

dine**x**t.
pi-sec GmbH

~ Envisioning Workshop ~



First things first:

- call will be recorded
- Please keep your microphone muted
- please feel free to tell us your thoughts, ideas, questions
- if a discussion is ongoing, please „raise your hand“
- anything else? let us know!

Envisioning

An Envisioning Workshop will help you understand the technologies, the challenges, the benefits, and the way ahead. That's why today's agenda looks like this:

- organizational overview of the project structure
- technical overview, what you can expect
- Microsoft 365 Defender in a nutshell
- next steps – and what you need to prepare

Agenda

- Who we are and what we do
- Touching base with Microsofts security strategy
- State of the nation: cyber attacks in 2021
- Security is no silver bullet
- Microsoft XDR – deep dive

Who we are:



Timo Breuer

Microsoft XDR



Holger Radecke

Information Protection & Compliance (MIP)



Fabio Gondorf

Endpoint Security (MDE, Defender)



Thomas Gross

Cloud Security (Azure Defender, Sentinel)



Dennis Pesch

Microsoft XDR



Thomas von Fragstein

Microsoft 365 Defender



Sven Bloch

Microsoft 365 Defender



Sanket Rajendra Shah

Data Scientist

pi-sec solution portfolio



Threat Protection



**Managed Detection
and Response**



Incident Response



**Information Protection
& Compliance**

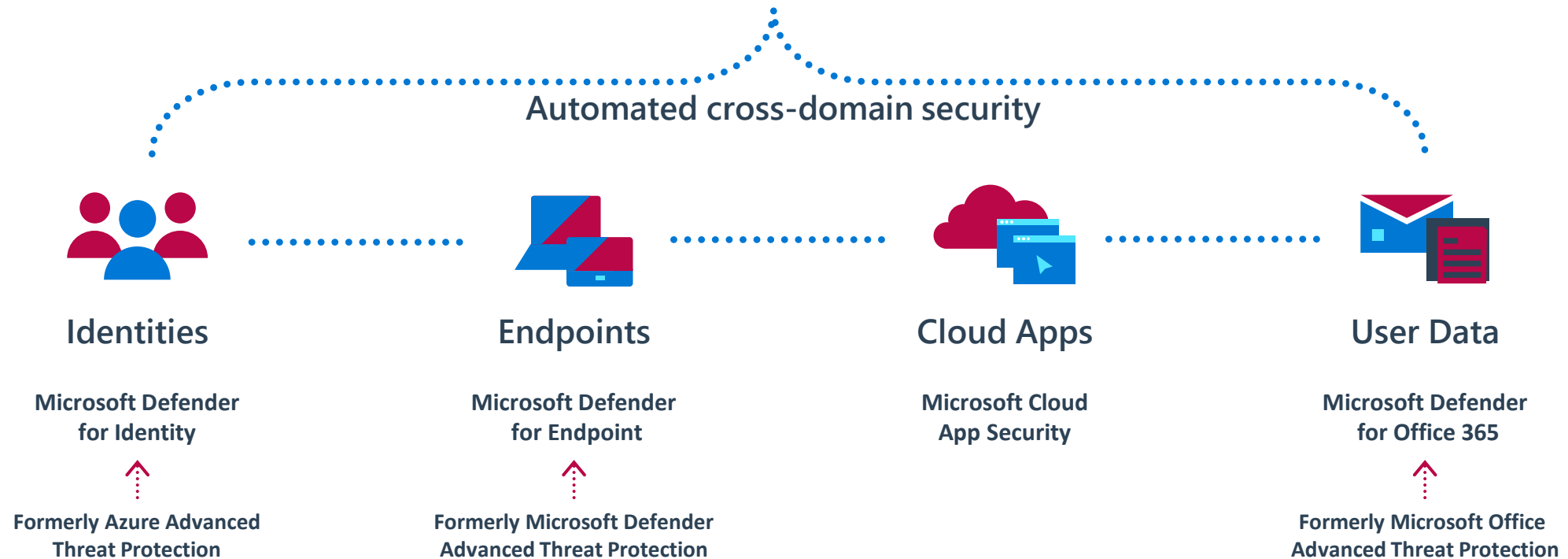


Attack Simulation



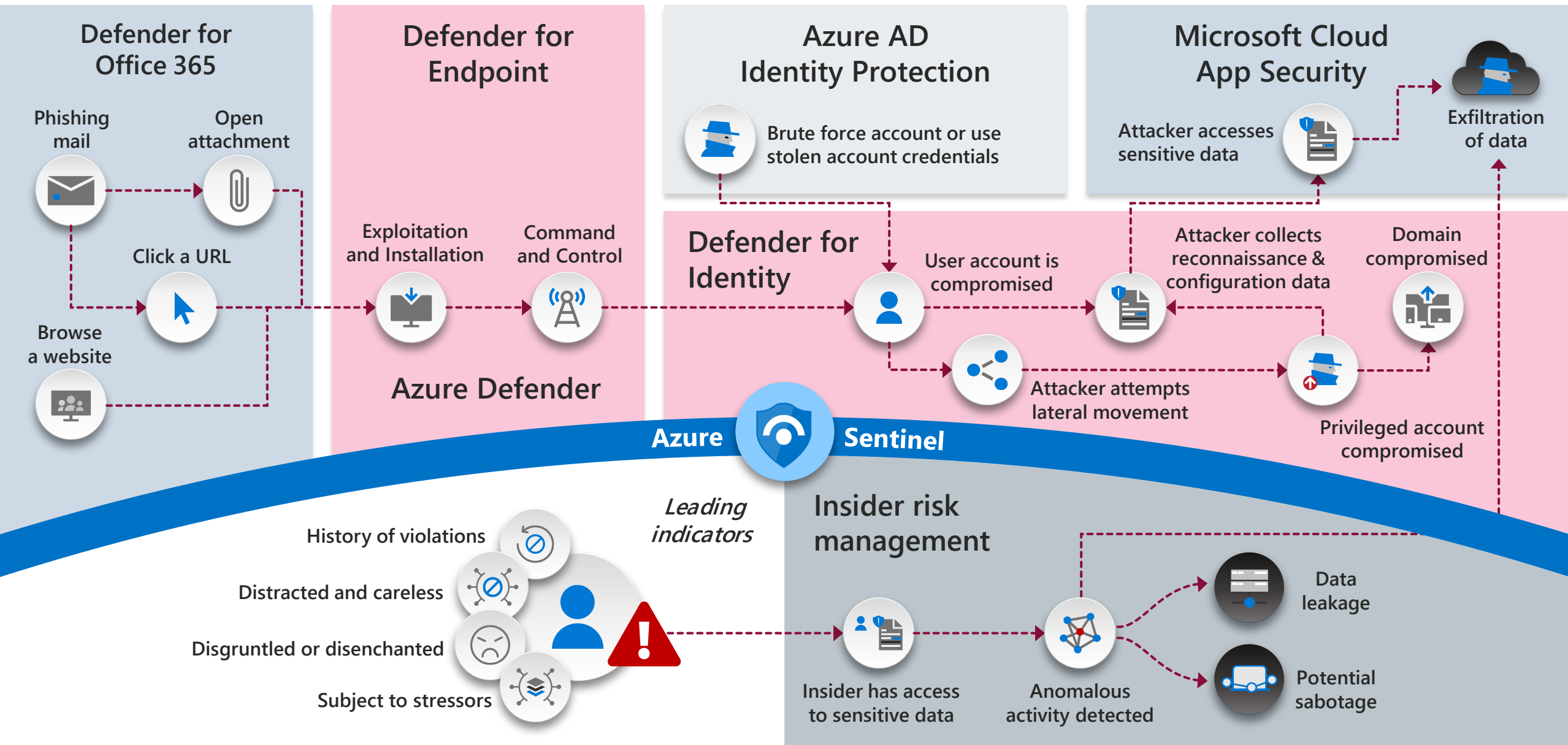
**Dashboards
& Data Science**

Microsoft 365 Defender

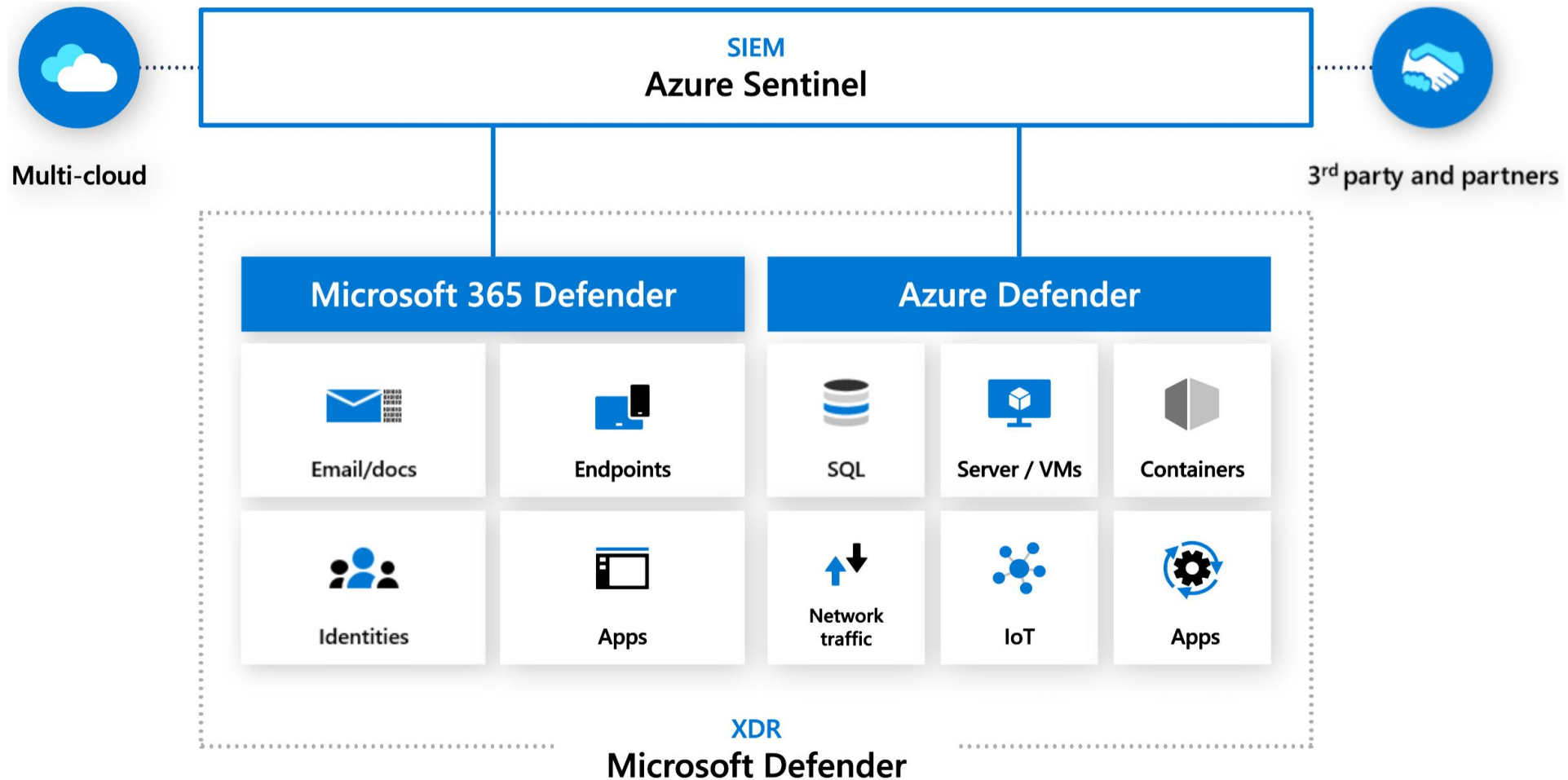


Shift from individual silos to coordinated cross-domain security

Defend across attack chains



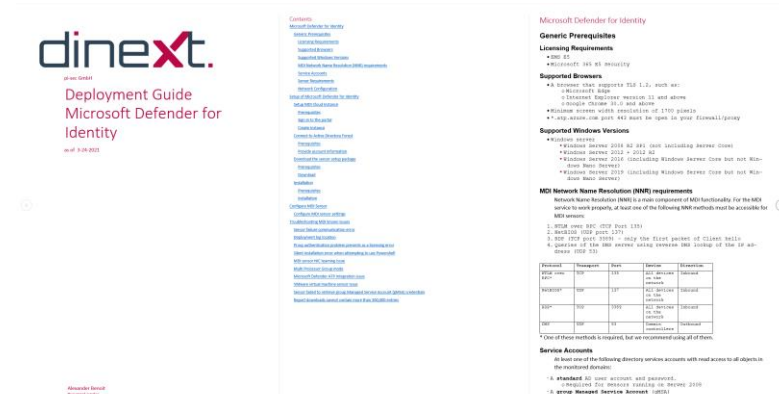
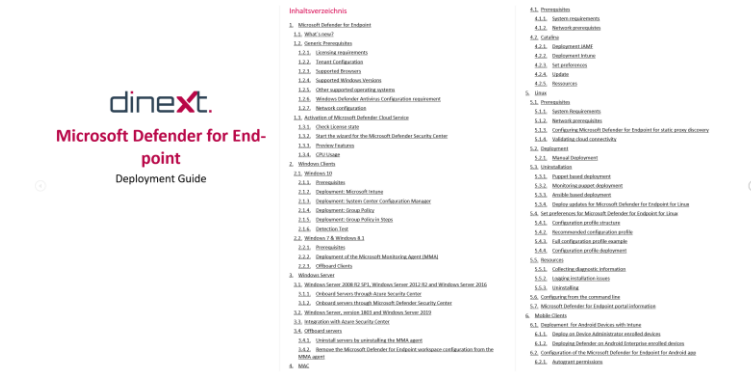
Threat Protection: Microsoft Defender XDR



Guides and documentation

We provide a strong guidance within the project based on our experience and proven concepts and guidelines. Part of our service are:

- Prerequisites Guides for Microsoft 365 Defender, Defender for **Endpoint**, Defender for **Identity**, Defender for **O365**, Microsoft **Cloud App Security**,
- **Deployment** Guides for **all** above **products**
- **Best practices** and how to guides like:
 - Role Based Access Configuration
 - Scoped Access Control
- **Works Council** Communication for all above products
- **Operations Manuals** - how to SecOps



Facebook Breach: Smishing Attacks

Home > News > Security > 533 million Facebook users' phone numbers leaked on hacker forum

533 million Facebook users' phone numbers leaked on hacker forum

By [Lawrence Abrams](#)

April 3, 2021 02:48 PM 7



The mobile phone numbers and other personal information for approximately 533 million Facebook users worldwide has been leaked on a popular hacker forum for free.

Wednesday, 21 April 2021



DHL: Your parcel is arriving, track here: <http://demo.mipunet.cn/a/?lrwlaoj8eo66>

05:12

USPS: the arranged delivery for the package 1z21406 has been changed. Please confirm here: w6fvc.info/x7DZip3vE

Text Message
Today 01:15

Dear Customer,

Your AppleID is due to expire Today, Please tap <http://bit.do/cRqb6> to update and prevent loss of services and data.

Apple smsSTOPto43420

Our approach: Security Operations

Pre-Operations

review and awareness

transition and
transfor-
mation

Operations

reporting & data
insights

forensics

continuous
challenging

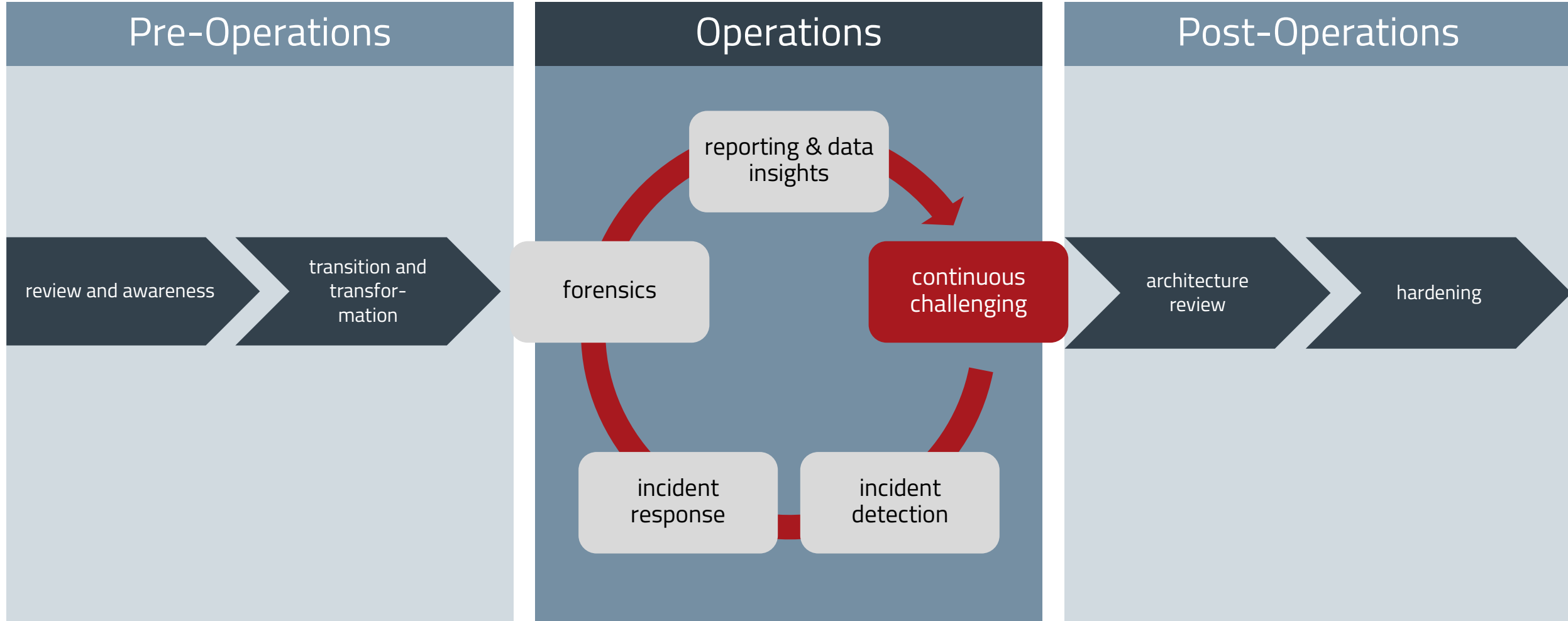
incident
response

incident
detection

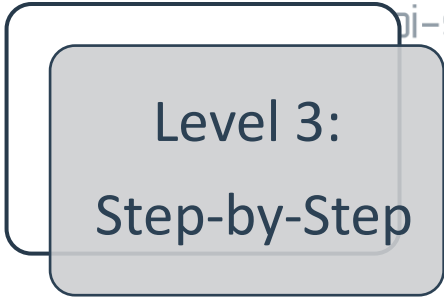
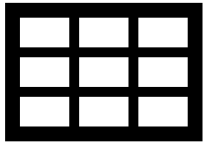
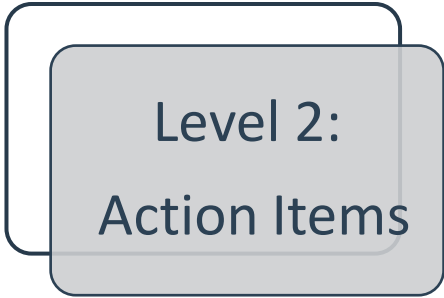
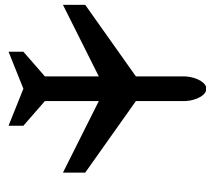
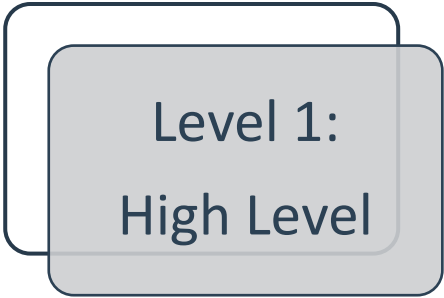
Post-Operations

architecture
review

hardening

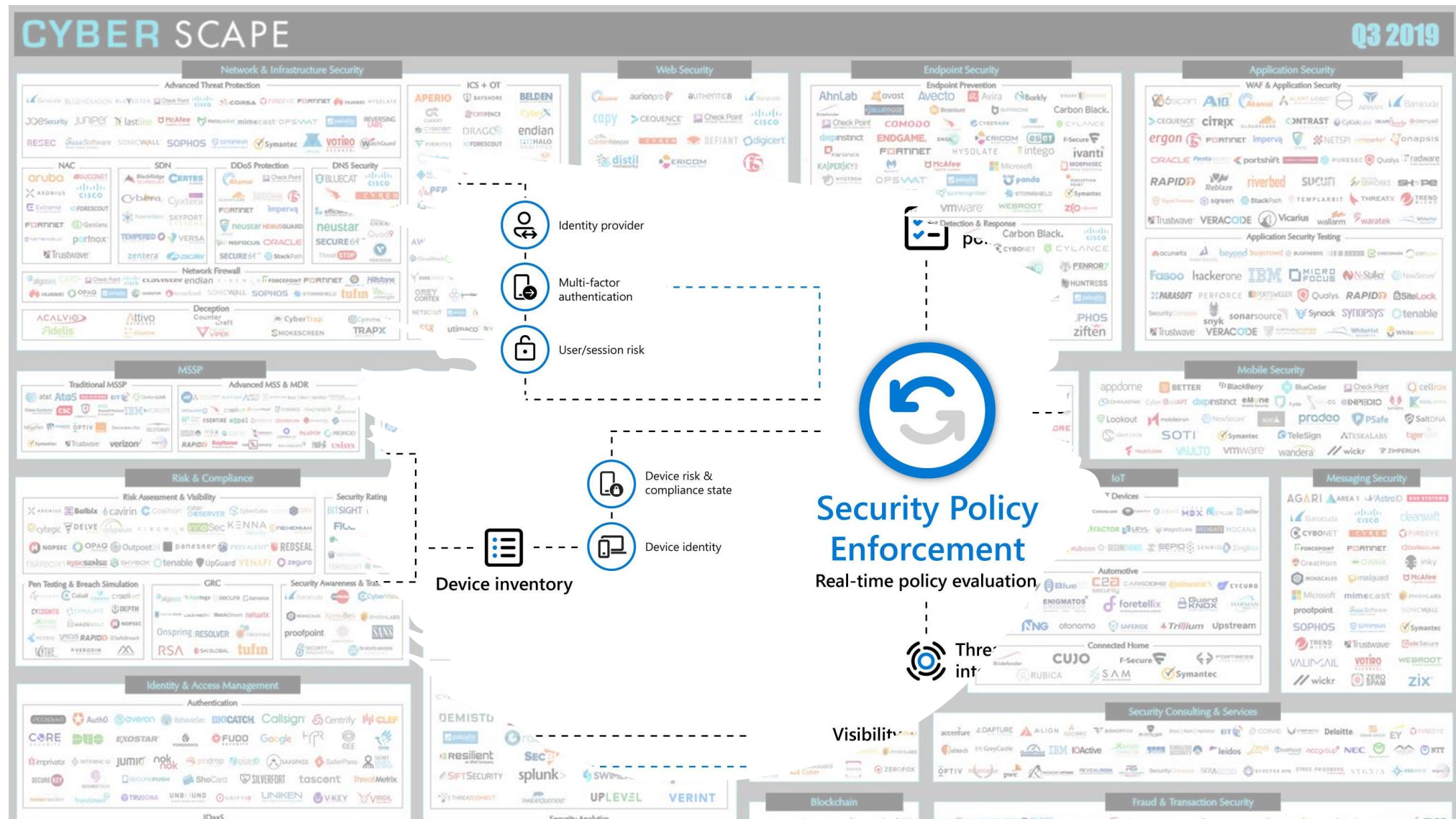


Sampling



	Level 1	Level 2	Level 3
<u>Purpose:</u>	High level process & workstream overview	Action item lists for each workstream with RACI	step-by-step documentation
<u>Informs about:</u>	Process phases, different process starts & frequencies, dependencies, main responsible stakeholder	Who needs to do which Action Items in which order to fulfill the workstreams	All needed details how to fulfill the Action Items
<u>Assembled in:</u>	Visio(s)	Excel	Word

...so how do you prove?



Breach & Attack Simulation

by  SafeBreach

Mitigate

- Remediate issues
- Track your progress
- Report back and make the case



Simulate Attacks

- Cloud, network, endpoint, email
- Infiltration, lateral movement, host level, exfiltration
- Any US-CERT, any emerging threat with 24 hours SLA

Prioritize Results

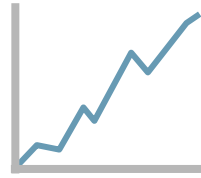
- Associate with overall risk
- Visualize attack path
- Filter and target critical issues for actionable results

Breach & Attack Simulation

by  SafeBreach



Measure
effectiveness of
current controls



Improve Security Tool
ROI



Threat specific visibility &
preparedness



SOC & IR
Training



Enhance Pen Testing and
Red Team Operation



Assess Risk in
M&A and Partner/Extranet
environment and processes



Vulnerability
Integration and
Prioritization



Measure Security and
validate controls in
ICS/OT environment



Cloud Native Security

dine^xt.
pi-sec GmbH

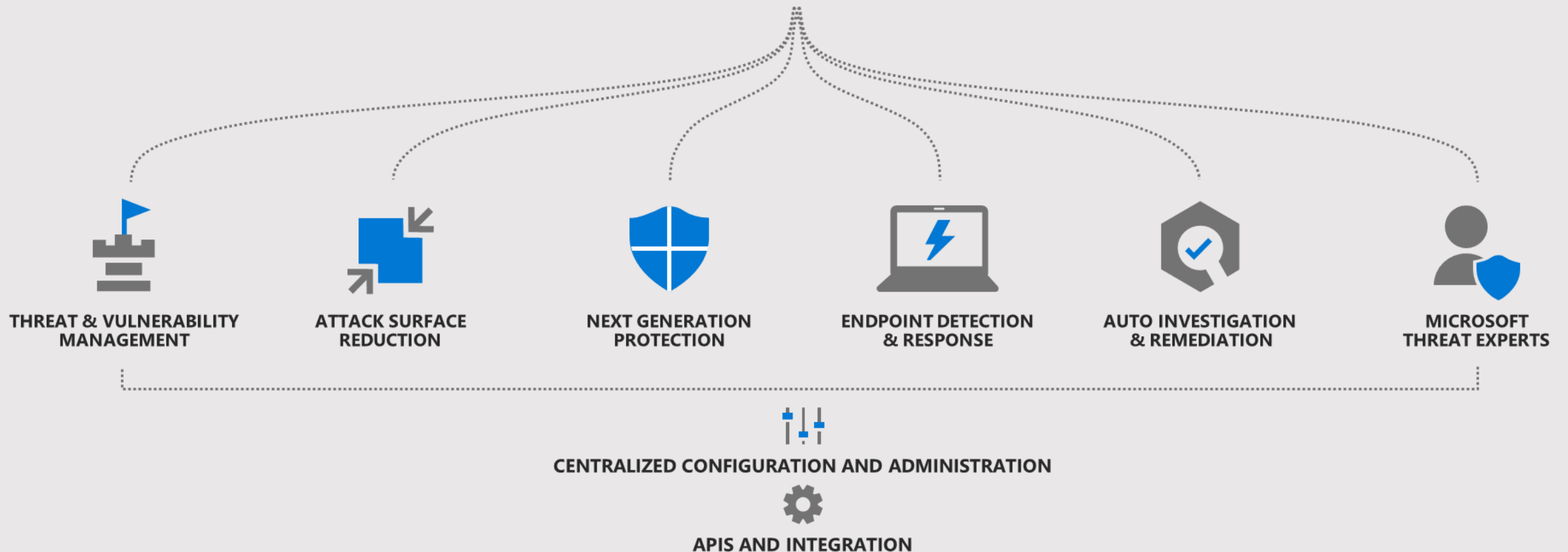
Microsoft Defender for
Endpoint





Microsoft Defender for Endpoint

Built-in. Cloud-powered.





Microsoft Defender for Endpoint

Built-in. Cloud-powered.



THREAT & VULNERABILITY
MANAGEMENT



1



Continuous Discovery

Broad secure configuration assessment



Operation system misconfiguration

- File Share Analysis
- Security Stack configuration
- OS baseline



Application misconfiguration

- Least-privilege principle
- Client/Server/Web application analysis
- SSL/TLS Certificate assessment



Account misconfiguration

- Password Policy
- Permission Analysis



Network misconfiguration

- Open ports analysis
- Network services analysis

Continuous Discovery

Extensive vulnerability assessment across the entire stack

Security recommendations

Customize columns
Export 30 items per page

Security recommendation	Weaknesses	Related component	Threats	Exposed devices	Status	Remediation type
Update Microsoft Windows 10 (OS and built-in applications)	52	Microsoft Windows 10	⊛ ⊛ ⊛	1 / 3		Active Software update
Block all Office applications from creating child processes	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Block JavaScript or VBScript from launching downloaded executable content	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Block process creations originating from PSEXEC and WMI commands	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Block untrusted and unsigned processes that run from USB	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Block Office communication application from creating child processes	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Block Adobe Reader from creating child processes	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Block persistence through WMI event subscription	1	Security controls (Attack Surface Reduction)	⊛ ⊛ ⊛	2 / 2		Active Configuration change
Update Microsoft Edge Chromium-based	29	Microsoft Edge Chromium-based	⊛ ⊛ ⊛	1 / 2		Active Software update
Update Adobe Acrobat Reader Dc	14	Adobe Acrobat Reader Dc	⊛ ⊛ ⊛	1 / 1		Active Software update
Update Microsoft Office	6	Microsoft Office	⊛ ⊛ ⊛	1 / 2		Active Software update
Turn on Microsoft Defender ATP sensor	1	Security controls (EDR)	⊛ ⊛ ⊛	2 / 3		Active Configuration change
Fix Defender ATP sensor data collection	1	Security controls (EDR)	⊛ ⊛ ⊛	2 / 3		Active Configuration change

1



Continuous Discovery

Extensive vulnerability assessment across the entire stack

Easiest to exploit



Application extension vulnerabilities

Application-specific vulnerabilities that relate to component within the application.
For example: Grammarly Chrome Extension (CVE-2018-6654)



Application run-time libraries vulnerabilities

Reside in a run-time libraries which is loaded by an application (dependency).
For example: Electron JS framework vulnerability (CVE-2018-1000136)



Application vulnerabilities (1st and 3rd party)

Discovered and exploited on a daily basis.
For example: 7-zip code execution (CVE-2018-10115)



OS kernel vulnerabilities

Becoming more and more popular in recent years due to OS exploit mitigation controls.
For example: Win32 elevation of privilege (CVE-2018-8233)



Hardware vulnerabilities (firmware)

Extremely hard to exploit, but can affect the root trust of the system.
For example: Spectre/Meltdown vulnerabilities (CVE-2017-5715)

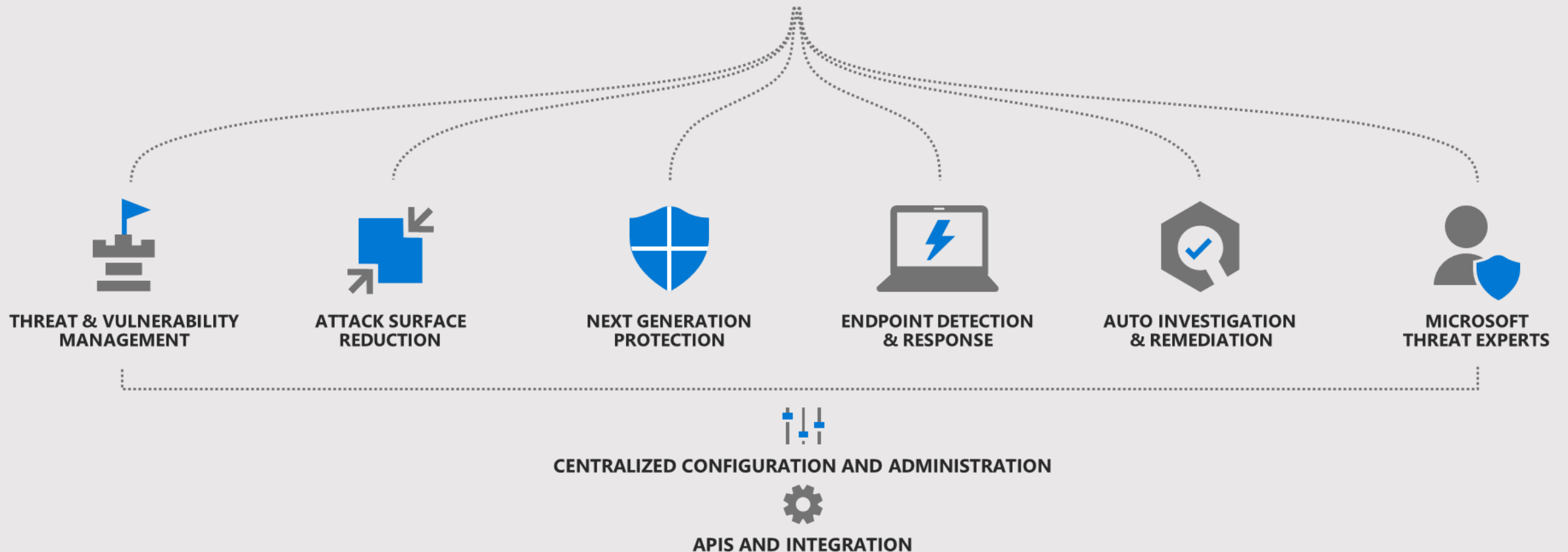
Hardest to discover





Microsoft Defender for Endpoint

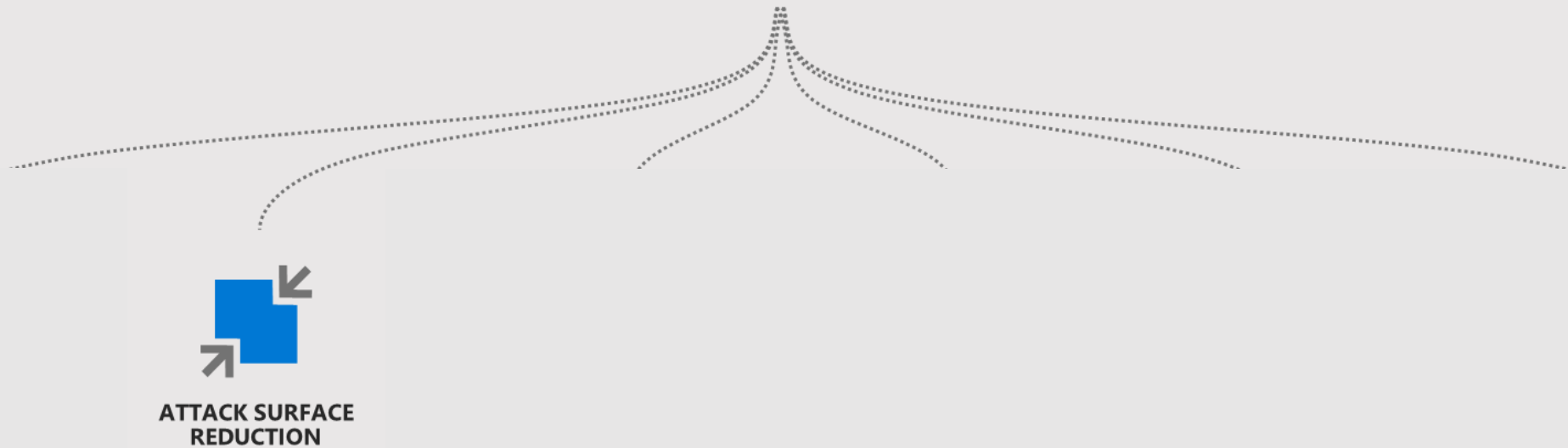
Built-in. Cloud-powered.





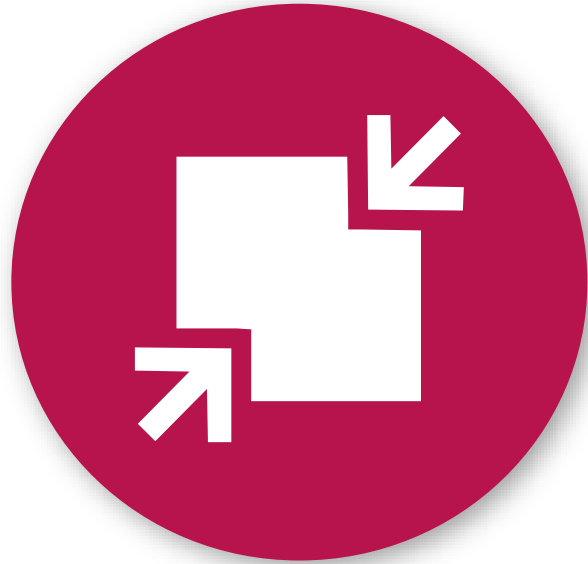
Microsoft Defender for Endpoint

Built-in. Cloud-powered.



Attack Surface Reduction

Resist attacks and exploitations



HW based isolation

Application control

Exploit protection

Network protection

Controlled folder access

Device control

Web protection

Ransomware protection

Isolate access to untrusted sites

Isolate access to untrusted Office files

Host intrusion prevention

Exploit mitigation

Ransomware protection for your files

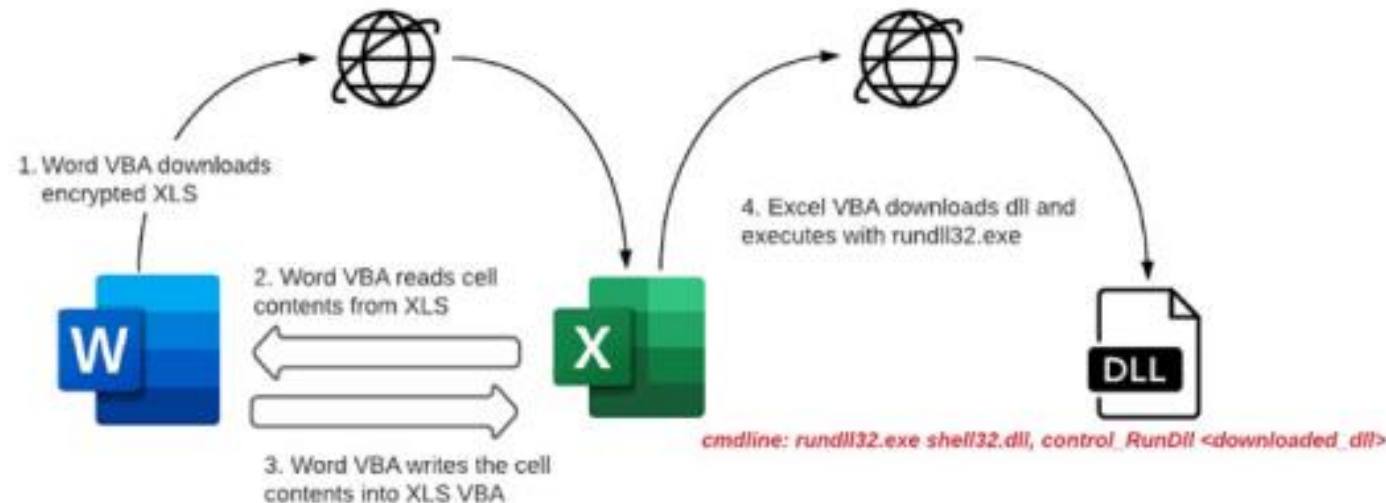
Block traffic to low reputation destinations

Protect your legacy applications

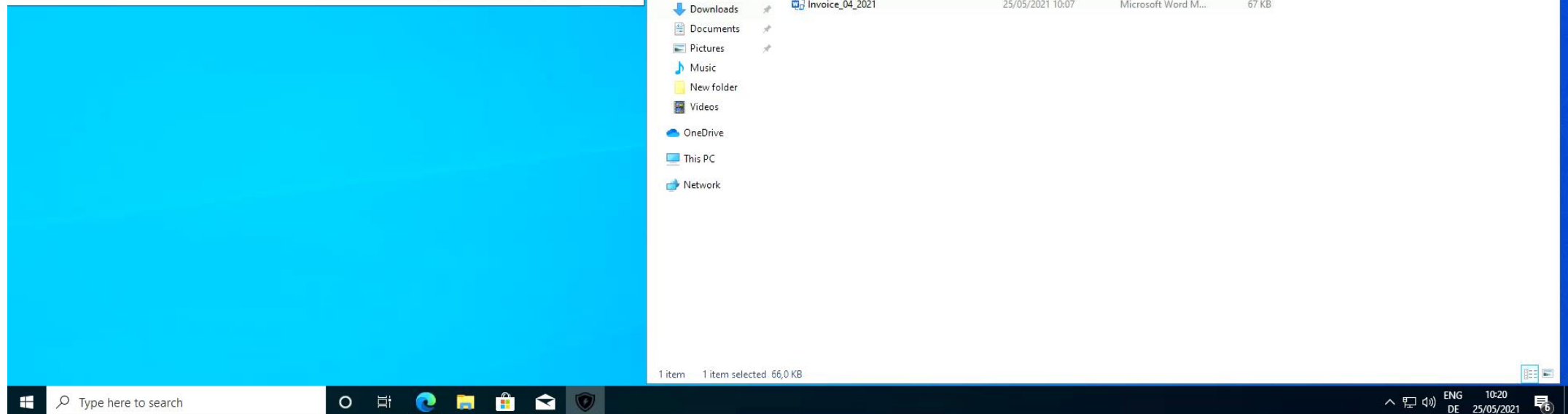
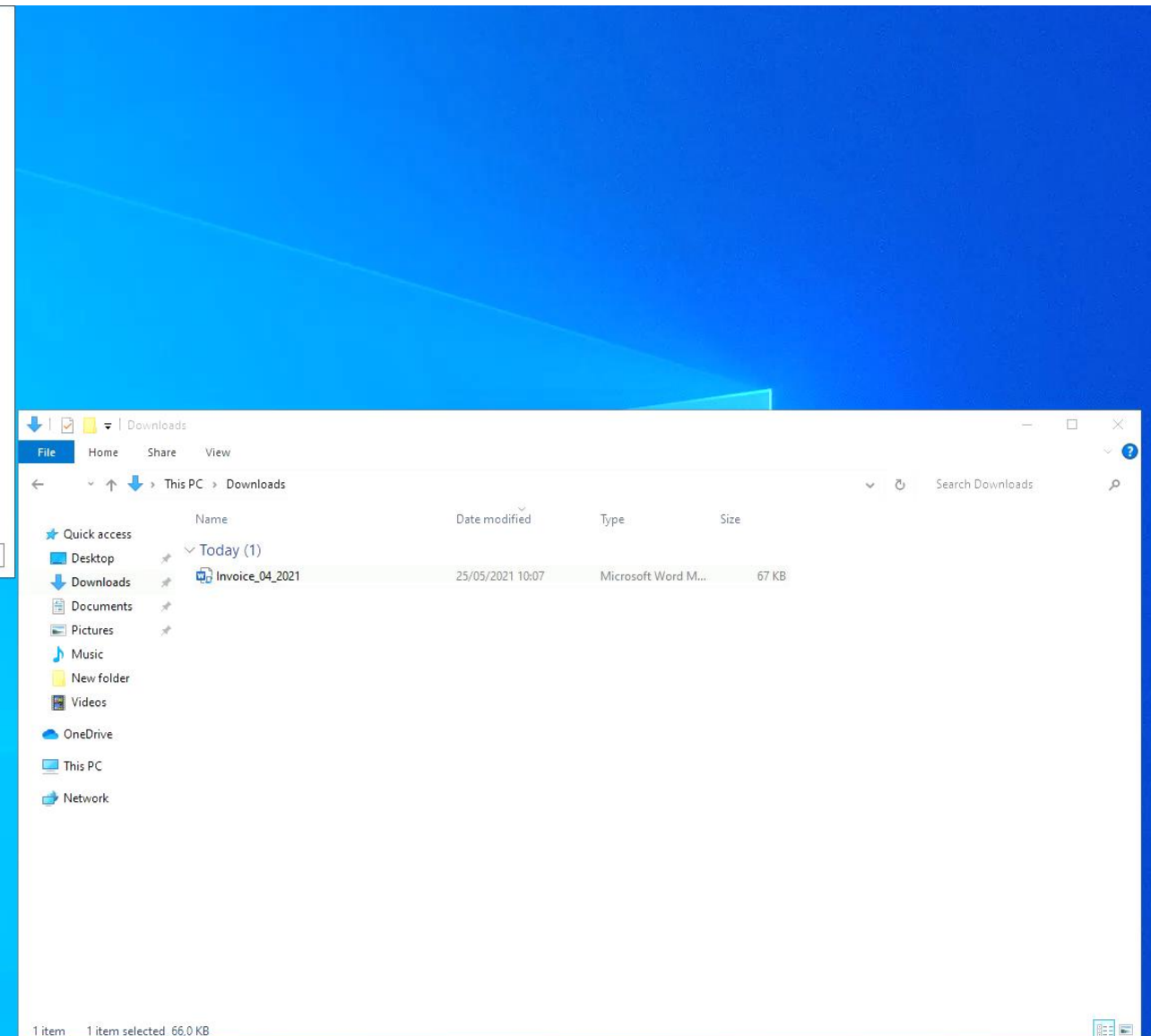
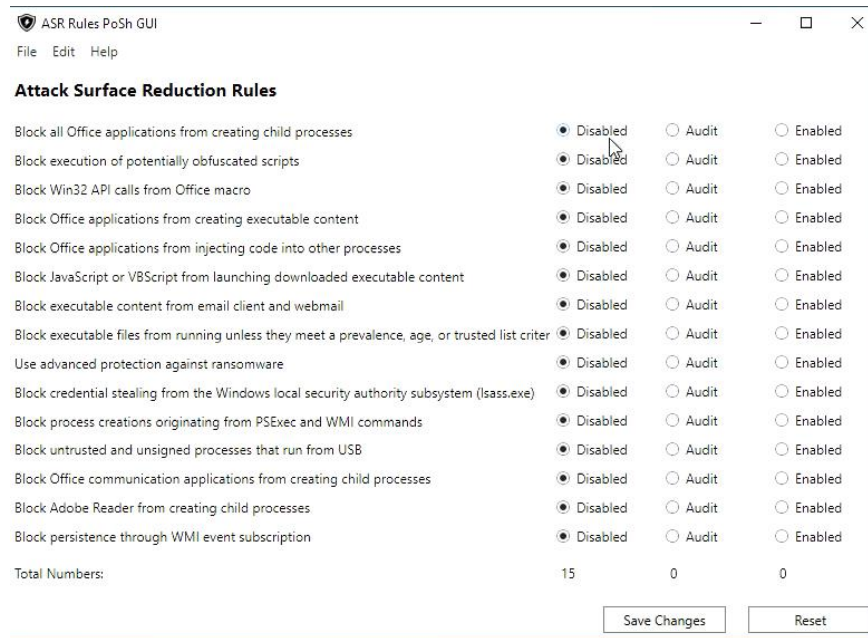
Only allow trusted applications to run

Hackers Use New Trick to Disable Macro Security Warnings in Malicious Office Files

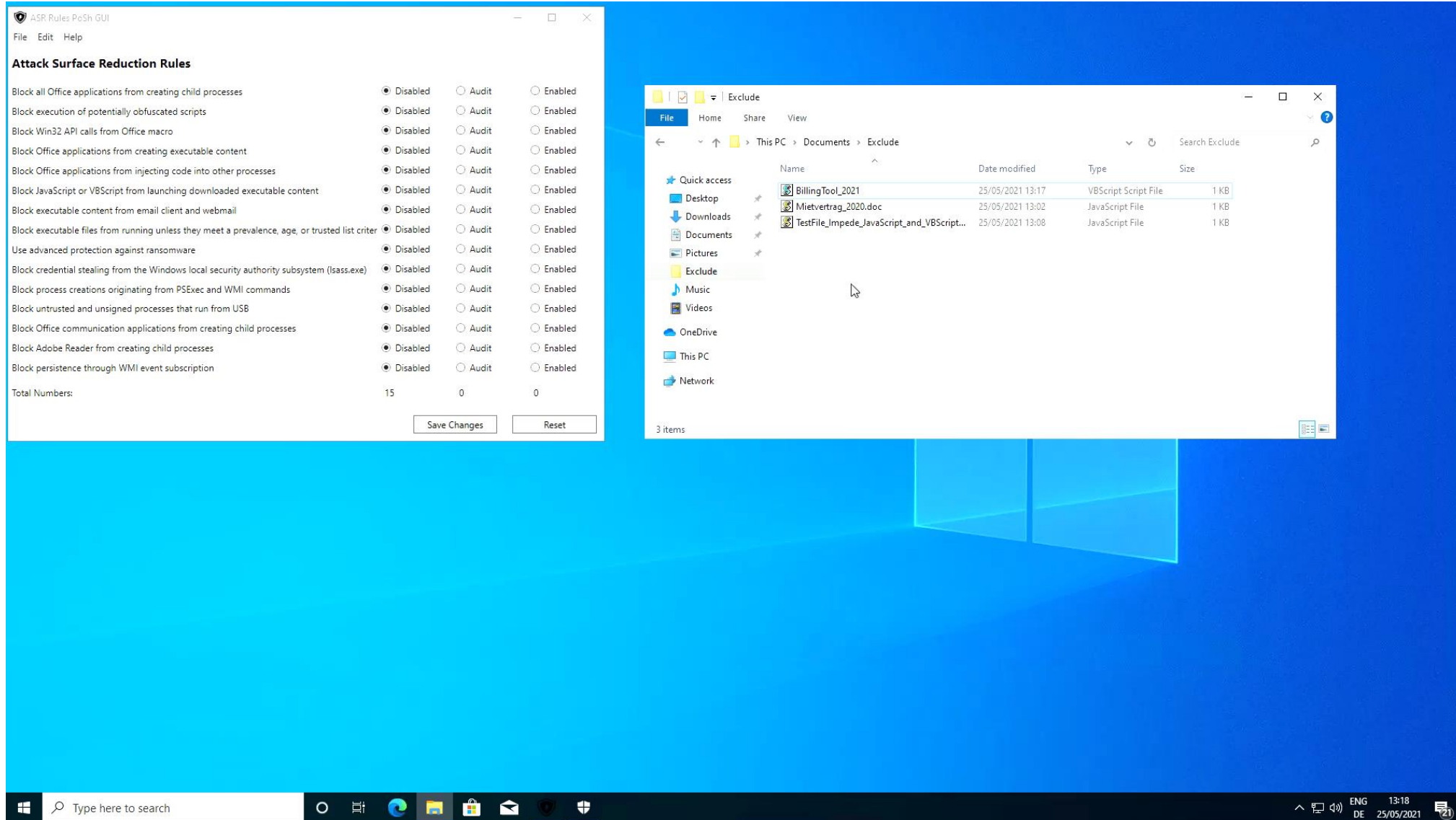
July 08, 2021 Ravi Lakshmanan



Block Office Apps Child Prozess



Block Process Creations originating from PSEXec & WMI commands



Attack Surface Reduction (ASR) Rules



Minimize the attack surface

Signature-less, control entry vectors, based on cloud intelligence. Attack surface reduction (ASR) controls, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats

- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

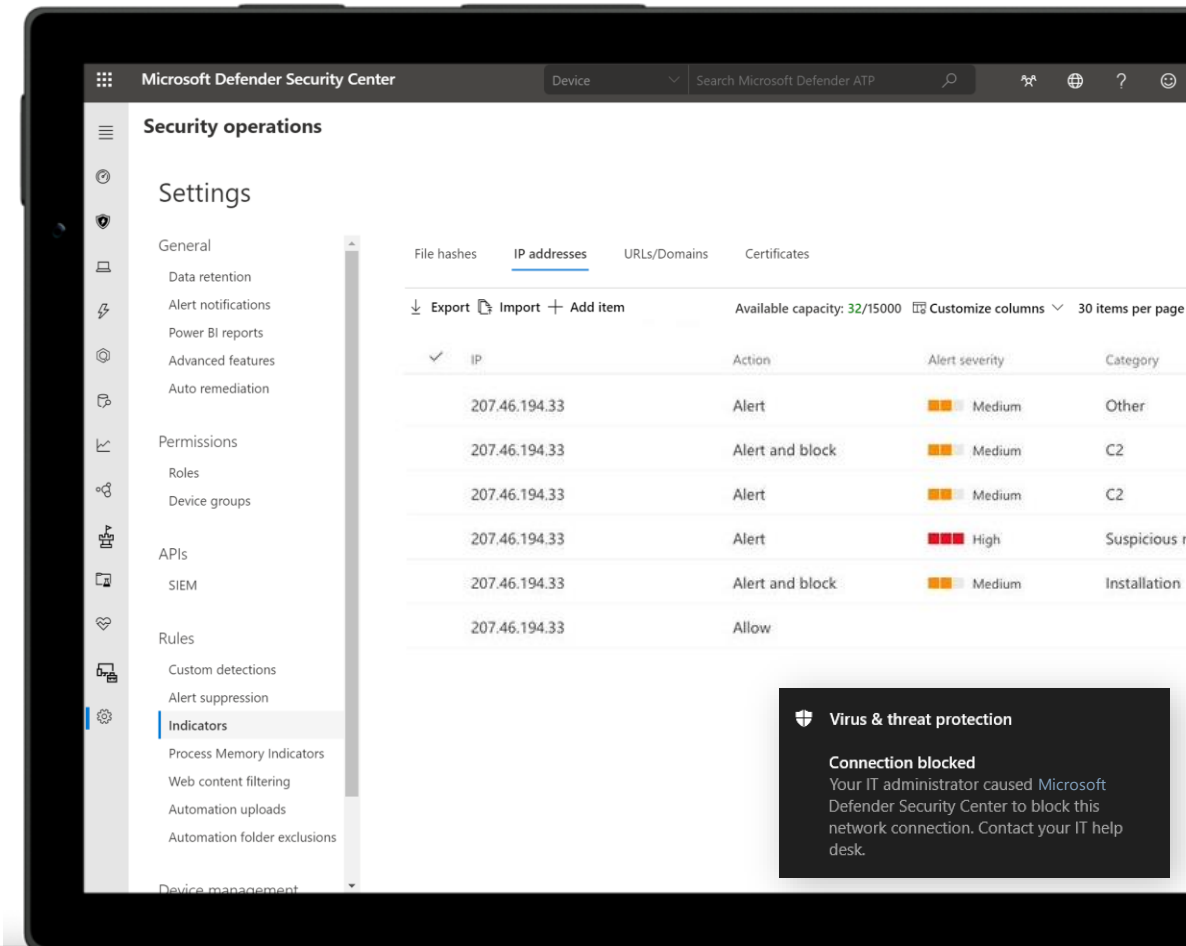
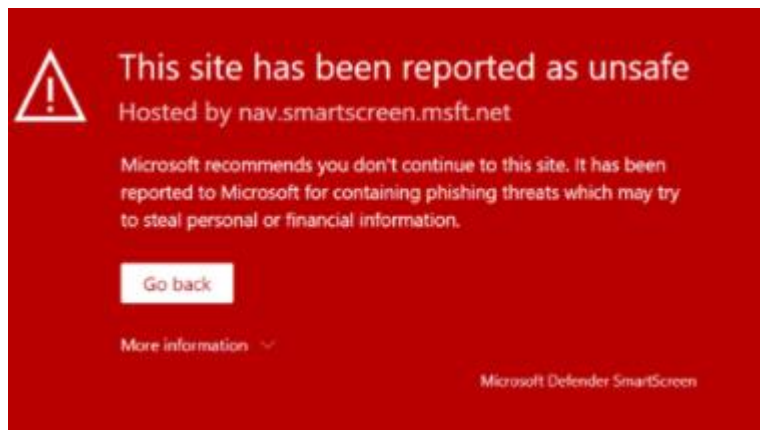
Lateral movement & credential theft

- Block process creations originating from PSEXEC and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

Network protection

Allow, audit and block

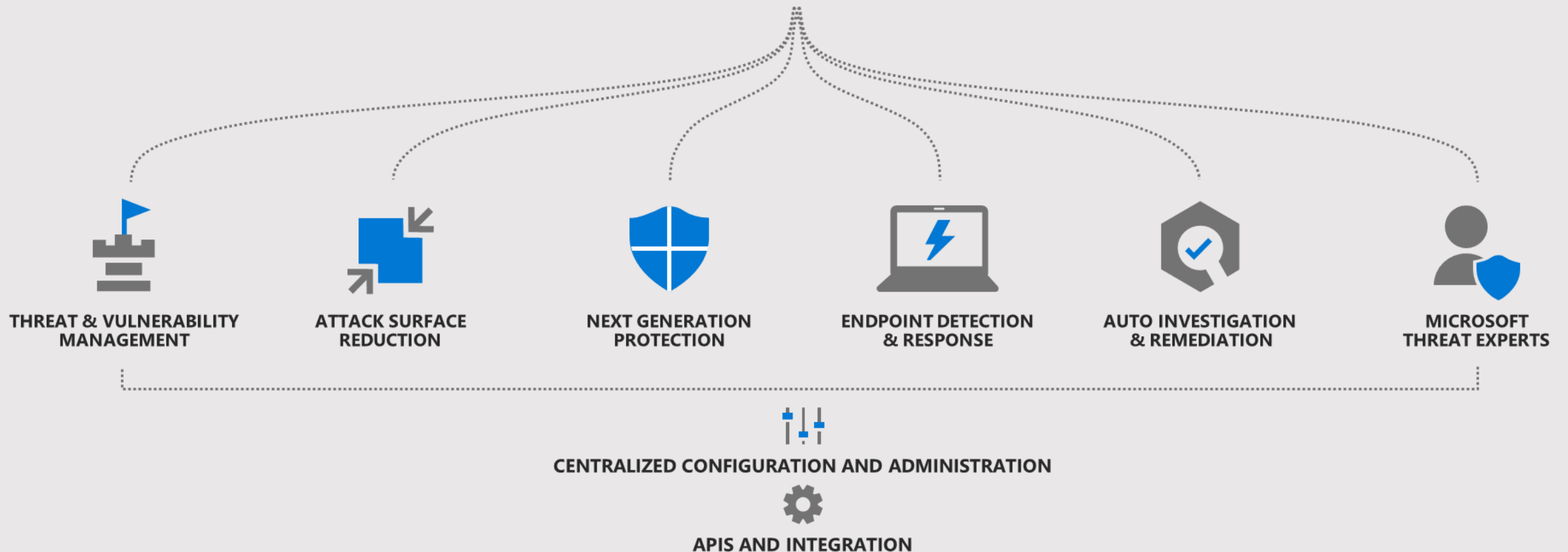
- Perimeter-less network protection ("SmartScreen in the box") preventing users from accessing malicious or suspicious network destinations, using any app on the device and not just Microsoft Edge.
- Customers can add their own TI in additional to trusting our rich reputation database.





Microsoft Defender for Endpoint

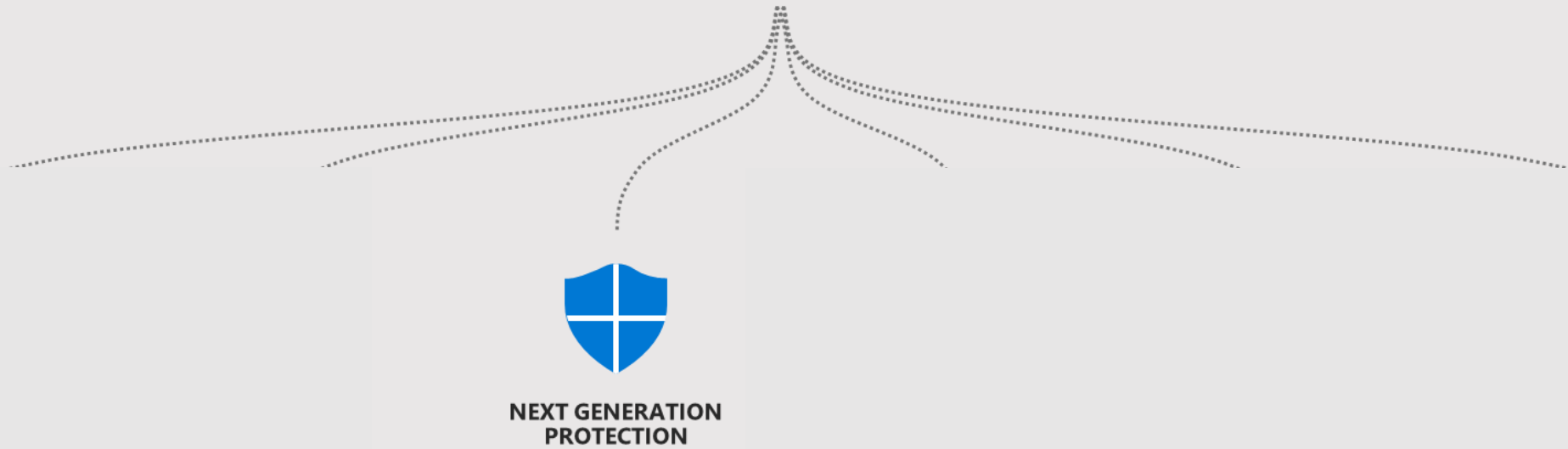
Built-in. Cloud-powered.





Microsoft Defender for Endpoint

Built-in. Cloud-powered.



Static vs Dynamic

Static signatures: focus on a file

Hashes
Strings
Emulators



Ineffective

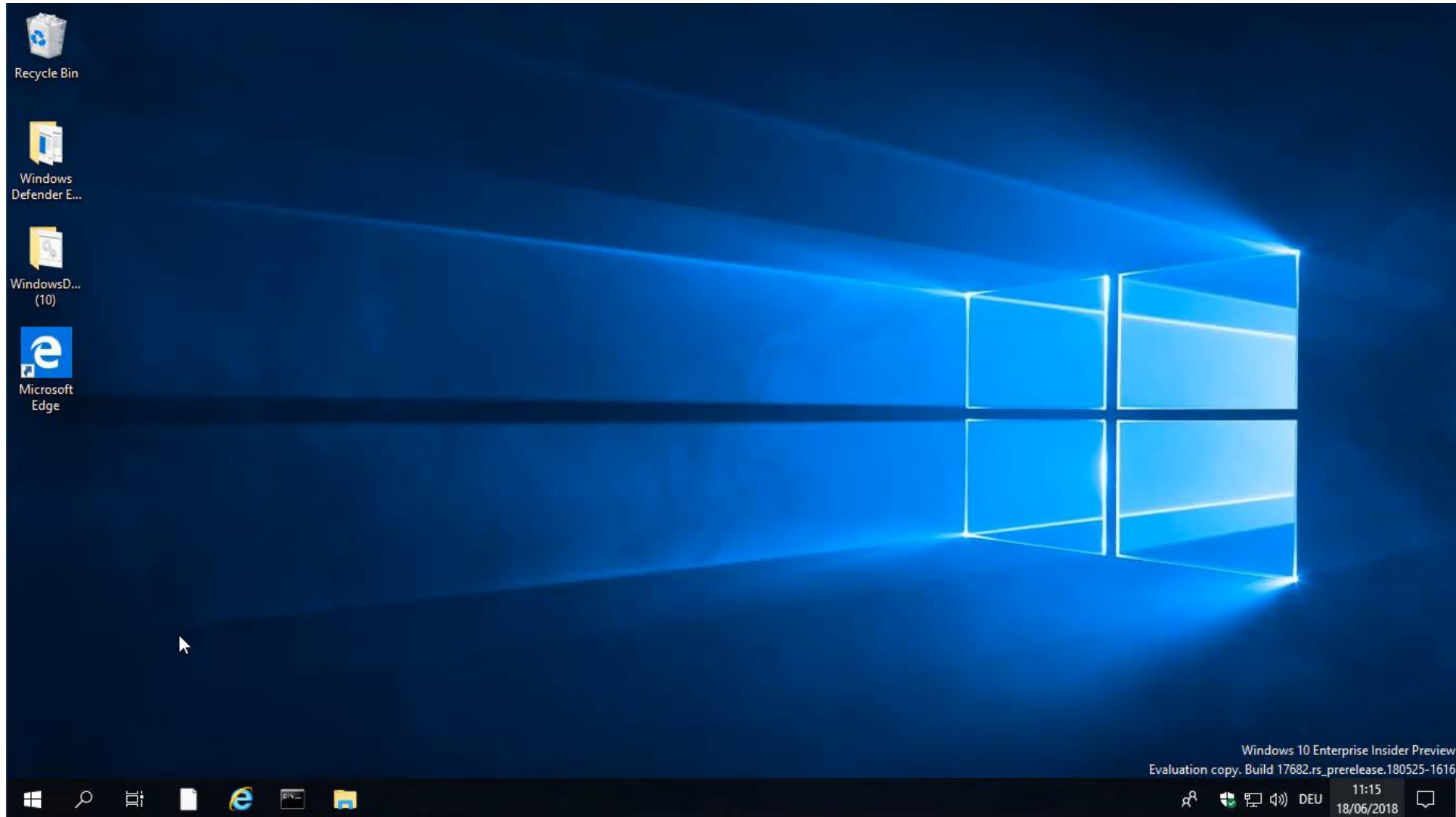
Dynamic heuristics: focus on *run-time behaviors*

Behavior monitoring
Memory scanning
AMSI
Command-line scanning



Effective

Standard AV isn't enough anymore:



The power of behaviour based detection

The screenshot displays the Windows Defender Security Center interface. The top navigation bar includes the title "Windows Defender Security Center", a search bar, and user information "captain@it-pirate.eu". The left sidebar contains icons for various security features.

The main content area shows "Security operations > vcli12". A log entry at 21:29:29 states: "Windows Defender AV detected 'Mikatz' high-severity malware". Below this, a detailed description of high-severity malware is provided.

A second log entry at 21:29:16 shows: "python.exe Access token was modified". To the right of this entry, a process flow diagram illustrates the execution of a command and subsequent actions.

The process flow diagram shows the following sequence:

- cmd.exe** (gear icon) executes the command: `cmd.exe`
- py.exe** (gear icon) is spawned by cmd.exe. Its details are:
 - Signature: Python Software Foundation
 - Path: `c:\windows\py.exe`
 - Command: `"py.exe" "C:\Exclude\mimikatz_trunk\x64\sigthief.py" -i C:\Windows\System32\consent.exe -t mimikatz.exe -o MSCredentialTool.exe`
- python.exe** (gear icon) is spawned by py.exe. Its details are:
 - Signature: Python Software Foundation
 - Path: `C:\Python36`
 - Command: `python.exe "C:\Exclude\mimikatz_trunk\x64\sigthief.py" -i C:\Windows\System32\consent.exe -t mimikatz.exe -o MSCredentialTool.exe`
- The final action is **Access token** (key icon), labeled "python.exe Access token was modified".

Next Generation Protection

Blocks and tackles sophisticated threats and malware



Behavioral based real-time protection



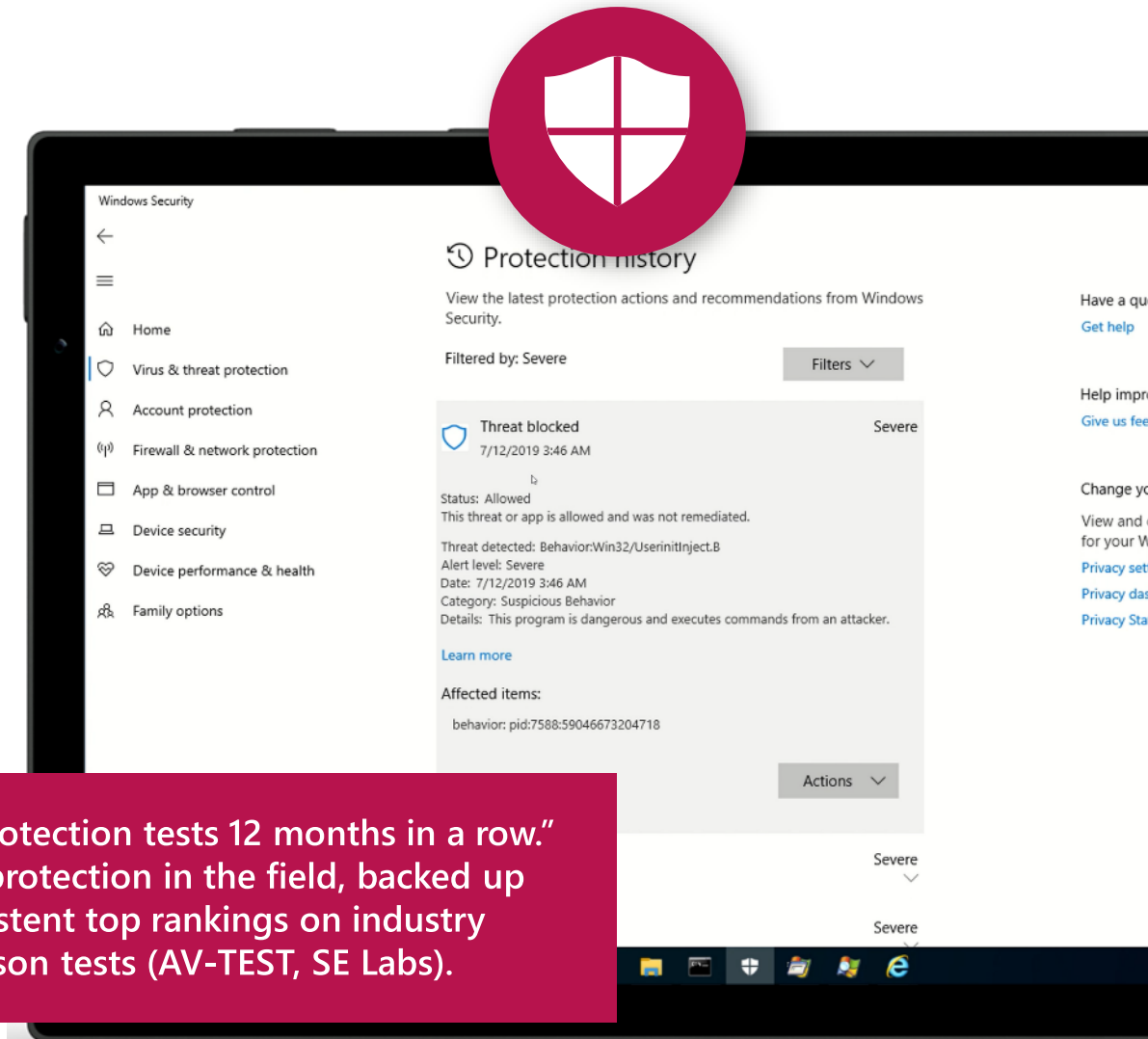
Blocks file-based and fileless malware



Stops malicious activity from trusted and untrusted applications



"Aced protection tests 12 months in a row."
Proven protection in the field, backed up
by consistent top rankings on industry
comparison tests (AV-TEST, SE Labs).



End to End Protection

PRE-BREACH

POST-BREACH

OFF MACHINE



O365 (Email)

- Reducing email attack vector
- Advanced sandbox detonation
- Exploit mitigation



Edge (Browser)

- Browser hardening
- Reduce script based attack surface
- App container hardening
- Reputation based blocking for downloads



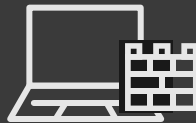
Windows Defender Exploit Guard (HIPS)

- Attack Surface Reduction**
- Set of rules to customize the attack surface
- Controlled Folder Access**
- Protecting data against access by untrusted process
- Exploit Protection**
- Mitigations against exploits
- Network Protection**
- Blocking outbound calls to low rep sources



Locked down device (Hardened platform)

- Windows 10S
- Device Guard



App Guard (Virtualized base security)

- App isolation



Application Control (Whitelist Executables)

- Only allowed apps can run

ON MACHINE



Windows Defender Antivirus (AV)

- Improved ML and heuristic protection
- Instantly protected with the cloud
- Enhanced Exploit Kit Detections



AntiMalware Scan Interface (Script based detection)

- Improved detection script based attacks
- AMSI for VBS/JS script runtime



Windows Defender Antivirus behavioral engine (Behavior Analysis)

- Enhanced behavioral and machine learning detection library
- Process tree visualizations
- Artifact searching capabilities
- Memory scanning capabilities



Microsoft Defender for Endpoint

- Enhanced behavioral and machine learning detection library
- Process tree visualizations
- Artifact searching capabilities
- Machine Isolation and quarantine



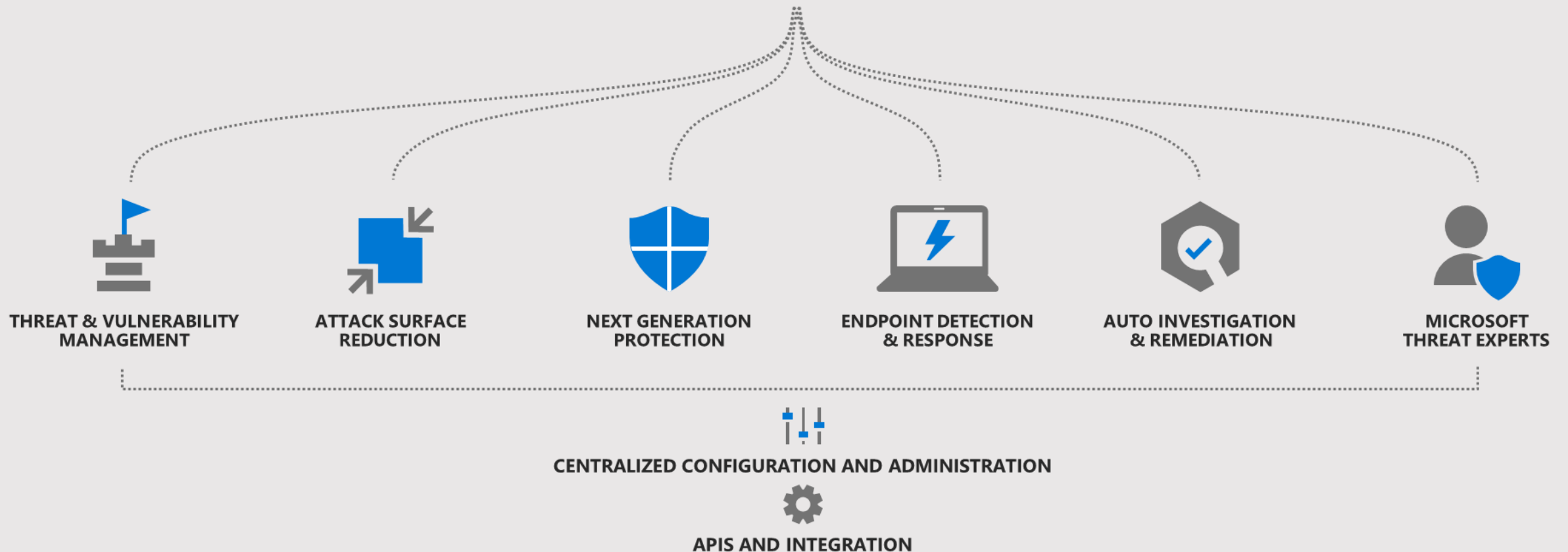
One Drive (Cloud Storage)

- Reliable versioned file storage in the cloud
- Point in time file recovery



Microsoft Defender for Endpoint

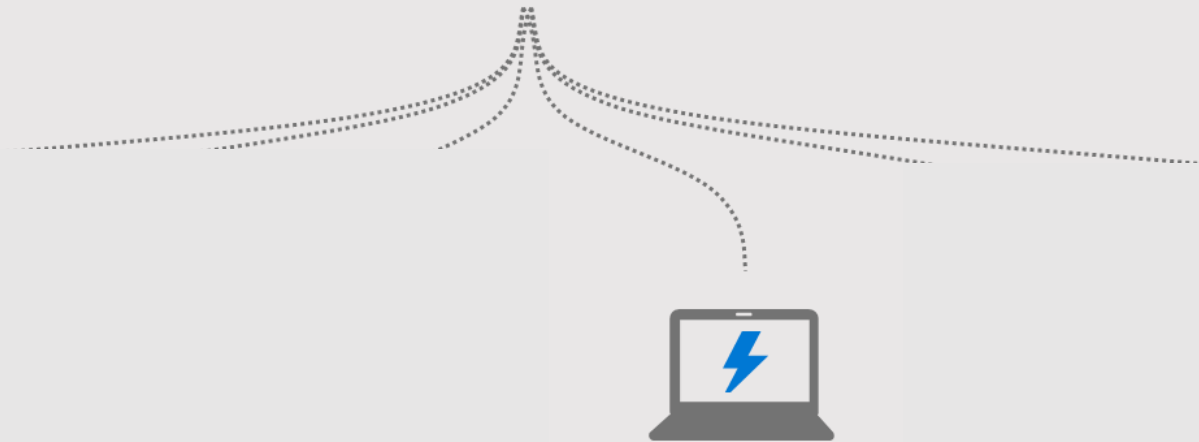
Built-in. Cloud-powered.





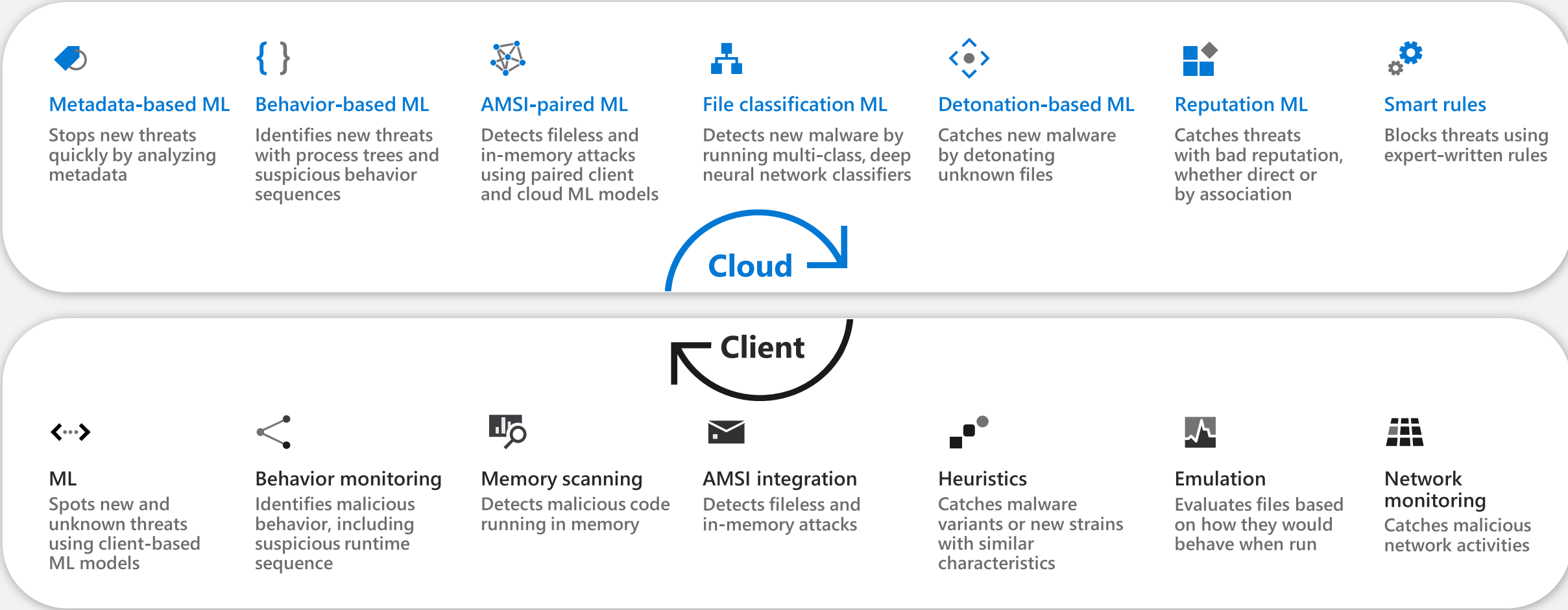
Microsoft Defender for Endpoint

Built-in. Cloud-powered.



ENDPOINT DETECTION
& RESPONSE

Microsoft Defender for Endpoint next generation protection engines



Innovations in Fileless Protection

- Dynamic and in context URL analysis to block call to malicious URL
- AMSI-paired machine learning uses pairs of client-side and cloud-side models that integrate with Antimalware Scan Interface ([AMSI](#)) to perform advanced analysis of scripting behavior
- DNS exfiltration analysis
- Deep memory analysis



Endpoint Detection & Response



Correlated post-breach detection

Investigation experience

Incident

Advanced hunting

Response actions (+EDR blocks)

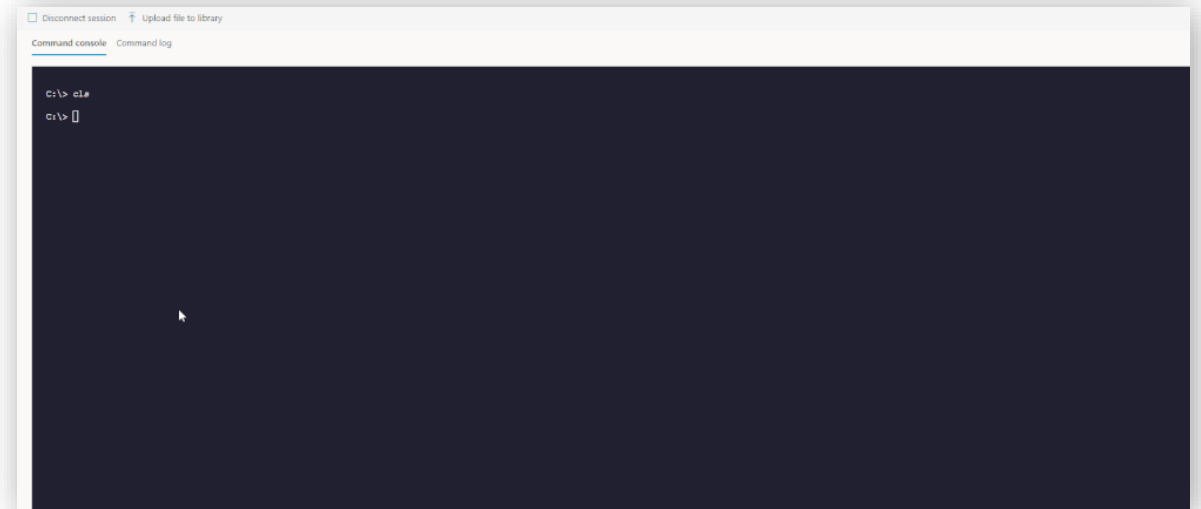
Deep file analysis

Live response

Threat analytics

Live Response

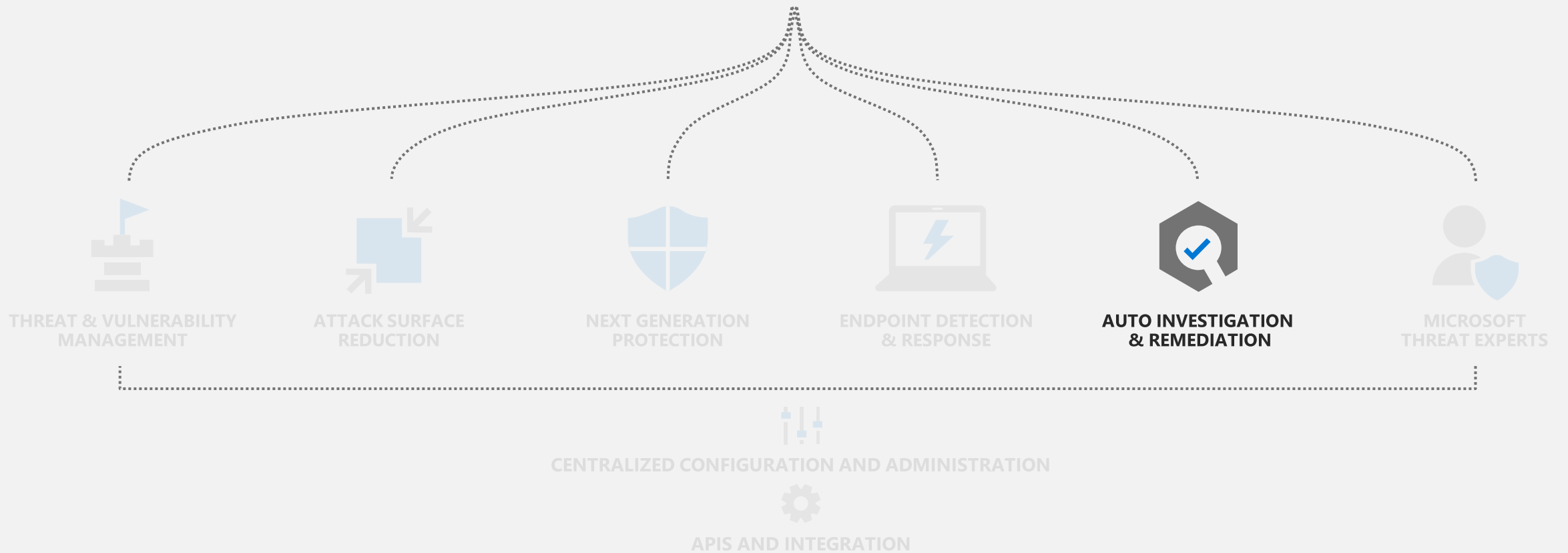
- Real-time live connection to a remote system
- Leverage Microsoft Defender for Endpoint Auto IR library (memory dump, MFT analysis, raw filesystem access, etc.)
 - Extended remediation command + easy undo
- Full audit
- Extendable (write your own command, build your own tool)
- RBAC+ Permissions
- Git-Repo (share your tools)





Microsoft Defender for Endpoint

Built-in. Cloud-powered.



What Is Microsoft Defender for Endpoint Auto IR?

Security automation is...

mimicking the ideal steps a human would take to investigate and remediate a cyber threat



Security automation is not...

if machine has alert → auto-isolate



When we look at the steps an analyst is taking as when investigating and remediating threats we can identify the following high-level steps:

1

Determining whether the threat requires action

2

Performing necessary remediation actions

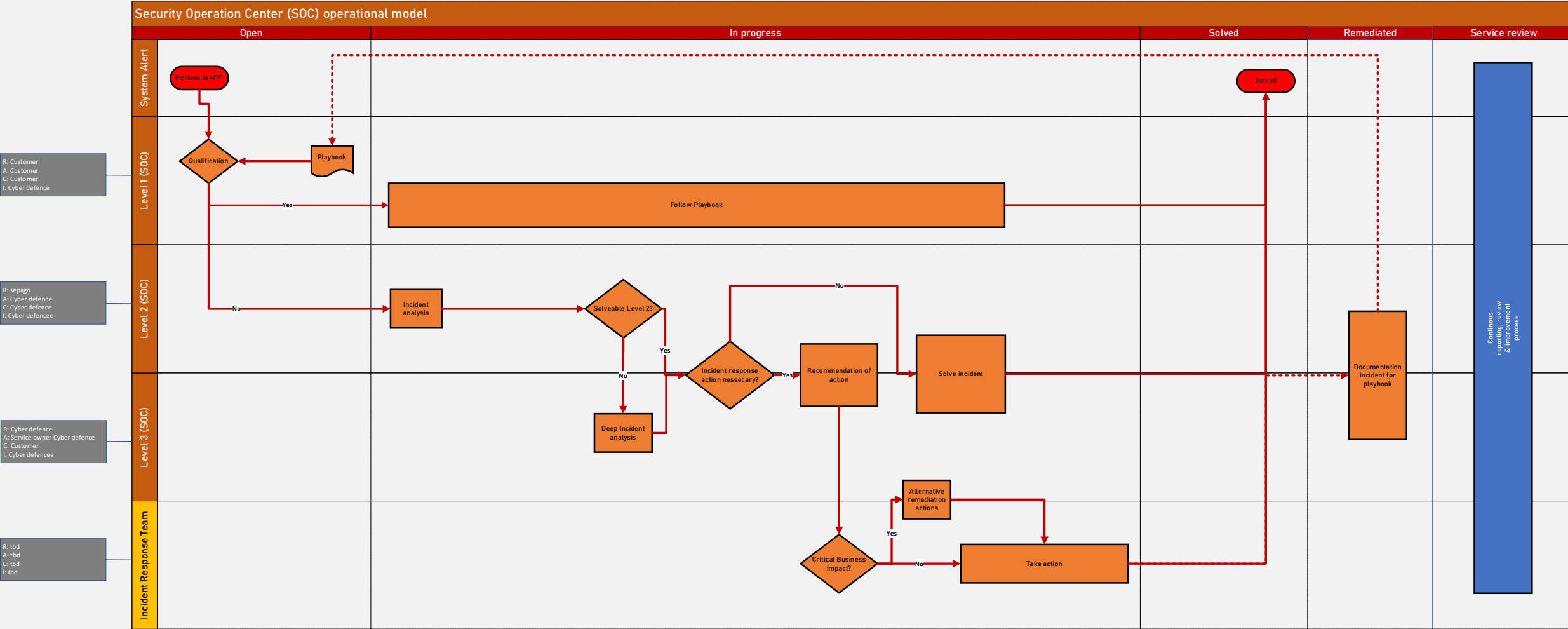
3

Deciding what additional investigations should be next

4

Repeating this as many times as necessary for every alert 😊

Blue Print Layer I: High Level



Grundsätze des RACI Modells

R	Wer ist für die Ausführung der Aufgabe verantwortlich?
A	Wer nimmt die Aufgabe ab und trägt die Verantwortung?
C	Wer steht beratend/unterstützend zur Seite?
I	Wer wird über die Ergebnisse informiert?

Principals of the RACI model

<u>R</u> esponsible	R			
<u>A</u> ccountable		A		
<u>C</u> onsulted			C	
<u>I</u> nformed				I

Blue Print Layer II: Action Items

Workstream Constitutional - Action Items	Median time/Incident	LVL1	LVL2	LVL3	SecSME	SocTL	SDM	SecEng	IR	SME	CISO
Phase: Open											
Incident in MDATP	0										
Check incident monitoring automation		R			A		C				
Monitor incident queue		R			A						
Decision: Qualification	10										
Assign incident to relevant Analyst		R	C		A						
Check for existing documentation in playbook		R	C		A						
If existing documentation in playbook: Follow-playbook		R	C		A						
If not existing documentation in playbook: Fill ticket template: Incident analysis		R	I		A						
Phase: In progress											
Follow-playbook (if existing documentation in playbook)	5										
Open playbook		R			A						
Search for incident category		R	C		A						
Follow playbook instructions		R	C		A						

Blue Print Layer III: Step by Step (runbooks)

To ensure **consistent quality** in the handling of security incidents, **standardized documentation** must be implemented.

This provides **step-by-step instructions** so that all security analysts - **regardless of their personal background and experience** - choose the same procedures and escalation levels.

3	PLAYBOOK
3.1	BACKDOOR
3.2	COLLECTION
3.3	COMMAND AND CONTROL
3.4	CREDENTIAL ACCESS
3.5	CREDENTIAL STEALING
3.6	CREDENTIAL THEFT
3.7	DEFENSE EVASION
3.8	DELIVERY
3.9	DISCOVERY
3.10	DOCUMENT EXPLOIT
3.11	ENTERPRISE POLICY
3.12	EXECUTION
3.13	EXFILTRATION
3.14	EXPLOIT
3.15	GENERAL
3.16	INITIAL ACCESS
3.16.1	SUSPICIOUS CONNECTION BLOCKED BY NETWORK PROTECTION
3.17	INSTALLATION
3.18	LATERAL MOVEMENT
3.19	MALWARE
3.19.1	'MIMIKATZ' HACKTOOL WAS DETECTED
3.20	MALWARE DOWNLOAD
3.21	NETWORK PROPAGATION
3.22	PERSISTENCE
3.23	PRIVILEGE ESCALATION
3.24	RANSOMWARE
3.25	RECONNAISSANCE
3.26	REMOTE ACCESS TOOL
3.27	SOCIAL ENGINEERING
3.28	SUSPICIOUS ACTIVITY

3.30.1 "XYZ" Detected on Endpoint & MDATP detected "XYZ" Trojan (Nearly any Trojan Related Incident)

Severity:	Informational to Medium
Detection Source:	AV, MDATP
Detection Status:	Detected/Prevented

Analysis:

This type of alerts usually has a severity of "Informational" or "Low". This is because the malicious file was detected stored on the local drive. Normally the timeline of the device states "remediated successfully" or "Prevented". Hence, the first check is to click in the Alert-View on "See in Timeline". If the detected file has a green entry "Remediated successfully" or "Prevented" detection status meaning the Windows Defender already remediated the threat.

Remediation:

If the timeline states "Remediation failed" or just "Detected" detection status, the device potentially disconnected before the remediation could be registered. Go to the detected file view and use the "Block & Quarantine" action if the machine is a windows machine. If machine is a non-windows machine or "Block & Quarantine" feature does not work on the platform, use the Add Indicator option with the "Alert & Block" option. This will prevent the file from execution.

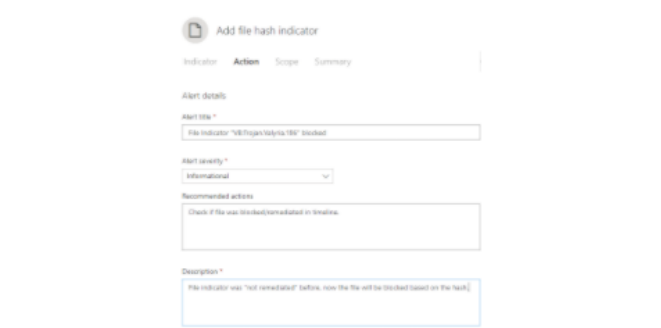


Figure 1: File indicator "Alert&Block" for non win10 machines

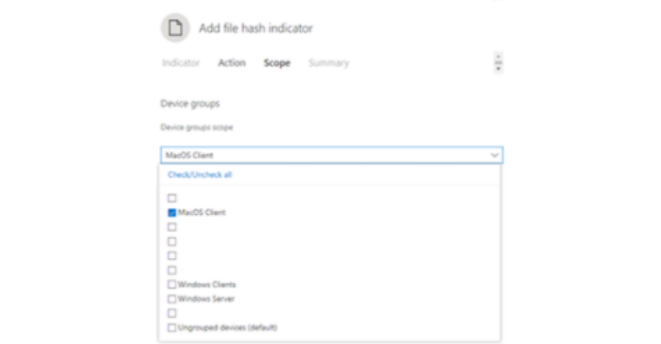


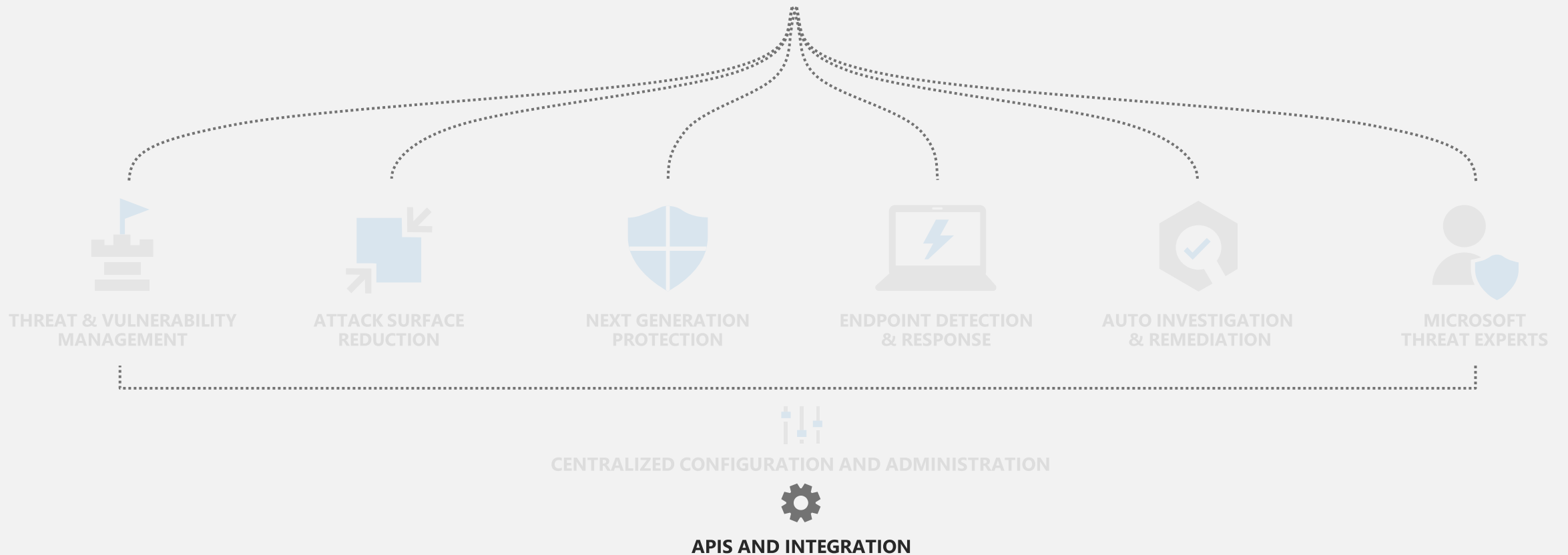
Figure 2: Scope of action

Should the file be blocked on all machines or only on the OS it was detected? For now only scope the Indicators on the OS, where the alert came up. Block on all OS -> could lead to more alerts than needed



Microsoft Defender for Endpoint

Built-in. Cloud-powered.

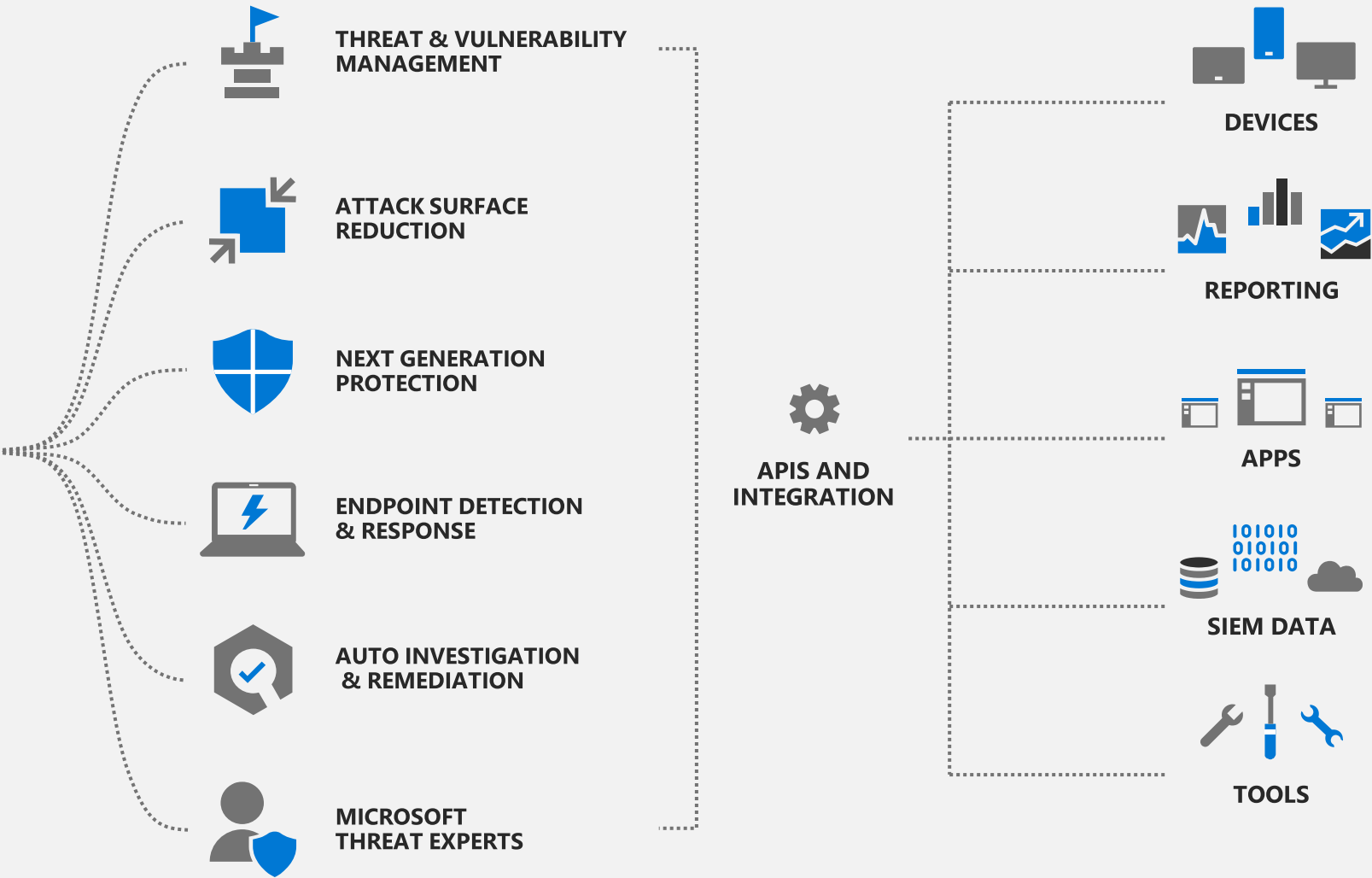


Connecting with the platform



Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Insights!

Threat and Vulnerability Management

Devices

70

Exposed Devices

58

CVEs in my org

1758

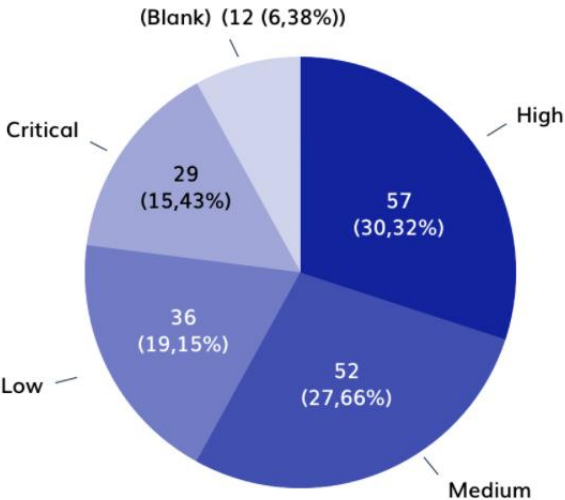
High Severity Devices

57

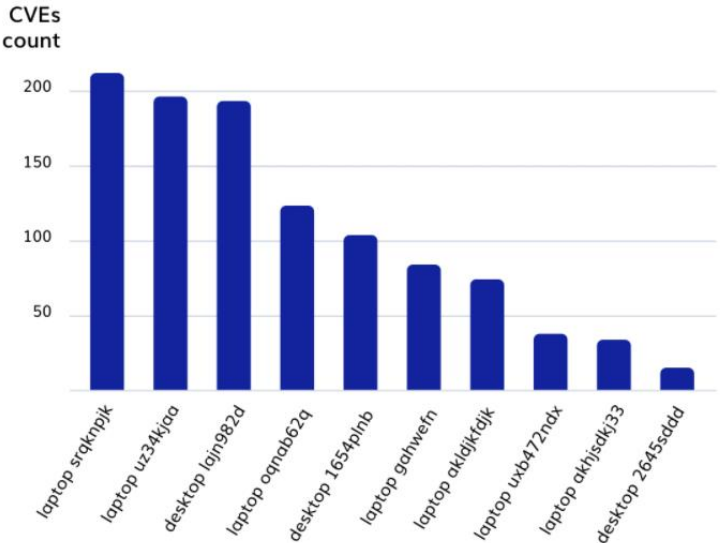
Critical Devices

29

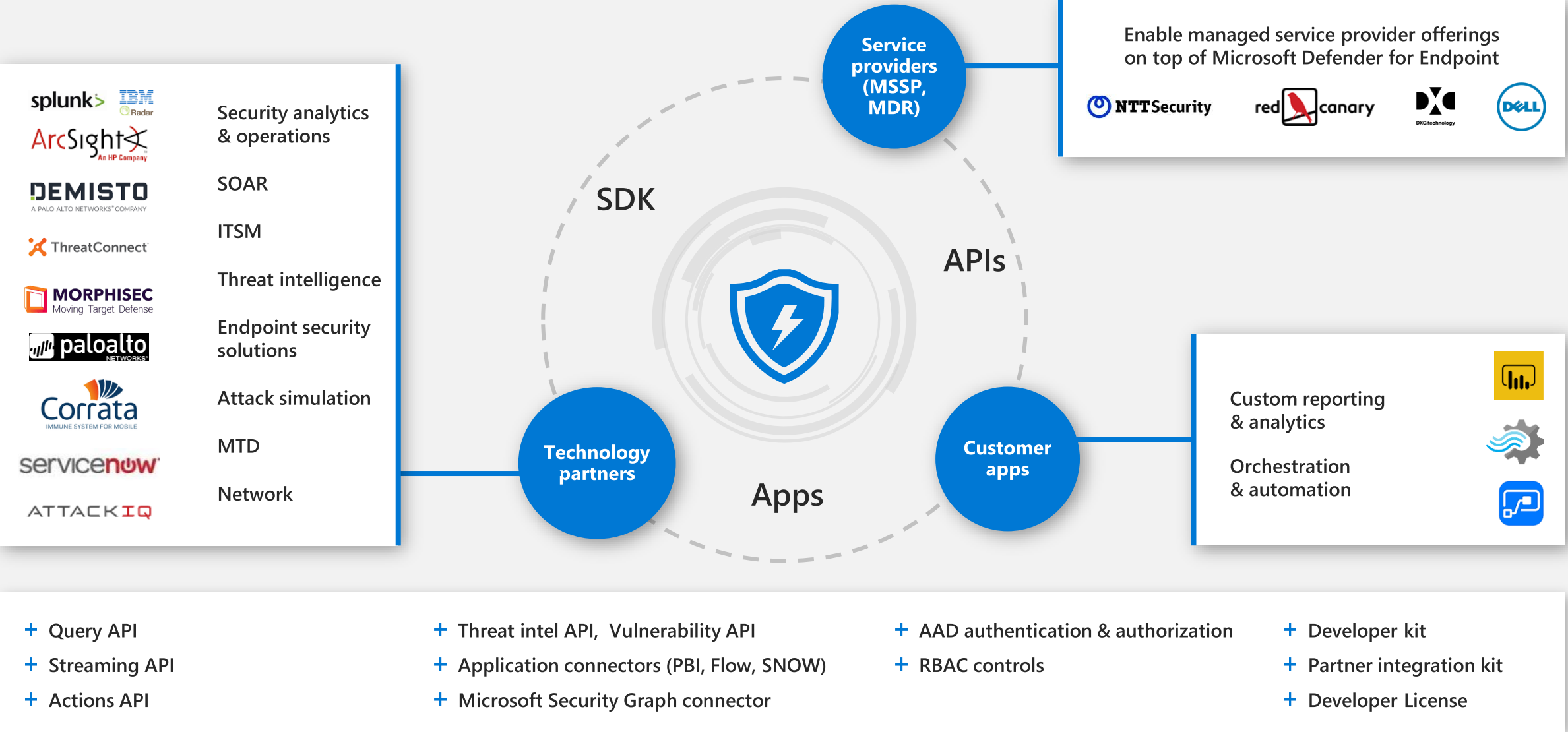
Number of devices with vulnerabilities by severity level



Top 10 of the most attacked devices



Microsoft Defender for Endpoint through ecosystem & API



Microsoft Defender for Endpoint APIs & partners

Easy development & tracking of connected solutions

API Explorer

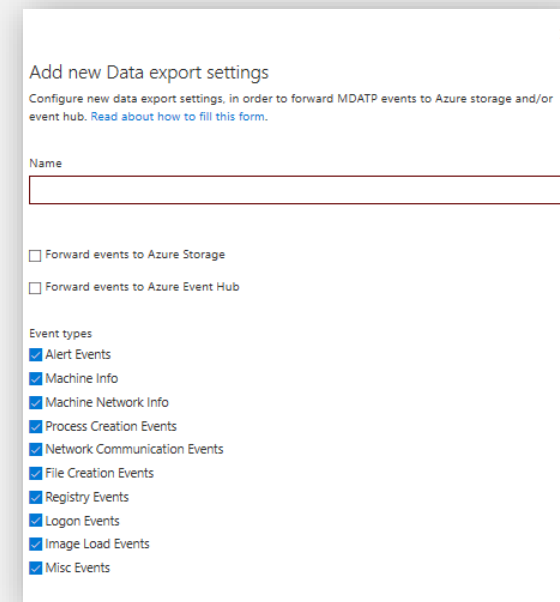
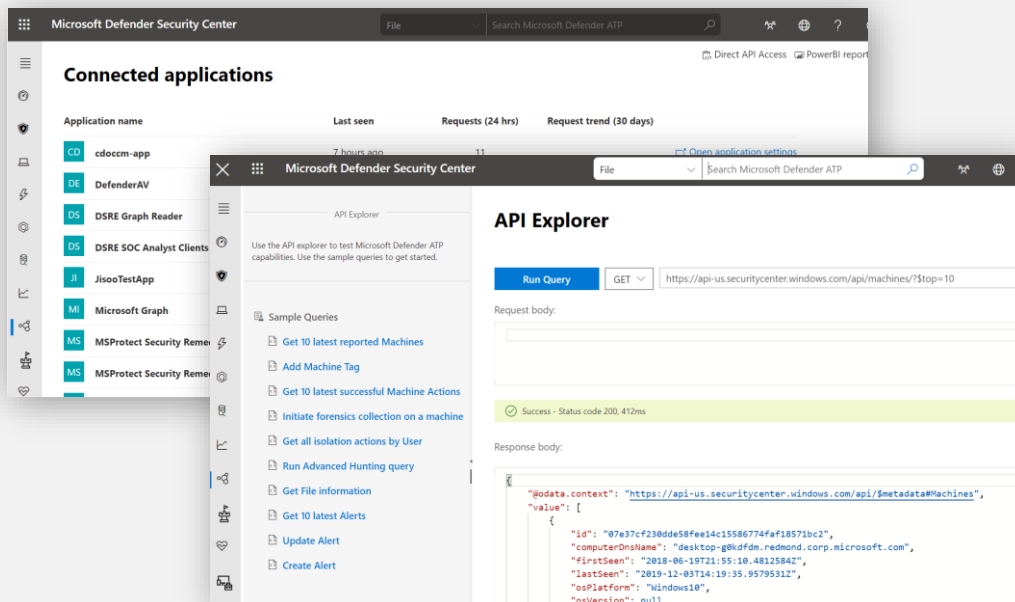
- Explore various Microsoft Defender for Endpoint APIs interactively

Integrated compliance assessment

- Track apps that integrates with Microsoft Defender for Endpoint platform in your organization.

Data Export API

- Configure Microsoft Defender for Endpoint to stream Advanced Hunting events to your storage account

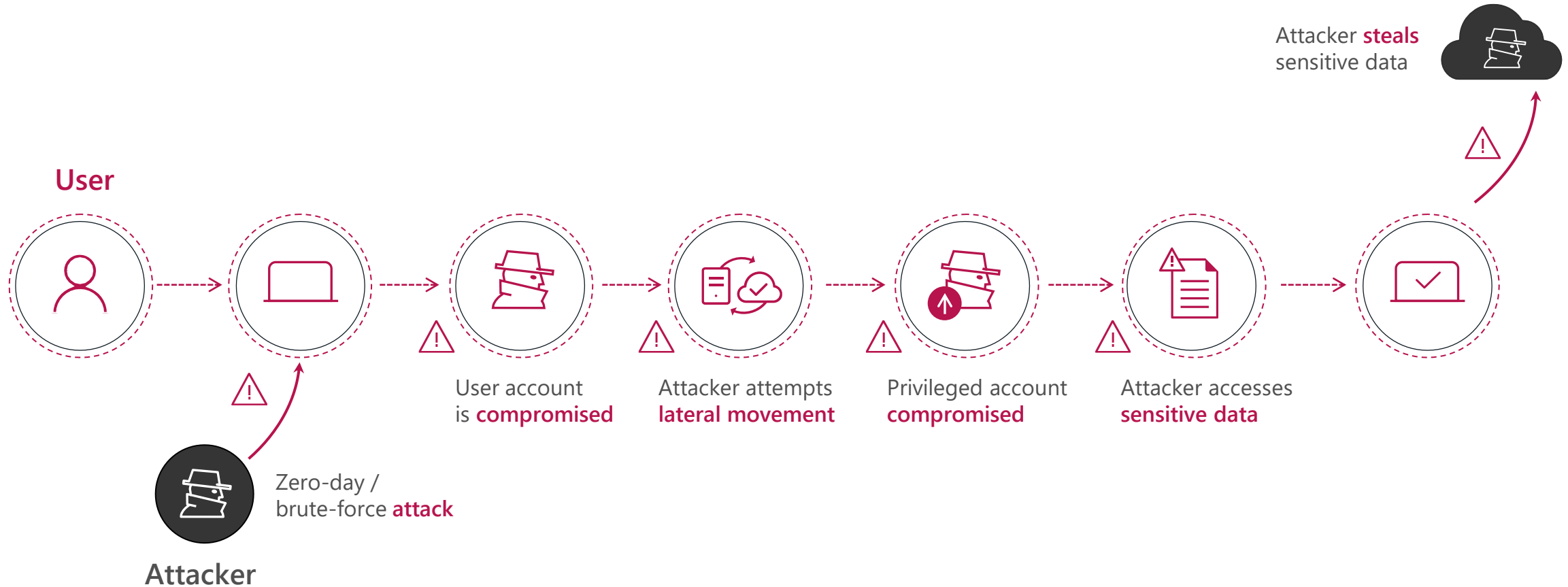


dinext.
pi-sec GmbH

Microsoft Defender for
Identity



The anatomy of an attack



Anomalous user behavior
Unfamiliar sign-in location

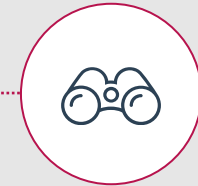


Lateral movement attacks
Escalation of privileges
Account impersonation

How do I detect **compromised credentials**?



How do I **detect attackers** moving laterally in my environment?



How do I **detect Pass-the-Hash? Pass-the-Ticket?**



Aren't **rule-based security solutions** enough?



Benefit from the **scale of the cloud**

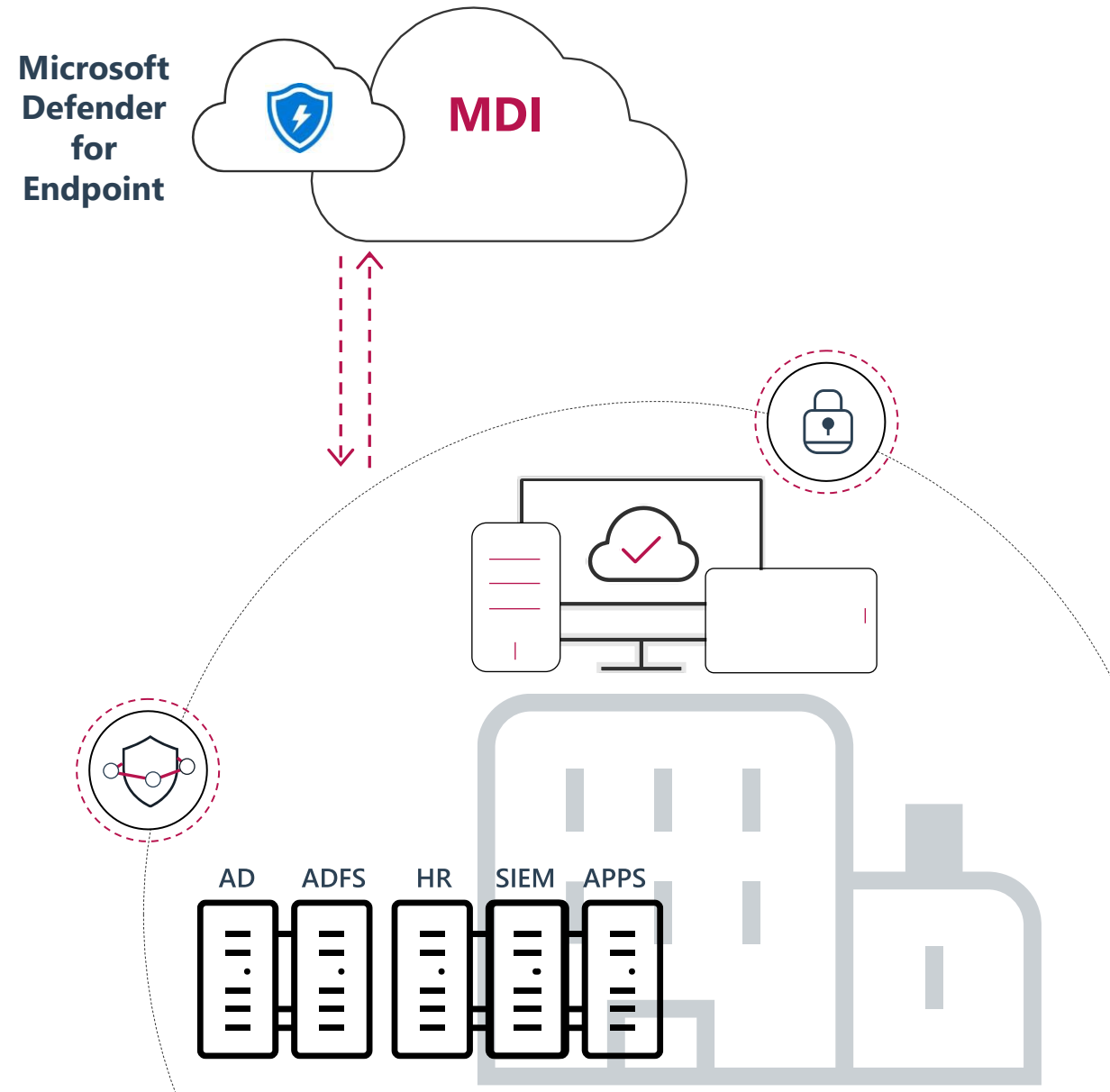
Monitor your **on-premises Active Directory** with a convenient cloud service

Reduce strain and cost in your on-premises environment with **analytics done in the cloud**

Scale your anomalous behavior detections with the power of the cloud

Pivot to and remediate a malicious attack in Microsoft Defender for Endpoint

Deploy with ease into your existing infrastructure



Microsoft Defender for Identity Profile Timeline



Jeff Victim

+ New

Email

JeffV@contoso.com

Office

Microsoft Way Re...

Phone

1-425-93-MSPHONE

First seen

Feb 20, 2018

Domain

contoso.com

Created on

Feb 7, 2018

SAM name

JeffV

4

3

ACTIVITIES

DIRECTORY DATA

Showing latest 100 distinct entities

4

Open security alerts

0

Logged on computers

0

Accessed resources

0

Accessed VPN locations

Go to

Filter by

Download activities

Today

11:09 AM

Phone number was changed from None to 1-425-93-MSPHONE

11:09 AM

Mail address was changed from None to JeffV@contoso.com

Wednesday

8:11 PM

Kerberos Golden Ticket activity

Suspicious usage of Jeff Victim's Kerberos ticket, indicating a potential Golden Ticket attack, was detected.

Started at 9:00 AM Feb 21, 2018

OPEN

Tuesday

8:56 PM

Replicated Directory Services data from VICTIM-PC

using Drsr | VICTIM-PC: 192.168.0.6

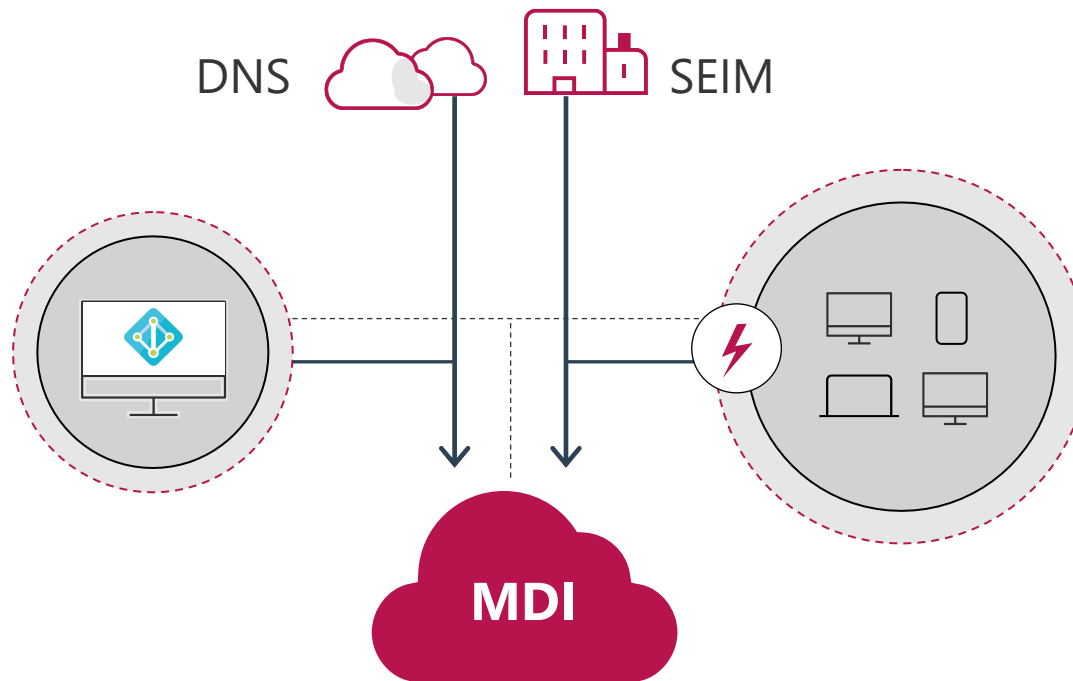
8:56 PM

Malicious replication of directory services

Malicious replication requests were successfully performed by Jeff Victim from VICTIM-PC against

OPEN

How Microsoft Defender for Identity works

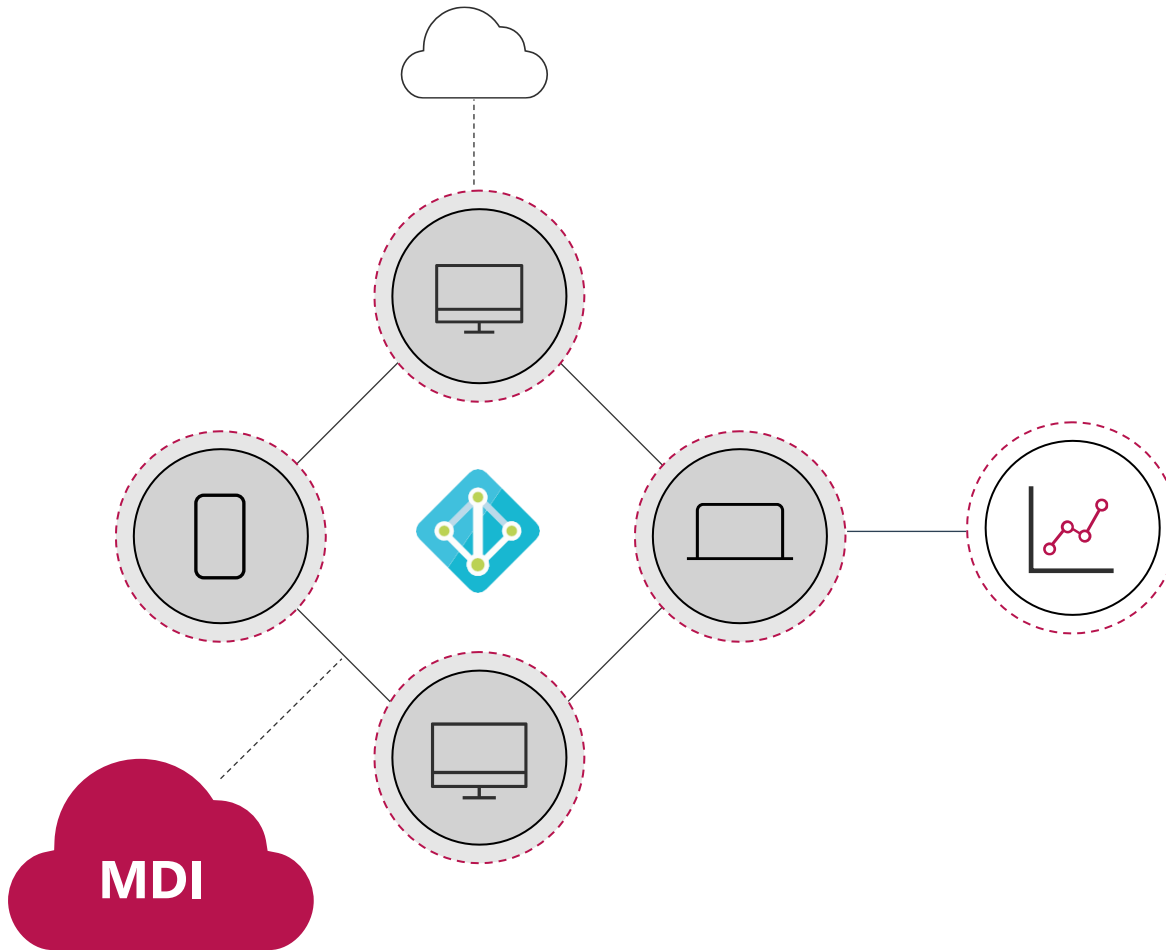


1. Collect

After installation:

- Deployed directly onto domain controllers or non-intrusive port mirroring
- Analyzes all Active Directory network traffic
- Collects relevant events from SIEM and information from Active Directory (titles, groups membership, and more)

How Microsoft Defender for Identity works



2. Analyze and Learn

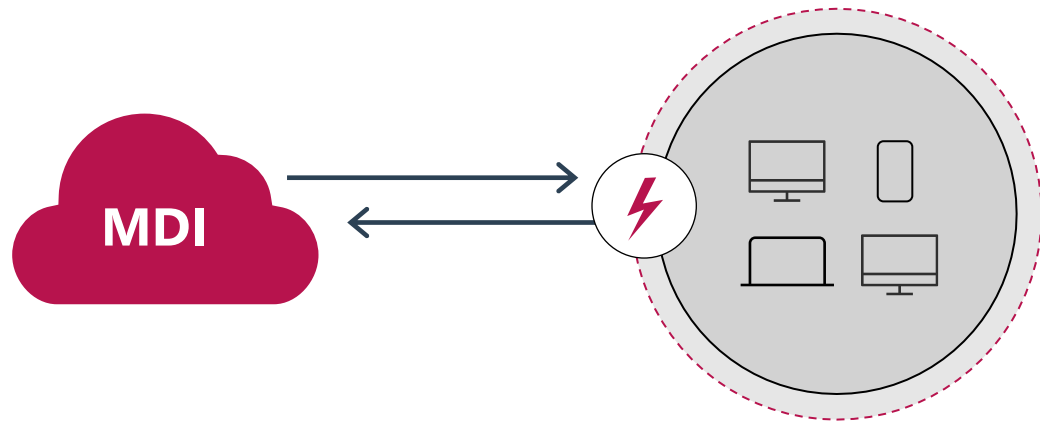
Microsoft Defender for Identity:

- Protect at scale with the power of Azure
- Automatically starts learning and profiling entity behavior
- Identifies normal behavior for entities
- Patented IP name resolution mechanism
- Learns continuously to update the activities of the users, devices, and resources

What is an entity?

Entity represents users, devices, or resources

How Microsoft Defender for Identity works



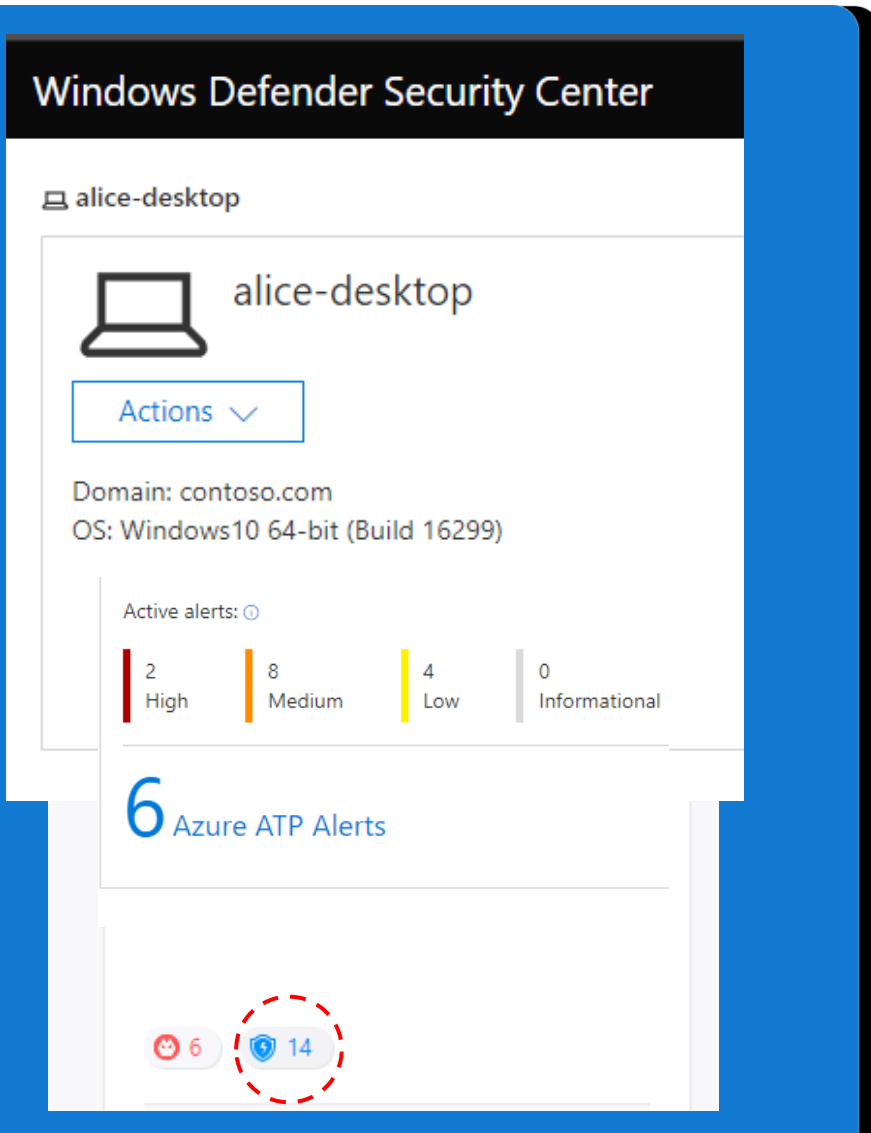
3. Detect

Microsoft Defender for Identity:

- Looks for abnormal behavior and identifies suspicious activities
- Only raises red flags if abnormal activities are contextually aggregated
- Leverages world-class security research to detect security risks and attacks in near real-time based on attackers Tactics, Techniques, and Procedures (TTPs)

MDI not only compares the entity's behavior to its own, but also to the behavior of entities in its interaction path.

How Microsoft Defender for Identity works

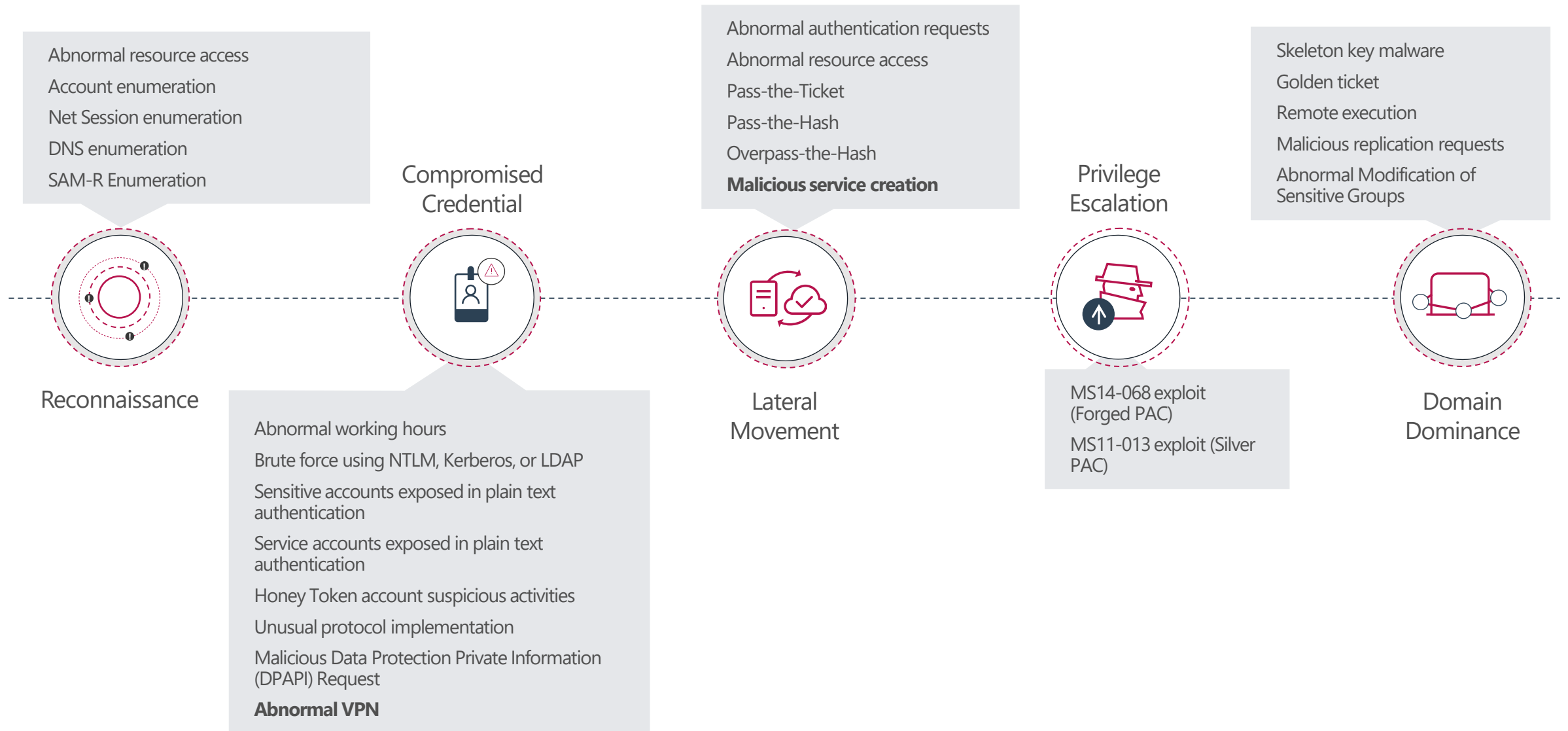


4. Alert & Investigate

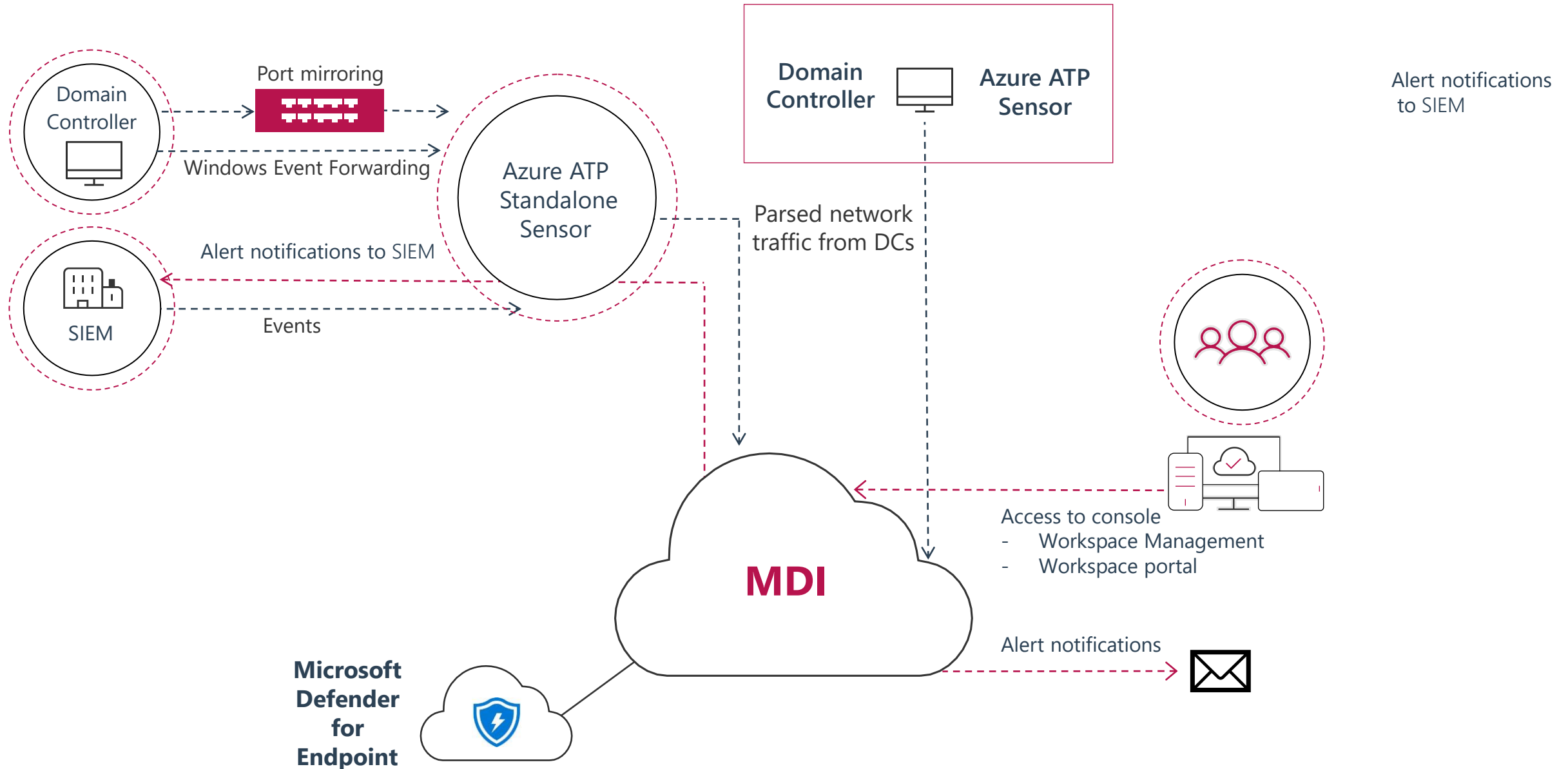
Microsoft Defender for Identity:

- Reports all suspicious activities on a **simple, functional, actionable** attack timeline
- Identifies **Who? What? When? How?**
- For each suspicious activity, provides **detailed information** for the investigation and remediation

MDI detects a wide range of suspicious activities



Microsoft Defender for Identity Architecture



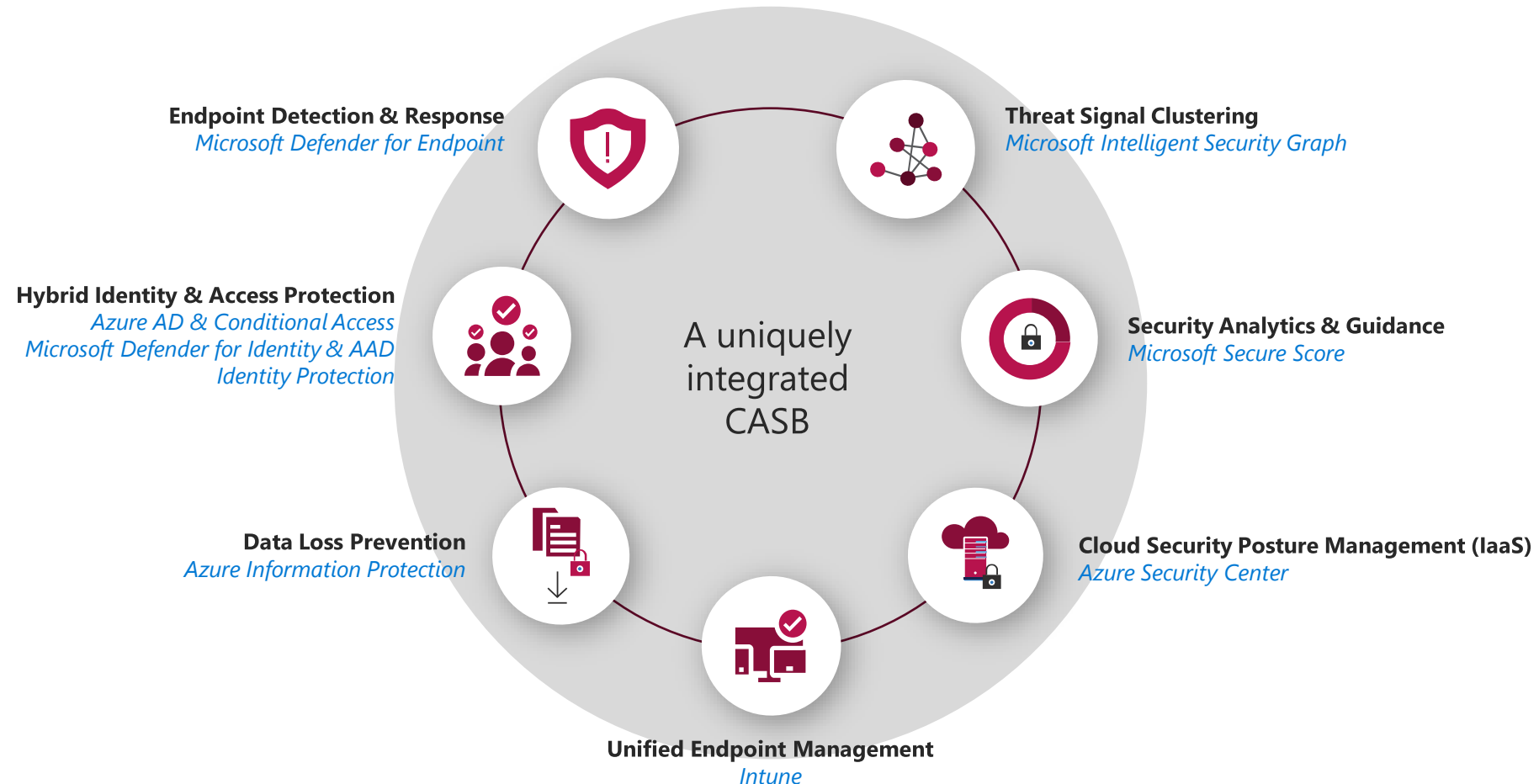
dine^xt.
pi-sec GmbH

Microsoft Cloud App
Security

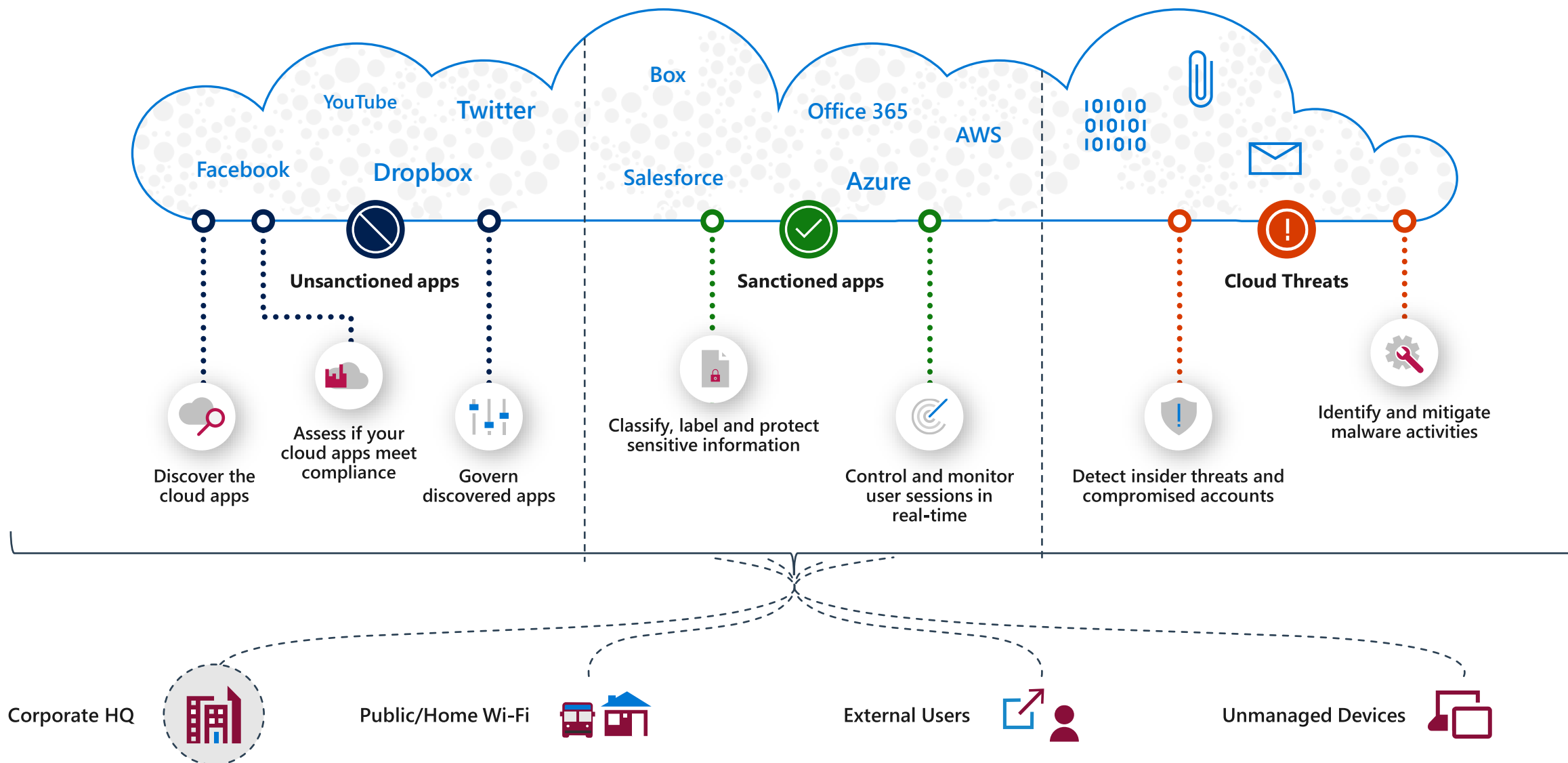


MICROSOFT CLOUD APP SECURITY

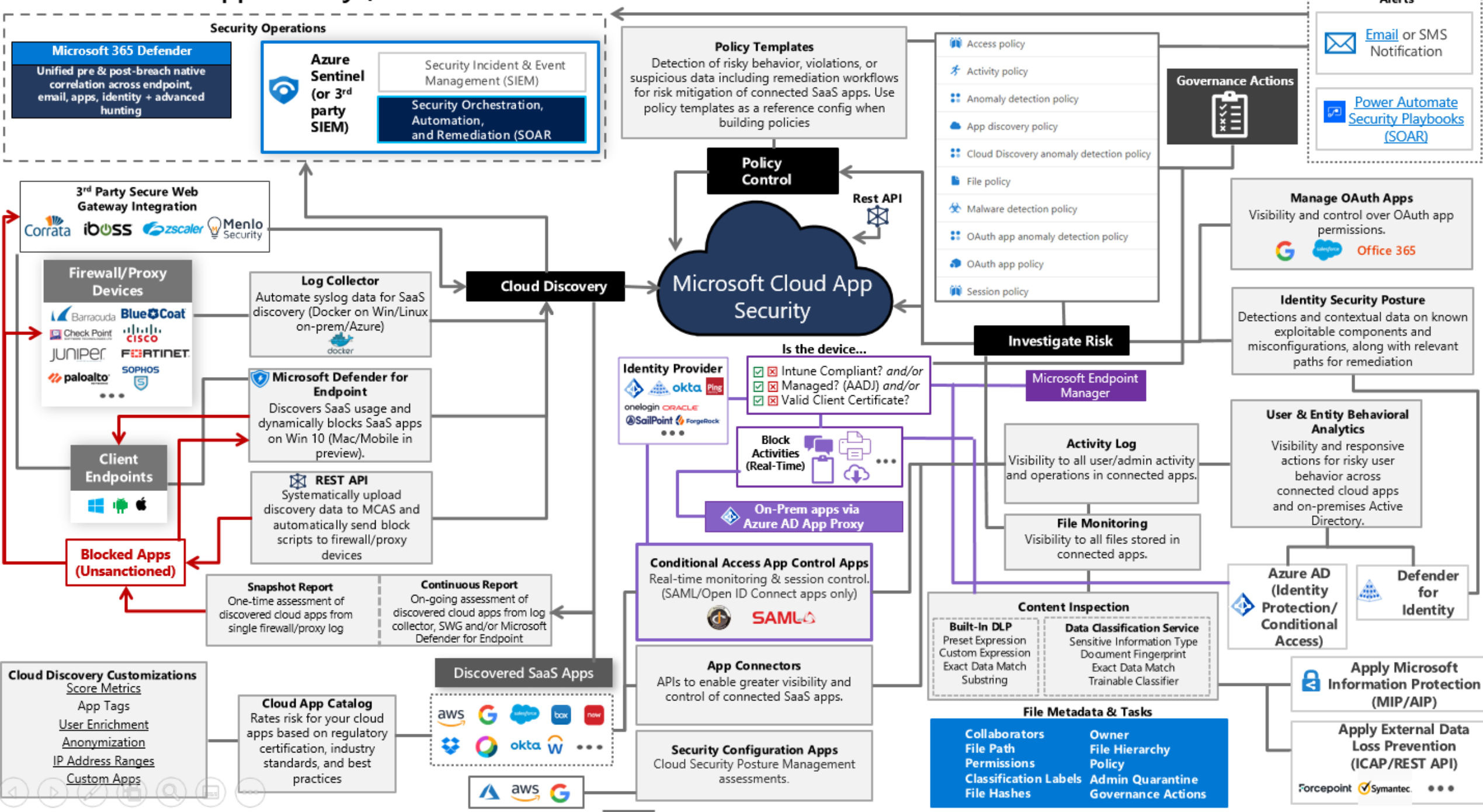
Elevate the security for all your cloud apps and services



MCAS



Microsoft Cloud App Security (DRAFT – AUTHOR MATT SOSEMAN *Reference Architecture*)



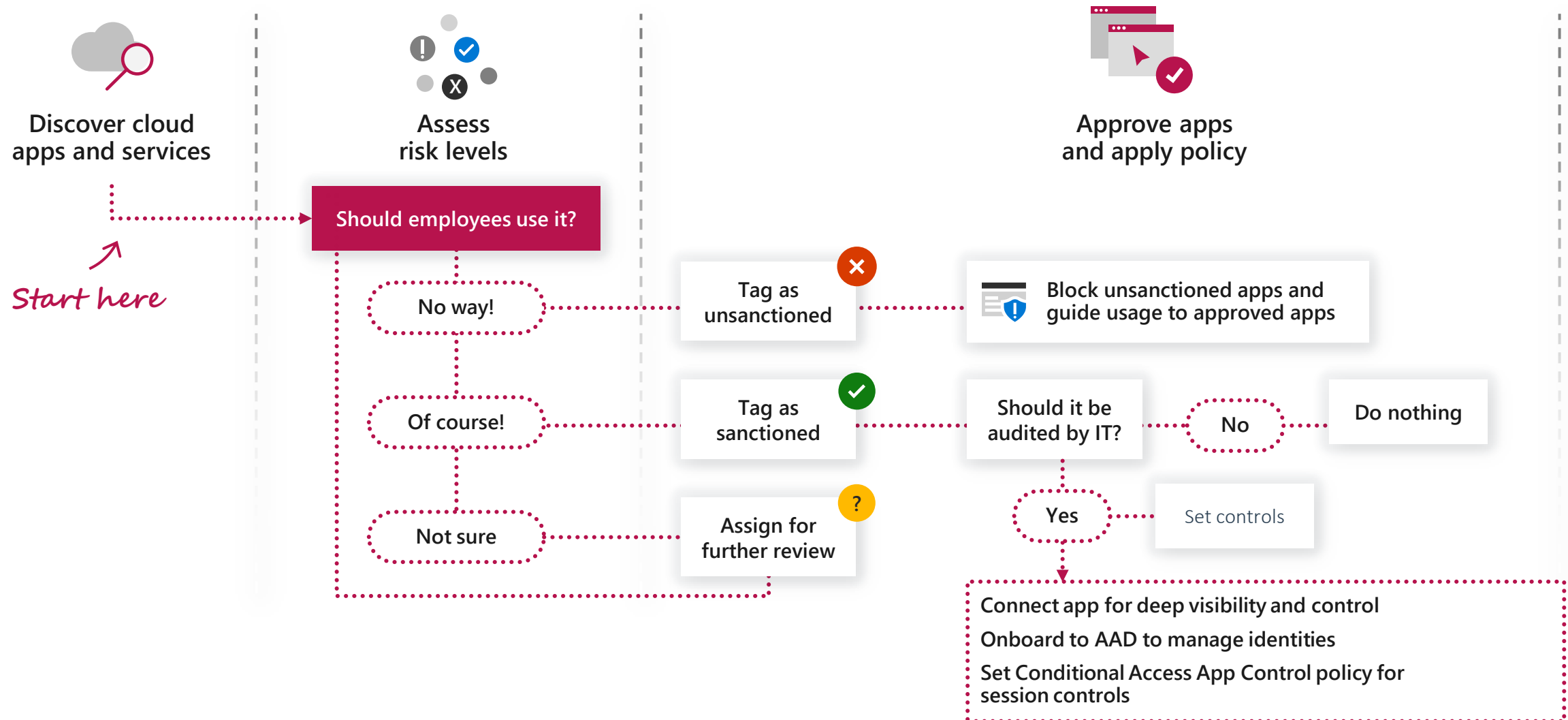


Shadow IT discovery identifies cloud apps, provides risk assessments, usage analytics and app lifecycle management and control capabilities.

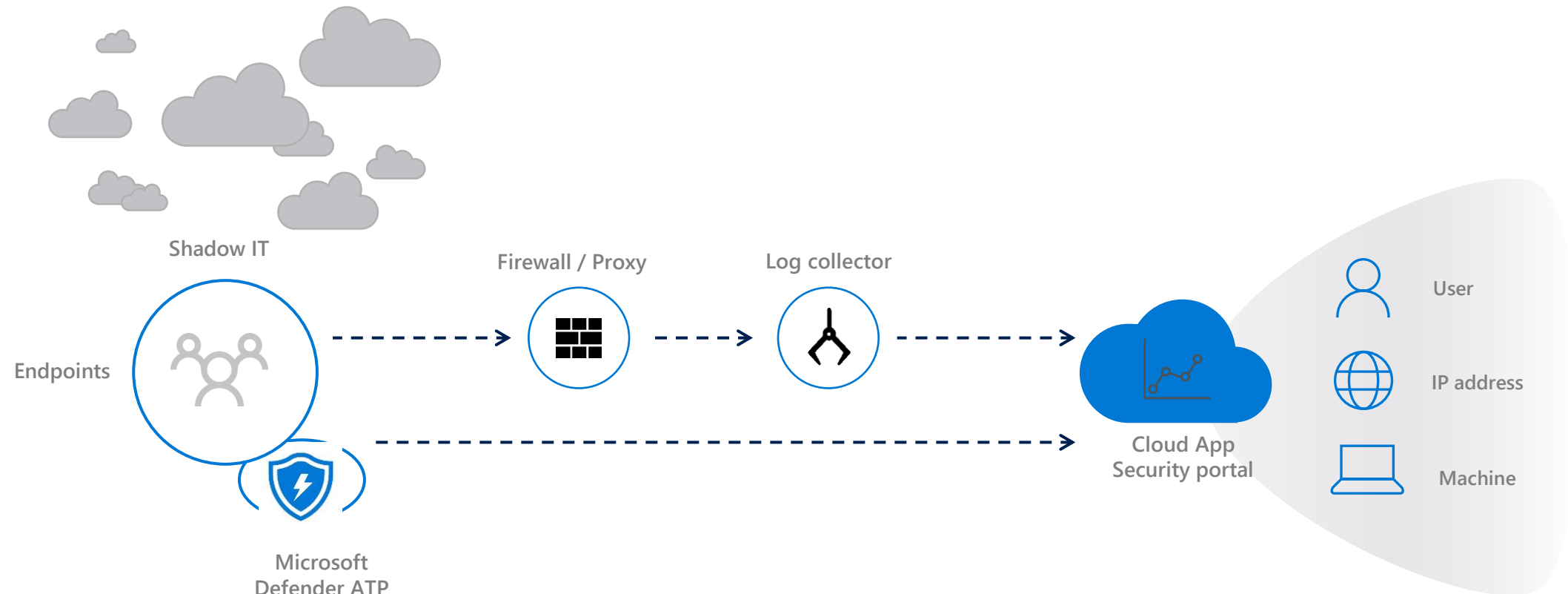


Discover and control apps in your environment


Take action: Manage newly discovered cloud app




DISCOVERY ARCHITECTURE WITH MDE



Cloud Discovery

 Continuous report
Win10 Endpoint Users

Timeframe
Last 30 days



- Dashboard
- Discovered apps
- IP addresses
- Users
- Devices

Updated on Jan 13, 2021

QUERIES
Select a query...

APPS
Apps...

APP TAG
☒ Sanctioned ☒ Unsanctioned ☐ None

RISK SCORE

0

4

10

COMPLIANCE RISK FACTOR
Select factors...

SECURITY RISK FACTOR
Select factors...

Save as Advanced

- Browse by category:
- Search for category...

Cloud storage 8

Content management 4

IT services 2

Hosting services 2

Advertising 2

Communications 2

Productivity 2





















Operations management 1

Online meetings 1

News and entertainment 1

1 - 20 of 34 discovered apps

New policy from search

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Devices	Last seen (UTC)	Actions
 File Dropper Cloud storage	2	14 MB	8 MB	5K	623	1000	625	Jan 12, 2021	  
 TWiki MONITORED Collaboration	3	498 KB	423 KB	141	121	89	122	Jan 12, 2021	  
 SendMyWay Cloud storage	3	453 KB	453 KB	154	132	98	133	Jan 12, 2021	  
 RegisterCompass IT services	2	452 KB	452 KB	151	132	93	133	Jan 12, 2021	  
 ClickDesk Customer support	3	450 KB	450 KB	147	122	96	124	Jan 12, 2021	  

Cloud Discovery

 Continuous report
Global ▾

Timeframe
Last 30 days ▾




- Dashboard
- Discovered apps
- IP addresses
- Users

Updated on Mar 26, 2019

QUERIES

Select a query... ▾

APPS

APP TAG 

RISK SCORE



COMPLIANCE RISK FACTOR

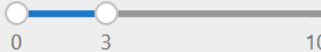
SECURITY RISK FACTOR

Save as

Advanced


Apps...

  None



Select factors... ▾

Select factors... ▾

- Browse by category:
- 
-
- ✓ Cloud storage 5

Marketing 3

IT services 3

Hosting services 3

Customer support 3



Website monitoring 2

Productivity 2

Collaboration 2


Advertising 2


Content management 2


 














1 - 5 of 5 discovered apps

New policy from search



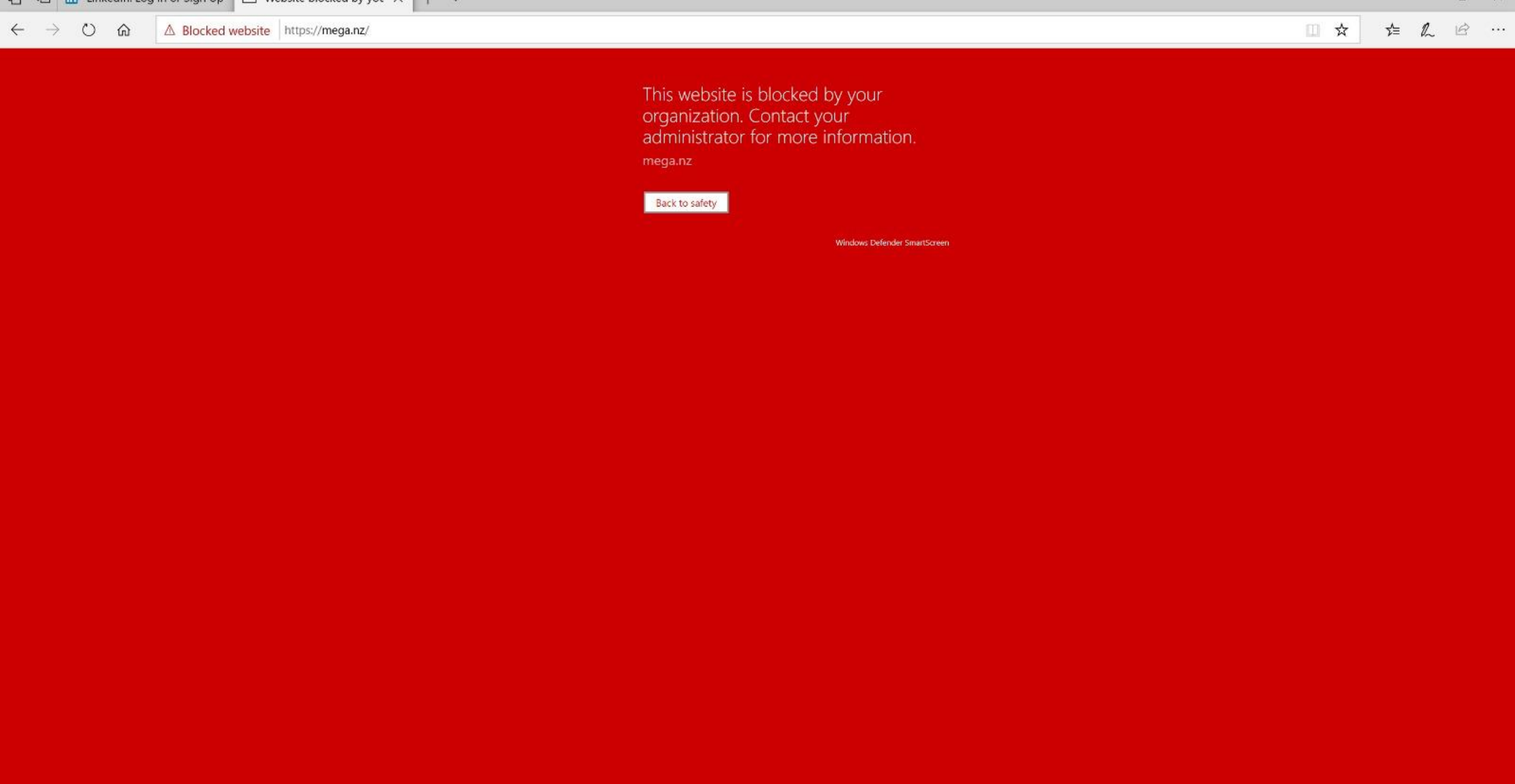




App	Score ▾	Traffic	Upload	Transactions	Users	IP addresses	Last seen (...)	Actions
 MEGA Cloud storage		90 MB	46 MB	86	62	56	Mar 25, 2019	  
 SendMyWay Cloud storage		90 MB	47 MB	83	70	45	M	
 PowerFolder Cloud storage		94 MB	49 MB	88	73	52	M	
 NetFortris Cloud storage		83 MB	42 MB	80	65	42	M	
 OwnCube Cloud storage		93 MB	48 MB	85	72	45	M	

- TAG APP
- Sanctioned
- ✓ Unsanctioned
- Custom app
- Accounting Dept
- Deprecated
- In legal review
- In review
- In technical POC
- Managed

Tag an app as unsanctioned to block it from being accessed by users in the future: Actions drop down



Endpoint-based control over access to risky and non-compliant apps via Microsoft Defender for Endpoint



Get started today: Shadow IT

1

Discover all cloud apps and services used in your organization

2

Govern discovered cloud apps and explore like solutions within your environment

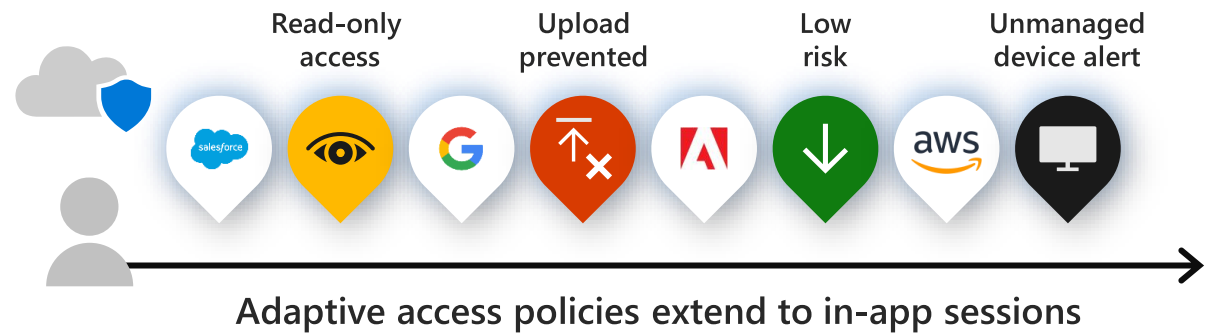
3

Assess the risk and compliance of all cloud apps

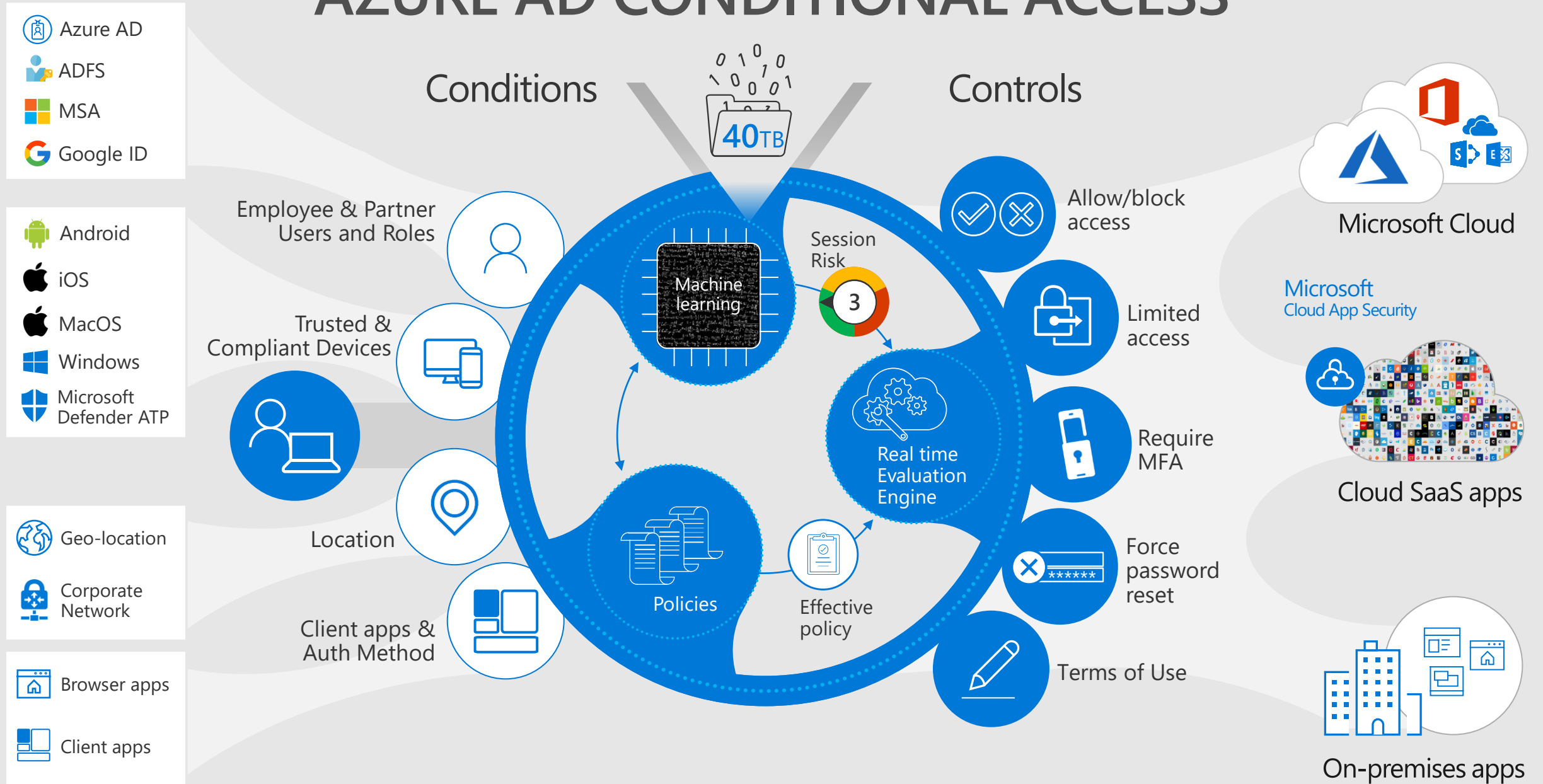


Secure Access

Integrating Microsoft Cloud App Security with your identity provider enables real-time enforcement of in-session actions.



AZURE AD CONDITIONAL ACCESS

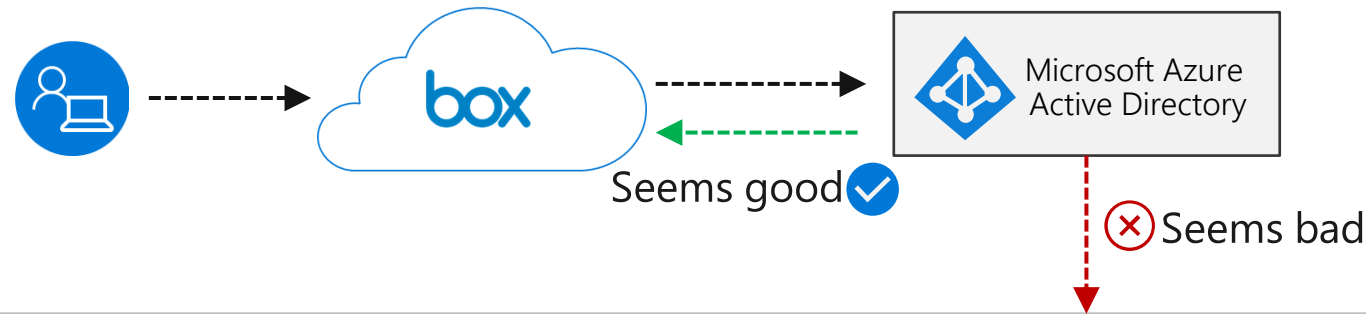


CONDITIONAL ACCESS APP CONTROL

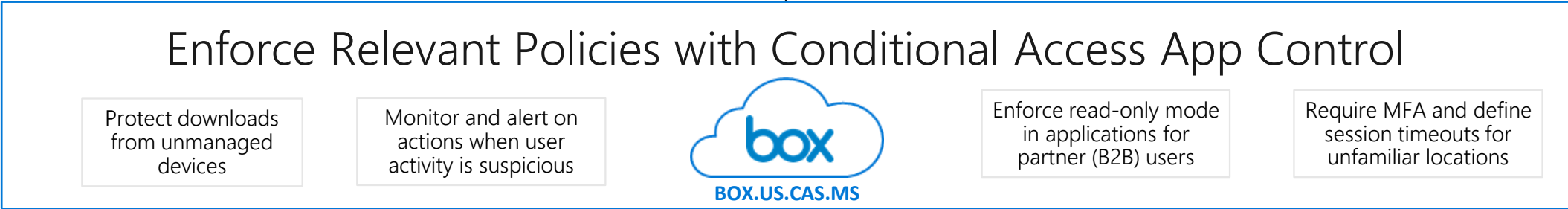
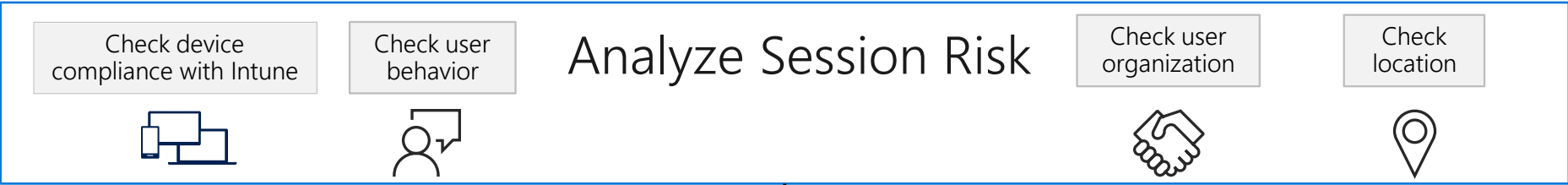
Cloud App Security integrates with:

- Azure Active Directory
- Azure Information Protection
- Microsoft Intune

to help protect any app in your organization.

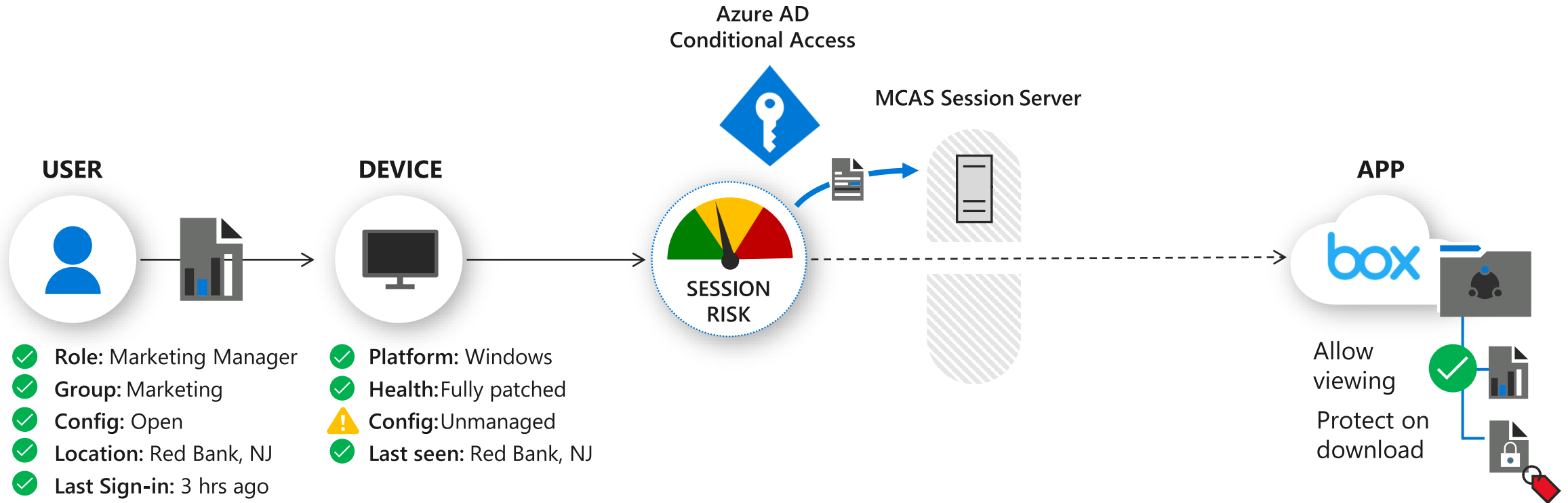


MICROSOFT CLOUD APP SECURITY



USE CASE: PREVENT DOWNLOAD OF LABELED FILES

Risk based in-session controls



⚠ Device is unmanaged



Get started today: Secure Access

1

Gain visibility into corporate data stored in the cloud

2

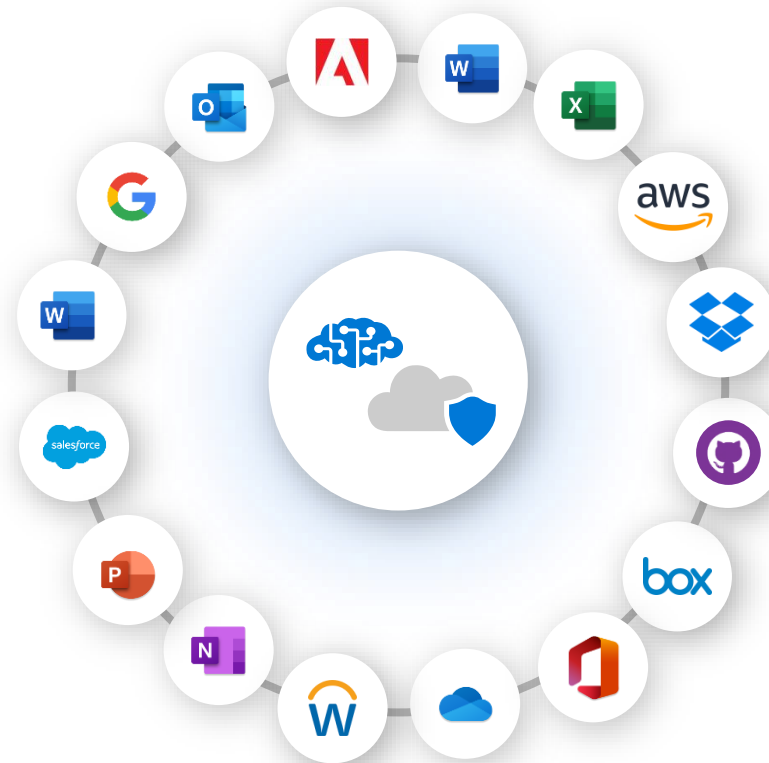
Enforce DLP and compliance policies for sensitive data stored in your cloud apps

3

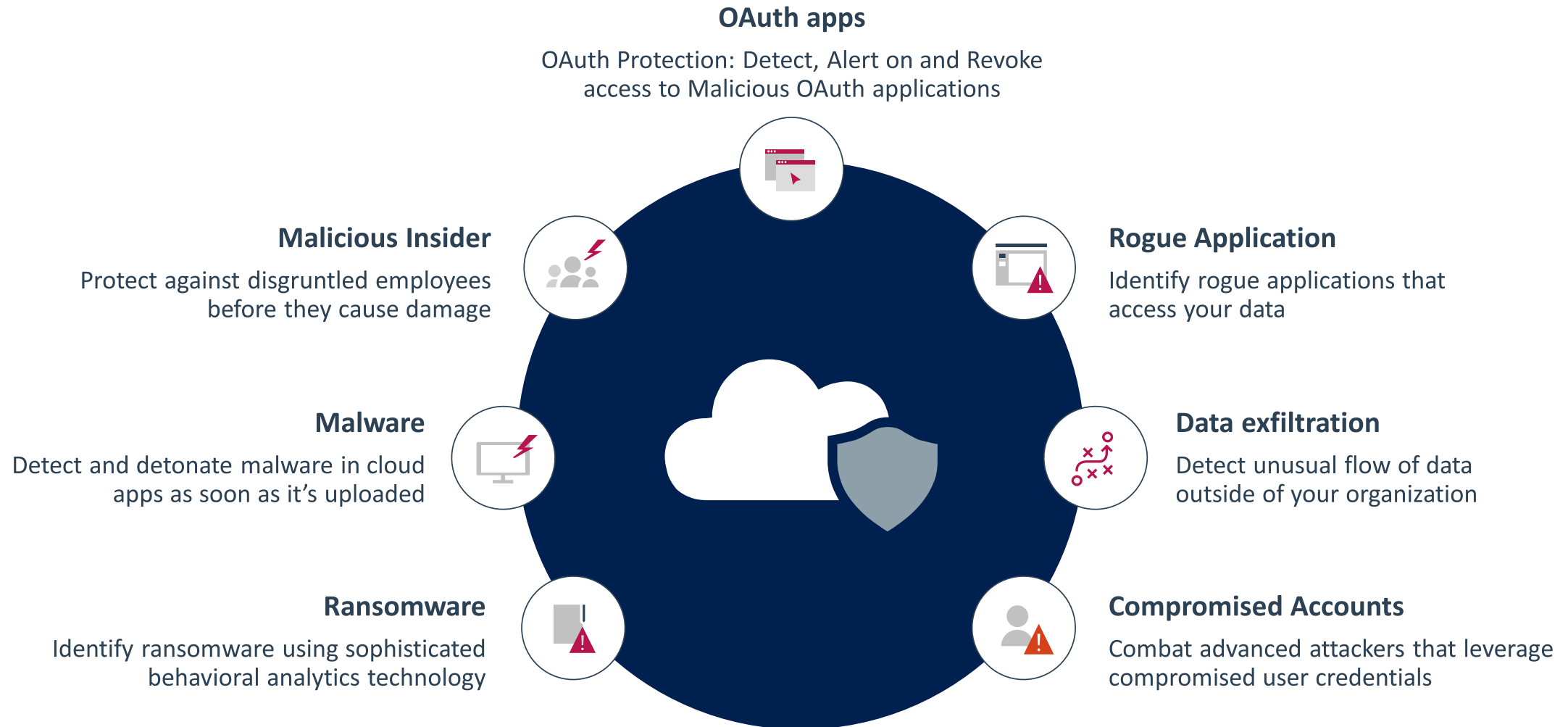
Ensure safe collaboration and data sharing practices in the cloud



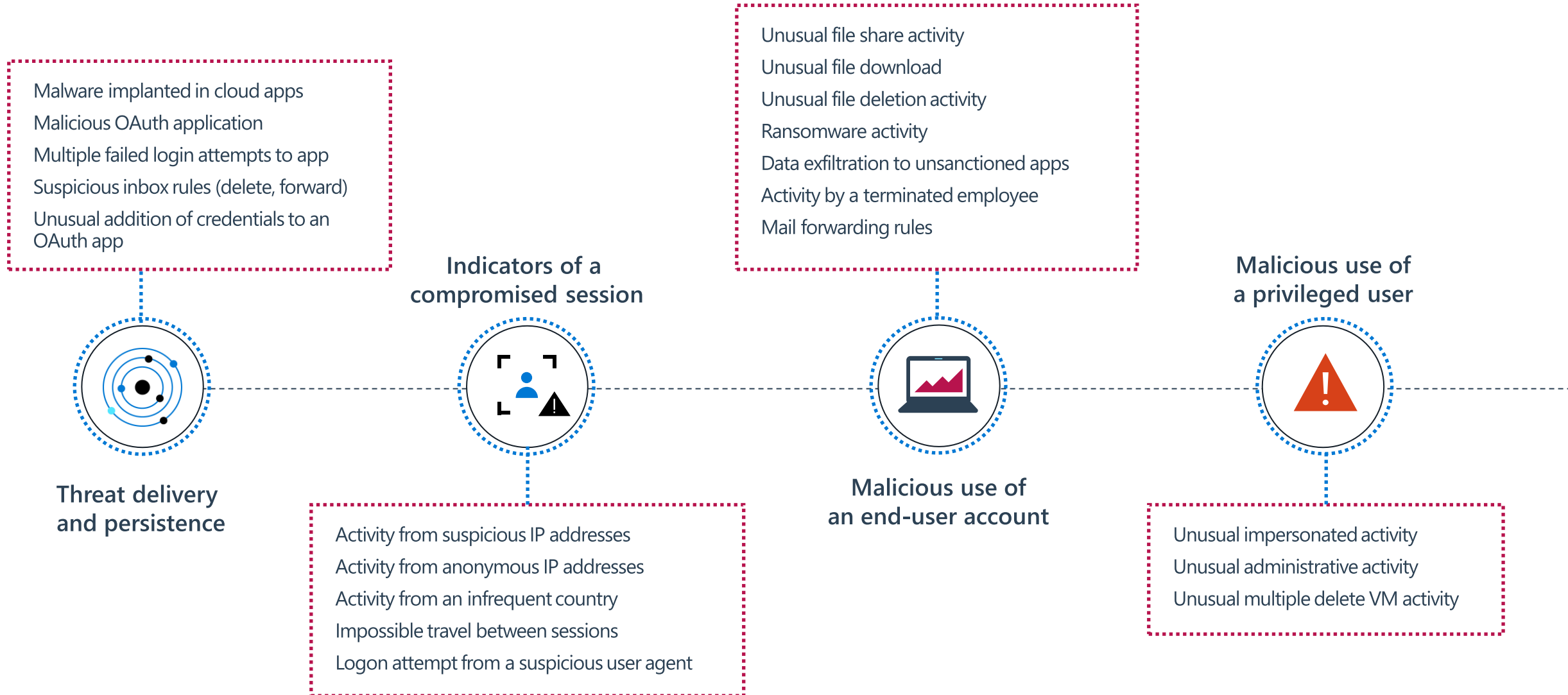
The integrated threat protection in Cloud App Security enables customers to detect advanced attackers and native cloud threats by detecting anomalous behavior and malicious activity in their cloud environment.



Protection against cloud threats



Detections across cloud apps

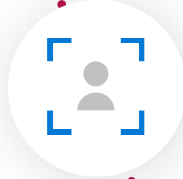




Protect organization
identities and leverage
unified investigation
across on-premises and
cloud activities



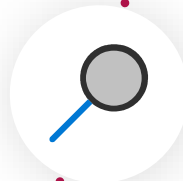
Microsoft Cloud App Security



Microsoft Defender for Identity



Azure AD Identity Protection



Unified SecOps experience to investigate
identity activities across on-prem and cloud



Investigation priority - based on
User and Entity Behavior Analytics



Policies

NAME

TYPE

STATUS

SEVERITY

CATEGORY

Advanced

Policy name...

Select type...














ACTIVE

DISABLED

Threat detection

1 - 20 of 32 Policies

Create policy

Policy	Count	Severity	Category			
 Potential ransomware activity Alert when a user uploads files to the cloud that might be infected with ransomware.	6 open alerts	<div></div> <div></div> <div></div>	 Threat			
 Logon from a risky IP address Alert when a user logs on to your sanctioned apps from a risky IP address. By default...	48 open alerts	<div></div> <div></div> <div></div>	 Threat			
 Malware campaign caught in delivery Several emails containing malware were detected within one session, indicating a p...	0 open alerts	<div></div> <div></div> <div></div>	 Threat detection		Jan 11, 2018	
 Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single app, and fails more than 10 ti...	11 open alerts	<div></div> <div></div> <div></div>	 Threat detection		Jun 3, 2018	
 Mass download by a single user Alert when a single user performs more than 30 downloads within 5 minutes.	18 open alerts	<div></div> <div></div> <div></div>	 Threat detection		Aug 12, 2018	



Alerts

RESOLUTION STATUS

OPEN

DISMISSED

RESOLVED

CATEGORY

Select risk category... ▼

SEVERITY

APP

Select apps... ▼

USER NAME

Select users... ▼

POLICY

Select policy... ▼

Advanced

1 - 12 of 12 alerts

Alert	App	Resolution	Severity	Date ▼
<div><div></div><div>Risky OAuth apps</div><div><div></div> 178.17.166.149 <div></div> Bill Dortch</div></div>	<div><div></div> Salesforce - General</div>	<div>RESOLVED</div>	<div><div></div><div></div><div></div></div> Low	2 days ago
<div><div></div><div>Ransomware activity</div><div><div></div> 178.17.166.149 <div></div> Bill Dortch</div></div>	<div><div></div> Amazon Web Service</div>	<div>RESOLVED</div>	<div><div></div><div></div><div></div></div> High	2 days ago
<div><div></div><div>Malware campaign caught in delivery</div><div><div></div> 178.17.166.149 <div></div> Bill Dortch</div></div>	<div><div></div> Slack - General - General</div>	<div>RESOLVED</div>	<div><div></div><div></div><div></div></div> Low	2 days ago
<div><div></div><div>Activity from a Tor IP address</div><div><div></div> 79.137.68.85 <div></div> Bill Dortch</div></div>	<div><div></div> Box - General - General</div>	<div>RESOLVED</div>	<div><div></div><div></div><div></div></div> Medium	2 days ago
<div><div></div><div>Alert on any session coming from a Risky IP address</div><div><div></div> 79.137.68.85 <div></div> Bill Dortch</div></div>	<div><div></div> Office 365</div>	<div>DISMISSED</div>	<div><div></div><div></div><div></div></div> Low	2 days ago
<div><div></div><div>Logon from a risky IP address</div><div><div></div> 79.137.68.85 <div></div> Bill Dortch</div></div>	<div><div></div> Workplace by Facebook...</div>	<div>DISMISSED</div>	<div><div></div><div></div><div></div></div> High	2 days ago



Alerts > Ransomware activity 3 months ago

+6 MEDIUM SEVERITY

Ransomware activity 2 Services 167.220.196.69 Bill Dortch

Resolution options: Bill Dortch ▾

Dismiss... Resolve... ▾

Description
The user Bill Dortch (billd@mcas-test9.com) uploaded a file known as a payment instructions file (https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/helpdecrypt.txt), which is common in ransomware attacks.

- Additional risks in this user session:
- This user is an administrator in Office 365 (Default).
 - Microsoft SharePoint Online (Default) was accessed from United Kingdom for the first time in 80 days.
 - Microsoft SharePoint Online (Default) was accessed from the ISP Sky Broadband for the first time in 80 days.
 - This user uploaded 416 unique files in a single session. 402 of them had the same file extension (locky).
 - This user uploaded 416 unique files in a single session. 402 of them were from the same folder (https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/encrypt_info/).

Activity log

1 - 10 of 437 activities ⓘ

Investigate in Activity log ⌵

Activity	User	App	IP address	Location	Device	Date ▾
Modify file: file https://mcastest9-my.sharepoint.com/personal/billd...	Bill Dortch (billd@mcas-test9.com)	Microsoft OneDrive...	167.220.196.69	United Kingdom		Feb 17, 2019, 10:46 AM ⋮

SHOW SIMILAR

General **User** IP address [Send us feedback...](#)

Bill Dortch
Groups: Office 365 (Default) administrator
INTERNAL

[Go to user page](#)
User actions ▾

OPEN ALERTS
7

CONNECTED FROM (30 DAYS)
 0 countries 0 ISPs 0 IP addresses

MATCHES
131

ACTIVITIES
13

USER ACTIVITIES (30 DAYS) [See all](#)

FREQUENT LOCATIONS

Frequent locations are not available for this user

Access file: file https://mcastest9-my.sharepoint.com/personal/billd ...

Bill Dortch (billd@mcas-test9.com)

Microsoft OneDrive...

167.220.196.69

United Kingdom

Feb 17, 2019, 10:46 AM ⋮

Policies > Malware detection

Infected files

History

AUTHORIZATION

APP



OWNER

ACCESS LEVEL

FILE TYPE

OWNER OU

Advanced




Select apps...

Select users...



Select access level...

















Select type...

Select organizational units...



1 - 6 of 6 files



File name	Malware	Confidence	Owner	App	Collaborators	Status	Detection date
 eicar.exe.txt	 EICAR-Test-File,...	 High	Super Admin (mcas-test...	 Box - US	 1 collaborator	Infected	Jul 19, 2018
<div>Path: All Files - View hierarchy</div> <div>URL: https://app.box.com/files/0/f/0/1/f_300544144254</div> <div>Type: text</div> <div>Owner: Super Admin (mcas-test9) (superadmin@mca...</div> <div>Created: Jun 25, 2018</div> <div>Policies:  G56: Publicly Shared Files, Malware detecti...</div> <div>MIME type: text/plain</div> <div>Owner OU: —</div> <div>File identifiers: View file identifiers</div> <div>Collaborators: 1 collaborator</div> <div>EICAR-Test-File, EICAR test file NOT a virus., EICAR test file, Eicar-Test-Signature, Virus.44D88612FEA8A8F3.Eicar, EICAR_TEST_FILE, EICAR-Test-File (not a virus), qex.eicar.gen.gen, Eicar test fil...</div> <div>Malware: EICAR-Test-File, EICAR test file NOT a viru...</div>							
 eicar.exe	 EICAR-Test-File,...	 High	Super Admin (mcas-test...	 Box - US		Infected	Jun 25, 2018
 HR_Summary_Nov...	 DOS/EICAR_Tes...	 High	MCAS Test 9 (admin@m...	 Microsoft SharePoin...	 3 collaborators	Infected	Apr 11, 2018



Get started today: Threat Protection

1

Identify compromised user accounts

2

Record an audit trail for all user and privileged account activities across hybrid environments

3

Detect and remediate malware in your cloud apps

dinext.
pi-sec GmbH

Microsoft Information
Protection



Leaders

May 6th 2017 edition >

Regulating the internet giants

The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules



Top Information Protection Use Cases

DISCOVER – CLASSIFY – PROTECT – MONITOR

Information Protection and Data Governance Strategy

- Label, track, and show data loss or manipulation of a file.
- Implement corporate policies to protect **different levels** of sensitive **data**

Protecting sensitive information

- Challenging to **discover and classify** data across mobile devices, SaaS, cloud infrastructure, and on-premises
- Need **full lifecycle data protection** for identified data including encryption, permissions, visual markings, access revocation, retention and deletion

Top Information Protection Use Cases

DISCOVER – CLASSIFY – PROTECT – MONITOR

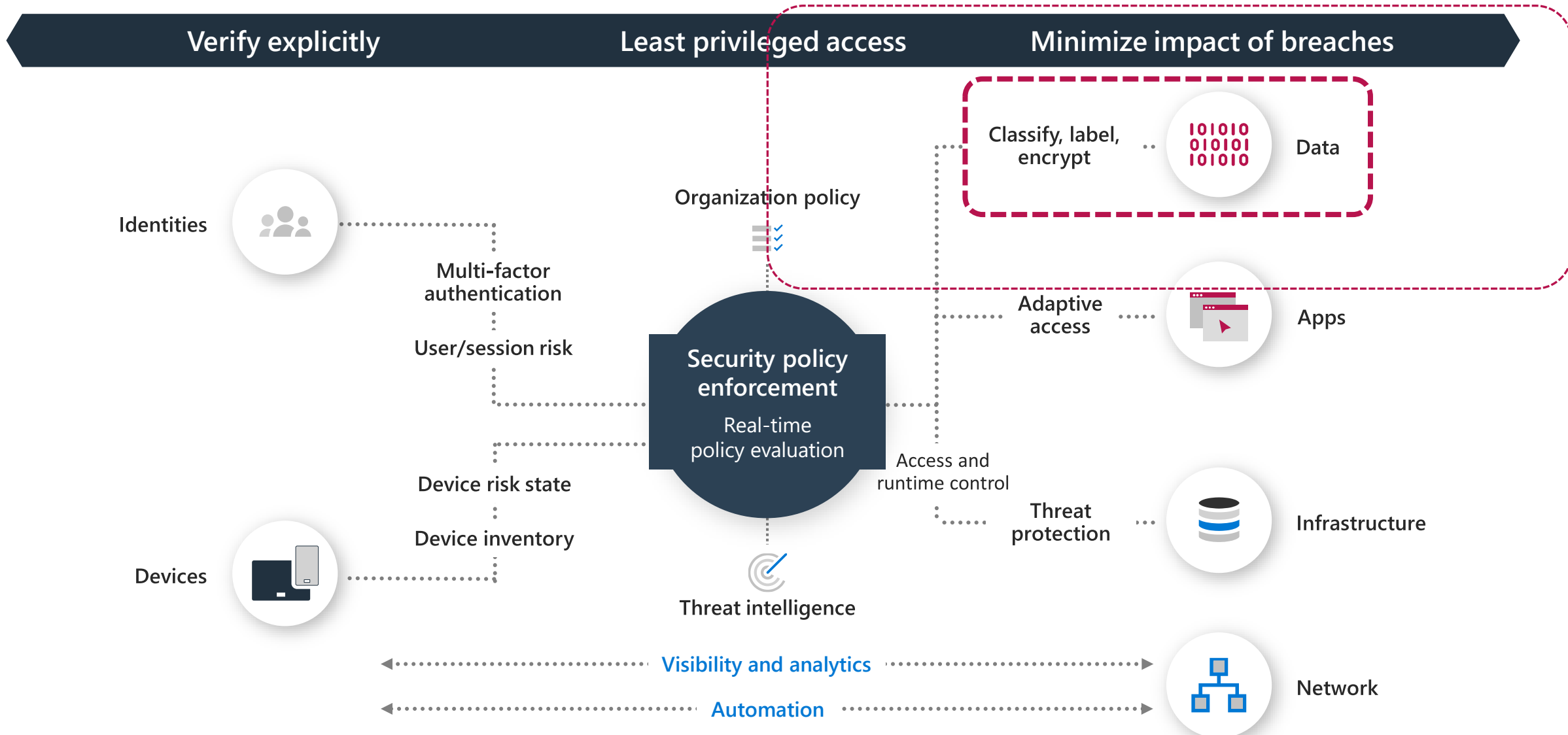
Highest level of protection of sensitive files

- protect files from the board of directors with **Double Key Encryption** where you hold a second key on premises in an HSM
- Configure Teams with **three tiers** of protection to ensure a smooth workflow

Use Data Loss Prevention holistically

- Protect your cloud resources with MCAS and DLP policies to ensure safety in the cloud
- Configure Endpoint DLP to enforce policies to secure your devices
- Use DLP **on premises scanner** to detect and protect sensitive data in your file shares, SharePoint libraries and folders

Information Protection incorporates Zero Trust principles

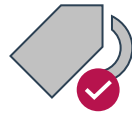


Microsoft Information Protection solutions

Protect your sensitive data—wherever it lives or travels



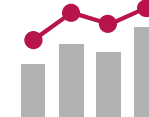
Discover



Classify



Protect



Monitor

Across



Devices



Apps

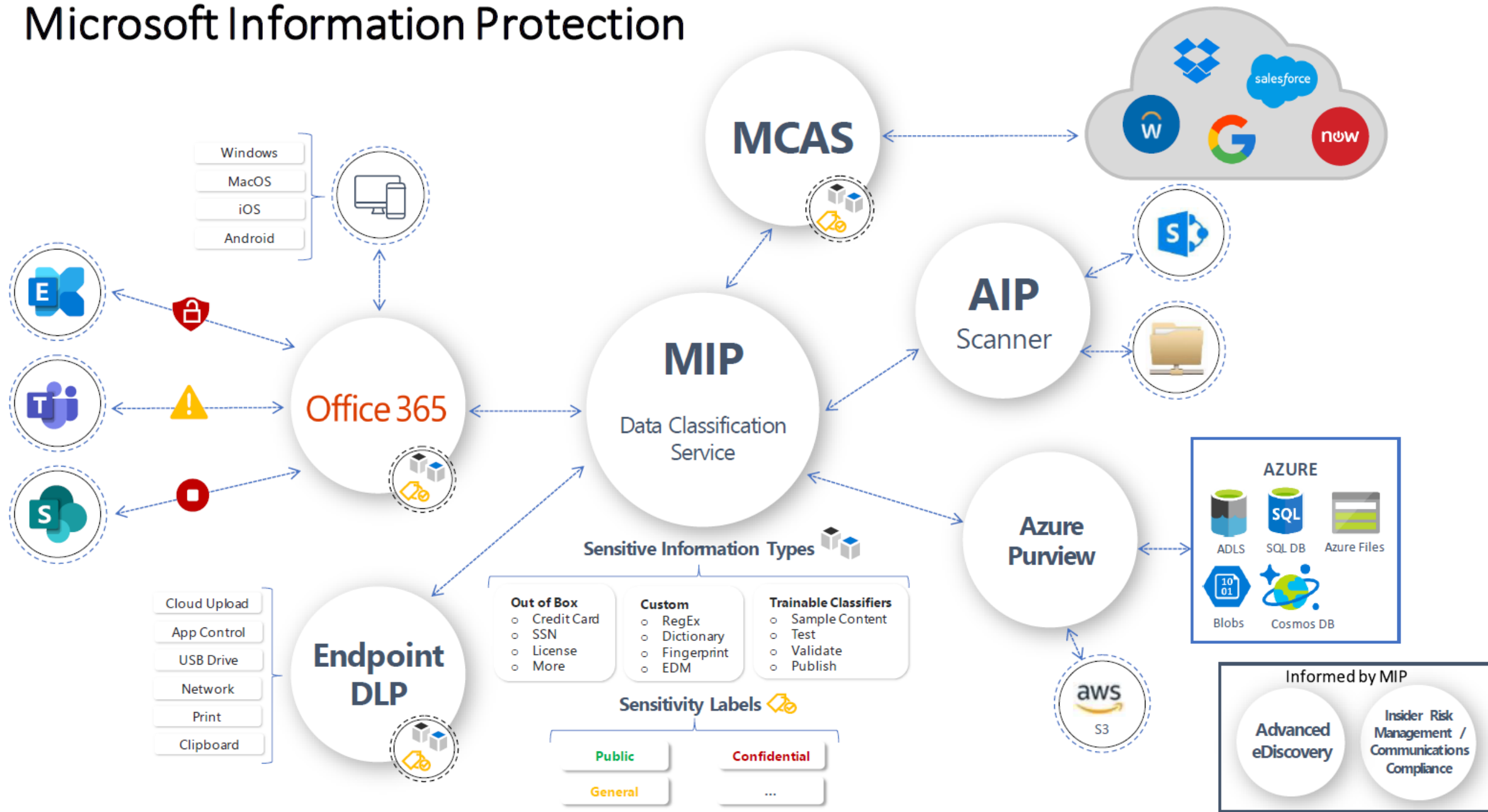


Cloud services



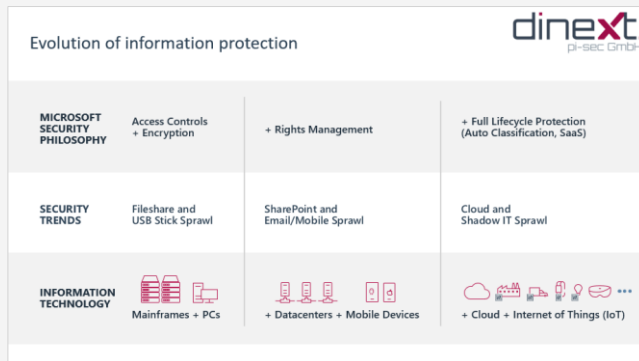
On-premises

Microsoft Information Protection

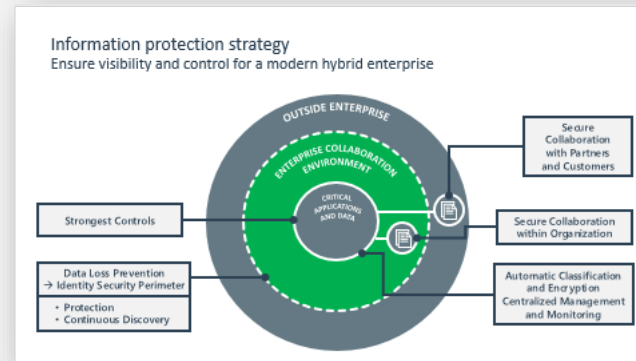


Information Protection

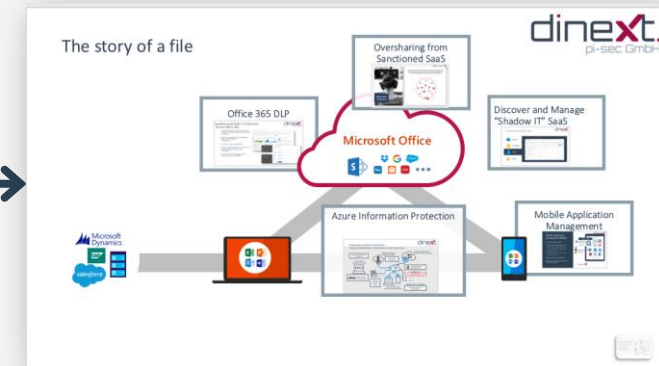
TRENDS AND STRATEGIES



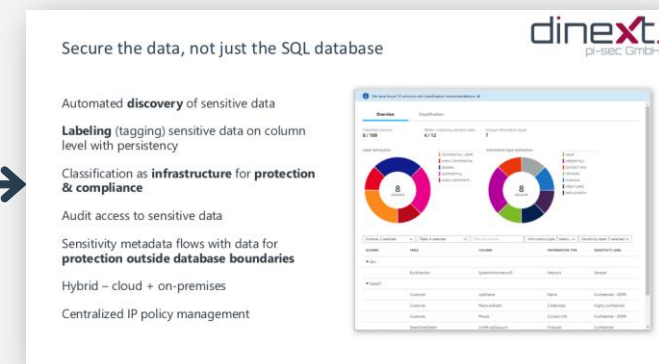
STRATEGY AND CAPABILITIES



INFORMATION PROTECTION STRATEGY



SENSITIVE DOCUMENTS



SQL AND STRUCTURED DATA / AZURE PURVIEW

Evolution of information protection

MICROSOFT SECURITY PHILOSOPHY

Access Controls
+ Encryption

+ Rights Management

+ Full Lifecycle Protection
(Auto Classification, SaaS)

SECURITY TRENDS

Fileshare and
USB Stick Sprawl

SharePoint and
Email/Mobile Sprawl

Cloud and
Shadow IT Sprawl

INFORMATION TECHNOLOGY



Mainframes + PCs



+ Datacenters + Mobile Devices



+ Cloud + Internet of Things (IoT)

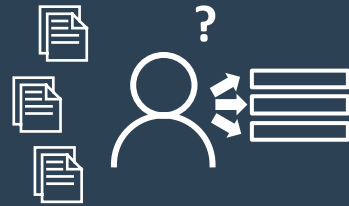
Data security challenges



Reduce and Manage Risk of User Errors

Collaboration to create new business value requires data sharing and data mobility

Critically important to prevent unauthorized disclosure, modification, or destruction



Classification is Challenging

Manual user classification is impractical at scale

Large set of existing documents and more being created all the time



Data Must Be Protected Outside of the Network

Data must be protected as it traverses mobile devices and cloud services

Data created outside the network must be classified and protected



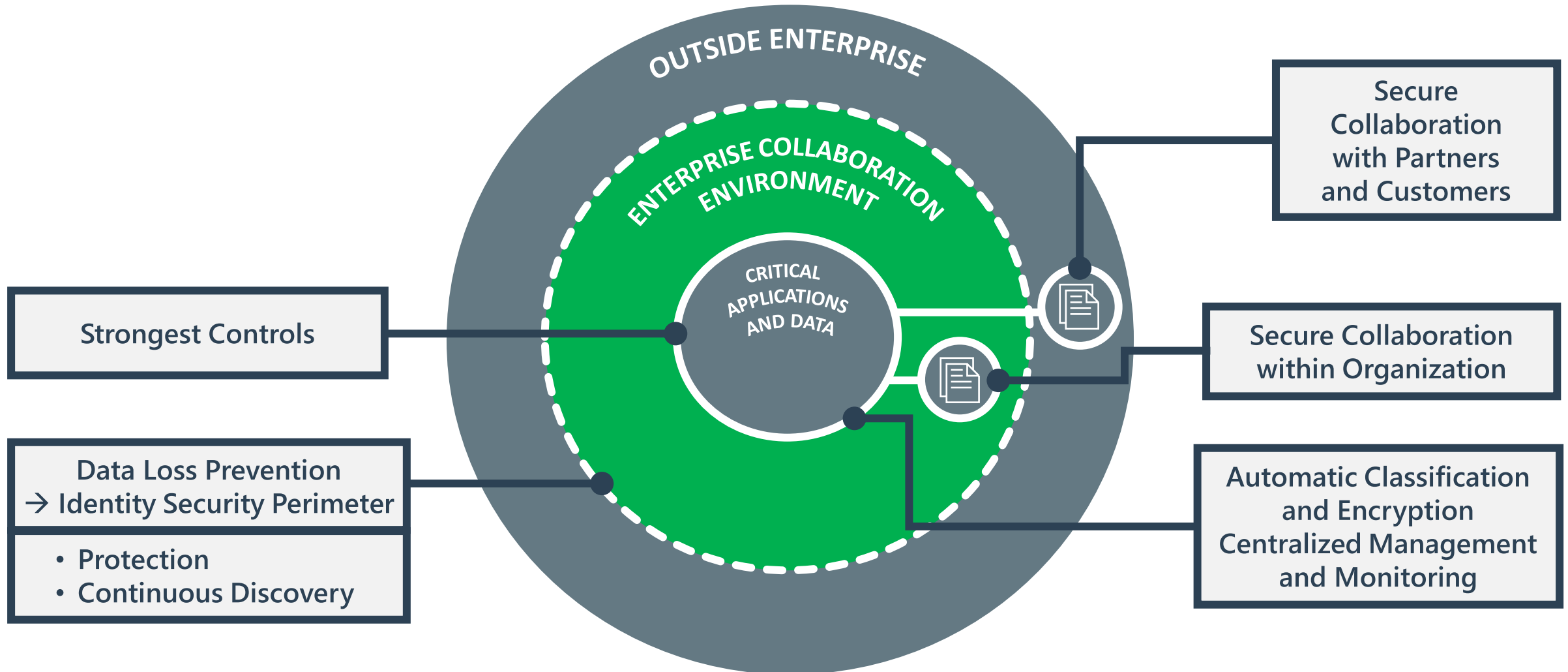
Compliance and Security Require a Complete Strategy

Compliance penalties are increasing and measuring outcomes vs. methods

Need full lifecycle protection for information assets (appropriate to valuation)

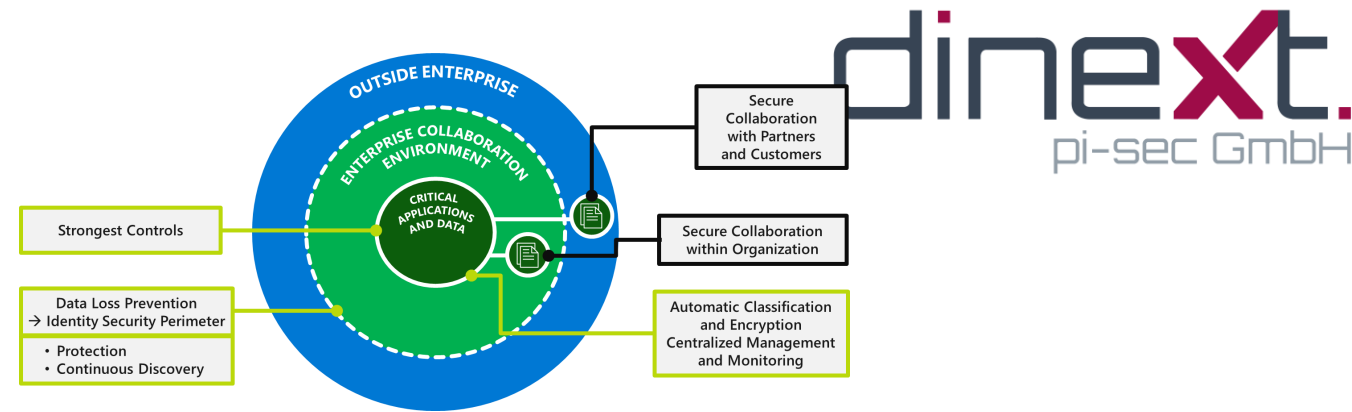
Information protection strategy

Ensure visibility and control for a modern hybrid enterprise



Strategy core goal

Protect at the appropriate level



3 HIGHEST VALUE ASSETS

Level 2 + Specialized Protection and processes

2 SENSITIVE INFORMATION

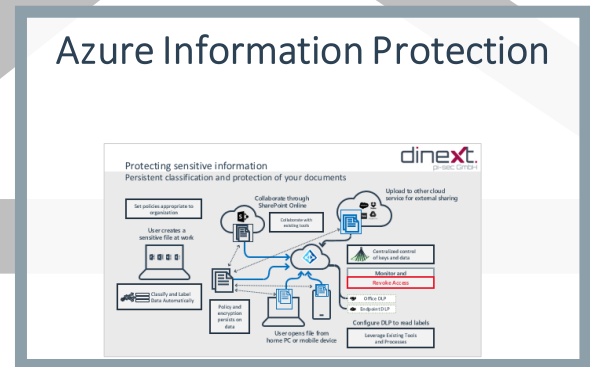
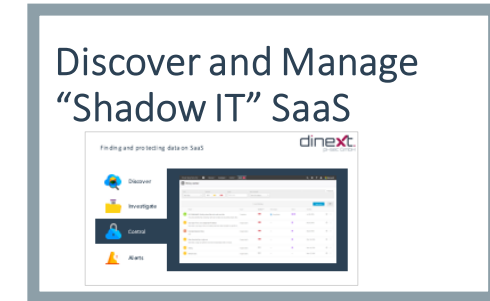
Reduce risk of theft, modification, and destruction

1 BASELINE PROTECTION

Building an Identity Security Perimeter



The story of a file



Sophisticated Built-in Protection Across Office 365

- Centralized console - define policy once, apply across Office 365 services and client end-points
- Built in to Exchange Online, SharePoint Online, and OneDrive for Business
- Focused on secure productivity
- Admins - Default policy for most common sensitive content (which can be customized)
- Users - Policy Tips integrate security education into user workflow

Home > Content Protection > Policies

Here's where you can see all of your content-based policies in one place – from Retention, Alerts, to Data Loss Prevention. Use these policies to protect your information from inadvertent disclosure, make sure its preserved and never lost through accidental deletions, and use alerts to get notified when there's suspicious activity.

Search for policies, settings, sensitive information, tags, or tasks

Data Loss Prevention

Here's your DLP activity in the last 7 days:

17k

Default Recommended

Data volume covered by Retention Policy:

25 TB
20 TB
15 TB
10 TB

Covered by policy
Covered by policy

Data by age:

178 TB Total

Current
Over 10 years
Over 5 years

Policy matches

Create a policy

☐ Name

☐ Default Office 365 Policy

☐ Default Alert Policy

☐ Recommended Office 365

You can skip steps or we'll let you know if you have to complete it.

☒ Choose the information to protect

☒ Name your policy

☐ Choose locations

☐ Policy settings

☐ Review your settings

Choose locations

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	SharePoint sites	All Include	None Exclude
<input checked="" type="checkbox"/>	OneDrive accounts	All Include	None Exclude
<input checked="" type="checkbox"/>	Exchange email	All	None

Back Next Cancel

Balancing User Productivity and risk

- Policy Tips help educate users when they are about to violate a policy
- Available in desktop, web, and mobile apps

The screenshot shows the Microsoft Excel interface with a green ribbon at the top. A yellow banner at the top of the worksheet area displays a policy tip: "POLICY TIP: This file conflicts with a policy in your organization. If you don't resolve this conflict, access to this file might be blocked. Go to the File menu for more information. Override". Below this, a white dialog box titled "Policy tip for '2015 Employee Roster.xlsx'" is open. The dialog contains the following text: "This item conflicts with a policy in your organization. Access to this item is blocked for everyone except its owner, last modifier, and the site owner." and "To dismiss the policy tip, [open the item](#) to fix the issues or click **Resolve** to override or report a problem with the policy tip." Below the text is a section titled "Issues" with a red minus icon, listing two points: "Item is shared with people outside your organization" and "Item contains the following sensitive information: U.S. Social Security Number (SSN)". At the bottom of the dialog, it says "Last scanned: 5 days ago" with an information icon. There are "Resolve" and "Close" buttons at the bottom right of the dialog. In the background, the OneDrive for Business interface is visible, showing a list of files and folders. A mobile app interface is also partially visible on the left side of the image.

2016 Employee Roster - Excel

File Home Insert Draw Page Layout Formulas Data Review View Inquire Tell me what you want to do

Cut Copy Paste Format Painter Clipboard Font Alignment Number Styles

Normal Bad Good Neutral

WELCOME TO YOUR ONEDRIVE FOR BUSINESS, THE PLACE TO STORE, SYNC, AND SHARE YOUR WORK. DOCUMENTS ARE PRIVATE UNTIL SHARED. [Learn more here.](#) Dismiss

new upload sync edit manage share

All Documents Shared with us

Name

Email attachments

My Stuff

Shared with Eve

2012 Expense A

2013 Expense A

2014 Employee

2014 Expense A

2015 Employee

2015 Expense A

January Expense

New Item Order

New Item Order Form -3-15

Notes from Staff Meeting

QT300 Accessories Specs(Draft)

Yesterday at 3:56 PM

Sunday at 1:23 AM

May 28, 2013

Shared

Only you

Sara Davis

Sara Davis

Sara Davis

Details

Social Security Number
SSN: 123-12-1234

Security Issue Report Form

1

Lifts and other Large equipment
Streamline Financial Reports Process
Customer Requests

Move Save Delete

Security Issue Report Form

View policy tips
This item conflicts with a policy in your organization

Keep offline

Type .DOCX
Size 22KB
Created 10/23/15 5:45 PM
Modified 3/23/16 1:29 PM

Policy tip for '2015 Employee Roster.xlsx'

This item conflicts with a policy in your organization. Access to this item is blocked for everyone except its owner, last modifier, and the site owner.

To dismiss the policy tip, [open the item](#) to fix the issues or click **Resolve** to override or report a problem with the policy tip.

Issues

- Item is shared with people outside your organization
- Item contains the following sensitive information: U.S. Social Security Number (SSN)

Last scanned: 5 days ago

Resolve Close

DLP Policy Rules - Conditions

- Describe the policy objective – model business risk and mitigation actions
- Set of conditions describing when rule applies
- Set of actions applied when conditions match
- Range of actions covering insights and automatic remediation
- Generic action behavior integrated for natural experience across each workload

U.S. Financial Data Low volume of content detected

Name

Conditions

Actions

User notifications

Admin alerts

^ Conditions

Use conditions to define what kind of content you want to protect.

When content contains sensitive information

any of these

Sensitive information type	Instance count		Match accuracy		
	min	max	min	max	
Credit Card Number	1	9	0	100	×
U.S. Bank Account Number	1	9	0	100	×
ABA Routing Number	1	9	0	100	×

[Add or change sensitive types](#)

+ Add sensitive information group

Content is shared with

Outside my organization

Detects when content is shared in an email message or shared in a document in SharePoint or OneDrive

+ Add a condition

DLP Policy Rules - Actions

- Describe the policy objective – model business risk and mitigation actions
- Set of conditions describing when rule applies
- Set of actions applied when conditions match
- Range of actions covering insights and automatic remediation
- Generic action behavior integrated for natural experience across each workload

U.S. Financial Data Low volume of content detected

Name	Conditions	Actions	User notifications	Admin alerts
------	------------	---------	--------------------	--------------

^ Actions

Use actions to protect content when the conditions are met.

Restrict action to the content

By default, people will be blocked from sharing or accessing shared content that matches this rule. You can also customize how users access sensitive content in different content locations.

SharePoint and OneDrive restrictions

☐ Block access to everyone except the person that owns the content, the last modifier of the content, and site admin where the content is stored.

☐ Allow internal people to access the content, but restrict all access to external recipients.

+ Add a condition

^ User notifications

Use Notifications to inform your users and help educate them on the proper use of sensitive information.

☒ **Email notifications**

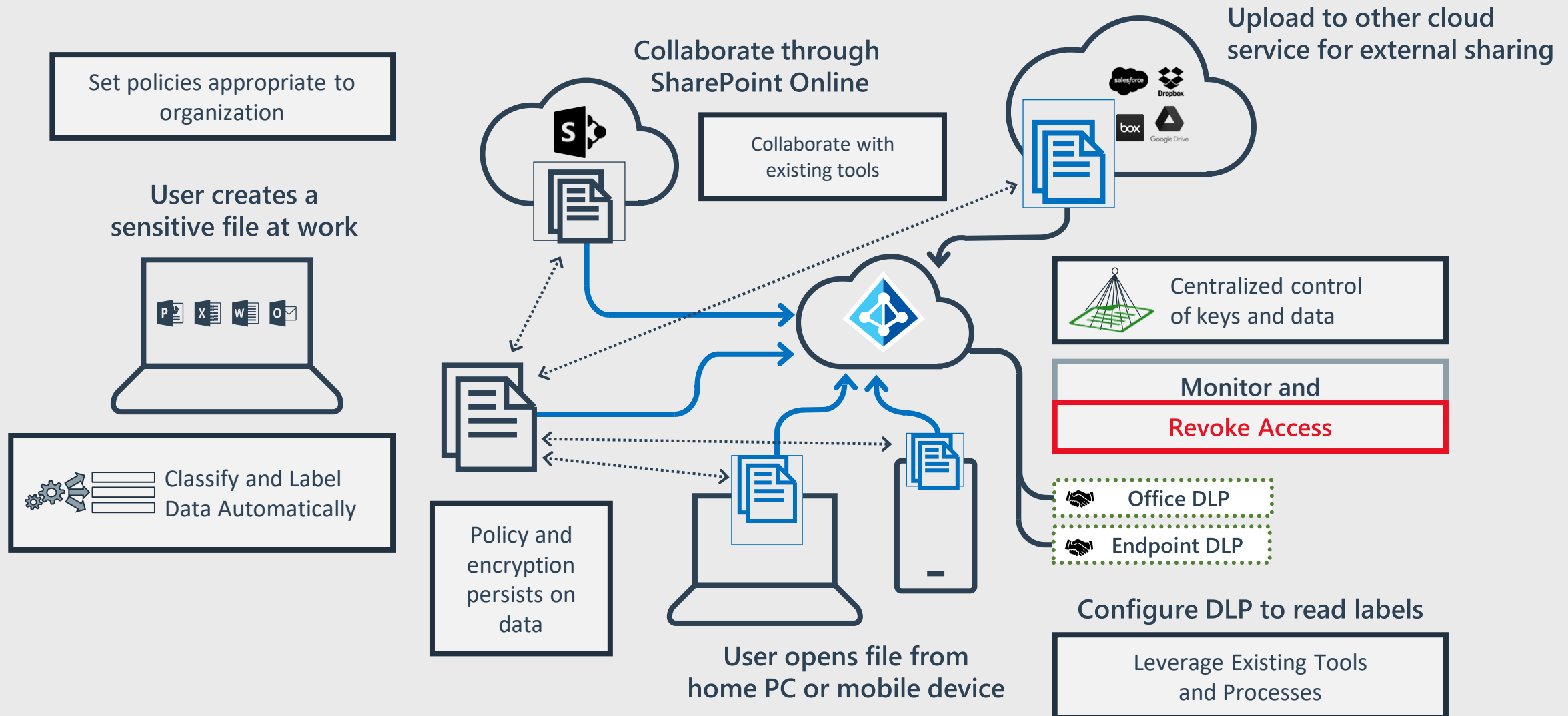
☐ Notify the user that sent, shared, or last modified the content.

☒ Let me choose who receives the notification

☒ The person that sent, shared, or modified the content

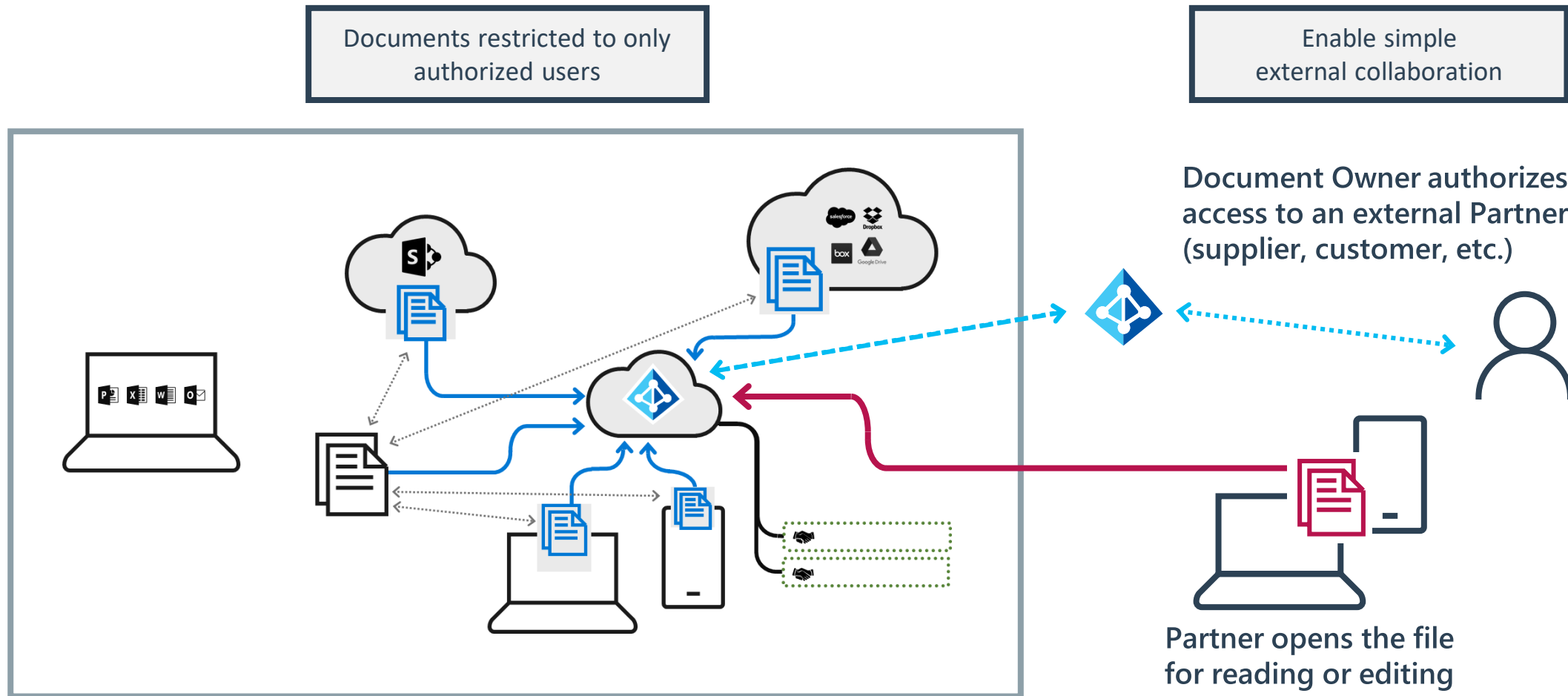
Protecting sensitive information

Persistent classification and protection of your documents



Modern information protection

Collaborate securely with partners



Key classification scenarios



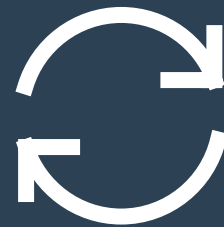
Automatic

Set policies to automatically applying classification and protection to data



Recommended

Prompt with suggested classification based on the content you're working on



Reclassification

Enable users to override a classification (and optionally require providing a justification)



User Set

Manually apply a sensitivity label to the email or file they are working on

Support required formats for sensitive data

Coverage for popular formats + extensibility

Microsoft Office Formats



PDF



AutoCAD



Others



Built into

Microsoft Office

Partner(s)



...and more

Partner(s)

SealPath



SAP Data Export

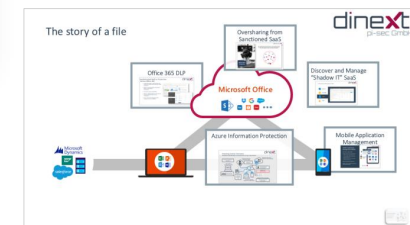
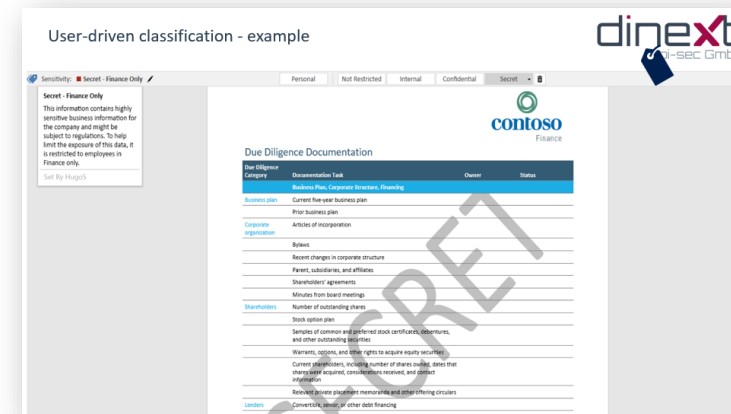
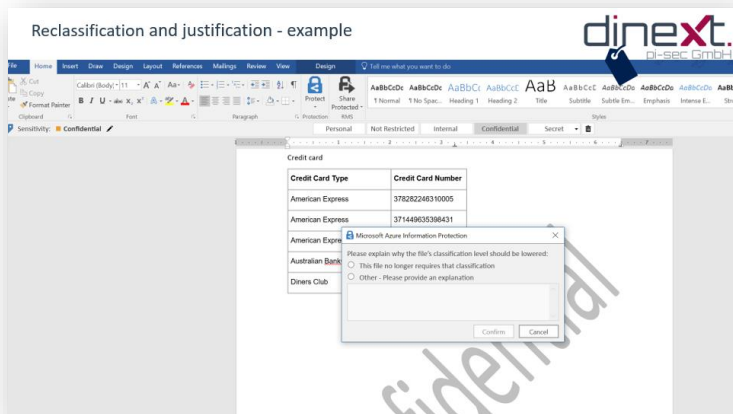
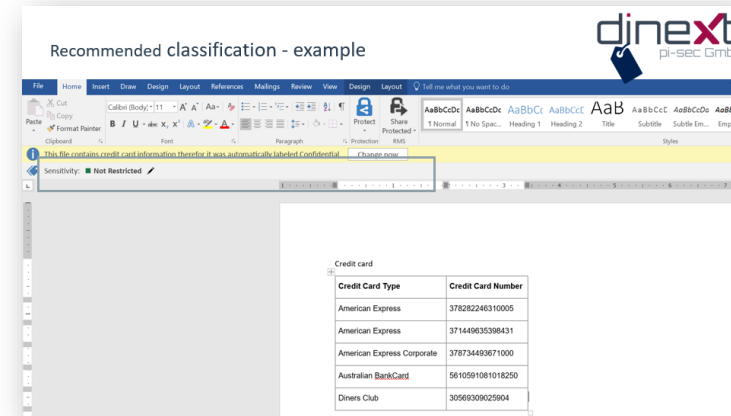
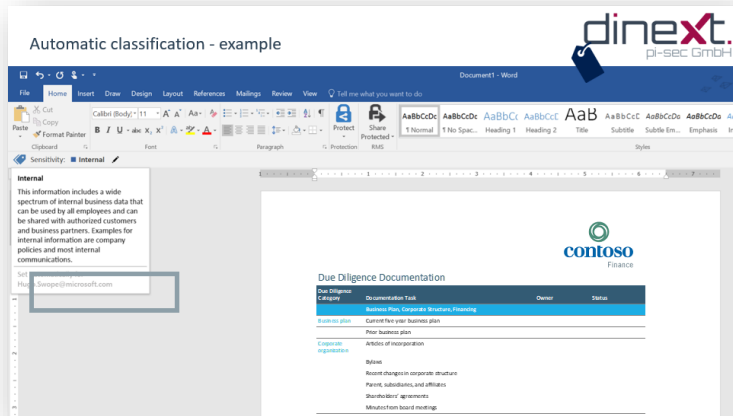


...and more



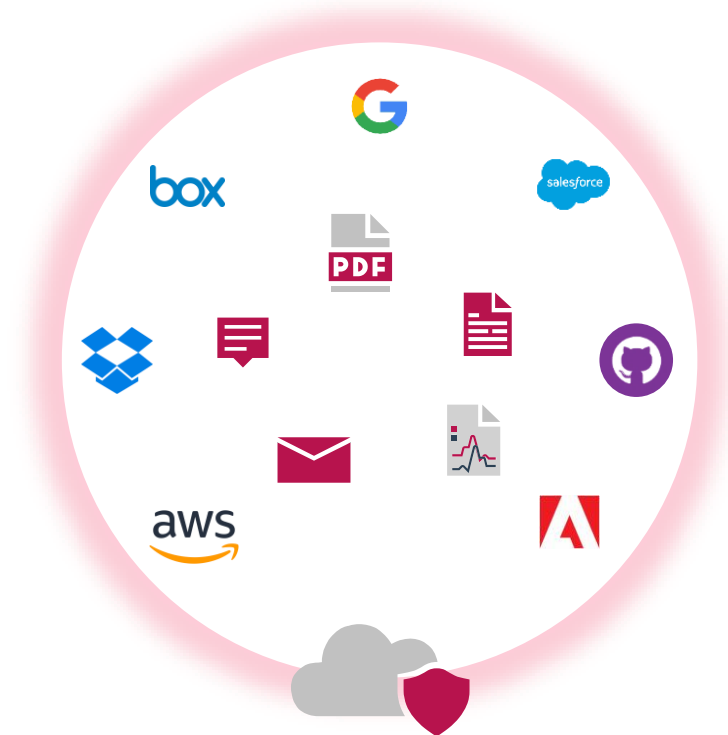
Software Development Kit

Azure Information Protection Experience





By leveraging information protection in Microsoft Cloud App Security, customers gain the power of Microsoft Information Protection applied to their environment holistically.



Protect your files and data in the cloud

Data is ubiquitous and you need to make it accessible and collaborative, while safeguarding it

101010
010101
101010

Understand your data and exposure in the cloud



Classify and protect your data no matter where it's stored



Monitor, investigate **and remediate violations**



Connect your apps via our API-based App Connectors

Visibility into sharing level, collaborators and classification labels

Quantify over-sharing exposure, external and compliance risks

Govern data in the cloud with granular DLP policies

Leverage Microsoft's IP capabilities for classification

Extend on-premises DLP solutions

Automatically protect and encrypt your data using Azure Information Protection

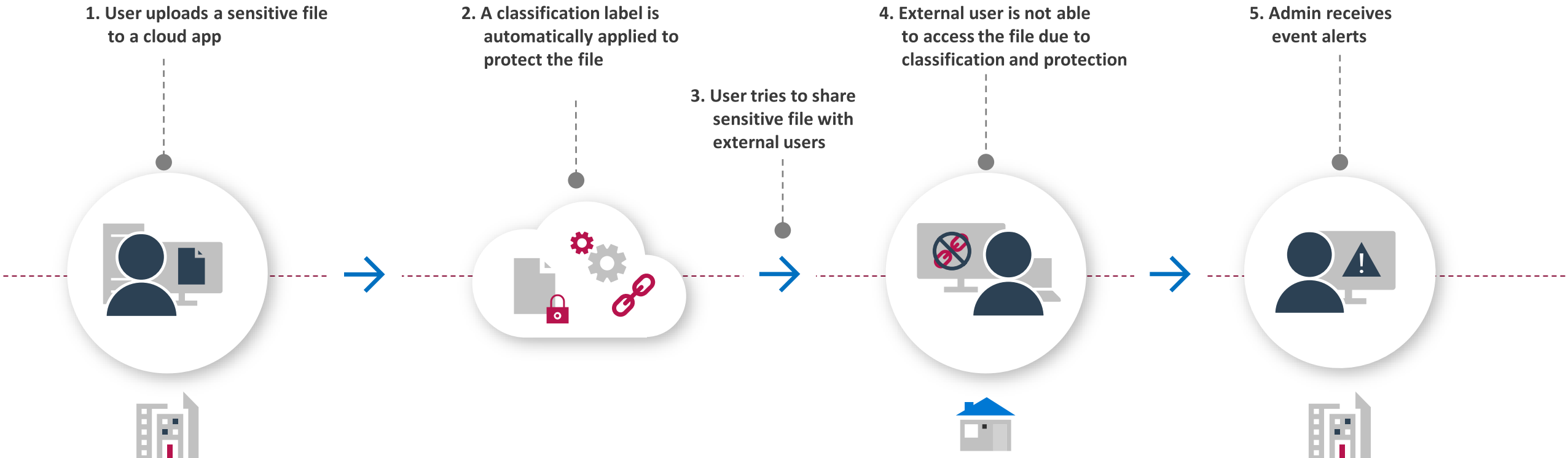
Create policies to generate alerts and trigger automatic governance actions

Identify policy violations

Investigate incidents and related activities

Quarantine files, remove permissions and notify users

Lifecycle of protecting sensitive files in the cloud



Detect and remediate overexposed files and anomalies

Create policies to generate alerts and trigger automatic governance actions

Policy creation is simple via our templates, or you can create your own custom policies which generate alerts, trigger automatic governance over certain actions and notify via Power Automate integrated workflows

Be notified to identify and investigate policy violations and related activities

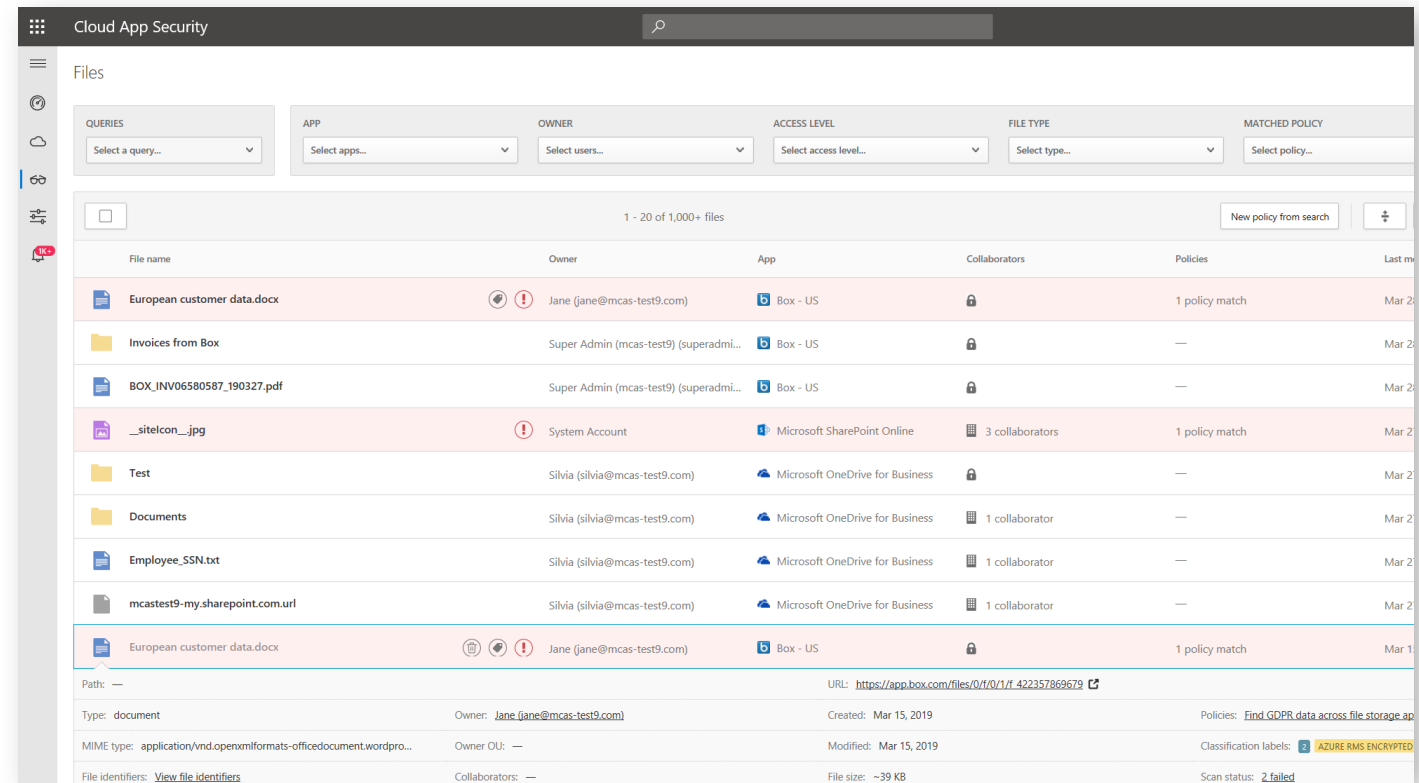
Notifications and investigations into violations of policy and any other activities are easy to sort, filter and compile to elevate your security teams' execution of security plans

Automatically remediate with built-in actions

Automatic remediation with Cloud App Security baseline actions or with additional granularity in Power Automate allow notify admin, quarantine, make private, authenticate and other key actions

Automatically label and protect existing sensitive information, and when new files are uploaded

Classify your sensitive data and then allow Cloud App Security to scale your protection through automatic labeling or other automatic remediation when new files when new files are uploaded to your environment



The screenshot displays the 'Files' section of the Cloud App Security dashboard. It features a table with columns for File name, Owner, App, Collaborators, Policies, and Last modified. The table lists several files, including 'European customer data.docx', 'Invoices from Box', 'BOX_INV06580587_190327.pdf', and 'Test'. The 'European customer data.docx' file is highlighted, showing a policy match and a scan status of '2 failed'.

File name	Owner	App	Collaborators	Policies	Last modified
European customer data.docx	Jane (jane@mcas-test9.com)	Box - US	1 collaborator	1 policy match	Mar 20, 2019
Invoices from Box	Super Admin (mcas-test9) (superadmi...)	Box - US	1 collaborator	—	Mar 20, 2019
BOX_INV06580587_190327.pdf	Super Admin (mcas-test9) (superadmi...)	Box - US	1 collaborator	—	Mar 20, 2019
__sitecon__.jpg	System Account	Microsoft SharePoint Online	3 collaborators	1 policy match	Mar 20, 2019
Test	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1 collaborator	—	Mar 20, 2019
Documents	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1 collaborator	—	Mar 20, 2019
Employee_SSN.txt	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1 collaborator	—	Mar 20, 2019
mcas-test9-my.sharepoint.com/url	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1 collaborator	—	Mar 20, 2019
European customer data.docx	Jane (jane@mcas-test9.com)	Box - US	1 collaborator	1 policy match	Mar 15, 2019

Path: — URL: <https://app.box.com/files/0/f/0/1/f/422357869679>

Type: document Owner: Jane (jane@mcas-test9.com) Created: Mar 15, 2019 Policies: Find GDPR data across file storage ap

MIME type: application/vnd.openxmlformats-officedocument.wordpro... Owner OU: — Modified: Mar 15, 2019 Classification labels: 2 AZURE RMS ENCRYPTED

File identifiers: View file identifiers Collaborators: — File size: ~39 KB Scan status: 2 failed

Key differentiators via Microsoft Information Protection approach

Unified labelling with Microsoft Information Protection

Leverage the powerful native integration of MIP with a streamlined experience across Office 365 Data Loss Prevention, Azure Information Protection and Cloud App Security

Over 150 built-in sensitive information types

Choose from 150+ built-in information types from credit card data, to data that triggers regulatory constraints such as GDPR or HIPAA

Custom sensitive information types using Regex, keywords and large dictionary

Ensure compliance and company policies are adhered to by further customizing your Cloud App Security information types

Custom and built-in classifiers as EDM, fingerprint, and trainable classifiers

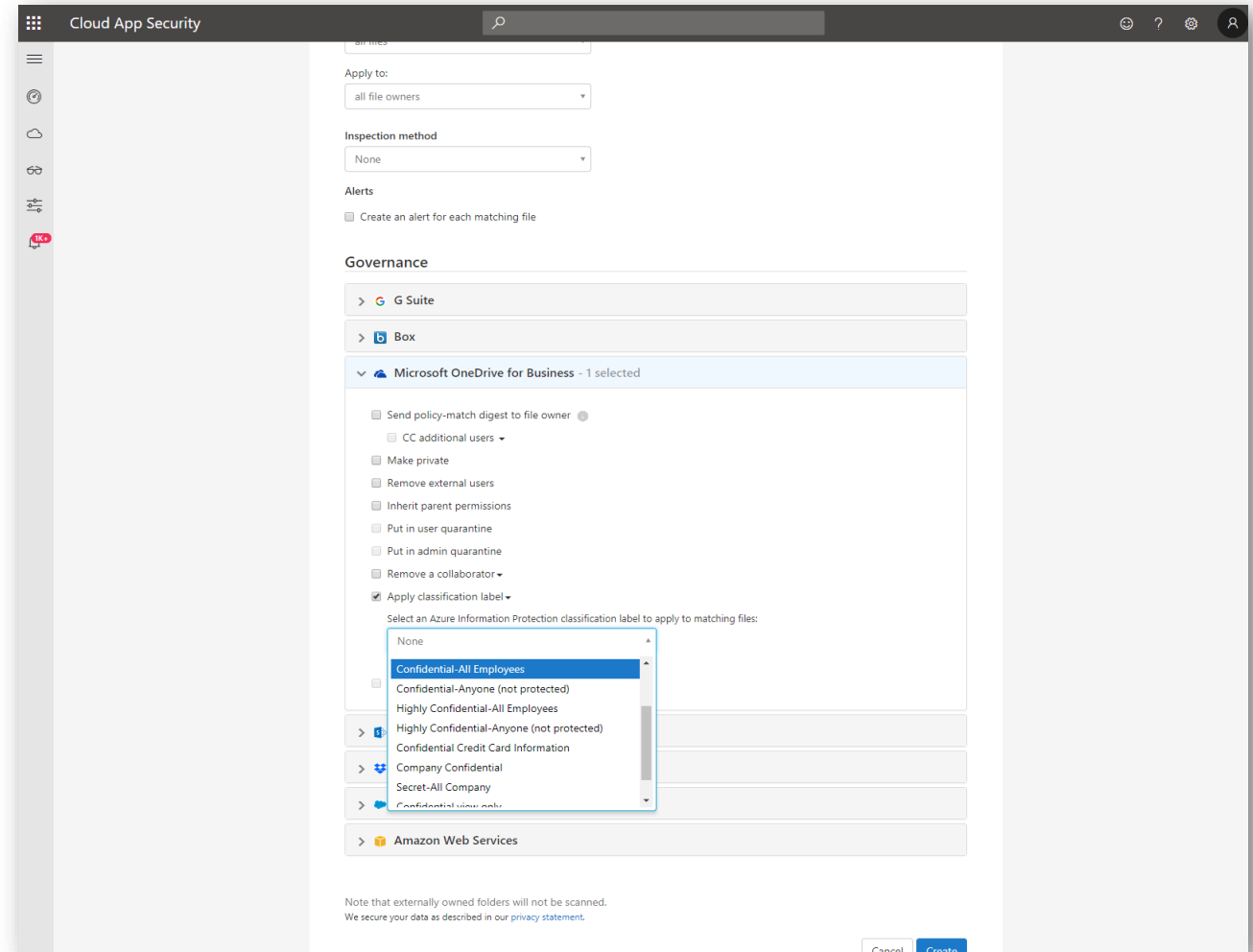
Powerful machine learning classifiers are put to work to help your Cloud App Security instance classify sensitive data types outside of the typical file types and data sources

Leverage any DLP engine for classification

Use your choice of data loss prevention engine to train your Cloud App Security instance or amplify your connections to Office DLP engines in addition to your custom set of classifications

Leverage AIP labels

Azure Information Protection labels work hard to provide simple and straightforward labels for your data so all your employees and admins know how to appropriately leverage your sensitive data



Finding and protecting data on SaaS



Discover



Investigate



Control



Alerts

Cloud App Security Discover Investigate Control Alerts 24 Search Settings Help User Microsoft

Policy center

TYPE: Select type... SEVERITY: Low Medium High NAME: Policy name... RISK CATEGORY: Select risk category... Advanced

1 - 6 of 6 Policies Create policy Filter

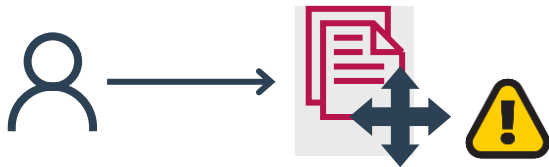
Report	Count	Severity	Risk category	Action	Modified
PCI COMPLIANCE: Publicly shared files with credit card info This policy identifies files containing credit card numbers and are publicly shared. Afte...	2 matches	High	Compliance		Jul 22, 2015
User logon from a non-categorized IP address Alert when a user logs on from an IP address that hasn't been included in a specific IP...	0 open alerts	High	—		Mar 8, 2016
Anomaly Detection Policy ADP	0 open alerts	High	—		Mar 8, 2016
Mass download by a single user Alert when a single user performs more than 30 downloads within 5 minutes.	0 open alerts	High	—		Mar 14, 2016
testing	0 open alerts	Medium	—		Mar 14, 2016
Demo for bla	0 open alerts	Medium	—	—	Mar 17, 2016

Scenario: oversharing from sanctioned SaaS

- 1 IT department sanctions SaaS application and provisions user access



- 2 User uploads sensitive file to SaaS and shares openly with everyone



- 3a Cloud app security detects oversharing of sensitive document, quarantines it, and issues alert

3

Unknown parties find and access the document, creating business risk



Mobile Application Management (MAM)

Works with or without MDM

Strong protections for corporate data

Restrict “Save as” and cut/copy/paste

Secure viewing of PDFs, images, videos

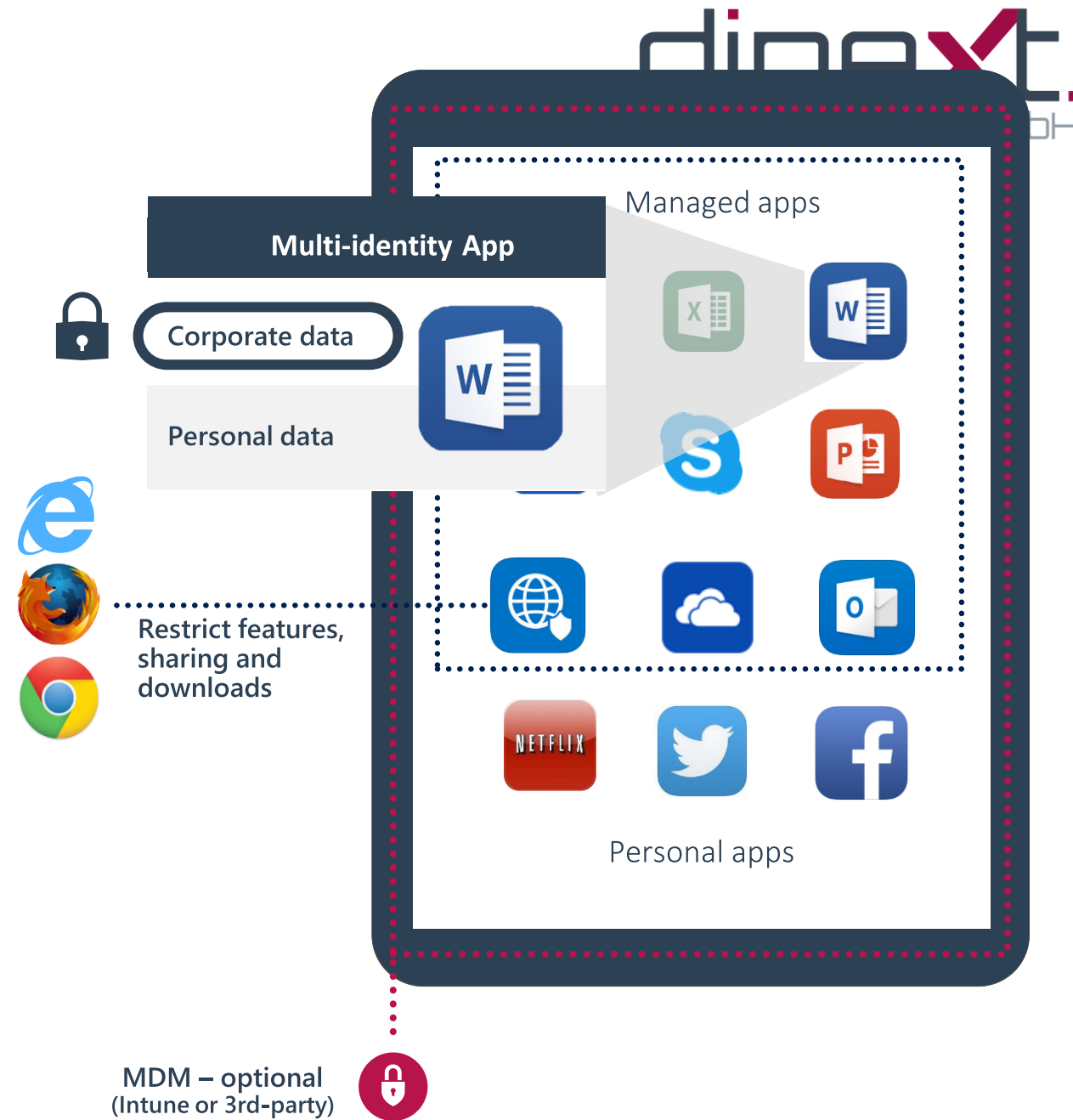
App encryption at rest

App access control – PIN or credentials

Managed web browsing

Support multi-identity applications

Selective wipe of corporate data without affecting personal data



Secure the data, not just the SQL database

Automated **discovery** of sensitive data

Labeling (tagging) sensitive data on column level with persistency

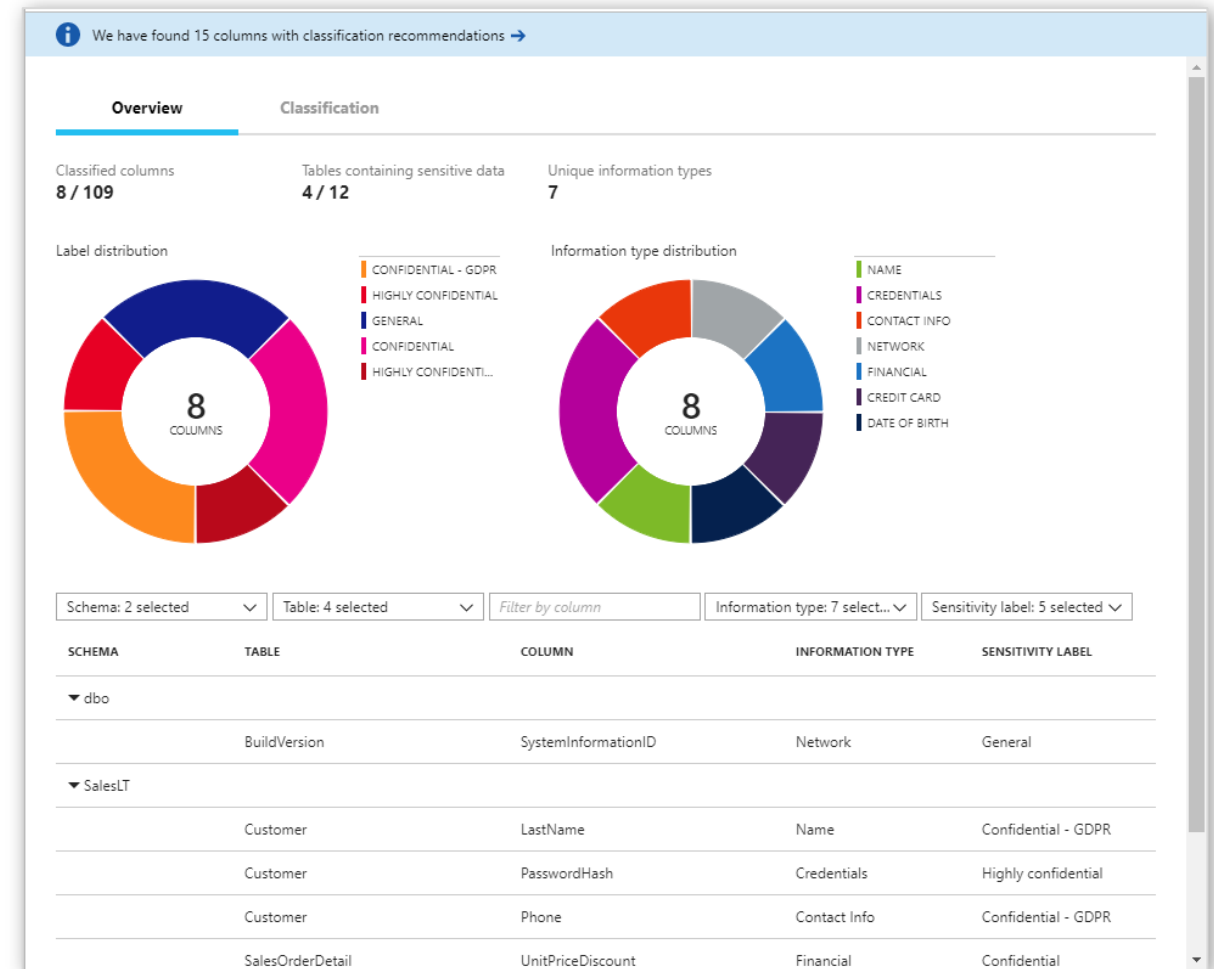
Classification as **infrastructure** for **protection & compliance**

Audit access to sensitive data

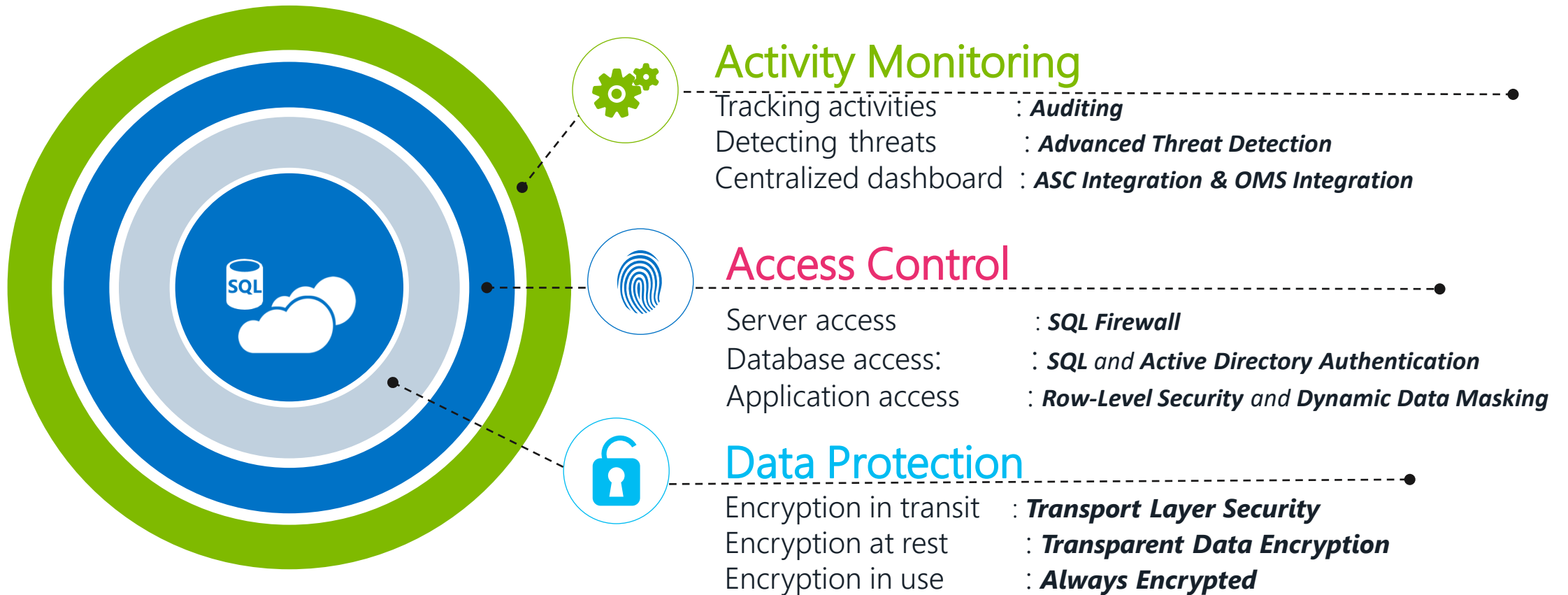
Sensitivity metadata flows with data for **protection outside database boundaries**

Hybrid – cloud + on-premises

Centralized IP policy management



Securing Structured Data in Azure SQL



Compliance: FedRAMP, HIPAA, PCI, EU Model Clauses , UK G-Cloud, ISO,
(government), (medical), (payment), (personal), (public sector)

Data protection & data governance go hand-in-hand

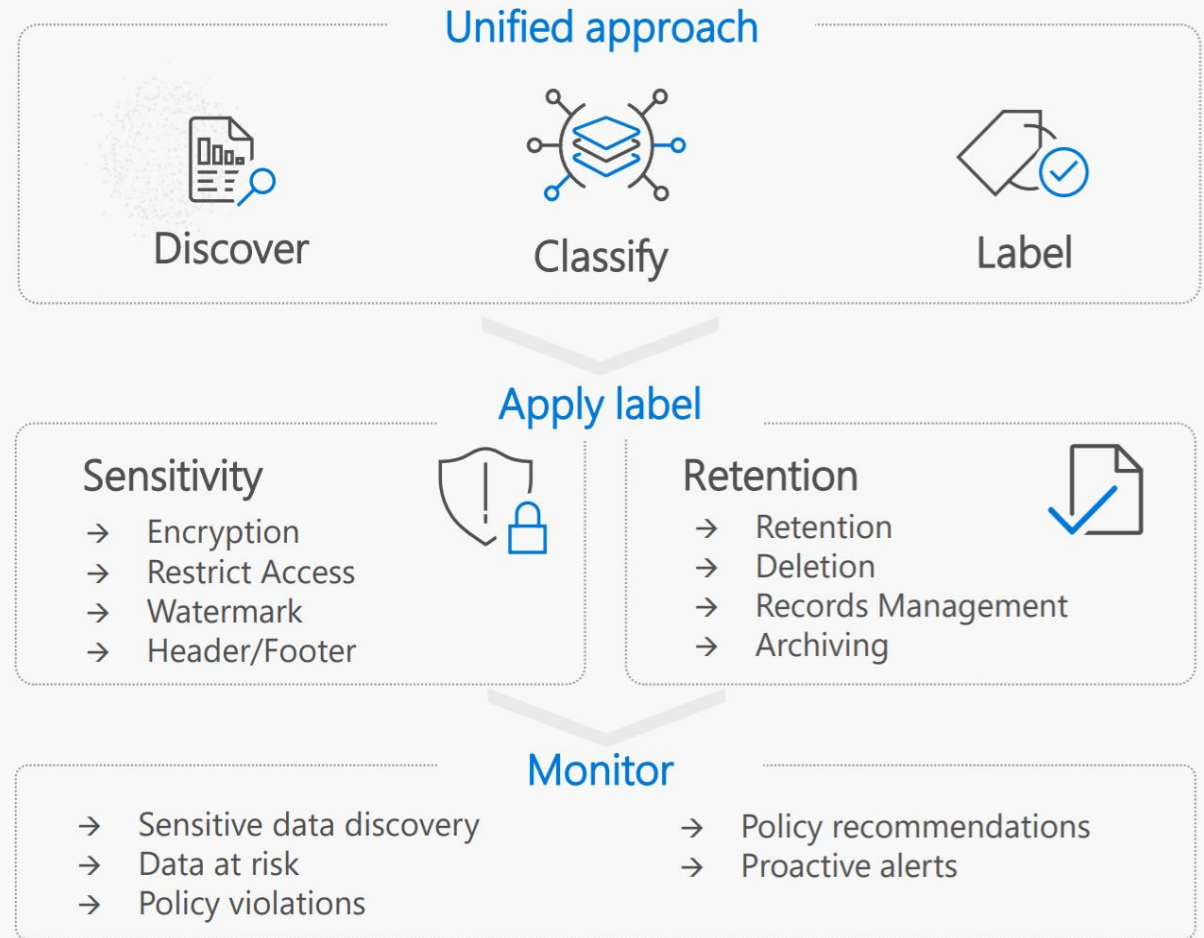
Comprehensive policies to protect and govern your most important data – throughout its lifecycle

Unified approach to discover, classify & label

Automatically apply policy-based actions

Proactive monitoring to identify risks

Broad coverage across locations



Compliance Manager

[Overview](#)
[Improvement actions](#)
[Solutions](#)
[Assessments](#)
[Assessment templates](#)

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

Overall compliance score

Your compliance score: 63%



12525/19571 points achieved

Your points achieved ⓘ

1004/ 8050

Microsoft managed points achieved ⓘ

11521/ 11521

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

Key improvement actions

Not completed **574**
 Completed **38**
 Out of scope **0**

Improvement action	Impact	Test status	Group	Action type
Conceal information with lock screen	+27 points	• None	Default Group	Technical
Use IRM to protect email messages and att...	+27 points	• None	Default Group	Technical
Use boundary protection devices for uncla...	+27 points	• None	Default Group	Technical
Use IRM to protect online documents and ...	+27 points	• None	Default Group	Technical
Require mobile devices to use encryption	+27 points	• None	Default Group	Technical
Use S/MIME	+27 points	• None	Default Group	Technical
Manage organizational users and groups	+27 points	• None	Default Group	Technical
Assign roles to endpoint users	+27 points	• None	Default Group	Technical
Ensure sufficient strength for authenticators	+27 points	• None	Default Group	Technical

Solutions that affect your score

Taking key actions in your compliance solutions will increase overall score.

Solution	Score contribution	Remaining
Audit	0/92 points	12
Azure	0/1 points	1
Azure Active Direct...	114/509 points	25
Azure Information P...	0/297 points	11
Azure Security Center	0/1 points	1
Cloud App Security	0/56 points	12
Communication co...	0/36 points	4
Compliance Manager	36/2515 points	311
Data classification	0/30 points	2

Compliance Manager

Overview Improvement actions Solutions Assessments Assessment templates

Actions you can take to improve your compliance score. Points may take up to 24 hours to update.

[Export](#) [Accept all updates](#) [Assign to user](#)

574 items

Filter [Reset](#) [Filters](#)

Regulations: **Any** ▾

Solutions: **Any** ▾

Groups: **Any** ▾

Test Status: **None, Not assessed, Failed low risk, +5** ✕

Categories: **Any** ▾

Assigned To: **Any** ▾

Improvement action	Points achieved	Regulations	Group	Solutions	Assessments	Categories	Test status	Action Type
Conceal information with lock screen	0/27	Data Protection Baseline	Default Gro...	Windows 10	Data Protection Baseline	Manage devices	• None	Technical
Use IRM to protect email messages and attachm...	0/27	Data Protection Baseline	Default Gro...	Azure Informati...	Data Protection Baseline	Protect informa...	• None	Technical
Use boundary protection devices for unclassified...	0/27	Data Protection Baseline	Default Gro...	Compliance Ma...	Data Protection Baseline	Manage compli...	• None	Technical
Use IRM to protect online documents and storage	0/27	Data Protection Baseline	Default Gro...	Azure Informati...	Data Protection Baseline	Protect informa...	• None	Technical
Require mobile devices to use encryption	0/27	Data Protection Baseline	Default Gro...	Exchange Onlin...	Data Protection Baseline	Protect informa...	• None	Technical
Use S/MIME	0/27	Data Protection Baseline	Default Gro...	Exchange Onlin...	Data Protection Baseline	Protect informa...	• None	Technical
Manage organizational users and groups	0/27	Data Protection Baseline	Default Gro...	Microsoft 365 a...	Data Protection Baseline	Control access	• None	Technical
Assign roles to endpoint users	0/27	Data Protection Baseline	Default Gro...	Intune	Data Protection Baseline	Manage devices	• None	Technical
Ensure sufficient strength for authenticators	0/27	Data Protection Baseline	Default Gro...	Compliance Ma...	Data Protection Baseline	Manage compli...	• None	Technical

Use a template to help you create assessments for your organization. Templates contain the controls and action data needed to track compliance with regulations, standards, and policies.

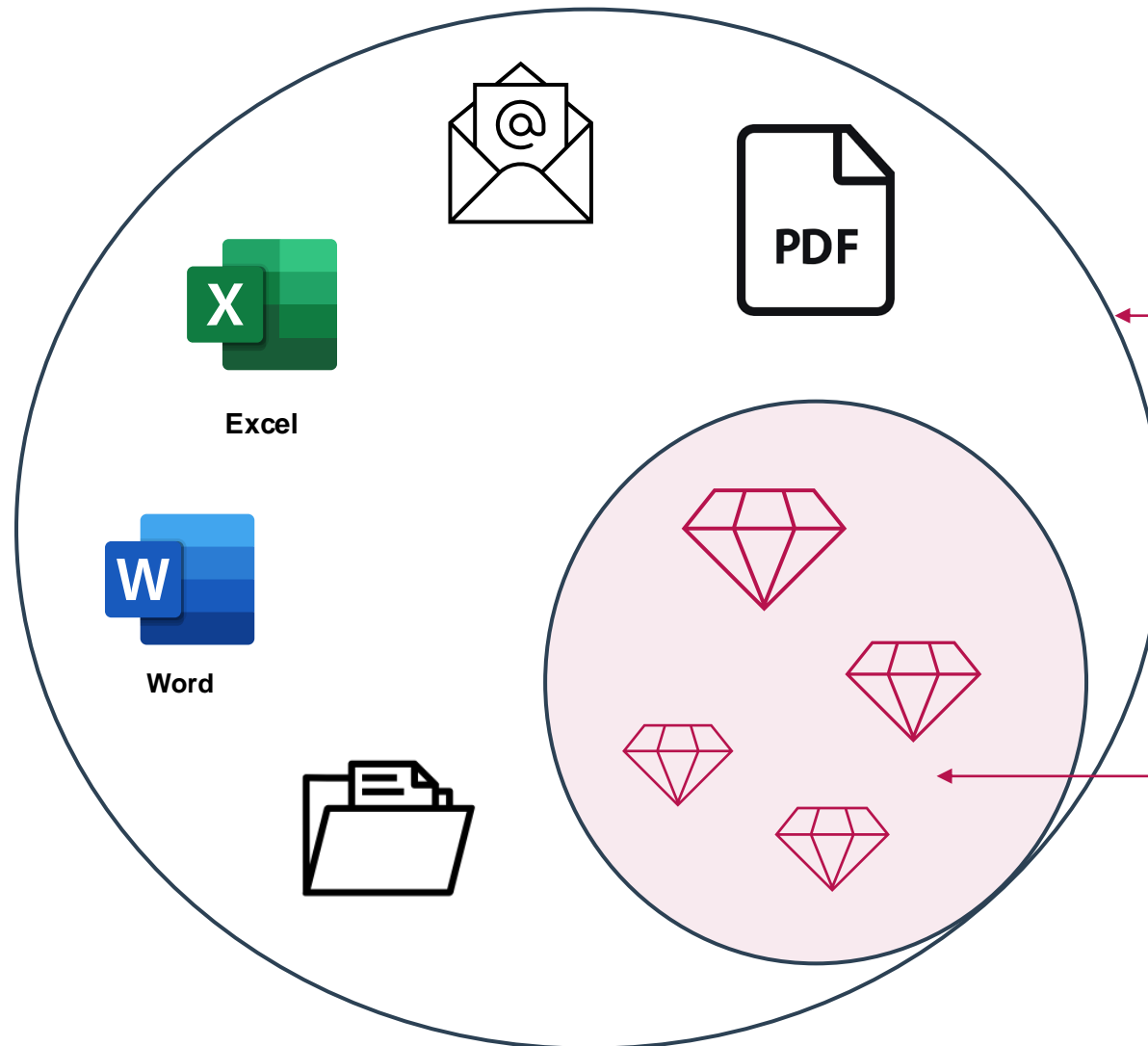
Activated/Licensed templates

0/0

[View details](#)[+ Create new template](#) [→ Export all actions](#)Filter  Reset  FiltersProduct scope: **Any** ▾ Certification: **Any** ▾ Created by: **Any** ▾

Assessment template	Availability	Product scope	Certification	Created by	Last updated
Included templates (5)					
EU GDPR	Included	Microsoft 365	EU GDPR	Microsoft	3/13/2021
Data Protection Baseline	Included	Microsoft 365	Data protection baseline	Microsoft	3/13/2021
ISO/IEC 27001:2013	Included	Microsoft 365	ISO 27001	Microsoft	3/13/2021
NIST 800-53 rev.4	Included	Microsoft 365	NIST 800-53	Microsoft	3/19/2021
NIST 800-53 rev.5	Included	Microsoft 365	NIST 800-53 rev.5	Microsoft	3/13/2021
Premium templates (328)					
CAN-SPAM Act	Premium	Microsoft 365	CAN-SPAM Act	Microsoft	2/23/2021
Computer Fraud and Abuse Act (CF...	Premium	Microsoft 365	CFAA	Microsoft	2/23/2021

Information Governance & Retention



Information Governance

Manage risk & liability by only keeping what you need and deleting what you don't across your entire digital estate.

Records Management

Manage high value content following the specialized workflows required to meet legal, business or regulatory recordkeeping obligations.

Information Governance

Retention policies and retention labels

Retain or delete content with policy management and a deletion workflow for email, documents, instant messages, and more

Archive third-party data

Import, archive, and apply compliance solutions to third-party data from social media platforms, instant messaging platforms, and document collaboration platforms

A large, downward-pointing chevron shape in a dark red color, containing the word 'Admin' in white text.

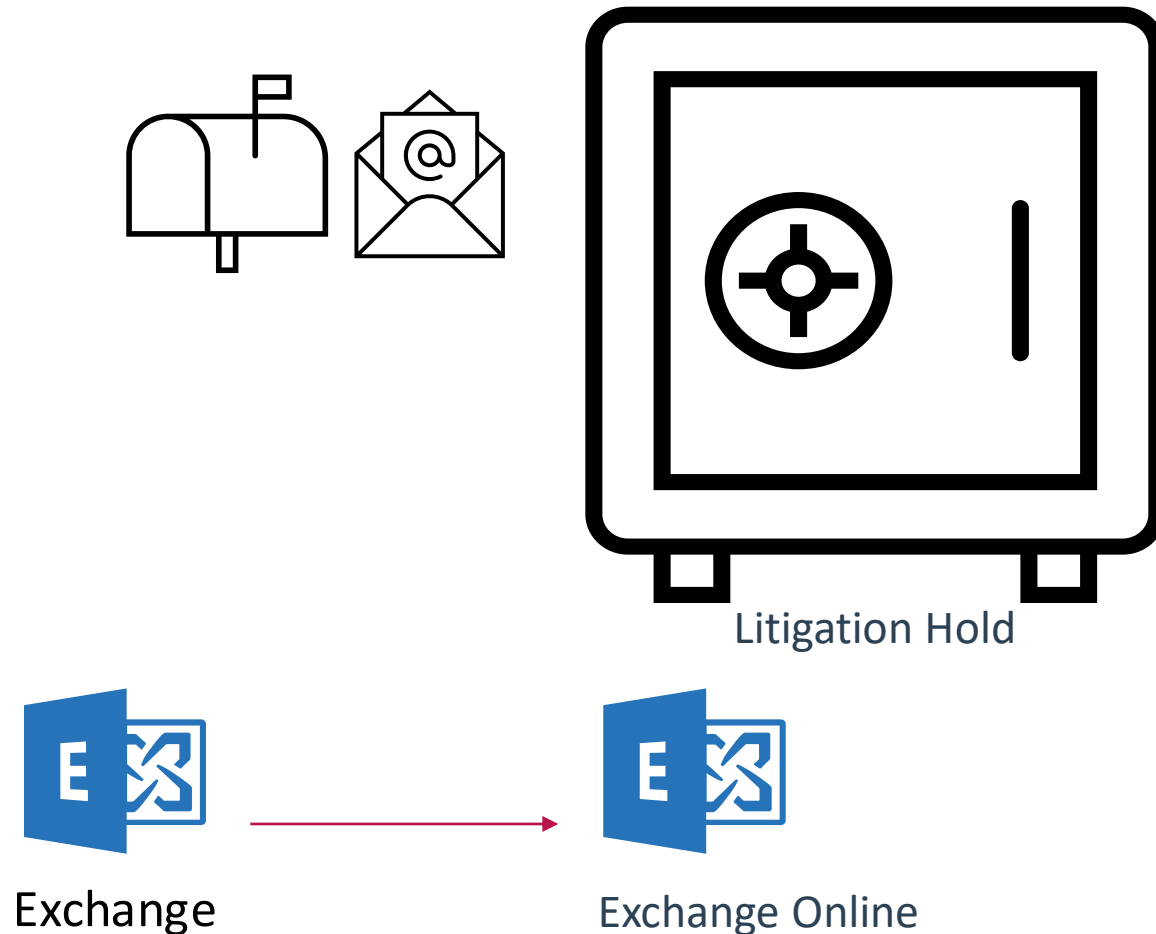
Admin

- Creates and auto-apply label
- creates policy and assigns label to location

A large, downward-pointing chevron shape in a dark red color, containing the text 'Office 365' in white text.

Office 365

- automatically applies label to content that matches the specified conditions
- Enforces retention rules on the content based on the applies label



Inactive mailboxes

Retain mailbox content after employees leave the organization

Import service (EX to EXO)

Bulk-import PST files to Exchange Online mailboxes to retain and search email messages for compliance or regulatory requirements

Records Management

A single solution for email and documents that incorporates retention schedules and requirements into a **file plan** that supports the full lifecycle of your content with records declaration, retention, and disposition

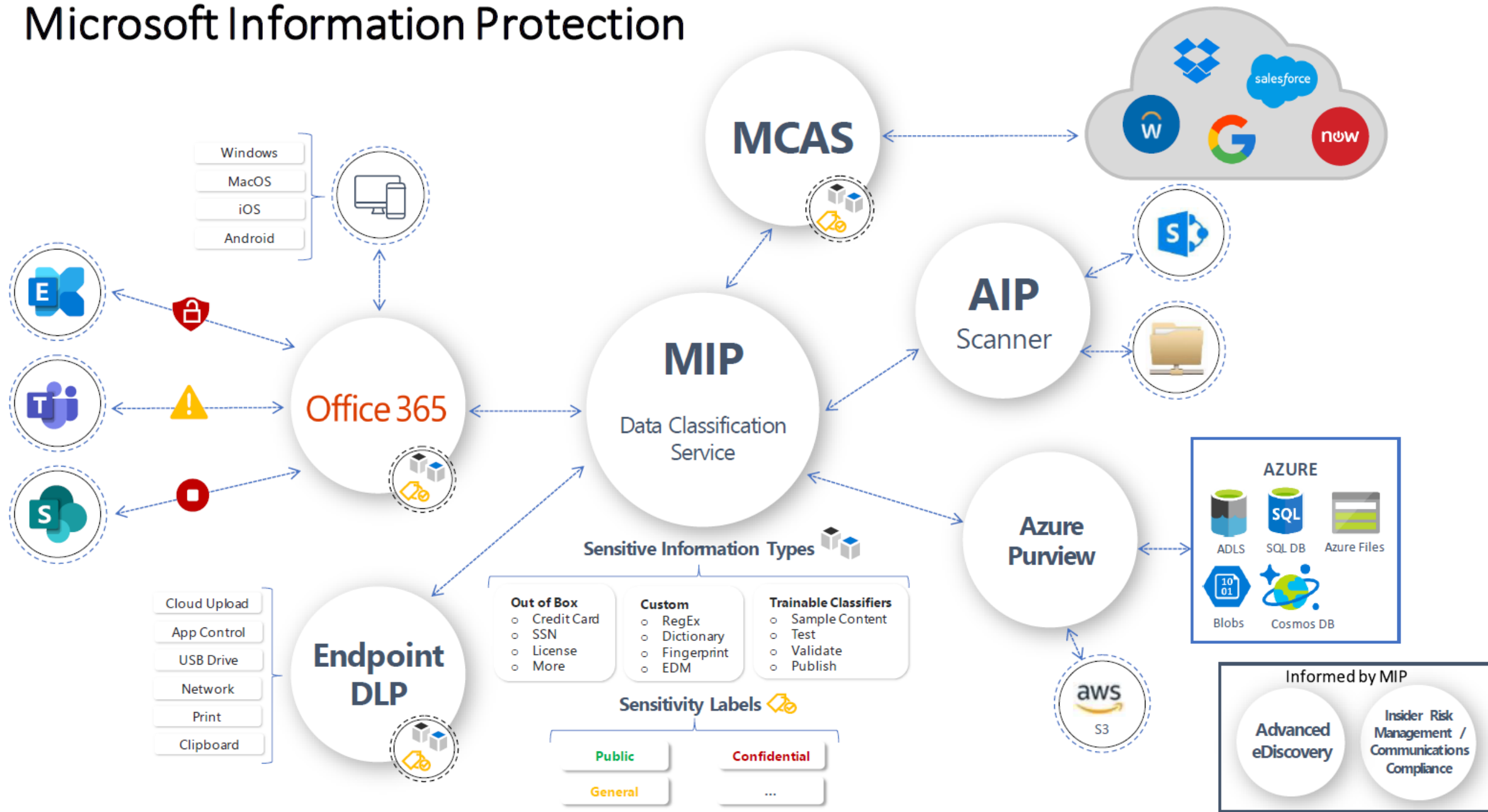
- Label content as a record. Create and configure retention labels to mark content as a record that can then be applied by users or automatically applied by identifying sensitive information, keywords, or content types.
- Migrate and manage your retention requirements with file plan. By using a file plan, you can bring in an existing retention plan to Microsoft 365, or build a new one for enhanced management capabilities.
- Configure retention and deletion settings with retention labels. Configure retention labels with the retention periods and actions based on various factors that include the date last modified or created.

Records Management

A single solution for email and documents that incorporates retention schedules and requirements into a **file plan** that supports the full lifecycle of your content with records declaration, retention, and disposition

- Start different retention periods when an event occurs with event-based retention.
- Review and validate disposition with disposition reviews and proof of records deletion.
- Export information about all disposed items with the export option.
- Set specific permissions for records manager functions in your organization to have the right access.
- Much more which is way above the scope of this presentation.

Microsoft Information Protection



dinext.

create your digital tomorrow



Holger Radecke



+49 1514 405 0964



holger.radecke@dinext.de



dinext.de

dinext.
pi-sec GmbH

Microsoft Defender for
Office 365



Email is the prevalent attack vector

91%

of cyberattacks start
with email



60%

Increase in Phish
in 2019



\$30B

in losses related to
BEC since July 2016



300%

Increase in attacks
on Identity



20% in 5 min

Clicks on URLs



68%

of breaches take > 1
month to discover



Email Filtering Overview - Inbound

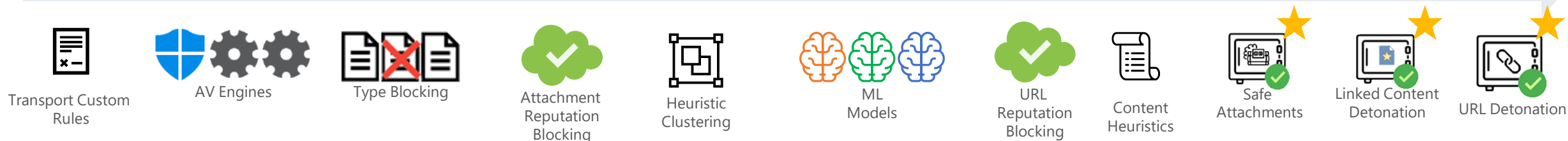
edge protection



sender intelligence



content filtering



post-delivery protection



★ MDO only

ZAP can act on emails due to mail content, URLs, or attachments.

Malware



ZAP enabled in Policy

Message not older than 48 hours

Phish



ZAP enabled in Policy

Message not older than 48 hours
and not marked safe by the policy

Policy set to take action

Junk mail processing is enabled for
the recipient (for action Move to
JMF)

Spam



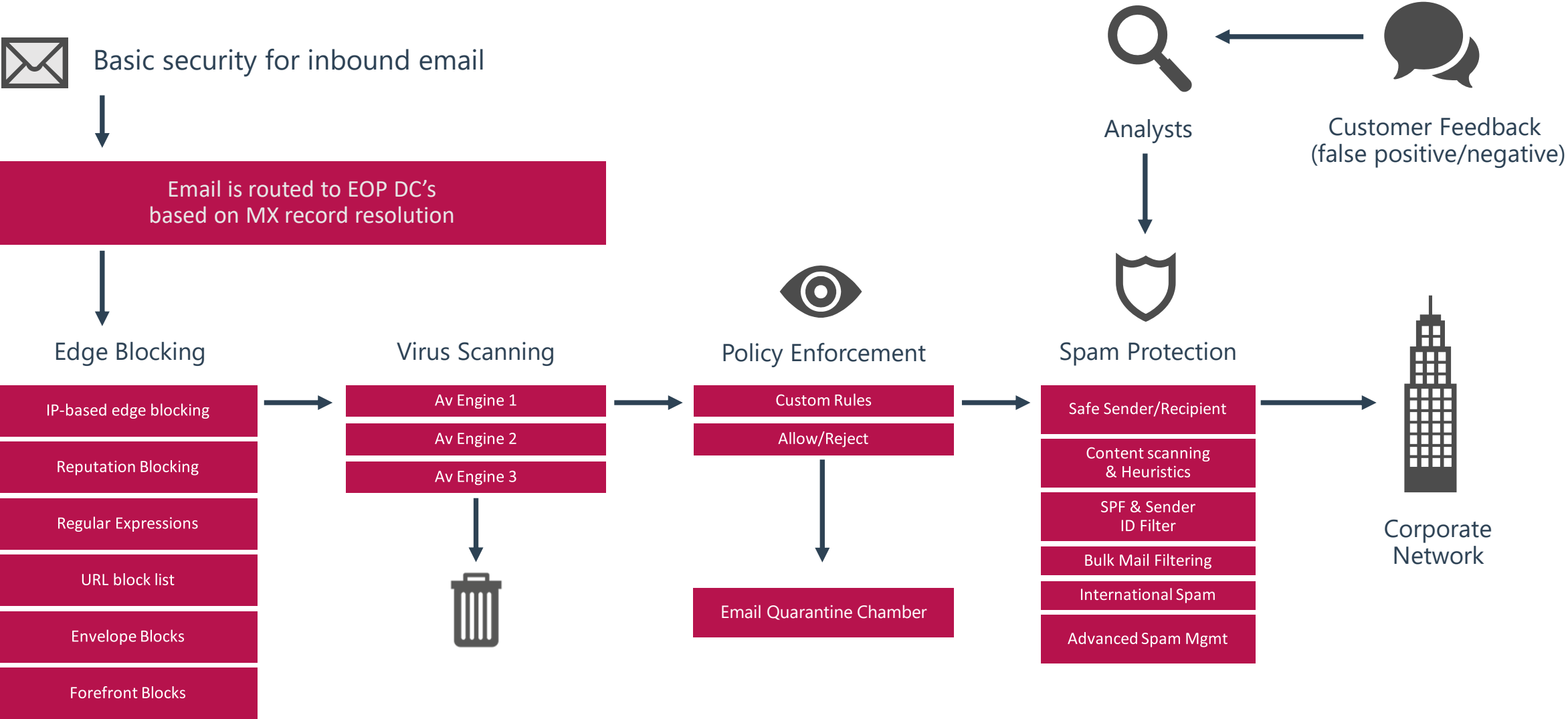
ZAP enabled in Policy

Message is **unread** not older than
48 hours and not marked safe by
the policy

Policy set to take action

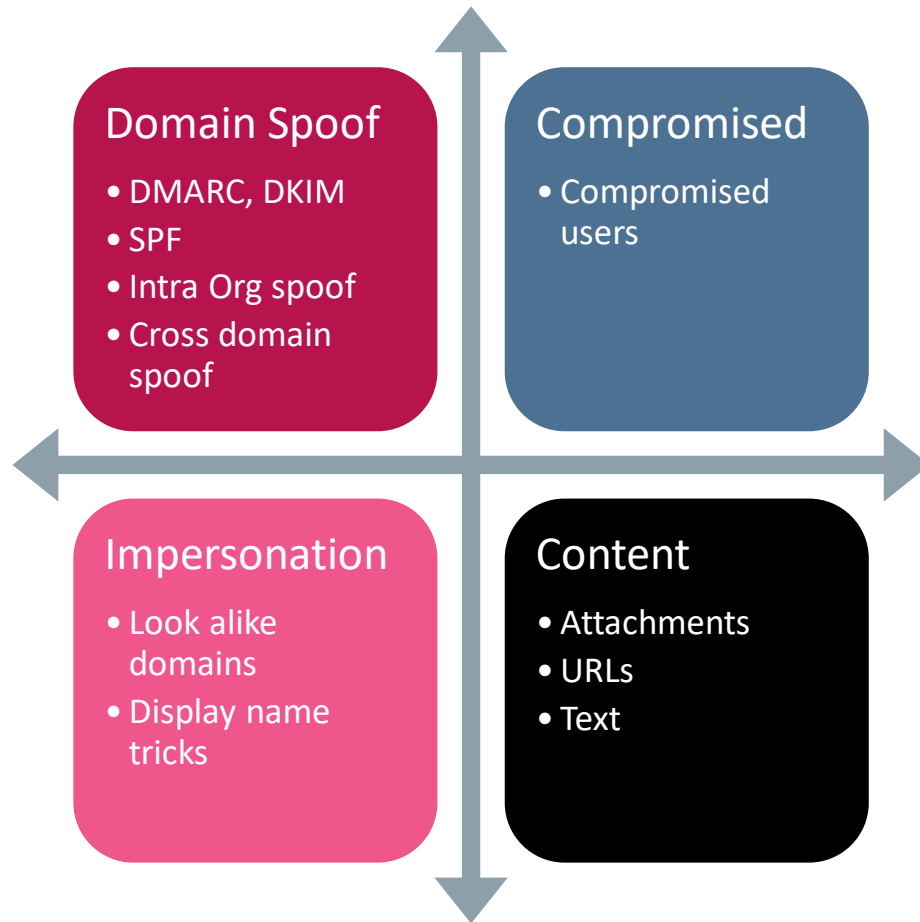
Junk mail processing is enabled for
the recipient (for action Move to
JMF)

Protect your data



Protect business critical data

Attack vectors used in email phishing



Standard protection

- Implicit Spoof Protection; DMARC; SPF
- Content based protection
- URL verification against known phishing lists
- Safety Tips for mails detected as phish
- Inline Reporting

Advanced protection

- Machine Learning Models
- Time of Click Protection (Safe links)
- Detonation of Content
- Users contact graph
- Automated Investigation & Response

Microsoft Defender for Office 365 offerings



Exchange Online Protection

Preventing broad
and volume-based
& known attacks



MDO 365 P1

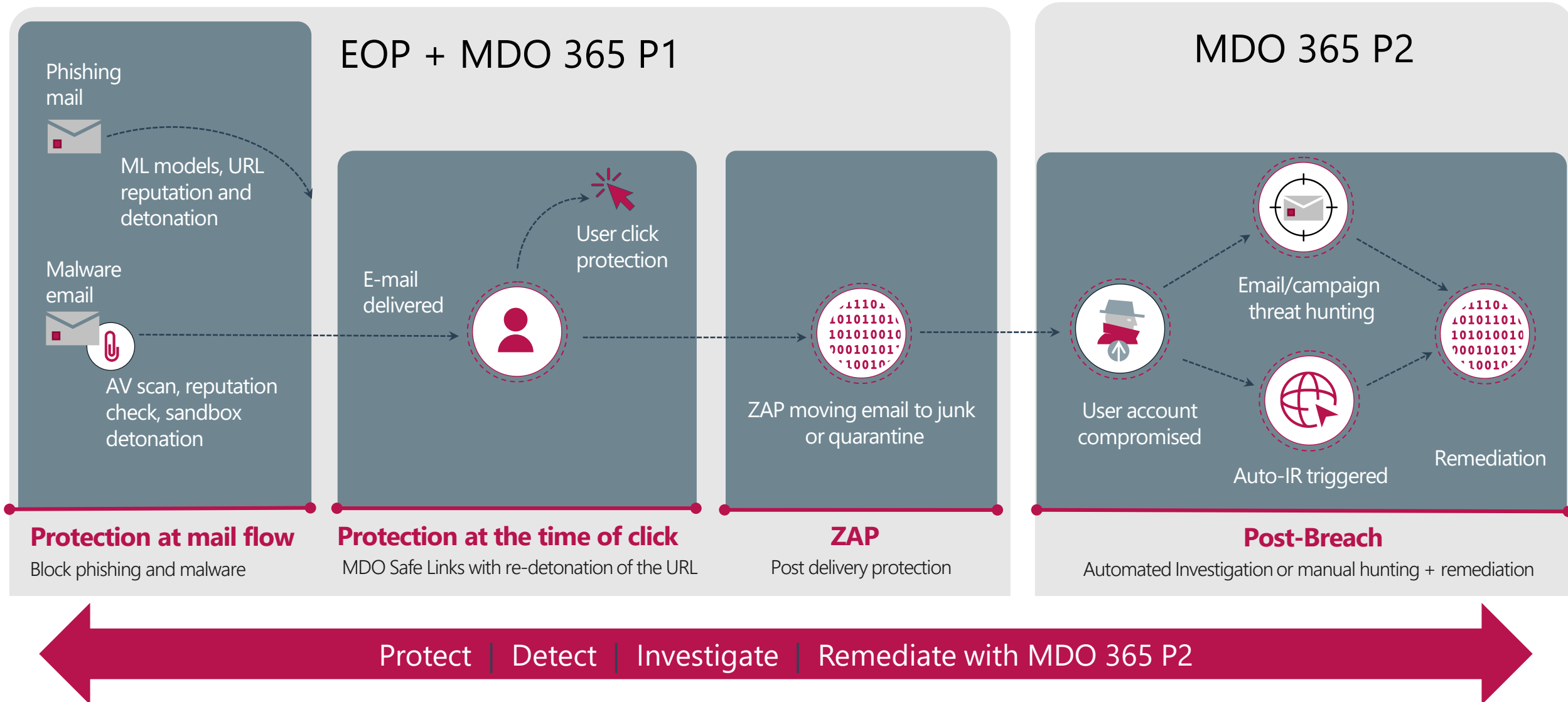
Protecting from
zero-day malware, URLs,
Business email compromise



MDO 365 P2

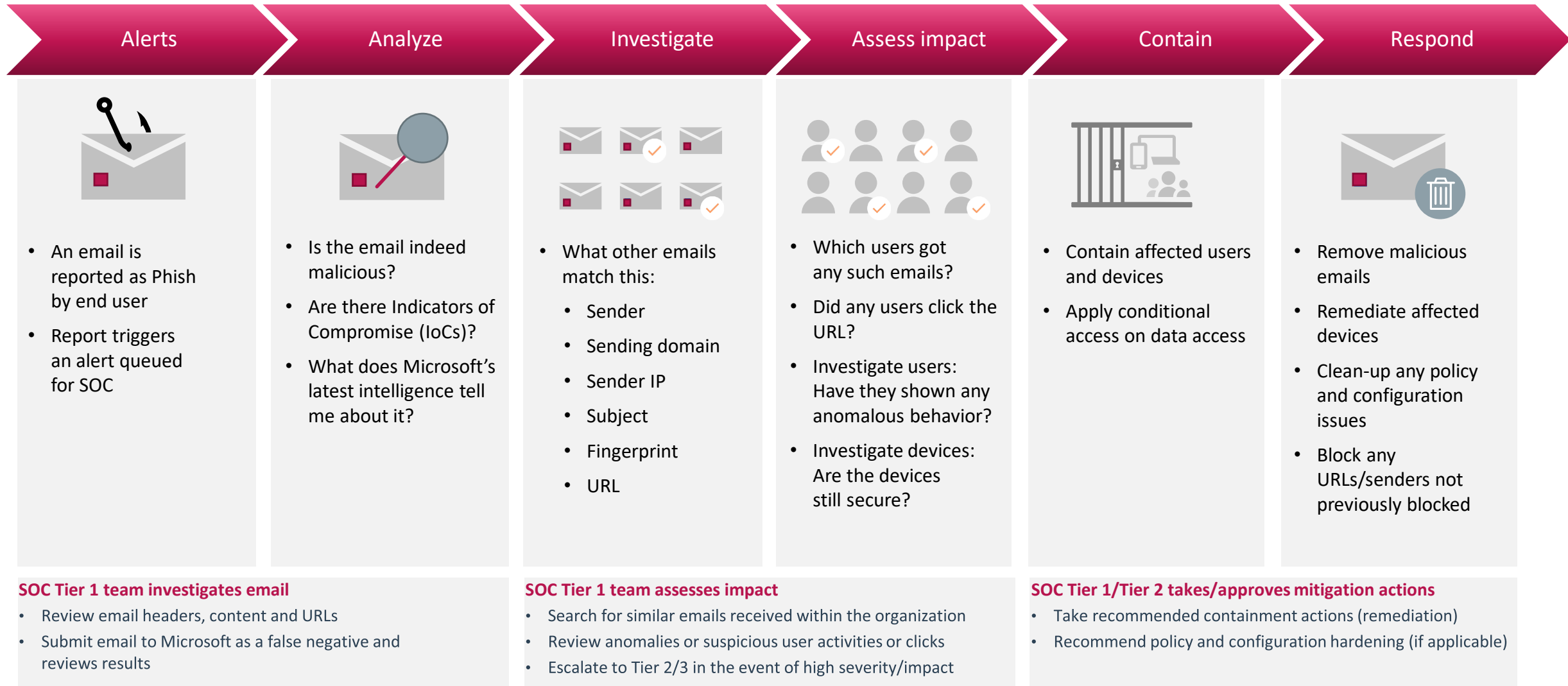
Post Breach Investigation,
Response, Automation and
Simulation/Training

MDO protection across the attack kill chain

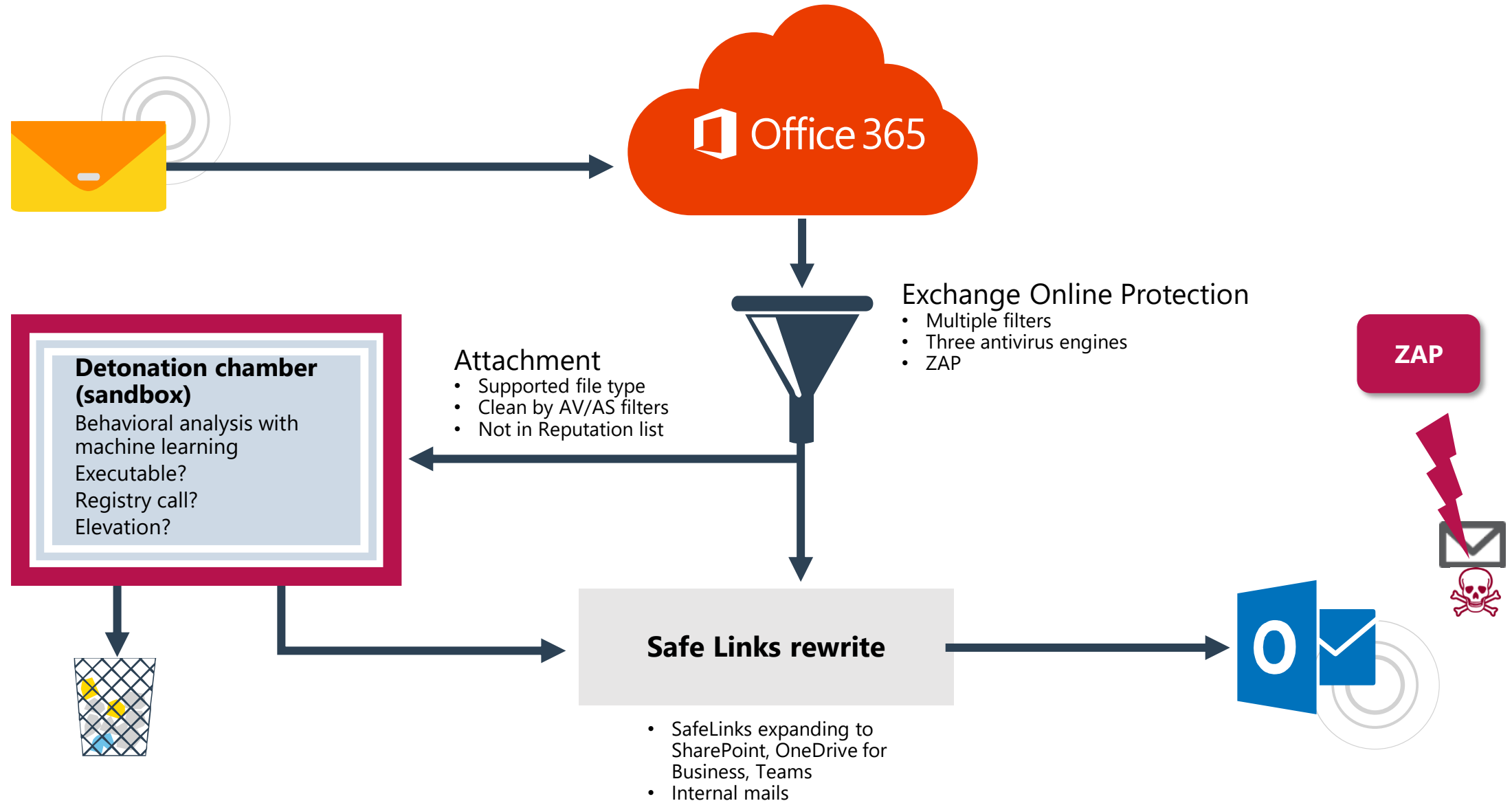


A day in the life of Security Operations teams

C-suite receives a suspicious message and reports it to the security team.

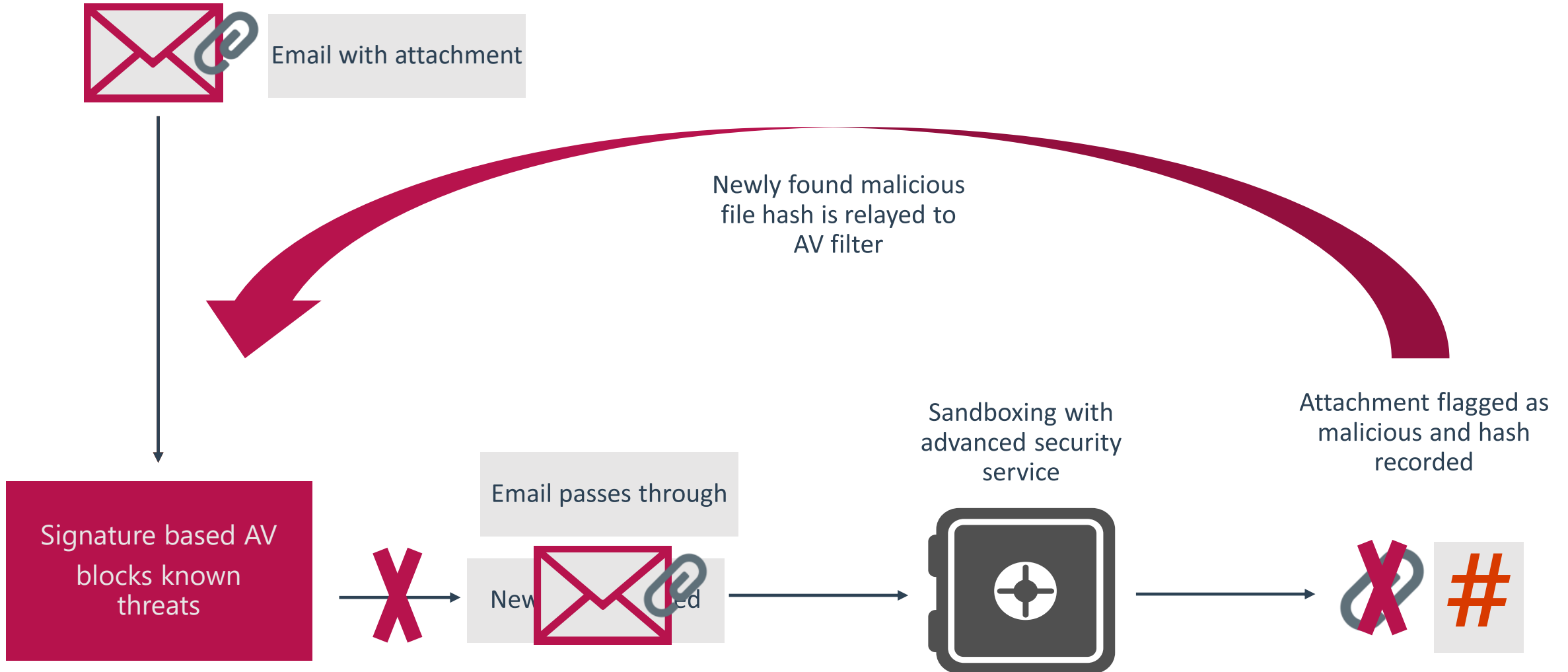


MDO Service Architecture



Protect your data

Our systems continuously update and enhance: Updating known "malware" after discovery of unknown file hash



Safe Attachments

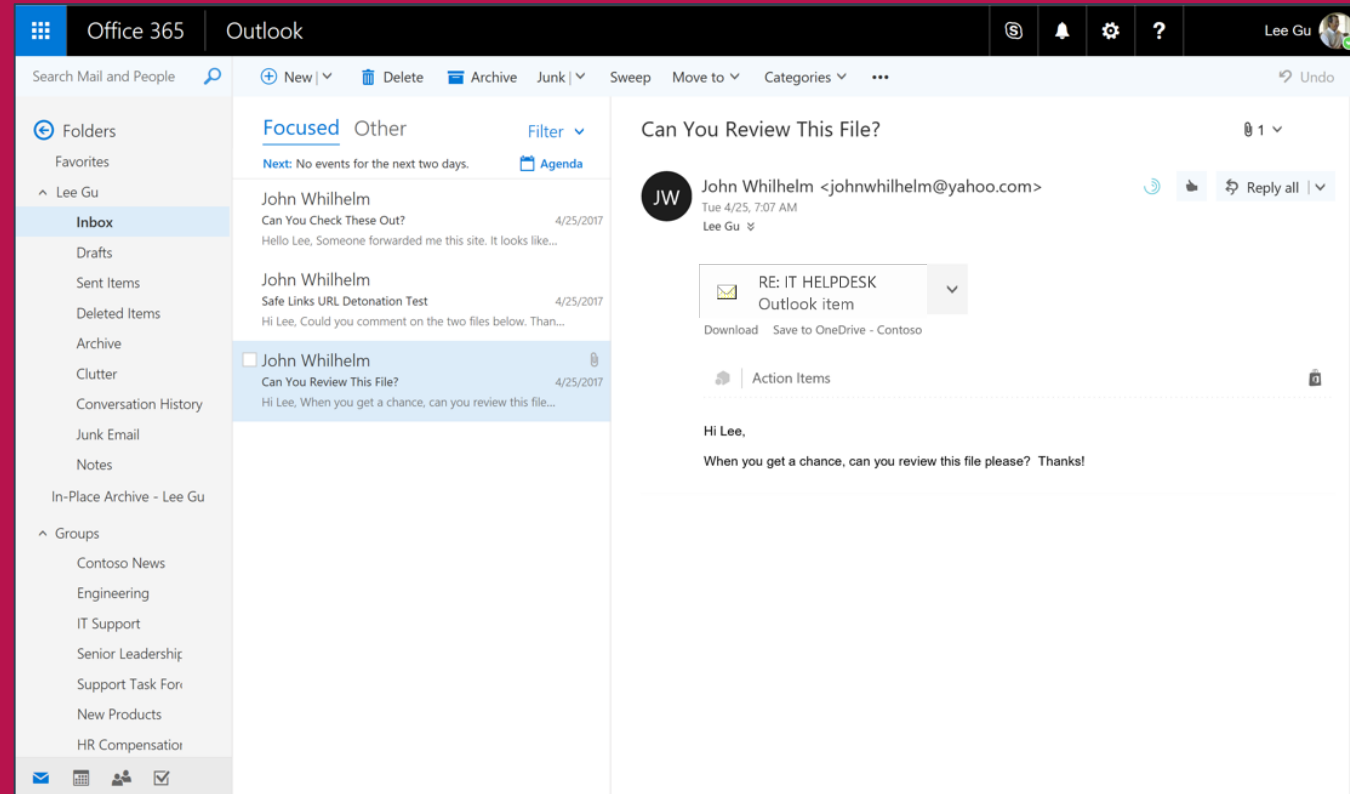
Detonate malicious attachments



Observed Behavior

Network Traffic

Downloaded Files



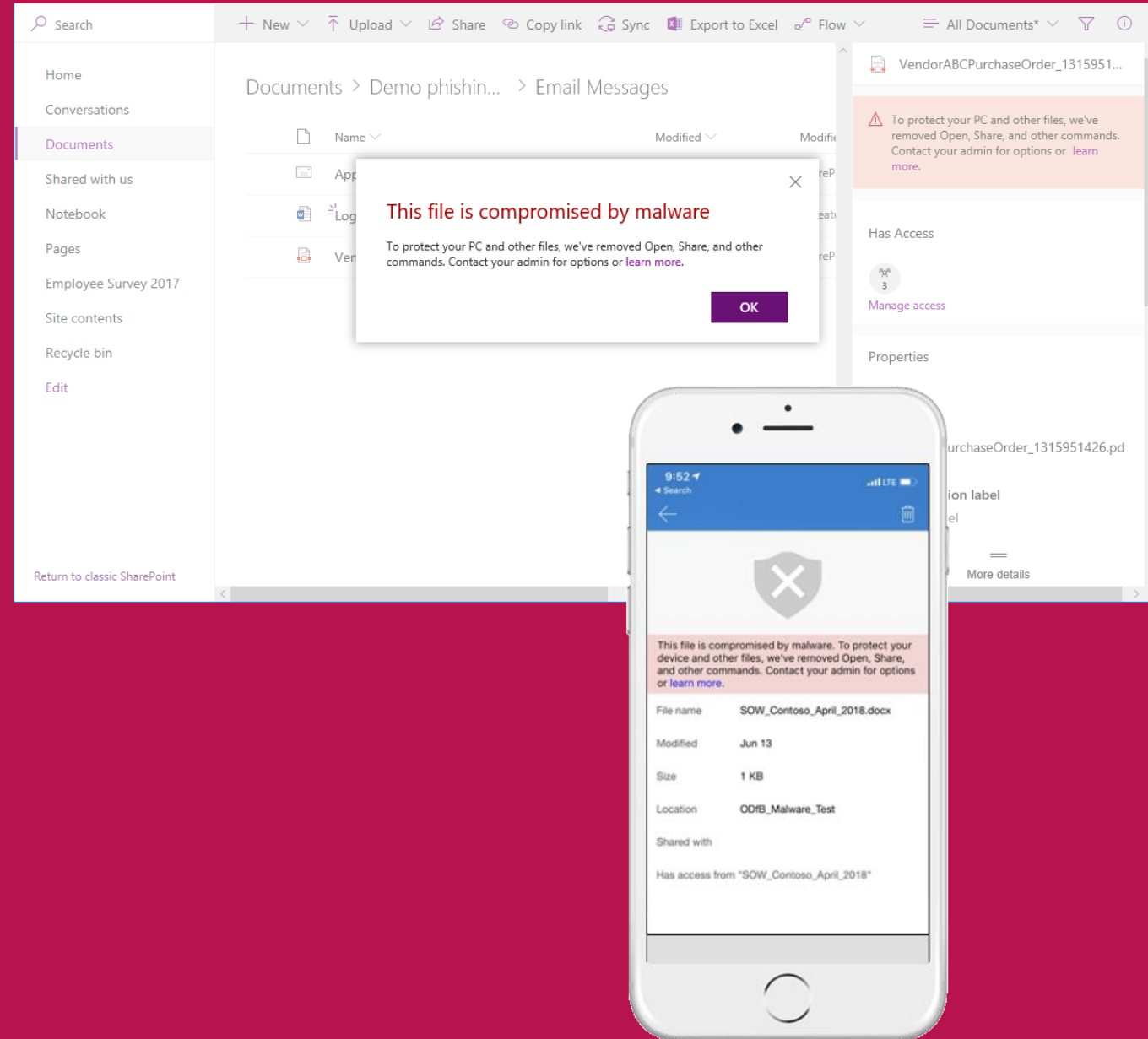
11B

Unique items
detonated in the MDO
sandbox in 2018

Safe Attachments

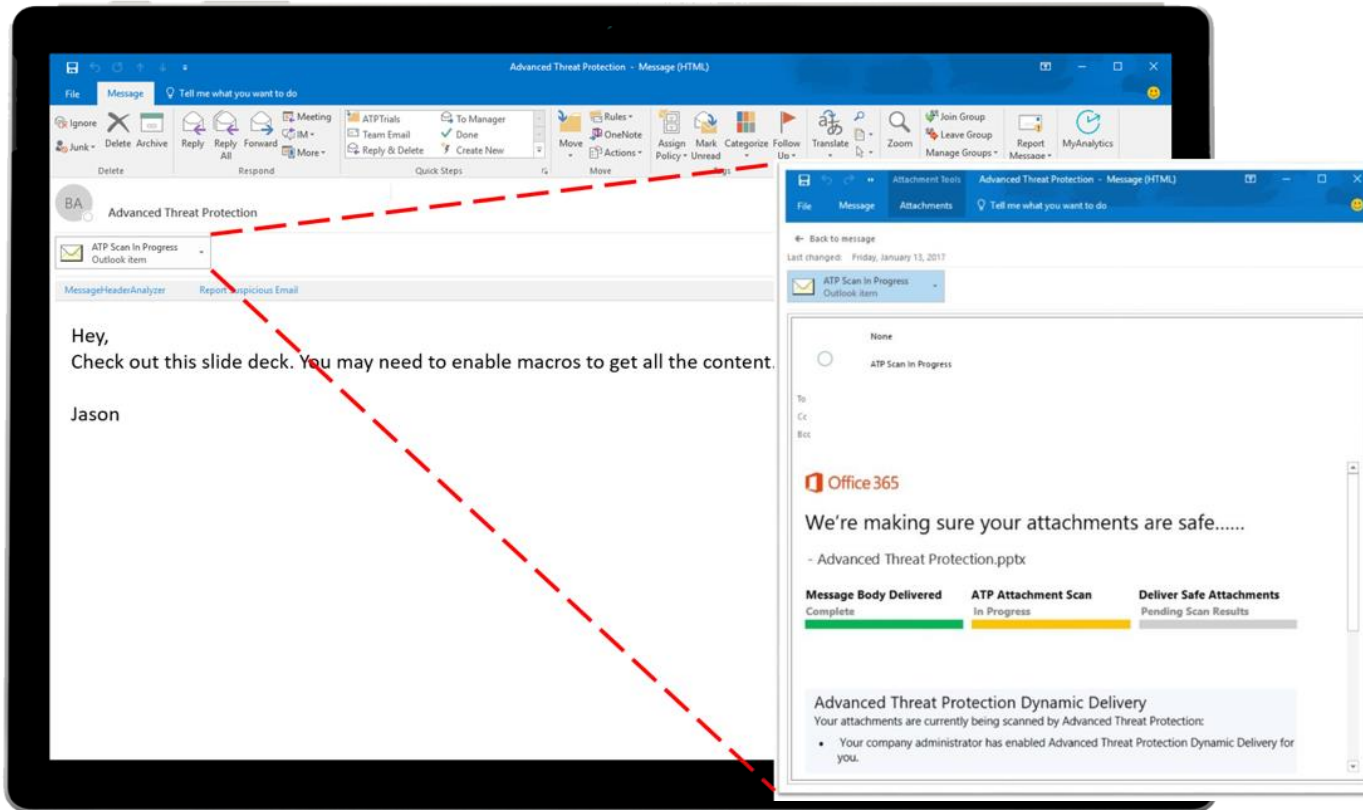
For SharePoint & OneDrive for Business

MDO Safe Attachments also scans for malicious files in SharePoint and OneDrive for Business by compromised, anonymous or guest accounts. When one is found, the file is locked down to prevent users from opening, sharing or downloading malicious content. Integrated experiences make users aware and guide them.

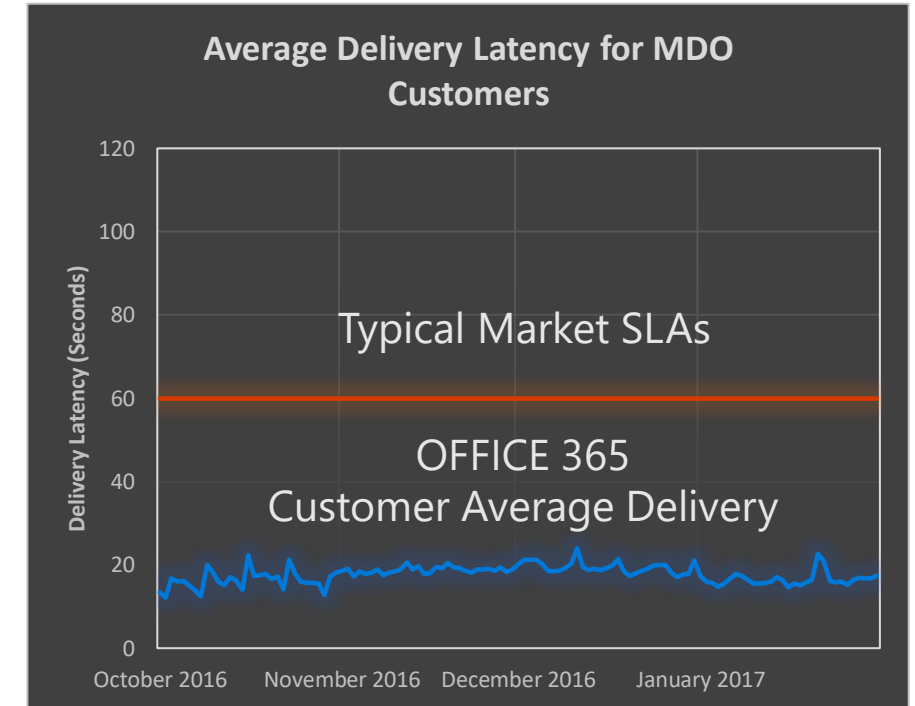


Protect your data

Our features and enhancements limit the impact to user productivity



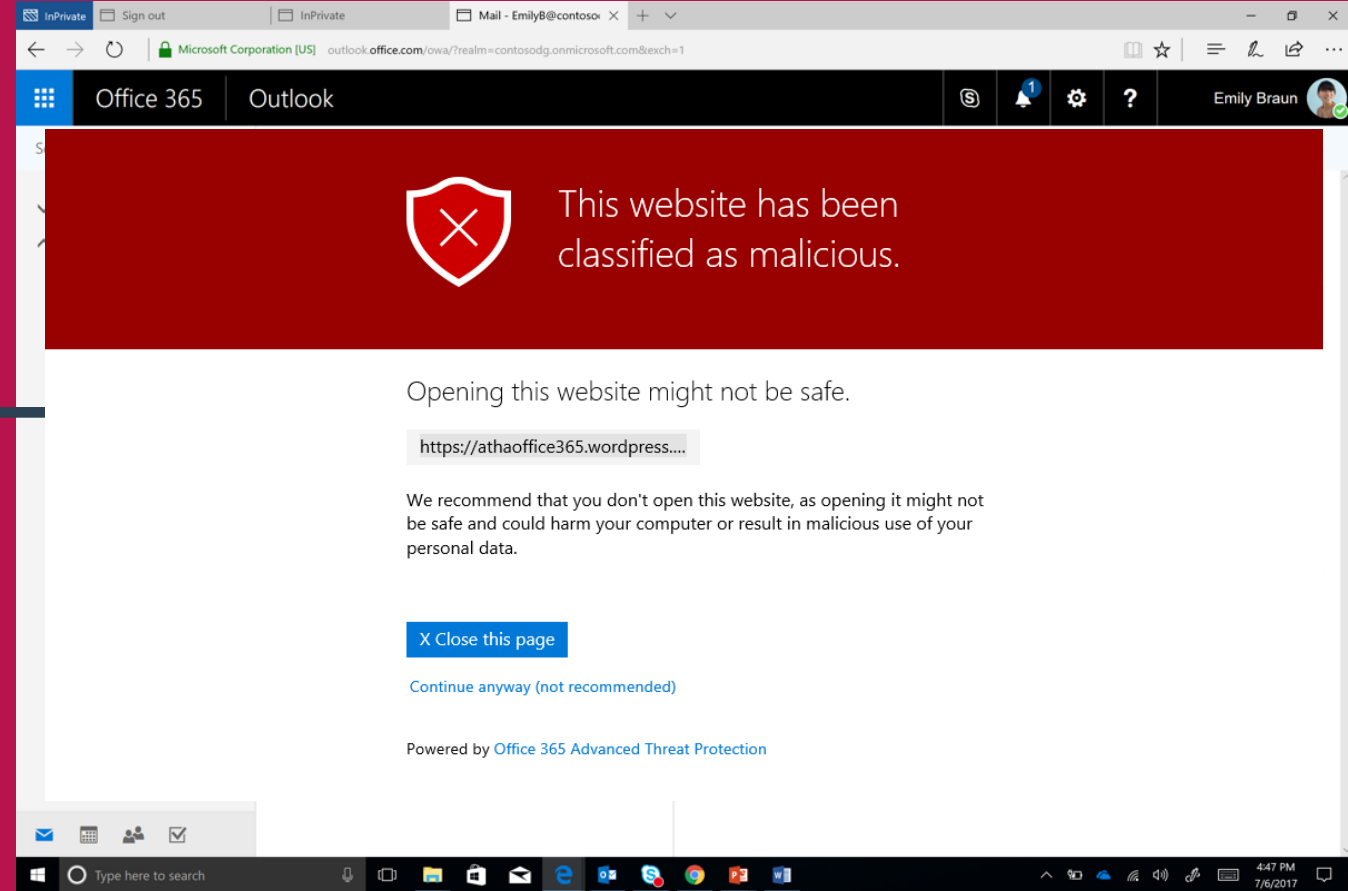
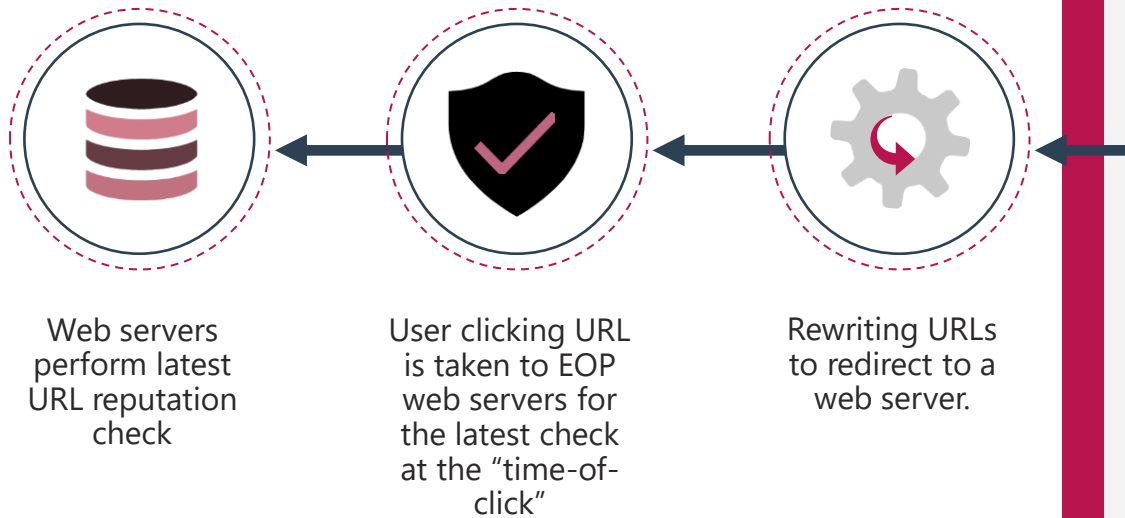
Dynamic delivery: Reducing the impact from sandboxing latency



Lower average latency than market SLAs

Safe Links Experience

Time-of-click protection for malicious links.



7B Safe Links URLs
protected in 2018

URL detonation

Time-of-click warnings provides granular details on why a link was flagged so they can understand when and why threats are blocked

Emails are analyzed to send **suspicious links for detonation**

Detonation happens in a **sandboxed environment** exposing thousands of signals about a file

Based on the verdict of detonation, users are **allowed or blocked** from following the link

Machine Learning models examining detonation artifacts **continuously improve**



This website has been classified as malicious.

Opening this website might not be safe.

<https://athaoffice365.wordpress...>

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

[X Close this page](#)

[Continue anyway \(not recommended\)](#)

Powered by [Office 365 Advanced Threat Protection](#)

Native Link rendering

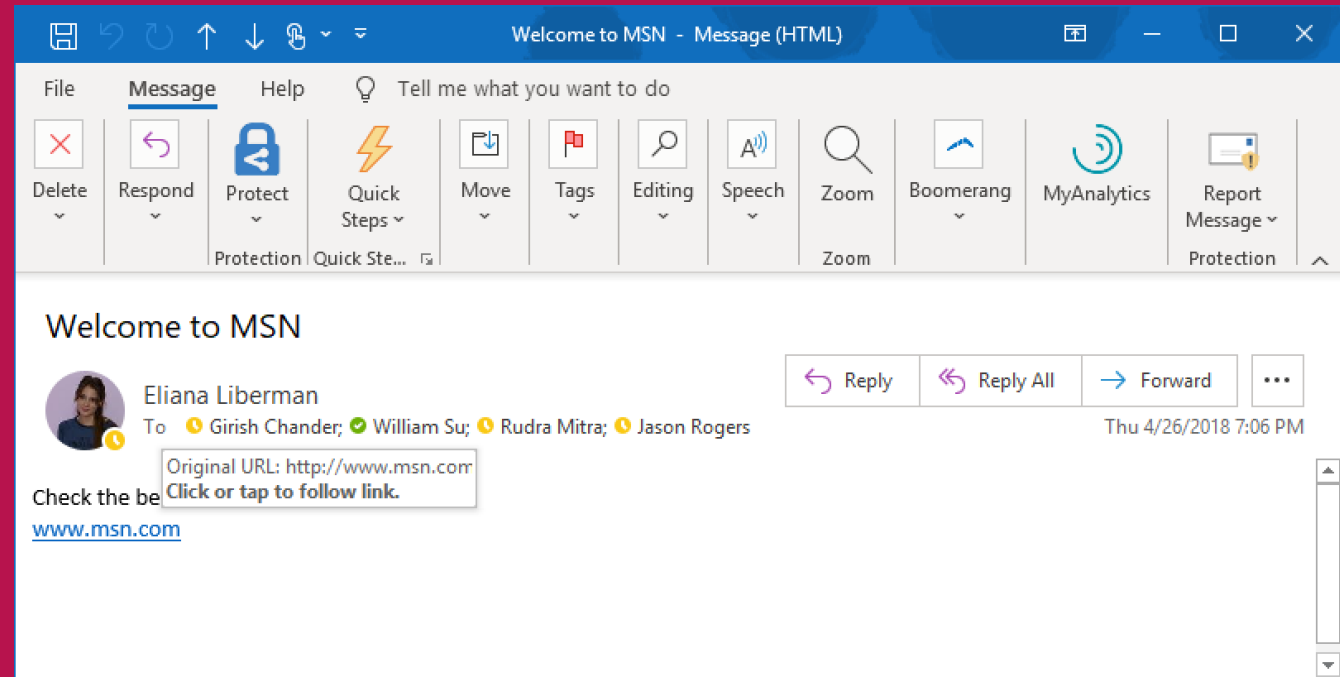
Users can **hover over URLs** in emails and see the original URL

Supports **end user education** by making them more aware of malicious URLs

Unique capability that no other vendor can offer

Available today on **OWA** and **Outlook in Office 365** on **Windows**

Coming soon for **Outlook in Office 365 (Mac OS)**, **Windows Mail App**, **Outlook for iOS**, and **Outlook for Android**



<https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.msn.com&data=04%7C01%7Cruiw...>

Protect your data

Threat protection extends to your entire Office 365 ecosystem

Email is only one attack vector

Threat protection has
extended coverage

Microsoft enables security for
multiple office workloads



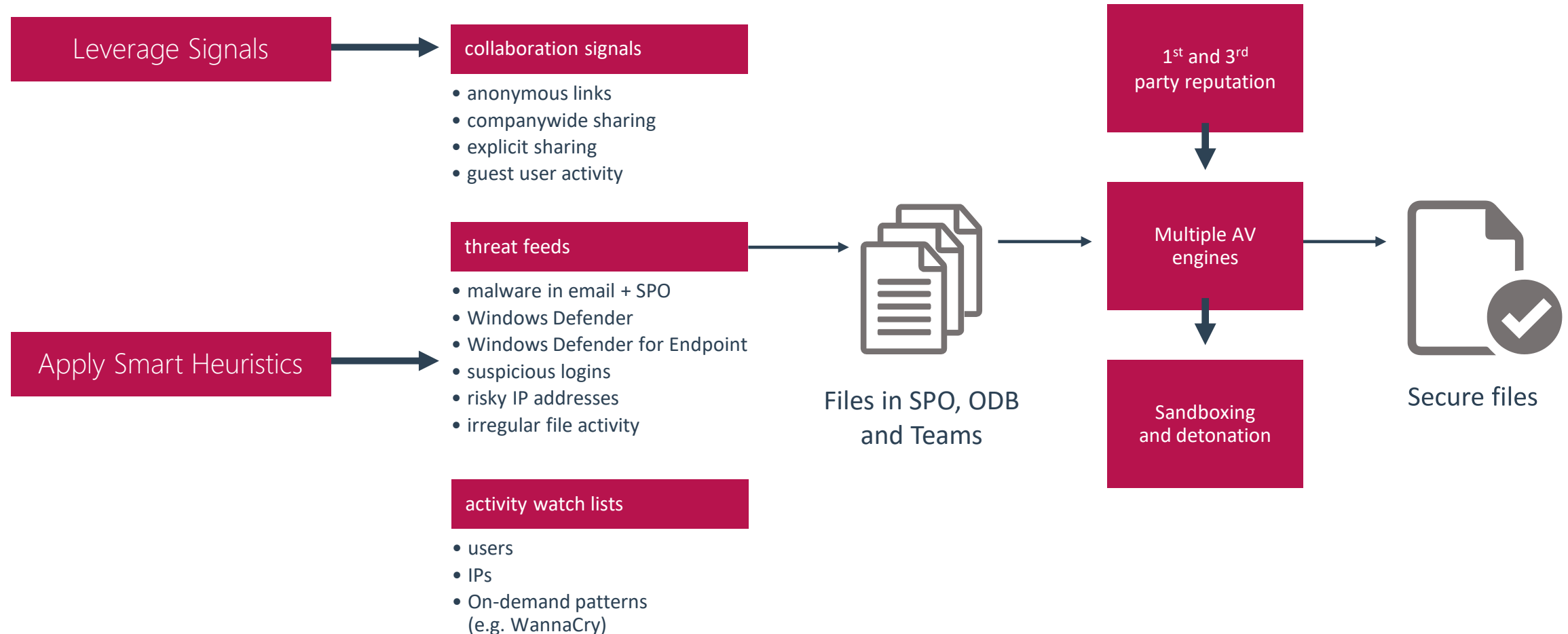
Protect your data

Advanced threat protection for your collaboration workloads

SharePoint

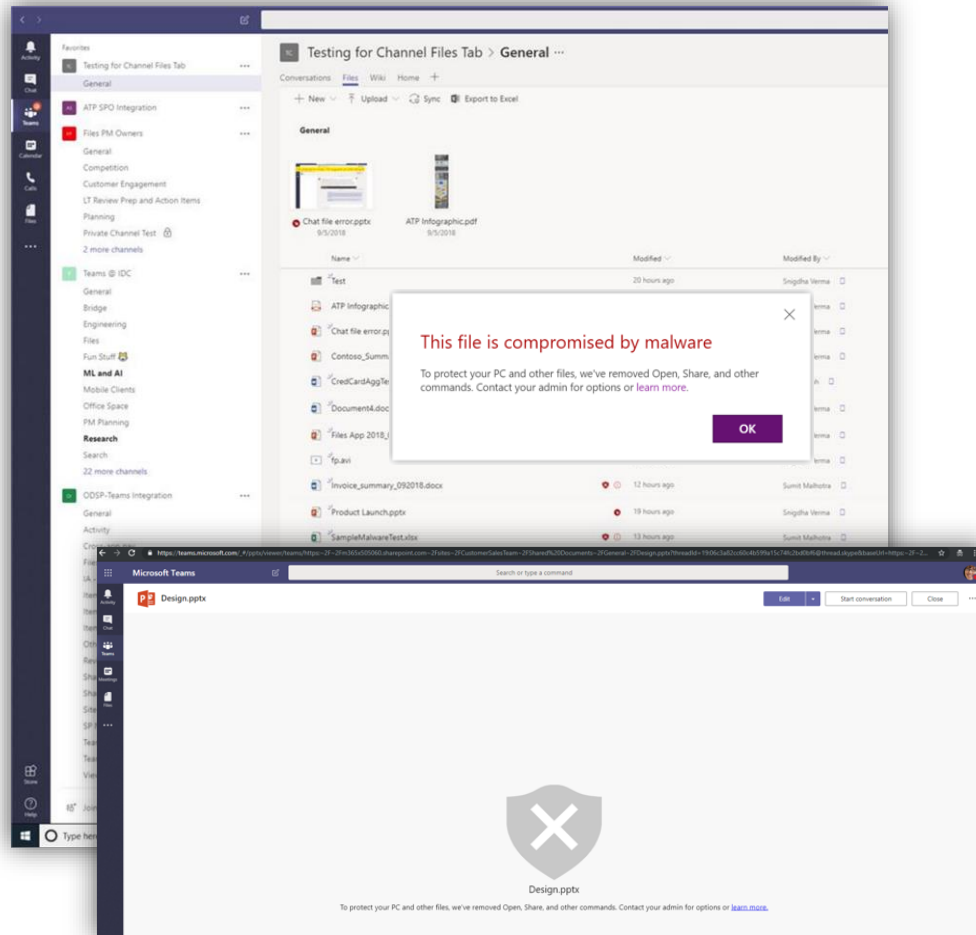
OneDrive

Microsoft Teams

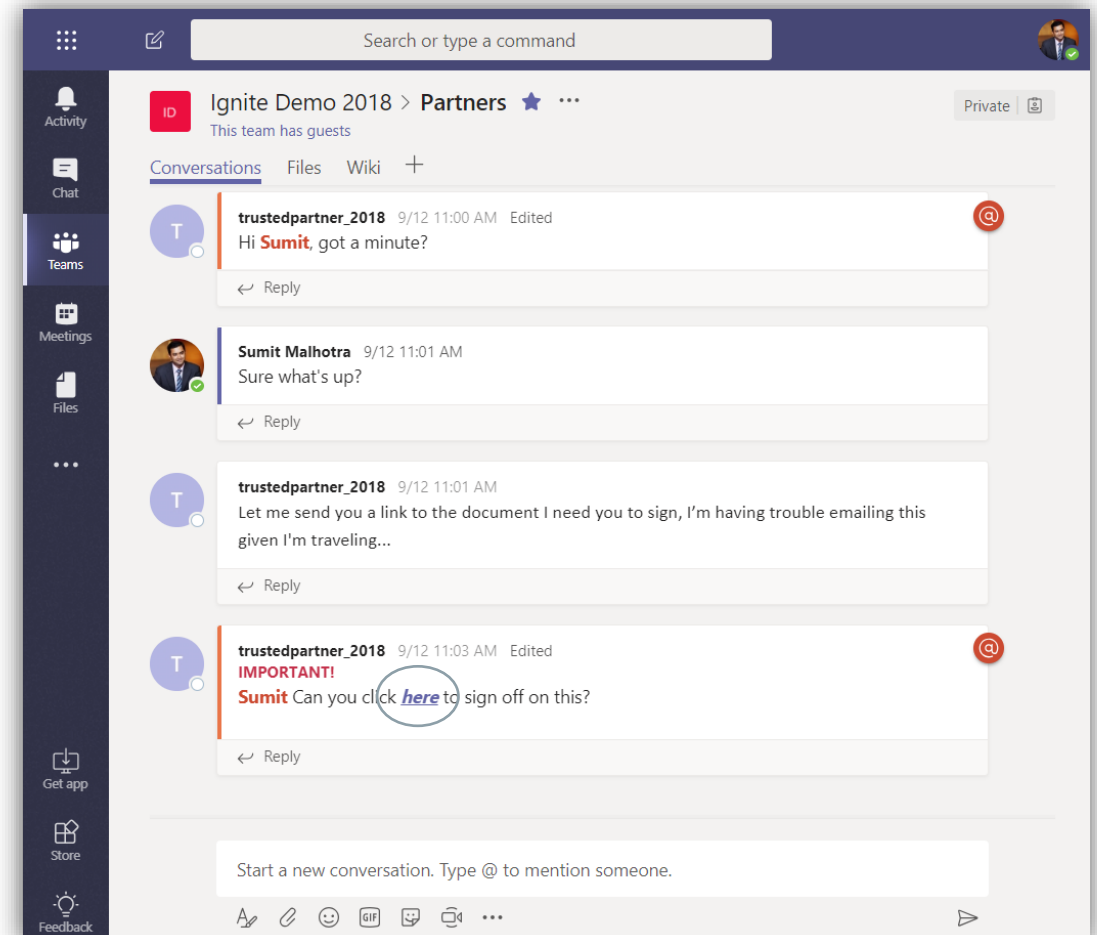


Protect your data

Cross-product integration delivers Safe Links and Safe Attachments to Teams



Microsoft Teams on Windows showing files detected and blocked by MDO



Malicious URL in conversations from Guest/External user in Microsoft Teams on Windows

Protect your data

Advanced security for your desktop clients

Word

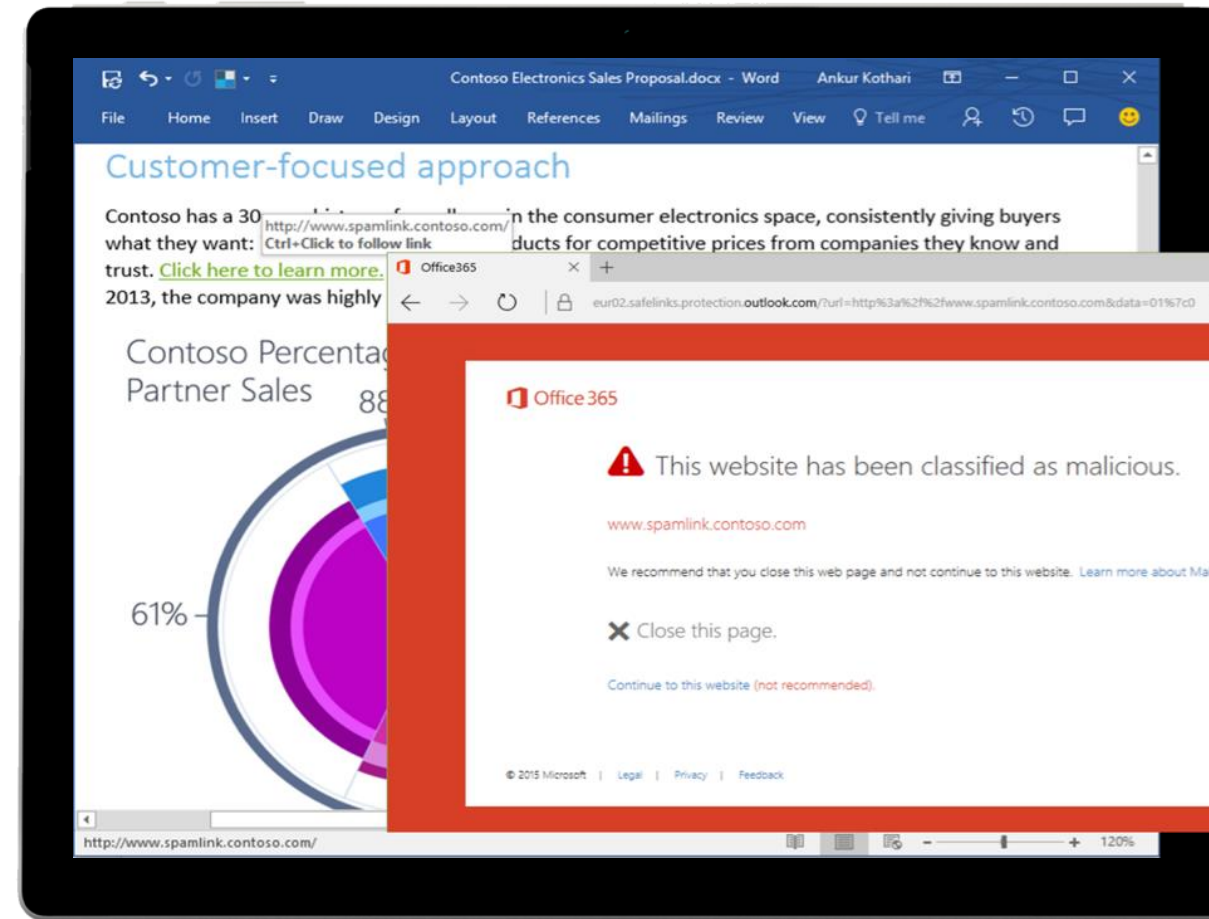
Excel

PowerPoint

Improve your security against advanced threats, unknown malware, and zero-day attacks

Protect users from malicious links with time-of-click protection

Safeguard your environment from malicious documents using virtual environments



Protect your data

INTRA ORG spoof intelligence

Office 365 | Security & Compliance

Anti-spam settings

Our standard settings cover the basics so you can have peace of mind that your organization is protected from spam. But if you want more control, switch to custom settings and take advantage of a robust set of features, including custom group filter policies that you can apply to users and groups. Learn more

Sender	Spoofed user	# of messages	# of user complaints	Authentication result	Decision set by	Last seen	Allowed to spoof?
1.1.1.2	phil@contoso.com	50	10	Passed	Spoof intelligence policy	3/19/2016	▼ No
1.1.1.2	kate@contoso.com	20	5	Passed	Admin	5/27/2016	▼ Yes

^ Spoof intelligence policy ☐ Lowest

Review senders that are spoofing your domain. You can block or allow these senders from spoofing your domain. [Learn about spoof intelligence](#)

[Show me senders I already reviewed](#)

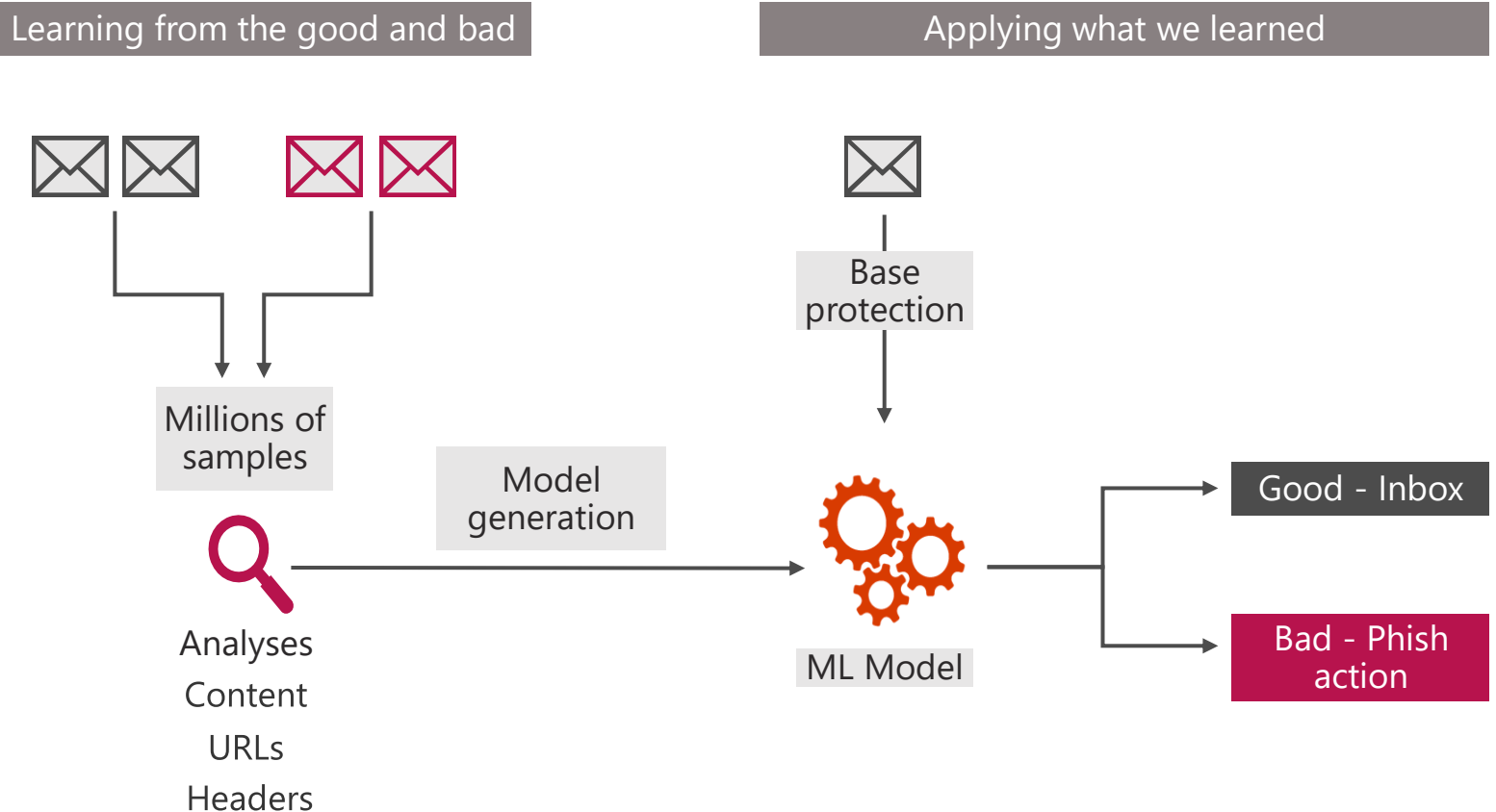
[Review new senders](#)

Admins can review senders who are spoofing their company to their users and then choose to allow the sender to continue or block the sender

Intelligent detection

- Scale of signals from the Intelligent Security Graph provide **extensive visibility** into the threat landscape
- The amount of data analyzed helps **flag suspicious content quickly** and **precisely**
- Machine learning models **continuously improve** to catch new unknown threats

Leveraging Machine Learning Models to identify suspicious content



Mailbox Intelligence Protection

Automatic protection for all users in an organization based on their contact graph

Edit impersonation policy

Add users to protect

Add domains to protect

Actions

Mailbox intelligence

Add trusted senders and domains

Review your settings

Anti-phishing policy

Editing Mailbox intelligence

Mailbox intelligence analyzes your cloud-based users' mail flow patterns to determine which contacts they communicate with most often. This helps us more easily identify when an email message might be from an attacker who's impersonating one of those contacts.

[Learn more about mailbox intelligence](#)

Enable mailbox intelligence?

☒ On

Enable Mailbox intelligence based impersonation?

☒ On

If an attacker impersonates a user known to mailbox intelligence, we'll apply the actions you choose here.

If email is sent by an impersonated user:

We'll deliver the message to the intended recipients without any other actions applied.

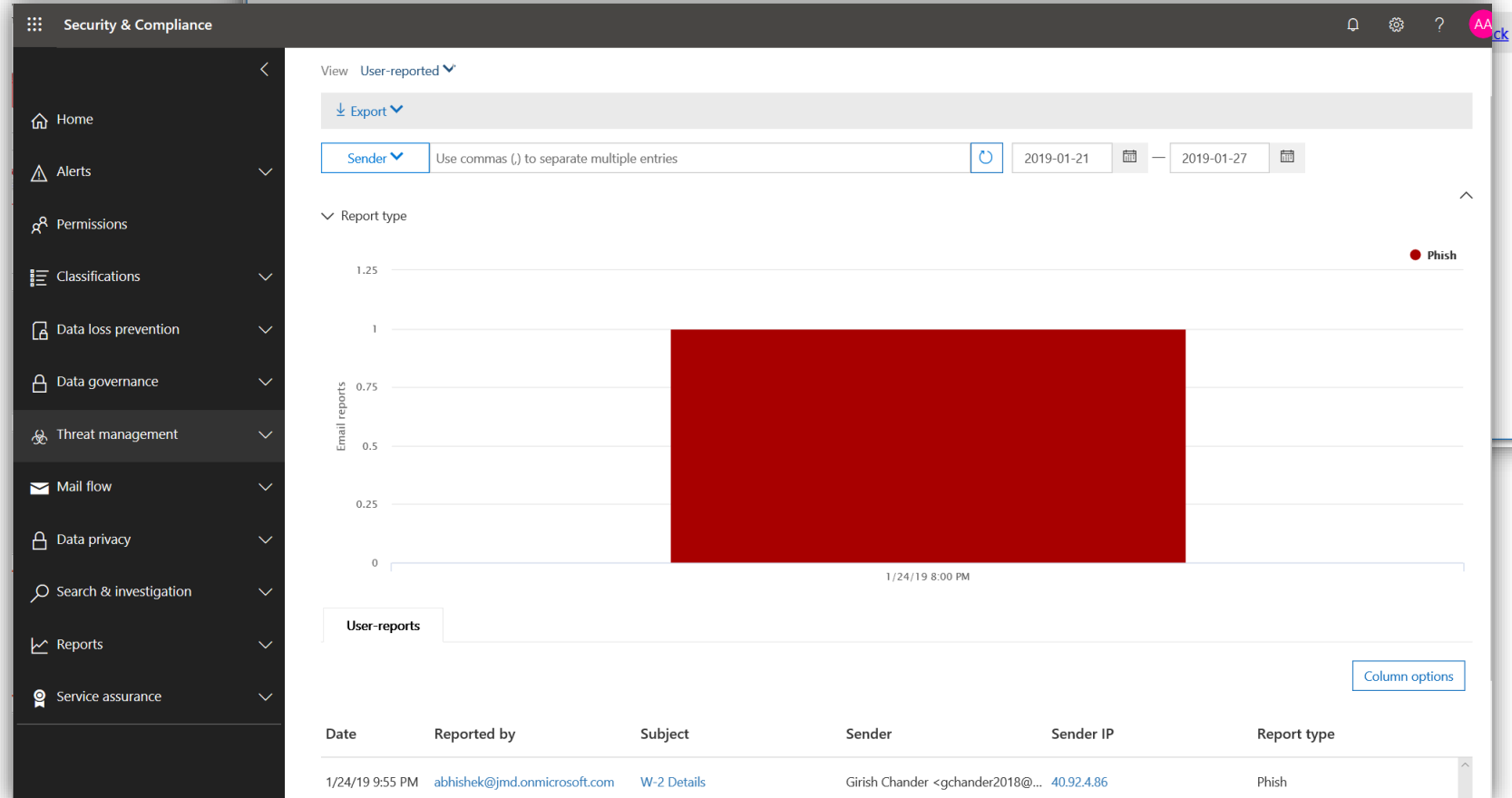
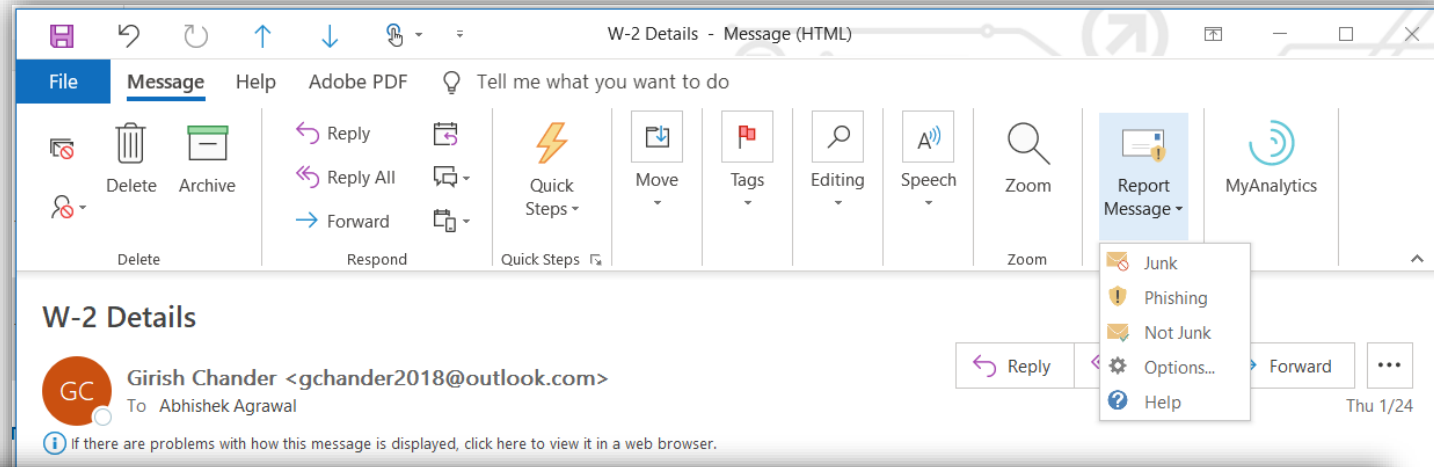
[Turn on impersonation safety tips](#) to show a warning in the recipient's email if we detect the message is an impersonation attack.

Save

Cancel

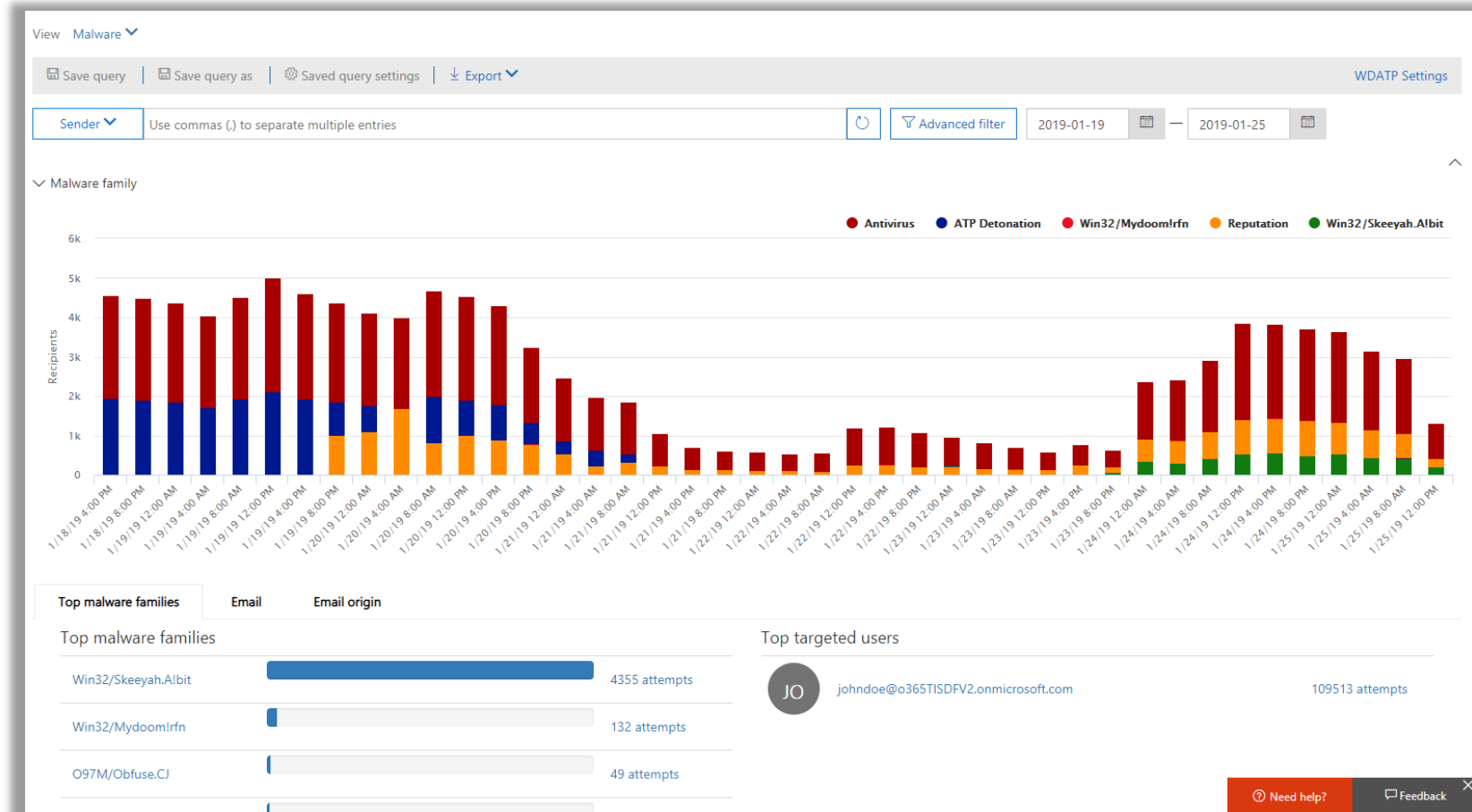
End User Reporting

- ✓ Users can Report Messages as Junk, Not Junk, or Phishing through their Outlook client or OWA
- ✓ Admins can review user-reported messages within the Security & Compliance Center



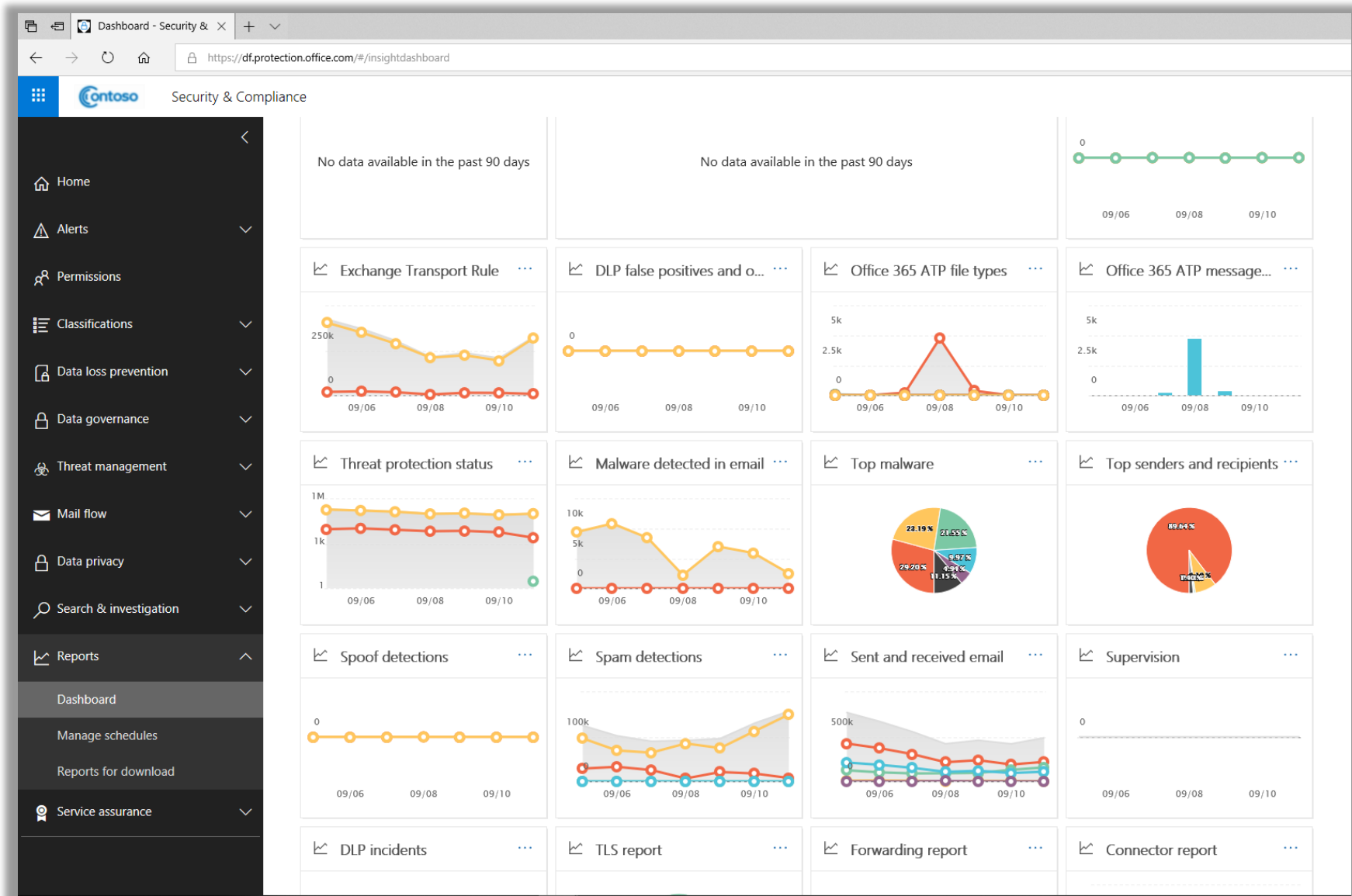
Reporting

- Real-time and trending report capabilities
- Out-of-box trending reports for threat management and compliance
- Reports can be customized and scheduled for delivery
- Data can be exported to .csv or via REST API for manual manipulation via Power BI or other data visualization tool



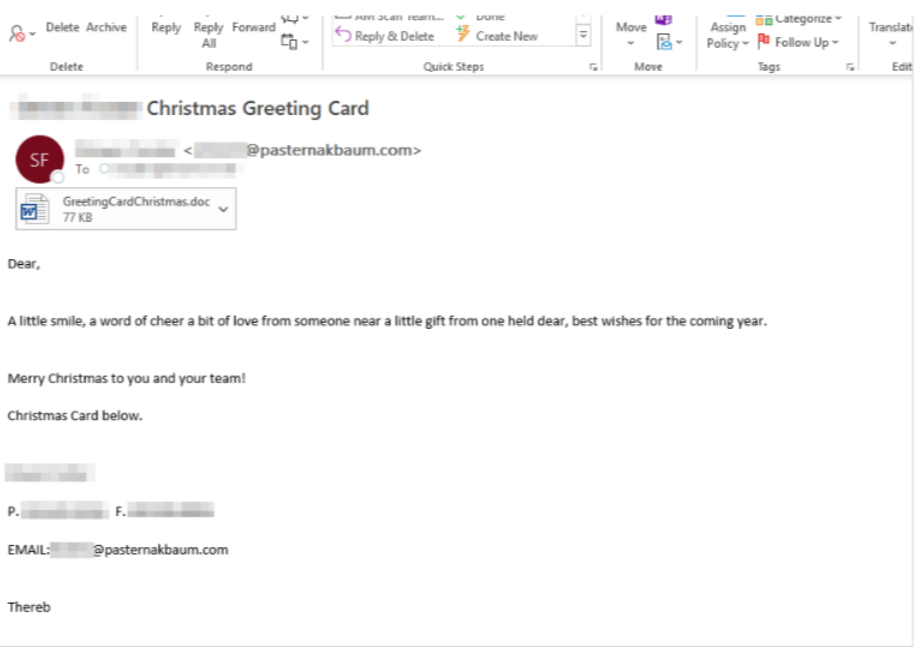
Detailed Threat Reporting

We are adding more phish catch details to the Threat Protection Status report, in addition to other trending report enhancements.



Threat Intelligence

- ✓ Unique Intel via 11B detonations
- ✓ Threat signals from Microsoft Security Graph
- ✓ Curated 3rd party Threat intelligence is automatically applied for protection
- ✓ Security Intelligence Reports from Microsoft
- ✓ Targeted attack and Nation State activity notifications via programs like AccountGuard
- ✓ Track IOCs via Threat Trackers



Christmas Greeting Card

Dear,

A little smile, a word of cheer a bit of love from someone near a little gift from one held dear, best wishes for the coming year.

Merry Christmas to you and your team!

Christmas Card below.

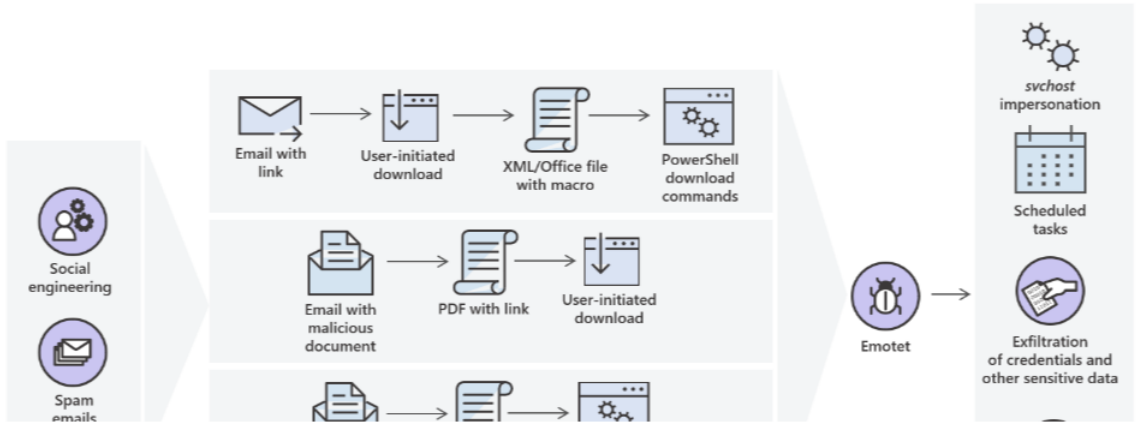
P. [redacted] F. [redacted]

EMAIL: [redacted]@pasternakbaum.com

Thereb

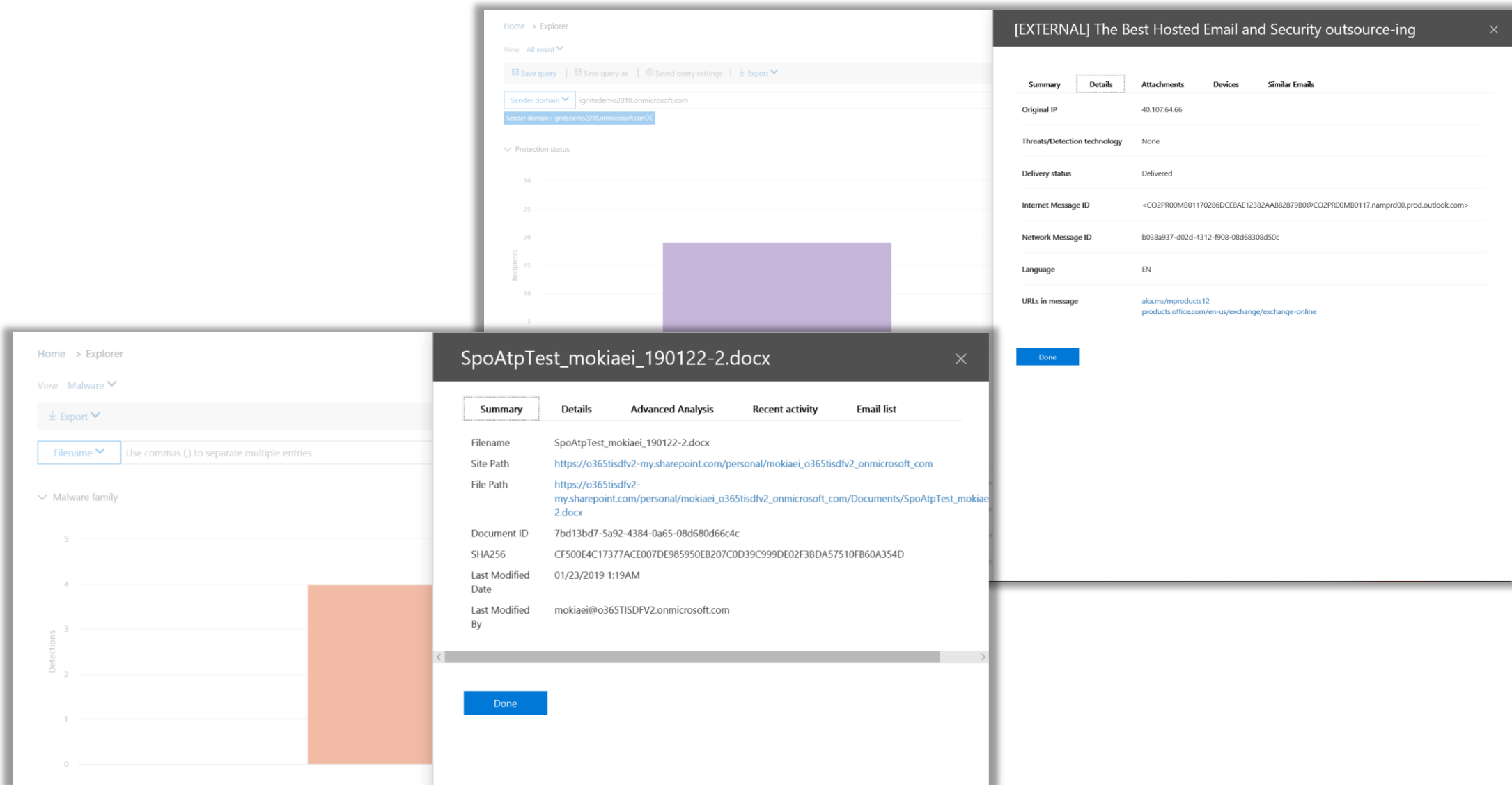
Emotet variants used in the holiday-themed campaigns generally employed the same techniques. They impersonated *svchost*, used scheduled tasks to maintain persistence, exfiltrated credential information, and dropped other credential-stealing trojans.

The following diagram describes the various Emotet delivery methods seen in the campaigns and how the trojan eventually maintains persistence and downloads other payloads.

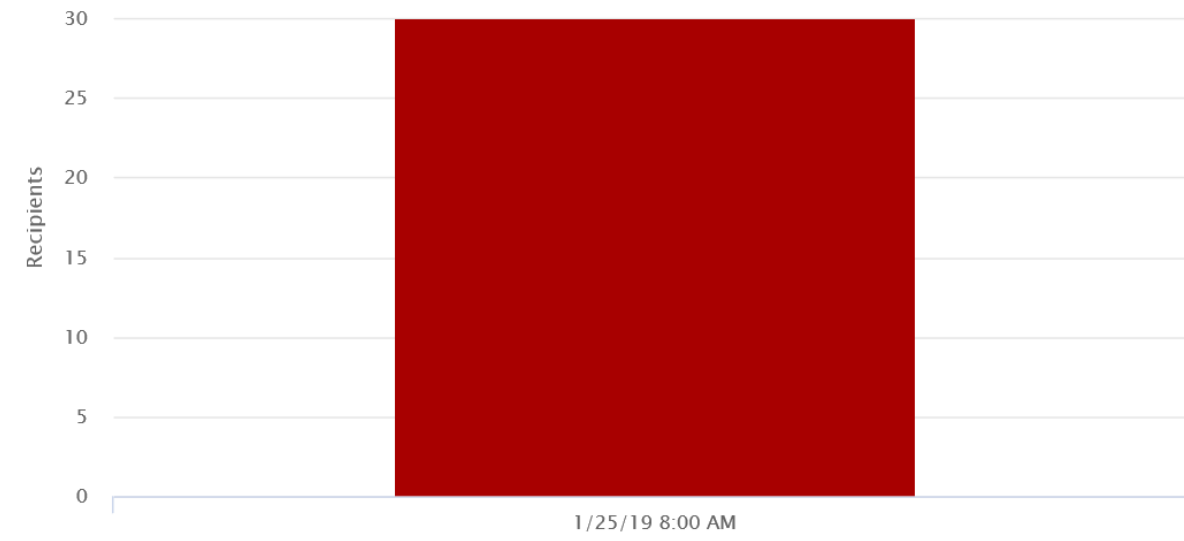


```
graph LR
    subgraph Social_Engineering [Social engineering]
        A[Email with link] --> B[User-initiated download]
        B --> C[XML/Office file with macro]
        C --> D[PowerShell download commands]
    end
    subgraph Spam_Email [Spam email]
        E[Email with malicious document] --> F[PDF with link]
        F --> G[User-initiated download]
    end
    subgraph Document_Path [Document Path]
        H[Document] --> I[PowerShell command]
    end
    D --> J[svchost impersonation]
    D --> K[Scheduled tasks]
    G --> L[Exfiltration of credentials and other sensitive data]
    I --> M[Emotet]
    J --> M
    K --> M
    L --> M
    M --> N[Exfiltration of credentials and other sensitive data]
```


Email and Content Investigation



Incident remediation



- Email
- URL clicks
- URLs
- Email origin

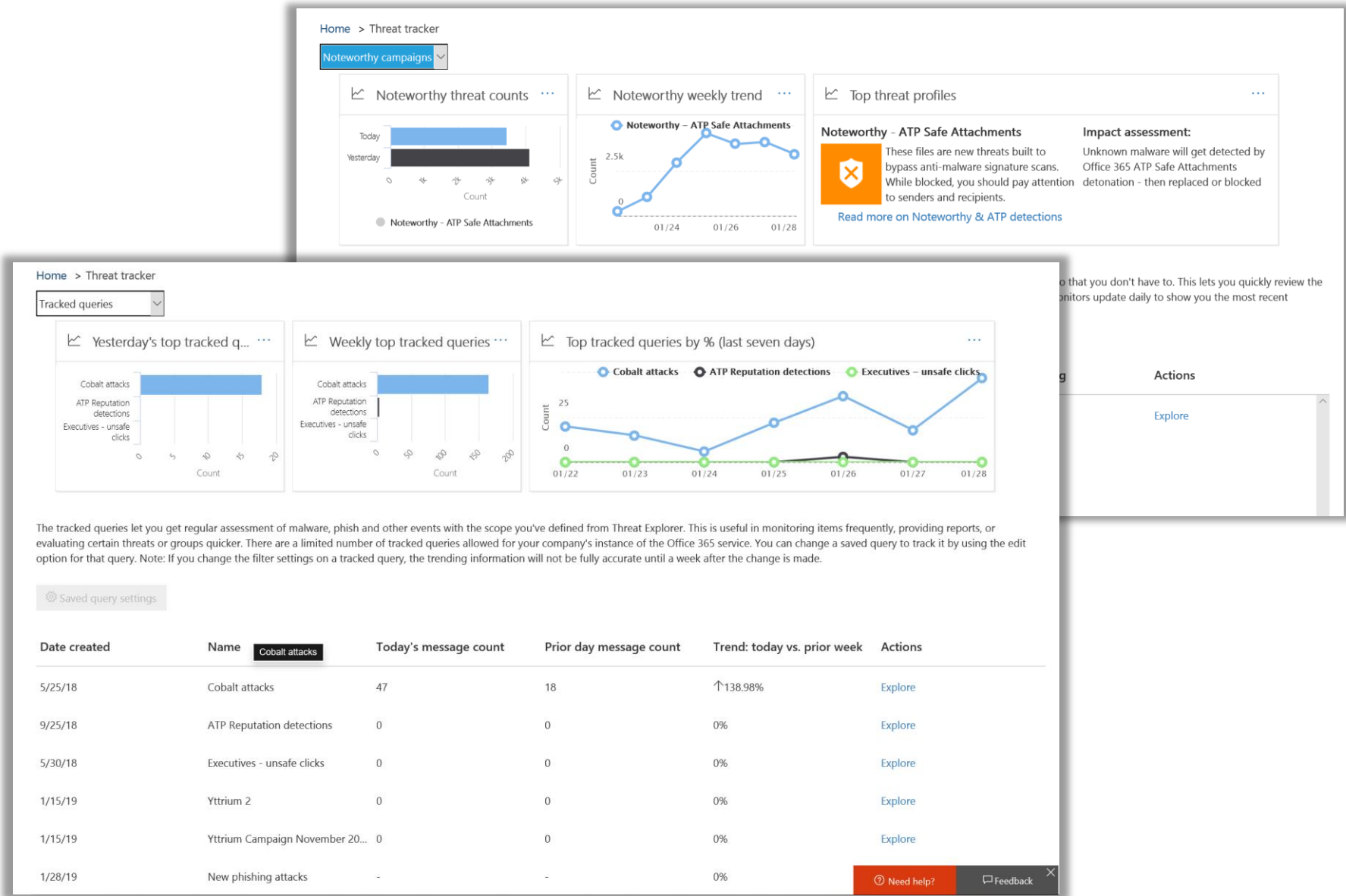
+ Actions ▾

- Email message
 - Move to junk
 - Move to deleted items
 - Soft delete
 - Hard delete
 - Move to inbox
- Track and notify
 - Investigate
 - Add emails to incident
 - Send a message to recipients

	Recipient	Sender
<input type="checkbox"/>	[EXTERNAL] The Best Hosted Email... stuartcl@o365tisdfv2.onmicrosoft...	jeffv@lgr...
<input type="checkbox"/>	[EXTERNAL] The Best Hosted Email... johne@o365tisdfv2.onmicrosoft.c...	jeffv@lgr...
<input type="checkbox"/>	[EXTERNAL] The Best Hosted Email... admin@o365tisdfv2.onmicrosoft....	jeffv@lgr...
<input type="checkbox"/>	[EXTERNAL] The Best Hosted Email... bobatp@o365tisdfv2.onmicrosoft...	jeffv@lgr...
<input checked="" type="checkbox"/>	1/25/19 12:34 PM [EXTERNAL] Get hosted email wit... johne@o365tisdfv2.onmicrosoft.c...	jeffv@lgr...

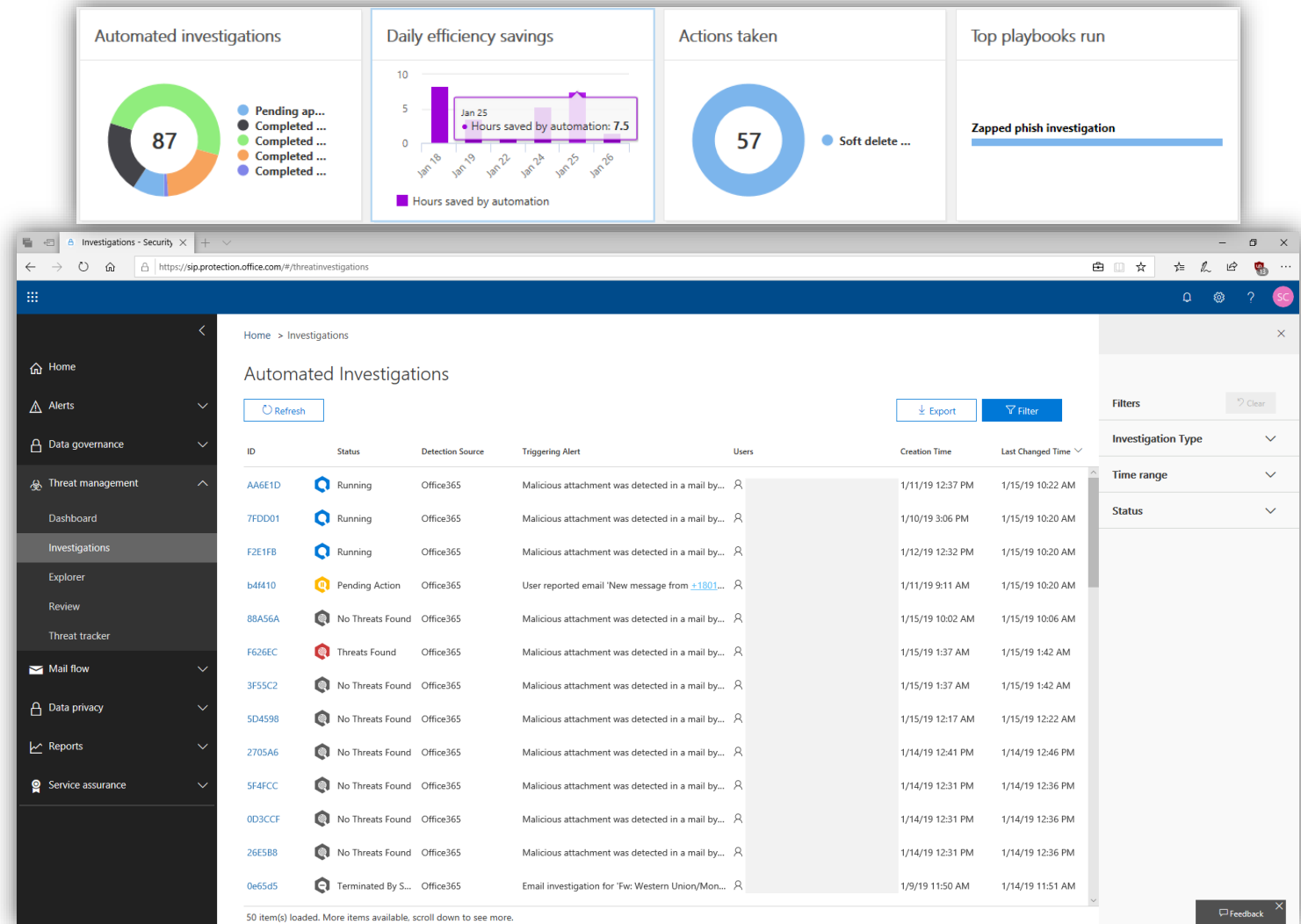
43 item(s) loaded.

Threat Trackers



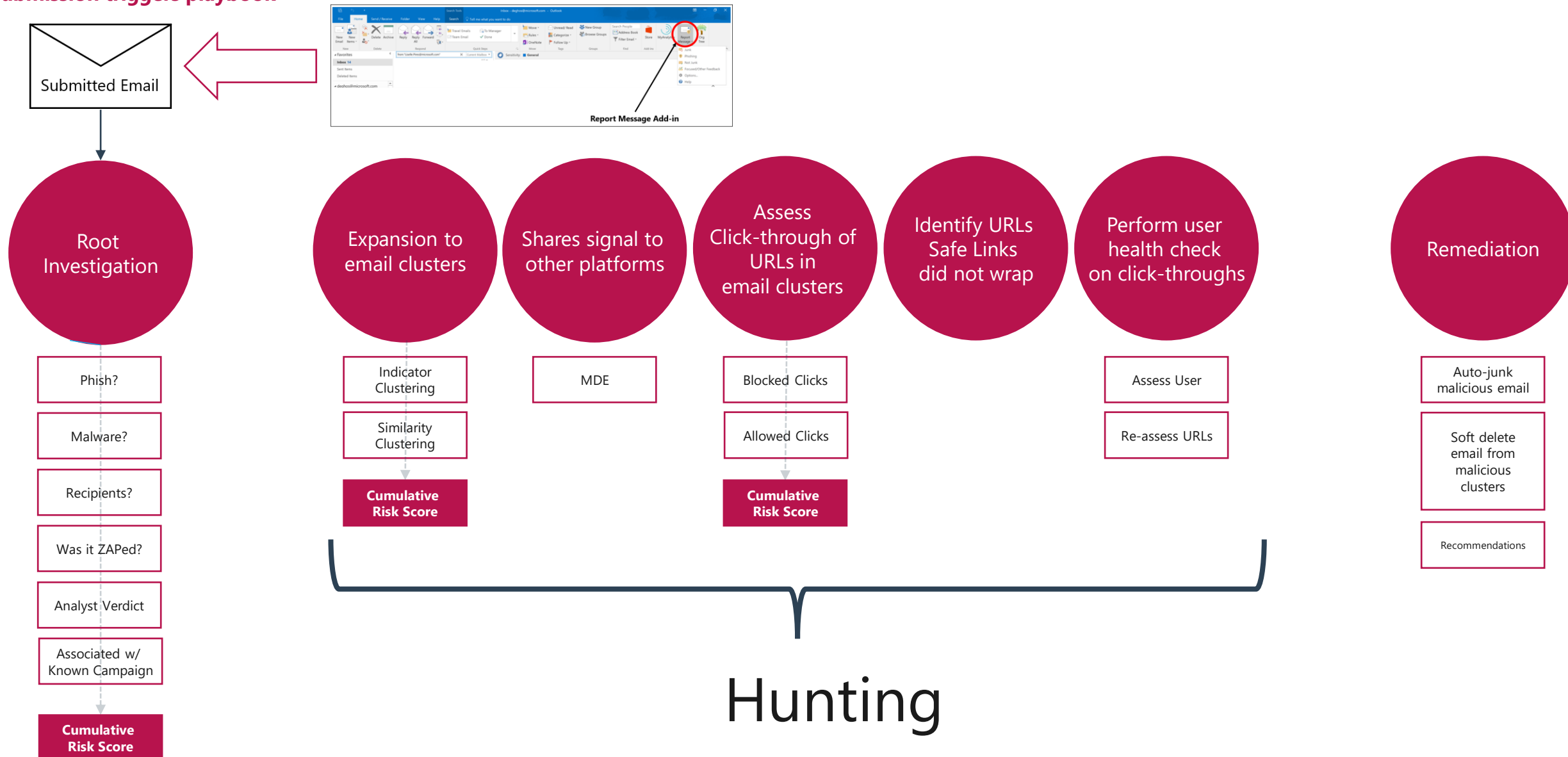
Automated Investigation & Response (AIR)

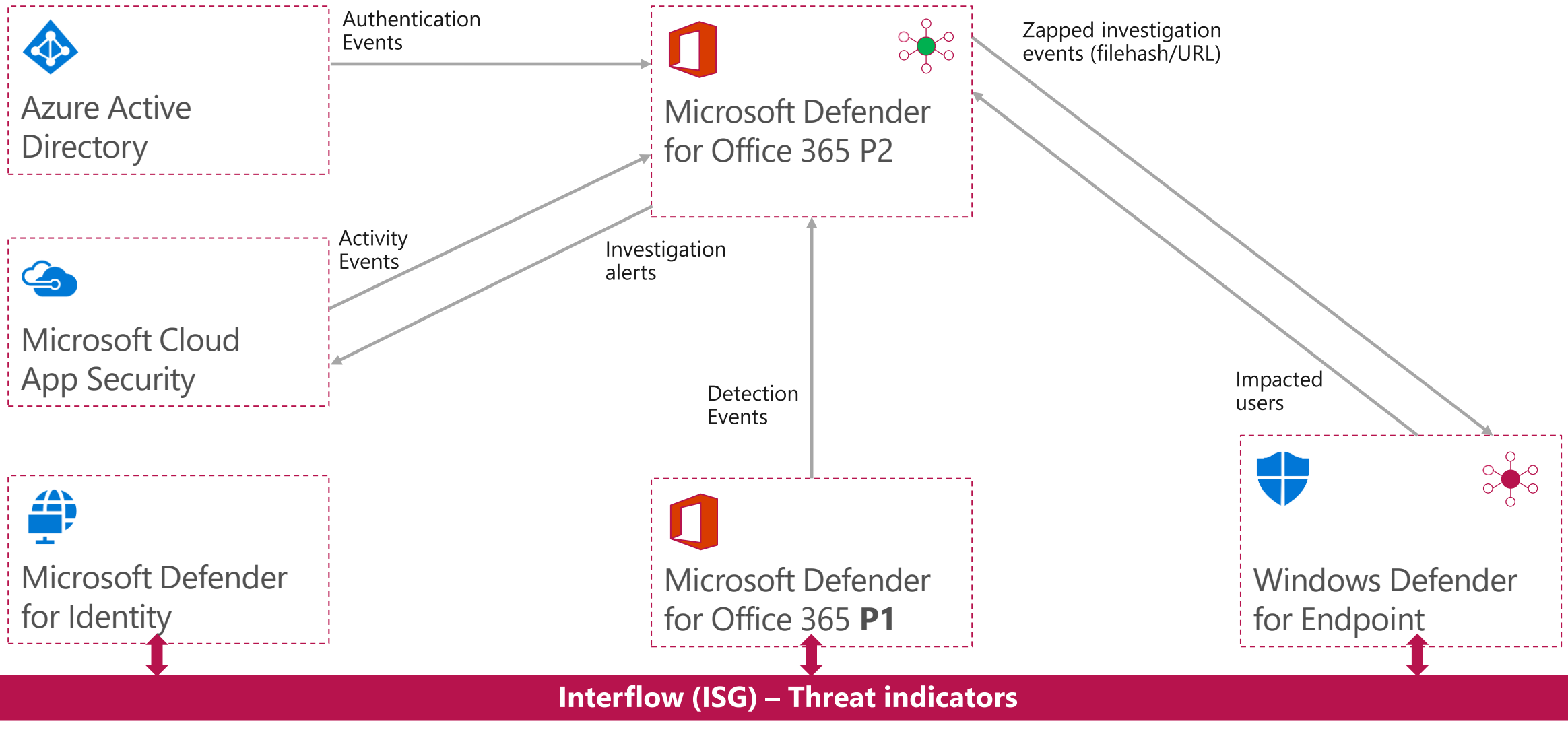
Automation and Orchestration is driven by having well known playbooks that run given a certain condition being met, the resulting automation drives the initial analysis of the investigation then automates the recommended actions to remediate, saving Sec Ops teams hours.



Components of MDO Security Playbooks

Submission triggers playbook



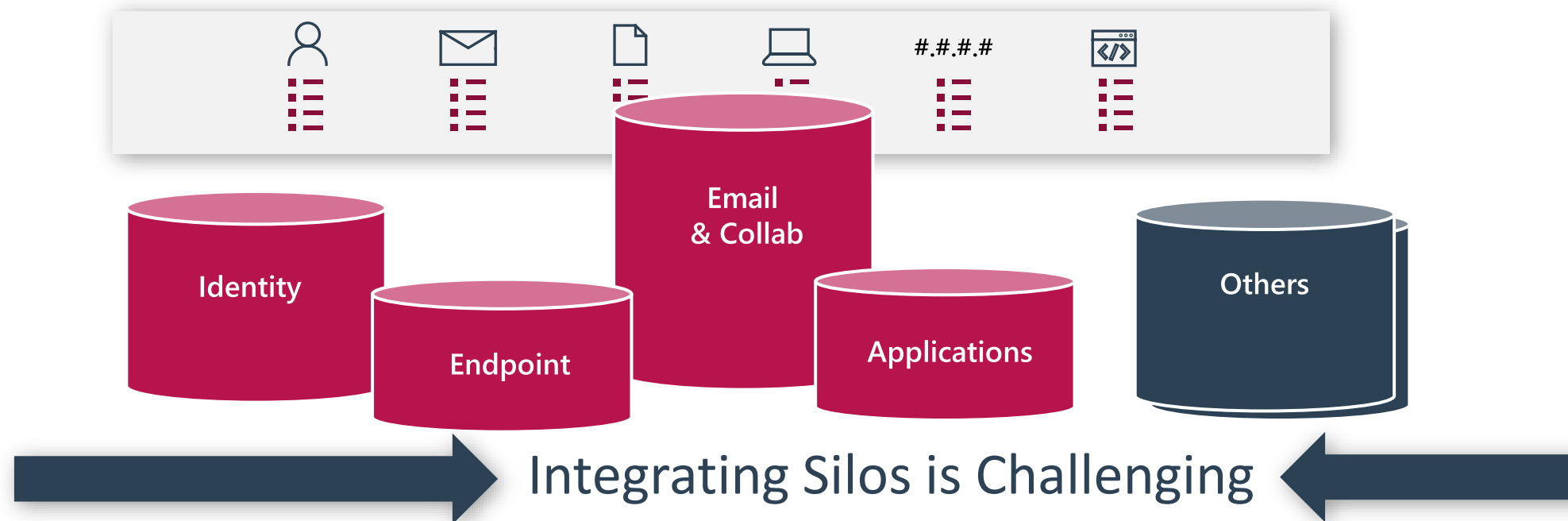


dinext.
pi-sec GmbH

Azure Sentinel



Silos are the Bane of Security Operations



MAPPING CHALLENGES

Tools Pivot on Different Attributes



STRONG BIASES/TENDENCIES

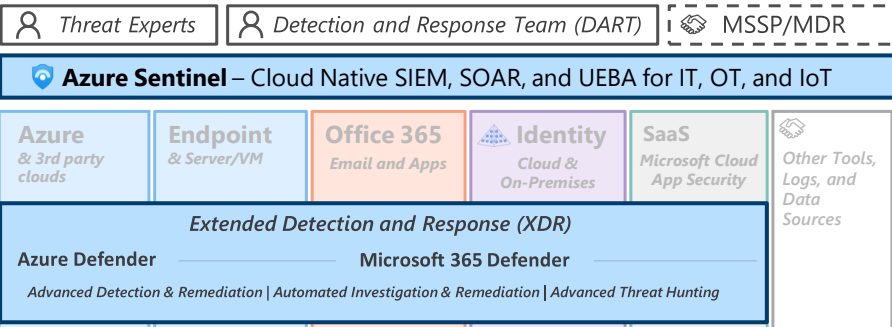
Identity ← → Endpoint

TRIAGE NEEDS TO BE ALIGNED AND PRACTICED

AUTOMATION CAPABILITIES GET IGNORED

...

Security Operations / SOC



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

May 2021 – <https://aka.ms/MCRA>

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. [Security Documentation](#)
2. [Microsoft Best Practices](#)
3. Azure Security [Top 10](#) | [Benchmarks](#) | [CAF](#) | [WAF](#)

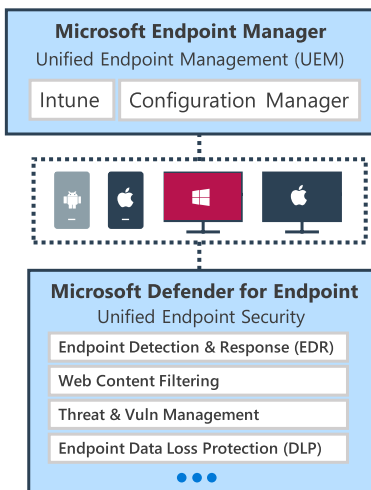
Software as a Service (SaaS)



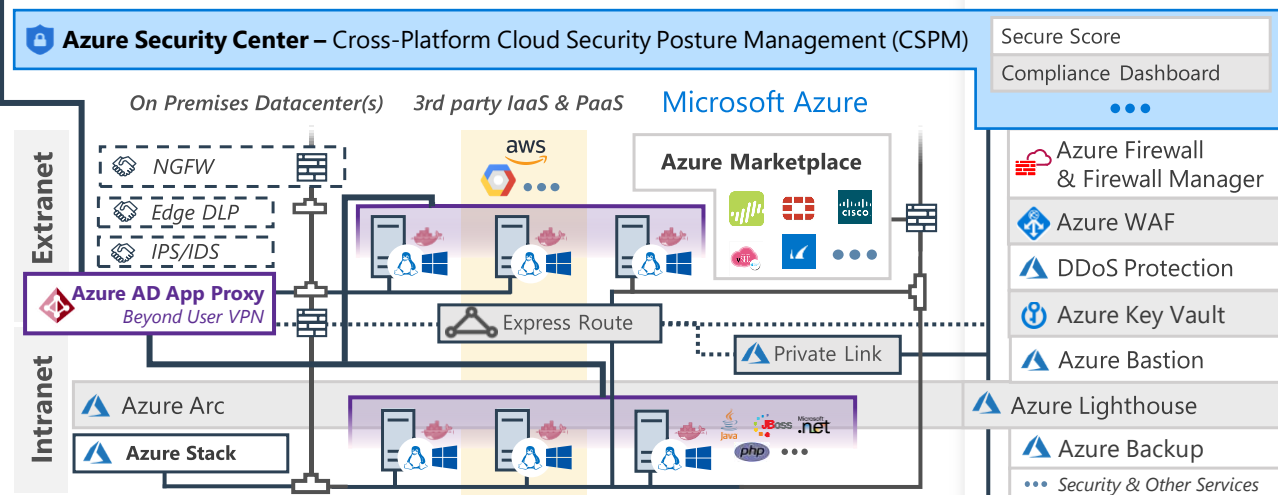
Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

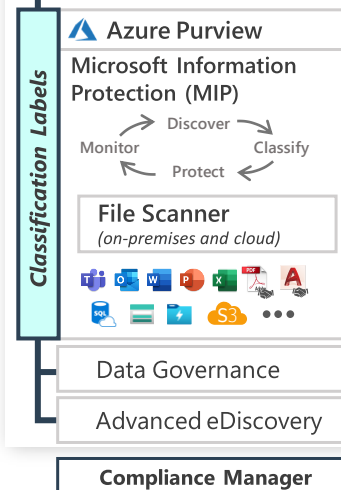
Endpoints & Devices



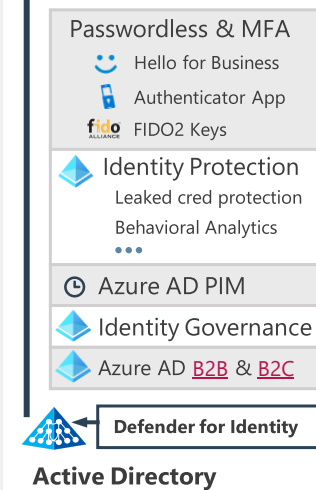
Hybrid Infrastructure – IaaS, PaaS, On-Premises



Information Protection



Azure Active Directory



Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) – Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls



IoT and Operational Technology (OT)



Azure Defender for IoT

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

Azure Defender – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

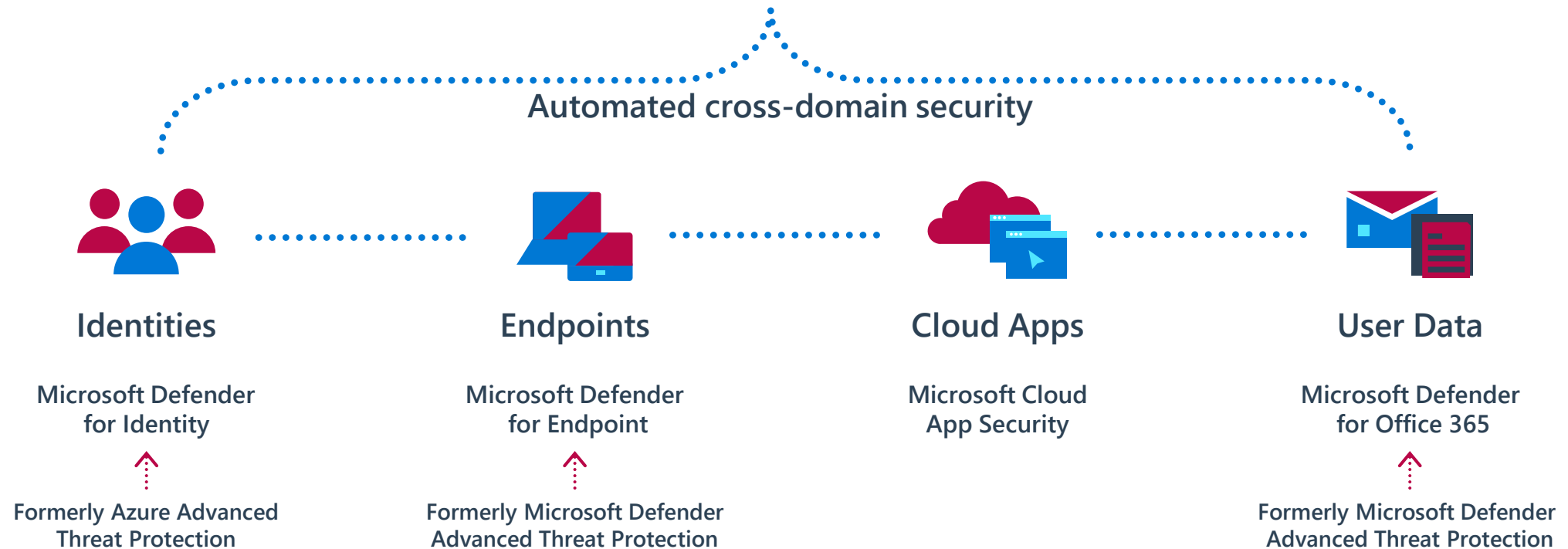
GitHub Advanced Security – Secure development and software supply chain

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

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Microsoft 365 Defender



Shift from individual silos to coordinated cross-domain security

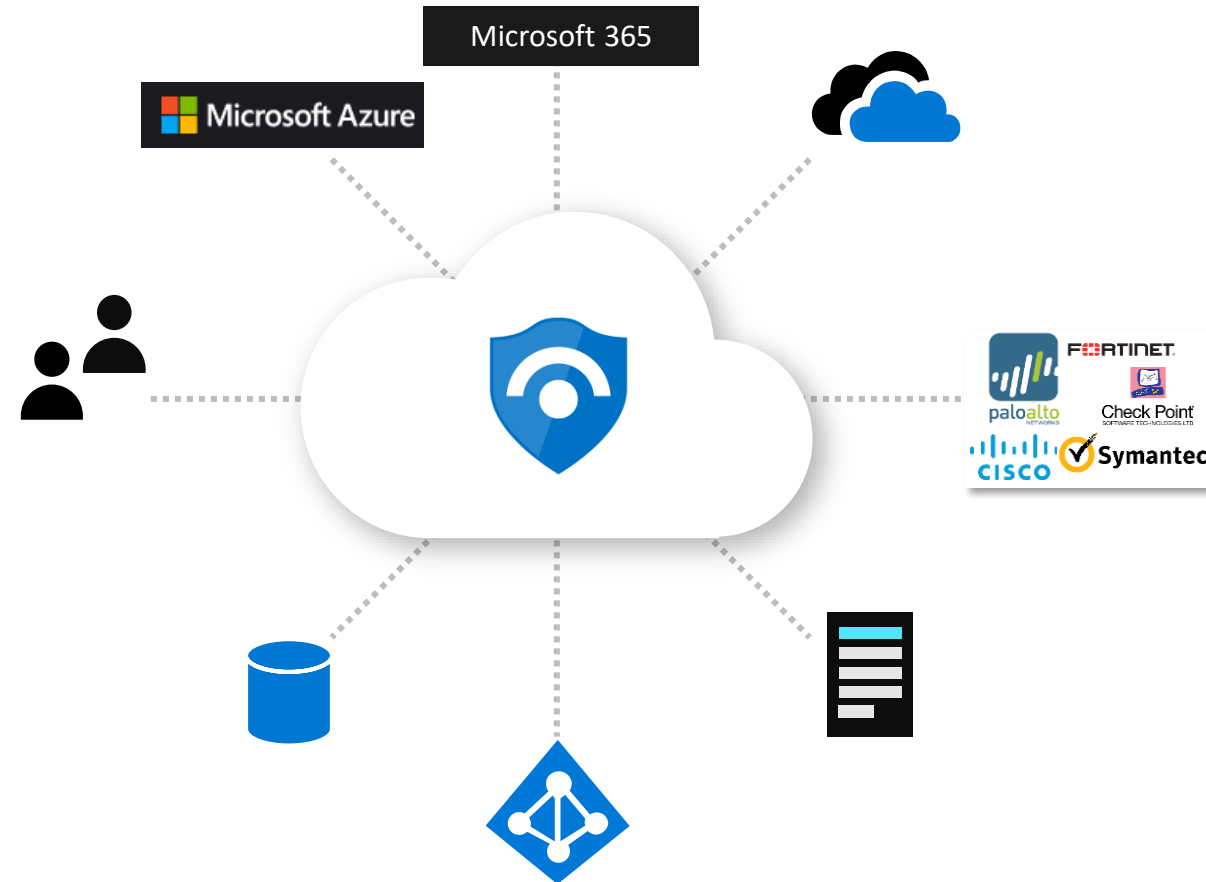
Collect security data at cloud scale from all sources across your enterprise

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

Proven log platform with more than 10
petabytes of daily ingestion

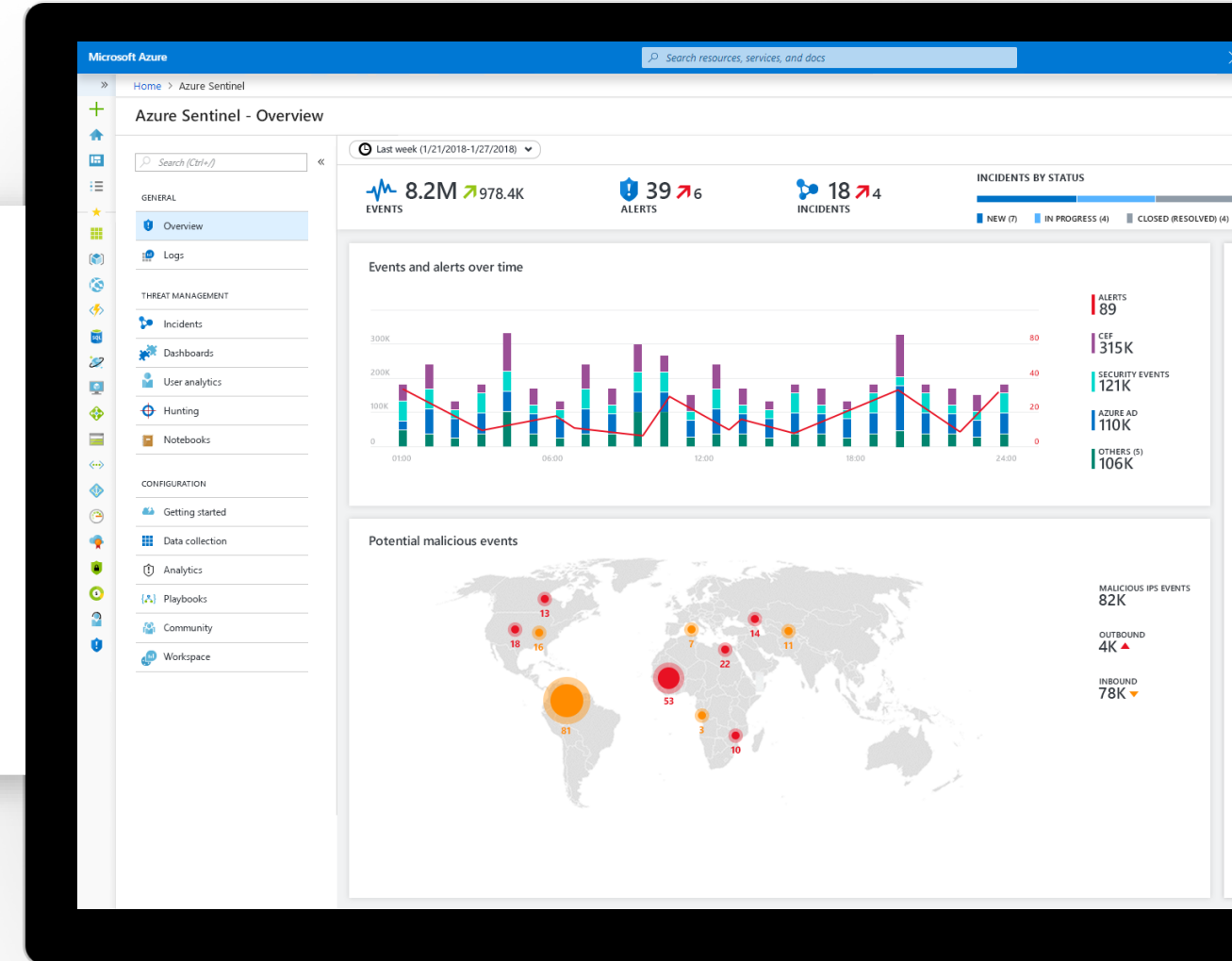


Focus on security, unburden
SecOps from IT tasks

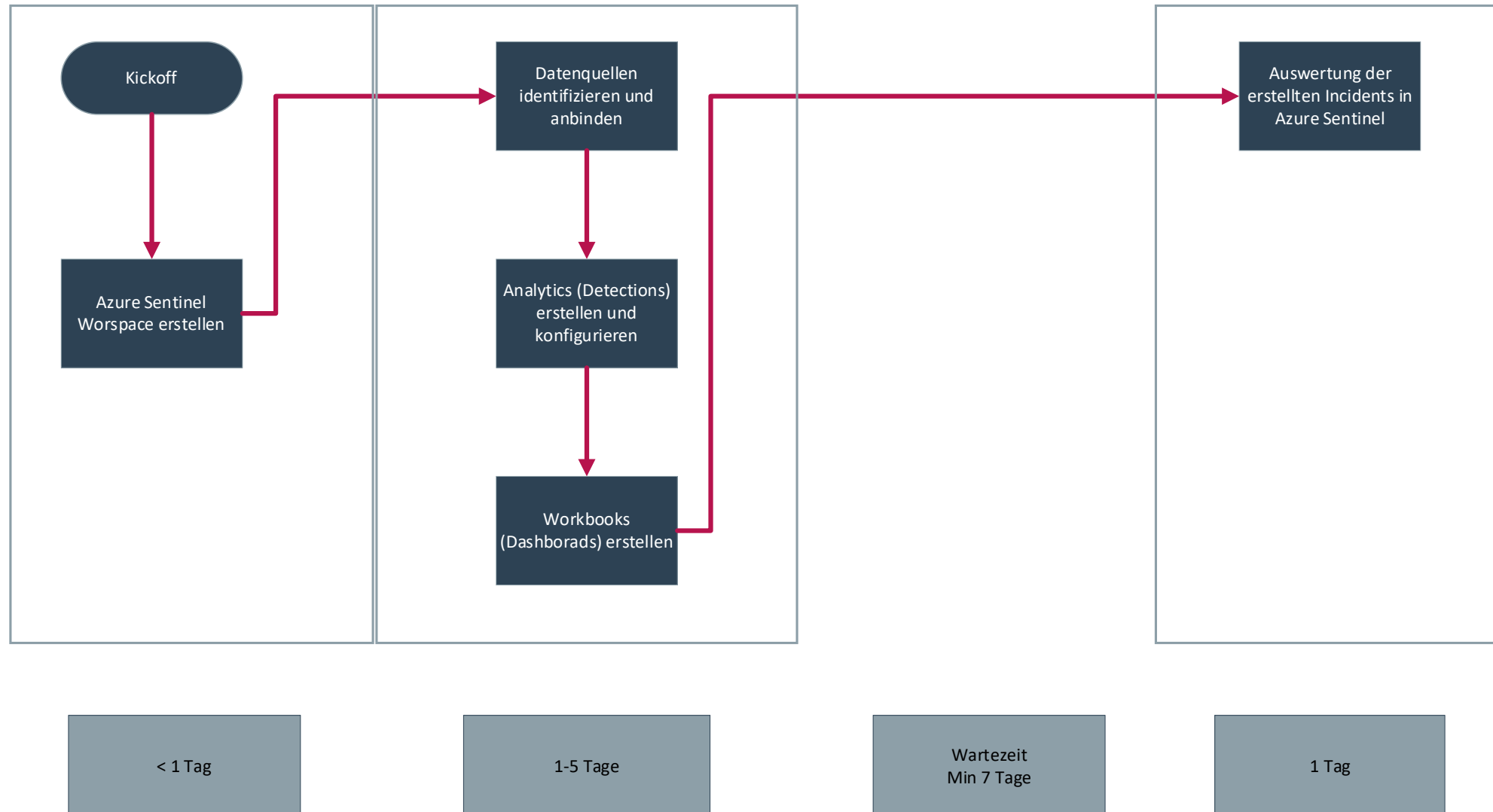
No infrastructure setup or maintenance

SIEM Service available in **Azure portal**

Scale automatically, put no limits
to compute or storage resources

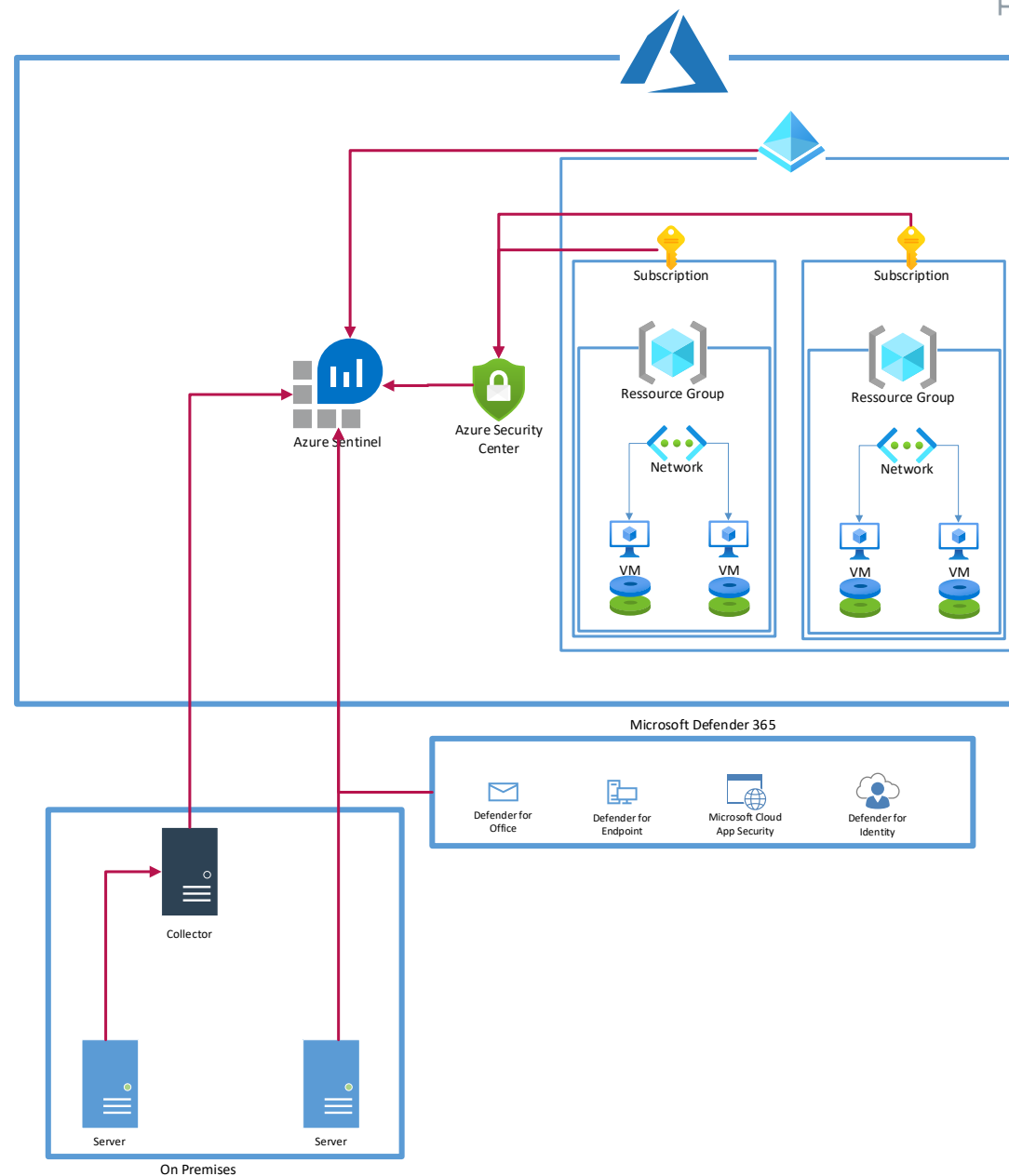


PoC Approach

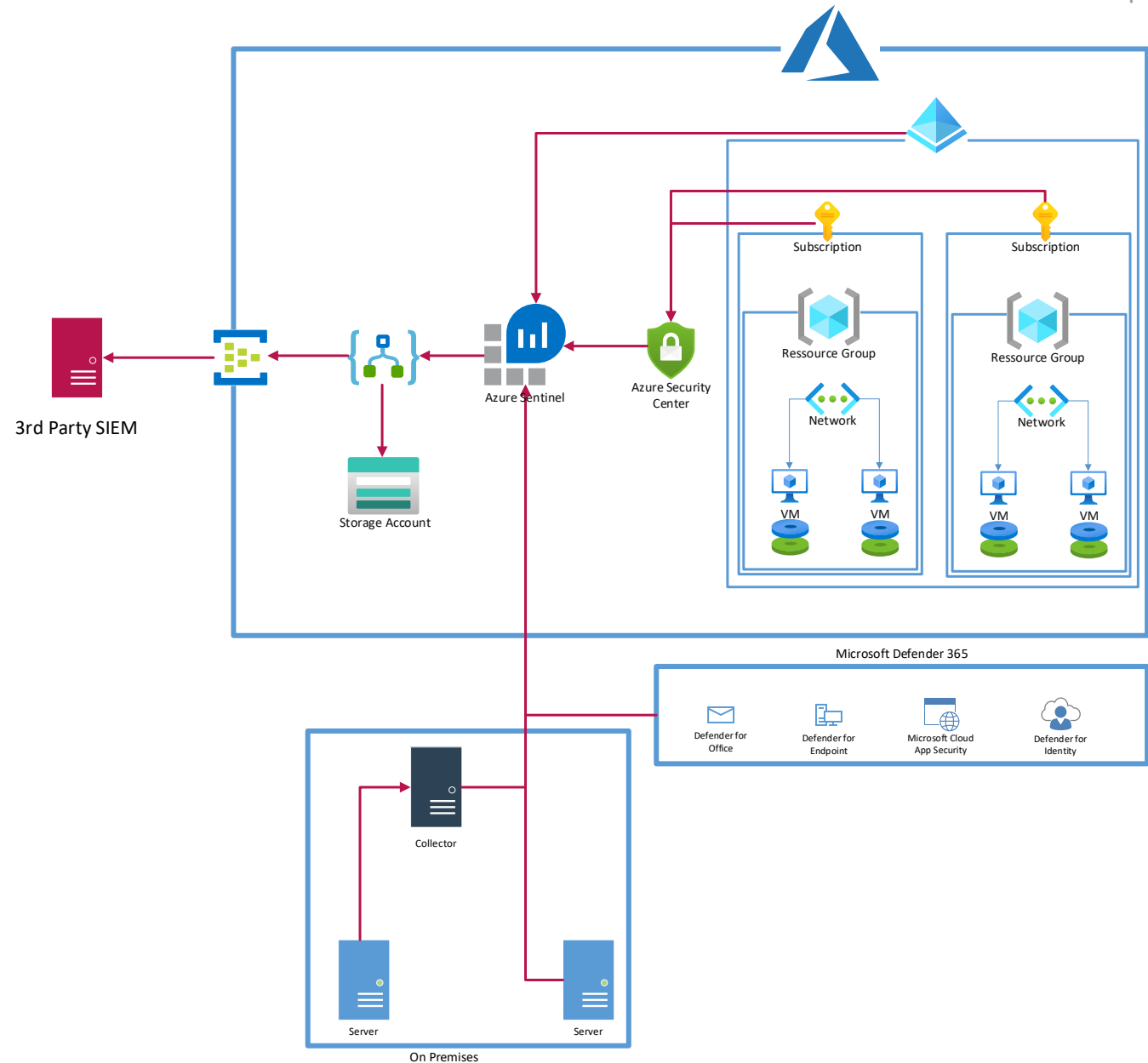




Use Case #2 Hybrid



Use Case #3 Side by Side



Data Connectors

- 116 Connectors
- Azure Service onboarding? → One Click

Azure Active Directory

Azure Active Directory

Connected Status

Microsoft Provider

6 minutes ago
Last Log Received

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received
05/21/21, 11:21 AM

Related content

8 Workbooks
 2 Queries
 39 Analytic rules templates

Data received

Go to log analytics

- SigninLogs
- AuditLogs
- AADNonInt...
- AADService...
- AADManag...
- AADProvisi...

Total data received 1/2 **654**
 Total data received **405**
 Total data received **16.34k**
 Total data received **0**

Data types

- SigninLogs 05/21/21, 11:13 AM
- AuditLogs 05/21/21, 10:50 AM
- AADNonInteractiveUserSigninLogs 05/21/21, 11:21 AM
- AADServicePrincipalSigninLogs --
- AADManagedIdentitySigninLogs 05/14/21, 4:54 PM
- AADProvisioningLogs --

Instructions Next steps

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Diagnostic Settings:** required read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Azure Active Directory logs to Azure Sentinel

Select Azure Active Directory log types:

- ☒ Sign-in logs
- ☒ Audit logs
- ☒ Non-interactive user sign-in log (Preview)
- ☒ Service principal sign-in logs (Preview)
- ☒ Managed Identity Sign-in logs (Preview)
- ☒ Provisioning logs (Preview)

Apply Changes

Incident Investigation

“Full Details”

Home > Azure Sentinel > Azure Sentinel >

Incident

Incident ID 10

Refresh

Multi-stage incident involving Persistence & Discovery...
Incident ID: 10
Investigate in Microsoft 365 Defender

Unassigned
Owner

New
Status

High
Severity

Alert product names

• Microsoft Defender for Identity

Evidence

N/A
Events

4
Alerts

0
Bookmarks

Last update time

05/12/21, 1:13 PM

Creation time

04/27/21, 11:43 AM

Entities (5)

Administrator

JeffL

samiraa

Tortuga

View all >

Tactics (2)

Persistence

Discovery

Incident workbook

Incident Overview

Timeline (Preview)

Alerts

Bookmarks

Entities

Comments

Search

Timeline content : All

Severity : All

Tactics : All

Mai 3
14:21

Suspected Golden Ticket usage (encryption downgrade)
Medium | Detected by Microsoft Defender for Identity | Tactics: Persistence

View playbooks

Mai 3
14:21

Suspected Golden Ticket usage (time anomaly)
High | Detected by Microsoft Defender for Identity | Tactics: Persistence

View playbooks

Mai 3
10:21

Suspected skeleton key attack (encryption downgrade)
Medium | Detected by Microsoft Defender for Identity | Tactics: Persistence

View playbooks

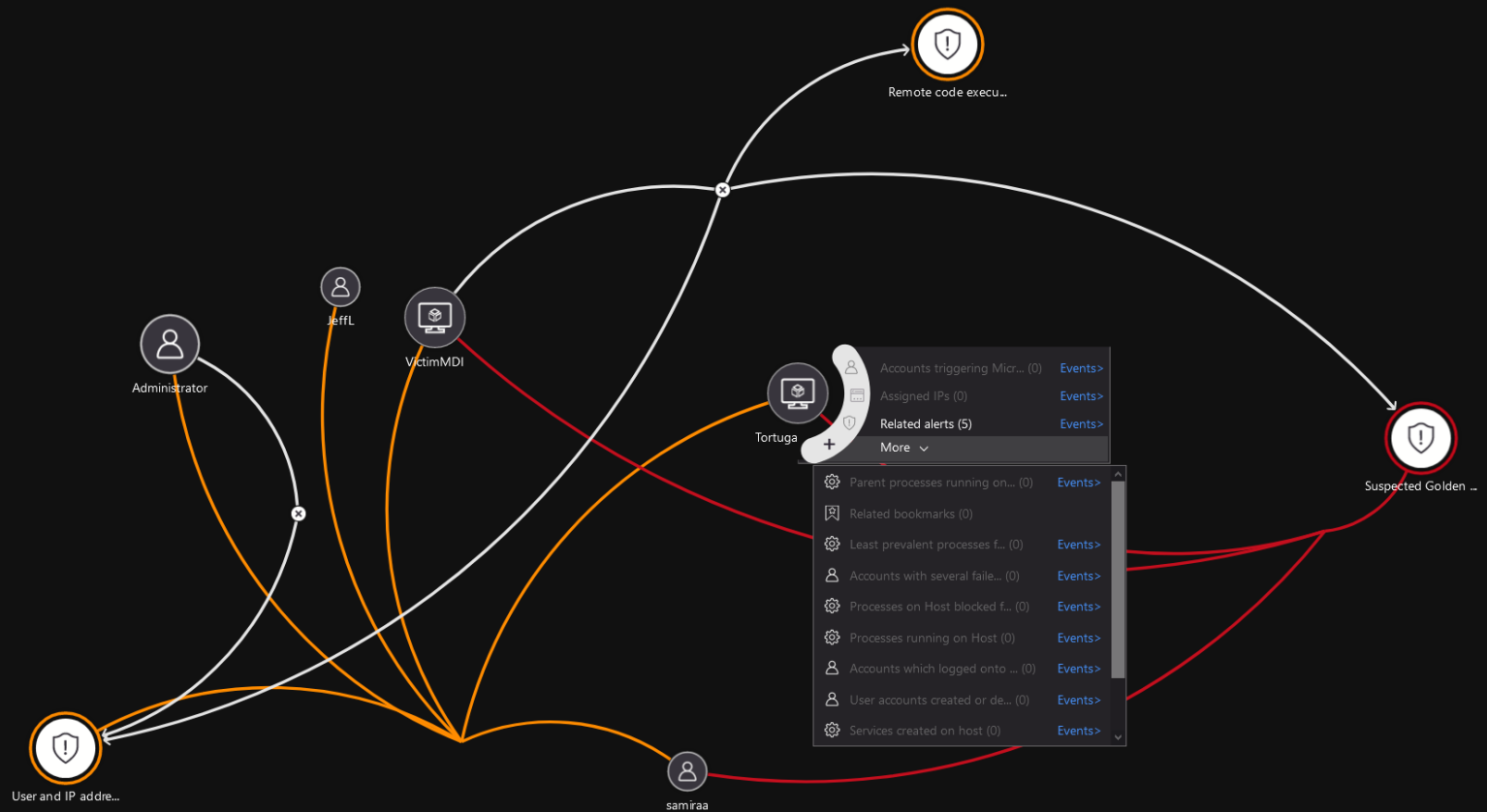
Apr 27
11:38

User and IP address reconnaissance (SMB)
Medium | Detected by Microsoft Defender for Identity | Tactics: Discovery

View playbooks

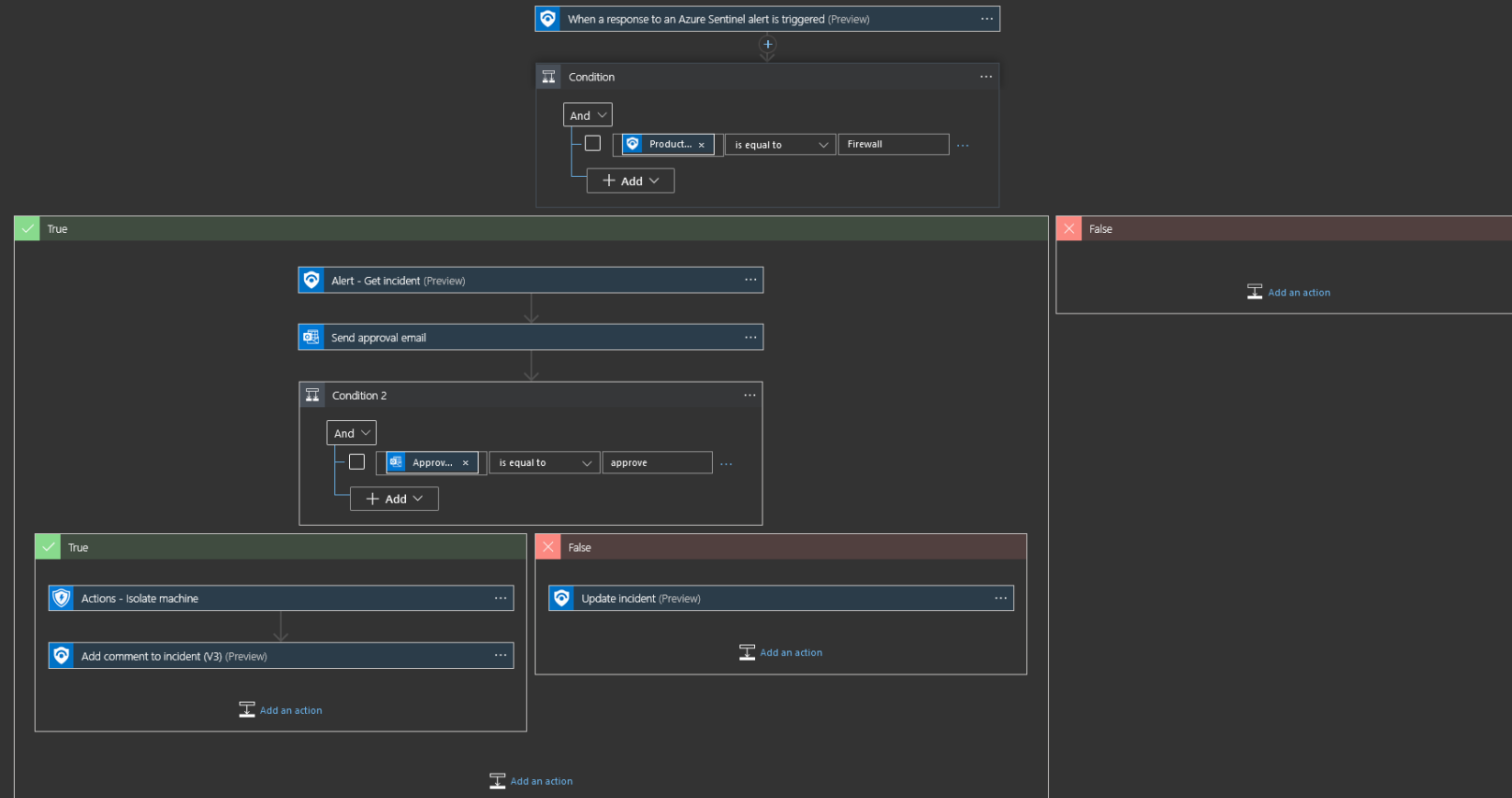
■ Investigation Graph

Incident Investigation



- Low Code programming

Automation

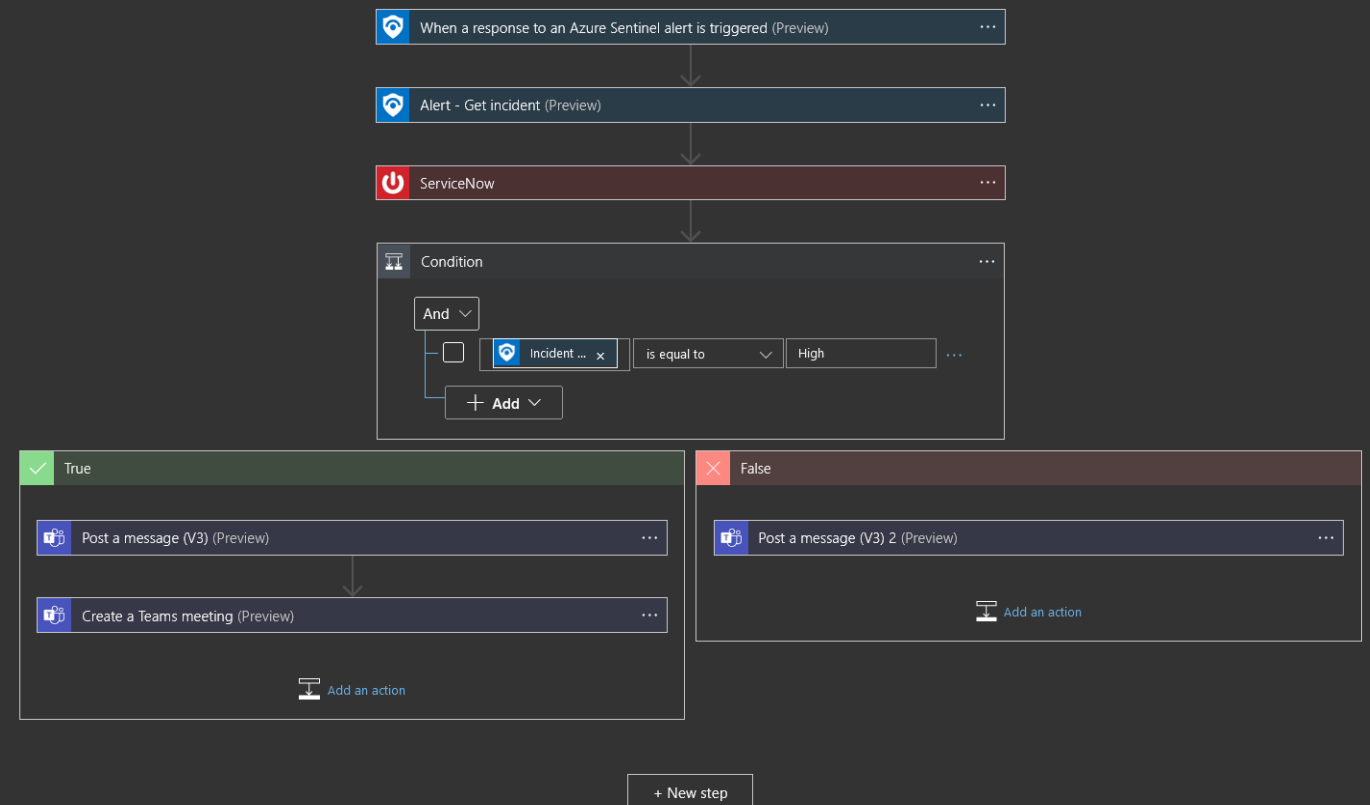


■ Low Code programming

Automation

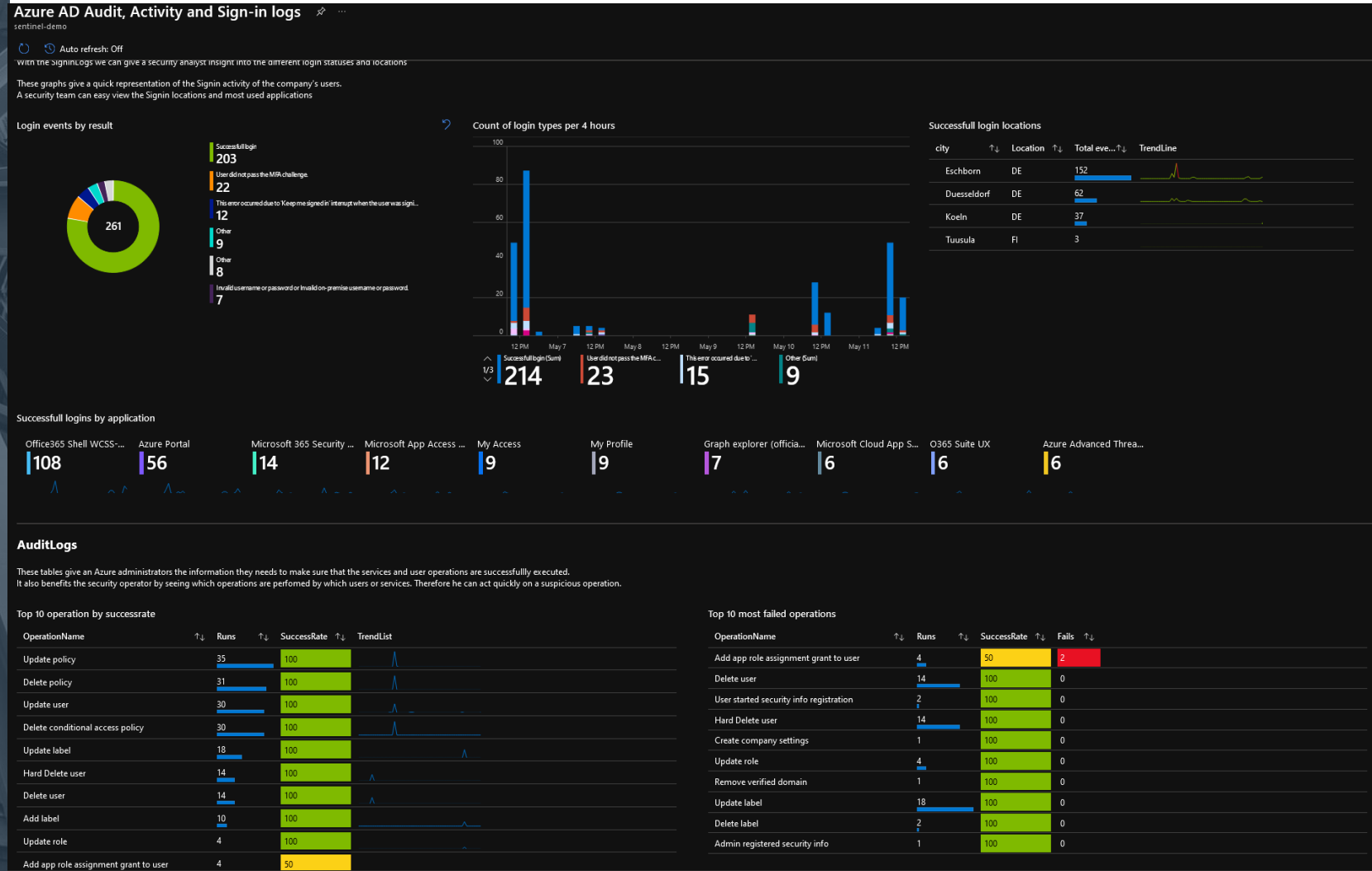
Logic Apps Designer

Save Discard Run Designer Code view Parameters Templates Connectors Help Info



■ 110 Templates

Dashboard



dinext.

create your digital tomorrow



Alex Benoit



+49 151 440 50 962



alexander.benoit@dinext.de



dinext.de