Microsoft Security

Microsoft Defender for Endpoint Overview

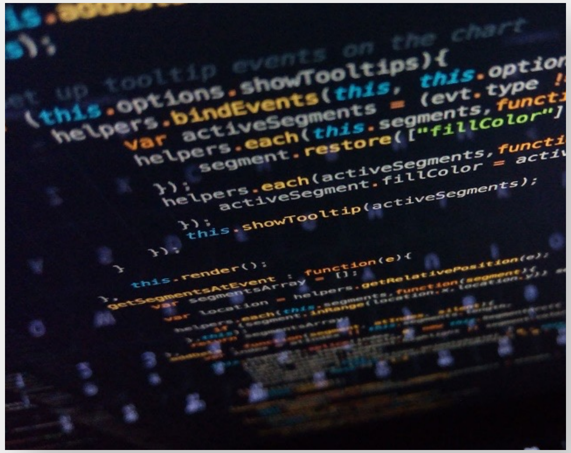
CROSSCIPHER TECHNOLOGIES PVT. LTD.

CROSS CIPHER

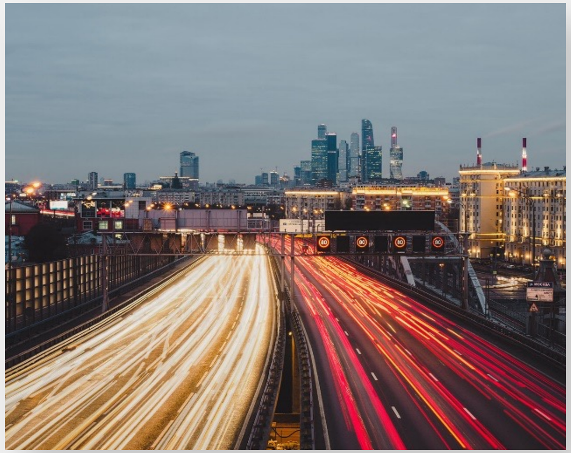
INDIA | SWITZERLAND | SINGAPORE

The era of flux and transformation

Everyone is now in the technology business



Conventional security tools have not kept pace

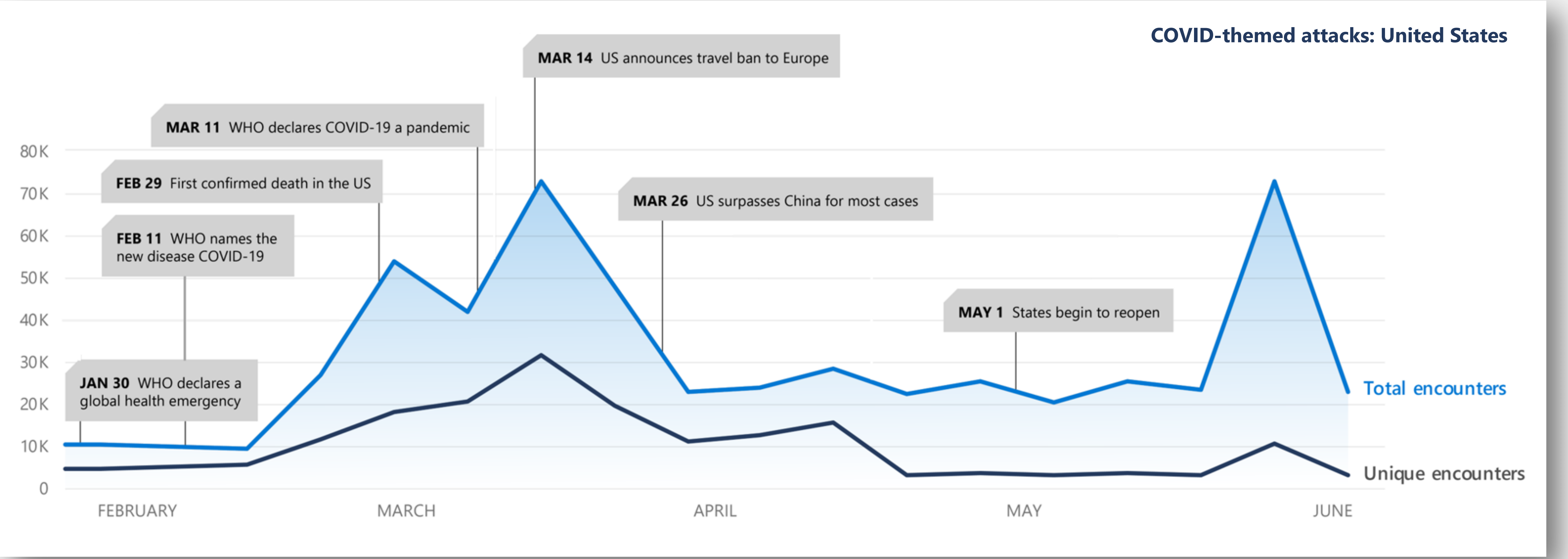


Security professionals alone can’t fill the gap

Regulatory requirements and costs are increasing

Today's threats: criminal groups follow opportunities

Malware encounters align with news headlines



JAN 30 WHO declares a global health emergency

FEB 11 WHO names the new disease COVID-19

FEB 29 First confirmed death in the US

MAR 11 WHO declares COVID-19 a pandemic

MAR 14 US announces travel ban to Europe

MAR 26 US surpasses China for most cases

MAY 1 States begin to reopen

Source: Microsoft Digital Defense Report 2020

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.

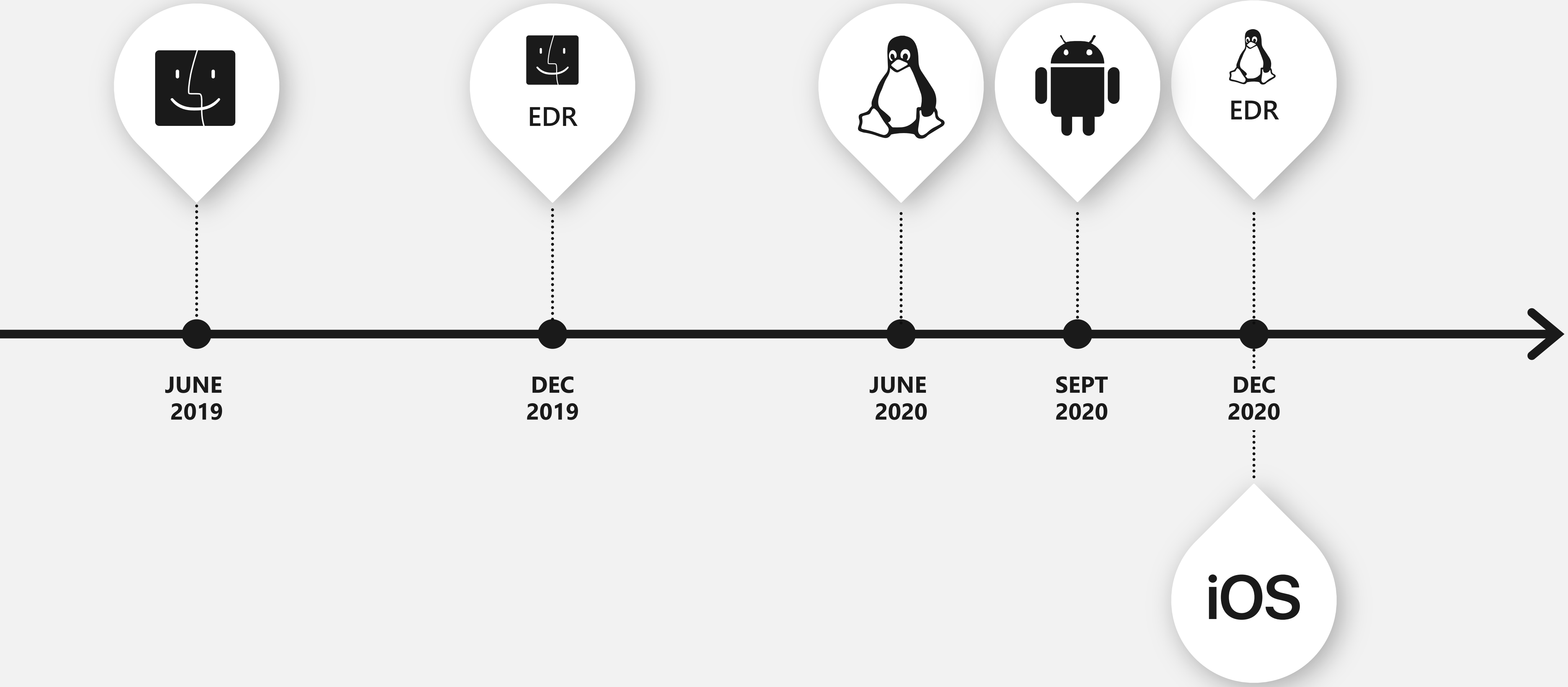
Our antimalware capabilities consistently achieve high scores in independent tests.

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

Microsoft won six security awards with Cyber Defense Magazine at RSAC 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 industry leading endpoint security across platforms



JUNE 2019

EDR

DEC 2019

JUNE 2020

SEPT 2020

EDR

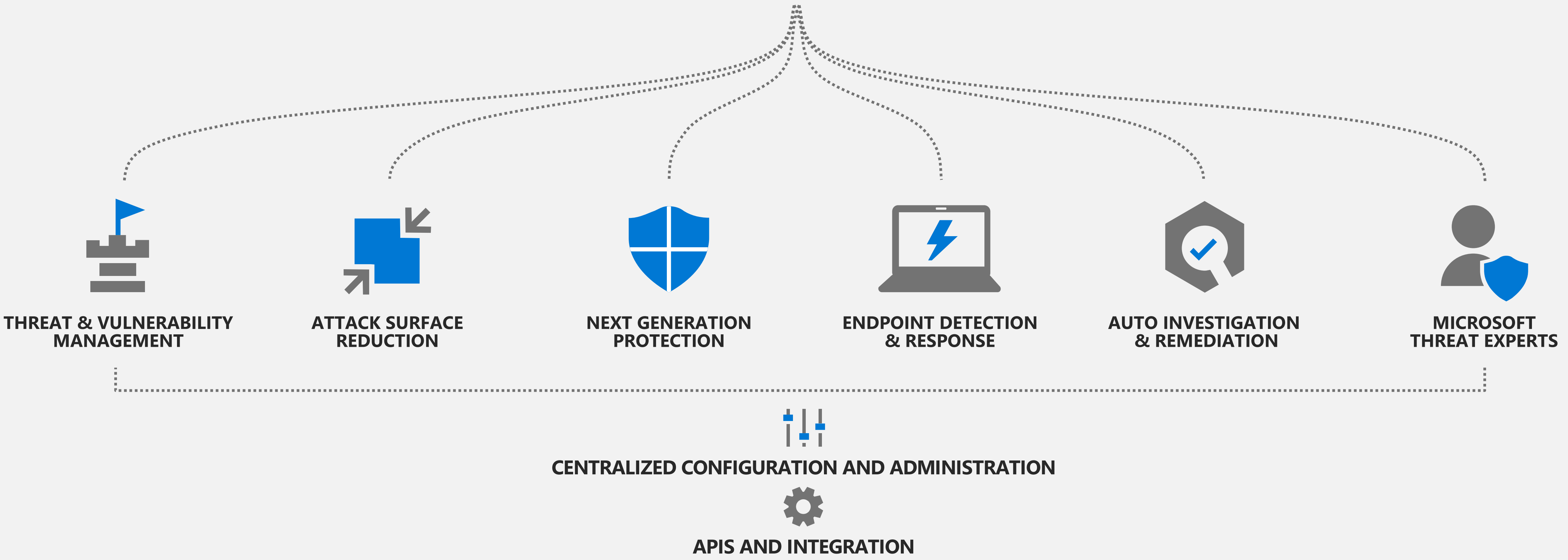
DEC 2020

iOS

General availability dates

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

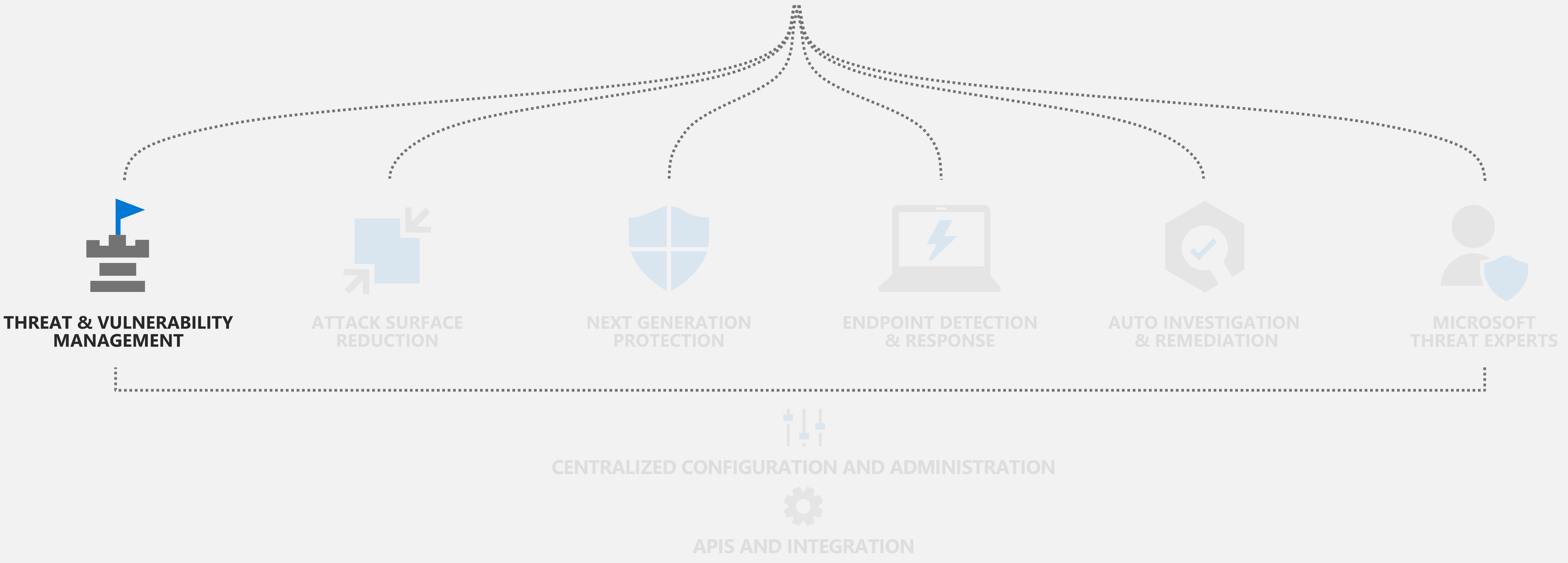
MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

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

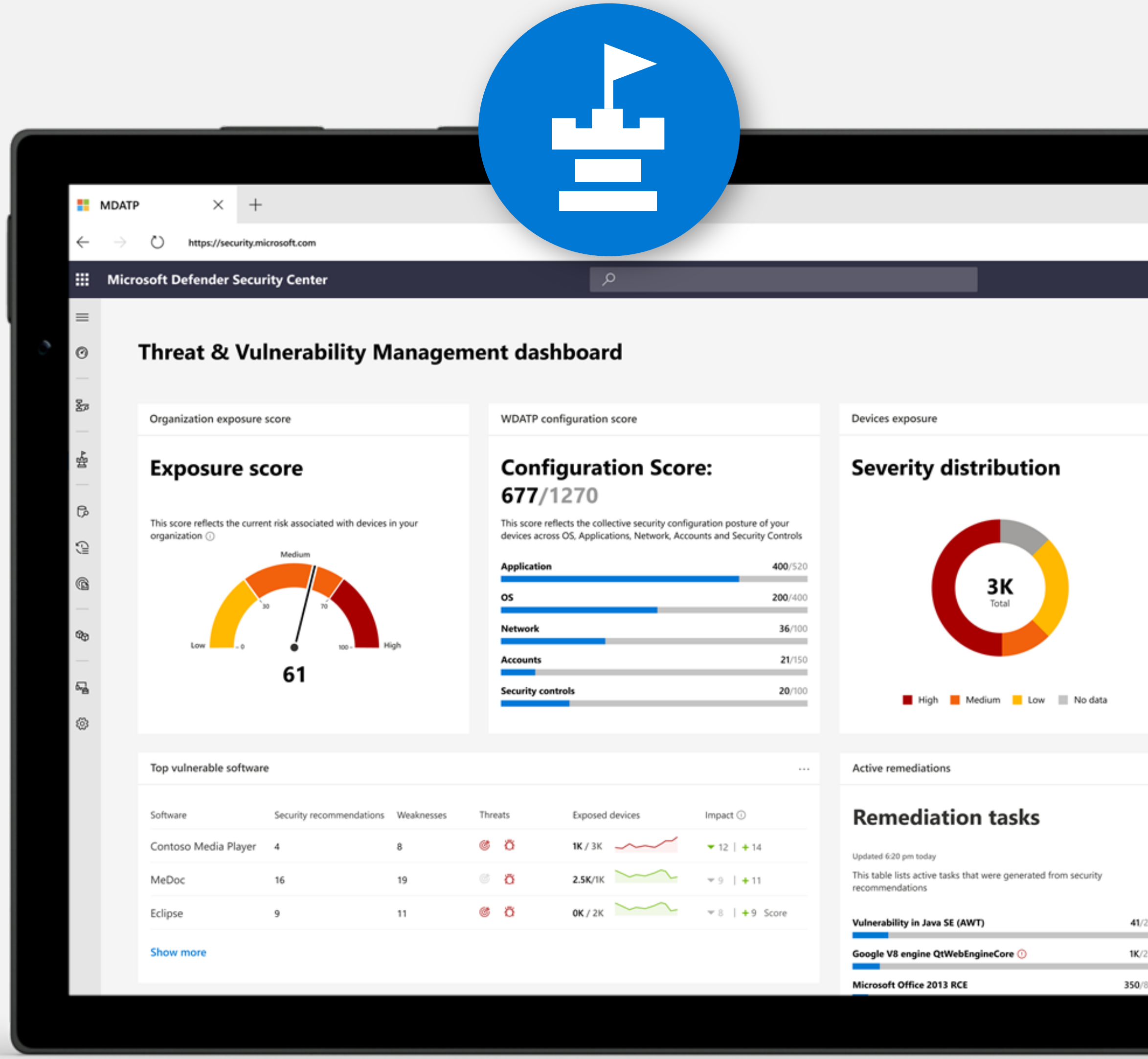
- → Waiting for a patch
- → No IT/Security bridge
- → Manual process
- → No validation

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



MDATP

https://security.microsoft.com

Microsoft Defender Security Center

Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current risk associated with devices in your organization ⓘ

WDATP configuration score

Configuration Score: 677/1270

This score reflects the collective security configuration posture of your devices across OS, Applications, Network, Accounts and Security Controls

Application	400/520
OS	200/400
Network	36/100
Accounts	21/150
Security controls	20/100

Devices exposure

Severity distribution

🟥 High 🟧 Medium 🟨 Low ⬜ No data

Top vulnerable software ···

Software	Security recommendations	Weaknesses	Threats	Exposed devices	Impact ⓘ
Contoso Media Player	4	8		1K / 3K	▼ 12 | + 14
MeDoc	16	19		2.5K/1K	▼ 9 | + 11
Eclipse	9	11		0K / 2K	▼ 8 | + 9 Score

Show more

Active remediations

Remediation tasks

Updated 6:20 pm today

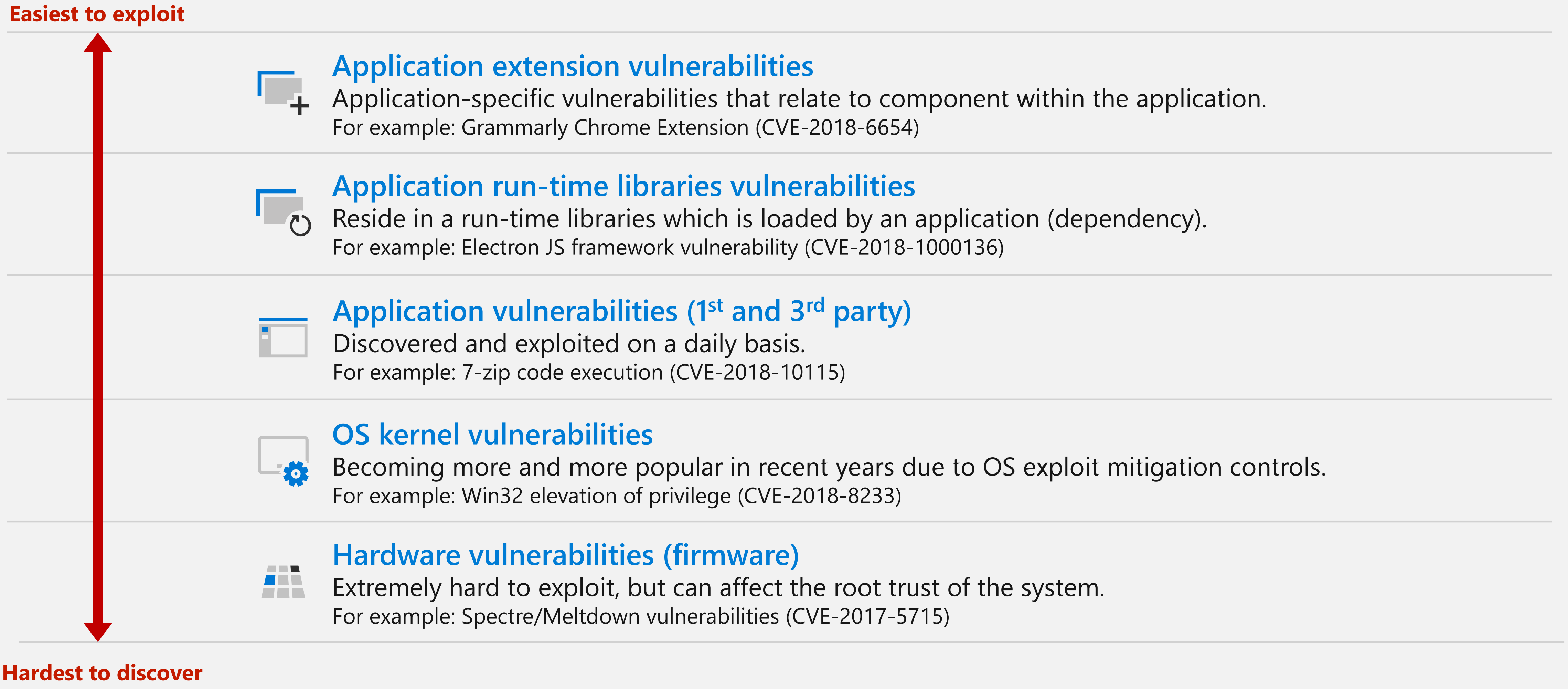
This table lists active tasks that were generated from security recommendations

Vulnerability in Java SE (AWT)	41/
Google V8 engine QtWebEngineCore ⓘ	1K/
Microsoft Office 2013 RCE	350/

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.

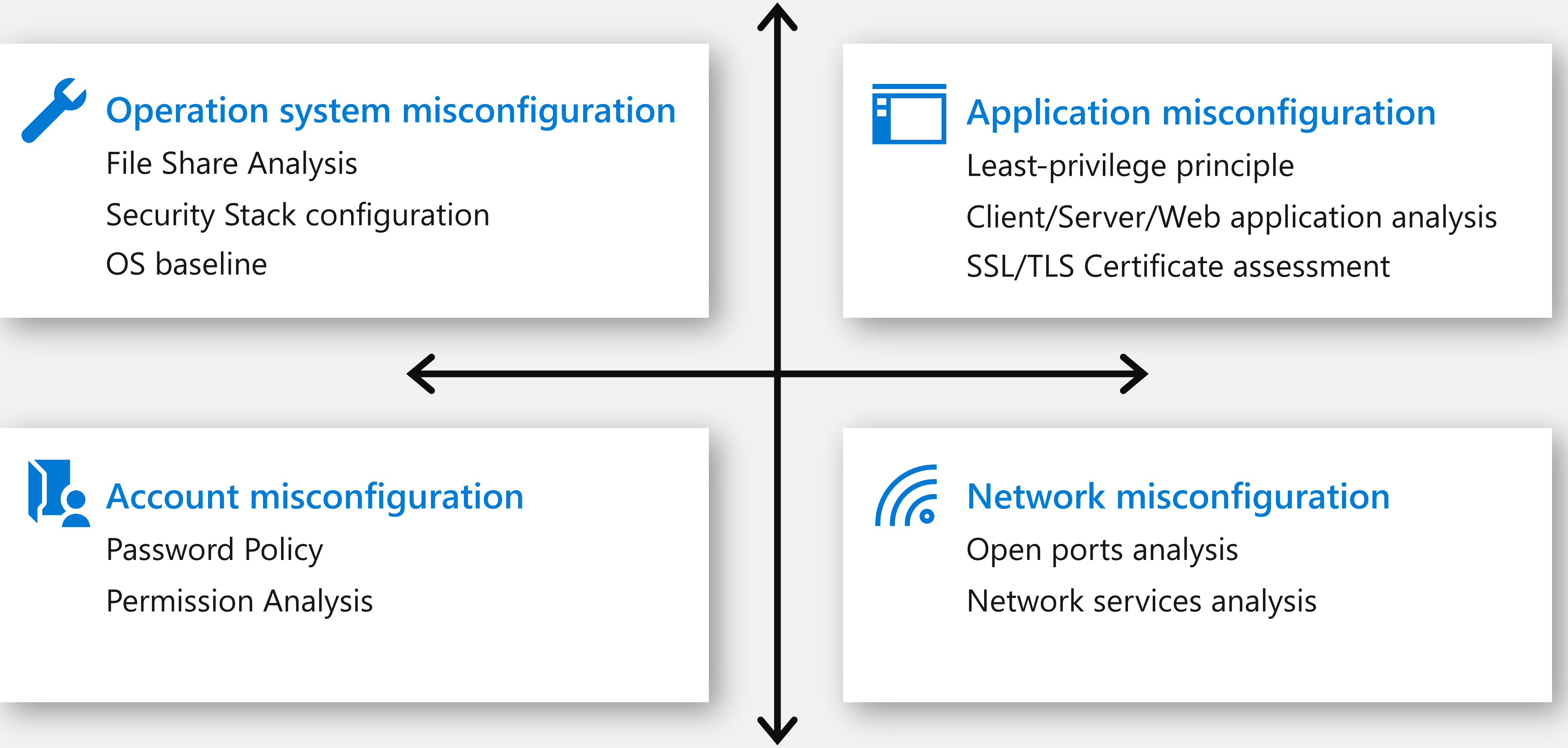
For example: Spectre/Meltdown vulnerabilities (CVE-2017-5715)

Hardest to discover

1

Continuous Discovery

Broad secure configuration assessment



Operation system misconfiguration

File Share Analysis

Security Stack configuration

OS baseline

Application misconfiguration

Least-privilege principle

Client/Server/Web application analysis

SSL/TLS Certificate assessment

Account misconfiguration

Password Policy

Permission Analysis

Network misconfiguration

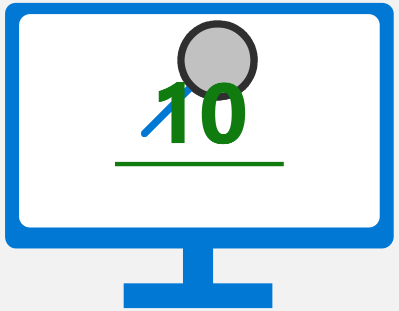
Open ports analysis

Network services analysis

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

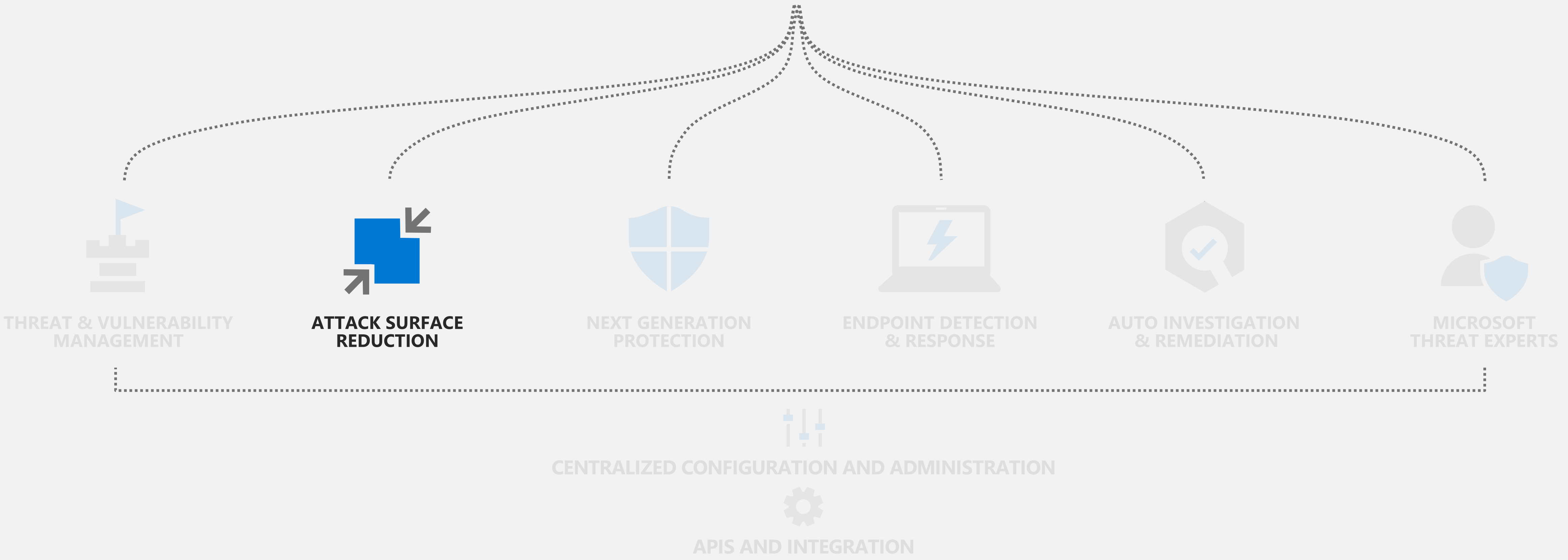
Tracking Mean-time-to-mitigate KPIs

Rich exception experience to mitigate/accept risk

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

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

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

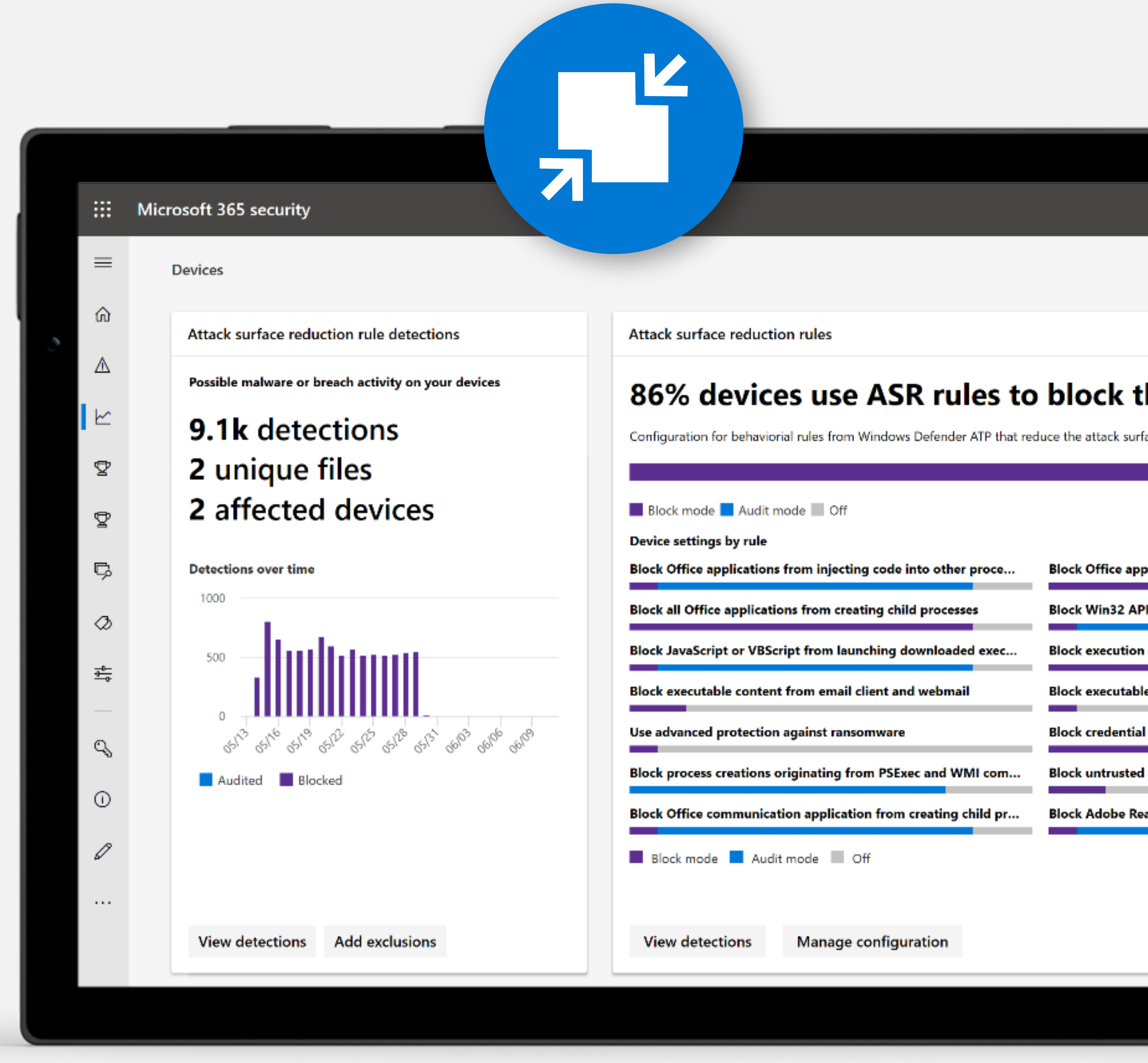
Heterogeneous environments make it challenging

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



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

View detections | Add exclusions

Attack surface reduction rules

86% devices use ASR rules to block t

Configuration for behaviorial rules from Windows Defender ATP that reduce the attack surfa

Block mode Audit mode Off

Device settings by rule

Block Office applications from injecting code into other proce...
Block all Office applications from creating child processes
Block JavaScript or VBScript from launching downloaded exec...
Block executable content from email client and webmail
Use advanced protection against ransomware
Block process creations originating from PSExec and WMI com...
Block Office communication application from creating child pr...

Block Office app
Block Win32 API
Block execution
Block executable
Block credential
Block untrusted
Block Adobe Rea

Block mode Audit mode Off

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

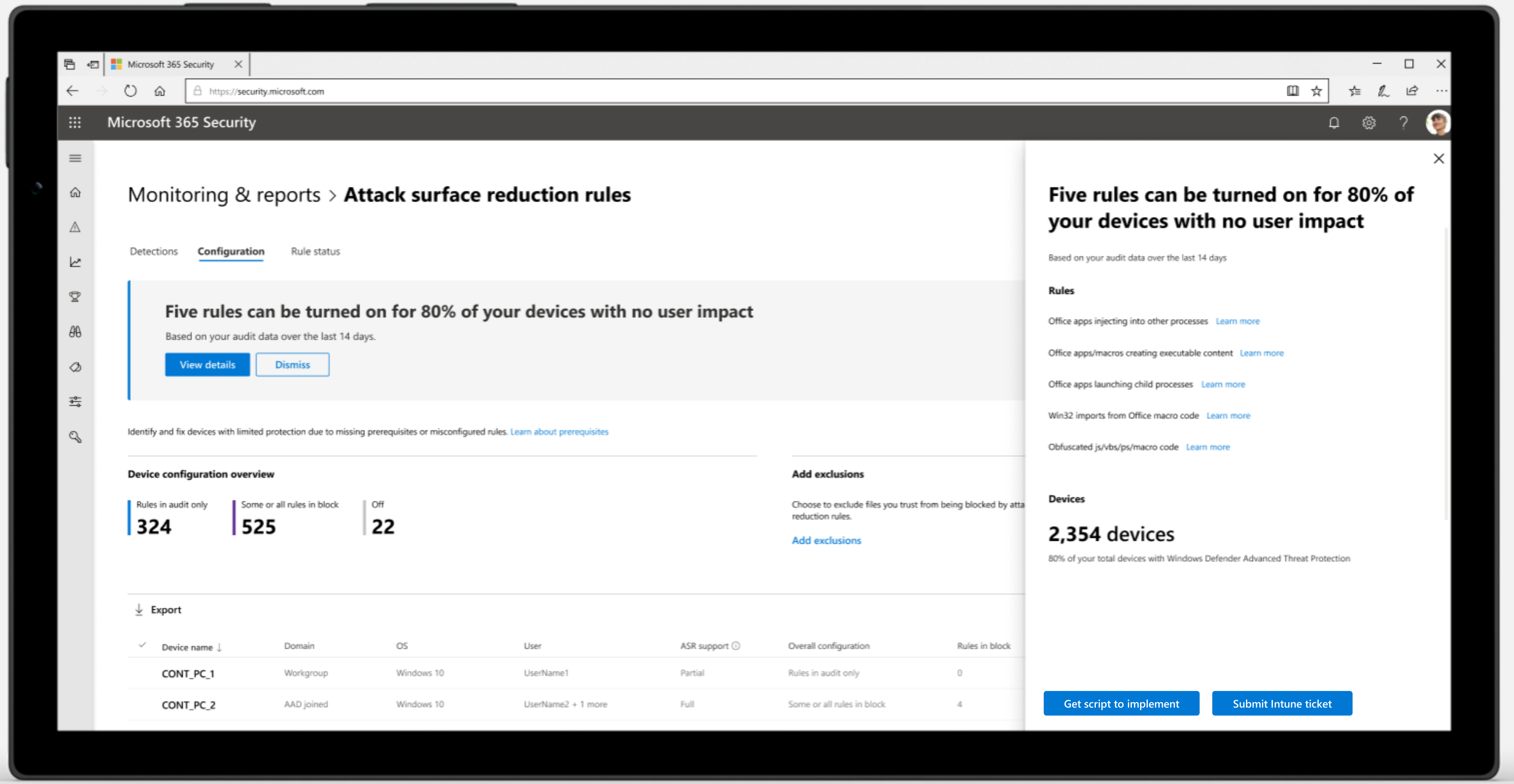
Polymorphic threats

- 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 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



Monitoring & reports > **Attack surface reduction rules**

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.

Identify and fix devices with limited protection due to missing prerequisites or misconfigured rules. Learn about prerequisites

Device configuration overview

Rules in audit only	Some or all rules in block	Off
324	525	22

Add exclusions

Choose to exclude files you trust from being blocked by atta reduction rules.

Device name ↓	Domain	OS	User	ASR support ⓘ	Overall configuration	Rules in block
CONT_PC_1	Workgroup	Windows 10	UserName1	Partial	Rules in audit only	0
CONT_PC_2	AAD joined	Windows 10	UserName2 + 1 more	Full	Some or all rules in block	4

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

Rules

Office apps injecting into other processes Learn more

Office apps/macros creating executable content Learn more

Office apps launching child processes Learn more

Win32 imports from Office macro code Learn more

Obfuscated js/vbs/ps/macro code Learn more

Devices

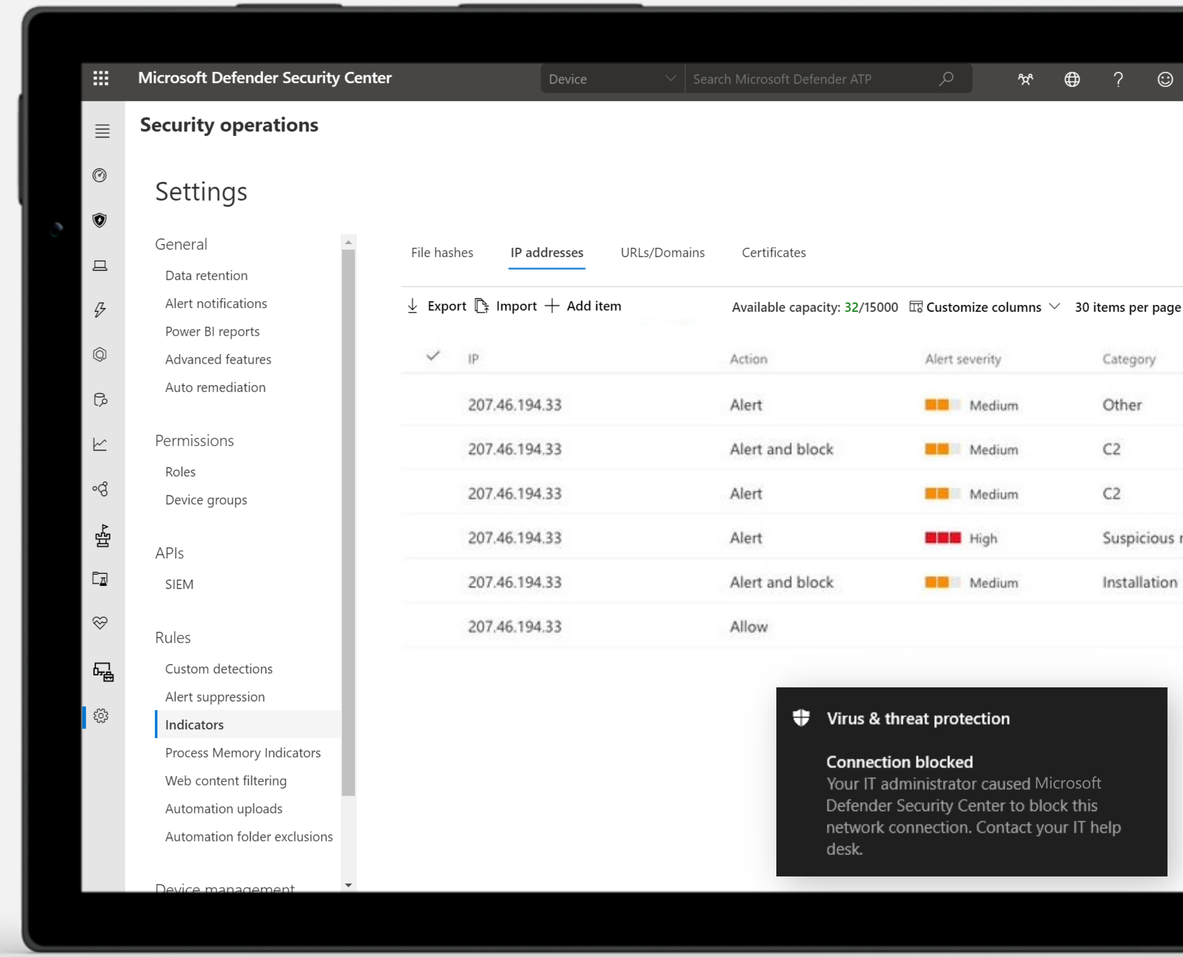
2,354 devices

80% of your total devices with Windows Defender Advanced Threat Protection

Network protection

Allow, audit and block

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



Microsoft Defender Security Center

Device

Search Microsoft Defender ATP

Security operations

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

File hashes | IP addresses | URLs/Domains | Certificates

Export | Import | Add item | Available capacity: 32/15000 | Customize columns | 30 items per page

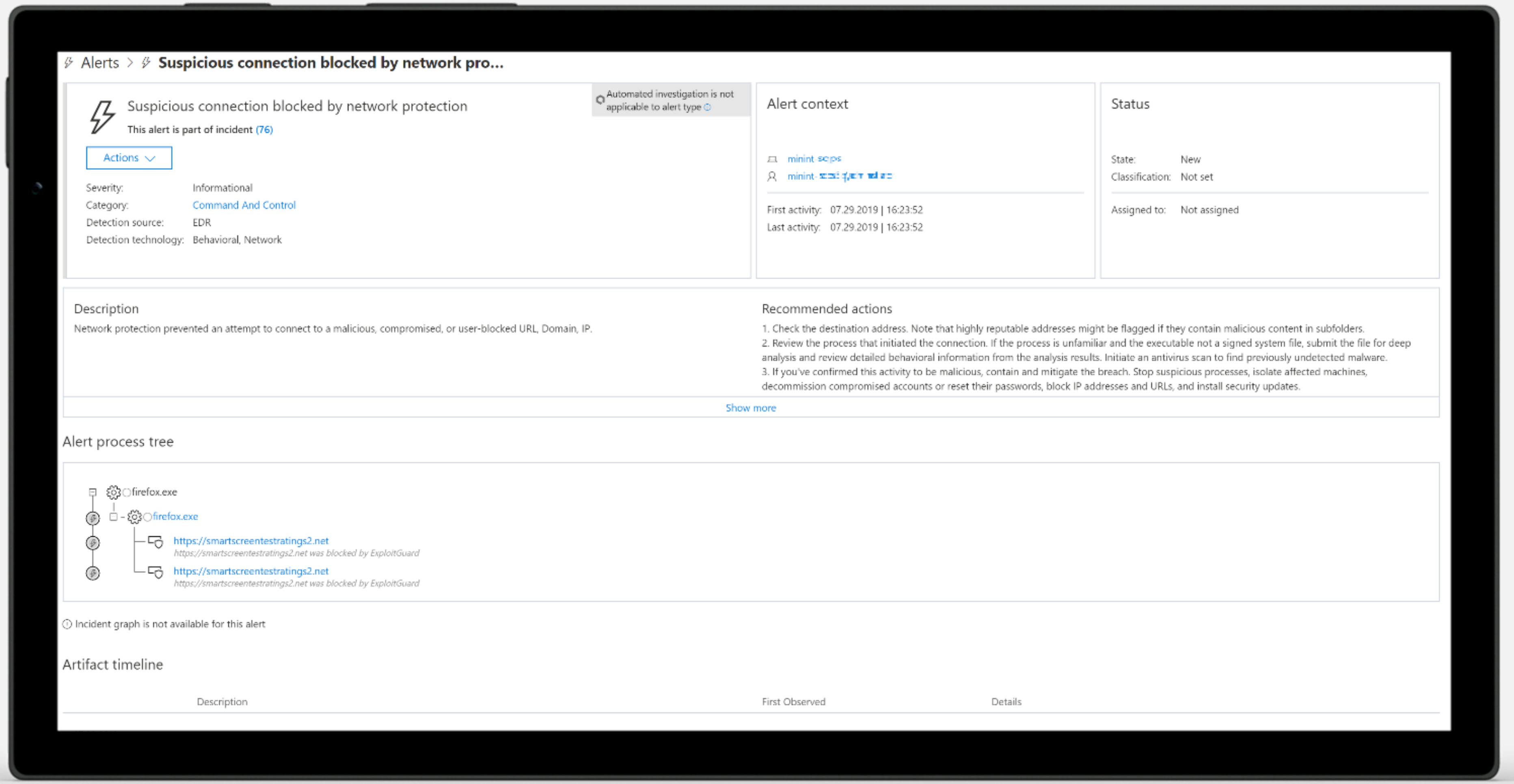
IP	Action	Alert severity	Category
207.46.194.33	Alert	🟧🟧 Medium	Other
207.46.194.33	Alert and block	🟧🟧 Medium	C2
207.46.194.33	Alert	🟧🟧 Medium	C2
207.46.194.33	Alert	🟥🟥🟥 High	Suspicious
207.46.194.33	Alert and block	🟧🟧 Medium	Installation
207.46.194.33	Allow		

Virus & threat protection

Connection blocked

Your IT administrator caused Microsoft Defender Security Center to block this network connection. Contact your IT help desk.

Web Threat Alerts



Alerts > Suspicious connection blocked by network pro...

Suspicious connection blocked by network protection

This alert is part of incident (76)

Automated investigation is not applicable to alert type

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

Alert context

minint-[redacted]

minint-[redacted]

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.

Alert process tree

firefox.exe

firefox.exe

https://smartscreentestratings2.net

https://smartscreentestratings2.net was blocked by ExploitGuard

https://smartscreentestratings2.net

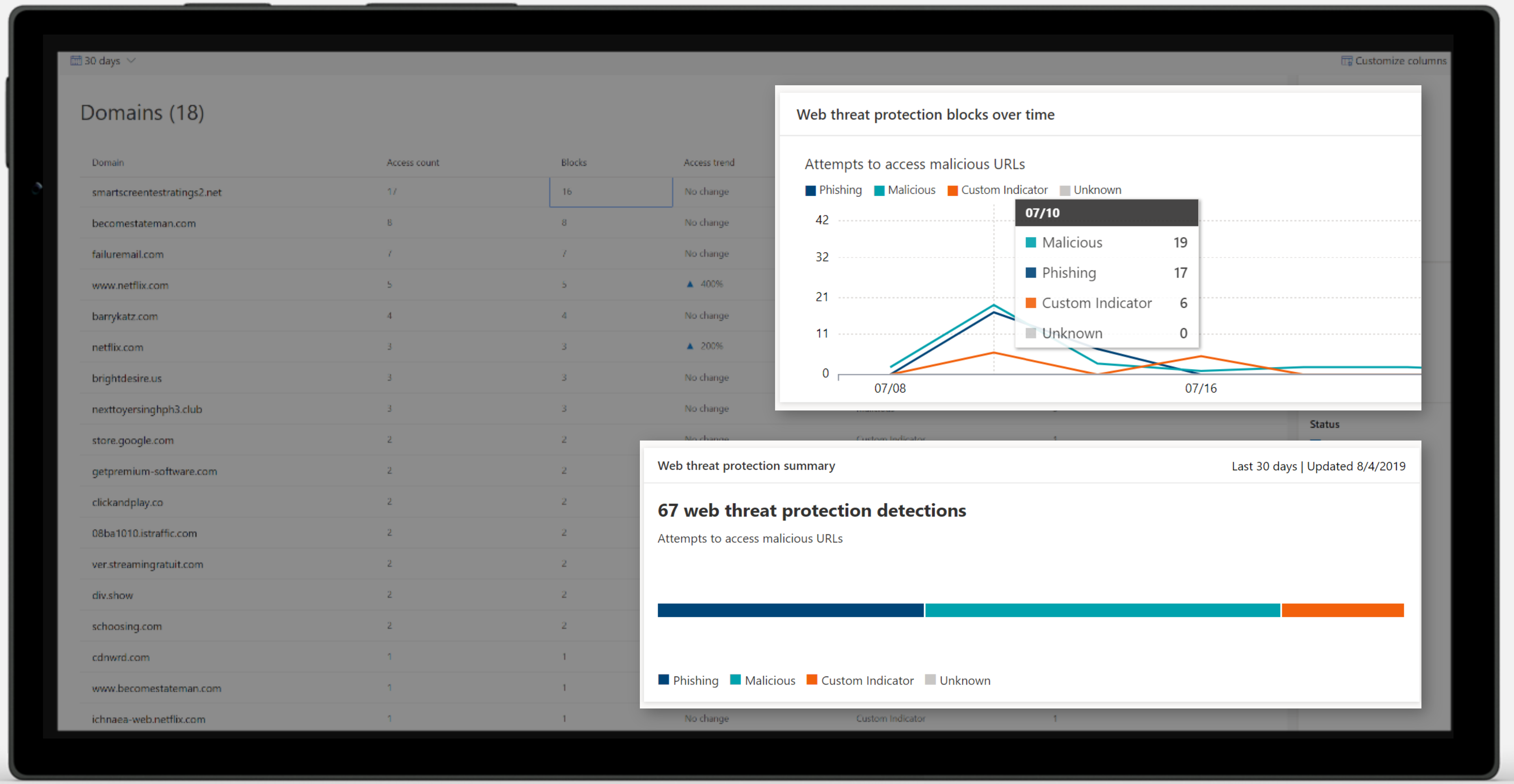
https://smartscreentestratings2.net was blocked by ExploitGuard

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		
smartscreentestratings2.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	Custom Indicator	1
getpremium-software.com	2	2			
clickandplay.co	2	2			
08ba1010.istraffic.com	2	2			
ver.streamingratuit.com	2	2			
div.show	2	2			
schoosing.com	2	2			
cdnwrd.com	1	1			
www.becomestateman.com	1	1			
ichnaea-web.netflix.com	1	1	No change	Custom Indicator	1

Status

Web threat protection blocks over time

Attempts to access malicious URLs

07/10

Malicious	19
Phishing	17
Custom Indicator	6
Unknown	0

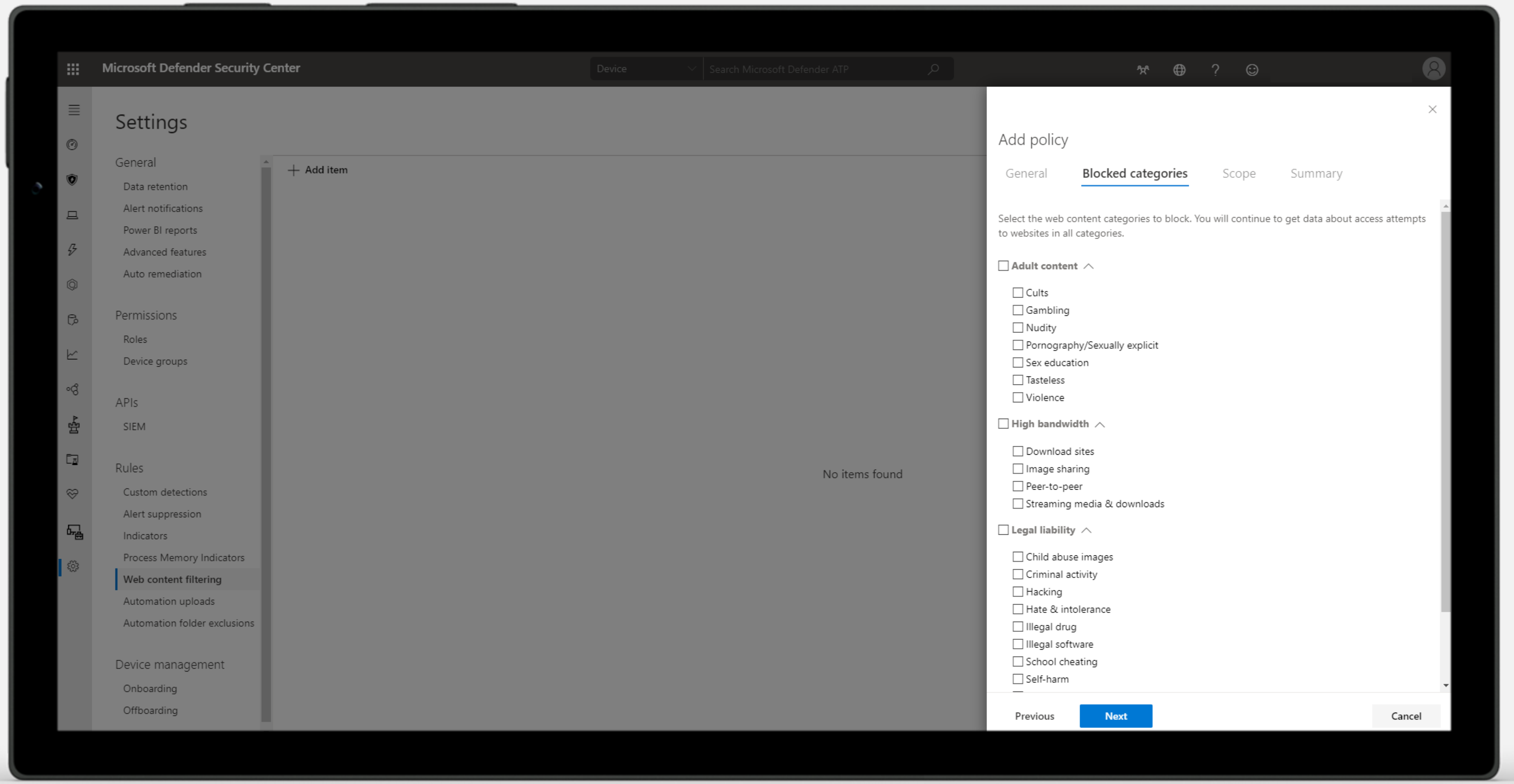
Web threat protection summary

Last 30 days | Updated 8/4/2019

67 web threat protection detections

Attempts to access malicious URLs

Web content filtering configuration



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

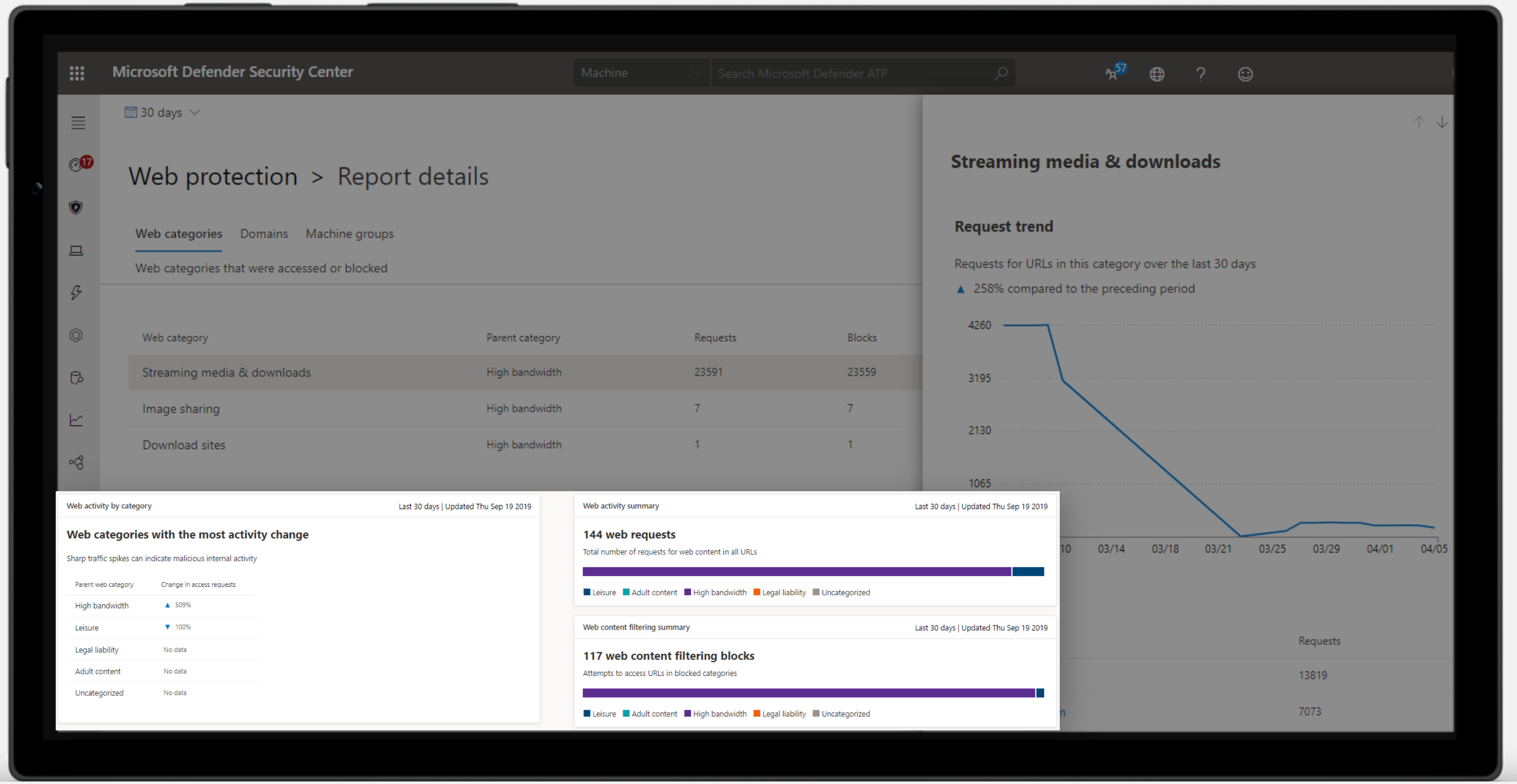
□ **High bandwidth**

- □ 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

Web Content Filtering reporting



Microsoft Defender Security Center

Machine | Search Microsoft Defender ATP

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

Streaming media & downloads

Request trend

Requests for URLs in this category over the last 30 days

▲ 258% compared to the preceding period

Requests
13819
7073

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	▲ 509%
Leisure	▼ 100%
Legal liability	No data
Adult content	No data
Uncategorized	No data

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

144 web requests

Total number of requests for web content in all URLs

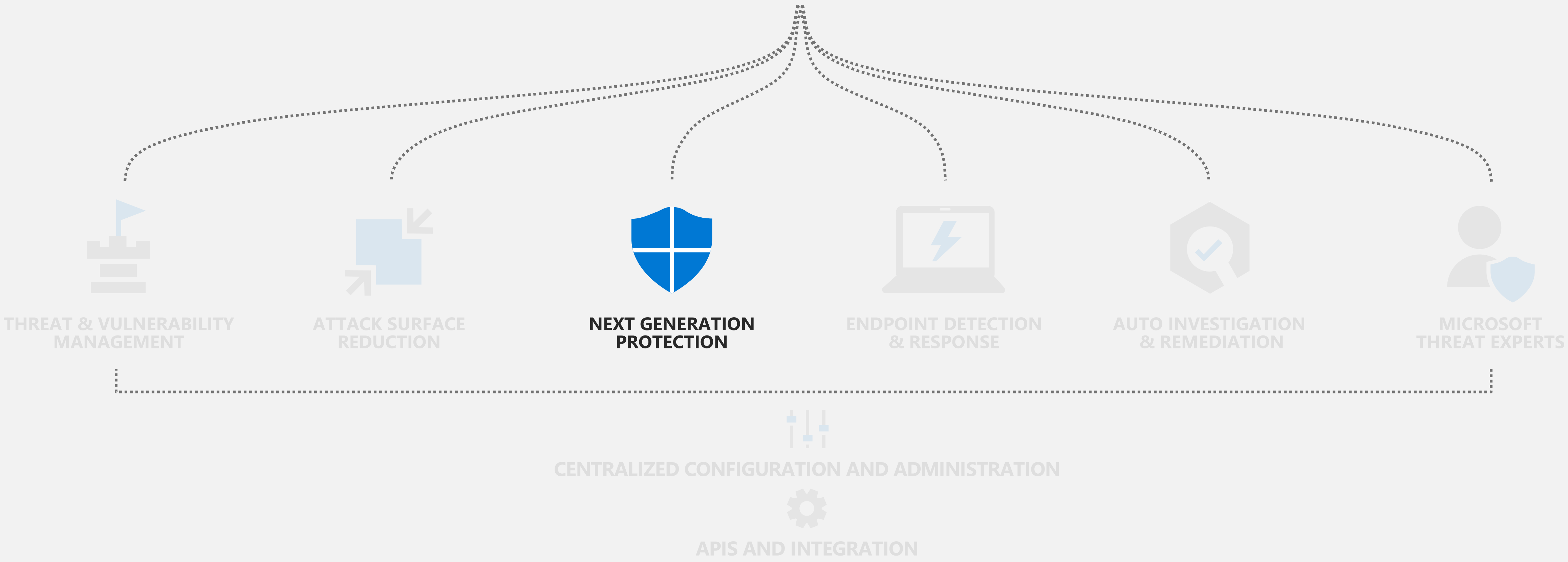
Web content filtering summary — Last 30 days | Updated Thu Sep 19 2019

117 web content filtering blocks

Attempts to access URLs in blocked categories

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

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

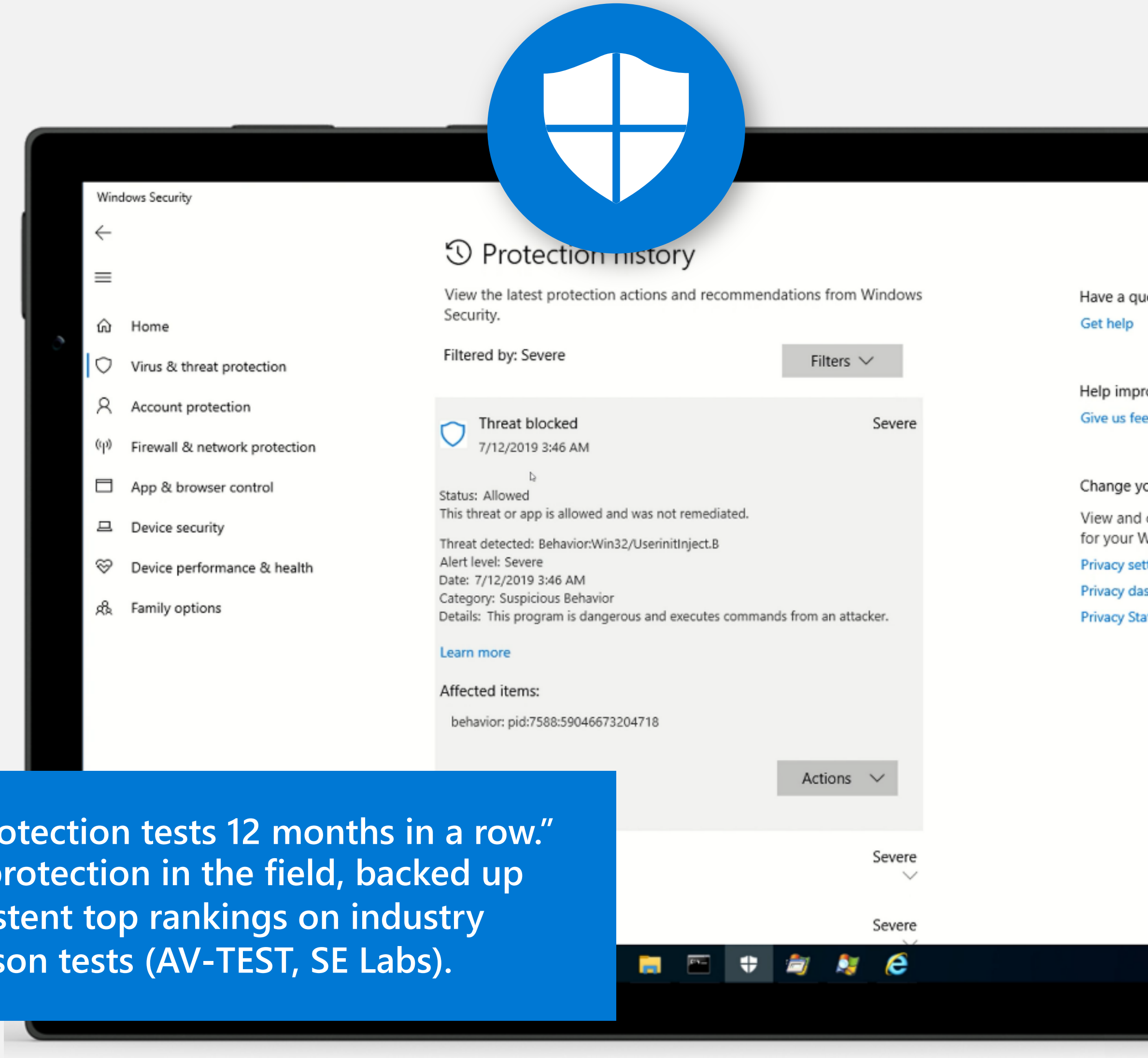
✓

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



Windows Security

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options

Protection history

View the latest protection actions and recommendations from Windows Security.

Filtered by: Severe

Threat blocked 7/12/2019 3:46 AM Severe

Status: Allowed
This threat or app is allowed and was not remediated.

Threat detected: Behavior:Win32/UserinitInject.B
Alert level: Severe
Date: 7/12/2019 3:46 AM
Category: Suspicious Behavior
Details: This program is dangerous and executes commands from an attacker.

Learn more

Affected items:

behavior: pid:7588:59046673204718

"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

Cloud

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

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

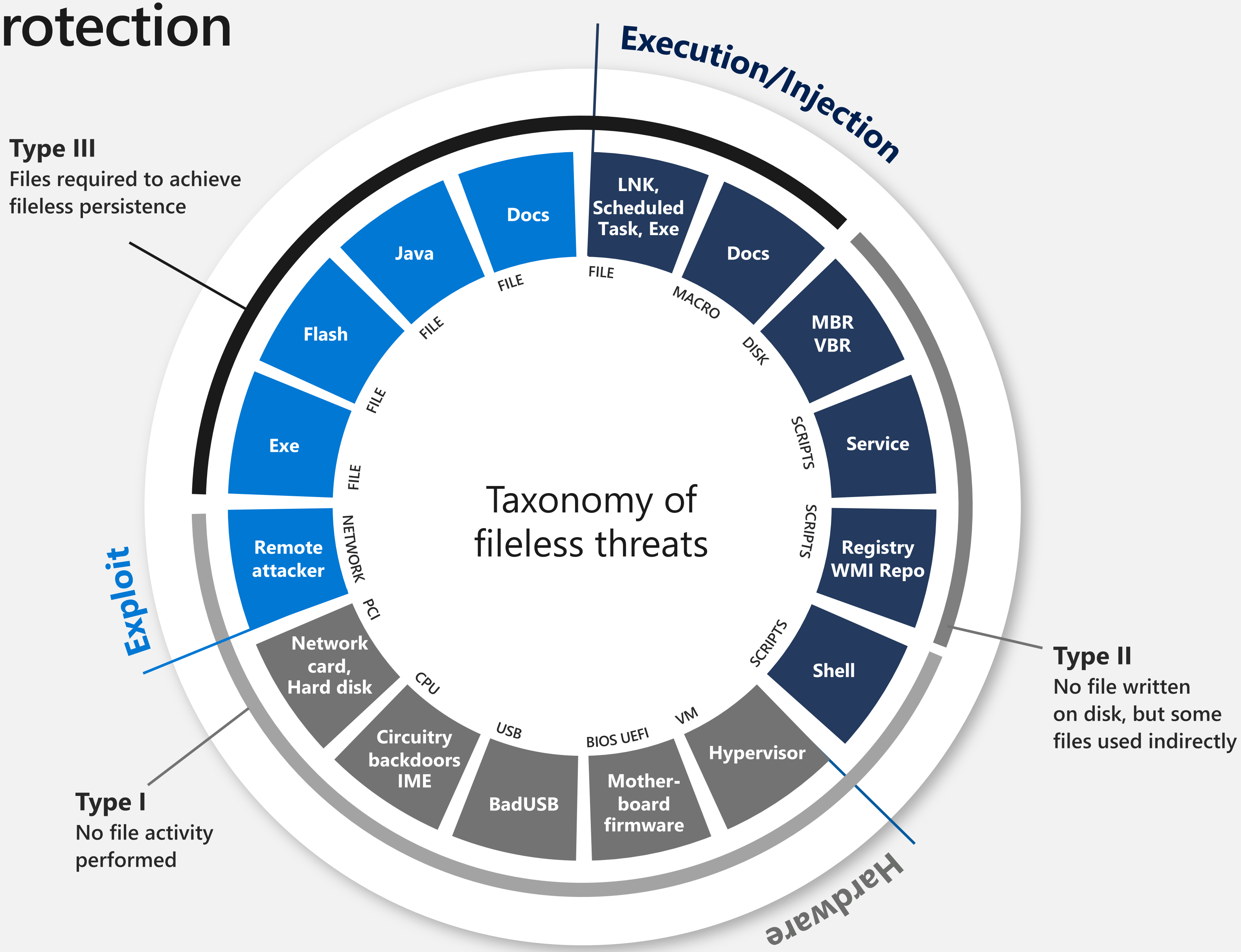
Heuristics
Catches malware variants or new strains with similar characteristics

Emulation
Evaluates files based on how they would behave when run

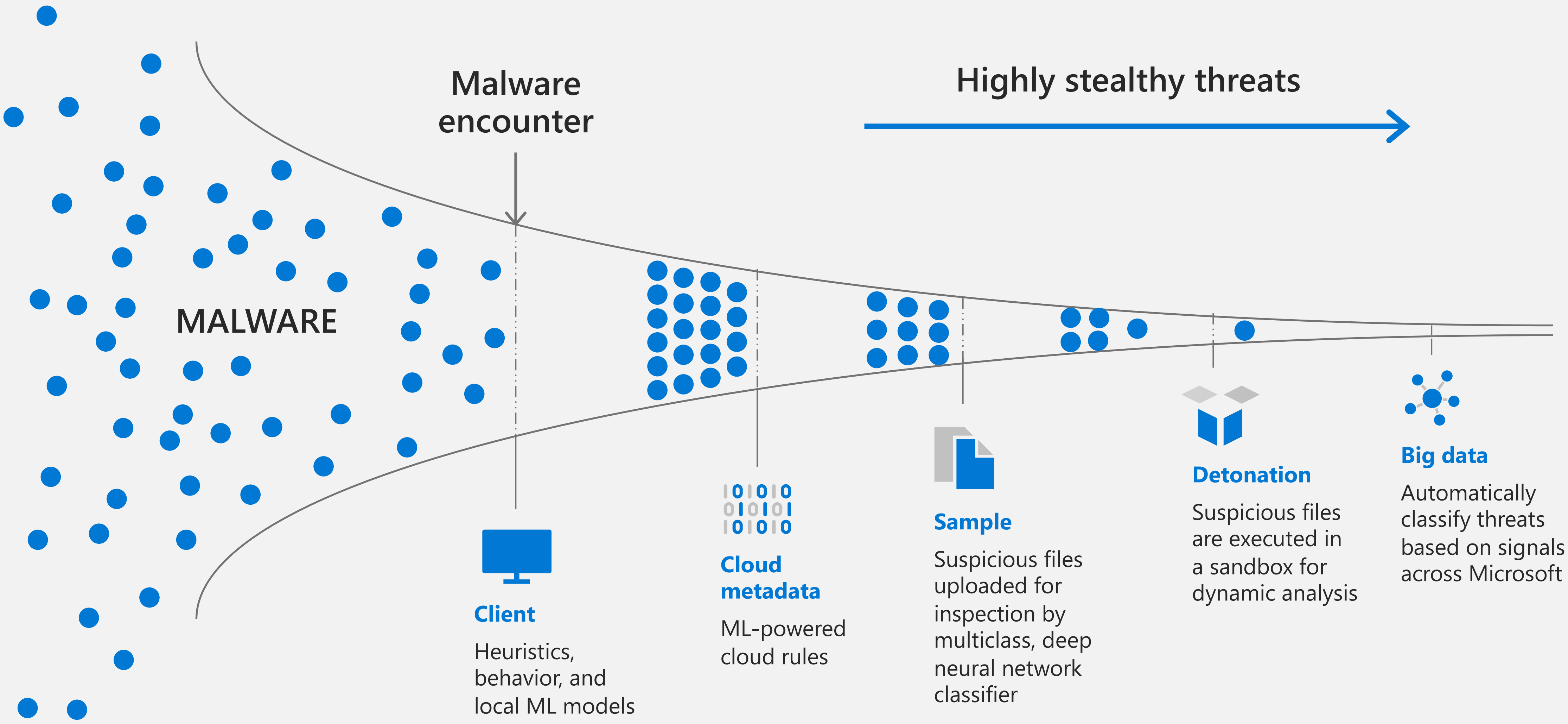
Network monitoring
Catches malicious network activities

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



Client

Heuristics, behavior, and local ML models

Cloud metadata

ML-powered cloud rules

Sample

Suspicious files uploaded for inspection by multiclass, deep neural network classifier

Detonation

Suspicious files are executed in a sandbox for dynamic analysis

Big data

Automatically classify threats based on signals across Microsoft

Dynamic: behavior monitoring

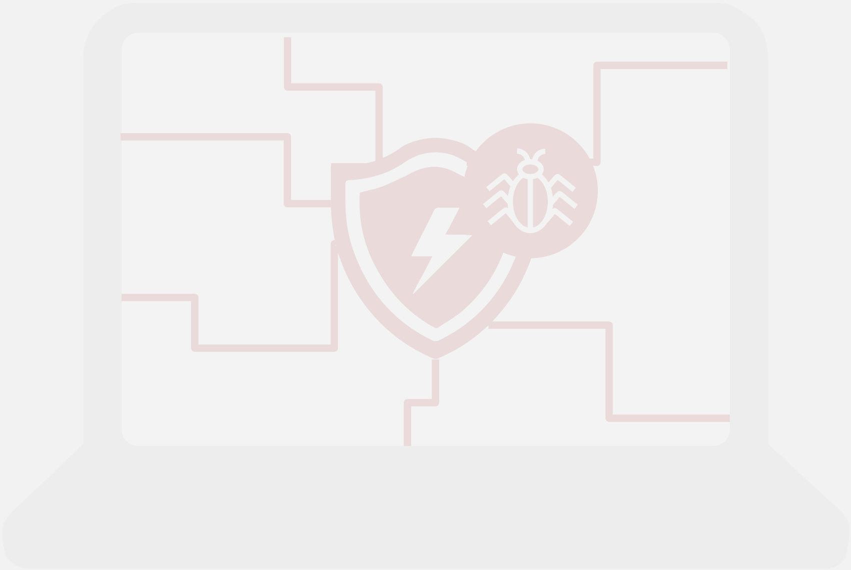
Monitors activity on:

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

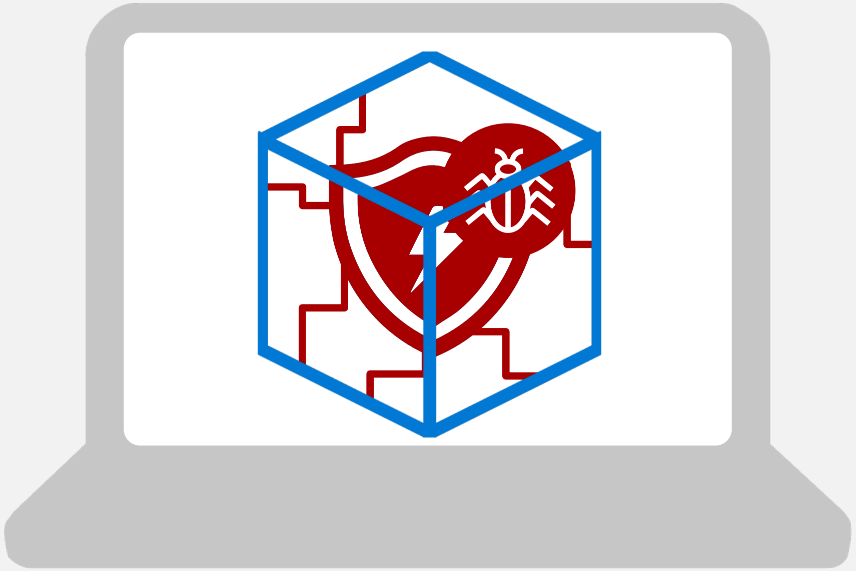
Heuristics can:

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

Sandboxing of the antivirus engine



Then

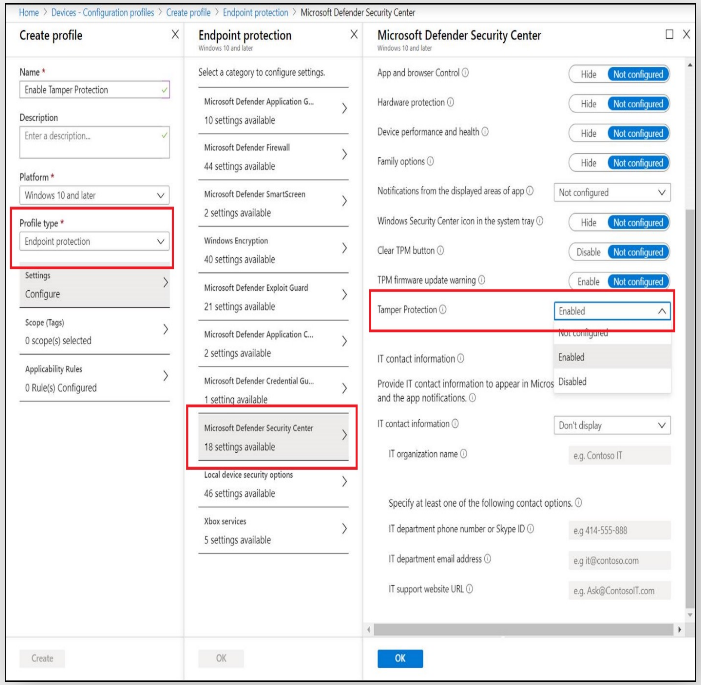


Now

Read the blog for more details

Tamper Protection – Password-less, secure, e2e

Seamless, secure and password less configuration



Home > Devices - Configuration profiles > Create profile > Endpoint protection > Microsoft Defender Security Center

Create profile

Name *
Enable Tamper Protection

Description
Enter a description...

Platform *
Windows 10 and later

Profile type *
Endpoint protection

Settings
Configure

Scope (Tags)
0 scope(s) selected

Applicability Rules
0 Rule(s) Configured

Create

Endpoint protection
Windows 10 and later

Select a category to configure settings.

- Microsoft Defender Application G... – 10 settings available
- Microsoft Defender Firewall – 44 settings available
- Microsoft Defender SmartScreen – 2 settings available
- Windows Encryption – 40 settings available
- Microsoft Defender Exploit Guard – 21 settings available
- Microsoft Defender Application C... – 2 settings available
- Microsoft Defender Credential Gu... – 1 setting available
- Microsoft Defender Security Center – 18 settings available
- Local device security options – 46 settings available
- Xbox services – 5 settings available

OK

Microsoft Defender Security Center
Windows 10 and later

App and browser Control	Hide / Not configured
Hardware protection	Hide / Not configured
Device performance and health	Hide / Not configured
Family options	Hide / Not configured
Notifications from the displayed areas of app	Not configured
Windows Security Center icon in the system tray	Hide / Not configured
Clear TPM button	Disable / Not configured
TPM firmware update warning	Enable / Not configured
Tamper Protection	Enabled

Not configured
Enabled
Disabled

IT contact information
Provide IT contact information to appear in Micros and the app notifications.

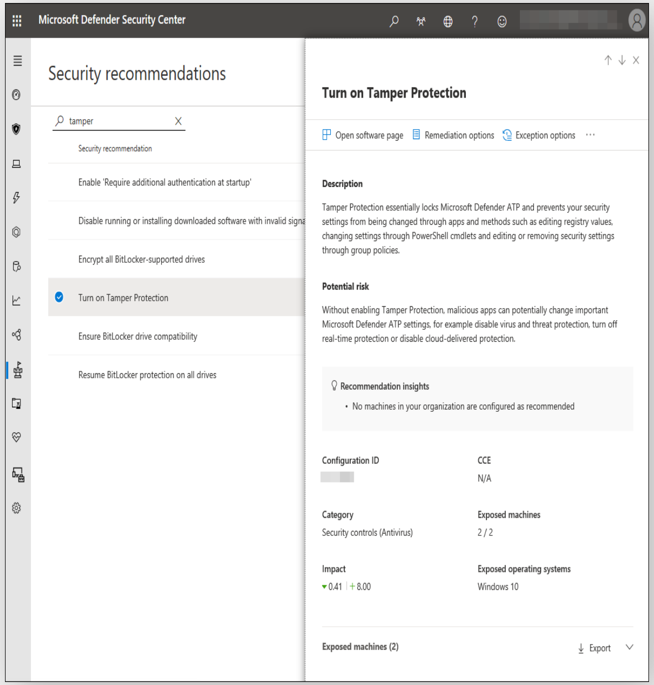
IT contact information	Don't display
IT organization name	e.g. Contoso IT

Specify at least one of the following contact options.

IT department phone number or Skype ID	e.g 414-555-888
IT department email address	e.g it@contoso.com
IT support website URL	e.g. Ask@ContosoIT.com

OK

Threat & vulnerability management – Security recommendation



Microsoft Defender Security Center [redacted]

Security recommendations

tamper

Security recommendation
- Enable 'Require additional authentication at startup'
- Disable running or installing downloaded software with invalid signa
- Encrypt all BitLocker-supported drives
- Turn on Tamper Protection
- Ensure BitLocker drive compatibility
- Resume BitLocker protection on all drives

Turn on Tamper Protection

Open software page | Remediation options | Exception options | ···

Description

Tamper Protection essentially locks Microsoft Defender ATP and prevents your security settings from being changed through apps and methods such as editing registry values, changing settings through PowerShell cmdlets and editing or removing security settings through group policies.

Potential risk

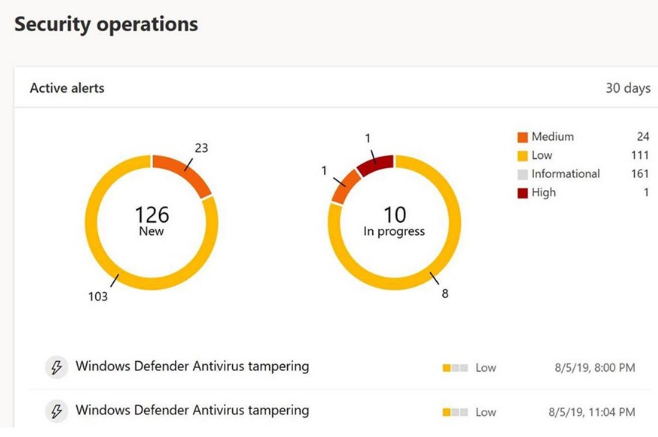
Without enabling Tamper Protection, malicious apps can potentially change important Microsoft Defender ATP settings, for example disable virus and threat protection, turn off real-time protection or disable cloud-delivered protection.

Recommendation insights
- No machines in your organization are configured as recommended

Configuration ID [redacted]	CCE N/A
Category Security controls (Antivirus)	Exposed machines 2 / 2
Impact ▾0.41 | +8.00	Exposed operating systems Windows 10

Exposed machines (2) Export

Tampering alert based on System Guard and EDR signals



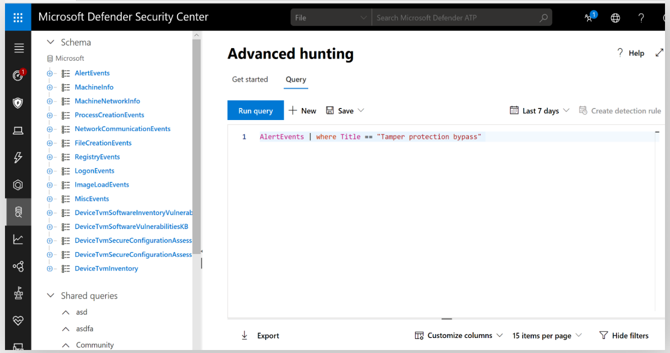
Security operations

Active alerts 30 days

🟧 Medium	24
🟨 Low	111
⬜ Informational	161
🟥 High	1

Windows Defender Antivirus tampering	Low	8/5/19, 8:00 PM
Windows Defender Antivirus tampering	Low	8/5/19, 11:04 PM

Advanced Hunting



Microsoft Defender Security Center File Search Microsoft Defender ATP

Advanced hunting

Get started | Query

Run query | + New | Save | Last 7 days | Create detection rule

```
AlertEvents | where Title == "Tamper protection bypass"
```

Schema
Microsoft
- AlertEvents
- MachineInfo
- MachineNetworkInfo
- ProcessCreationEvents
- NetworkCommunicationEvents
- FileCreationEvents
- RegistryEvents
- LogonEvents
- ImageLoadEvents
- MiscEvents
- DeviceTvmSoftwareInventoryVulnerab
- DeviceTvmSoftwareVulnerabilitiesKB
- DeviceTvmSecureConfigurationAssess
- DeviceTvmSecureConfigurationAssess
- DeviceTvmInventory

Shared queries
- asd
- asdfa
- Community

Export | Customize columns | 15 items per page | Hide filters

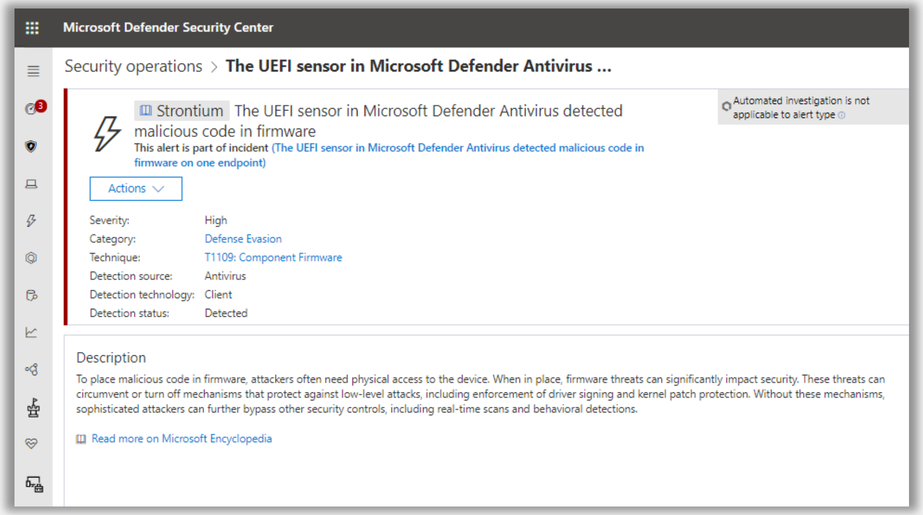
Read the blog for more details

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


Microsoft Defender Security Center
Security operations > The UEFI sensor in Microsoft Defender Antivirus ...
Actions
3

Strontium The UEFI sensor in Microsoft Defender Antivirus detected malicious code in firmware

This alert is part of incident (The UEFI sensor in Microsoft Defender Antivirus detected malicious code in firmware on one endpoint)

Automated investigation is not applicable to alert type

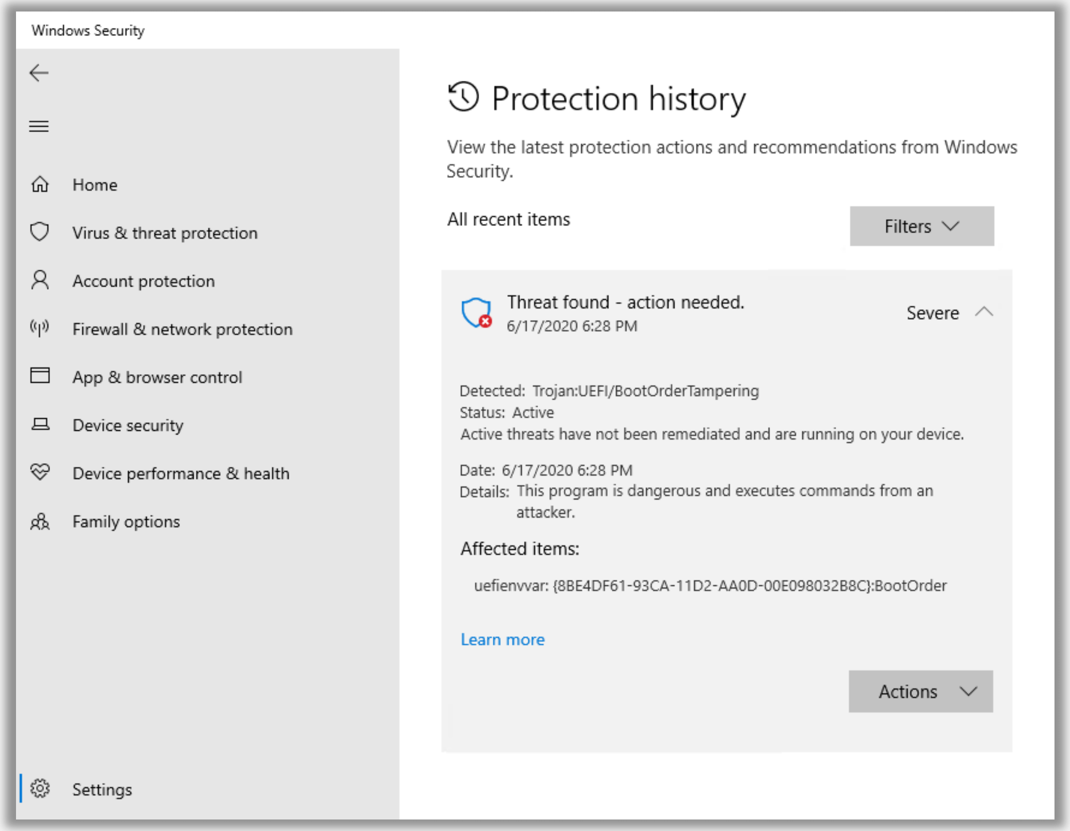
Severity:	High
Category:	Defense Evasion
Technique:	T1109: Component Firmware
Detection source:	Antivirus
Detection technology:	Client
Detection status:	Detected

Description

To place malicious code in firmware, attackers often need physical access to the device. When in place, firmware threats can significantly impact security. These threats can circumvent or turn off mechanisms that protect against low-level attacks, including enforcement of driver signing and kernel patch protection. Without these mechanisms, sophisticated attackers can further bypass other security controls, including real-time scans and behavioral detections.

Read more on Microsoft Encyclopedia

Scanning and detection



Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

Threat found - action needed.
6/17/2020 6:28 PM

Detected: Trojan:UEFI/BootOrderTampering
Status: Active
Active threats have not been remediated and are running on your device.

Date: 6/17/2020 6:28 PM
Details: This program is dangerous and executes commands from an attacker.

Affected items:

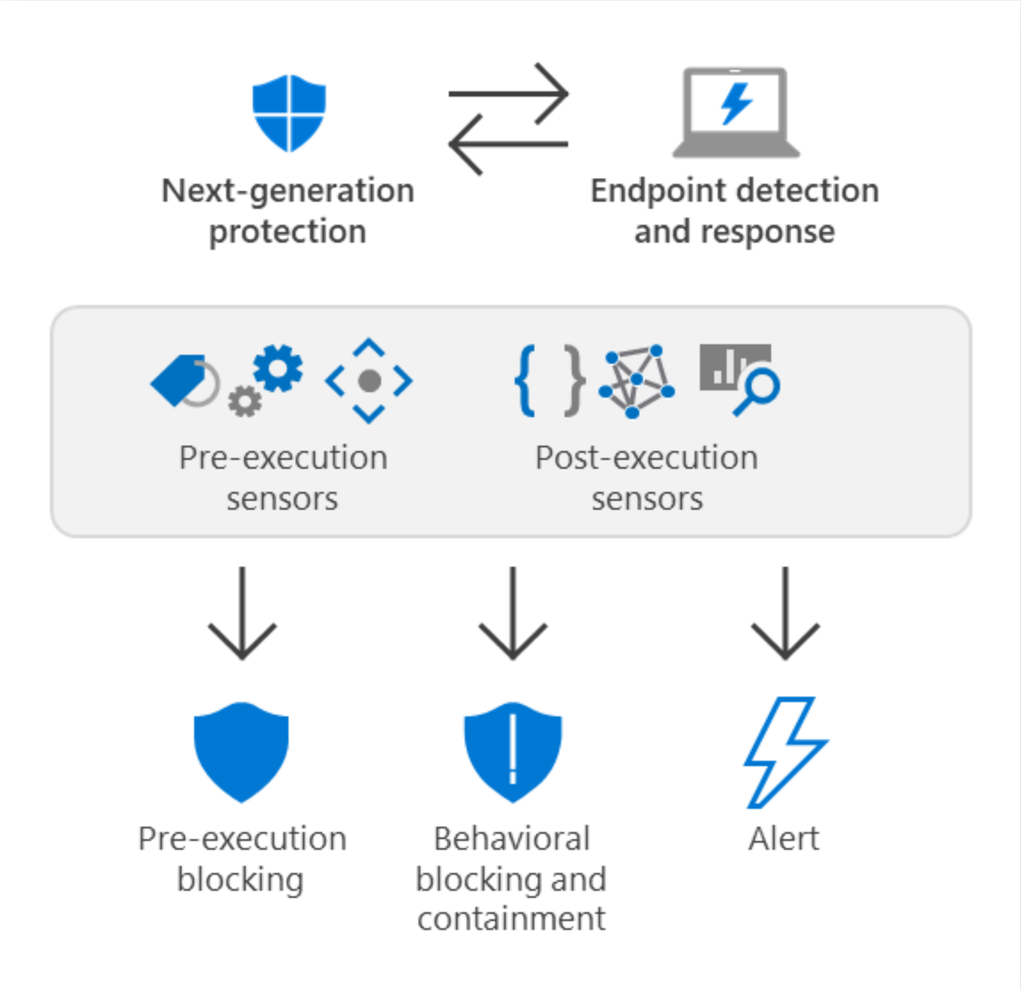
uefienvvar: {8BE4DF61-93CA-11D2-AA0D-00E098032B8C}:BootOrder

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

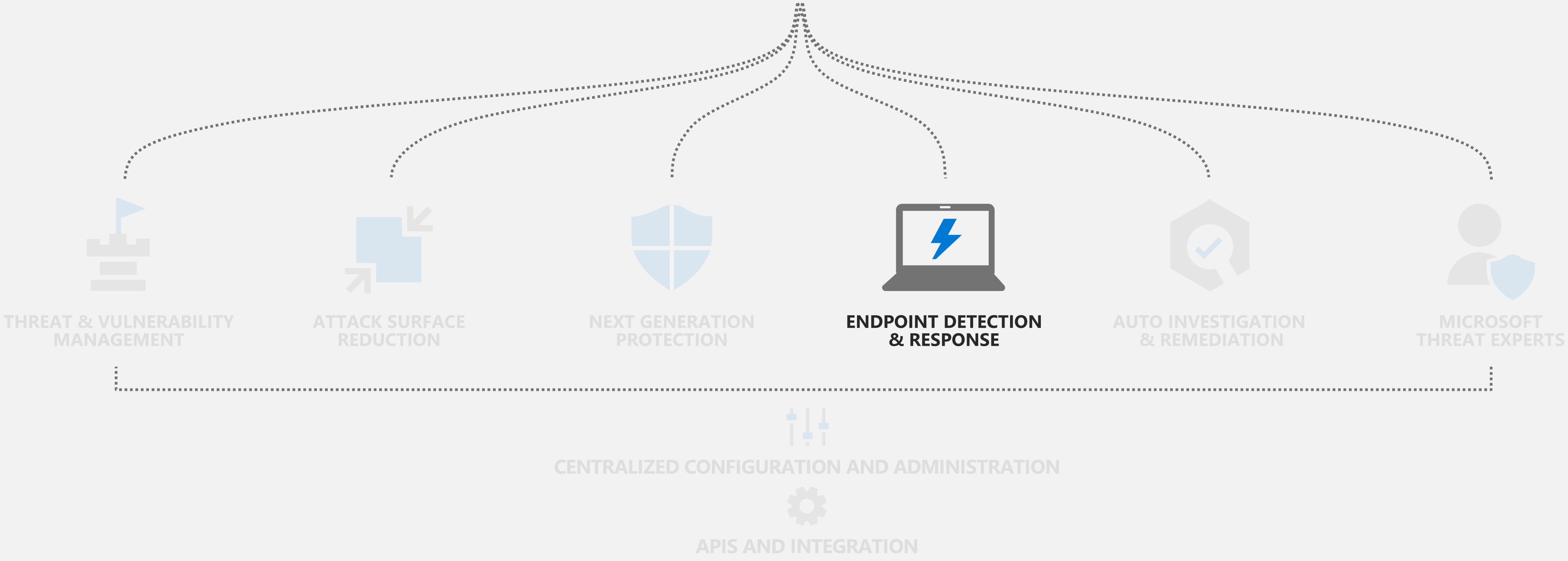
Read the blog for more details



Next-generation protection
Endpoint detection and response
Pre-execution sensors
Post-execution sensors
Pre-execution blocking
Behavioral blocking and containment
Alert

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

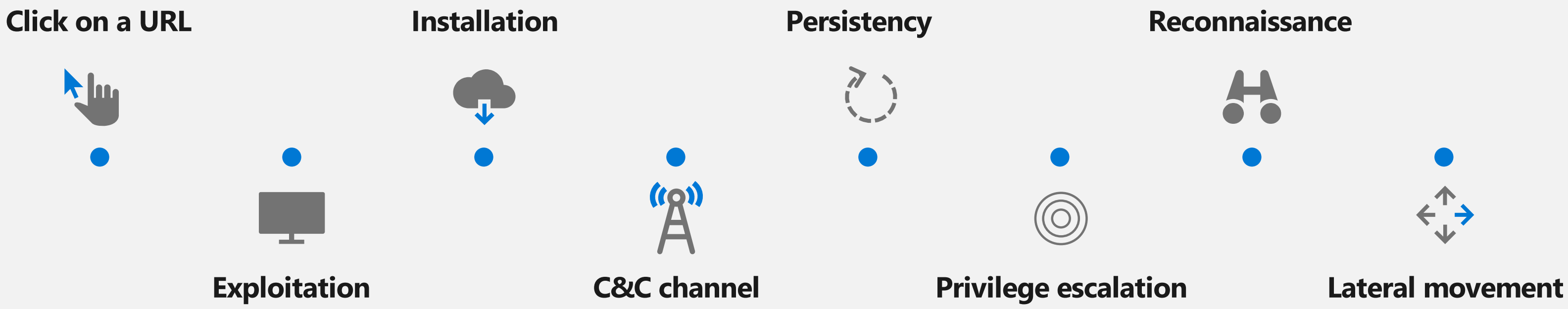
MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

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

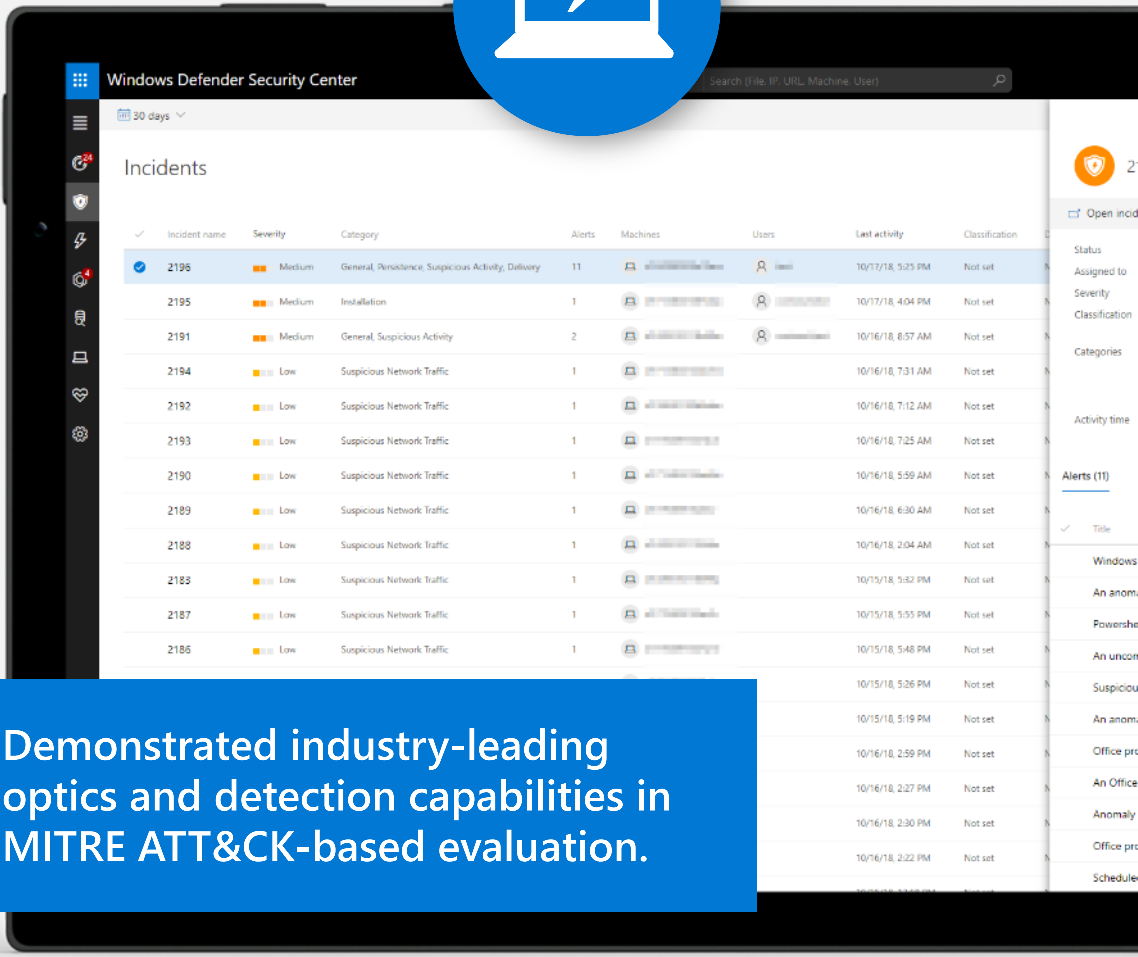
Collecting evidence and alerts, even from 1 infected device, can be a long time-consuming process

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



Windows Defender Security Center

Search (File, IP, URL, Machine, User)

30 days

Incidents

✓	Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification
✓	2196	Medium	General, Persistence, Suspicious Activity, Delivery	11	[redacted]	[redacted]	10/17/18, 5:25 PM	Not set
	2195	Medium	Installation	1	[redacted]	[redacted]	10/17/18, 4:04 PM	Not set
	2191	Medium	General, Suspicious Activity	2	[redacted]	[redacted]	10/16/18, 8:57 AM	Not set
	2194	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:31 AM	Not set
	2192	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:12 AM	Not set
	2193	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:25 AM	Not set
	2190	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 5:59 AM	Not set
	2189	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 6:30 AM	Not set
	2188	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:04 AM	Not set
	2183	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:32 PM	Not set
	2187	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:55 PM	Not set
	2186	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:48 PM	Not set
							10/15/18, 5:26 PM	Not set
							10/15/18, 5:19 PM	Not set
							10/16/18, 2:59 PM	Not set
							10/16/18, 2:27 PM	Not set
							10/16/18, 2:30 PM	Not set
							10/16/18, 2:22 PM	Not set

21

Open incid

Status

Assigned to

Severity

Classification

Categories

Activity time

Alerts (11)

✓	Title
	Windows
	An anom
	Powershe
	An uncon
	Suspiciou
	An anom
	Office pro
	An Office
	Anomaly
	Office pro
	Schedule

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

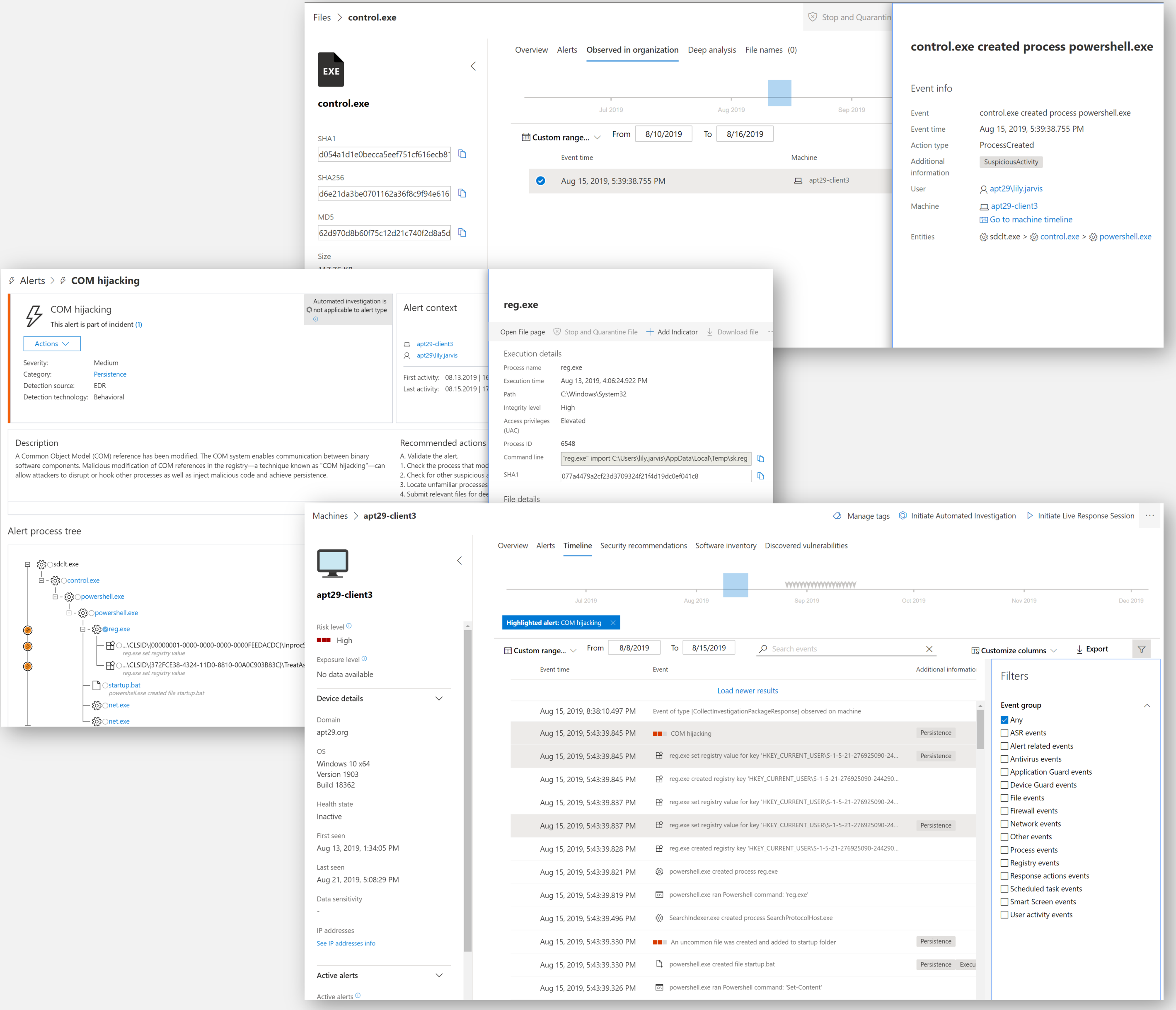
Full machine timeline to drill into activities, filter and search.

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.



control.exe

SHA1: d054a1d1e0becca5eef751cf616ecb8

SHA256: d6e21da3be0701162a36f8c9f94e616

MD5: 62d970d8b60f75c12d21c740f2d8a5d

Size

From 8/10/2019 To 8/16/2019

Event time	Machine
Aug 15, 2019, 5:39:38.755 PM	apt29-client3

control.exe created process powershell.exe

Event info

Event	control.exe created process powershell.exe
Event time	Aug 15, 2019, 5:39:38.755 PM
Action type	ProcessCreated
Additional information	SuspiciousActivity
User	apt29\lily.jarvis
Machine	apt29-client3 Go to machine timeline
Entities	sdclt.exe > control.exe > powershell.exe

COM hijacking

This alert is part of incident (1)

Automated investigation is not applicable to alert type

Severity:	Medium
Category:	Persistence
Detection source:	EDR
Detection technology:	Behavioral

apt29-client3
apt29\lily.jarvis

First activity: 08.13.2019 | 16
Last activity: 08.15.2019 | 17

Description

A Common Object Model (COM) reference has been modified. The COM system enables communication between binary software components. Malicious modification of COM references in the registry—a technique known as "COM hijacking"—can allow attackers to disrupt or hook other processes as well as inject malicious code and achieve persistence.

Recommended actions

A. Validate the alert.
1. Check the process that mod
2. Check for other suspicious a
3. Locate unfamiliar processes
4. Submit relevant files for dee

```
sdclt.exe
  control.exe
    powershell.exe
      powershell.exe
        reg.exe
          ...\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\InprocS
            reg.exe set registry value
          ...\CLSID\{372FCE38-4324-11D0-8810-00A0C903B83C}\TreatAs
            reg.exe set registry value
        startup.bat
          powershell.exe created file startup.bat
        net.exe
        net.exe
```

Execution details

Process name	reg.exe
Execution time	Aug 13, 2019, 4:06:24.922 PM
Path	C:\Windows\System32
Integrity level	High
Access privileges (UAC)	Elevated
Process ID	6548
Command line	"reg.exe" import C:\Users\lily.jarvis\AppData\Local\Temp\sk.reg
SHA1	077a4479a2cf23d3709324f21f4d19dc0ef041c8

apt29-client3

Risk level: High

Exposure level: No data available

Device details

Domain	apt29.org
OS	Windows 10 x64 Version 1903 Build 18362
Health state	Inactive
First seen	Aug 13, 2019, 1:34:05 PM
Last seen	Aug 21, 2019, 5:08:29 PM
Data sensitivity	-
IP addresses	See IP addresses info

Active alerts

Active alerts

From 8/8/2019 To 8/15/2019

Event time	Event	Additional informatio
Aug 15, 2019, 8:38:10.497 PM	Event of type [CollectInvestigationPackageResponse] observed on machine	
Aug 15, 2019, 5:43:39.845 PM	COM hijacking	Persistence
Aug 15, 2019, 5:43:39.845 PM	reg.exe set registry value for key 'HKEY_CURRENT_USER\S-1-5-21-276925090-24...	Persistence
Aug 15, 2019, 5:43:39.845 PM	reg.exe created registry key 'HKEY_CURRENT_USER\S-1-5-21-276925090-244290...	
Aug 15, 2019, 5:43:39.837 PM	reg.exe set registry value for key 'HKEY_CURRENT_USER\S-1-5-21-276925090-24...	
Aug 15, 2019, 5:43:39.837 PM	reg.exe set registry value for key 'HKEY_CURRENT_USER\S-1-5-21-276925090-24...	Persistence
Aug 15, 2019, 5:43:39.828 PM	reg.exe created registry key 'HKEY_CURRENT_USER\S-1-5-21-276925090-244290...	
Aug 15, 2019, 5:43:39.821 PM	powershell.exe created process reg.exe	
Aug 15, 2019, 5:43:39.819 PM	powershell.exe ran Powershell command: 'reg.exe'	
Aug 15, 2019, 5:43:39.496 PM	SearchIndexer.exe created process SearchProtocolHost.exe	
Aug 15, 2019, 5:43:39.330 PM	An uncommon file was created and added to startup folder	Persistence
Aug 15, 2019, 5:43:39.330 PM	powershell.exe created file startup.bat	Persistence Execu
Aug 15, 2019, 5:43:39.326 PM	powershell.exe ran Powershell command: 'Set-Content'	

Filters

Event group

- ☑ Any
- □ ASR events
- □ Alert related events
- □ Antivirus events
- □ Application Guard events
- □ Device Guard events
- □ File events
- □ Firewall events
- □ Network events
- □ Other events
- □ Process events
- □ Registry events
- □ Response actions events
- □ Scheduled task events
- □ Smart Screen events
- □ User activity events

Incident

Narrates the end-to-end attack story

Reconstructing the story

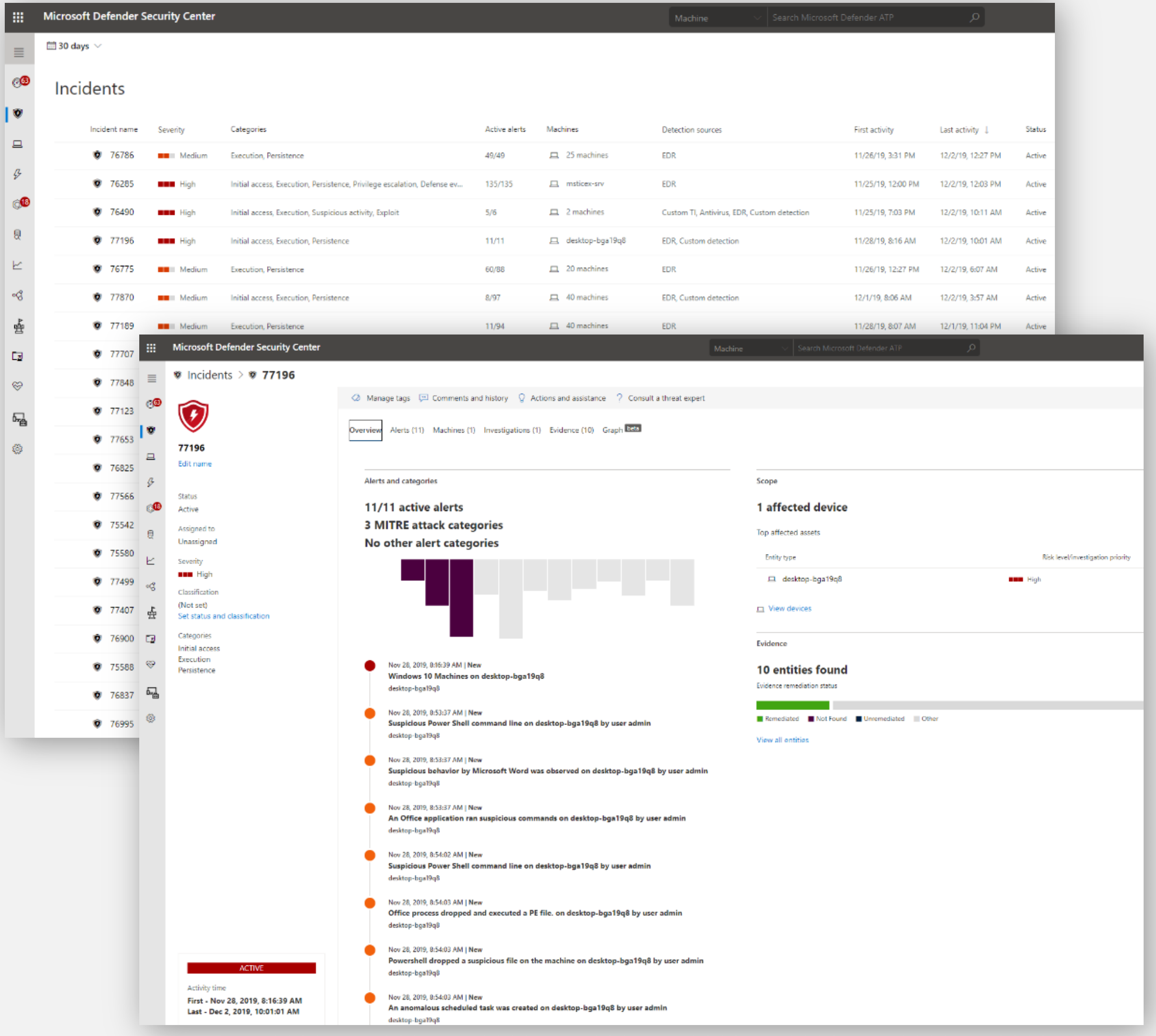
The broader attack story is better described when relevant alerts and related entities are brought together.

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.


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
30 days

Incidents

Incident name	Severity	Categories	Active alerts	Machines	Detection sources	First activity	Last activity ↓	Status
76786	Medium	Execution, Persistence	49/49	25 machines	EDR	11/26/19, 3:31 PM	12/2/19, 12:27 PM	Active
76285	High	Initial access, Execution, Persistence, Privilege escalation, Defense ev...	135/135	msticex-srv	EDR	11/25/19, 12:00 PM	12/2/19, 12:03 PM	Active
76490	High	Initial access, Execution, Suspicious activity, Exploit	5/6	2 machines	Custom TI, Antivirus, EDR, Custom detection	11/25/19, 7:03 PM	12/2/19, 10:11 AM	Active
77196	High	Initial access, Execution, Persistence	11/11	desktop-bga19q8	EDR, Custom detection	11/28/19, 8:16 AM	12/2/19, 10:01 AM	Active
76775	Medium	Execution, Persistence	60/88	20 machines	EDR	11/26/19, 12:27 PM	12/2/19, 6:07 AM	Active
77870	Medium	Initial access, Execution, Persistence	8/97	40 machines	EDR, Custom detection	12/1/19, 8:06 AM	12/2/19, 3:57 AM	Active
77189	Medium	Execution, Persistence	11/94	40 machines	EDR	11/28/19, 8:07 AM	12/1/19, 11:04 PM	Active
77707								
77848								
77123								
77653								
76825								
77566								
75542								
75580								
77499								
77407								
76900								
75588								
76837								
76995								

77196

Edit name

Status: Active

Assigned to: Unassigned

Severity: High

Classification: (Not set)

Set status and classification

Categories: Initial access, Execution, Persistence

ACTIVE

Activity time
First - Nov 28, 2019, 8:16:39 AM
Last - Dec 2, 2019, 10:01:01 AM

Alerts and categories

11/11 active alerts
3 MITRE attack categories
No other alert categories

Nov 28, 2019, 8:16:39 AM | New
Windows 10 Machines on desktop-bga19q8
desktop-bga19q8

Nov 28, 2019, 8:53:37 AM | New
Suspicious Power Shell command line on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:53:37 AM | New
Suspicious behavior by Microsoft Word was observed on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:53:37 AM | New
An Office application ran suspicious commands on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:02 AM | New
Suspicious Power Shell command line on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:03 AM | New
Office process dropped and executed a PE file. on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:03 AM | New
Powershell dropped a suspicious file on the machine on desktop-bga19q8 by user admin
desktop-bga19q8

Nov 28, 2019, 8:54:03 AM | New
An anomalous scheduled task was created on desktop-bga19q8 by user admin
desktop-bga19q8

Scope

1 affected device

Top affected assets

Entity type	Risk level/investigation priority
desktop-bga19q8	High

View devices

Evidence

10 entities found

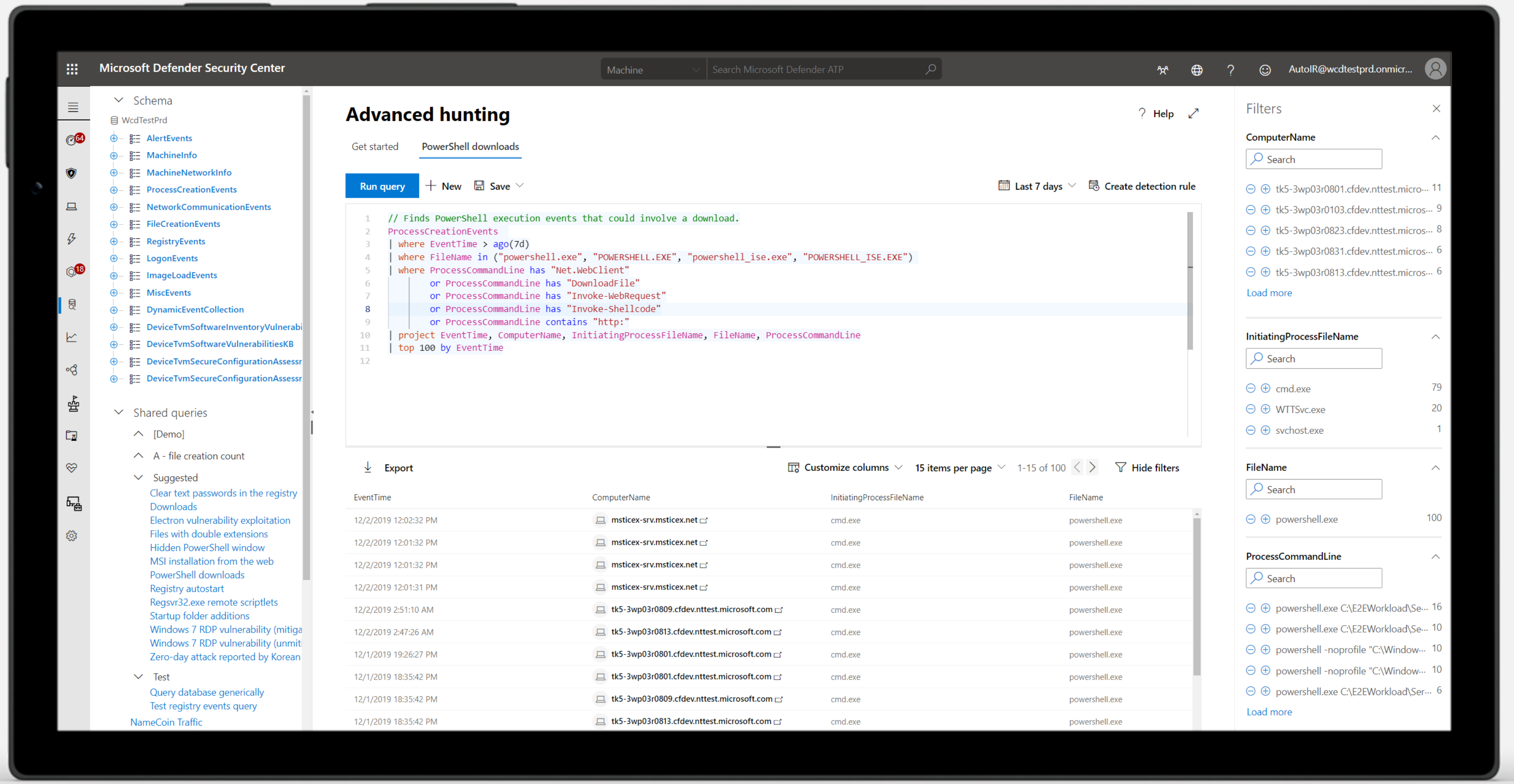
Evidence remediation status

🟩 Remediated ■ Not Found ■ Unremediated ■ Other

View all entities

Announcement blog

Advanced hunting with custom detection and custom response



Schema

WcdTestPrd

- AlertEvents
- MachineInfo
- MachineNetworkInfo
- ProcessCreationEvents
- NetworkCommunicationEvents
- FileCreationEvents
- RegistryEvents
- LogonEvents
- ImageLoadEvents
- MiscEvents
- DynamicEventCollection
- DeviceTvmSoftwareInventoryVulnerabi
- DeviceTvmSoftwareVulnerabilitiesKB
- DeviceTvmSecureConfigurationAssessr
- DeviceTvmSecureConfigurationAssessr

Shared queries

- [Demo]
- A - file creation count
- Suggested
  - Clear text passwords in the registry
  - Downloads
  - Electron vulnerability exploitation
  - Files with double extensions
  - Hidden PowerShell window
  - MSI installation from the web
  - PowerShell downloads
  - Registry autostart
  - Regsvr32.exe remote scriptlets
  - Startup folder additions
  - Windows 7 RDP vulnerability (mitiga
  - Windows 7 RDP vulnerability (unmiti
  - Zero-day attack reported by Korean
- Test
  - Query database generically
  - Test registry events query
- NameCoin Traffic

```
// 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
```

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

Filters

ComputerName	
tk5-3wp03r0801.cfdev.nttest.micro...	11
tk5-3wp03r0103.cfdev.nttest.micros...	9
tk5-3wp03r0823.cfdev.nttest.micros...	8
tk5-3wp03r0831.cfdev.nttest.micros...	6
tk5-3wp03r0813.cfdev.nttest.micros...	6

Load more

InitiatingProcessFileName	
cmd.exe	79
WTTSvc.exe	20
svchost.exe	1

FileName	
powershell.exe	100

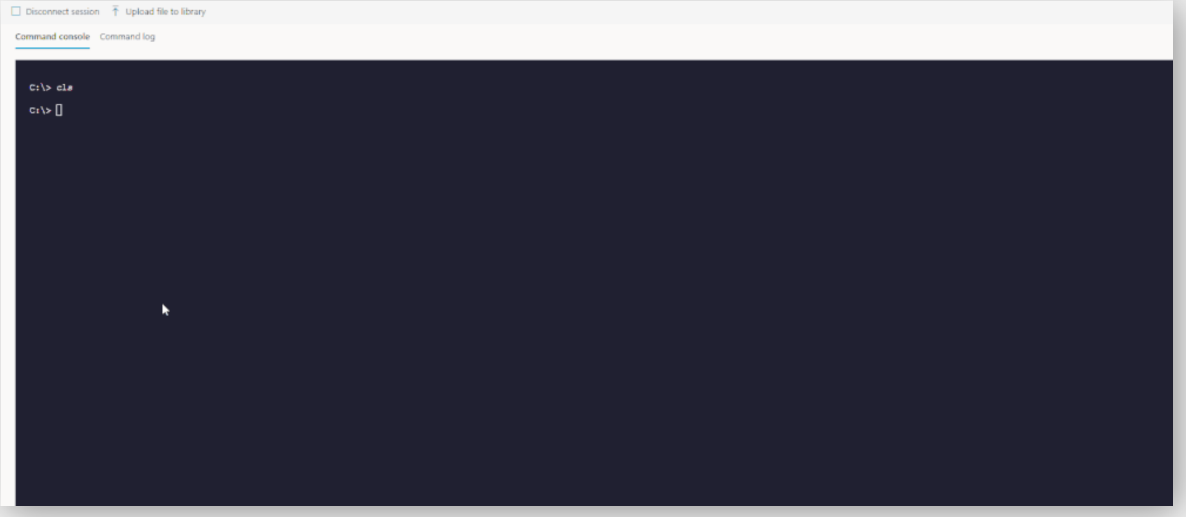
ProcessCommandLine	
powershell.exe C:\E2EWorkload\Se...	16
powershell.exe C:\E2EWorkload\Se...	10
powershell -noprofile "C:\Window...	10
powershell -noprofile "C:\Window...	10
powershell.exe C:\E2EWorkload\Ser...	6

Load more

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)

```
C:\> ▯
```



```
C:\> cls
C:\> ▯
```

Threat Analytics

See how you do against major threats

Threat to posture view

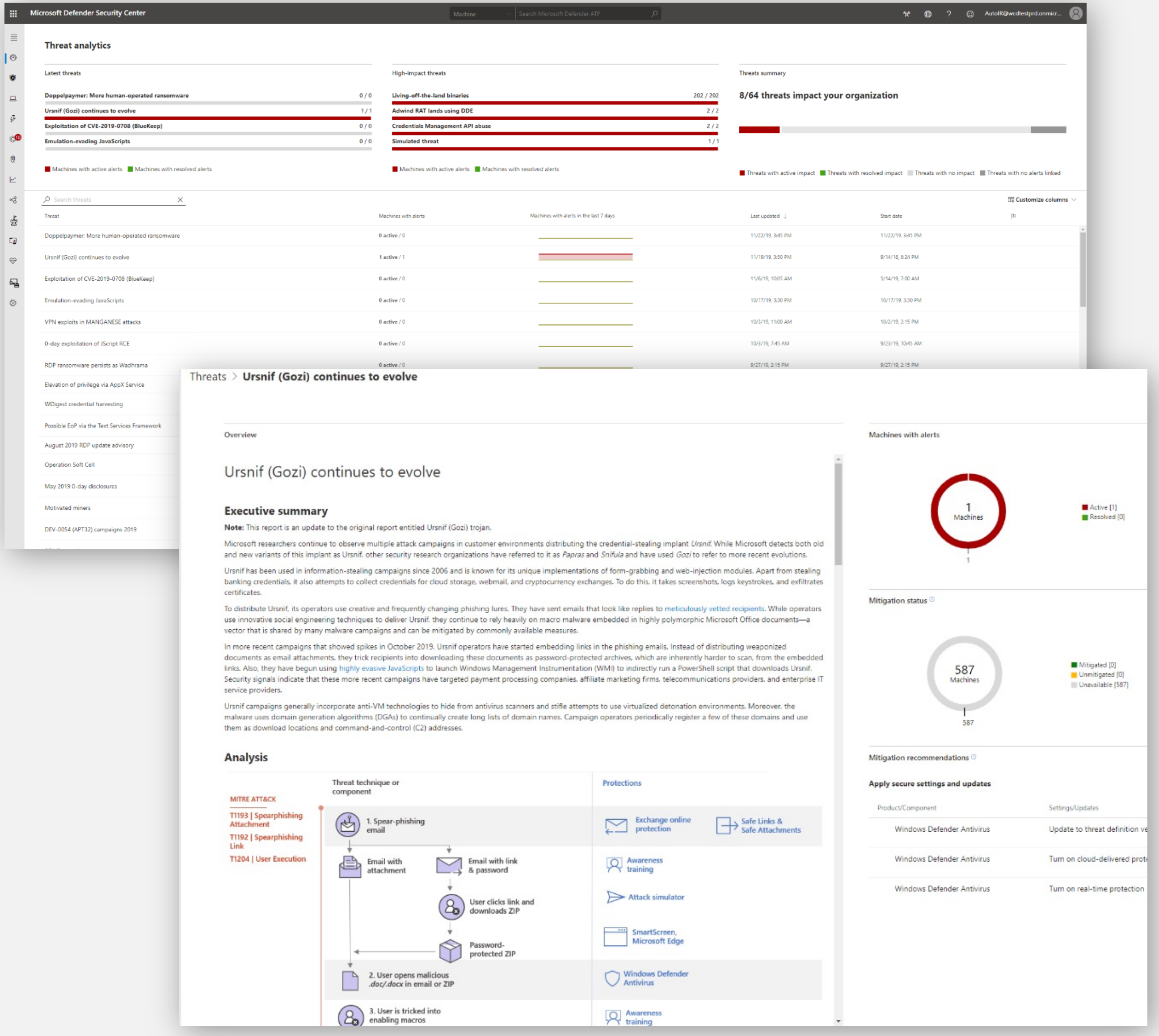
See how you score against significant and emerging campaigns with interactive reports.

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 Security Center

Machine | Search Microsoft Defender ATP | AutoIR@wcdtestprd.onmicr...

Threat analytics

Latest threats

Doppelpaymer: More human-operated ransomware	0 / 0
Ursnif (Gozi) continues to evolve	1 / 1
Exploitation of CVE-2019-0708 (BlueKeep)	0 / 0
Emulation-evading JavaScripts	0 / 0

🟥 Machines with active alerts 🟩 Machines with resolved alerts

High-impact threats

Living-off-the-land binaries	202 / 202
Adwind RAT lands using DDE	2 / 2
Credentials Management API abuse	2 / 2
Simulated threat	1 / 1

🟥 Machines with active alerts 🟩 Machines with resolved alerts

Threats summary

8/64 threats impact your organization

🟥 Threats with active impact 🟩 Threats with resolved impact ▨ Threats with no impact ▨ Threats with no alerts linked

Search threats

Customize columns

Threat	Machines with alerts	Machines with alerts in the last 7 days	Last updated ↓	Start date
Doppelpaymer: More human-operated ransomware	0 active / 0		11/22/19, 3:45 PM	11/22/19, 3:45 PM
Ursnif (Gozi) continues to evolve	1 active / 1		11/19/19, 3:50 PM	9/14/18, 6:24 PM
Exploitation of CVE-2019-0708 (BlueKeep)	0 active / 0		11/6/19, 10:05 AM	5/14/19, 7:00 AM
Emulation-evading JavaScripts	0 active / 0		10/17/19, 3:30 PM	10/17/19, 3:30 PM
VPN exploits in MANGANESE attacks	0 active / 0		10/3/19, 11:00 AM	10/2/19, 2:15 PM
0-day exploitation of JScript RCE	0 active / 0		10/3/19, 7:45 AM	9/23/19, 10:45 AM
RDP ransomware persists as Wadhrama	0 active / 0		9/27/19, 2:15 PM	9/27/19, 2:15 PM
Elevation of privilege via AppX Service				
WDigest credential harvesting				
Possible EoP via the Text Services Framework				
August 2019 RDP update advisory				
Operation Soft Cell				
May 2019 0-day disclosures				
Motivated miners				
DEV-0054 (APT32) campaigns 2019				

Threats > **Ursnif (Gozi) continues to evolve**

Overview

Ursnif (Gozi) continues to evolve

Executive summary

Note: This report is an update to the original report entitled Ursnif (Gozi) trojan.

Microsoft researchers continue to observe multiple attack campaigns in customer environments distributing the credential-stealing implant *Ursnif*. While Microsoft detects both old and new variants of this implant as Ursnif, other security research organizations have referred to it as *Papras* and *Snifula* and have used *Gozi* to refer to more recent evolutions.

Ursnif has been used in information-stealing campaigns since 2006 and is known for its unique implementations of form-grabbing and web-injection modules. Apart from stealing banking credentials, it also attempts to collect credentials for cloud storage, webmail, and cryptocurrency exchanges. To do this, it takes screenshots, logs keystrokes, and exfiltrates certificates.

To distribute Ursnif, its operators use creative and frequently changing phishing lures. They have sent emails that look like replies to meticulously vetted recipients. While operators use innovative social engineering techniques to deliver Ursnif, they continue to rely heavily on macro malware embedded in highly polymorphic Microsoft Office documents—a vector that is shared by many malware campaigns and can be mitigated by commonly available measures.

In more recent campaigns that showed spikes in October 2019, Ursnif operators have started embedding links in the phishing emails. Instead of distributing weaponized documents as email attachments, they trick recipients into downloading these documents as password-protected archives, which are inherently harder to scan, from the embedded links. Also, they have begun using highly evasive JavaScripts to launch Windows Management Instrumentation (WMI) to indirectly run a PowerShell script that downloads Ursnif. Security signals indicate that these more recent campaigns have targeted payment processing companies, affiliate marketing firms, telecommunications providers, and enterprise IT service providers.

Ursnif campaigns generally incorporate anti-VM technologies to hide from antivirus scanners and stifle attempts to use virtualized detonation environments. Moreover, the malware uses domain generation algorithms (DGAs) to continually create long lists of domain names. Campaign operators periodically register a few of these domains and use them as download locations and command-and-control (C2) addresses.

Analysis

MITRE ATT&CK
T1193 | Spearphishing Attachment
T1192 | Spearphishing Link
T1204 | User Execution
Threat technique or component
1. Spear-phishing email
Email with attachment
Email with link & password
User clicks link and downloads ZIP
Password-protected ZIP
2. User opens malicious .doc/.docx in email or ZIP
3. User is tricked into enabling macros
Protections
Exchange online protection
Safe Links & Safe Attachments
Awareness training
Attack simulator
SmartScreen, Microsoft Edge
Windows Defender Antivirus
Awareness training

Machines with alerts

🟥 Active [1]
🟩 Resolved [0]

Mitigation status

🟩 Mitigated [0]
🟨 Unmitigated [0]
▨ Unavailable [587]

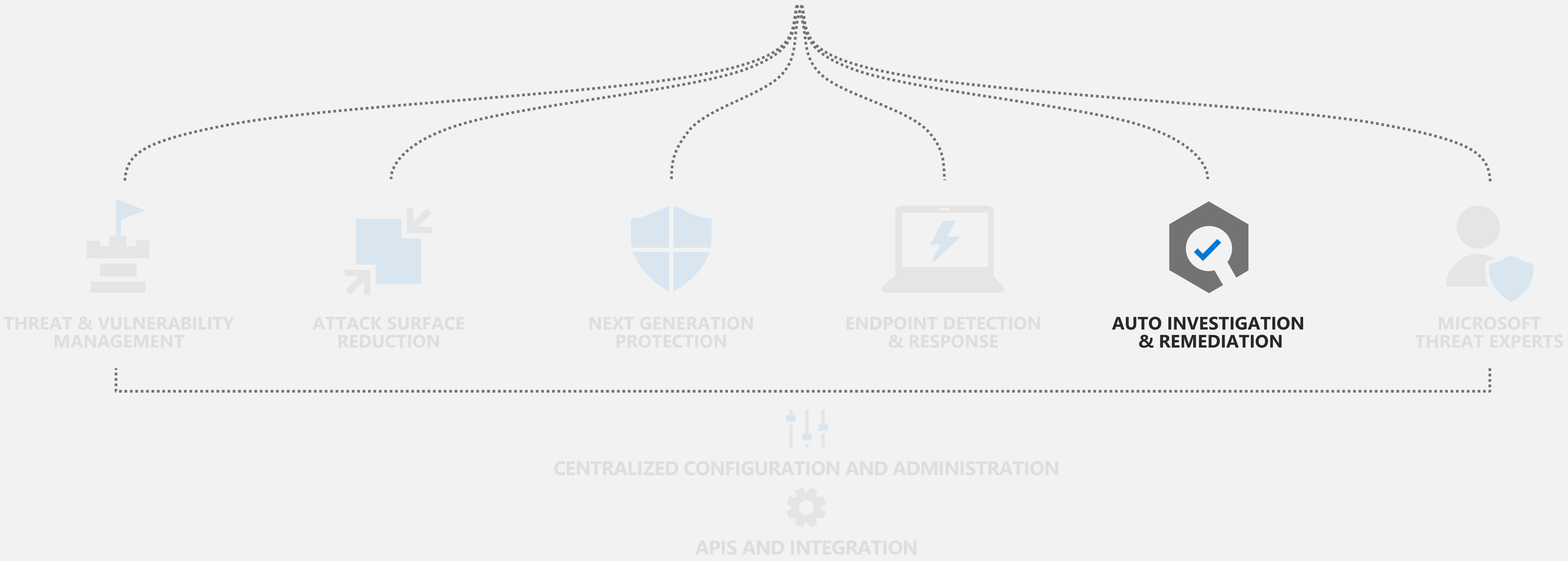
Mitigation recommendations

Apply secure settings and updates

Product/Component	Settings/Updates
Windows Defender Antivirus	Update to threat definition ve
Windows Defender Antivirus	Turn on cloud-delivered prote
Windows Defender Antivirus	Turn on real-time protection

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

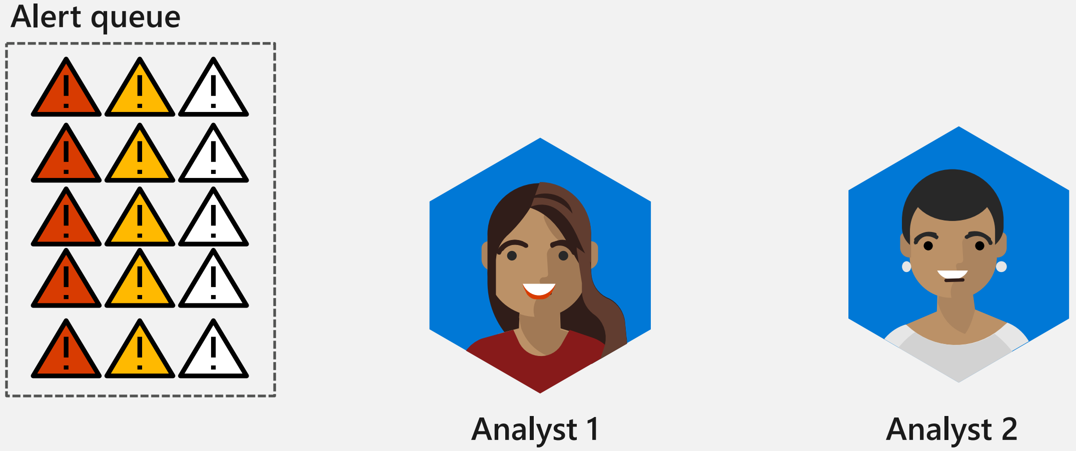
CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

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



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

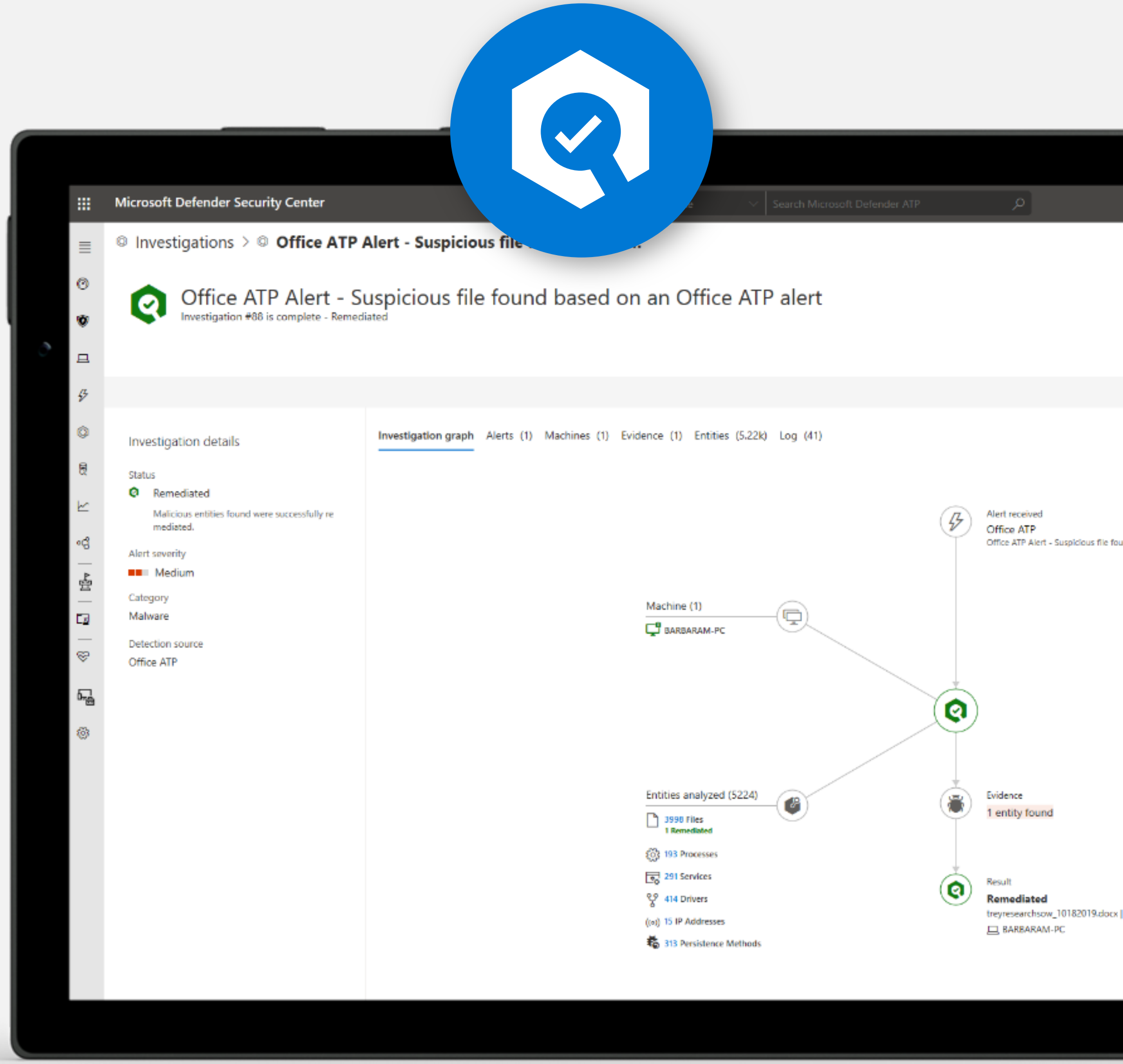
When we look at the steps an analyst is taking as when investigating and remediating threats we can identify the following high-level steps:

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


Microsoft Defender Security Center
Search Microsoft Defender ATP
Investigations > Office ATP Alert - Suspicious file
Investigation graph
Alerts (1)
Machines (1)
Evidence (1)
Entities (5.22k)
Log (41)

Office ATP Alert - Suspicious file found based on an Office ATP alert

Investigation #88 is complete - Remediated

Investigation details

Status

Remediated

Malicious entities found were successfully re mediated.

Alert severity

Medium

Category

Malware

Detection source

Office ATP

Alert received

Office ATP

Office ATP Alert - Suspicious file fou

Machine (1)

BARBARAM-PC

Entities analyzed (5224)

3998 Files

1 Remediated

193 Processes

291 Services

414 Drivers

15 IP Addresses

313 Persistence Methods

Evidence

1 entity found

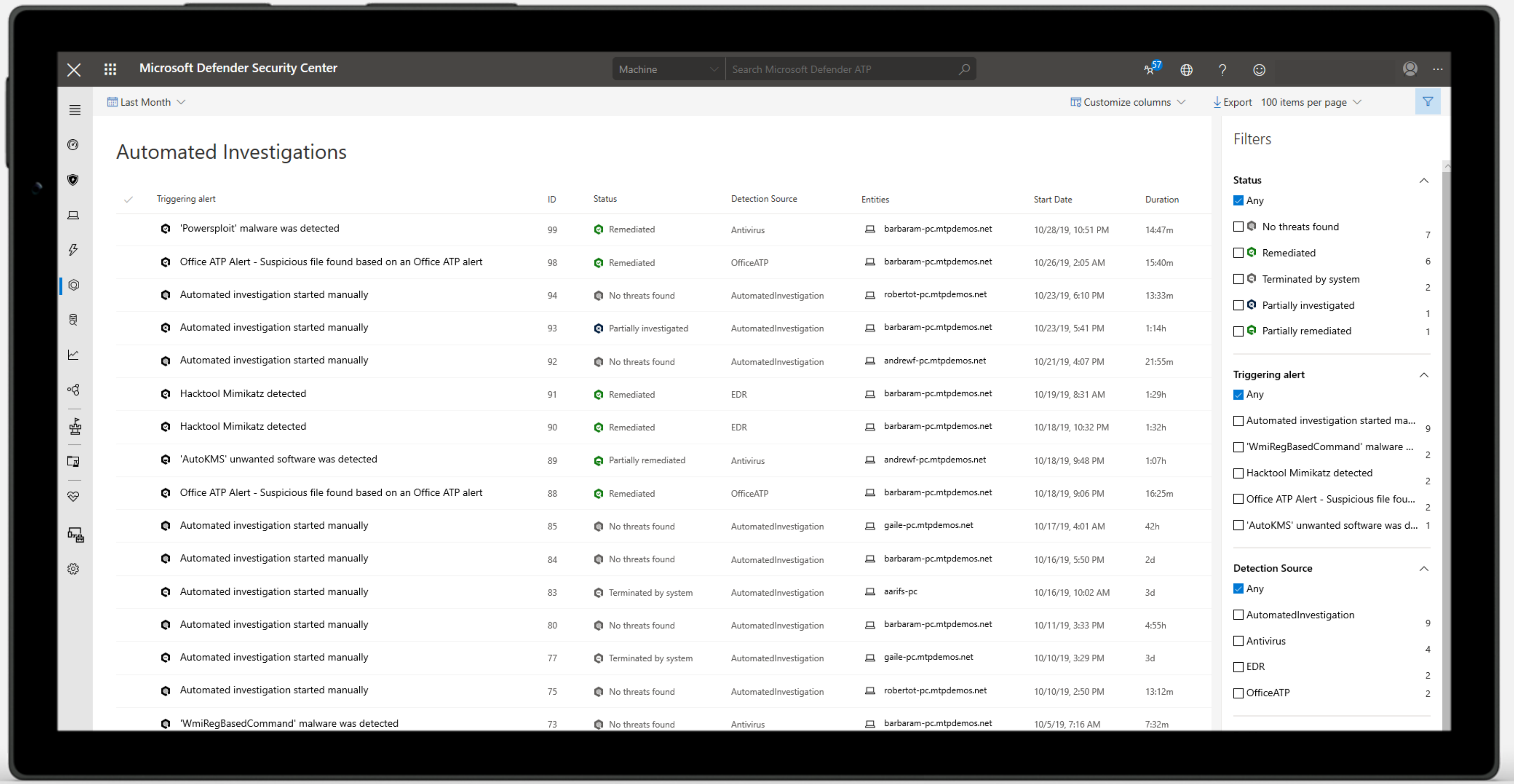
Result

Remediated

treyresearchsow_10182019.docx |

BARBARAM-PC

Auto investigation queue



Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
57
Last Month
Customize columns
Export
100 items per page

Automated Investigations

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

Filters

Status

- ☑ Any
- □ No threats found 7
- □ Remediated 6
- □ Terminated by system 2
- □ Partially investigated 1
- □ Partially remediated 1

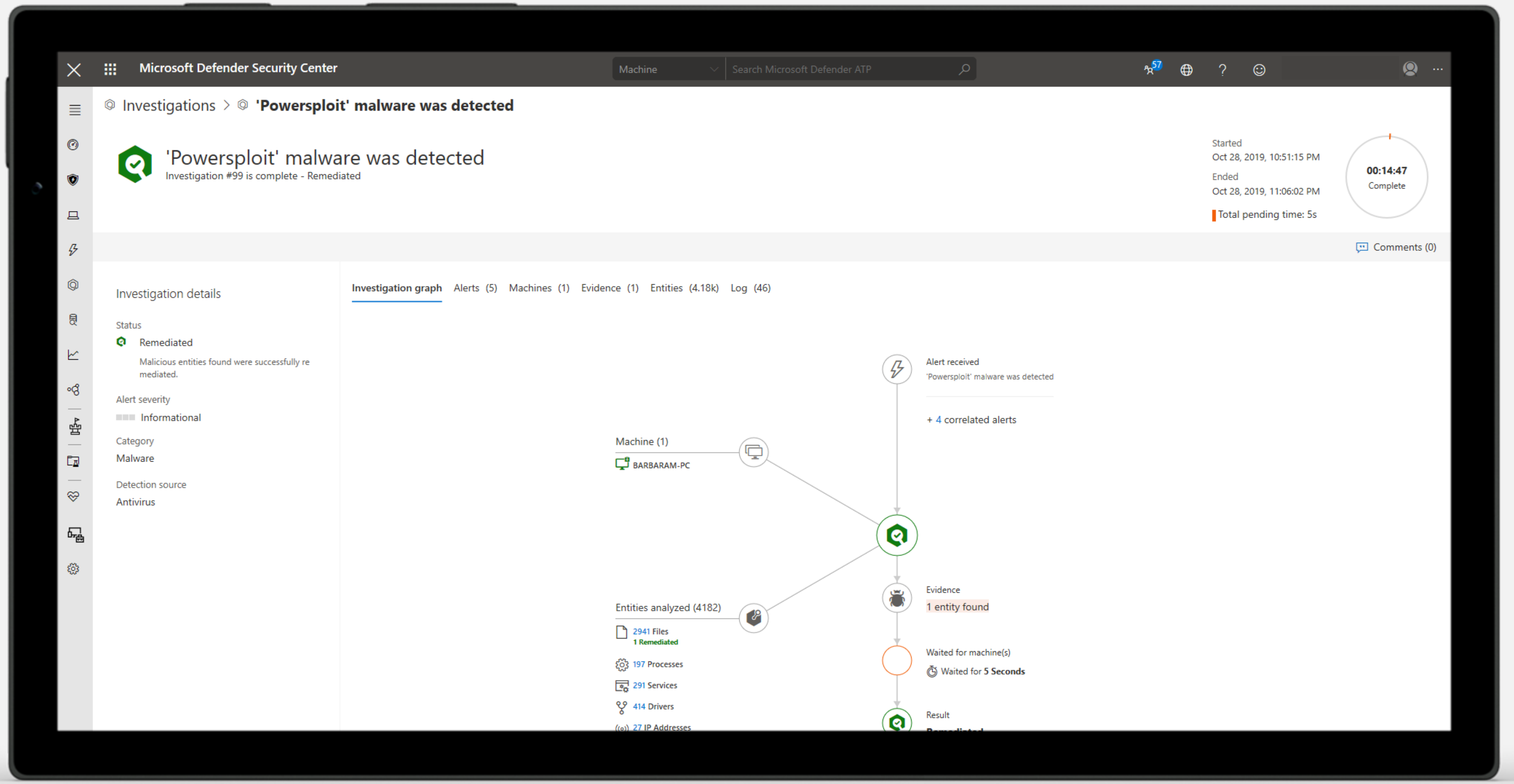
Triggering alert

- ☑ Any
- □ Automated investigation started ma... 9
- □ 'WmiRegBasedCommand' malware ... 2
- □ Hacktool Mimikatz detected 2
- □ Office ATP Alert - Suspicious file fou... 2
- □ 'AutoKMS' unwanted software was d... 1

Detection Source

- ☑ Any
- □ AutomatedInvestigation 9
- □ Antivirus 4
- □ EDR 2
- □ OfficeATP 2

Investigation graph



Microsoft Defender Security Center

Machine | Search Microsoft Defender ATP

Investigations > 'Powersploit' malware was detected

'Powersploit' malware was detected

Investigation #99 is complete - Remediated

Started
Oct 28, 2019, 10:51:15 PM

Ended
Oct 28, 2019, 11:06:02 PM

Total pending time: 5s

00:14:47
Complete

Comments (0)

Investigation details

Status
Remediated
Malicious entities found were successfully re mediated.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (5) | Machines (1) | Evidence (1) | Entities (4.18k) | Log (46)

Alert received
'Powersploit' malware was detected

+ 4 correlated alerts

Machine (1)
BARBARAM-PC

Entities analyzed (4182)
2941 Files
1 Remediated
197 Processes
291 Services
414 Drivers
27 IP Addresses

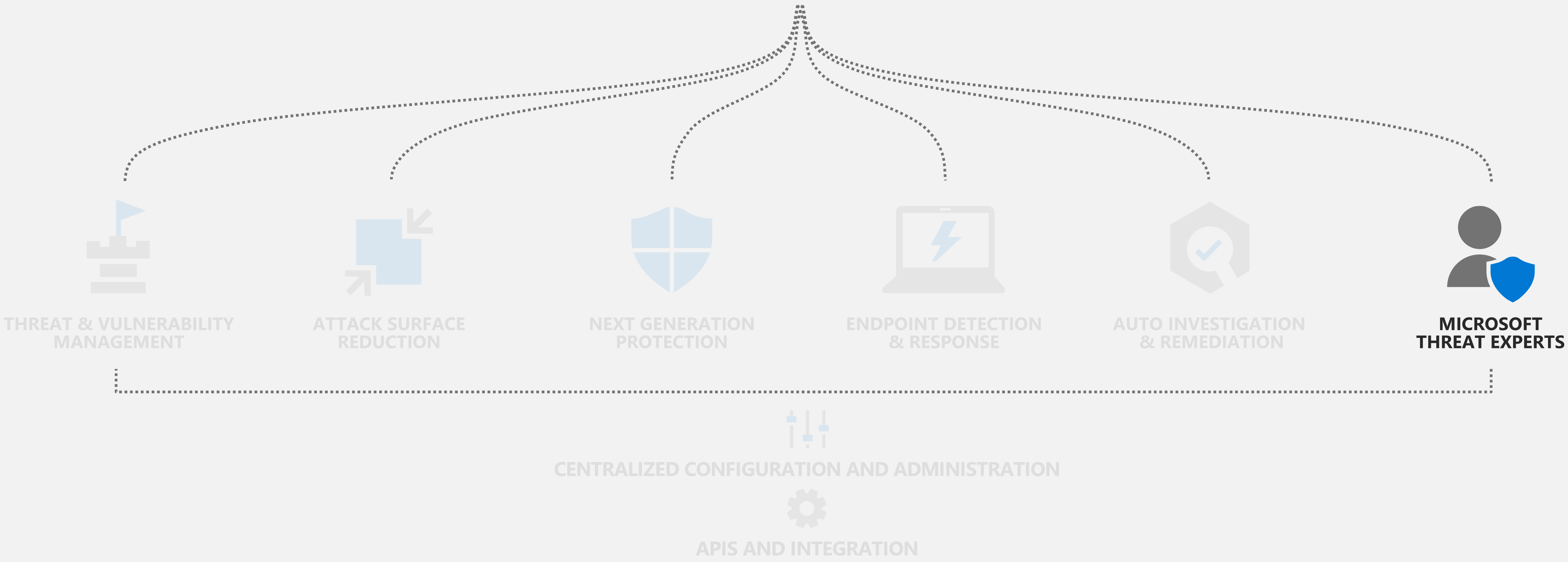
Evidence
1 entity found

Waited for machine(s)
Waited for 5 Seconds

Result
Remediated

Microsoft Defender
for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

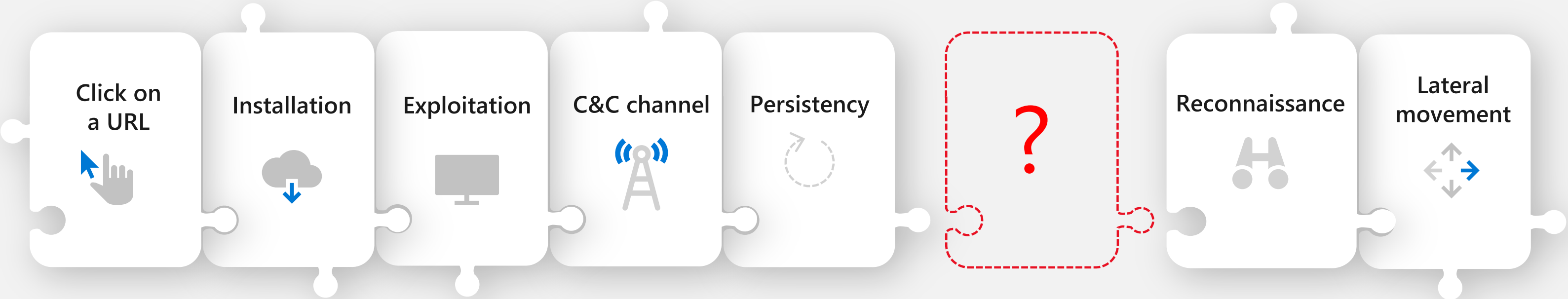
MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

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

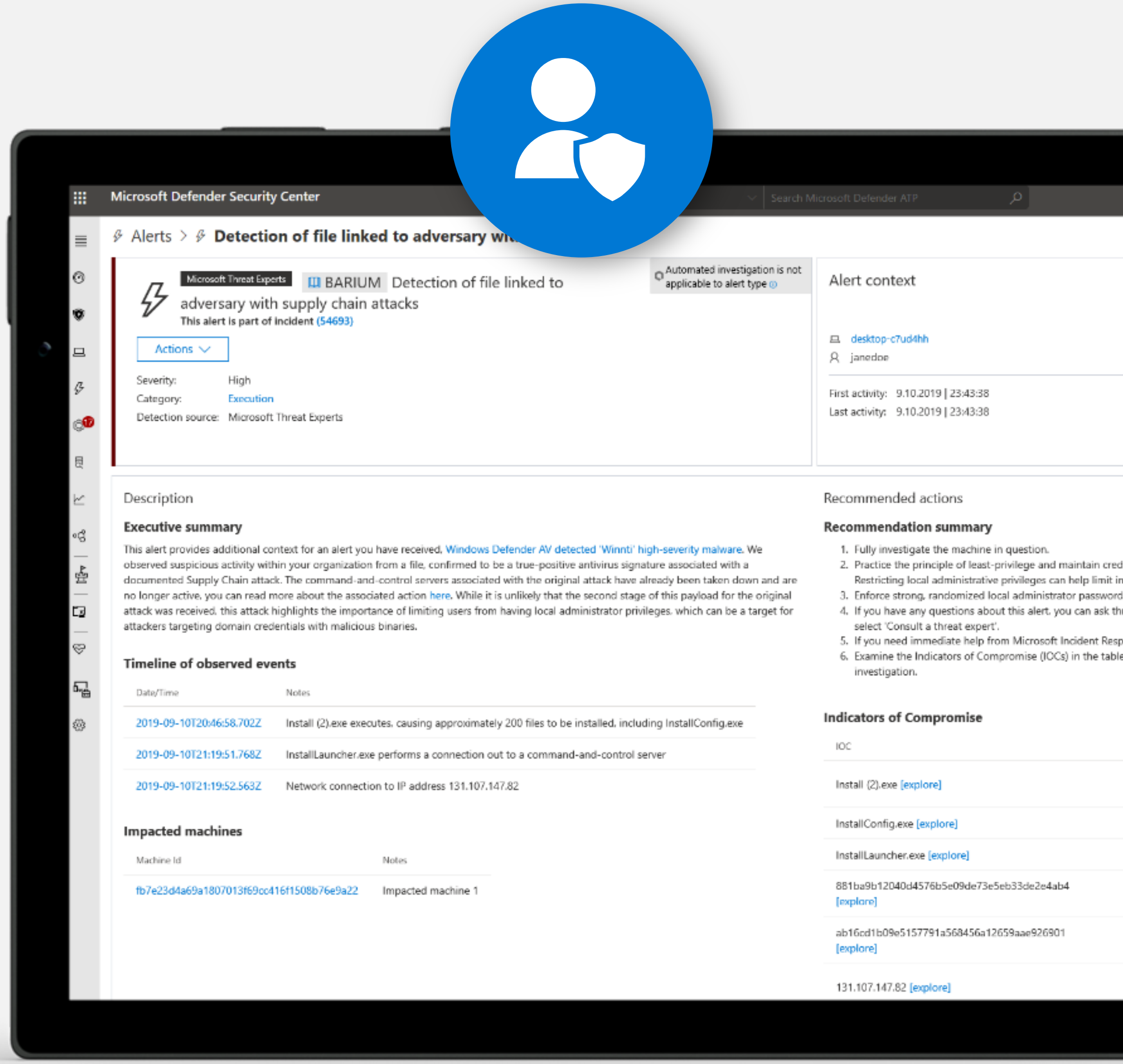
Important alerts might get missed

Does this alert or event really matter to my org?

Microsoft Threat Experts

Bring deep knowledge and proactive threat hunting to your SOC

- Expert level threat monitoring and analysis
- Environment-specific context via alerts
- Direct access to world-class hunters



Microsoft Defender Security Center
Search Microsoft Defender ATP
Alerts > Detection of file linked to adversary wi
Microsoft Threat Experts
BARIUM
Actions

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

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 question.
2. Practice the principle of least-privilege and maintain cred
   Restricting local administrative privileges can help limit in
3. Enforce strong, randomized local administrator password
4. If you have any questions about this alert, you can ask th
   select 'Consult a threat expert'.
5. If you need immediate help from Microsoft Incident Resp
6. Examine the Indicators of Compromise (IOCs) in the table
   investigation.

Indicators of Compromise

IOC
Install (2).exe [explore]
InstallConfig.exe [explore]
InstallLauncher.exe [explore]
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 [explore]
ab16cd1b09e5157791a568456a12659aae926901 [explore]
131.107.147.82 [explore]

Microsoft Threat Experts

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

Targeted attack notifications

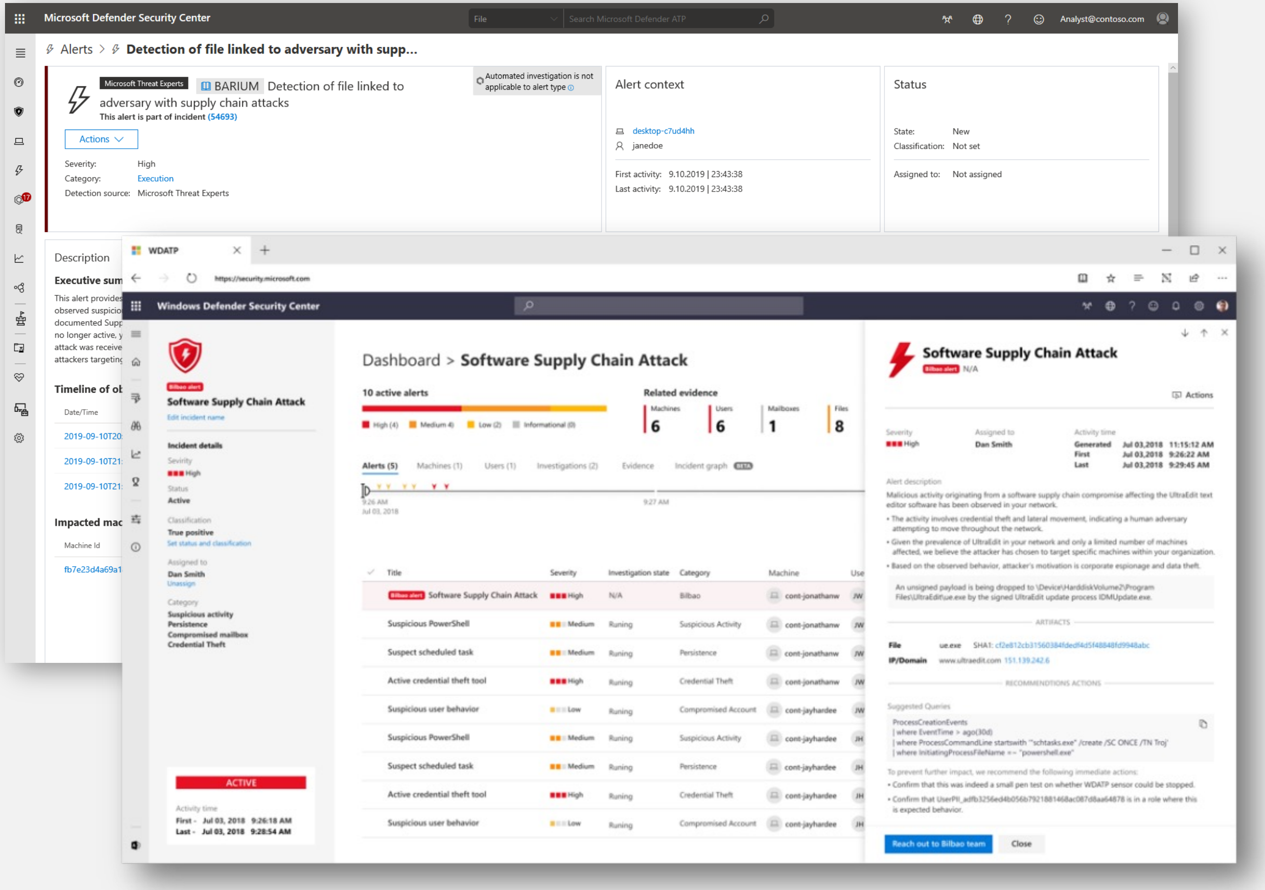
Threat hunters have your back.

Microsoft 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 Defender Security Center
File
Search Microsoft Defender ATP
Analyst@contoso.com

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

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

WDATP
https://security.microsoft.com
Windows Defender Security Center

Bilbao alert

Software Supply Chain Attack

Edit incident name

Incident details

Severity
High

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Suspicious activity
Persistence
Compromised mailbox
Credential Theft

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Dashboard > Software Supply Chain Attack

10 active alerts

High (4) Medium 4) Low (2) Informational (0)

Related evidence

Machines	Users	Mailboxes	Files
6	6	1	8

Title	Severity	Investigation state	Category	Machine	Use
Bilbao alert Software Supply Chain Attack	High	N/A	Bilbao	cont-jonathanw	JW
Suspicious PowerShell	Medium	Runing	Suspicious Activity	cont-jonathanw	JW
Suspect scheduled task	Medium	Runing	Persistence	cont-jonathanw	JW
Active credential theft tool	High	Runing	Credential Theft	cont-jonathanw	JW
Suspicious user behavior	Low	Runing	Compromised Account	cont-jayhardee	JW
Suspicious PowerShell	Medium	Runing	Suspicious Activity	cont-jayhardee	JH
Suspect scheduled task	Medium	Runing	Persistence	cont-jayhardee	JH
Active credential theft tool	High	Runing	Credential Theft	cont-jayhardee	JH
Suspicious user behavior	Low	Runing	Compromised Account	cont-jayhardee	JH

Software Supply Chain Attack

Bilbao alert N/A

Severity
High

Assigned to
Dan Smith

Activity time
Generated Jul 03,2018 11:15:12 AM
First Jul 03,2018 9:26:22 AM
Last Jul 03,2018 9:29:45 AM

Alert description

Malicious activity originating from a software supply chain compromise affecting the UltraEdit text editor software has been observed in your network.

- The activity involves credential theft and lateral movement, indicating a human adversary attempting to move throughout the network.
- Given the prevalence of UltraEdit in your network and only a limited number of machines affected, we believe the attacker has chosen to target specific machines within your organization.
- Based on the observed behavior, attacker's motivation is corporate espionage and data theft.

An unsigned payload is being dropped to \Device\HarddiskVolume2\Program Files\UltraEdit\ue.exe by the signed UltraEdit update process IDMUpdate.exe.

ARTIFACTS

File ue.exe SHA1: cf2e812cb31560384fdedf4d5f48848fd9948abc
IP/Domain www.ultraedit.com 151.139.242.6

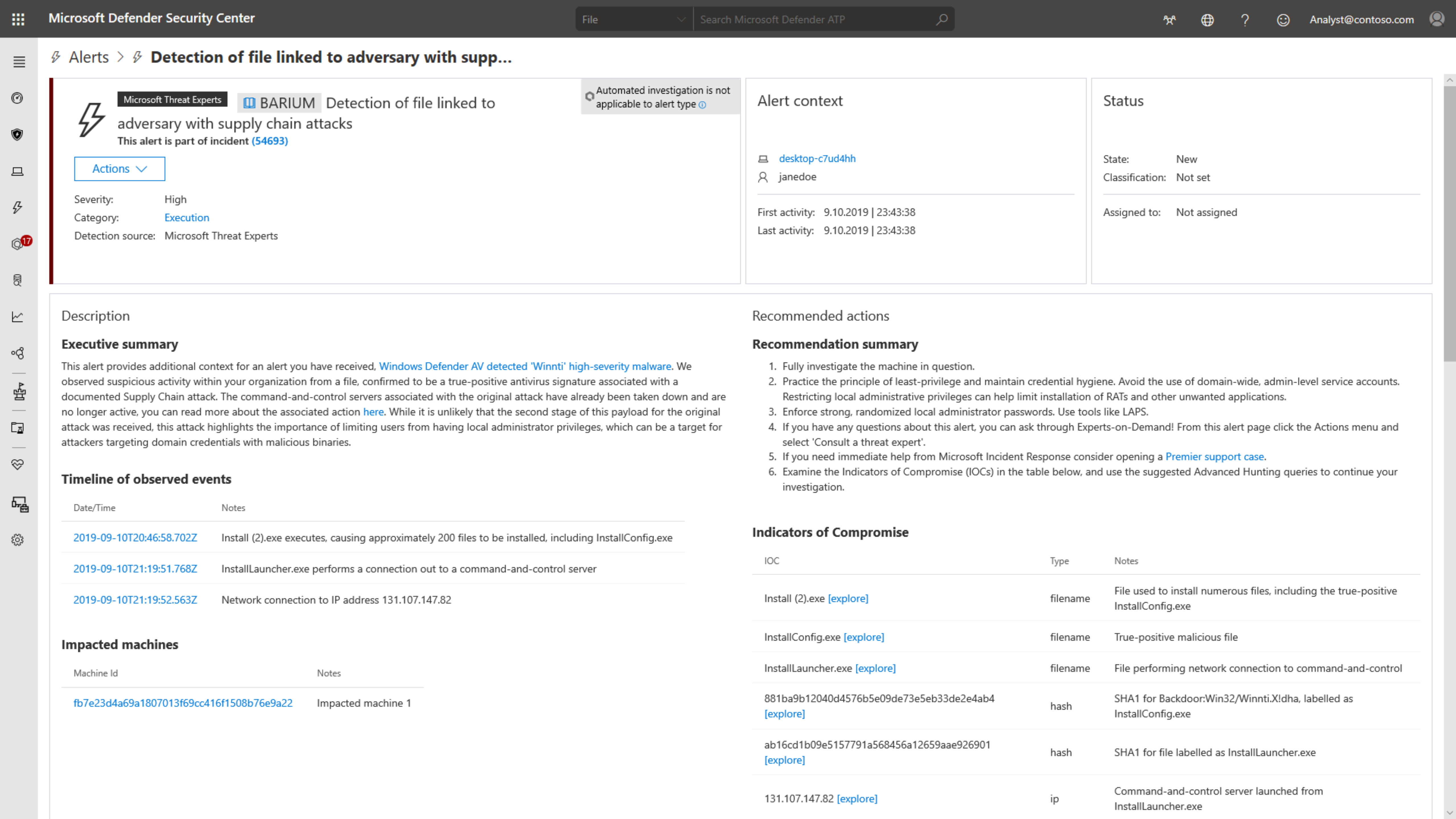
RECOMMENDTIONS ACTIONS

Suggested Queries

```
ProcessCreationEvents
| where EventTime > ago(30d)
| where ProcessCommandLine startswith '"schtasks.exe" /create /SC ONCE /TN Troj'
| where InitiatingProcessFileName =~ "powershell.exe"
```

To prevent further impact, we recommend the following immediate actions:

- Confirm that this was indeed a small pen test on whether WDATP sensor could be stopped.
- Confirm that UserPII_adfb3256ed4b056b7921881468ac087d8aa64878 is in a role where this is expected behavior.


Microsoft Defender Security Center
File
Search Microsoft Defender ATP
Analyst@contoso.com
17

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

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

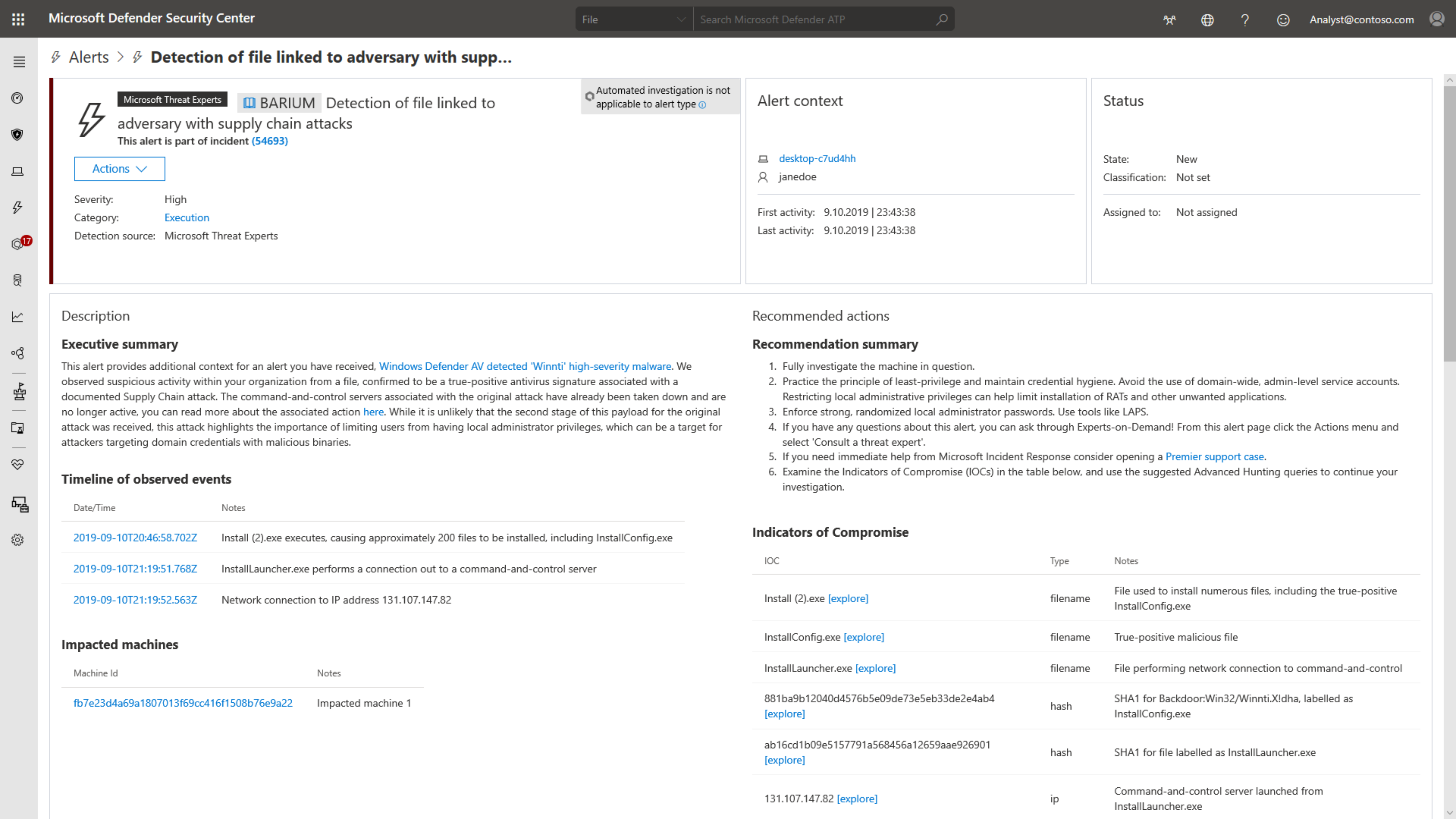
Recommended actions

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 Defender Security Center
File
Search Microsoft Defender ATP
Analyst@contoso.com
17

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

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

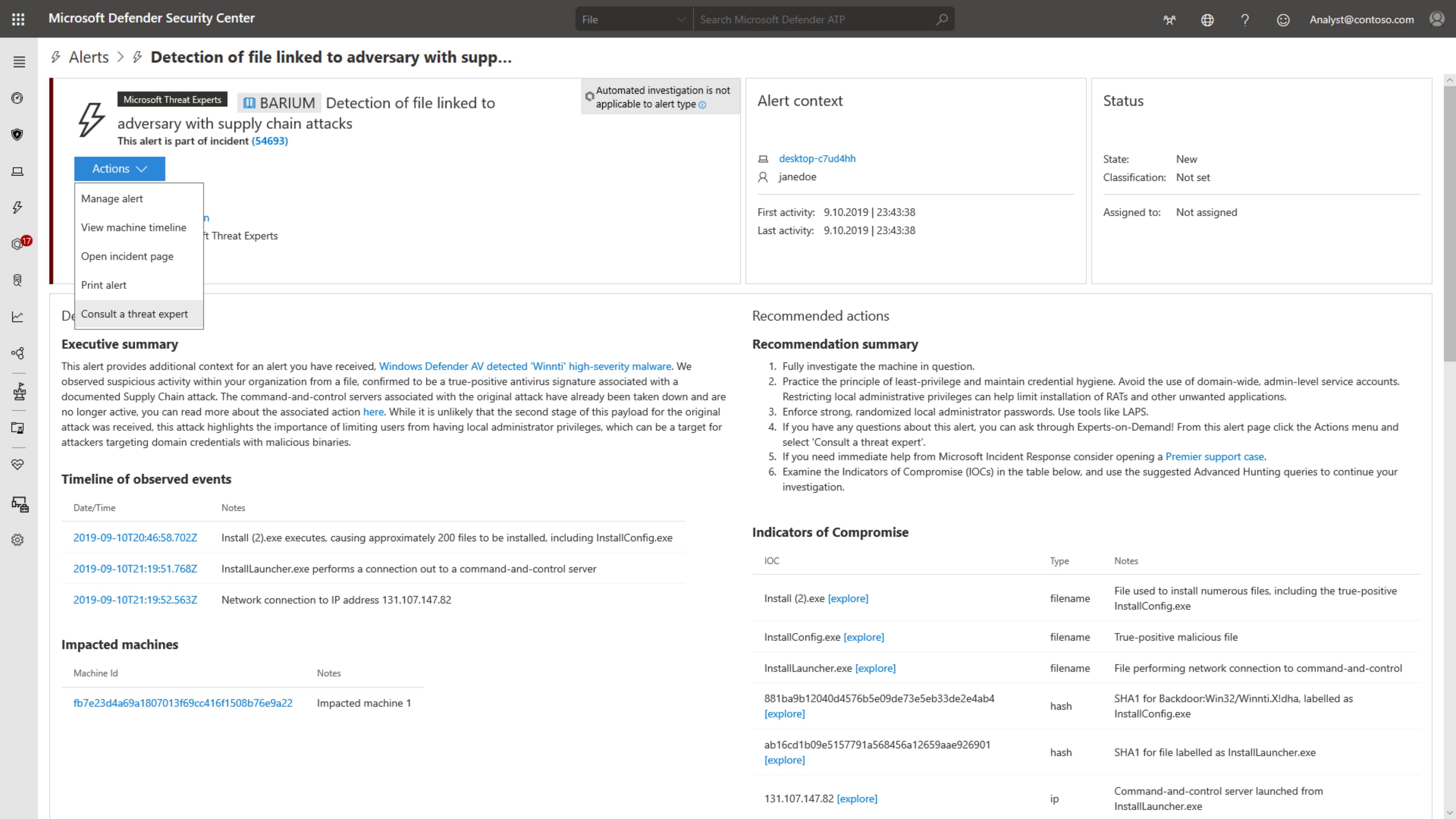
Recommended actions

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



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

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

De

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

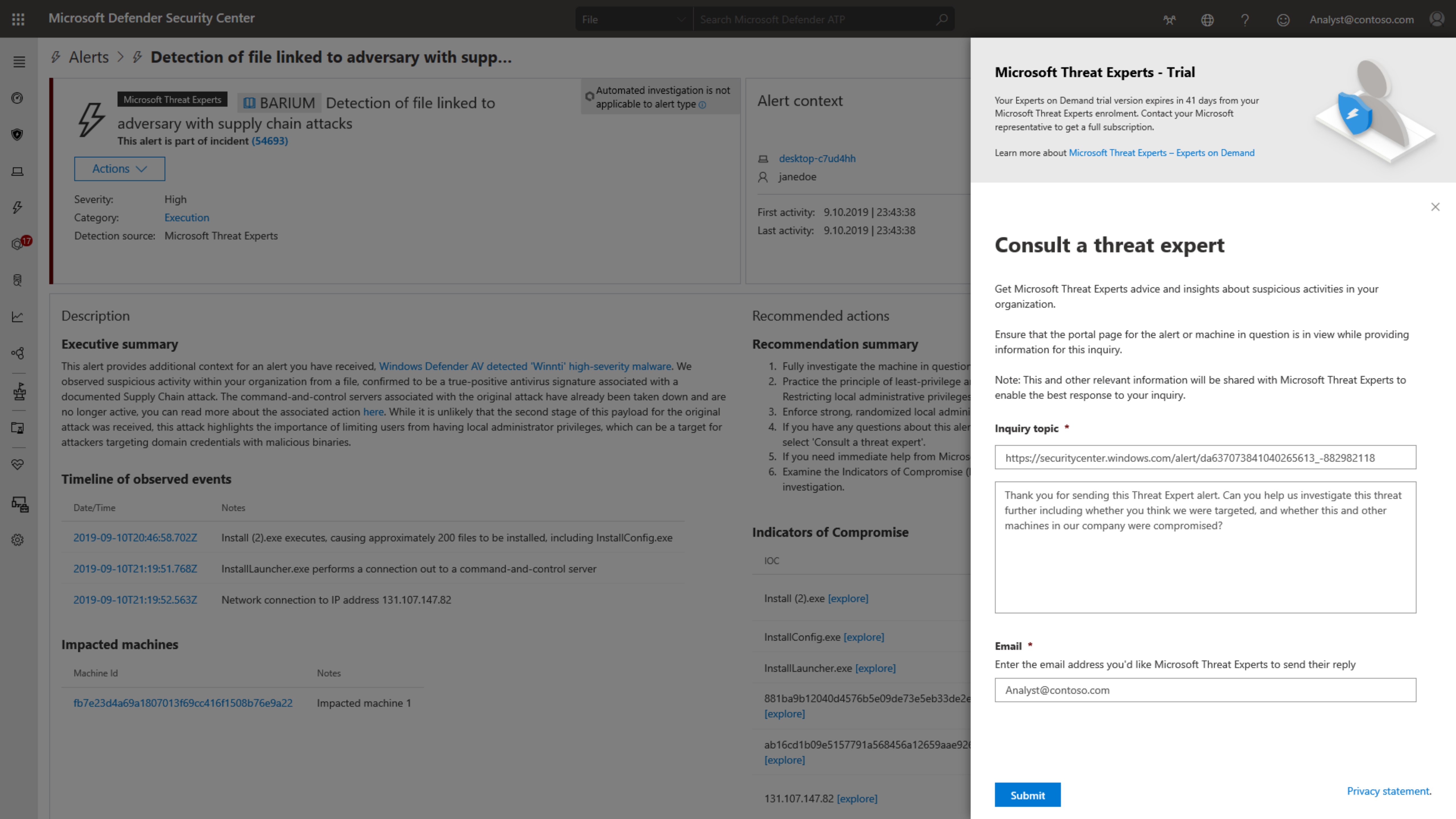
Recommended actions

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 Defender Security Center
File
Search Microsoft Defender ATP
Analyst@contoso.com
17
Actions
Submit
Privacy statement.

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

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 questior
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?

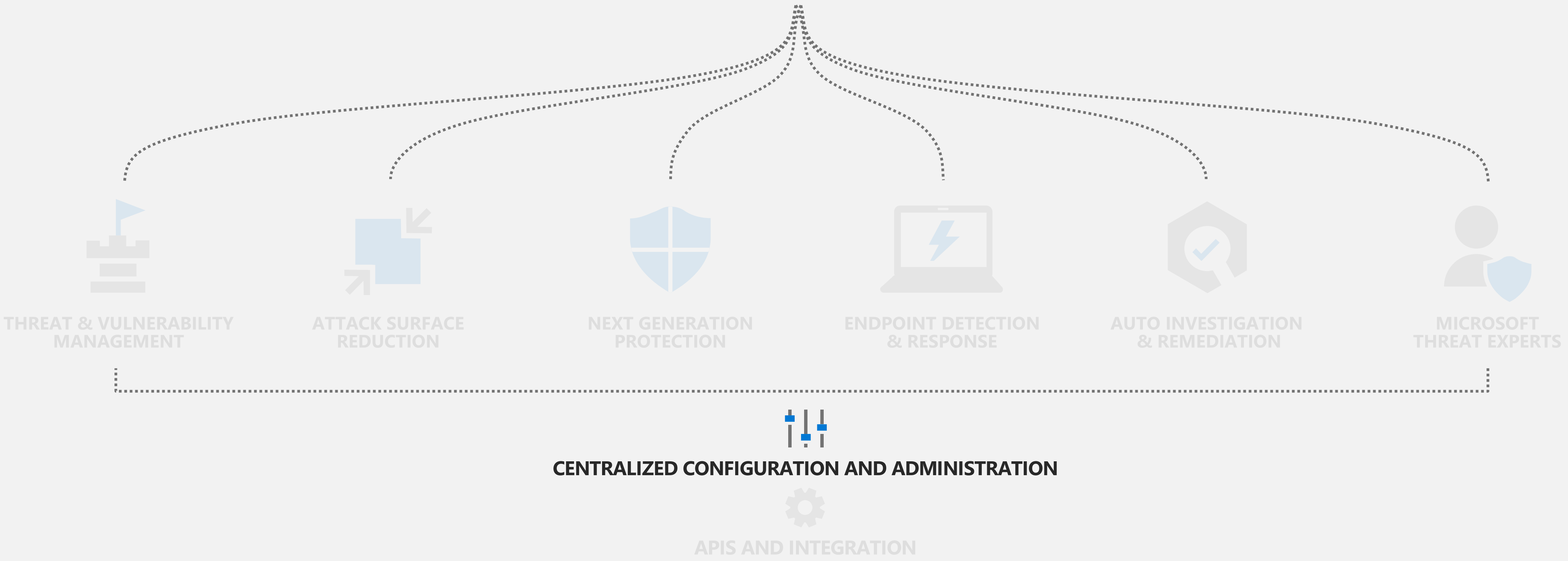
Email *

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

Analyst@contoso.com

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

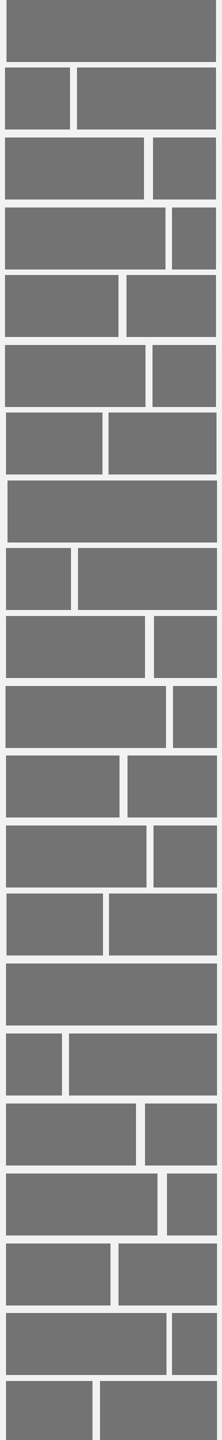
CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

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

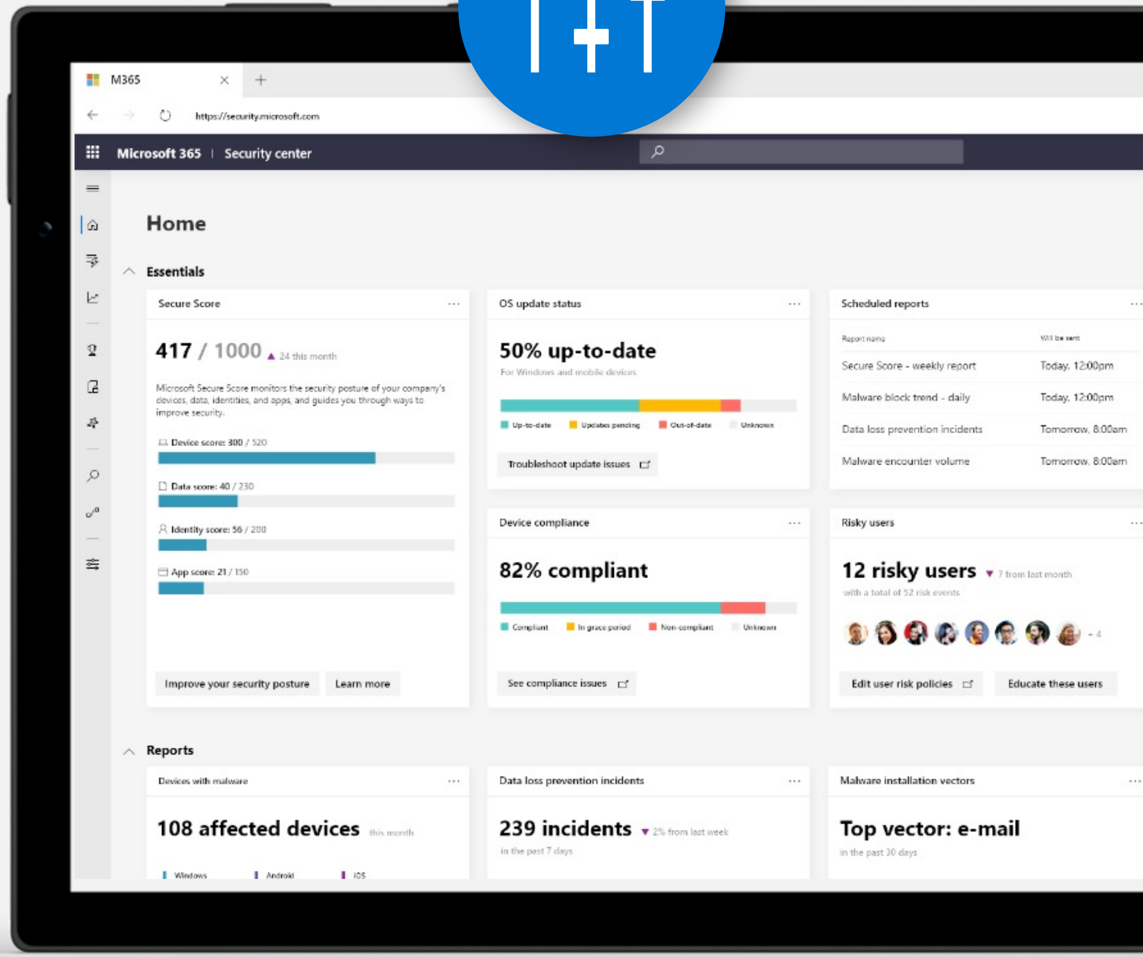
Continuous assessment and reporting of endpoint state

Seamless and frictionless

Security Management

Assess, configure and respond to changes in your environment

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


M365
https://security.microsoft.com
Microsoft 365 | Security center
Home
Essentials

Secure Score

417 / 1000 ▲ 24 this month

Microsoft Secure Score monitors the security posture of your company's devices, data, identities, and apps, and guides you through ways to improve security.

Device score: 300 / 520

Data score: 40 / 230

Identity score: 56 / 200

App score: 21 / 150

Improve your security posture
Learn more

OS update status

50% up-to-date

For Windows and mobile devices

Up-to-date
Updates pending
Out-of-date
Unknown
Troubleshoot update issues

Scheduled reports

Report name	Will be sent
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

Device compliance

82% compliant

Risky users

12 risky users ▼ 7 from last month

with a total of 52 risk events

Devices with malware

108 affected devices this month

Data loss prevention incidents

239 incidents ▼ 2% from last week

in the past 7 days

Malware installation vectors

Top vector: e-mail

in the past 30 days

Endpoint Security Management

All devices

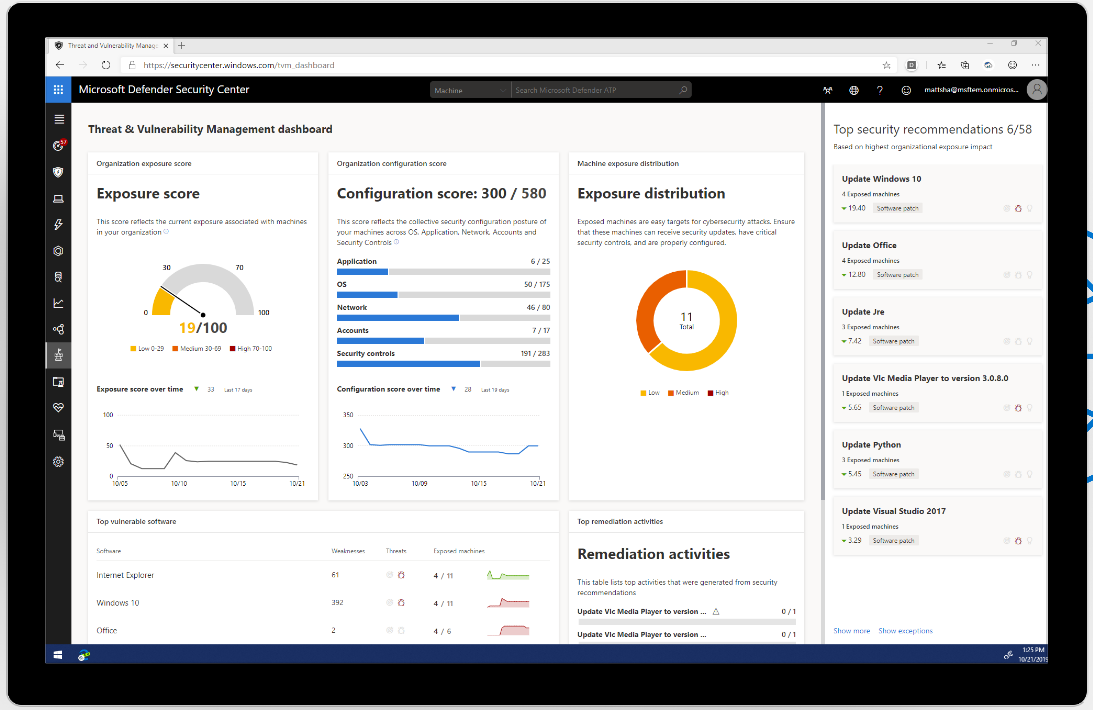
Sec Admin experiences

Security baselines

Security tasks

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

Seamless integration



Threat and Vulnerability Manage
https://securitycenter.windows.com/tvm_dashboard
Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
mattsha@msftem.onmicros...

Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with machines in your organization

30
70
0
100
19/100
Low 0-29
Medium 30-69
High 70-100

Exposure score over time ▼ 33 Last 17 days

100
50
0
10/05
10/10
10/15
10/21

Organization configuration score

Configuration score: 300 / 580

This score reflects the collective security configuration posture of your machines across OS, Application, Network, Accounts and Security Controls

Application	6 / 25
OS	50 / 175
Network	46 / 80
Accounts	7 / 17
Security controls	191 / 283

Configuration score over time ▼ 28 Last 19 days

Machine exposure distribution

Exposure distribution

Exposed machines are easy targets for cybersecurity attacks. Ensure that these machines can receive security updates, have critical security controls, and are properly configured.

Top vulnerable software

Software	Weaknesses	Threats	Exposed machines
Internet Explorer	61		4 / 11
Windows 10	392		4 / 11
Office	2		4 / 6

Top remediation activities

Remediation activities

This table lists top activities that were generated from security recommendations

Update Vlc Media Player to version ... ⚠	0 / 1
Update Vlc Media Player to version ...	0 / 1

Top security recommendations 6/58

Based on highest organizational exposure impact

Update Windows 10
4 Exposed machines
▼ 19.40 Software patch

Update Office
4 Exposed machines
▼ 12.80 Software patch

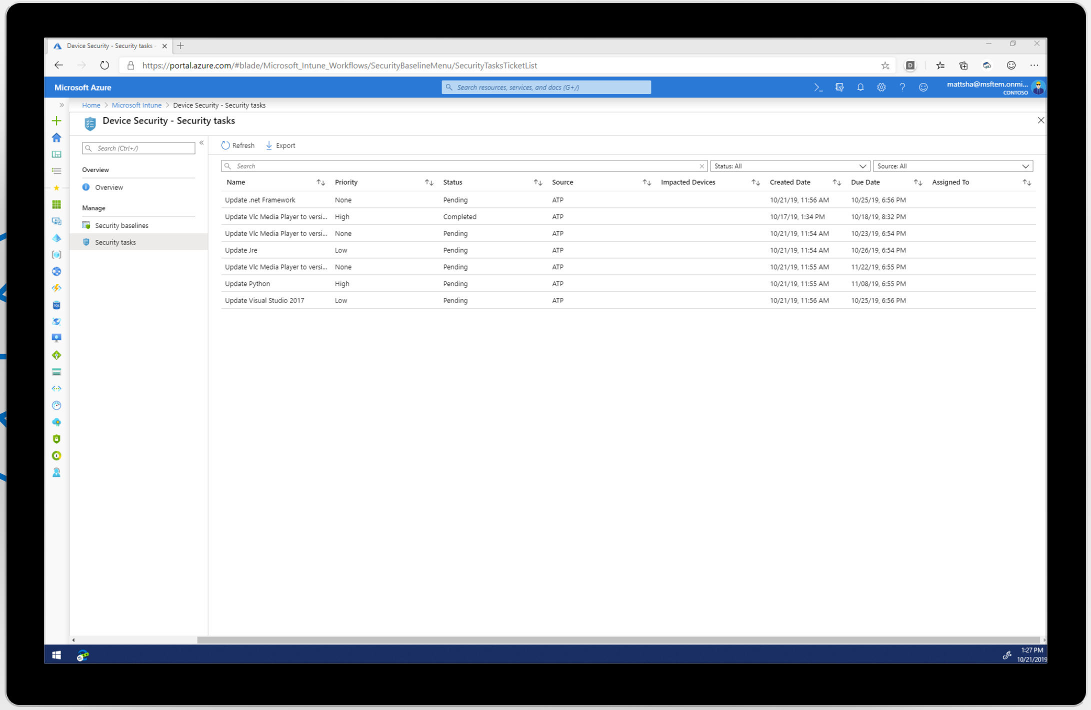
Update Jre
3 Exposed machines
▼ 7.42 Software patch

Update Vlc Media Player to version 3.0.8.0
1 Exposed machines
▼ 5.65 Software patch

Update Python
3 Exposed machines
▼ 5.45 Software patch

Update Visual Studio 2017
1 Exposed machines
▼ 3.29 Software patch

Show more Show exceptions



Device Security - Security tasks
https://portal.azure.com/#blade/Microsoft_Intune_Workflows/SecurityBaselineMenu/SecurityTasksTicketList
Microsoft Azure
Search resources, services, and docs (G+/)
mattsha@msftem.onmi...
CONTOSO
Home > Microsoft Intune > Device Security - Security tasks
Search (Ctrl+/)
Overview
Overview
Manage
Security baselines
Security tasks
Refresh
Export
Search

Device Security - Security tasks

Status: All
Source: All

Name	Priority	Status	Source	Impacted Devices	Created Date	Due Date	Assigned To
Update .net Framework	None	Pending	ATP		10/21/19, 11:56 AM	10/25/19, 6:56 PM	
Update Vlc Media Player to versi...	High	Completed	ATP		10/17/19, 1:34 PM	10/18/19, 8:32 PM	
Update Vlc Media Player to versi...	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 versi...	None	Pending	ATP		10/21/19, 11:55 AM	11/22/19, 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	

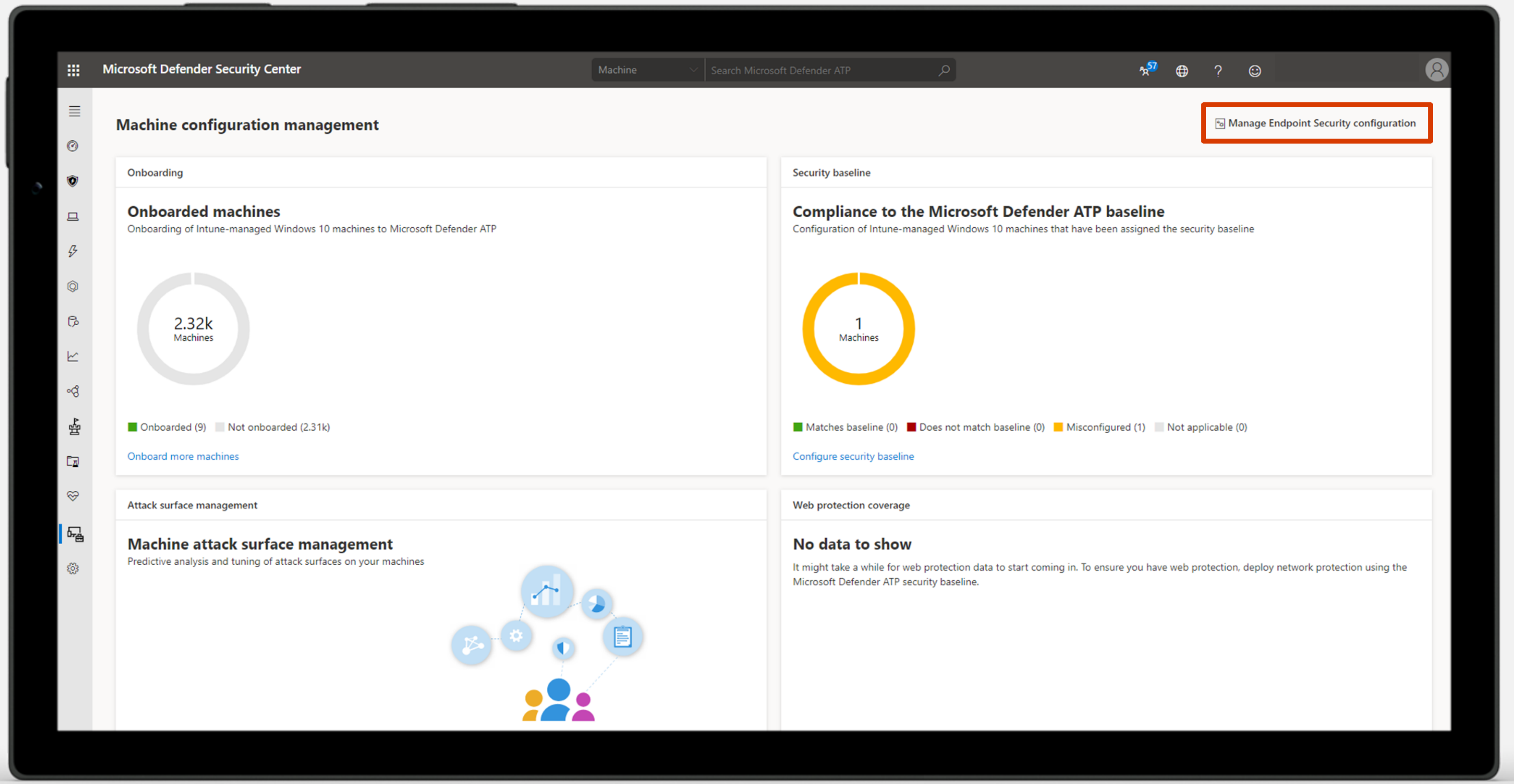
Microsoft Defender for Endpoint

Policy Assessment

Microsoft Endpoint Manager

Policy Enforcement

Easily access management controls from the console


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
57
Manage Endpoint Security configuration
Onboard more machines
Configure security baseline

Machine configuration management

Onboarding

Onboarded machines

Onboarding of Intune-managed Windows 10 machines to Microsoft Defender ATP

2.32k Machines

🟩 Onboarded (9) ⬜ Not onboarded (2.31k)

Security baseline

Compliance to the Microsoft Defender ATP baseline

Configuration of Intune-managed Windows 10 machines that have been assigned the security baseline

1 Machines

🟩 Matches baseline (0) 🟥 Does not match baseline (0) 🟨 Misconfigured (1) ⬜ Not applicable (0)

Attack surface management

Machine attack surface management

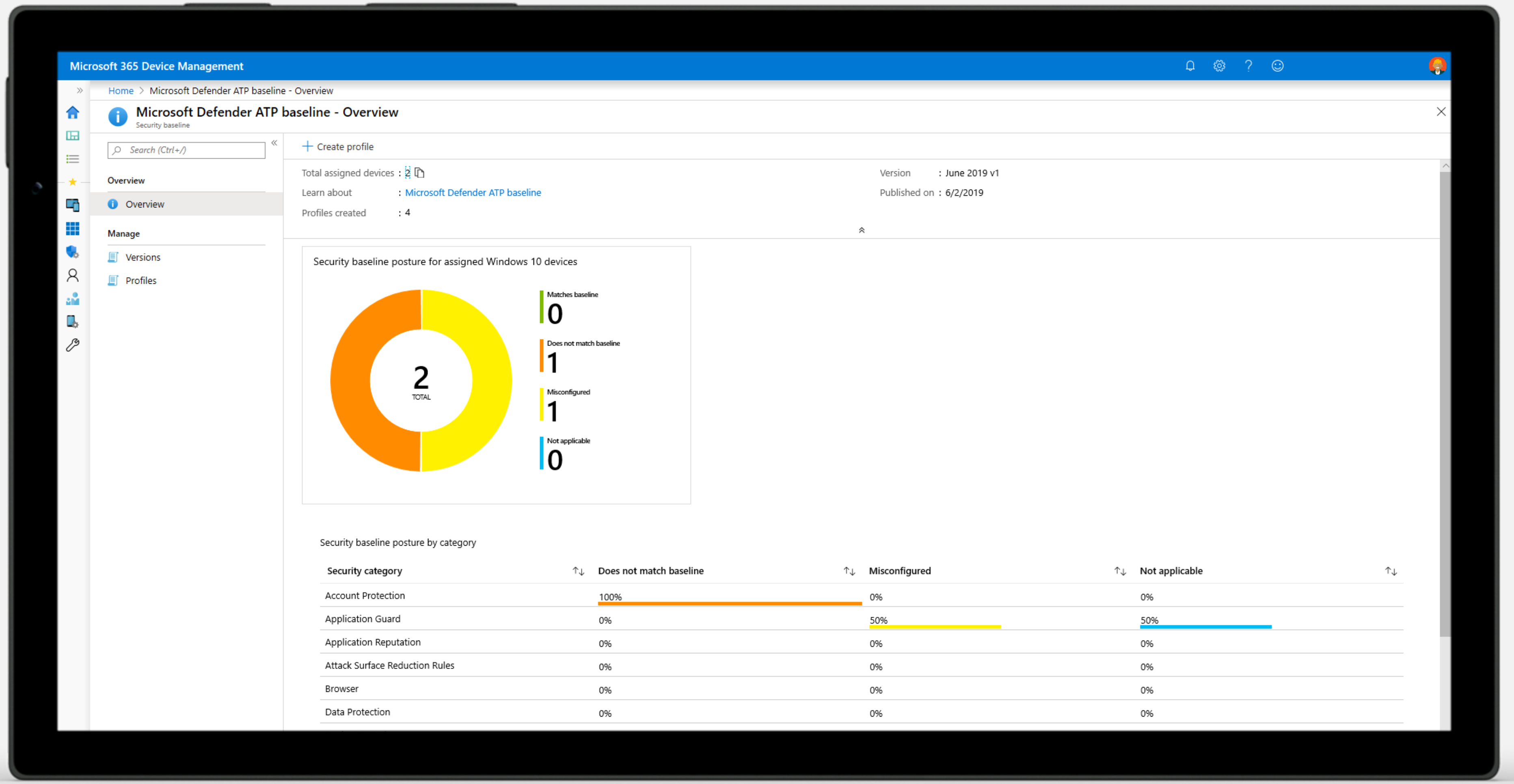
Predictive analysis and tuning of attack surfaces on your machines

Web protection coverage

No data to show

It might take a while for web protection data to start coming in. To ensure you have web protection, deploy network protection using the Microsoft Defender ATP security baseline.

Set security controls and baselines in Microsoft Endpoint Manager



Microsoft 365 Device Management

Home > Microsoft Defender ATP baseline - Overview

Microsoft Defender ATP baseline - Overview

Security baseline

Search (Ctrl+/)

Overview

- Overview

Manage

- Versions
- Profiles

+ Create profile

Total assigned devices : 2

Learn about : Microsoft Defender ATP baseline

Profiles created : 4

Version : June 2019 v1

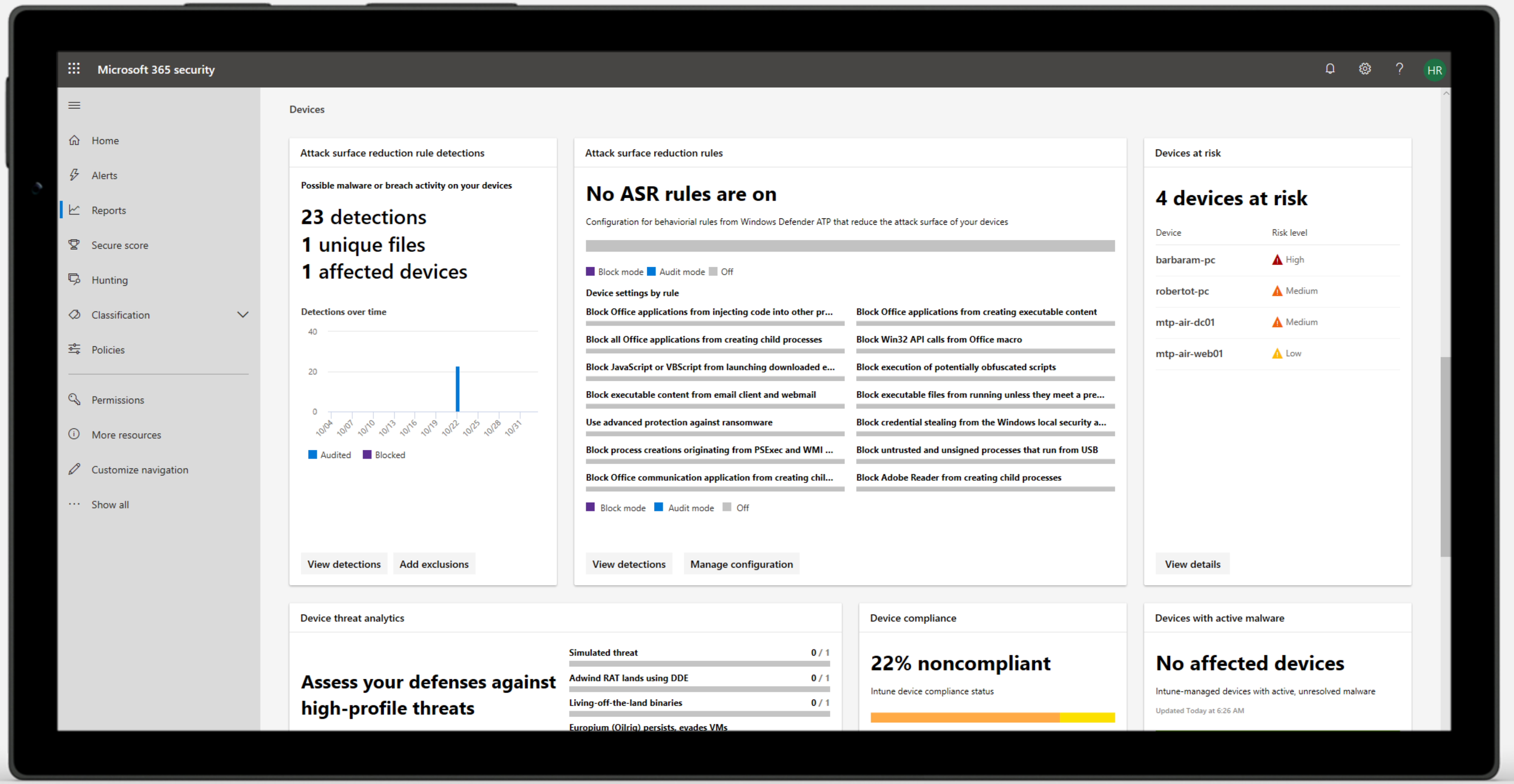
Published on : 6/2/2019

Security baseline posture for assigned Windows 10 devices

Security baseline posture by category

Security category	Does not match baseline	Misconfigured	Not applicable
Account Protection	100%	0%	0%
Application Guard	0%	50%	50%
Application Reputation	0%	0%	0%
Attack Surface Reduction Rules	0%	0%	0%
Browser	0%	0%	0%
Data Protection	0%	0%	0%

Get rich reporting in Microsoft Defender for Endpoint



Microsoft 365 security

HR

- Home
- Alerts
- Reports
- Secure score
- Hunting
- Classification
- Policies
- Permissions
- More resources
- Customize navigation
- Show all

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

View detections | Add exclusions

Attack surface reduction rules

No ASR rules are on

Configuration for behaviorial rules from Windows Defender ATP that reduce the attack surface of your devices

🟪 Block mode 🟦 Audit mode ⬜ Off

Device settings by rule

- 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 Office applications from creating executable content
- 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

🟪 Block mode 🟦 Audit mode ⬜ Off

View detections | Manage configuration

Devices at risk

4 devices at risk

Device	Risk level
barbaram-pc	⚠ High
robertot-pc	⚠ Medium
mtp-air-dc01	⚠ Medium
mtp-air-web01	⚠ Low

View details

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	

Device compliance

22% noncompliant

Intune device compliance status

Devices with active malware

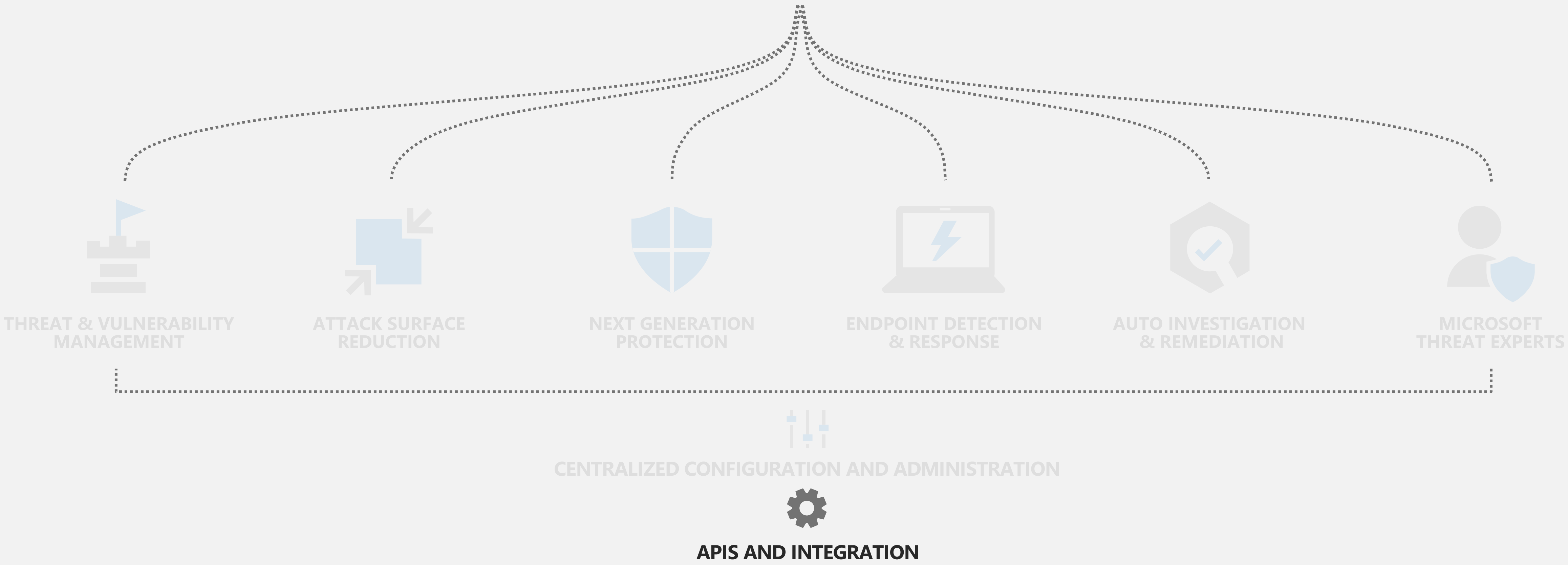
No affected devices

Intune-managed devices with active, unresolved malware

Updated Today at 6:26 AM

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

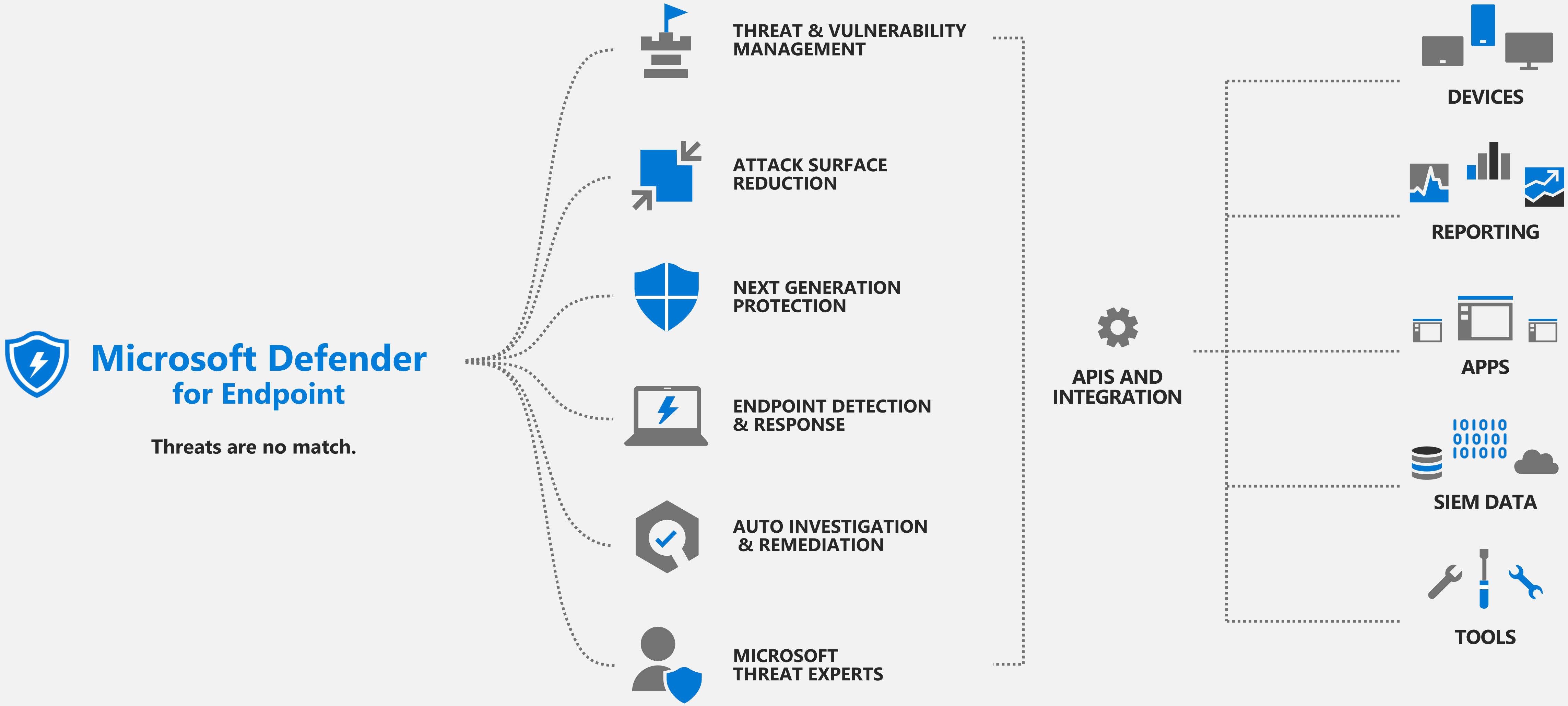
AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

Connecting with the platform



Microsoft Defender for Endpoint

Threats are no match.

THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

APIS AND INTEGRATION

DEVICES

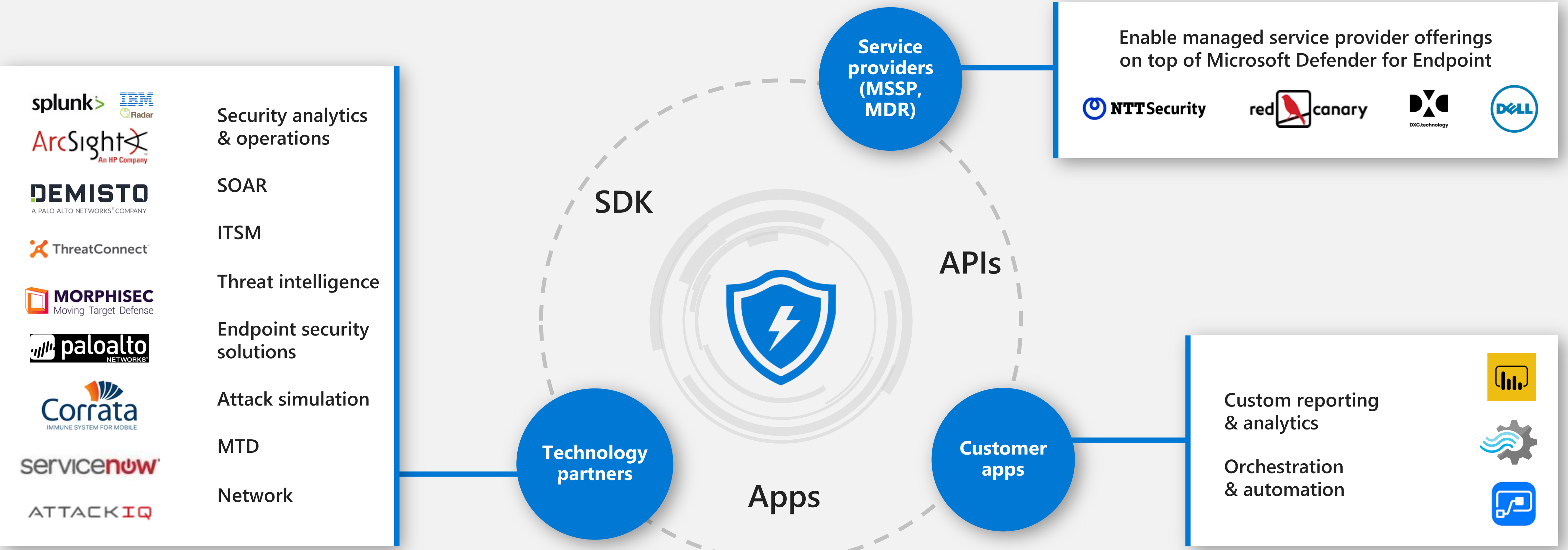
REPORTING

APPS

SIEM DATA

TOOLS

Microsoft Defender for Endpoint through ecosystem & API



Security analytics & operations

SOAR

ITSM

Threat intelligence

Endpoint security solutions

Attack simulation

MTD

Network

Technology partners

Service providers (MSSP, MDR)

Enable managed service provider offerings on top of Microsoft Defender for Endpoint

Customer apps

Custom reporting & analytics

Orchestration & automation

- + 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

Microsoft Defender for Endpoint APIs & partners

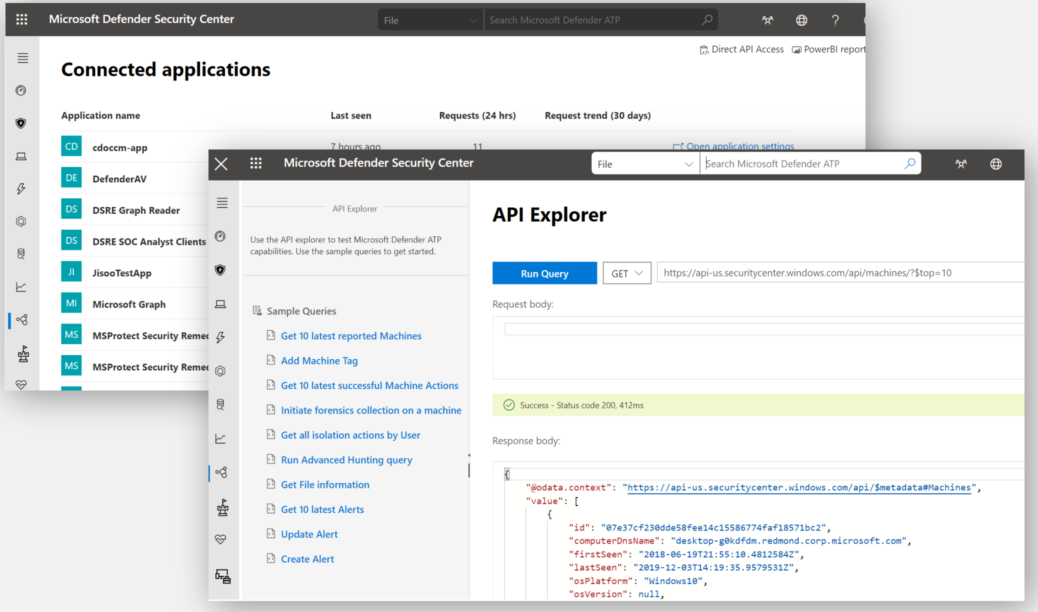
Easy development & tracking of connected solutions

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.


Microsoft Defender Security Center
File
Search Microsoft Defender ATP
Direct API Access
PowerBI report

Connected applications

Application name	Last seen	Requests (24 hrs)	Request trend (30 days)
CD cdoccm-app	7 hours ago	11	Open application settings
DE DefenderAV			
DS DSRE Graph Reader			
DS DSRE SOC Analyst Clients			
JI JisooTestApp			
MI Microsoft Graph			
MS MSProtect Security Reme			
MS MSProtect Security Reme			

Microsoft Defender Security Center
File
Search Microsoft Defender ATP
API Explorer

Use the API explorer to test Microsoft Defender ATP capabilities. Use the sample queries to get started.

Sample Queries

- Get 10 latest reported Machines
- Add Machine Tag
- Get 10 latest successful Machine Actions
- Initiate forensics collection on a machine
- Get all isolation actions by User
- Run Advanced Hunting query
- Get File information
- Get 10 latest Alerts
- Update Alert
- Create Alert

API Explorer

https://api-us.securitycenter.windows.com/api/machines/?$top=10

Request body:

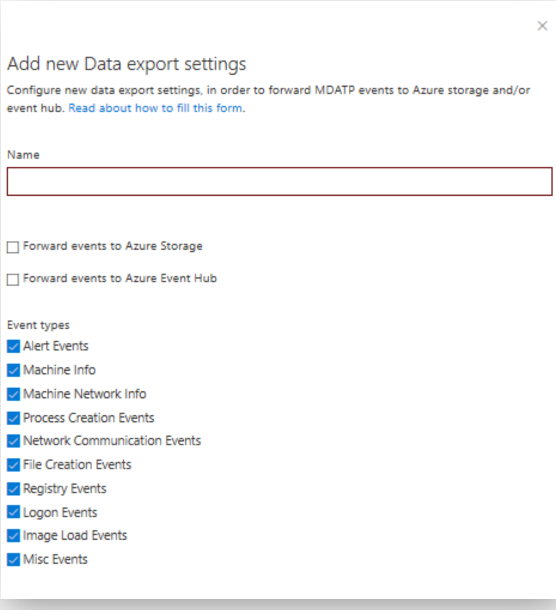
Success - Status code 200, 412ms

Response body:

```
{
  "@odata.context": "https://api-us.securitycenter.windows.com/api/$metadata#Machines",
  "value": [
    {
      "id": "07e37cf230dde58fee14c15586774faf18571bc2",
      "computerDnsName": "desktop-g0kdfdm.redmond.corp.microsoft.com",
      "firstSeen": "2018-06-19T21:55:10.4812584Z",
      "lastSeen": "2019-12-03T14:19:35.9579531Z",
      "osPlatform": "Windows10",
      "osVersion": null,
```

Data Export API

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



Add new Data export settings

Configure new data export settings, in order to forward MDATP events to Azure storage and/or event hub. Read about how to fill this form.

Name

□ Forward events to Azure Storage

□ Forward events to Azure Event Hub

Event types

☑ Alert Events
☑ Machine Info
☑ Machine Network Info
☑ Process Creation Events
☑ Network Communication Events
☑ File Creation Events
☑ Registry Events
☑ Logon Events
☑ Image Load Events
☑ Misc Events

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

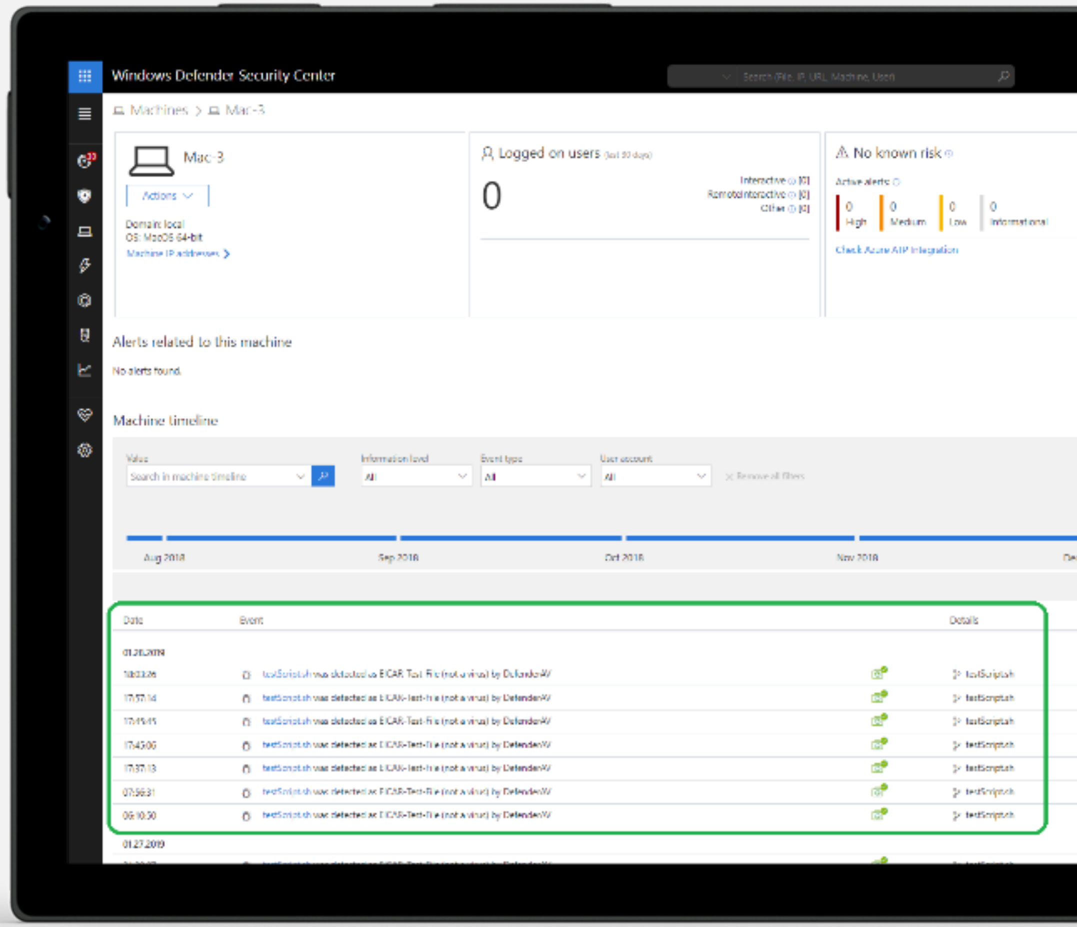
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

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


Windows Defender Security Center
Search (File, IP, URL, Machine, User)
Actions
Aug 2018
Sep 2018
Oct 2018
Nov 2018
Remove all filters

Machines > Mac-3

Mac-3

Domain: local
OS: MacOS 64-bit
Machine IP addresses >

Logged on users (last 30 days)

0

Interactive [0]
RemoteInteractive [0]
Other [0]

No known risk

Active alerts

0	0	0	0
High	Medium	Low	Informational

Check Azure ATP integration

Alerts related to this machine

No alerts found.

Machine timeline

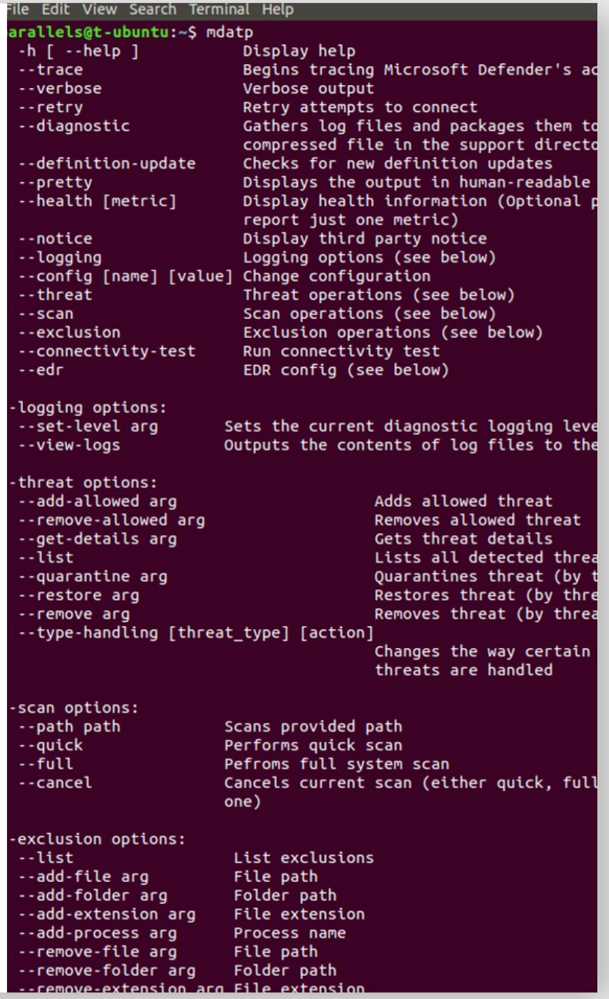
Value: Search in machine timeline
Information level: All
Event type: All
User account: All

Date	Event	Details
01.28.2019		
18:03:26	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:57:14	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:49:45	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:45:06	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:37:13	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
07:56:31	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
06:10:30	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
01.27.2019		

Microsoft Defender for Endpoint (Linux)

On the client:

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



```
arallels@t-ubuntu:~$ mdatp
 -h [ --help ]           Display help
 --trace                 Begins tracing Microsoft Defender's ac
 --verbose               Verbose output
 --retry                 Retry attempts to connect
 --diagnostic            Gathers log files and packages them to
                         compressed file in the support directo
 --definition-update     Checks for new definition updates
 --pretty                Displays the output in human-readable
 --health [metric]       Display health information (Optional p
                         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 leve
 --view-logs           Outputs the contents of log files to the

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

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

-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) current offering

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

Microsoft Defender for Endpoint (iOS) current offering

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

How to get started

POC & REPORTS

Setup

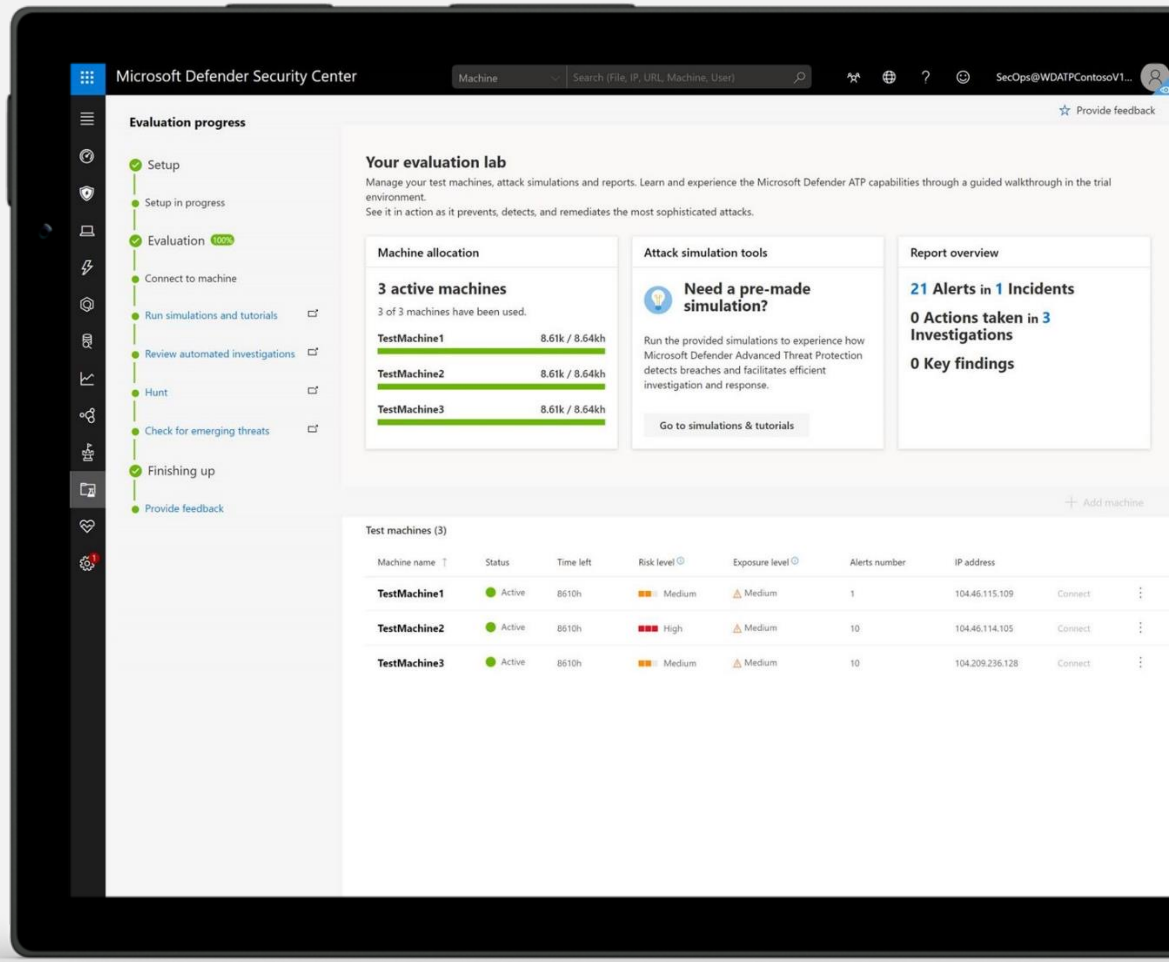
- Latest OS version
- Pre-configured to security baseline
- Onboarded to Microsoft Defender for Endpoint
- Full Audit mode across the stack.
- Pre-populated with evaluation tools
- Multiple interconnected devices (lateral movement)

Simulation

- Microsoft Defender for Endpoint pre-made simulations
- Wizard based experience
- Full flexibility (real-machine RDP accessible)
- Training & education

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



Microsoft Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
☆ Provide feedback

Evaluation progress

- ✓ Setup
- Setup in progress
- ✓ Evaluation 100%
- Connect to machine
- Run simulations and tutorials
- Review automated investigations
- Hunt
- Check for emerging threats
- ✓ Finishing up
- Provide feedback

Your evaluation lab

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.

Machine allocation

3 active machines

3 of 3 machines have been used.

TestMachine1	8.61k / 8.64kh
TestMachine2	8.61k / 8.64kh
TestMachine3	8.61k / 8.64kh

Attack simulation tools

Need a pre-made simulation?

Run the provided simulations to experience how Microsoft Defender Advanced Threat Protection detects breaches and facilitates efficient investigation and response.

Report overview

21 Alerts in 1 Incidents

0 Actions taken in 3 Investigations

0 Key findings

Test machines (3)

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

Thank you.

CROSS
CIPHER