Agenda

08:00 - 08:30 - Registration & Gathering & Welcome Day 2

08:30 - 09:15 - Windows Defender Advanced Threat Protection Overview & Demo

09:15 - 10:00 - Windows Information Protection Overview & Demo

10:00 - 10:15 – Break

10:15 - 11:15 - Microsoft Intune Overview & Demo

11:15 - 12:15 - Intune and Windows Information Protection Hands on Labs

12:15 -13:00 – Lunch

13:00 - 16:00 - Office 365 Security & Compliance Overview and Demo

Windows

Microsoft

Windows Defender Advanced Threat Protection (ATP)

Sophie Chanialaki
Partner Technical Architect @ Microsoft 365 Modern Desktop
Microsoft Central and Eastern Europe

Windows

Windows Defender ATP

Built-in. Cloud-powered.

Trusted by IT. Loved by security teams.

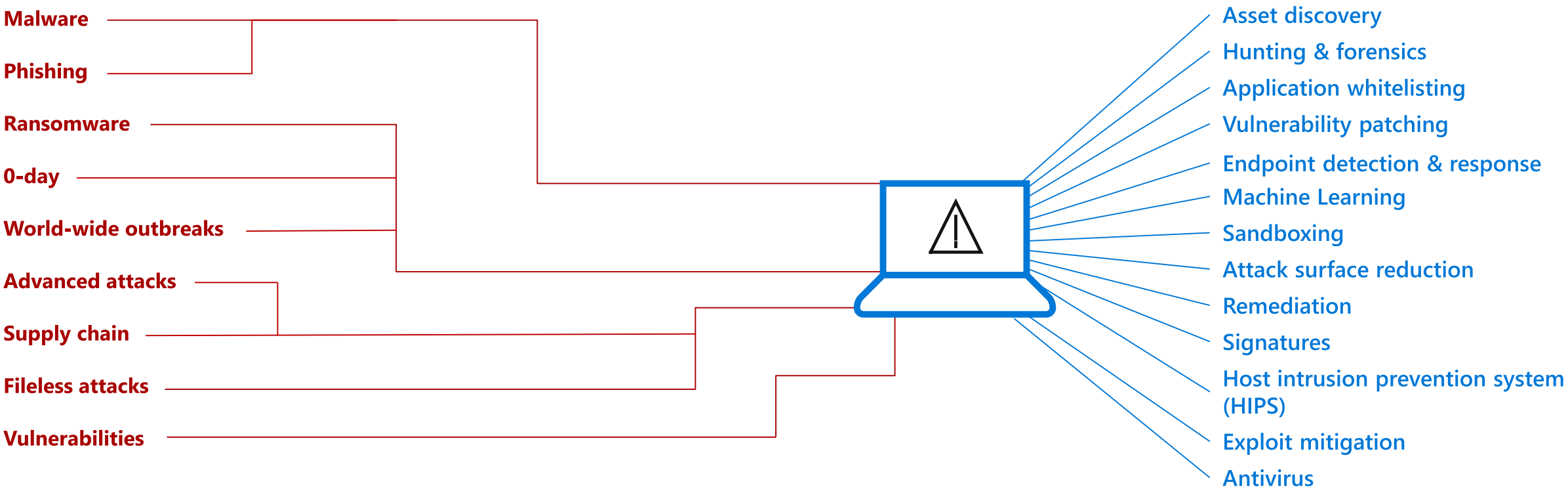
Windows

Protecting an endpoint is hard

PERFORMANCE
Hit on your endpoints

SECURITY TEAM
Time and skills

COST
Multiple solutions and on-prem infrastructure



Windows

Protecting an endpoint ~~is~~ was hard.

Malware

Phishing

Ransomware

0-day

World-wide outbreaks

Advanced attacks

Supply chain

Fileless attacks

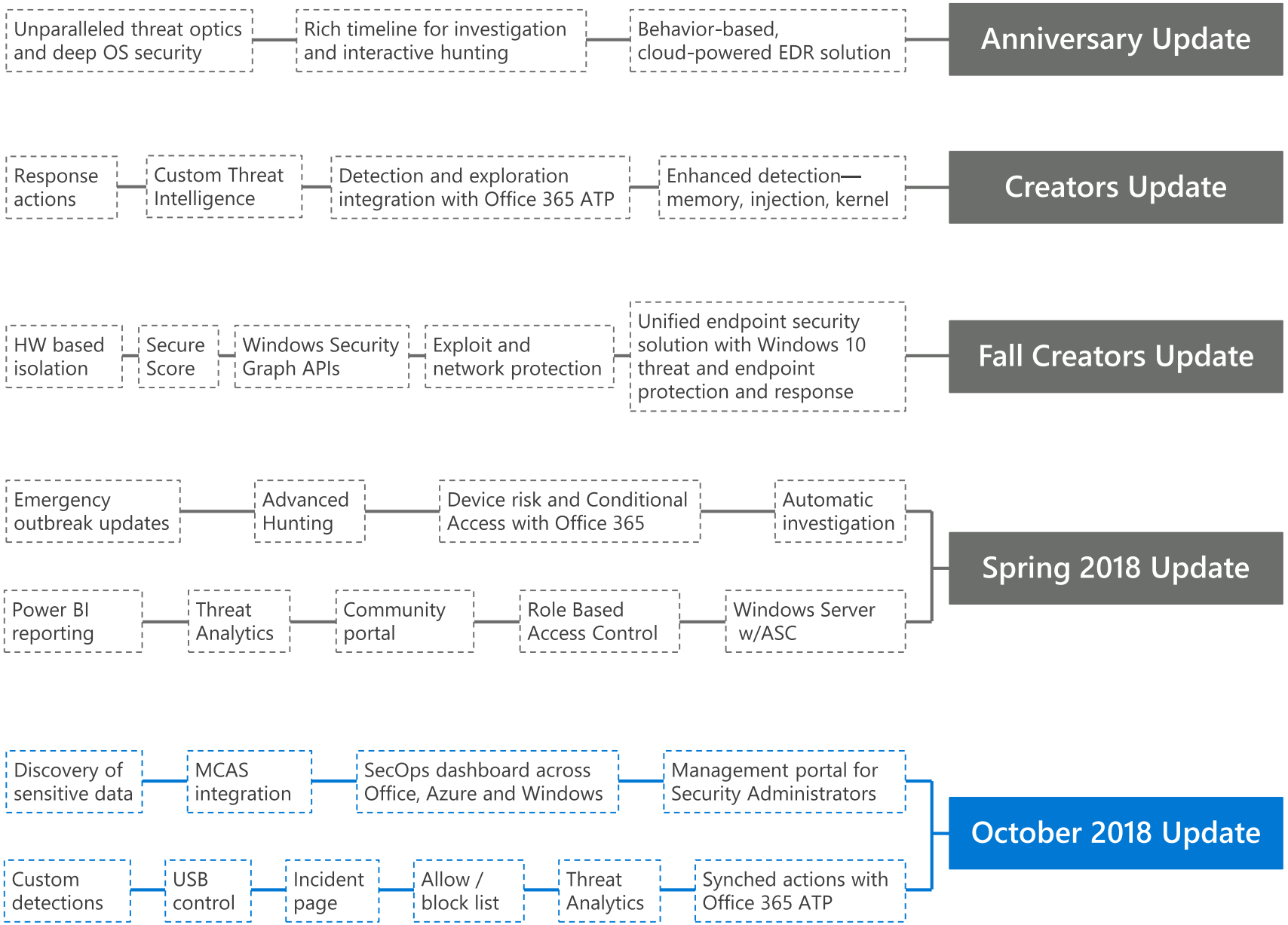
Vulnerabilities

Windows Defender ATP

Built-in. Cloud-powered.

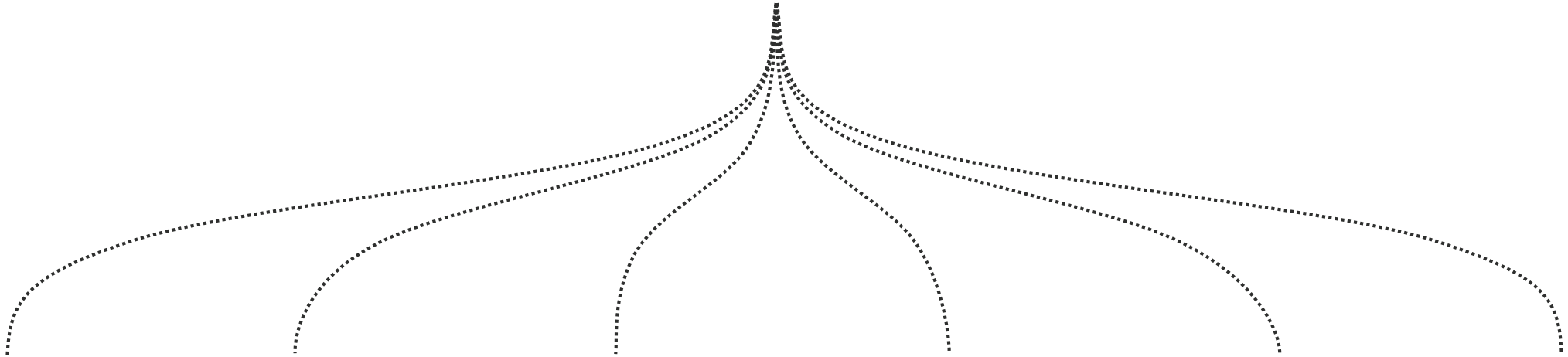
Windows

Windows 10


Unparalleled threat optics and deep OS security
Rich timeline for investigation and interactive hunting
Behavior-based, cloud-powered EDR solution
Anniversary Update
Response actions
Custom Threat Intelligence
Detection and exploration integration with Office 365 ATP
Enhanced detection— memory, injection, kernel
Creators Update
HW based isolation
Secure Score
Windows Security Graph APIs
Exploit and network protection
Unified endpoint security solution with Windows 10 threat and endpoint protection and response
Fall Creators Update
Emergency outbreak updates
Advanced Hunting
Device risk and Conditional Access with Office 365
Automatic investigation
Power BI reporting
Threat Analytics
Community portal
Role Based Access Control
Windows Server w/ASC
Spring 2018 Update
Discovery of sensitive data
MCAS integration
SecOps dashboard across Office, Azure and Windows
Management portal for Security Administrators
Custom detections
USB control
Incident page
Allow / block list
Threat Analytics
Synched actions with Office 365 ATP
October 2018 Update

Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations

NEXT GENERATION PROTECTION

Protect against all types of emerging threats

ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks

AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale

SECURITY POSTURE

Track and improve your organization security posture

ADVANCED HUNTING

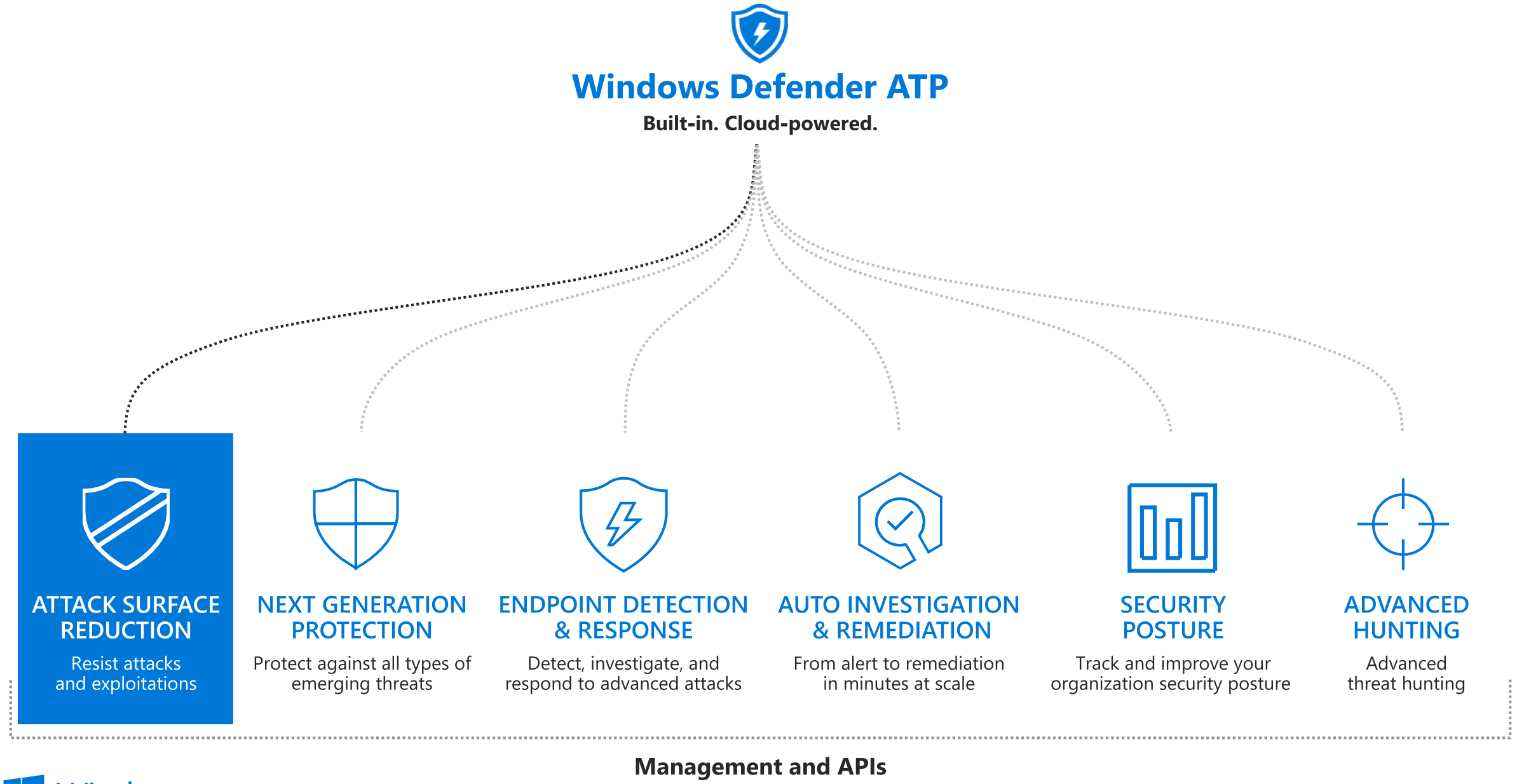
Advanced threat hunting

Management and APIs

Windows

Let’s take a closer look

Windows

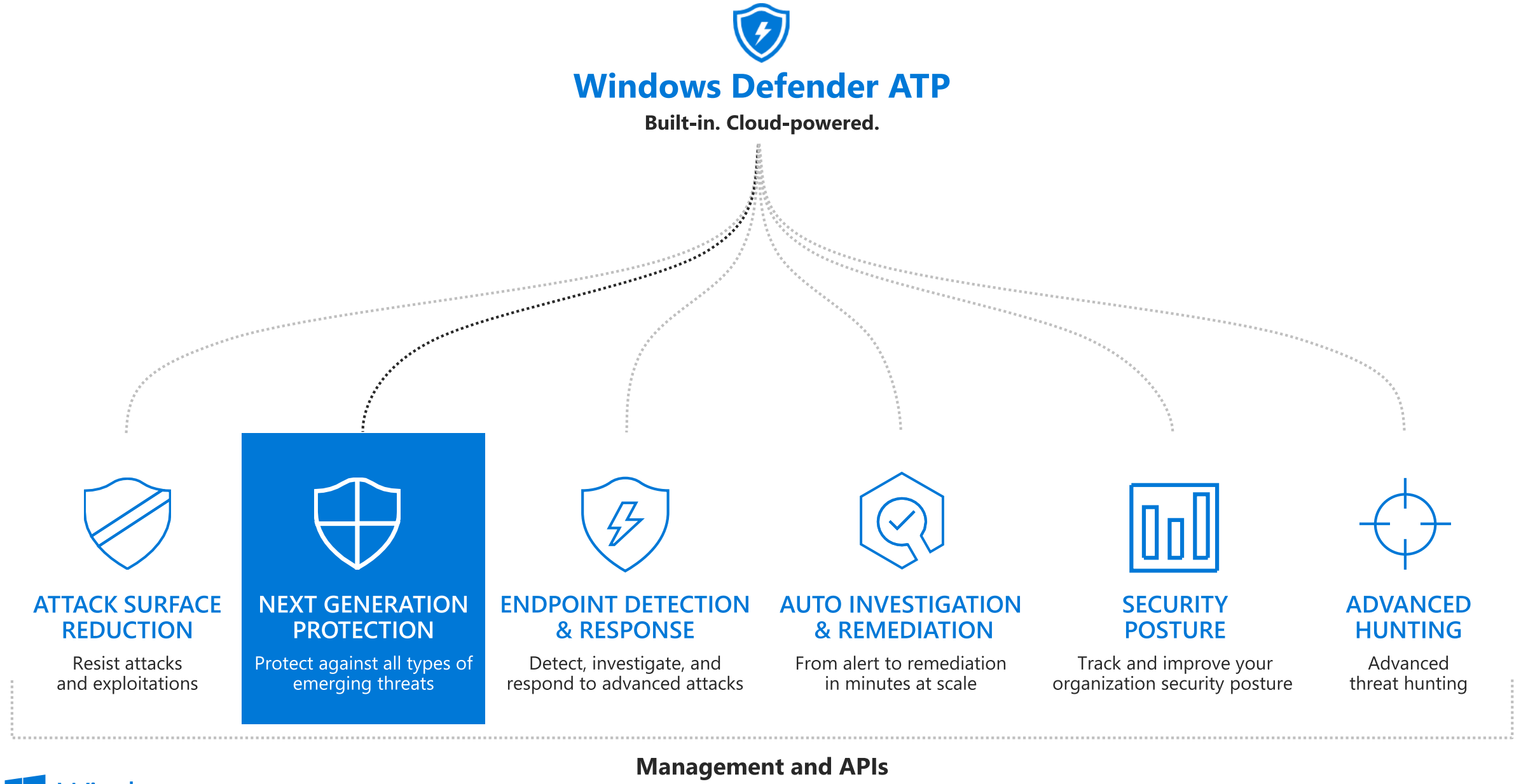

Windows Defender ATP
Built-in. Cloud-powered.
ATTACK SURFACE REDUCTION
Resist attacks and exploitations
NEXT GENERATION PROTECTION
Protect against all types of emerging threats
ENDPOINT DETECTION & RESPONSE
Detect, investigate, and respond to advanced attacks
AUTO INVESTIGATION & REMEDIATION
From alert to remediation in minutes at scale
SECURITY POSTURE
Track and improve your organization security posture
ADVANCED HUNTING
Advanced threat hunting
Management and APIs
Windows

Attack Surface Reduction

Resist attacks and exploitations

HW BASED ISOLATION	**Isolate access to untrusted sites**
	Isolate access to untrusted Office files
APPLICATION CONTROL	**Host intrusion prevention**
	Exploit mitigation
EXPLOIT PROTECTION	**Ransomware protection for your files**
	Block traffic to low reputation destinations
NETWORK PROTECTION	**Protect your legacy applications**
	Only allow trusted applications to run
CONTROLLED FOLDER ACCESS	

Windows


Windows Defender ATP
Built-in. Cloud-powered.
ATTACK SURFACE REDUCTION
Resist attacks and exploitations
NEXT GENERATION PROTECTION
Protect against all types of emerging threats
ENDPOINT DETECTION & RESPONSE
Detect, investigate, and respond to advanced attacks
AUTO INVESTIGATION & REMEDIATION
From alert to remediation in minutes at scale
SECURITY POSTURE
Track and improve your organization security posture
ADVANCED HUNTING
Advanced threat hunting
Management and APIs
Windows

Next generation protection

Protect against all types of emerging threats

Client

Protection in milliseconds
Most common malware are blocked by high-precision detection in Windows Defender AV

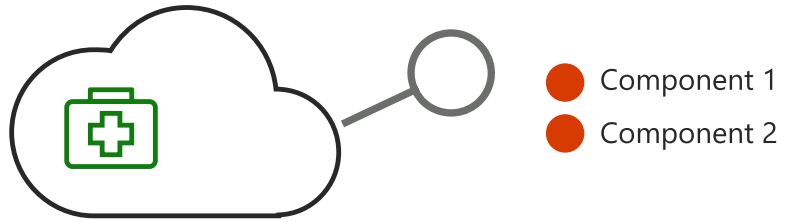
Cloud

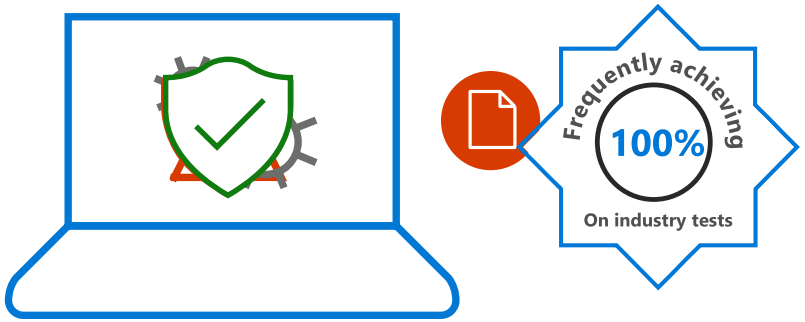
Protection in milliseconds
ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query and make a determination

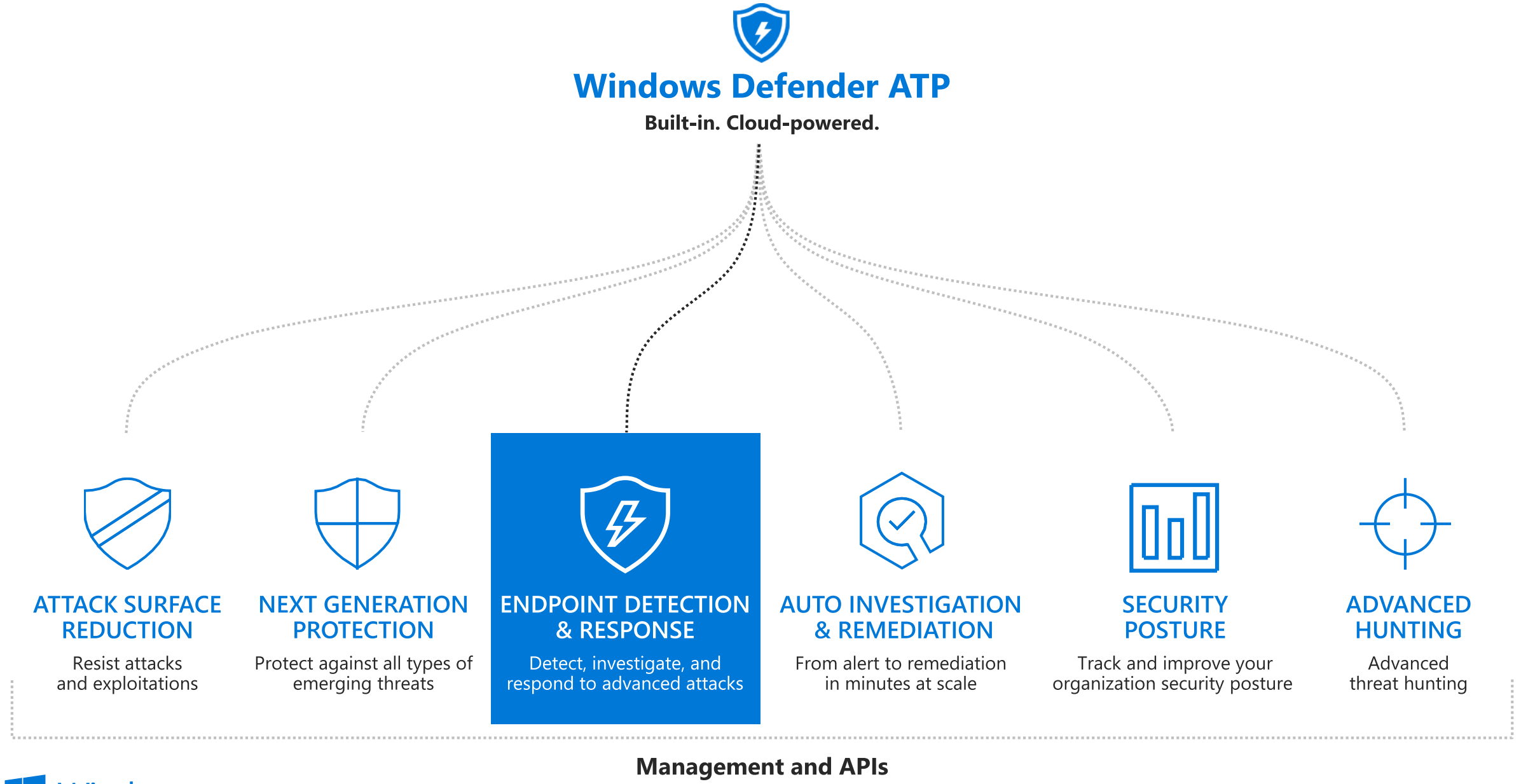
Protection in seconds
If needed a copy of the suspicious file is uploaded for inspection by multi-class ML classifiers

Protection in minutes
If additional checking is required the suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

Protection in hours
The most advanced and innovative samples can be further checked against ML models and expert rules using correlated signals from a vast network of sensors to automatically classify threats






Windows Defender ATP
Built-in. Cloud-powered.
ATTACK SURFACE REDUCTION
Resist attacks and exploitations
NEXT GENERATION PROTECTION
Protect against all types of emerging threats
ENDPOINT DETECTION & RESPONSE
Detect, investigate, and respond to advanced attacks
AUTO INVESTIGATION & REMEDIATION
From alert to remediation in minutes at scale
SECURITY POSTURE
Track and improve your organization security posture
ADVANCED HUNTING
Advanced threat hunting
Management and APIs
Windows

Endpoint detection & response

Detect. Investigate.
Respond to advanced attacks.

Client

Deep OS recording sensor

Cloud

Machine learning, behavioral & anomaly detection

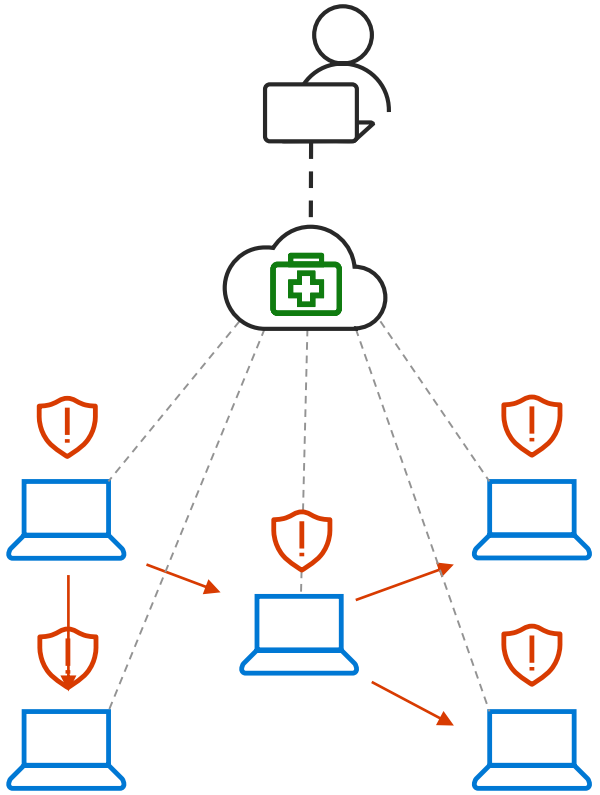
Response and containment

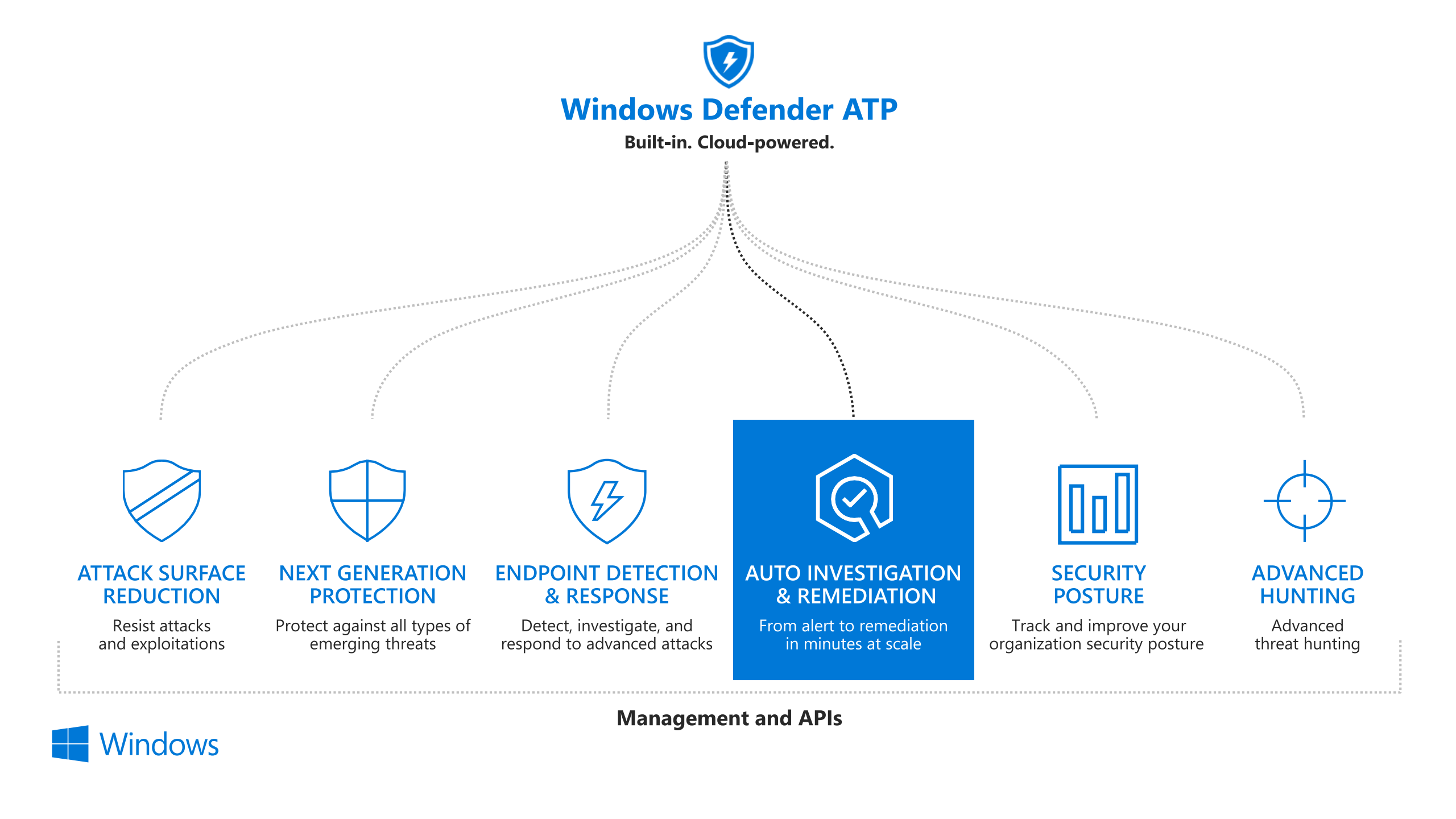
Sandbox analysis

Rich investigation across machines, files, users, IPs, URLs

Realtime and historical threat hunting

Threat intelligence and custom detections




Windows Defender ATP
Built-in. Cloud-powered.
ATTACK SURFACE REDUCTION
Resist attacks and exploitations
NEXT GENERATION PROTECTION
Protect against all types of emerging threats
ENDPOINT DETECTION & RESPONSE
Detect, investigate, and respond to advanced attacks
AUTO INVESTIGATION & REMEDIATION
From alert to remediation in minutes at scale
SECURITY POSTURE
Track and improve your organization security posture
ADVANCED HUNTING
Advanced threat hunting
Management and APIs
Windows

Automated investigation & remediation

From alert to remediation in minutes at scale

Client

Forensic collector

Response orchestrator

Cloud

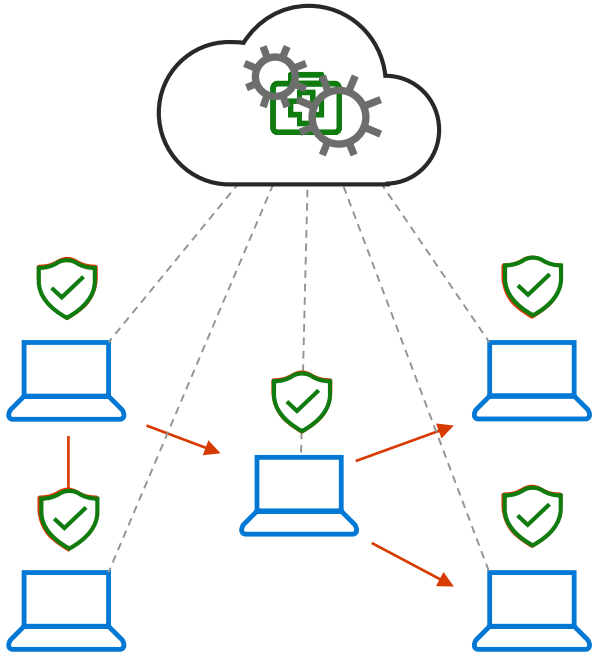
Historical endpoint data

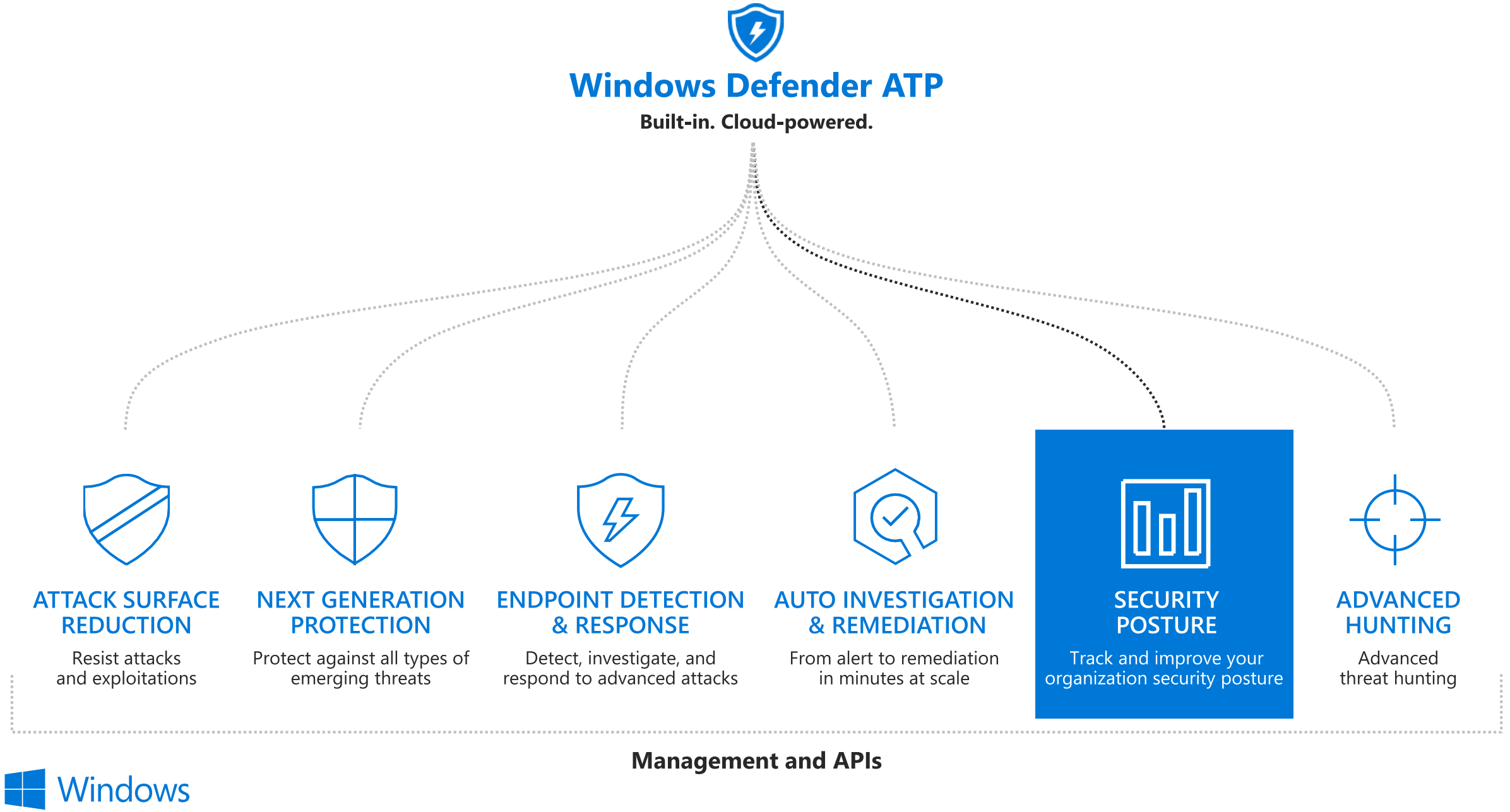
Response orchestration

AI-based response playbooks

File/IP reputation

Sandbox




Windows Defender ATP
Built-in. Cloud-powered.
ATTACK SURFACE REDUCTION
Resist attacks and exploitations
NEXT GENERATION PROTECTION
Protect against all types of emerging threats
ENDPOINT DETECTION & RESPONSE
Detect, investigate, and respond to advanced attacks
AUTO INVESTIGATION & REMEDIATION
From alert to remediation in minutes at scale
SECURITY POSTURE
Track and improve your organization security posture
ADVANCED HUNTING
Advanced threat hunting
Management and APIs
Windows

Security posture

Understand and improve your organization security posture

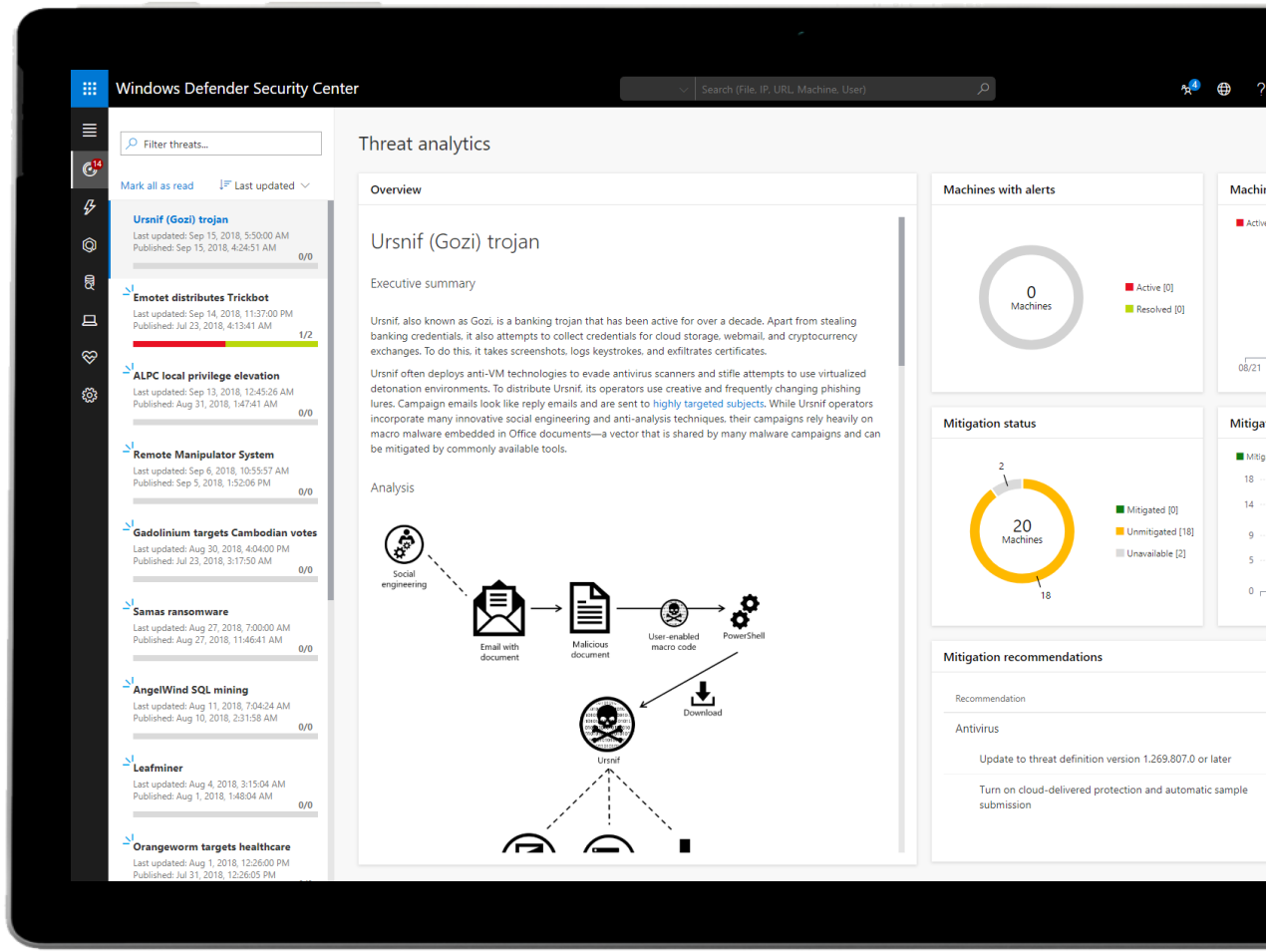
Asset inventory

Identify unprotected systems

Recommended improvement actions

Prioritize your next steps

Threat to posture view



Security management

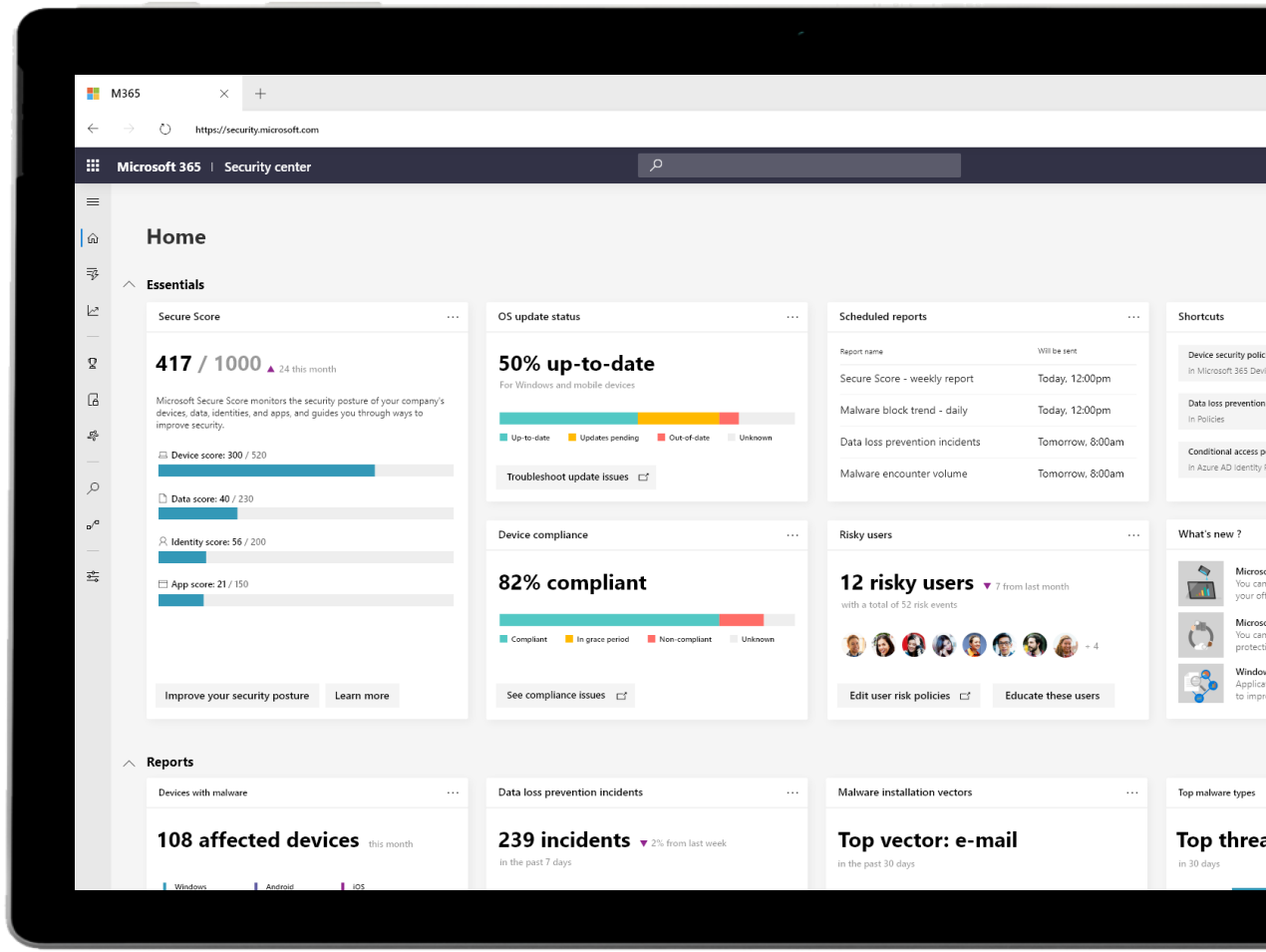
Understand what is happening, has happened and prepare for the future

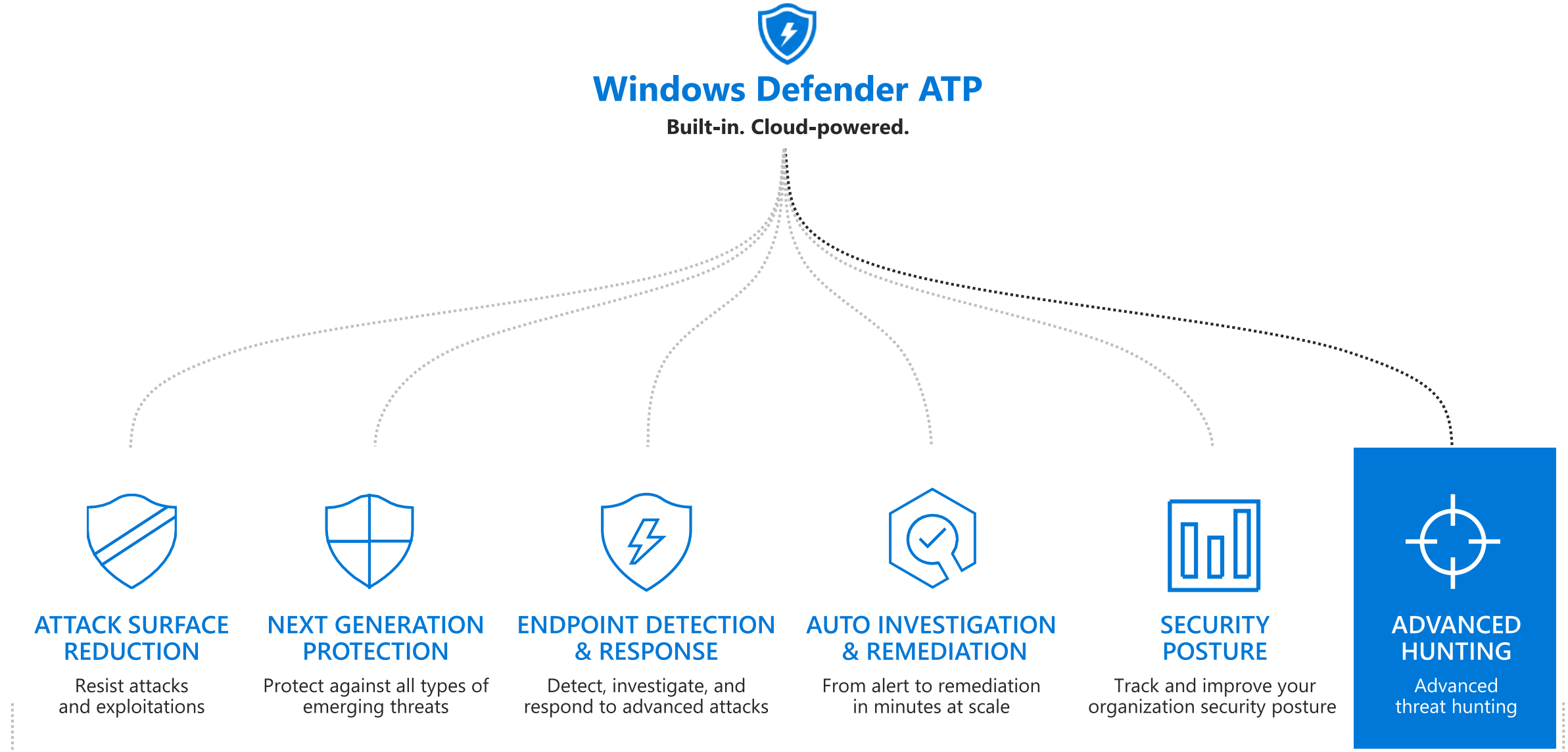
Dashboards and trends

Threat monitoring

Threat reporting

Configuration management



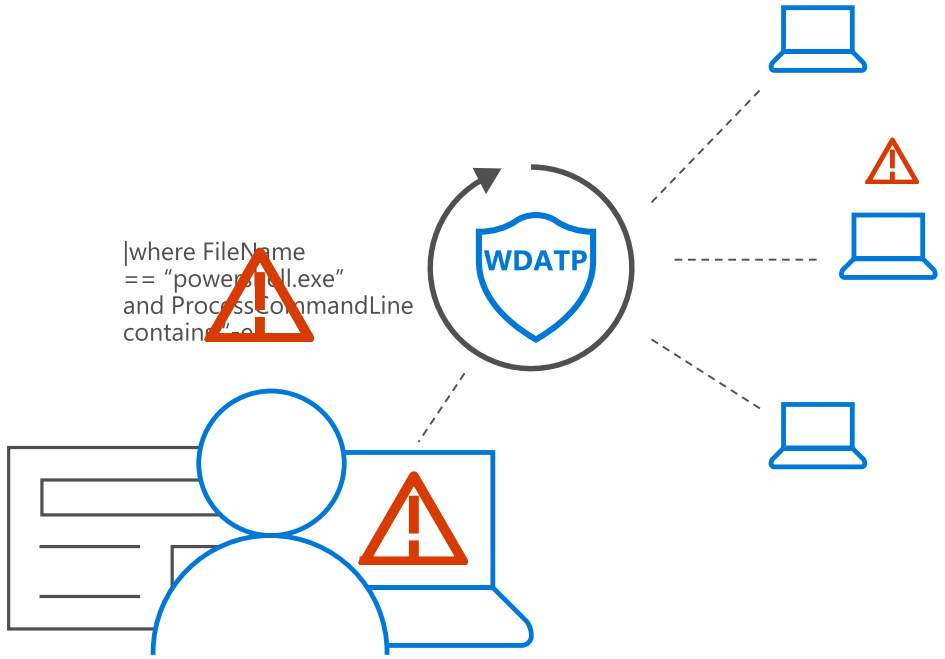

Windows Defender ATP
Built-in. Cloud-powered.
ATTACK SURFACE REDUCTION
Resist attacks and exploitations
NEXT GENERATION PROTECTION
Protect against all types of emerging threats
ENDPOINT DETECTION & RESPONSE
Detect, investigate, and respond to advanced attacks
AUTO INVESTIGATION & REMEDIATION
From alert to remediation in minutes at scale
SECURITY POSTURE
Track and improve your organization security posture
ADVANCED HUNTING
Advanced threat hunting
Management and APIs
Windows

Custom TI detection and advanced hunting

Sec ops reads about a new threat they heard from insider in same vertical

They use advanced hunting to create a query for detection

Windows Defender ATP will continue to run custom detection logic automictically and will alert Sec Ops if a detection is found



Windows Defender ATP

Built-in. Cloud-powered.

ATTACK SURFACE REDUCTION

Resist attacks and exploitations

NEXT GENERATION PROTECTION

Protect against all types of emerging threats

ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks

AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale

SECURITY POSTURE

Track and improve your organization security posture

ADVANCED HUNTING

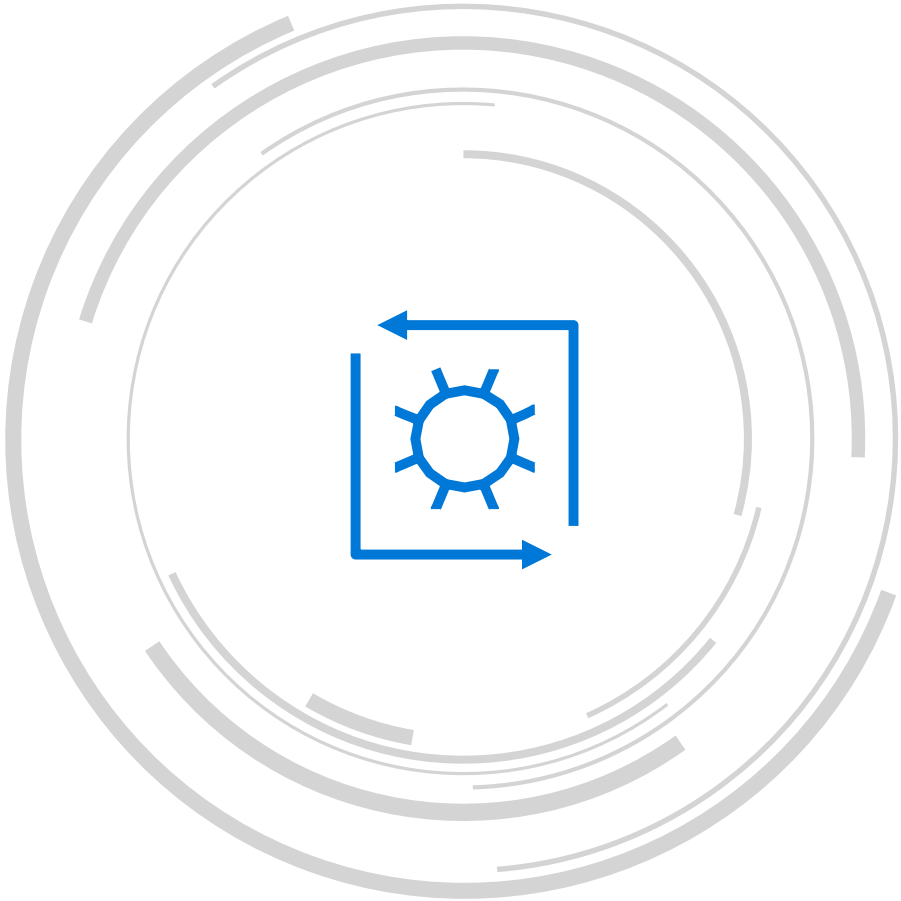
Advanced threat hunting

Management and APIs

Windows

APIs

Customize and enhance your data



AUTOMATE YOUR OWN WORKFLOWS

INTEGRATE YOUR EXISTING SOLUTIONS

QUERY DATA

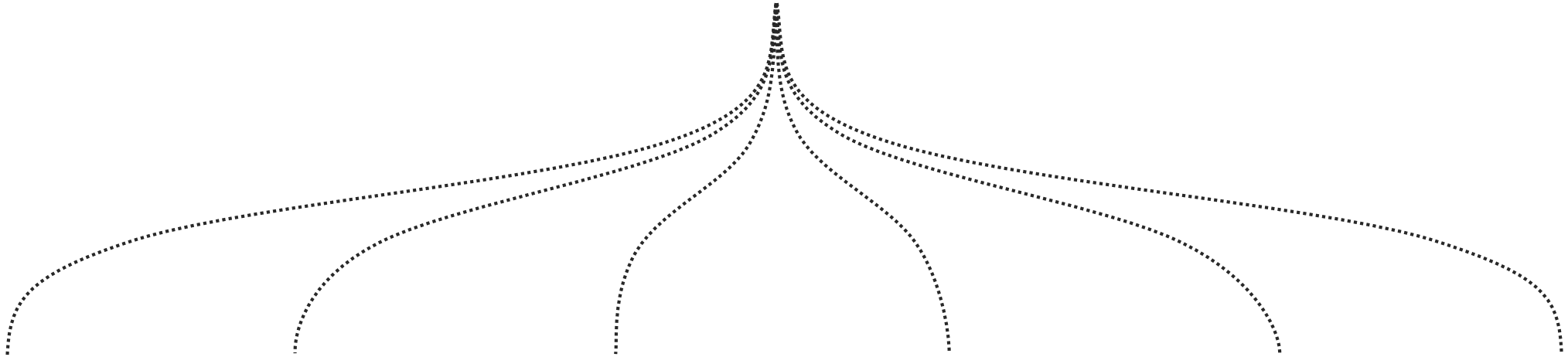
DRIVE REMEDIATION ACTIONS

CREATE CUSTOM DETECTIONS

Windows

Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations

NEXT GENERATION PROTECTION

Protect against all types of emerging threats

ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks

AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale

SECURITY POSTURE

Track and improve your organization security posture

ADVANCED HUNTING

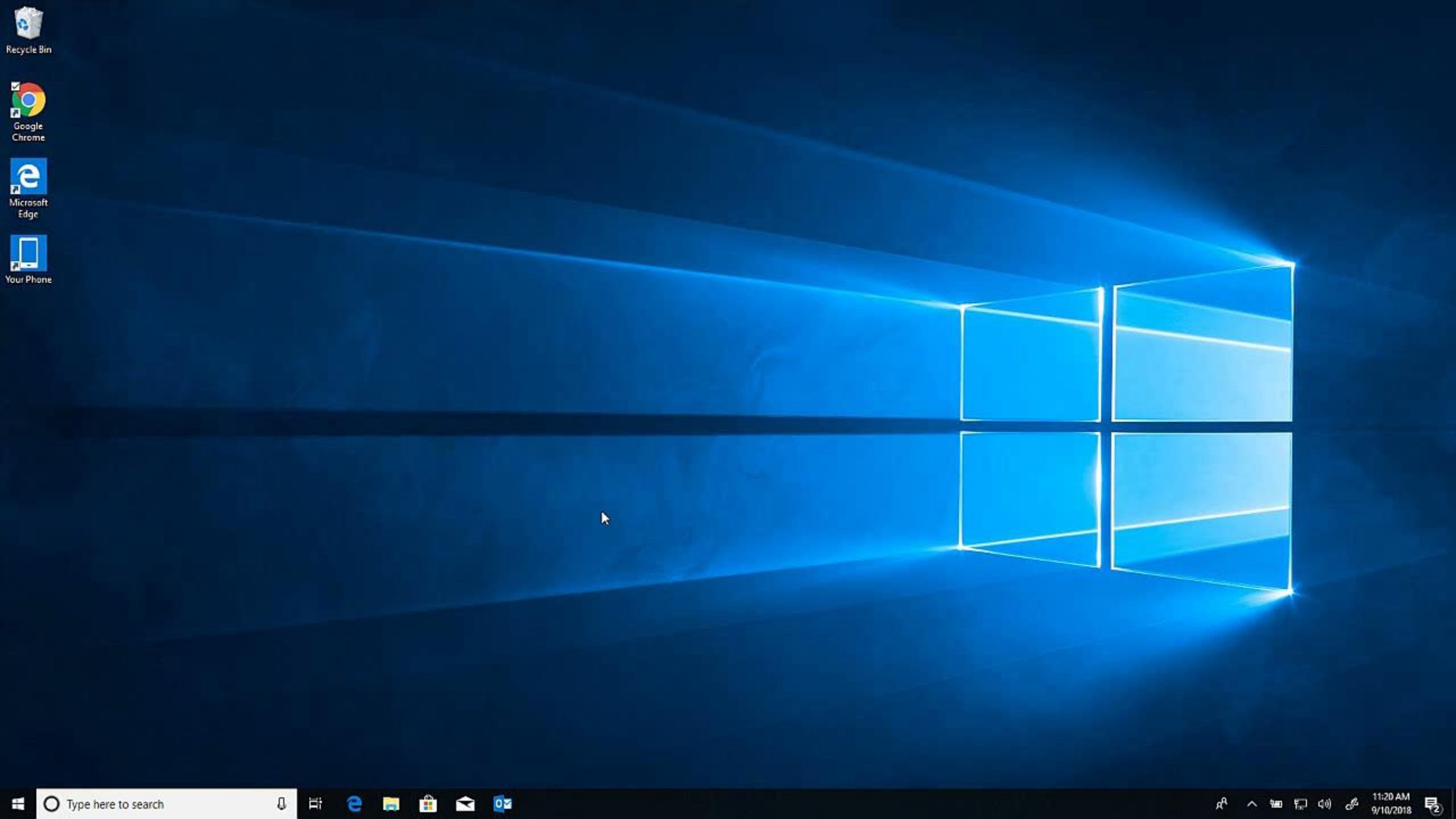
Advanced threat hunting

Management and APIs

Windows

Demos
Windows Defender ATP

Hardware isolation demo


Recycle Bin
Google Chrome
Microsoft Edge
Your Phone
Type here to search
11:20 AM
9/10/2018

Application control demo

Configure app control policies

We can use algorthims to automatically add commonly used files to the whitelist. Choose your desired block level to find the right balance of securing your app control vs empowering end users to use less commonly used or known files enabling end-user choice.

Set default baseline for allowed apps and files

No files allowed | Some files allowed | All files allowed

Known bad files are never included when app control is enabled.

Policy breakdown

Publishers allowed
80/100

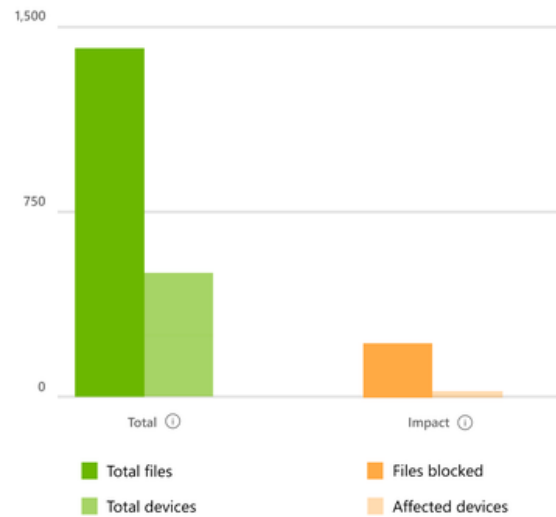
Unsigned files allowed
800/1,000

File paths allowed
8/10

Policy impact simulation

286 files blocked

8 devices affected



Known bad files that will be blocked

24 known bad files blocked

14 devices affected

Export policy | Review policy | Cancel

Configure app control policies

Baseline simulator | Publishers | File hashes | File paths | Review report

This is a three step process. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas risus neque, vehicula vel lacus sit amet, tristique ultricies diam. Mauris luctus elementum neque, ut egestas libero bibendum at.

Allow the following publishers and associated files

112 publishers | Search | Filter

Publisher name	Publisher Hash	File list	Device list	% Devices	Publisher rep
Amazon	5FSSDSWEWDD990	14	14	48	Known good
Google	5FSSDSWEWDD991	32	32	44	Known good
SmartRecruiters	5FSSDSWEWDD992	3	3	32	Unknown
Workday	5FSSDSWEWDD992	8	8	32	Known good
Publisher name	5FSSDSWEWDD992	14	14	31	Unknown
Publisher name	5FSSDSWEWDD992	11	11	28	Known good
Publisher name	5FSSDSWEWDD992	4	4	14	Known good
Publisher name	5FSSDSWEWDD992	48	48	11	Known good
Publisher name	5FSSDSWEWDD992	31	31	9	Known good
Publisher name	5FSSDSWEWDD992	5	5	9	Unknown
Publisher name	5FSSDSWEWDD992	14	14	8	Known good
Publisher name	5FSSDSWEWDD992	14	14	7	Known bad
Publisher name	5FSSDSWEWDD992	14	14	7	Unknown
Publisher name	5FSSDSWEWDD992	14	14	6	Unknown
Publisher name	5FSSDSWEWDD992	14	14	4	Unknown
Publisher name	5FSSDSWEWDD992	14	14	4	Unknown
Publisher name	5FSSDSWEWDD992	14	14	3	Unknown

Export policy | Review policy | Cancel

Impact summary

Policy impact simulation

286 files blocked

8 devices affected

Known bad files that will be blocked

24 known bad files blocked

14 devices affected

Configure app control policies

Baseline simulator | Publishers | File hashes | File paths | Review report

This is a three step process. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas risus neque, vehicula vel lacus sit amet, tristique ultricies diam. Mauris luctus elementum neque, ut egestas libero bibendum at.

Review allow & block policies for all files

12,432 files | Search | Filter

Known good files (986)

File name	Publisher	File path	Device list	% Devices	Allow/Block
Amazon_Client.exe	Amazon	C:\Progam Files\Amazon\	14	48	Allow
Chrome.exe	Chrome	C:\Progam Files\Google\	32	44	Allow
RecruiterPlatform.exe	SmartRecruiter	C:\Progam Files\Recruiter\	3	32	Allow
TimeSheets.exe	Workday	C:\Progam Files\Workday\	8	32	Allow
Filename.exe	N/A	C:\Progam Files\Folder\	14	31	Allow
Filename.exe	Publisher	C:\Progam Files\Folder\	11	28	Allow
Filename.exe	Publisher	C:\Progam Files\Folder\	4	14	Allow
Filename.exe	Publisher	C:\Progam Files\Folder\	48	11	Allow
Filename.exe	Publisher	C:\Progam Files\Folder\	31	9	Allow
Filename.exe	Publisher	C:\Progam Files\Folder\	5	9	Allow
Filename.exe	Publisher	C:\Progam Files\Folder\	14	8	Block
Filename.exe	Publisher	C:\Progam Files\Folder\	14	7	Block
Filename.exe	N/A	C:\Progam Files\Folder\	14	7	Block
Filename.exe	Publisher	C:\Progam Files\Folder\	14	6	Block
Filename.exe	Publisher	C:\Progam Files\Folder\	14	4	Allow

Export policy | Cancel

Current impact

Impacted files and devices

286 files blocked

8 devices affected

Known bad files that will be blocked

24 known bad files blocked

14 devices affected

Exploit protection demo

Home
Alerts
Monitoring & reports
Secure score
Advanced hunting
Classification
Policies
Permissions

Share | Manage schedule

Secure score

Updated 6:20pm today

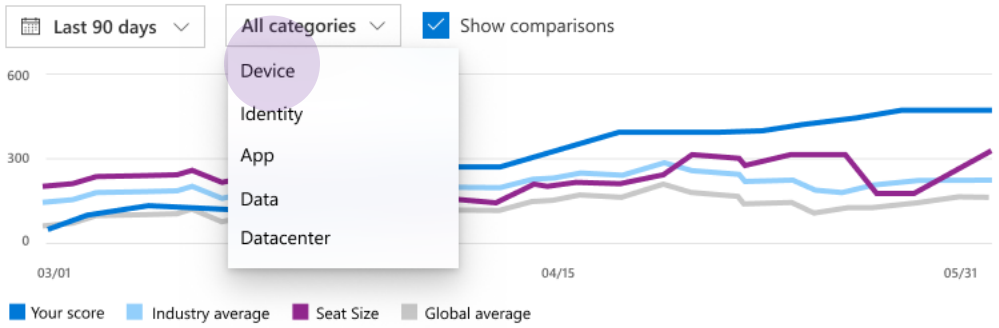
View security state and improvement actions for your company's devices, data, identities, apps, and datacenter. Learn more

Your Microsoft secure score

Total score: 465 / 990

Devices	320/520
Data	60/230
Identity	44/100
Apps	21/140
Infrastructure	20/100

Score over time



View history

Improvement actions

All statuses

To do	29
Completed	14
Third party	8
Ignored	3

Export | Search | Filter | Group by

Improvement actions	Score impact	Category	User impact	Implementation cost	Source	Status	Notes
Block Office apps from launching child processes	+50	Devices	High	Low	Windows Defender ATP	To do	-
Remove just in time access eligible admins that no longer need access	+10	Identity	Low	Low	Azure Active Directory	Complete	-
Remove external accounts with owner from your subscription	+30	Datacenter	Medium	Low	Azure Security Center	To do	
Enable sign in risk policy	+30	Identity	Medium	Medium	Azure Active Directory	To do	-
Discover risky & non-compliant shadow IT applications	+10	Apps	Low	Low	Microsoft Cloud App Security	Ignore	-
Do not allow anonymous calendar sharing	+10	Data	Medium	Low	Office 365	Done	

M365

https://security.microsoft.com

Microsoft 365 Security Center

Share | Manage schedule

Updated 6:20pm today

Secure score

View security state and improvement actions for your company's devices, data, identities, apps, and datacenter. Learn more

- Home
- Alerts
- Monitoring & reports
- Secure score
- Advanced hunting
- Classification
- Policies
- Permissions

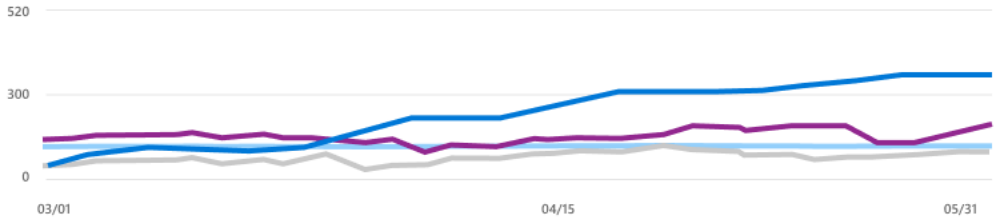
Your Microsoft secure score

Device score: 320 / 520

Devices	320/520
Data	60/230
Identity	44/100
Apps	21/140
Infrastructure	20/100

Score over time

Last 90 days | Device | Show comparisons



View history

Improvement actions

All statuses

To do	11
Completed	6
Third party	2
Ignored	2

Export | Search | Filter | Group by

Improvement actions	Score impact	Category	User impact	Implementation cost	Source	Status	Notes
Block Office apps from launching child processes	+50	Devices	High	Low	Windows Defender ATP	To do	-
Turn on Windows Defender ApplicationGuard	+30	Devices	High	Low	Windows Defender ATP	To do	-
Turn on Credential Guard	+30	Devices	High	Low	Windows Defender ATP	To do	-
Encrypt all supported drives	+20	Devices	Low	Low	Windows Defender ATP	To do	-
Set SmartScreen for Microsoft Edge to warn or block	+20	Devices	Medium	Low	Windows Defender ATP	To do	-
Turn on firewall	+10	Devices	Low	Low	Windows Defender ATP	Done	-

M365

https://security.microsoft.com

Microsoft 365 Security Center

- Home
- Alerts
- Monitoring & reports
- Secure score
- Advanced hunting
- Classification
- Policies
- Permissions

Secure score

View security state and improvement actions for your company's devices, data, identities, apps, and datacenter. Learn more

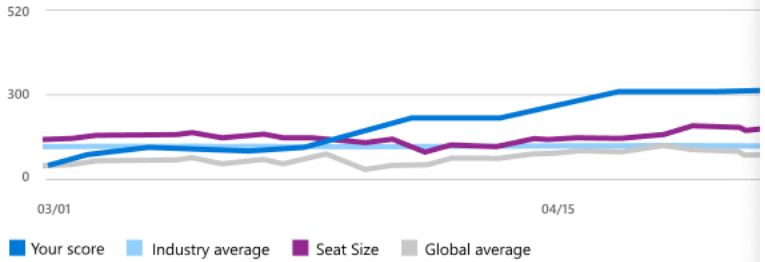
Your Microsoft secure score

Device score: 320 / 520

Devices	**320**/520
Data	60/230
Identity	44/100
Apps	21/140
Infrastructure	20/100

Score over time

Last 90 days | Device | Show comparisons



View history

Improvement actions	Score impact	Category	User impact	Implementation
Block Office apps from launching child processes	+50	Devices	High	Low
Turn on Windows Defender ApplicationGuard	+30	Devices	High	Low
Turn on Credential Guard	+30	Devices	High	Low
Encrypt all supported drives	+20	Devices	Low	Low
Set SmartScreen for Microsoft Edge to warn or block	+20	Devices	Medium	Low
Turn on firewall	+10	Devices	Low	Low

Block Office apps from launching child processes

+50 points

Status To do

Description
Office apps will not be allowed to create child processes. This includes Word, Excel, PowerPoint, OneNote, and Access. This is a typical malware behavior, especially for macro-based attacks that attempt to use Office apps to launch or download malicious executables.

Category	Protects against	User impact	Implementation cost
Devices	Data Exfiltration Data Deletion Elevation of Privilege	High	Low

What am I about to change?
Block Office apps from launching child processes.

How will this affect my users?
Turning on this block will impact users that need to use tools and apps that use this functionality. You may however choose to exclude specific files from the block to mitigate user impact. Click Manage in Intune to configure this in audit mode, so you can view how it will impact your organization, before you configure the block.

Devices affected (All)
Sell all devices

More resources
Attack surface reduction rules

My notes
Enabled in audit mode on 7/31/18
Edit notes

Review audit results | Manage in Intune

Home
Alerts
Monitoring & reports
Secure score
Advanced hunting
Classification
Policies
Permissions

Share | Manage schedule

Secure Score > Attack surface reduction

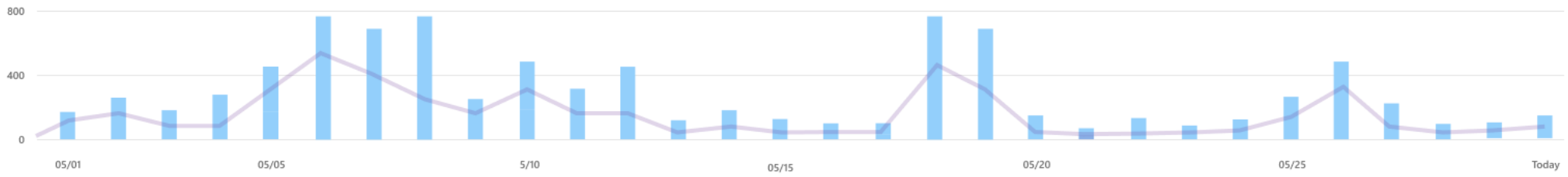
Updated 6:20pm today

View configuration for behavioral rules that reduce the attack surface of your devices, and monitor for detections of those risky behaviors.

Detections | Configuration | Impact simulator

Last 30 days | Block Office apps launchin... | Audit

Updated 6:20pm today



2,145 detections

Export | Search | Filter | Group by

Date/time detected	File name	Publisher	Block/Audit?	Rule	Source app	Device	User	Device owner
05/31/2018, 8:15am	Unknownfile.ext	Microsoft	Audit	Office apps injecting into...	Outlook.exe	CONT_PC_342	Kat Larson	Kat Larson
05/31/2018, 6:45 am	Coolstuff.ext	Open Source Developer	Audit	Office apps/macros creatin...	Word.exe	CONT_PC_742	Danny Smith	Kat Larson
05/31/2018, 12:30 am	Appfile.ext	Google	Audit	Office apps injecting into...	Outlook.exe	CONT_PC_863	Edgar Nelson	Edgar Nelson
05/30/2018, 10:40 pm	FileName.ext	Open Source Developer	Audit	Office apps/macros creatin...	Word.exe	CONT_PC_1112	Penny Arnold	Penny Arnold
05/30/2018, 6:22 pm	Productivity.ext	Microsoft	Audit	Office apps injecting into...	Outlook.exe	CONT_PC_3	Lemon Hall	Kat Larson
05/30/2018, 4:18 pm	BestGame.ext	Open Source Developer	Audit	Office apps injecting into...	Word.exe	CONT_PC_88	Katie Wonder	Katie Wonder
05/30/2018, 2:28 pm	FantasticFile.ext	Open Source Developer	Audit	Office apps/macros creatin...	Outlook.exe	CONT_PC_112	Shia Webber	Shia Webber

Group by:
- File
- Device
- User
- Rule
- No grouping

M365

https://security.microsoft.com

Microsoft 365 Security Center

Home
Alerts
Monitoring & reports
Secure score
Advanced hunting
Classification
Policies
Permissions

Share
Manage schedule

Secure Score > Attack surface reduction

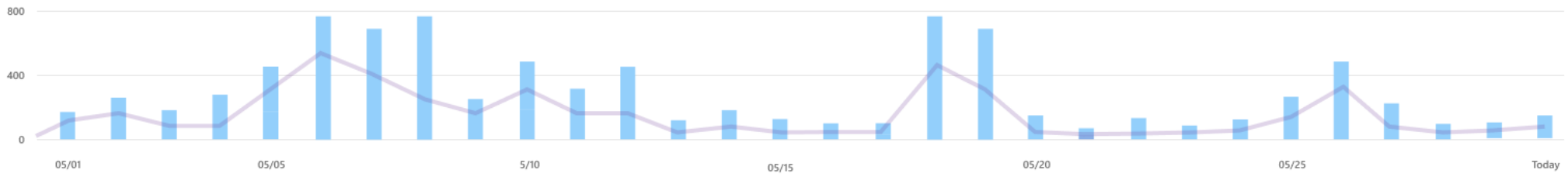
Updated 6:20pm today

View configuration for behavioral rules that reduce the attack surface of your devices, and monitor for detections of those risky behaviors.

Detections Configuration Impact simulator

Last 30 days | Block Office apps launchin... | Audit

Updated 6:20pm today



2,145 detections

Export

Date/time detected	File name	Publisher	Block/Audit?	Rule	Source app	Device
ContosoProcurement.ext (435 devices; 892 detections)						
ContosoInventory.ext (243 devices; 371 detections)						
Productivity.ext (185 devices; 185 detections)						
Appfile.ext (33 devices; 37 detections)						
Coolstuff.ext (33 devices; 34 detections)						
BestGame.ext (32 devices; 32 detections)						
FantasticFile.ext (29 devices; 37 detections)						

M365

https://security.microsoft.com

Microsoft 365 Security Center

- Home
- Alerts
- Monitoring & reports
- Secure score
- Advanced hunting
- Classification
- Policies
- Permissions

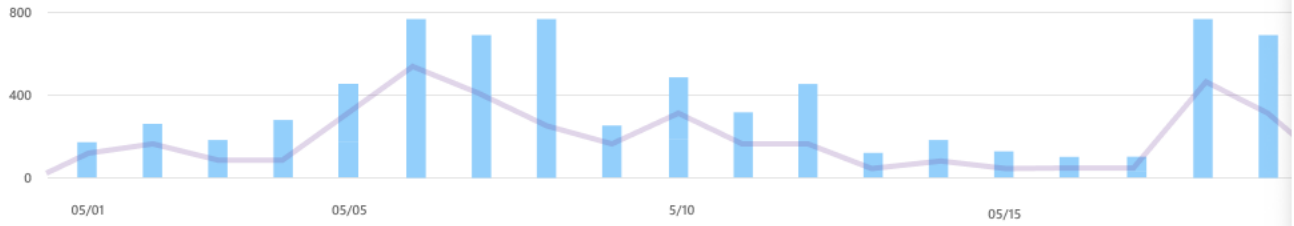
Secure Score > **Attack surface reduction**

View configuration for behavioral rules that reduce the attack surface of your devices, and monitor for detections of those risky behaviors.

Detections | Configuration | Impact simulator

Last 30 days | Block Office apps launchin... | Audit

Updated 6:20pm today



2,145 detections

Date/time detected	File name	Publisher	Block/Audit?	Rule	Source app
ContosoProcurement.ext (435 devices; 892 detections)					
ContosoInventory.ext (243 devices; 371 detections)					
Productivity.ext (185 devices; 185 detections)					
Appfile.ext (33 devices; 37 detections)					
Coolstuff.ext (33 devices; 34 detections)					
BestGame.ext (32 devices; 32 detections)					
FantasticFile.ext (29 devices; 37 detections)					

ASR detection: ContosoProcurement.ext

File info

File name
ContosoProcurement.ext

File hash
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
View in VirusTotal

Publisher
Open Source Developer

Exclusion path
%/long/path/name/ContosoProcurement.ext
Manage exclusions

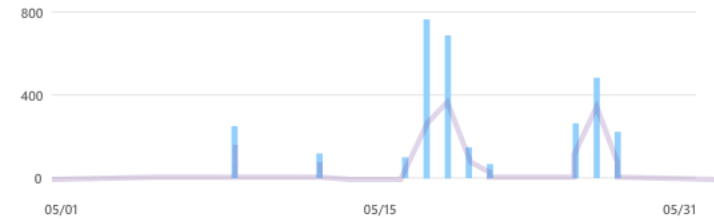
Detections

Last 30 days | Block Office apps launchin... | Audit

892 total detections

435 affected devices

Updated 6:20pm today



See all detections

See all affected devices

Simulate exclusion

M365

https://security.microsoft.com

Microsoft 365 Security Center

Share | Manage schedule

Updated 6:20pm today

- Home
- Alerts
- Monitoring & reports
- Secure score
- Advanced hunting
- Classification
- Policies
- Permissions

Secure Score > Attack surface reduction

View configuration for behavioral rules that reduce the attack surface of your devices, and monitor for detections of those risky behaviors. Manage Attack surface reduction in Intune.

Detections | Configuration | **Impact simulator**

Simulate impact for Detections in 30 days | Block Office apps launchin... | Include audit detections

Reduce impact by adding the following exclusions:

Find a file by name or publisher

2 selected files

ContosoProcuremen... (435 devices; 892 detections)

Export file list

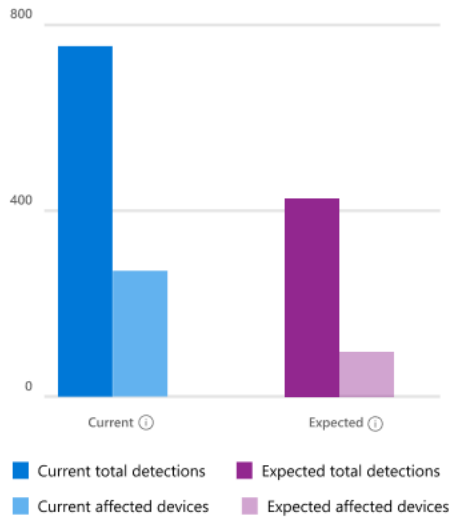
Commonly detected files

- **ContosoInventory.ext** (243 devices; 371 detections)
- **Appfile.ext** (33 devices; 37 detections)
- **Coolstuff.ext** (33 devices; 36 detections)
- **BestGame.ext** (33 devices; 34 detections)
- **FantasticFile.ext** (32 devices; 34 detections)
- **SecretStuff.ext** (29 devices; 39 detections)

Result

▼ **380** less detections

▼ **129** less affected devices



Device list

Export devices with no impact from simulation
These devices don't require the added exclusions

Export devices impacted by simulation
These devices may need the added exclusions

Enable simulated settings

1) Export file list and both device lists

2) Go to the M365 Device Management portal

3) Create a device group for devices impacted by simulation

4) Enable desired Attack surface reduction rules in Block mode for these devices, with the exported file list set as exclusions.

5) For devices with no impact that still have the desired rules in audit mode, create a new device group if needed, and switch to Block mode with no additional exclusions.

* Note, some rules will not honor any exclusions.

Learn more

Open ServiceNow Ticket

Manage in Intune

Home
Alerts
Monitoring & reports
Secure score
Advanced hunting
Classification
Policies
Permissions

Share | Manage schedule

Updated 6:20pm today

Secure Score > Attack surface reduction

View configuration for behavioral rules that reduce the attack surface of your devices, and monitor for detections of those risky behaviors. Manage Attack surface reduction in Intune.

Detections | Configuration | **Impact simulator**

Simulate impact for Detections in 30 days | Block Office apps launchin... | Include audit detections

Reduce impact by adding the following exclusions:

Find a file by name or publisher

2 selected files

- **ContosoProcuremen...** (435 devices; 892 detections)
- **ContosoInventory.ext** (243 devices; 371 detections)

Export file list

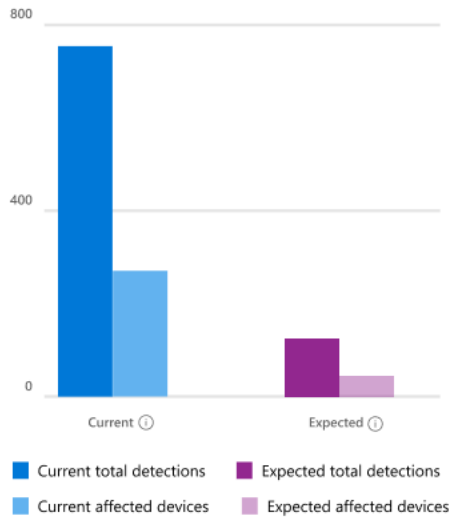
Commonly detected files

- **Appfile.ext** (33 devices; 37 detections)
- **Coolstuff.ext** (33 devices; 36 detections)
- **BestGame.ext** (33 devices; 34 detections)
- **FantasticFile.ext** (32 devices; 34 detections)
- **SecretStuff.ext** (29 devices; 39 detections)

Result

▼ **652** less detections

▼ **247** less affected devices



Device list

Export devices with no impact from simulation
These devices don't require the added exclusions

Export devices impacted by simulation
These devices may need the added exclusions

Enable simulated settings

1) Export file list and both device lists

2) Go to the M365 Device Management portal

3) Create a device group for devices impacted by simulation

4) Enable desired Attack surface reduction rules in Block mode for these devices, with the exported file list set as exclusions.

5) For devices with no impact that still have the desired rules in audit mode, create a new device group if needed, and switch to Block mode with no additional exclusions.

* Note, some rules will not honor any exclusions.

Learn more

Open ServiceNow Ticket

Manage in Intune

M365

https://security.microsoft.com

Microsoft 365 Security Center

Edit sections | Add cards

Prevention

Microsoft Secure Score

Secure score: 515 / 990 ▲ +50 points

Microsoft Secure Score monitors the security state of your company's devices, data, identities, apps, and Azure resources.

Devices	▲ 370/520
Data	60/230
Identity	44/100
Apps	21/140
Infrastructure	20/100

Improve your security state | View history

Device compliance

68% devices compliant

Of your 190k enrolled devices, 68% are compliant with the device compliance policies you created.

Updated 6:20pm today

Compliant | Not compliant | In grace period | Not evaluated

View details in Device Management Admin Console

Device malware state

85 unresolved malware

Of detections by Windows Defender Antivirus in the last 24 hours:

Updated 6:20pm today

Active | Action failed | Allowed | Resolved

View details

Email protection overview

Malicious email content blocked by Office Advanced Threat Protection in the past 30 days.

Updated 6:20pm today

8067 Phishing blocked

1272 Malware blocked

View details in Office 365 Security & Compliance Center

Identity protection overview

For accounts protected by Azure AD Identity Protection:

Updated 6:20pm today

55 Users flagged for risk

88 Risky sign-in events in 30 days

8 Global admins

View details in Azure AD Identity Protection

Top discovered app categories

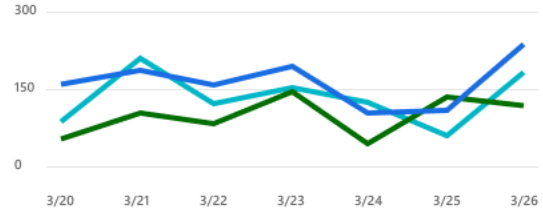
Cloud storage	200GB
Collaboration	191GB
CRM	185GB
Webmail	170GB

Sanctioned | Unsanctioned | Other

View all in Cloud App Security

DLP policy matches

Updated 6:20am today



Policy 1 | Policy 2 | Policy 3

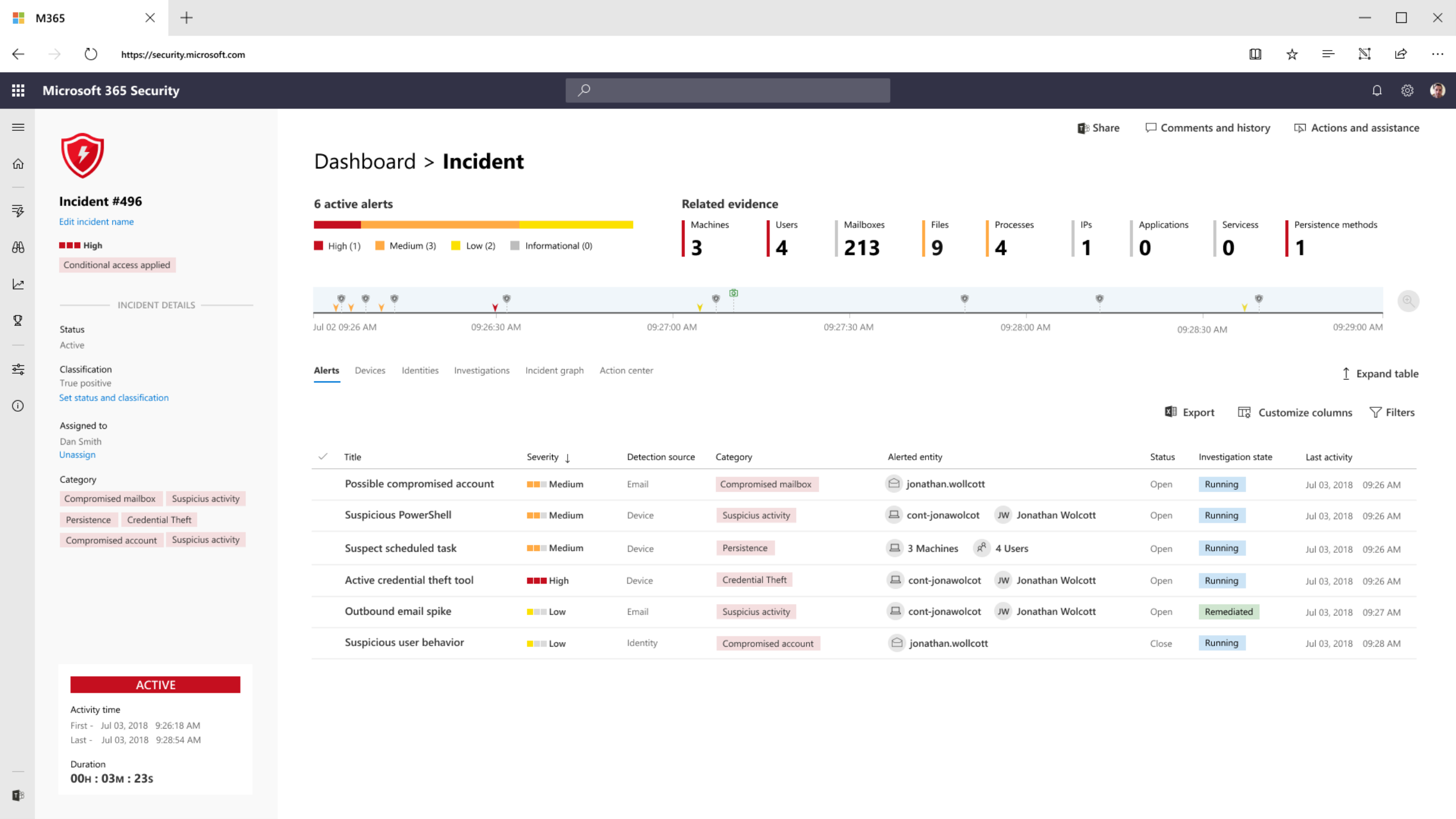
Infrastructure protection overview

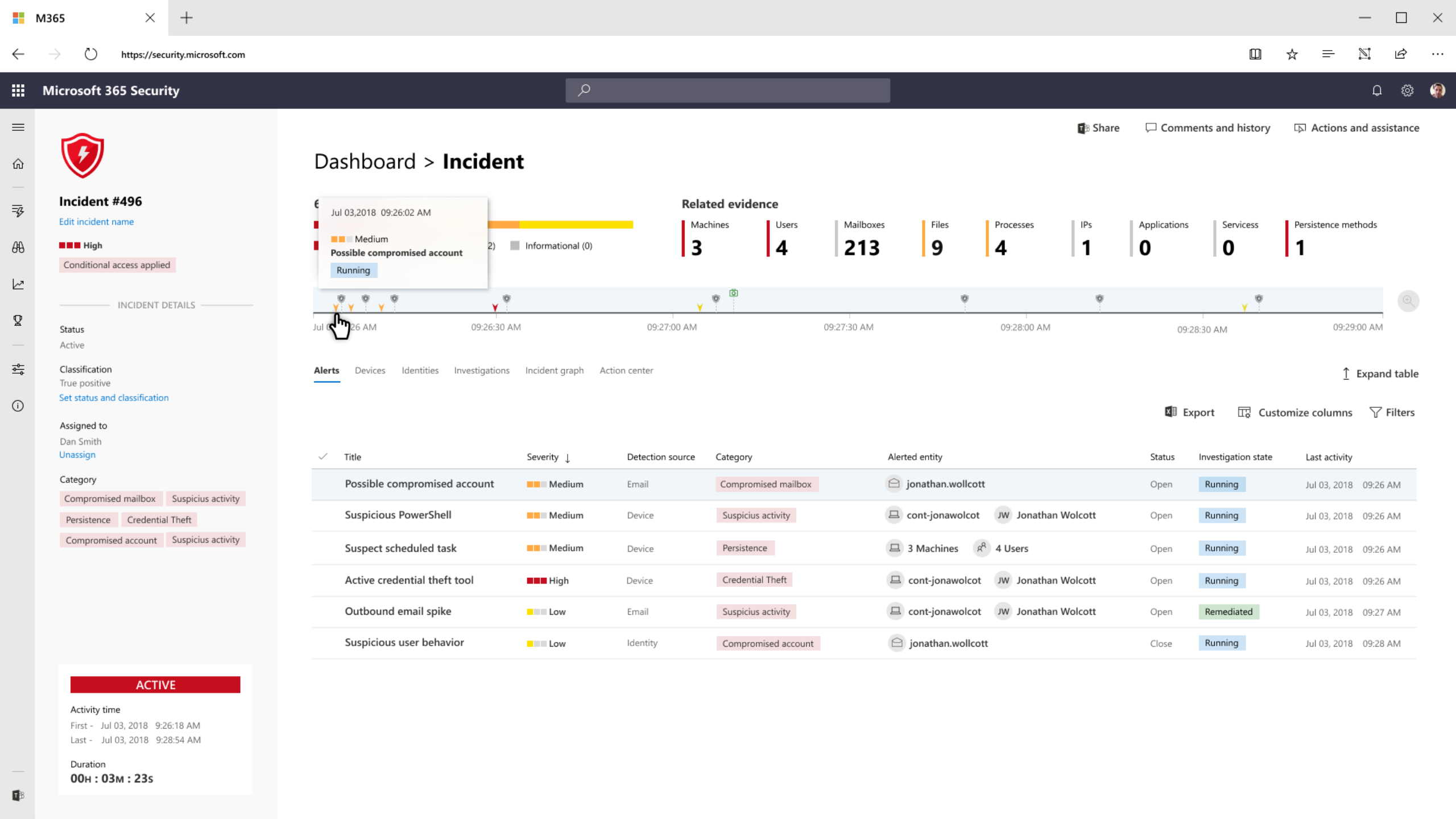
185 protected resources

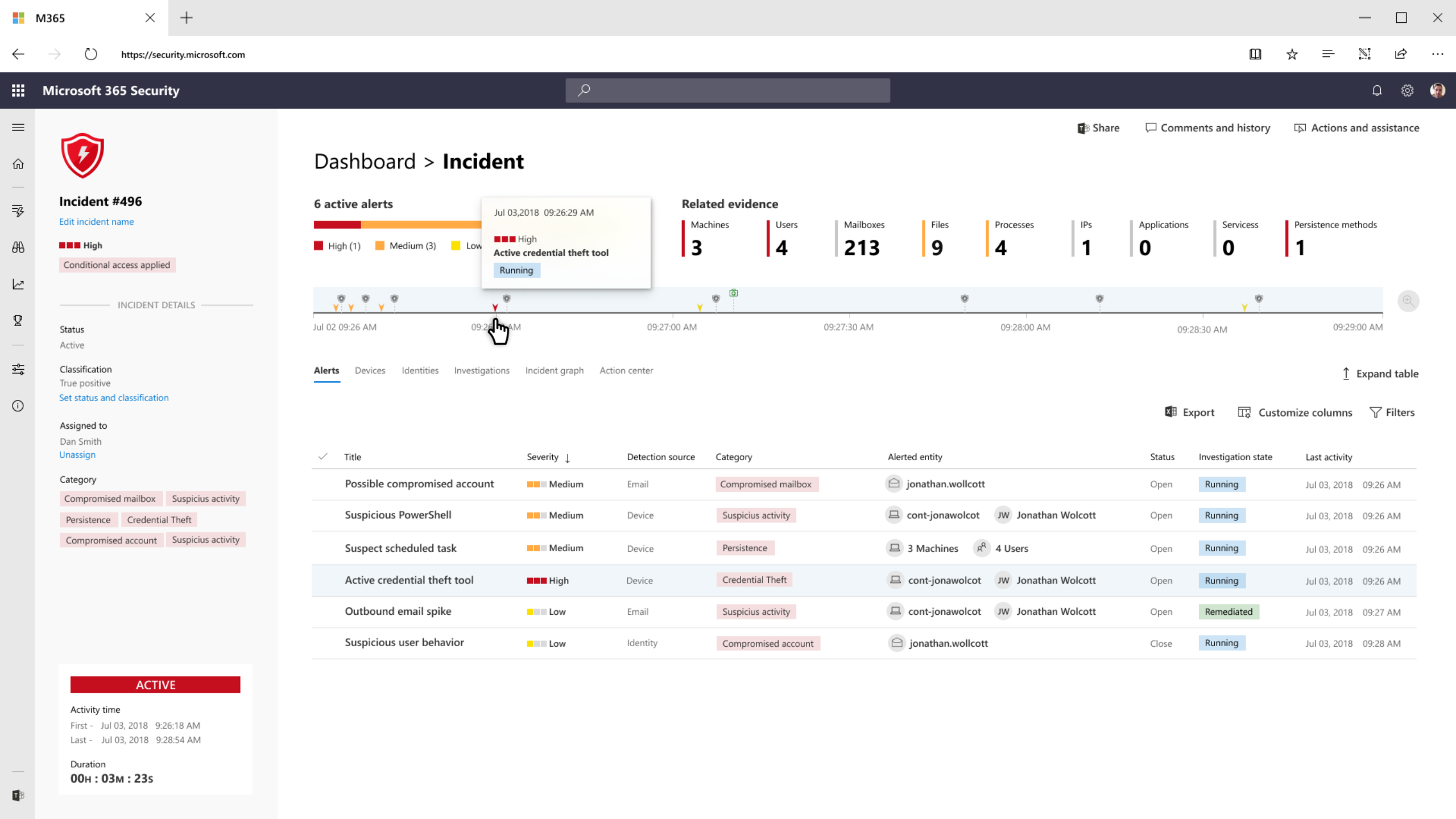
Covered by your Azure Security Center subscription.

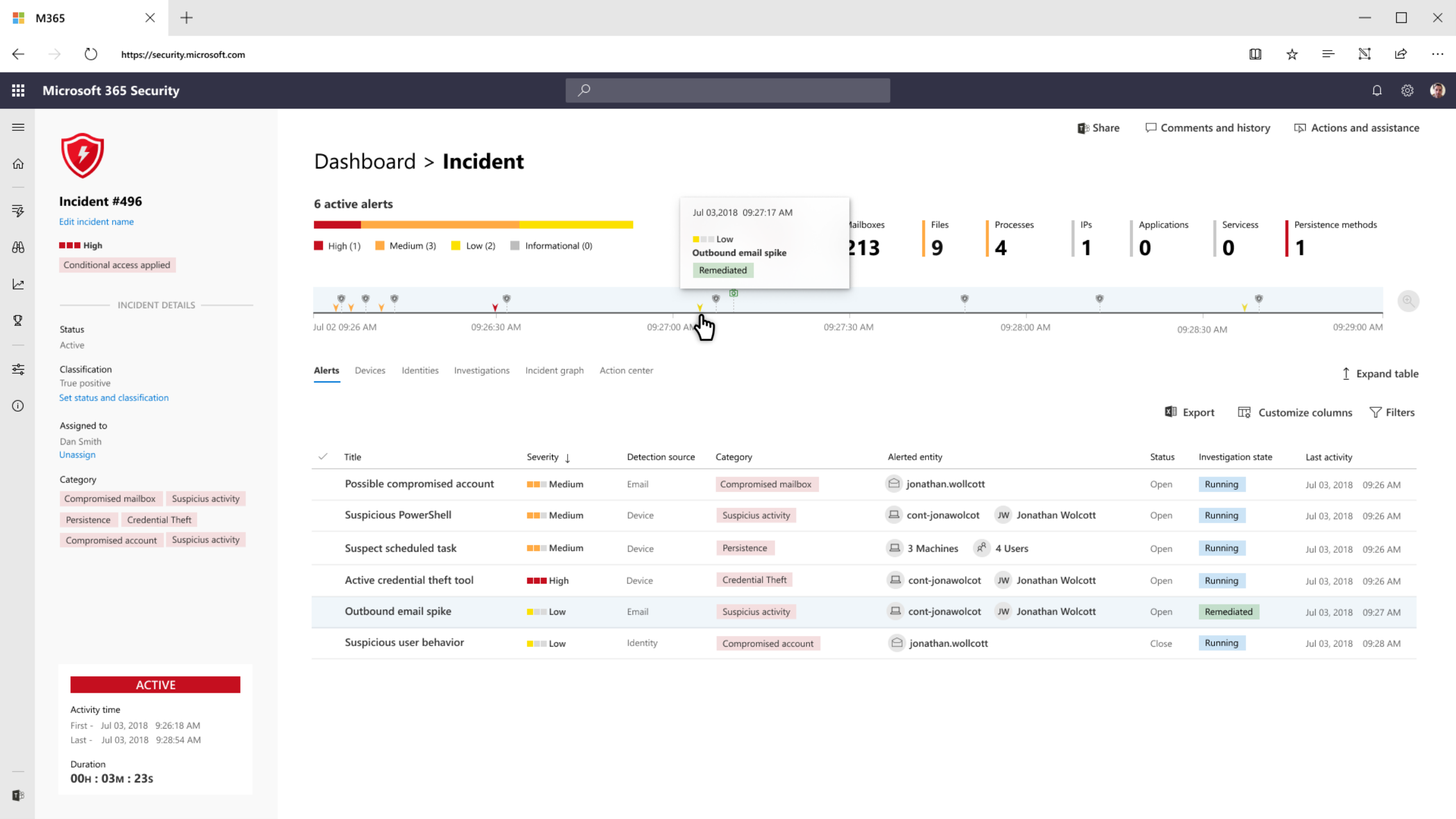
2 alerts

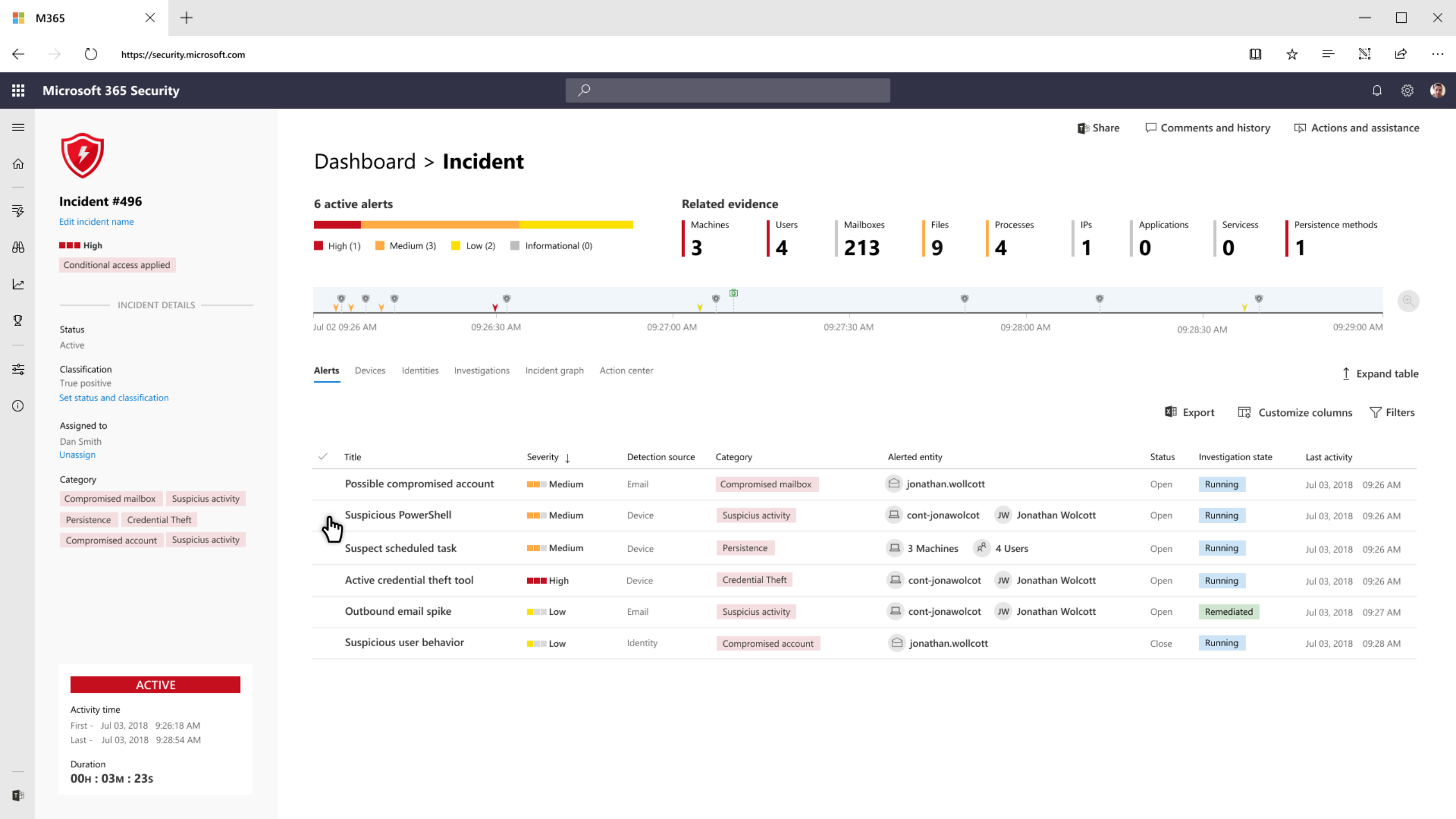
Endpoint detection & response demo

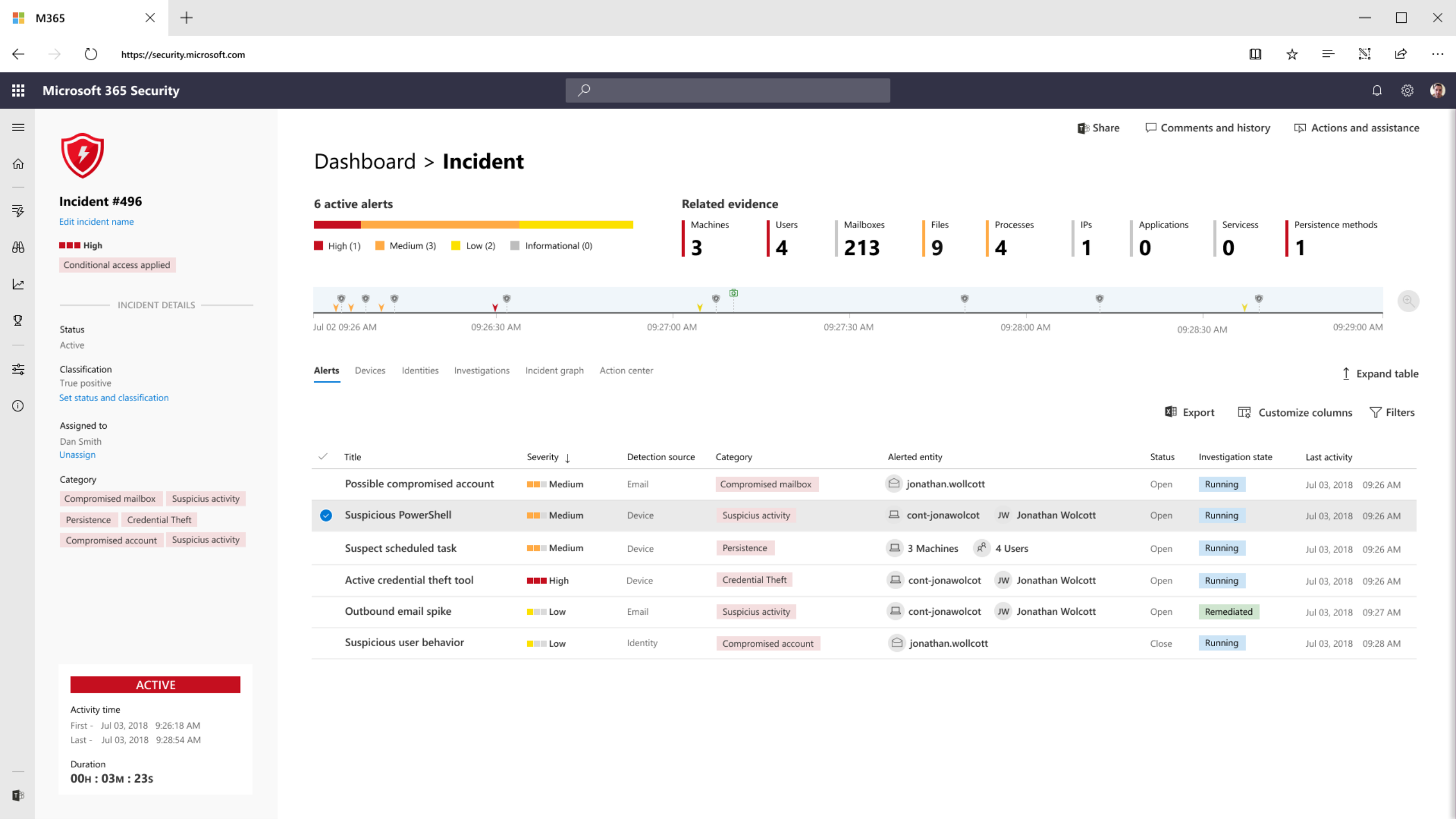

M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines
3
Users
4
Mailboxes
213
Files
9
Processes
4
IPs
1
Applications
0
Servicess
0
Persistence methods
1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM

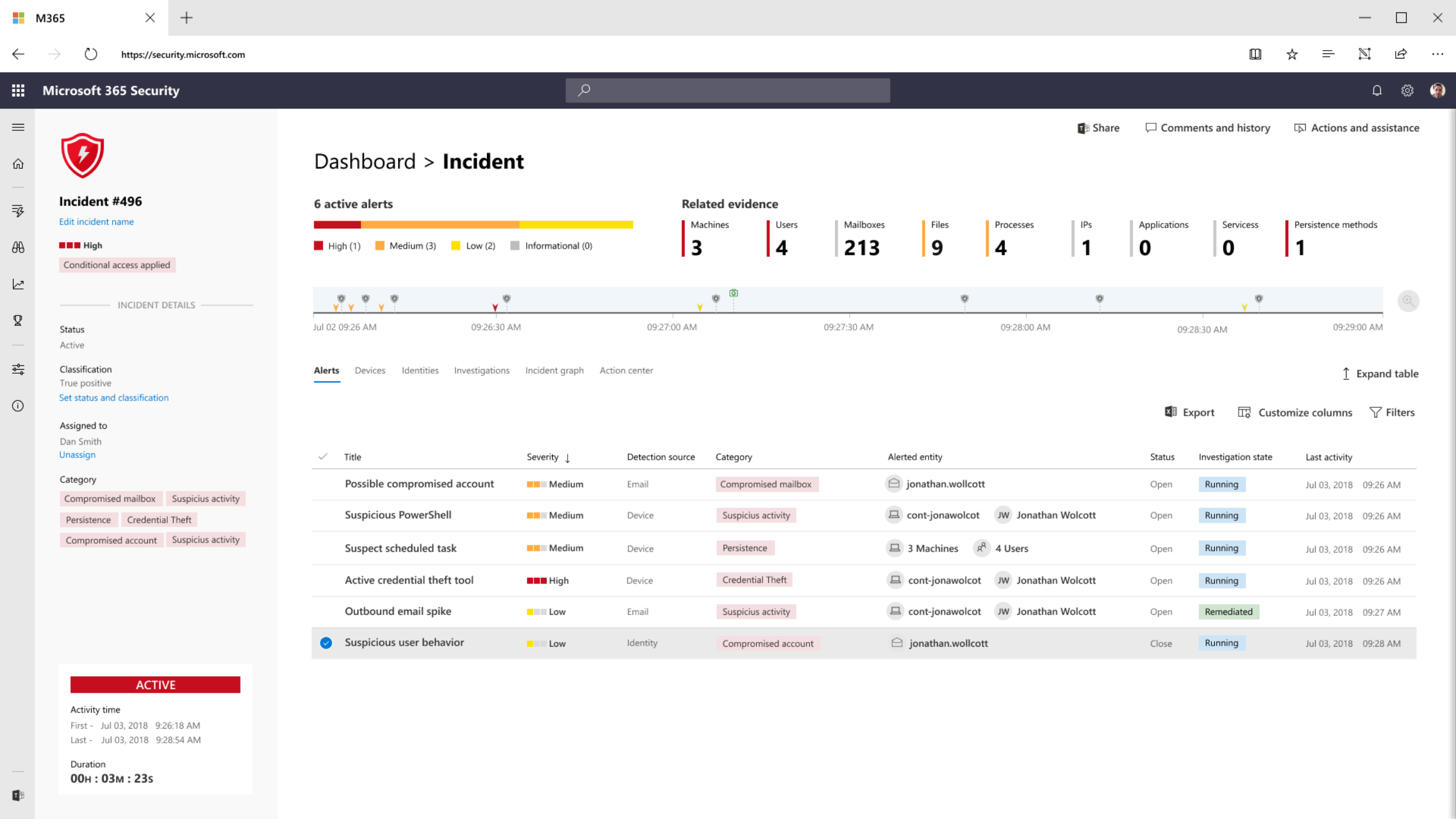

M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
Jul 03,2018 09:26:02 AM
Medium
Possible compromised account
Running
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account | Medium | Email | Compromised mailbox | jonathan.wollcott | Open | Running | Jul 03, 2018 09:26 AM
Suspicious PowerShell | Medium | Device | Suspicius activity | cont-jonawolcot | Jonathan Wolcott | Open | Running | Jul 03, 2018 09:26 AM
Suspect scheduled task | Medium | Device | Persistence | 3 Machines | 4 Users | Open | Running | Jul 03, 2018 09:26 AM
Active credential theft tool | High | Device | Credential Theft | cont-jonawolcot | Jonathan Wolcott | Open | Running | Jul 03, 2018 09:26 AM
Outbound email spike | Low | Email | Suspicius activity | cont-jonawolcot | Jonathan Wolcott | Open | Remediated | Jul 03, 2018 09:27 AM
Suspicious user behavior | Low | Identity | Compromised account | jonathan.wollcott | Close | Running | Jul 03, 2018 09:28 AM

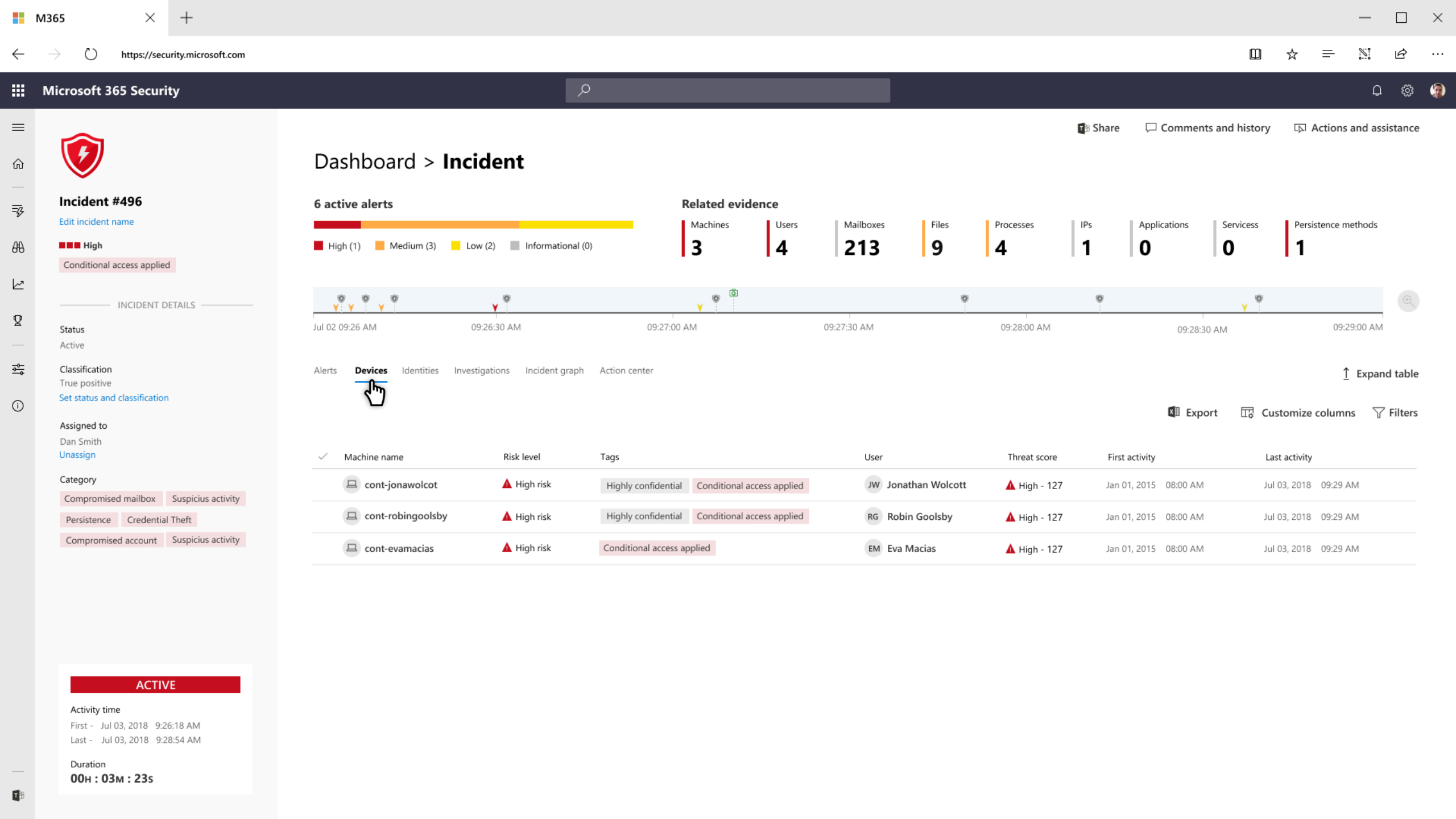

M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Jul 03,2018 09:26:29 AM
High
Active credential theft tool
Running
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account | Medium | Email | Compromised mailbox | jonathan.wollcott | Open | Running | Jul 03, 2018 09:26 AM
Suspicious PowerShell | Medium | Device | Suspicius activity | cont-jonawolcot | Jonathan Wolcott | Open | Running | Jul 03, 2018 09:26 AM
Suspect scheduled task | Medium | Device | Persistence | 3 Machines | 4 Users | Open | Running | Jul 03, 2018 09:26 AM
Active credential theft tool | High | Device | Credential Theft | cont-jonawolcot | Jonathan Wolcott | Open | Running | Jul 03, 2018 09:26 AM
Outbound email spike | Low | Email | Suspicius activity | cont-jonawolcot | Jonathan Wolcott | Open | Remediated | Jul 03, 2018 09:27 AM
Suspicious user behavior | Low | Identity | Compromised account | jonathan.wollcott | Close | Running | Jul 03, 2018 09:28 AM

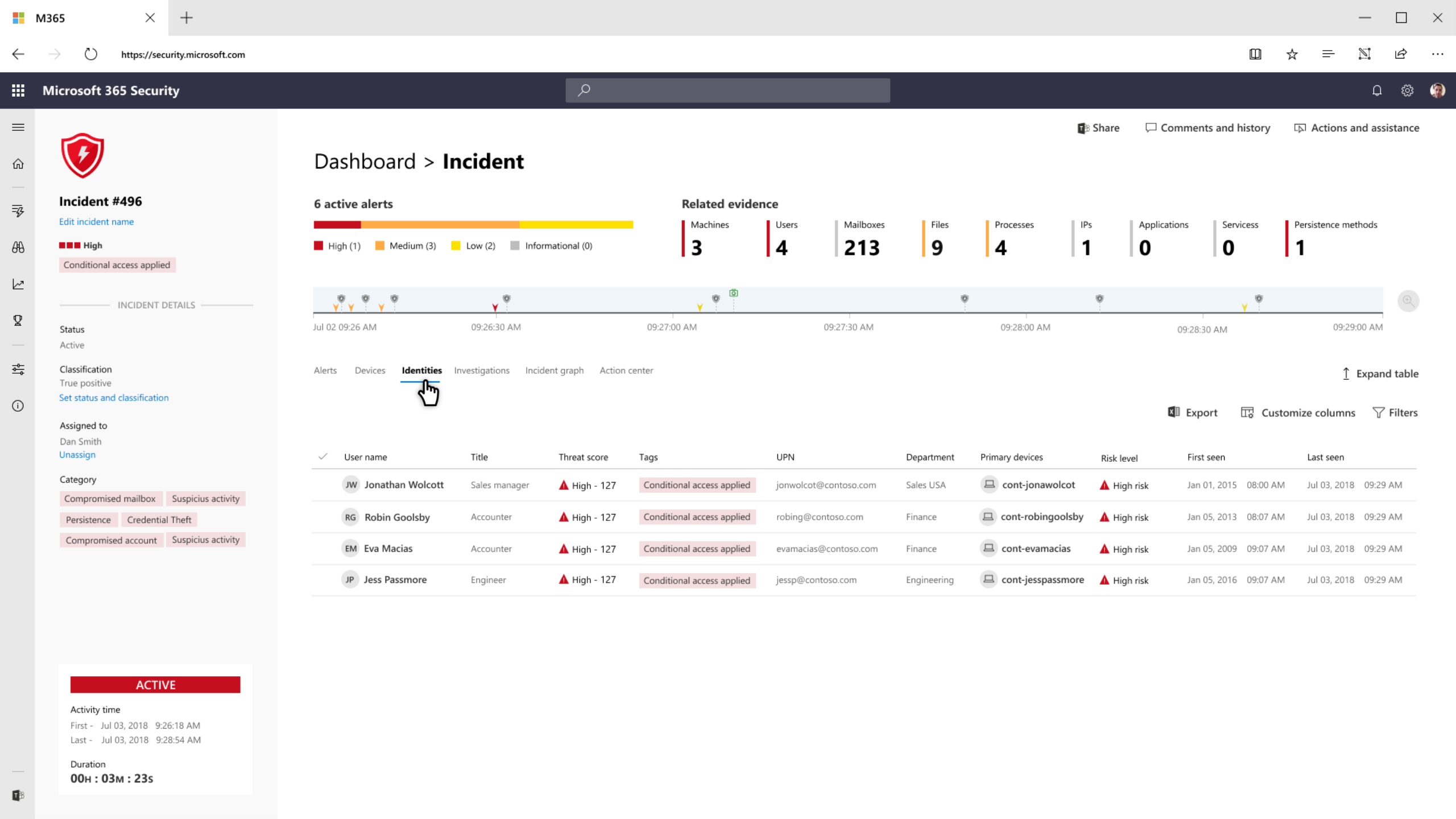

M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Jul 03,2018 09:27:17 AM
Low
Outbound email spike
Remediated
213
Files
9
Processes
4
IPs
1
Applications
0
Servicess
0
Persistence methods
1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23s
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Machine name
Risk level
Tags
User
Threat score
First activity
Last activity
cont-jonawolcot
High risk
Highly confidential
Conditional access applied
JW Jonathan Wolcott
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
cont-robingoolsby
High risk
Highly confidential
Conditional access applied
RG Robin Goolsby
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
cont-evamacias
High risk
Conditional access applied
EM Eva Macias
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
User name
Title
Threat score
Tags
UPN
Department
Primary devices
Risk level
First seen
Last seen
Jonathan Wolcott
Sales manager
High - 127
Conditional access applied
jonwolcot@contoso.com
Sales USA
cont-jonawolcot
High risk
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
Robin Goolsby
Accounter
High - 127
Conditional access applied
robing@contoso.com
Finance
cont-robingoolsby
High risk
Jan 05, 2013 08:07 AM
Jul 03, 2018 09:29 AM
Eva Macias
Accounter
High - 127
Conditional access applied
evamacias@contoso.com
Finance
cont-evamacias
High risk
Jan 05, 2009 09:07 AM
Jul 03, 2018 09:29 AM
Jess Passmore
Engineer
High - 127
Conditional access applied
jessp@contoso.com
Engineering
cont-jesspassmore
High risk
Jan 05, 2016 09:07 AM
Jul 03, 2018 09:29 AM

M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > Incident

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

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

Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Running	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20

M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > Incident

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

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

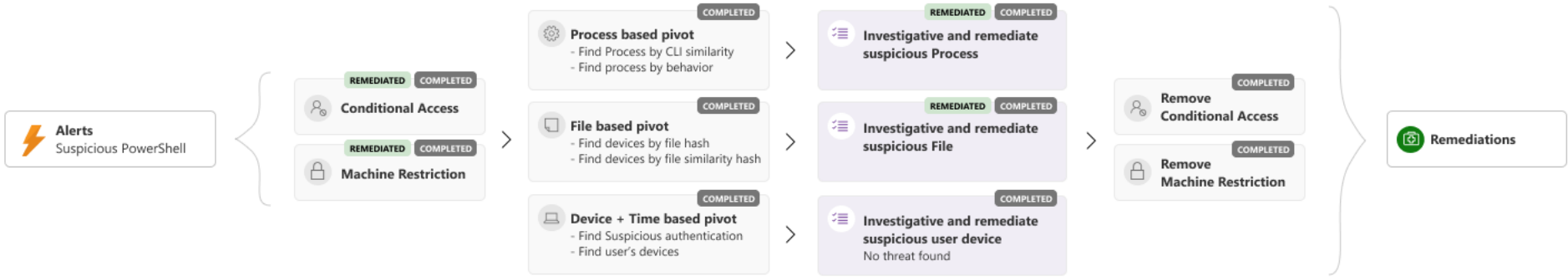
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > Incident

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

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

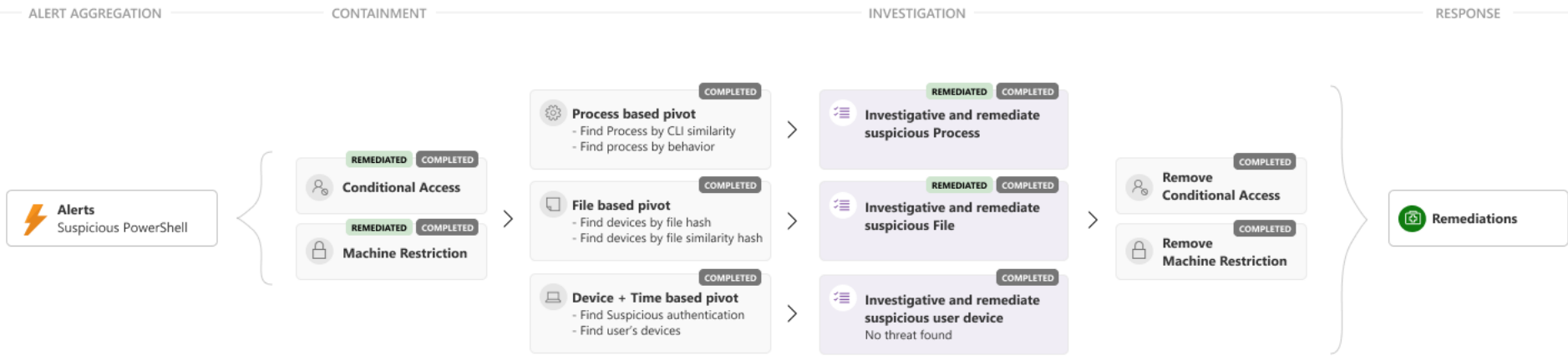
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > Incident

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

	Triggering alert	Investigation state	Investigated entities	Start date	Duration
	Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
✓	Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
	Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
	Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

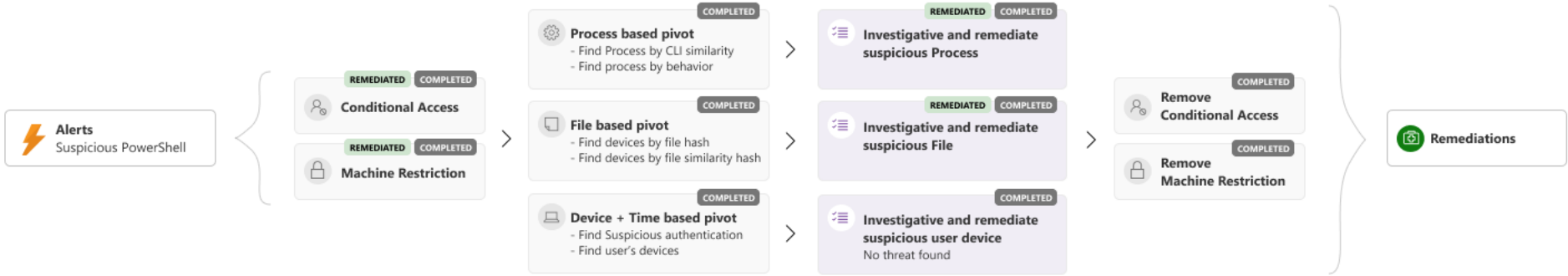
Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

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

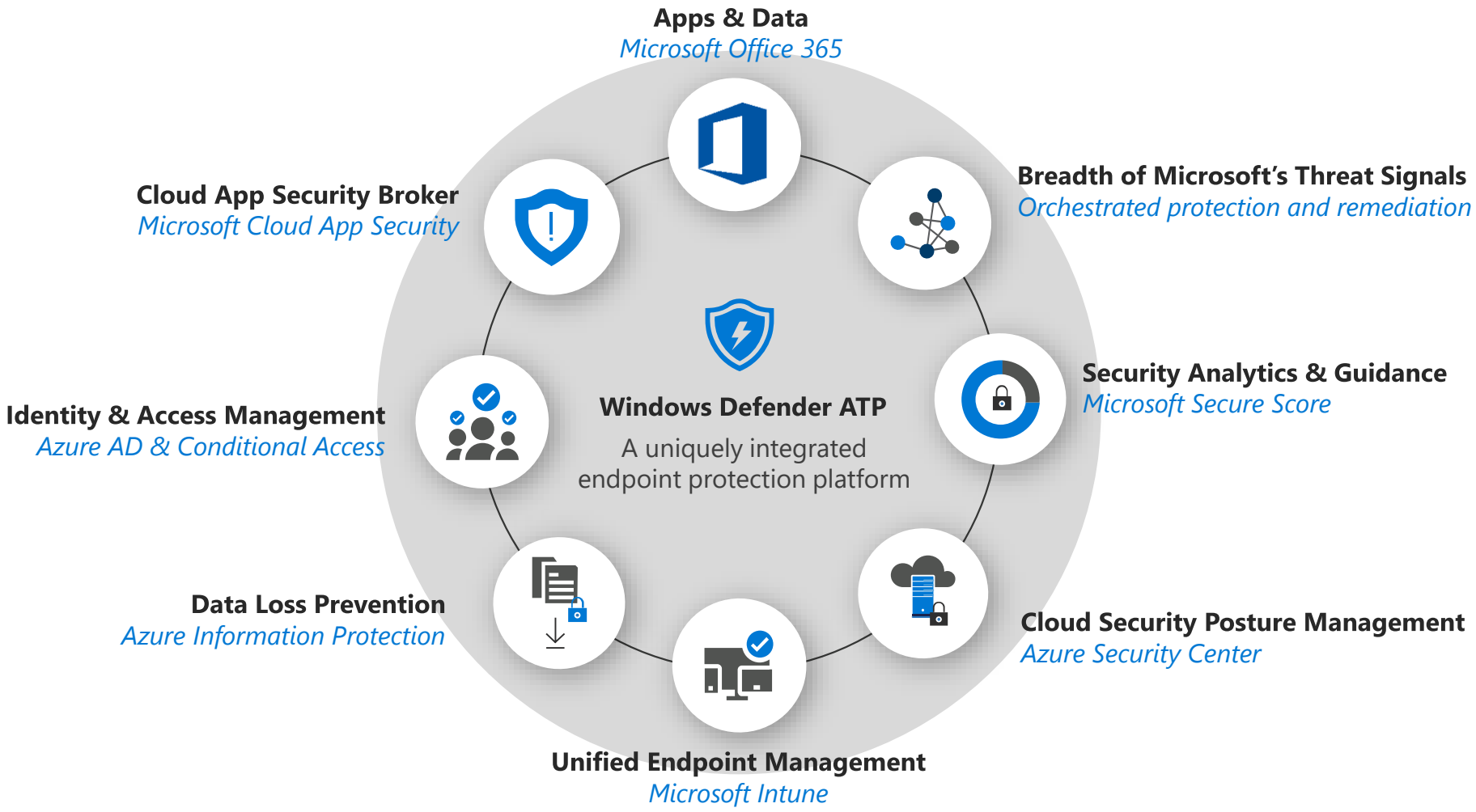
Duration
00H : 03M : 23S

ALERT AGGREGATION | CONTAINMENT | INVESTIGATION | RESPONSE



Windows Defender ATP

Elevate the security for all your workloads



SIGN UP FOR THE TRIAL
https://aka.ms/wdatp

DOCS RESOURCES
https://aka.ms/technet-wdatp

READ MSFT CASE STUDY
https://aka.ms/wdatp-cs

Windows Defender
Advanced Threat Protection

Intelligence-driven protection, detection and response.

START TRIAL > REQUEST A QUOTE >

Windows Defender ATP

Built-in. Cloud-powered.

Trusted by IT. Loved by security teams.