Microsoft Defender for Endpoint

Webinar | 25.11.2021 | Karim Trivier - IT Project Engineer

Agenda.

1. Bechtle
2. Overview
3. Incident Response
4. Onboarding
5. Features
6. Licensing
7. Next steps
8. Q&A

Bechtle Suisse SA.

Bechtle Suisse SA – en Romandie

>250

EMPLOYES

+65 EXPERTS

SUISSE ROMANDE

4

BUSINESS UNITS

PROFESSIONAL SERVICES
MANAGED SERVICES
DATA & ANALYTICS
SKILLS MANAGEMENT

>300 CLIENTS
en Suisse Romande

>20

PARTENAIRES

Top-level certifications

CITRIX	NINTEX
CISCO	POWELL
DELL	TRENDMICRO
FORTINET	VEEAM
HPE	VMWARE
MICROSOFT	…

CONSEILS
PERSONNALISES

20

ANNEES
D' EXPERIENCE

ORGANISATION
CENTRALE
AVEC SPOC

PME,
ENTERPRISE
ET PUBLIC

PLAN
BUILD
RUN

NOS PROPRES
DATA CENTERS
En SUISSE

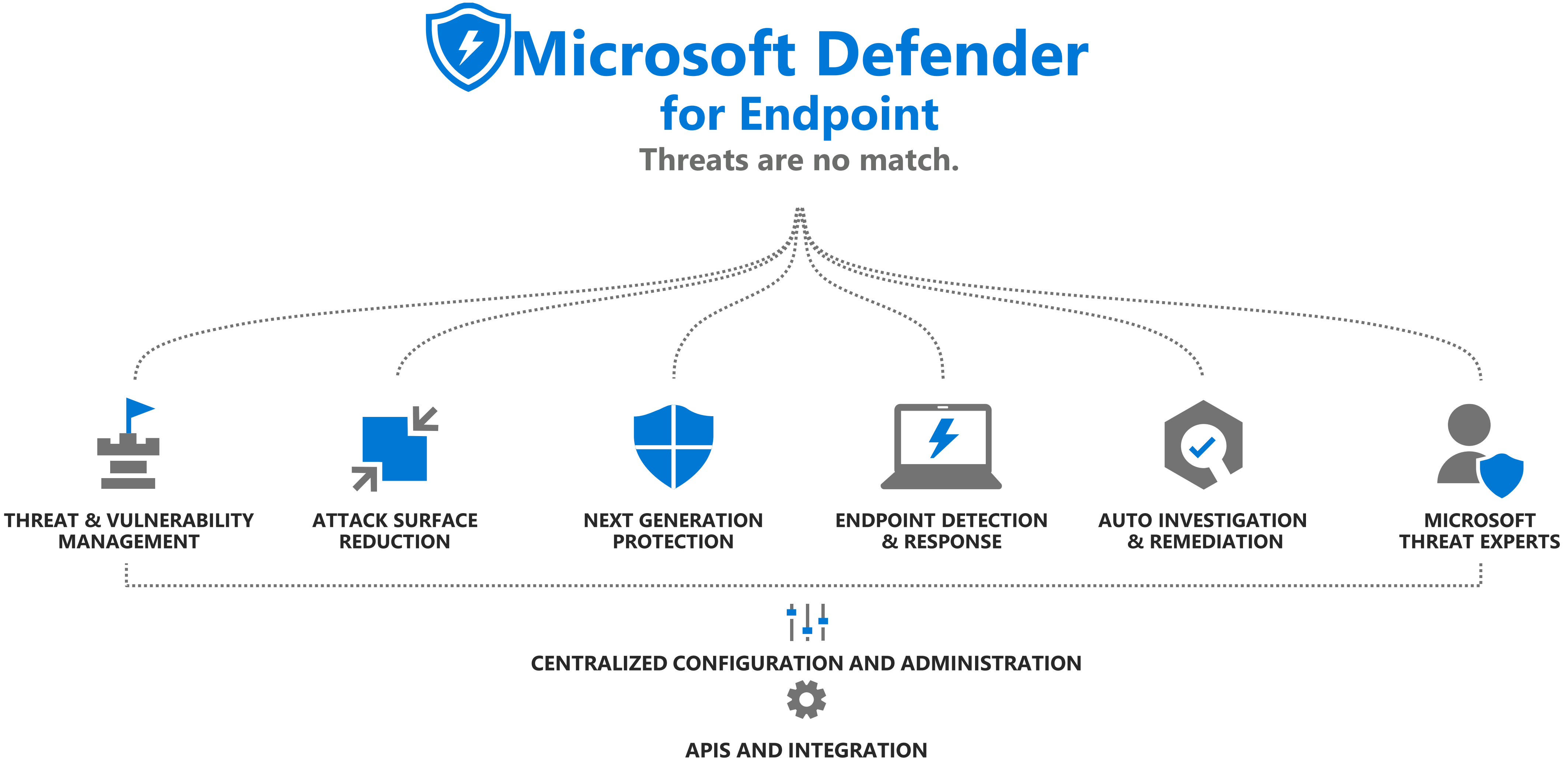
+500

PROJETS / AN

Overview.

Microsoft Defender for Endpoint

Solution overview



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

Why they are 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.

Microsoft Defender for Endpoint

An industry leader in endpoint security

Gartner names Microsoft a Leader in 2021 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

Microsoft Defender for Endpoint

Delivering industry leading endpoint security across platforms

- Windows 7 SP1 to 11
- Windows Server 2008 R2 and 2012 R2
- Windows Server 2016 to 2022

- RHEL and CentOS 6.7+
- RHEL and CentOS 7.2+
- Ubuntu 16.04 LTS+
- Debian 9+
- SUSE LES 12+
- Oracle Linux 7.2+
- Amazon Linux 2
- Fedora 33+

- macOS 10.14 to 12
- iOS 12 to 15
- iPadOS 12 to 15

Android 6+

Incident Response.

Incident Response

SANS Incident Handler’s Handbook – Response Plan

1. PREPARATION
2. IDENTIFICATION
3. CONTAINMENT
4. ERADICATION
5. RECOVERY
6. LESSONS LEARNED

Onboarding.

Microsoft Defender for Endpoint

Delivering industry leading endpoint security across platforms

Windows Supported (10, 11, 2012 R2 to 2022)

- Local Script
- GPO
- MECM
- Intune
- Microsoft Defender for Cloud

Windows Legacy (7, 8.1 and 2008 R2)

- Microsoft Monitoring Agent

- Manual (app & onboarding package)
- Puppet
- Ansible
- Chef

macOS

- Manual (app & onboarding package)
- JAMF
- Other UEM

iOS and iPadOS

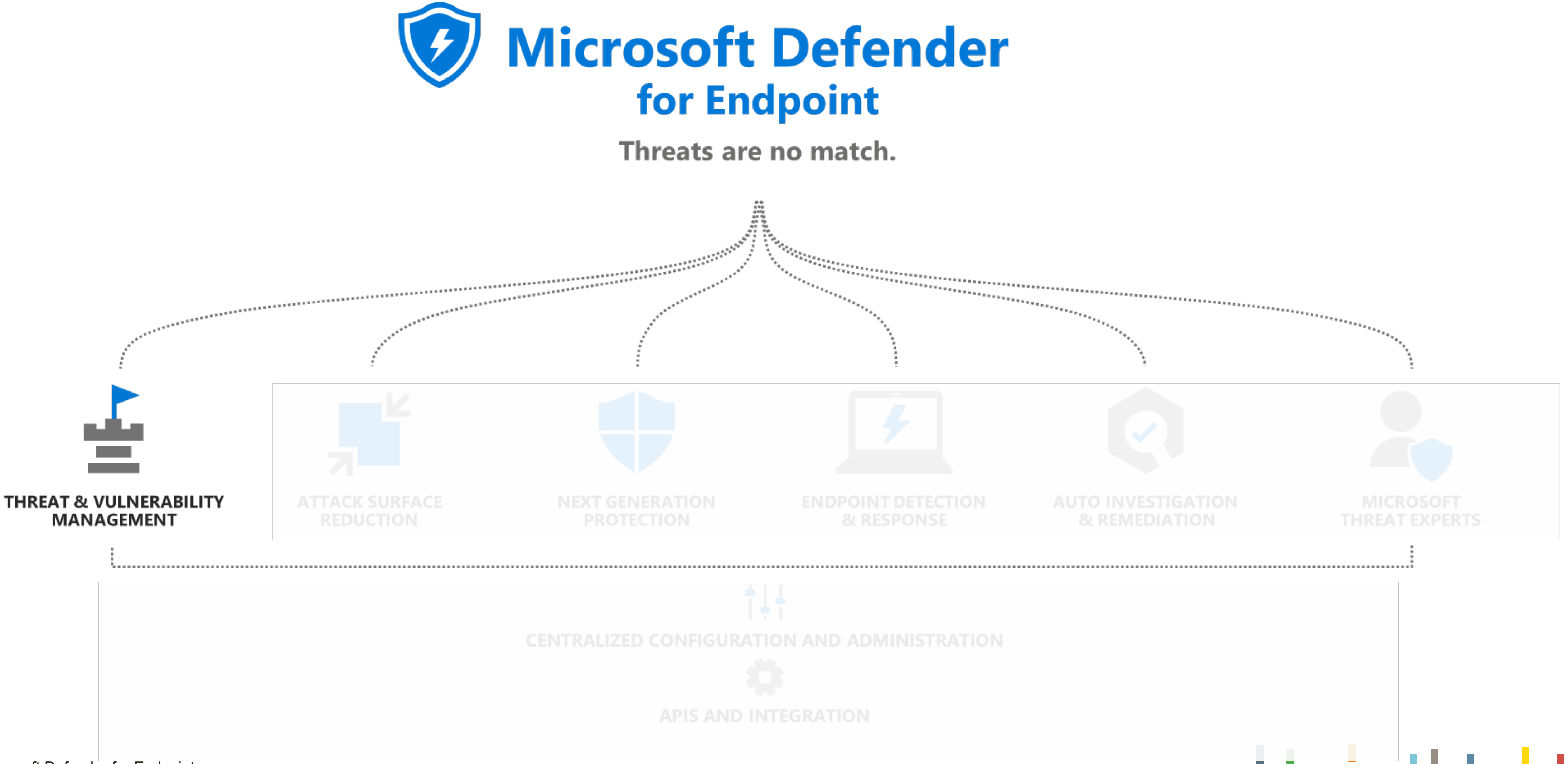
- Microsoft Defender for Endpoint app

Microsoft Defender for Endpoint app

Features.

Microsoft Defender for Endpoint

Threat & Vulnerability Management



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

Threat & Vulnerability Management

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

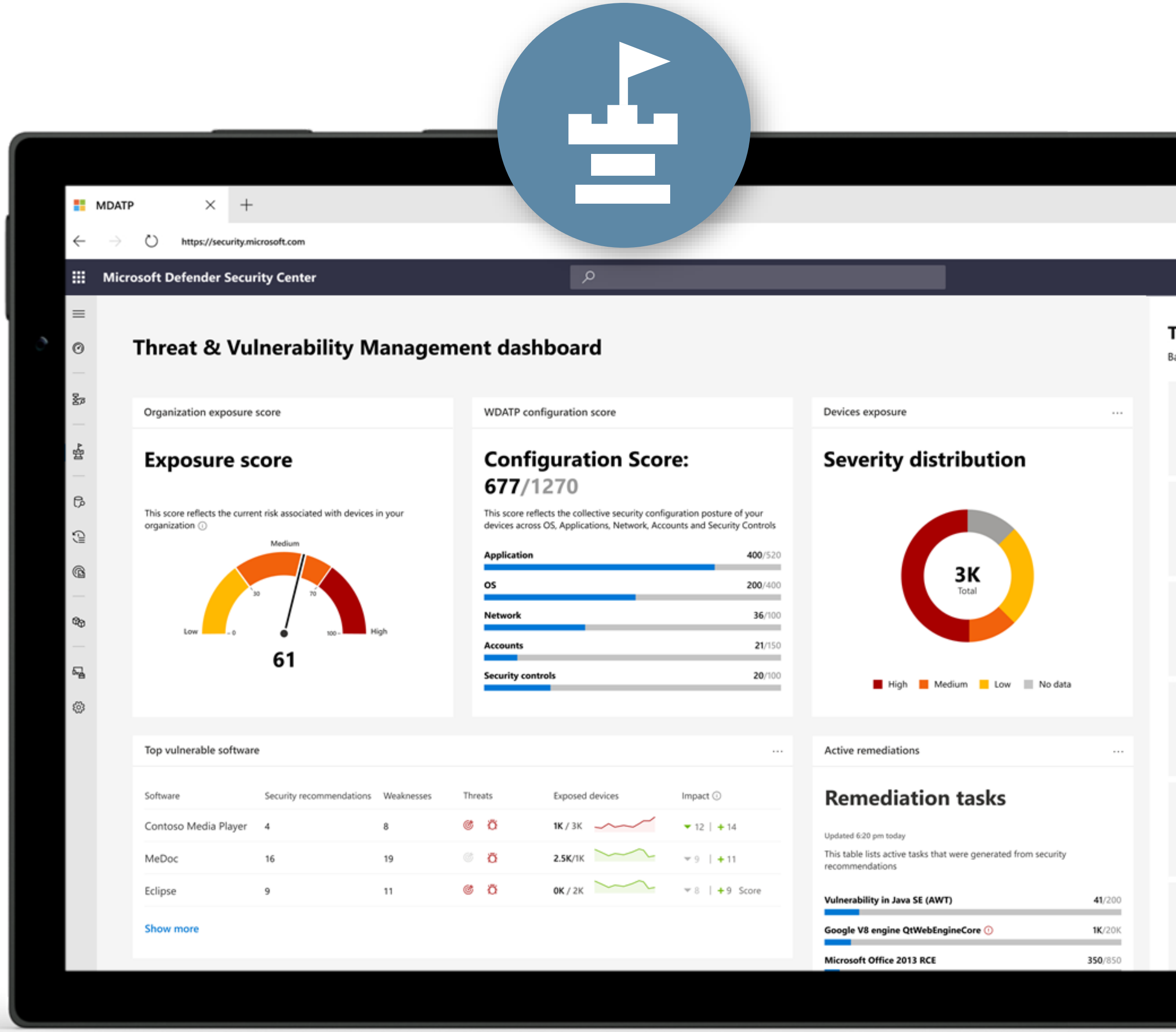
Bottom line: Organizations remain highly vulnerable, despite high maintenance costs

Microsoft Defender for Endpoint

Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

- Continuous real-time discovery
- Context-aware prioritization
- 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

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

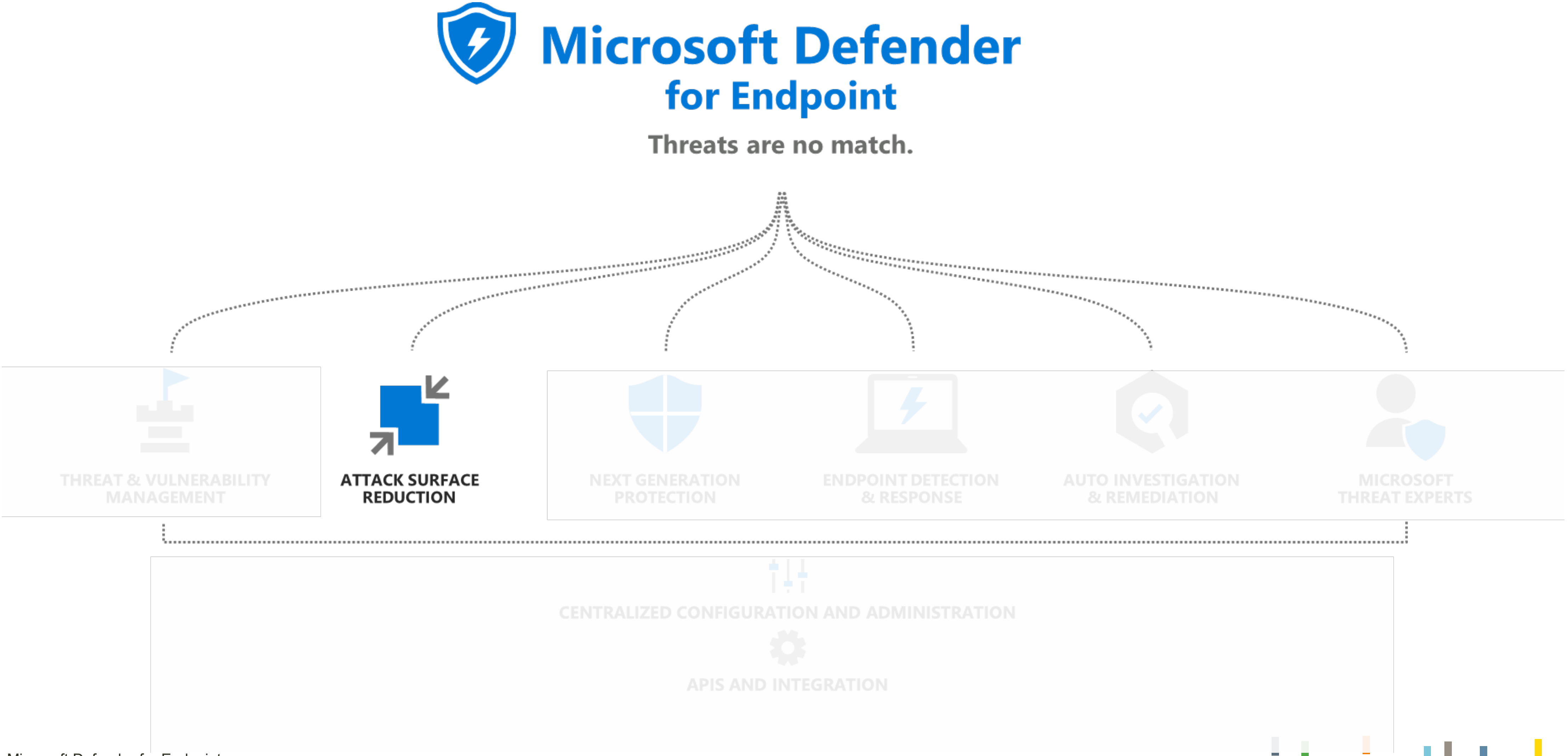
This table lists active tasks that were generated from security recommendations

Vulnerability in Java SE (AWT)	41/200
Google V8 engine QtWebEngineCore	1K/20K
Microsoft Office 2013 RCE	350/850

Demo.

Microsoft Defender for Endpoint

Attack Surface Reduction


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

Attack Surface Reduction

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

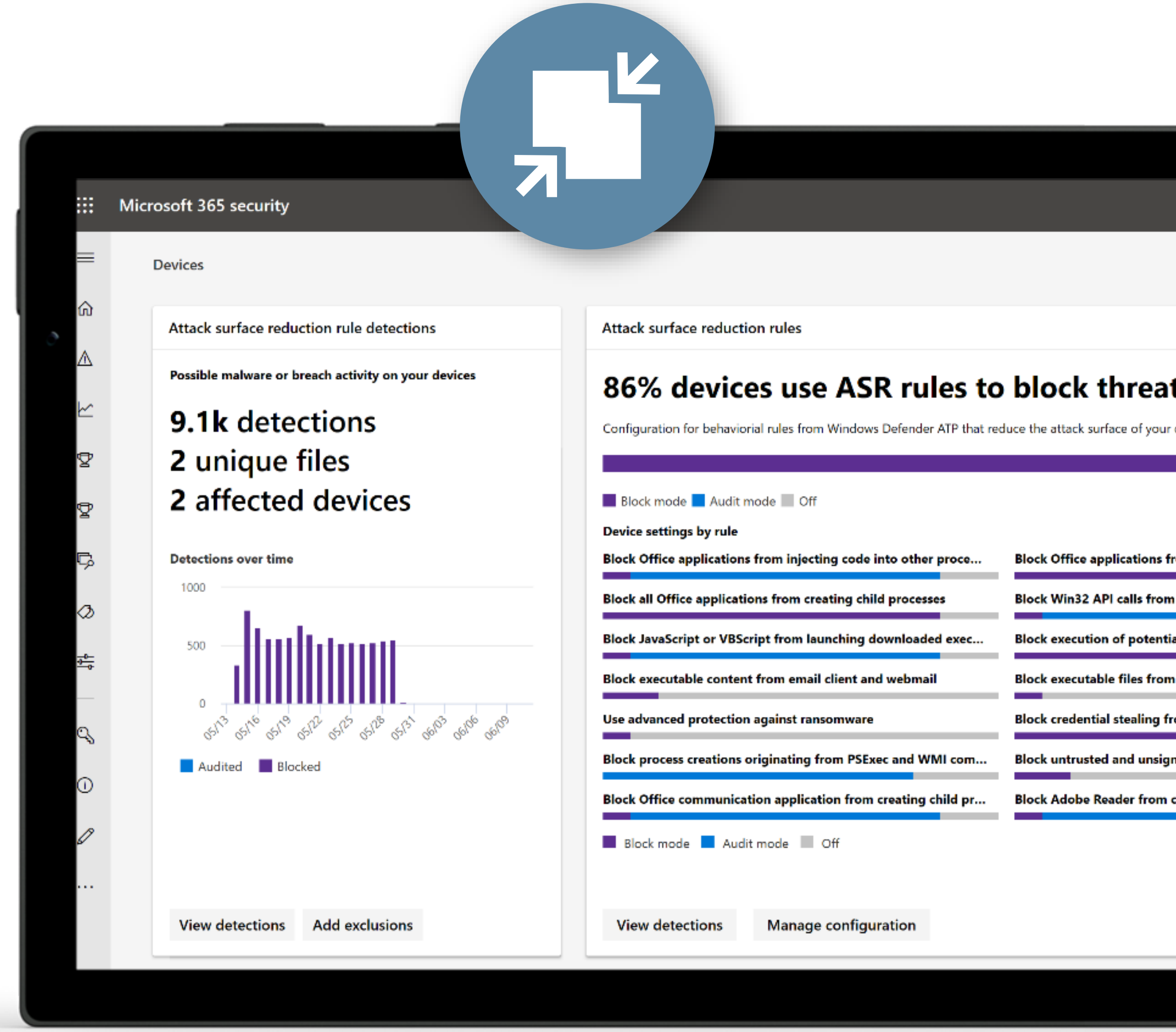
Bottom line: Organizations struggle to proactively adjust their security posture

Microsoft Defender for Endpoint

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

🟦 Audited 🟪 Blocked

View detections | Add exclusions

Attack surface reduction rules

86% devices use ASR rules to block threat

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

🟪 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 applications fr

Block Win32 API calls from

Block execution of potentia

Block executable files from

Block credential stealing fr

Block untrusted and unsign

Block Adobe Reader from c

🟪 Block mode 🟦 Audit mode ⬜ Off

View detections | Manage configuration

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

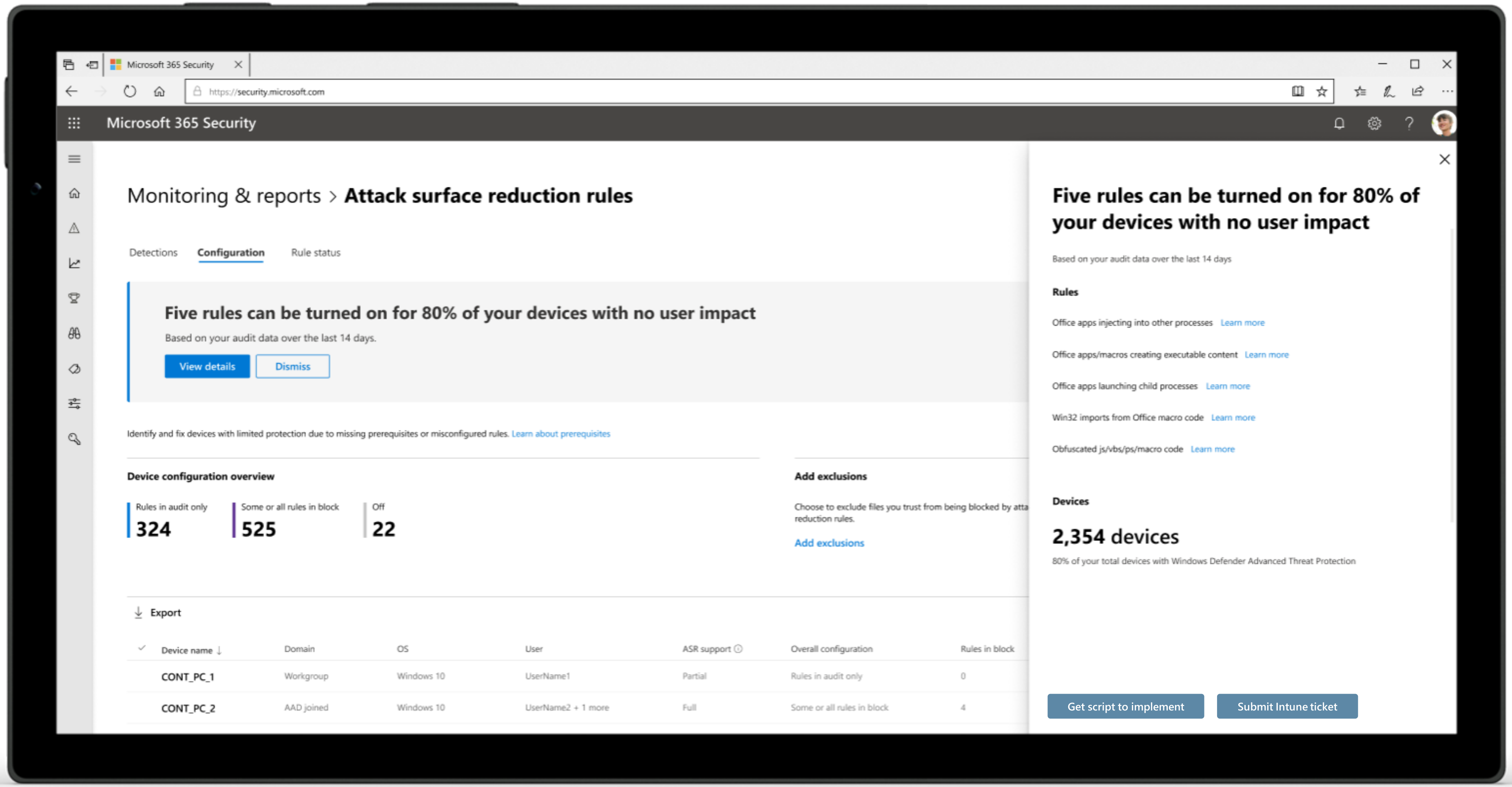
- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

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

Attack Surface Reduction

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.

Add exclusions

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

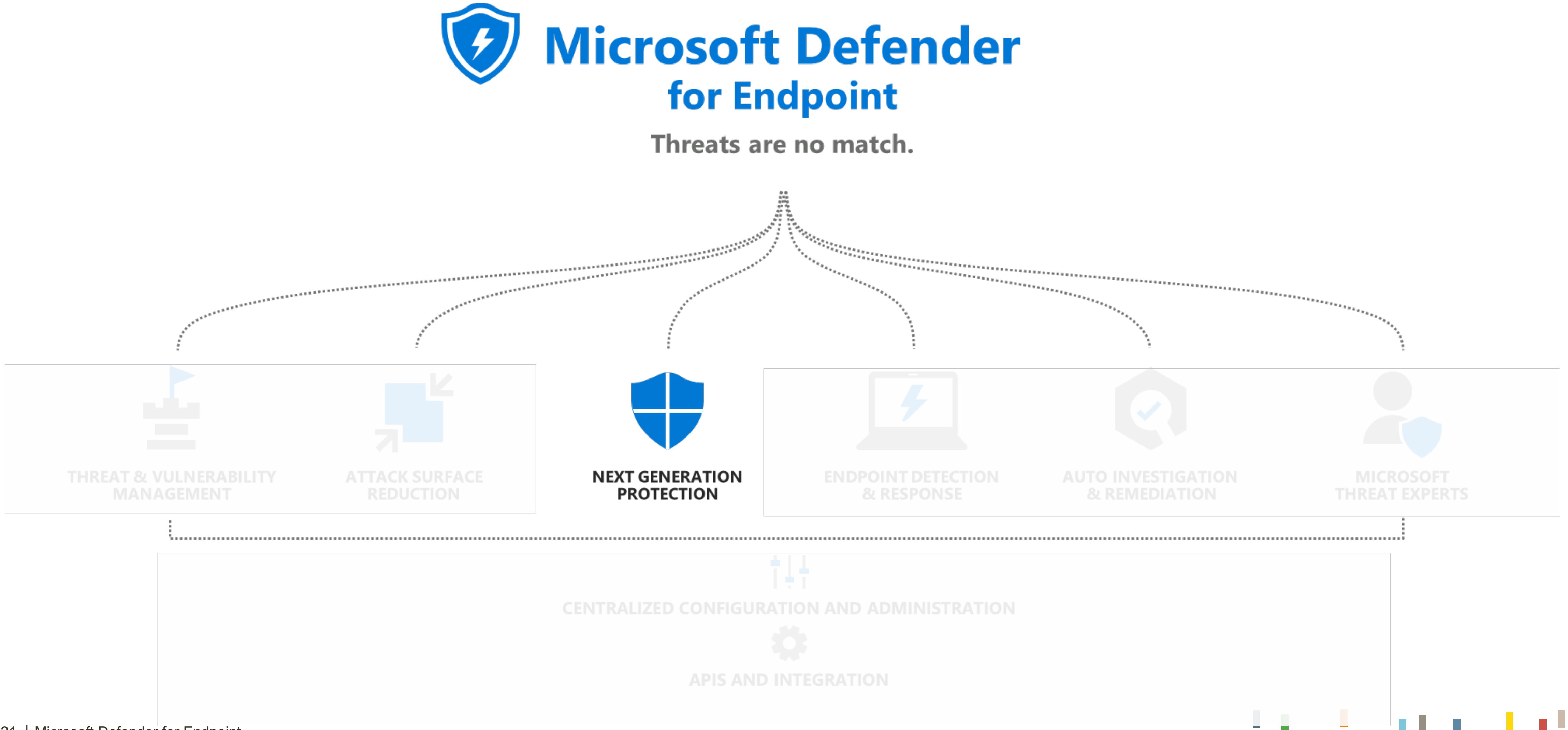
Devices

2,354 devices

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

Microsoft Defender for Endpoint

Next Generation 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

Next Generation Protection

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

Next Generation Protection

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

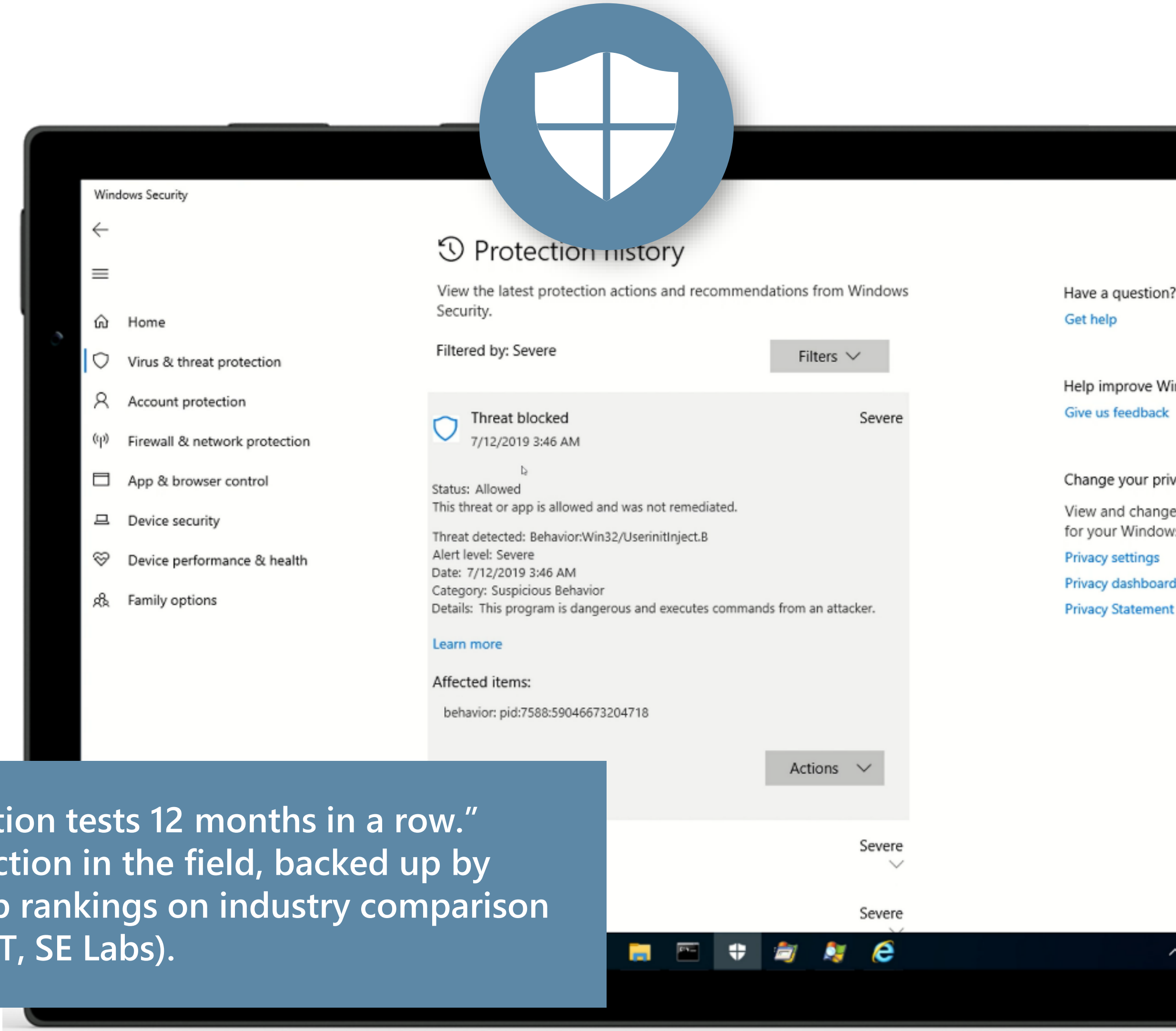
Effective

Microsoft Defender for Endpoint

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



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

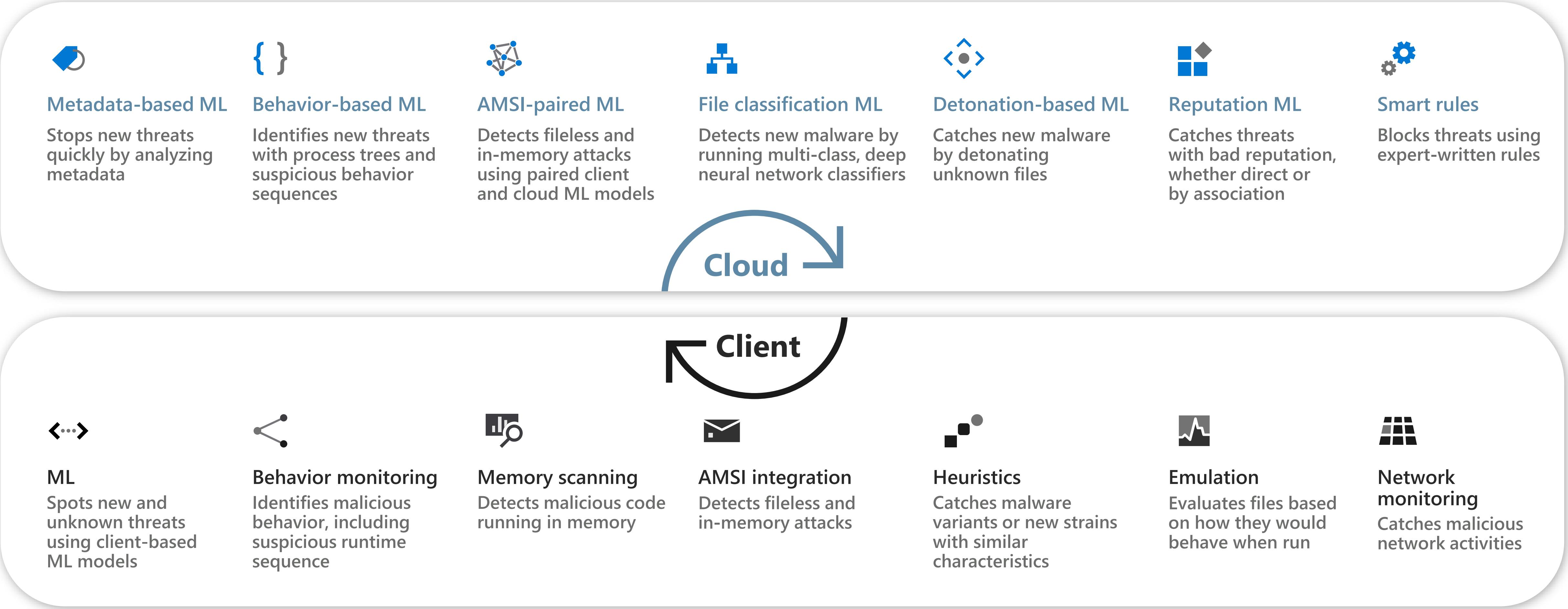
Severe

Severe

"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).

Next Generation Protection

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

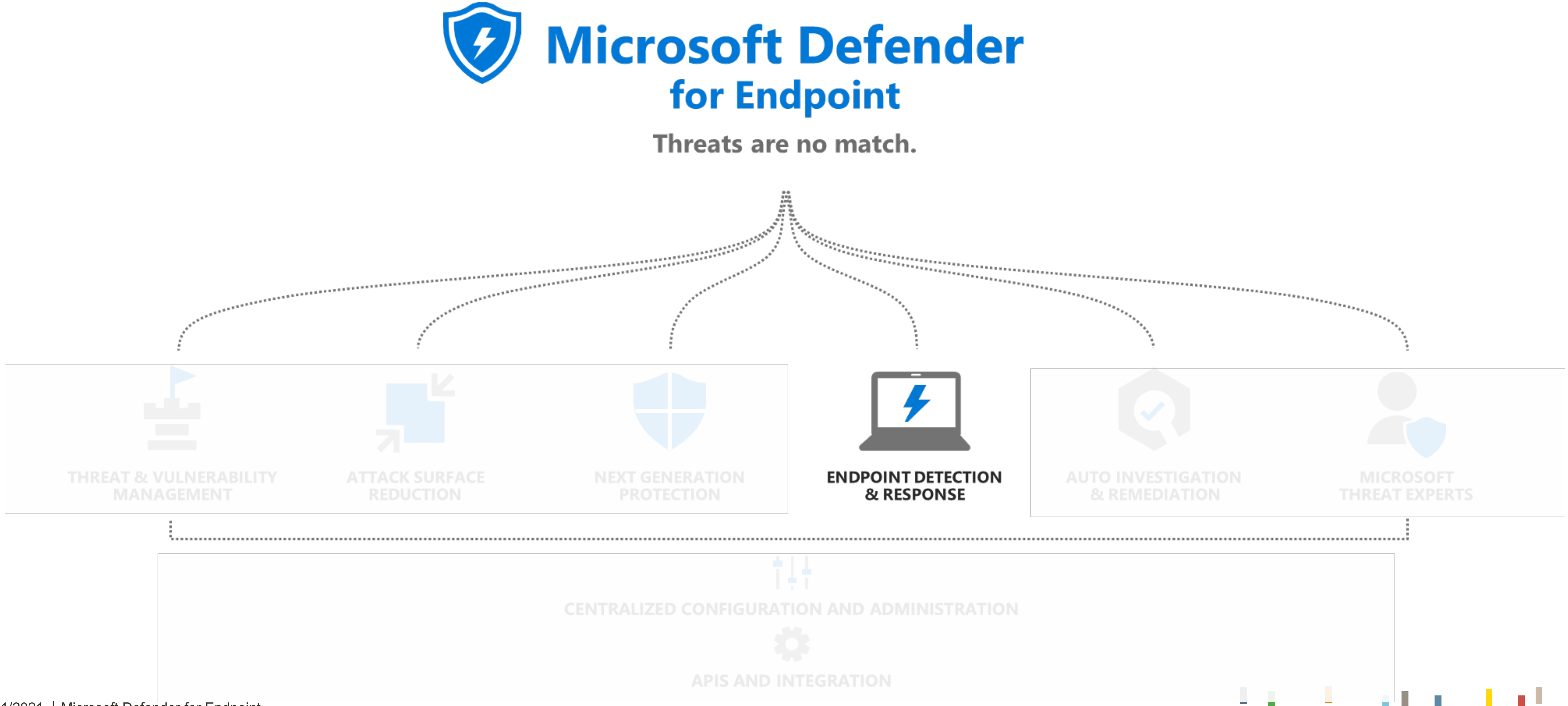
Heuristics
Catches malware variants or new strains with similar characteristics

Emulation
Evaluates files based on how they would behave when run

Network monitoring
Catches malicious network activities

Microsoft Defender for Endpoint

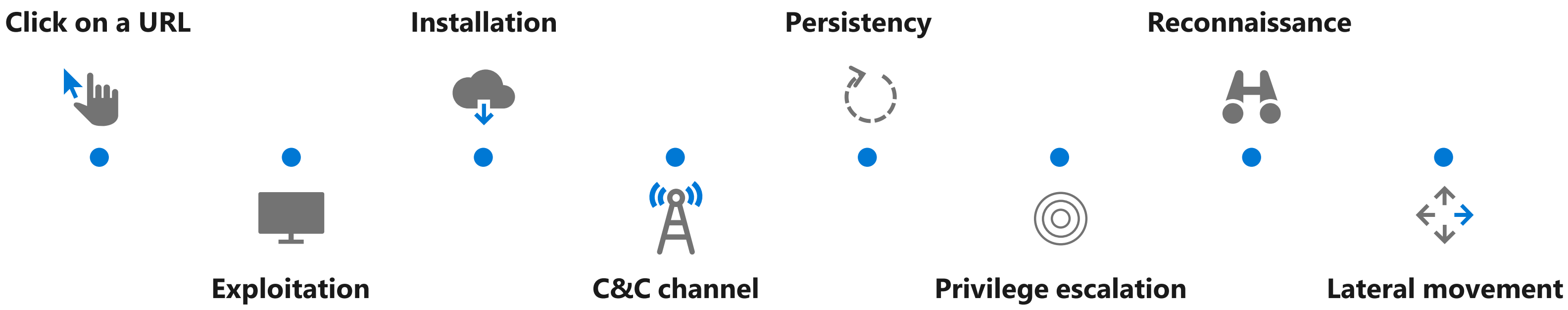
Endpoint Detection & Response


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

Endpoint Detection & Response

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

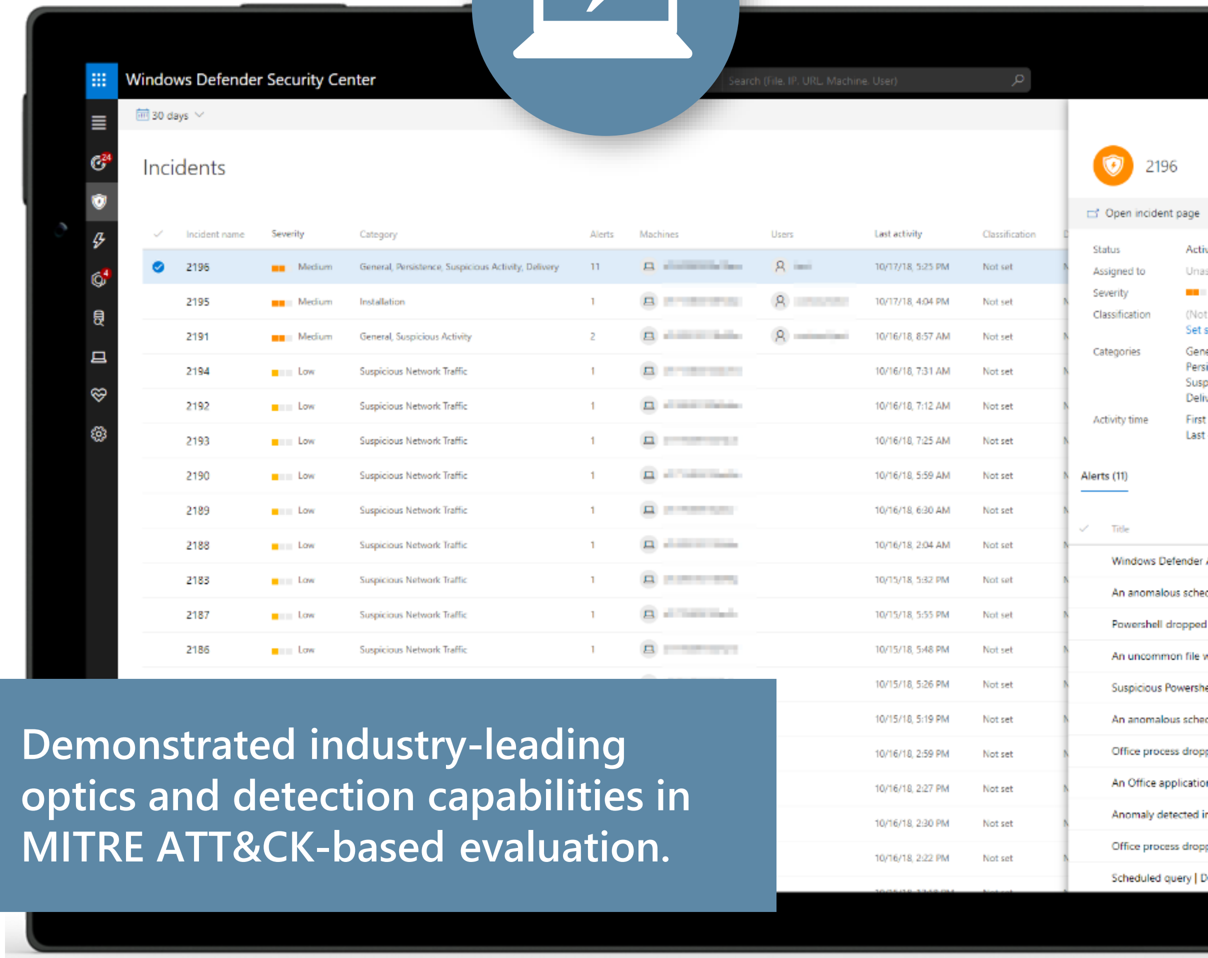
Living off the land - Attackers use evasion-techniques

Microsoft Defender for Endpoint

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

2196

Open incident page

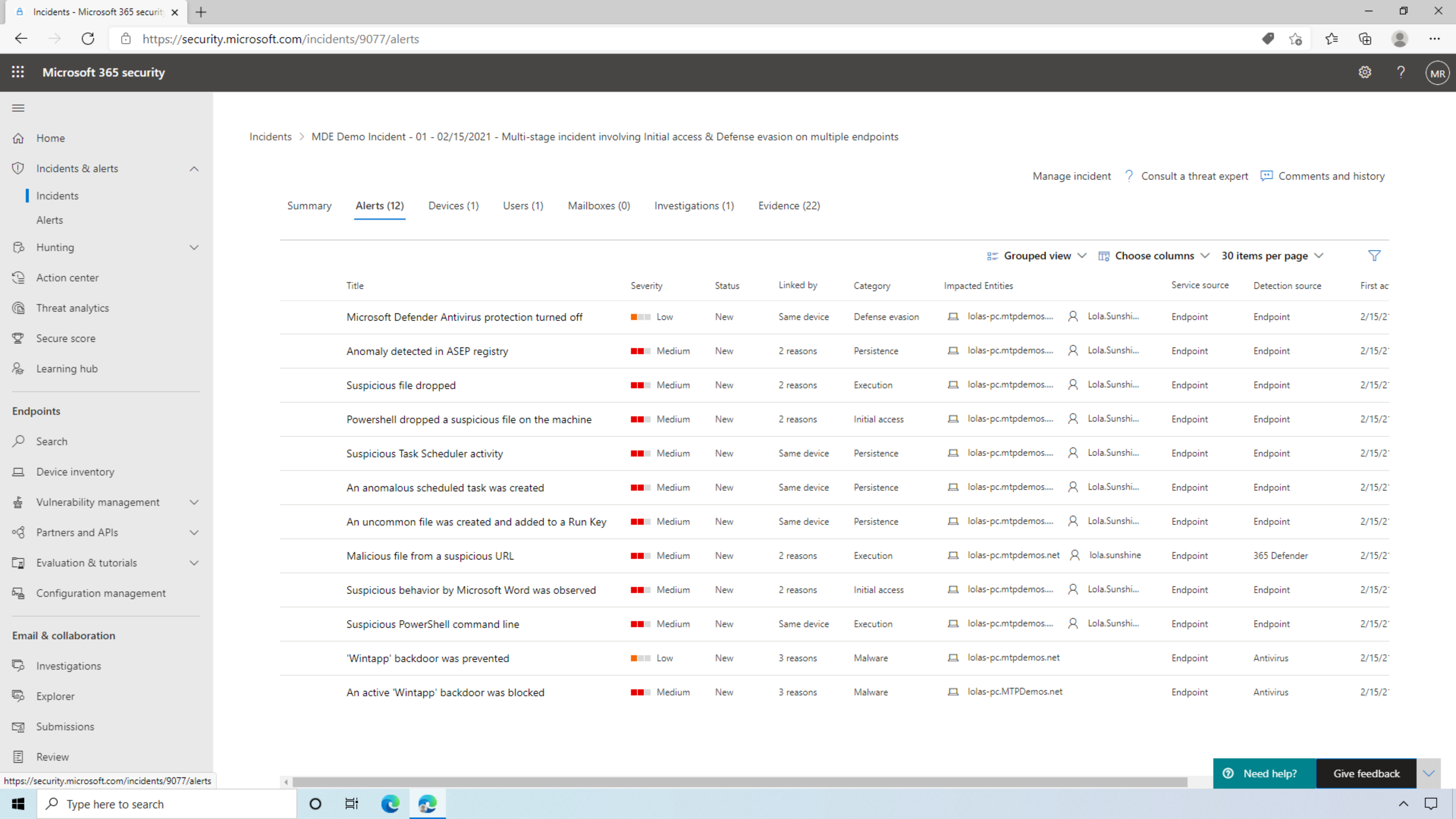
Status	Activ
Assigned to	Unas
Severity	■■□
Classification	(Not Set s
Categories	Gene Persi Susp Deliv
Activity time	First Last

Alerts (11)

✓	Title
	Windows Defender
	An anomalous schec
	Powershell dropped
	An uncommon file w
	Suspicious Powershe
	An anomalous schec
	Office process dropp
	An Office application
	Anomaly detected in
	Office process dropp
	Scheduled query | D

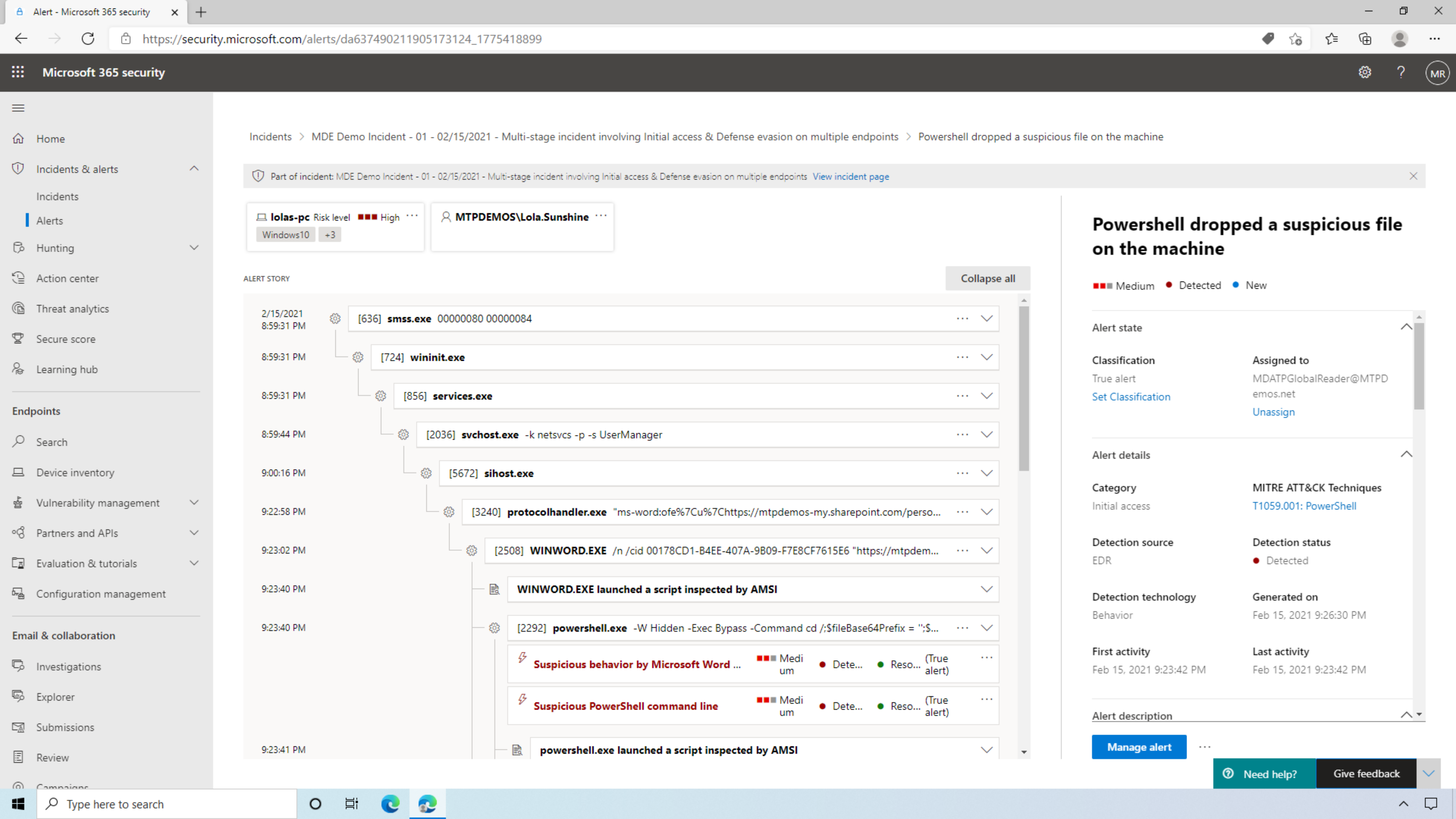
Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation.

Demo.



Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints

Title	Severity	Status	Linked by	Category	Impacted Entities		Service source	Detection source	First ac
Microsoft Defender Antivirus protection turned off	Low	New	Same device	Defense evasion	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
Anomaly detected in ASEP registry	Medium	New	2 reasons	Persistence	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
Suspicious file dropped	Medium	New	2 reasons	Execution	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
Powershell dropped a suspicious file on the machine	Medium	New	2 reasons	Initial access	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
Suspicious Task Scheduler activity	Medium	New	Same device	Persistence	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
An anomalous scheduled task was created	Medium	New	Same device	Persistence	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
An uncommon file was created and added to a Run Key	Medium	New	Same device	Persistence	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
Malicious file from a suspicious URL	Medium	New	2 reasons	Execution	lolas-pc.mtpdemos.net	lola.sunshine	Endpoint	365 Defender	2/15/2
Suspicious behavior by Microsoft Word was observed	Medium	New	2 reasons	Initial access	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
Suspicious PowerShell command line	Medium	New	Same device	Execution	lolas-pc.mtpdemos....	Lola.Sunshi...	Endpoint	Endpoint	2/15/2
'Wintapp' backdoor was prevented	Low	New	3 reasons	Malware	lolas-pc.mtpdemos.net		Endpoint	Antivirus	2/15/2
An active 'Wintapp' backdoor was blocked	Medium	New	3 reasons	Malware	lolas-pc.MTPDemos.net		Endpoint	Antivirus	2/15/2



Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints > Powershell dropped a suspicious file on the machine

Part of incident: MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints View incident page

lolas-pc Risk level ■■■ High
Windows10 +3

MTPDEMOS\Lola.Sunshine

ALERT STORY

2/15/2021 8:59:31 PM	[636] **smss.exe** 00000080 00000084
8:59:31 PM	[724] **wininit.exe**
8:59:31 PM	[856] **services.exe**
8:59:44 PM	[2036] **svchost.exe** -k netsvcs -p -s UserManager
9:00:16 PM	[5672] **sihost.exe**
9:22:58 PM	[3240] **protocolhandler.exe** "ms-word:ofe%7Cu%7Chttps://mtpdemos-my.sharepoint.com/perso...
9:23:02 PM	[2508] **WINWORD.EXE** /n /cid 00178CD1-B4EE-407A-9B09-F7E8CF7615E6 "https://mtpdem...
9:23:40 PM	**WINWORD.EXE launched a script inspected by AMSI**
9:23:40 PM	[2292] **powershell.exe** -W Hidden -Exec Bypass -Command cd /;$fileBase64Prefix = ";$...
	Suspicious behavior by Microsoft Word ... ■■■ Medium ● Dete... ● Reso... (True alert)
	Suspicious PowerShell command line ■■■ Medium ● Dete... ● Reso... (True alert)
9:23:41 PM	**powershell.exe launched a script inspected by AMSI**

Powershell dropped a suspicious file on the machine

■■■ Medium ● Detected ● New

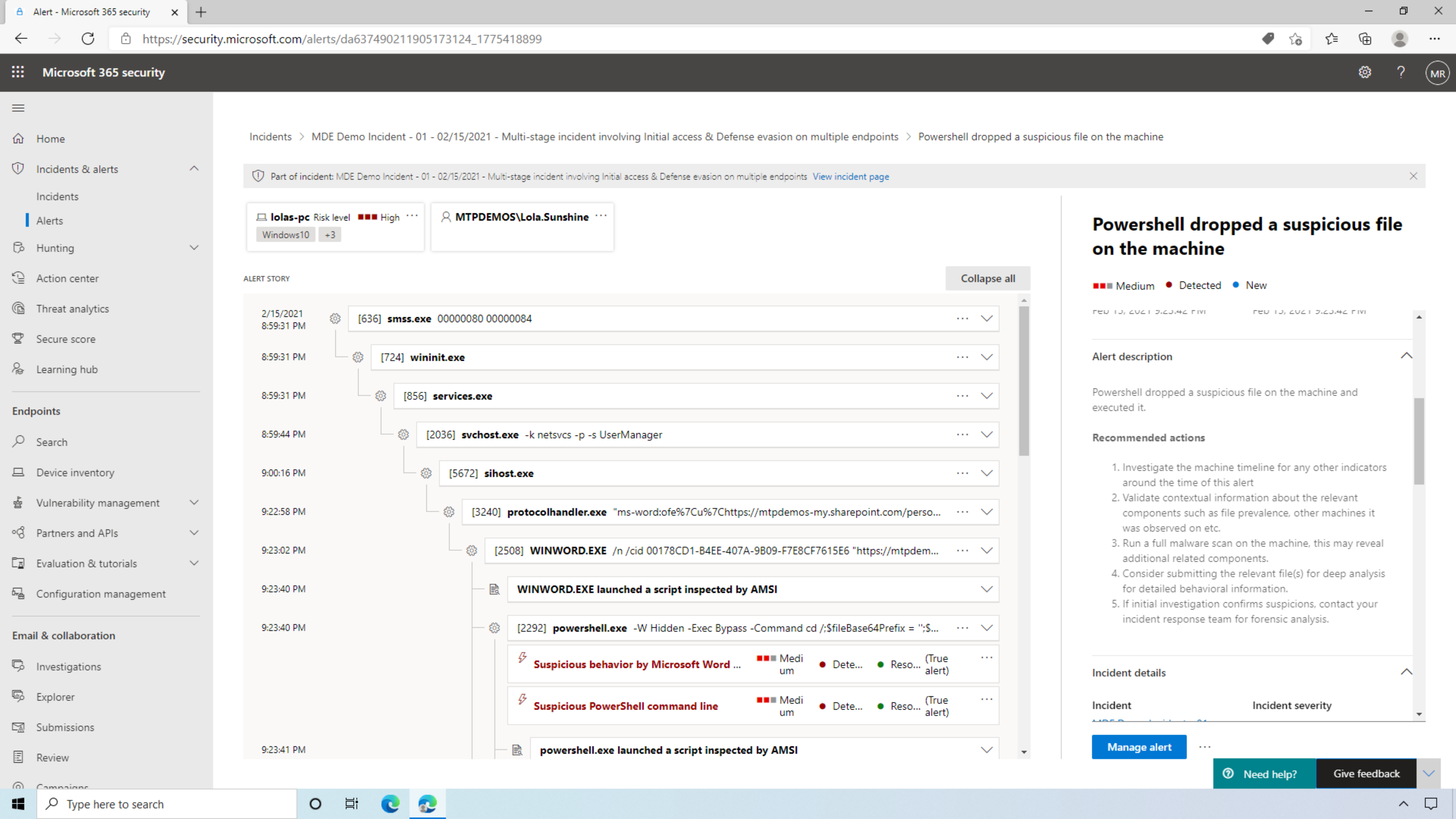
Alert state

Classification	Assigned to
True alert Set Classification	MDATPGlobalReader@MTPDemos.net Unassign

Alert details

Category	MITRE ATT&CK Techniques
Initial access	T1059.001: PowerShell
Detection source	Detection status
EDR	● Detected
Detection technology	Generated on
Behavior	Feb 15, 2021 9:26:30 PM
First activity	Last activity
Feb 15, 2021 9:23:42 PM	Feb 15, 2021 9:23:42 PM

Alert description



Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints > Powershell dropped a suspicious file on the machine

Part of incident: MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints View incident page

lolas-pc Risk level ■■■ High ···
Windows10 +3

MTPDEMOS\Lola.Sunshine ···

ALERT STORY

Collapse all

```
2/15/2021
8:59:31 PM   [636] smss.exe 00000080 00000084
8:59:31 PM     [724] wininit.exe
8:59:31 PM       [856] services.exe
8:59:44 PM         [2036] svchost.exe -k netsvcs -p -s UserManager
9:00:16 PM           [5672] sihost.exe
9:22:58 PM             [3240] protocolhandler.exe "ms-word:ofe%7Cu%7Chttps://mtpdemos-my.sharepoint.com/perso...
9:23:02 PM               [2508] WINWORD.EXE /n /cid 00178CD1-B4EE-407A-9B09-F7E8CF7615E6 "https://mtpdem...
9:23:40 PM                 WINWORD.EXE launched a script inspected by AMSI
9:23:40 PM                 [2292] powershell.exe -W Hidden -Exec Bypass -Command cd /;$fileBase64Prefix = ";$...
                             Suspicious behavior by Microsoft Word ...   ■■■ Medium   ● Dete...   ● Reso...   (True alert)
                             Suspicious PowerShell command line          ■■■ Medium   ● Dete...   ● Reso...   (True alert)
9:23:41 PM                   powershell.exe launched a script inspected by AMSI
```

Powershell dropped a suspicious file on the machine

■■■ Medium ● Detected ● New

Feb 15, 2021 9:23:42 PM   Feb 15, 2021 9:23:42 PM

Alert description

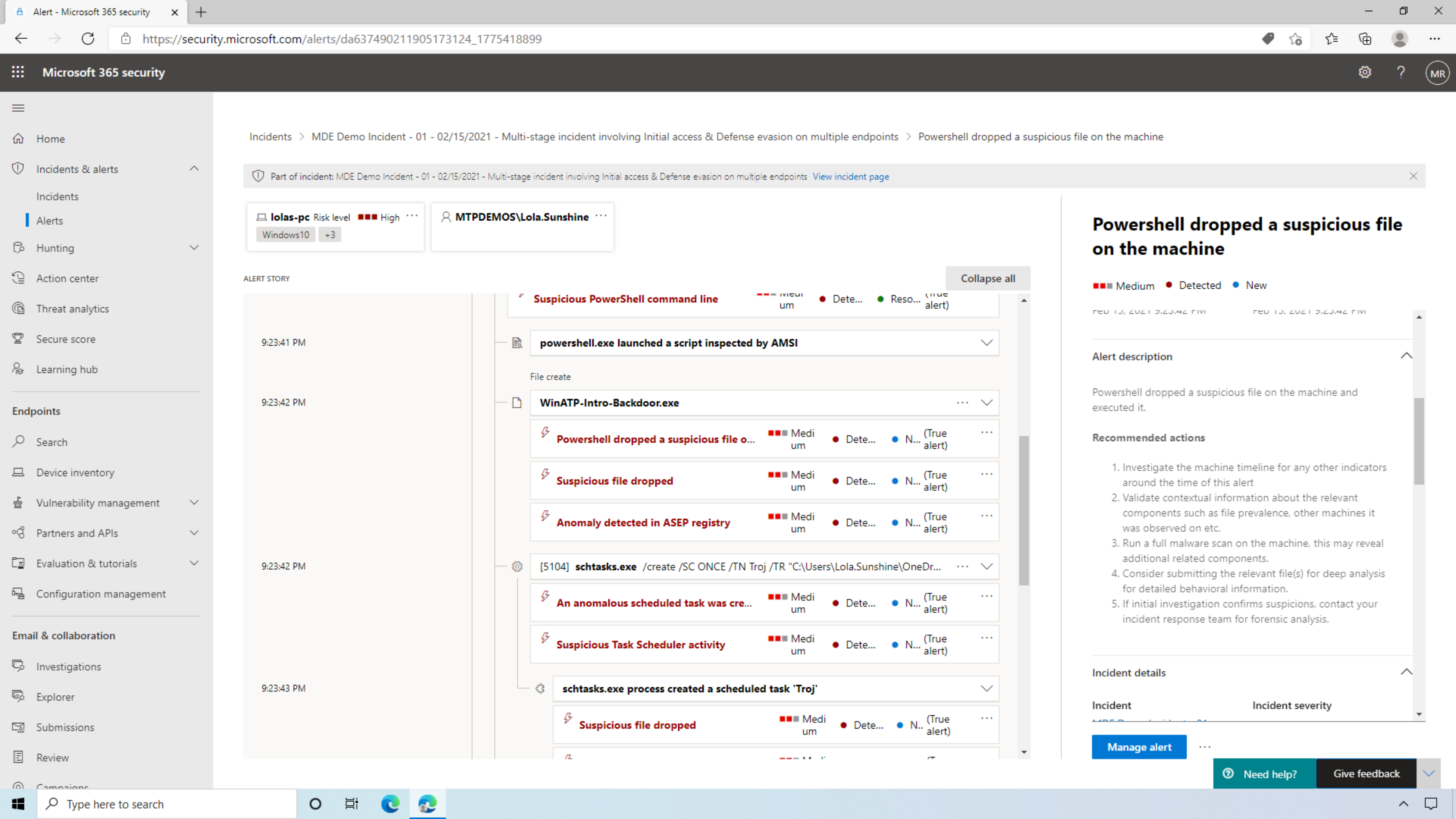
Powershell dropped a suspicious file on the machine and executed it.

Recommended actions

1. Investigate the machine timeline for any other indicators around the time of this alert
2. Validate contextual information about the relevant components such as file prevalence, other machines it was observed on etc.
3. Run a full malware scan on the machine, this may reveal additional related components.
4. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.
5. If initial investigation confirms suspicions, contact your incident response team for forensic analysis.

Incident details

Incident   Incident severity



Alert - Microsoft 365 security

https://security.microsoft.com/alerts/da637490211905173124_1775418899

Microsoft 365 security

Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints > Powershell dropped a suspicious file on the machine

Part of incident: MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints View incident page

lolas-pc Risk level High
Windows10 +3

MTPDEMOS\Lola.Sunshine

ALERT STORY

Collapse all

	Suspicious PowerShell command line	Medium	Dete...	Reso...	(True alert)
9:23:41 PM	powershell.exe launched a script inspected by AMSI				
	File create				
9:23:42 PM	WinATP-Intro-Backdoor.exe				
	Powershell dropped a suspicious file o...	Medium	Dete...	N...	(True alert)
	Suspicious file dropped	Medium	Dete...	N...	(True alert)
	Anomaly detected in ASEP registry	Medium	Dete...	N...	(True alert)
9:23:42 PM	[5104] schtasks.exe /create /SC ONCE /TN Troj /TR "C:\Users\Lola.Sunshine\OneDr...				
	An anomalous scheduled task was cre...	Medium	Dete...	N...	(True alert)
	Suspicious Task Scheduler activity	Medium	Dete...	N...	(True alert)
9:23:43 PM	schtasks.exe process created a scheduled task 'Troj'				
	Suspicious file dropped	Medium	Dete...	N..	(True alert)

Powershell dropped a suspicious file on the machine

Medium ● Detected ● New

Feb 15, 2021 9:23:42 PM Feb 15, 2021 9:23:42 PM

Alert description

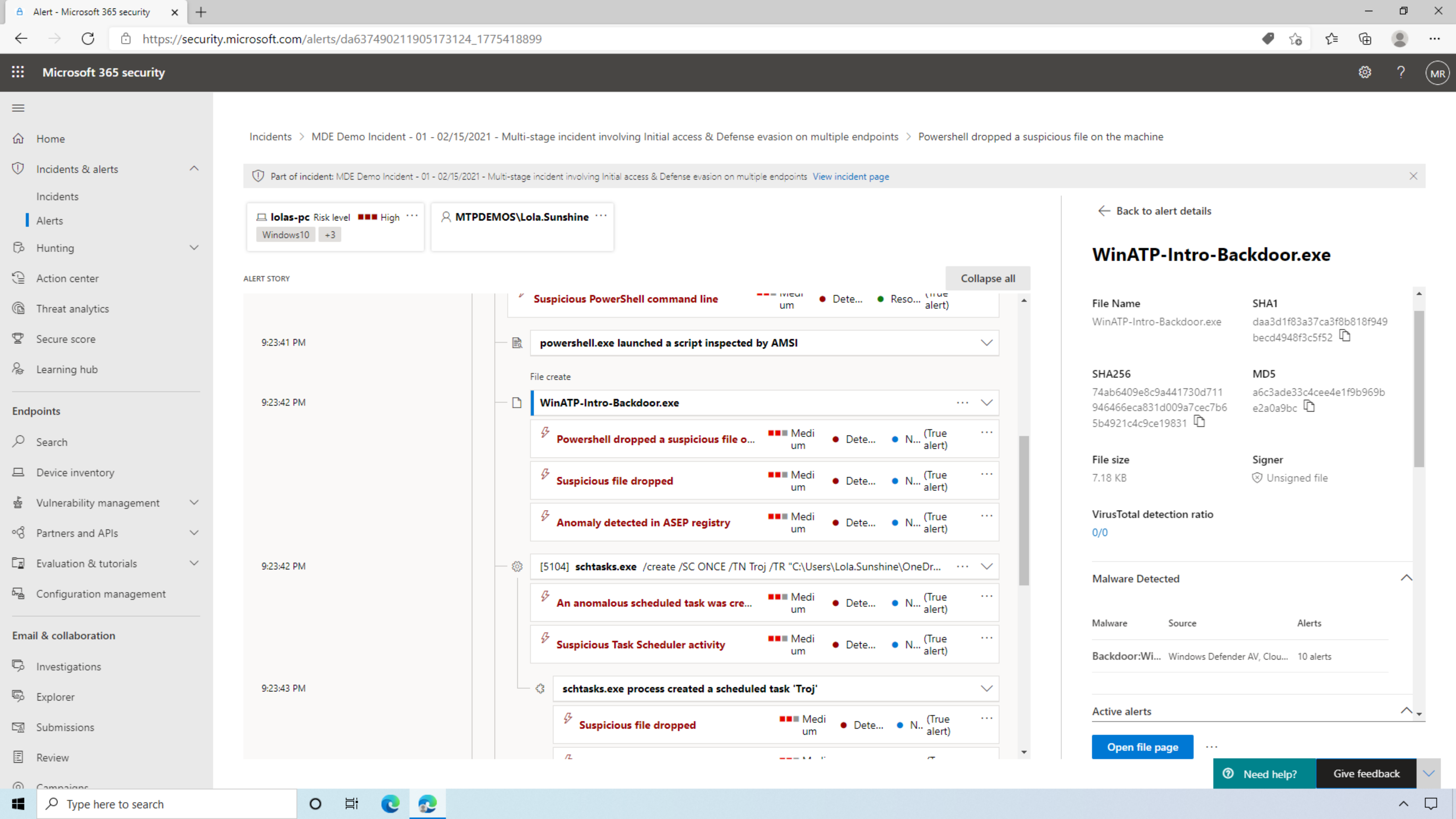
Powershell dropped a suspicious file on the machine and executed it.

Recommended actions

1. Investigate the machine timeline for any other indicators around the time of this alert
2. Validate contextual information about the relevant components such as file prevalence, other machines it was observed on etc.
3. Run a full malware scan on the machine, this may reveal additional related components.
4. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.
5. If initial investigation confirms suspicions, contact your incident response team for forensic analysis.

Incident details

Incident Incident severity



Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints > Powershell dropped a suspicious file on the machine

Part of incident: MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints View incident page

lolas-pc Risk level High
Windows10 +3

MTPDEMOS\Lola.Sunshine

ALERT STORY

Suspicious PowerShell command line — Medium — Dete... — Reso... — (True alert)

9:23:41 PM powershell.exe launched a script inspected by AMSI

File create

9:23:42 PM WinATP-Intro-Backdoor.exe

Alert	Severity	Status		Classification
Powershell dropped a suspicious file o...	Medium	Dete...	N...	(True alert)
Suspicious file dropped	Medium	Dete...	N...	(True alert)
Anomaly detected in ASEP registry	Medium	Dete...	N...	(True alert)

9:23:42 PM [5104] schtasks.exe /create /SC ONCE /TN Troj /TR "C:\Users\Lola.Sunshine\OneDr...

Alert	Severity	Status		Classification
An anomalous scheduled task was cre...	Medium	Dete...	N...	(True alert)
Suspicious Task Scheduler activity	Medium	Dete...	N...	(True alert)

9:23:43 PM schtasks.exe process created a scheduled task 'Troj'

Alert	Severity	Status		Classification
Suspicious file dropped	Medium	Dete...	N..	(True alert)

WinATP-Intro-Backdoor.exe

File Name: WinATP-Intro-Backdoor.exe

SHA1: daa3d1f83a37ca3f8b818f949becd4948f3c5f52

SHA256: 74ab6409e8c9a441730d711946466eca831d009a7cec7b65b4921c4c9ce19831

MD5: a6c3ade33c4cee4e1f9b969be2a0a9bc

File size: 7.18 KB

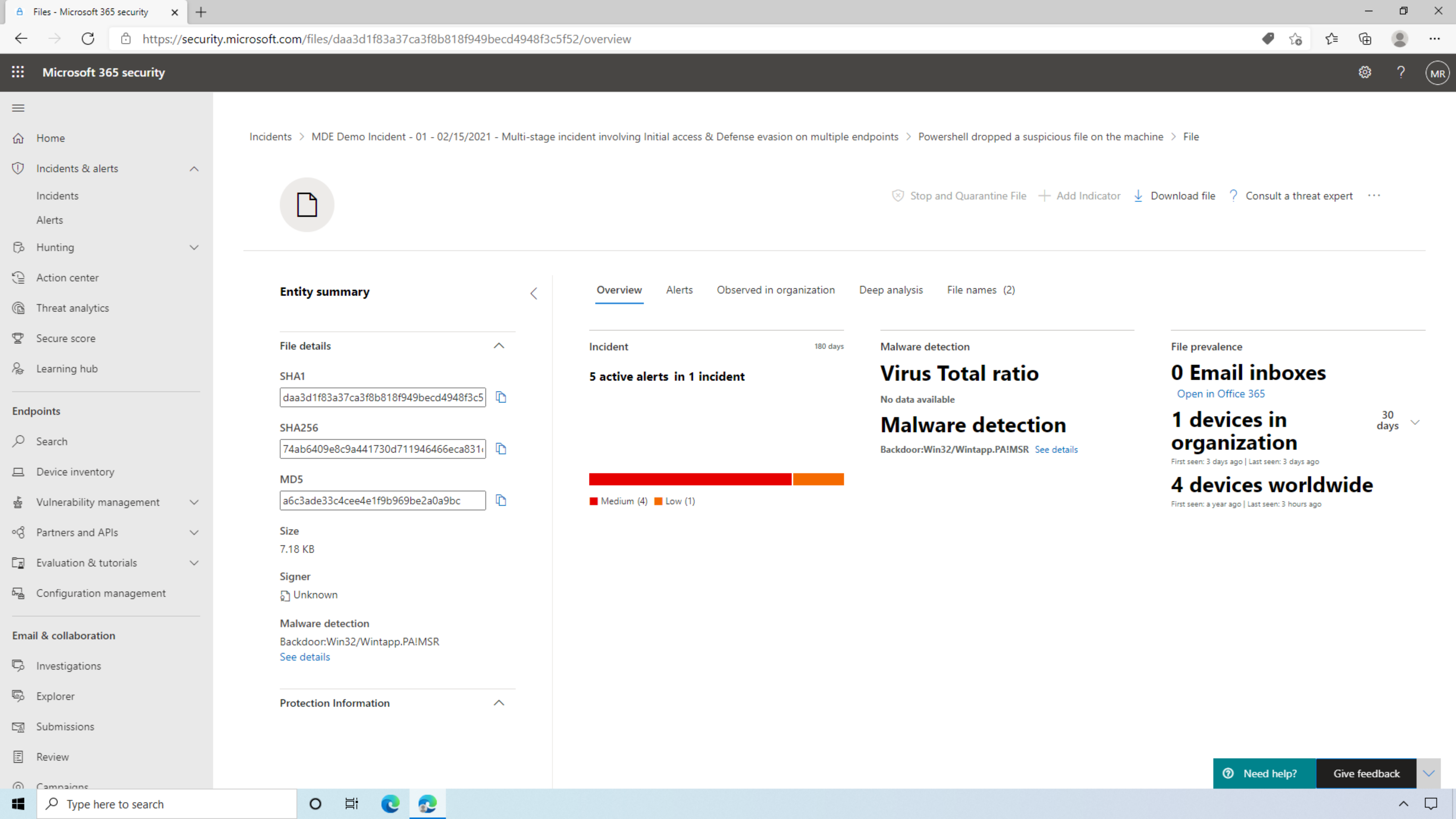
Signer: Unsigned file

VirusTotal detection ratio: 0/0

Malware Detected

Malware	Source	Alerts
Backdoor:Wi...	Windows Defender AV, Clou...	10 alerts

Active alerts



Files - Microsoft 365 security

https://security.microsoft.com/files/daa3d1f83a37ca3f8b818f949becd4948f3c5f52/overview

Microsoft 365 security

Home

Incidents & alerts

Incidents

Alerts

Hunting

Action center

Threat analytics

Secure score

Learning hub

Endpoints

Search

Device inventory

Vulnerability management

Partners and APIs

Evaluation & tutorials

Configuration management

Email & collaboration

Investigations

Explorer

Submissions

Review

Campaigns

Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints > Powershell dropped a suspicious file on the machine > File

Stop and Quarantine File | Add Indicator | Download file | Consult a threat expert | ···

Entity summary

File details

SHA1
daa3d1f83a37ca3f8b818f949becd4948f3c5

SHA256
74ab6409e8c9a441730d711946466eca831

MD5
a6c3ade33c4cee4e1f9b969be2a0a9bc

Size
7.18 KB

Signer
Unknown

Malware detection
Backdoor:Win32/Wintapp.PA!MSR
See details

Protection Information

Overview | Alerts | Observed in organization | Deep analysis | File names (2)

Incident — 180 days

5 active alerts in 1 incident

🟥 Medium (4) 🟧 Low (1)

Malware detection

Virus Total ratio

No data available

Malware detection

Backdoor:Win32/Wintapp.PA!MSR See details

File prevalence

0 Email inboxes

Open in Office 365

1 devices in organization — 30 days

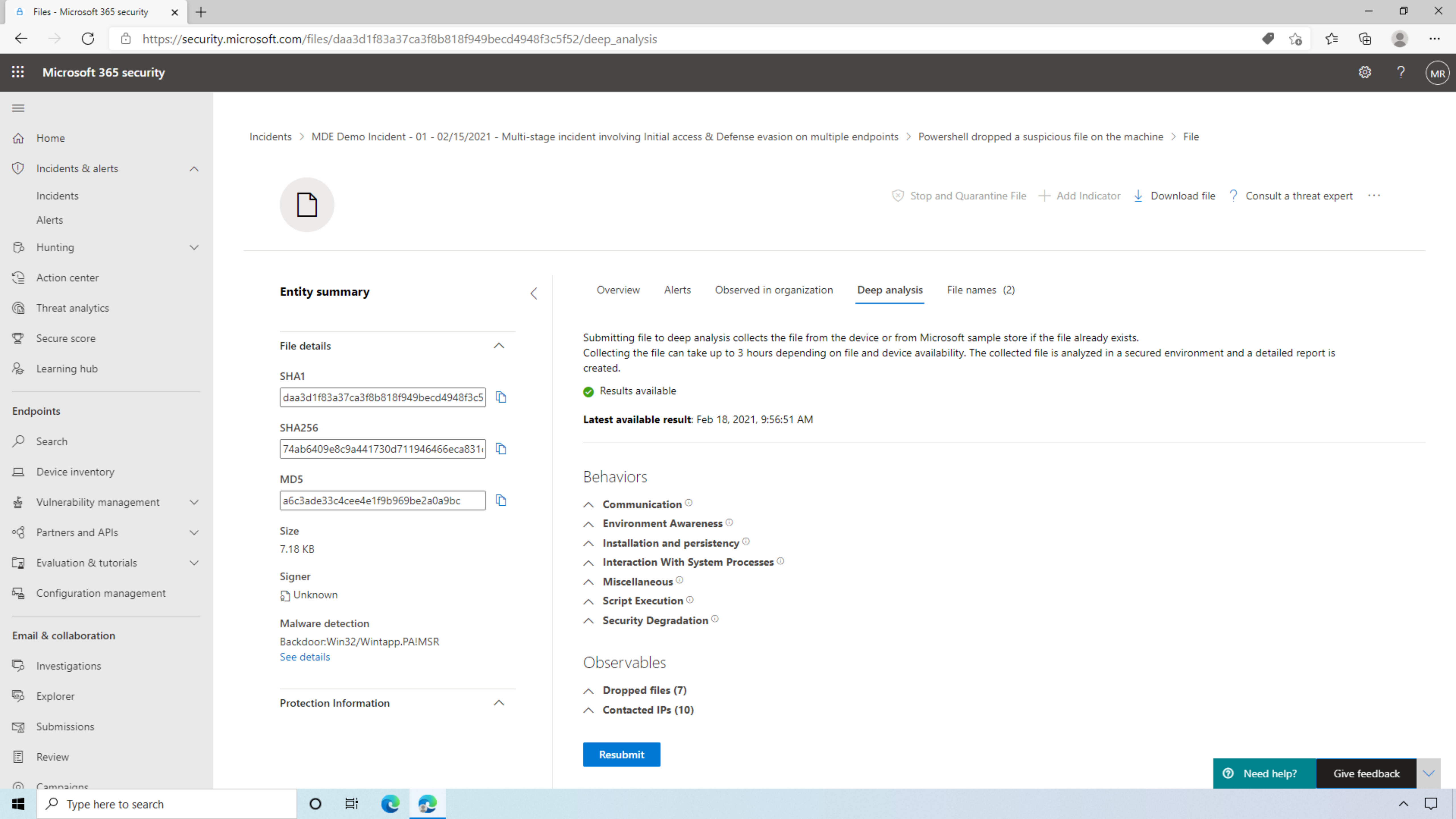
First seen: 3 days ago | Last seen: 3 days ago

4 devices worldwide

First seen: a year ago | Last seen: 3 hours ago

Need help? | Give feedback

Type here to search



File details

SHA1: daa3d1f83a37ca3f8b818f949becd4948f3c5

SHA256: 74ab6409e8c9a441730d711946466eca831

MD5: a6c3ade33c4cee4e1f9b969be2a0a9bc

Size: 7.18 KB

Signer: Unknown

Malware detection: Backdoor:Win32/Wintapp.PA!MSR

See details

Protection Information

Submitting file to deep analysis collects the file from the device or from Microsoft sample store if the file already exists.
Collecting the file can take up to 3 hours depending on file and device availability. The collected file is analyzed in a secured environment and a detailed report is created.

✓ Results available

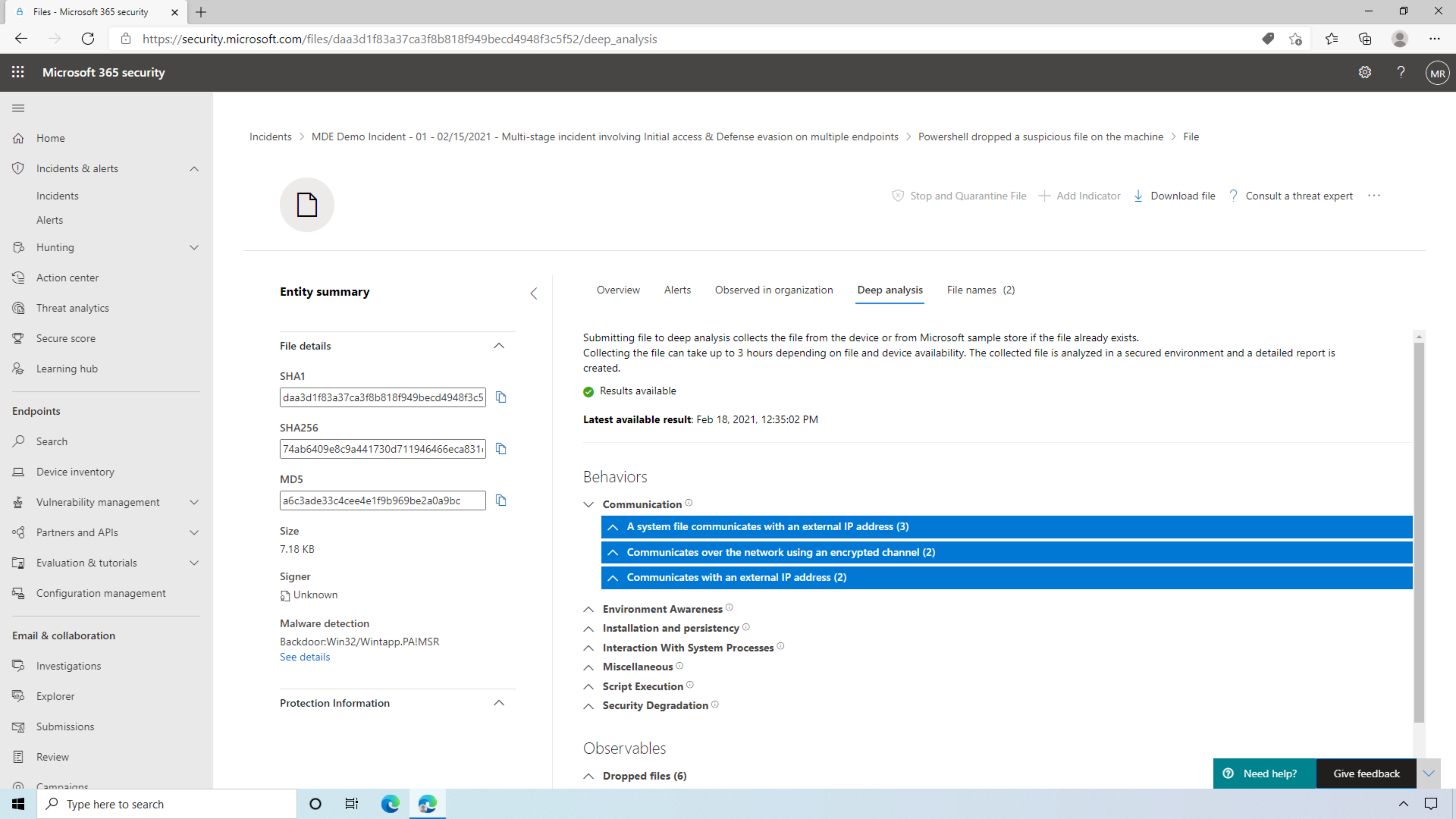
Latest available result: Feb 18, 2021, 9:56:51 AM

Behaviors

- Communication
- Environment Awareness
- Installation and persistency
- Interaction With System Processes
- Miscellaneous
- Script Execution
- Security Degradation

Observables

- Dropped files (7)
- Contacted IPs (10)



Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints > Powershell dropped a suspicious file on the machine > File

Entity summary

File details

SHA1: daa3d1f83a37ca3f8b818f949becd4948f3c5

SHA256: 74ab6409e8c9a441730d711946466eca831

MD5: a6c3ade33c4cee4e1f9b969be2a0a9bc

Size: 7.18 KB

Signer: Unknown

Malware detection: Backdoor:Win32/Wintapp.PA!MSR

See details

Protection Information

Submitting file to deep analysis collects the file from the device or from Microsoft sample store if the file already exists.
Collecting the file can take up to 3 hours depending on file and device availability. The collected file is analyzed in a secured environment and a detailed report is created.

✓ Results available

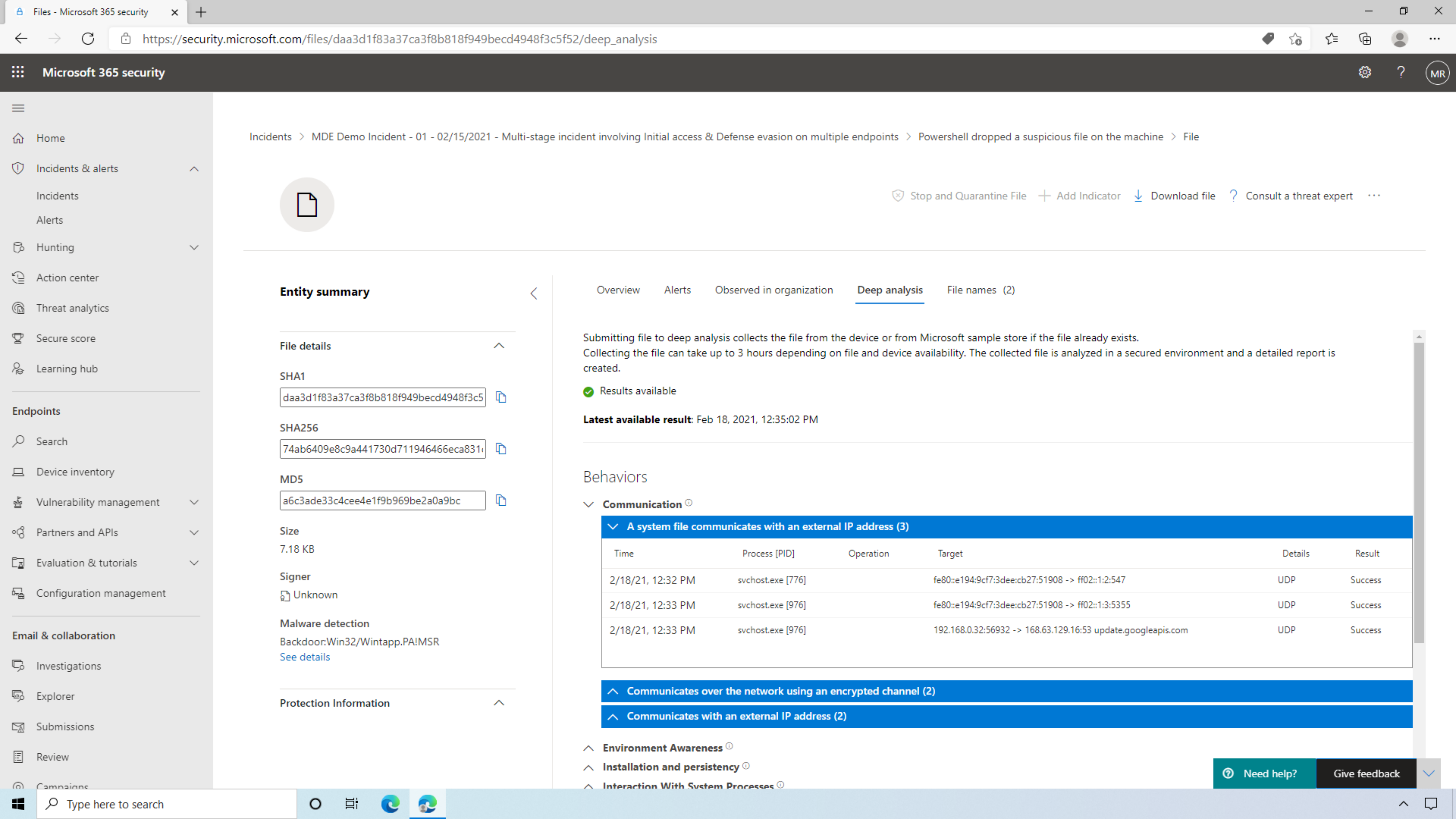
Latest available result: Feb 18, 2021, 12:35:02 PM

Behaviors

- **Communication**
  - A system file communicates with an external IP address (3)
  - Communicates over the network using an encrypted channel (2)
  - Communicates with an external IP address (2)
- **Environment Awareness**
- **Installation and persistency**
- **Interaction With System Processes**
- **Miscellaneous**
- **Script Execution**
- **Security Degradation**

Observables

- **Dropped files (6)**



Incidents > MDE Demo Incident - 01 - 02/15/2021 - Multi-stage incident involving Initial access & Defense evasion on multiple endpoints > Powershell dropped a suspicious file on the machine > File

Entity summary

File details

SHA1
daa3d1f83a37ca3f8b818f949becd4948f3c5

SHA256
74ab6409e8c9a441730d711946466eca831

MD5
a6c3ade33c4cee4e1f9b969be2a0a9bc

Size
7.18 KB

Signer
Unknown

Malware detection
Backdoor:Win32/Wintapp.PA!MSR
See details

Protection Information

Submitting file to deep analysis collects the file from the device or from Microsoft sample store if the file already exists.
Collecting the file can take up to 3 hours depending on file and device availability. The collected file is analyzed in a secured environment and a detailed report is created.

✓ Results available

Latest available result: Feb 18, 2021, 12:35:02 PM

Behaviors

Communication

A system file communicates with an external IP address (3)

Time	Process [PID]	Operation	Target	Details	Result
2/18/21, 12:32 PM	svchost.exe [776]		fe80::e194:9cf7:3dee:cb27:51908 -> ff02::1:2:547	UDP	Success
2/18/21, 12:33 PM	svchost.exe [976]		fe80::e194:9cf7:3dee:cb27:51908 -> ff02::1:3:5355	UDP	Success
2/18/21, 12:33 PM	svchost.exe [976]		192.168.0.32:56932 -> 168.63.129.16:53 update.googleapis.com	UDP	Success

Communicates over the network using an encrypted channel (2)

Communicates with an external IP address (2)

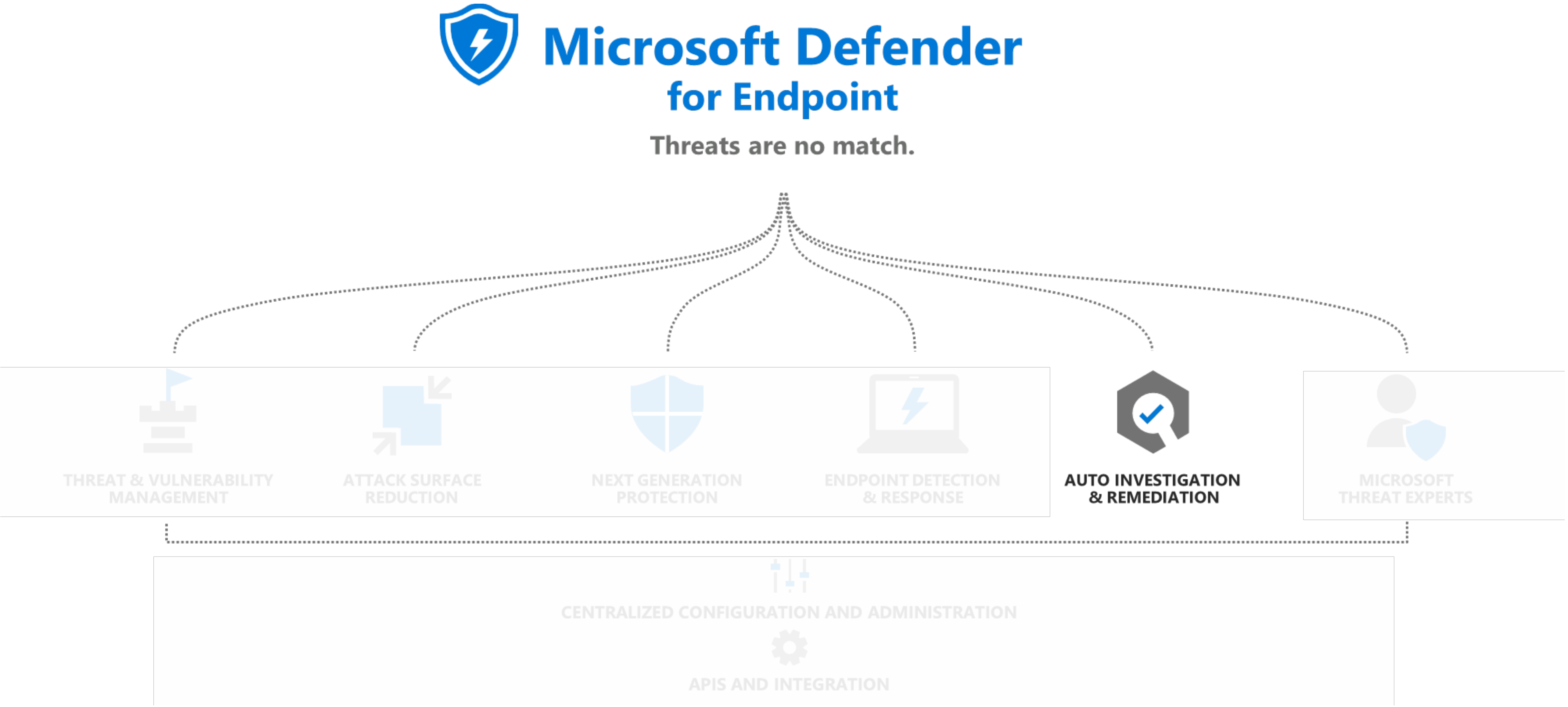
Environment Awareness

Installation and persistency

Interaction With System Processes

Microsoft Defender for Endpoint

Auto Investigation & Remediation

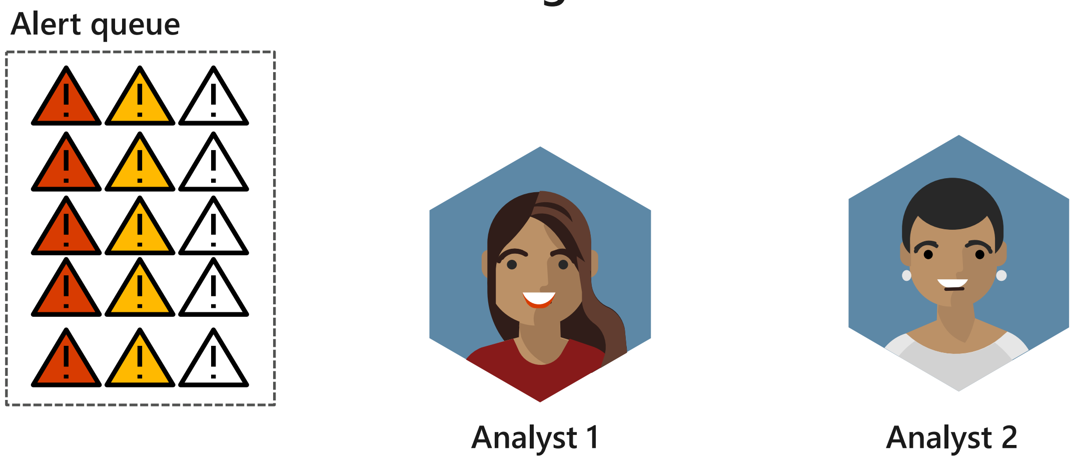

Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION

Auto Investigation & Remediation

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



Auto Investigation & Remediation

What is it?

✓

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:

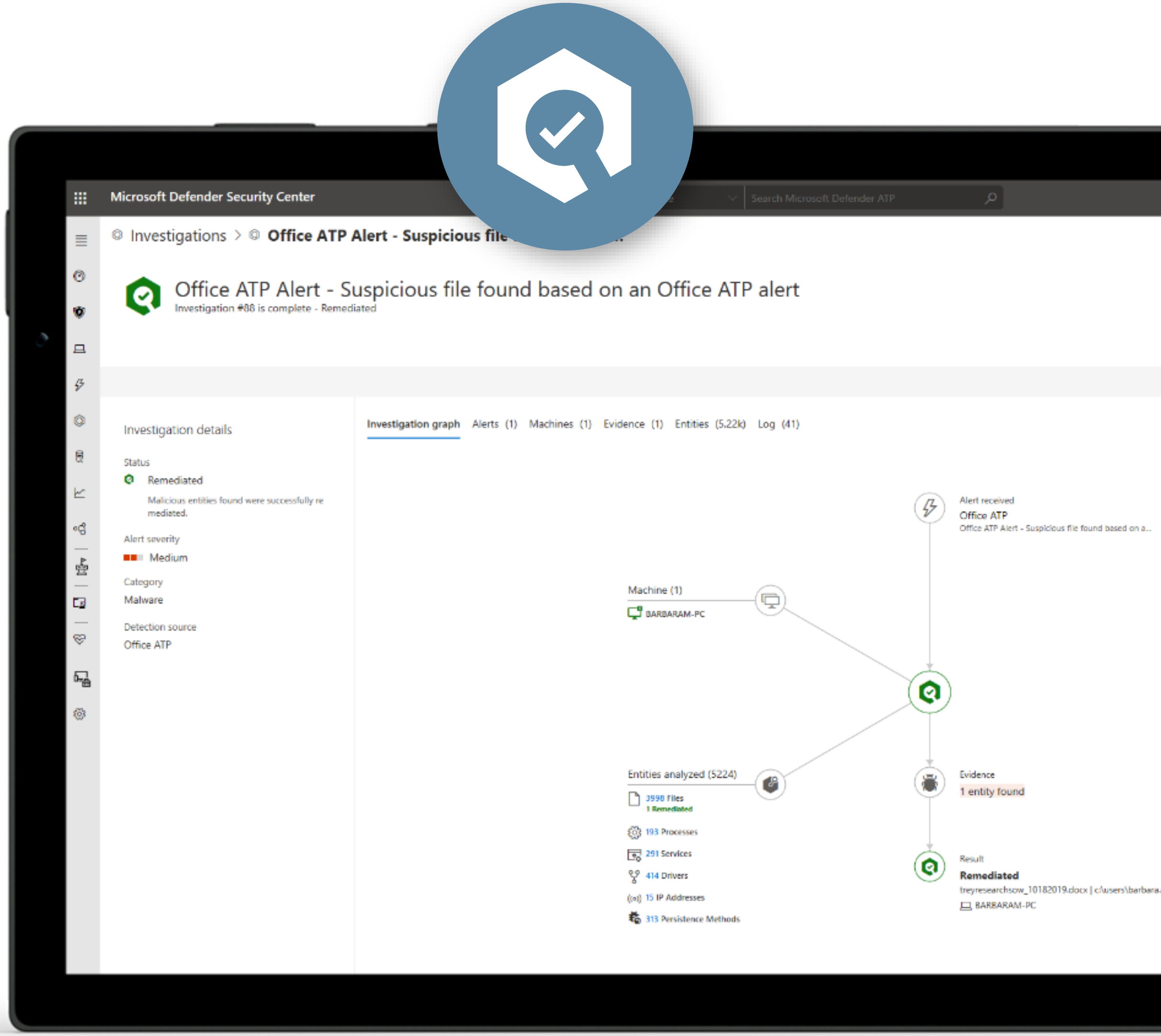
1. Determining whether the threat requires action
2. Performing necessary remediation actions
3. Deciding what additional investigations should be next
4. Repeating this as many times as necessary for every alert

Microsoft Defender for Endpoint

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

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 remediated.

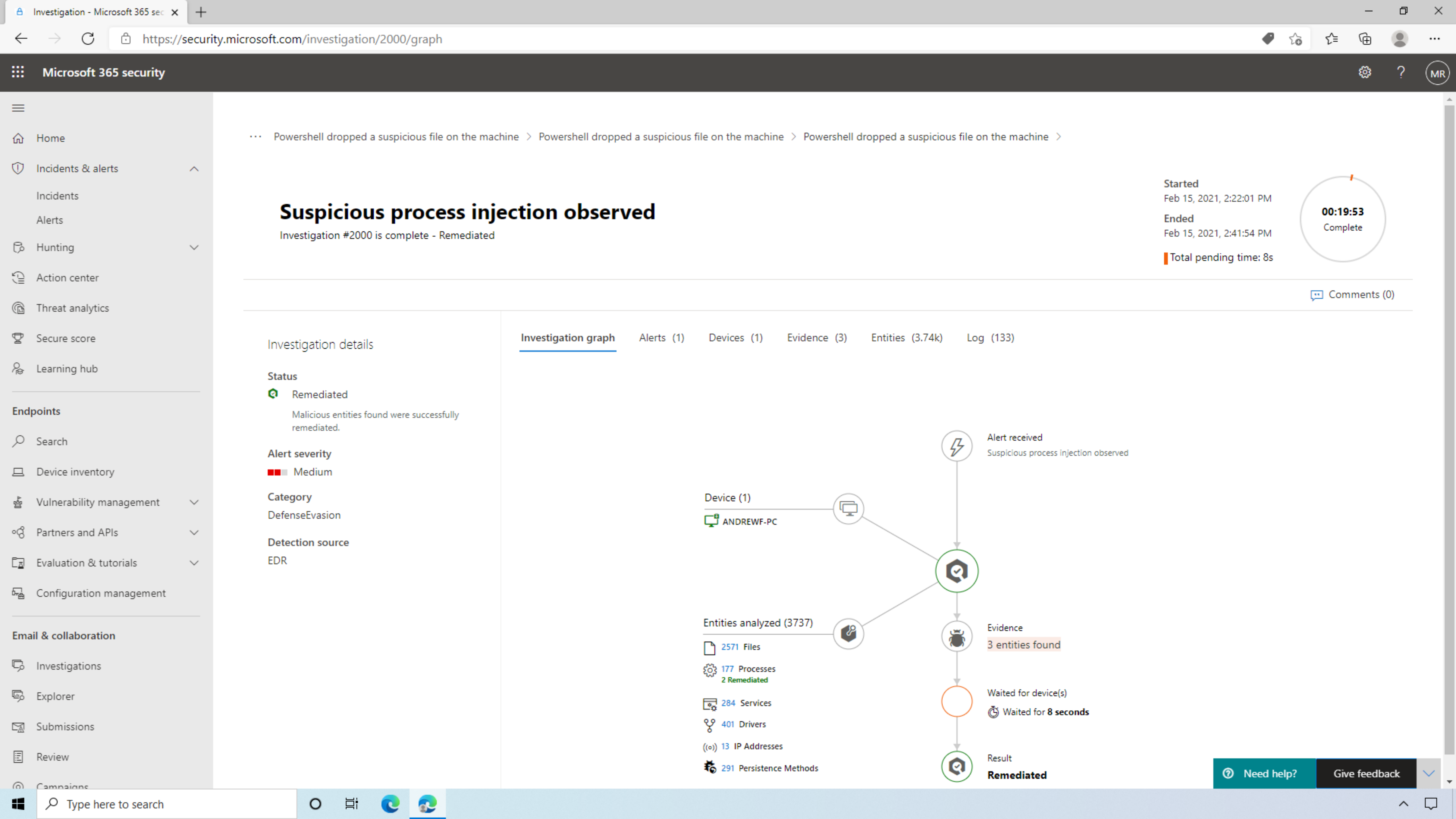
Alert severity
Medium

Category
Malware

Detection source
Office ATP

Investigation graph | Alerts (1) | Machines (1) | Evidence (1) | Entities (5.22k) | Log (41)

Demo.



··· Powershell dropped a suspicious file on the machine > Powershell dropped a suspicious file on the machine > Powershell dropped a suspicious file on the machine >

Suspicious process injection observed

Investigation #2000 is complete - Remediated

Started
Feb 15, 2021, 2:22:01 PM
Ended
Feb 15, 2021, 2:41:54 PM
Total pending time: 8s

00:19:53
Complete

Comments (0)

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Medium

Category
DefenseEvasion

Detection source
EDR

Alert received
Suspicious process injection observed

Device (1)
ANDREWF-PC

Entities analyzed (3737)
2571 Files
177 Processes
2 Remediated
284 Services
401 Drivers
13 IP Addresses
291 Persistence Methods

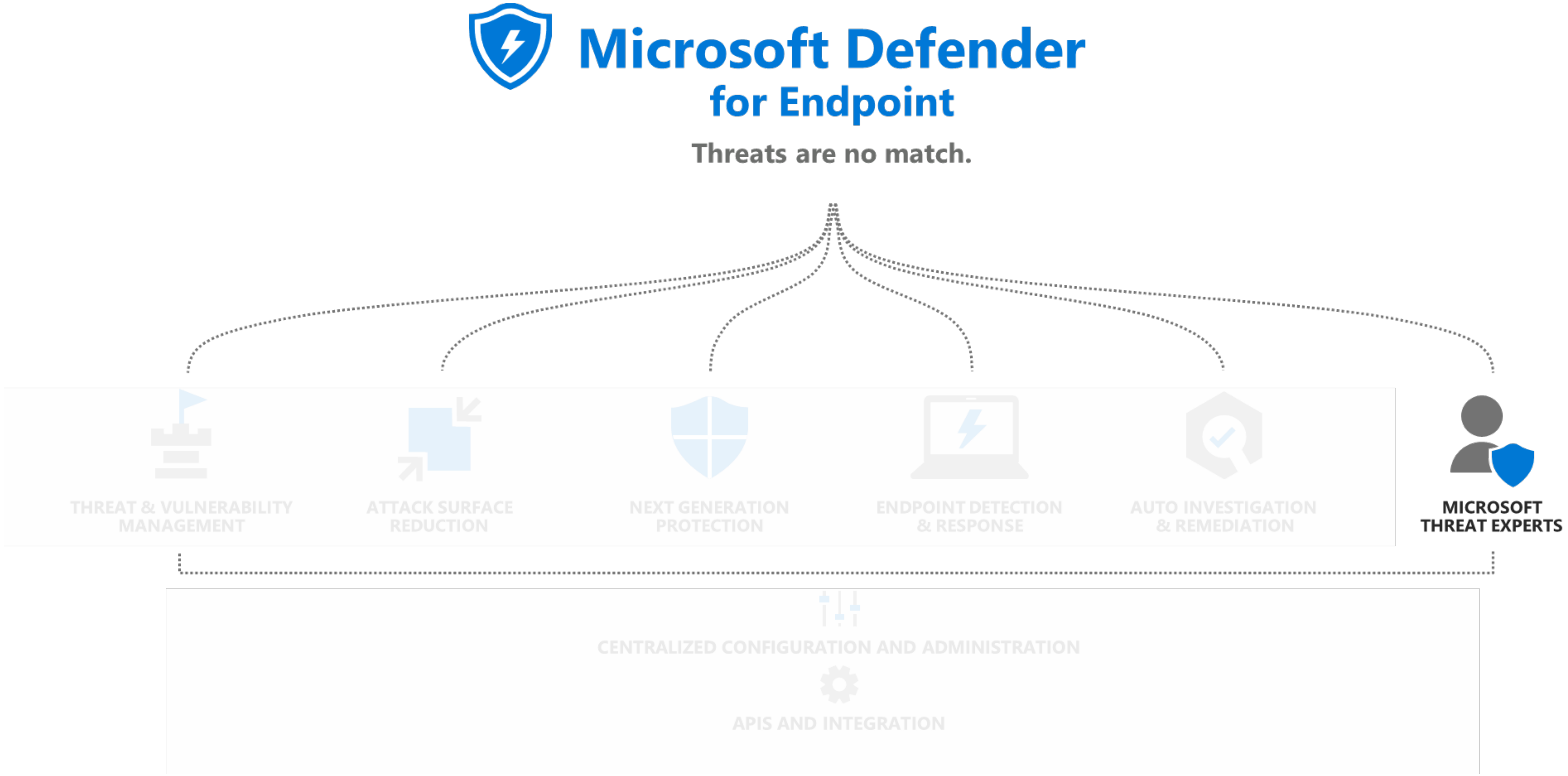
Evidence
3 entities found

Waited for device(s)
Waited for **8 seconds**

Result
Remediated

Microsoft Defender for Endpoint

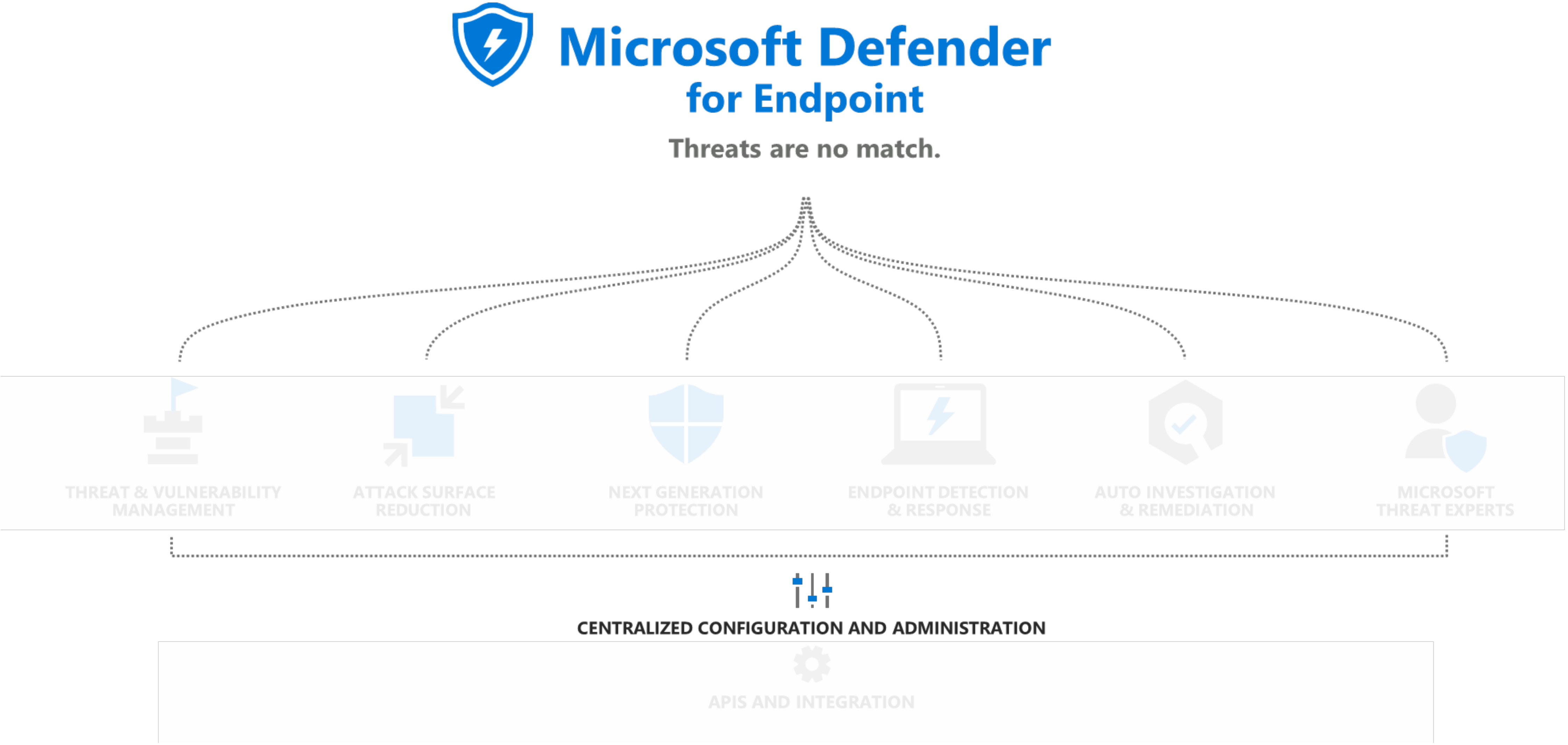
Microsoft Threat Experts


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

Demo.

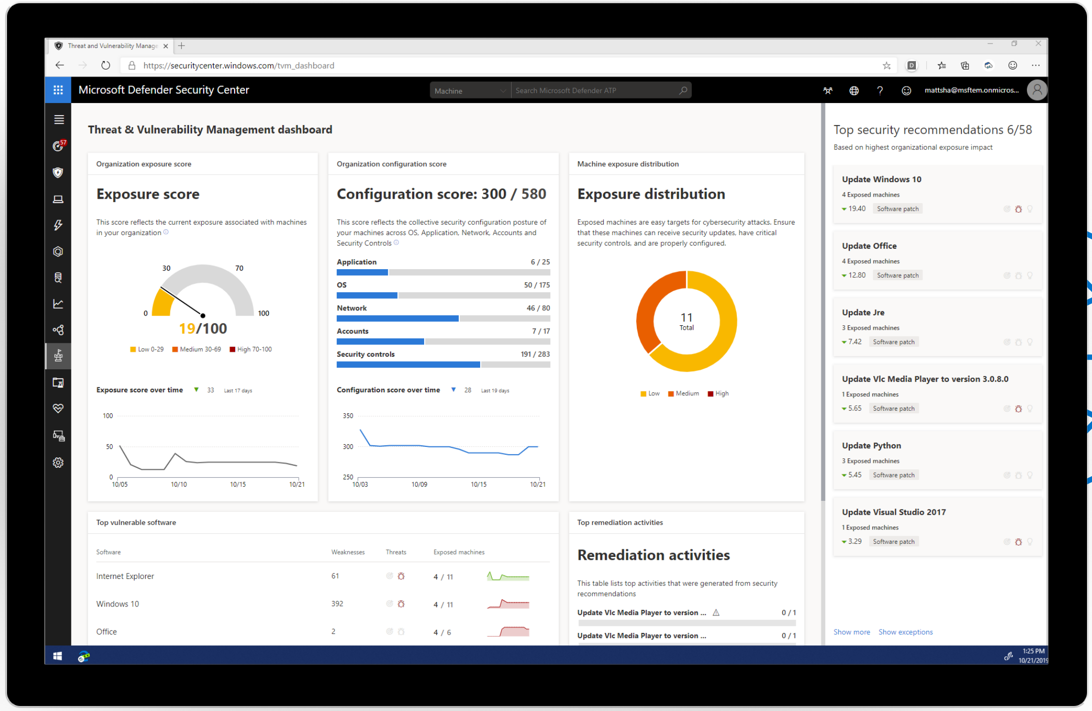
Microsoft Defender for Endpoint

Centralized Configuration and Administration


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

Centralized Configuration and Administration

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

19/100

Exposure score over time ▼ 33 Last 17 days

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 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

Top vulnerable software

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

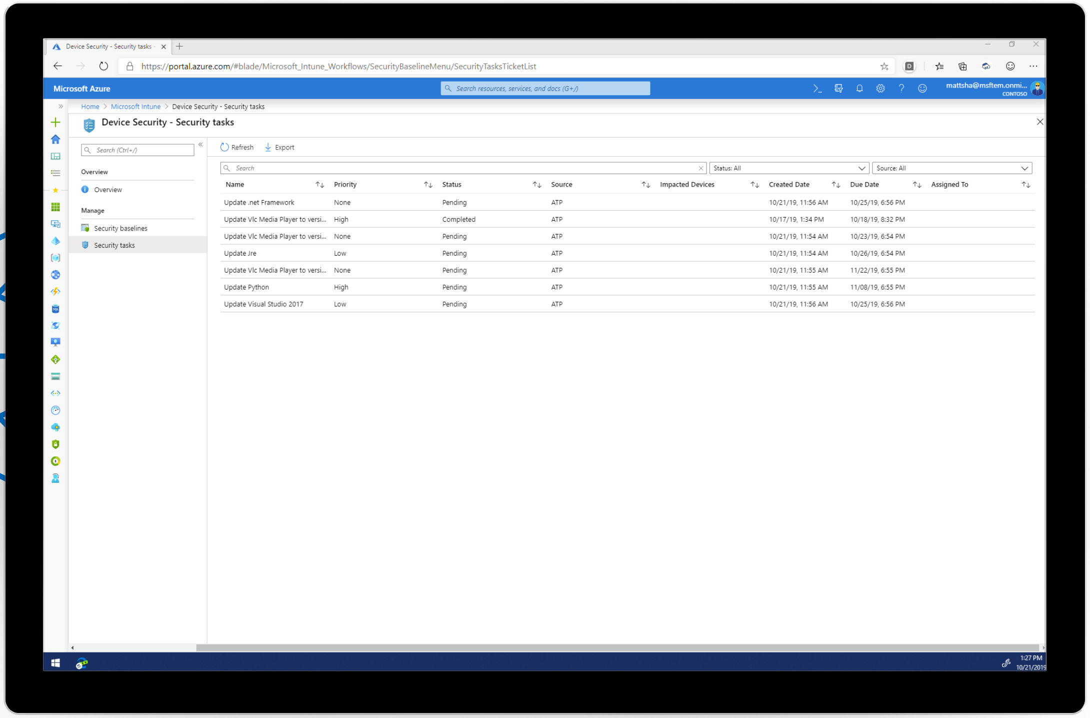
Top remediation activities

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

1:25 PM 10/21/2019



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

Device Security - Security tasks

Search (Ctrl+/)

Overview
- Overview

Manage
- Security baselines
- Security tasks

Refresh | Export

Search | 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	

1:27 PM 10/21/2019

Microsoft Defender for Endpoint

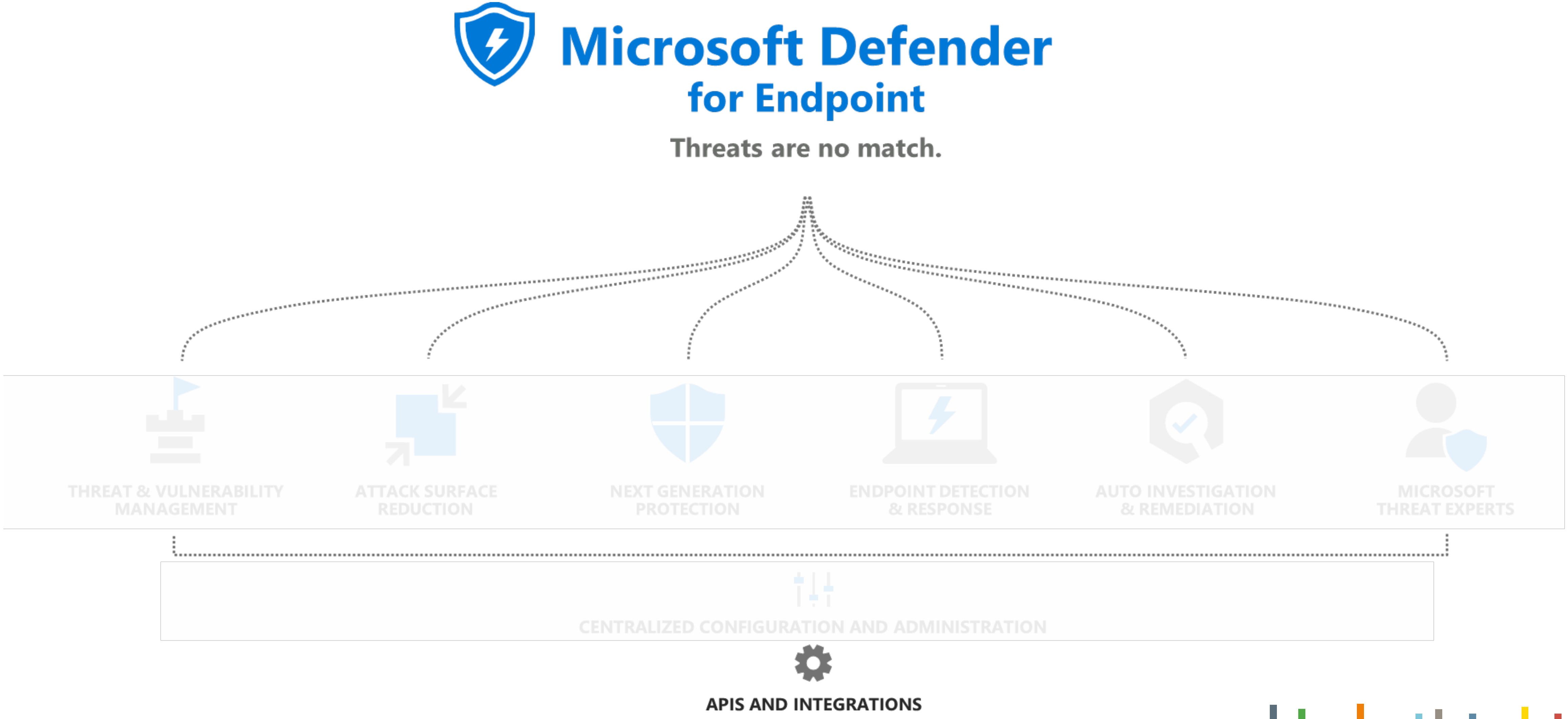
Policy Assessment

Microsoft Endpoint Manager

Policy Enforcement

Microsoft Defender for Endpoint

APIs and Integrations



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 INTEGRATIONS

Microsoft Defender for Endpoint

Reference Architecture

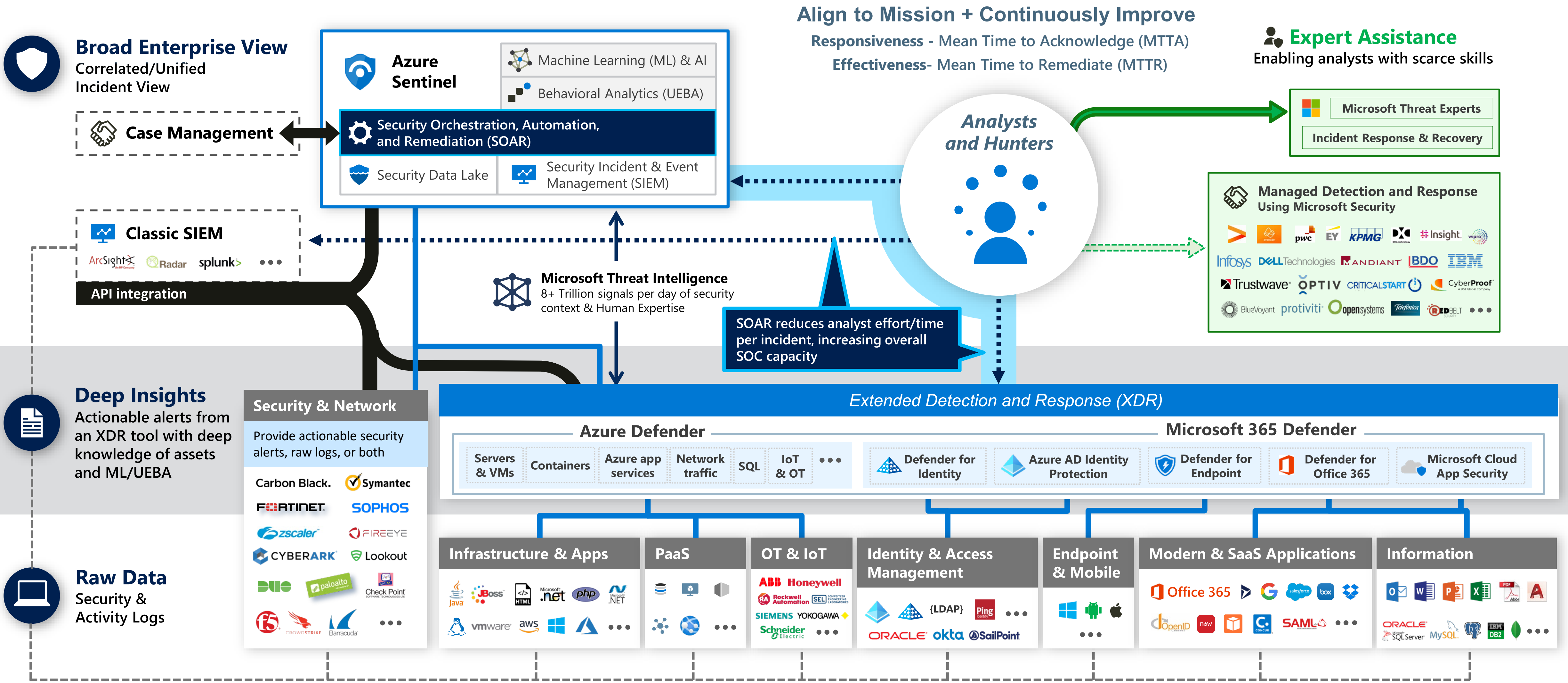
Legend

▬ ▬ ▬	Event Log Based Monitoring	⇢	Outsourcing
▪▪▪▪▪	Investigation & Proactive Hunting	➡	Consulting and Escalation
		▬	Native Resource Monitoring

Microsoft

May 2021 – https://aka.ms/MCRA

BECHTLE



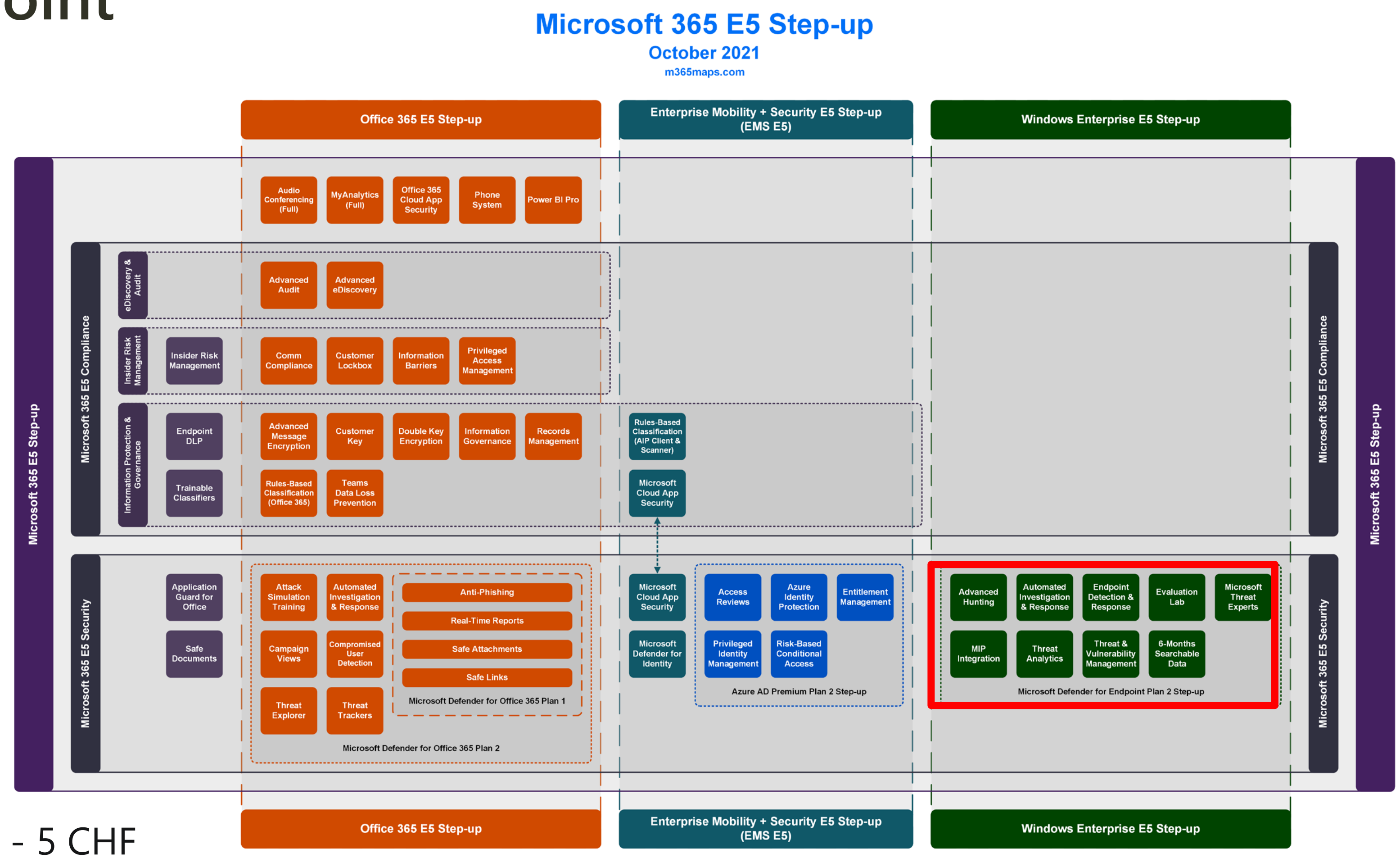
Licensing.

Microsoft Defender for Endpoint

P2 and Servers

End-users *(Per user per month, up to 5 devices)*

- **M365 E5** – 62.70 CHF
- **M365 E5 Security** – 9.50 CHF
- **Windows E5** – 10.20 CHF
- **Microsoft Defender for Endpoint P2** – 5 CHF


Microsoft 365 E5 Step-up
October 2021
m365maps.com
Office 365 E5 Step-up
Enterprise Mobility + Security E5 Step-up (EMS E5)
Windows Enterprise E5 Step-up
Microsoft 365 E5 Step-up
Microsoft 365 E5 Compliance
Microsoft 365 E5 Security
Audio Conferencing (Full)
MyAnalytics (Full)
Office 365 Cloud App Security
Phone System
Power BI Pro
eDiscovery & Audit
Advanced Audit
Advanced eDiscovery
Insider Risk Management
Insider Risk Management
Comm Compliance
Customer Lockbox
Information Barriers
Privileged Access Management
Information Protection & Governance
Endpoint DLP
Trainable Classifiers
Advanced Message Encryption
Customer Key
Double Key Encryption
Information Governance
Records Management
Rules-Based Classification (Office 365)
Teams Data Loss Prevention
Rules-Based Classification (AIP Client & Scanner)
Microsoft Cloud App Security
Application Guard for Office
Safe Documents
Attack Simulation Training
Automated Investigation & Response
Campaign Views
Compromised User Detection
Threat Explorer
Threat Trackers
Anti-Phishing
Real-Time Reports
Safe Attachments
Safe Links
Microsoft Defender for Office 365 Plan 1
Microsoft Defender for Office 365 Plan 2
Microsoft Cloud App Security
Microsoft Defender for Identity
Access Reviews
Azure Identity Protection
Entitlement Management
Privileged Identity Management
Risk-Based Conditional Access
Azure AD Premium Plan 2 Step-up
Advanced Hunting
Automated Investigation & Response
Endpoint Detection & Response
Evaluation Lab
Microsoft Threat Experts
MIP Integration
Threat Analytics
Threat & Vulnerability Management
6-Months Searchable Data
Microsoft Defender for Endpoint Plan 2 Step-up
Office 365 E5 Step-up
Enterprise Mobility + Security E5 Step-up (EMS E5)
Windows Enterprise E5 Step-up

Servers *(Per server per month)*

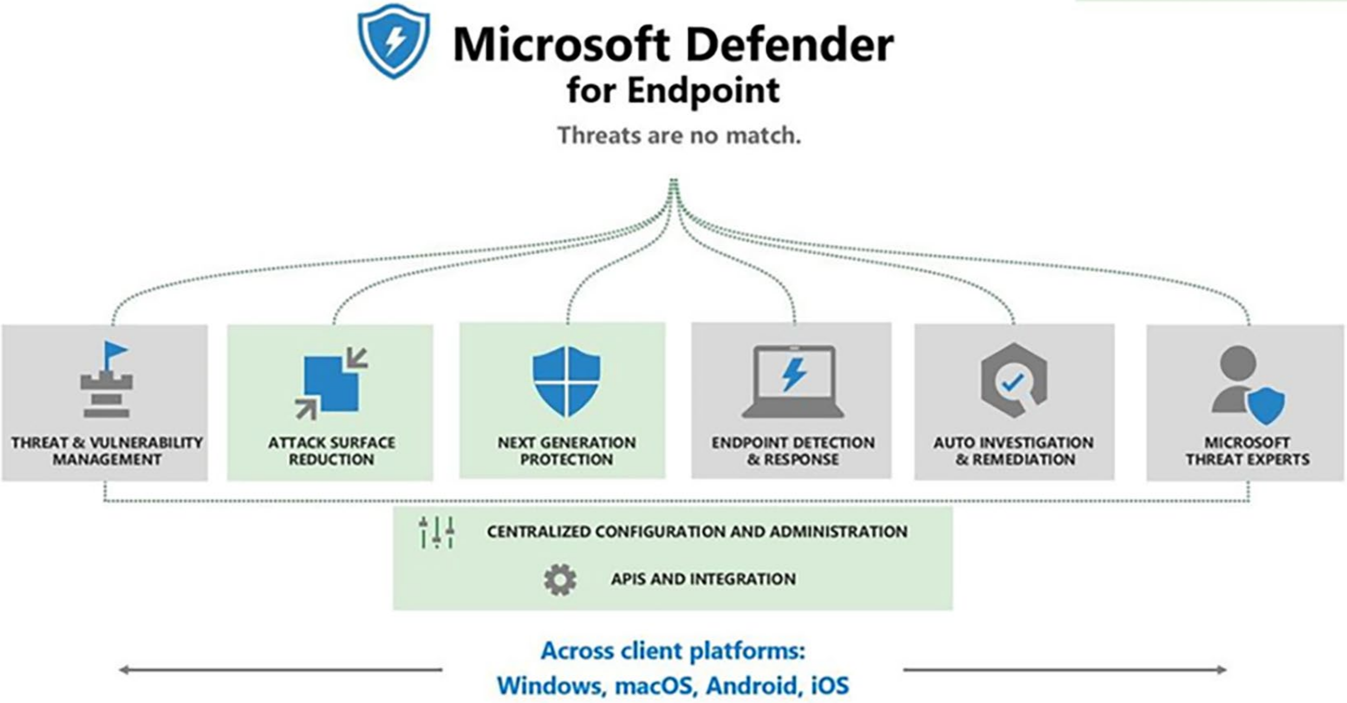
- **Microsoft Defender for Endpoint for Servers*** - 5 CHF
- **Microsoft Defender for Cloud** – *Azure Consumption*

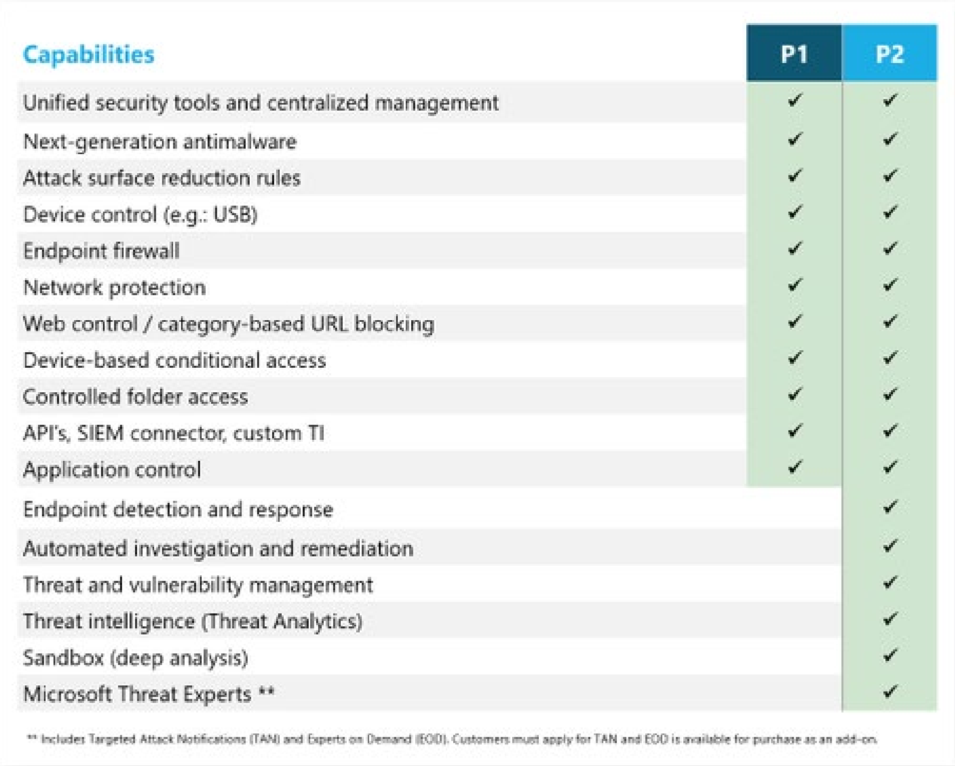
* *Available after min. 50 MDE or WE5 or M365 E5/Security licenses purchased*

Microsoft Defender for Endpoint

P1 vs P2

Plan 1 capabilities


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
Across client platforms:
Windows, macOS, Android, iOS



Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL blocking	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
API's, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts **		✓

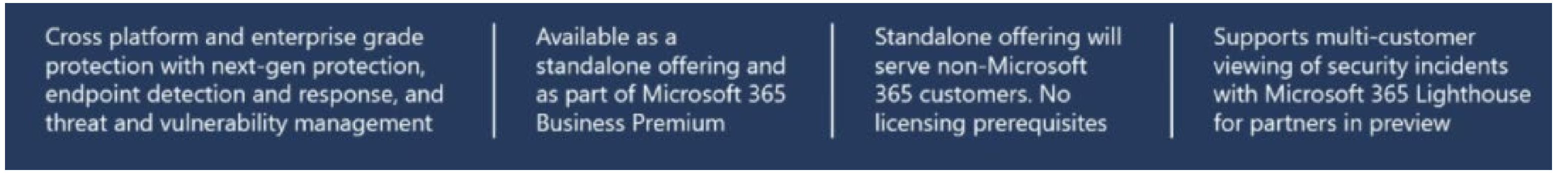
** Includes Targeted Attack Notifications (TAN) and Experts on Demand (EOD). Customers must apply for TAN and EOD is available for purchase as an add-on.

- **Microsoft Defender for Endpoint P1** – 3 CHF
- **M365 E3** – 28 CHF*

* Q1 2022

Microsoft Defender for Business

Enterprise-grade security for SMEs!



Cross platform and enterprise grade protection with next-gen protection, endpoint detection and response, and threat and vulnerability management

Available as a standalone offering and as part of Microsoft 365 Business Premium

Standalone offering will serve non-Microsoft 365 customers. No licensing prerequisites

Supports multi-customer viewing of security incidents with Microsoft 365 Lighthouse for partners in preview

Customer size	**< 300 seats**	**> 300 seats**	
Endpoint capabilities / SKU	**Microsoft Defender for Business**	**Microsoft Defender for Endpoint Plan 1**	**Microsoft Defender for Endpoint Plan 2**
Centralized management	✓	✓	✓
Simplified client configuration	✓		
Threat and Vulnerability Management	✓		✓
Attack Surface Reduction	✓	✓	✓
Next-Gen Protection	✓	✓	✓
Endpoint Detection and Response	✓[2]		✓
Automated Investigation and Response	✓[2]		✓
Threat Hunting and 6-months data retention			✓
Threat Analytics	✓[2]		✓
Cross platform support for Windows, MacOS, iOS and Android	✓	✓	✓
Microsoft Threat Experts			✓
Partner APIs	✓[2]	✓	✓
Microsoft 365 Lighthouse for viewing security incidents and customers	✓		

Note that not all capabilities may be available in preview

[1] Limited [2] Optimized for SMB [3] Additional capabilities planned

Microsoft Defender for Business

Licensing

Microsoft Defender Business ($3 pupm) →

Entreprise-grade endpoint security

Per user licence

- ✓ Next generation protection
- ✓ Cross Platform support (iOS, Android, Windows, MacOS)
- ✓ Endpoint Detection and Response
- ✓ Threat and Vulnerability Management
- ✓ … and more

Microsoft 365 Business Premium ($20 pipm)

Comprehensive productivity and security solution

Per user licence

Microsoft 365 Business Standard ($12.50)
Office apps and services, Teams

+

- ✓ Microsoft Defender for Business
- ✓ Microsoft Defender for Office 365 Plan 1
- ✓ Intune
- ✓ Azure AD Premium Plan 1
- ✓ Azure Information Protection Premium P1
- ✓ Exchange Online Archiving
- ✓ Autopilot
- ✓ Azure Virtual Desktop license
- ✓ Windows 10/11 Business
- ✓ Shared Computer Activation

Note that not all capabilities may be available in preview

1. **As standalone SKU**
Entitlement for use on up to 5 devices
Generally available H1 2022

2. **Included as part of Microsoft 365 Business Premium**
Microsoft Defender for Business will roll out to new and existing M365 Business Premium customers, post GA

Next steps.

WEBINARS

08 décembre 2021 | Prenez le contrôle de vos données avec Microsoft Azure Information Protection

Vers les
événements
Bechtle Suisse SA

Merci !

Des questions?

Nous restons à votre disposition pour vous accompagner dans vos projets futurs.