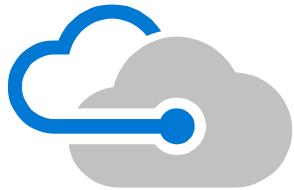




Microsoft Defender for Endpoint

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

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

FORRESTER

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

MITRE ATT&CK™

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



Our antimalware capabilities
consistently achieve high scores
in independent tests.

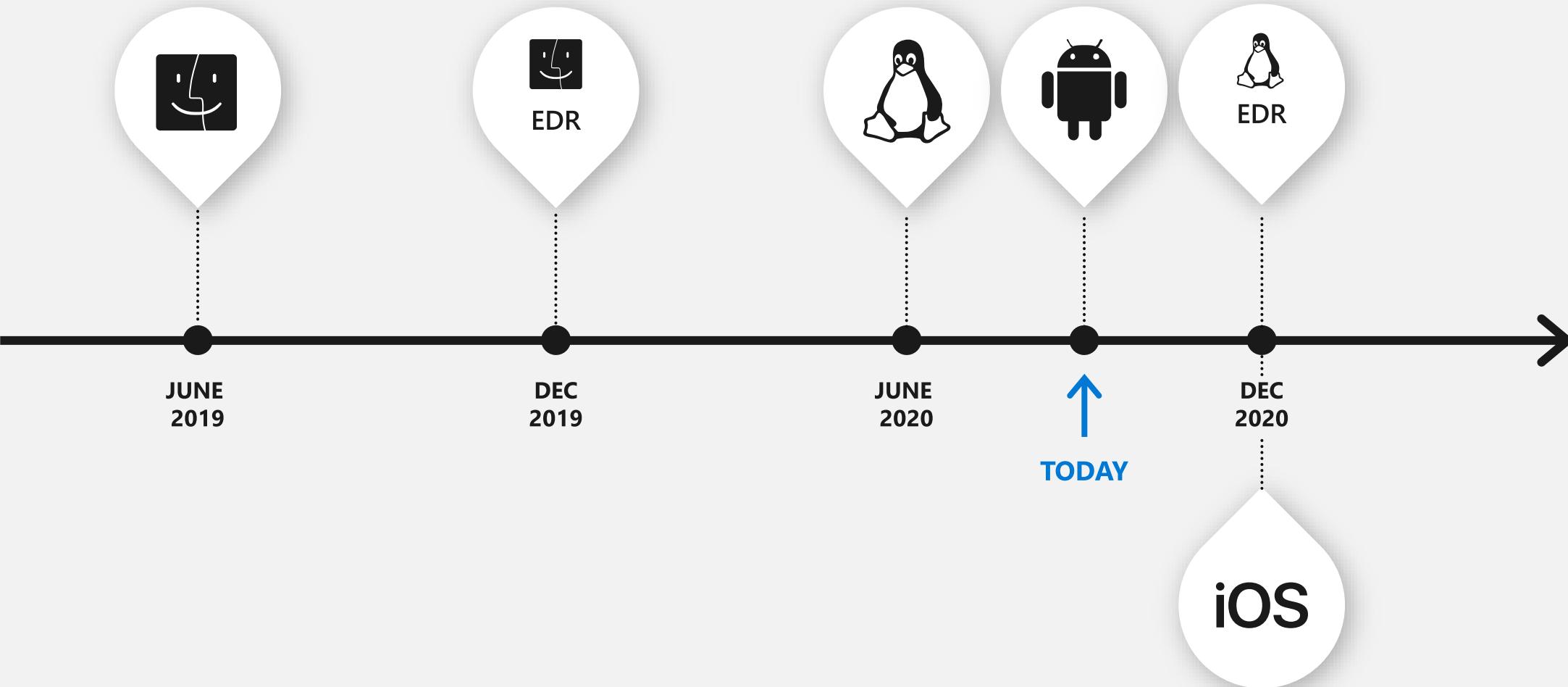


Microsoft Defender ATP awarded a
perfect 5-star rating by SC Media in
their 2020 Endpoint Security Review



- ✓ 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

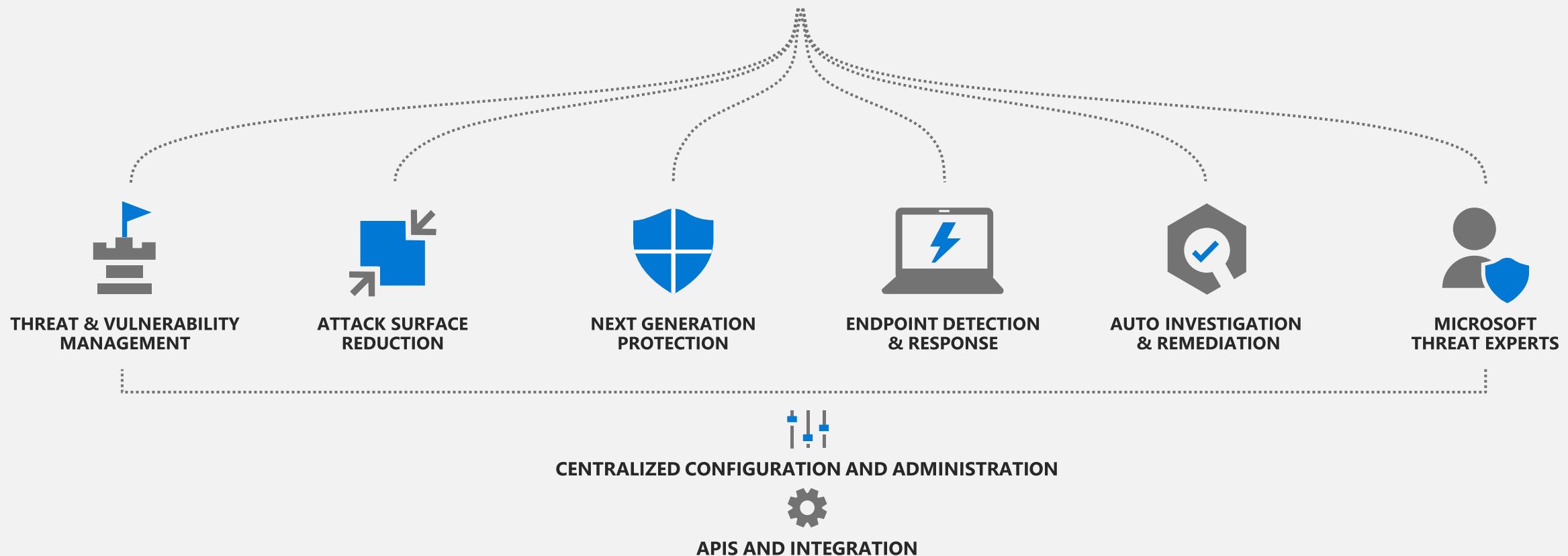
Delivering Microsoft Defender for Endpoint across platforms





Microsoft Defender for Endpoint

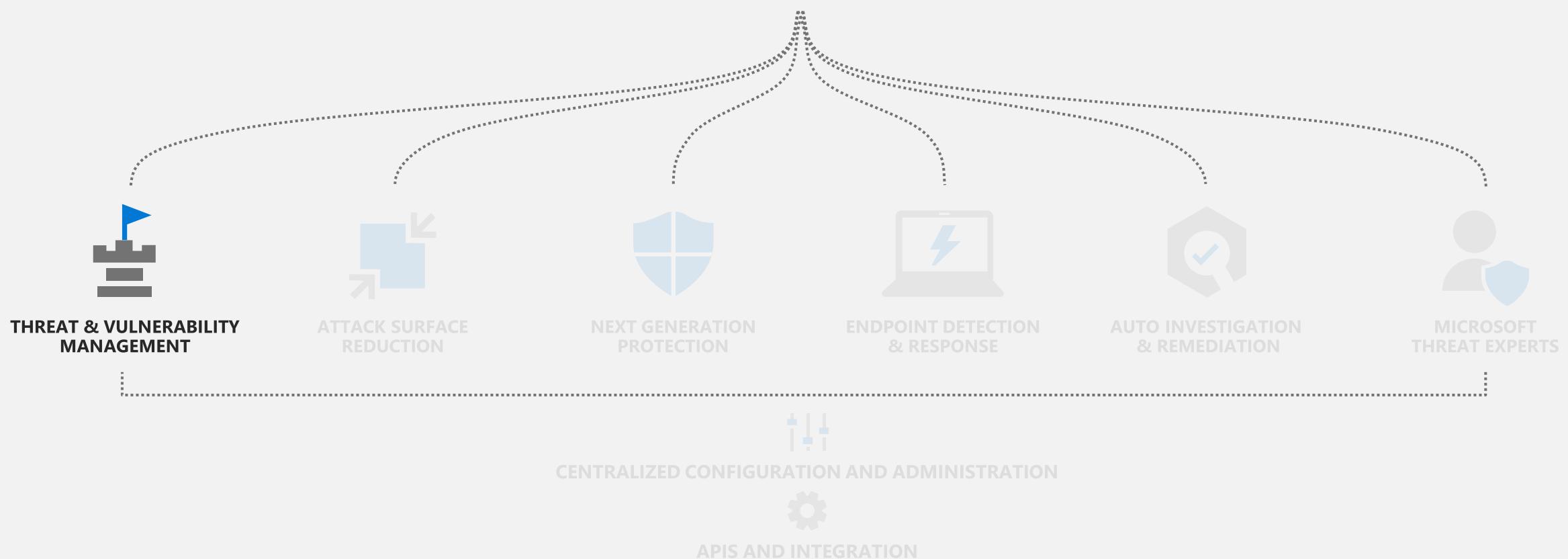
Built-in. Cloud-powered.





Microsoft Defender for Endpoint

Built-in. Cloud-powered.

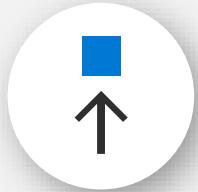


Key customer pain points



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

The screenshot shows the Microsoft Defender Security Center Threat & Vulnerability Management dashboard. At the top, there's a large blue circular icon with a white castle and flag logo. Below it, the dashboard has several sections:

- Organization exposure score:** A gauge showing a score of 61.
- Configuration Score:** A score of 677/1270.
- Severity distribution:** A donut chart showing 3K total vulnerabilities, with segments for High (red), Medium (orange), Low (yellow), and No data (grey).
- Top vulnerable software:** A table listing software, security recommendations, weaknesses, threats, exposed devices, and impact. Examples include Contoso Media Player, MeDoc, and Eclipse.
- Active remediations:** A section showing active tasks generated from security recommendations.
- Remediation tasks:** A table showing tasks updated at 6:20 pm today, including Google V8 engine QtWebEngineCore and Microsoft Office 2013 RCE.
- Vulnerability in Java SE (AWT):** A table showing vulnerabilities in Java SE (AWT) with rows for Google V8 engine QtWebEngineCore and Microsoft Office 2013 RCE.



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)

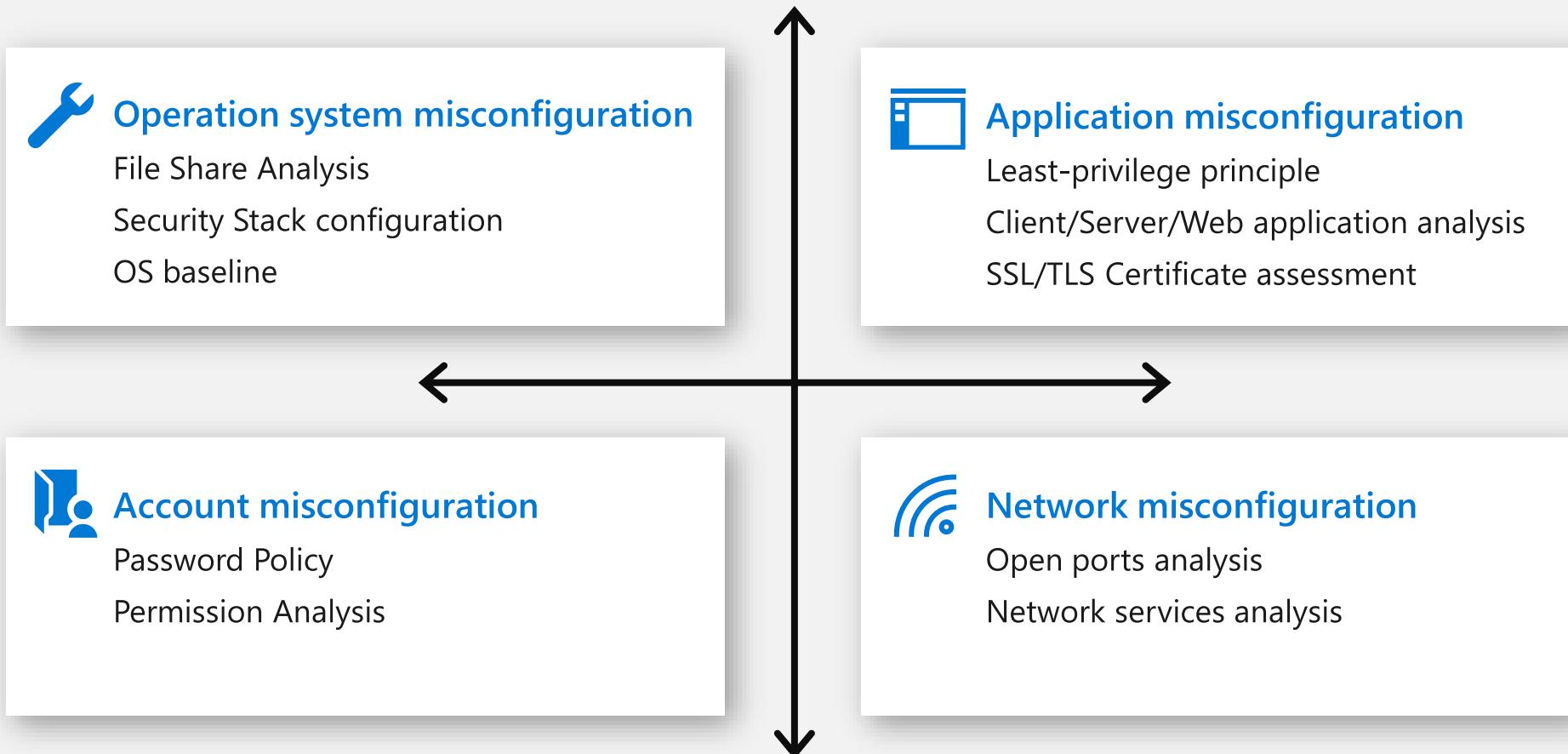
Hardest to discover

1



Continuous Discovery

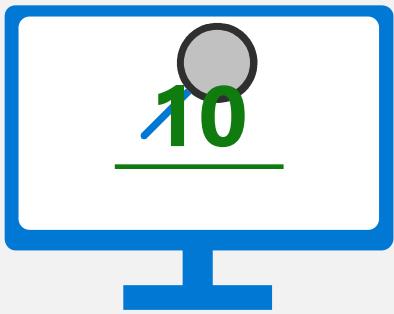
Broad secure configuration assessment





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

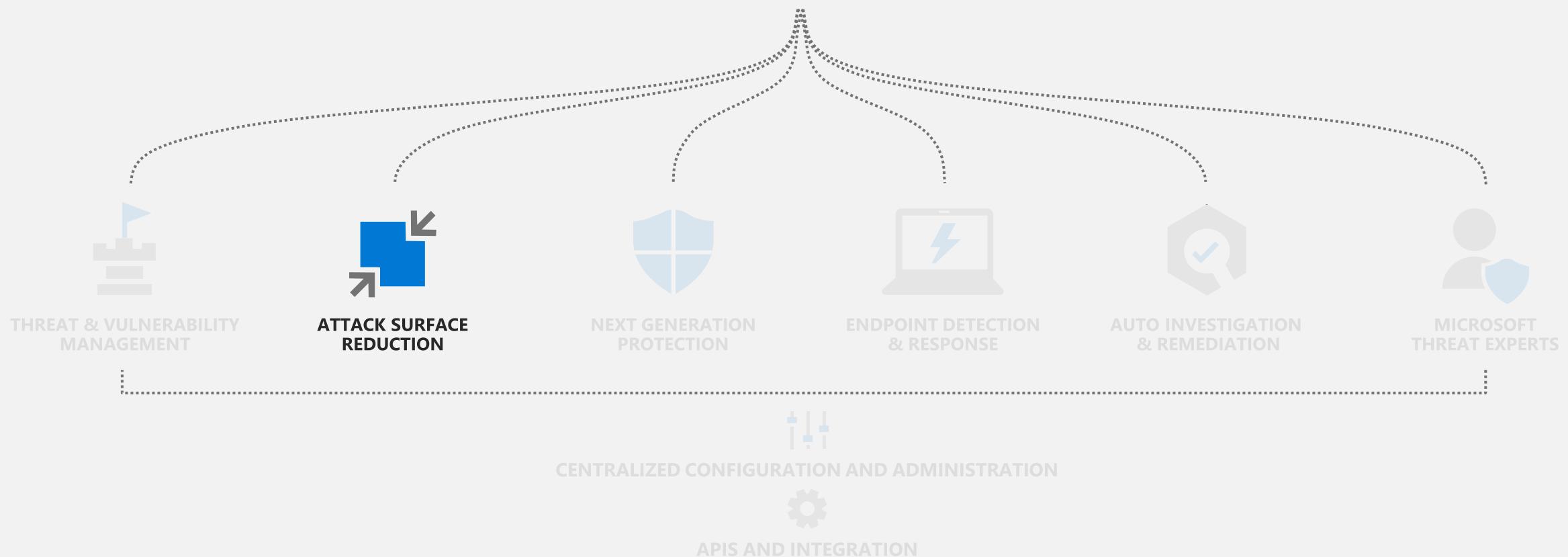
Game changing bridge between IT and Security teams

- 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

The screenshot shows the Microsoft 365 security interface with a blue circular overlay containing a white document icon with arrows pointing to it.

Microsoft 365 security

Devices

Attack surface reduction rule detections

Possible malware or breach activity on your devices

9.1k detections
2 unique files
2 affected devices

Detections over time

1000

500

0

05/13 05/16 05/19 05/22 05/25 05/28 05/31 06/03 06/06 06/09

■ Audited ■ Blocked

Attack surface reduction rules

86% devices use ASR rules to block the following behaviors

Configuration for behavioral rules from Windows Defender ATP that reduce the attack surface

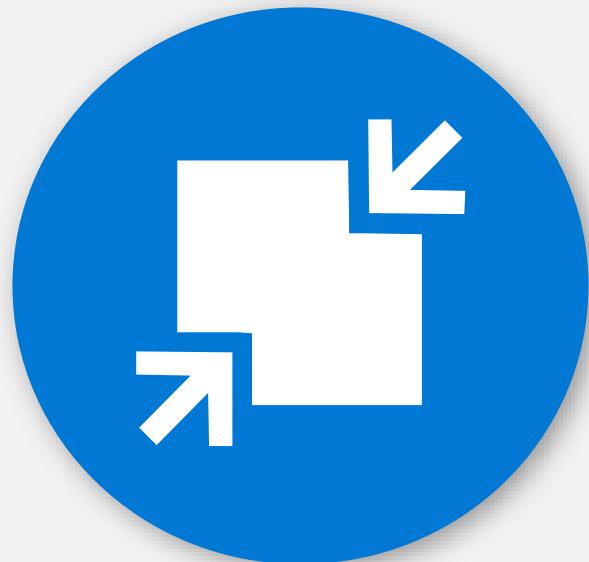
Behavior	Status
Block Office applications from injecting code into other processes	Block mode
Block all Office applications from creating child processes	Block mode
Block JavaScript or VBScript from launching downloaded executables	Block mode
Block executable content from email client and webmail	Block mode
Use advanced protection against ransomware	Block mode
Block process creations originating from PSEXEC and WMI commands	Block mode
Block untrusted Office communication application from creating child processes	Block mode

View detections **Add exclusions**

View detections **Manage configuration**

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 PSEnc 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

The screenshot shows the Microsoft 365 Security interface with the following details:

- Header:** Microsoft 365 Security, https://security.microsoft.com
- Breadcrumbs:** Monitoring & reports > Attack surface reduction rules
- Navigation:** Detections, Configuration (selected), Rule status
- Alert:** Five rules can be turned on for 80% of your devices with no user impact (Based on your audit data over the last 14 days). Buttons: View details, Dismiss.
- Device configuration overview:** Rules in audit only: 324, Some or all rules in block: 525, Off: 22.
- Add exclusions:** Choose to exclude files you trust from being blocked by attack reduction rules. Button: Add exclusions.
- Rules section:** Lists five categories with 'Learn more' links:
 - Office apps injecting into other processes
 - Office apps/macros creating executable content
 - Office apps launching child processes
 - Win32 imports from Office macro code
 - Obfuscated js/vbs/ps/macro code
- Devices section:** 2,354 devices. 80% of your total devices with Windows Defender Advanced Threat Protection.
- Buttons at bottom:** Get script to implement, Submit Intune ticket.

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 addition to trusting our rich reputation database.

The screenshot shows the Microsoft Defender Security Center interface. On the left, a sidebar lists various security operations: General, Permissions, APIs, Rules, and Indicators. The 'Indicators' section is currently selected. The main area displays a table titled 'IP addresses' under the 'Settings' tab. The table has columns for IP, Action, Alert severity, and Category. It shows several entries for the IP 207.46.194.33, with actions ranging from 'Alert' to 'Allow'. A status bar at the bottom right indicates a 'Virus & threat protection' alert: 'Connection blocked' with the message 'Your IT administrator caused Microsoft Defender Security Center to block this network connection. Contact your IT help desk.'

File hashes	IP addresses	URLs/Domains	Certificates
Export	Import	Add item	
Available capacity: 32/15000			
Customize columns			
30 items per page			
IP	Action	Alert severity	Category
207.46.194.33	Alert	Medium	Other
207.46.194.33	Alert and block	Medium	C2
207.46.194.33	Alert	Medium	C2
207.46.194.33	Alert	High	Suspicious
207.46.194.33	Alert and block	Medium	Installation
207.46.194.33	Allow		

Web Threat Alerts

Alerts > Suspicious connection blocked by network protection

Suspicious connection blocked by network protection
This alert is part of incident (76)

Actions

Severity: Informational
Category: Command And Control
Detection source: EDR
Detection technology: Behavioral, Network

Automated investigation is not applicable to alert type

Alert context

minint scps
minint smt: net msc

First activity: 07.29.2019 | 16:23:52
Last activity: 07.29.2019 | 16:23:52

Status

State: New
Classification: Not set
Assigned to: Not assigned

Description

Network protection prevented an attempt to connect to a malicious, compromised, or user-blocked URL, Domain, IP.

Recommended actions

1. Check the destination address. Note that highly reputable addresses might be flagged if they contain malicious content in subfolders.
2. Review the process that initiated the connection. If the process is unfamiliar and the executable not a signed system file, submit the file for deep analysis and review detailed behavioral information from the analysis results. Initiate an antivirus scan to find previously undetected malware.
3. If you've confirmed this activity to be malicious, contain and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset their passwords, block IP addresses and URLs, and install security updates.

Show more

Alert process tree

```
graph TD; A[firefox.exe] --> B[firefox.exe]; B --> C["https://smartscreentestratings2.net"]; C --> D["https://smartscreentestratings2.net"]
```

Incident graph is not available for this alert

Artifact timeline

Description	First Observed	Details

Web Threat Reports

30 days ▾

Customize columns

Domains (18)

Domain	Access count	Blocks	Access trend
smartscreentestings2.net	17	16	No change
becomestateman.com	8	8	No change
failuremail.com	7	7	No change
www.netflix.com	5	5	▲ 400%
barrykatz.com	4	4	No change
netflix.com	3	3	▲ 200%
brightdesire.us	3	3	No change
nexttoyersinghph3.club	3	3	No change
store.google.com	2	2	No change
getpremium-software.com	2	2	No change
clickandplay.co	2	2	No change
08ba1010.istraffic.com	2	2	No change
ver.streaminggratuit.com	2	2	No change
div.show	2	2	No change
schoosing.com	2	2	No change
cdnwrd.com	1	1	No change
www.becomestateaman.com	1	1	No change
ichnaea-web.netflix.com	1	1	No change

Web threat protection blocks over time

Attempts to access malicious URLs

07/10

Type	Count
Malicious	19
Phishing	17
Custom Indicator	6
Unknown	0

07/08 07/16

Status

Web threat protection summary

Last 30 days | Updated 8/4/2019

67 web threat protection detections

Attempts to access malicious URLs

No change Custom Indicator 1

Type	Count
Phishing	17
Malicious	19
Custom Indicator	6
Unknown	0

Web content filtering configuration

The screenshot shows the Microsoft Defender Security Center interface. On the left, a sidebar menu is open under the 'Settings' section, with 'Web content filtering' selected. The main content area displays a list titled 'Add policy' with the sub-tab 'Blocked categories' selected. A descriptive text states: 'Select the web content categories to block. You will continue to get data about access attempts to websites in all categories.' Below this, there are three expandable sections: 'Adult content', 'High bandwidth', and 'Legal liability', each containing a list of categories with checkboxes. At the bottom of the dialog are buttons for 'Previous', 'Next', and 'Cancel'.

Microsoft Defender Security Center

Device | Search Microsoft Defender ATP

Settings

General

- Data retention
- Alert notifications
- Power BI reports
- Advanced features
- Auto remediation

Permissions

- Roles
- Device groups

APIs

- SIEM

Rules

- Custom detections
- Alert suppression
- Indicators
- Process Memory Indicators
- Web content filtering**
- Automation uploads
- Automation folder exclusions

Device management

- Onboarding
- Offboarding

+ Add item

No items found

Add policy

General **Blocked categories** Scope Summary

Select the web content categories to block. You will continue to get data about access attempts to websites in all categories.

Adult content ▾

- Cults
- Gambling
- Nudity
- Pornography/Sexually explicit
- Sex education
- Tasteless
- Violence

High bandwidth ▾

- Download sites
- Image sharing
- Peer-to-peer
- Streaming media & downloads

Legal liability ▾

- Child abuse images
- Criminal activity
- Hacking
- Hate & intolerance
- Illegal drug
- Illegal software
- School cheating
- Self-harm

Previous Next Cancel

Web Content Filtering reporting

Microsoft Defender Security Center

Machine | Search Microsoft Defender ATP

57

30 days

Web protection > Report details

Web categories Domains Machine groups

Web categories that were accessed or blocked

Web category	Parent category	Requests	Blocks
Streaming media & downloads	High bandwidth	23591	23559
Image sharing	High bandwidth	7	7
Download sites	High bandwidth	1	1

Web activity by category Last 30 days | Updated Thu Sep 19 2019

Web categories with the most activity change

Sharp traffic spikes can indicate malicious internal activity

Parent web category	Change in access requests
High bandwidth	▲ 50%
Leisure	▼ 100%
Legal liability	No data
Adult content	No data
Uncategorized	No data

Streaming media & downloads

Request trend

Requests for URLs in this category over the last 30 days

▲ 258% compared to the preceding period

4260
3195
2130
1065

03/14 03/18 03/21 03/25 03/29 04/01 04/05

Web activity summary Last 30 days | Updated Thu Sep 19 2019

144 web requests

Total number of requests for web content in all URLs

Leisure Adult content High bandwidth Legal liability Uncategorized

Web content filtering summary Last 30 days | Updated Thu Sep 19 2019

117 web content filtering blocks

Attempts to access URLs in blocked categories

Leisure Adult content High bandwidth Legal liability Uncategorized

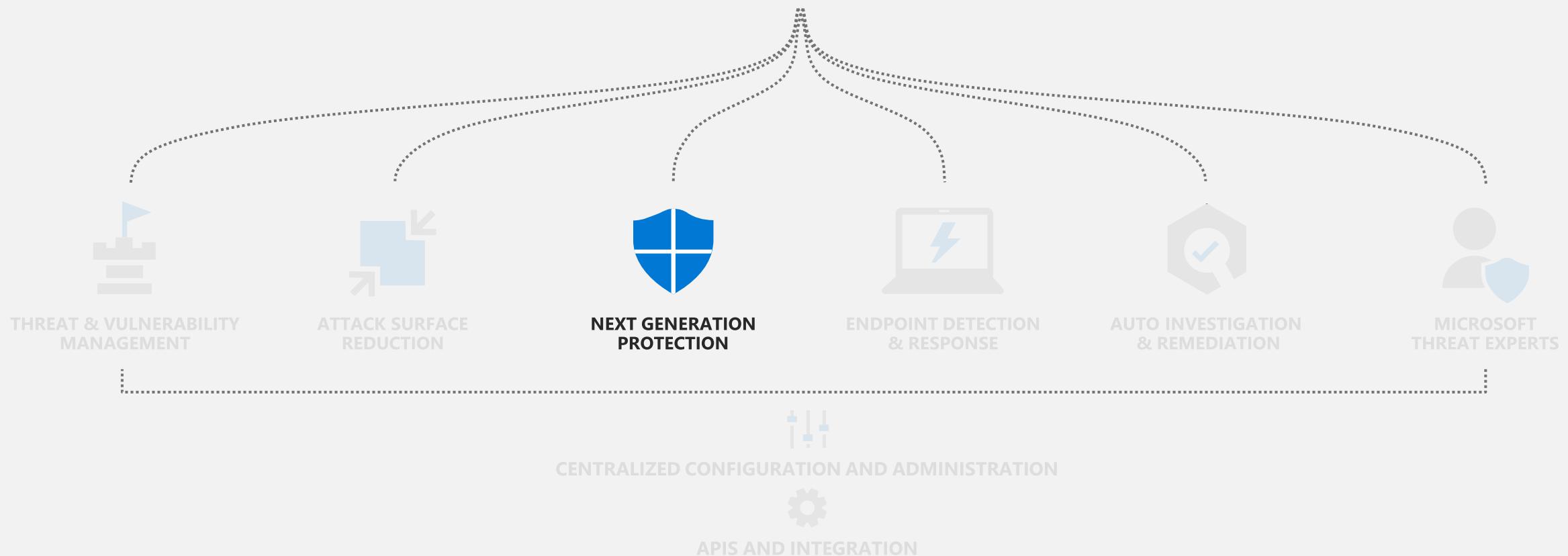
Requests

Category	Requests
Leisure	13819
Adult content	7073



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



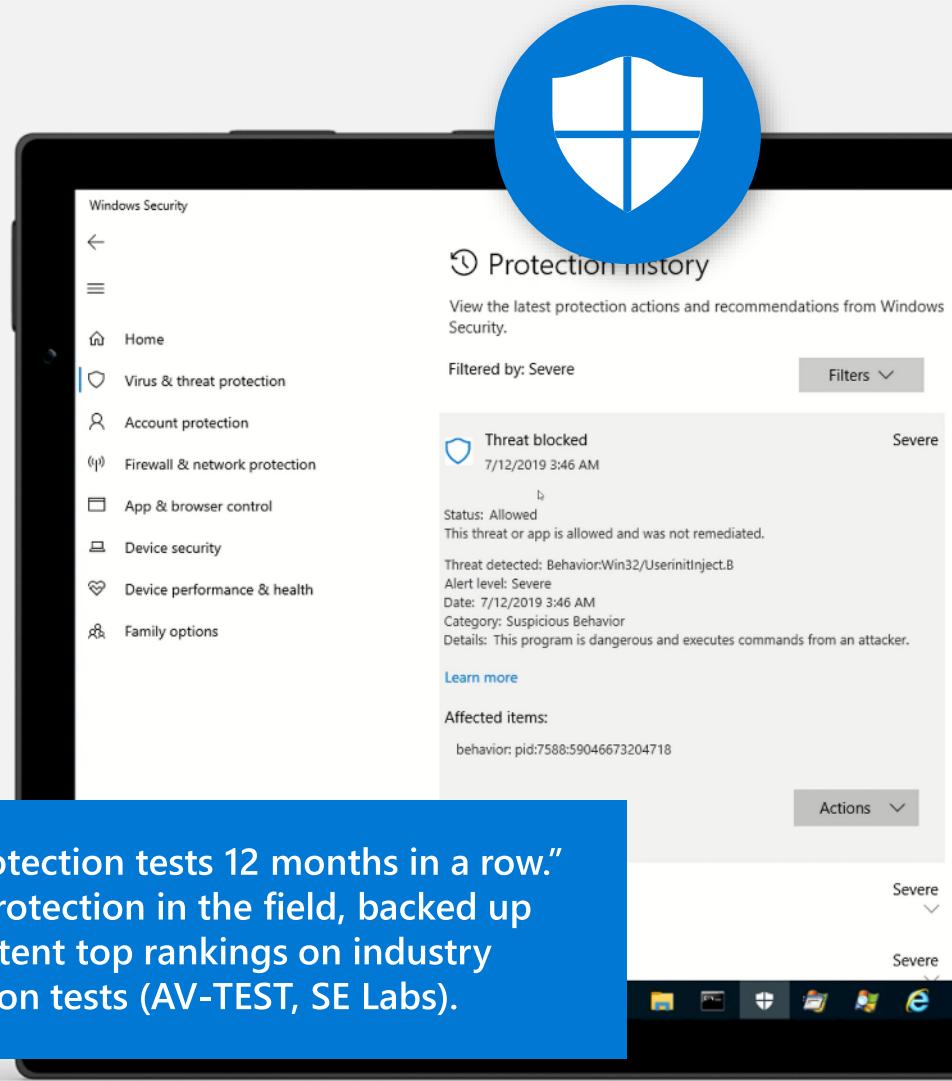
Blocks file-based and fileless malware



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



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

Cloud

Client



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

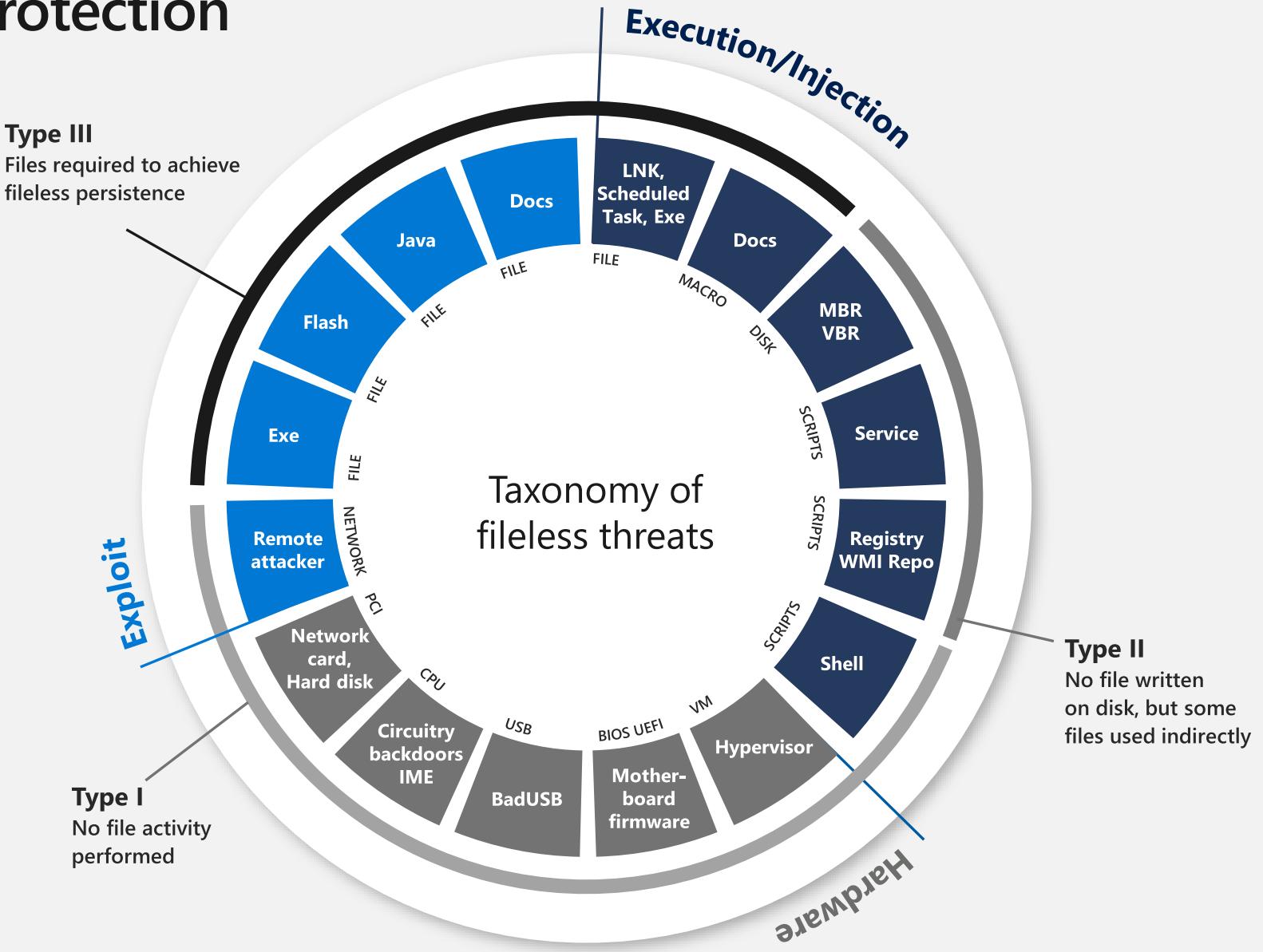


Network monitoring

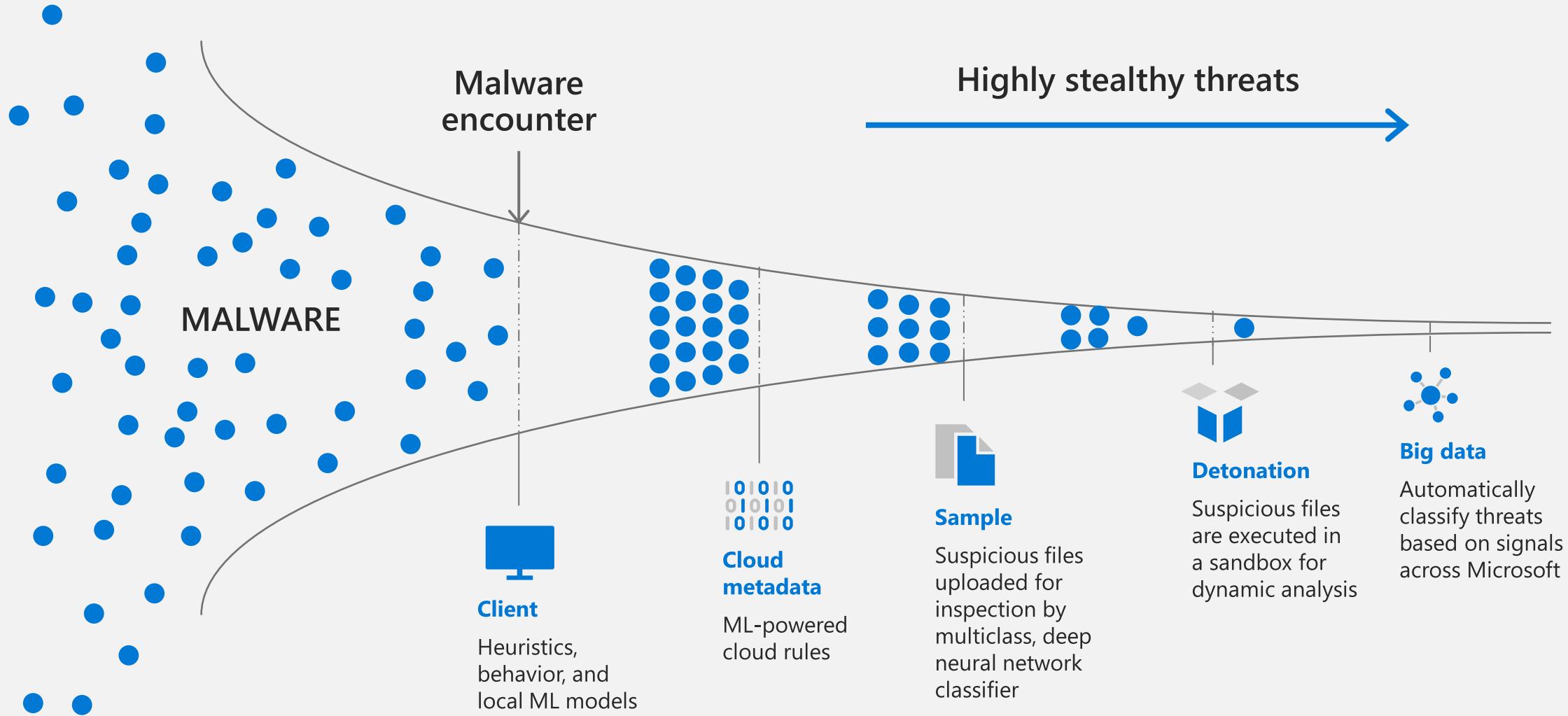
Catches malicious network activities

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

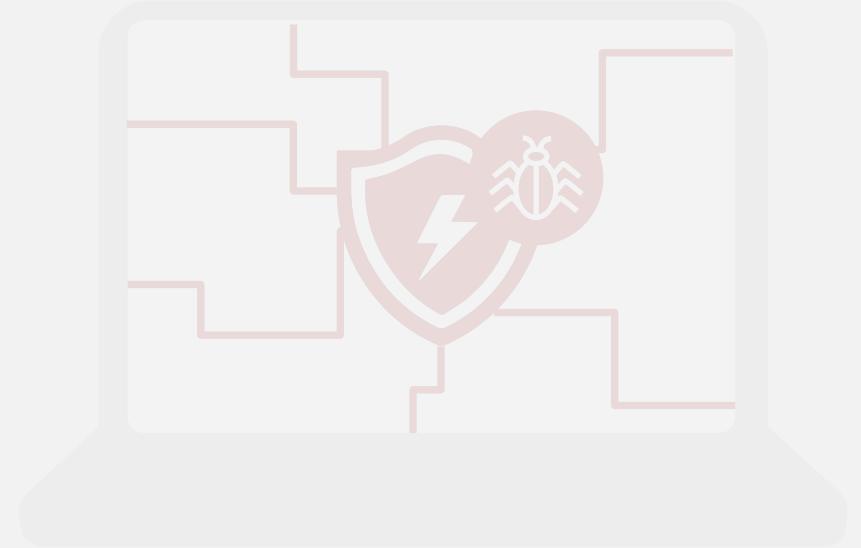


Heuristics can:

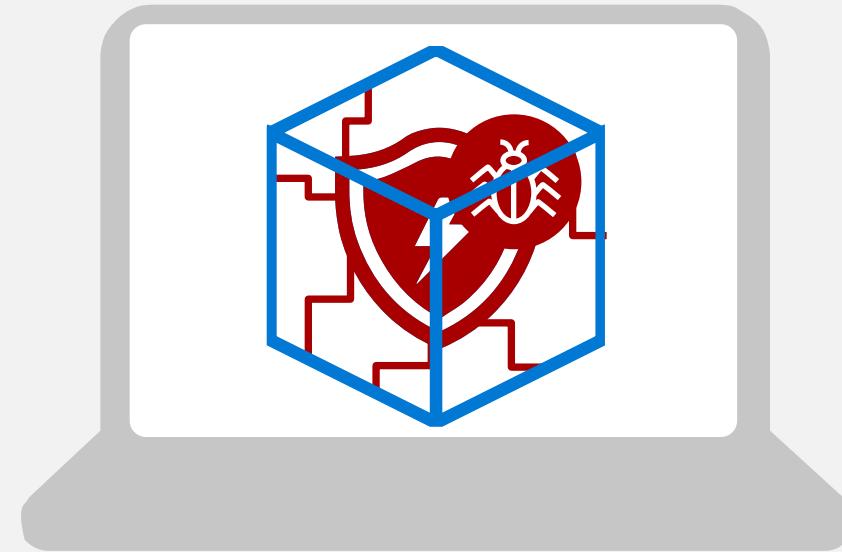
- Detect sequences of events
E.g. a file named "malware.exe" is created
- Inspect event data
E.g. an AutoRun key is created and contains "malware.exe"
- Correlate with other static signals
E.g. "malware.exe" has an attribute indicating it is a DotNet executable
- Perform some basic remediation
E.g. delete "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

The screenshot shows the 'Create profile' screen in Microsoft Defender Security Center. A red box highlights the 'Profile type' dropdown set to 'Endpoint protection'. Another red box highlights the 'Microsoft Defender Security Center' section under 'Settings', which contains 18 settings available.

Threat & vulnerability management – Security recommendation

The screenshot shows a 'Turn on Tamper Protection' recommendation in the 'Security recommendations' section. A red box highlights the 'Tamper Protection' status as 'Enabled'. The recommendation details that Tamper Protection locks Microsoft Defender ATP and prevents changes to security settings through apps and methods like registry editing.

Tampering alert based on System Guard and EDR signals

The screenshot shows the 'Active alerts' section of the Microsoft Security Operations dashboard. It displays two circular charts: one for 'Windows Defender Antivirus tampering' (126 New, 1 In progress) and another for 'Windows Defender Antivirus tampering' (103). A legend indicates alert levels: Medium (orange), Low (yellow), Informational (light gray), and High (dark red).

Advanced Hunting

The screenshot shows the 'Advanced hunting' interface in Microsoft Defender Security Center. The left sidebar lists schema categories like AlertEvents, MachineInfo, and NetworkCommunicationEvents. The main area shows a query editor with the following command: 'AlertEvents | where Title == "Tamper protection bypass"'.

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

The screenshot shows a Microsoft Defender Security Center alert titled "Strontium: The UEFI sensor in Microsoft Defender Antivirus detected malicious code in firmware". The alert details include:

- Severity: High
- Category: Defense Evasion
- Technique: T1109: Component Firmware
- Detection source: Antivirus
- Detection technology: Client
- Detection status: Detected

A note states that automated investigation is not applicable to this alert type. Below the alert, there's a "Description" section explaining the threat and a link to the Microsoft Encyclopedia.

Scanning and detection

The screenshot shows the Windows Security interface under "Protection history". A recent threat was detected on 6/17/2020 at 6:28 PM, identified as a "Trojan:UEFI/BootOrderTampering". The threat is active and has not been remediated. The details indicate it's a dangerous program executing commands from an attacker. The affected item is listed as uefienvvar: {8BE4DF61-93CA-11D2-AA0D-00E098032B8C};BootOrder. An "Actions" button is visible at the bottom right.



Read the [blog](#) for more details

Behavioral Blocking and Containment

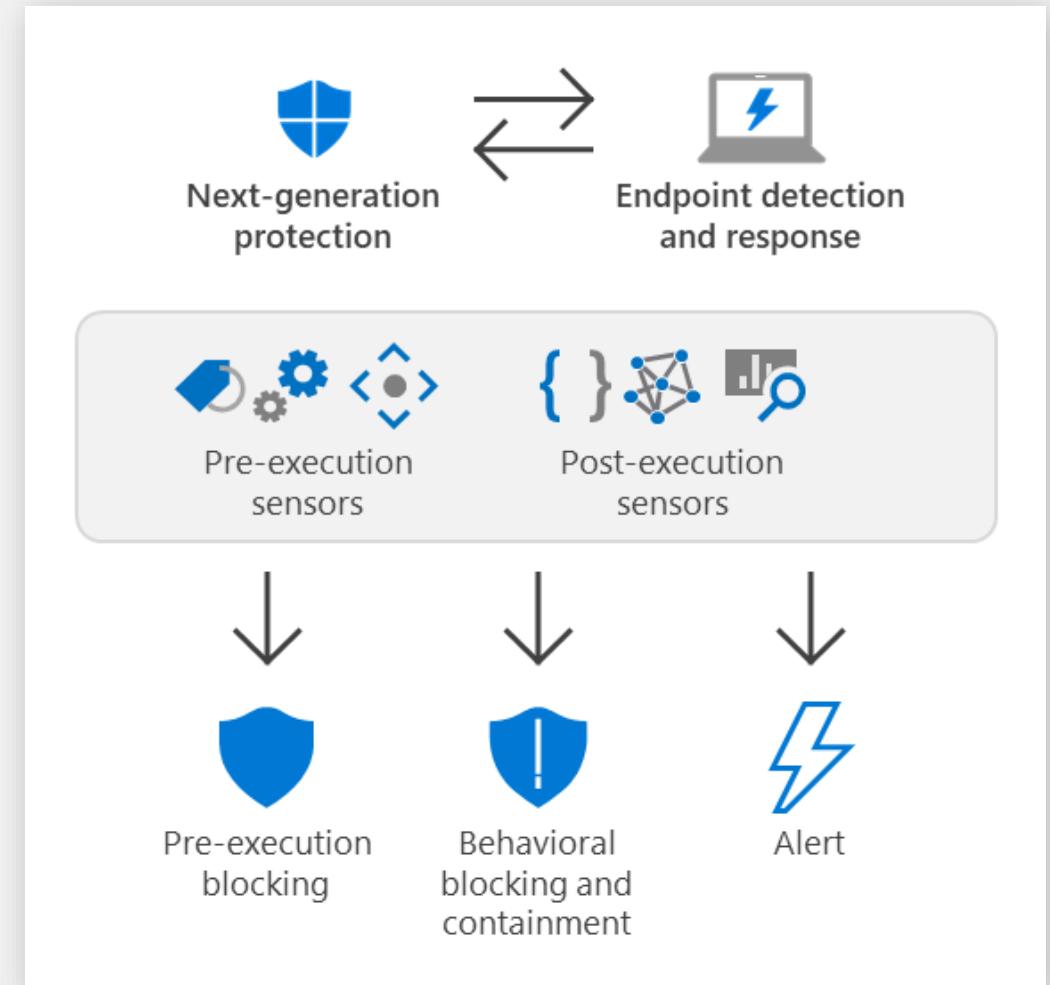
- Immediately stops threat before it can progress
- Microsoft has the unique ability to scan signals across kill chains and payloads (endpoints, Office, Identity, etc.)

→ 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



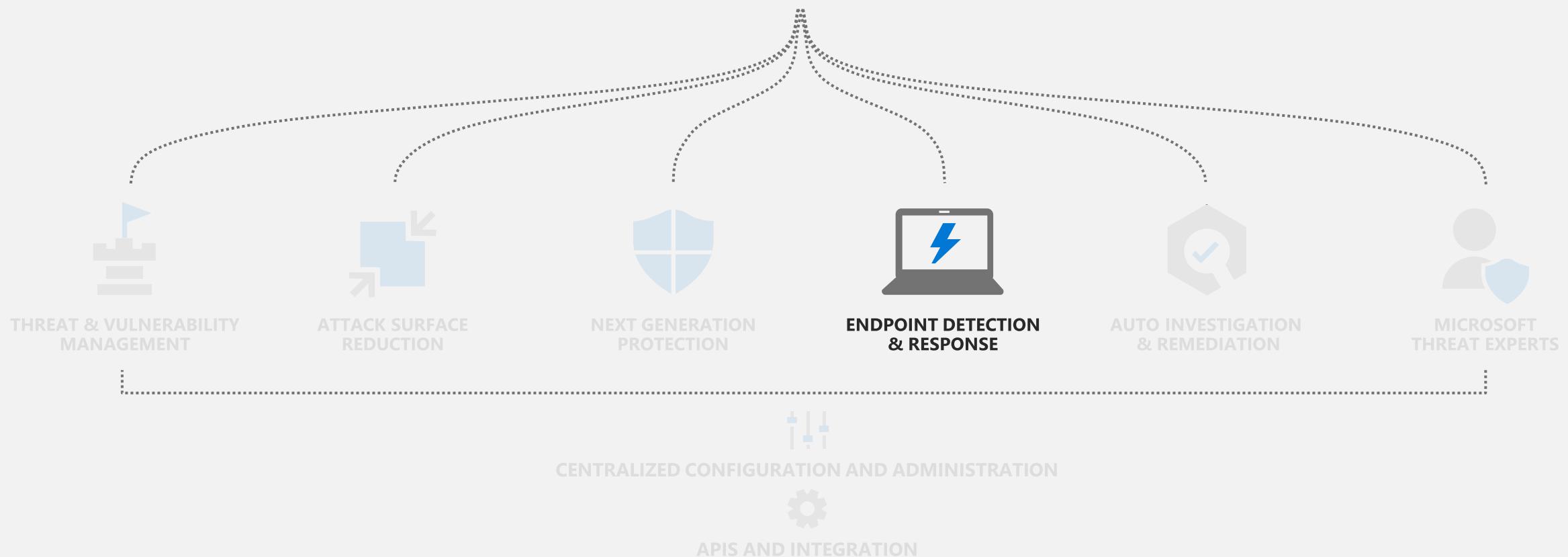
Read the [blog](#) for more details





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

Click on a URL



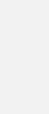
Exploitation

Installation



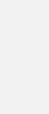
C&C channel

Persistency



Privilege escalation

Reconnaissance



Lateral movement

! 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



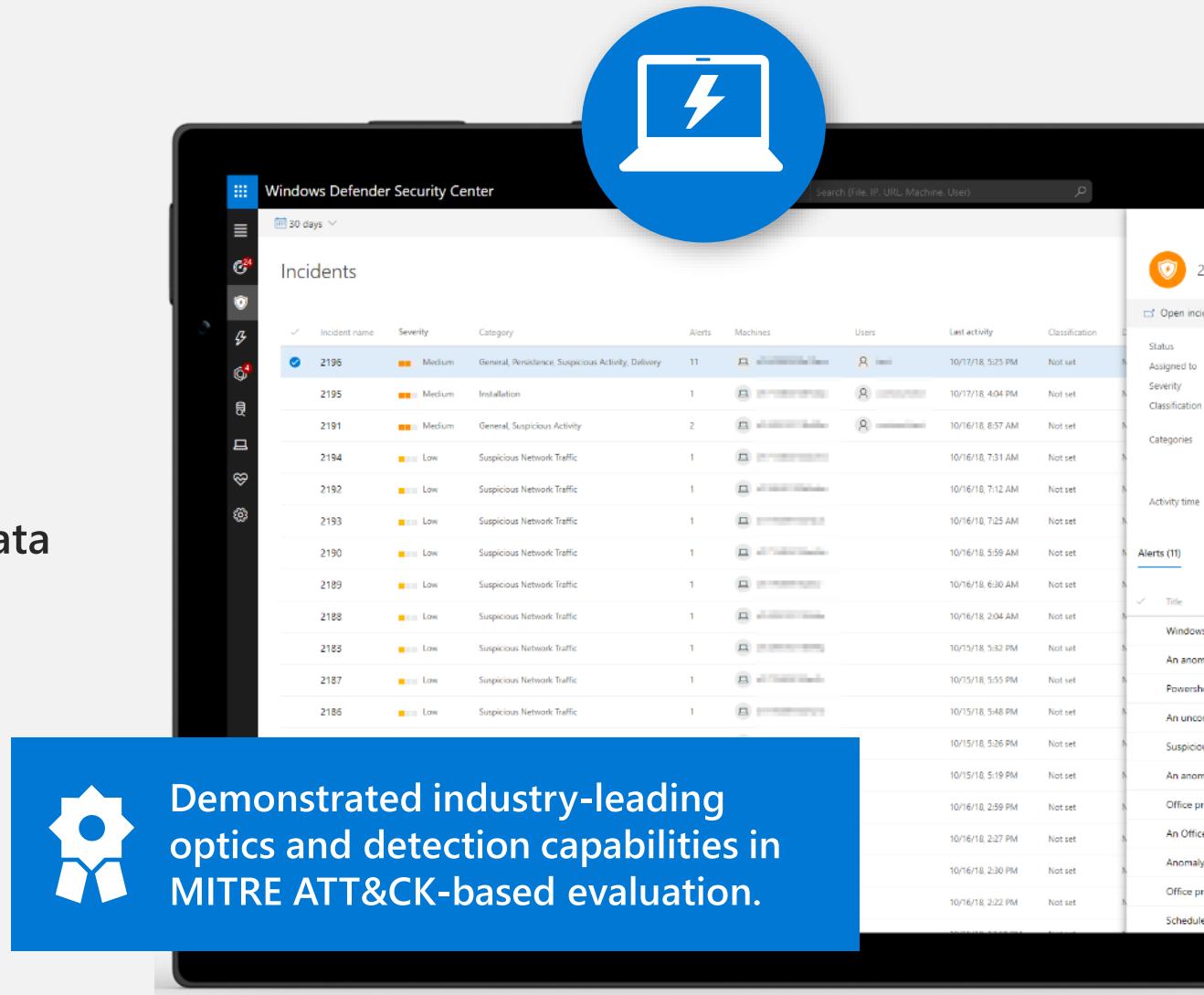
Correlated behavioral alerts



Investigation & hunting over 6 months of data



Rich set of response actions



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.

The screenshot displays a comprehensive security investigation interface across four main panels:

- Alerts > COM hijacking:** Shows an alert for "COM hijacking" with severity Medium, category Persistence, and detection source EDR. It includes a description of the technique, recommended actions (Validate the alert, Check for other suspicious activity, Locate unfamiliar processes, Submit relevant files for deep analysis), and a process execution tree showing the flow from sdclt.exe to control.exe to powershell.exe.
- Files > control.exe:** Provides file details for control.exe, including SHA1, SHA256, MD5, and size. It shows an event for "control.exe created process powershell.exe" on Aug 15, 2019, at 5:39:38.755 PM on machine apt29-client3.
- reg.exe:** Shows details for reg.exe, including execution time (Aug 13, 2019, 4:06:24.922 PM), path (C:\Windows\System32), integrity level (High), and access privileges (Elevated). It lists a command line: "reg.exe" import C:\Users\lilly.jarvis\AppData\Local\Temp\sk.reg and a SHA1 hash: 077aa479a2c23d3709324f214d19dc0ef041c8.
- Machines > apt29-client3:** Displays the machine timeline for apt29-client3 from July 2019 to December 2019. A highlighted alert for "COM hijacking" is shown. The timeline includes various events such as registry key changes, file creation, and PowerShell command execution. A sidebar provides device details like domain (apt29.org), OS (Windows 10 x64, Version 1903, Build 18362), and health state (Inactive).
- Event Timeline:** A large panel showing a timeline of events from August 8, 2019, to August 15, 2019. Events include "Event of type [CollectInvestigationPackageResponse] observed on machine", "COM hijacking", and multiple registry key changes for "HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run".
- Filters:** A sidebar on the right for filtering events by event group (Any, ASR events, Alert related events, etc.) and specific categories like Antivirus events, Application Guard events, File events, Network events, Other events, Process events, Registry events, Response actions events, Scheduled task events, Smart Screen events, and User activity events.

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.

The screenshot displays the Microsoft Defender Security Center interface. The main window shows a list of incidents, each with a unique ID, severity (e.g., Medium, High), categories (e.g., Execution, Persistence), active alerts, machines affected, detection sources (e.g., EDR, Custom detection), first activity, last activity, and status. A specific incident, 77196, is selected and expanded. The detailed view for incident 77196 includes:

- Overview:** Shows 11/11 active alerts, 3 MITRE attack categories (No other alert categories), and a timeline of events from Nov 28, 2019, to Dec 2, 2019.
- Alerts and categories:** Lists 11/11 active alerts across three MITRE attack categories.
- Scope:** Details the affected device as desktop-bga19q8, which is identified as a top affected asset with a high risk level/investigation priority.
- Evidence:** Shows 10 entities found, with a legend indicating remediation status: Remediated (green), Not Found (blue), Unremediated (red), and Other (grey).

The timeline of events for incident 77196 includes:

- Nov 28, 2019, 8:56:39 AM | New Windows 10 Machines on desktop-bga19q8
- Nov 28, 2019, 8:53:37 AM | New Suspicious Power Shell command line on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:53:07 AM | New Suspicious behavior by Microsoft Word was observed on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:53:07 AM | New An Office application ran suspicious commands on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New Suspicious Power Shell command line on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New Office process dropped and executed a PE file. on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New Powershell dropped a suspicious file on the machine on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New An anomalous scheduled task was created on desktop-bga19q8 by user admin

The bottom of the timeline indicates the active period: First - Nov 28, 2019, 8:16:39 AM and Last - Dec 2, 2019, 10:01:01 AM.

[Announcement blog](#)

Advanced hunting with custom detection and custom response

The screenshot shows the Microsoft Defender Security Center interface, specifically the Advanced hunting section. The left sidebar contains navigation links like Schema, Shared queries, and Test. The main area displays a PowerShell query and its results.

Advanced hunting

Run query + New Save

```
// Finds PowerShell execution events that could involve a download.  
ProcessCreationEvents  
| where EventTime > ago(7d)  
| where FileName in ("powershell.exe", "POWERSHELL.EXE", "powershell_ise.exe", "POWERSHELL_ISE.EXE")  
| where ProcessCommandLine has "Net.WebClient"  
| or ProcessCommandLine has "Downloadfile"  
| or ProcessCommandLine has "Invoke-WebRequest"  
| or ProcessCommandLine has "Invoke-Shellcode"  
| or ProcessCommandLine contains "http"  
| project EventTime, ComputerName, InitiatingProcessFileName, FileName, ProcessCommandLine  
| top 100 by EventTime
```

Get started PowerShell downloads

Last 7 days Create detection rule

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 12:51:10 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	tk5-3wp03r0809.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 18:35:42 PM	tk5-3wp03r0813.cfdev.nttest.microsoft.com	cmd.exe	powershell.exe

Filters

ComputerName

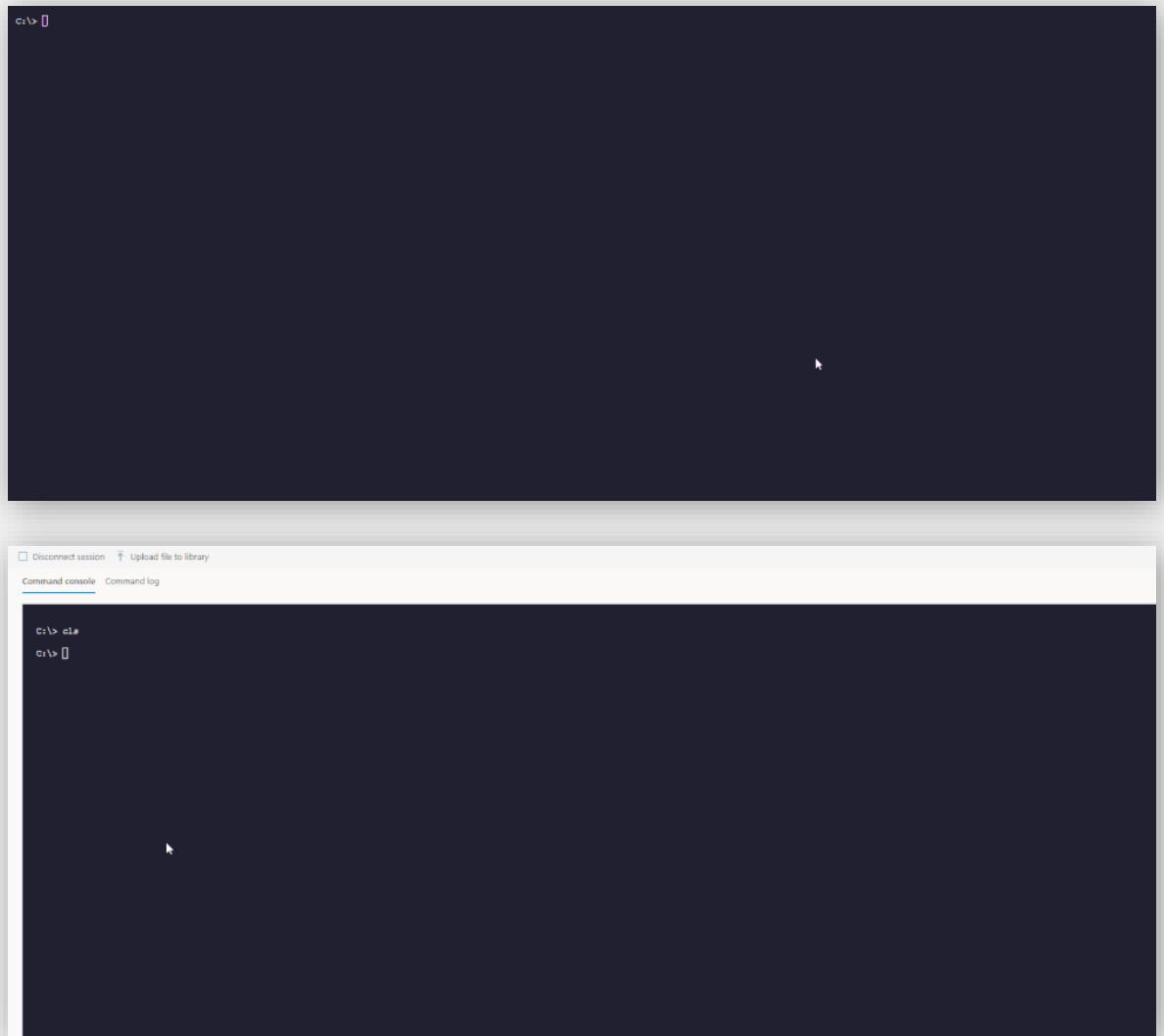
InitiatingProcessFileName

FileName

ProcessCommandLine

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

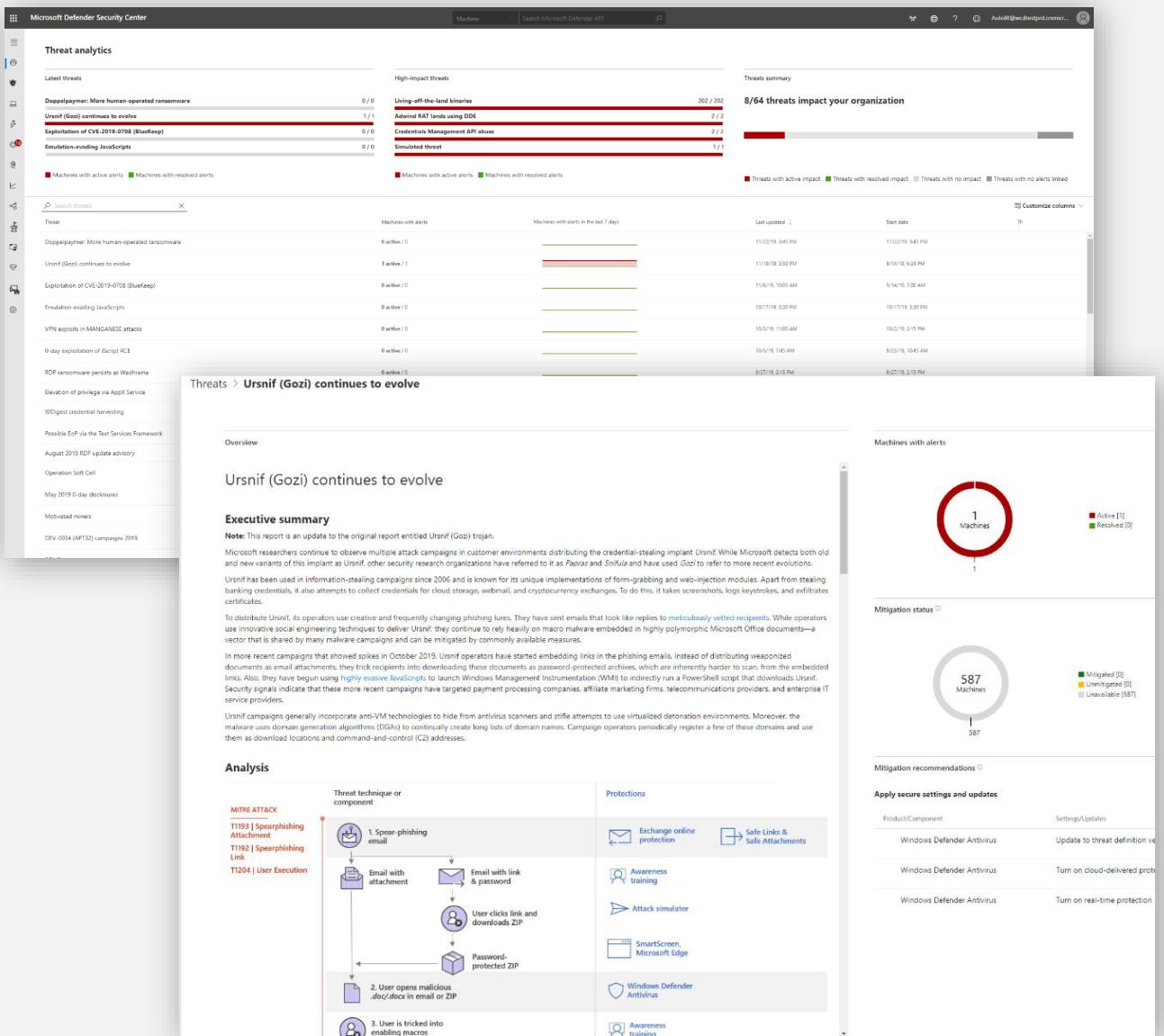
See how you score against significant and emerging campaigns with interactive reports.

Identify unprotected systems

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

Get guidance

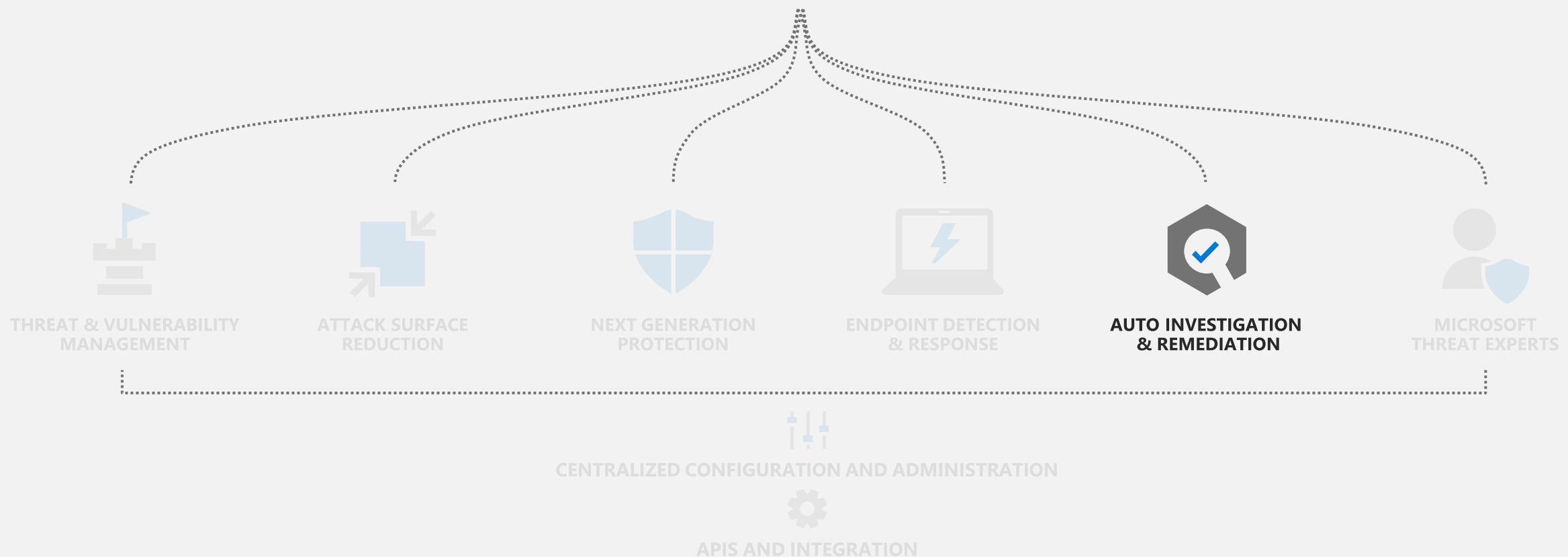
Provides recommended actions to increase security resilience, to prevention, or contain the threat.





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

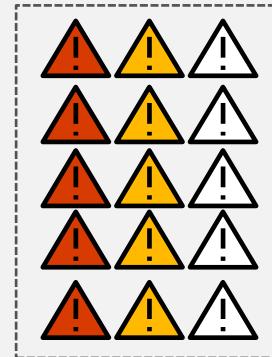


Talent shortage in
cybersecurity



Analysts overwhelmed by manual alert
investigation & remediation

Alert queue



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



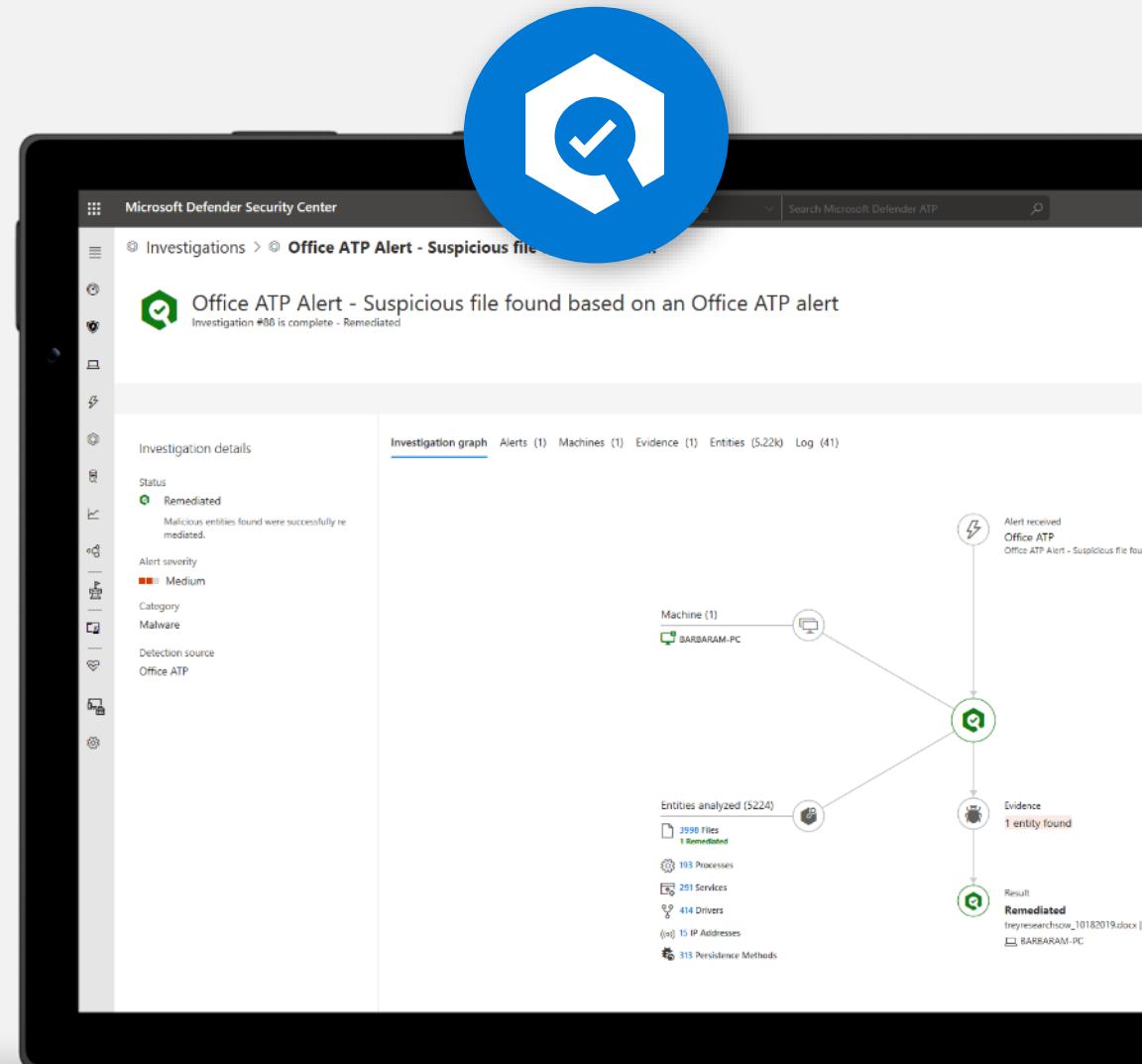
Mimics the ideal steps analysts would take



Tackles file or memory-based attacks



Works 24x7, with unlimited capacity



Auto investigation queue

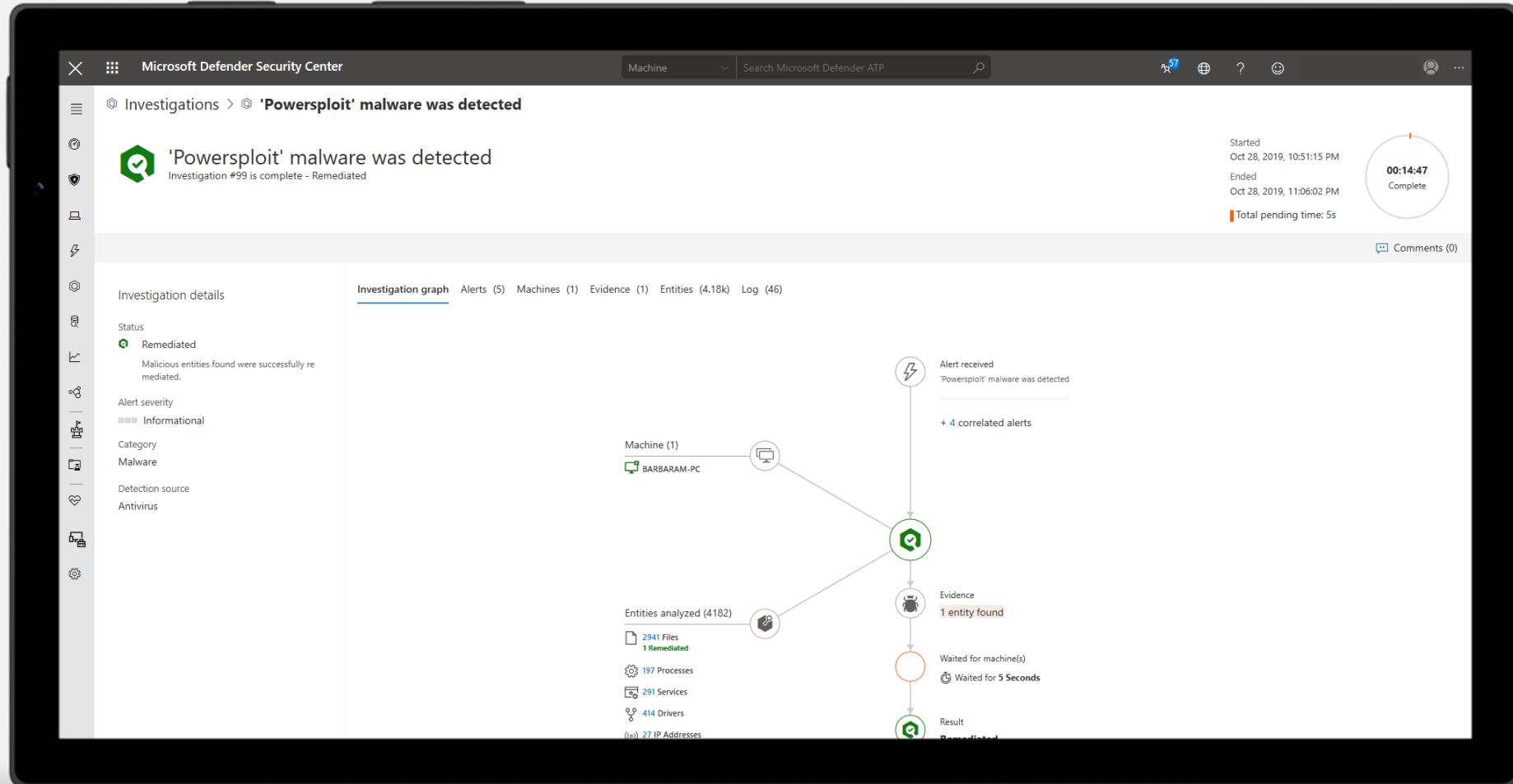
The screenshot shows the Microsoft Defender Security Center interface, specifically the 'Automated Investigations' section. The left sidebar features a dark theme with various navigation icons. The main area has a light background with a header bar containing 'Microsoft Defender Security Center', 'Machine', a search bar, and several status indicators.

The central part of the screen displays a table titled 'Automated Investigations' with the following columns: ID, Status, Detection Source, Entities, Start Date, and Duration. The table lists 20 entries, each corresponding to a different threat detection or investigation event. The 'Status' column includes icons for Remediated, No threats found, and Terminated by system.

On the right side, there is a 'Filters' panel with three expandable sections: 'Status', 'Triggering alert', and 'Detection Source'. Each section contains a list of filter options with checkboxes. For example, under 'Status', 'Any' is checked, while 'Remediated' is also listed. Under 'Triggering alert', several specific alerts are listed, such as 'Powersploit' malware detected and 'Hacktool Mimikatz detected'. Under 'Detection Source', 'Any' is checked, along with 'Antivirus', 'EDR', 'OfficeATP', and 'AutomatedInvestigation'.

ID	Status	Detection Source	Entities	Start Date	Duration
99	Remediated	Antivirus	bararam-pc.mtpdemos.net	10/28/19, 10:51 PM	14:47m
98	Remediated	OfficeATP	bararam-pc.mtpdemos.net	10/26/19, 2:05 AM	15:40m
94	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/23/19, 6:10 PM	13:33m
93	Partially investigated	AutomatedInvestigation	bararam-pc.mtpdemos.net	10/23/19, 5:41 PM	1:14h
92	No threats found	AutomatedInvestigation	andrewf-pc.mtpdemos.net	10/21/19, 4:07 PM	21:55m
91	Remediated	EDR	bararam-pc.mtpdemos.net	10/19/19, 8:31 AM	1:29h
90	Remediated	EDR	bararam-pc.mtpdemos.net	10/18/19, 10:32 PM	1:32h
89	Partially remediated	Antivirus	andrewf-pc.mtpdemos.net	10/18/19, 9:48 PM	1:07h
88	Remediated	OfficeATP	bararam-pc.mtpdemos.net	10/18/19, 9:06 PM	16:25m
85	No threats found	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/17/19, 4:01 AM	42h
84	No threats found	AutomatedInvestigation	bararam-pc.mtpdemos.net	10/16/19, 5:50 PM	2d
83	Terminated by system	AutomatedInvestigation	aarifs-pc	10/16/19, 10:02 AM	3d
80	No threats found	AutomatedInvestigation	bararam-pc.mtpdemos.net	10/11/19, 3:33 PM	4:55h
77	Terminated by system	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/10/19, 3:29 PM	3d
75	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/10/19, 2:50 PM	13:12m
73	No threats found	Antivirus	bararam-pc.mtpdemos.net	10/5/19, 7:16 AM	7:32m

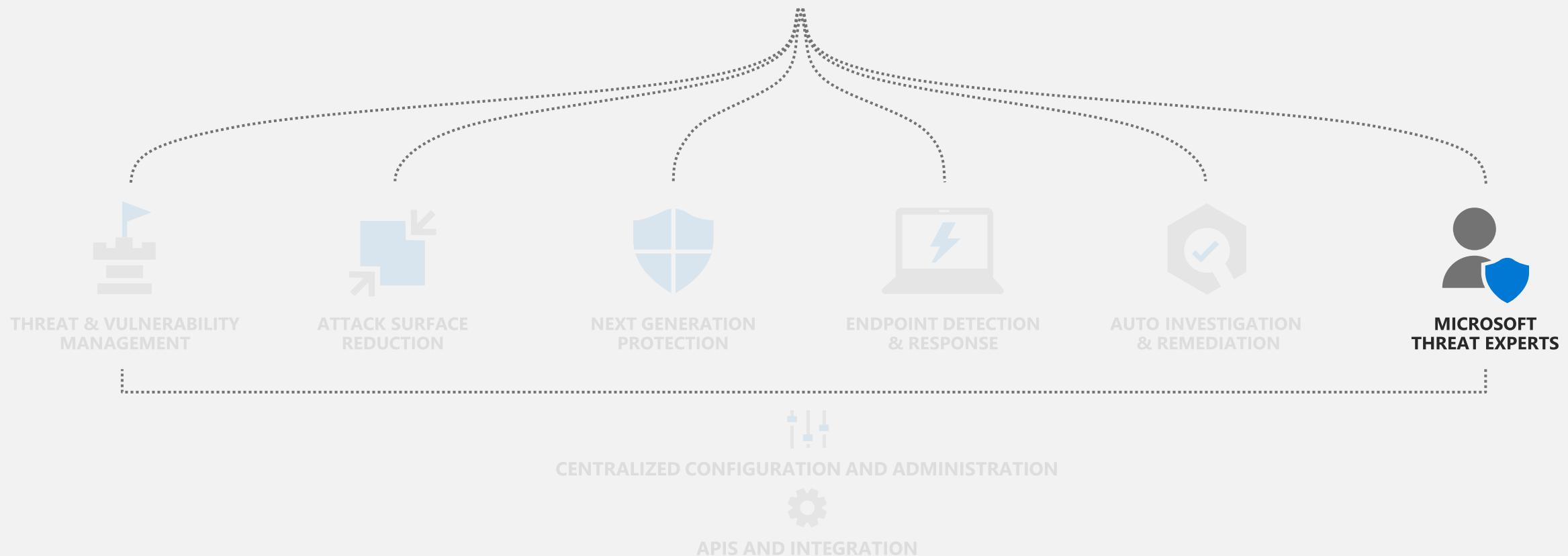
Investigation graph





Microsoft Defender for Endpoint

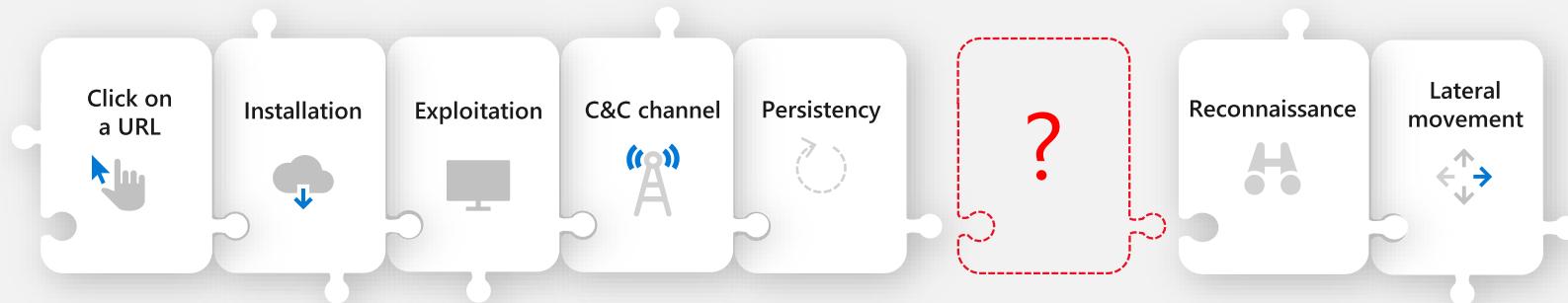
Built-in. Cloud-powered.



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.

The screenshot displays three windows from the Microsoft Defender Security Center:

- Microsoft Defender Security Center - Alerts:** Shows a single alert titled "Detection of file linked to adversary with supp..." with a severity of High and category Execution. It includes details like "This alert is part of incident (54693)" and "Actions".
- Windows Defender Security Center - Software Supply Chain Attack:** A dashboard showing 10 active alerts (High 4, Medium 4, Low 2, Informational 0), related evidence (Machines 6, Users 6, Mailboxes 1, Files 8), and a timeline from Jul 03, 2018, 9:26 AM to Jul 03, 2018, 9:29 AM.
- Software Supply Chain Attack - Alert Detail:** A detailed view of an alert titled "Software Supply Chain Attack" (Severity: High) assigned to Dan Smith. It shows the alert originated from a suspicious PowerShell script and was detected by WDATP. The alert is listed in the "Alerts (5)" section of the main dashboard.

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

The screenshot shows the Microsoft Defender Security Center interface. A large blue circular icon with a white user silhouette and shield is overlaid on the top right. The main window displays an alert titled "Detection of file linked to adversary with supply chain attacks". The alert details include:

- Microsoft Threat Experts**
- BARIUM**
- Detection of file linked to adversary with supply chain attacks**
- This alert is part of Incident (54693)
- Actions** dropdown menu
- Severity:** High
- Category:** Execution
- Detection source:** Microsoft Threat Experts

Below the alert details, there are sections for **Description**, **Executive summary**, **Timeline of observed events**, and **Impacted machines**. The **Executive summary** notes a Windows Defender AV detection of 'Winnti' malware. The **Timeline of observed events** table shows three entries:

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

The **Impacted machines** section lists one machine:

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f150b76e9a22	Impacted machine 1
881ba9b12040d4576b5e09de73e5eb33de2c4ab4	[explore]
ab16cd1b09e5157791a569456a12659aae926901	[explore]
131.107.147.82	[explore]

On the right side of the screen, there are sections for **Alert context** (listing desktop c7ud4hh and janedoe), **Recommended actions** (with a numbered list of steps), **Recommendation summary** (with a numbered list of steps), and **Indicators of Compromise** (listing various file hashes with [explore] links).

[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)

Actions ▾

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

Automated investigation is not applicable to alert type

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.Xldha, 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)

Actions ▾

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

Automated investigation is not applicable to alert type

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.Xldha, 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)

Actions ▾

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

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

Alert context

Automated investigation is not applicable to alert type

- 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

Recommended actions

Recommendation summary

- Fully investigate the machine in question.
- 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.
- Enforce strong, randomized local administrator passwords. Use tools like LAPS.
- 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'.
- If you need immediate help from Microsoft Incident Response consider opening a [Premier support case](#).
- 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.Xldha, 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)

Actions ▾

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

Automated investigation is not applicable to alert type

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

Alert context

desktop-c7ud4hh
janedoe

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

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/da63707384104026513_-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?

Indicators of Compromise

IOC

Install (2).exe [explore]

InstallConfig.exe [explore]

InstallLauncher.exe [explore]

881ba9b12040d4576b5e09de73e5eb33de2e [explore]

ab16cd1b09e5157791a568456a12659aae926 [explore]

131.107.147.82 [explore]

Email *

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

Analyst@contoso.com

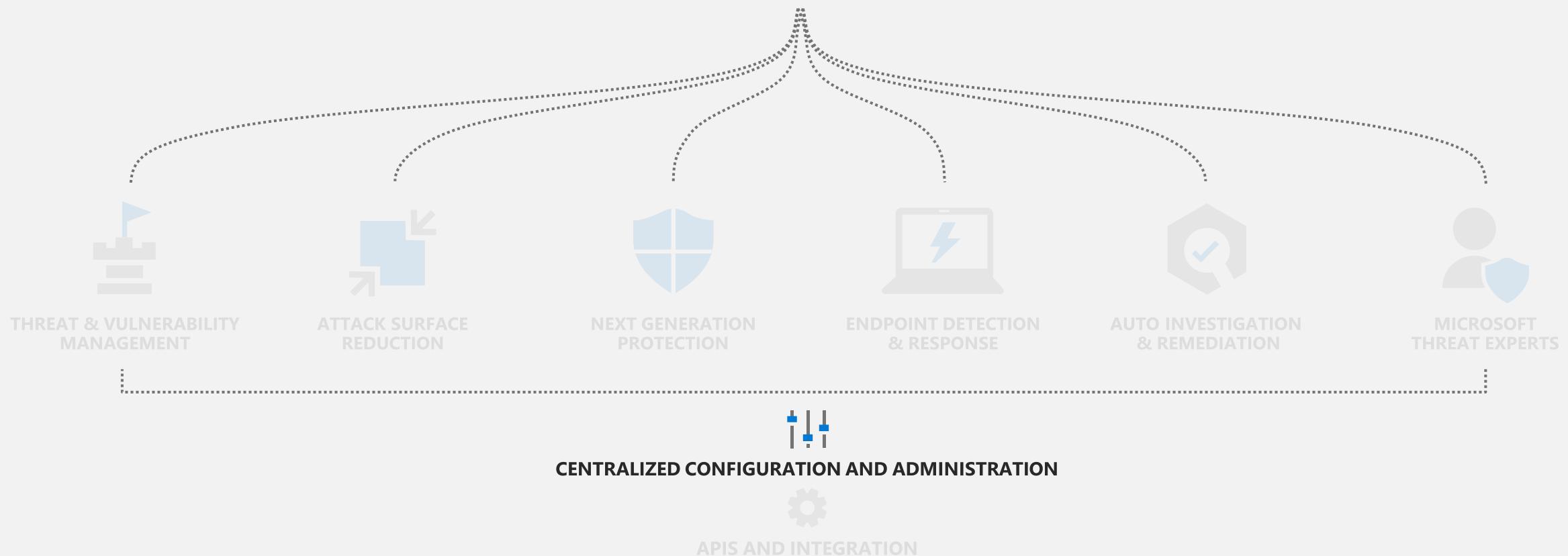
Submit

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



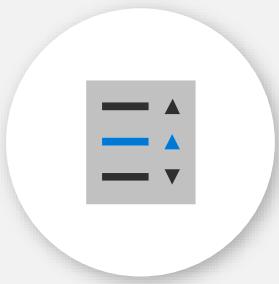
IT Team

- 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

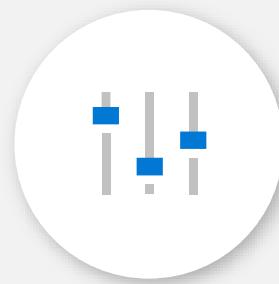
Customer needs



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

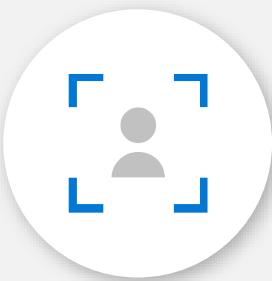
The screenshot displays the Microsoft 365 Security Center dashboard. At the top, there's a large blue circular icon containing three white 't' symbols. The dashboard is divided into several sections:

- Home**: Shows a Secure Score of 417 / 1000 (▲ 24 this month), OS update status (50% up-to-date), Device compliance (82% compliant), and Reports (108 affected devices, 239 incidents).
- Essentials**: Provides a breakdown of the Secure Score: Device score (800 / 520), Data score (40 / 230), Identity score (58 / 200), and App score (21 / 150).
- Scheduled reports**: Lists scheduled reports with their next execution time:
 - Secure Score - weekly report: Today, 12:00pm
 - Malware block trend - daily: Today, 12:00pm
 - Data loss prevention incidents: Tomorrow, 8:00am
 - Malware encounter volume: Tomorrow, 8:00am
- Risky users**: Shows 12 risky users with a total of 52 risk events, accompanied by small user profile icons.
- Reports**: Details data loss prevention incidents (239 incidents) and malware installation vectors (Top vector: e-mail in the past 30 days).

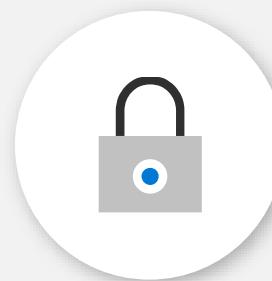
Endpoint Security Management



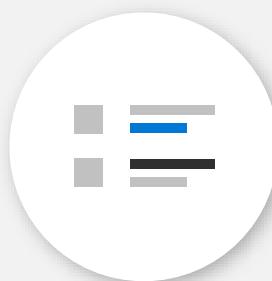
All
devices



Sec Admin
experiences



Security
baselines



Security
tasks

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

Seamless integration

The screenshot shows the Microsoft Defender Security Center Threat & Vulnerability Management dashboard. It features a central 'Exposure distribution' donut chart with a total of 11 items. To the left is a 'Configuration score' section with a score of 300 / 580. Below it is a 'Remediation activities' table:

Task	Status	Source	Created Date	Due Date	Assigned To
Update Windows 10	Pending	ATP	10/21/19, 11:58 AM	10/25/19, 6:56 PM	
Update Office	Completed	ATP	10/17/19, 1:34 PM	10/18/19, 8:32 PM	
Update Jre	Pending	ATP	10/21/19, 11:54 AM	10/23/19, 6:54 PM	
Update Vlc Media Player to version 3.0.8.0	Pending	ATP	10/21/19, 11:55 AM	10/22/19, 6:55 PM	
Update Python	Pending	ATP	10/21/19, 11:55 AM	11/08/19, 6:55 PM	
Update Visual Studio 2017	Pending	ATP	10/21/19, 11:56 AM	10/25/19, 6:56 PM	

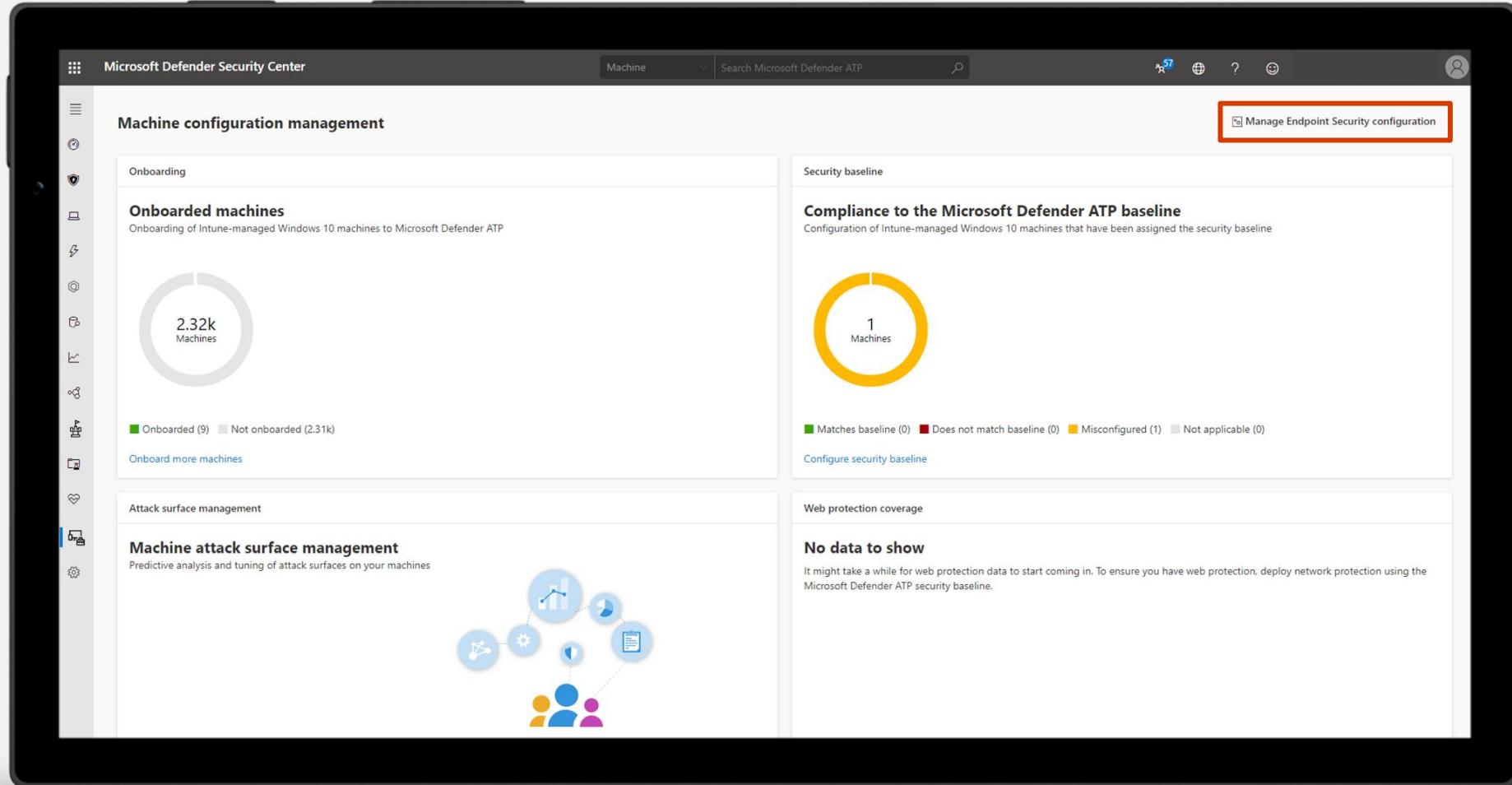
The screenshot shows the Microsoft Azure Device Security - Security tasks page. A large 'X' is overlaid on the interface. The table lists various security tasks:

Name	Priority	Status	Source	Impacted Devices	Created Date	Due Date	Assigned To
Update .net Framework	None	Pending	ATP		10/21/19, 11:58 AM	10/25/19, 6:56 PM	
Update Vlc Media Player to vers...	High	Completed	ATP		10/17/19, 1:34 PM	10/18/19, 8:32 PM	
Update Vlc Media Player to vers...	None	Pending	ATP		10/21/19, 11:54 AM	10/23/19, 6:54 PM	
Update Jre	Low	Pending	ATP		10/21/19, 11:54 AM	10/26/19, 6:54 PM	
Update Vlc Media Player to vers...	None	Pending	ATP		10/21/19, 11:55 AM	10/22/19, 6:55 PM	
Update Python	High	Pending	ATP		10/21/19, 11:55 AM	11/08/19, 6:55 PM	
Update Visual Studio 2017	Low	Pending	ATP		10/21/19, 11:56 AM	10/25/19, 6:56 PM	

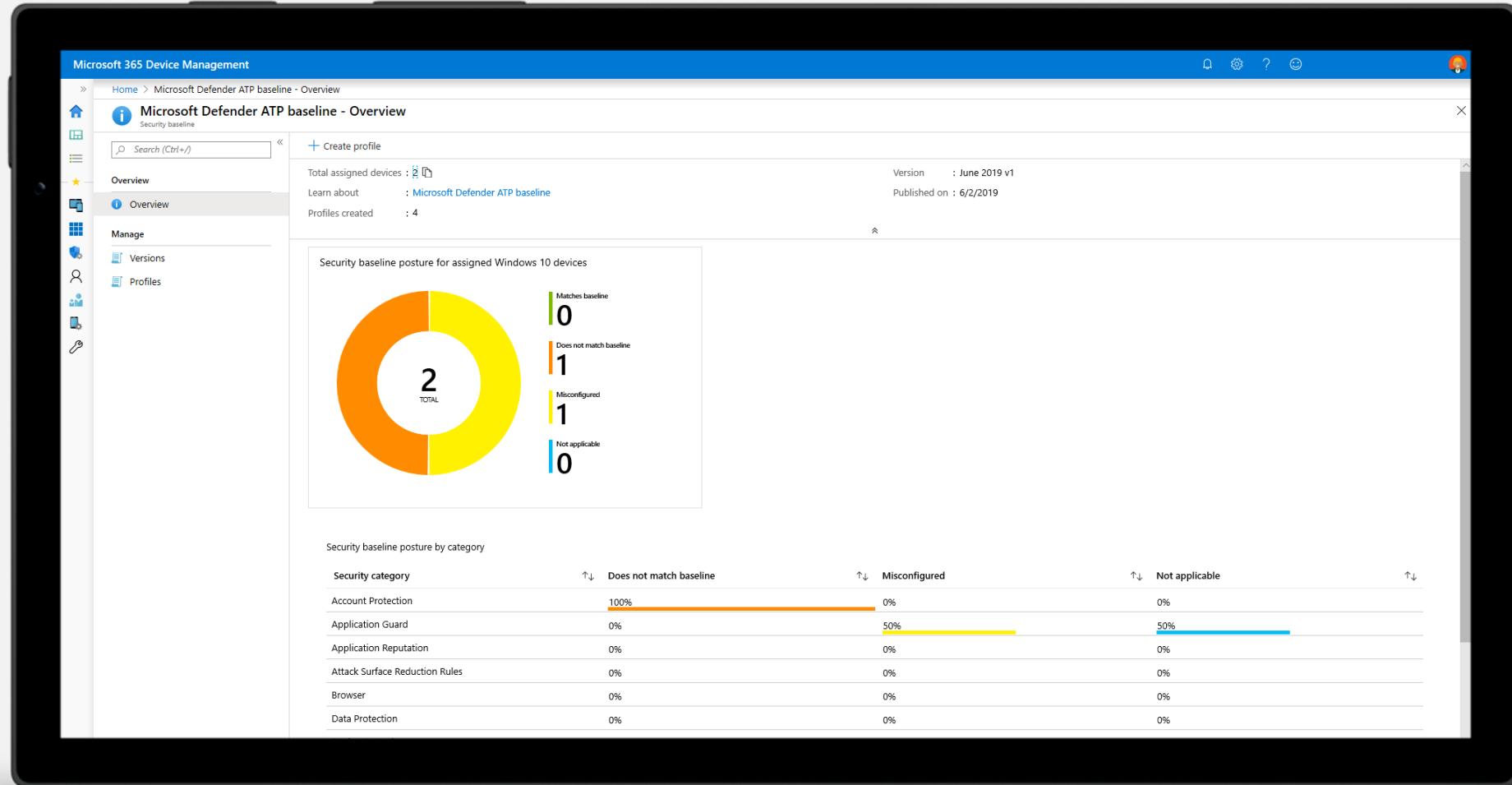
Microsoft Defender for Endpoint
Policy Assessment

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

The screenshot shows the Microsoft Defender for Endpoint dashboard on a tablet. The interface is dark-themed with white and light gray highlights. The left sidebar includes links for Home, Alerts, Reports (which is selected), Secure score, Hunting, Classification, Policies, Permissions, More resources, and Customize navigation. The main content area is divided into several sections:

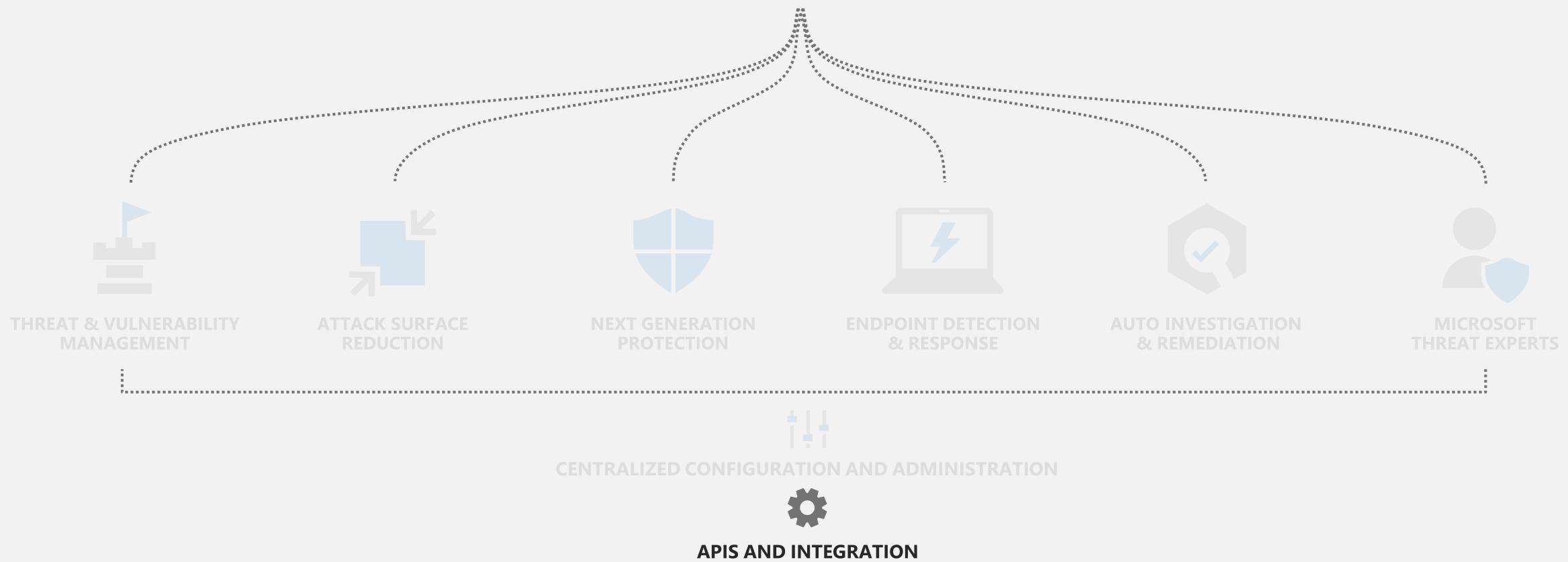
- Devices**:
 - Attack surface reduction rule detections**:
Possible malware or breach activity on your devices
23 detections, **1 unique files**, **1 affected devices**
Detections over time chart showing 23 detections on 10/22.
Legend: Audited (blue bar), Blocked (purple bar).
 - Attack surface reduction rules**:
No ASR rules are on
Configuration for behavioral rules from Windows Defender ATP that reduce the attack surface of your devices.
List of rules:
 - Block mode (purple square)
 - Audit mode (blue square)
 - Off (gray square)
 - Block Office applications from injecting code into other pr...
 - Block all Office applications from creating child processes
 - Block JavaScript or VBScript from launching downloaded e...
 - Block executable content from email client and webmail
 - Use advanced protection against ransomware
 - Block process creations originating from PSEXEC and WMI ...
 - Block Office communication application from creating chil...
 - Block Win32 API calls from Office macro
 - Block execution of potentially obfuscated scripts
 - Block executable files from running unless they meet a pre...
 - Block credential stealing from the Windows local security a...
 - Block untrusted and unsigned processes that run from USB
 - Block Adobe Reader from creating child processes
- Devices at risk**:
4 devices at risk

Device	Risk level
barbaram-pc	High (red triangle)
robertot-pc	Medium (orange triangle)
mtp-air-dc01	Medium (orange triangle)
mtp-air-web01	Low (yellow triangle)
- Device threat analytics**:
Assess your defenses against high-profile threats
Simulated threat: 0 / 1
Adwind RAT lands using DDE: 0 / 1
Living-off-the-land binaries: 0 / 1
Europium (Oilrig) persists, evades VMs: 0 / 1
- Device compliance**:
22% noncompliant
Intune device compliance status: 22% noncompliant (progress bar)
- Devices with active malware**:
No affected devices
Intune-managed devices with active, unresolved malware. Updated Today at 6:26 AM.



Microsoft Defender for Endpoint

Built-in. Cloud-powered.

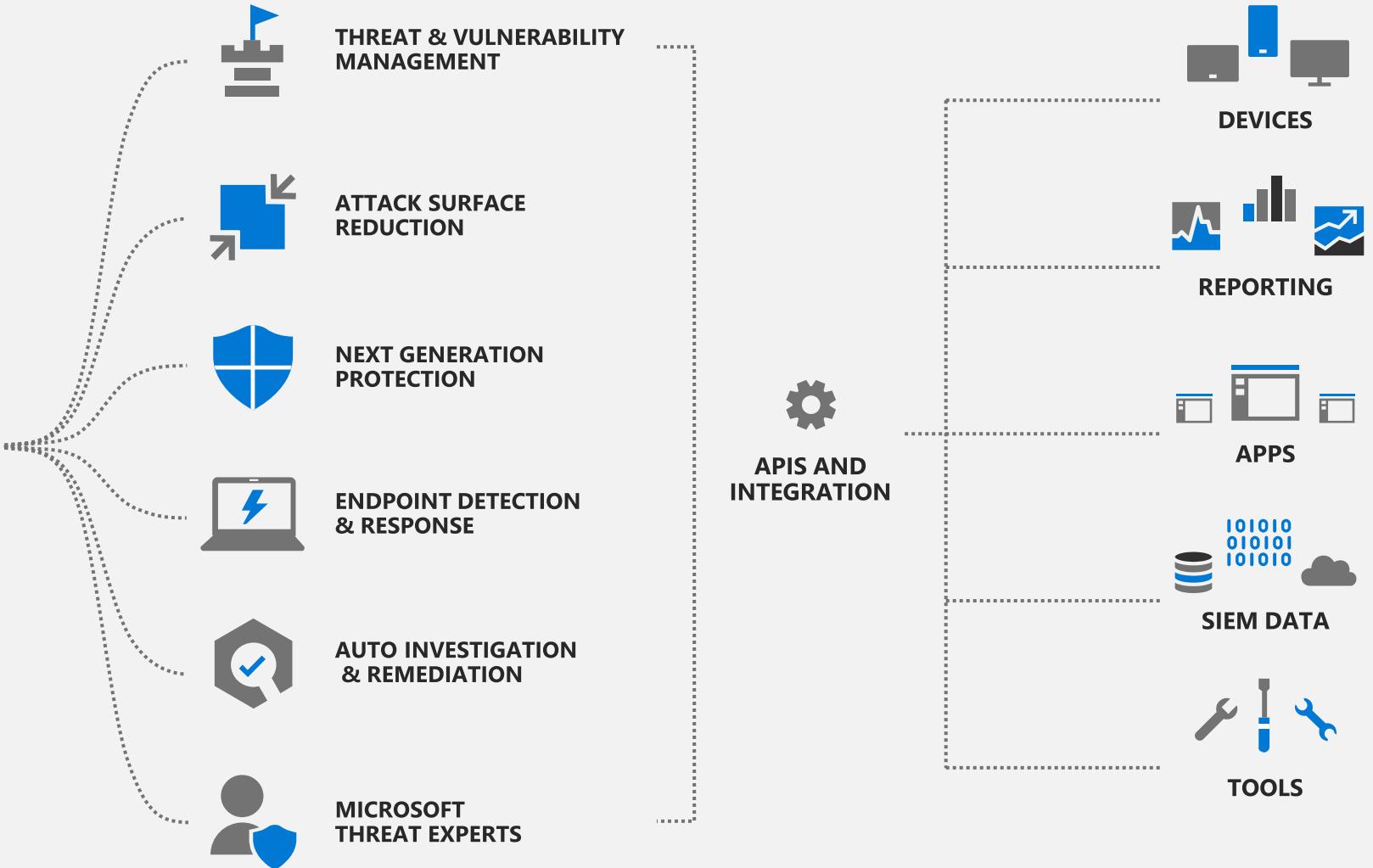


Connecting with the platform



Microsoft Defender for Endpoint

Built-in. Cloud-powered.



Microsoft Defender for Endpoint APIs & partners

Easy development & tracking of connected solutions

API Explorer

- Explore various Microsoft Defender for Endpoint APIs interactively

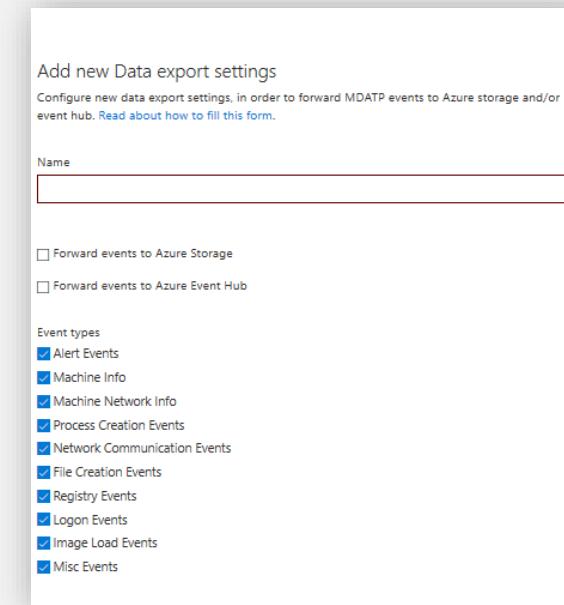
Integrated compliance assessment

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

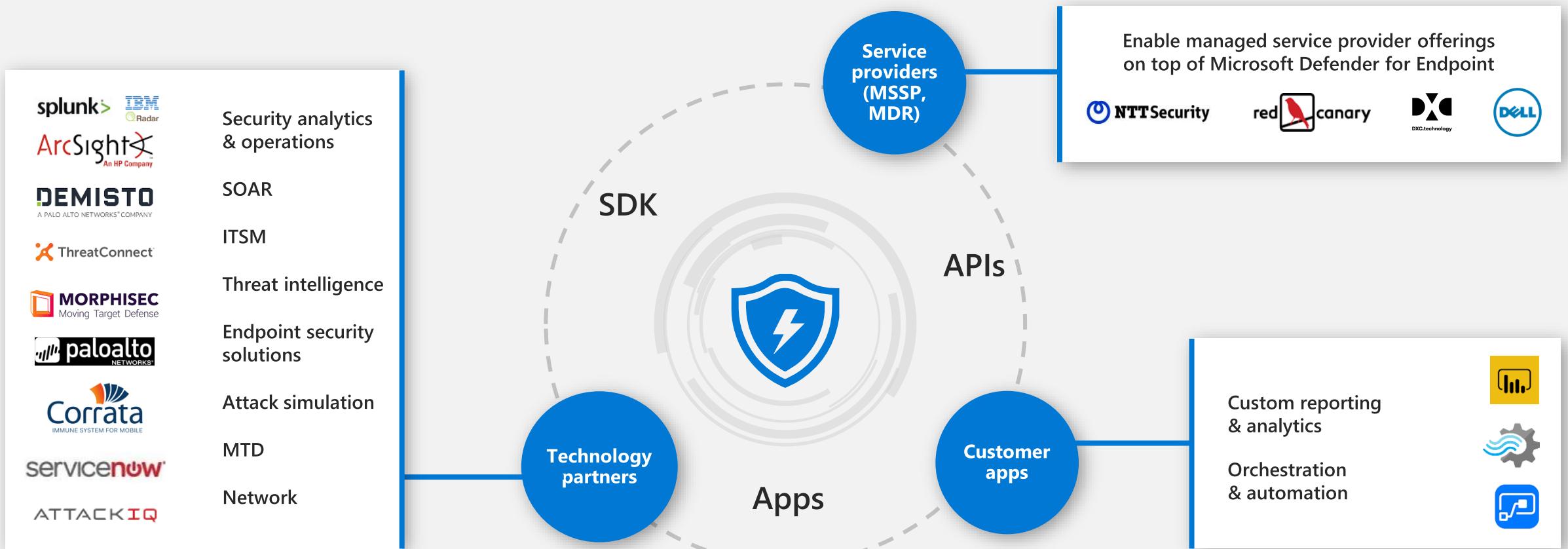
The screenshot shows two overlapping windows. The top window is the Microsoft Defender Security Center with a sidebar titled 'Connected applications' listing various services like cdocm-app, DefenderAV, DSRE Graph Reader, DSRE SOC Analyst Clients, JisooTestApp, Microsoft Graph, MSProtect Security Remover, and another instance of Microsoft Defender Security Center. Below this is the 'API Explorer' window, which has a 'Run Query' button, a dropdown menu set to 'GET', and a URL field containing 'https://api-us.securitycenter.windows.com/api/machines/?\$top=10'. The 'Request body:' field is empty. The 'Response body:' section shows a JSON response with a success status code of 200 and a duration of 412ms. The JSON output includes metadata about the machine, such as its ID, computer name, first seen date, last seen date, operating system platform, and version.

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 (Power BI, 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

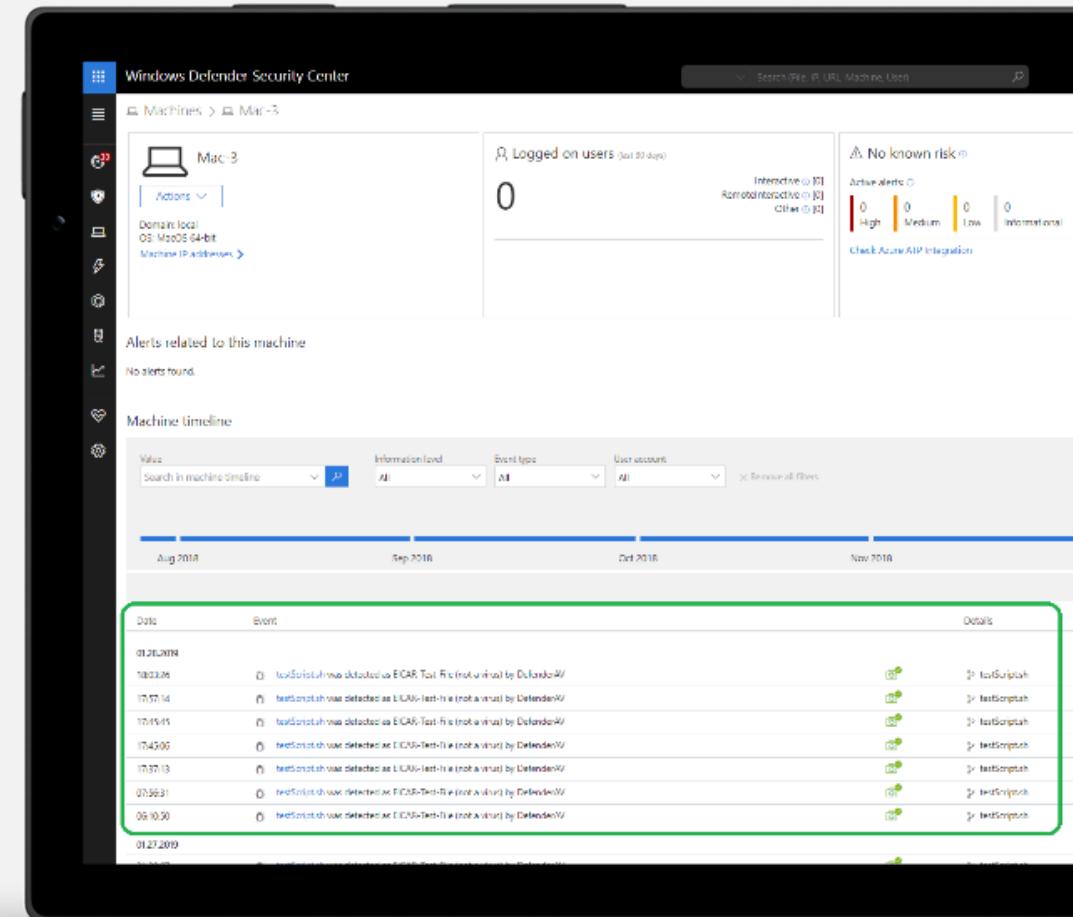
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

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)

```
File Edit View Search Terminal Help
parallels@t-ubuntu:~$ mdatp
-h [ --help ]          Display help
--trace                Begins tracing Microsoft Defender's activity
--verbose              Verbose output
--retry                Retry attempts to connect
--diagnostic            Gathers log files and packages them into a compressed file in the support directory
--definition-update    Checks for new definition updates
--pretty               Displays the output in human-readable format
--health [metric]       Display health information (Optional parameter, report just one metric)
--notice               Display third party notice
--logging              Logging options (see below)
--config [name] [value] Change configuration
--threat                Threat operations (see below)
--scan                  Scan operations (see below)
--exclusion             Exclusion operations (see below)
--connectivity-test     Run connectivity test
--edr                  EDR config (see below)

-logging options:
--set-level arg         Sets the current diagnostic logging level
--view-logs             Outputs the contents of log files to the terminal

-threat options:
--add-allowed arg       Adds allowed threat
--remove-allowed arg    Removes allowed threat
--get-details arg       Gets threat details
--list                  Lists all detected threats
--quarantine arg        Quarantines threat (by threat ID)
--restore arg           Restores threat (by threat ID)
--remove arg             Removes threat (by threat ID)
--type-handling [threat_type] [action] Changes the way certain threats are handled

-scan options:
--path path             Scans provided path
--quick                 Performs quick scan
--full                  Performs full system scan
--cancel                Cancels current scan (either quick, full or both)

-exclusion options:
--list                  List exclusions
--add-file arg          File path
--add-folder arg         Folder path
--add-extension arg     File extension
--add-process arg        Process name
--remove-file arg        File path
--remove-folder arg      Folder path
--remove-extension arg   File extension
```



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

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a vertical navigation bar with icons for Home, Threats, Machine, Reports, and Settings. The main area is titled "Evaluation progress" and shows a checklist of tasks: Setup (Completed), Setup in progress, Evaluation (100%), Connect to machine, Run simulations and tutorials, Review automated investigations, Hunt, Check for emerging threats, Finishing up, and Provide feedback. To the right, there's a section titled "Your evaluation lab" which says "Manage your test machines, attack simulations and reports. Learn and experience the Microsoft Defender ATP capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks." It shows "3 active machines": TestMachine1, TestMachine2, and TestMachine3, each with a progress bar at 8.61k / 8.64kh. There's also a "Need a pre-made simulation?" button and a "Report overview" section with metrics like 21 Alerts in 1 Incidents, 0 Actions taken in 3 Investigations, and 0 Key findings. At the bottom, there's a table titled "Test machines (3)" with columns for Machine name, Status, Time left, Risk level, Exposure level, Alerts number, and IP address. The three machines listed are all Active, with Medium risk and exposure levels, and 1 alert each.

Machine name	Status	Time left	Risk level	Exposure level	Alerts number	IP address
TestMachine1	Active	8610h	Medium	Medium	1	104.46.115.109
TestMachine2	Active	8610h	High	Medium	10	104.46.114.105
TestMachine3	Active	8610h	Medium	Medium	10	104.209.236.128



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>



THANK YOU!
