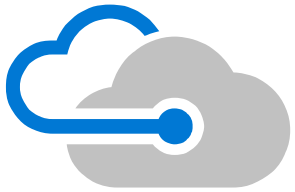
Microsoft 365

Microsoft Defender for Endpoint

Steve Newby (@steve_newby)
Senior Program Manager

Why we're different



Agentless, cloud powered

No additional deployment or infrastructure. No delays or update compatibility issues. Always up to date.

Unparalleled optics

Built on the industry's deepest insight into threats and shared signals across devices, identities, and information.

Automated security

Take your security to a new level by going from alert to remediation in minutes—at scale.

An industry leader in endpoint security

Gartner names Microsoft a Leader in 2019 Endpoint Protection Platforms Magic Quadrant.

Forrester names Microsoft a Leader in 2020 Enterprise Detection and Response Wave.

Microsoft Threat Protection leads in real-world detection in MITRE ATT&CK evaluation.

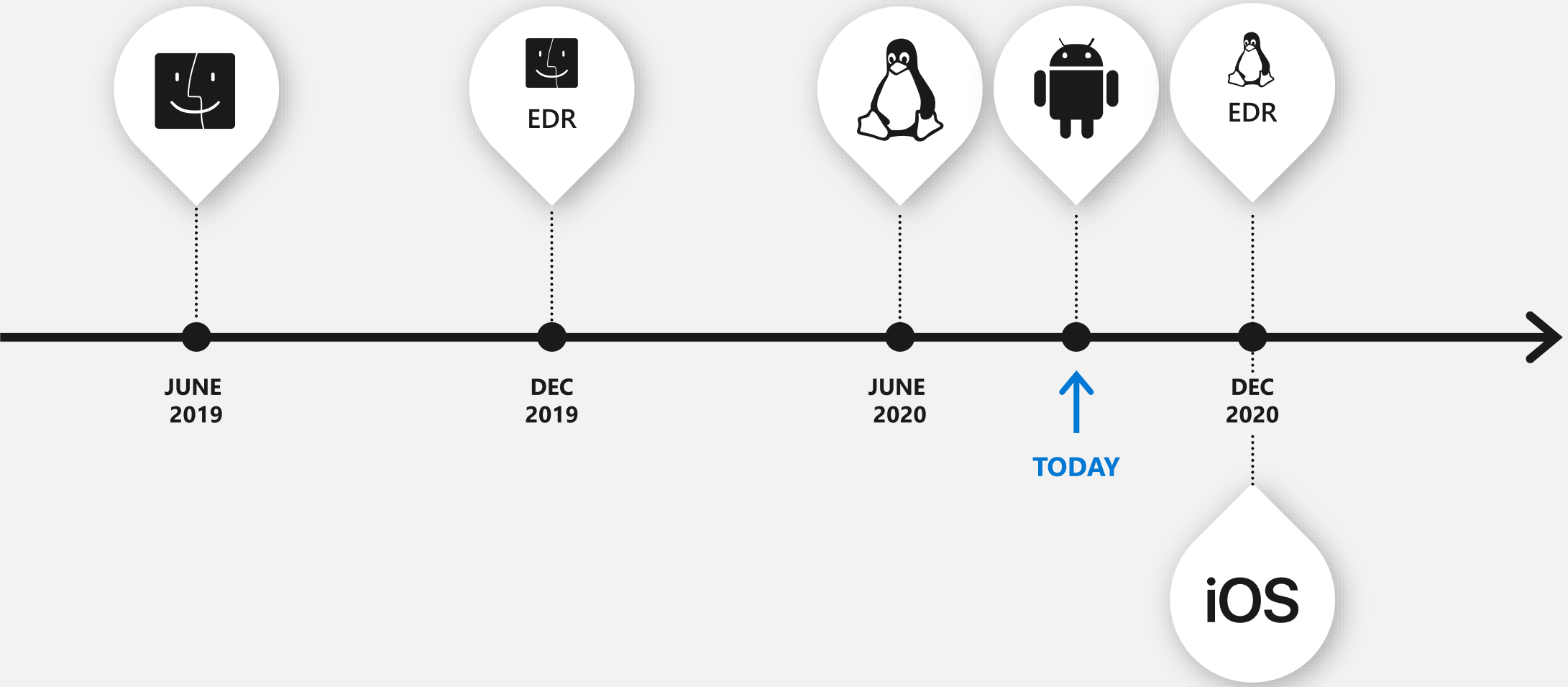
Our antimalware capabilities consistently achieve high scores in independent tests.

Microsoft Defender ATP awarded a perfect 5-star rating by SC Media in their 2020 Endpoint Security Review

Microsoft won six security awards with Cyber Defense Magazine at RSA 2020:

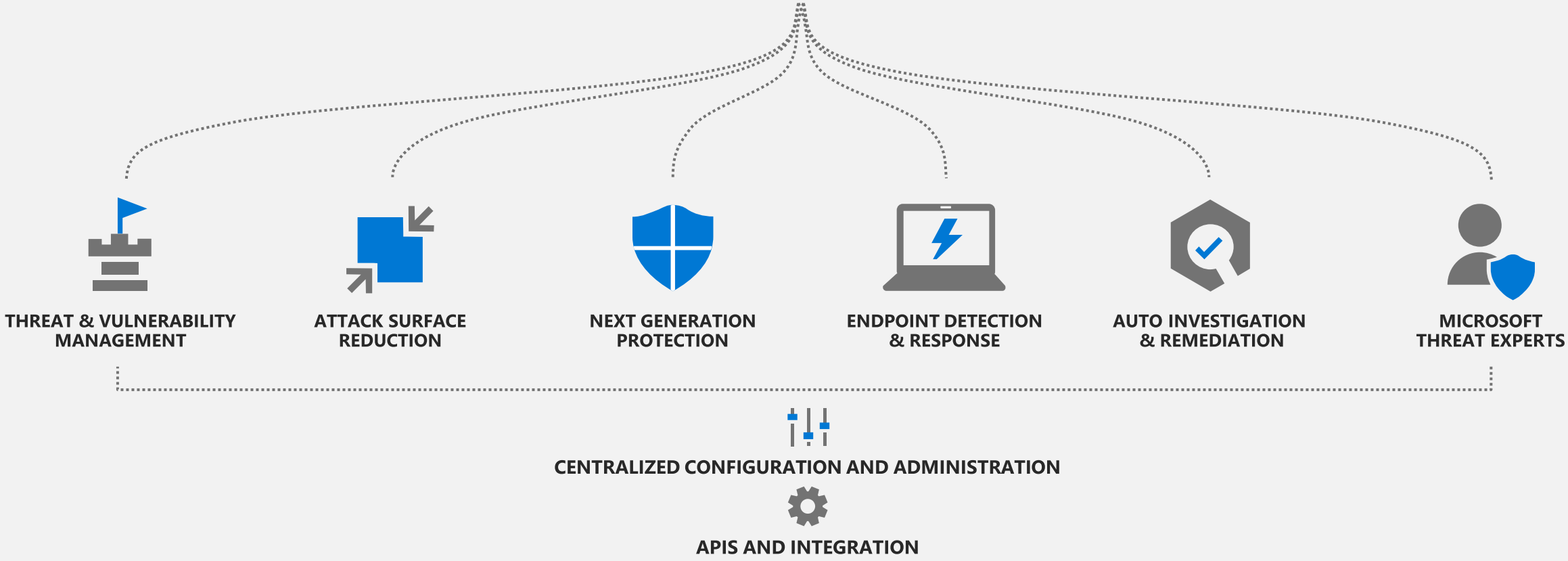
- ✓ Application Isolation – Next Gen
- ✓ Endpoint Security – Editor's Choice
- ✓ Threat and Vulnerability Management – Most Innovative
- ✓ Malware Detection – Best Product
- ✓ Managed Detection and Response – Market Leader
- ✓ Enterprise Threat Protection – Hot Company

Delivering Microsoft Defender for Endpoint across platforms



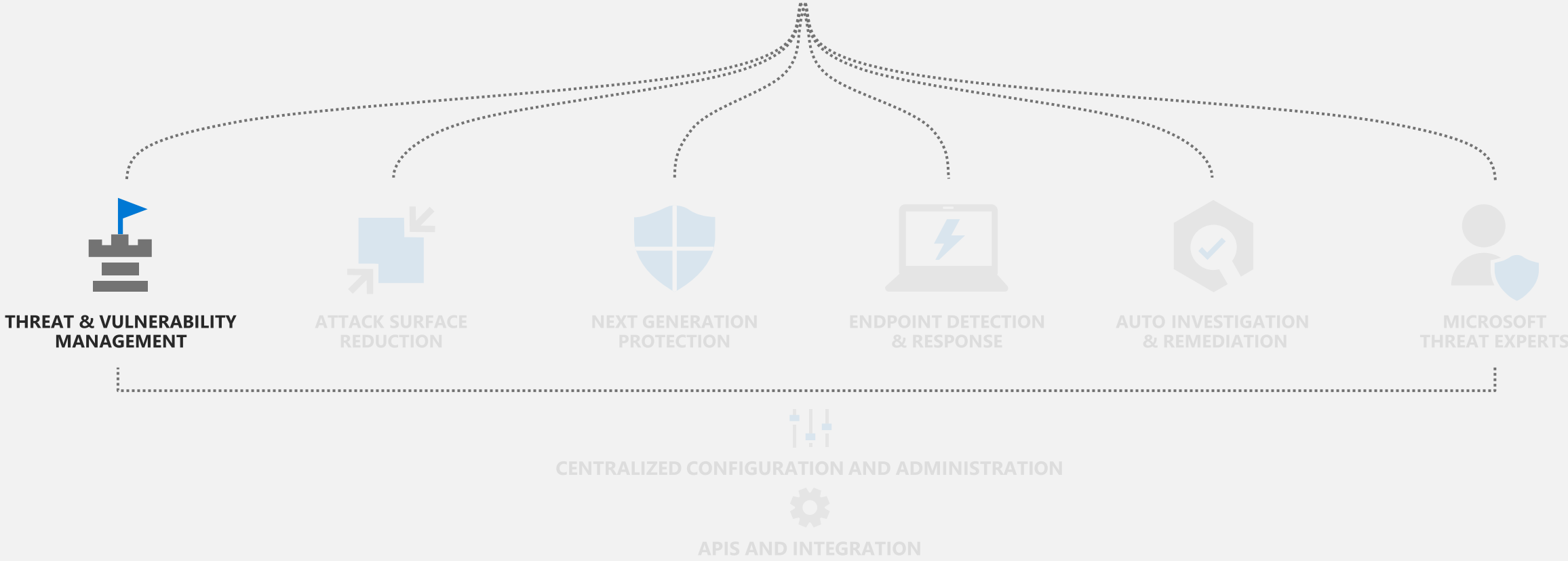
Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Microsoft Defender for Endpoint

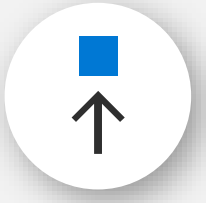
Built-in. Cloud-powered.



Key customer pain points

Discover

- Periodic scanning
- Blind spots
- No run-time info
- “Static snapshot”



Prioritize

- Based on severity
- Missing org context
- No threat view
- Large threat reports

Compensate

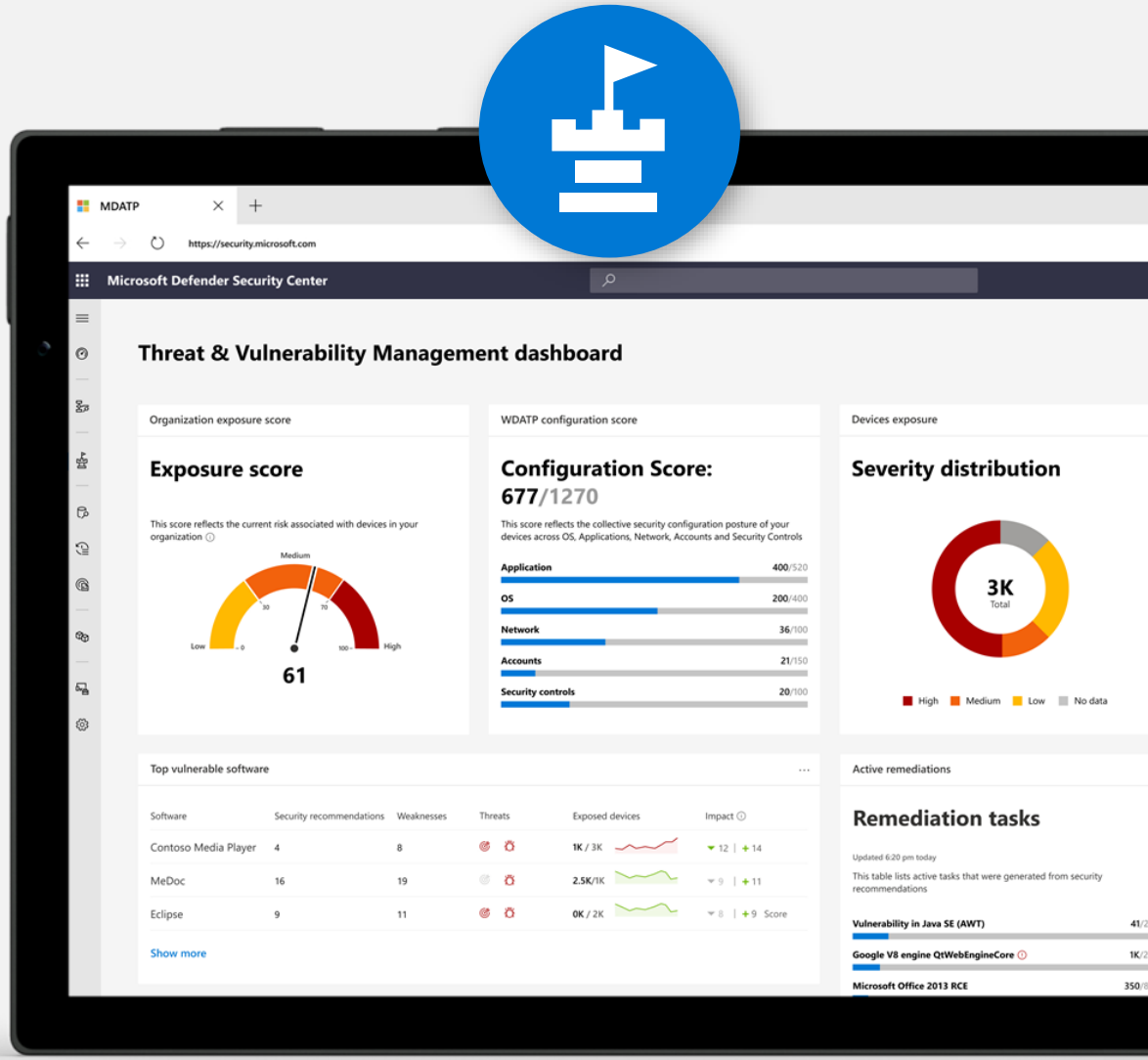
- Waiting for a patch
- No IT/Security bridge
- Manual process
- No validation

Bottom line: Organizations remain highly vulnerable, despite high maintenance costs

Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

1. Continuous real-time discovery
2. Context-aware prioritization
3. Built-in end-to-end remediation process



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)

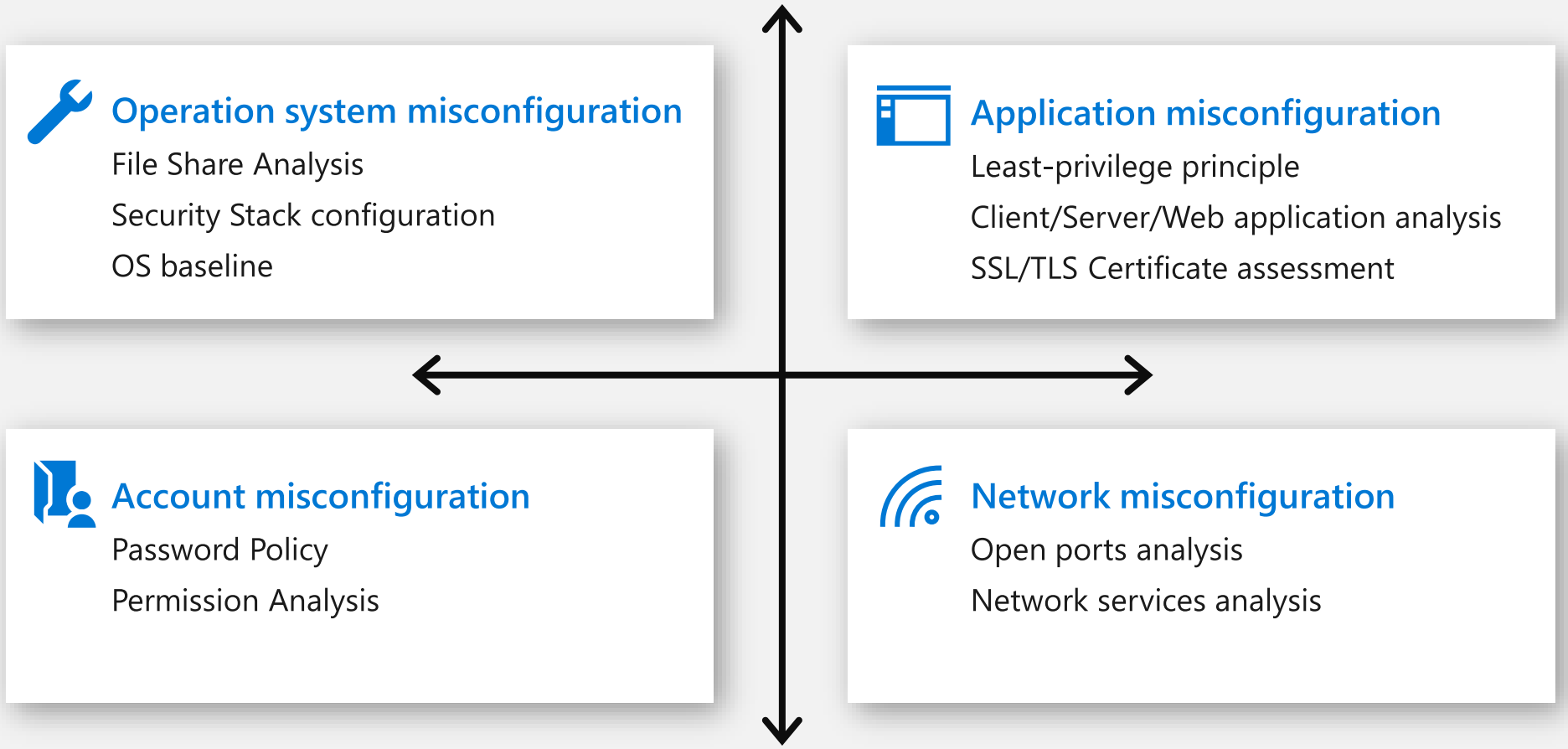
Hardware vulnerabilities (firmware)
Extremely hard to exploit, but can affect the root trust of the system.
For example: Spectre/Meltdown vulnerabilities (CVE-2017-5715)

Hardest to discover

1

Continuous Discovery

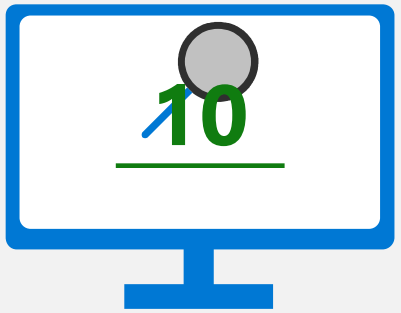
Broad secure configuration assessment



2

Threat & Business Prioritization (“TLV”)

Helping customers focus on the right things at the right time



T

Threat Landscape

Vulnerability characteristics (CVSS score, days vulnerable)

Exploit characteristics (public exploit & difficulty, bundle)

EDR security alerts (Active alerts, breach history)

Threat analytics (live campaigns, threat actors)

L

Breach Likelihood

Current security posture

Internet facing

Exploit attempts in the org

V

Business Value

HVA analysis (WIP, HVU, critical process)

Run-time & Dependency analysis

3

Automated Compensation

Bridging between the IT and Security admins

Game changing bridge between IT and Security teams

1-click remediation requests via Intune/SCCM

Automated task monitoring via run-time analysis

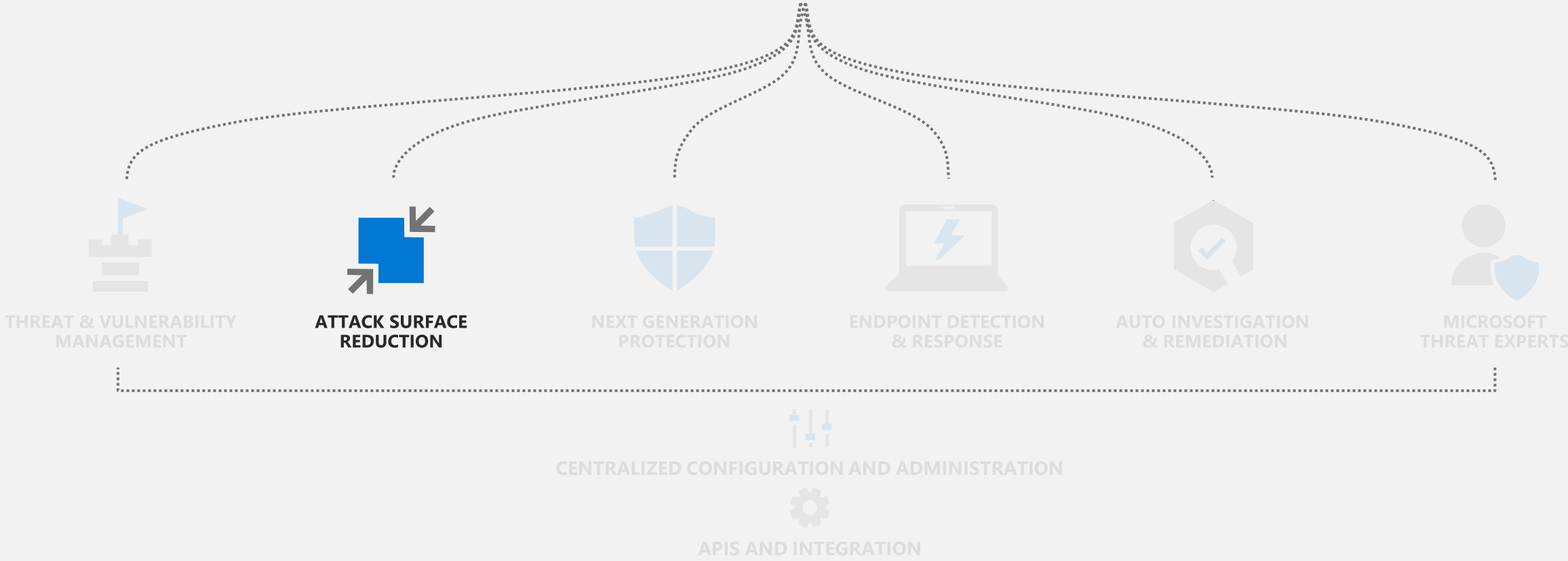
Tracking Mean-time-to-mitigate KPIs

Rich exception experience to mitigate/accept risk

Ticket management integration (Intune, Planner, Service Now, JIRA)

Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Key customer pain points

Zero days

Zero days continue to plague the industry

Network boundaries

Perimeters are eroding, unique solutions are required to harden

Cross-platform

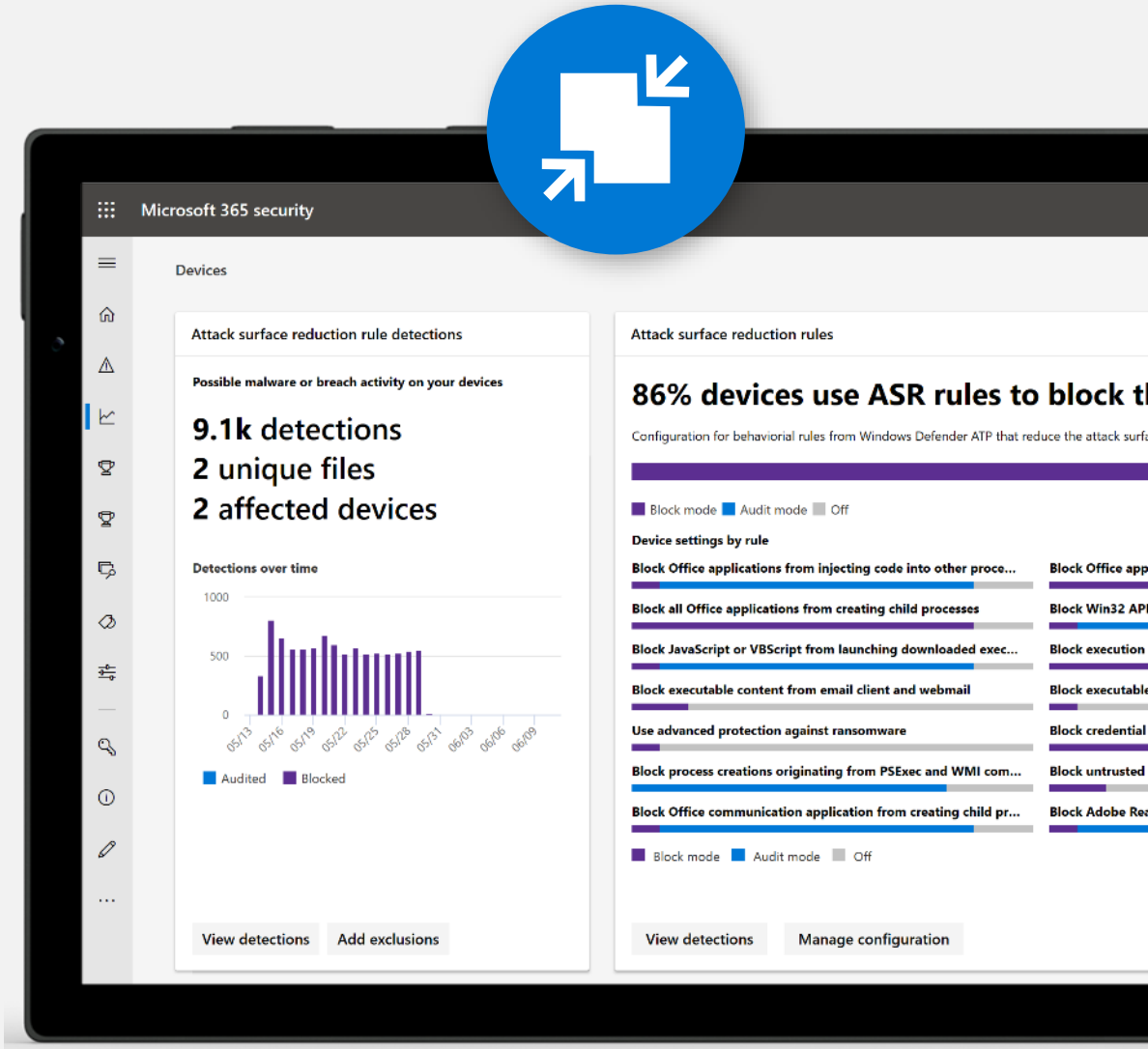
Heterogeneous environments make it challenging

Bottom line: Organizations struggle to proactively adjust their security posture

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

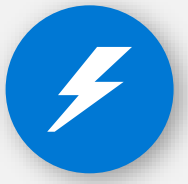
Ransomware protection for your files

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

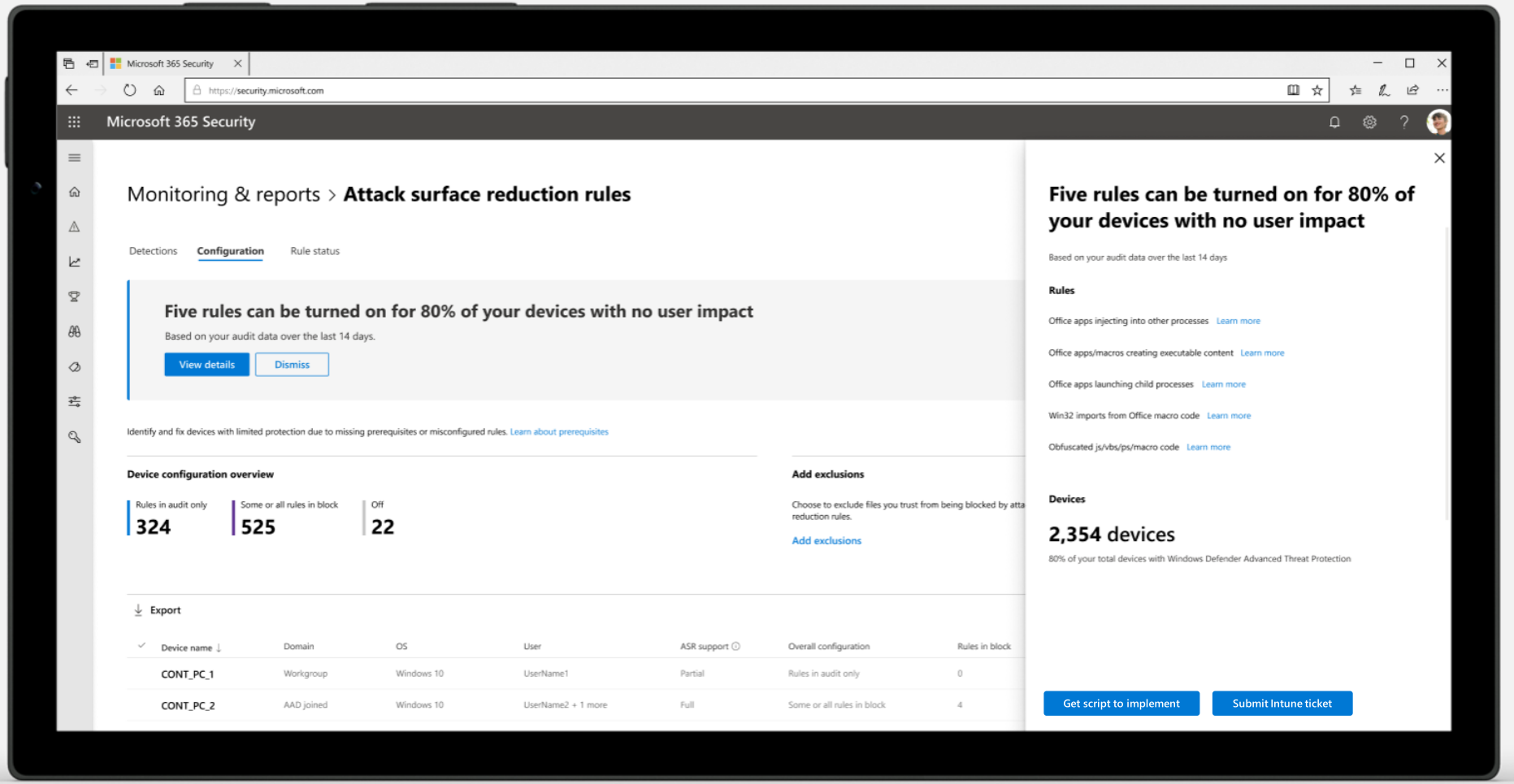
Polymorphic threats

- 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

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

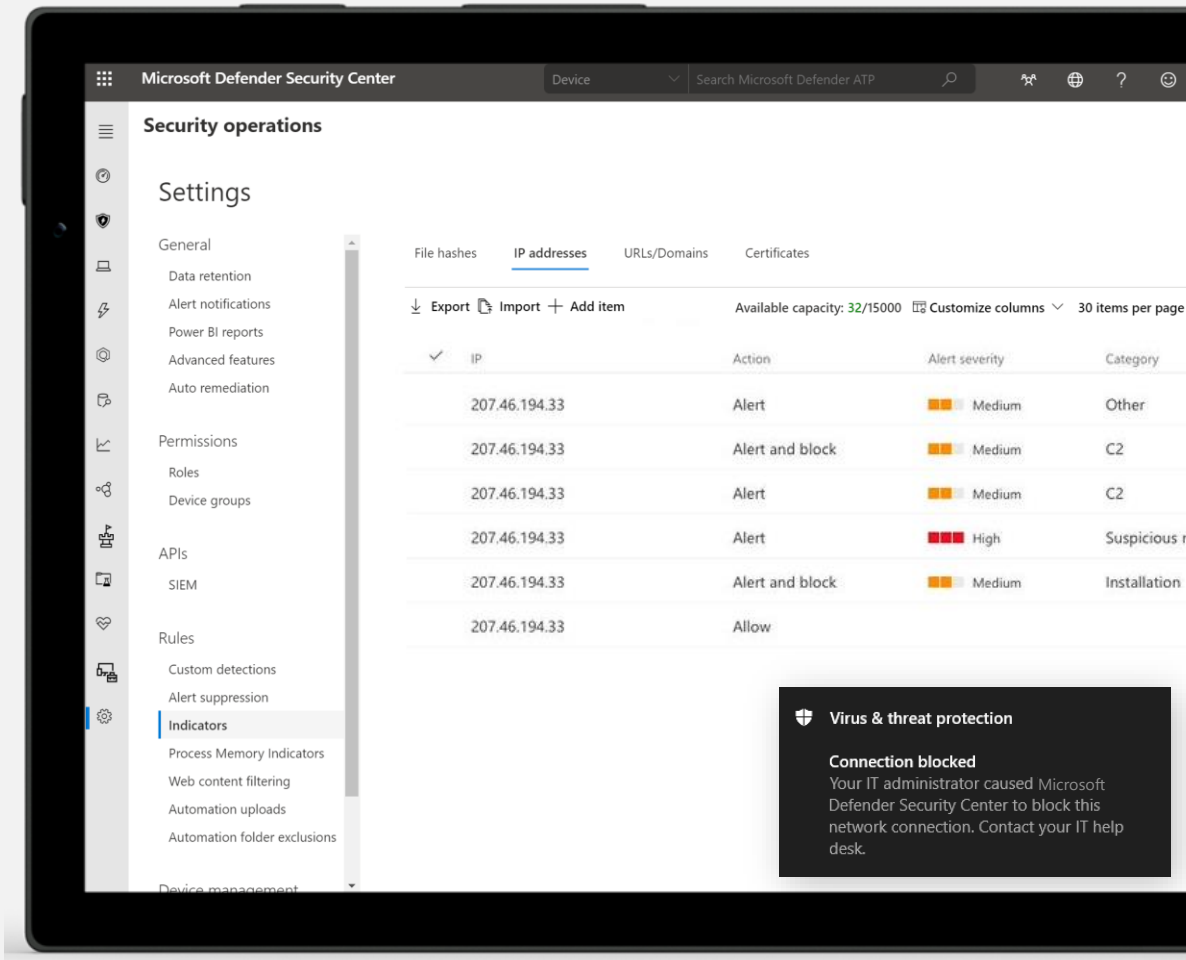
Easy button: turn on block



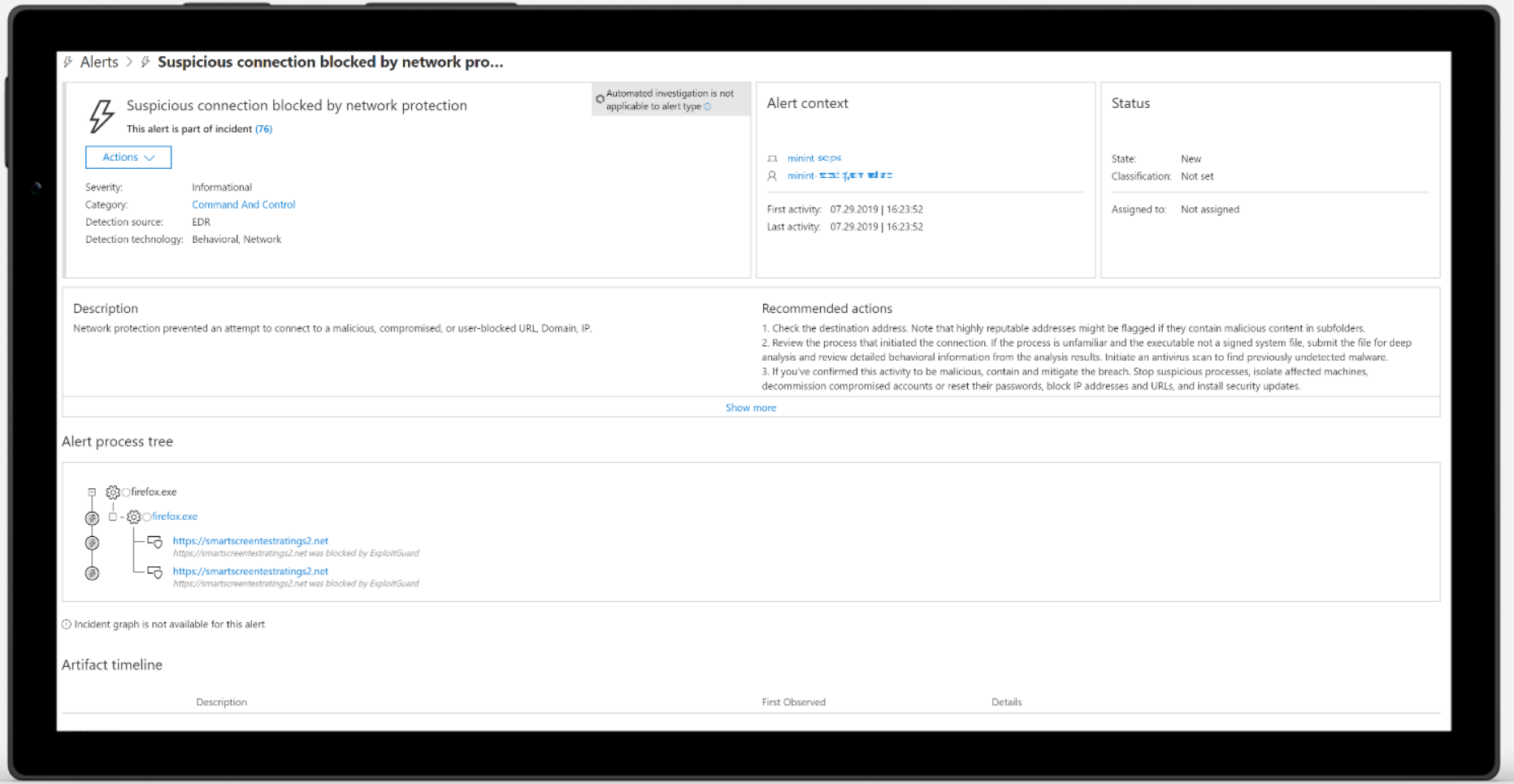
Network protection

Allow, audit and block

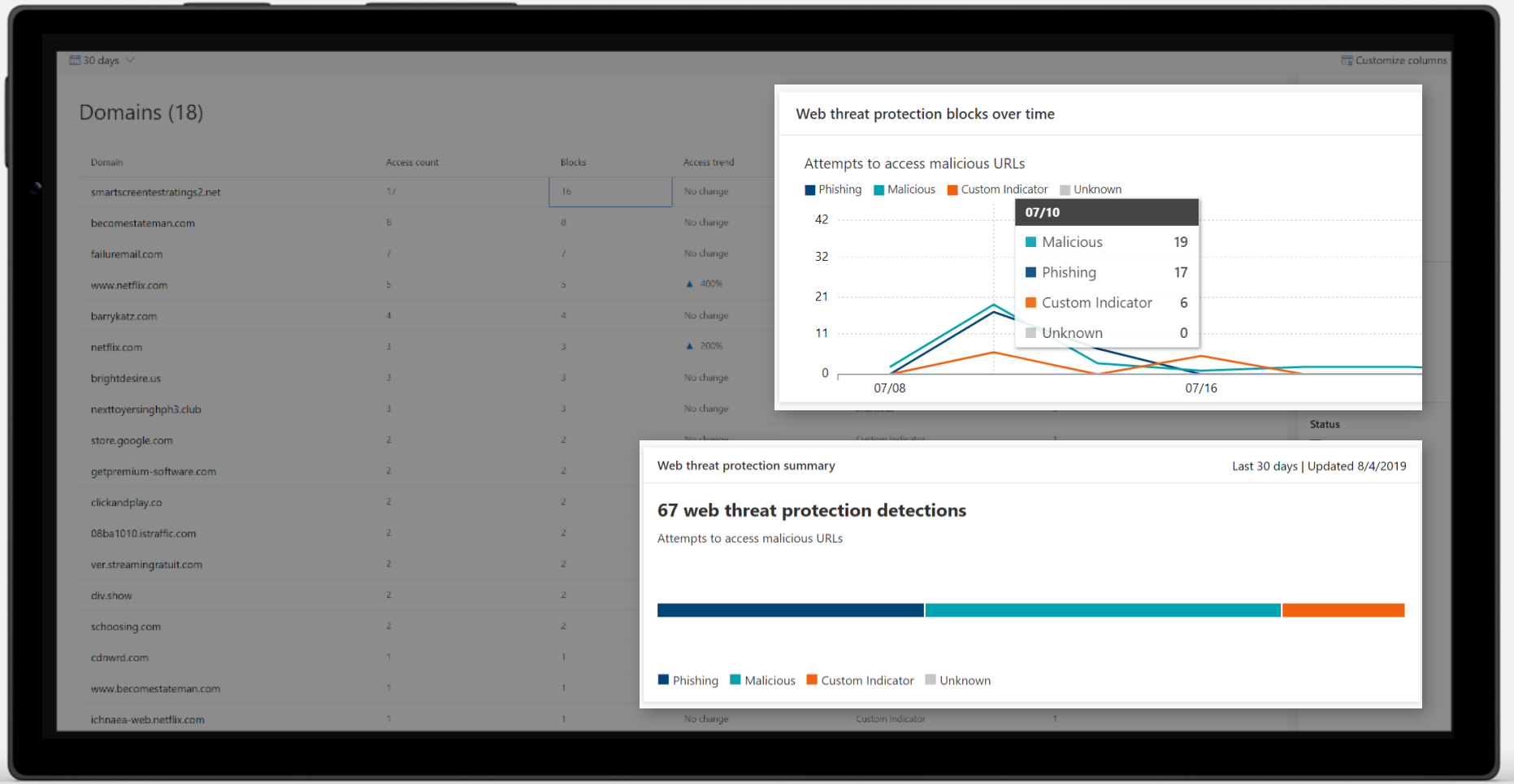
- Perimeter-less network protection ("SmartScreen in the box") preventing users from accessing malicious or suspicious network destinations, **using any app on the device and not just Microsoft Edge.**
- Customers can add their own TI in additional to trusting our rich reputation database.



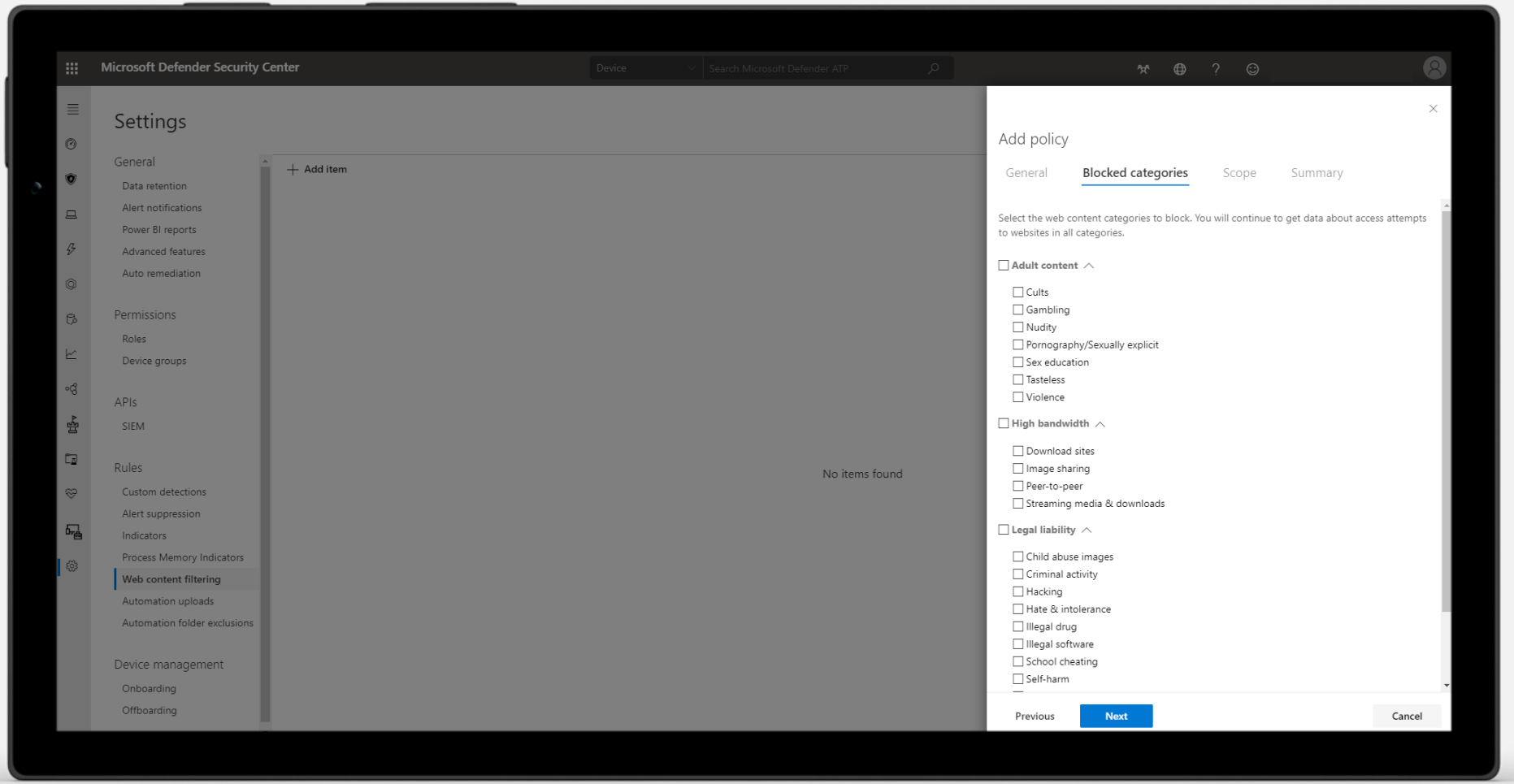
Web Threat Alerts



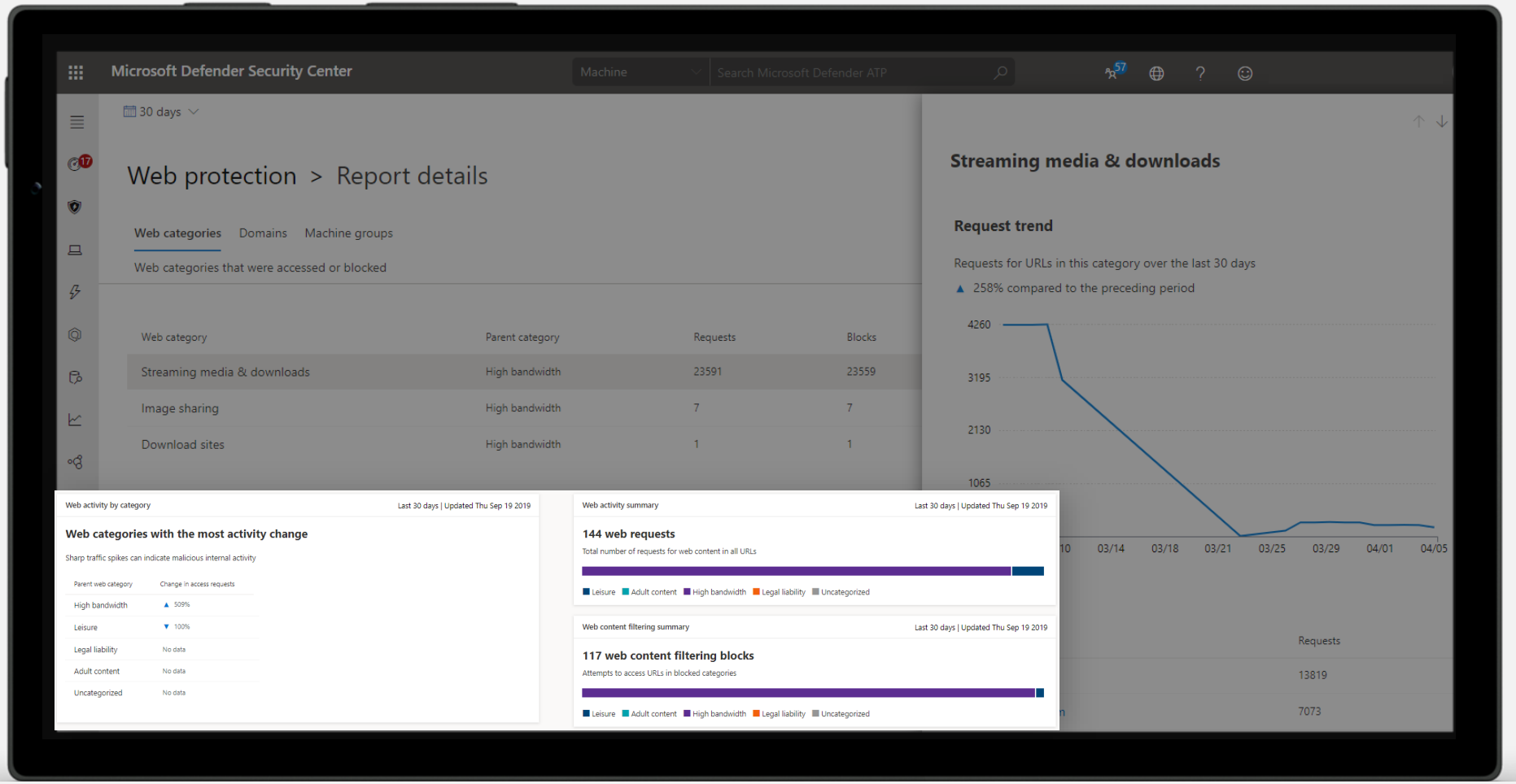
Web Threat Reports



Web content filtering configuration

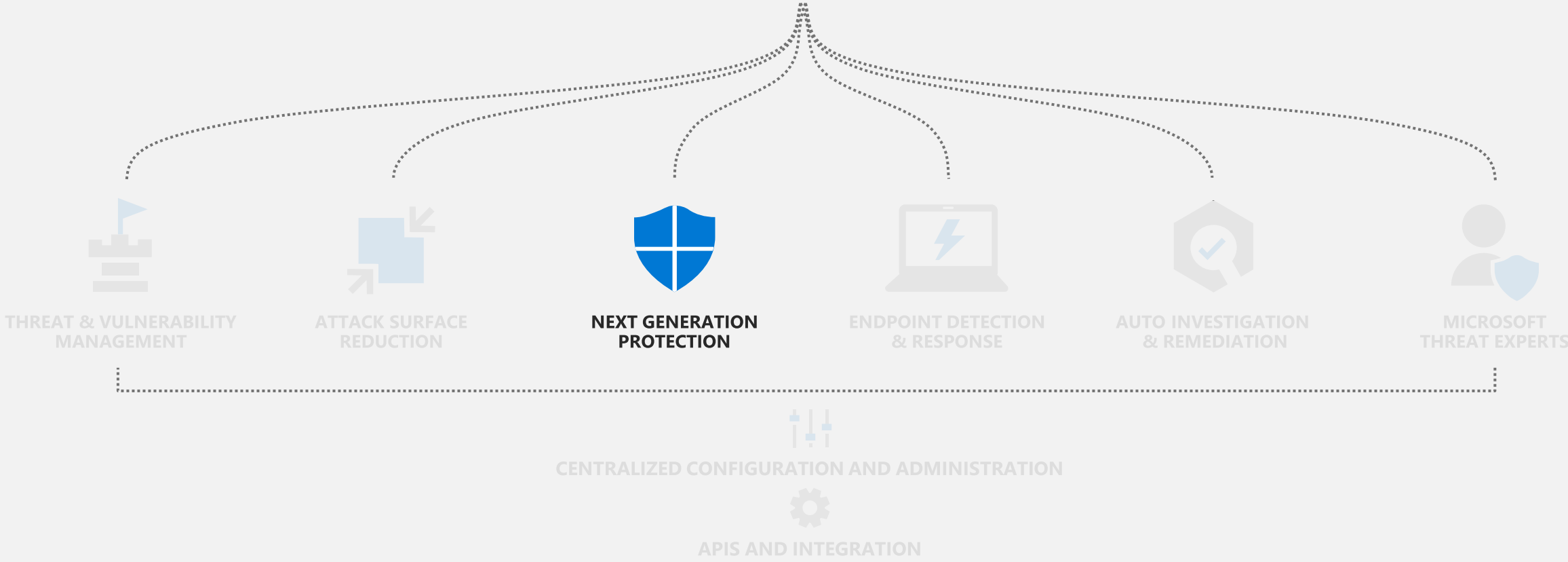


Web Content Filtering reporting



Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Key customer pain points

Solutions that depend on regular updates can not protect against the 7 million unique threats that emerge per hour

The game has shifted from blocking recognizable executable files to malware that uses sophisticated exploit techniques (e.g: fileless)

While Attack Surface Reduction can dramatically increase your security posture you still need detection for the surfaces that remain

We live in a world of hyper polymorphic threats with 5 billion unique instances per month

Static vs Dynamic

Static signatures: focus on a file

Hashes
Strings
Emulators

Ineffective

Dynamic heuristics: focus on *run-time behaviors*

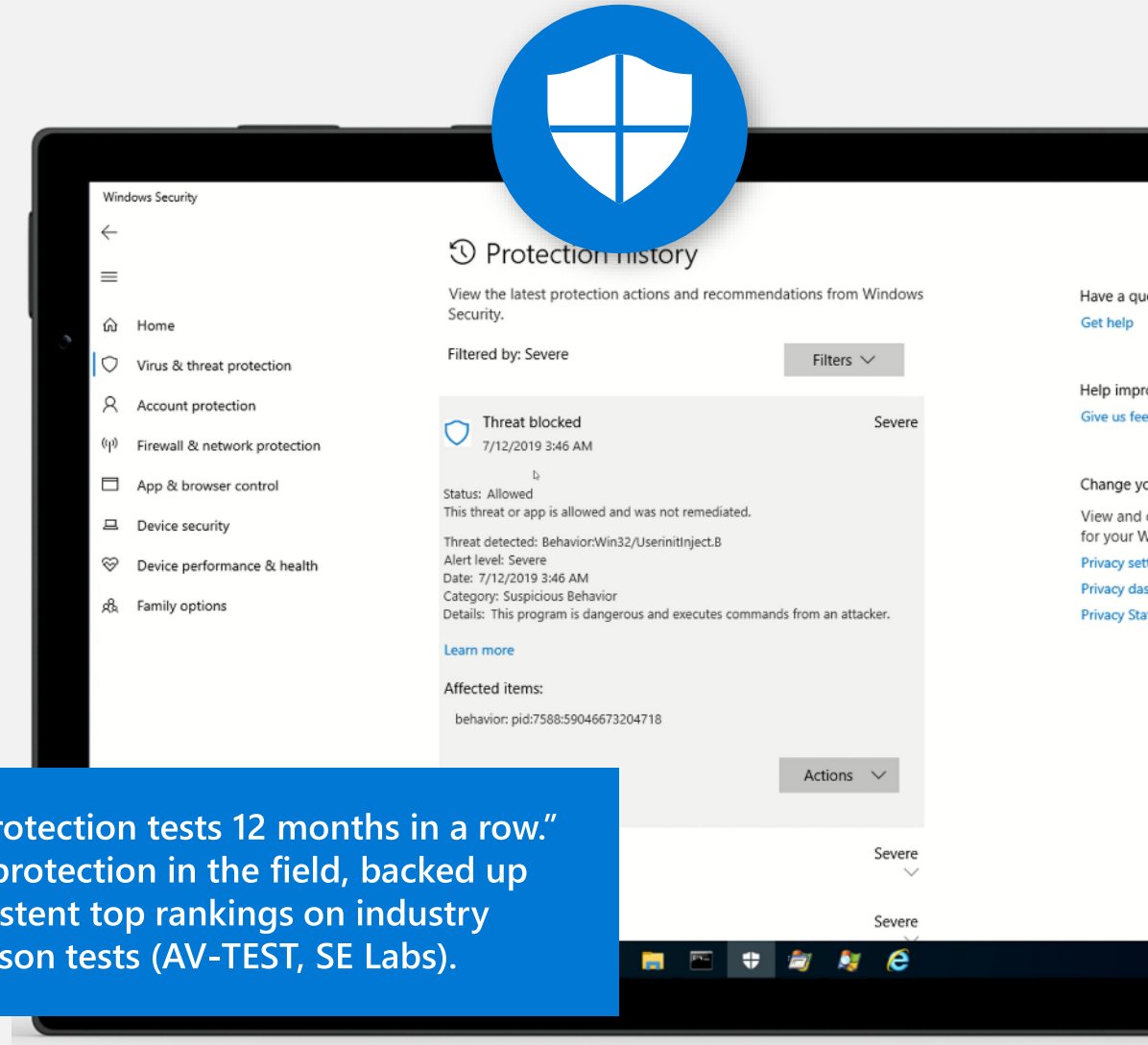
Behavior monitoring
Memory scanning
AMSI
Command-line scanning

Effective

Next Generation Protection

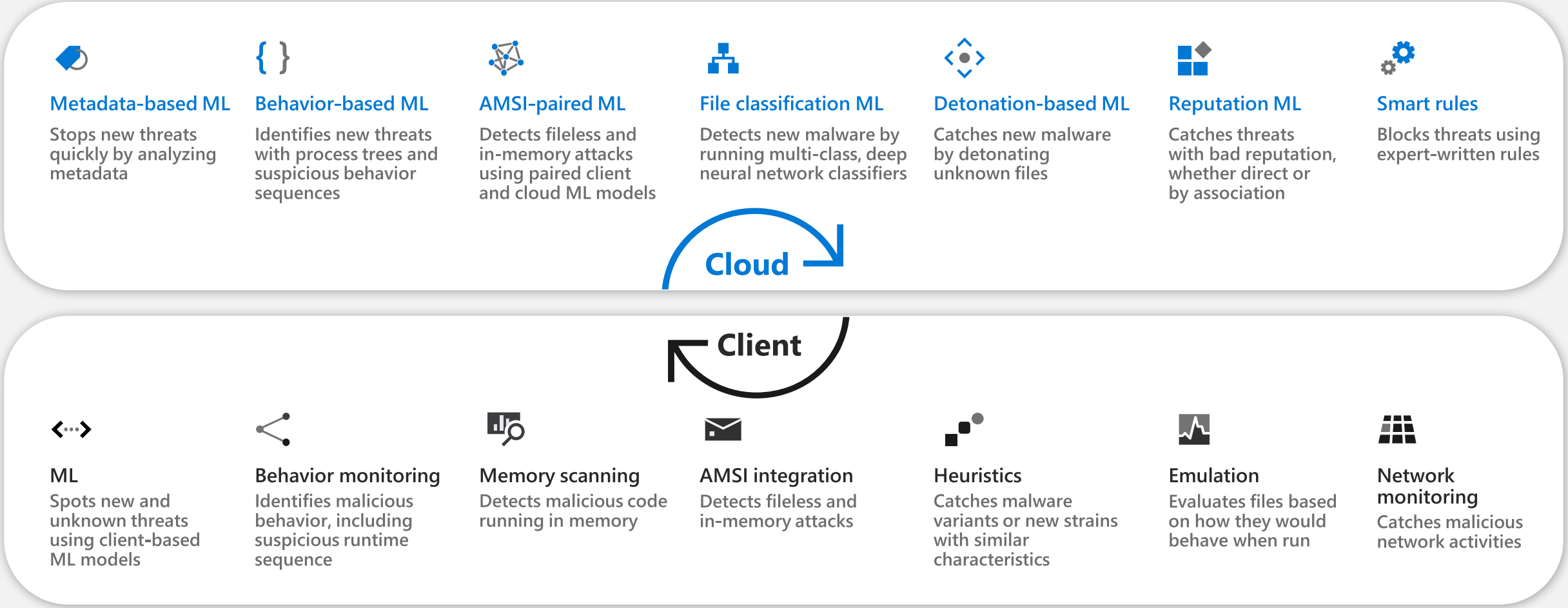
Blocks and tackles sophisticated threats and malware

- Behavioral based real-time protection
- Blocks file-based and fileless malware
- Stops malicious activity from trusted and untrusted applications



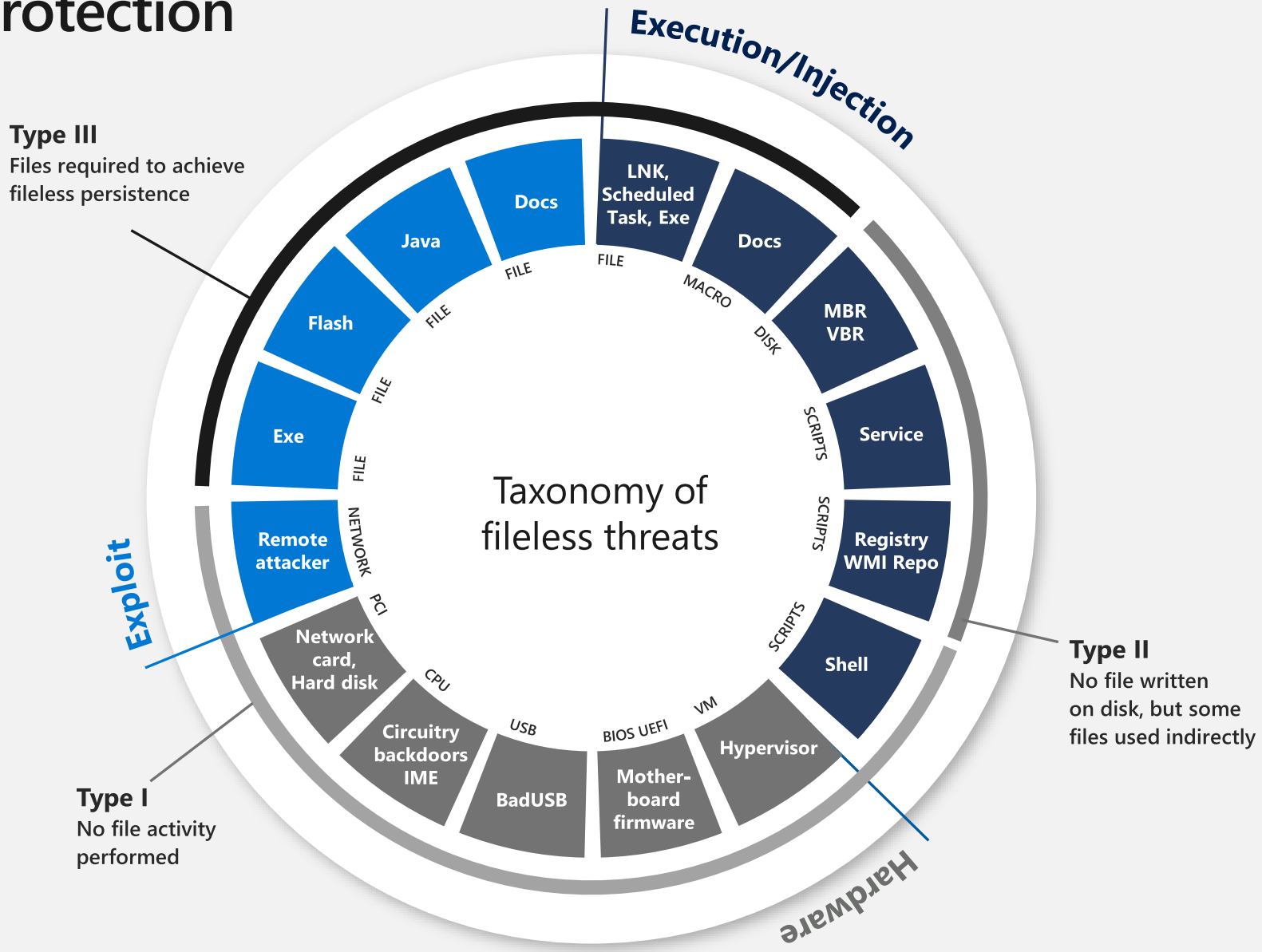
"Aced protection tests 12 months in a row." Proven protection in the field, backed up by consistent top rankings on industry comparison tests (AV-TEST, SE Labs).

Microsoft Defender for Endpoint next generation protection engines

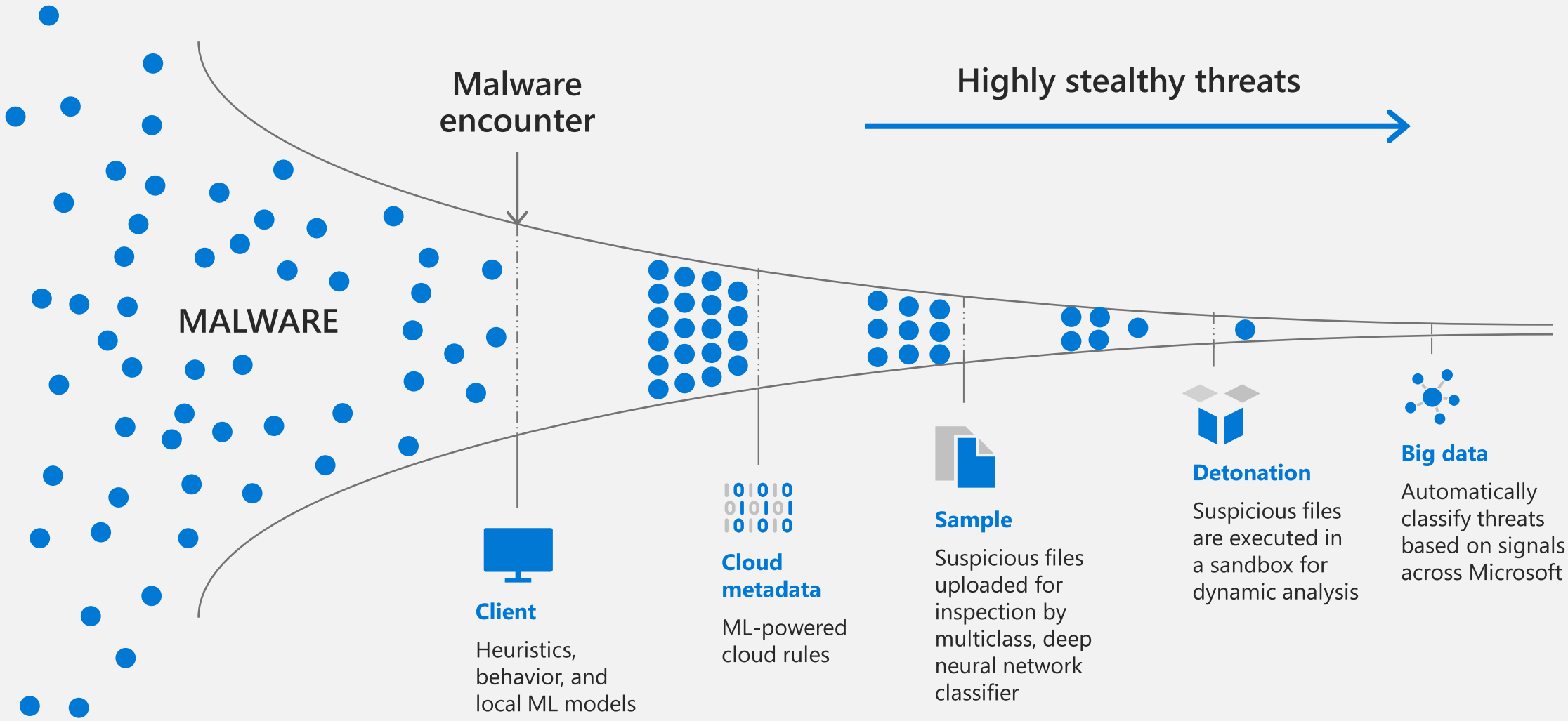


Innovations in Fileless Protection

- 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



Microsoft Defender for Endpoint's NGP protection pipeline



Dynamic: behavior monitoring

Monitors activity on:

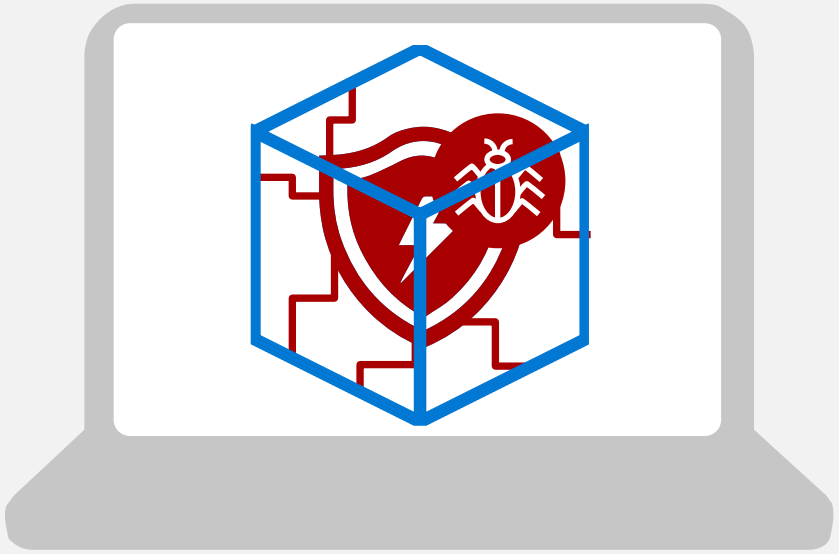
- Files
- Registry keys
- Processes
- Network (basic HTTP inspection)
- … and few other specific activities

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

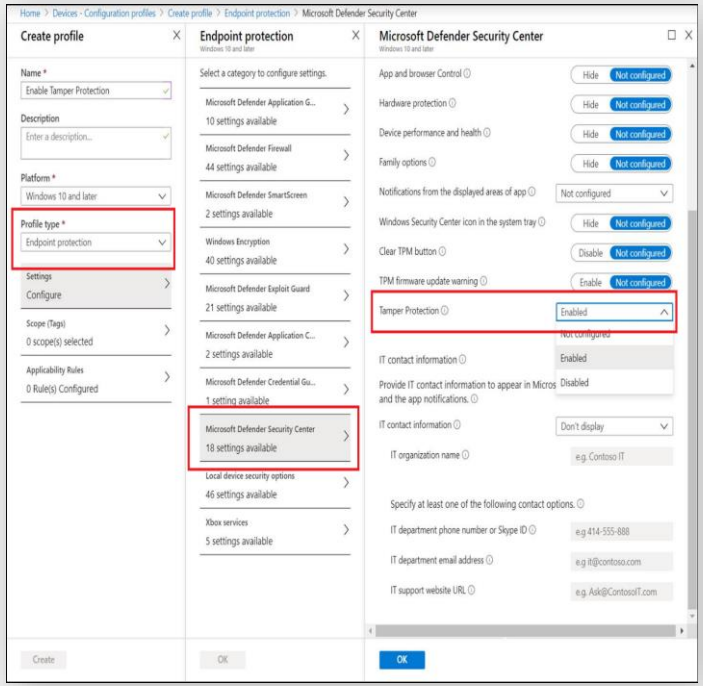


Now

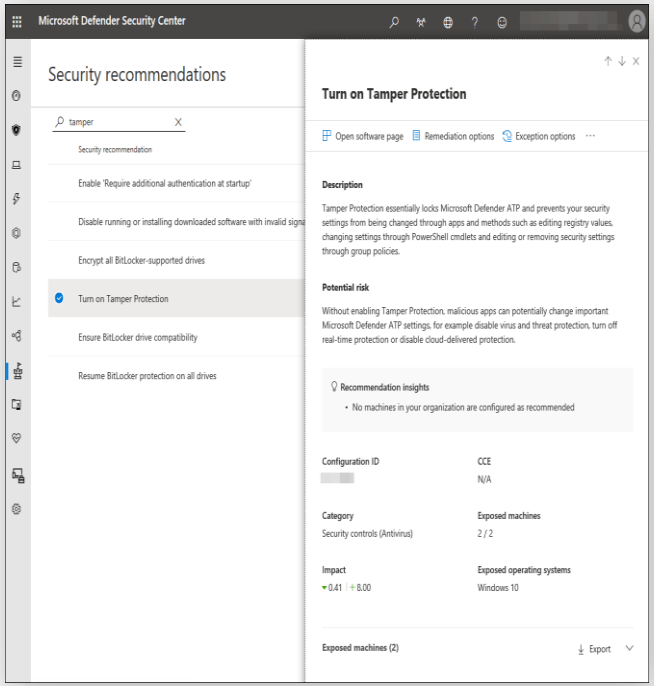
[Announcement blog]

Tamper Protection – Password-less, secure, e2e

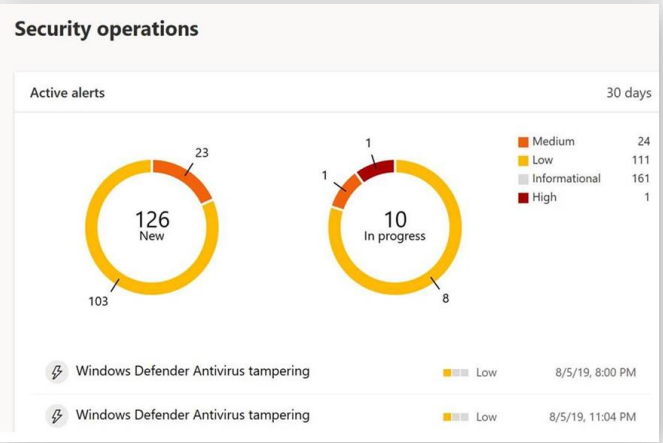
Seamless, secure and password less configuration



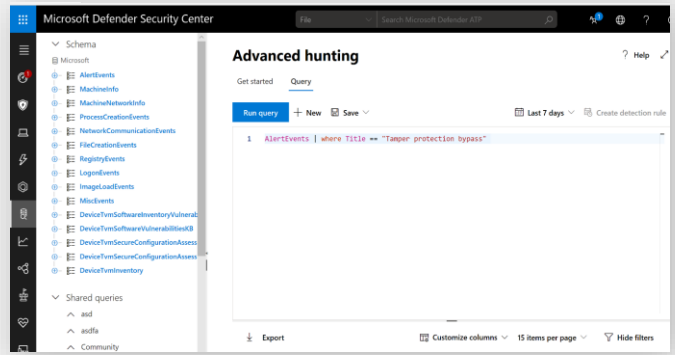
Threat & vulnerability management – Security recommendation



Tampering alert based on System Guard and EDR signals



Advanced Hunting



Read the blog for more details

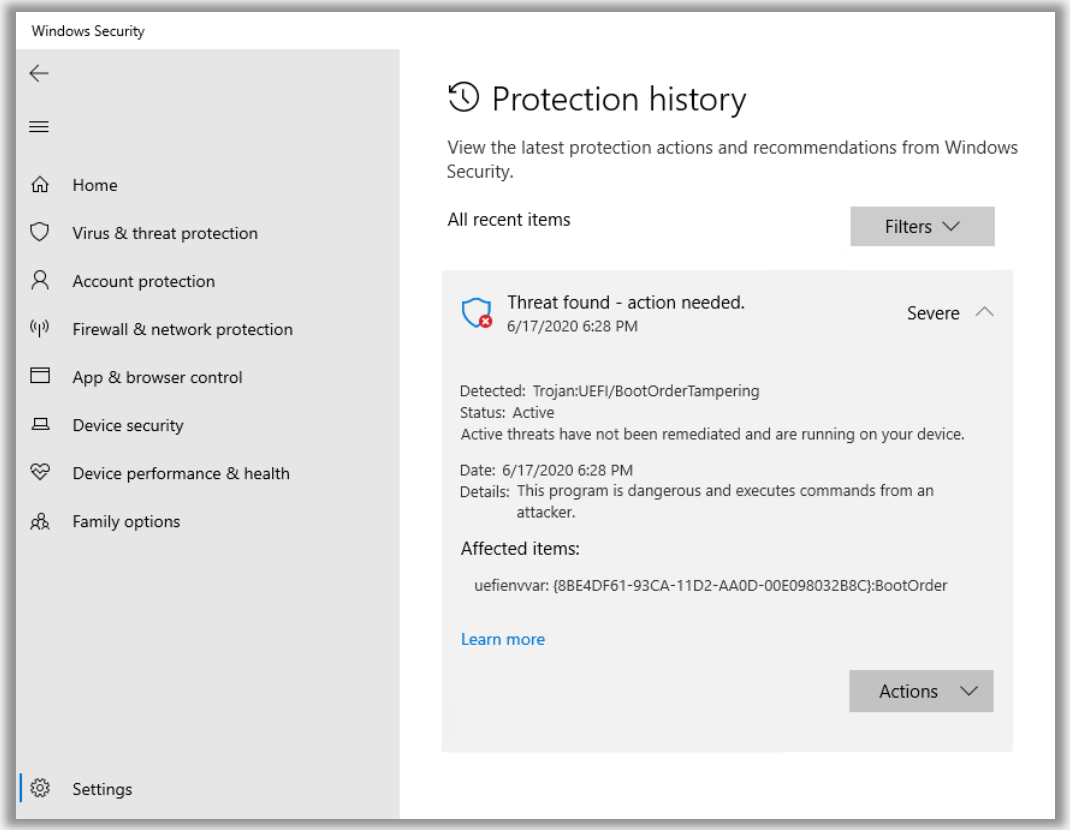
Firmware & hardware protections

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

Microsoft Defender Security Center

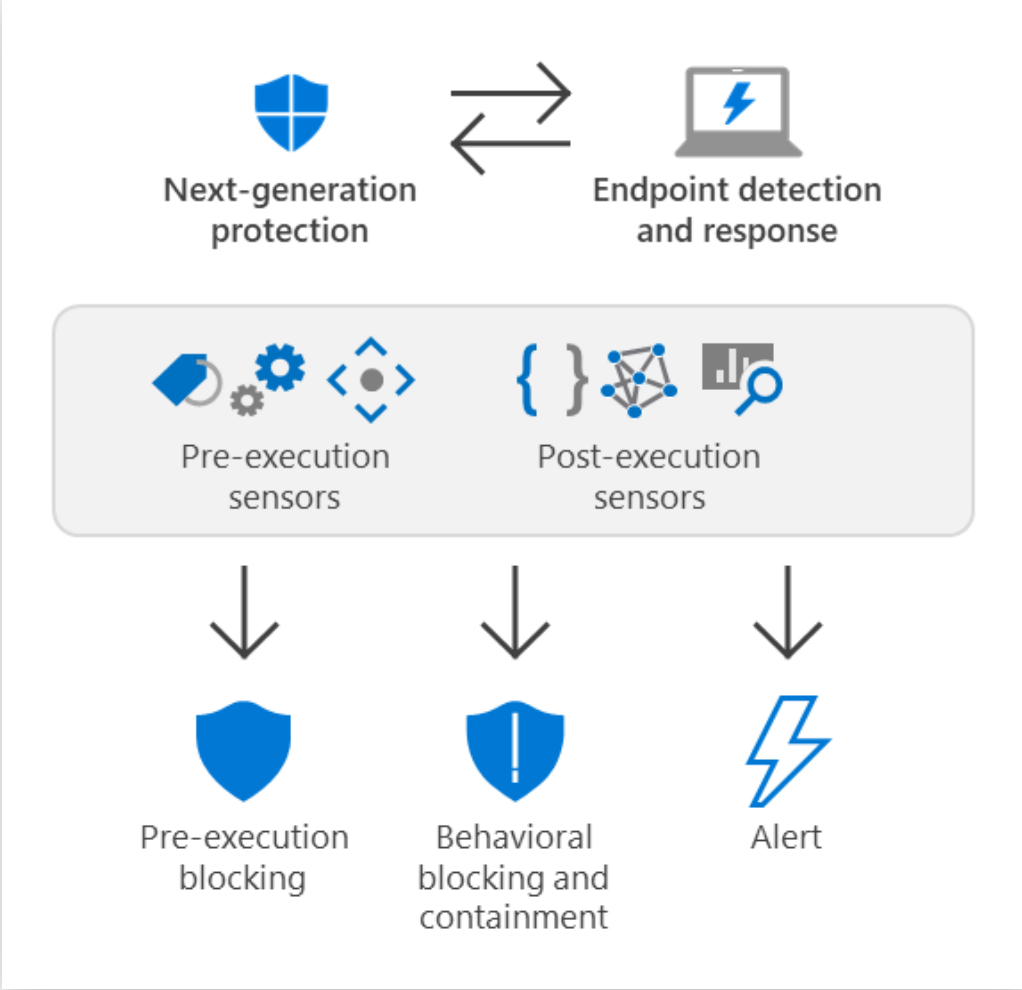
Scanning and detection



Read the blog for more details

Behavioral Blocking and Containment

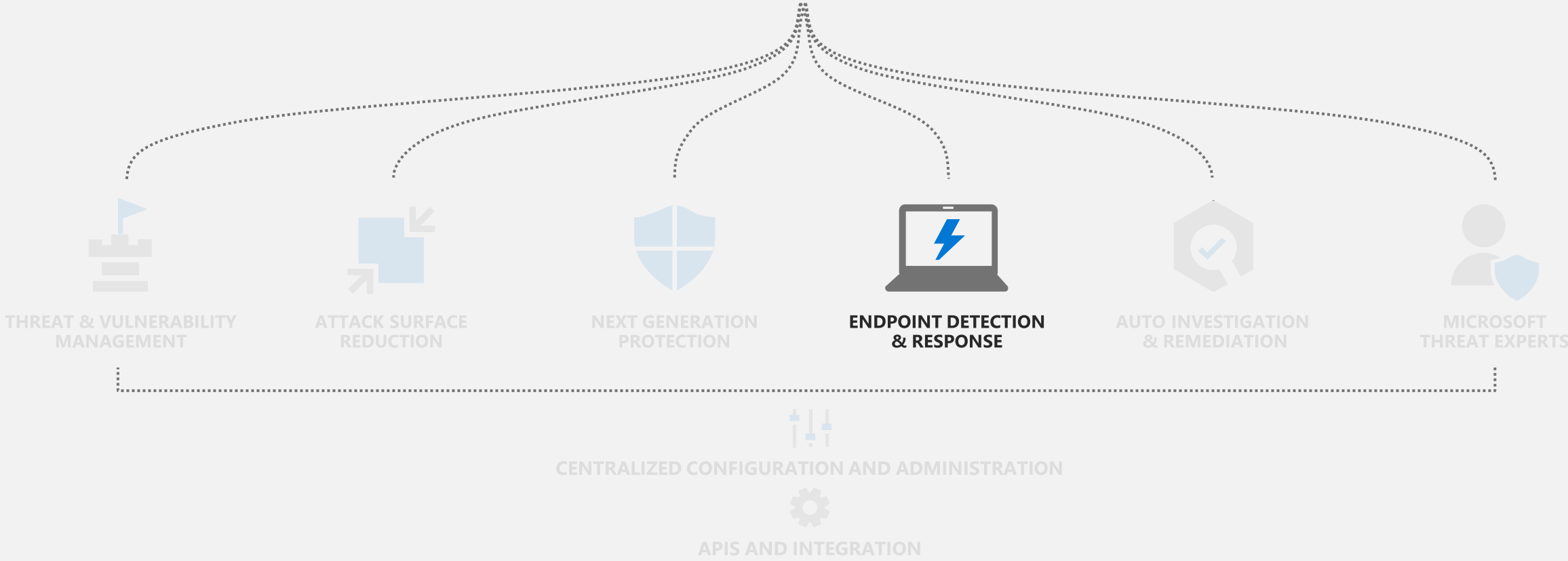
- Immediately stops threat before it can progress
- Microsoft has the unique ability to scan signals across kill chains and payloads (endpoints, Office, Identity, etc.)
- Some highlights:
  - Pre and Post breach AI- and ML- based behavioral blocking and containment
  - Detect malware after first sight 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

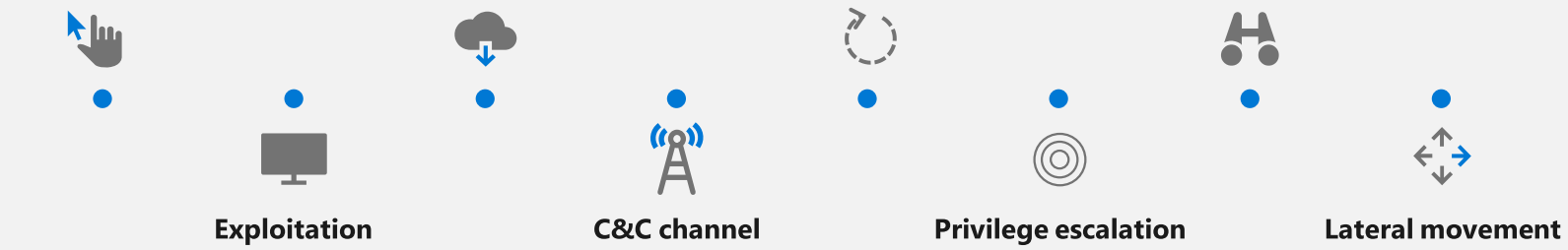
Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Key customer pain points

As attacks become more complex and multi-staged, it's difficult to make sense of the threats detected



46% of compromised systems had no malware on them

Following an advanced attack across the network and different sensors can be challenging

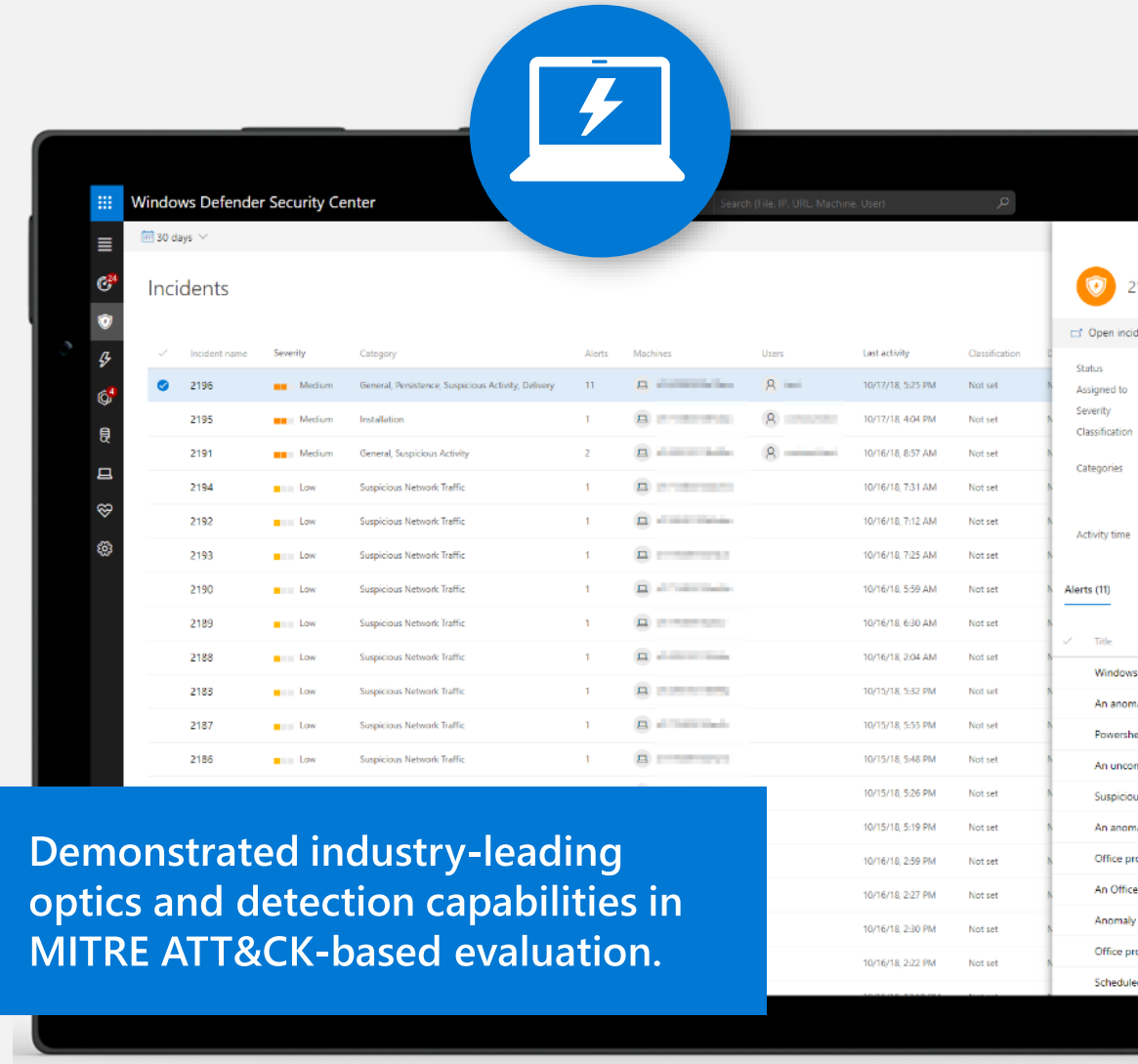
Collecting evidence and alerts, even from 1 infected device, can be a long time-consuming process

Living off the land - Attackers use evasion-techniques

Endpoint Detection & Response

Detect and investigate advanced persistent attacks

- Correlated behavioral alerts
- Investigation & hunting over 6 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 & Investigation

Understand what was alerted

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

Investigate device activity

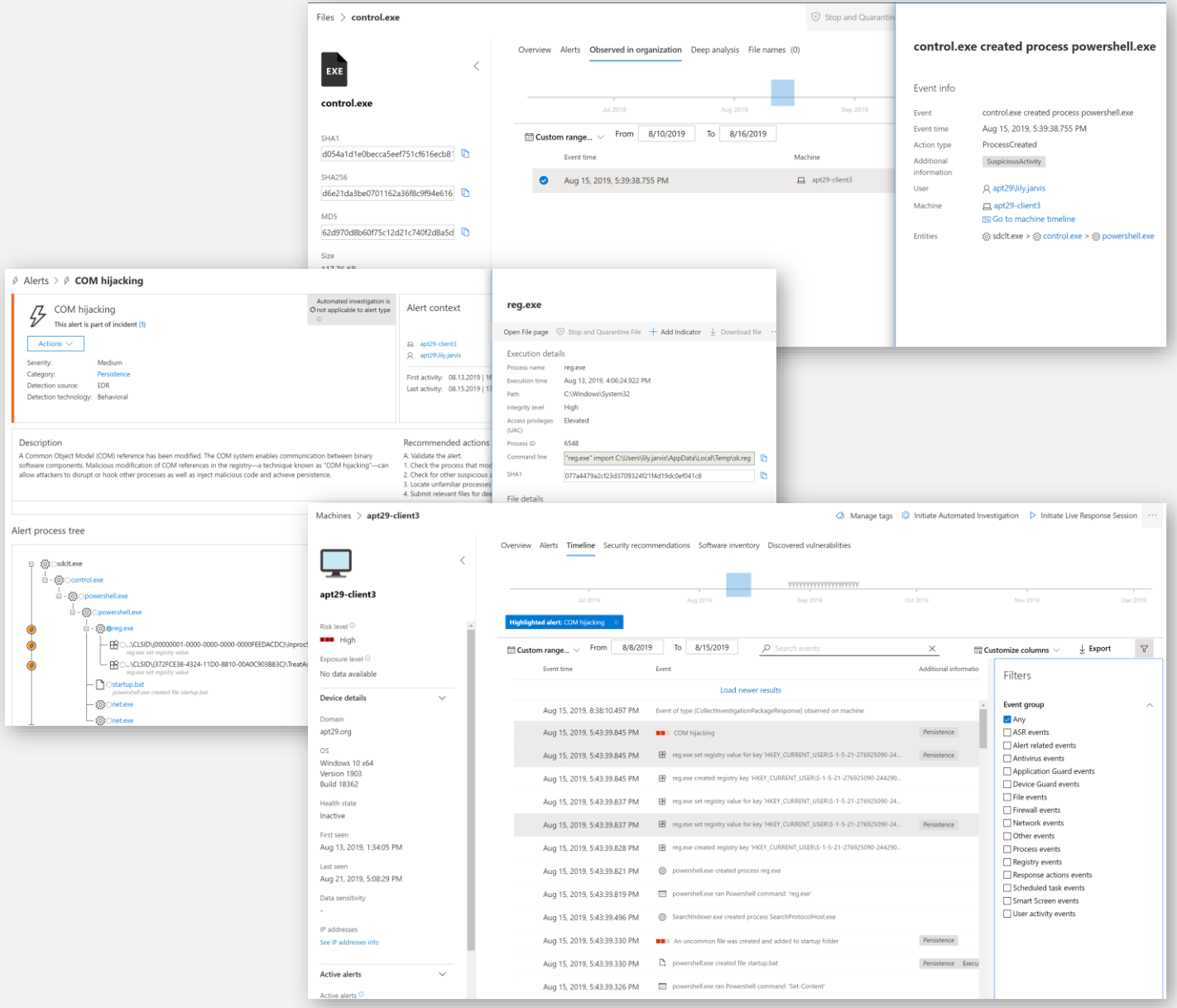
Full machine timeline to drill into activities, filter and search.

Rich supporting data & tools

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

Expand scope of breach

In-context pivoting to other affected machines/users.



Incident

Narrates the end-to-end attack story

Reconstructing the story

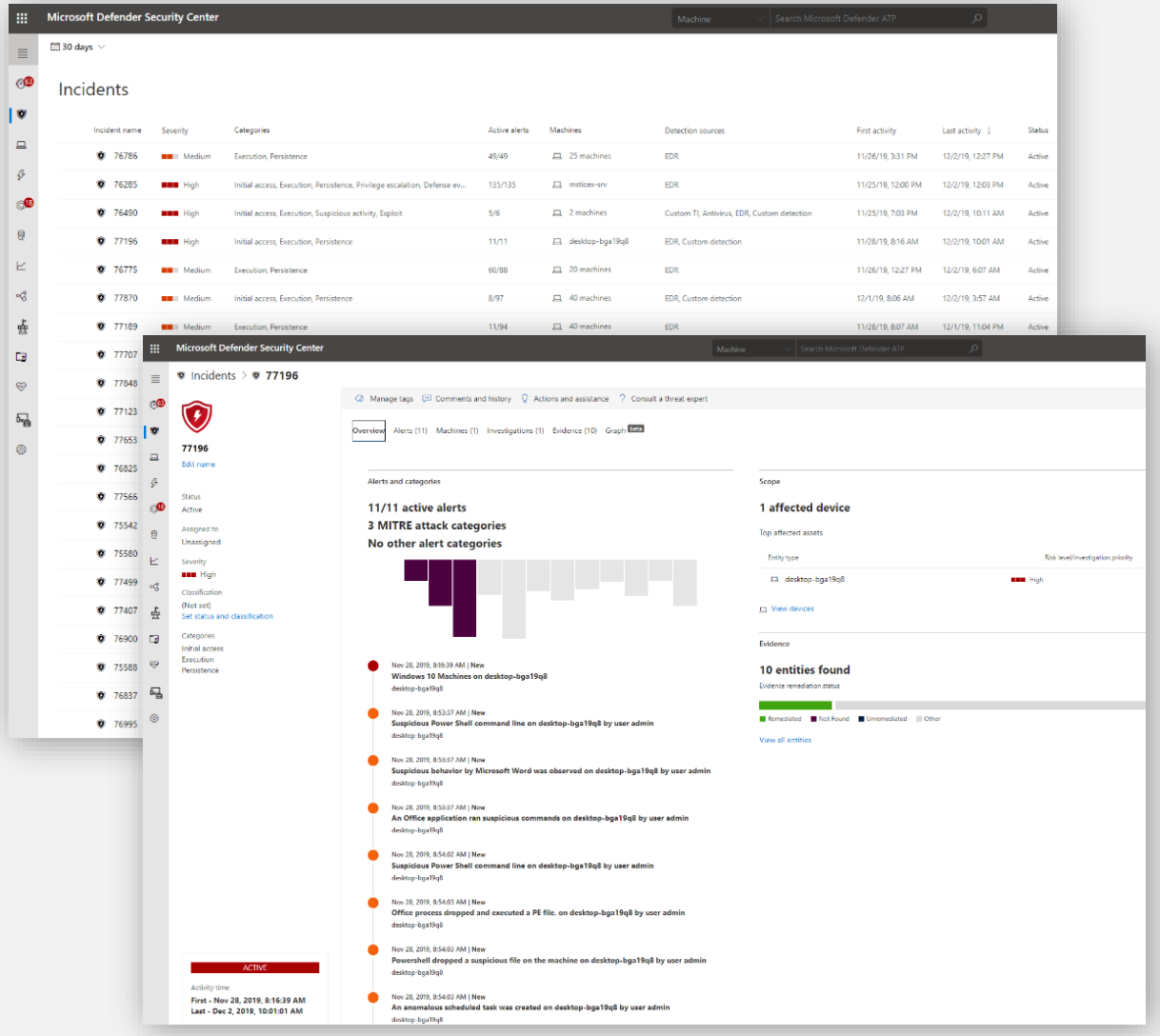
The broader attack story is better described when relevant alerts and related entities are brought together.

Incident scope

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

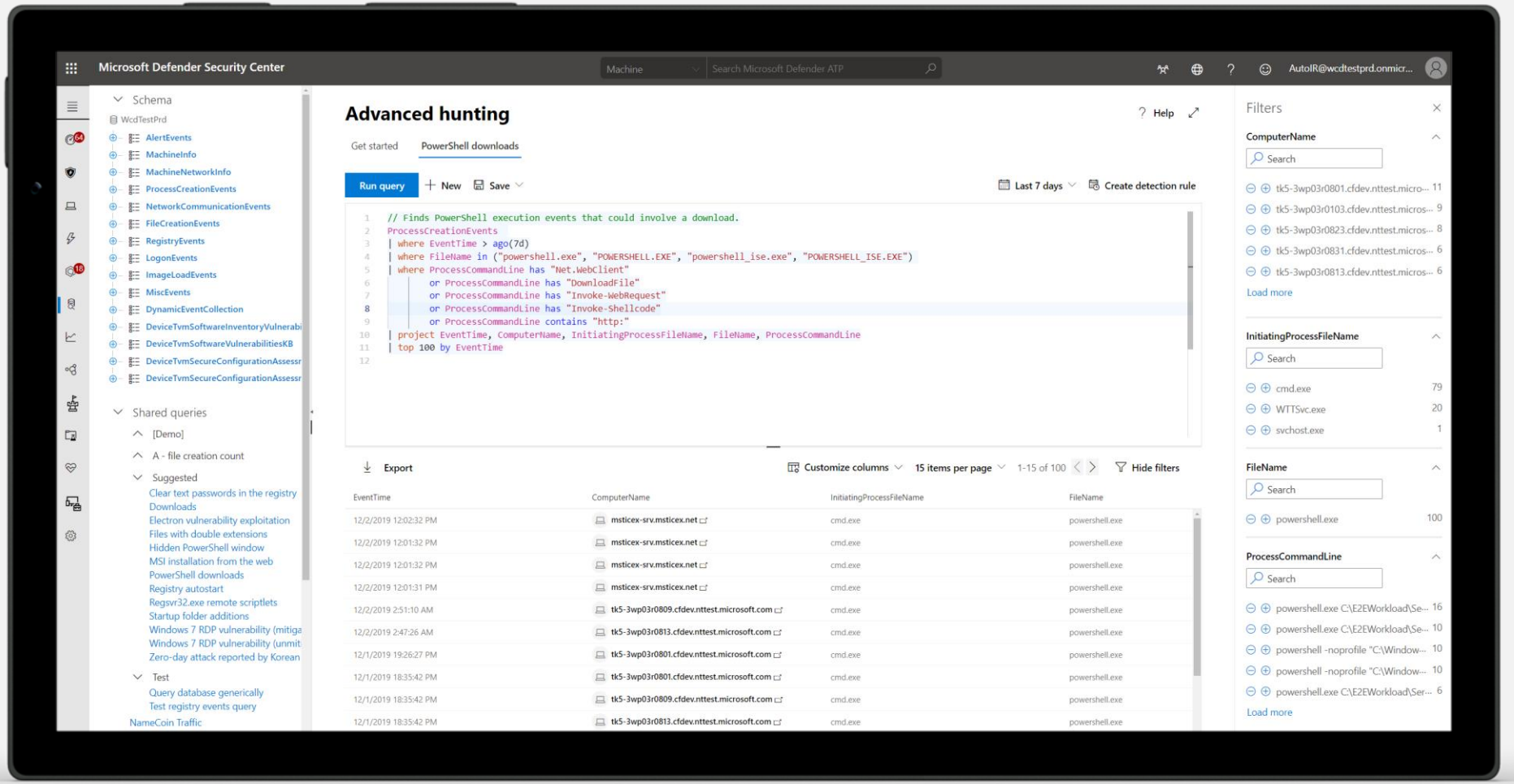
Higher fidelity, lower noise

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



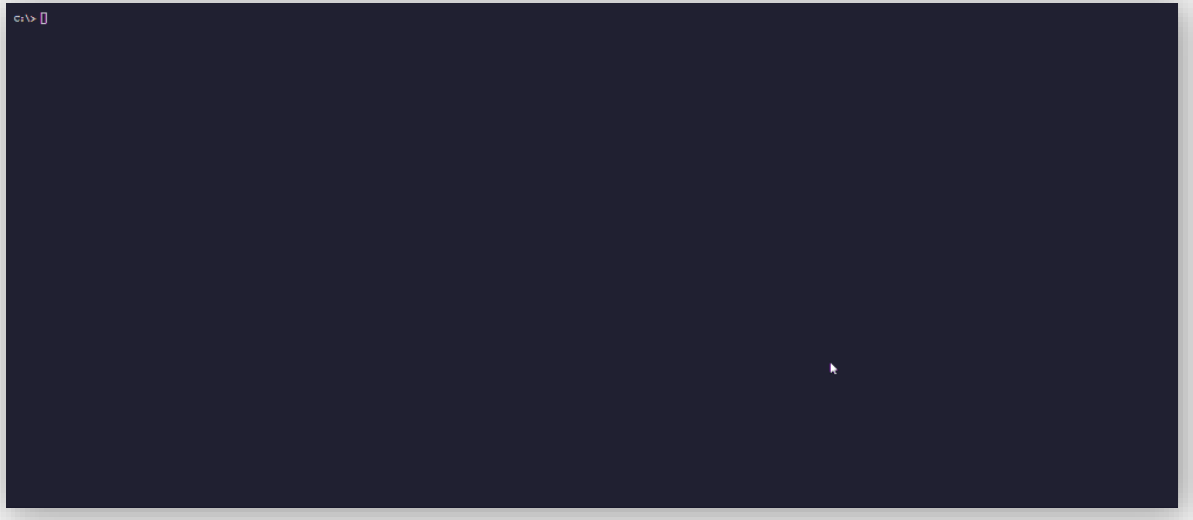
[Announcement blog]

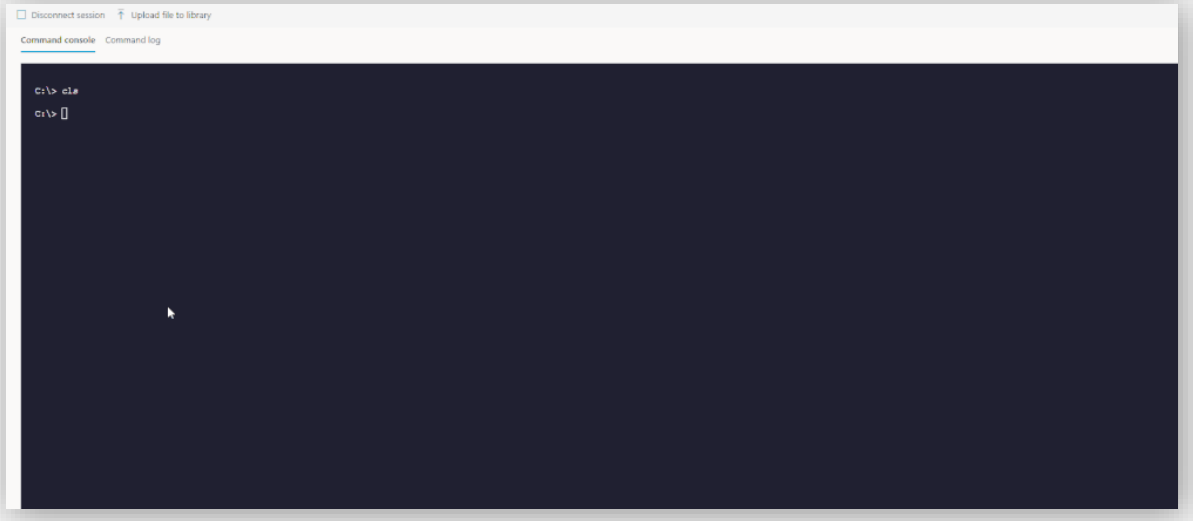
Advanced hunting with custom detection and custom response



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)





Threat Analytics

See how you do against major threats

Threat to posture view

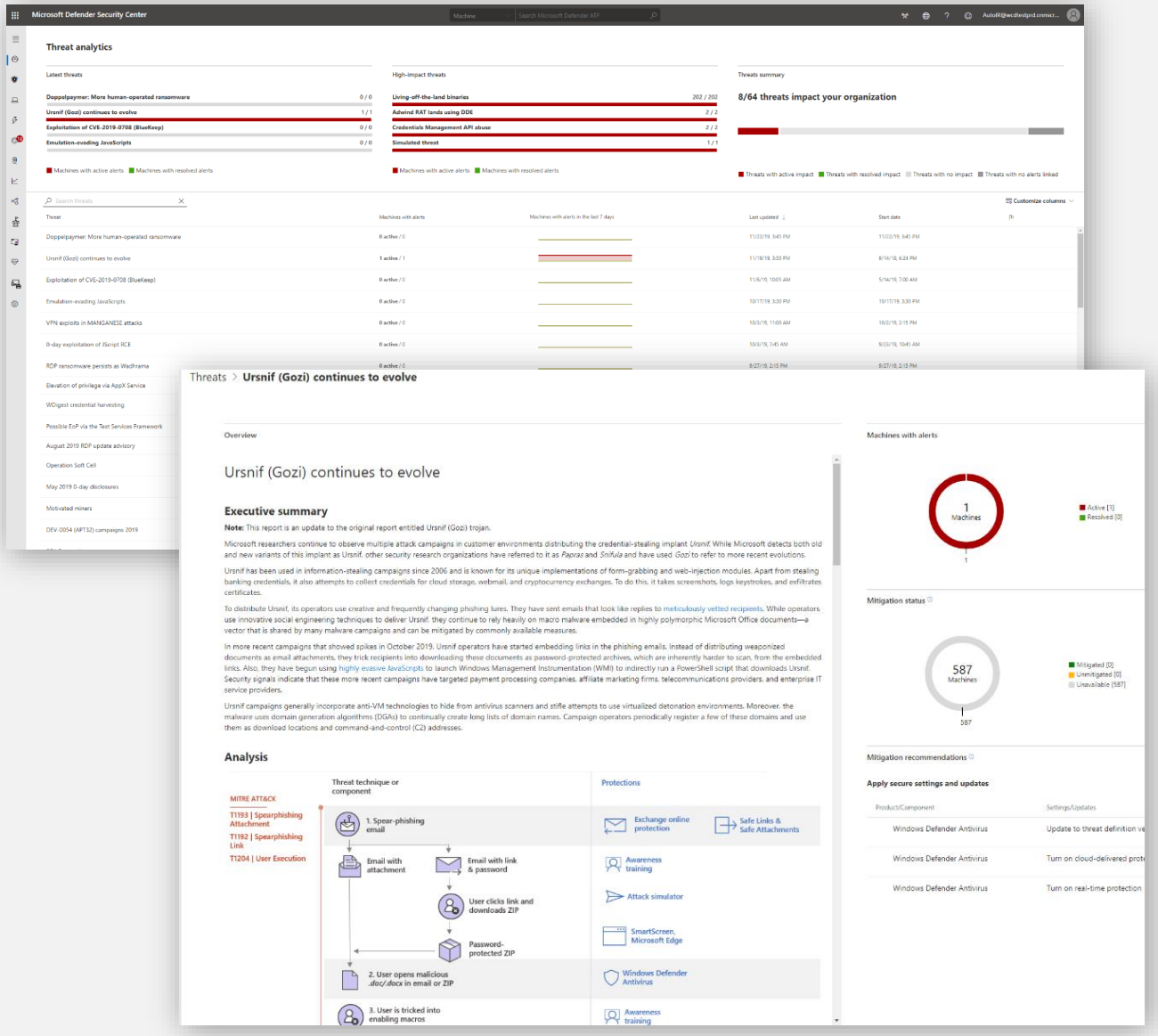
See how you score against significant and emerging campaigns with interactive reports.

Identify unprotected systems

Get real-time insights to assess the impact of the threat on your environment.

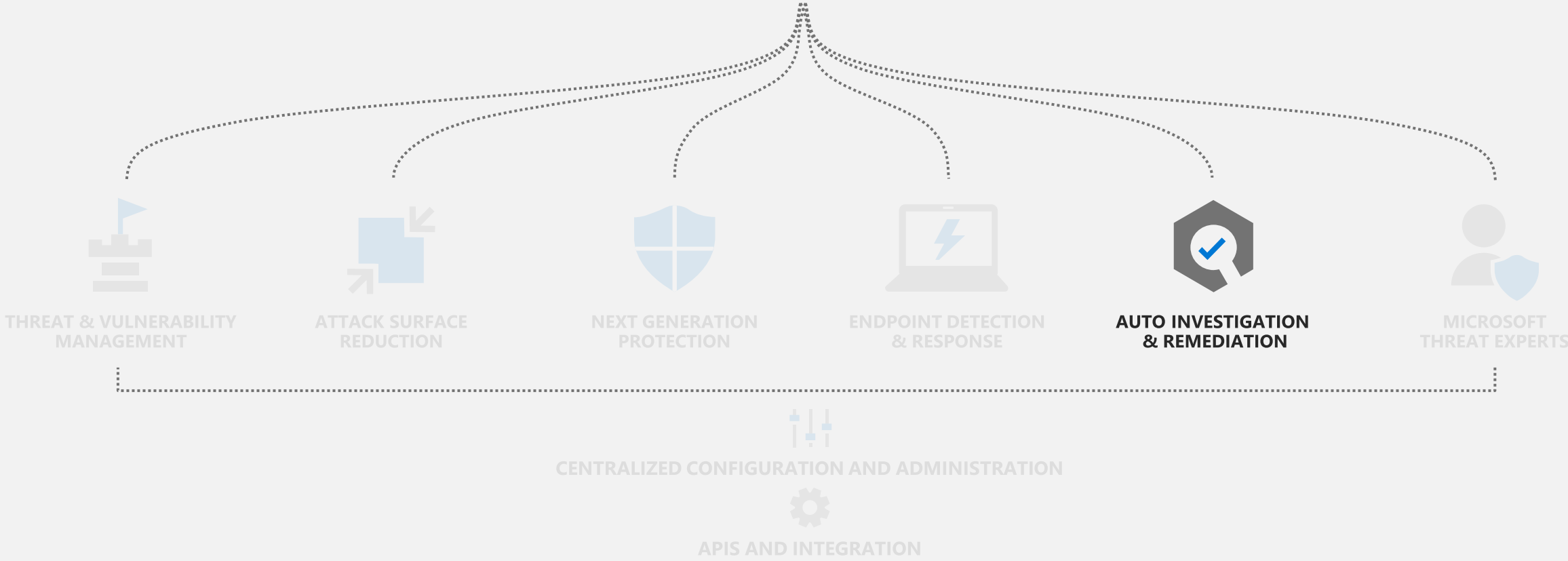
Get guidance

Provides recommended actions to increase security resilience, to prevention, or contain the threat.



Microsoft Defender for Endpoint

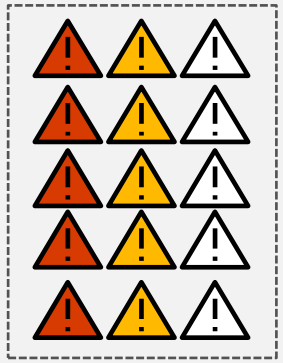
Built-in. Cloud-powered.



Key customer pain points

- More threats, more alerts leads to analyst fatigue
- Alert investigation is time-consuming
- Expertise is expensive
- Manual remediation requires time
- Talent shortage in cybersecurity

Analysts overwhelmed by manual alert investigation & remediation




Analyst 1


Analyst 2

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

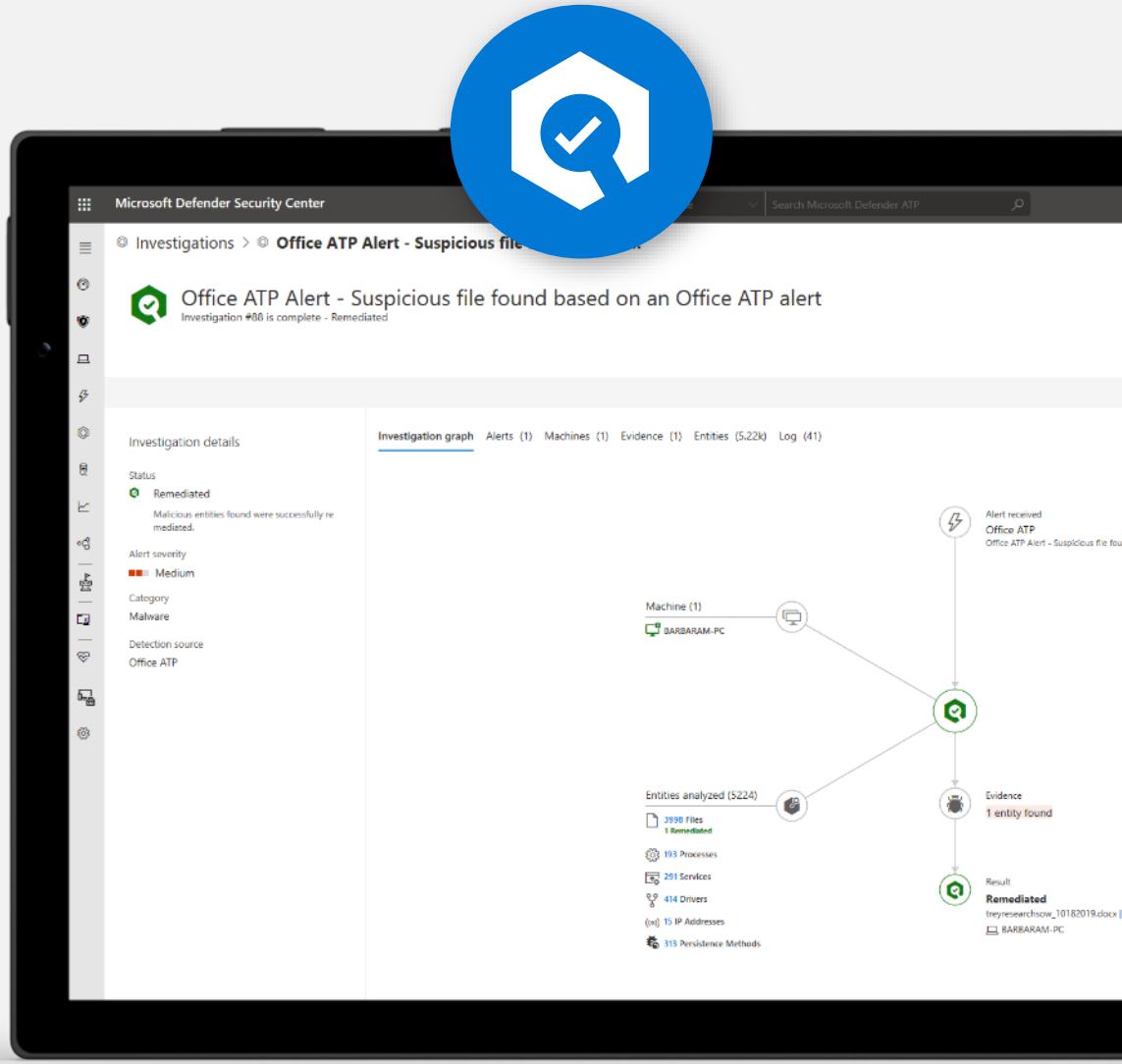
When we look at the steps an analyst is taking as when investigating and remediating threats we can identify the following high-level steps:

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 ☺

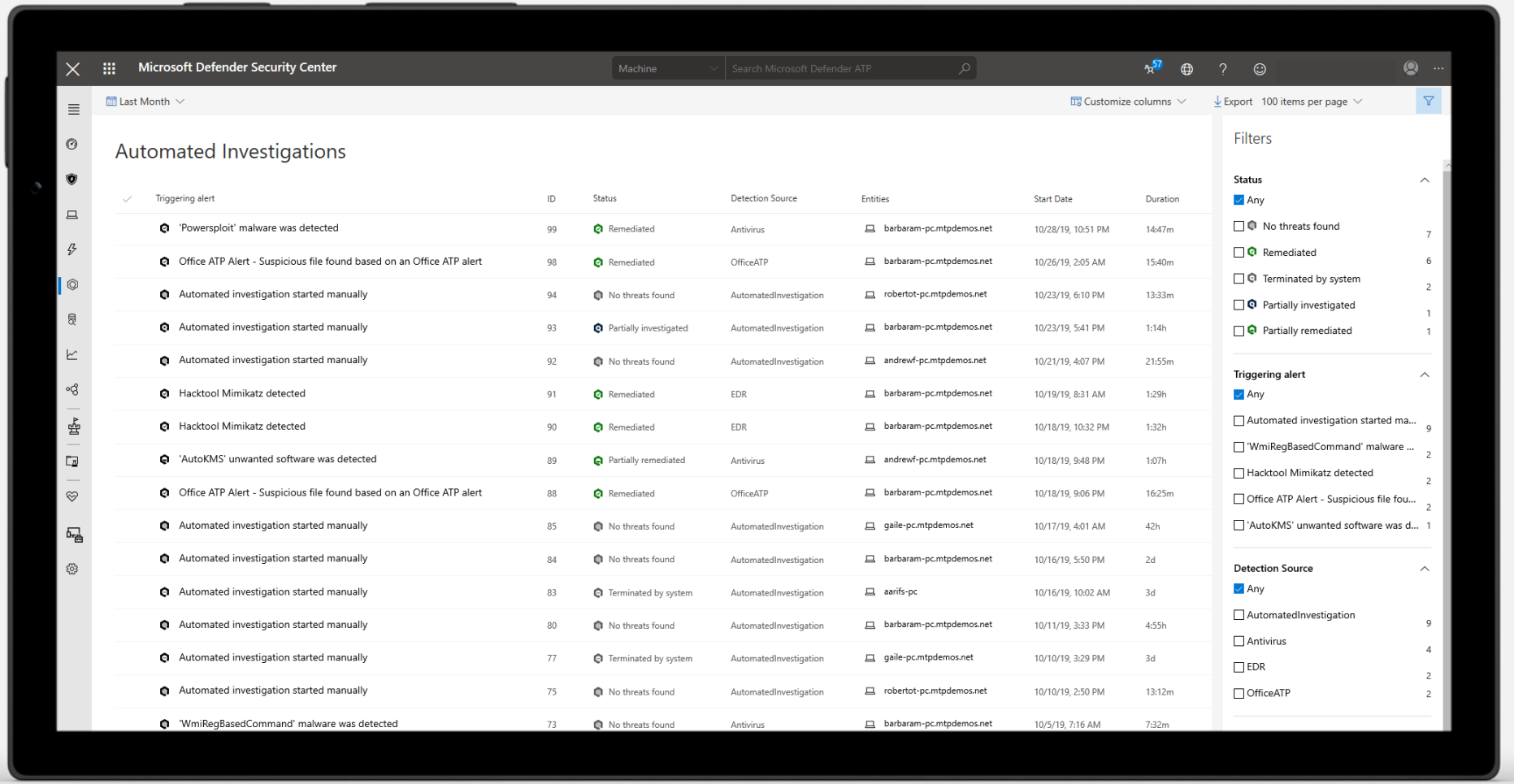
Auto Investigation & Remediation

Automatically investigates alerts and remediates complex threats in minutes

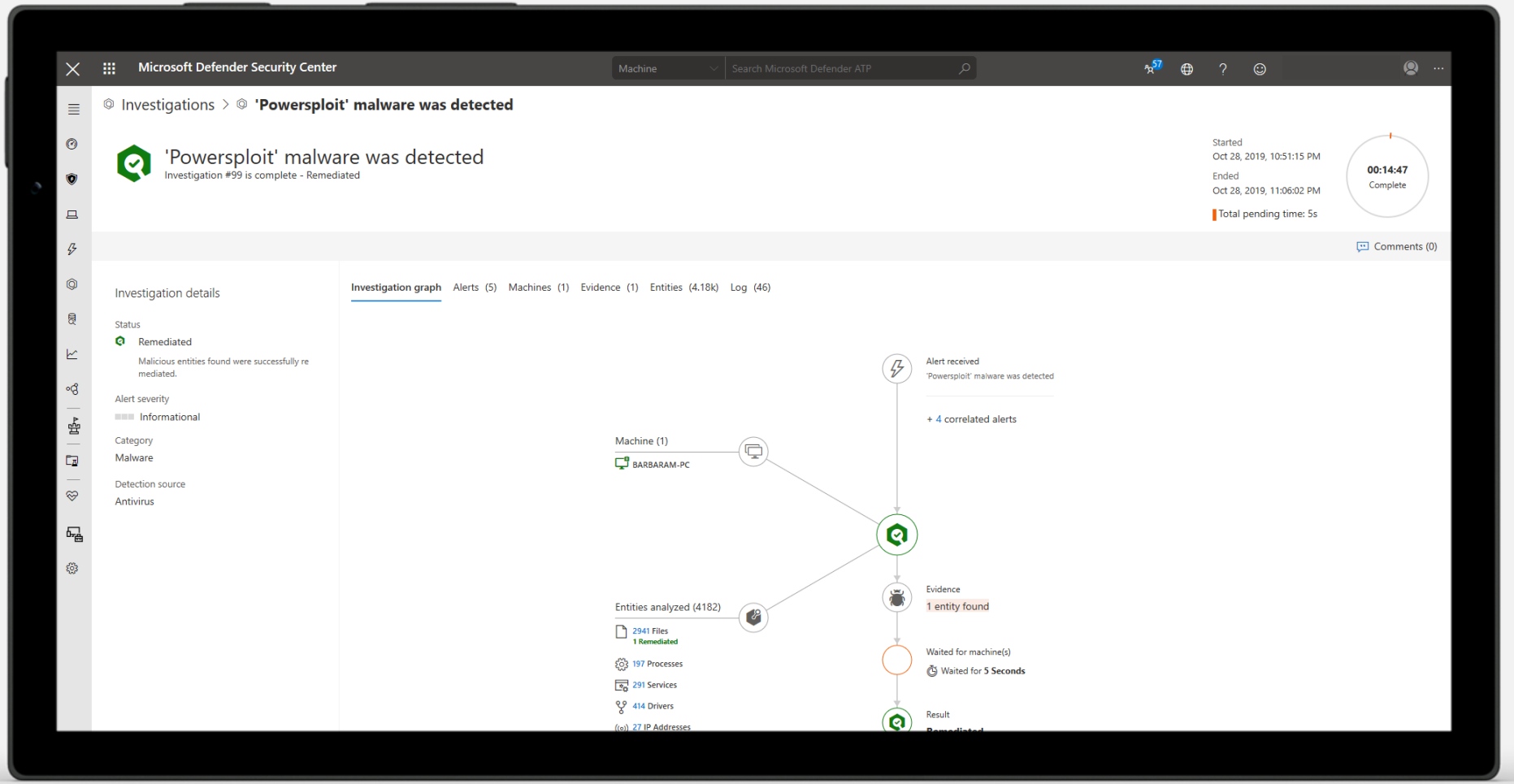
- Mimics the ideal steps analysts would take
- Tackles file or memory-based attacks
- Works 24x7, with unlimited capacity



Auto investigation queue

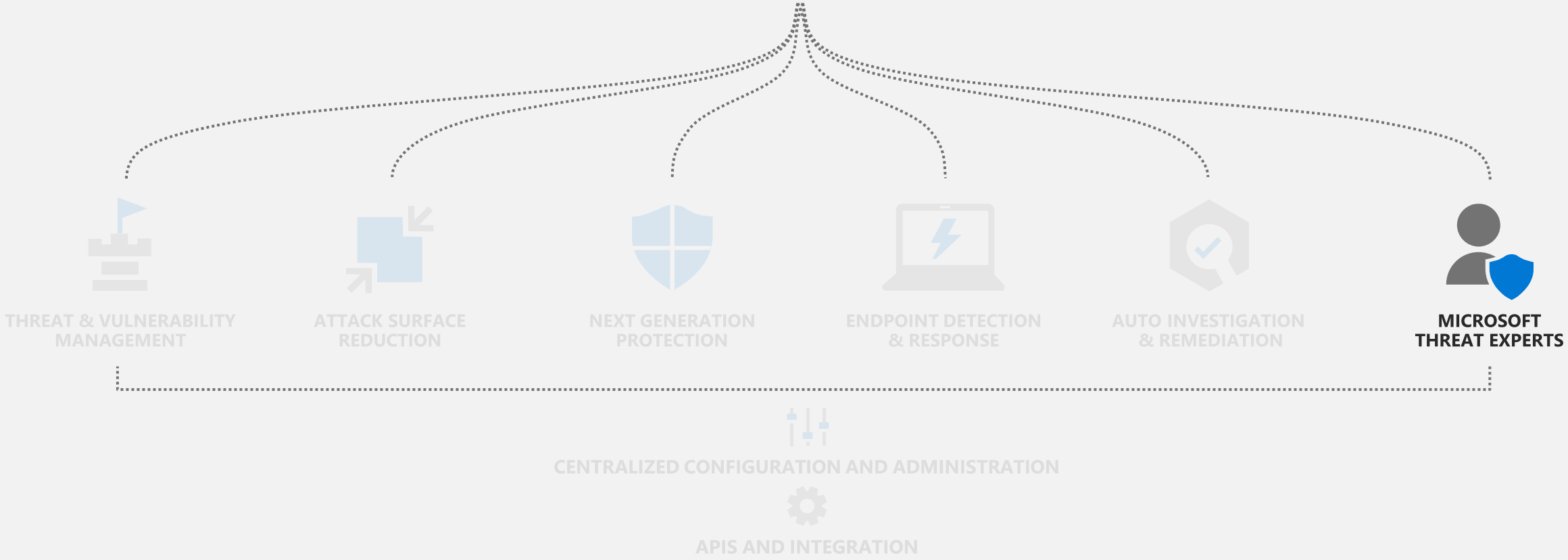


Investigation graph



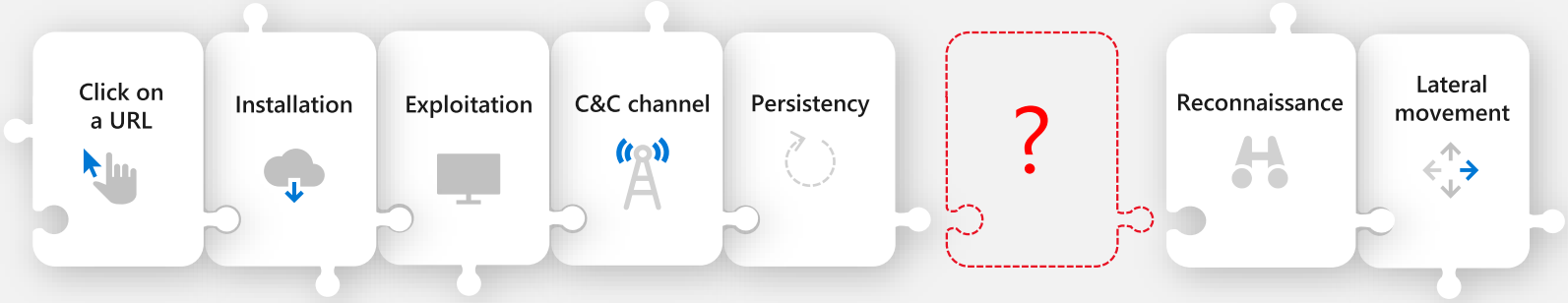
Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Key customer pain points

As threats are becoming complex,
I could 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?

Managed Threat Hunting service

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

Don’t miss the breach

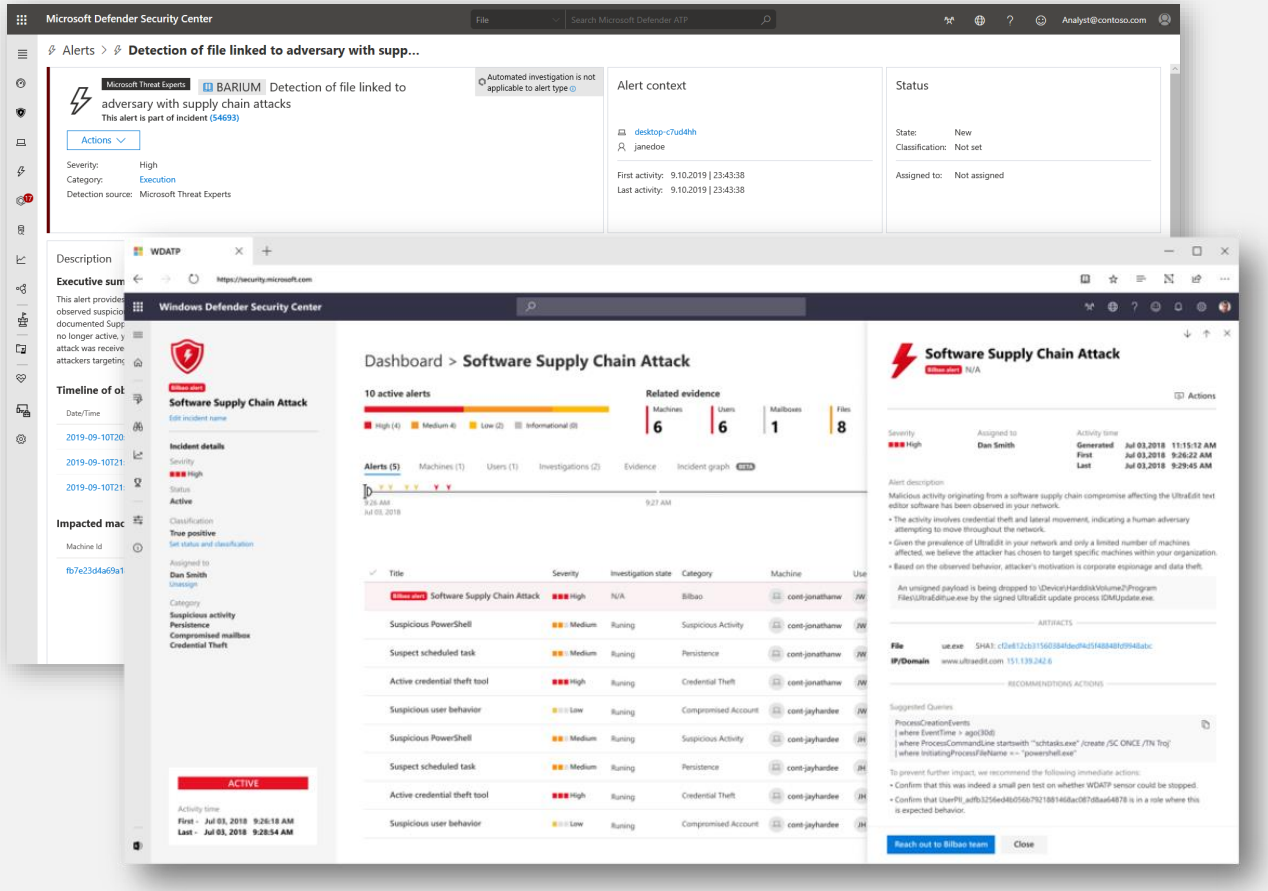
Threat hunters have your back.

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

Experts on demand

World-class expertise at your fingertips.

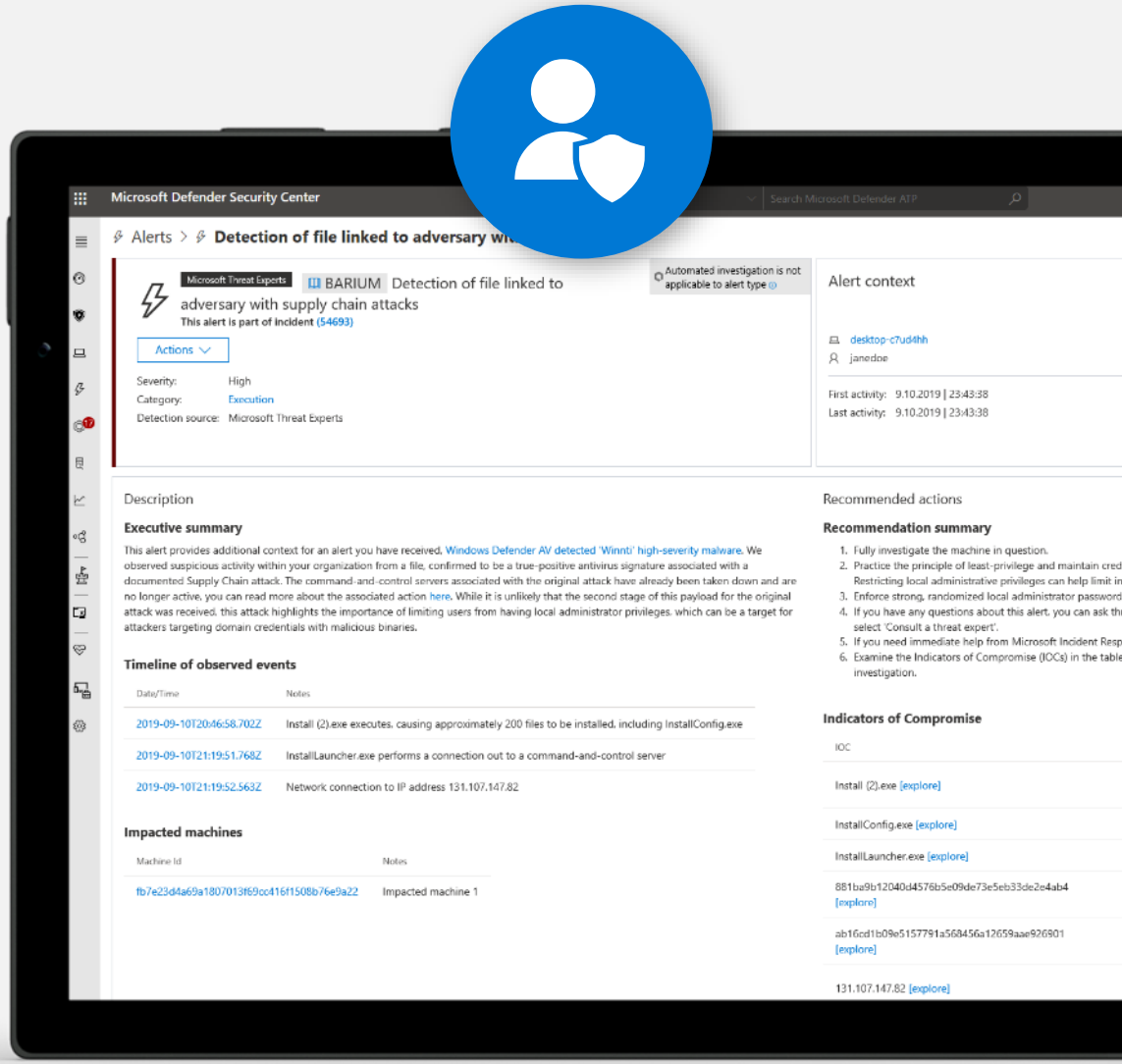
Got questions about alert, malware, or threat context? Ask a seasoned Microsoft Threat Expert.



Microsoft Threat Experts

Brings 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



Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Execution
Detection source: Microsoft Threat Experts

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 23:43:38

Status

State: New
Classification: Not set

Assigned to: Not assigned

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. Avoid the use of domain-wide, admin-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
3. Enforce strong, randomized local administrator passwords. Use tools like LAPS.
4. If you have any questions about this alert, you can ask through Experts-on-Demand! From this alert page click the Actions menu and select 'Consult a threat expert'.
5. If you need immediate help from Microsoft Incident Response consider opening a Premier support case.
6. Examine the Indicators of Compromise (IOCs) in the table below, and use the suggested Advanced Hunting queries to continue your investigation.

Indicators of Compromise

IOC	Type	Notes
Install (2).exe [explore]	filename	File used to install numerous files, including the true-positive InstallConfig.exe
InstallConfig.exe [explore]	filename	True-positive malicious file
InstallLauncher.exe [explore]	filename	File performing network connection to command-and-control
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 [explore]	hash	SHA1 for Backdoor:Win32/Winnti.X!dha, labelled as InstallConfig.exe
ab16cd1b09e5157791a568456a12659aae926901 [explore]	hash	SHA1 for file labelled as InstallLauncher.exe
131.107.147.82 [explore]	ip	Command-and-control server launched from InstallLauncher.exe

Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Execution
Detection source: Microsoft Threat Experts

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 23:43:38

Status

State: New
Classification: Not set

Assigned to: Not assigned

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. Avoid the use of domain-wide, admin-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
3. Enforce strong, randomized local administrator passwords. Use tools like LAPS.
4. If you have any questions about this alert, you can ask through Experts-on-Demand! From this alert page click the Actions menu and select 'Consult a threat expert'.
5. If you need immediate help from Microsoft Incident Response consider opening a Premier support case.
6. Examine the Indicators of Compromise (IOCs) in the table below, and use the suggested Advanced Hunting queries to continue your investigation.

Indicators of Compromise

IOC	Type	Notes
Install (2).exe [explore]	filename	File used to install numerous files, including the true-positive InstallConfig.exe
InstallConfig.exe [explore]	filename	True-positive malicious file
InstallLauncher.exe [explore]	filename	File performing network connection to command-and-control
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 [explore]	hash	SHA1 for Backdoor:Win32/Winnti.X!dha, labelled as InstallConfig.exe
ab16cd1b09e5157791a568456a12659aae926901 [explore]	hash	SHA1 for file labelled as InstallLauncher.exe
131.107.147.82 [explore]	ip	Command-and-control server launched from InstallLauncher.exe

Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

- Manage alert
- View machine timeline
- Open incident page
- Print alert
- Consult a threat expert

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 23:43:38

Status

State: New
Classification: Not set

Assigned to: Not assigned

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. Avoid the use of domain-wide, admin-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
3. Enforce strong, randomized local administrator passwords. Use tools like LAPS.
4. If you have any questions about this alert, you can ask through Experts-on-Demand! From this alert page click the Actions menu and select 'Consult a threat expert'.
5. If you need immediate help from Microsoft Incident Response consider opening a Premier support case.
6. Examine the Indicators of Compromise (IOCs) in the table below, and use the suggested Advanced Hunting queries to continue your investigation.

Indicators of Compromise

IOC	Type	Notes
Install (2).exe [explore]	filename	File used to install numerous files, including the true-positive InstallConfig.exe
InstallConfig.exe [explore]	filename	True-positive malicious file
InstallLauncher.exe [explore]	filename	File performing network connection to command-and-control
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 [explore]	hash	SHA1 for Backdoor:Win32/Winnti.X!dha, labelled as InstallConfig.exe
ab16cd1b09e5157791a568456a12659aae926901 [explore]	hash	SHA1 for file labelled as InstallLauncher.exe
131.107.147.82 [explore]	ip	Command-and-control server launched from InstallLauncher.exe

Alerts > **Detection of file linked to adversary with supp...**

Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Execution
Detection source: Microsoft Threat Experts

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 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 questio
2. Practice the principle of least-privilege a
   Restricting local administrative privileges
3. Enforce strong, randomized local admini
4. If you have any questions about this aler
   select 'Consult a threat expert'.
5. If you need immediate help from Micros
6. Examine the Indicators of Compromise (
   investigation.

Indicators of Compromise

IOC
Install (2).exe [explore]
InstallConfig.exe [explore]
InstallLauncher.exe [explore]
881ba9b12040d4576b5e09de73e5eb33de2e [explore]
ab16cd1b09e5157791a568456a12659aae92 [explore]
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

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

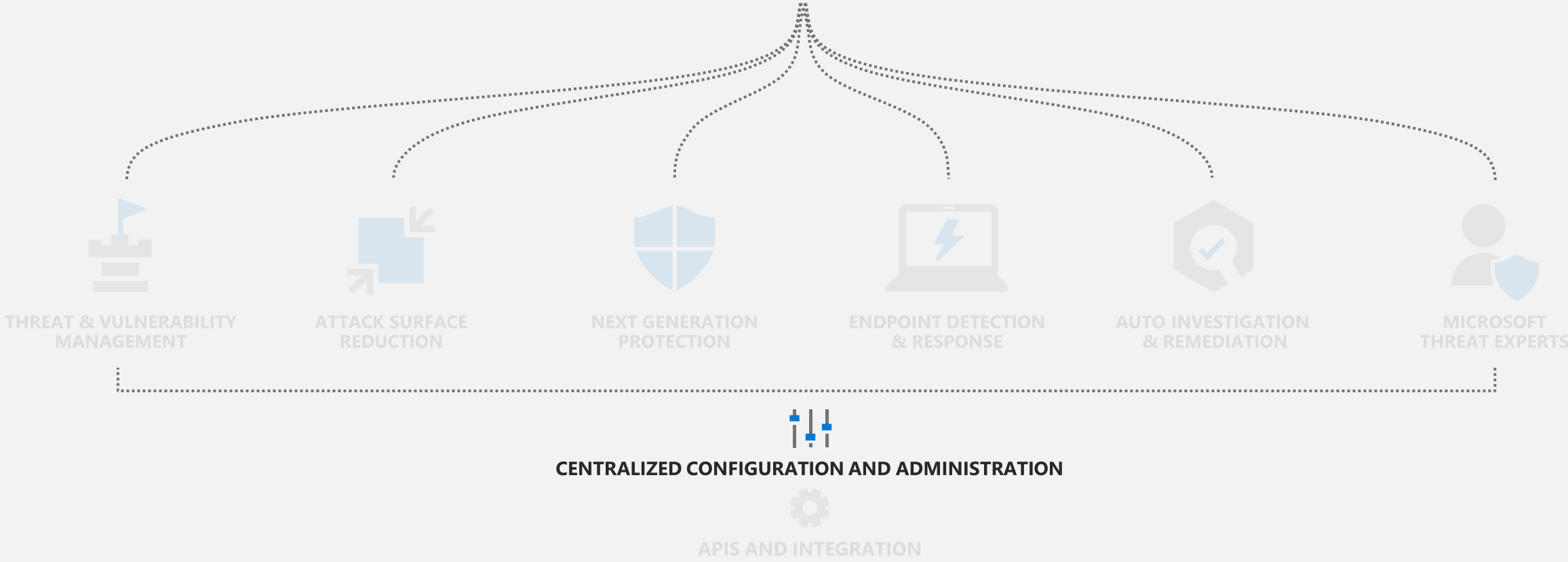
Analyst@contoso.com

Submit

Privacy statement.

Microsoft Defender
for Endpoint

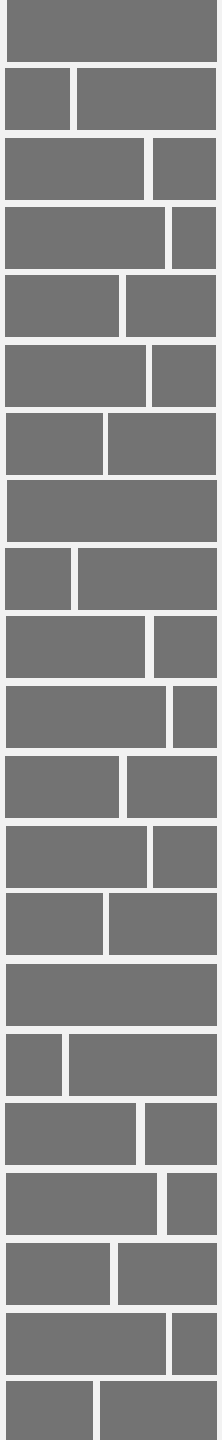
Built-in. Cloud-powered.



Historical roles & 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

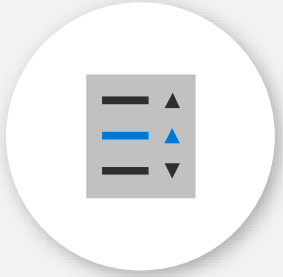


IT Team

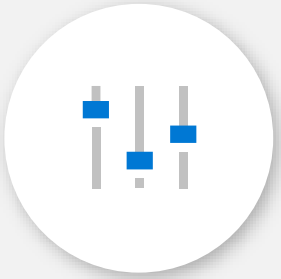
- Responsible for policy configuration including security policies
- Analyzes change impact and stages rollout of global policies
- Priority is a stable IT environment and low costs

Customer needs

Simple, cross-platform, unified endpoint security management console



Intuitive, advanced policy management capabilities



Security controls granularity and completeness

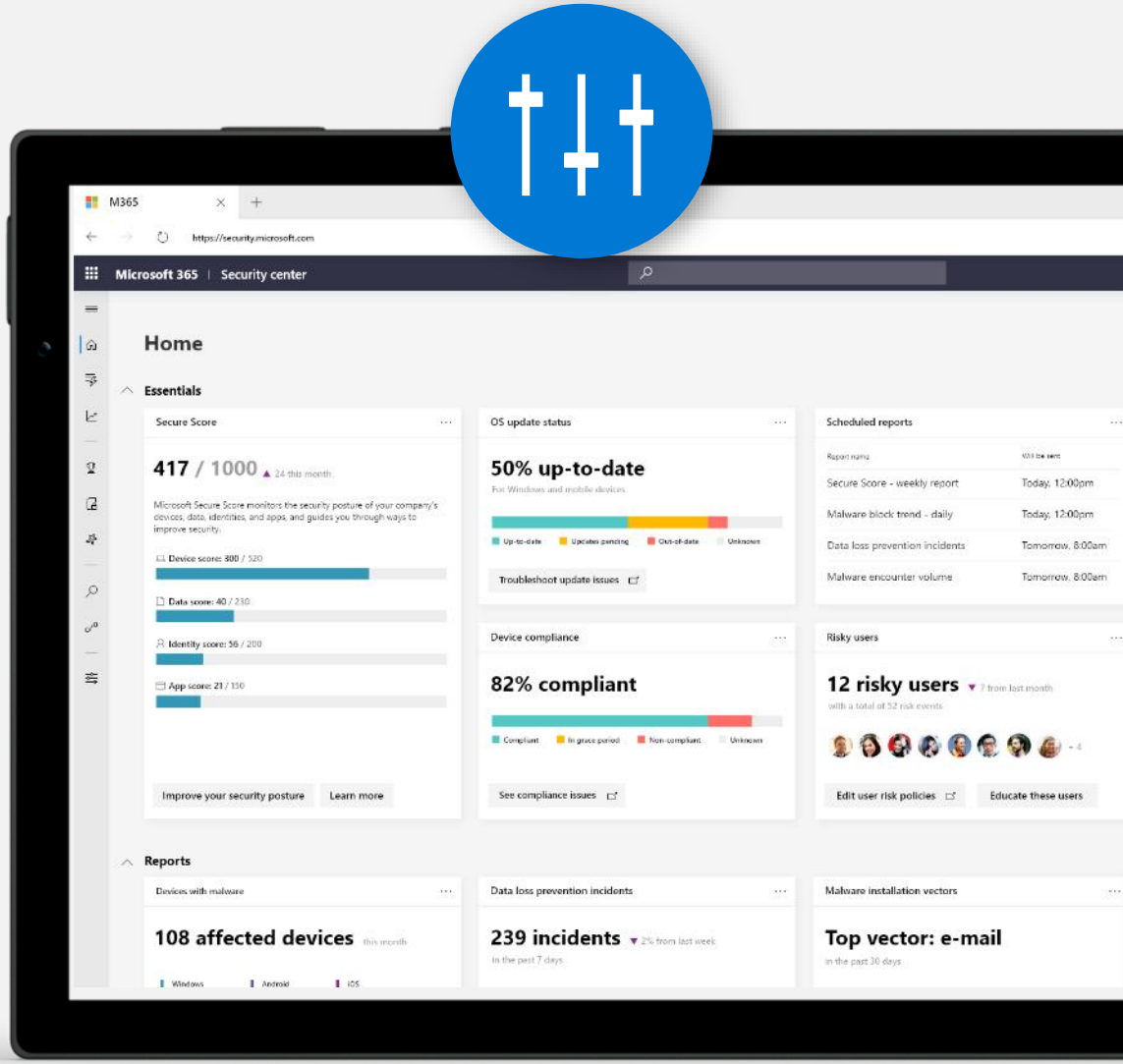
Continuous assessment and reporting of endpoint state

Seamless and frictionless

Security Management

Assess, configure and respond to changes in your environment

- Centrally asses & configure your security
- Variety of reports and dashboards for detailed monitoring and visibility
- Seamless integration between policy assessment and policy enforcement



Endpoint Security Management

All devices

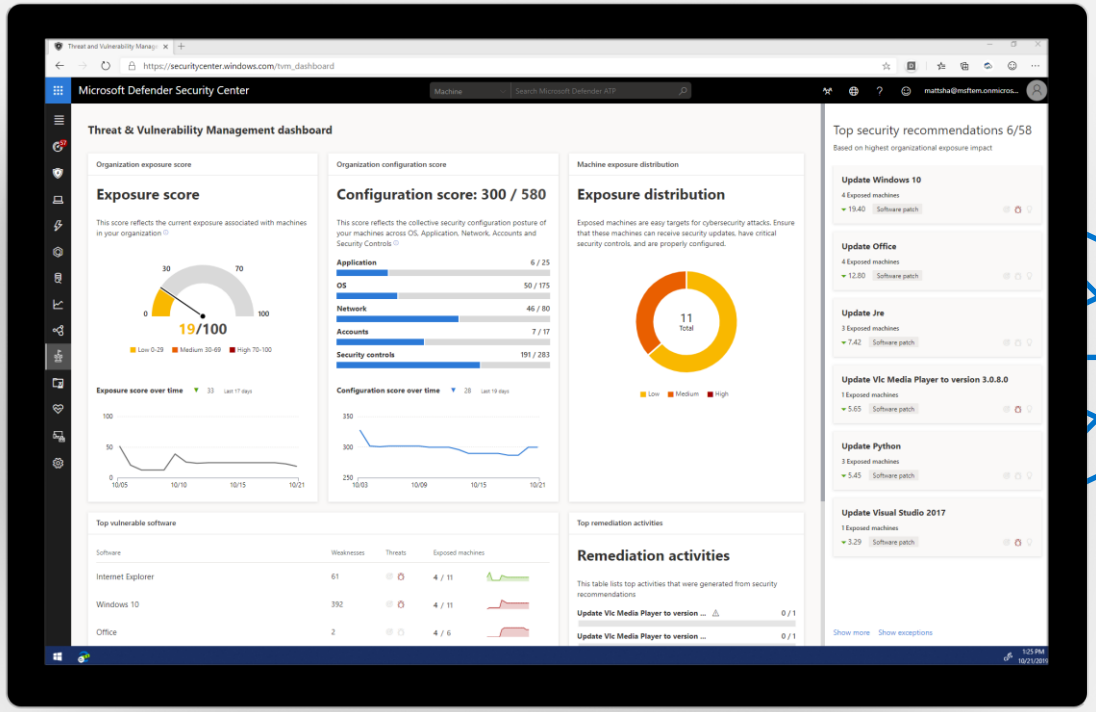
Sec Admin experiences

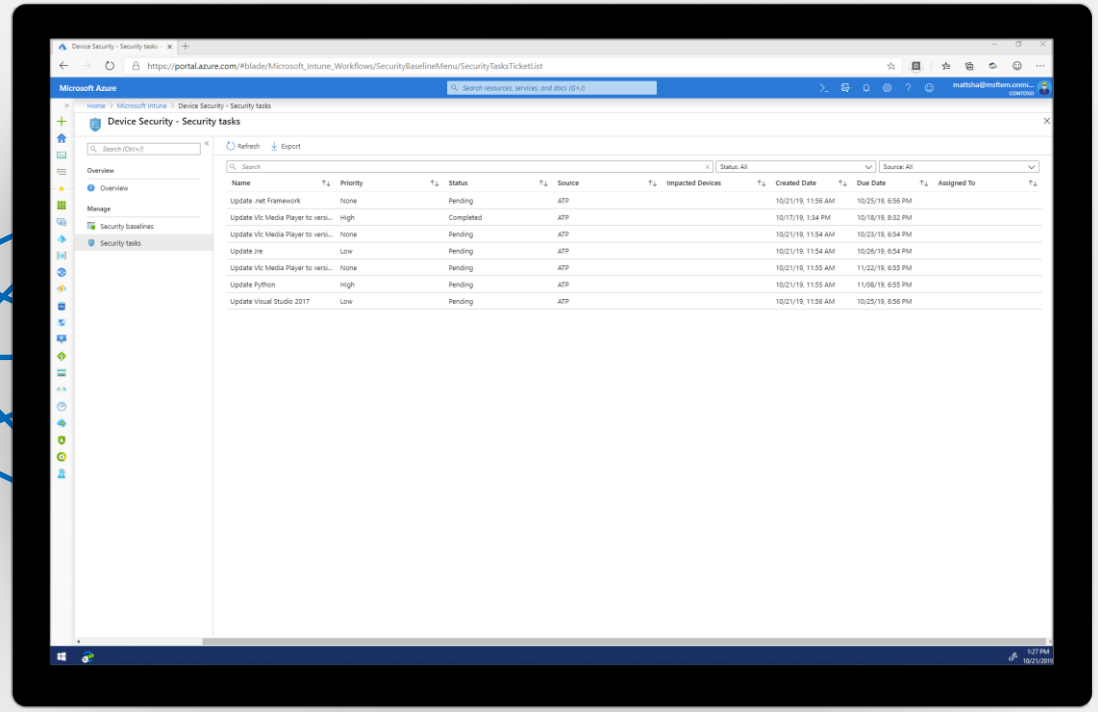
Security baselines

Security tasks

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

Seamless integration





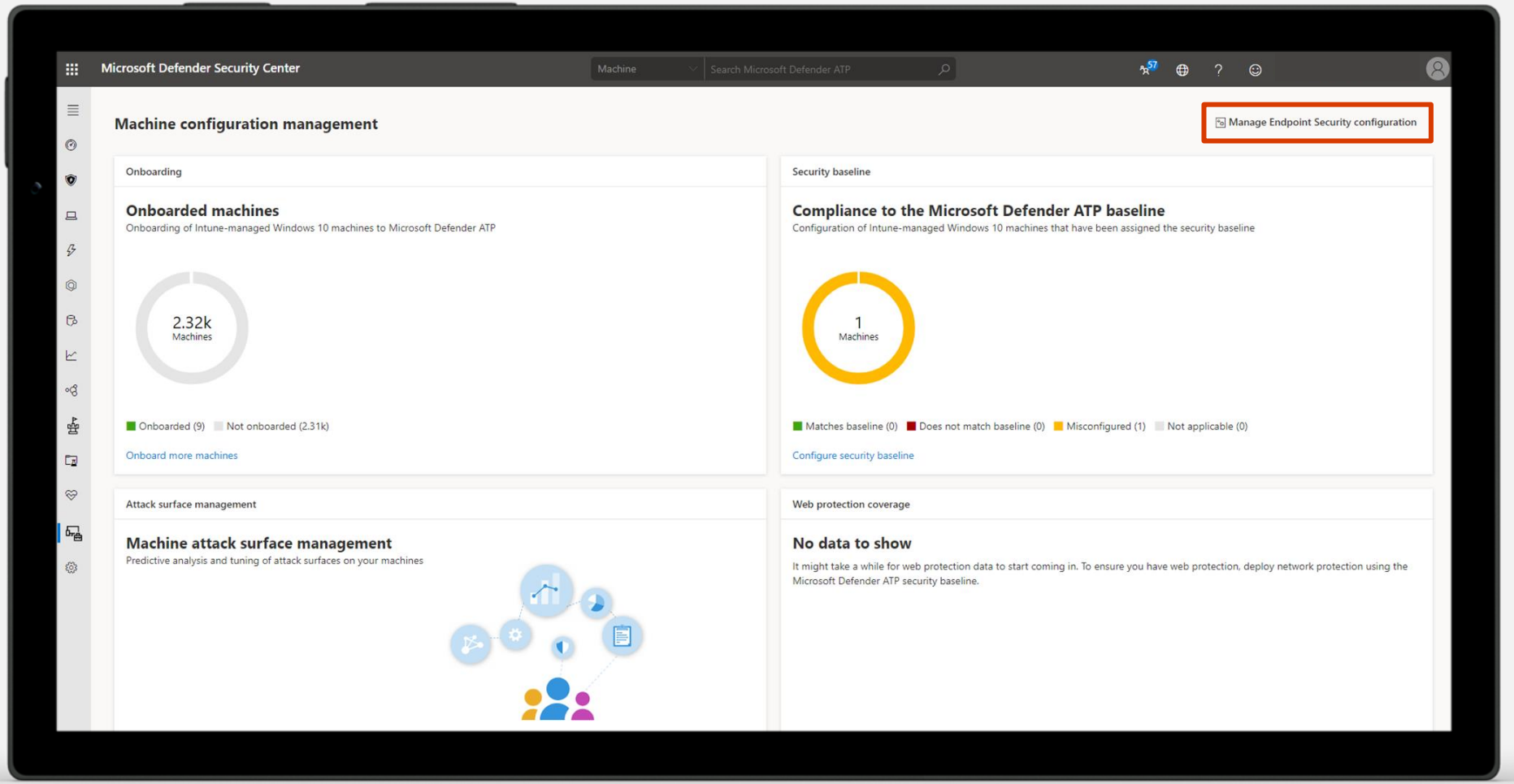
Microsoft Defender for Endpoint

Policy Assessment

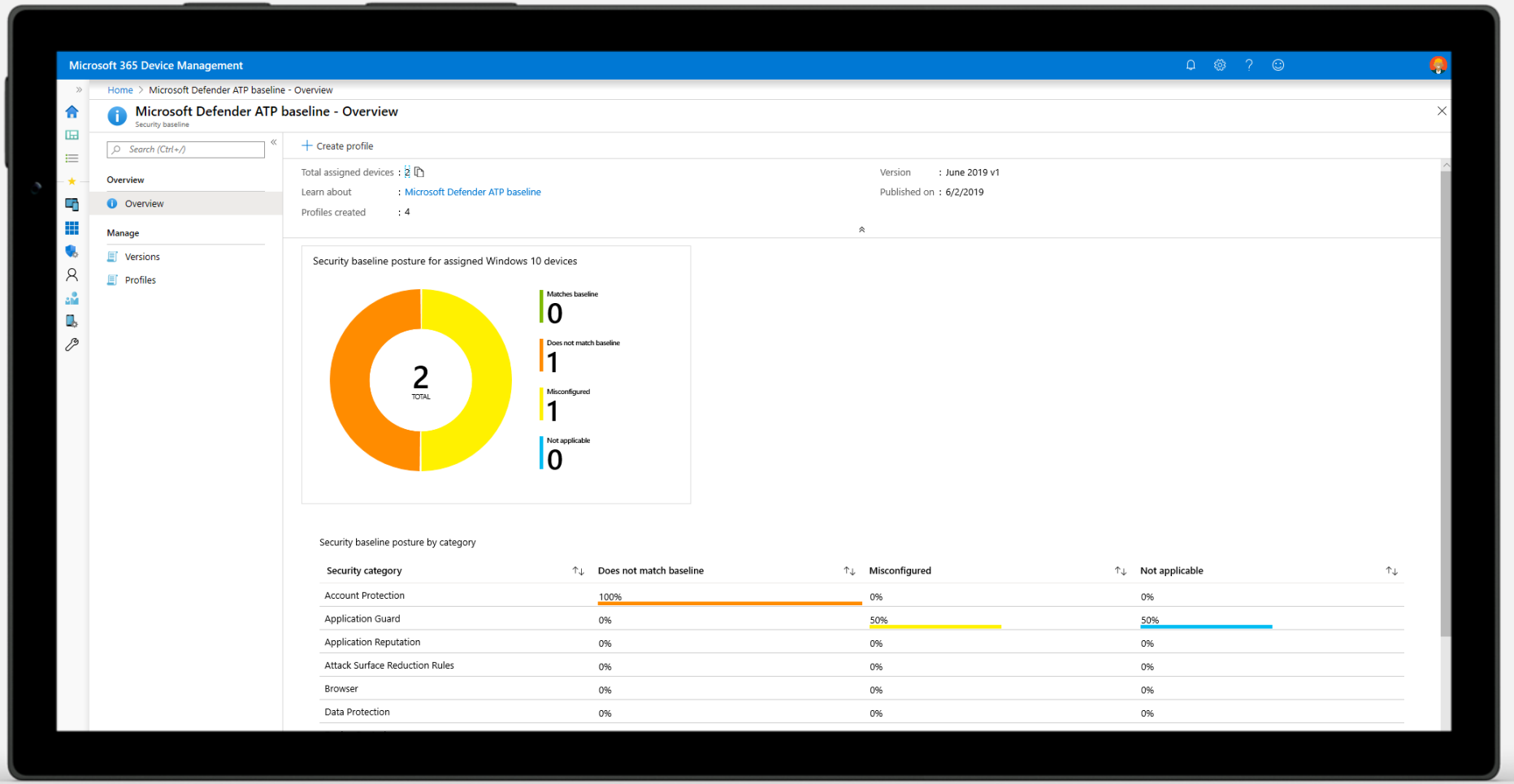
Microsoft Endpoint Manager

Policy Enforcement

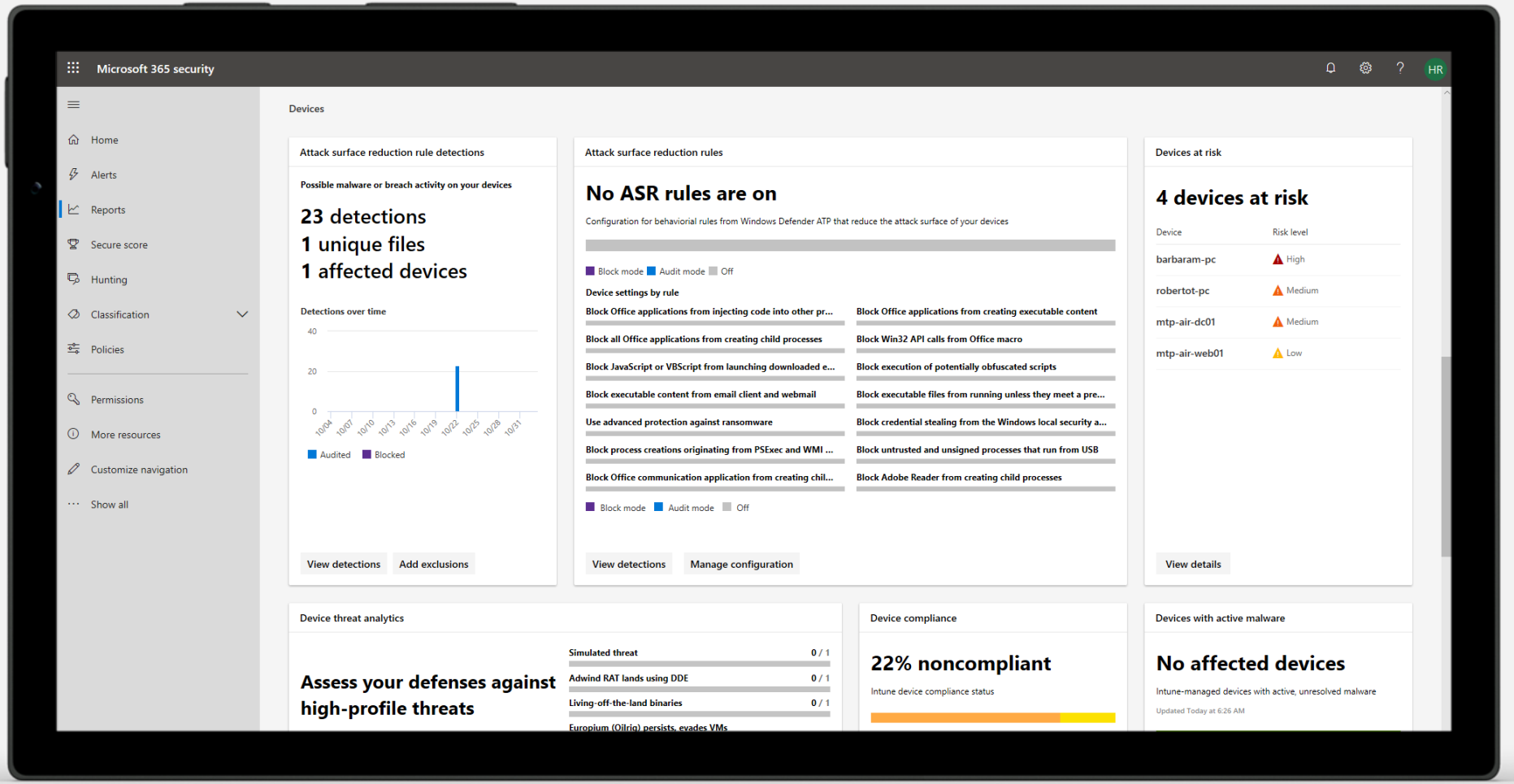
Easily access management controls from the console



Set security controls and baselines in Microsoft Endpoint Manager

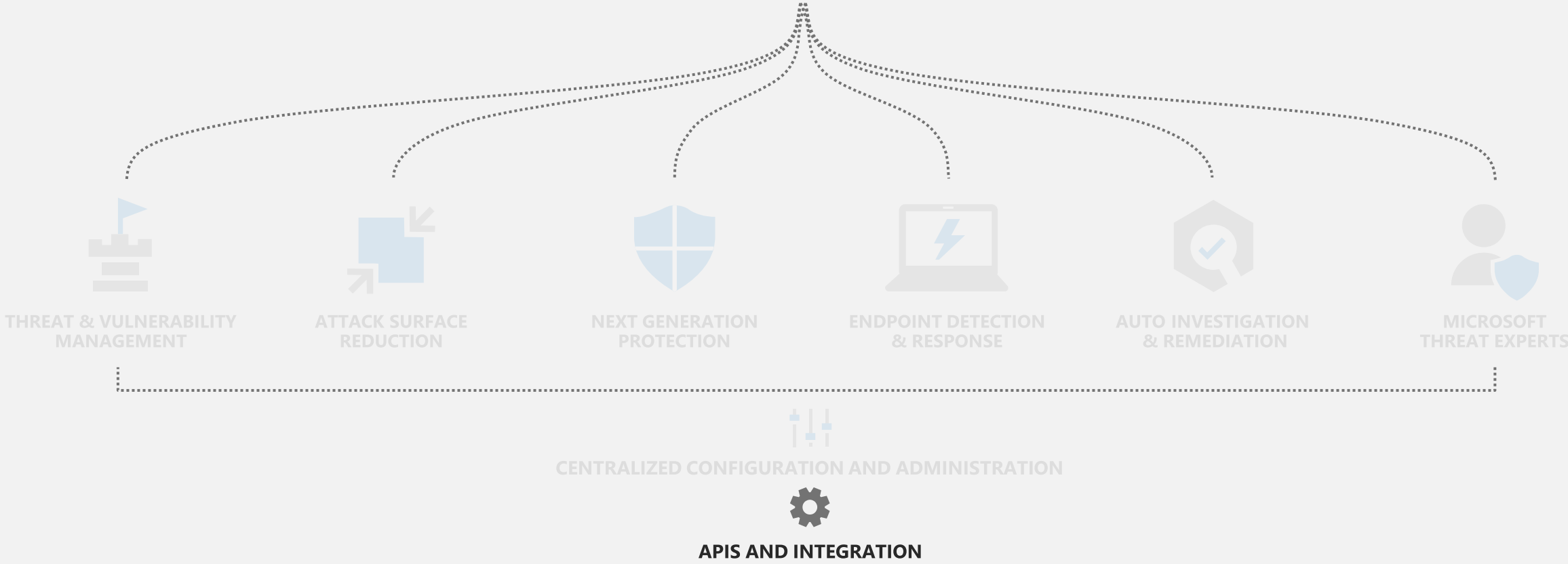


Get rich reporting in Microsoft Defender for Endpoint

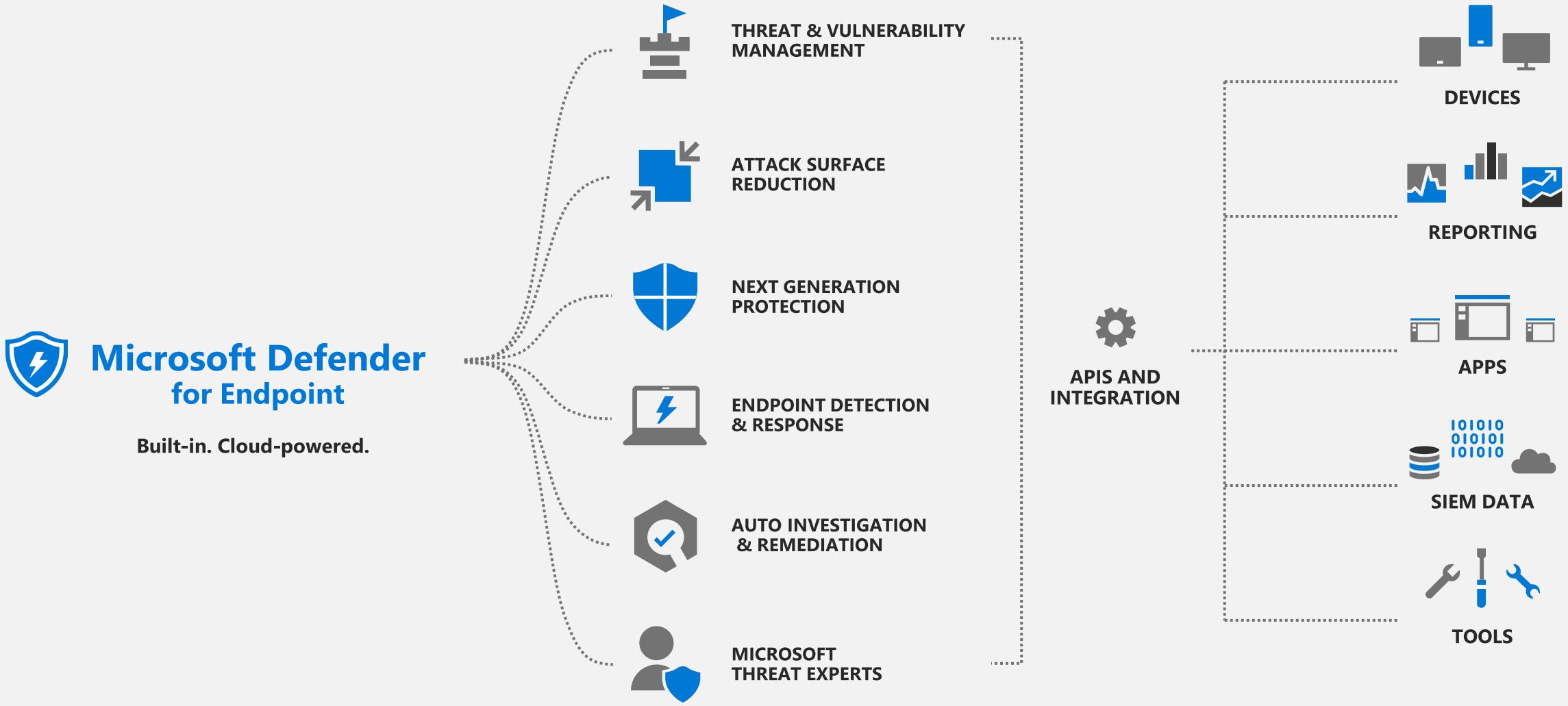


Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Connecting with the platform



Microsoft Defender for Endpoint APIs & partners

Easy development & tracking of connected solutions

API Explorer

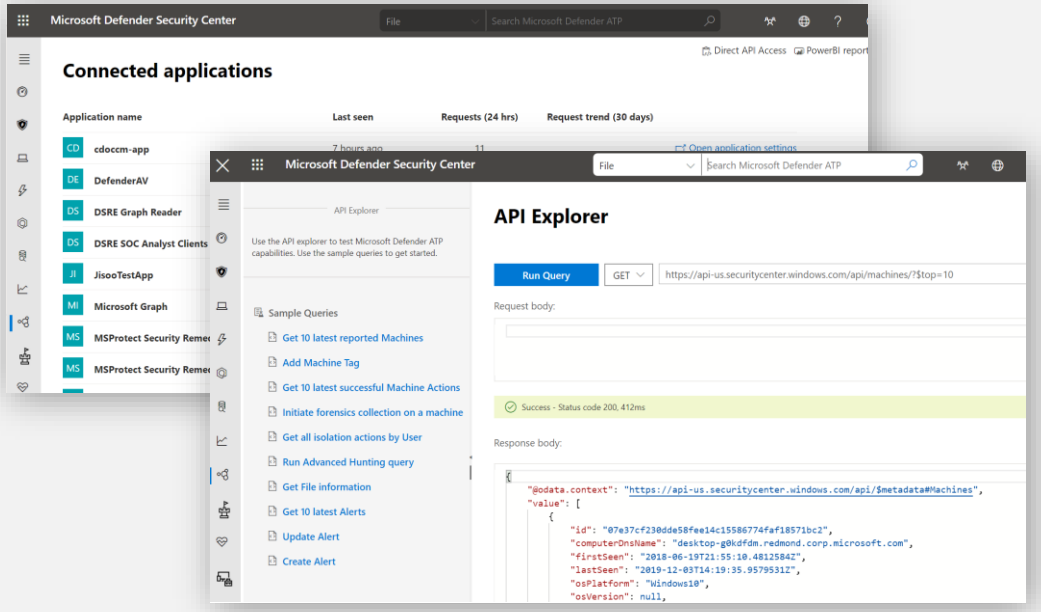
- Explore various Microsoft Defender for Endpoint APIs interactively

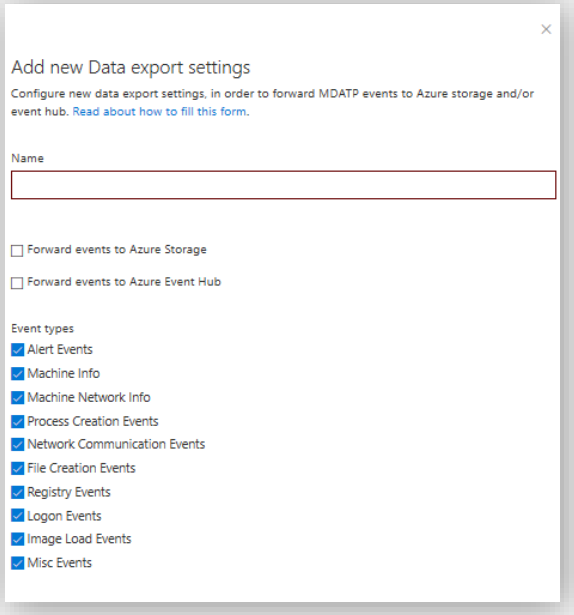
Integrated compliance assessment

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

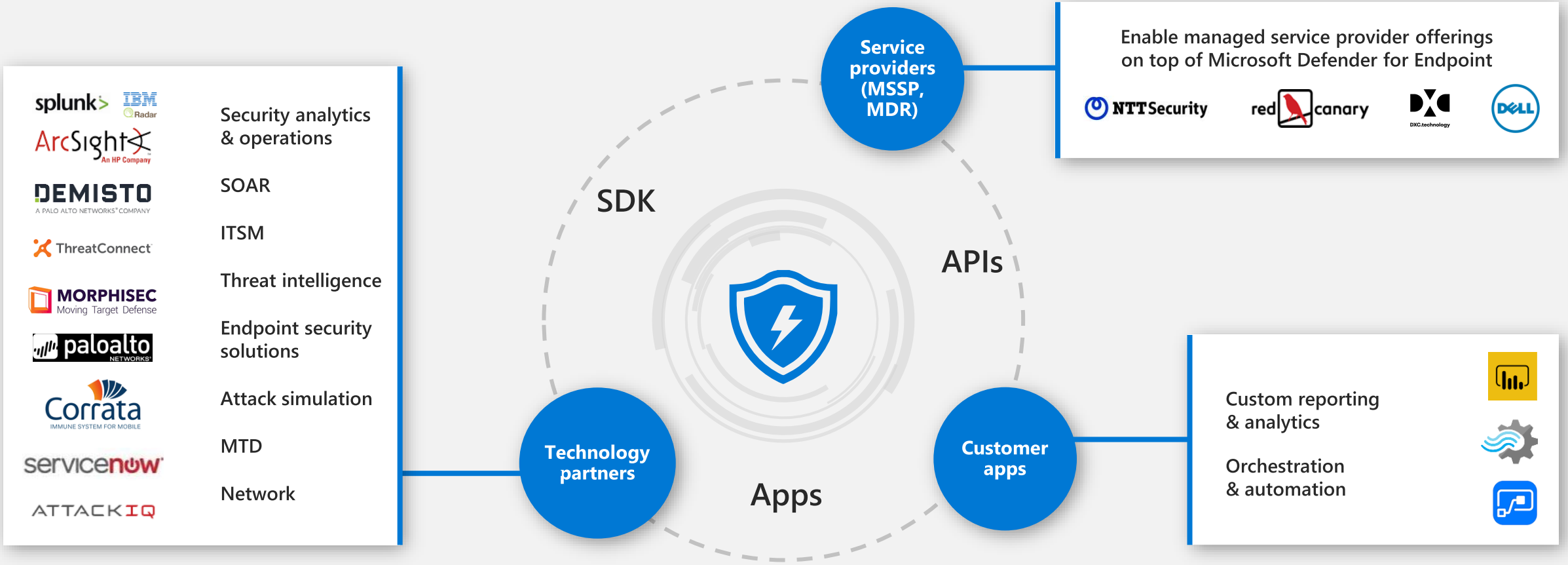
Data Export API

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





Microsoft Defender for Endpoint through ecosystem & API



+ Query API
+ Streaming API
+ Actions API
+ Threat intel API, Vulnerability API
+ Application connectors (PBI, Flow, SNOW)
+ Microsoft Security Graph connector
+ AAD authentication & authorization
+ RBAC controls
+ Developer kit
+ Partner integration kit
+ Developer License

Cross-platform

Microsoft Defender for Endpoint (Mac)

The first step in our cross-platform journey

Threat prevention

- Realtime MW protection for Mac OS
- Malware detection alerts visible in the Microsoft Defender for Endpoint console

Rich cyber data enabling attack detection and investigation

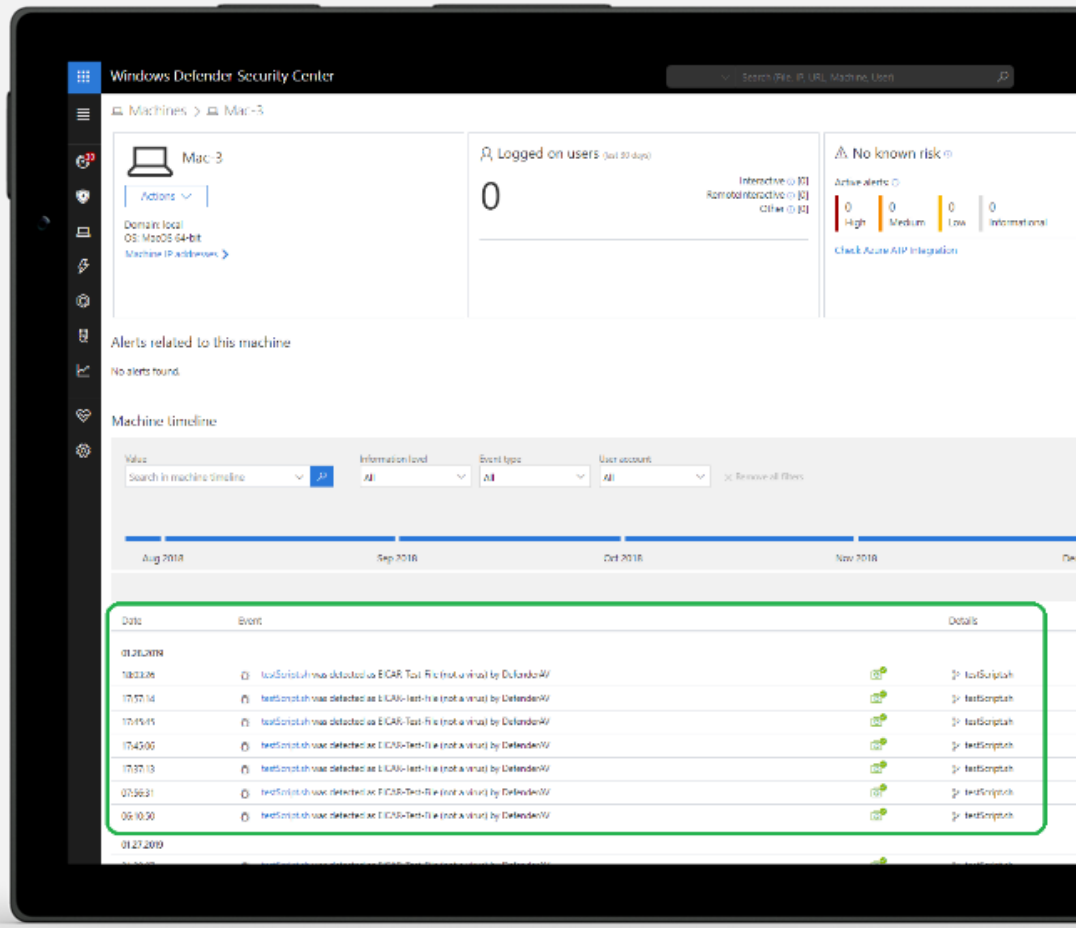
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

Enterprise Grade

- Lightweight deployment & onboarding process
- Performant, none intrusive
- Aligned with compliance, privacy & data sovereignty requirements

Seamlessly integrated with Microsoft Defender for Endpoint capabilities

- Detection dictionary across the kill chain
- 6 months of raw data on all machines inc Mac OS
- Reputation data for all entities being logged
- Single pane of glass across all endpoints Mac OS
- Advanced hunting on all raw data including Mac OS
- Custom TI
- API access to the entire data model inc Mac OS
- SIEM integration
- Compliance & Privacy
- RBAC



Microsoft Defender for Endpoint (Linux)

On the client:

- AV prevention
- Full command line experience (scanning, configuring, agent health)

In the Microsoft Defender Security Center, you'll see basic alerts and machine information.

EDR functionality will be gradually lit up in upcoming waves.

Antivirus alerts:

- ✓ Severity
- ✓ Scan type
- ✓ Device information (hostname, machine identifier, tenant identifier, app version, and OS type)
- ✓ File information (name, path, size, and hash)
- ✓ Threat information (name, type, and state)

Device information:

- ✓ Machine identifier
- ✓ Tenant identifier
- ✓ App version
- ✓ Hostname
- ✓ OS type
- ✓ OS version
- ✓ Computer model
- ✓ Processor architecture
- ✓ Whether the device is a virtual machine

Microsoft Defender for Endpoint (Android): GA scope

Web Protection

- Anti-phishing
- Block unsafe network connections
- Custom indicators: allow/block URLs

Malware Scan

- Alerts for malware, PUA
- Files scan
- Storage and memory peripheral scans

Single Pane of Glass Reporting

- Alerts for phishing
- Alerts for malicious apps
- Auto-connection for reporting in Microsoft Defender Security Center

Conditional Access

- Block risky devices
- Mark devices non-compliant

Supported Configurations

- Device Administrator
- Android Enterprise (Work Profile)

Licensed by Microsoft

- Included in per user licenses that offer Microsoft Defender for Endpoint
- Part of the 5 qualified devices for eligible licensed users
- Reach out to your account team or CSP

Microsoft Defender for Endpoint (iOS): Public Preview scope

Web Protection

- Anti-Phishing
- Block unsafe network connections
- Custom Indicators: allow/block URLs

Single Pane of Glass Reporting

- Alerts for phishing
- Auto connection for reporting in Microsoft Defender Security Center

Supported Configurations

- Supervised
- Unsupervised

Licensed by Microsoft

- Included in per user licenses that offer Microsoft Defender for Endpoint
- Part of the 5 qualified devices for eligible licensed users
- Reach out to your account team or CSP

How to get started

Evaluation Lab & Tutorials

Setup

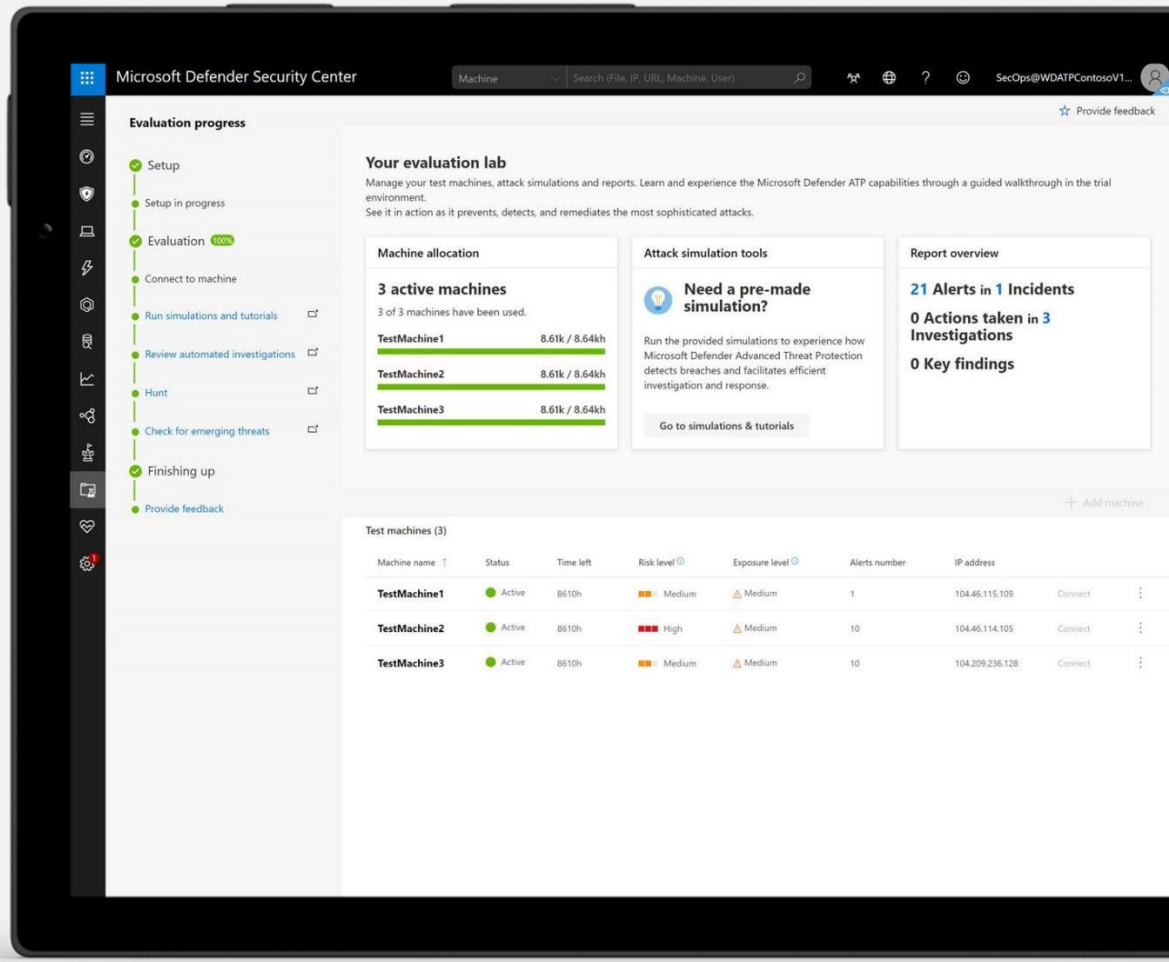
- Latest OS version
- Pre-configured to security baseline
- Onboarded to Microsoft Defender for Endpoint
- Full Audit mode across the stack.
- Pre-populated with evaluation tools
- Multiple interconnected devices (lateral movement)

Simulation

- Microsoft Defender for Endpoint pre-made simulations “Do it yourself” scenarios
- Wizard based experience (walk customers through product capabilities)
- Full flexibility (real-machine RDP accessible)
- Training & education is a critical part of successful PoC

Reports

- Guided experience
- Report is generated in real-time
- Results are self-contained (separate customer tenant data)
- Summary report
- Highlighting additional Microsoft Defender for Endpoint relevant features



Using Microsoft Defender for Endpoint? Turn on Public Preview features

Sign up for a trial: https://aka.ms/DefenderEndpoint
Check our blog: https://aka.ms/MSDEBlog

Microsoft 365

THANK YOU!