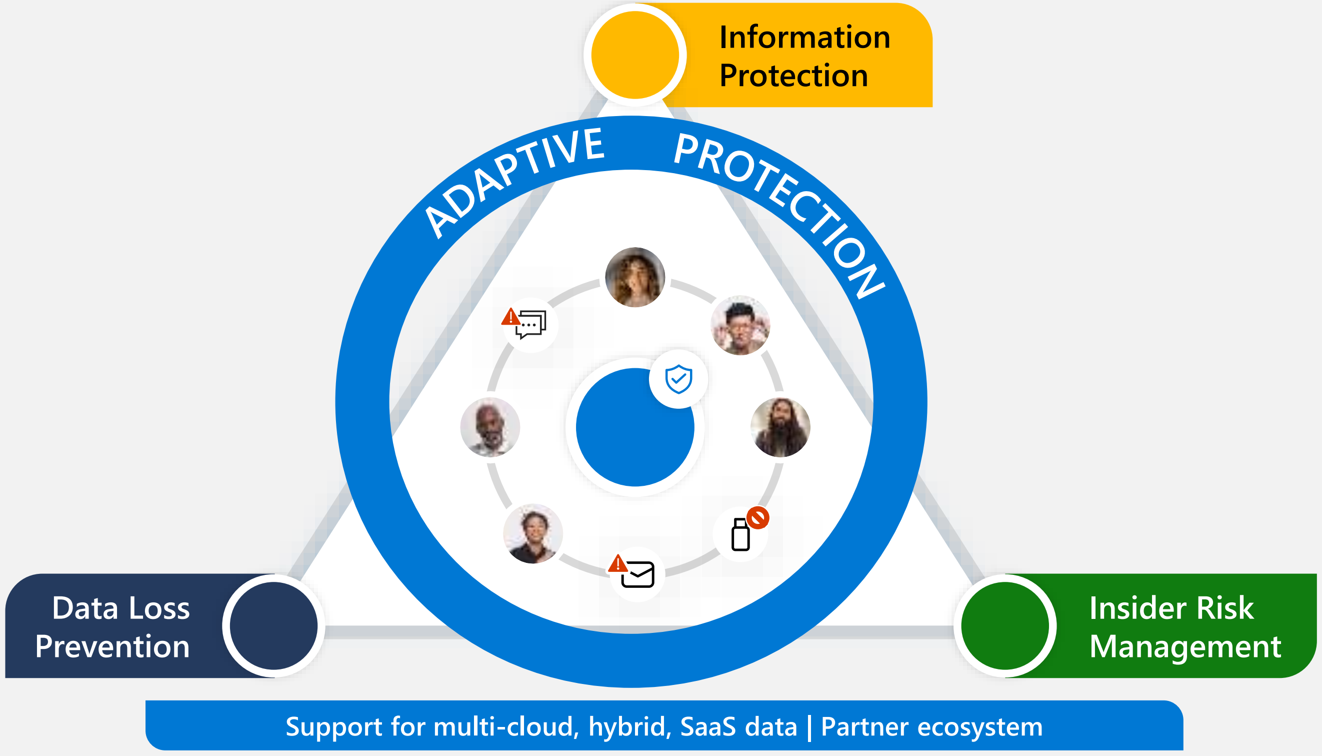
Data exposure by negligent insider

Fortify data security with an integrated approach

Discover and auto-classify data and prevent it from unauthorized use across apps, services, and devices

Understand the **user intent and context around sensitive data** to identify the most critical risks

Enable **Adaptive Protection** to assign appropriate DLP policies to high-risk users



Adaptive Protection in Microsoft Purview

Optimize data security automatically

Context-aware detection

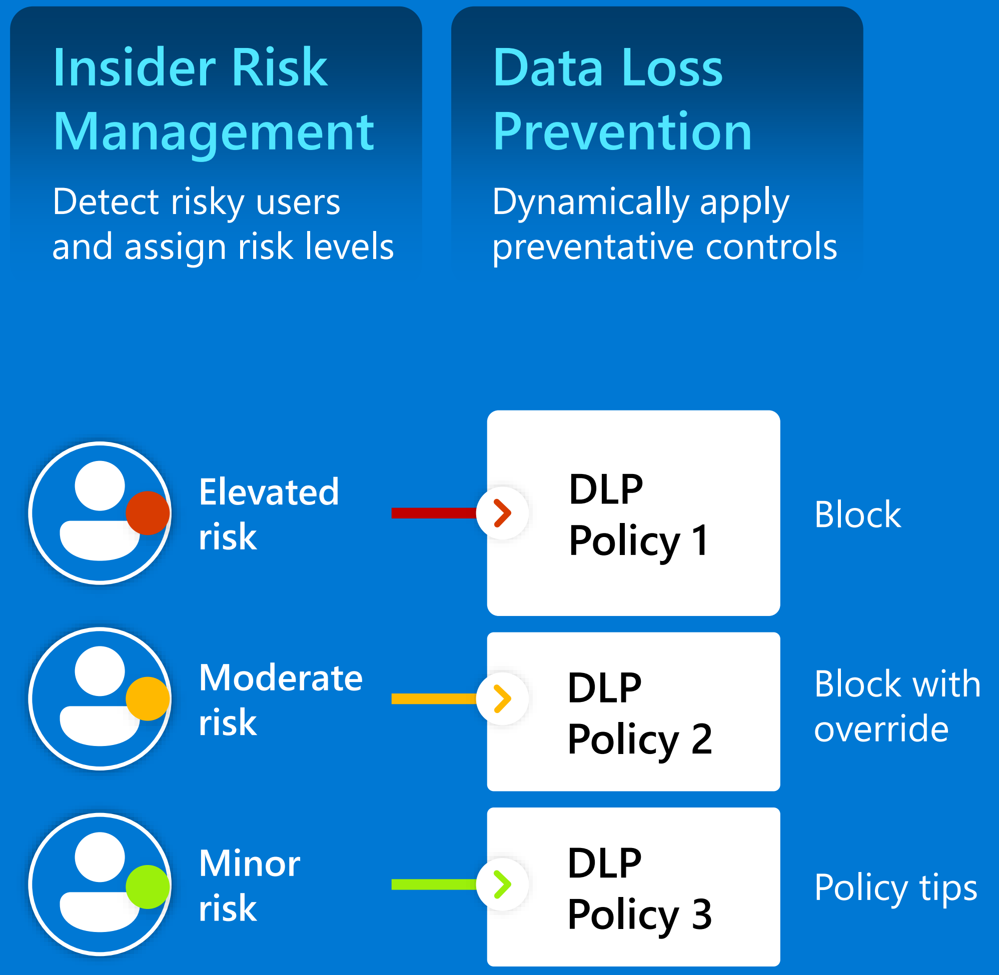
Identify the most critical risks with ML-driven analysis of both content and user activities

Dynamic controls

Enforce effective controls on high-risk users while others maintain productivity

Automated mitigation

Minimize the impact of potential data security incidents and reduce admin overhead



Insider Risk Management

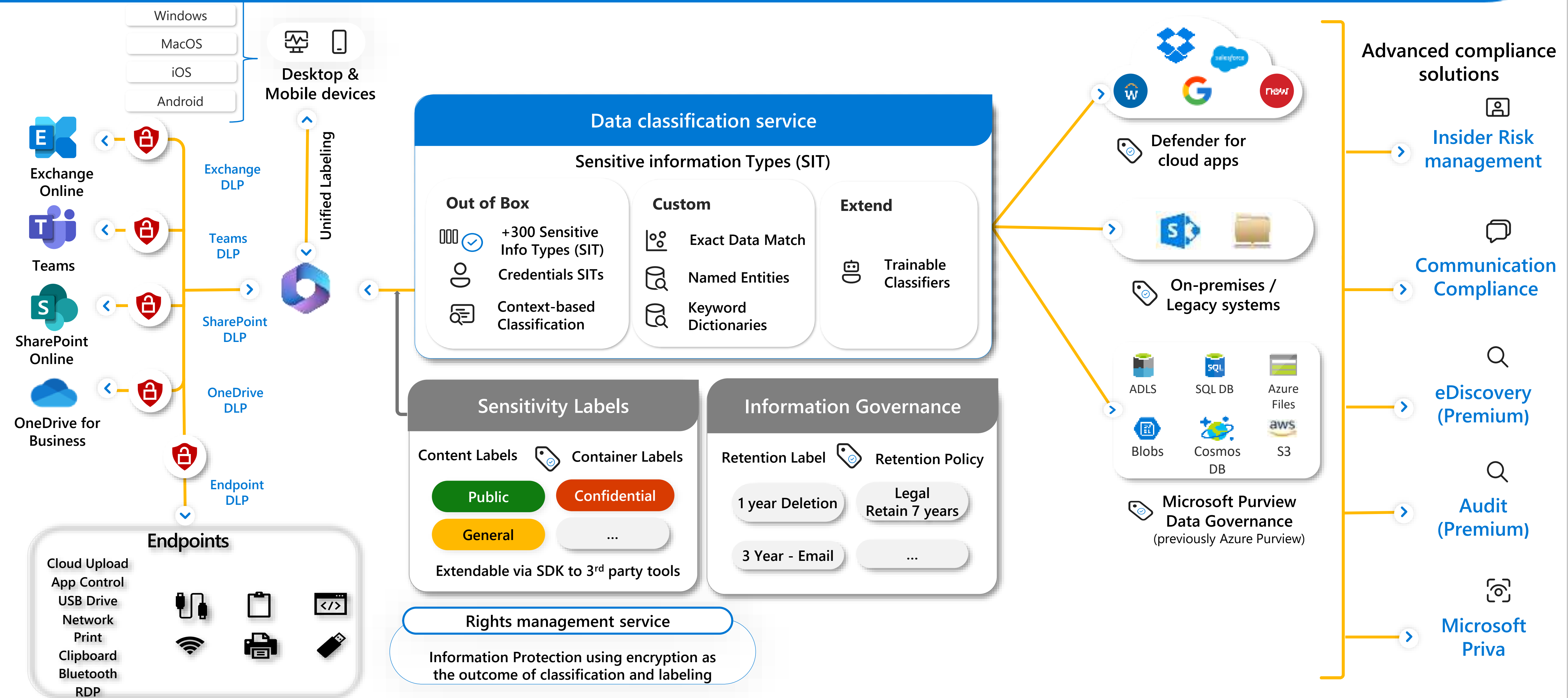
Detect risky users and assign risk levels

Data Loss Prevention

Dynamically apply preventative controls

Elevated risk	DLP Policy 1	Block
Moderate risk	DLP Policy 2	Block with override
Minor risk	DLP Policy 3	Policy tips

Microsoft Purview Data Security



Windows
MacOS
iOS
Android

Desktop & Mobile devices

Unified Labeling

Exchange Online

Teams

SharePoint Online

OneDrive for Business

Exchange DLP

Teams DLP

SharePoint DLP

OneDrive DLP

Endpoint DLP

Endpoints

Cloud Upload
App Control
USB Drive
Network
Print
Clipboard
Bluetooth
RDP

Data classification service

Sensitive information Types (SIT)

Out of Box
- +300 Sensitive Info Types (SIT)
- Credentials SITs
- Context-based Classification

Custom
- Exact Data Match
- Named Entities
- Keyword Dictionaries

Extend
- Trainable Classifiers

Sensitivity Labels

Content Labels
Container Labels

Public
Confidential
General
...

Extendable via SDK to 3rd party tools

Information Governance

Retention Label
Retention Policy

1 year Deletion
Legal Retain 7 years
3 Year - Email
...

Rights management service

Information Protection using encryption as the outcome of classification and labeling

Defender for cloud apps

On-premises / Legacy systems

ADLS
SQL DB
Azure Files
Blobs
Cosmos DB
S3

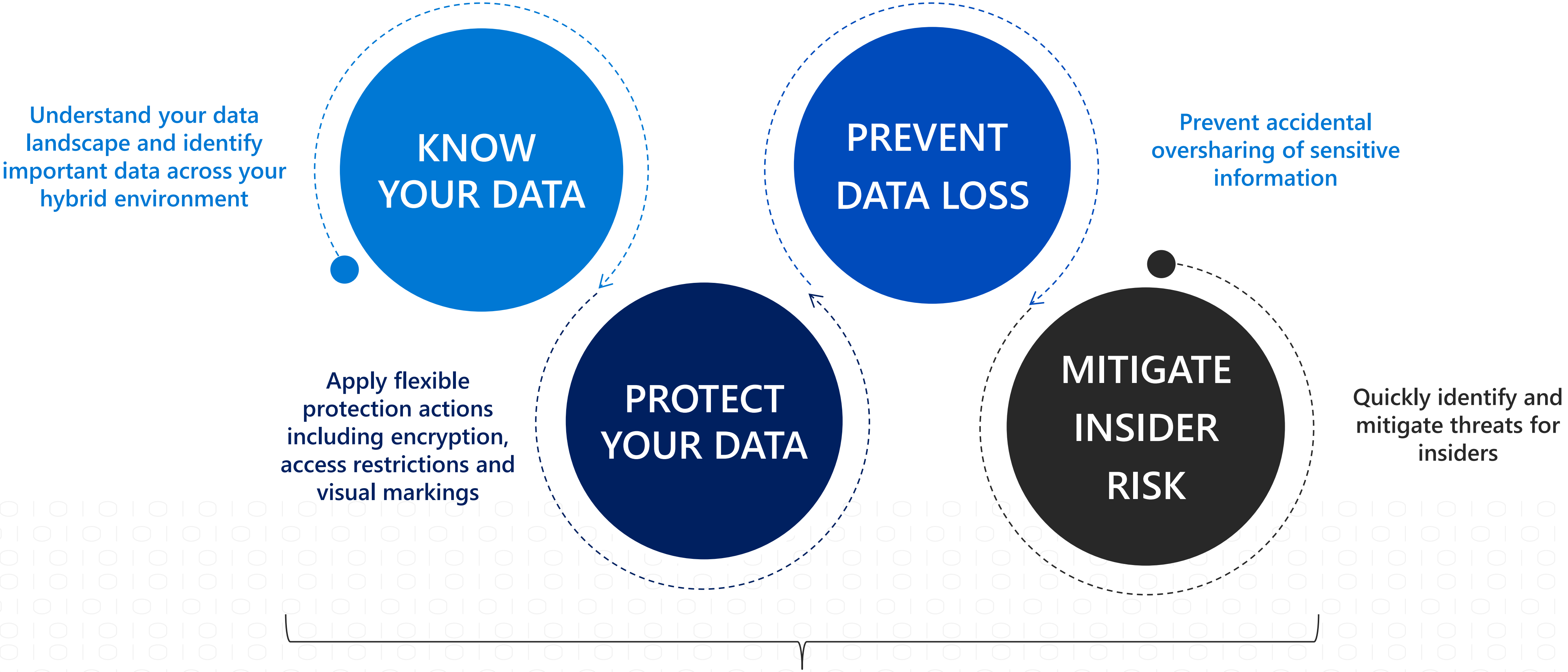
Microsoft Purview Data Governance
(previously Azure Purview)

Advanced compliance solutions

- Insider Risk management
- Communication Compliance
- eDiscovery (Premium)
- Audit (Premium)
- Microsoft Priva

Data Security

Protecting your digital crown jewels


Understand your data landscape and identify important data across your hybrid environment
KNOW YOUR DATA
PREVENT DATA LOSS
Prevent accidental oversharing of sensitive information
Apply flexible protection actions including encryption, access restrictions and visual markings
PROTECT YOUR DATA
MITIGATE INSIDER RISK
Quickly identify and mitigate threats for insiders

Powered by an intelligent platform

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

Microsoft Purview Suite

Microsoft

Compliance Management

Microsoft offers the most comprehensive set of compliance offerings to help you comply with national, regional, and ***industry-specific requirements*** (**NIST**, **CJIS, IRS Pub 1075**, **HIPAA** ...)

Data Security & Governance

Information protection

Discover, classify, and protect sensitive and business-critical content throughout its lifecycle across your organization.

Data loss prevention

Detects sensitive content as it's used and shared throughout your organization, in the cloud and on devices, and helps prevent accidental data loss.

Data Lifecycle Management

Manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't.

Records management

Uses intelligent classification to automate and simplify the retention schedule for regulatory, legal and business-critical records in your organization.

Risk Management

Insider risk management

Detects risky activity across your organization to help you quickly identify, investigate, and take actions on insider risks and threats.

Communication compliance

Minimizes communication risks by helping you automatically capture inappropriate messages, investigate possible policy violations, and take steps to remediate.

Data Security Posture Management for AI

Provides reports to quickly gain insights into AI use within your organization. One-click policies help you protect your data and comply with regulatory requirements.

Discover & Respond

eDiscovery

Helps respond to FOIL and litigation discovery requests using core and advanced solutions for identifying, preserving, analyzing, and exporting data.

Audit

Records user and admin activity from your organization so you can search the audit log and investigate a comprehensive list of activities across all locations and services.

Privacy Management (Microsoft Priva)

GDPR

Generates actionable insights on enterprise *personal data to help you spot issues and reduce risks and to respond to data subject requests*.

Fortify data security with Microsoft Purview

Information Protection

- **Discover, classify, and protect** data at scale, using automation and ML
- Productivity tools with built-in **user-selectable sensitivity labels** for precise controls
- Data is **protected (encrypted) across environments**, throughout its lifecycle

Insider Risk Management

- Leverage **analytics, machine learning, sequencing** to understand user context and intent
- Investigate potential incidents with **curated, high-quality, and enriched** alerts and evidence
- Ensure user privacy while identifying **highest risk users**

Data Loss Prevention

- **Prevent unauthorized use,** like improperly saving, storing or printing sensitive data
- Create, deploy, and manage DLP policies **across all cloud, apps, and devices from a single location**
- Leverage data classification, labeling, and user **insights to finetune and adapt DLP policies**

Adaptive Protection

- Dynamically adjust data security controls based on user risk level

Blueprint for securing data by default (4 phases)

	Foundational	Managed	Optimized	Strategic
	Start with recommended labels	**Address files with highest sensitivity**	**Expand to your entire M365 data estate**	**Operate, expand, and retroactive actions**
Activities	Start with ***default labels*** and protection at ***file and site*** level	Manually configure priority sites ***default library*** labeling	Auto-label sensitive files ***on clients*** (low thresholds)	***Operational review*** of user labeling behaviors
	Turn on data security pre-requisites and adv. Analytics (currently in preview)	Autolabeling for credentials and contextual conditions *(low hanging fruit to protect city)*	***Simulate*** auto-labeling sensitive files at rest	***Iterate*** with new labeling scenarios
	Train users on managing exceptions *(make policy tips part of cyber awareness training)*	Turn on DLP for content that is ***not*** labeled *(PCI, PHI, PII, IP, IRS, etc)*	Reduce false positives with advanced classifiers	Set up accountability chain and lifecycle management
	Turn on DLP for labeled content *(Sensitive & Restricted)*	Turn on ***Adaptive Protection*** and data leak behavioral rules *(Requires Insider Risk Management)*	Automate and improve M365 protection to historical and in use data *(Automatic label policies – SP/OD/EXO)*	***Extend protection*** to Azure SQL, Fabric, and other non-M365 storage *(file shares)*
Outcomes	M365 new/updated content protected	M365 priority content protected	M365 historical content protected	Protection beyond M365
Efforts	1 week	2 weeks	2 weeks iteration	Situational

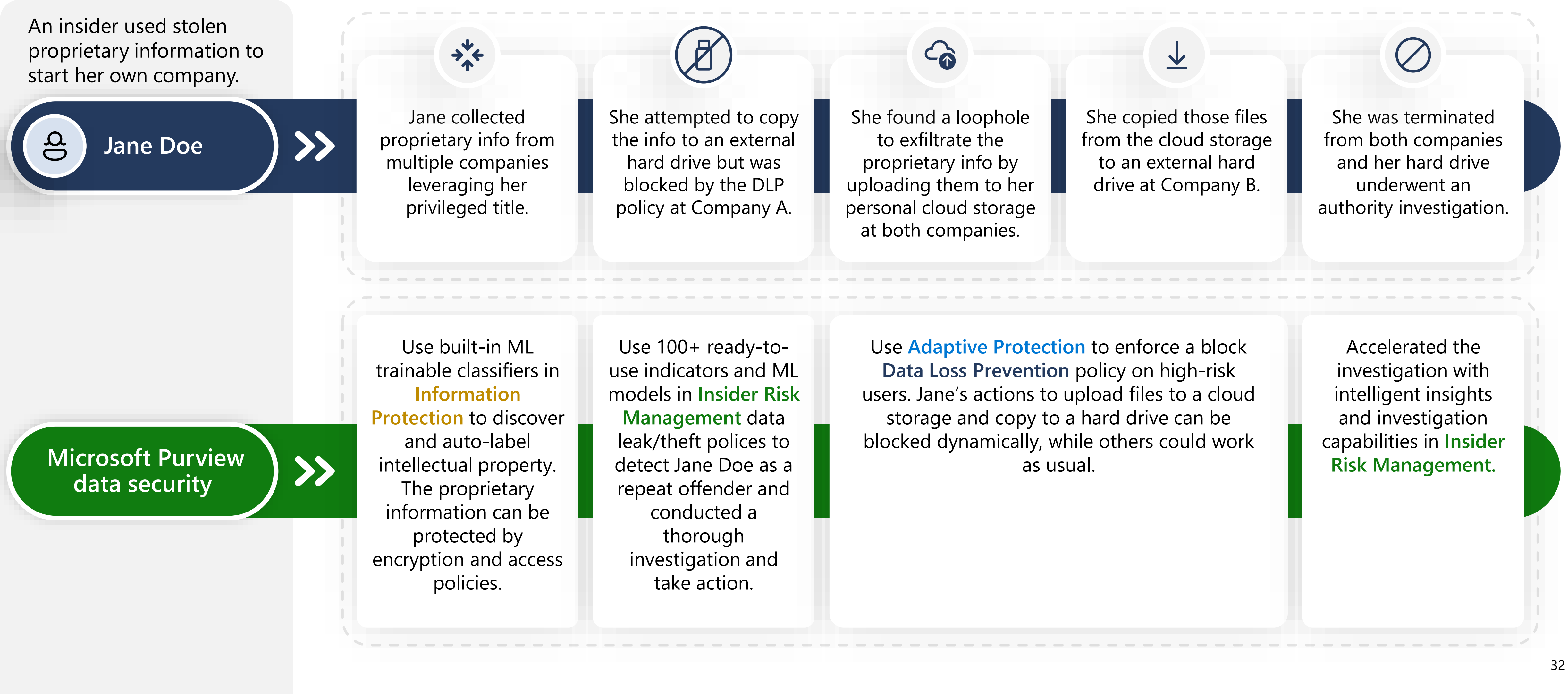
https://aka.ms/PurviewDeploymentModels/SecureByDefault

Last updated: August 27, 2025

Classified as Microsoft Confidential

Let’s go back to Jane Doe…

This incident illustrates data protection gaps Microsoft Purview was designed to cover



An insider used stolen proprietary information to start her own company.

Jane Doe

Jane collected proprietary info from multiple companies leveraging her privileged title.

She attempted to copy the info to an external hard drive but was blocked by the DLP policy at Company A.

She found a loophole to exfiltrate the proprietary info by uploading them to her personal cloud storage at both companies.

She copied those files from the cloud storage to an external hard drive at Company B.

She was terminated from both companies and her hard drive underwent an authority investigation.

Microsoft Purview data security

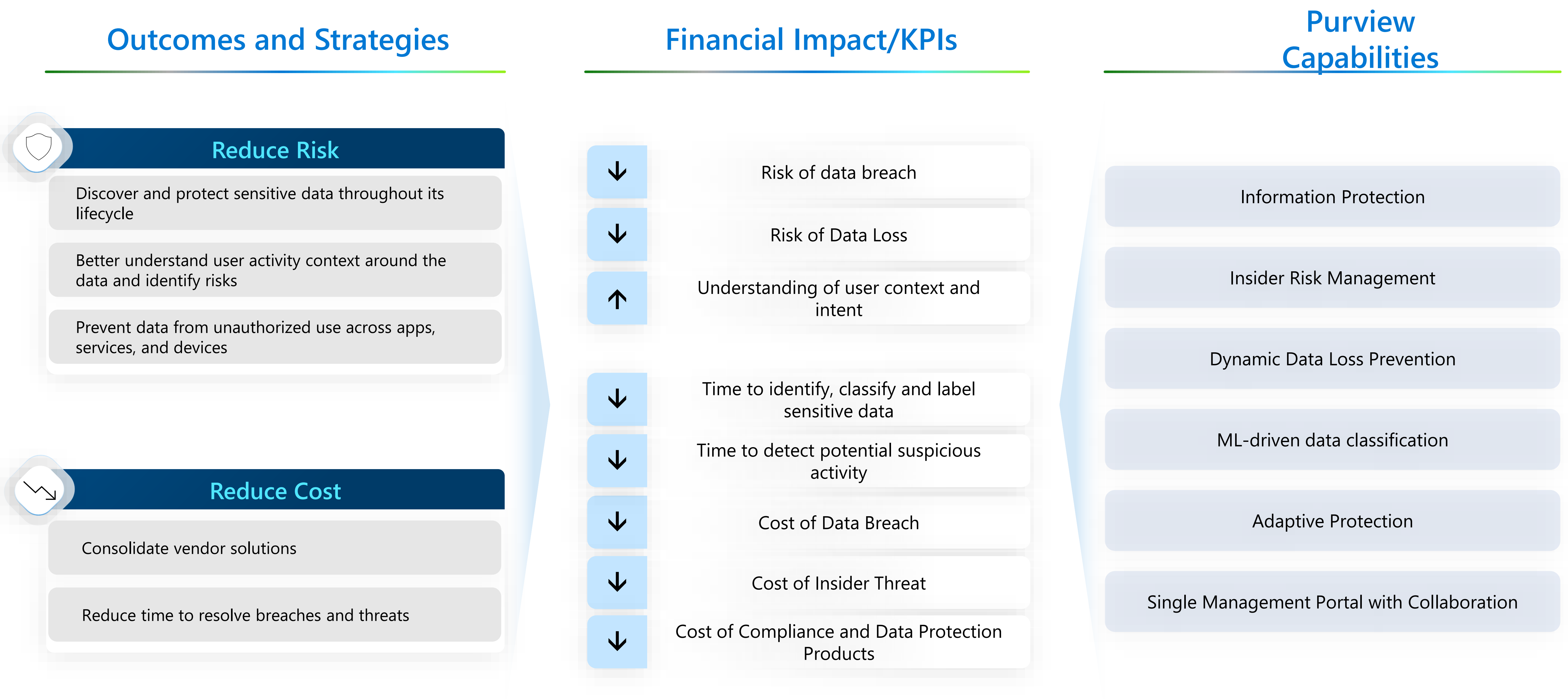
Use built-in ML trainable classifiers in Information Protection to discover and auto-label intellectual property. The proprietary information can be protected by encryption and access policies.

Use 100+ ready-to-use indicators and ML models in Insider Risk Management data leak/theft polices to detect Jane Doe as a repeat offender and conducted a thorough investigation and take action.

Use Adaptive Protection to enforce a block Data Loss Prevention policy on high-risk users. Jane’s actions to upload files to a cloud storage and copy to a hard drive can be blocked dynamically, while others could work as usual.

Accelerated the investigation with intelligent insights and investigation capabilities in Insider Risk Management.

Purview Data Security value map



Outcomes and Strategies

Reduce Risk

- Discover and protect sensitive data throughout its lifecycle
- Better understand user activity context around the data and identify risks
- Prevent data from unauthorized use across apps, services, and devices

Reduce Cost

- Consolidate vendor solutions
- Reduce time to resolve breaches and threats

Financial Impact/KPIs

- ↓ Risk of data breach
- ↓ Risk of Data Loss
- ↑ Understanding of user context and intent
- ↓ Time to identify, classify and label sensitive data
- ↓ Time to detect potential suspicious activity
- ↓ Cost of Data Breach
- ↓ Cost of Insider Threat
- ↓ Cost of Compliance and Data Protection Products

Purview Capabilities

- Information Protection
- Insider Risk Management
- Dynamic Data Loss Prevention
- ML-driven data classification
- Adaptive Protection
- Single Management Portal with Collaboration

Microsoft Purview *A5 Compliance Suite* Microsoft

Data Map and Data Catalog

Maximize the business value of data for your consumers by creating a unified map to automate and manage metadata from hybrid sources. Make data easily discoverable and understand the origin of your data with interactive data lineage visualization. ***Azure subscription required***

Compliance Manager

Reduce risk by translating complex regulatory requirements into specific improvement actions that help you raise your score and track progress ***(Baseline template + any 3 templates of your choice)***

Information protection

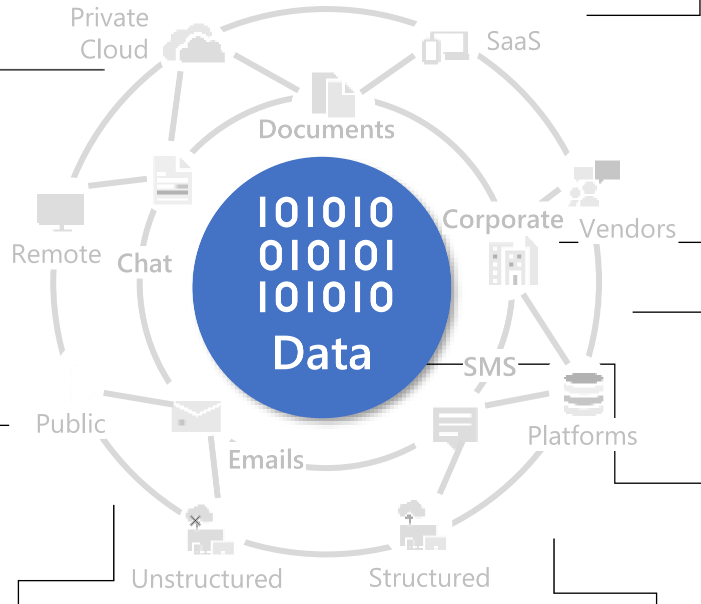
Discover, identify, classify, and protect sensitive data that is business critical, then manage and protect it across your environment. ***(Automatic Labeling, CASB Content Explorer, Activity Explorer, Trainable classifiers***)

Privacy management ***(Add-on feature)***

Generates actionable insights on enterprise personal data to help you spot issues and reduce risks and to respond to data subject requests for GDPR.

Data loss prevention

Automatically protect sensitive information from risky and unauthorized access across apps, services, endpoints, and on-premises files. ***(also covers Teams, Endpoints, file shares)***



Audit (Premium)

Records user and admin activity from your organization so you can search the audit log and investigate a comprehensive list of activities across all locations and services. ***(One year log retention, forensic investigation)***

Data Lifecycle Management

Classify and govern data at scale to meet your legal, business, privacy, and regulatory content obligations. ***(Automati retention labels, Adaptive scopes)***

eDiscovery (Premium)

Discover and manage your data in-place with end-to-end workflows for internal or legal investigations.

Records management

Uses intelligent classification to automate and simplify the retention schedule for regulatory, legal and business-critical records in your organization.

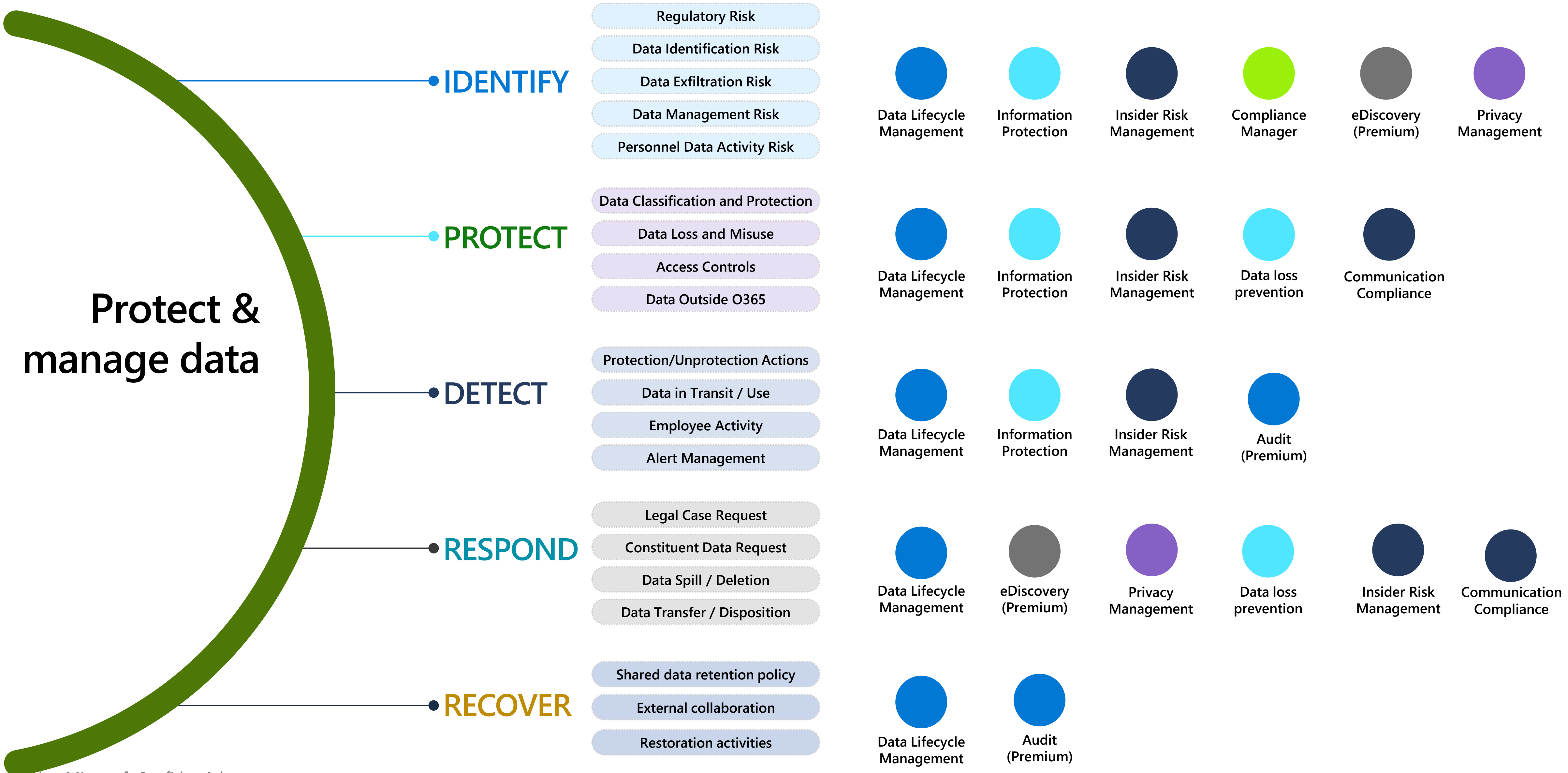
Communication compliance

Reduce risk by translating complex regulatory requirements into specific improvement actions that help you raise your score and track progress.

Insider risk management

Detect, investigate, and take action on critical risks in your organization, including data theft, data leaks, and security policy violations.

Map of Microsoft Purview capabilities to NIST Cybersecurity Framework



Protect & manage data

IDENTIFY

- Regulatory Risk
- Data Identification Risk
- Data Exfiltration Risk
- Data Management Risk
- Personnel Data Activity Risk

Data Lifecycle Management · Information Protection · Insider Risk Management · Compliance Manager · eDiscovery (Premium) · Privacy Management

PROTECT

- Data Classification and Protection
- Data Loss and Misuse
- Access Controls
- Data Outside O365

Data Lifecycle Management · Information Protection · Insider Risk Management · Data loss prevention · Communication Compliance

DETECT

- Protection/Unprotection Actions
- Data in Transit / Use
- Employee Activity
- Alert Management

Data Lifecycle Management · Information Protection · Insider Risk Management · Audit (Premium)

RESPOND

- Legal Case Request
- Constituent Data Request
- Data Spill / Deletion
- Data Transfer / Disposition

Data Lifecycle Management · eDiscovery (Premium) · Privacy Management · Data loss prevention · Insider Risk Management · Communication Compliance

RECOVER

- Shared data retention policy
- External collaboration
- Restoration activities

Data Lifecycle Management · Audit (Premium)

Classified as Microsoft Confidential

Summary of M365 A5 Components

PRODUCTIVITY

Office Pro Plus
Office apps on up to 5 PCs & Macs

Mobile Office Apps
Office Apps for Tablet & Smartphones

Windows 10 Enterprise – per user

My Analytics:
Individual and team effectiveness

COLLABORATION

Exchange :
Business-class email & Calendar

OneDrive:
Cloud Storage and file sharing

SharePoint:
Team sites & internal portals

Skype for Business:
Online Meetings, IM, video chat

Yammer:
Private social networking

Teams
Persistent chat-based collaboration

Audio Conferencing:
Worldwide dial-in for your online meetings

SECURITY

Anti Virus :
Signature based AV/AS

Data Loss Prevention
Prevent sensitive data leaks (Exchange, SharePoint, ODFB)

Basic eDiscovery
Discovery content across email, docs, IM.

Entra ID P1 (formerly AAD P1)
SSO, MFA, Conditional Access, Reporting

Intune
MDM, SCCM, Endpoint Protection

Azure Info Protection Premium P1
Encrypt and track all files

Adv Threat Analytics
Protection from advanced targeted attacks by applying user and entity behavior analytics

Secure Score
Assesses your current O365 security health

Compliance Manager
Data protection base line

A5 SECURITY

Defender for O365 (MDO)
Adv e-mail protection, sandboxing, URL re-writes, investigations, Automated IR

Defender for Identity (MDI)
End User Identity Behavioral Analysis – Look for abnormalities in your on-prem environment (domain controller, ADFS)

Defender for Endpoint (MDE)
Next generation protection including zero-day virus and malware protection, EPP, EDR, automated IR for Windows and MacOS, attack surface reduction, asset discovery and vulnerability management, auto investigation & remediation (AIR), built-in (agentless) for Windows 10/11

Defender for Cloud Apps (MDA)
Discover cloud-based apps, gain insight into shadow IT and assess risk.

Entra ID P2 (formerly AAD P2)
Risk based conditional access, Privileged Identity Management (PIM), identity protection, identity governance

A5 COMPLIANCE (Purview)

Information Protection & Governance:
DLP (adds Teams, end points, cloud and on-prem)
Information Protection
Data Lifecycle Management (formerly Information Governance)
Records Management
Rules-based auto classification
Machine Learning-based auto classification
Customer Key
Advanced Message Encryption

Insider Risk Management:
Insider Risk Management
Communication Compliance
Information Barriers
Customer Lockbox

eDiscovery & Audit
Audit Premium
eDiscovery Premium

Compliance Manager
3 Premium templates

Data Connectors

ANALYTICS

Power BI Pro:
Live business analytics and visualization

VOICE

Teams Phone:
Business phone system in the cloud

M365 A3

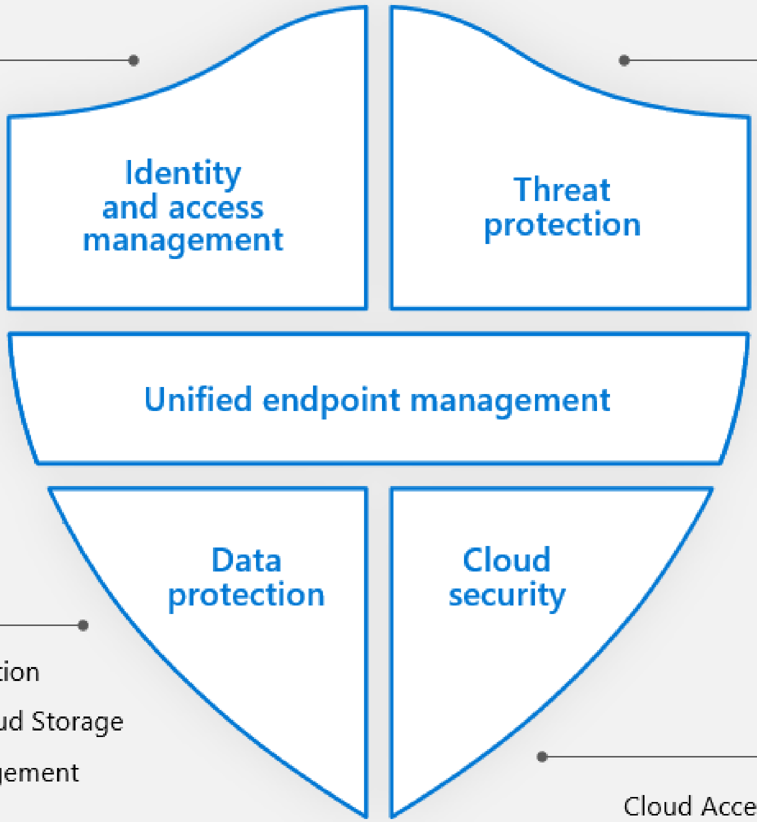
Microsoft 365 A5

Microsoft Confidential
Classified as Microsoft Confidential

Consolidate security

Streamline and strengthen

Replace up to 50 disparate products with integrated, end-to-end security.



Single Sign on + Self-Service Reset
Multifactor + Passwordless Authentication
Conditional Access
Privileged Access Management
Identity Governance
Active Directory

Mobile Application Management
Mobile Device Management

Data Discovery
Data Classification
Data Loss Prevention
Insider Risk Management
Database Security
Information and Messaging Encryption

Device Encryption
Encrypted Cloud Storage
Secrets Management

Endpoint Detection and Response
Endpoint Protection Platform
Forensic Tools
Intrusion Prevention System
Threat Vulnerability Management
Anti-phishing
User and Entity Behavior Analytics
Threat Intelligence Feeds
App and Browser Isolation
Attachment Sandboxing

Application Control
End-user Training
Network Firewall (URL Detonation)
Host Firewall
Secure Email Gateway
Security Assessment
SIEM
SOAR
Incident Response Services
DDoS Protection
IoT Protection

Cloud Access Security Broker
Cloud Workload Protection Platform
Cloud Security Posture Management