

Herzlich Willkommen

# Keine Chance für Angreifer – mit Rundum-Security von Microsoft.

---



**Rick Schwabe**

Cloud Solution Architect  
Lead Competence Center  
Microsoft Security

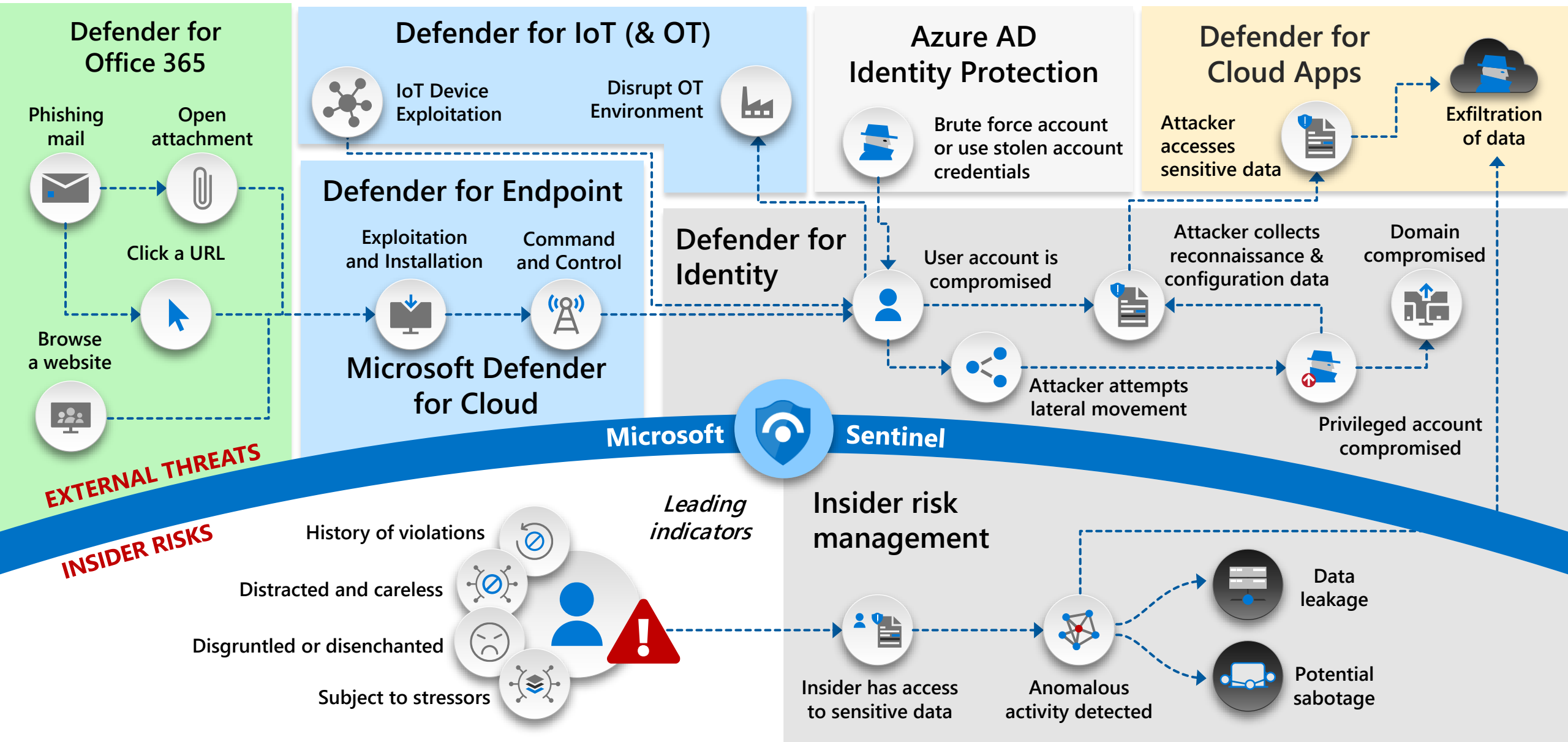
A large, stylized image of a man and a woman looking at a screen. The man is wearing glasses and a blue shirt, and the woman is wearing a grey blazer. The image is tilted and has a blue and green color scheme.

BECHTLE



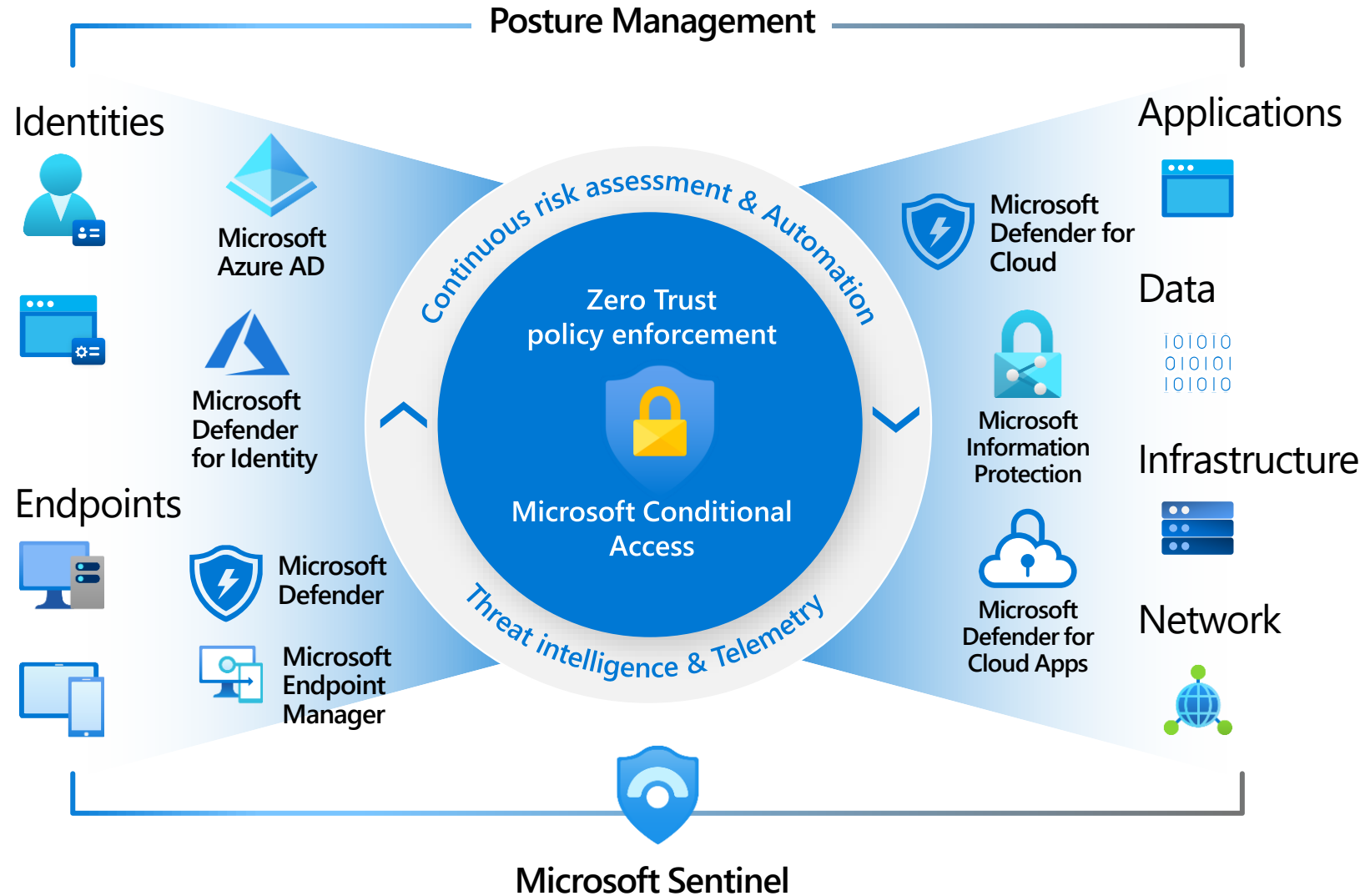
# Defend across attack chains

*Insider and external threats*





# Microsoft Zero Trust Capabilities





**Umfrage – Nutzen Sie in ihrem Unternehmen schon die Defender Produktpalette ?**

**Ja**

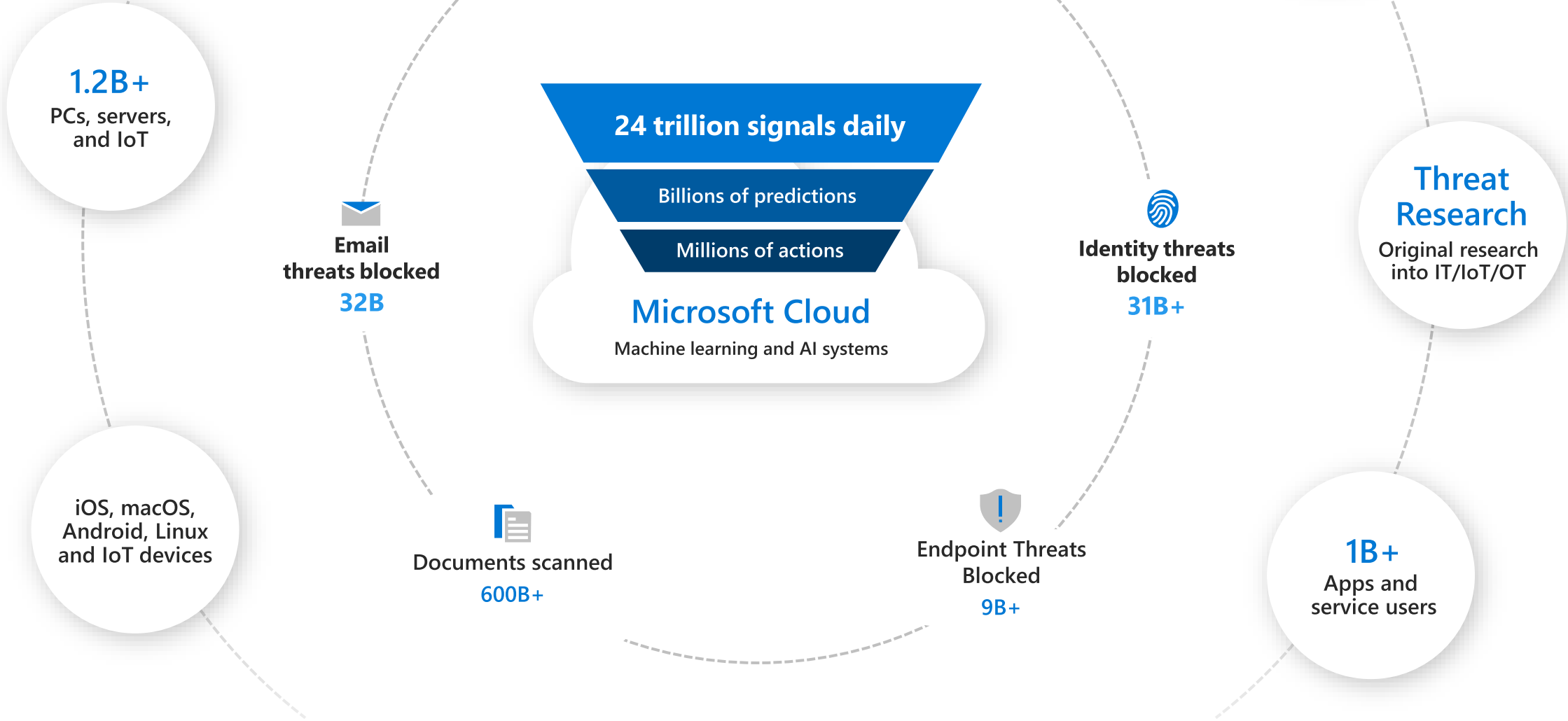
**Nein**

**Teilweise**



# Microsoft Threat Intelligence

*Built on diverse signal sources and AI*





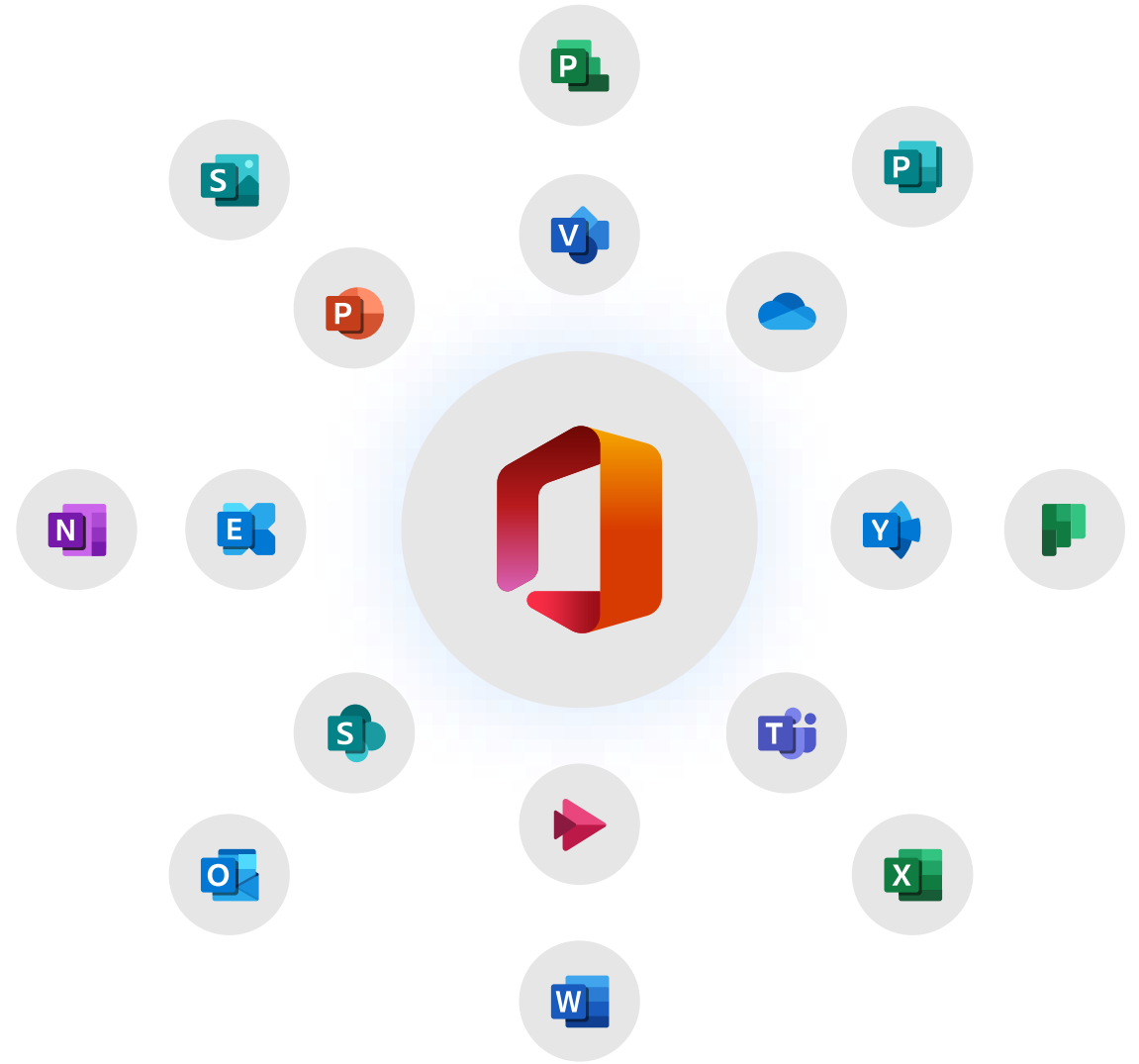
# Microsoft Defender for Office 365



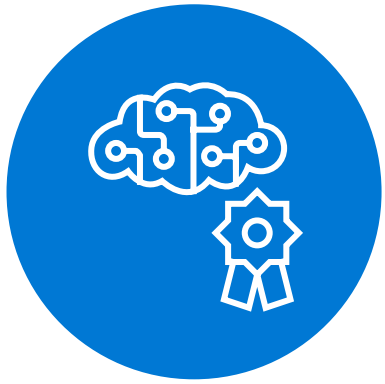




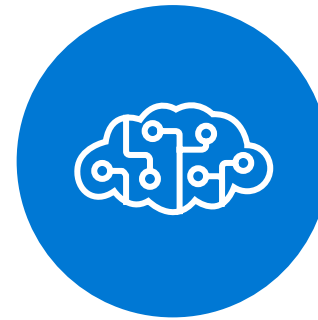
# Native protection for Office 365



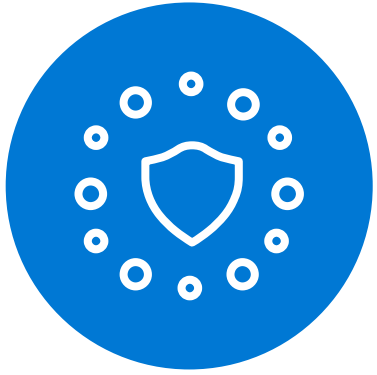




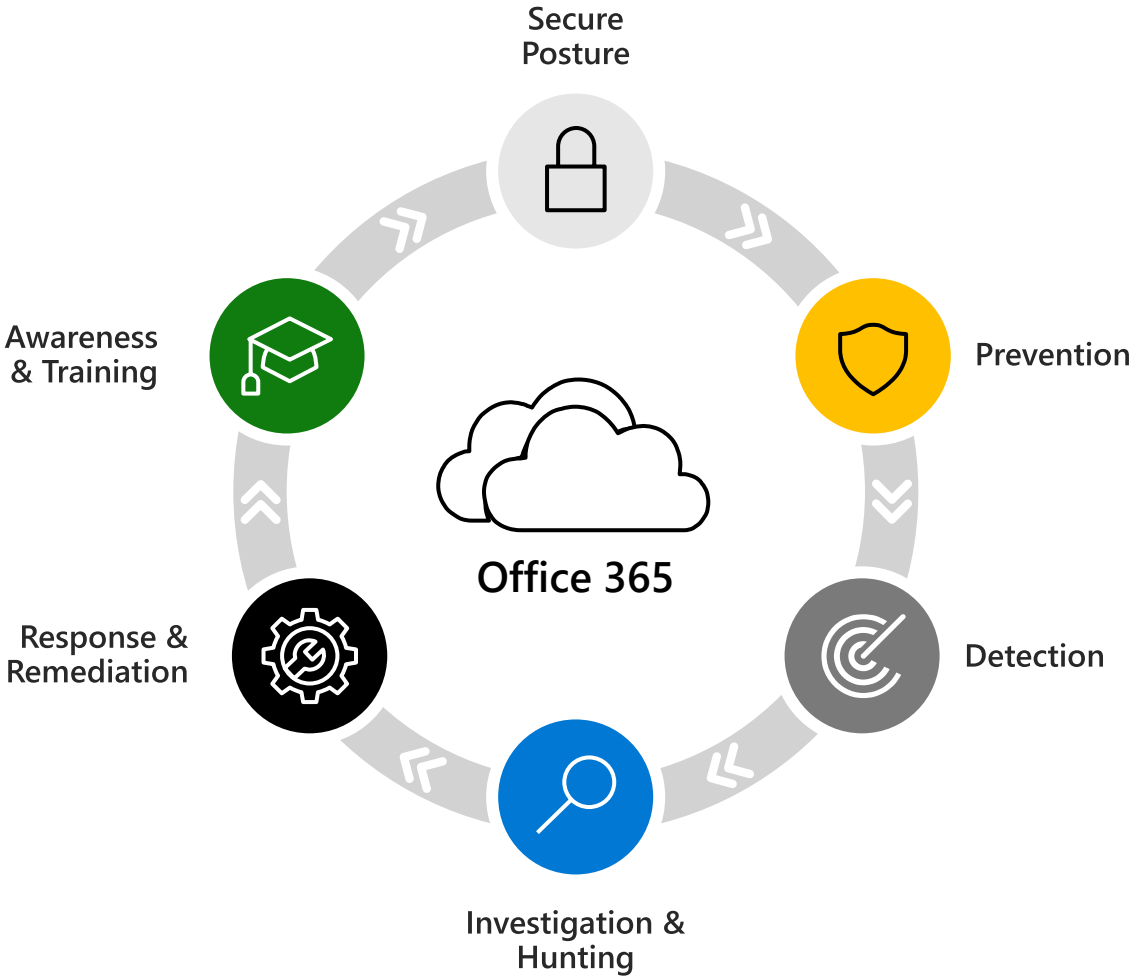
Industry-leading  
AI and automation







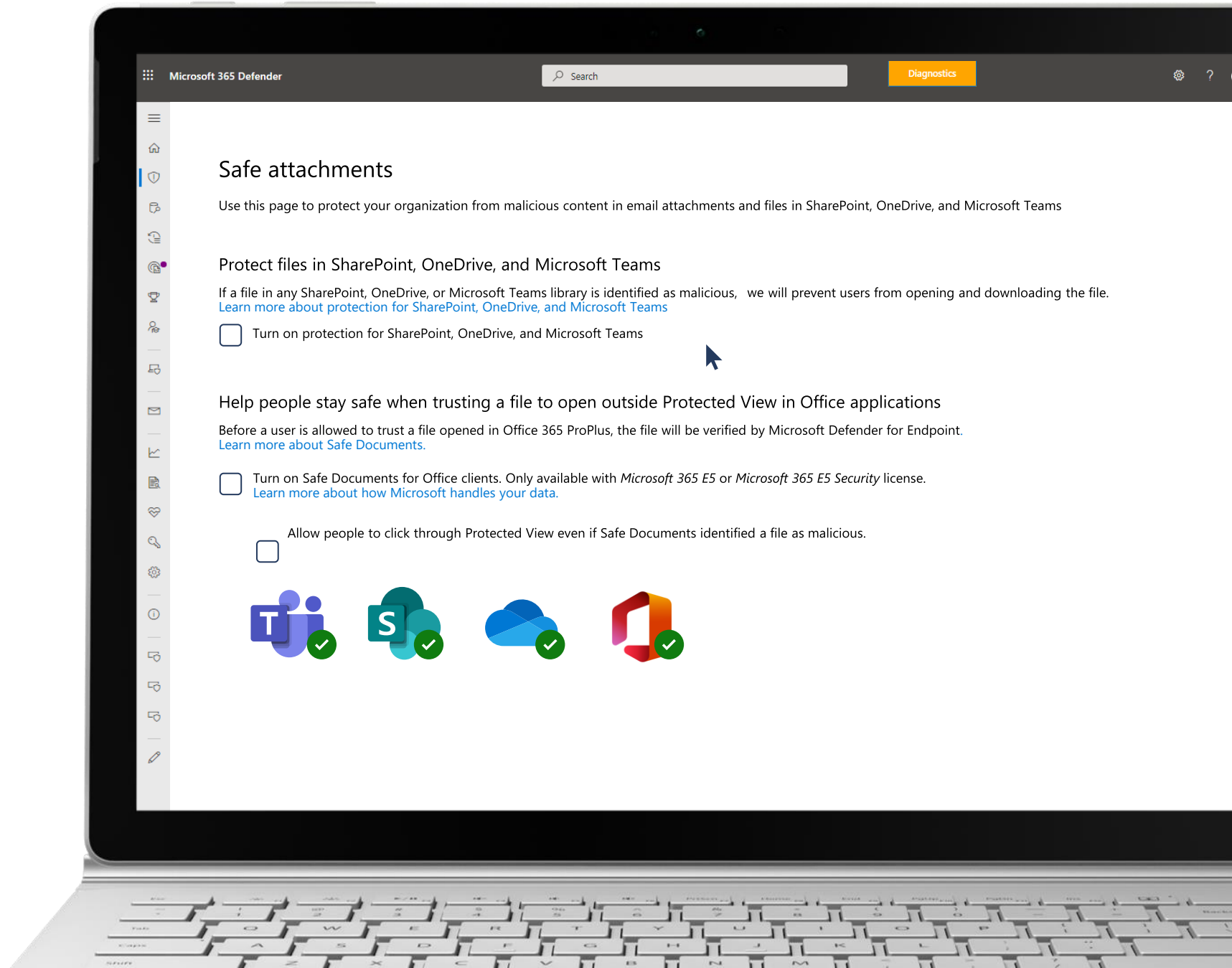
# Comprehensive approach





# Prevention

- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance
- Advanced protection against credential phishing, BEC, and account takeover
- Protection beyond email

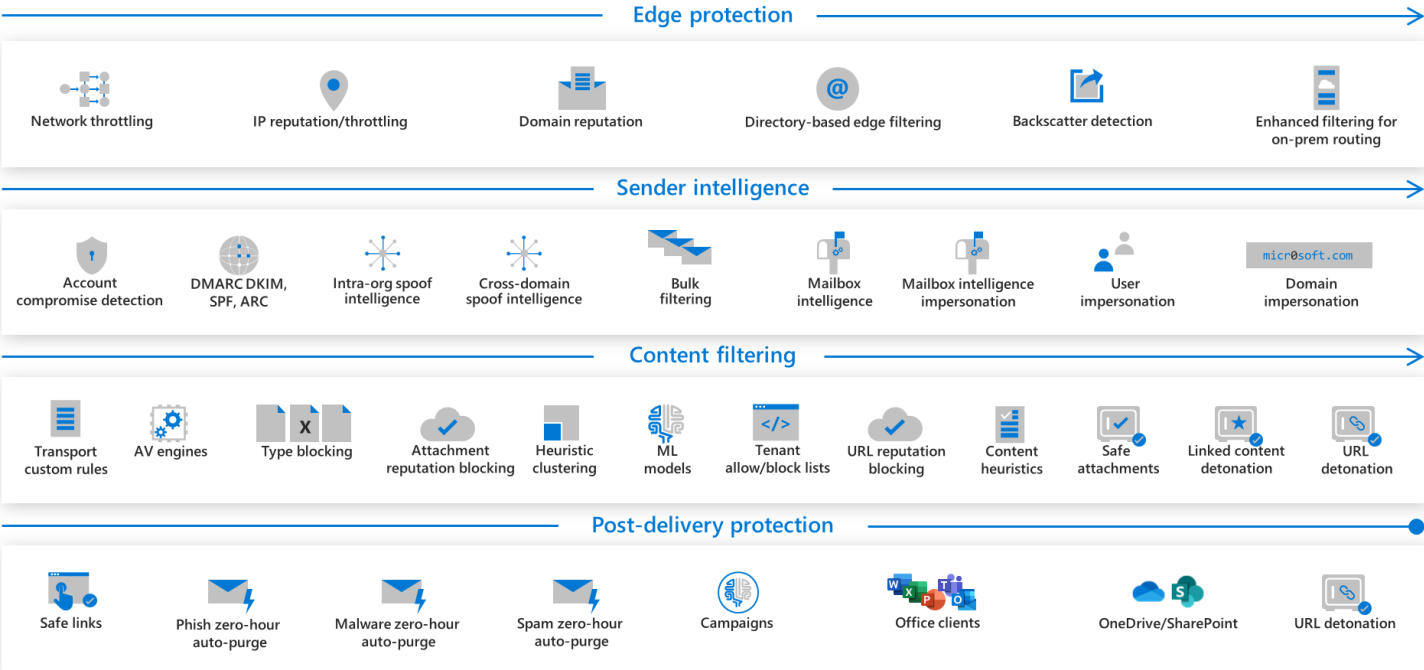




# Prevention

→ Multi-layered protection stack stops a wide variety of attacks

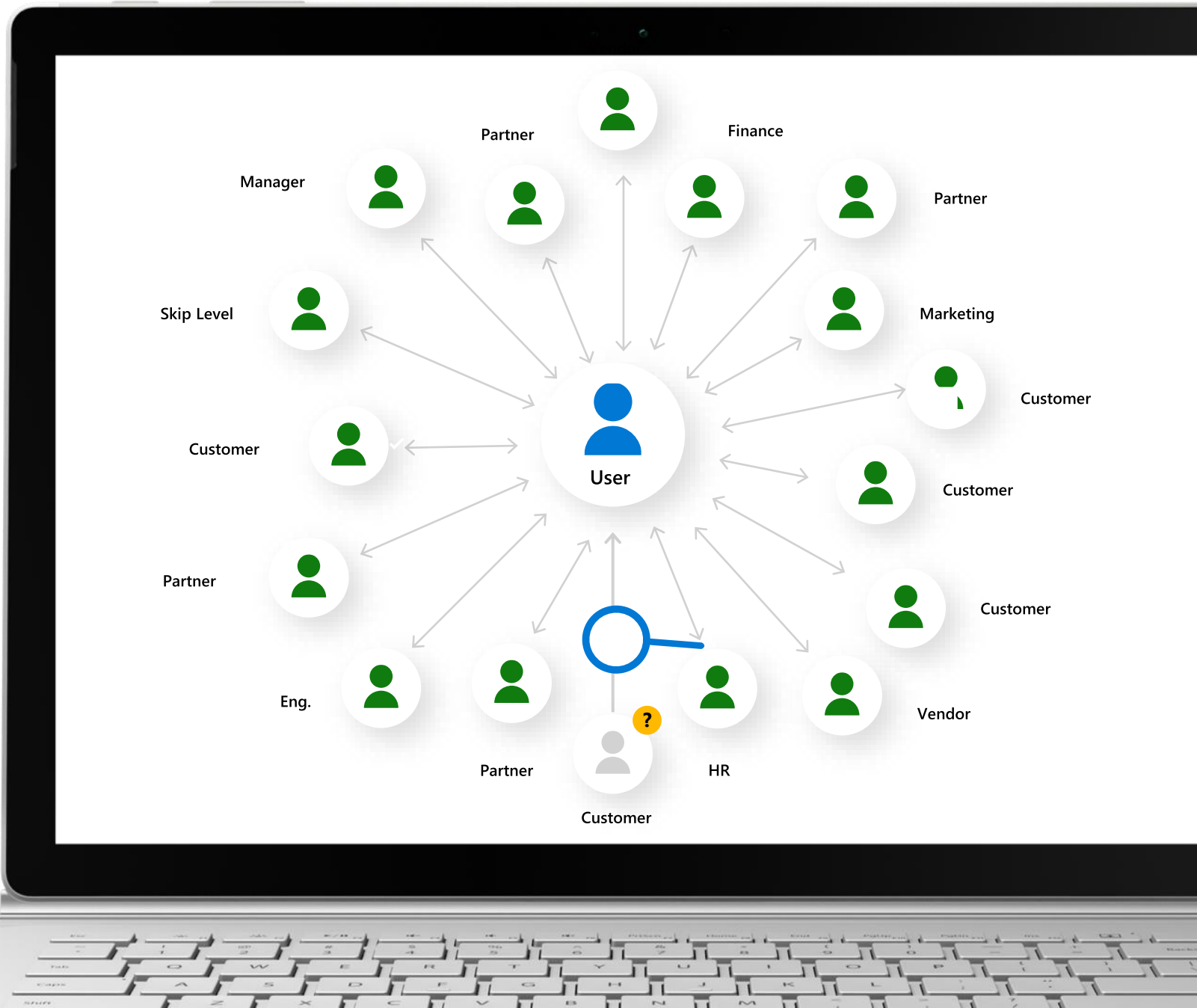
## Multi-Layered protection stack





# Prevention

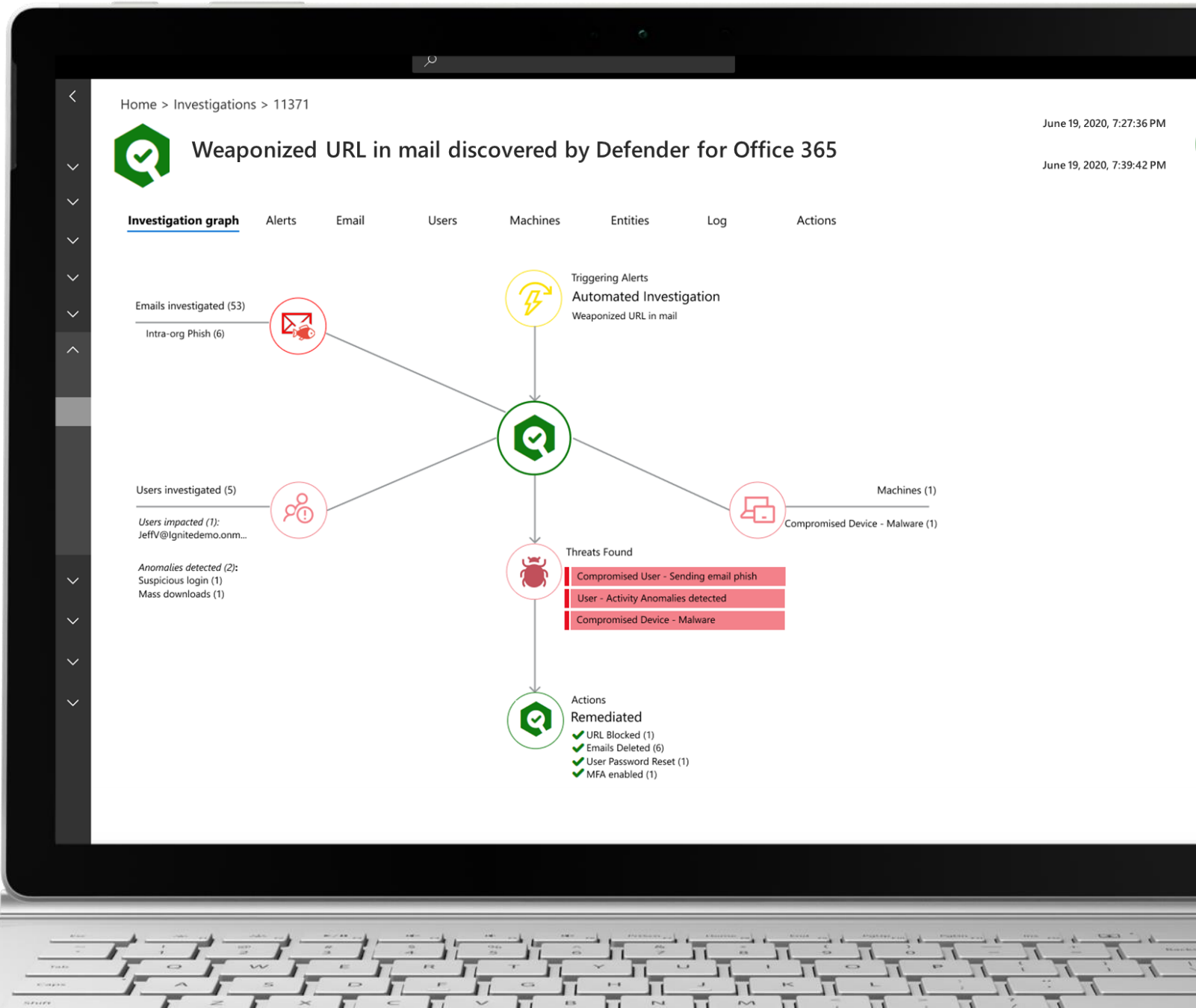
- Multi-layered protection stack stops a wide variety of attacks
- Simplified configuration guidance
- Advanced protection against credential phishing, BEC, and account takeover





# Response & Remediation

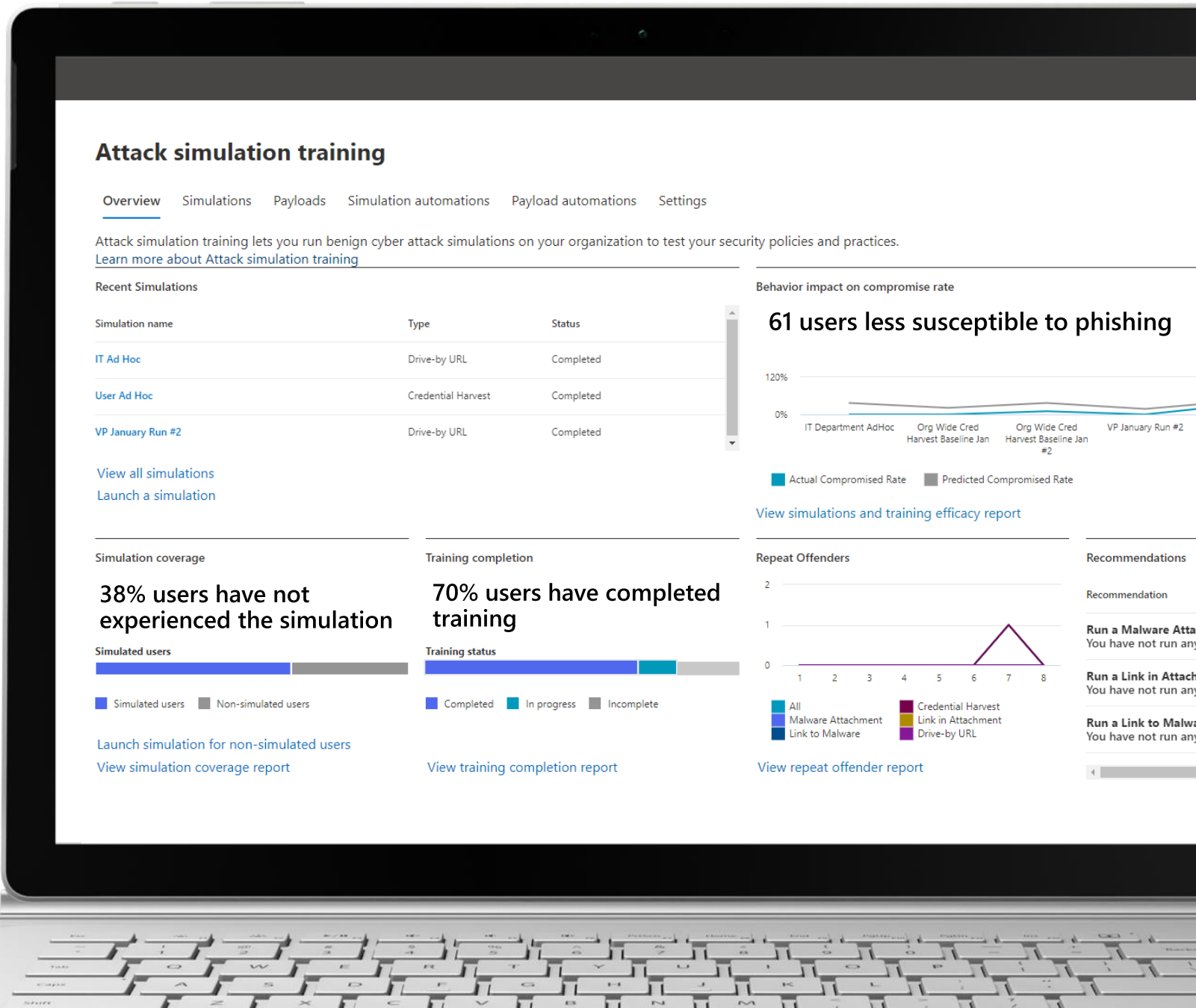
- Guided hunting with inline actions
- Centralized action queue
- Automated response playbooks





# Awareness & Training

→ Enhanced simulation management



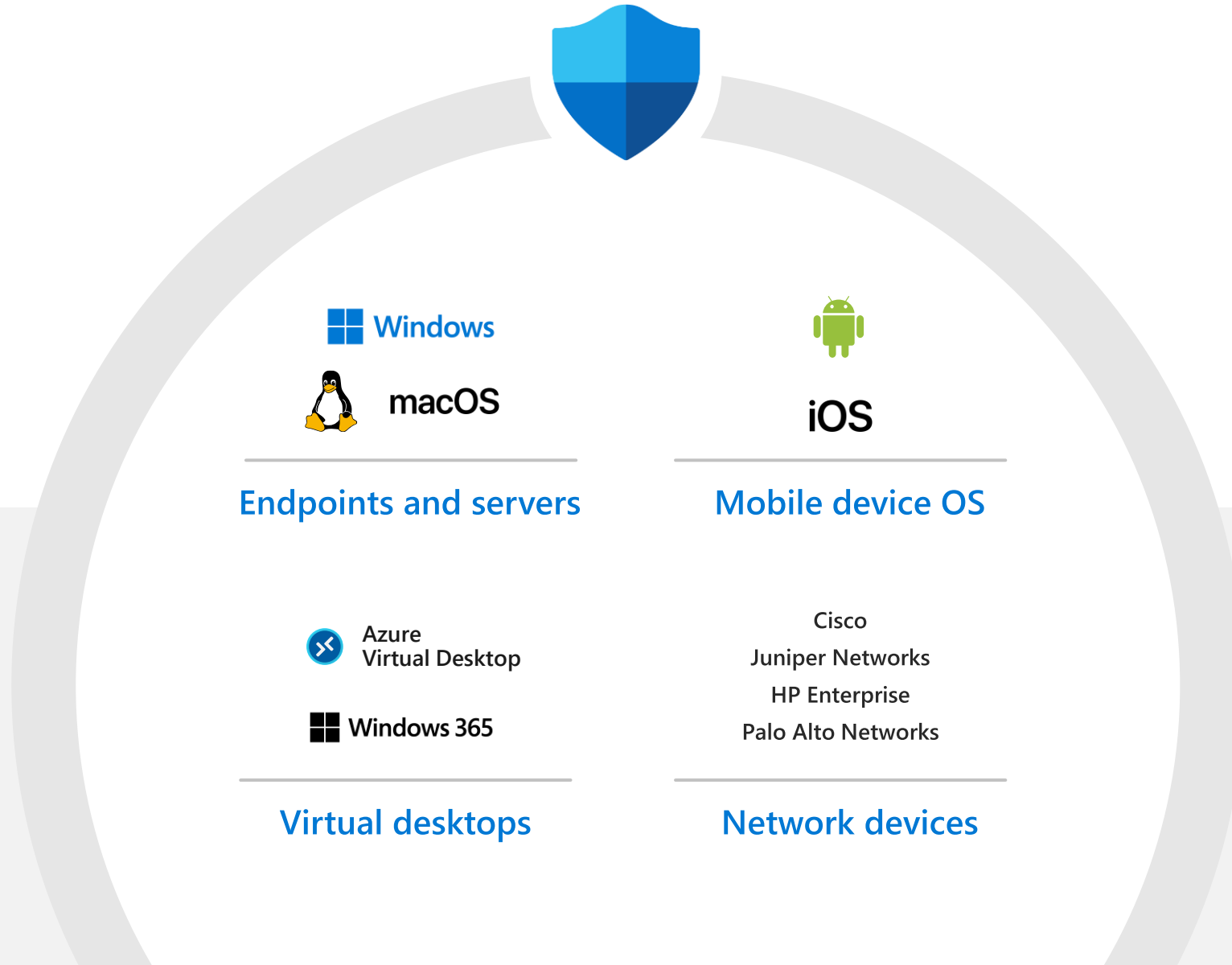


# Microsoft Defender for Endpoint





# Delivering endpoint security across platforms

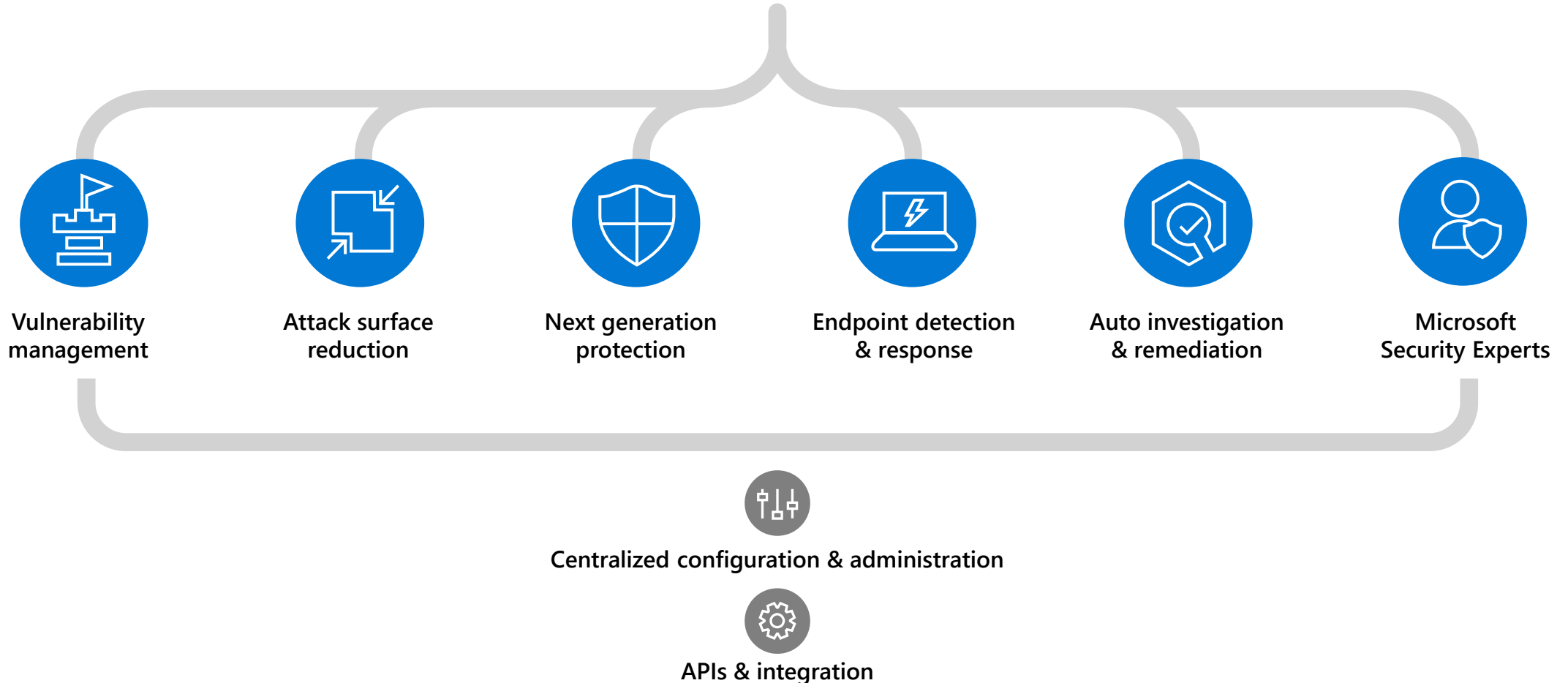






# Microsoft Defender for Endpoint

**Threats are no match.**

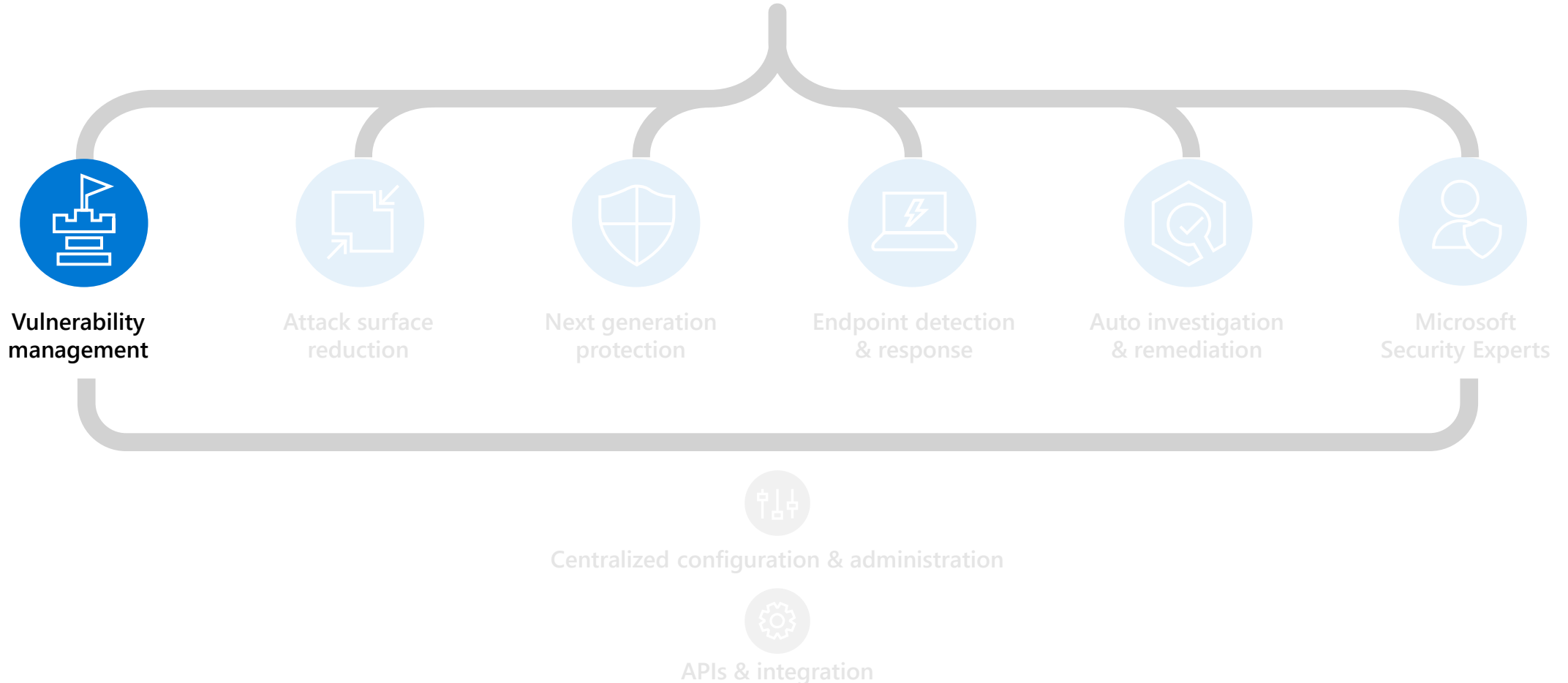






# Microsoft Defender for Endpoint

**Threats are no match.**





# Vulnerability management

A risk-based approach to prioritize and remediate your vulnerabilities



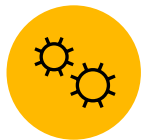
Continuous real-time discovery



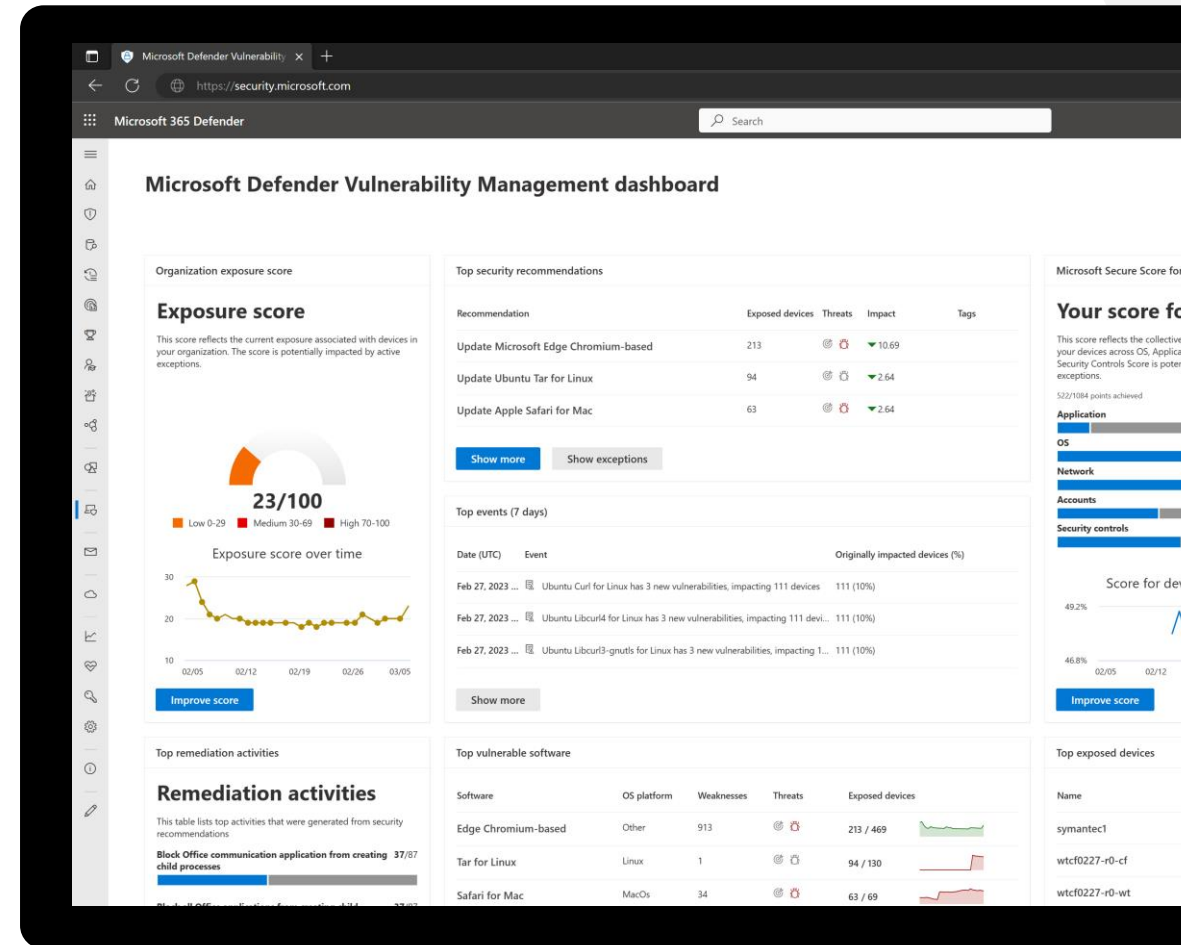
Context-aware prioritization



Built-in end-to-end remediation process



Powered by Microsoft Defender Vulnerability Management

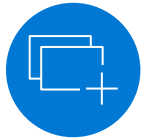




# Consolidated inventories and continuous discovery

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)



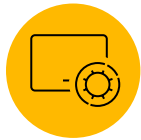
## Application run-time libraries vulnerabilities

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



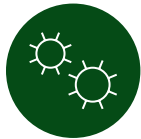
## Application vulnerabilities (first-party and third-party)

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



# In-depth vulnerability assessments

Expanded entity-level inventories and assessments



Security baselines assessments



Hardware and firmware assessments



Digital certificate assessments



Network shares analysis



Browser extensions assessments



Authenticated scans for vulnerability assessments



Leverage vulnerability data from multiple security feeds in a single prioritized view with Security Recommendations



Leverage Microsoft threat intelligence to prioritize vulnerabilities



Identify how risk is introduced through new vulnerabilities via the event timeline



1



# Continuous discovery

Broad secure configuration assessment

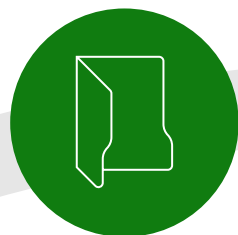
## Operation system misconfiguration

- » File Share Analysis
- » Security Stack configuration
- » OS baseline



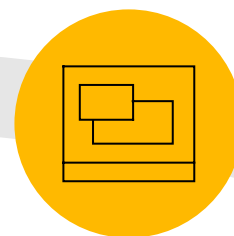
## Account misconfiguration

- » Password Policy
- » Permission Analysis



## Application misconfiguration

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



## Network misconfiguration

- » Open ports analysis
- » Network services analysis





**Get continuous baseline assessment and monitoring of endpoints against industry security benchmarks such as CIS, STIG and Microsoft Benchmarks.**

Microsoft 365 Defender

Search

Home

Incidents & alerts

Hunting

Actions & submissions

Threat analytics

Learning hub

Partner catalog

Assets

Devices

Endpoints

Vulnerability management

Dashboard

Recommendations

Remediation

Inventories

Weaknesses

Event timeline

Baselines assessment

Partners and APIs

Connected applications

API explorer

Security baselines assessment > regt

regt

Active

Configurations

Devices

Profile summary

Profile details

Description

None

Created by

gilad@wdgcp.com

Created on

6/8/2022

Last updated by

No updates

Last updated

No updates

Devices passed

0

Devices passed (%)

0.00

Configurations passed

2

Configurations passed (%)

33.33

Customized configurations

0 / 6

Export

6 items

Search

Customize columns

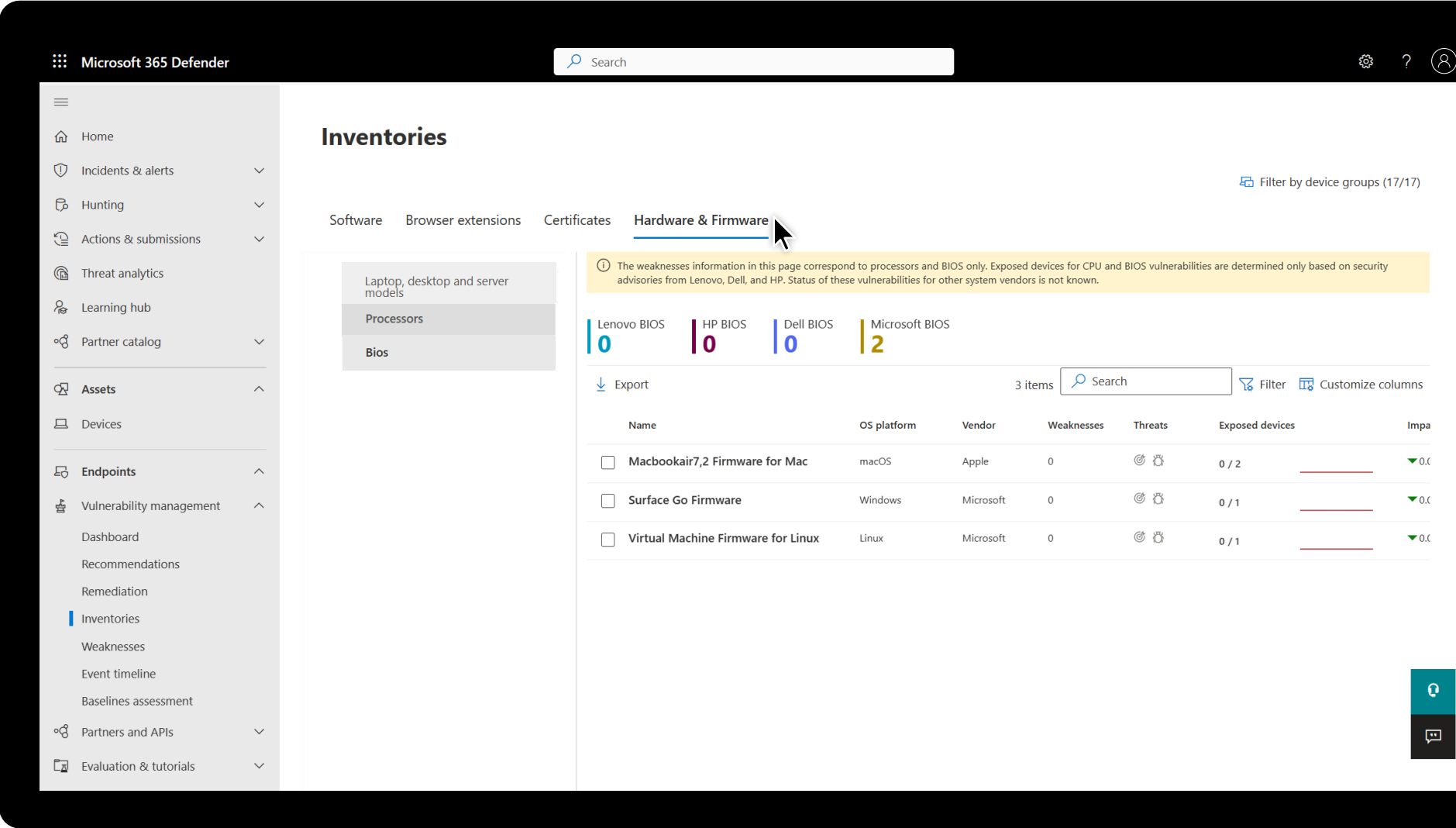
Filter

Configuration ID	Name	Category	Compliant devices	Compliance level
<input type="checkbox"/> 1.1.2	(L1) Ensure 'Maximum password age' is set to '365 or fewer days,...	Password Policy	2/2	Level 1 (L1) - Corp...
<input type="checkbox"/> 1.1.7	(L1) Ensure 'Store passwords using reversible encryption' is set to...	Password Policy	2/2	Level 1 (L1) - Corp...
<input type="checkbox"/> 1.1.6	(L1) Ensure 'Relax minimum password length limits' is set to 'Ena...	Password Policy	0/2	Level 1 (L1) - Corp...
<input type="checkbox"/> 1.1.3	(L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	Password Policy	0/2	Level 1 (L1) - Corp...
<input type="checkbox"/> 1.1.4	(L1) Ensure 'Minimum password length' is set to '14 or more char...	Password Policy	0/2	Level 1 (L1) - Corp...
<input type="checkbox"/> 1.1.5	(L1) Ensure 'Password must meet complexity requirements' is set ...	Password Policy	0/2	Level 1 (L1) - Corp...



# Hardware and firmware assessments

Full visibility into device manufacturer, processors and BIOS information to assess vulnerabilities and firmware risk

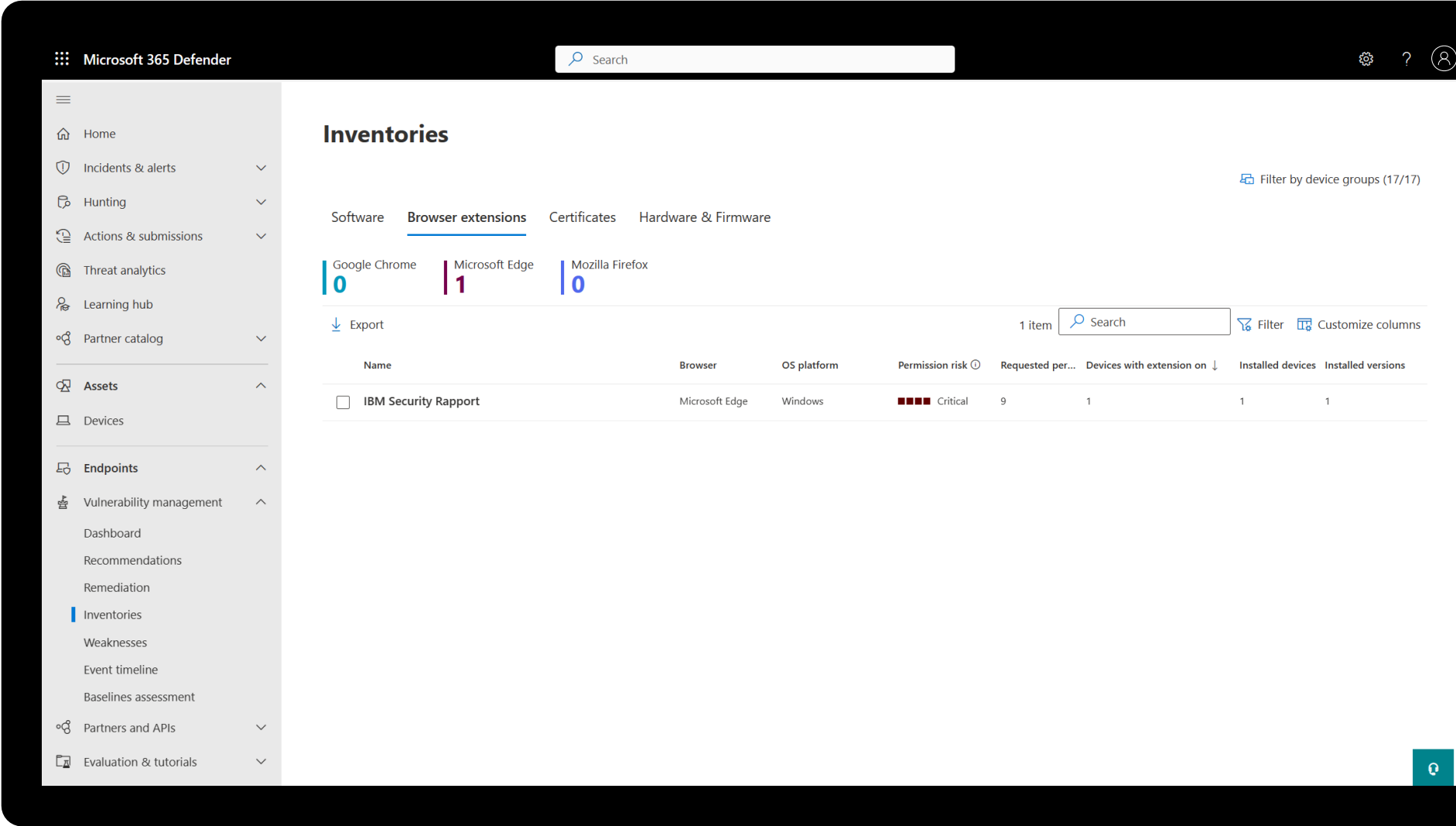




# Vulnerability and configuration assessment tools to cover more risks

## Browser extensions assessments

Expand your asset coverage beyond devices and gain entity-level visibility into the various browser extensions installed across assets, permissions requested, and associated risks





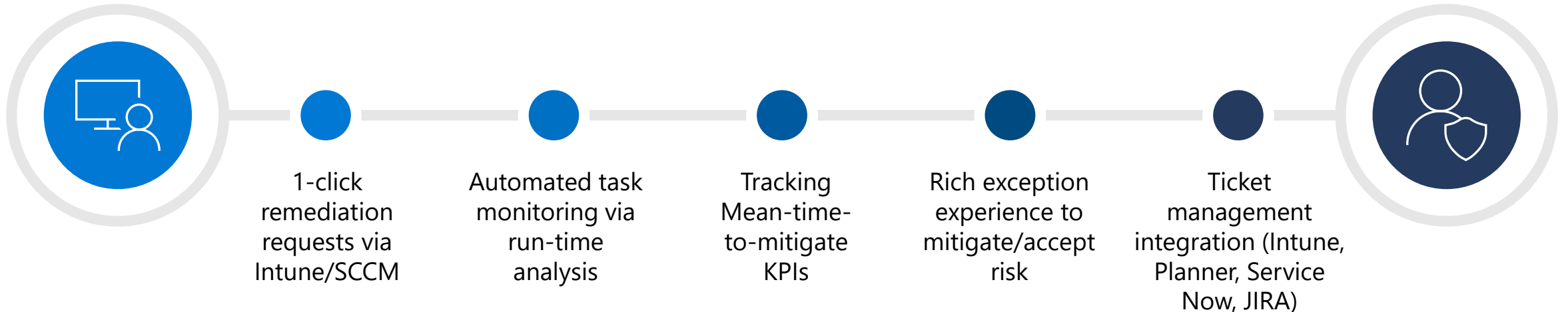
3



## Automated compensation

Simplifying the handover from Security to IT teams

Game changing bridge between IT and Security teams

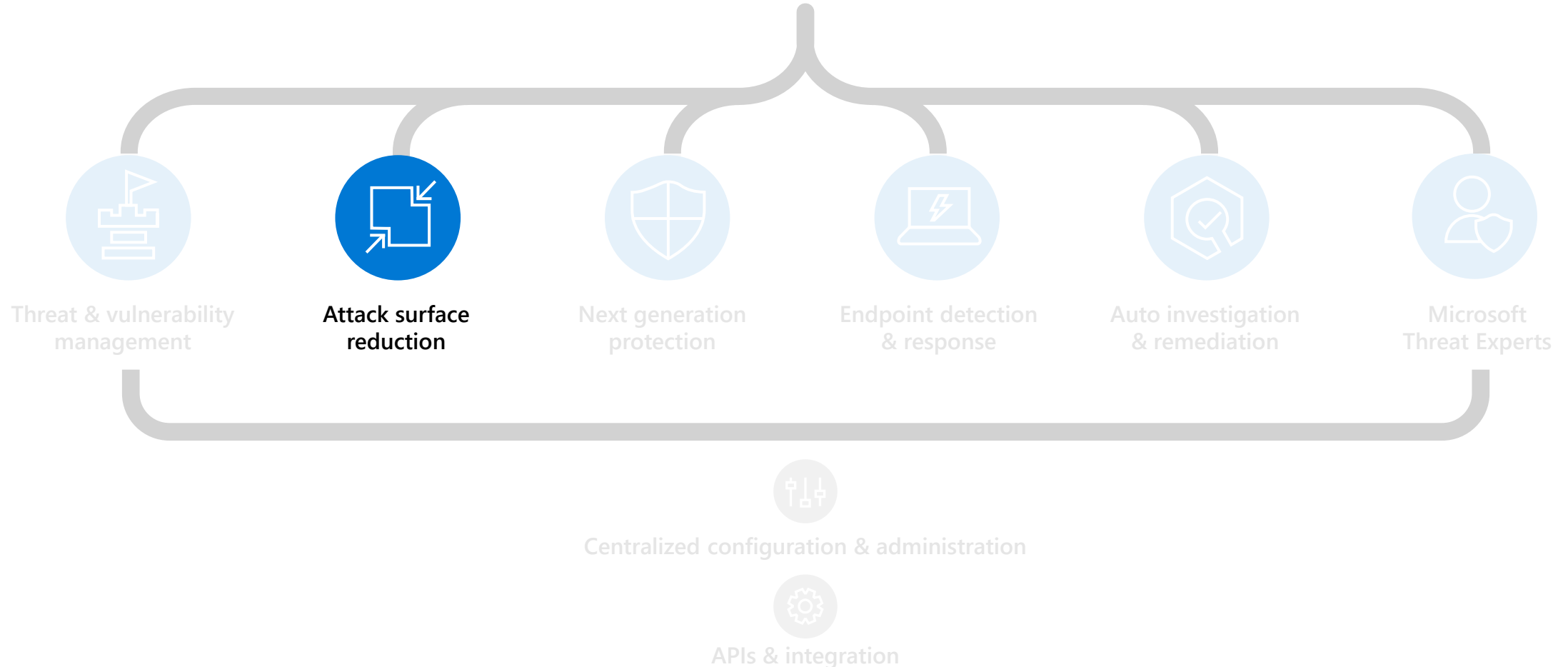






# Microsoft Defender for Endpoint

**Threats are no match.**





# Attack surface reduction

Eliminate risks by reducing the surface area of attack



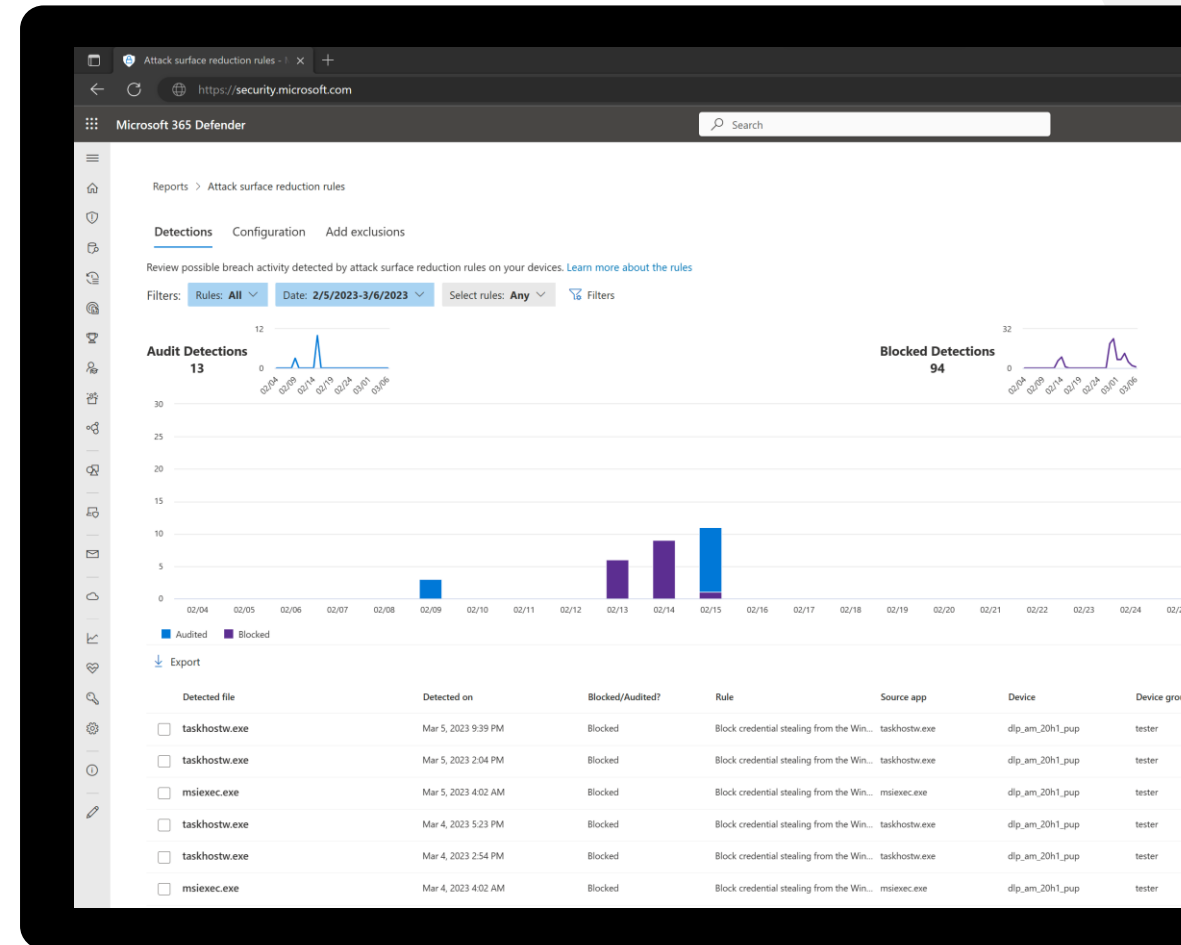
System hardening without disruption



Customization that fits your organization



Visualize the impact and simply turn it on





# 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



# 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

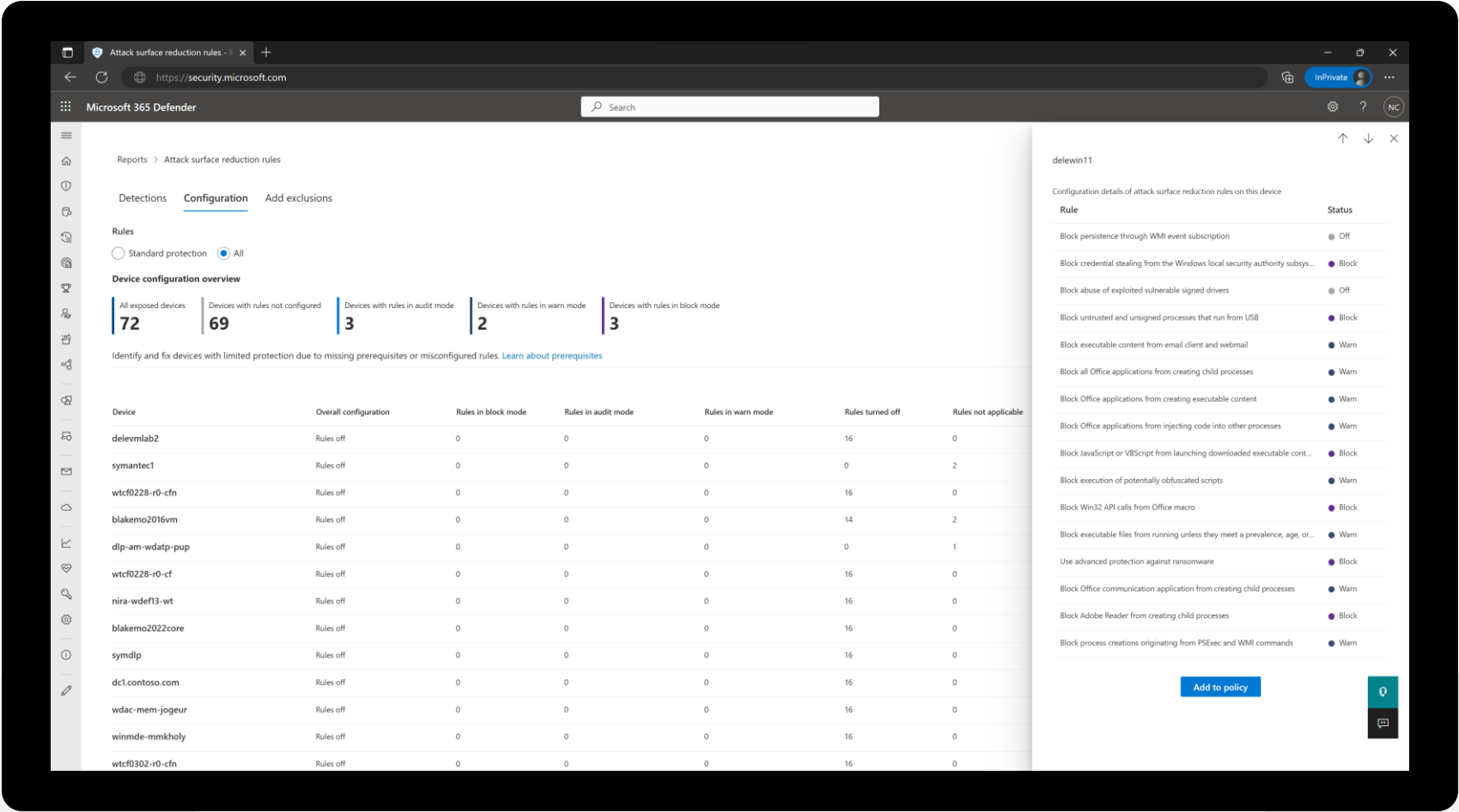
- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware
- Block abuse of exploited vulnerable signed drivers

### Lateral movement and 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



# Easy button: turn on block

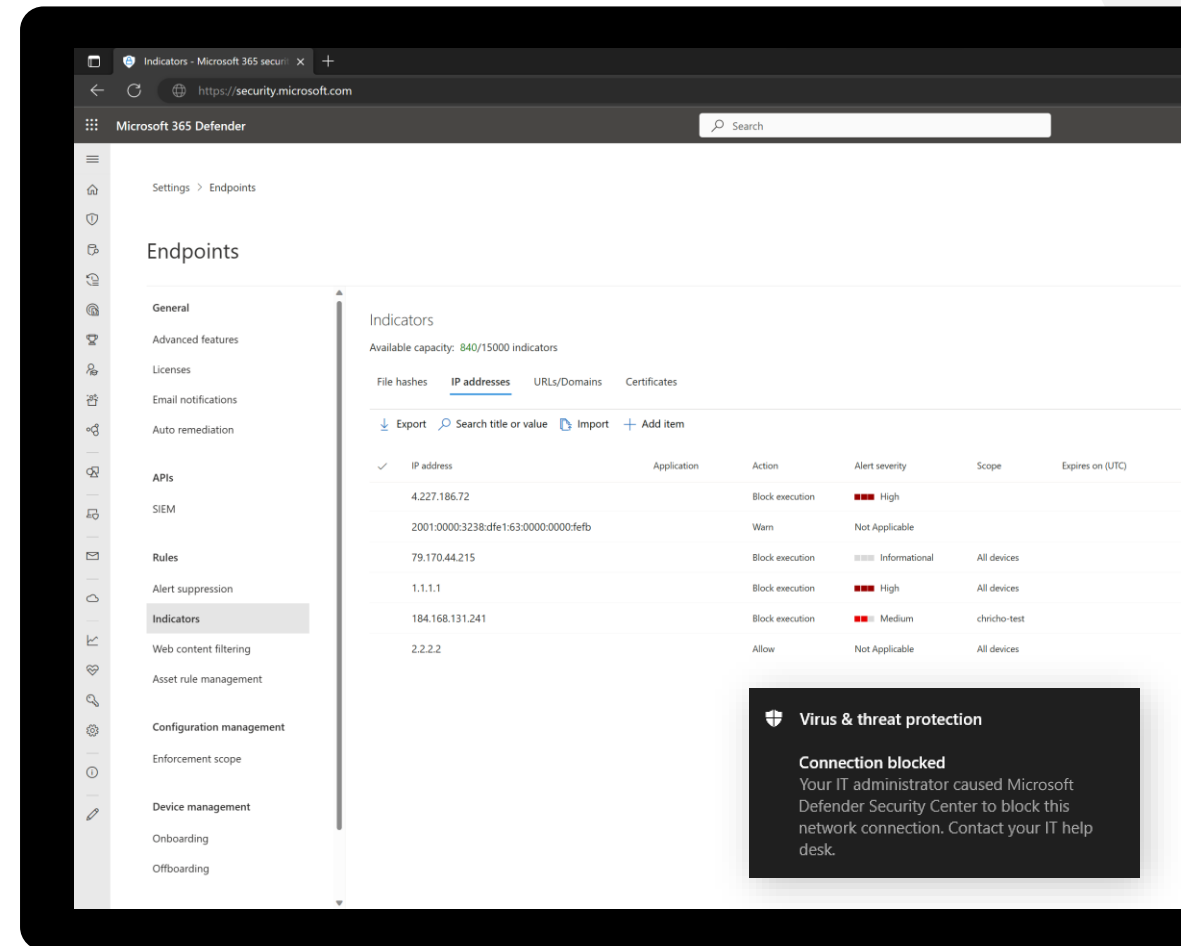




# Network protection

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





# Web threat alerts

The screenshot displays the Microsoft 365 Defender web interface. The browser address bar shows `https://security.microsoft.com`. The page title is "Alert - Microsoft 365 security". The main content area is titled "Alerts > Network Protection blocked a potential C2 connection".

At the top, there are two notification banners:

- The MDE SIEM API deprecation date has been set to December 31, 2023. Please see the [announcement](#) to plan your migration to a supported API.
- Part of incident: Multi-stage incident involving Initial access & Command and control including Ransomware on one endpoint. [View incident page](#)

The alert details show:

- Entity: `blakemowin1...` (Risk level: High)
- Source: `BLAKEMOWIN10VM\Blake`
- Operating System: Windows10
- Group: BLAKEMO
- Group: Blakemo Group

The "Alert story" section shows a timeline of events:

- 2:56:33 PM: `[7184] explorer.exe`
- 2:56:59 PM: `[10012] chrome.exe`
- 2:57:01 PM: `[11216] chrome.exe --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1752.56638547986399417...`
- 3:03:14 PM: Network connect Outbound connection from 10.0.0.108:61361 to 23.99.0.12:443
  - Network Protection blocked a potential C2 connection (Medium, Detected, New)
  - Suspicious connection blocked by network protection (Informational, Detected, New)
- 3:03:15 PM: Network Filter Lookup Service blocked chrome.exe from accessing `https://commandcontrol.smartscreentestratings.com`
  - Network Protection blocked a potential C2 connection (Medium, Detected, New)
  - Suspicious connection blocked by network protection (Informational, Detected, New)
- 3:03:15 PM: Network connect Outbound connection from 10.0.0.108:61361 to 23.99.0.12:443
  - Network Protection blocked a potential C2 connection (Medium, Detected, New)
  - Suspicious connection blocked by network protection (Informational, Detected, New)
- 3:03:16 PM: Network Filter Lookup Service blocked chrome.exe from accessing `https://commandcontrol.smartscreentestratings.com`
  - Suspicious connection blocked by network protection (Informational, Detected, New)

The right-hand panel shows the "Details" tab for the alert:

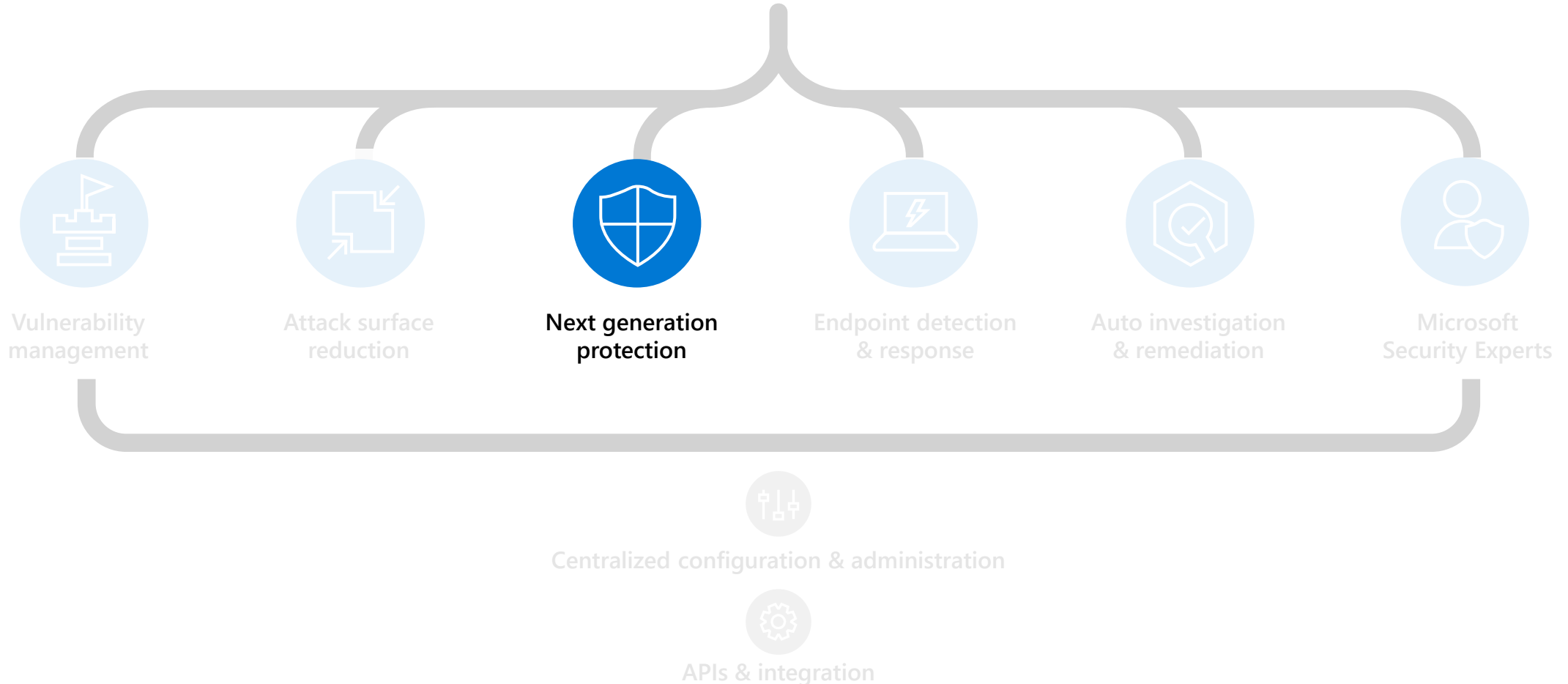
- Network Protection blocked a potential C2 connection** (Medium, Detected, New)
- Buttons: Manage alert, See in timeline, Create suppression rule
- Details** tab is active. It includes an "INSIGHT" section with a "Classify alert" button and a "View 1 similar alert" link.
- Alert state** section: Classification is "Assigned to Not Set", Remediation Status is "Unassigned". A "Set Classification" button is available.
- Alert details** section: Evidence is shown for the URL `https://commandcontrol.smartscreentestratings.com`.





# Microsoft Defender for Endpoint

**Threats are no match.**





# Static versus dynamic



**Ineffective**

Static signatures:  
focus on a file

- » Hashes
- » Strings
- » Emulators

**Effective**



Dynamic heuristics:  
focus on *run-time* behaviors

- » Behavior monitoring
- » Memory scanning
- » AMSI
- » Command-line scanning



# Next generation protection

Blocks and tackles sophisticated threats and malware



Behavioral based real-time protection



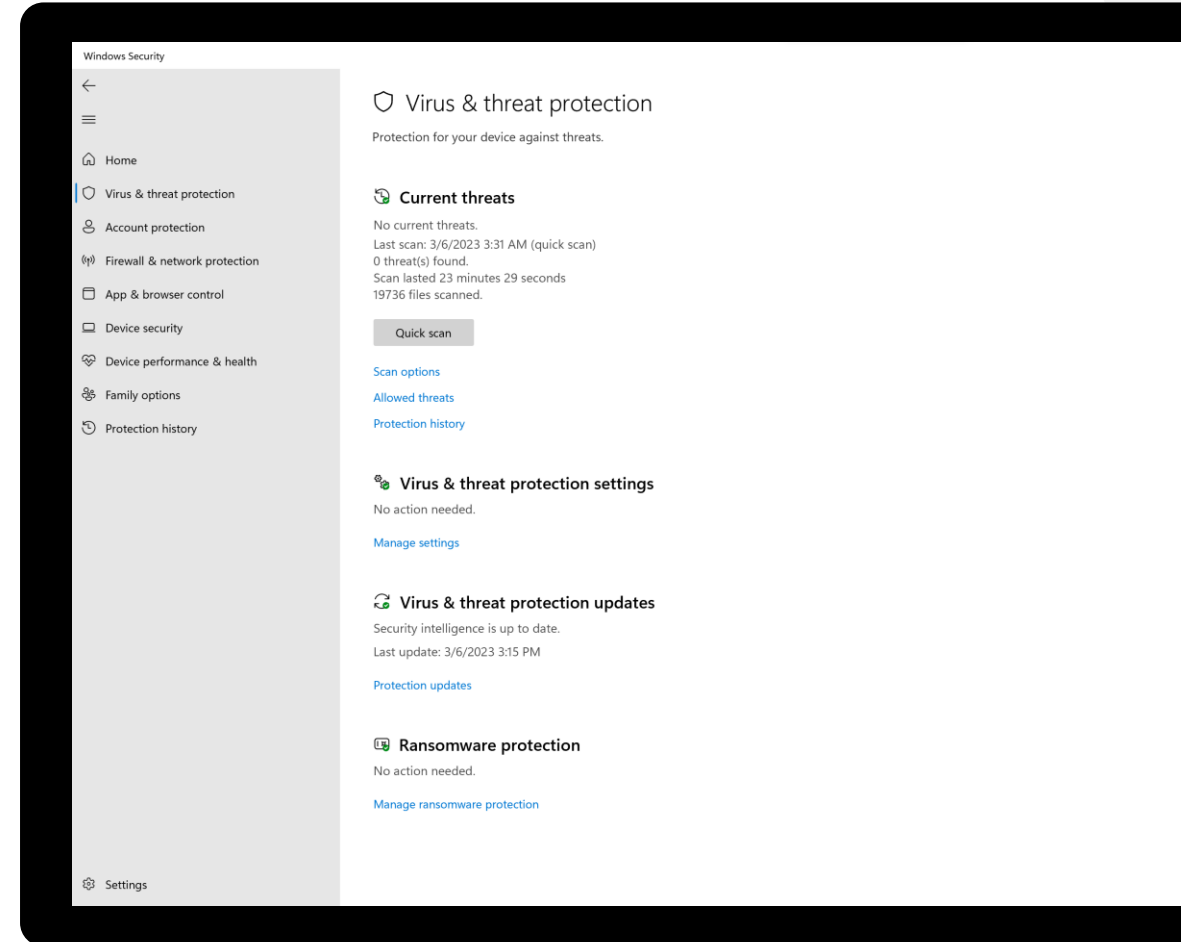
Blocks file-based and fileless malware



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).





# Microsoft Defender for Endpoint next generation protection engines



**Metadata-based ML**  
Stops new threats quickly by analyzing metadata



**Behavior-based ML**  
Identifies new threats with process trees and suspicious behavior sequences



**AMSI-paired ML**  
Detects fileless and in-memory attacks using paired client and cloud ML models



**File classification ML**  
Detects new malware by running multi-class, deep neural network classifiers



**Detonation-based ML**  
Catches new malware by detonating unknown files



**Reputation ML**  
Catches threats with bad reputation, whether direct or by association



**Smart rules**  
Blocks threats using expert-written rules



**ML**  
Spots new and unknown threats using client-based ML models



**Behavior monitoring**  
Identifies malicious behavior, including suspicious runtime sequence



**Memory scanning**  
Detects malicious code running in memory



**AMSI integration**  
Detects fileless and in-memory attacks



**Heuristics**  
Catches malware variants or new strains with similar characteristics



**Emulation**  
Evaluates files based on how they would behave when run



**Network monitoring**  
Catches malicious network activities

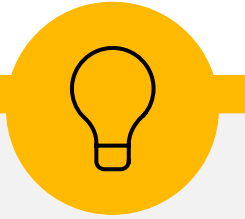


# Dynamic: behavior monitoring



## Monitors activity on:

- » Files
- » Registry keys
- » Processes
- » Network (basic HTTP inspection)
- » ...and few other specific activities

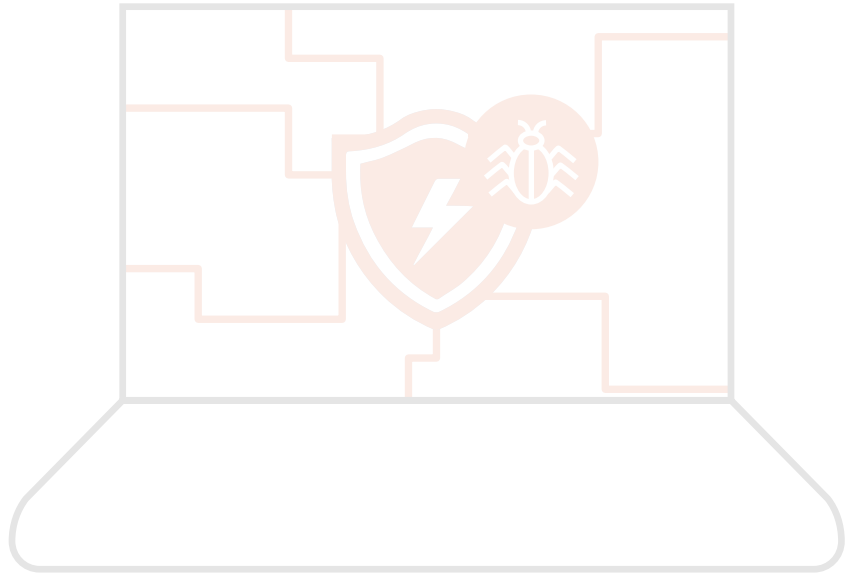


## Heuristics can:

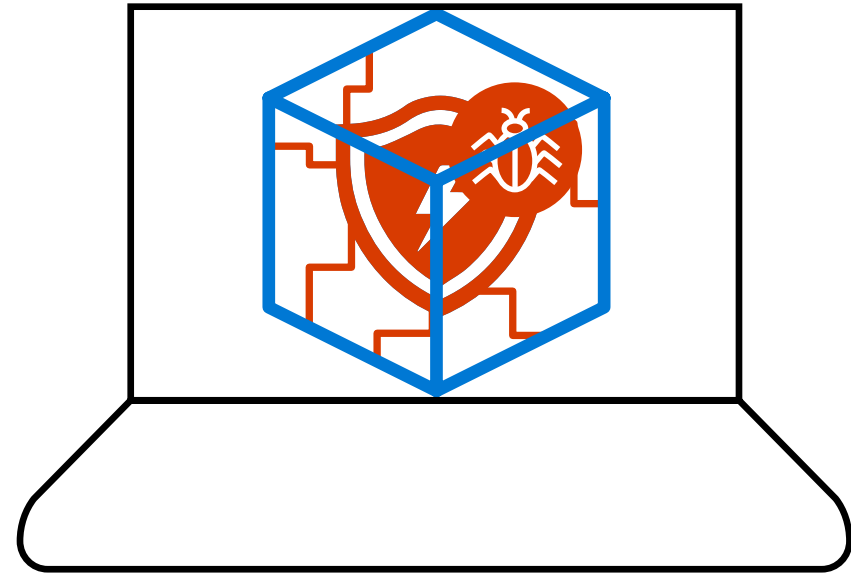
- » **Detect sequences of events**  
E.g., a file named "malware.exe" is created
- » **Inspect event data**  
E.g., an AutoRun key is created and contains "malware.exe"
- » **Correlate with other static signals**  
E.g., "malware.exe" has an attribute indicating it is a DotNet executable
- » **Perform some basic remediation**  
E.g., delete "malware.exe" if the BM event reported infection
- » **Request memory scan of running processes**



# Sandboxing of the antivirus engine



Then



Now



Read the [blog](#) for more details



# Firmware and hardware protections

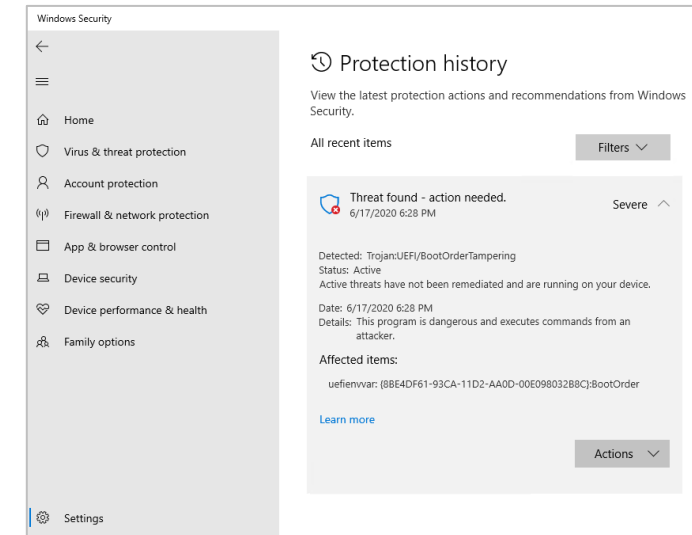
UEFI scanner reads firmware file system at runtime by interacting with the motherboard chipset, performing dynamic analysis using multiple solution components:

- UEFI anti-rootkit, which reaches the firmware through Serial Peripheral Interface (SPI)
- Full filesystem scanner, which analyzes content inside the firmware
- Detection engine, which identifies exploits and malicious behaviors

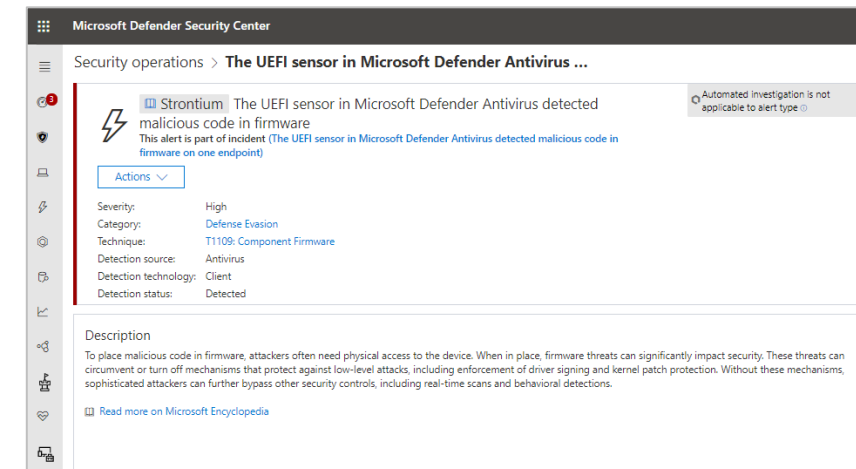


Read the [blog](#) for more details

## Scanning and detection



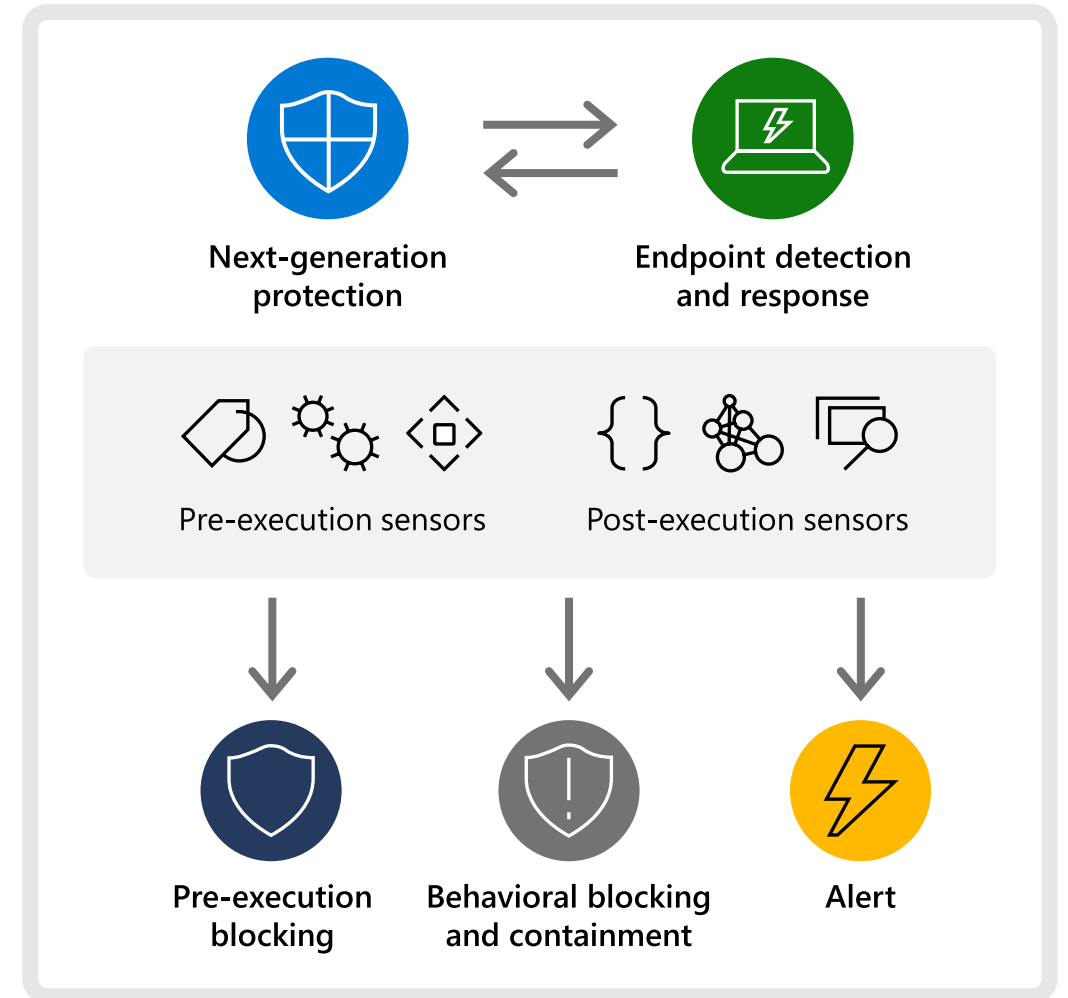
## Microsoft Defender Security Center





# Behavioral blocking and containment

- Immediately stops threat before it can progress
- Microsoft has the unique ability to scan signals across kill chains and payloads (endpoints, Office, Identity, etc.)
- Some highlights:
  - Pre and post breach AI- and ML- based behavioral blocking and containment
  - Detect malware after first sight and block it on other endpoints within minutes (1 – 5 minutes)
  - Microsoft Defender for Endpoint provides an additional protection layer by blocking/preventing malicious behavior even if we are not the primary AV



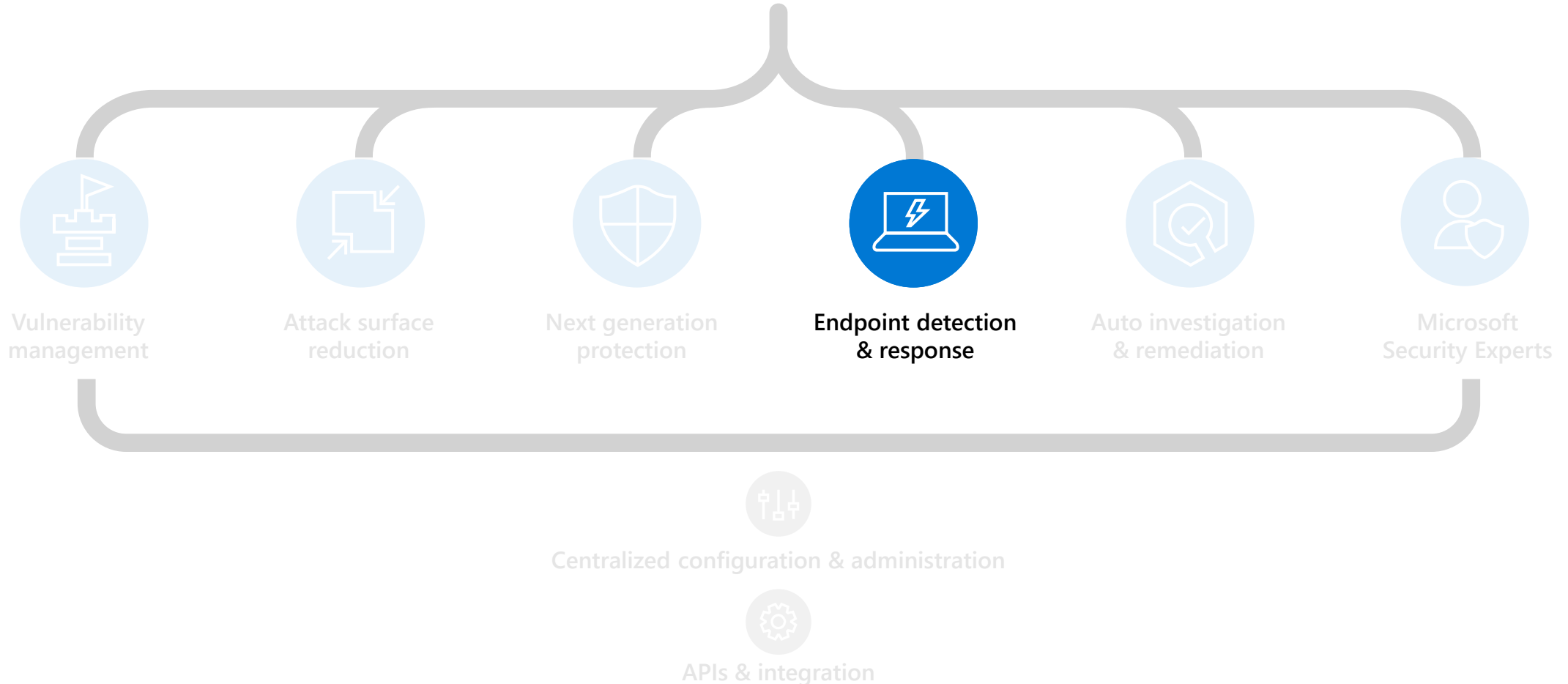
Read the [blog](#) for more details





# Microsoft Defender for Endpoint

**Threats are no match.**





# Endpoint detection & response

Detect and investigate advanced persistent attacks



Correlated behavioral alerts



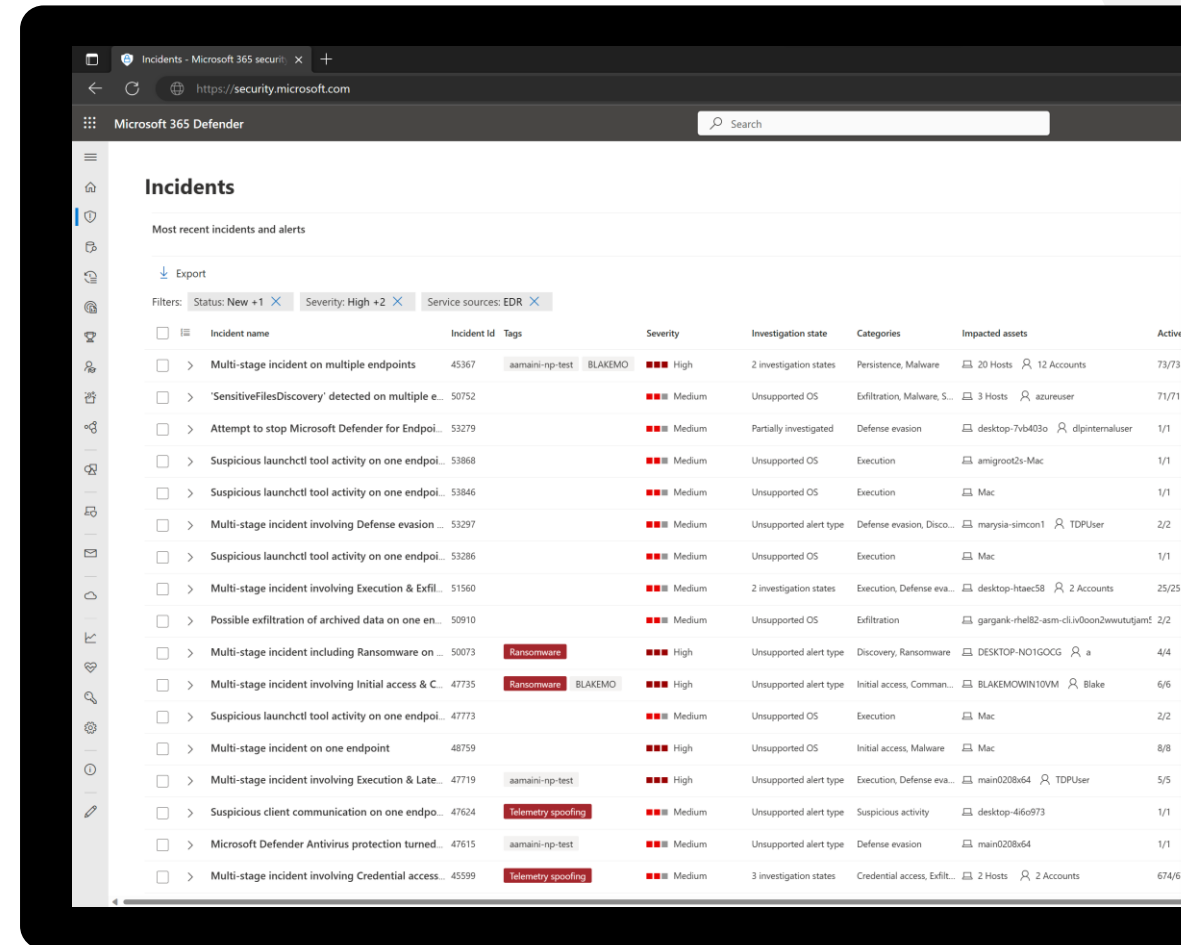
Investigation and hunting over six months of data



Rich set of response actions



Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation





# Endpoint detection & response



Correlated post-breach detection

Investigation experience

Incident

Advanced hunting

Response actions (+EDR blocks)

Deep file analysis

Live response

Threat analytics





# Triage and investigation

## Understand what was alerted

Alert investigation experience provides detailed description, rich context, full process execution tree

## Investigate device activity

Full machine timeline to drill into activities, filter and search

## Rich supporting data and tools

Supporting profiles for files, IPs, URLs including org and world prevalence, deep analysis sandbox

## Expand scope of breach

In-context pivoting to other affected machines/users

The collage displays five screenshots from a security investigation tool:

- Files > control.exe**: Shows file details for `control.exe`, including SHA1, SHA256, MD5, and Size. It also shows a timeline of activity from July 2019 to September 2019.
- Alerts > COM hijacking**: Shows an alert for "COM hijacking" with a severity of Medium. It includes a description of the alert, a list of recommended actions, and a process tree diagram.
- Machines > apt29-client3**: Shows details for the machine `apt29-client3`, including its domain, OS, version, build, health state, and first/last seen times.
- Timeline**: Shows a timeline of events for the machine `apt29-client3`, including a highlighted alert for "COM hijacking" and a list of events with their timestamps and descriptions.
- control.exe created process powershell.exe**: Shows event information for the process `powershell.exe` created by `control.exe`, including the event time, action type, and user.



# Incidents

Narrate the end-to-end attack story

## Reconstructing the story

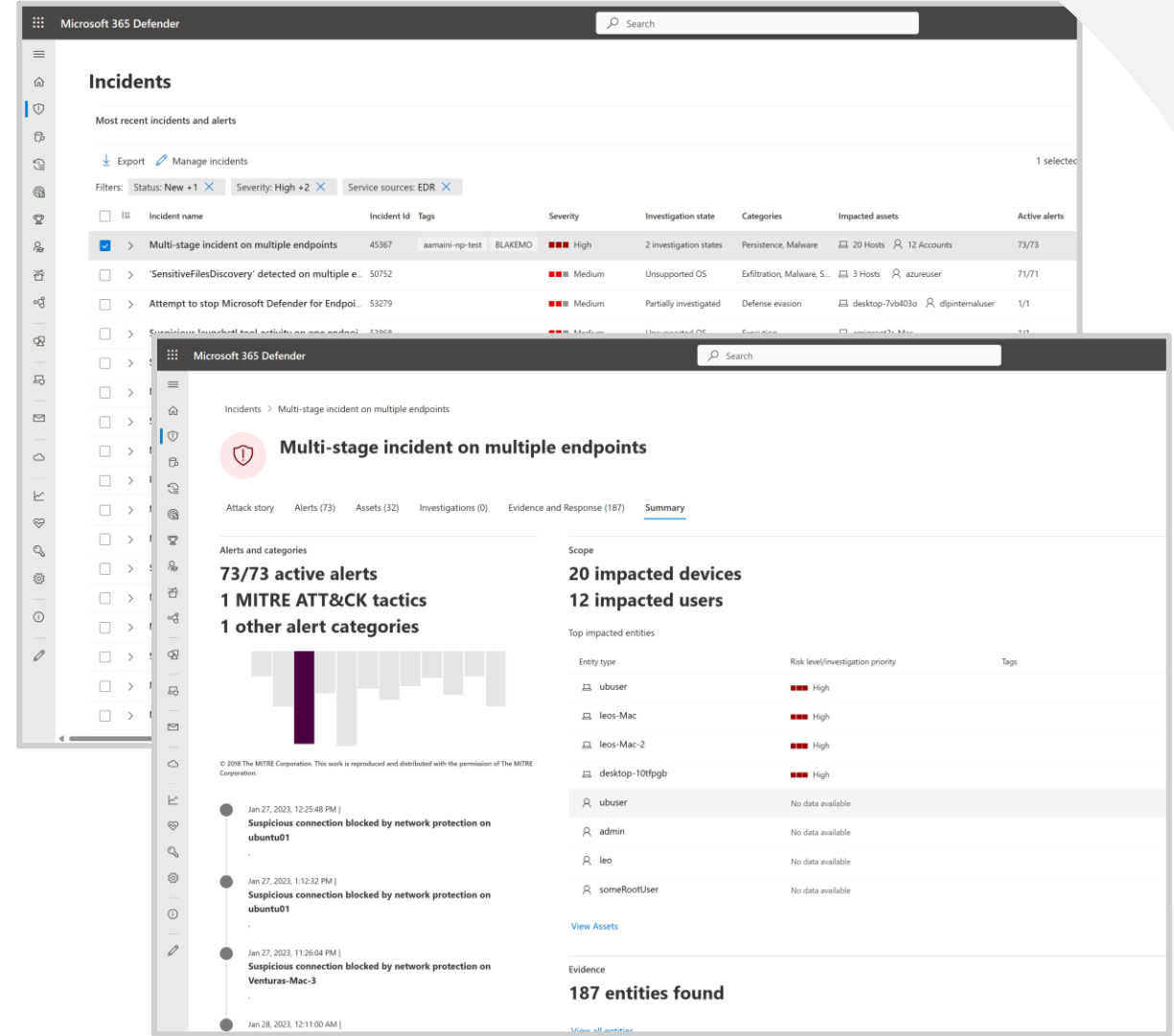
The broader attack story is better described when relevant alerts and related entities are brought together

## Incident scope

Analysts receive better perspective on the purview of complex threats containing multiple entities

## Higher fidelity, lower noise

Effectively reduces the load and effort required to investigate and respond to attacks



Read the [blog](#) for more details



# Advanced hunting with custom detection and custom response

The screenshot displays the Microsoft 365 Defender Advanced Hunting interface. The left sidebar shows the 'Schema' tree with categories like 'AlertEvents', 'MachineInfo', and 'NetworkCommunicationEvents'. The main area is titled 'Advanced hunting' and shows a custom KQL query for 'PowerShell downloads'. The query is as follows:

```
1 // Finds PowerShell execution events that could involve a download.
2 ProcessCreationEvents
3 | where EventTime > ago(7d)
4 | where FileName in ("powershell.exe", "POWERSHELL.EXE", "powershell_ise.exe", "POWERSHELL_ISE.EXE")
5 | where ProcessCommandLine has "Net.WebClient"
6 |   or ProcessCommandLine has "DownloadFile"
7 |   or ProcessCommandLine has "Invoke-WebRequest"
8 |   or ProcessCommandLine has "Invoke-Shellcode"
9 |   or ProcessCommandLine contains "http:"
10 | project EventTime, ComputerName, InitiatingProcessFileName, FileName, ProcessCommandLine
11 | top 100 by EventTime
```

The results table shows the following data:

EventTime	ComputerName	InitiatingProcessFileName	FileName
12/2/2019 12:02:32 PM	msticex-srv.msticex.net	cmd.exe	powershell.exe
12/2/2019 12:01:32 PM	msticex-srv.msticex.net	cmd.exe	powershell.exe
12/2/2019 12:01:32 PM	msticex-srv.msticex.net	cmd.exe	powershell.exe
12/2/2019 12:01:31 PM	msticex-srv.msticex.net	cmd.exe	powershell.exe
12/2/2019 2:51:10 AM	tk5-3wp03r0809.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe
12/2/2019 2:47:26 AM	tk5-3wp03r0813.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe
12/1/2019 19:26:27 PM	tk5-3wp03r0801.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe
12/1/2019 18:35:42 PM	tk5-3wp03r0801.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe
12/1/2019 18:35:42 PM	tk5-3wp03r0809.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe
12/1/2019 18:35:42 PM	tk5-3wp03r0813.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe
12/1/2019 18:35:41 PM	tk5-3wp03r0823.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe

The right sidebar contains filters for 'ComputerName', 'InitiatingProcessFileName', 'FileName', and 'ProcessCommandLine'. The 'ComputerName' filter shows a list of hosts, and the 'InitiatingProcessFileName' filter shows 'cmd.exe' as the most common initiator.



# 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)

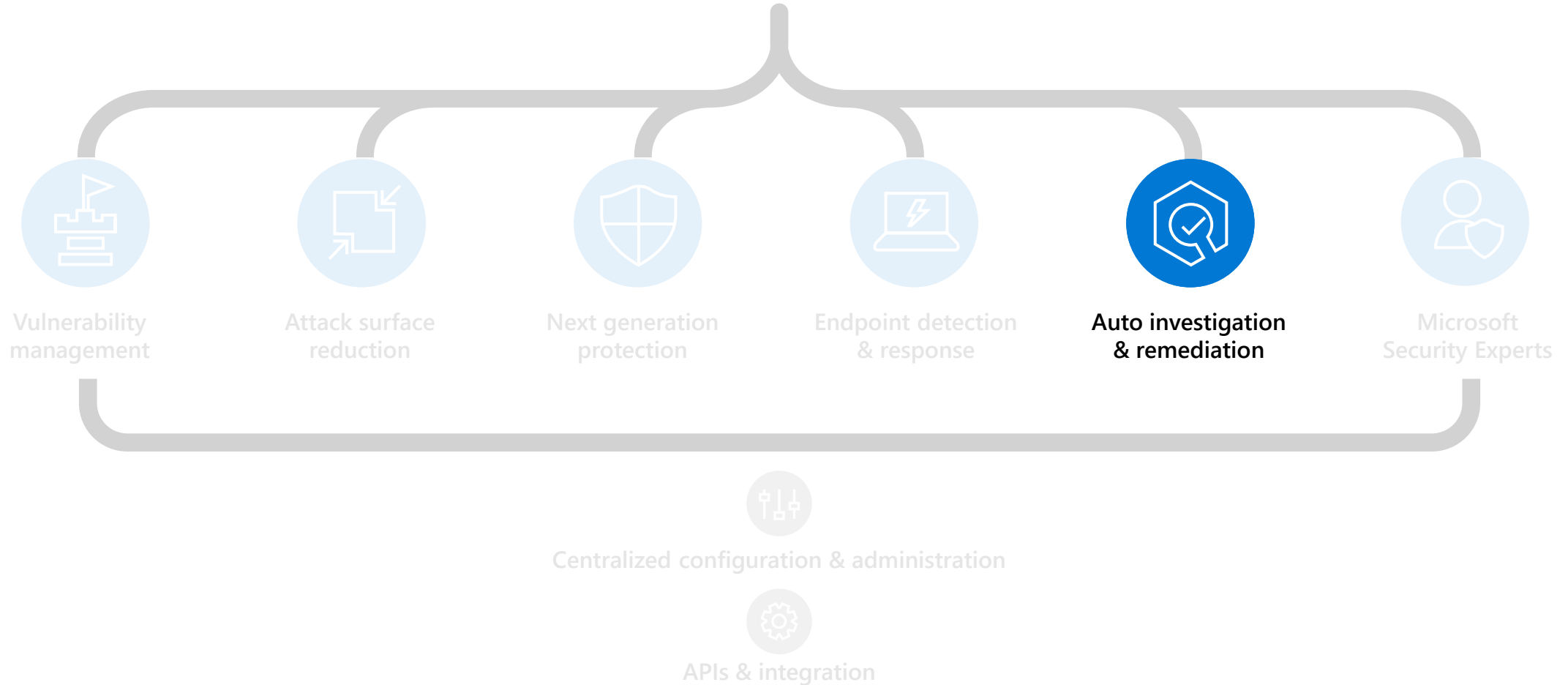






# Microsoft Defender for Endpoint

**Threats are no match.**





# What is 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

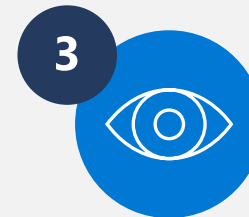
When we look at the steps an analyst is taking as when investigating and remediating threats we can identify the following high-level steps:



Determining whether the threat requires action



Performing necessary remediation actions



Deciding what additional investigations should be next



Repeating this as many times as necessary for every alert



# Auto investigation & remediation

Automatically investigates alerts and remediates complex threats in minutes



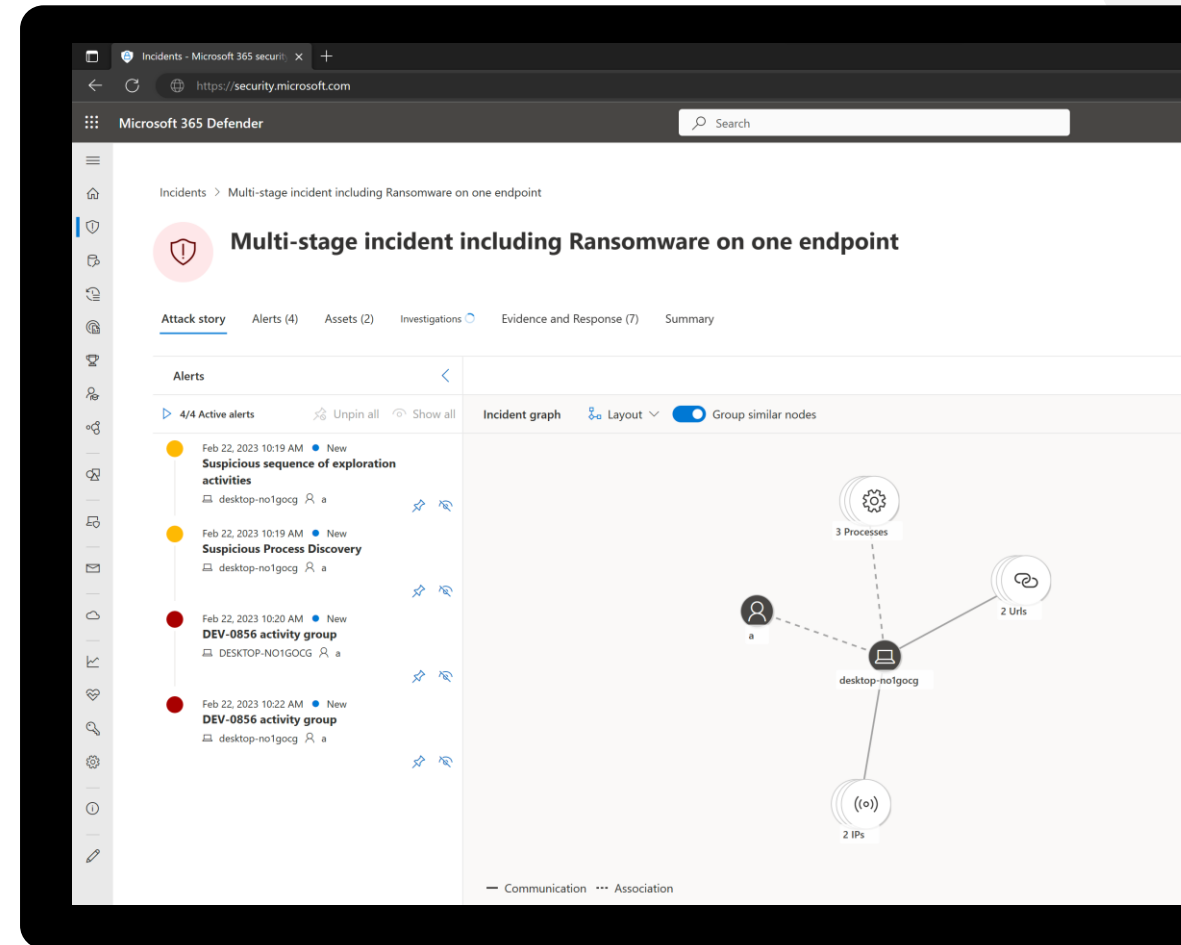
Mimics the ideal steps analysts would take



Tackles file or memory-based attacks



Works 24x7, with unlimited capacity





# Auto investigation queue

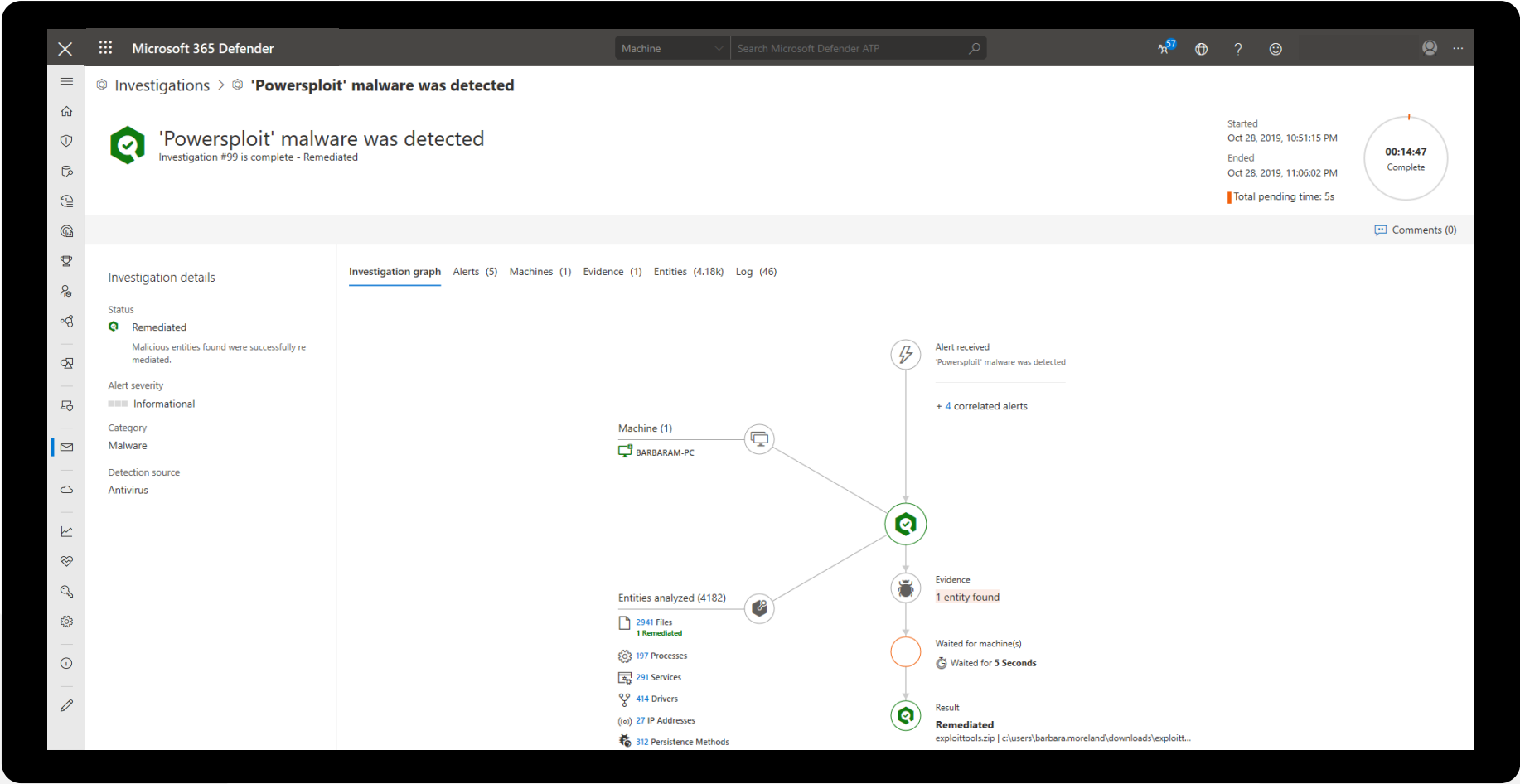
The screenshot displays the Microsoft 365 Defender interface, specifically the 'Automated Investigations' section. The page shows a list of investigation events with columns for Triggering alert, ID, Status, Detection Source, Entities, Start Date, and Duration. The status of each investigation is indicated by a green checkmark (Remediated), a green circle with a checkmark (Partially remediated), or a grey circle with a checkmark (No threats found). The detection source is listed as Antivirus, OfficeATP, AutomatedInvestigation, or EDR. The entities are listed as various PC names (e.g., barbaram-pc.mtpdemos.net, robertot-pc.mtpdemos.net, andrewf-pc.mtpdemos.net, gaile-pc.mtpdemos.net, aarifs-pc). The start date and duration are also provided for each investigation.

Triggering alert	ID	Status	Detection Source	Entities	Start Date	Duration
'Powersploit' malware was detected	99	Remediated	Antivirus	barbaram-pc.mtpdemos.net	10/28/19, 10:51 PM	14:47m
Office ATP Alert - Suspicious file found based on an Office ATP alert	98	Remediated	OfficeATP	barbaram-pc.mtpdemos.net	10/26/19, 2:05 AM	15:40m
Automated investigation started manually	94	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/23/19, 6:10 PM	13:33m
Automated investigation started manually	93	Partially investigated	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/23/19, 5:41 PM	1:14h
Automated investigation started manually	92	No threats found	AutomatedInvestigation	andrewf-pc.mtpdemos.net	10/21/19, 4:07 PM	21:55m
Hacktool Mimikatz detected	91	Remediated	EDR	barbaram-pc.mtpdemos.net	10/19/19, 8:31 AM	1:29h
Hacktool Mimikatz detected	90	Remediated	EDR	barbaram-pc.mtpdemos.net	10/18/19, 10:32 PM	1:32h
'AutoKMS' unwanted software was detected	89	Partially remediated	Antivirus	andrewf-pc.mtpdemos.net	10/18/19, 9:48 PM	1:07h
Office ATP Alert - Suspicious file found based on an Office ATP alert	88	Remediated	OfficeATP	barbaram-pc.mtpdemos.net	10/18/19, 9:06 PM	16:25m
Automated investigation started manually	85	No threats found	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/17/19, 4:01 AM	42h
Automated investigation started manually	84	No threats found	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/16/19, 5:50 PM	2d
Automated investigation started manually	83	Terminated by system	AutomatedInvestigation	aarifs-pc	10/16/19, 10:02 AM	3d
Automated investigation started manually	80	No threats found	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/11/19, 3:33 PM	4:55h
Automated investigation started manually	77	Terminated by system	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/10/19, 3:29 PM	3d
Automated investigation started manually	75	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/10/19, 2:50 PM	13:12m
'WmiRegBasedCommand' malware was detected	73	No threats found	Antivirus	barbaram-pc.mtpdemos.net	10/5/19, 7:16 AM	7:32m

The interface includes a sidebar with navigation icons, a top bar with search and settings, and a right-hand panel with filters for Status, Triggering alert, Detection Source, and Entities. The status filter is currently set to 'Any', showing 7 items. The triggering alert filter is also set to 'Any', showing 9 items. The detection source filter is set to 'Any', showing 9 items. The entities filter is set to 'Any', showing 1 item.



# Investigation graph

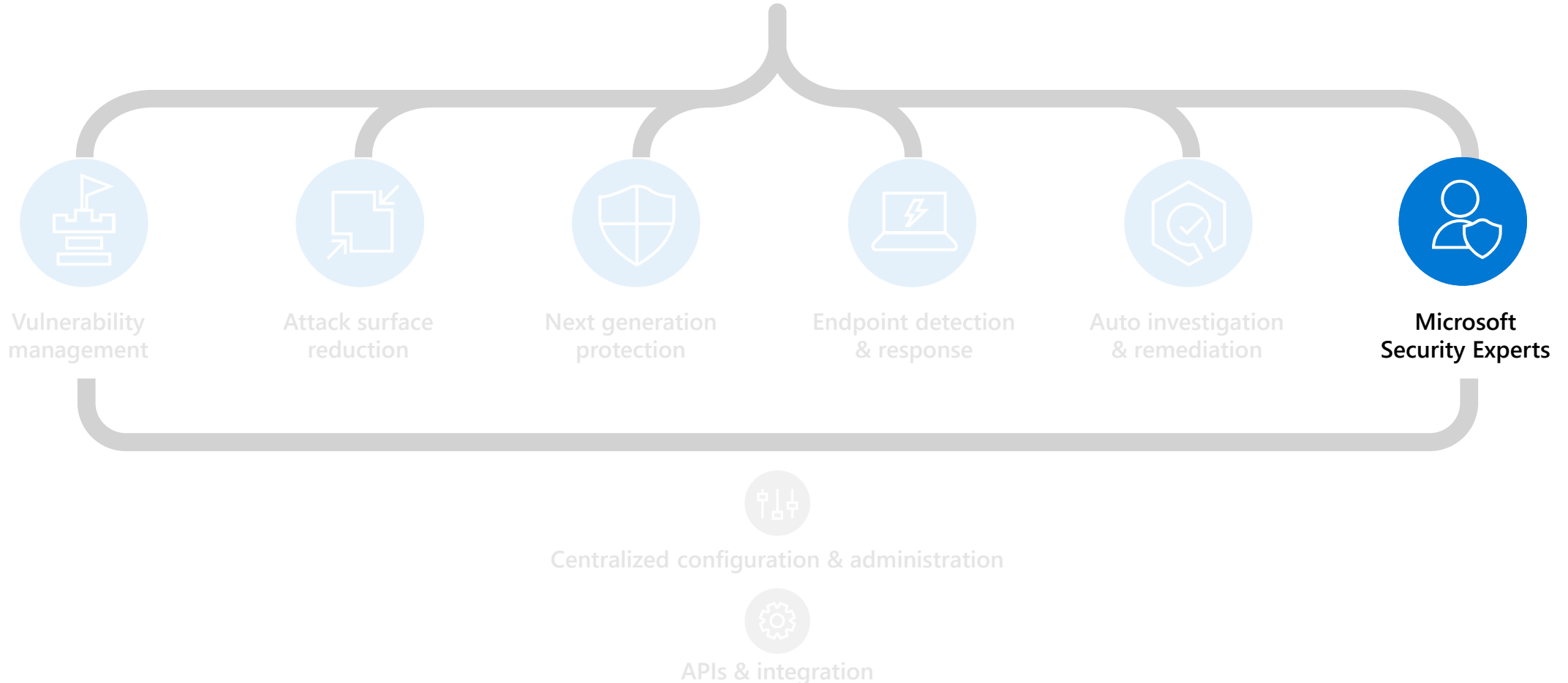






# Microsoft Defender for Endpoint

**Threats are no match.**

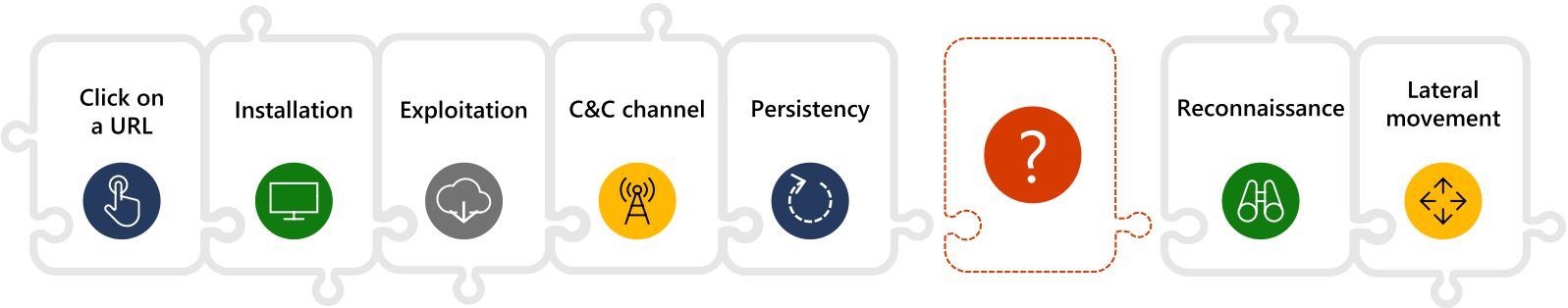




# Key customer pain points



As threats are becoming complex, I need additional context and guidance on alert handling



Need for additional threat context



No threat expert to contact when needed



Missing guidance on alert handling



Important alerts might get missed



Does this alert or event really matter to my org?



# Microsoft Security Experts

Bring deep knowledge and proactive threat hunting to your SOC



Expert level threat monitoring and analysis



Environment-specific context via alerts



Direct access to world-class hunters

The screenshot displays the Microsoft Defender Security Center interface. The main alert is titled "Detection of file linked to adversary with supply chain attacks" and is categorized as "High" severity. The alert is linked to an incident (54693) and is part of a supply chain attack. The alert context shows the affected machine as "desktop-c7ud4th" and the user as "jane.doe". The alert was first and last active on 9/10/2019 at 23:43:38.

**Description**

**Executive summary**

This alert provides additional context for an alert you have received. Windows Defender AV detected 'Winnti' high-severity malware. We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action [here](#). While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

**Timeline of observed events**

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

**Impacted machines**

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f1508b76e9a22	Impacted machine 1

**Recommended actions**

**Recommendation summary**

1. Fully investigate the machine in question.
2. Practice the principle of least-privilege and maintain credential hygiene. Restricting local administrative privileges can help limit installation of malware.
3. Enforce strong, randomized local administrator passwords. Use to restrict local administrative privileges.
4. If you have any questions about this alert, you can ask through E-mail or the Microsoft Security community.
5. Consult a threat expert.
6. If you need immediate help from Microsoft Incident Response contact your Microsoft Incident Response team.
6. Examine the Indicators of Compromise (IOCs) in the table below.

**Indicators of Compromise**

IOC	Type
Install (2).exe <a href="#">[explore]</a>	filename
InstallConfig.exe <a href="#">[explore]</a>	filename
InstallLauncher.exe <a href="#">[explore]</a>	filename
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 <a href="#">[explore]</a>	hash
ab16cd1b09e5157791a563456a12659aae926901 <a href="#">[explore]</a>	hash
131.107.147.82 <a href="#">[explore]</a>	ip



# Microsoft Security Experts

An additional layer of oversight and analysis to help ensure that threats don't get missed

## Targeted attack notifications

### Threat hunters have your back

Microsoft Security Experts proactively hunt to spot anomalies or known malicious behavior in your unique environment

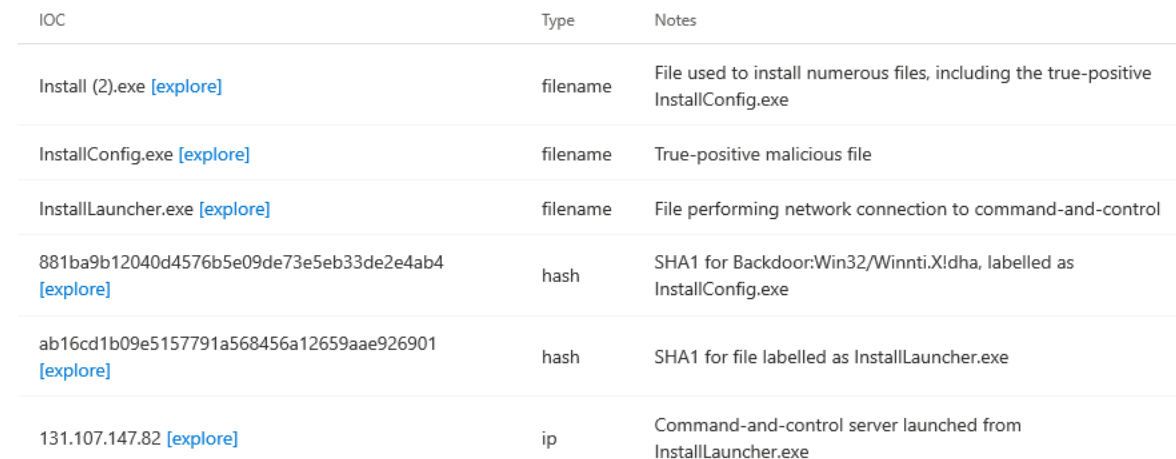
## Experts on demand

### World-class expertise at your fingertips

Got questions about alert, malware, or threat context? Ask a seasoned Microsoft Security Expert

The image displays two overlapping screenshots of the Microsoft Defender Security Center interface. The top screenshot shows an alert titled 'Detection of file linked to adversary with supply chain attacks'. It includes details such as severity (High), category (Execution), and detection source (Microsoft Threat Experts). The bottom screenshot shows a detailed view of a 'Software Supply Chain Attack' incident, including a dashboard with 10 active alerts, a timeline of events, and a list of impacted machines. The incident details section shows the attack was detected on July 3, 2018, at 9:26:18 AM, and is currently active. The timeline shows the attack was detected on July 3, 2018, at 9:26:18 AM, and is currently active. The impacted machines section shows the machine ID 7b7e23d4d69a.















Detection source: Microsoft Threat Experts

## Alert context

 janedoe

Last activity: 9.10.2019 | 23:43:38

## Executive summary

This alert provides additional context for an alert you have received, [Windows Defender AV detected 'Winnti' high-severity malware](#). We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action [here](#). While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

## Timeline of observed events

Network connection to IP address 131.107.147.82

## Impacted machines

Impacted machine 1

## Recommended actions

## Recommendation summary

1. Fully investigate the machine in question
2. Practice the principle of least-privilege and Restricting local administrative privileges
3. Enforce strong, randomized local admin
4. If you have any questions about this alert select 'Consult a threat expert'.
5. If you need immediate help from Microsoft
6. Examine the Indicators of Compromise (IoC) investigation.

## Indicators of Compromise

131.107.147.82 [\[explore\]](#)

## Microsoft Threat Experts - Trial

Your Experts on Demand trial version expires in 41 days from your Microsoft Threat Experts enrolment. Contact your Microsoft representative to get a full subscription.

Learn more about [Microsoft Threat Experts – Experts on Demand](#)



## Consult a threat expert

Get Microsoft Threat Experts advice and insights about suspicious activities in your organization.

Ensure that the portal page for the alert or machine in question is in view while providing information for this inquiry.

Note: This and other relevant information will be shared with Microsoft Threat Experts to enable the best response to your inquiry.

**Inquiry topic** 

[https://securitycenter.windows.com/alert/da637073841040265613\\_-882982118](https://securitycenter.windows.com/alert/da637073841040265613_-882982118)

Thank you for sending this Threat Expert alert. Can you help us investigate this threat further including whether you think we were targeted, and whether this and other machines in our company were compromised?

## Email ✉

Enter the email address you'd like Microsoft Threat Experts to send their reply

Analyst@contoso.com

Submit

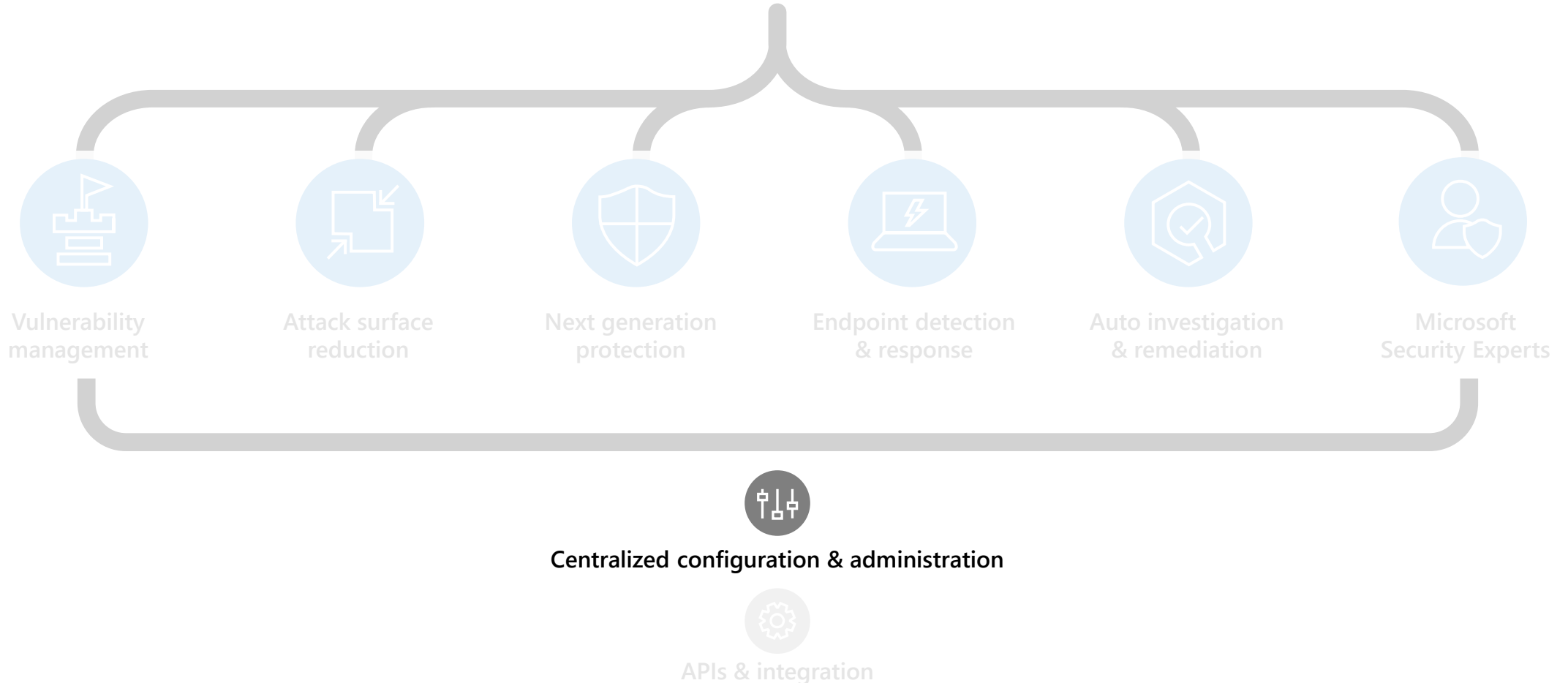
[Privacy statement.](#)





# Microsoft Defender for Endpoint

**Threats are no match.**





# Historical roles and friction



## Security Team

- Responsible for security monitoring and reducing risk
- Analyze threats, security incidents, exposure and identify mitigations
- Define security policies
- Priority is on quick remediation on impacted devices/users



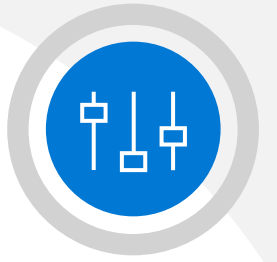
## IT Team

- Responsible for policy configuration including security policies
- Analyzes change impact and stages rollout of global policies
- Priority is a stable IT environment and low costs



# Security management

Assess, configure and respond to changes in your environment



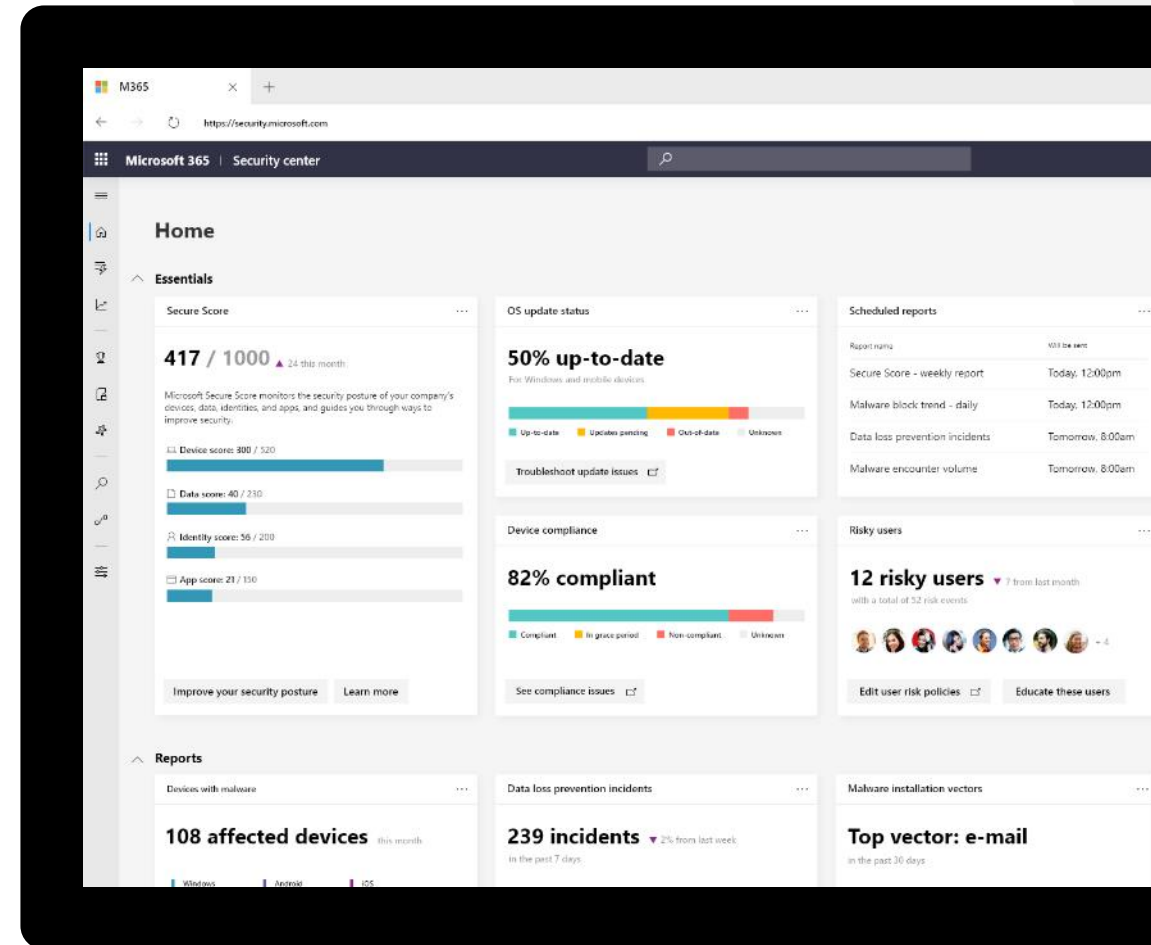
Centrally assess and configure your security



Variety of reports and dashboards for detailed monitoring and visibility



Seamless integration between policy assessment and policy enforcement





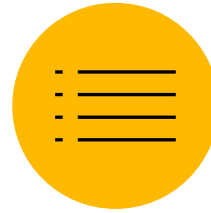
# Endpoint security management



Security baselines



All devices



Security tasks



Sec Admin experiences

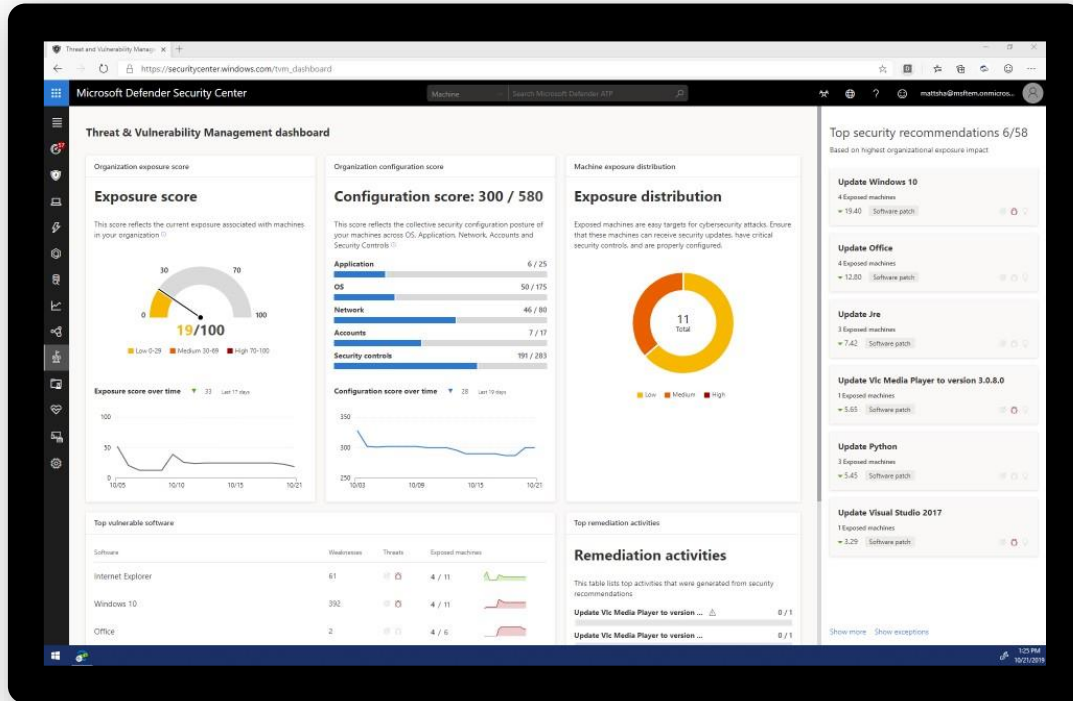


iOS

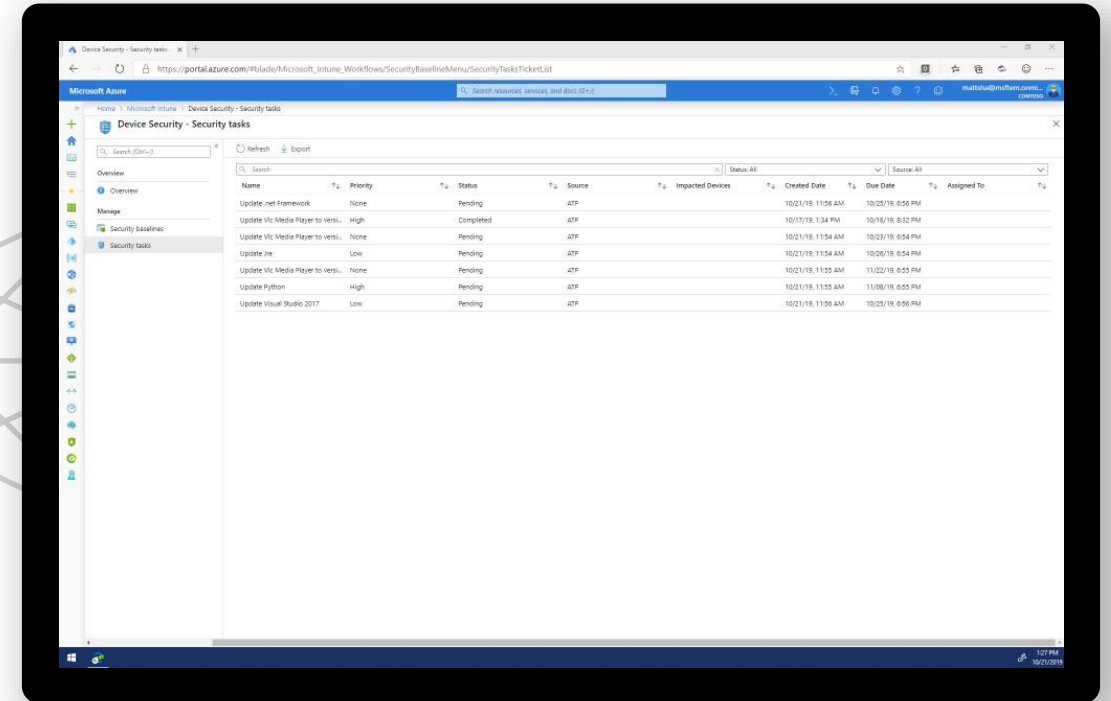
Target security policy to any device across Windows, Mac, Linux, Android, or iOS



# Seamless integration



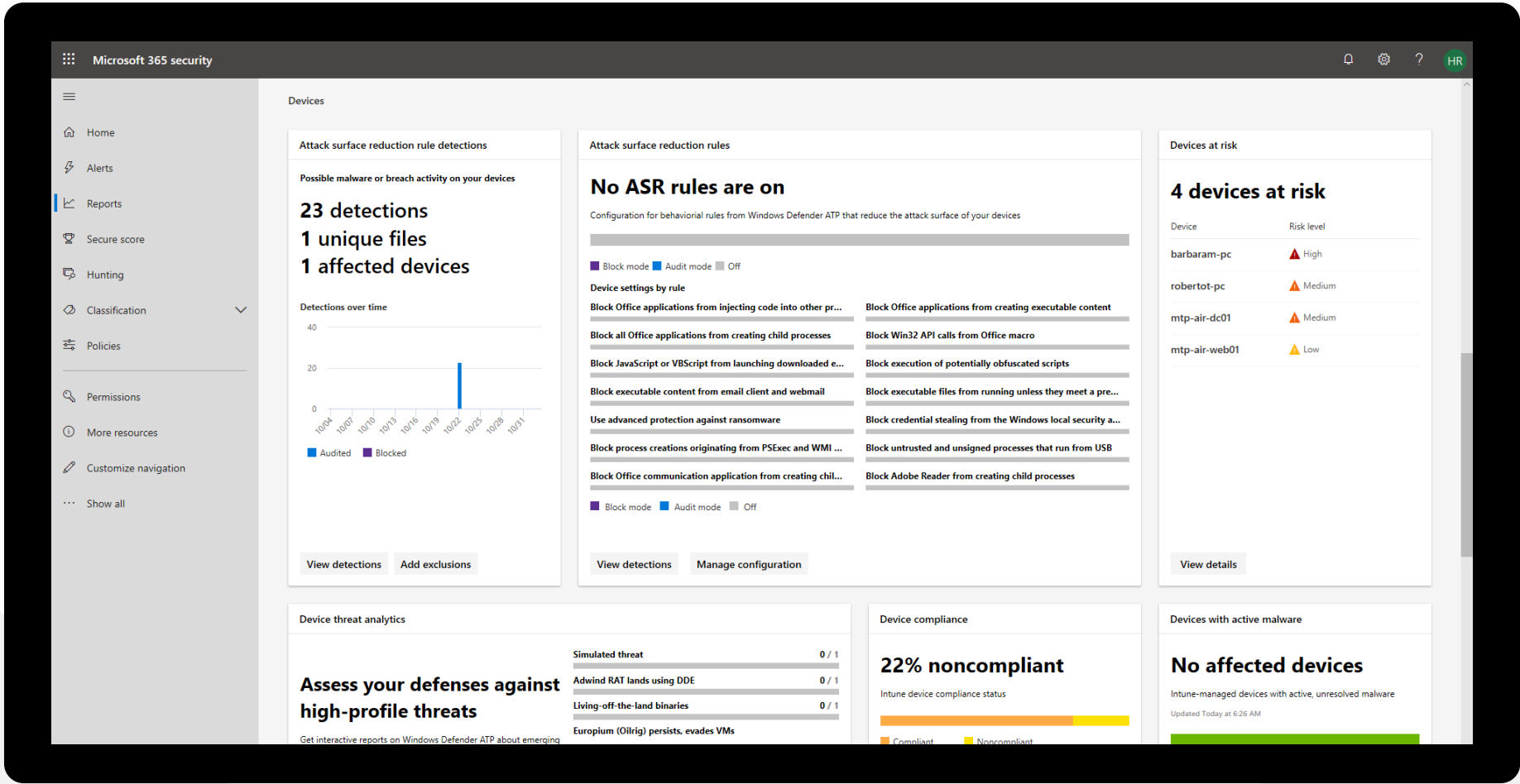
Microsoft Defender for Endpoint  
Policy assessment



Microsoft Intune  
Policy enforcement



# Get rich reporting in Microsoft Defender for Endpoint

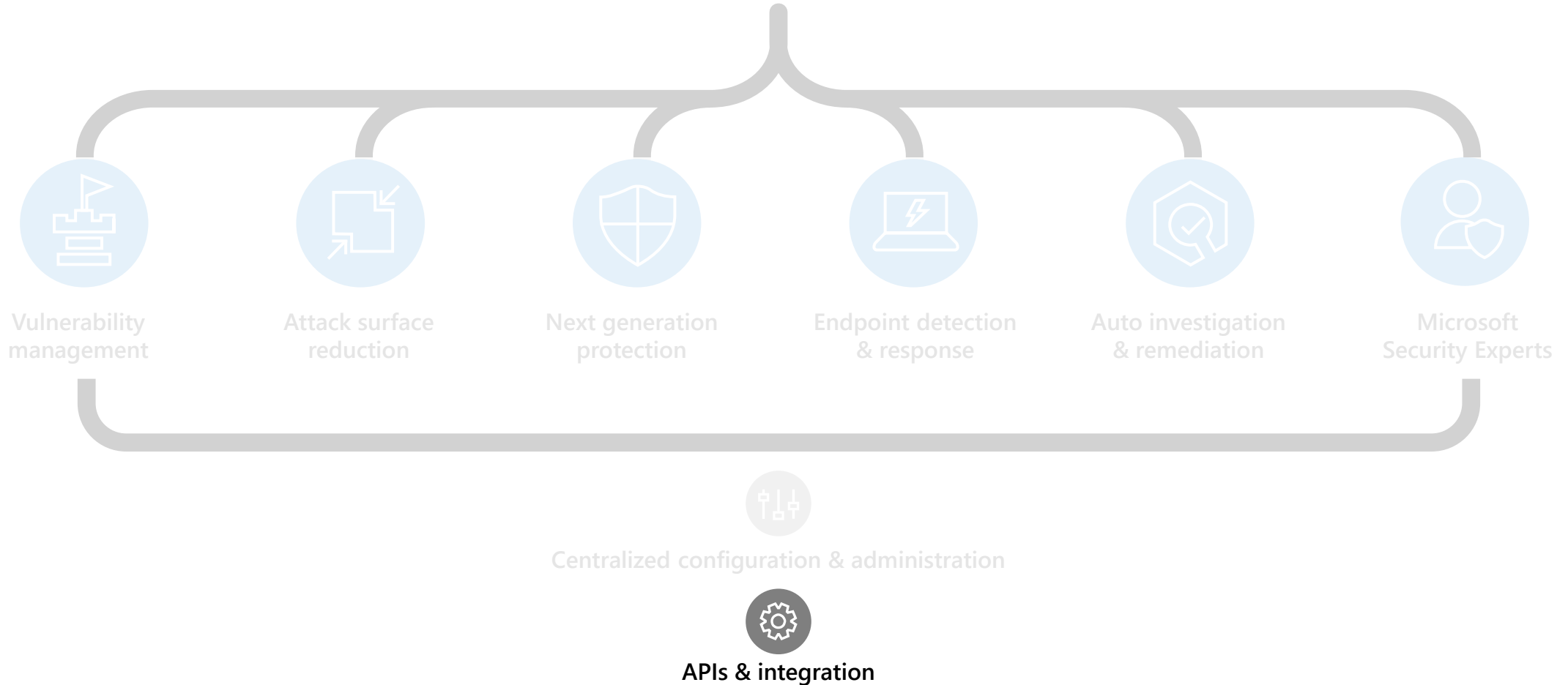






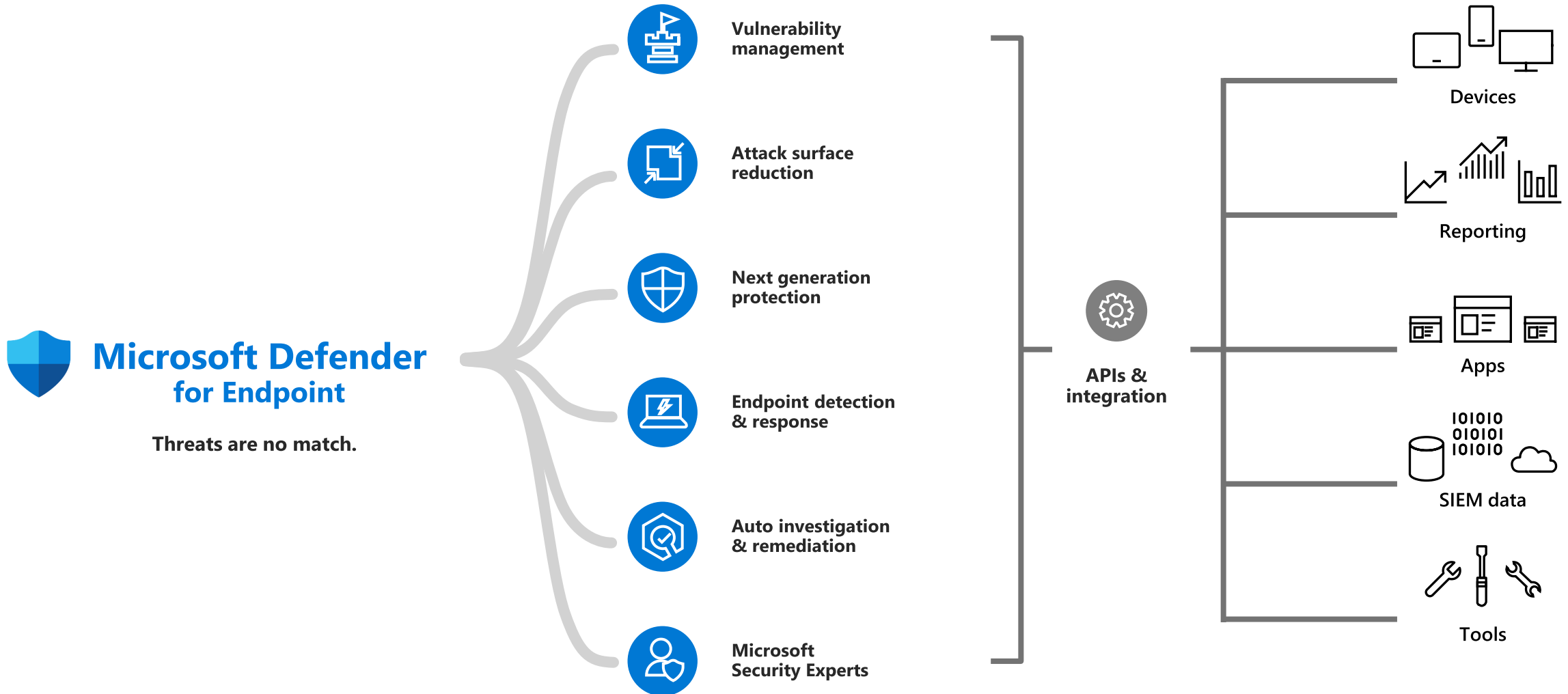
# Microsoft Defender for Endpoint

**Threats are no match.**



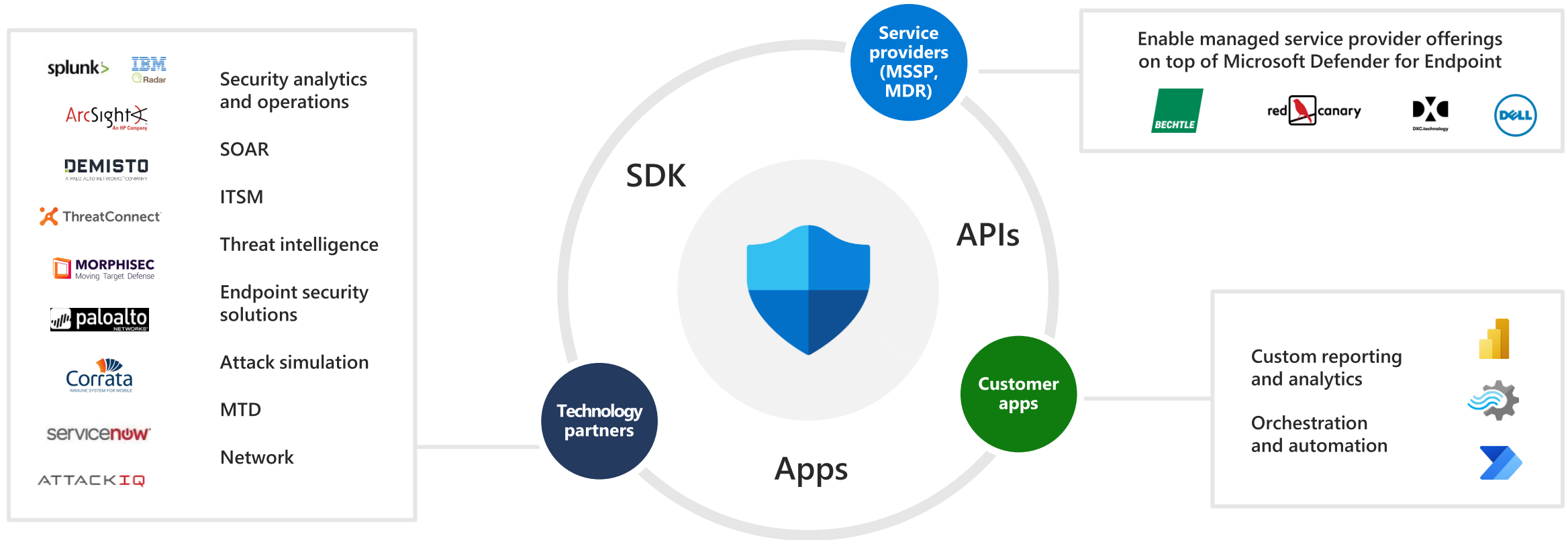


# Connecting with the platform





# Microsoft Defender for Endpoint through ecosystem and API



- + Query API
- + Streaming API
- + Actions API

- + Threat intel API, Vulnerability API
- + Application connectors (PBI, Flow, SNOW)
- + Microsoft Security Graph connector

- + AAD authentication and authorization
- + RBAC controls

- + Developer kit
- + Partner integration kit
- + Developer License



# Microsoft Defender Vulnerability Management and Defender for Endpoint feature matrix

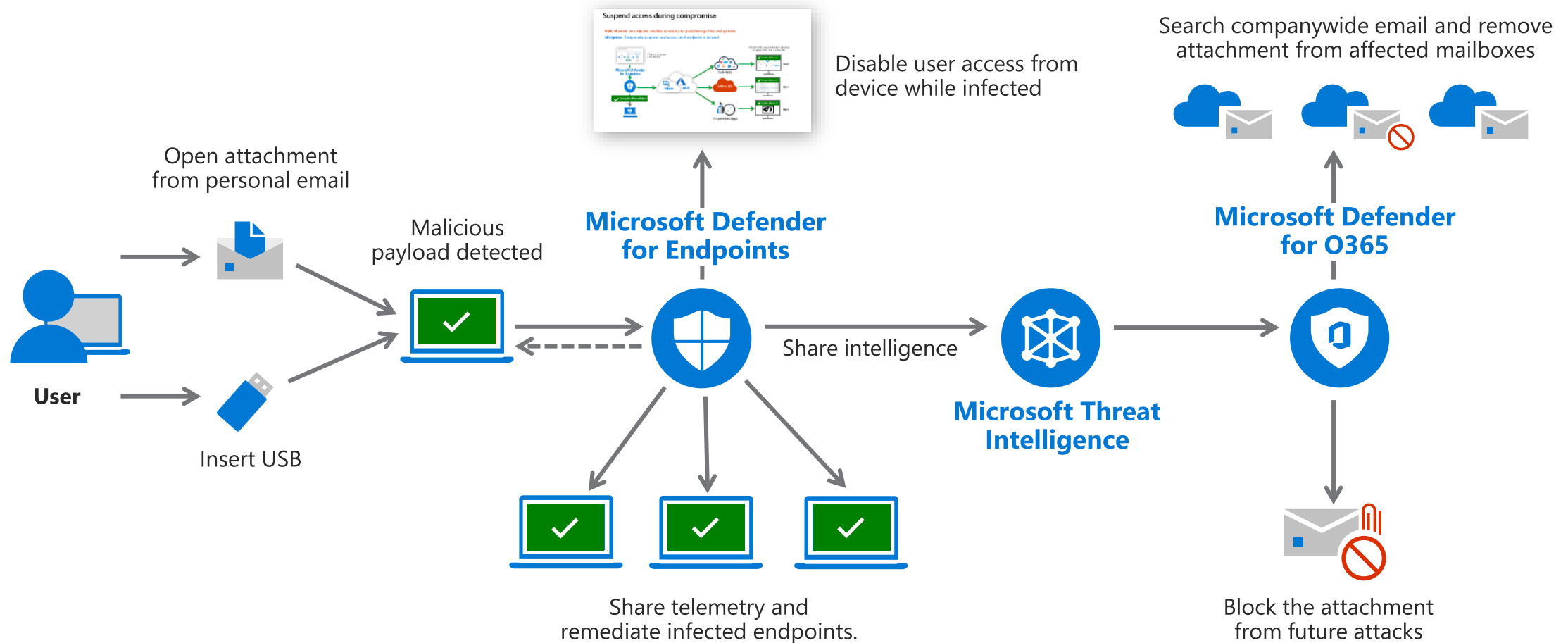
Feature		MDE P1	MDVM Standalone	MDE P2	MDE P2 + MDVM Add-On
Endpoint detection and response	Unified security tools & centralized management	●		●	●
	Next generation antimalware	●		●	●
	Attack surface reduction rules	●		●	●
	Device control	●		●	●
	Endpoint firewall	●		●	●
	Network protection	●		●	●
	Web control URL blocking	●		●	●
	Device-based conditional access	●		●	●
	Controlled folder access	●		●	●
	APIs, SIEM connector	●		●	●
	App control	●		●	●
	Endpoint detection & response			●	●
	Auto investigation & remediation			●	●
	Sandbox (deep analysis)			●	●
	Microsoft Threat Experts			●	●
	Threat analytics / Threat intelligence			●	●
	Device Discovery (unmanaged)		●	●	●
	Device inventory (managed)	●	●	●	●
Vulnerability management	Device inventory (network devices)		●	●	●
	Vulnerability assessment		●	●	●
	Configuration assessment		●	●	●
	Risk-based prioritization		●	●	●
	Remediation tracking		●	●	●
	Continuous monitoring		●	●	●
	Software apps vulnerability assessment		●	●	●
	Browser extensions assessment		●		●
	Digital certificates assessment		●		●
	Security baselines assessment		●		●
	Firmware and hardware assessment		●		●
	Authenticated scans for vulnerability assessment		●		●
	Block vulnerable applications		●		●
	Network share analysis		●		●



# Compromised endpoint

**Risk:** Devices can be infected by **personal email, USB, and other vectors**

**Mitigation:** Rapidly detect and clean all managed devices, email, and other resources across environment and customers

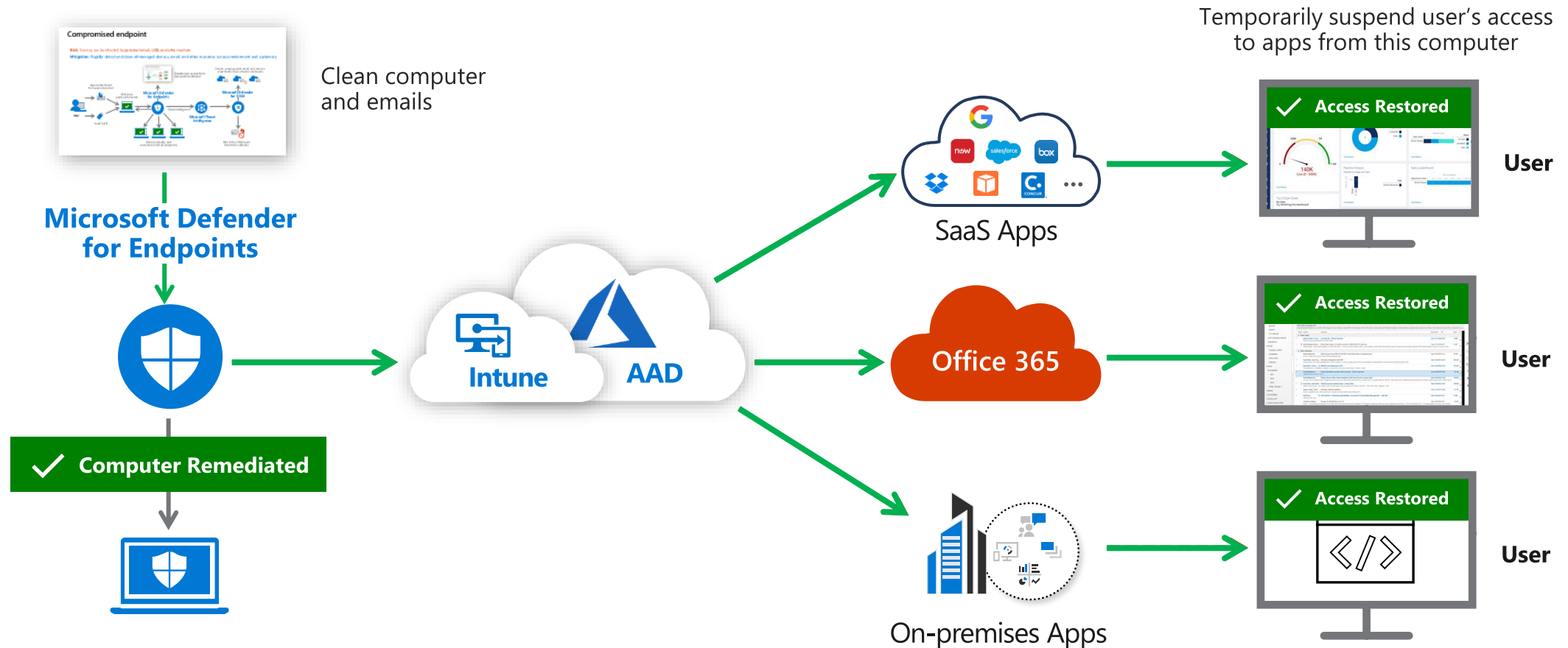




# Suspend access during compromise

**Risk:** Malware on endpoint enables adversary to steal/damage files and systems

**Mitigation:** Temporarily suspend user access until endpoint is cleaned





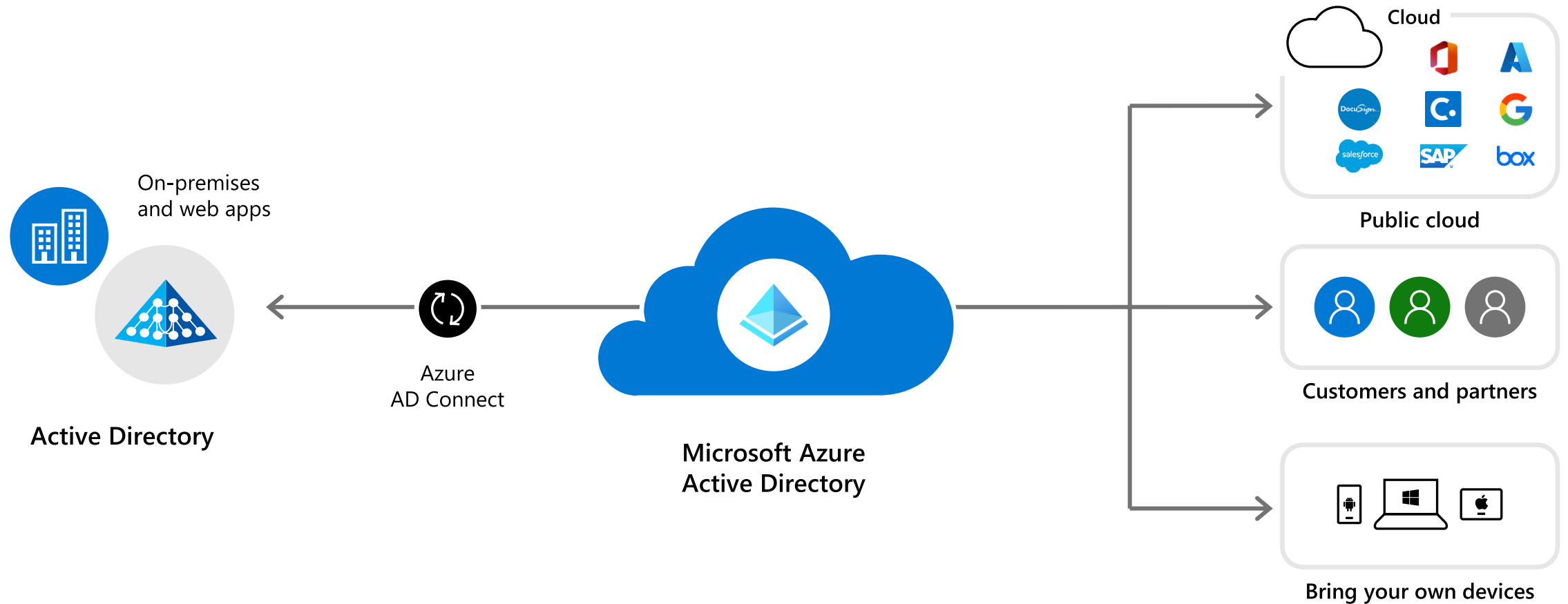
# Microsoft Defender for Identity





# The complexity of the enterprise identity security landscape

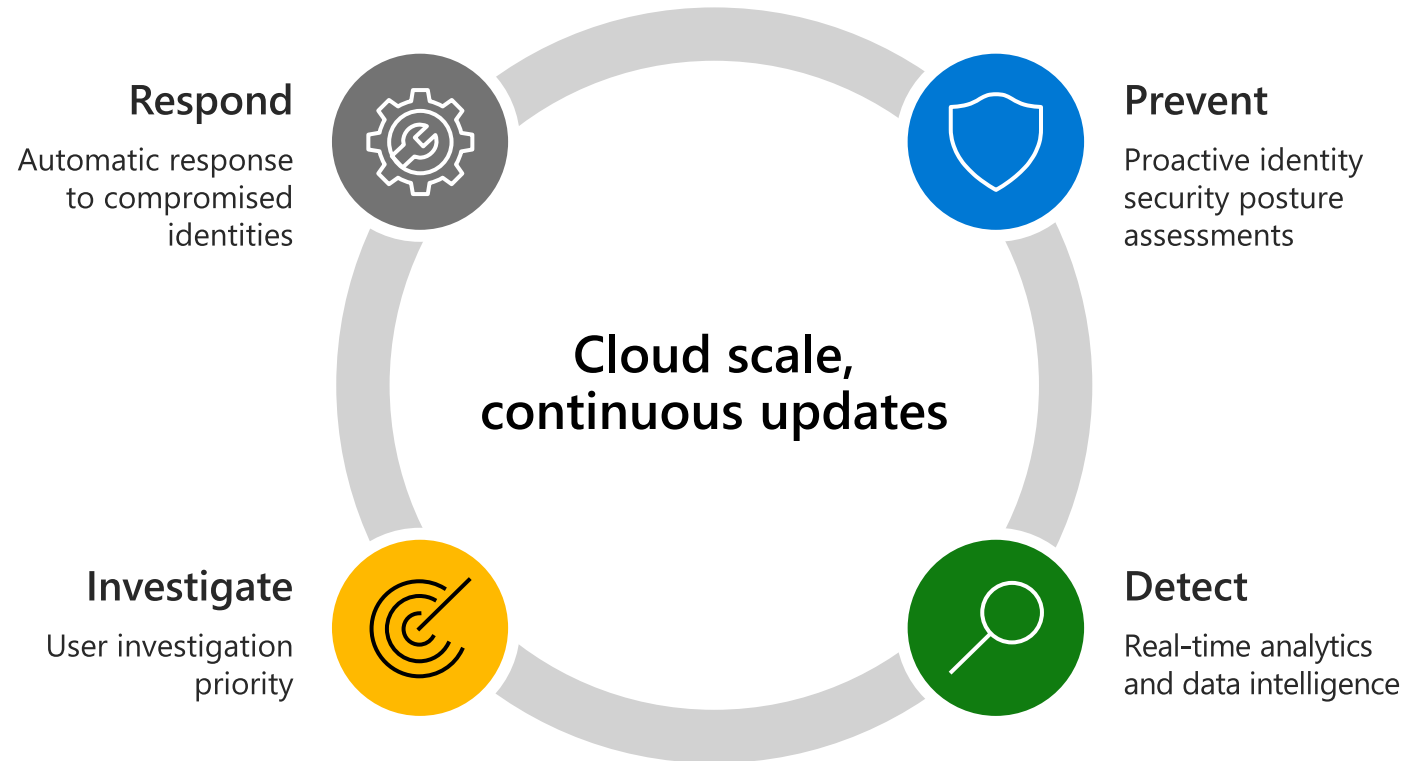
Enterprise security environments are complex—and include both on-premises and cloud assets





# Microsoft Defender for Identity for on-premises identity protection

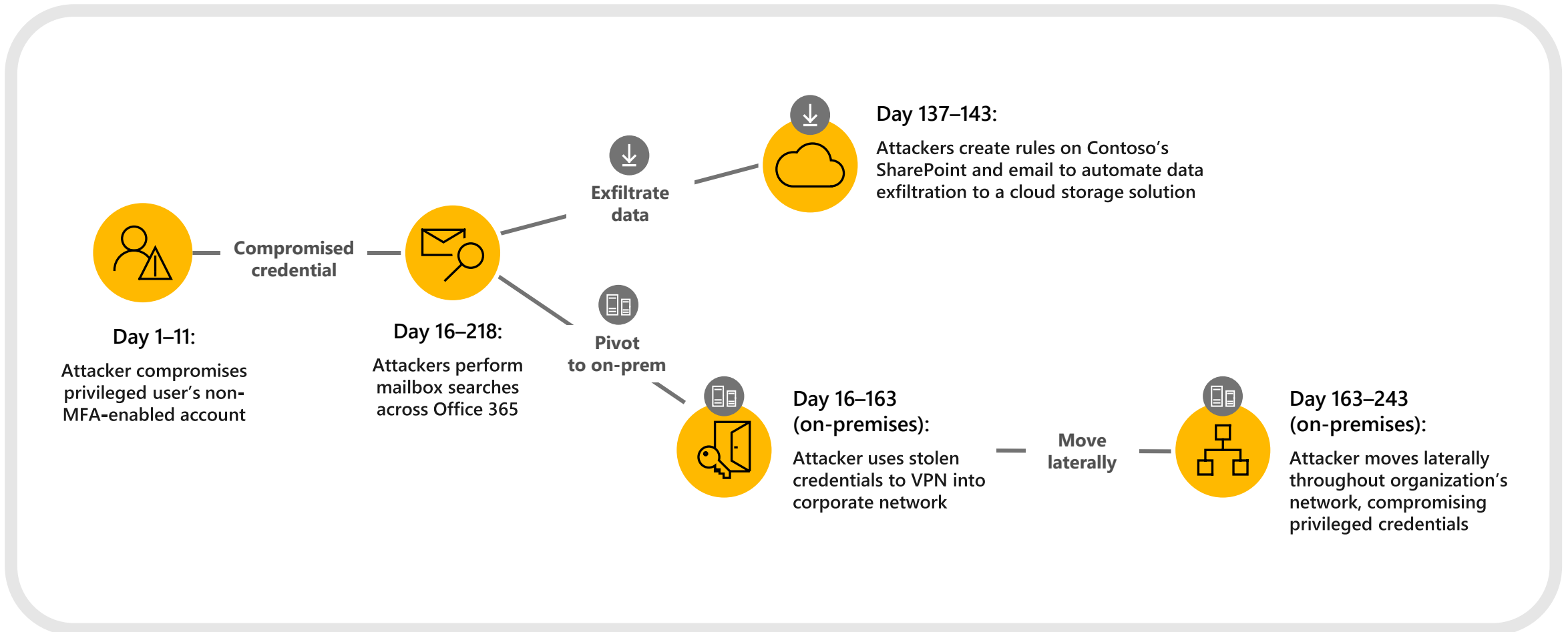
Microsoft Defender for Identity helps security operations teams protect user identity as part of on-premises and cloud enterprise environments





# Anatomy of an on-premises and cloud environment attack

One example of how an attack happens and compromises an entire organization





**Ist Ihr Unternehmen schon einmal von einem Cyberangriff  
betroffen gewesen ?**

**Ja**

**Nein**



# Identity security posture assessments

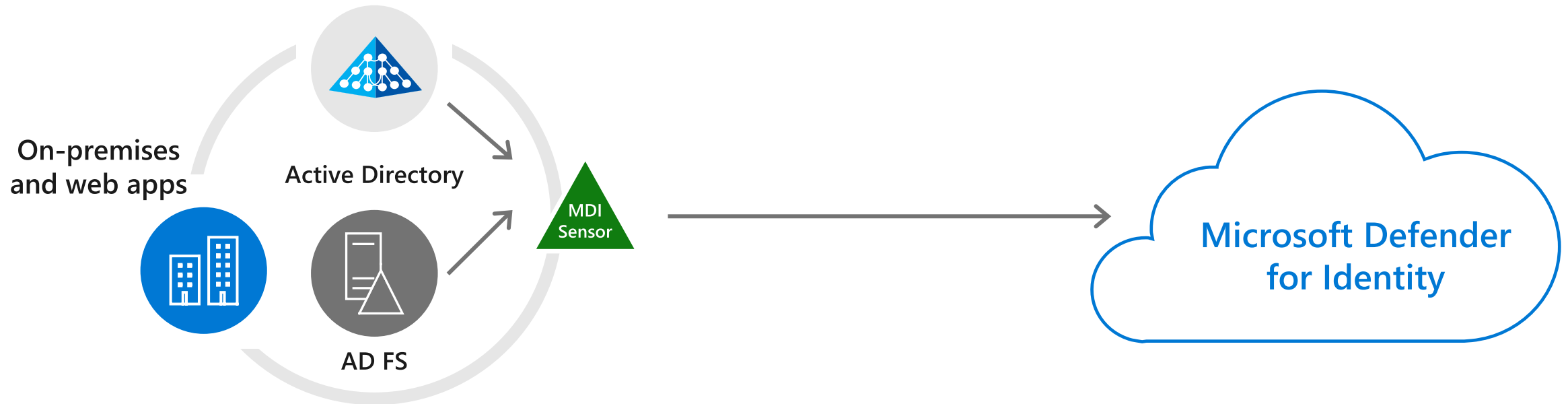
Gain visibility to potential identity risks to reduce the attack surface

- Entities exposing credentials in clear text
- Legacy protocols usage
- Weak cipher usage
- Unsecure Kerberos delegation
- Domain controllers with Print Spooler service available
- Dormant entities in sensitive groups
- Unmonitored domain controllers
- Microsoft LAPS usage
- Risky lateral movement paths
- Unsecure SID history attributes
- Unsecure account attributes





# Detections based on a rich host of data sources



## Network traffic analytics

Inspect network traffic: NTLM, Kerberos, LDAP, RPC, DNS, SMB

## Security events and Active Directory data

Inspect events, event tracing and profile active directory entities

## User behavior analytics

Profile users and entities behavior, identify behavior anomalies

## Cloud based real-time detections

Data enrichment and correlation in the cloud, for real time detections



# Reduce investigation time with Microsoft 365 Defender incidents

Summary Alerts (107) Devices (6) Users (10) Mailboxes (16) Investigations (18) Evidence and Response (311)									
1-30 of 57 < > Choose columns 30 items per page									
Title	Tags	Severity	Status	Linked by	Category	Impacted Entities	Service source	Detection sour...	
Suspicious behavior by Microsoft Word was observed	Demo Machine +2	Medium	New	7 reasons	Initial access	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
An Office application ran suspicious commands	Demo Machine +2	Medium	New	Same device	Initial access	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
Anomalous account lookups	Demo Machine +2	Low	New	Manual association	Discovery	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
User and IP address reconnaissance (SMB)									
Demo Machine +2		Medium	New	3 reasons					
Unexpected behavior observed by a process ran with no c...	Demo Machine +2	Medium	New	Same device	Execution	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
'Mikatz' high-severity malware was detected	Data sensitivity: High +4	High	Resolved	2 reasons	Malware	mtp-air-dc01.mtpdemos.net	Endpoint	Antivirus	
'Mimilove' high-severity malware was detected	Data sensitivity: High +4	High	Resolved	2 reasons	Malware	mtp-air-dc01.mtpdemos.net	Endpoint	Antivirus	
An active 'Mimikatz' hacktool was detected	Data sensitivity: High +4	Medium	New	3 reasons	Malware	mtp-air-dc01.mtpdemo...	Endpoint	Antivirus	
> 2 alerts: Suspected overpass-the-hash attack (Kerberos)									
Demo Machine +4		High	Multiple	7 reasons					
Successful login using overpass-the-hash with potentially ...	Data sensitivity: High +3	Medium	Resolved	4 reasons	Lateral movement	annetteh-pc.mtpdemo...	Endpoint	365 Defender	
Suspected identity theft (pass-the-ticket)									
Data sensitivity: High +3		High	In progre...	2 reasons					

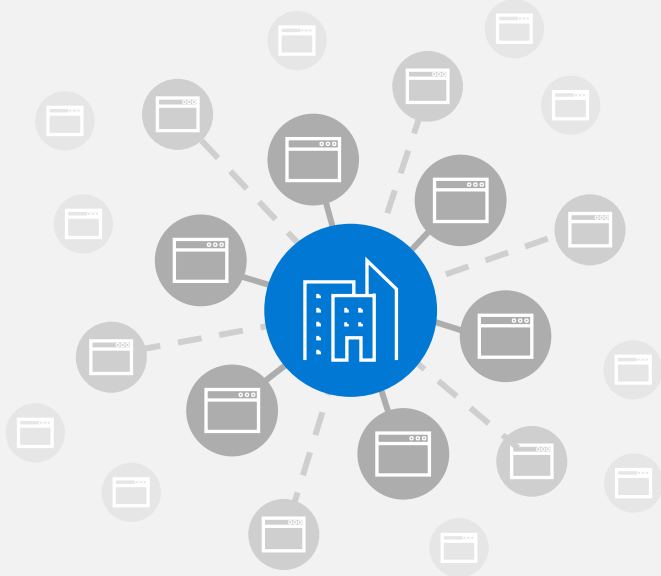


# Microsoft Defender for Cloud Apps

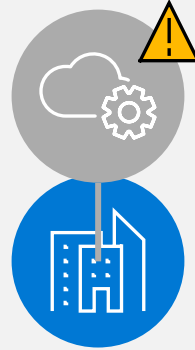




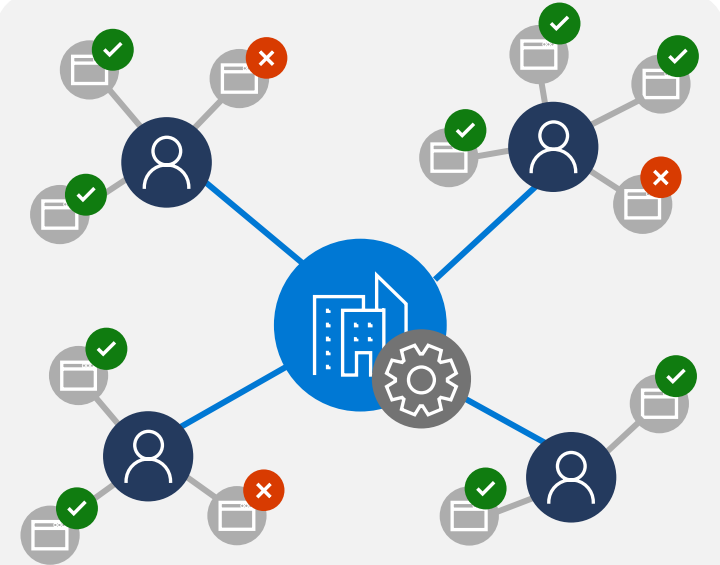
# Today's challenges:



The number of applications in an organization's environment is growing at a rapid rate making it harder for to gain visibility across the apps that are used in an IT organization, especially apps that pose high risk



SaaS app misconfigurations can lead to a potential breach and have emerged as a common attack vector



Organizations need a way to manage their apps and implement controls to ensure users are only accessing approved and safe apps



# SaaS Security @ Microsoft

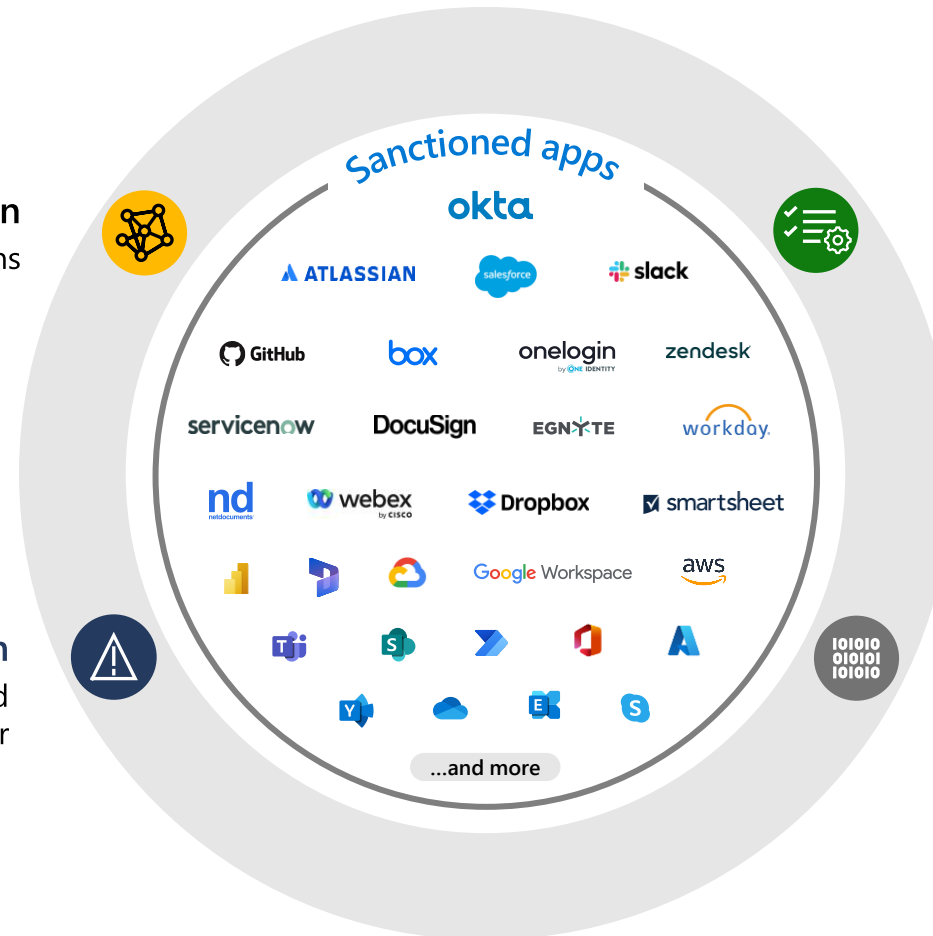


Discover SaaS applications



**App to app protection**  
Discover and remediate third-party integrations

**Continuous threat protection**  
Detect, investigate and respond to attacks with Microsoft 365 Defender



**SaaS security posture management (SSPM)**  
Misconfigurations | Best practices  
Remediate risky configurations

**Information protection:**  
Sensitive data exposure  
Governance file violation



# SaaS discovery and posture phases

Safely adopting SaaS apps

## Phase 1

*Discover and Identify*



### Discover Shadow IT

Identify which apps are being used in your organization from an app catalog of over 31,000 cloud apps and custom apps.



### Identify the risk levels of your apps

Understand the risk associated with discovered apps, based on more than 90 risk factors including, security factors, industry and legal regulations - with the ability to customize risk scoring.

## Phase 2

*Evaluate and Analyze*



### Evaluate compliance

Evaluate whether the discovered apps meet the compliance standards of your organization against factors like GDPR or HIPAA.



### Analyze usage

Understand the usage patterns based on traffic data, top users and IP addresses, app categories and devices.



### Govern your SaaS apps

Use governance actions such as sanction, unsanction, onboard to Azure AD for single sign-on (SSO), marking them for review or blocking them from your network.

## Phase 3

*Manage and Continuous monitoring*



### Assess security posture

Identify misconfigurations in your SaaS apps and take the recommended actions to ensure they follow best practices



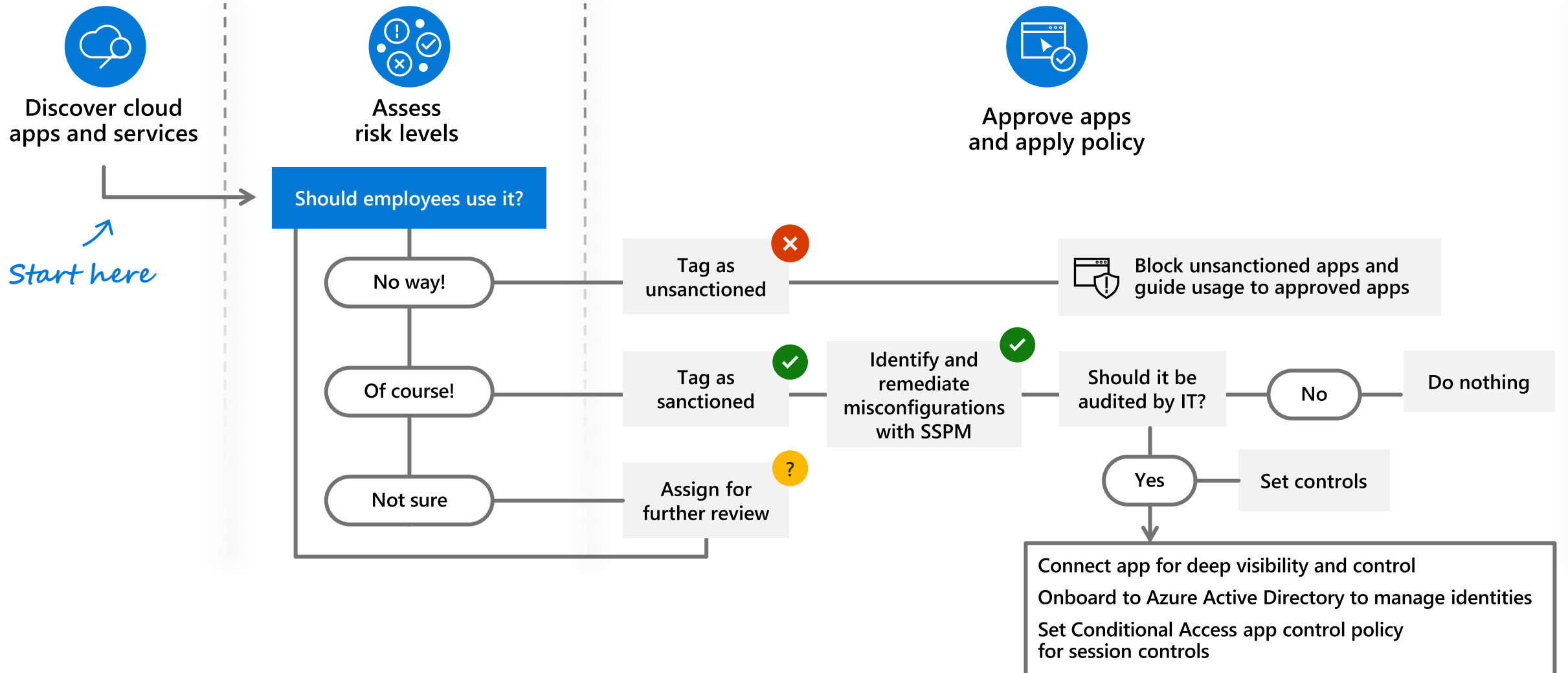
### Continuous monitoring

Be alerted when new, risky or high-volume apps are discovered in your environment for continuous monitoring and ongoing control.



# Discover and control apps in your environment

Take action: Manage newly discovered cloud app





# App Governance in Microsoft Defender for Cloud

Prevent and remediate inappropriate app behavior

Apps



Deep visibility and insights into app configuration and high-risk behaviors



Policy-driven governance for Azure-connected apps to meet security and compliance mandates for data access



Comprehensive machine learning based detection and remediation of unusual app activity



App Governance automatically shuts down apps determined to be malicious – integration with Microsoft 365 Defender





# Business email compromise (BEC) killchain

Microsoft Defender for Cloud Apps

Microsoft 365 Defender

Microsoft Defender for Office

	Initial access	Persistence	Defense evasion	Lateral movement	Exfiltration
Kenyetta Elsea (Kelsea)	<div>1. Phish</div> <div>Malicious phishing campaign was sent to the organization (Reported by user Jackson Hall)</div> <div></div>		<div>3. Hide artifacts</div> <div>Inbox manipulation rule set to hide internal phishing campaign</div> <div></div>	<div>4. Internal phish</div> <div>Phishing email is sent from Kenyetta's mailbox to his manager Oscar</div> <div></div>	
	<div>Email reported by user as malware of phish</div>		<div>Suspicious inbox manipulation rule</div>	<div>Activity from a TOR IP address</div>	
	<div>2. Compromise</div> <div>Kenyetta clicks on link and enters credentials</div> <div></div>		<div>Activity from a TOR IP address</div>		
	<div>Suspicious URL clicked</div> <div>Email message containing malicious URL removed after delivery</div> <div>User accessed a link in a ZAP-quarantined email</div>				
Oscar King (Oking)		<div>6. Email persistence</div> <div>Inbox forwarding rule is created in Oscar's account to forward all mails to an external account</div> <div></div>		<div>5. Lateral compromise</div> <div>Oscar clicks on link coming from a mail from Kenyetta and enters credentials</div> <div></div>	<div>7. OneDrive exfiltration</div> <div>The adversary downloads multiple files from Oscar's OneDrive account</div> <div></div>
		<div>Activity from a TOR IP address</div> <div>Creation of forward /redirect rule</div>		<div>User accessed a link in a ZAP-quarantined email</div>	<div>Activity from a TOR IP address</div> <div>Mass download</div>
		<div>Activity from infrequent country</div> <div>Suspicious inbox forwarding rule</div>			<div>Activity from a TOR IP address</div> <div>Suspicious massive data read</div>



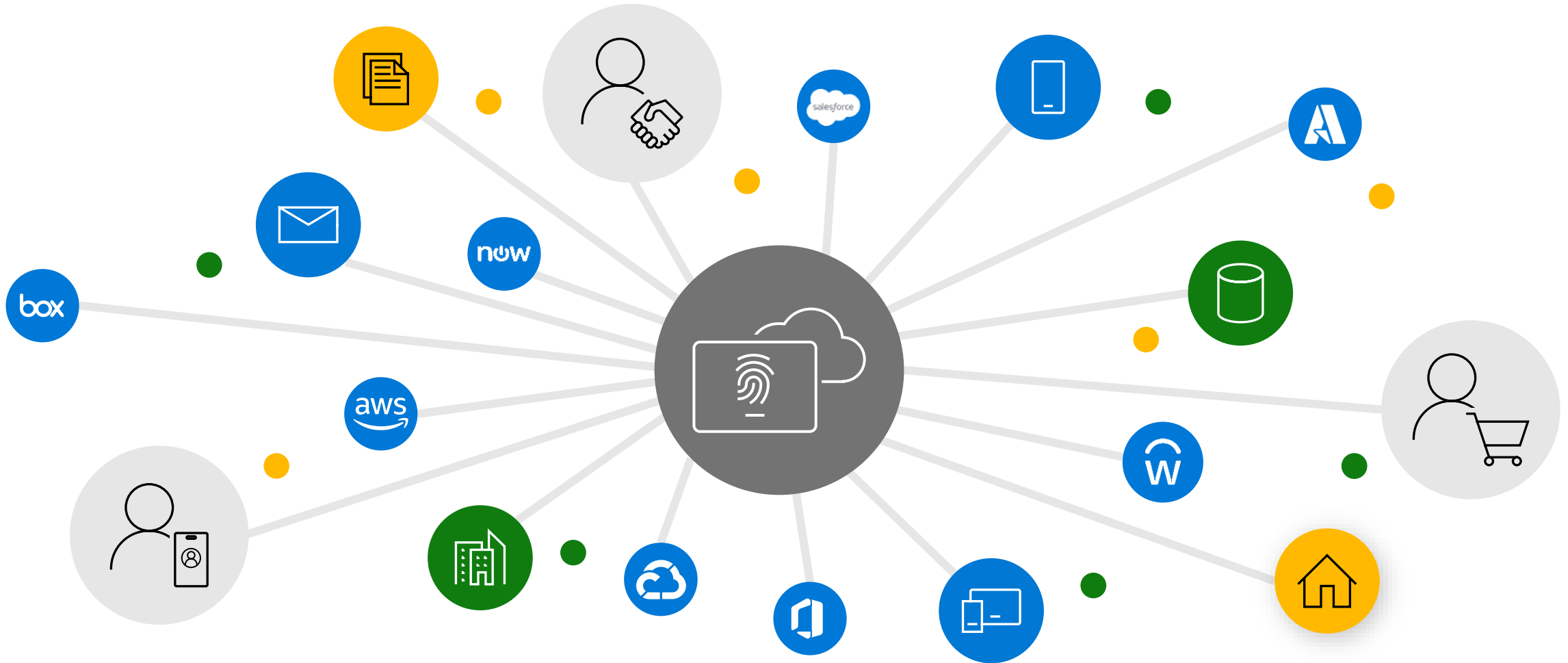
# Microsoft Identity Protection





# Identity is the control plane

Secure access for a connected world





# Azure Active Directory Identity Protection

Intelligently detect and respond to compromised accounts



Enhanced logging



Threat alerts



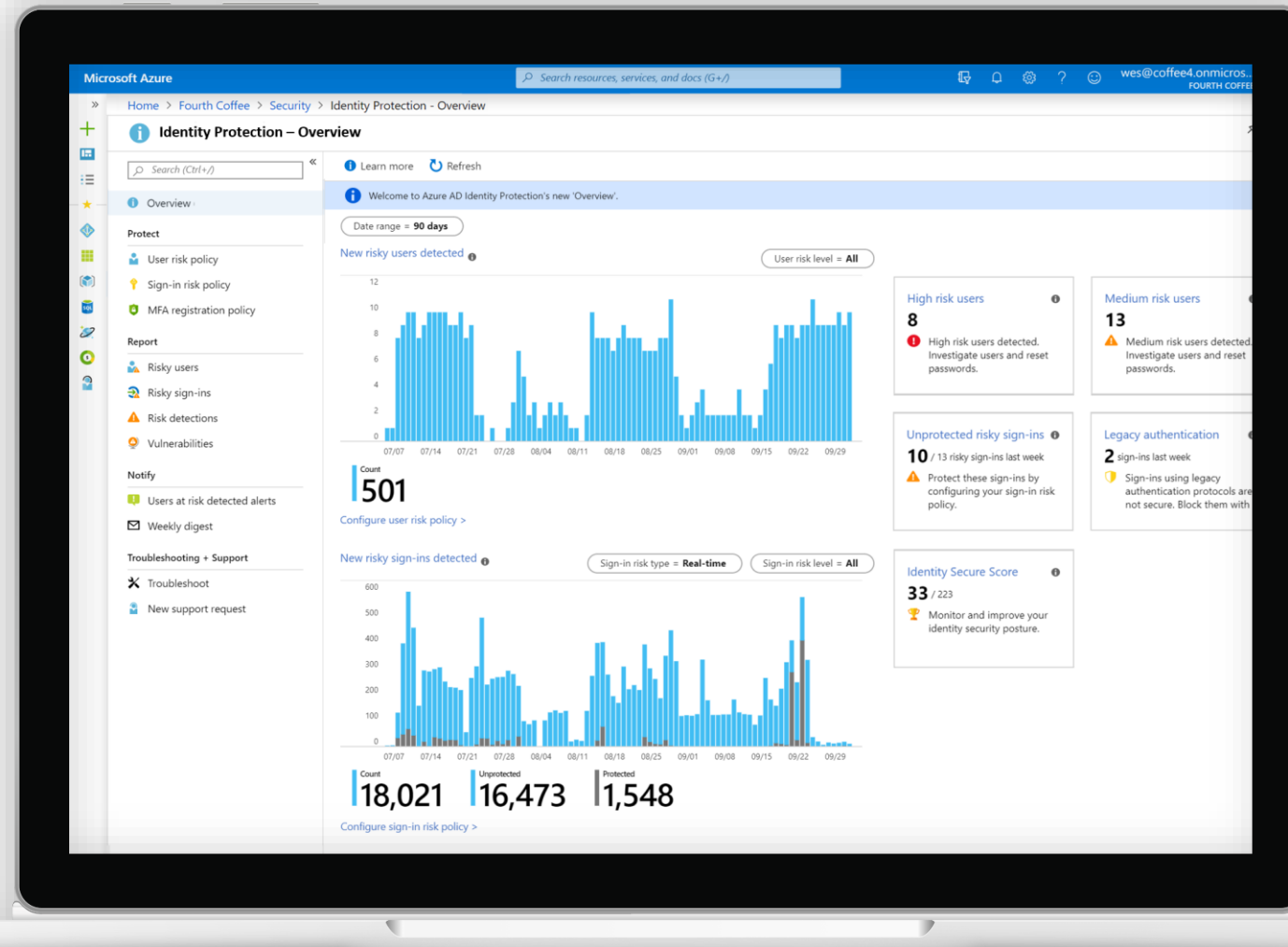
Risk scores



Sign-in reports



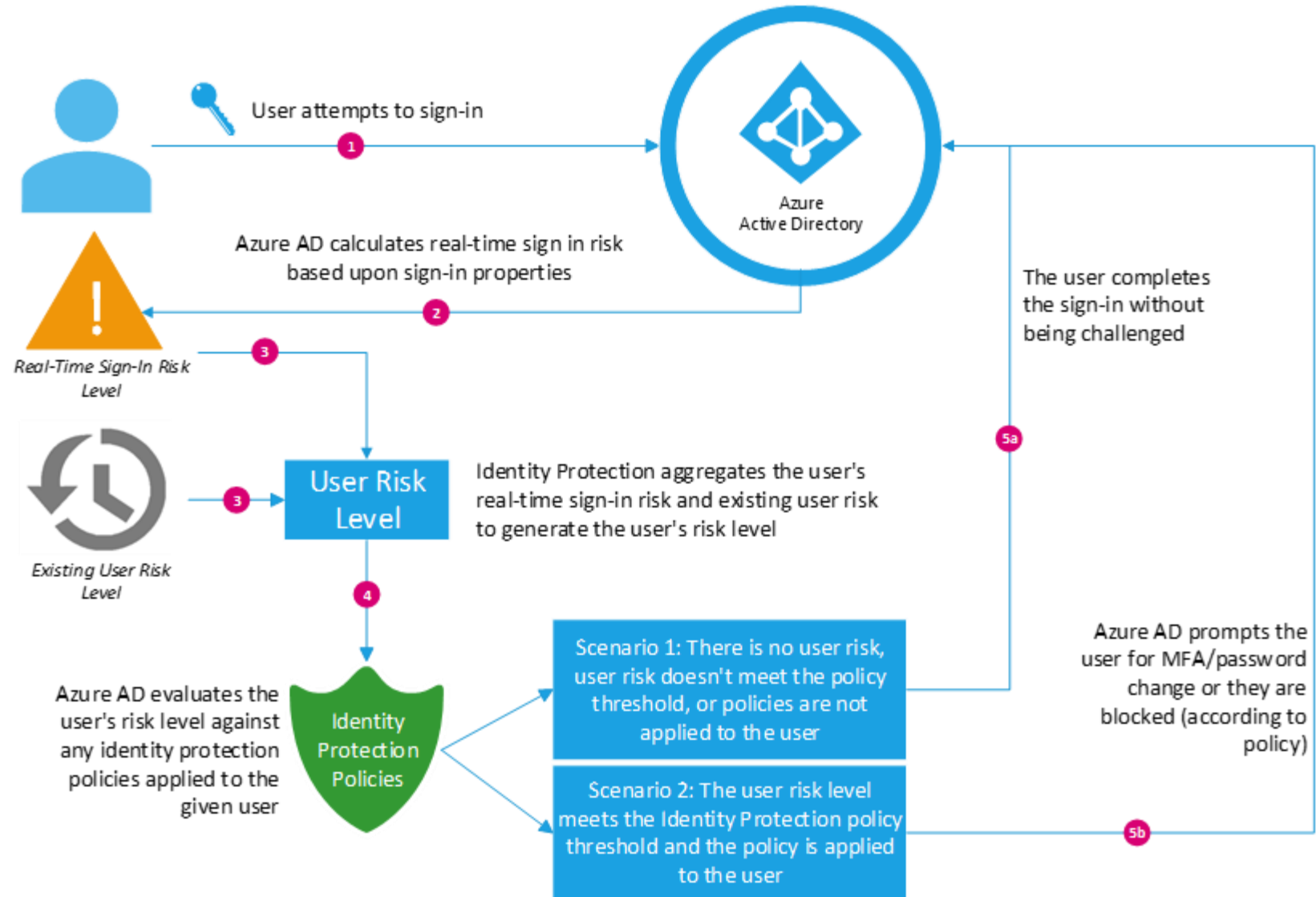
Privileged access insights





# How does it work?

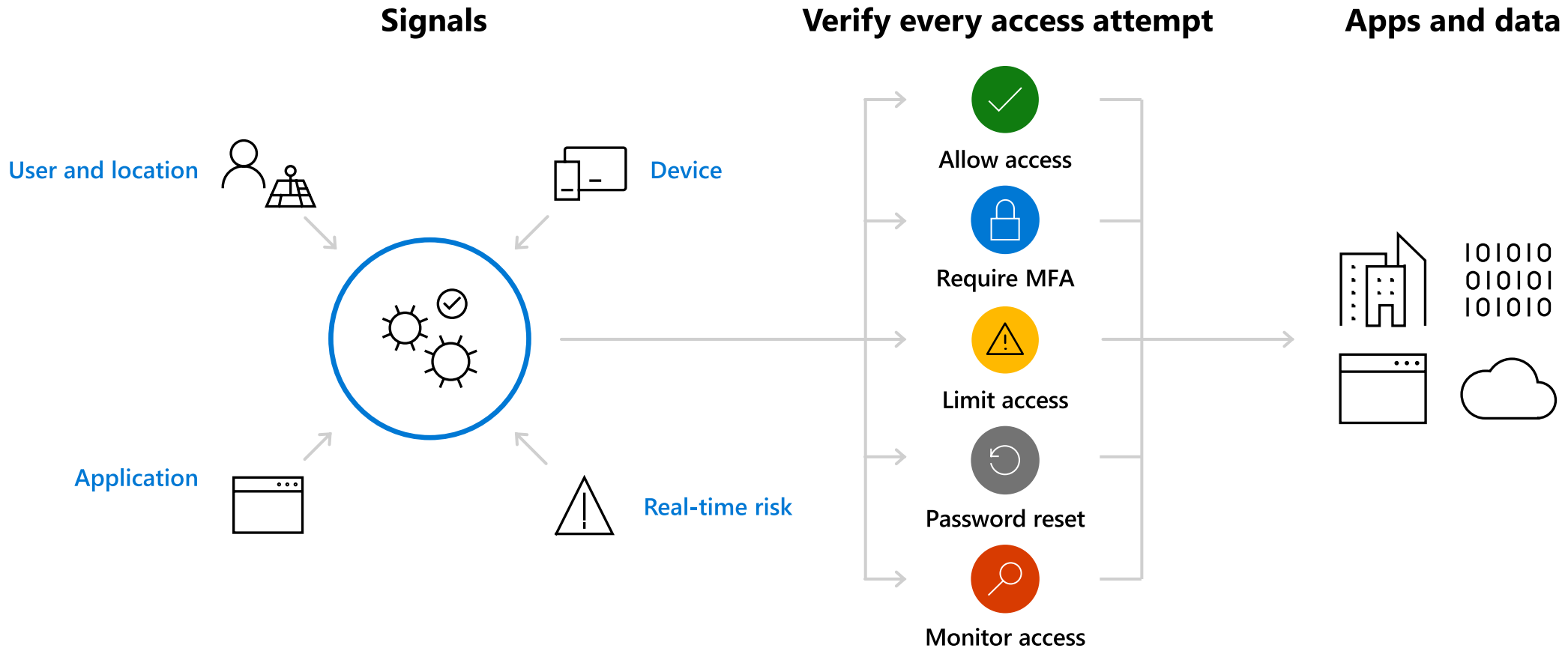
- Enable policies alerting to compromised identities and/or sign-ins
- Self-remediation for risk alerts
- Enable reports to see risk detections for users and sign-ins
- Set up notifications for risk alerts
- Export risk detection data to third-party utilities for further analysis





# Protect resources with Conditional Access

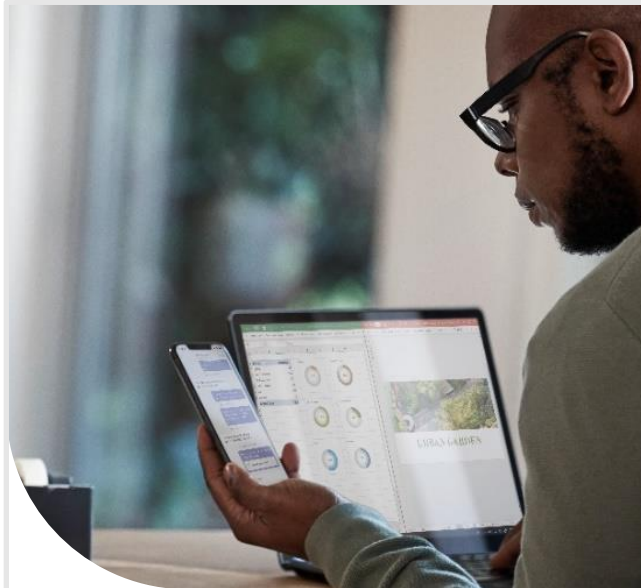
Enable Zero Trust with strong authentication and adaptive policies





# Multi-factor authentication

Verify user identities with strong authentication



We support a **broad range of multi-factor authentication options**

Including passwordless technology



Microsoft  
Authenticator



Windows  
Hello



FIDO2  
Security key



Biometrics



Push  
Notification



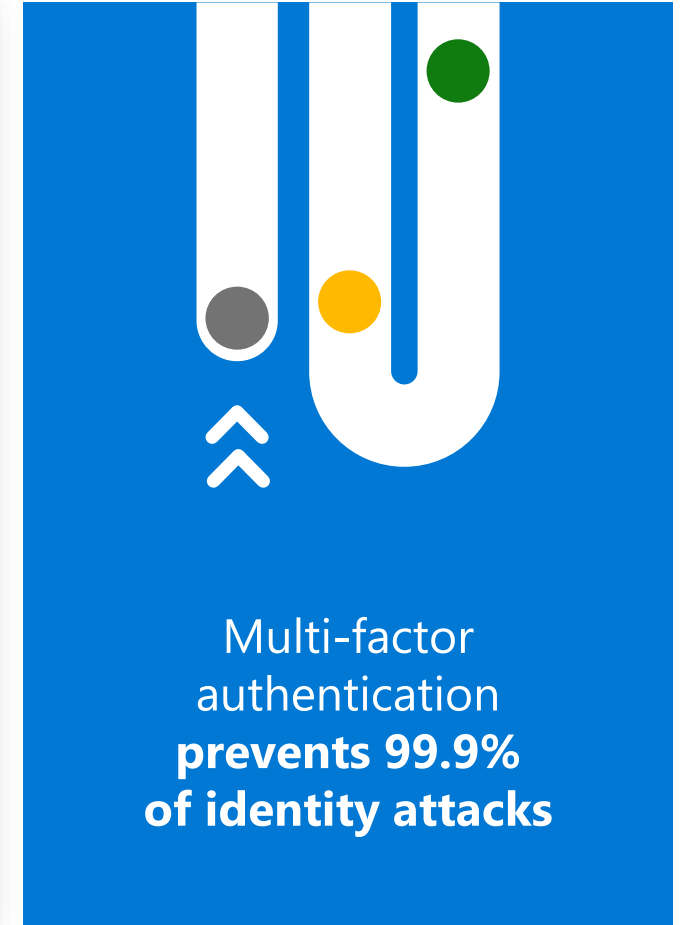
Soft  
Tokens OTP



Hard  
Tokens OTP

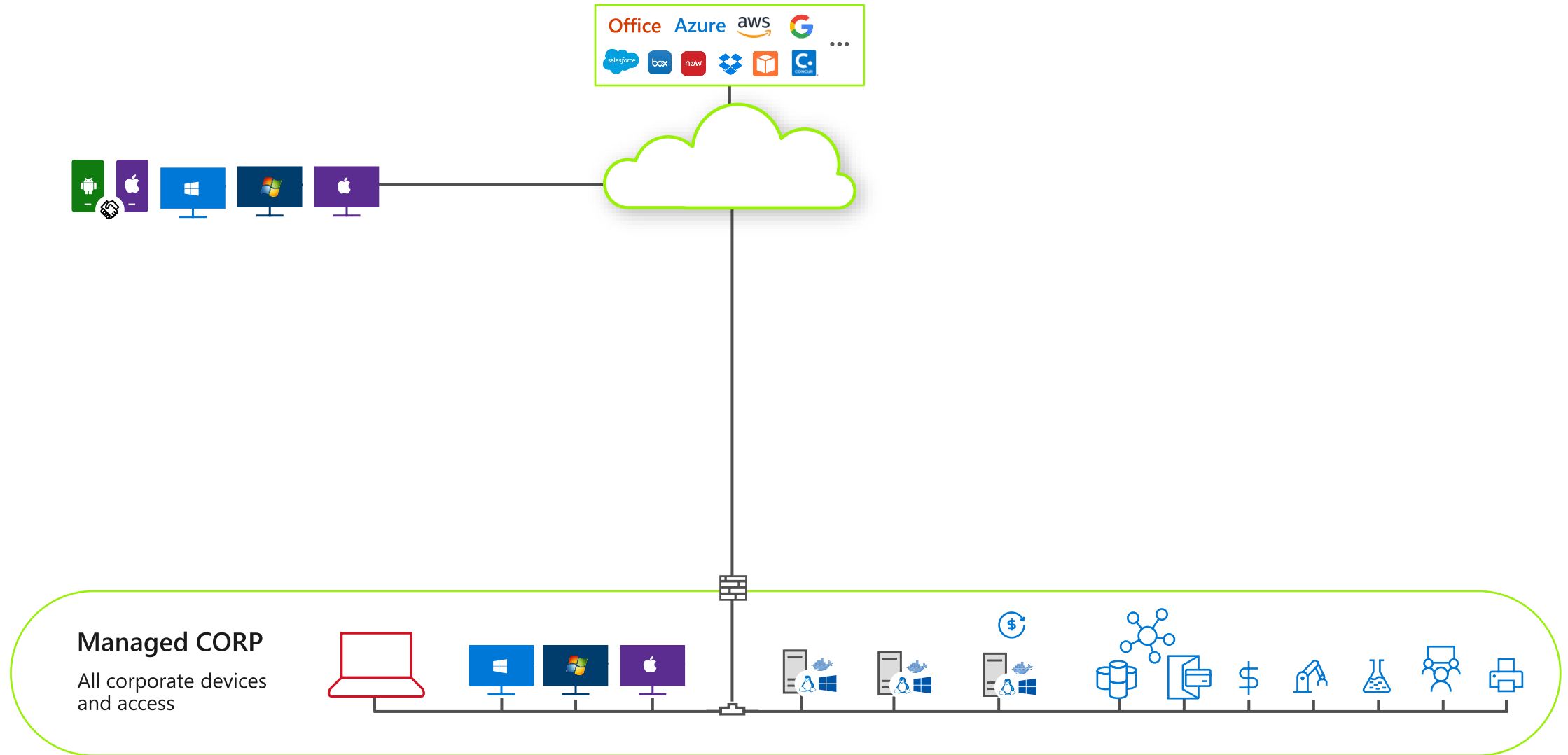


SMS,  
Voice



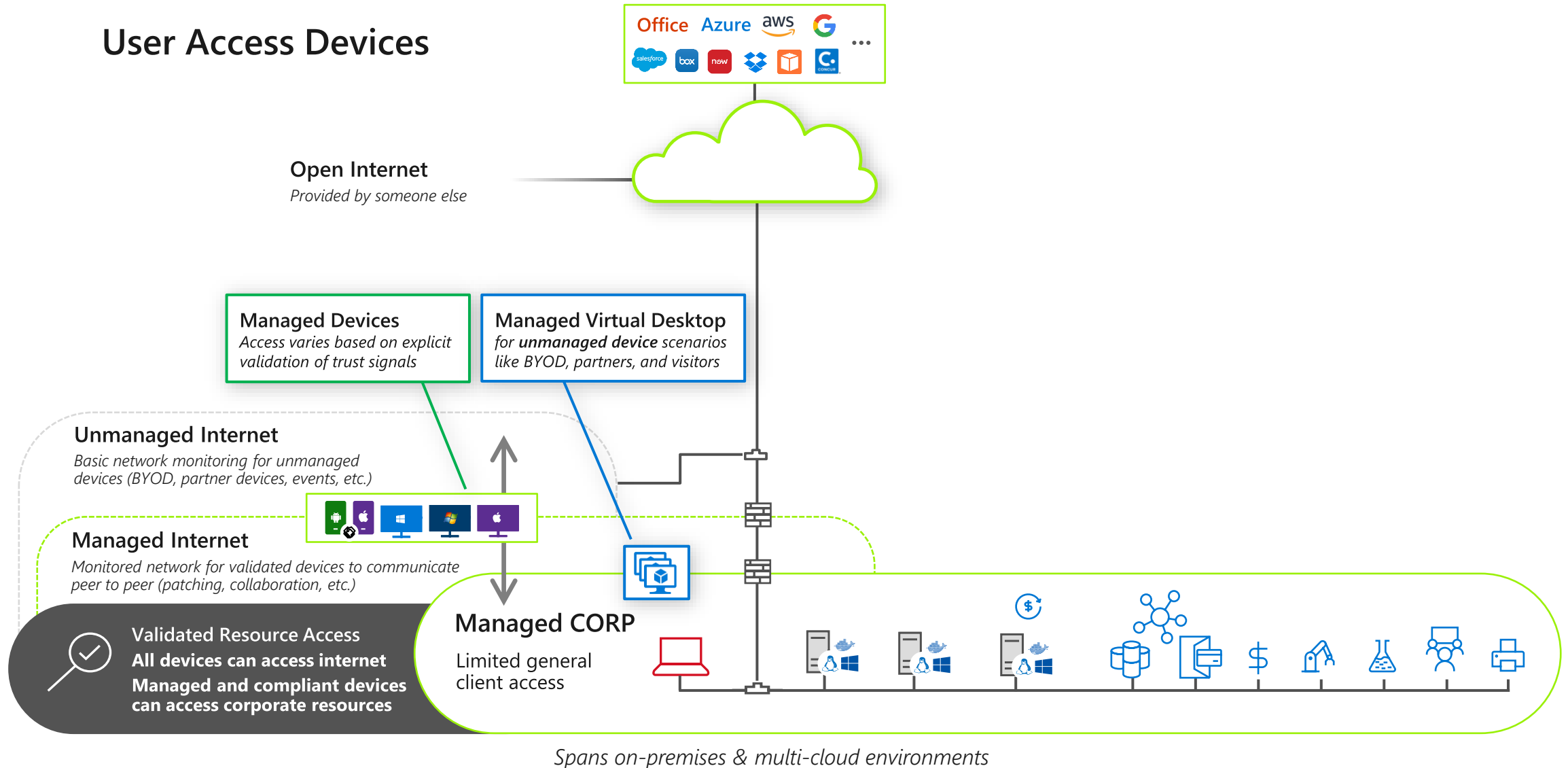


# Typical 'Flat' Network



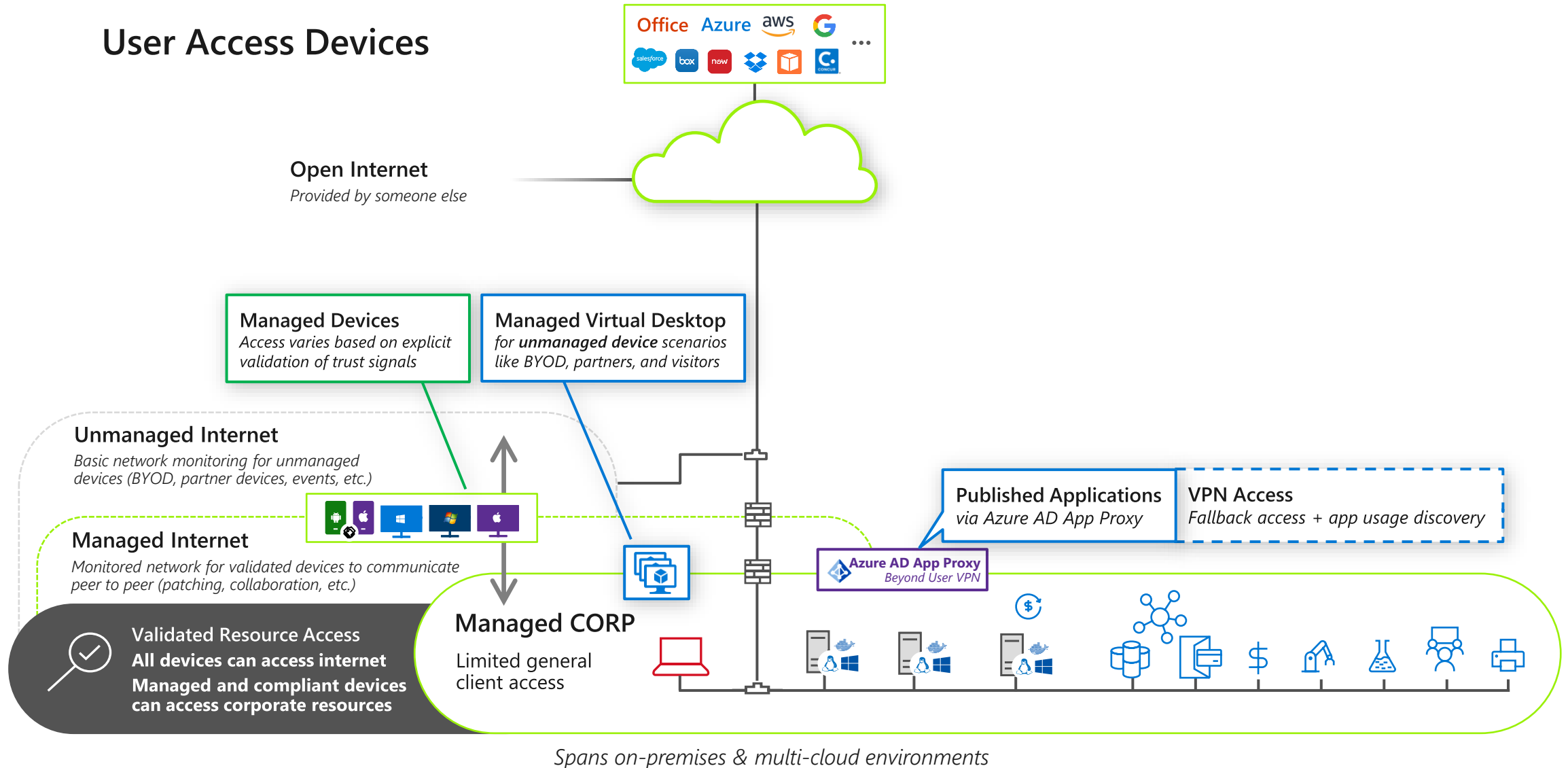


# Zero Trust – Client Security Transformation



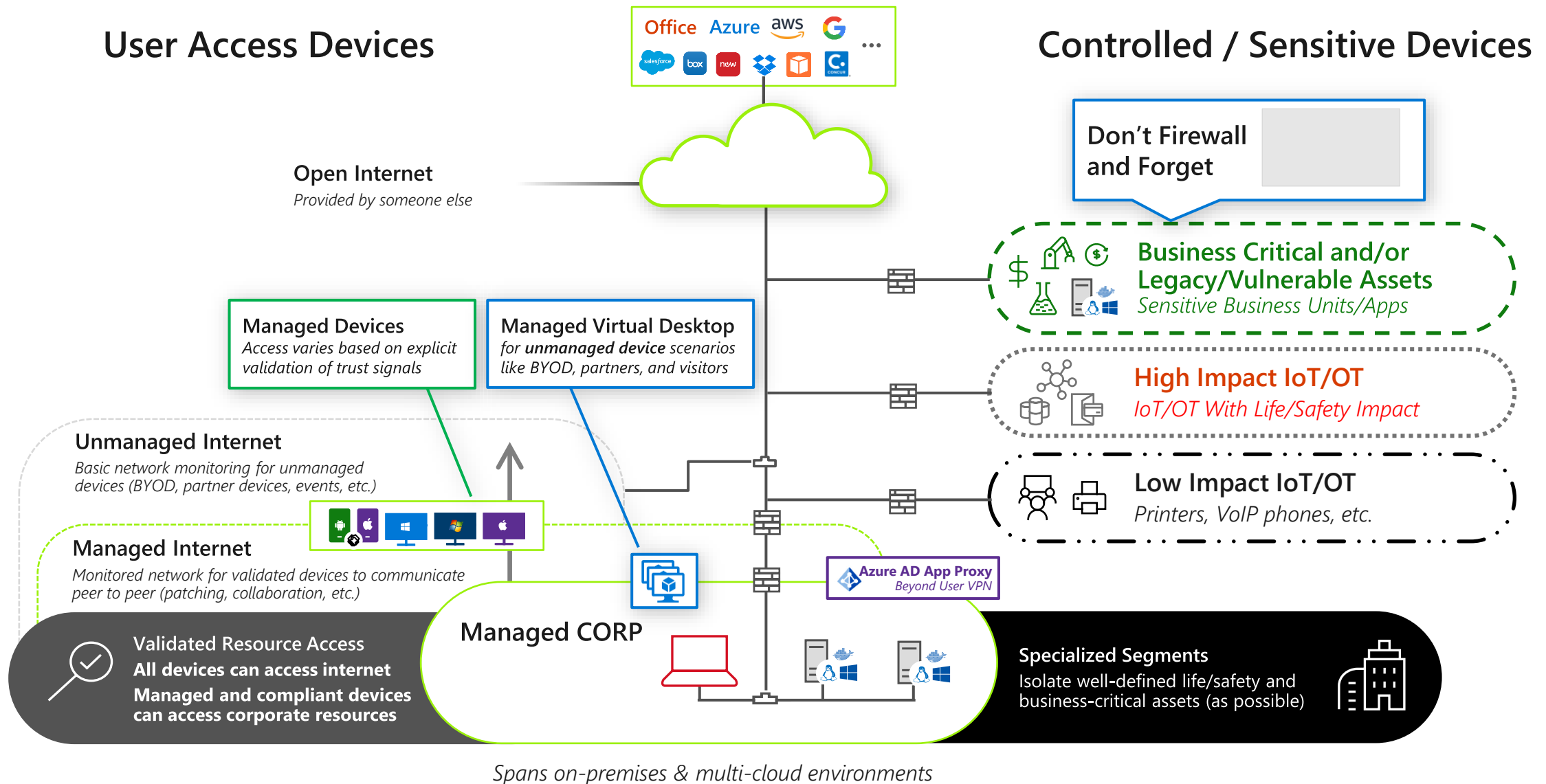


# Zero Trust – App Access for Clients





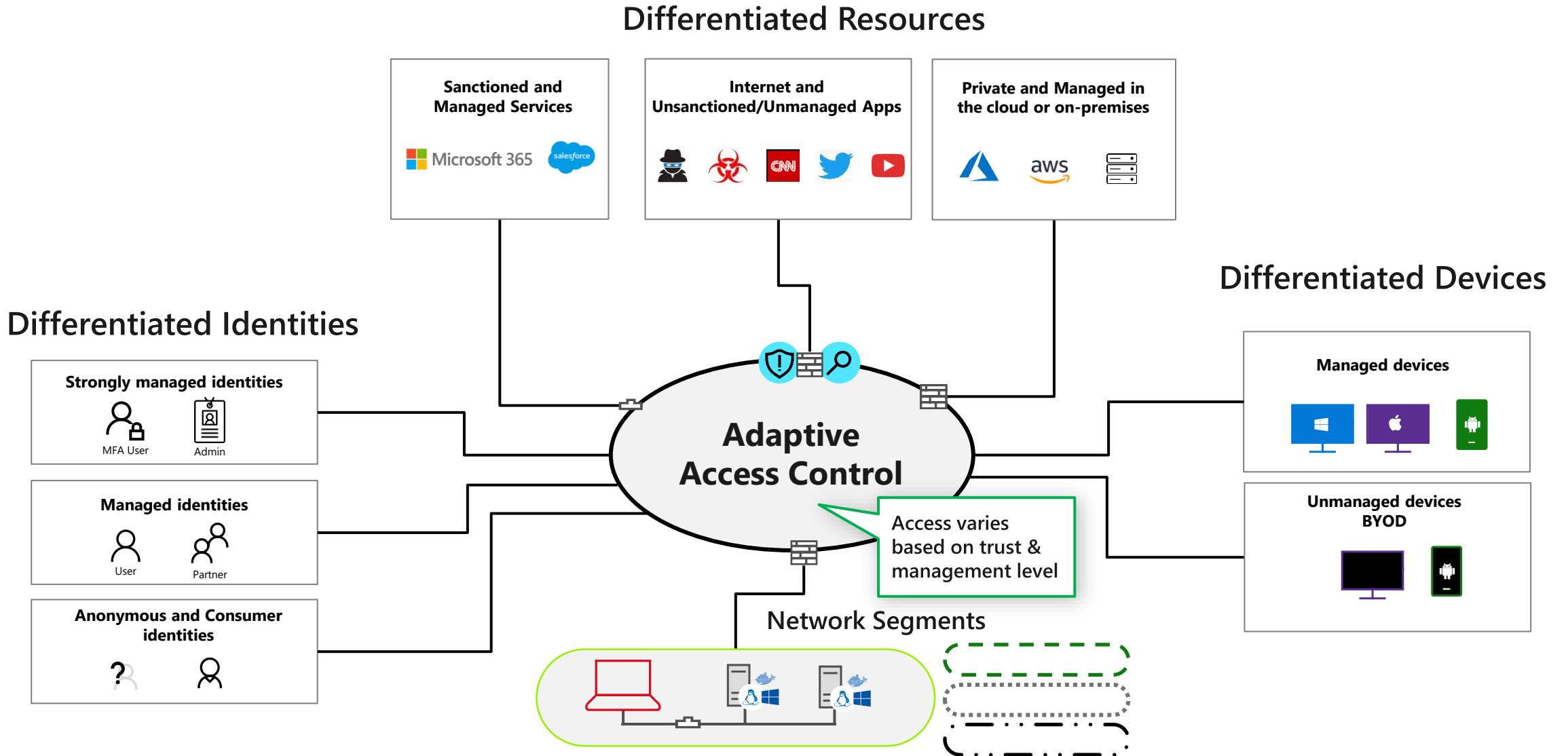
# Zero Trust – Network Segment Transformation





# Full Zero Trust End State

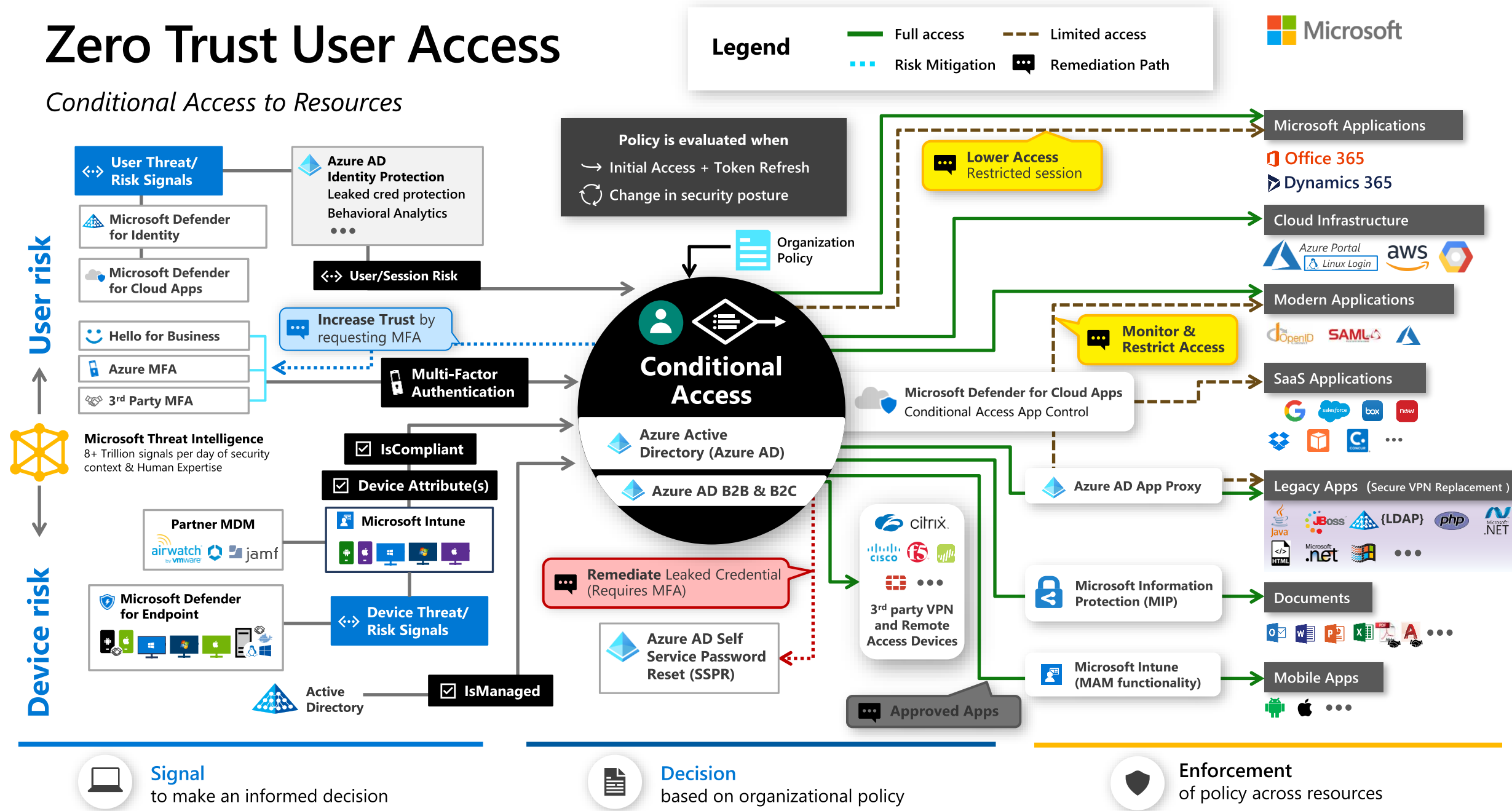
*Bringing the best of both worlds*





# Zero Trust User Access

## Conditional Access to Resources





# Vielen Dank.

Haben Sie Fragen?

---



Jetzt QR-Code scannen und  
weitere Informationen erhalten.

[bechtle.com/security](https://bechtle.com/security)

A photograph of a man and a woman in a professional setting, looking intently at a computer screen. The man is wearing glasses and a light blue shirt, while the woman is wearing a grey blazer. The background is dark with some blue light accents.

**BECHTLE**