South Coast Summit

Security, Compliance & Identity Hack

South Coast Summit

Meet the team

Ally Turnbull

Sr. Technical Architect,
Microsoft Technology Center

Al Eardley

Sr. Technical Architect,
Microsoft Technology Center

Graham Hosking

Director, Advisory
Lighthouse Global

Leon Butler

Director, Advisory
Lighthouse Global

Luke Evans

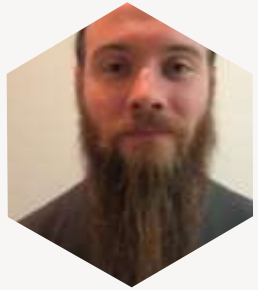
Solutions Architect,

codelooks

Jose Lazaro Pinos

Cloud Solution Architect

Global Partner Solution,
Microsoft



Ru Campbell MVP

Security Architect,
Threatscape

Housekeeping

South Coast Summit

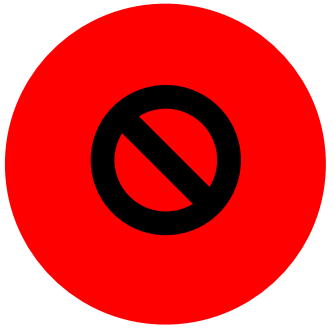
There will be breaks & speaker changes throughout

Keep the questions coming!

This session in NOT recorded

Feedback – aka.ms/TBC

Where possible we will share slides with you



All content is under your customer NDA

Agenda

South Coast Summit

08:00 – 09:00 - Registration

09:00 – 09:15 - Intros

09:15 – 10:15 - Overview / Ignite News

10:15 - Break 15 mins

11:30 – Hack Challenge Intro

12:00 - Lunch

13:15 – Get hacking - Breakout sessions as required

16:30 – Wrap Up

Intros – 2 mins

South Coast Summit

- Name
- Your current role
- Your Industry
- What skills you have around SCI Stack (Azure + M365) any exams such as MS-500, AZ-500, SC-200, SC-300, SC-400, SC-100 that you may have completed.

Microsoft on the Front Lines

Monitoring

140+[3]

Threat groups

40+[3]

Nation state-groups

Serving billions of global customers, learning and predicting what's next

43T[1]

Analyzing

Threat signals daily

32B[1]

Blocking

email threats annually

$20B[1]

in the next 5 years

Investing to improve and share knowledge, gain insights, and combat cybercrime

Keeping you secure, while saving you time and resources

60%

Up to **savings**, on average, over multi-vendor security solutions

15K[1]

partners in security ecosystem

785K[2]

customers rely on Microsoft for their multicloud, multiplatform infrastructure security

Trusted globally, protecting organizations' multi-Cloud and multi-platform infrastructures

1. Earnings Press Release, FY22 Q4. July 26, 2022, Microsoft Investor Relations
2. "Microsoft Digital Defense Report". October 2021, Microsoft Security
3. Earnings Press Release, FY22 Q2. December 16, 2021, Microsoft Investor Relations

Defend across attack chains

Insider and external threats

Microsoft

May 2021 – https://aka.ms/MCRA

Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Defender for Endpoint

Exploitation and Installation

Command and Control

Defender for Cloud

Azure AD Identity Protection

Brute force account or use stolen account credentials

Microsoft Cloud App Security

Attacker accesses sensitive data

Exfiltration of data

Defender for Identity

User account is compromised

Attacker collects reconnaissance & configuration data

Domain compromised

Attacker attempts lateral movement

Privileged account compromised

EXTERNAL THREATS

Microsoft Sentinel

INSIDER RISKS

Leading indicators

History of violations

Distracted and careless

Disgruntled or disenchanted

Subject to stressors

Insider risk management

Insider has access to sensitive data

Anomalous activity detected

Data leakage

Potential sabotage

Multi-Cloud and Cross-Platform Technology

Secure the enterprise you have

Microsoft

December 2021
https://aka.ms/MCRA

Microsoft Information Protection and Azure Purview

Discovery, Classify, Protect, and Monitor unstructured data (documents, spreadsheets, files, etc.), structured data (SQL, Databases, etc.) and identify critical risks (Open S3 buckets, SaaS Sharing Risks, etc.)

Identity & Access

Information Protection

Identity Enablement

Access cloud and legacy applications for Enterprise users, Partners (B2B), and Customers/Citizens (B2C)

Azure Active Directory

Identity Security

Zero Trust Access Control using Behavioral Analytics, Threat Intelligence, and integration of device and app trust signals

GitHub Advanced Security – Secure development capabilities

Securing components common most enterprise software supply chains

Endpoints & Devices

Intune
Unified Endpoint Management (UEM)

Software as a Service (SaaS)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

On-Premises IaaS PaaS

Continuous Cross-Platform Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWPP)

IoT Devices

Operational Technology (OT)

Security Operations [Center] (SOC)

Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Microsoft 365 Defender

Microsoft Defender for Endpoint
Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Data Loss Protection (DLP)
- Web Content Filtering
- Threat & Vuln Management

Microsoft Defender for Cloud Apps

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

Microsoft Defender - *Extended Detection and Response (XDR)*

Threat visibility and capabilities tailored to resources

- *Threat & Vulnerability Management*
- *Integrated data classification*
- *Threat analytics on top attacks*
- *Advanced Detection & Remediation*
- *Automated Investigation & Remediation*
- *Advanced Threat Hunting*

Microsoft Defender for Cloud

XDR for IaaS, PaaS, and On-Premises

- VMs, Servers, App Environments
- Storage and Databases
- Containers and Orchestration
- and more

Microsoft Defender for IoT

- ICS, SCADA, OT
- Internet of Things (IoT)
- Industrial IoT (IIoT)
- Asset & Vulnerability management
- Threat Detection & Response

Azure Arc

Threat Intelligence – 8+ Trillion signals per day of security context

South Coast Summit

Microsoft Ignite Identity / Endpoint Updates

Microsoft Entra Identity Governance	Workload Identities	Certificate-based Authentication (CBA)	Conditional Access	Endpoint Management Rename
Joiner, Mover, Leaver Templates	• Conditional Access • Identity Protection • Access Reviews	• Remove ADFS - **authenticate with a X.509 certificate** directly against Azure AD and eliminate ADFS	• Auth Strength Methods based on resource • Phishing-resistant MFA is needed.	Back to Intune ☺

South Coast Summit

Microsoft Ignite XDR / Endpoint Updates

Defender for DevOps	Microsoft Defender Cloud Security Posture Management (CSPM)	Zeek / Network protection integration	Microsoft Tunnel for MAM / Multi Tenant MAM	Endpoint Privilege Management
A new solution that will provide visibility across multiple DevOps environments to centrally manage DevOps security, strengthen cloud resource configurations in code and help prioritize remediation of critical issues in code across multi-pipeline and multicloud environments. With this preview, leading platforms like GitHub and Azure DevOps are supported and other major DevOps platforms will be supported shortly.	This solution, available in preview, will build on existing capabilities to deliver integrated insights across cloud resources including DevOps, runtime infrastructure, and external attack surfaces, and will provide contextual risk-based information to security teams. Defender CSPM provides proactive attack path analysis, built on the new cloud security graph, to help identify the most exploitable resources across connected workloads to help reduce recommendation noise by up to 99%.	MDE will integrate with Corelight Zeek for enhanced network inspection. Zeek essentially mirrors network traffic into processed data based on protocols. These logs allow you to improve C2 detection and response, and meaningful craft detections.	Coming Jan '23 – you no longer need to enroll the full device in MDM to benefit from Tunnel-enabled apps. MAM policies will also start to support multi-tenant.	Remove the risk of standing access to admin permissions with the dynamic evaluation of standard users to admin rights.

South Coast Summit

Microsoft Ignite Compliance Updates

Data Loss Prevention	Information Protection	Records Management	Compliance Manager	eDiscovery
▪ Loop support (CY Q4). ▪ Support for Authorized Printer, USB, File Paths, and sanctioned sites in Endpoint DLP. ▪ Improved responsiveness for Teams DLP.	▪ Label support with Loop (CY Q4). ▪ New "Credential" Sensitive Information Types. ▪ New "Business" Trainable Classifiers. ▪ Co-authoring of encrypted documents. ▪ Adobe Acrobat native support. ▪ AIP Scanner administration improvements.	▪ Files tab support for retention labels. ▪ Retention of shared versions. ▪ Enhanced automation through Power Automate. ▪ Microsoft Graph API support for managing labels and events.	▪ Assessment Data Residency. ▪ Updated templates across 350+ regulations. ▪ Improvements to supported controls for continuous assessments. ▪ Recommendation Engine.	▪ Document version at time of sharing (Preview). ▪ Reactions in Teams messages. ▪ eDiscovery Graph API now GA.

https://news.microsoft.com/ignite-2022-book-of-news/

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/bg-p/MicrosoftSecurityandCompliance

Identity and access management

Secure access for a connected world

- Unified identity management
- Seamless user experiences
- Secure adaptive access
- Simplified identity governance

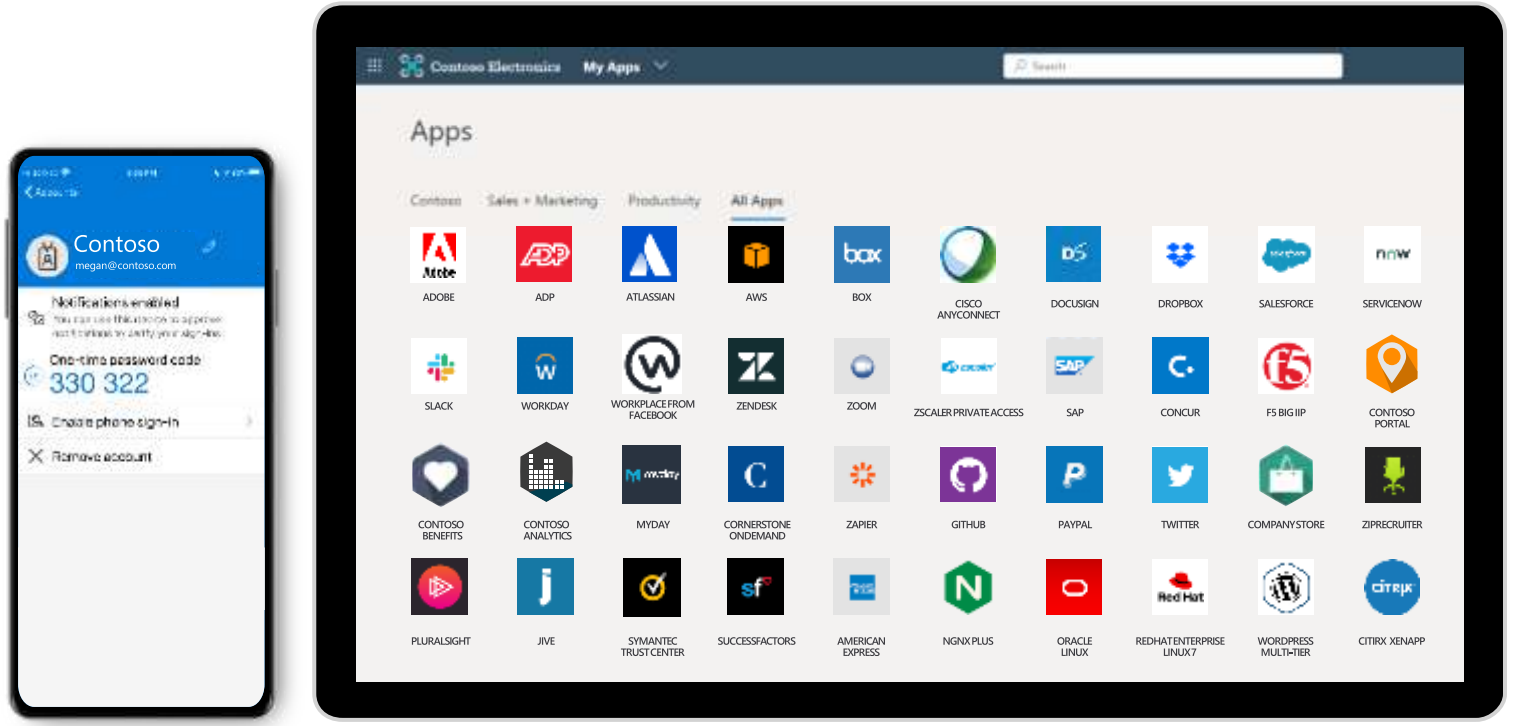
Unified identity management

Manage all your identities and access to all your applications across your hybrid environment

Seamless user experiences

Provide an easy, fast sign-in experience to keep you and your users productive

- Passwordless authentication
- Single sign-on (SSO) for any user type
- User self-service management
- Application portal



Microsoft Zero Trust Principles

Guidance for technical architecture

Verify explicitly

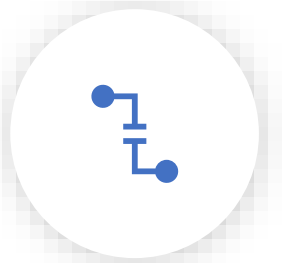
Always validate all available data points including

- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors



Assume breach

Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

Secure adaptive access

Advance your Zero Trust strategy with strong authentication and risk-based access policies

Strong authentication

Secure access to resources with a broad range of flexible multi-factor authentication and passwordless methods

Real-time adaptive policies

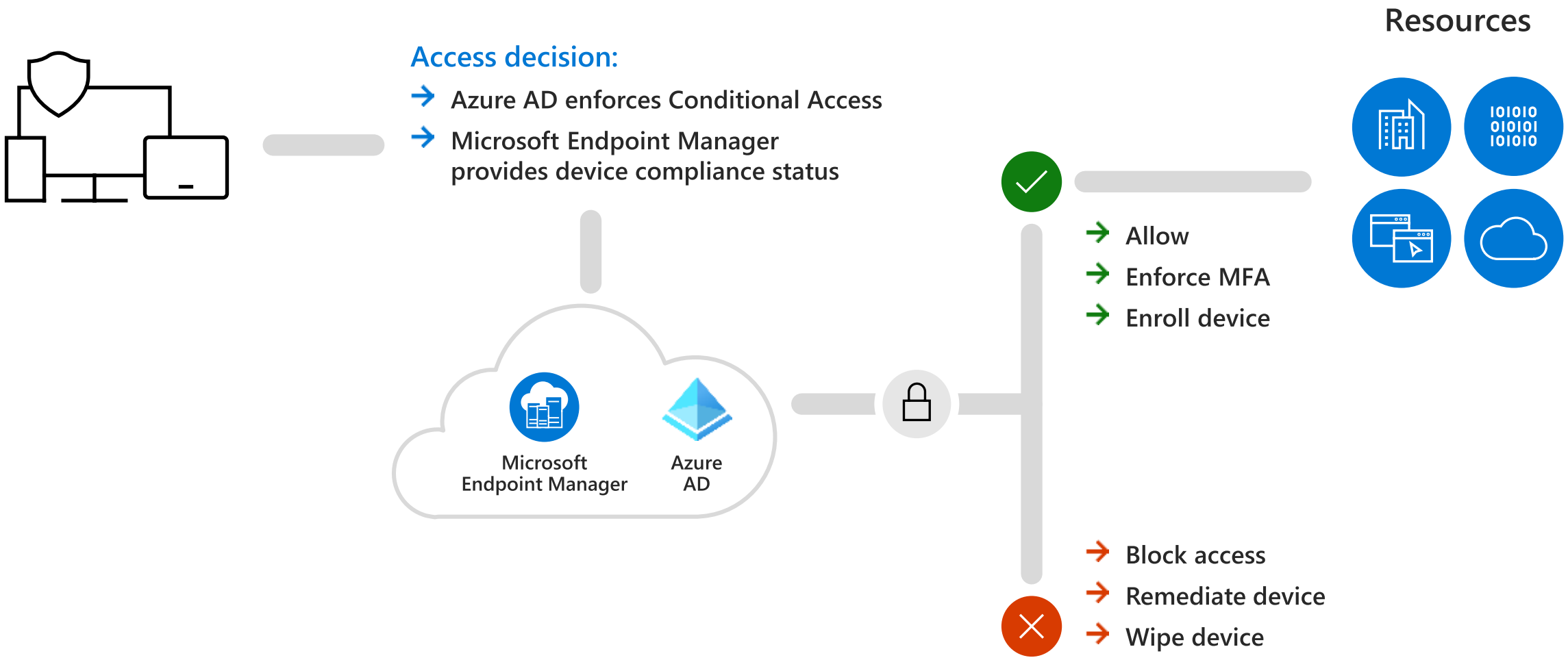
Use configurable Conditional Access policies based on context and risk assessment

Risk detection and remediation

Intelligently detect and respond to compromised accounts using cloud-based AI

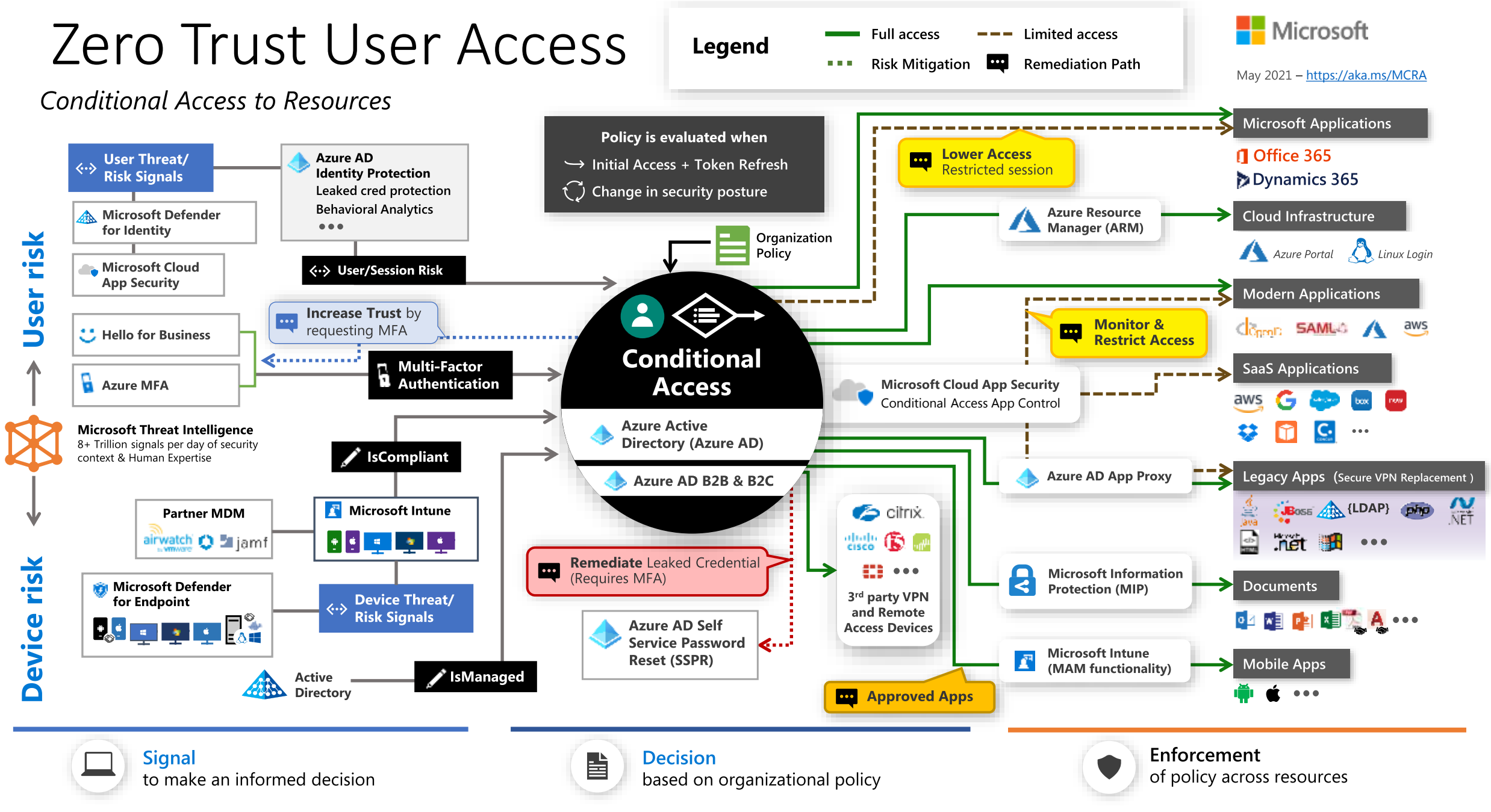
Protect against endpoint compromise

Secure access to apps and data on your devices with Conditional Access



Zero Trust User Access

Conditional Access to Resources



Simplified identity governance

Efficiently automate identity governance to control access to apps and data for all users and admins

Identity lifecycle

Enable HR-driven user provisioning and automate lifecycle management

Privileged access

Mitigate risk of privileged access using time-limited access, and role-based access control

Audit report

Ensure to meet compliance obligations with audit reporting capabilities

Zero Trust Rapid Modernization Plan (RaMP)

Prioritize rapid progress on highest positive impact

Slide – aka.ms/MCRA
Docs – aka.ms/ZTRAMP

Prioritize Privileged Access
- High impact and likelihood attacks
- IT Admins provide technical feedback

Top Priorities – *critical security modernization steps*

Secure Identities and Access

1. **Explicitly validate trust for all access requests (via Azure AD Conditional Access)**
   a. **User Accounts -** Require Passwordless or MFA for all users + measure risk with threat intelligence & behavior analytics
   b. **Endpoints -** Require device integrity for access (configuration compliance first, then XDR signals)
   c. **Apps -** Enable Azure AD for all SaaS, for VPN authentication, and for legacy apps (on-premises + IaaS) via App Proxy
   d. **Network -** Establish basic traffic filtering and segmentation to isolate business-critical or highly vulnerable resources

Data, Compliance & Governance

Align to business and mission

2. **Ransomware Recovery Readiness -** Ensure backups are validated, secure, and immutable to enable rapid recovery
3. **Data -** Discover and protect sensitive data (via Microsoft Info Protection, Defender for Cloud Apps, CA App Control)

Modern Security Operations

4. **Streamline response** to common attacks with XDR for Endpoint/Email/Identity + Cloud (via M365 & Defender for Cloud)
5. **Unify Visibility** with modern Security Information and Event Management (SIEM via Microsoft Sentinel)
6. **Reduce manual effort -** using automated investigation/remediation (SOAR), enforcing alert quality, and threat hunting

As Needed – *typically driven by cloud adoption or OT/IoT usage*

Infrastructure & Development

Datacenter & DevOps Security

Security Hygiene – Rigorously monitor security posture and remediate configurations, security updates, privilege creep, etc.

Reduce Legacy Risk – Retire or isolate legacy technology (Unsupported OS/Applications, legacy protocols)

DevOps Integration – Integrate infrastructure + development security practices into DevOps with minimal friction

Microsegmentation – Additional *identity and network* restrictions (dynamic trust-based and/or static rules)

Operational Technology (OT) and Industrial IoT

Discover – Find & classify assets with business critical, life safety, and operational/physical impact (via Defender for IoT)

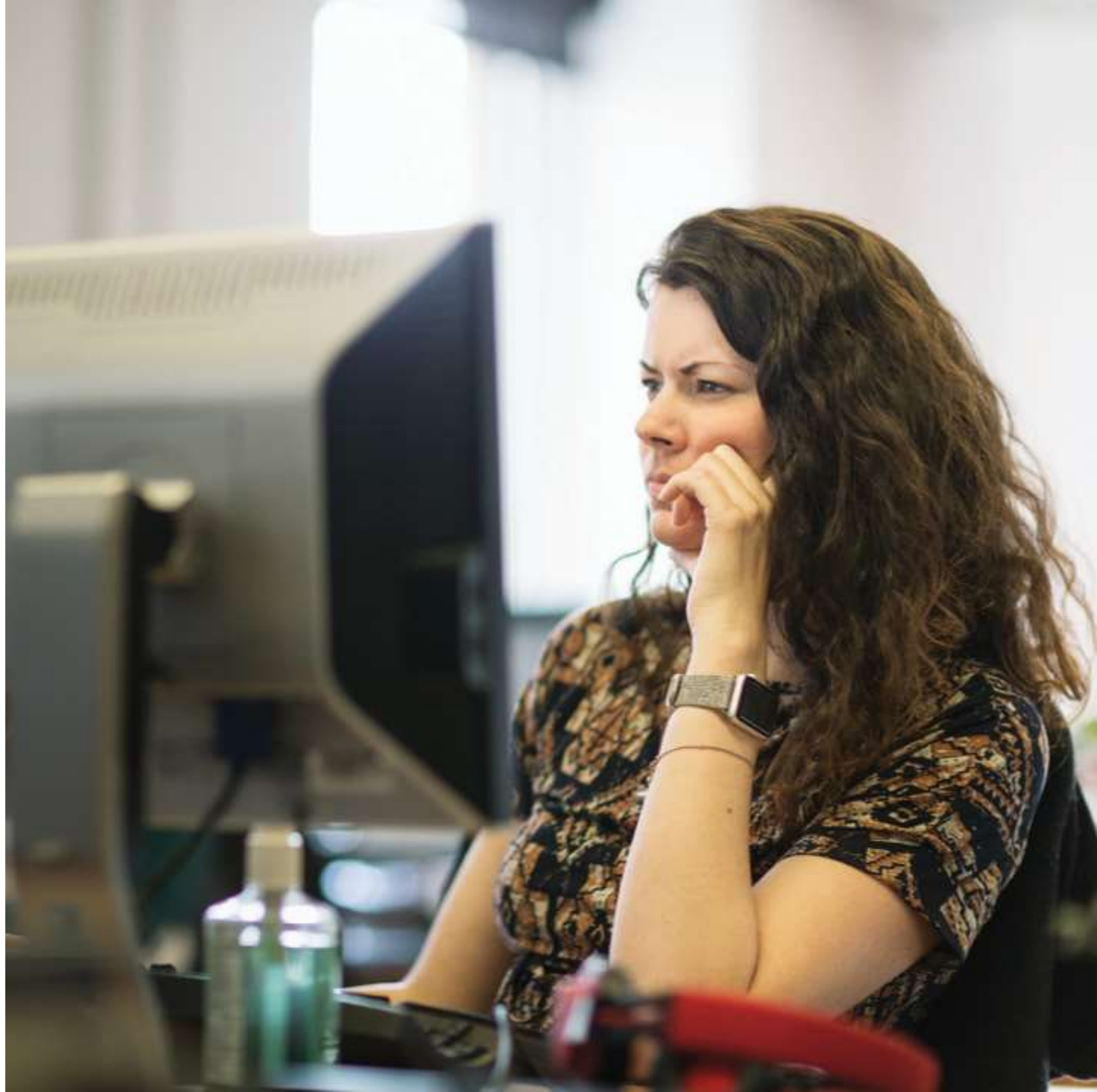
Protect – isolate assets from unneeded internet/production access with static and dynamic controls

Monitor – unify threat detection and response processes for OT, IT, and IoT assets (via Microsoft Defender for IoT)

Know your data

Gain visibility across your data estate

- What kinds of sensitive data do I have in my organisation?
- Where does this sensitive data live?
- How is this data being accessed and shared?



Today's focus

Compliance beyond Microsoft 365

Information Protection & Governance

Safeguard sensitive data across clouds, apps and endpoints

Data Loss Prevention | Information Protection and Encryption | Information Governance | Records Management | Azure Purview

Risk Management

Identify and remediate critical risks within your organization

Insider Risk Management | Communication Compliance | Advanced eDiscovery | Advanced Audit | Information Barriers | Privileged Access Management | Customer Lockbox

Compliance Management

Assess compliance and respond to regulatory requirements

Compliance Manager

Privacy Management

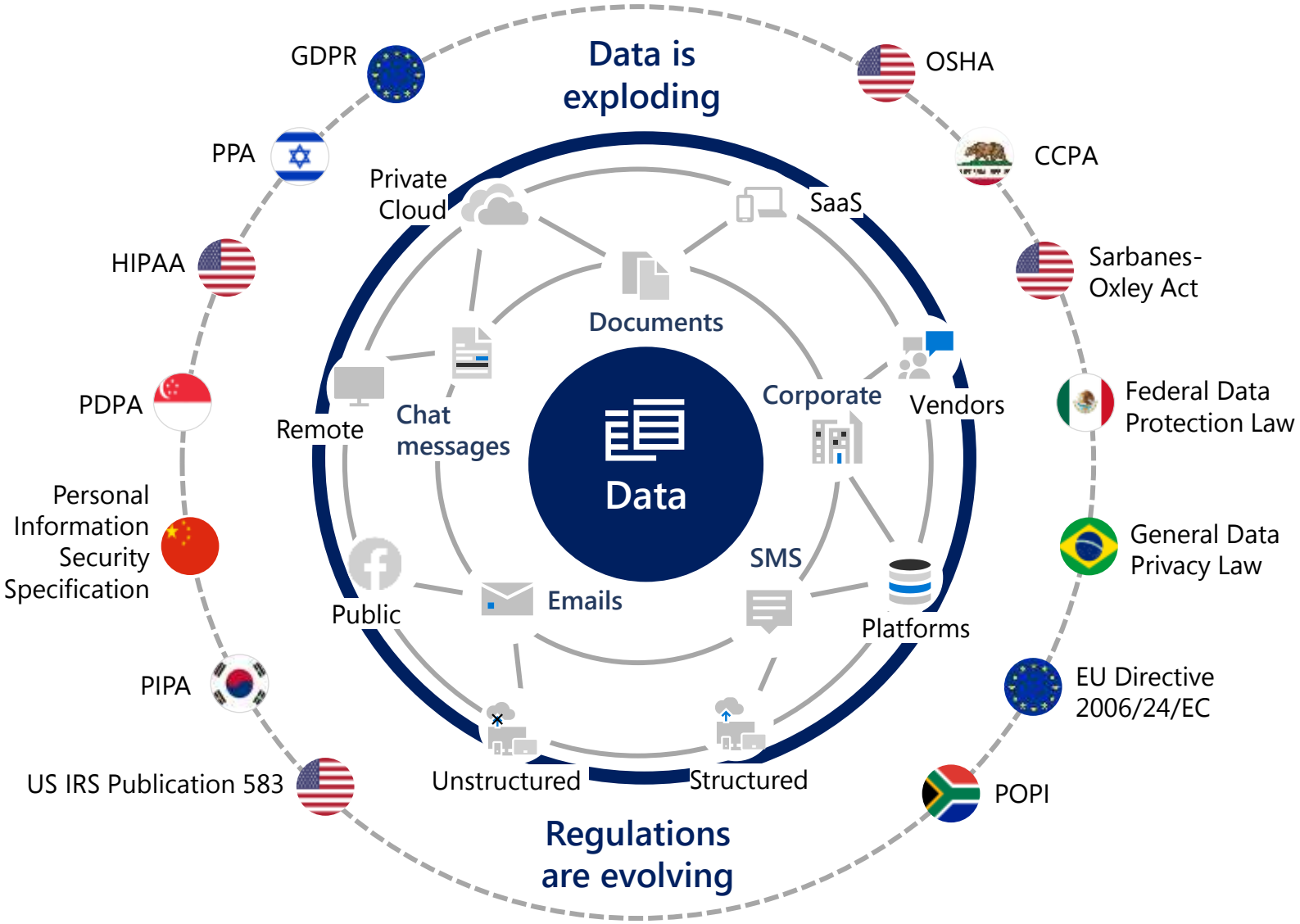
Safeguard personal data and build a privacy resilient workplace

Manage risk scenarios | Manage subject rights requests

Extending beyond Microsoft 365

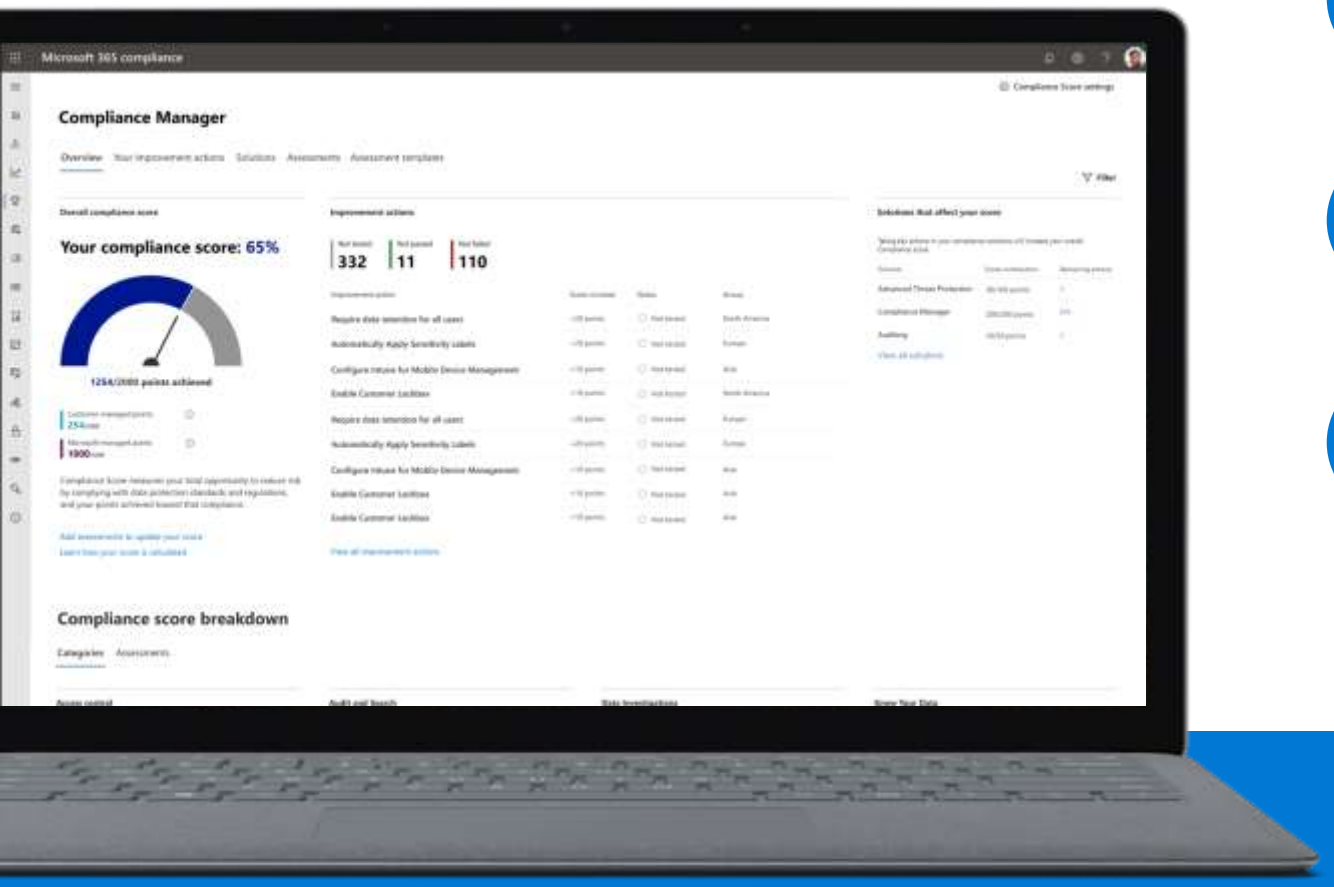
Connectors | Graph APIs | MIP SDK | OMA-Audit APIs | Power Automate

Privacy and regulatory requirements are increasing



Microsoft Purview Compliance Manager

Simplify compliance and reduce risk



Intuitive management

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

Scalable assessments

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

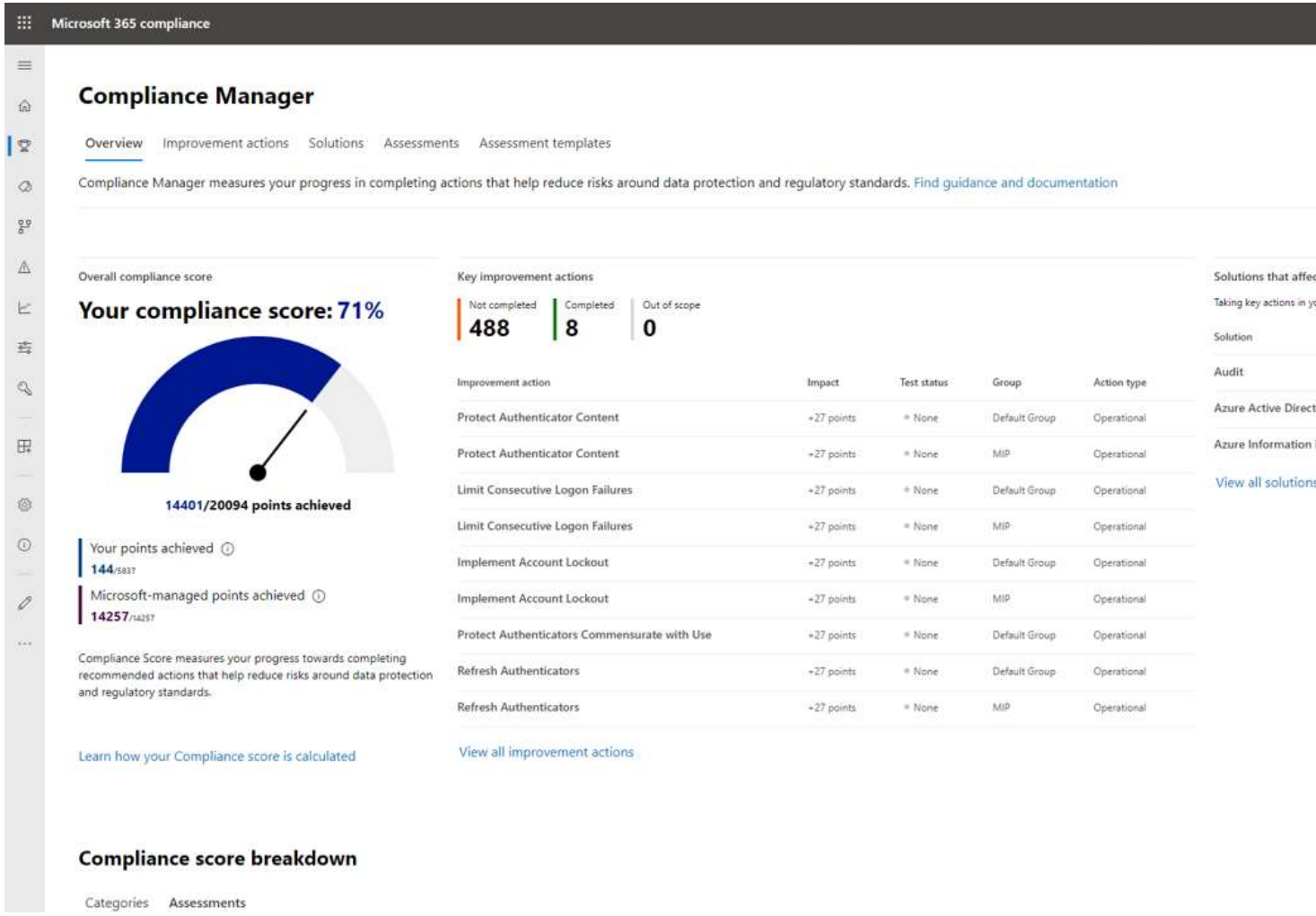
Built-in capabilities

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

Compliance score

Compliance score is a capability within Compliance Manager and:

- Provides a quantifiable measure of compliance
- Helps prioritize compliance actions with the most impact to the organization compliance posture
- Automatic test status and test date updates



Universal assessments

Universal assessments are available alongside premium assessments and:

- Help map regulatory assessment templates to any non-Microsoft 365 products or services
- One place to assess, manage, and track multi-cloud compliance
- Available alongside premium assessments at no additional cost

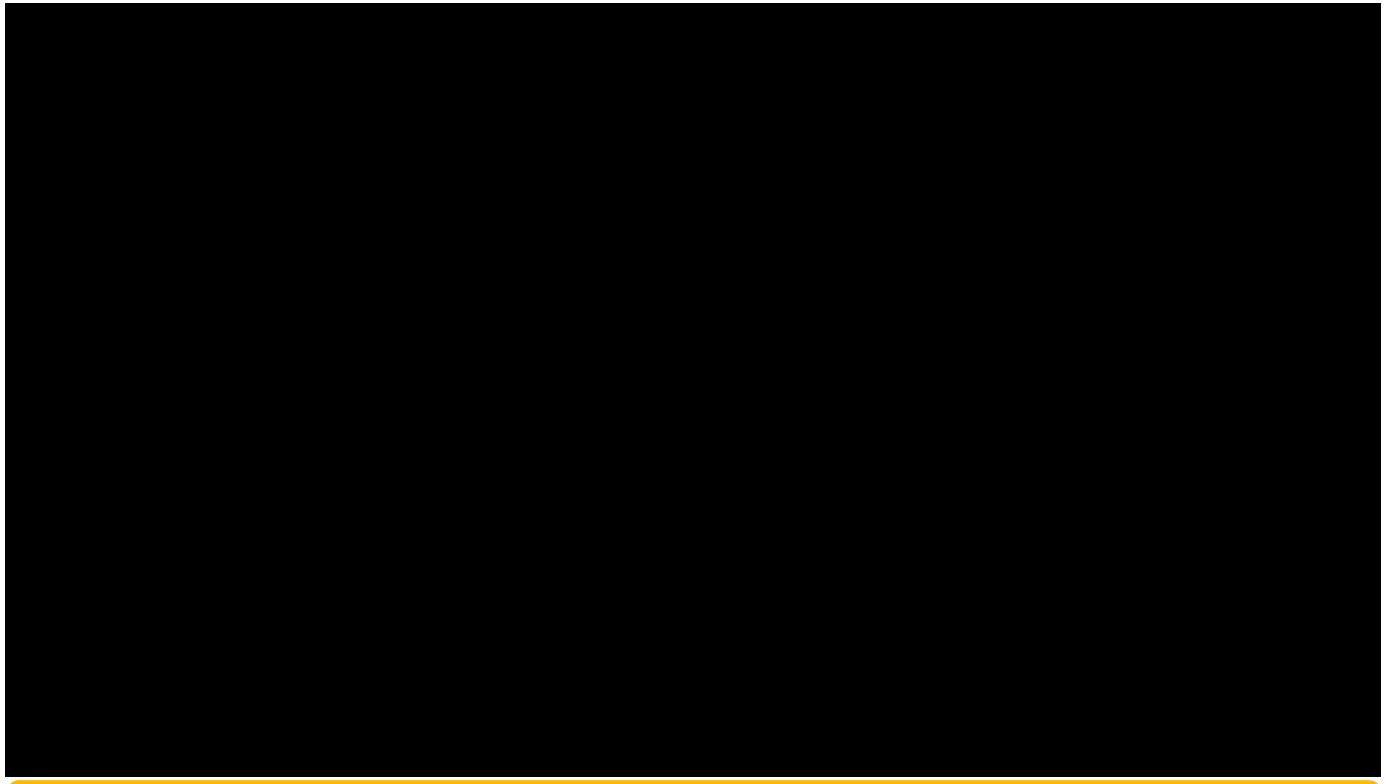
Example: CCPA template with Product Scope 'Universal'
Can map CCPA template to any product or service and access CCPA compliance across multi-cloud deployments

Over 320+ universal assessments are available alongside premium assessments within Compliance Manager

Custom assessments

Custom assessments are premium value in Compliance Manager and provide:

- Ability to customize an existing template
- Ability to create a template from scratch
- Ability to add custom controls, custom control families, and custom action.

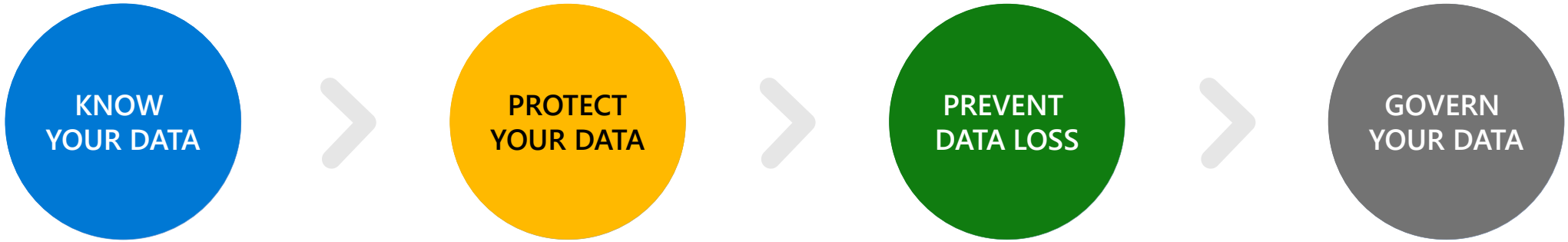


Example: Extend the Microsoft ISO template to add custom actions and control families

Custom assessments are available to customers with E5 subscription

Information protection & governance

Protect and govern data wherever it lives



Understand your data landscape and identify important data across your hybrid environment

Classify data with sensitivity labels, apply flexible protection, encryption, access restrictions and visual markings

Prevent unauthorized or accidental sharing, transfer, or use of sensitive data with policies

Automatically retain, delete, and store data and records in a compliant manner

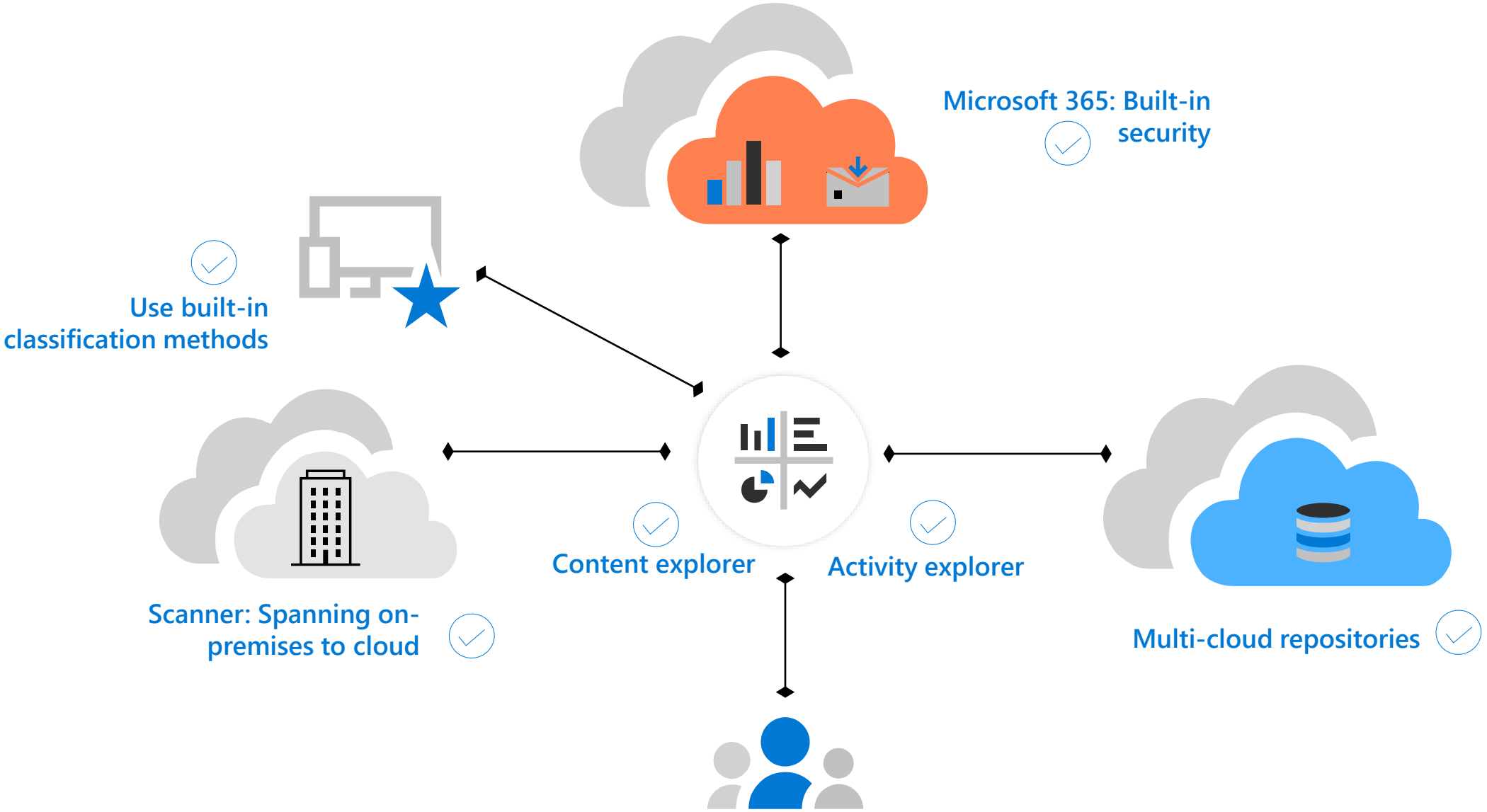
POWERED BY AN INTELLIGENT PLATFORM

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

Devices | Apps | Cloud services | On-premises | ISV/3rd party

Flexible options to know your data

Understand what's sensitive, what's business-critical & across your environment



Encryption in Microsoft 365 for added protection and control

Data in-transit

Network

Transport Layer Security (TLS)

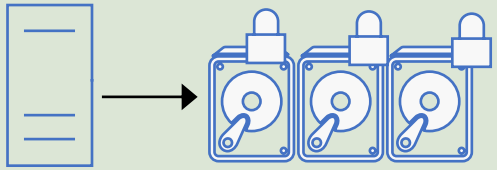
Content

Emails,
Documents

Office 365 Message Encryption
Office 365 Advanced Message Encryption

Data at-rest

Hardware

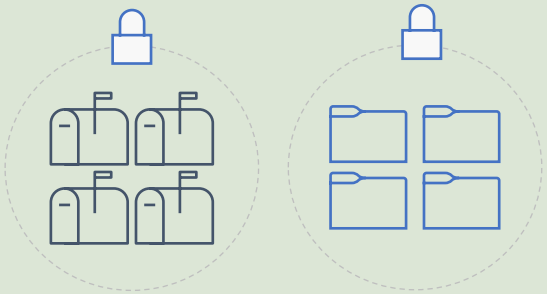


Windows Server

Disk

BitLocker

Application



Exchange Online Mailboxes

SharePoint and OneDrive Files

Service Encryption

Encryption key management options in Microsoft 365

Data in-transit

Network

Content

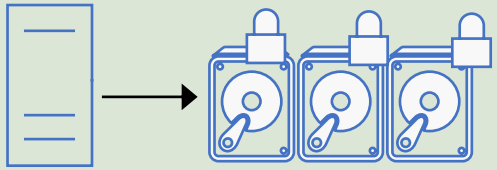
Emails,
Documents

Bring Your Own Key (BYOK)

Hold Your Own Key (HYOK)
Double Key Encryption

Data at-rest

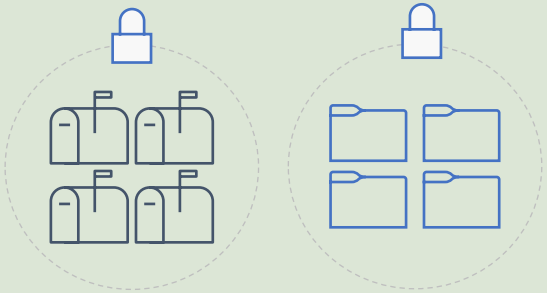
Hardware



Windows Server

Disk

Application



Exchange Online Mailboxes

SharePoint and OneDrive Files

Customer Key
Microsoft Managed Key

Microsoft Purview Information Protection

Windows
MacOS
iOS
Android

Office 365

Endpoint DLP

Cloud Upload
App Control
USB Drive
Network
Print
Clipboard
Bluetooth
RDP

Data Classification Service

Sensitive Information Types

Out of the Box
CCN/SSN/License
Double Key Encryption
Named entity
10 templates (Finance, IP, Legal, Healthcare...)

Custom
RegEx
Dictionary
Fingerprint
Exact Data Match (EDM)

Trainable Classifiers
Sample Content
Test
Validate
Publish

Sensitivity Labels

Public
General
Confidential
...

Extendable via SDK to 3rd party tools

Defender for Cloud Apps

On-premises

Microsoft Purview data governance services

ADLS
SQL DB
Azure Files
Blobs
Cosmos DB
S3

Advanced compliance solutions

eDiscovery (Premium)
Insider Risk Management
Communication Compliance
Microsoft Priva

Example Classification Labels

Sensitive

- Insider information
- Selected (strategic) projects
- Trade secrets or IP
- Consolidated financial information
- Passwords/Encryption keys
- Sensitive personal information

- This concerns sensitive information which should only be made available to the immediately authorised recipient.
- Breach of this classification can cause very extensive damage.

Confidential

- Personally identifiable information
- Salary or performance review
- Business information including contracts (inc. templates and negotiation details)
- Strategic information
- Unpublished financial figures

- Information which is only accessible to a limited group of users. Information is made available based on trust
- Breach of this classification can cause serious direct or indirect damage.

Internal

- Internal messages
- Organisational setups
- Steering documents
- Internal policies/procedures
- Internal newsletters

- Information which may or must be accessible to the organisation
- Confidentiality is low
- Violation of this classification can cause some direct or indirect damage

Public

- Publish media and social media content
- Published internet content
- Sales/marketing brochures
- Non-confidential external materials

- All information is generally accessible to everyone and shared externally by the organisation
- Breach of this classification is not possible

Sensitivity Labels

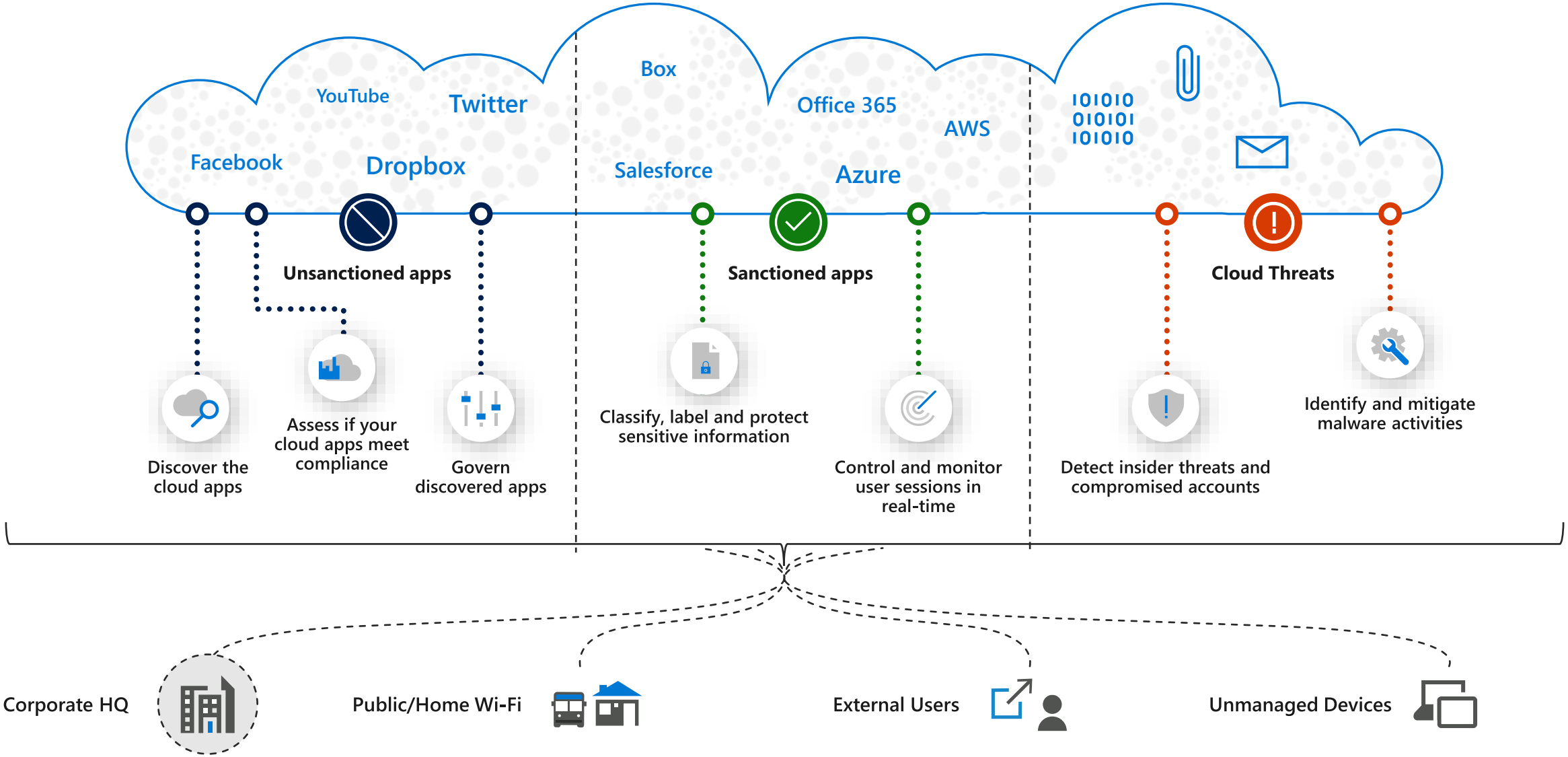
Labels that follow the data

Scope	Data labels	Controls	Policy
File Email	Public General Confidential • Recipients only • Internal only Sensitive • Recipients only • Internal only	Content Marking Encryption	Targeting users/groups Label required Downgrade justification Default label Auto labelling (SITs)

Licensing

Scope	Container labels	Conditional access	Controls
Teams SharePoint M365 group	Internal	Managed Device	Full app access eDLP
	External (x-tenant)	Managed Device	Full app or web access MDCA
	External	Unmanaged Device	Web access only MDCA

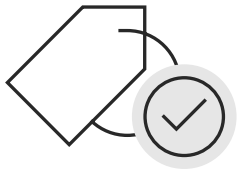
TOP CASB USE CASES



MICROSOFT INFORMATION PROTECTION SOLUTIONS

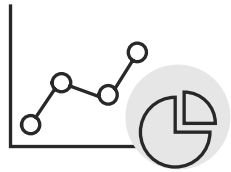
Comprehensive protection of sensitive data throughout its lifecycle—across devices, apps, cloud services, and on-premises

Discover



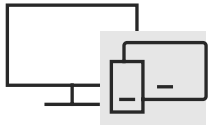
Classify

Protect



Monitor

Across



Devices

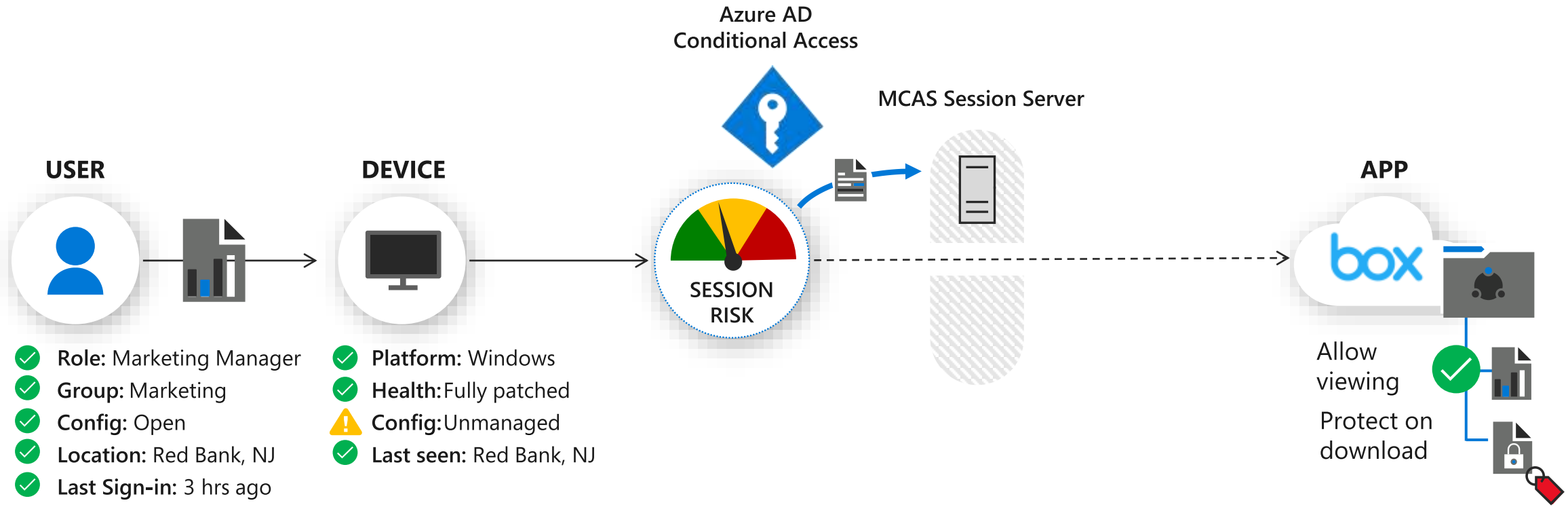
Apps

Cloud services

On-premises

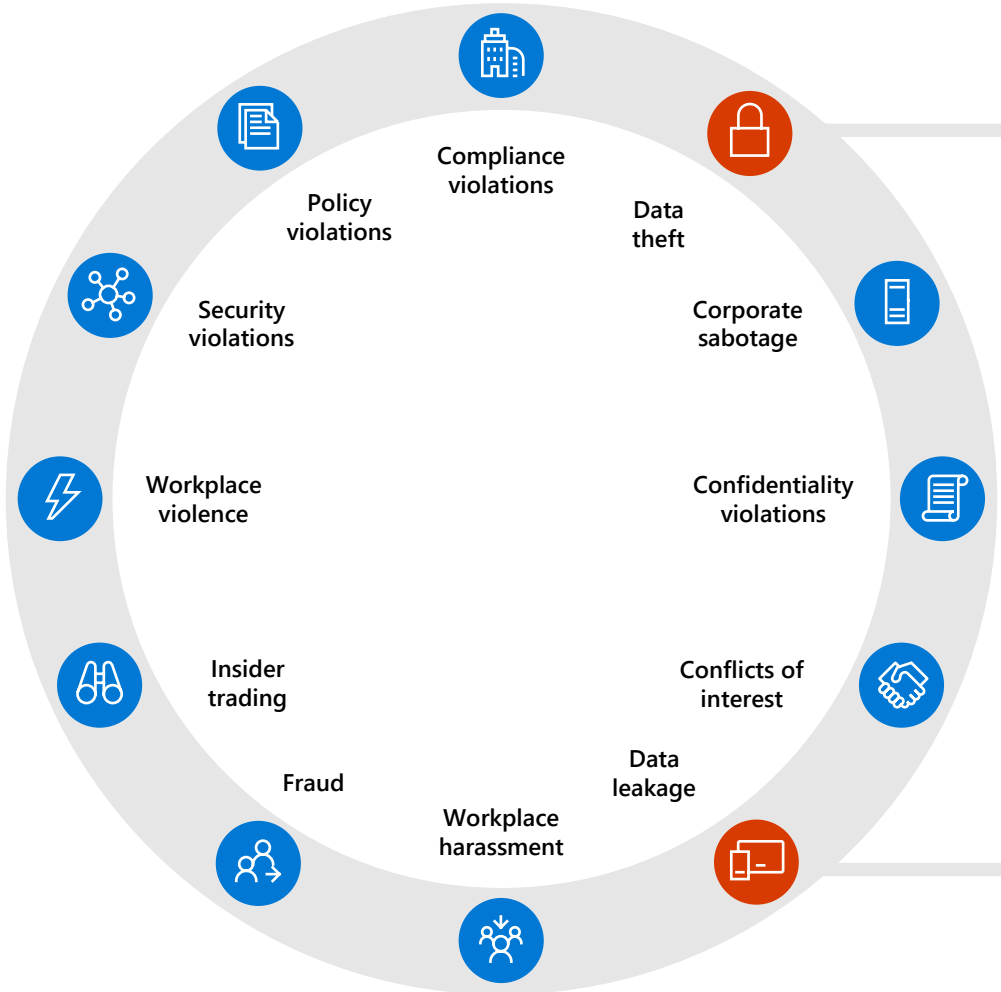
USE CASE: PREVENT DOWNLOAD OF FILES

Risk based in-session controls



Device is unmanaged

Organizations face a broad range of risks from insiders

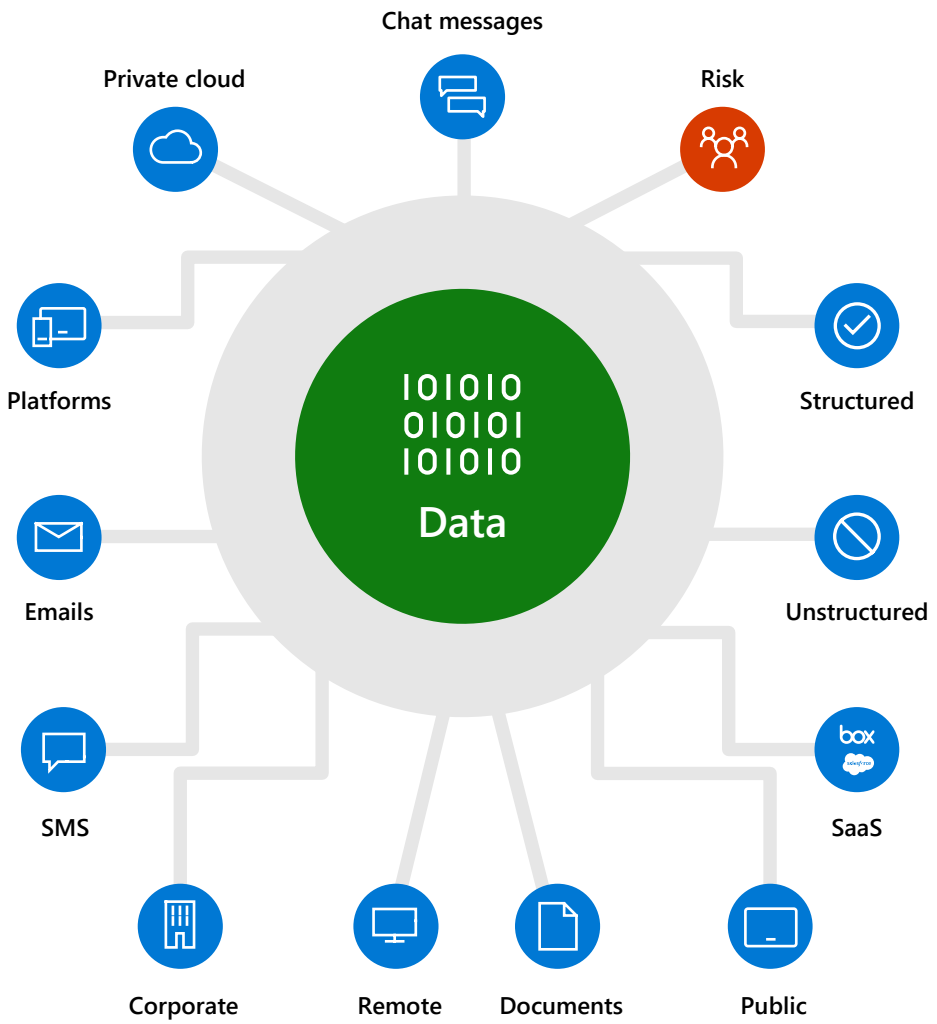


Certain risks are more prevalent, with significant negative impacts.

Data theft by departing employees

Data leakage, both malicious and inadvertent

Fragmented approach to identifying and managing risks



Risks are difficult to identity and manage

Traditional approaches have limitations

- Configurations requiring scripting
- Deployment of endpoint agents
- Scale and performance issues
- Low visibility into content
- Low sentiment analysis
- Limited signal correlation

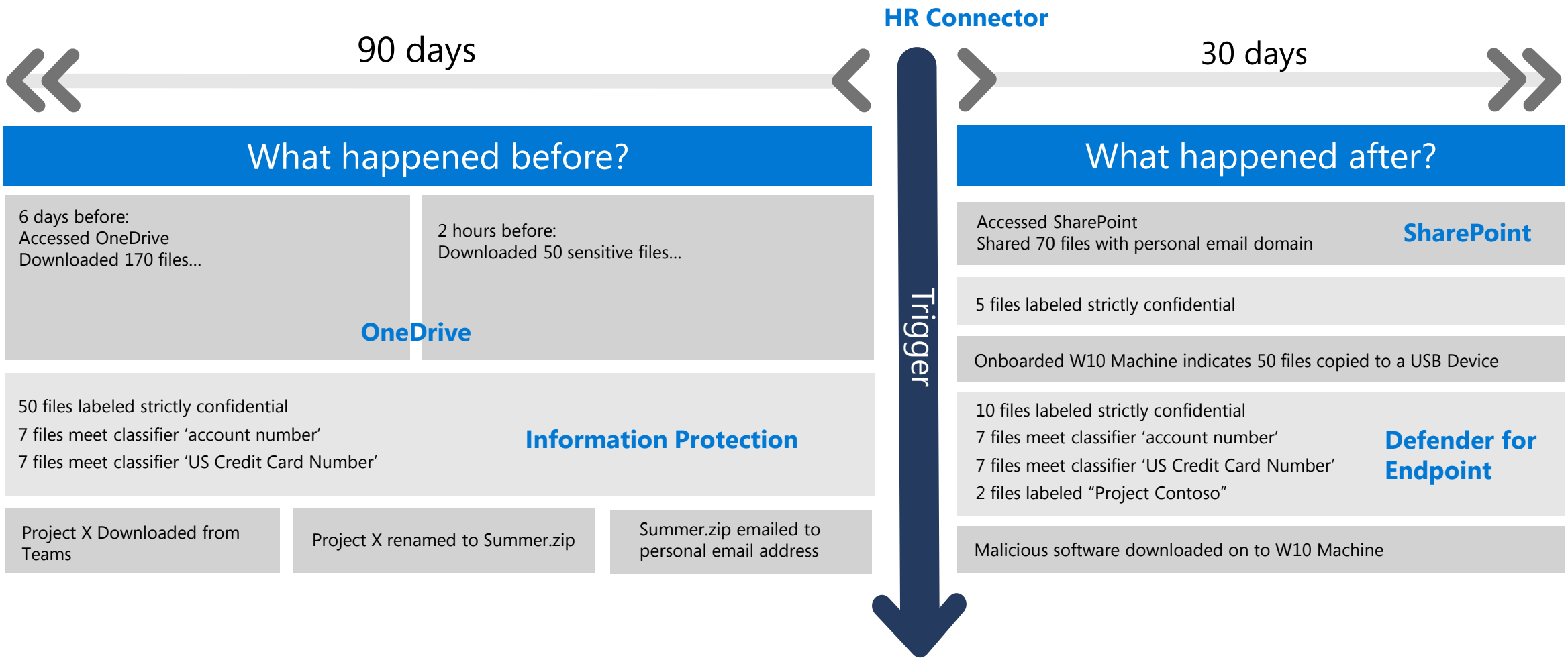
UEBA
(User and entity behavior analytics)

UAM
(User activity monitoring)

DLP
(Data loss prevention)

Scenario: how Insider Risk Management works with E5

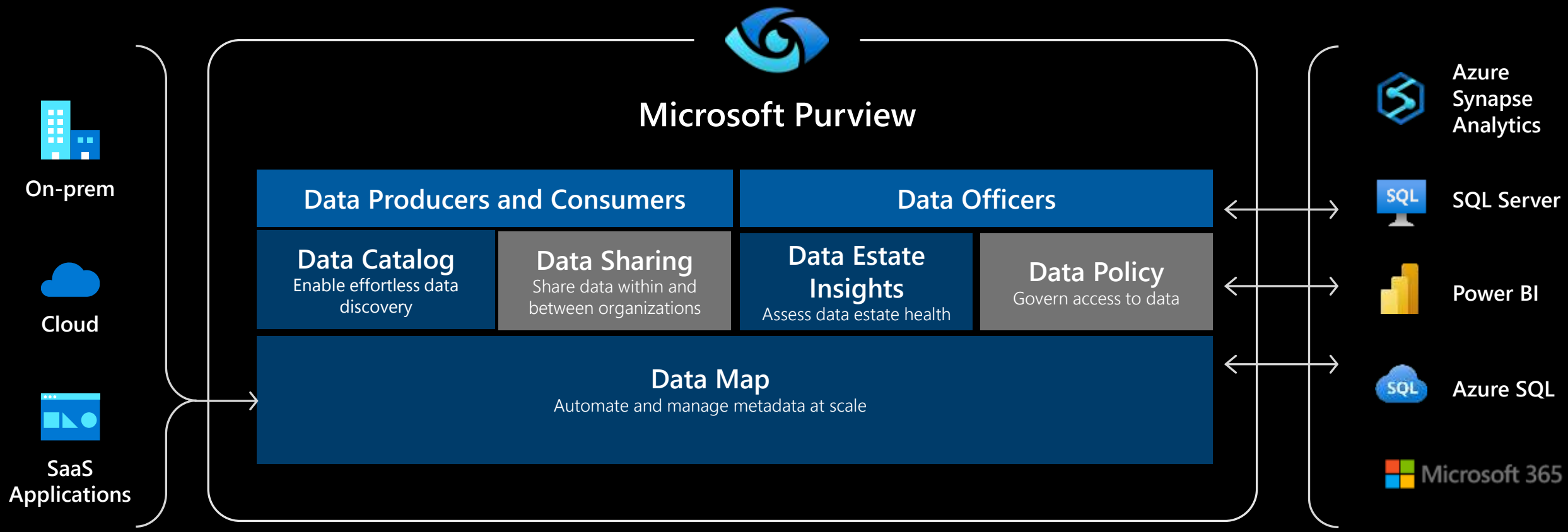
An employee enters resignation date in HR tool…



Unified Data Governance with Microsoft Purview

Generally Available

Preview



Microsoft

Break

Please return at 10:40am

Wi-Fi

Hilton Honours: Hilton19

Microsoft Defender for Identity

Discovery

Account enumeration

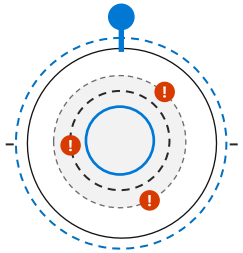
Security principal enumeration (LDAP)

Users group membership enumeration

Users & IP address enumeration

Hosts & server name enumeration (DNS)

Resource access suspicious activities



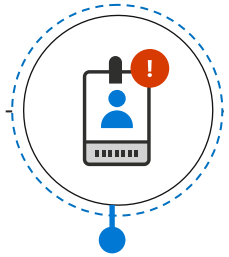
Credential access

Brute force attempts

Suspicious VPN connection

Honey Token account suspicious activities

Logon/Failed logon suspicious activities



Lateral movement

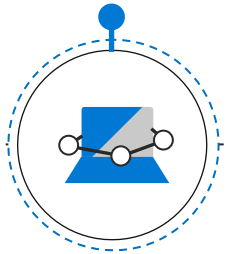
NTLM Relay & NTLM tampering

Pass-the-Ticket

Pass-the-Hash

Overpass-the-Hash

Suspicious groups membership changes



Persistence

Golden ticket attack

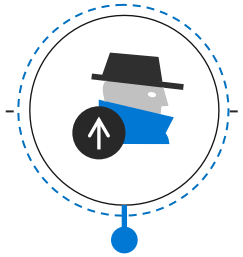
DCShadow, DCSync

Data exfiltration

Code execution/Service creation on DC

SMB packet manipulation

Skeleton Key



Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a CASB at empowers you to manage shadow IT, first and third-party clouds, and protect against cyber threats + anomalies

Discover

Cloud app catalogue
Cloud discovery

Alerts

Access
Activities
Discovery

Files
Sessions
OAuth

Investigate

Activity log
Files
Identities
Security configuration

Control

Access
Activities
Discovery

Files
Sessions
OAuth

Microsoft

Microsoft Sentinel

Cloud Native SIEM + SOAR

Security: Microsoft Sentinel

Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

Rising infrastructure costs and upfront investment

Too many disconnected products

Lack of automation

Security skills in short supply

Cloud Native SIEM + SOAR

MICROSOFT SENTINEL

Core capabilities

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security solutions

Analyze & detect threats

Machine learning, UEBA

Investigate & hunt suspicious activities

Interactive Attack Visualization, Azure Notebooks

Automate & orchestrate response

Playbooks

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (log analytics)

Integrate

ServiceNow

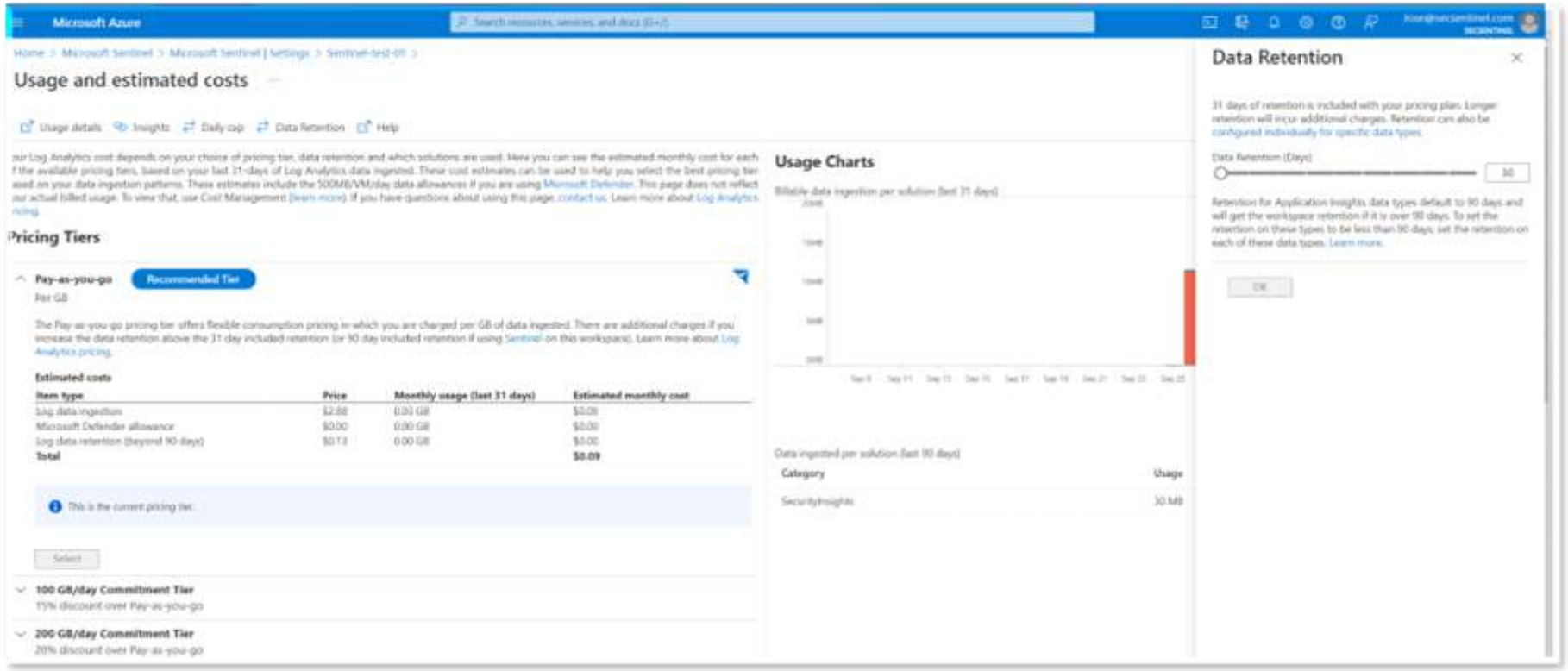
Other tools

Community

Log Analytics Workspace

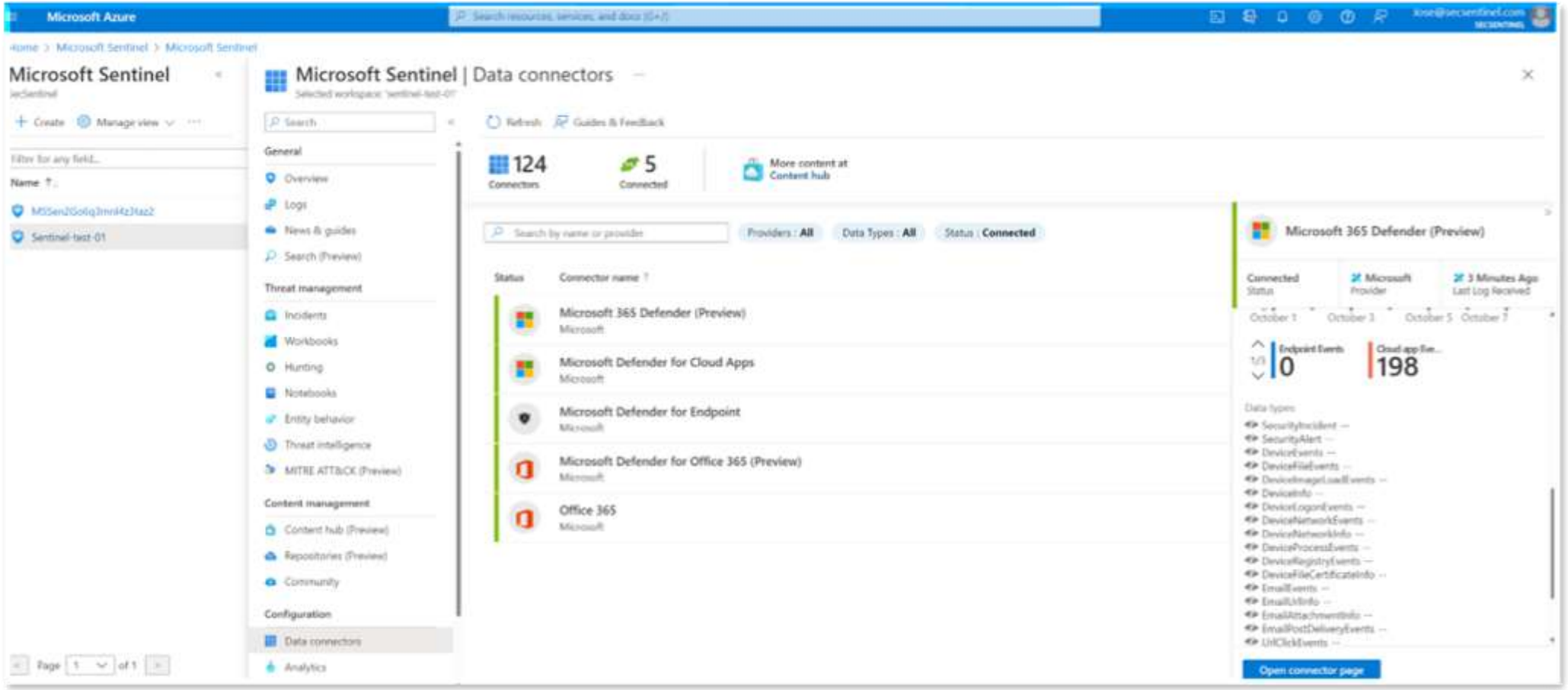
Log Analytics & Data Retention

- By default, Log Analytics will store data for 30 days and can be set to a maximum of 730 days.
- You can adjust the Data Retention based on your business needs. First 90 days are free of charge.
- How long you keep your SIEM data available?



Data Connectors

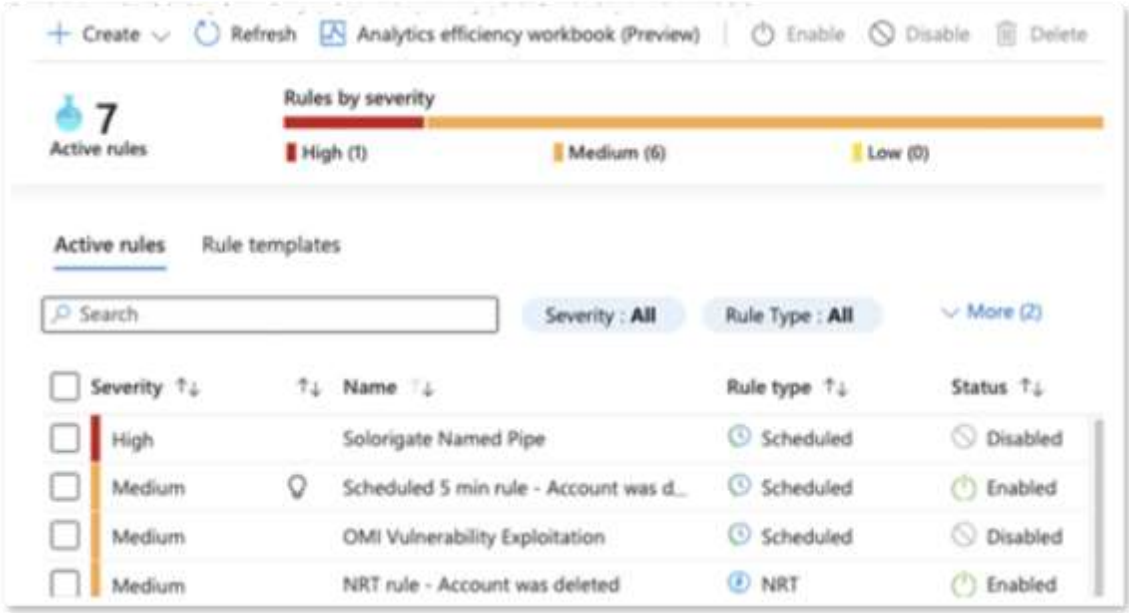
Data Connectors



Sentinel Analytics

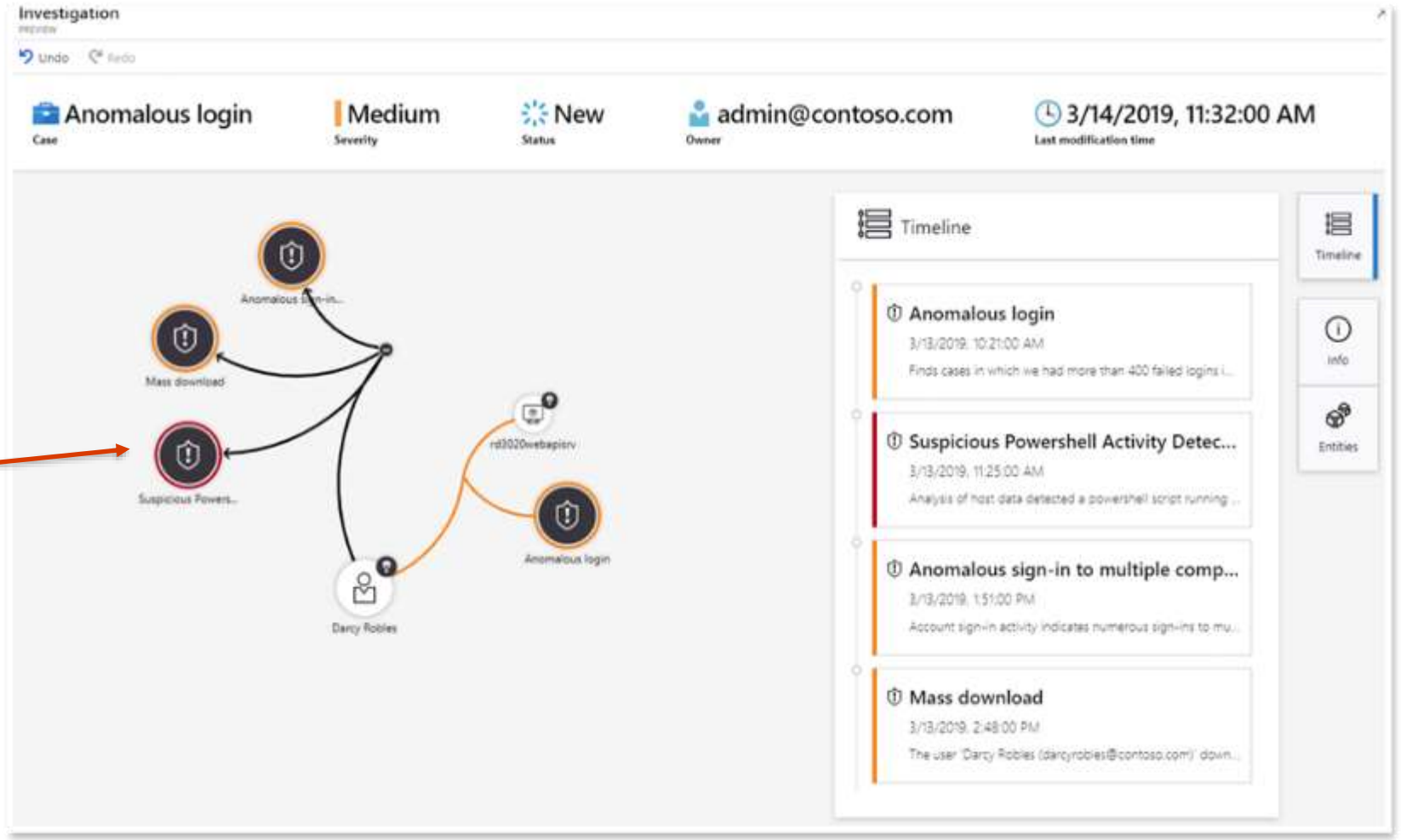
Built-in detections

- **Microsoft Security:** Incident from alerts generated in other security solutions
- **Fusion:** enabled by default and allows detection of advanced multi-stage attacks.
- **Machine learning:** based on learning algorithms. You cannot see the logic and only possible to create from templates.
- **Anomaly:** Also utilizes machine learning to detect specific behaviors, improves detection and investigation experience.
- **Scheduled:** Built-in and written by Microsoft Security Experts. You can see the logic and make changes.
- **NRT:** set of scheduled rules designed to run once every minute. Like scheduled rules.



Investigations

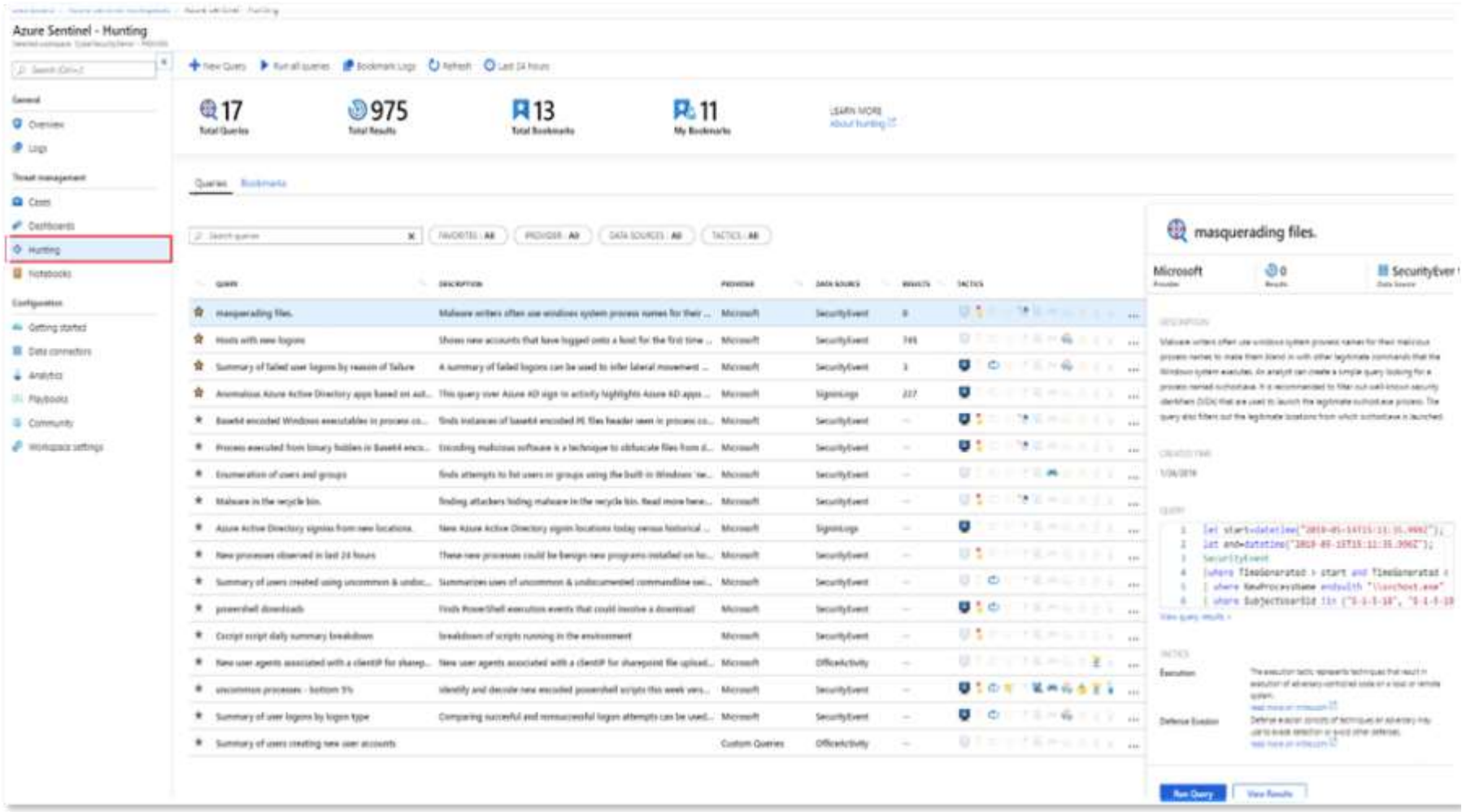
- The Investigation map allows you to view the Related alerts, 5 top hosts logged on, and Hosts logged on by user.



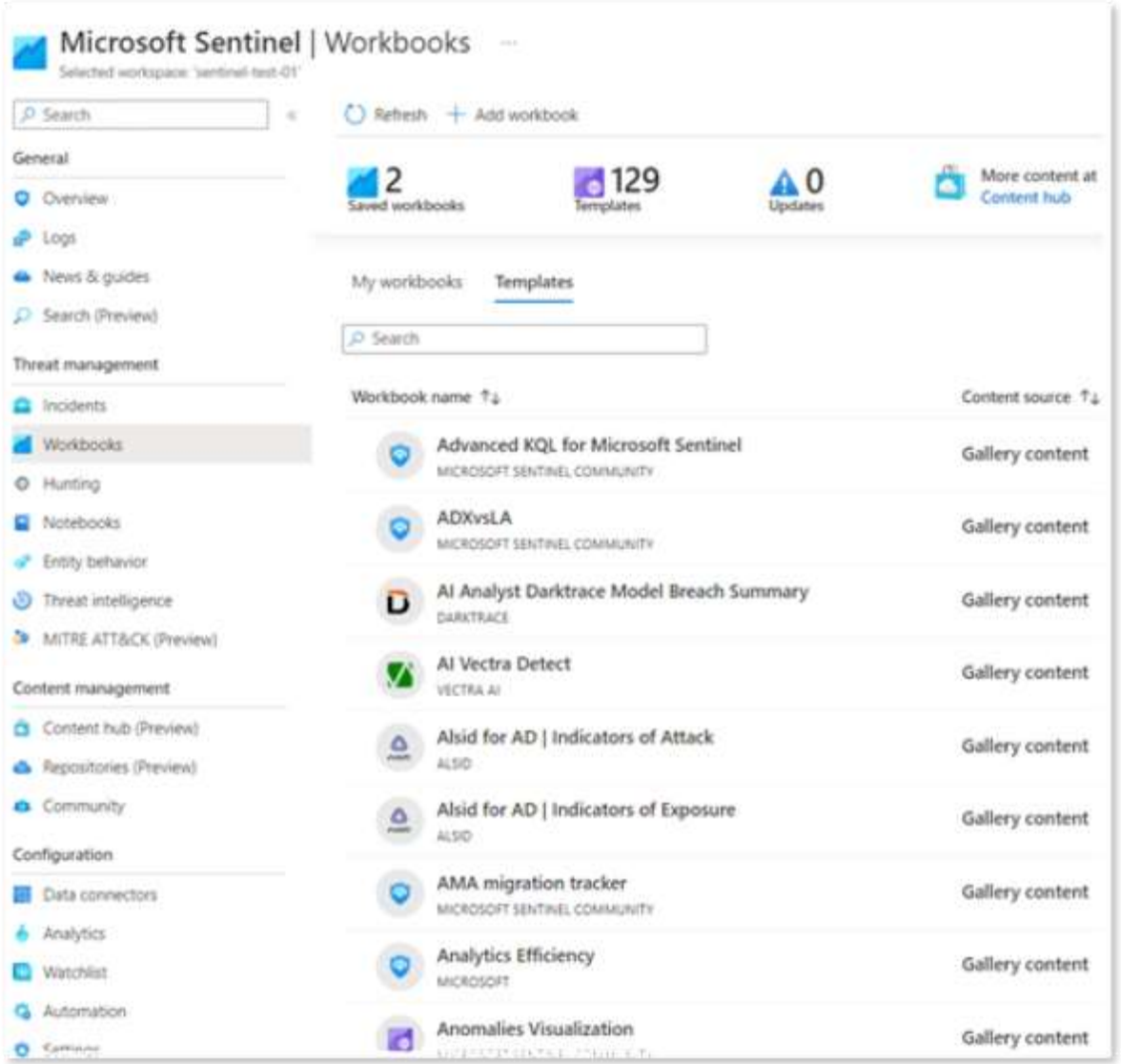
Hunting

Hunting

- The built-in hunting queries can be run, add to favorites, edited, or cloned.
- When you save a query as a favorite the query will run automatically each time you open the Hunting blade.
- The yellow star next to the query represents your favorites.
- When a query is run the number of matches will display in the table.



Workbooks


Microsoft Sentinel | Workbooks
Selected workspace: 'sentinel-test-01'
Search
Refresh
Add workbook
General
Overview
Logs
News & guides
Search (Preview)
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
2
Saved workbooks
129
Templates
0
Updates
More content at
Content hub
My workbooks
Templates
Search
Workbook name
Content source
Advanced KQL for Microsoft Sentinel
MICROSOFT SENTINEL COMMUNITY
Gallery content
ADXvsLA
MICROSOFT SENTINEL COMMUNITY
Gallery content
AI Analyst Darktrace Model Breach Summary
DARKTRACE
Gallery content
AI Vectra Detect
VECTRA AI
Gallery content
Alsid for AD | Indicators of Attack
ALSID
Gallery content
Alsid for AD | Indicators of Exposure
ALSID
Gallery content
AMA migration tracker
MICROSOFT SENTINEL COMMUNITY
Gallery content
Analytics Efficiency
MICROSOFT
Gallery content
Anomalies Visualization
Gallery content

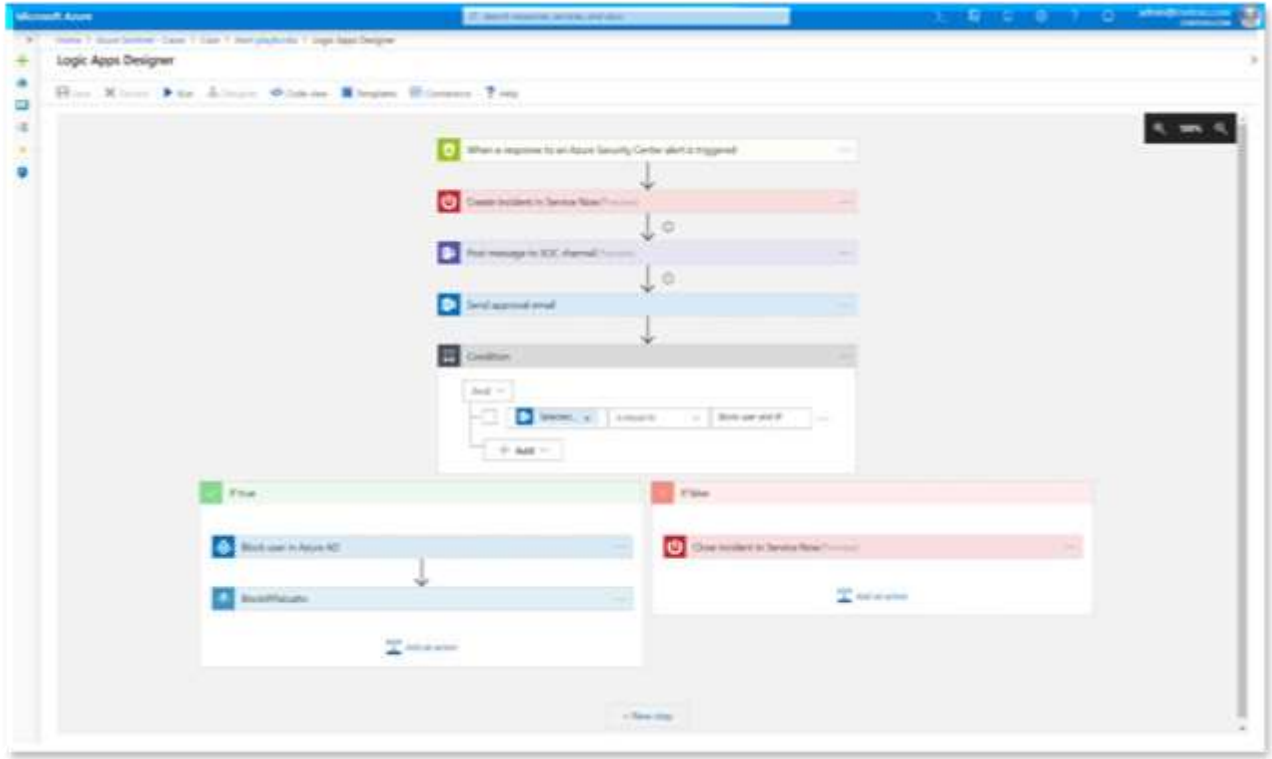

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
Microsoft Sentinel Cost - sentinel-test-01
sentinel-test-01
Edit
Open
Help
Auto refresh: Off
Microsoft Sentinel cost summary
TimeRange: Last 60 days
Workspace: All
Ingestion price: 4
Retention price: 0.1
Ingestion summary
Average billable GBs/day ingested in the last > ago(60d)
0
Total billable ingestion and cost in the last > ago(60d)
30.7 MB
$0.1
Breakdown of billable ingestion by log category in the last > ago(60d)
Log Type
Table Size
Estimated cost
Microsoft Defender for Endpoint
26.658M
$0.11
Microsoft Defender for Cloud Apps
2.403MI
$0.01
Other
1.46MB
$0.01
User Entity Behavior Analytics
149.507I
$0.00
Microsoft Defender Alert Evidence
30.173kI
$0.00

Playbooks

Security Playbooks

- A security playbook is a collection of procedures that can be run from Microsoft Sentinel in response to an alert.
  - Can help to automate and orchestrate your response
  - Can be run manually or set to run automatically when specific alerts are triggered

- Security Playbooks in Microsoft Sentinel are based on Azure Logic Apps.
  - You can use the templates provided under the security category in Logic Apps templates and modify them based on your needs.
  - or create new playbooks using Azure Logic Apps workflow using Security Center as your trigger.



Threat Intelligence

Microsoft Sentinel uses the power of AI and threat intelligence

- Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.
- Sentinel uses threat intelligence and the power of AI to minimize false positives.
- Scenario: computers can become nodes in a botnet when attackers illicitly install malware that secretly connects the computer to the command and control. Threat intelligence can also identify potential threats coming from underground communication channels, such as the dark web.
- Sentinel also allows you to bring your own threat intelligence.
- Scenario: If you get an alert from a specific IP address, your threat intelligence provider integration will be able to let you know if that IP address was recently found to be malicious, Microsoft Sentinel enables integration with threat intelligence providers.

Lunch Break

Please return at 13:00

South Coast Summit

SCI HACK

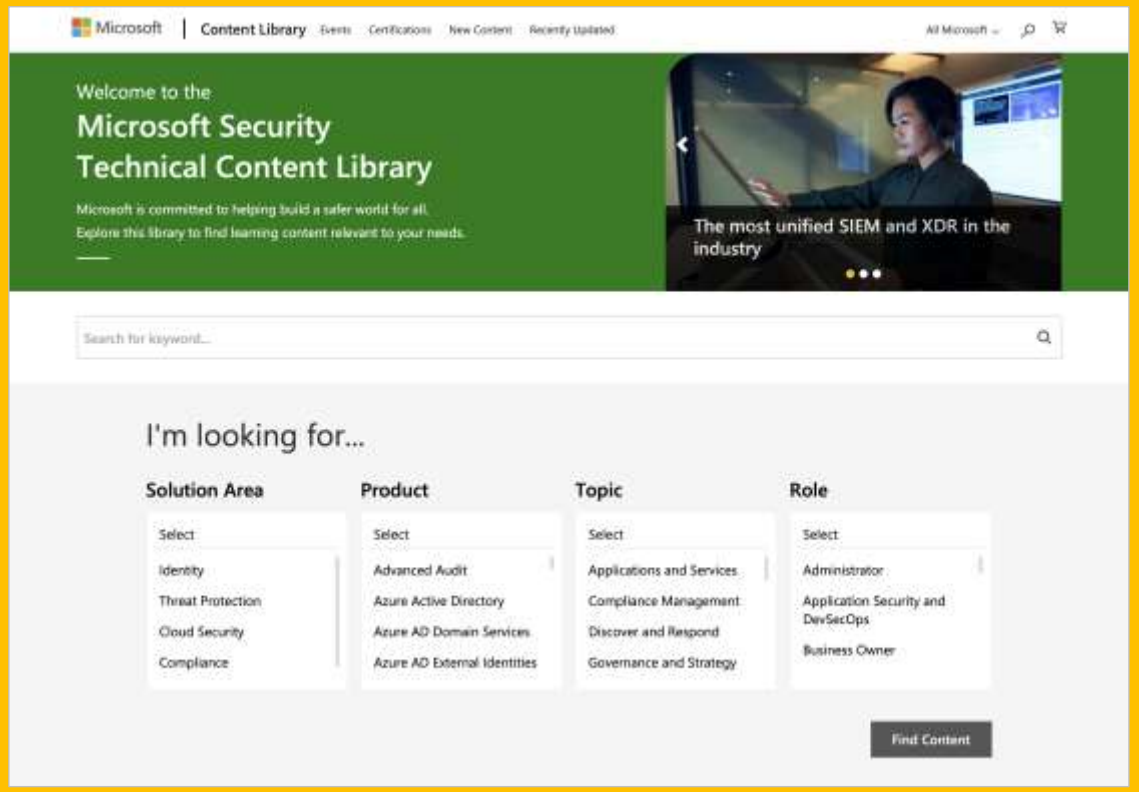
- You will be shown how to get started then its over to you.
- Give us a shout if you need any help
- Hack Details be found - https://aka.ms/scs-sci-repo

South Coast Summit

Conditional Access Links

- Claus Jespersen on LinkedIn: Conditional Access Guidance December 2021 | 51 comments
- Conditional Access demystified: My recommended default set of policies | Modern Workplace Blog (vansurksum.com)
- How to Manage Conditional Access as Code – The Ultimate Guide – Daniel Chronlund Cloud Tech Blog

Microsoft Security Technical Content Library



Developed to ensure customers have the skilling and learning resources available to stay educated in the world of complex cybersecurity attacks.

No matter a customer's role or experience level, the Microsoft Security Technical Content Library enables you to support our customers, helping them grow their skills and learn how to utilize the full breadth of Microsoft Security solutions.

- **Use search filters**
- **Access content based on your needs**
- **Start learning today**

Click here to access the Microsoft Security Technical Content Library.

Microsoft

Microsoft Cybersecurity Reference Architectures

We are excited to announce an **update to the Microsoft Cybersecurity Reference Architectures (MCRA).** The MCRA describes Microsoft cybersecurity capabilities. The diagrams describe how Microsoft security capabilities integrate with Microsoft platforms and third-party platforms such as Microsoft 365, Microsoft Azure, third-party apps such as ServiceNow and Salesforce, and third-party platforms such as Amazon Web Services (AWS) and Google Cloud Platform (GCP).

View the update and download the file here.

Capabilities

What cybersecurity capabilities does Microsoft have?

Build Slide

Azure Native Controls

What native security is available?

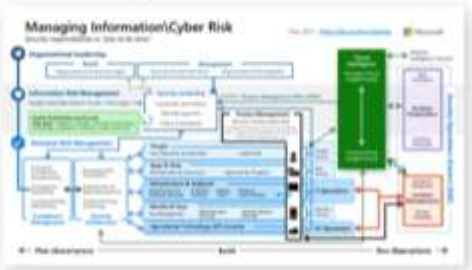
Attack Chain Coverage

How does this map to insider and external attacks?

Build Slide

People

How are roles & responsibilities evolving with cloud and zero trust?



Multi-Cloud & Cross-Platform

What clouds and platforms does Microsoft protect?

aka.ms/MCRA | May 2021 | Microsoft

Zero Trust User Access

How to validate trust of user/devices for all resources?

Security Operations

How to enable rapid incident response?

Operational Technology

How to enable Zero Trust Security for OT?

Security, Compliance, Identity Certifications and Exams

Fundamental Certifications

Microsoft Security, Compliance, and Identity Fundamentals (SC-900)

Training includes
- 7 hours of Microsoft Learn content

Associate Certifications

Microsoft Cybersecurity Architect (SC-100)

- NEW! Exam is available
  Register here

Training includes:
- 4.5 hours of Microsoft Learn content
- 4-day instructor-led training (English)

Microsoft Security Operations Analyst (SC-200)

Training includes
- 30 hours of Microsoft Learn content

Microsoft Identity and Access Administrator (SC-300)

Training includes
- 12 hours of Microsoft Learn content

Microsoft Purview Information Protection Administrator (SC-400)

Training includes
- 10 hours of Microsoft Learn content

Azure Security Engineer (AZ-500)

Training includes
- 32 hours of Microsoft Learn content

Microsoft 365 Security Administrator Associate (MS-500)

Training includes
- 14 hours of Microsoft Learn content

*Azure Network Engineer Associate (AZ-700)

Training includes
- 10 hours of Microsoft Learn content

Go here for the latest certification roadmap:
Microsoft training and certifications.

This page lists the certifications and exams that are recommended for partners looking to build and extend their Microsoft security, compliance, and identity practices.

The Microsoft Security, Compliance, and Identity certification portfolio includes the following certifications:

- Microsoft Security, Compliance, and Identity Fundamentals
- Microsoft Security Operations Analyst
- Microsoft Identity and Access Administrator
- Microsoft Purview Information Protection Administrator
- Azure Security Engineer
- Microsoft 365 Security Administrator

*Azure Network Engineer Associate is categorized in the Azure certification portfolio and is also relevant to our partners.

Go here for the latest certification roadmap Microsoft training and certifications.

Legend ■ Microsoft learning path ▸ YouTube playlist ◉ Interactive guide

Se Additional Resources

Fundamental > Intermediate > Advanced

Overview
Fundamental Knowledge of Microsoft 365 Security and Compliance Capabilities ■
Intro to Security in Microsoft 365 ■
Manage Security with Microsoft 365 ■
Azure Security Fundamentals ■

SIEM + XDR
SIEM + XDR Announcement

Microsoft Defender
Intro to Threat Protection with Microsoft 365 ■
Azure Defender Overview

Azure Sentinel
Deploy Azure Sentinel and Connect Data Sources ■
Introduction to Azure Sentinel ■
Azure Sentinel Overview
Azure Sentinel Video Overview
Deploy Azure Sentinel and Connect Data Sources ■
Top 10 Best Practices for Azure Security ▸

Azure Security Center
Azure Security Center Overview
Identify Security Threats with Azure Security Center ■
Protect Against Security Threats on Azure ■

Microsoft Cloud App Security
Secure Cloud Apps Using Microsoft Cloud App Security ■
Discover and Manage Cloud App Usage with Microsoft Cloud App Security ◉
Protect and Control Information with Microsoft Cloud App Security ◉
Automate Alerts Management with Microsoft Power Automate and Cloud App Security ◉

Microsoft 365 Defender
Microsoft Defender: Extended Detection and Response (XDR) ▸
Threat Protection Technical Deep-Dive ■
Defend Against Threats with Microsoft Threat Protection ■
Protect Your Organization with Microsoft 365 Defender ◉
Stop Attacks & Reduce Operations Workloads by 50%

Azure Security Center
Azure Security Center ■
How to Effectively Perform an Azure Security Center PoC ■
Protect Your Hybrid Cloud with Azure Security Center ◉
Resolve Threats with Azure Security Center ■
Design a Holistic Monitoring Strategy on Azure
Implement Virtual Machine Host Security in Azure ■
Improve Your Cloud Security Posture with Azure Security Center ■

Microsoft Defender for Identity
Identify Attacks ◉
Investigate Attacks ◉

Microsoft Defender For Endpoint
Investigate and Remediate Threats ◉
Threat Vulnerability Management ◉
Microsoft Defender for Endpoint Ninja Training

Microsoft Defender for Office 365
Microsoft Defender for Office 365 ■
Safeguard Your Organization with Microsoft Defender for Office 365 ◉

Azure Sentinel
Modernize Your SOC with Azure Sentinel ◉
Deploy Azure Sentinel and Connect Data Sources ■
Implement Windows Server Hybrid Cloud Management, Monitoring, and Security ■
Improve SecOps with Azure Sentinel, Your Cloud-Native SIEM

Microsoft Cloud App Security
Detect Threats and Protect Information in Cloud Apps Using Microsoft Cloud App Security ■
Detect Threats & Manage Alerts ◉
Discover, Protect, and Control Apps ◉
Safeguard Multi-cloud Apps and Resources with Cloud Security Solutions ■

Azure Sentinel
Azure Sentinel Ninja Training
Detect Unknown Threats with User and Entity Behavior Analytics

Microsoft Defender
Improve SecOps with Azure Sentinel, Cloud-Native SIEM
Web Shell Attack Deep Dive

Microsoft 365 Defender
Microsoft 365 Defender Ninja Training
Best Practices for Hunting Across Domains

Azure Security Center
Azure Security Center Ninja Training

Microsoft Defender for Endpoint
Microsoft Defender for Endpoint Ninja Training

Microsoft Cloud App Security
Microsoft Cloud App Security Ninja Training
Configure Microsoft Cloud App Security for Advanced Scenarios ■

Identity certifications SC-300, SC-900

Microsoft

Improve your infrastructure and development security

You can implement ASB security controls to individual service baselines throughout your organization's benchmark planning, approval, and implementation processes across high-level control domains:

- Network security (NS)
- Identity Management (IM)
- Privileged Access (PA)
- Data Protection (DP)
- Asset Management (AM)
- Logging and Threat Detection (LT)
- Incident Response (IR)
- Posture and Vulnerability Management (PV)
- Endpoint Security (ES)
- Backup and Recovery (BR)
- DevOps Security (DS)
- Governance and Strategy (GS)

Find Microsoft-recommended infrastructure and development security practices and recommendations that can help improve the security of workloads, data, and services in Azure.

The guidance supplements Microsoft tools and security guides, including Microsoft Cloud Adoption Framework for Azure overview, Azure Security Benchmark (ASB) introduction, and other supporting technical documentation.

Microsoft Defender for Endpoint Virtual Ninja Training with Heike Ritter

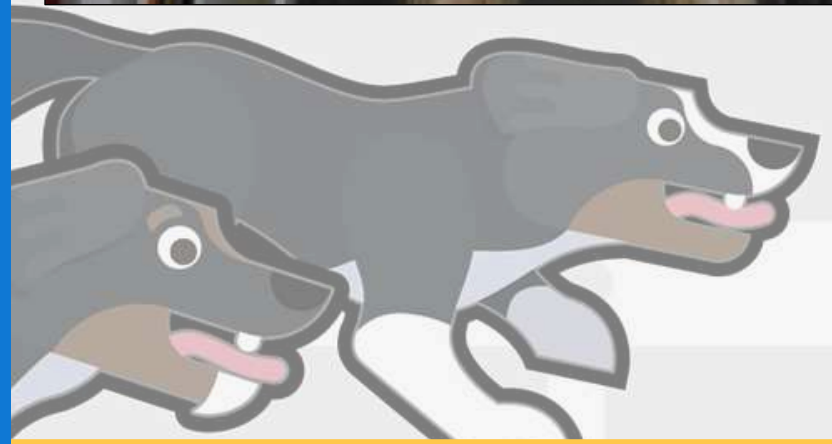
This training series is based on the Ninja blog and brings you up to speed quickly on Microsoft Defender for Endpoint.

Our experts guide you through the powerful features and functions of Microsoft Defender for Endpoint that can help you keep your environment secure.

We start with the fundamentals and dive deeper as the show continues.

Watch on demand

View past episodes on demand and catch up on the next live training.

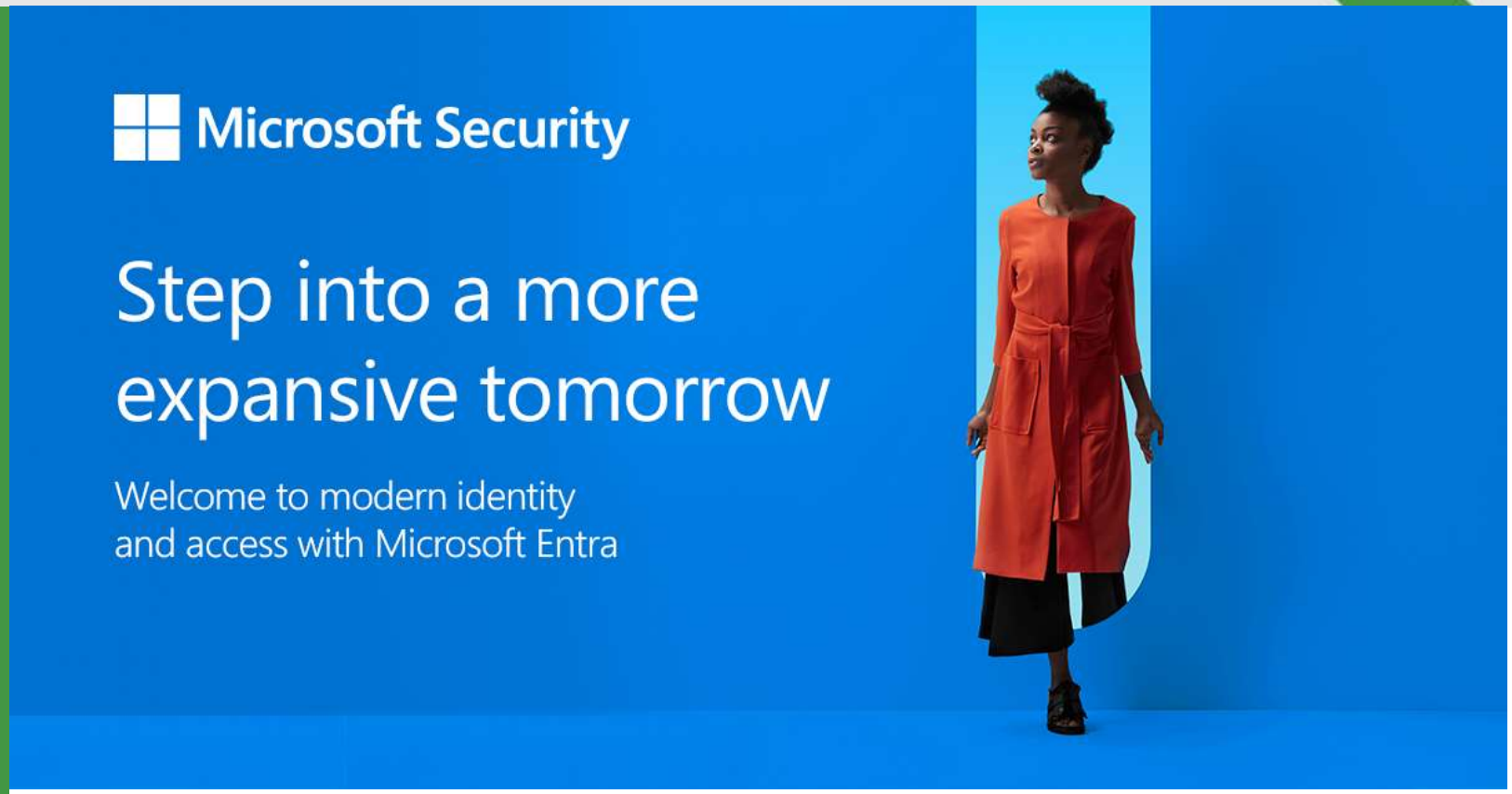


Season 2 is coming soon with more Ninja Training on the way! Stay tuned for details.

Microsoft

Microsoft Entra: Secure access for a connected world

Microsoft Entra is a product family that encompasses the Microsoft identity and access capabilities.
The Entra family includes Microsoft Azure Active Directory and two innovative product categories: Cloud Infrastructure Entitlement Management (CIEM) and decentralized identity.
The products in the Entra family will help provide secure access to everything for everyone by providing identity and access management, cloud infrastructure entitlement management, and identity verification.



[Learn more about Microsoft Entra - Secure Identities and Access]

It’s about community

Support is just a click away

Help your customers learn, get Microsoft certified, and join other security professionals in the online Microsoft Security community. They can participate in discussions about additional training and enablement, find key role resources, and more.

Join

Microsoft 365 Security, Compliance & Identity Partners Yammer Community

Security, Compliance, and Identity – Microsoft Tech Community

Certifications

SC-900: Microsoft Security, Compliance, and Identity Fundamentals

SC-100: Microsoft Cybersecurity Architect (beta)

SC-200: Microsoft Security Operations Analyst

SC-300: Microsoft Identity and Access Administrator

SC-400: Microsoft Purview Information Protection Administrator

MS-900: Microsoft 365 Fundamentals

MS-500: Microsoft 365 Security Administration

AZ-900: Azure Fundamentals

AZ-500: Microsoft Azure Security Technologies

AZ-700: Designing and Implementing Microsoft Azure Networking Solutions

Resources

Microsoft Security Technical Content Library

Microsoft Security website

Azure website

Microsoft Security blog

Security documentation

Microsoft Sentinel documentation

Microsoft Learn for Security, Compliance, and Identity

Follow Us

Microsoft Security on Twitter

Microsoft Azure Active Directory on Twitter

Microsoft Security on LinkedIn

Microsoft Security YouTube channel

Microsoft

THANK YOU

Share your thoughts, feedback and training requests via our survey!

https://aka.ms/scs-predayscifeedback

https://meetup.com/M365SandCUG
https://aka.ms/scs-sci-repo