

#POWERCON2022

Microsoft Defender for Business: la soluzione
antimalware Microsoft per la PMI

Nicola Ferrini

Microsoft MVP – Cloud and Datacenter Management



/nicolaferrini.it



@nicolaferrini

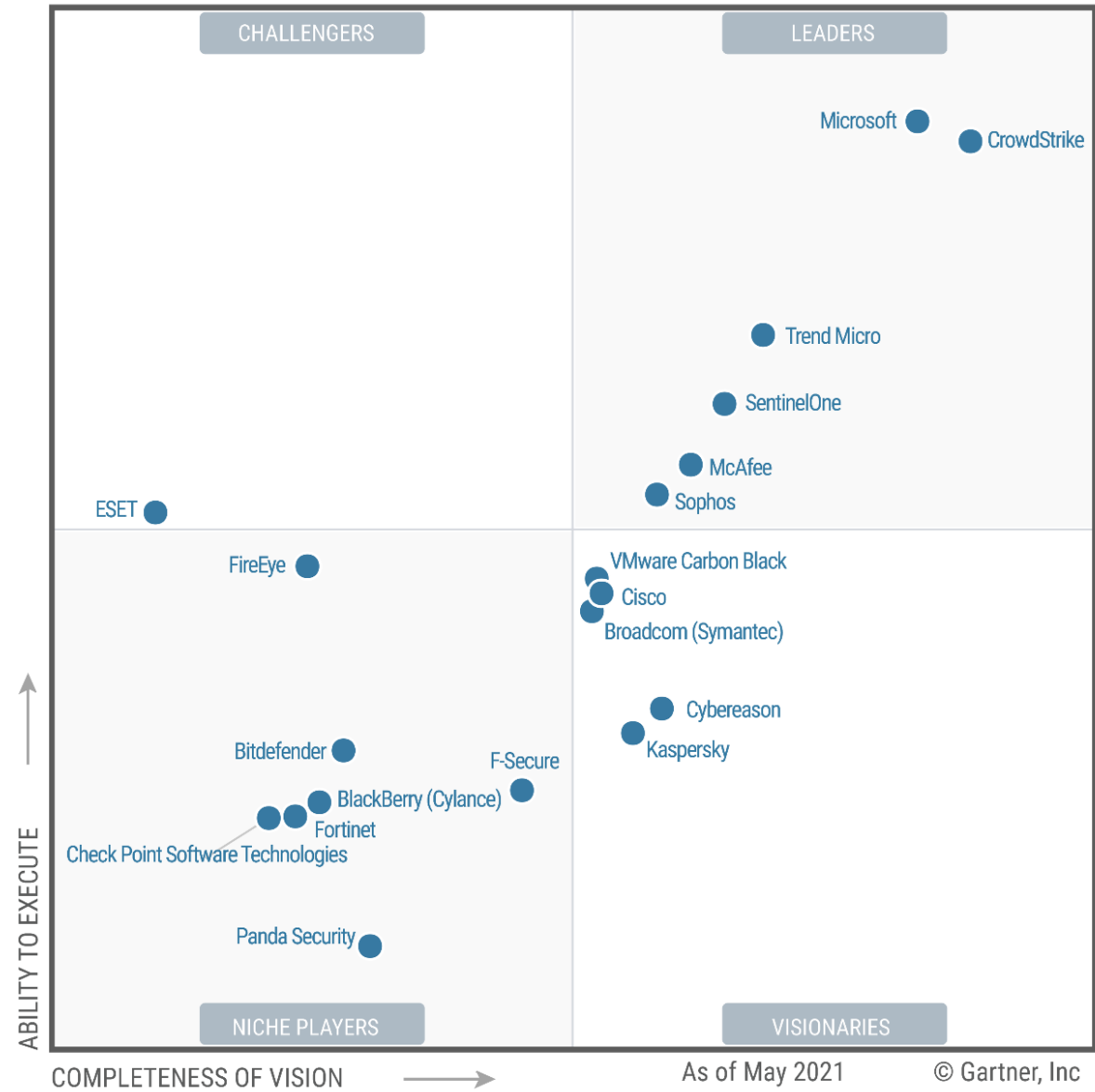


/nicolaferrini

Agenda

- Microsoft Defender for Business overview

Figure 1: Magic Quadrant for Endpoint Protection Platforms



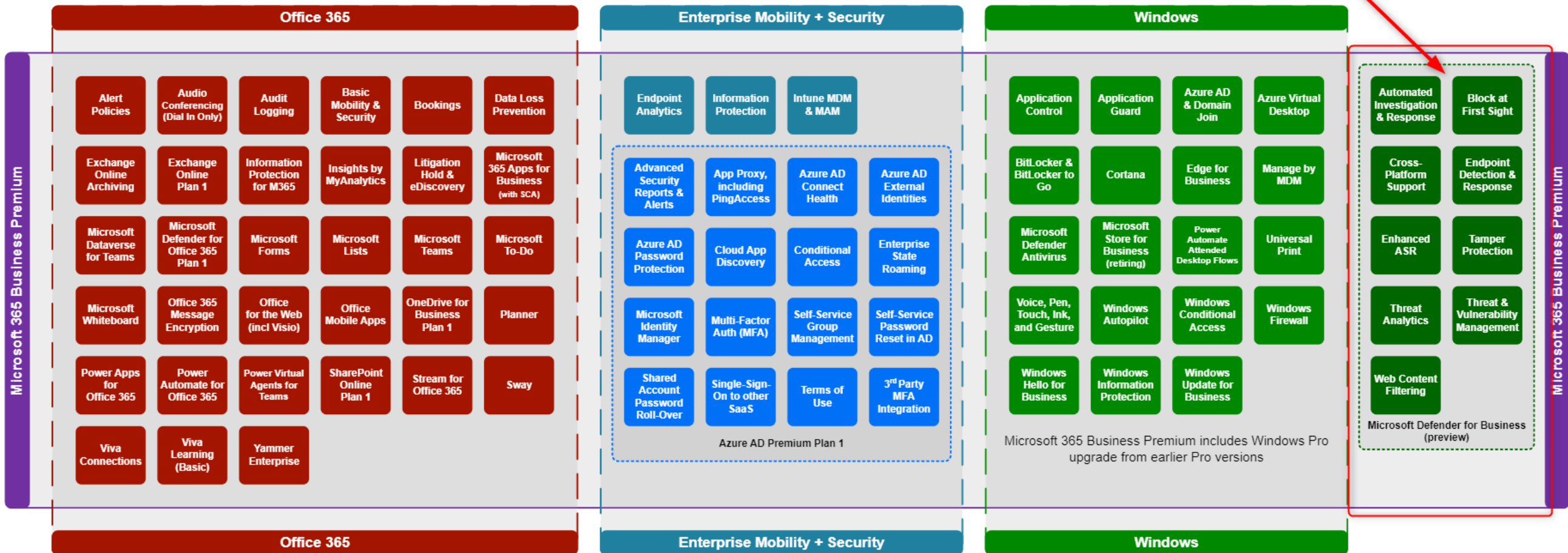
Source: Gartner (May 2021)

Microsoft 365 Premium License

Microsoft 365 Business Premium

January 2022

m365maps.com



Microsoft Defender for Business

Microsoft Defender for Business (preview)

**Automated
Investigation
& Response**

**Block at
First Sight**

**Cross-
Platform
Support**

**Endpoint
Detection &
Response**

**Enhanced
ASR**

**Tamper
Protection**

**Threat
Analytics**

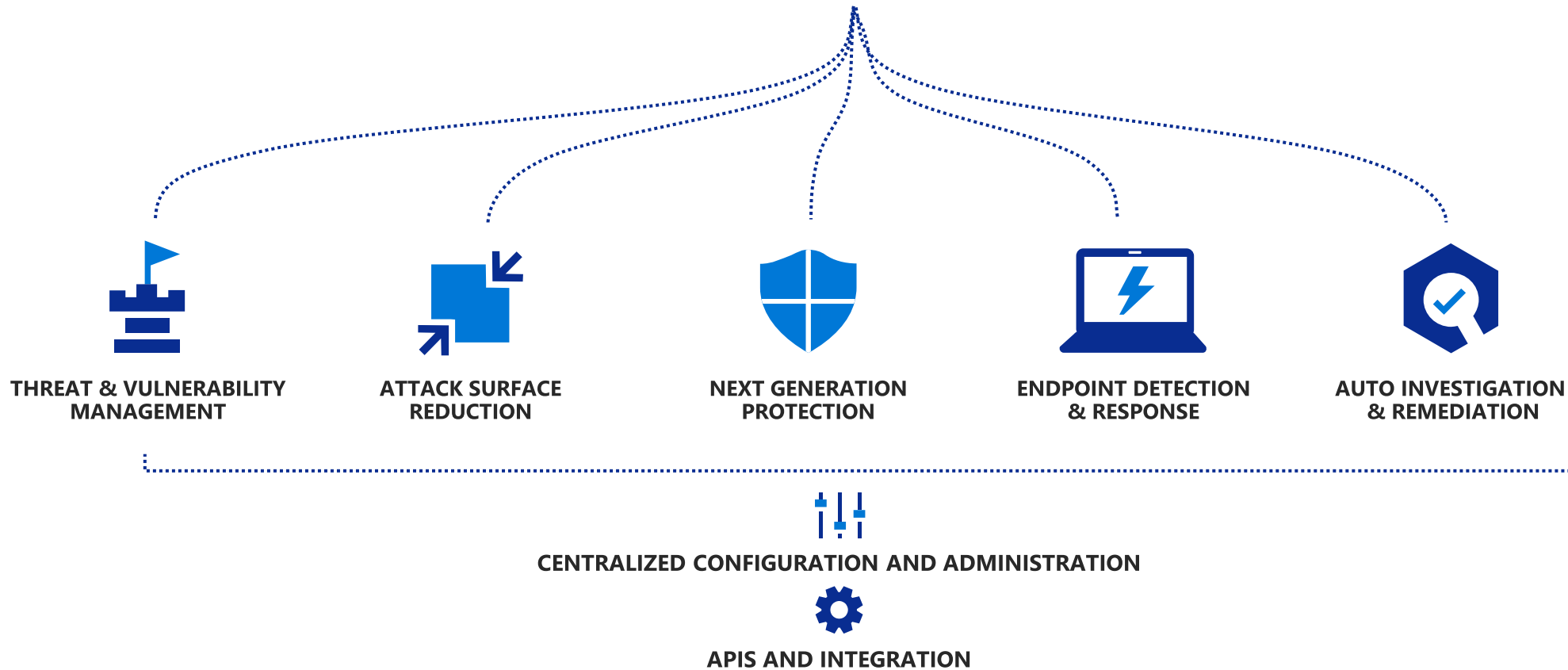
**Threat &
Vulnerability
Management**

**Web Content
Filtering**



Microsoft Defender for Business

Threats are no match.



Delivering endpoint security across platforms



 Windows



macOS



iOS

 Windows 365



Azure Virtual Desktop



Cisco

Juniper Networks



HP Enterprise

Palo Alto Networks

Endpoints and servers

Mobile device OS

Virtual desktops




Network devices

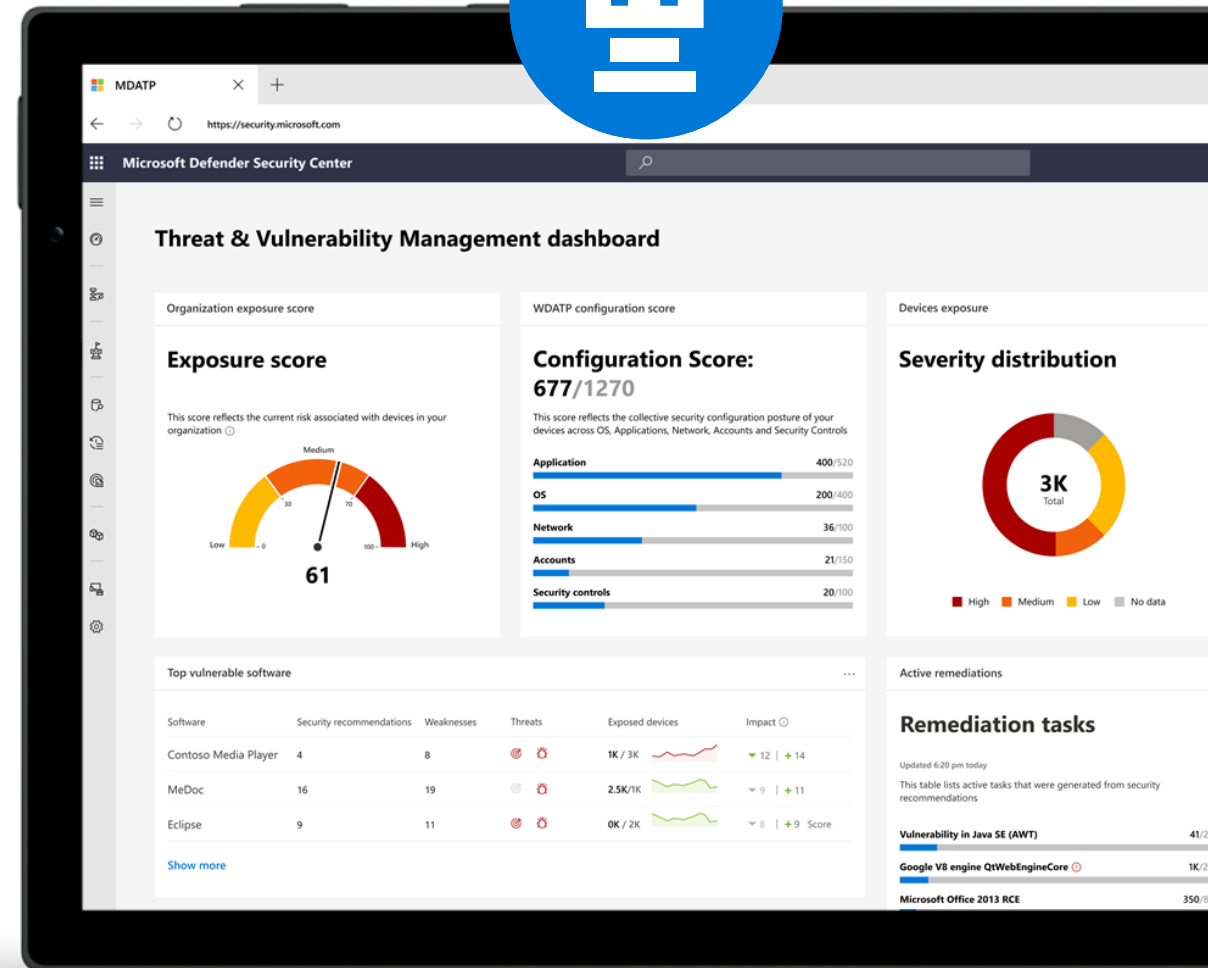
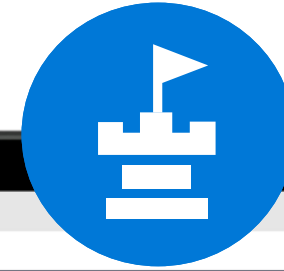
Threat & Vulnerability Management



Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

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





Continuous Discovery

Extensive vulnerability assessment across the entire stack

Easiest to exploit



Application extension vulnerabilities

Application-specific vulnerabilities that relate to component within the application.
For example: Grammarly Chrome Extension (CVE-2018-6654)



Application run-time libraries vulnerabilities

Reside in a run-time libraries which is loaded by an application (dependency).
For example: Electron JS framework vulnerability (CVE-2018-1000136)



Application vulnerabilities (1st and 3rd party)

Discovered and exploited on a daily basis.
For example: 7-zip code execution (CVE-2018-10115)



OS kernel vulnerabilities

Becoming more and more popular in recent years due to OS exploit mitigation controls.
For example: Win32 elevation of privilege (CVE-2018-8233)



Hardware vulnerabilities (firmware)

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

Hardest to discover



Continuous Discovery

Broad secure configuration assessment



Operation system misconfiguration

File Share Analysis

Security Stack configuration

OS baseline



Application misconfiguration

Least-privilege principle

Client/Server/Web application analysis

SSL/TLS Certificate assessment



Account misconfiguration

Password Policy

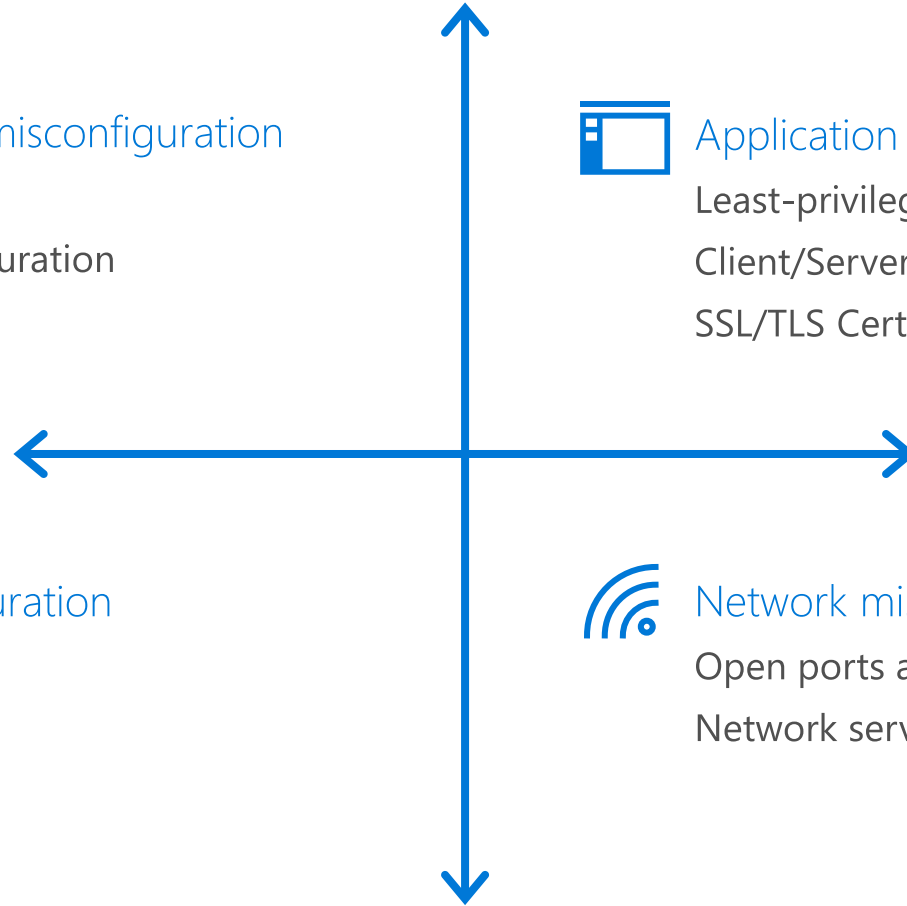
Permission Analysis



Network misconfiguration

Open ports analysis

Network services analysis



Attack Surface Reduction



Attack Surface Reduction

Eliminate risks by reducing the surface area of attack



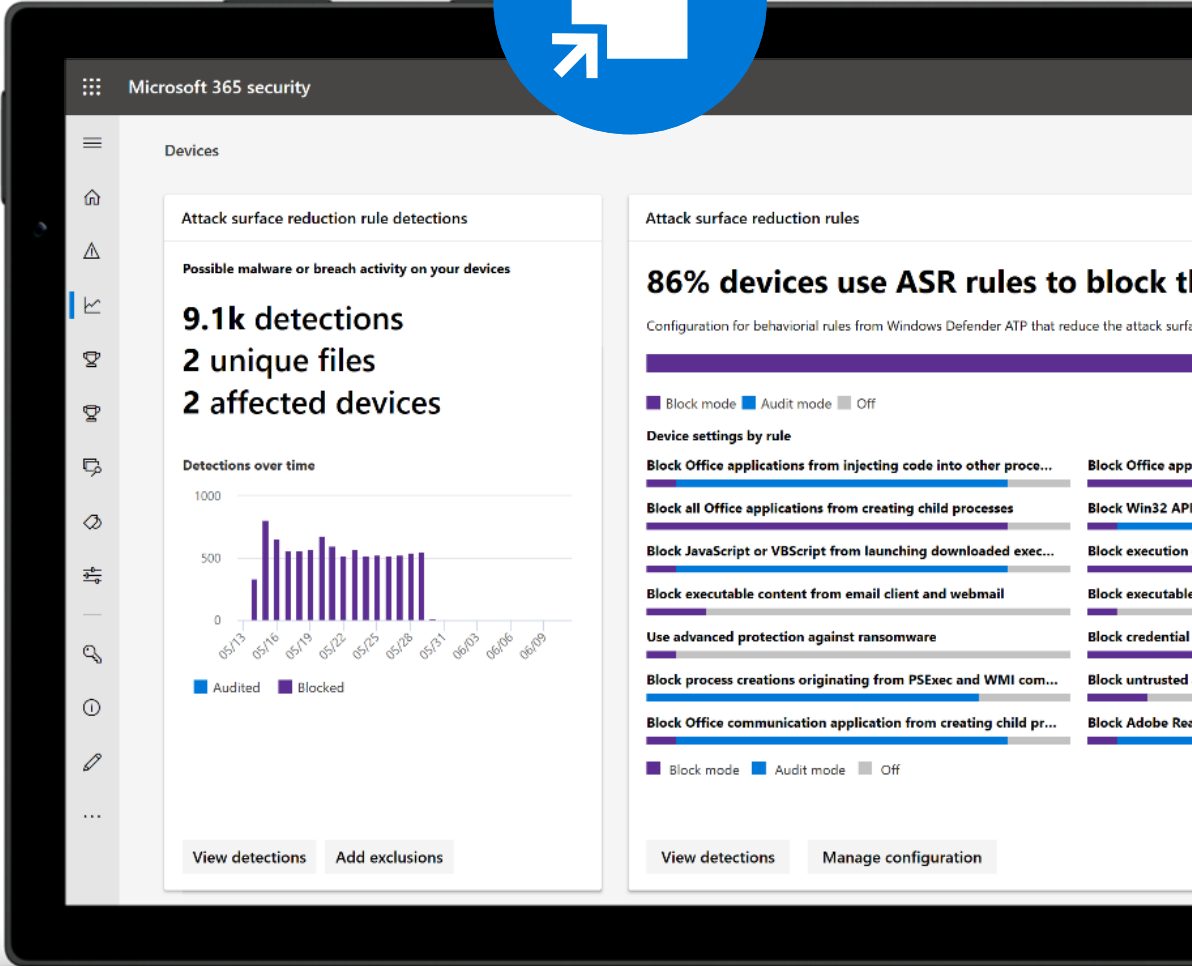
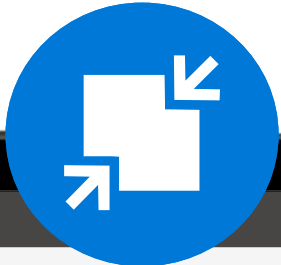
System hardening without disruption



Customization that fits your organization

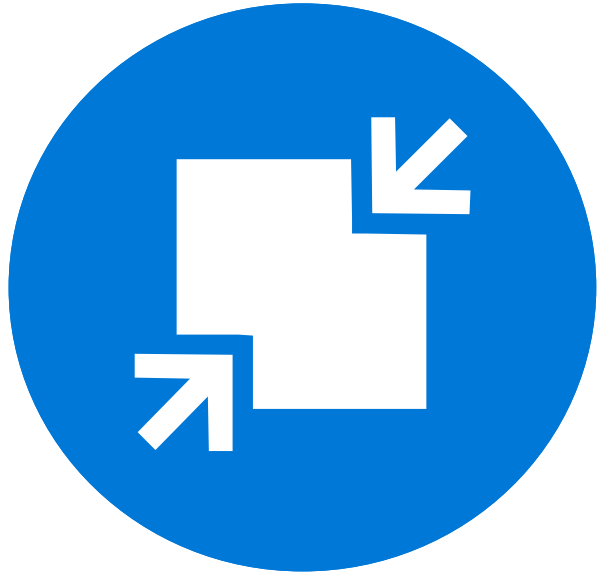


Visualize the impact and simply turn it on



Attack Surface Reduction

Resist attacks and exploitations



HW based isolation

Application control

Exploit protection

Network protection

Controlled folder access

Device control

Web protection

Ransomware protection

Isolate access to untrusted sites

Isolate access to untrusted Office files

Host intrusion prevention

Exploit mitigation

Ransomware protection for your files

Block traffic to low reputation destinations

Protect your legacy applications

Only allow trusted applications to run

Attack Surface Reduction (ASR) Rules



Minimize the attack surface

Signature-less, control entry vectors, based on cloud intelligence. Attack surface reduction (ASR) controls, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats

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

Lateral movement & credential theft

- Block process creations originating from PSEXEC and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

Easy button: turn on block

Microsoft 365 Security

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

Detections **Configuration** Rule status

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.
[View details](#) [Dismiss](#)

Identify and fix devices with limited protection due to missing prerequisites or misconfigured rules. [Learn about prerequisites](#)

Device configuration overview

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

Add exclusions
Choose to exclude files you trust from being blocked by attack surface reduction rules.
[Add exclusions](#)

Export

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](#)

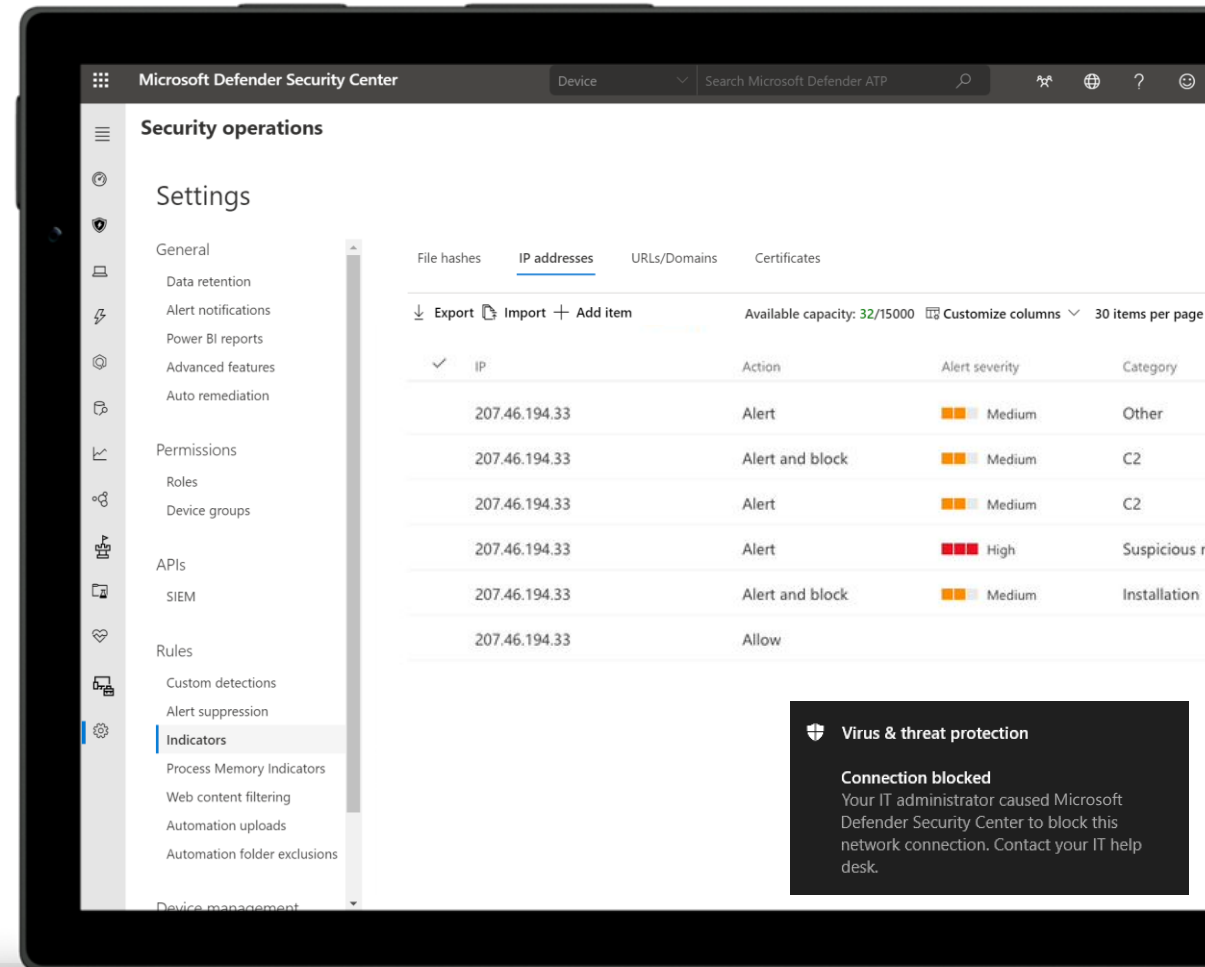
Devices
2,354 devices
80% of your total devices with Windows Defender Advanced Threat Protection

[Get script to implement](#) [Submit Intune ticket](#)

Network protection

Allow, audit and block

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



Web Threat Alerts

Alerts > Suspicious connection blocked by network pro...

Suspicious connection blocked by network protection Automated investigation is not applicable to alert type

This alert is part of incident (76)

Actions

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

Alert context

minint.scps
minint: [IP address]

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

Status

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

Description

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

Recommended actions

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

[Show more](#)

Alert process tree

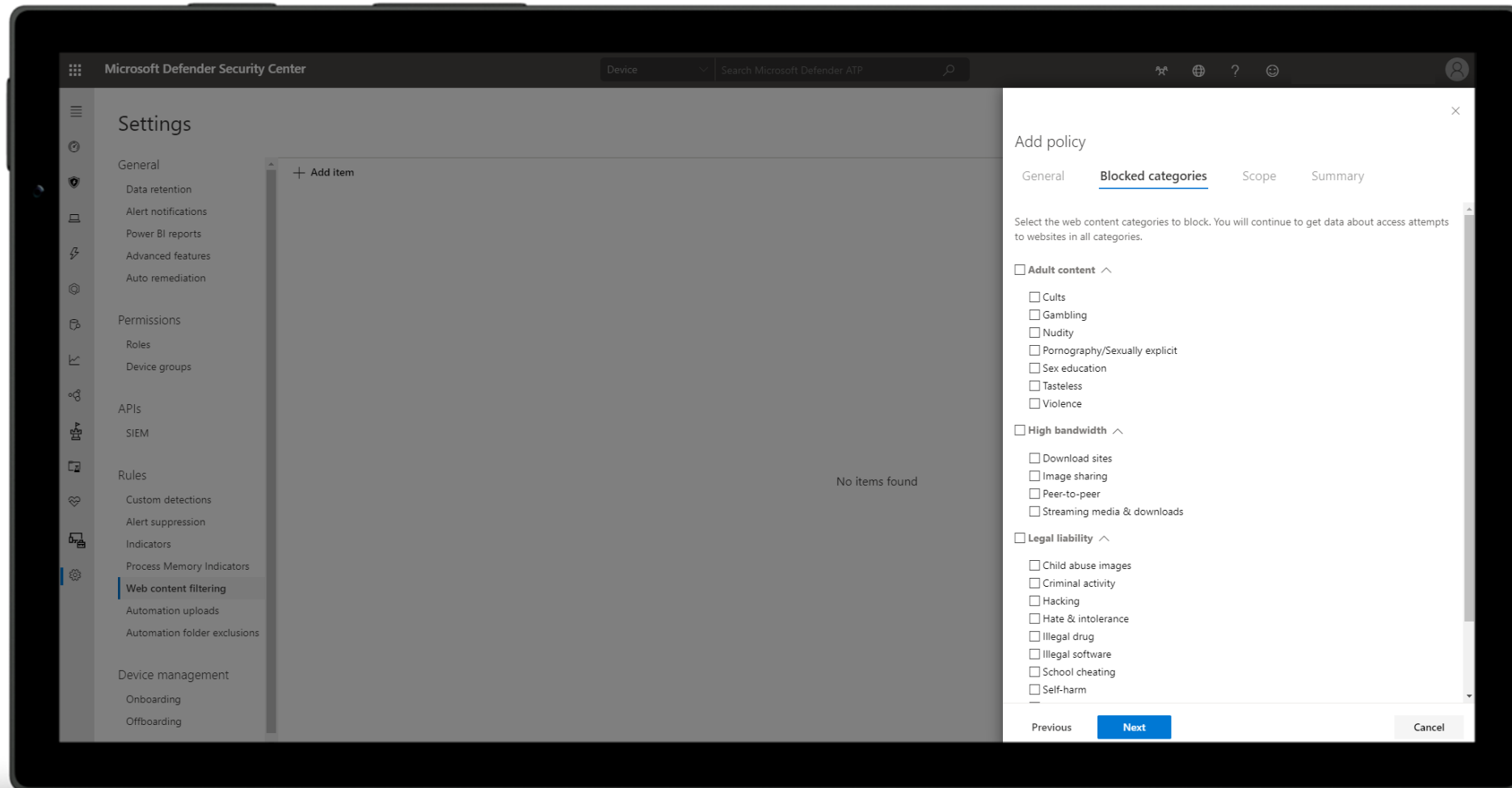
```
graph TD
  A[firefox.exe] --> B[firefox.exe]
  B --> C["https://smartscreentestrings2.net  
https://smartscreentestrings2.net was blocked by ExploitGuard"]
  B --> D["https://smartscreentestrings2.net  
https://smartscreentestrings2.net was blocked by ExploitGuard"]
```

Incident graph is not available for this alert

Artifact timeline

Description	First Observed	Details
-------------	----------------	---------

Web content filtering configuration



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

Blocks and tackles sophisticated threats and malware



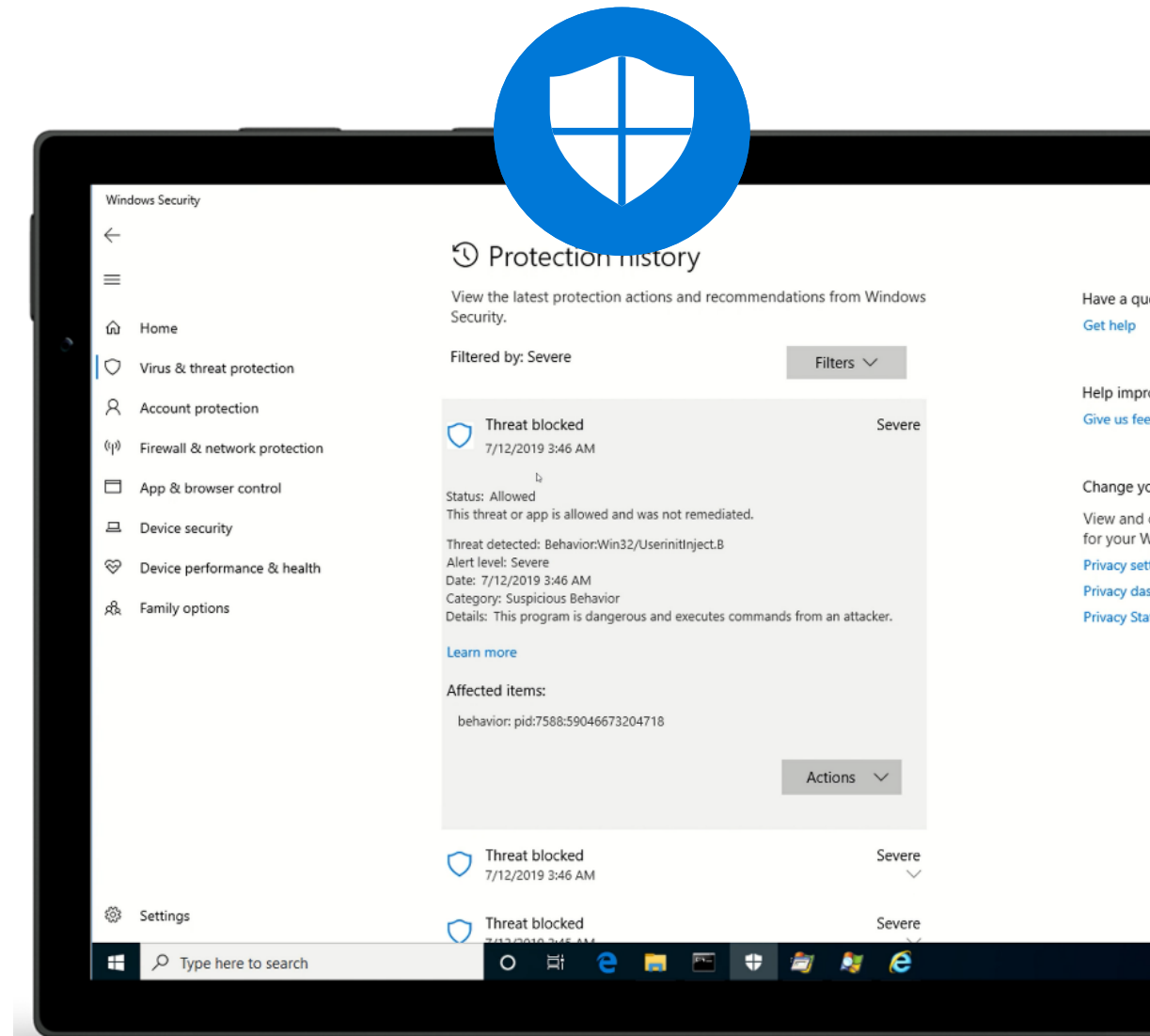
Behavioral based real-time protection



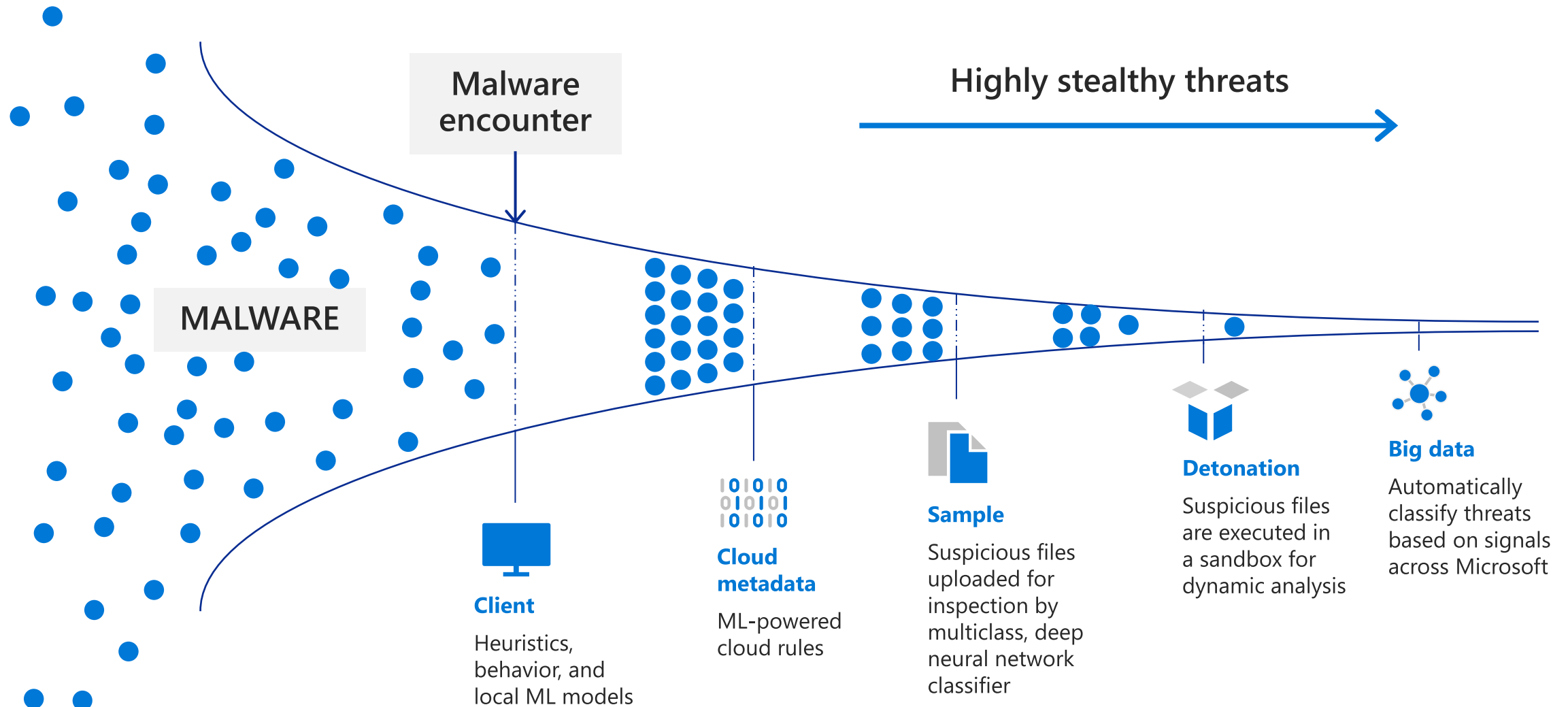
Blocks file-based and fileless malware



Stops malicious activity from trusted and untrusted applications



Microsoft Defender for Business's NGP protection pipeline



Endpoint detection and response



Endpoint Detection & Response

Detect and investigate advanced persistent attacks



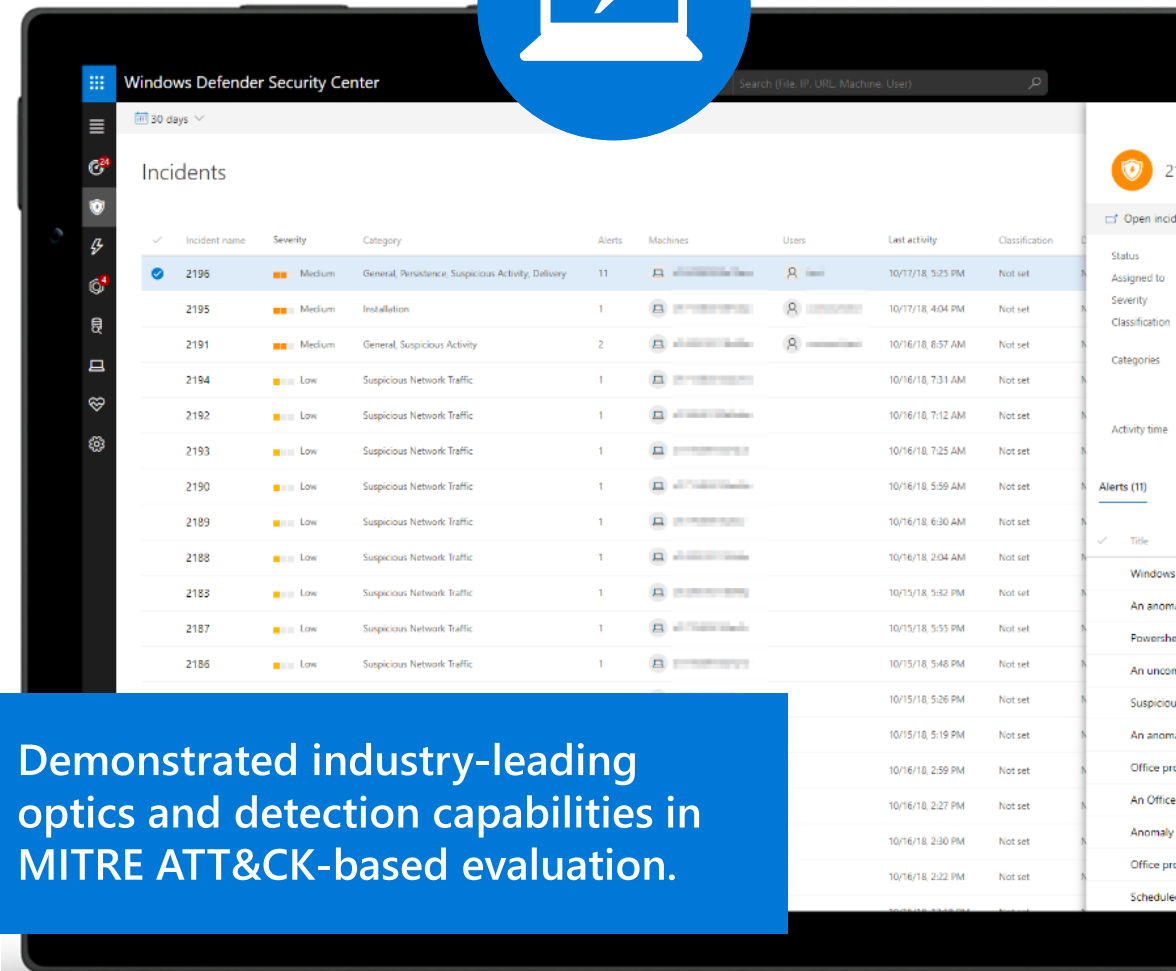
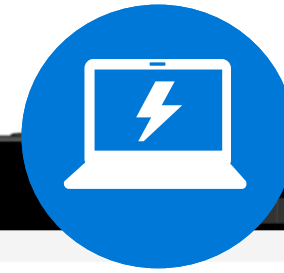
Correlated behavioral alerts



Investigation & hunting over 6 months of data



Rich set of response actions



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

Automated investigation and response



Key customer pain points



More threats, more alerts leads to analyst fatigue



Alert investigation is time-consuming



Expertise is expensive



Manual remediation requires time

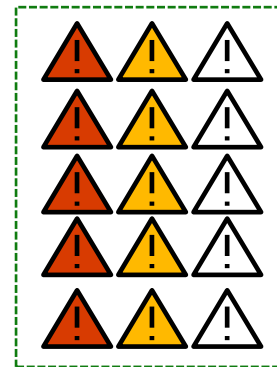


Talent shortage in cybersecurity



Analysts overwhelmed by manual alert investigation & remediation

Alert queue



Analyst 1



Analyst 2

Auto Investigation & Remediation

Automatically investigates alerts and remediates complex threats in minutes



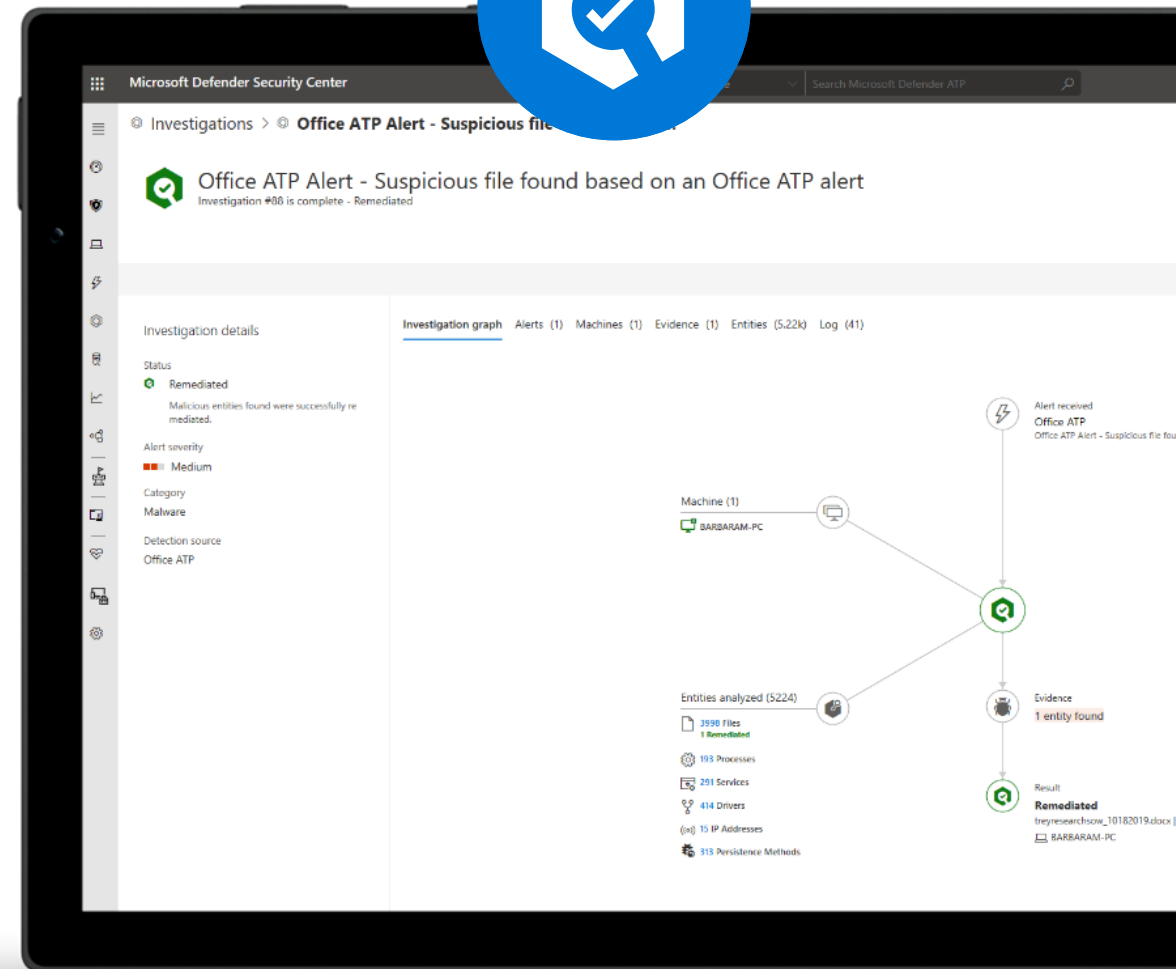
Mimics the ideal steps analysts would take



Tackles file or memory-based attacks



Works 24x7, with unlimited capacity



Auto investigation queue

The screenshot displays the Microsoft Defender Security Center interface, specifically the 'Automated Investigations' section. The interface includes a search bar at the top, a navigation sidebar on the left, and a main table of investigation records. A 'Filters' panel on the right allows for filtering by status and triggering alert.

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

Filters

Status

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

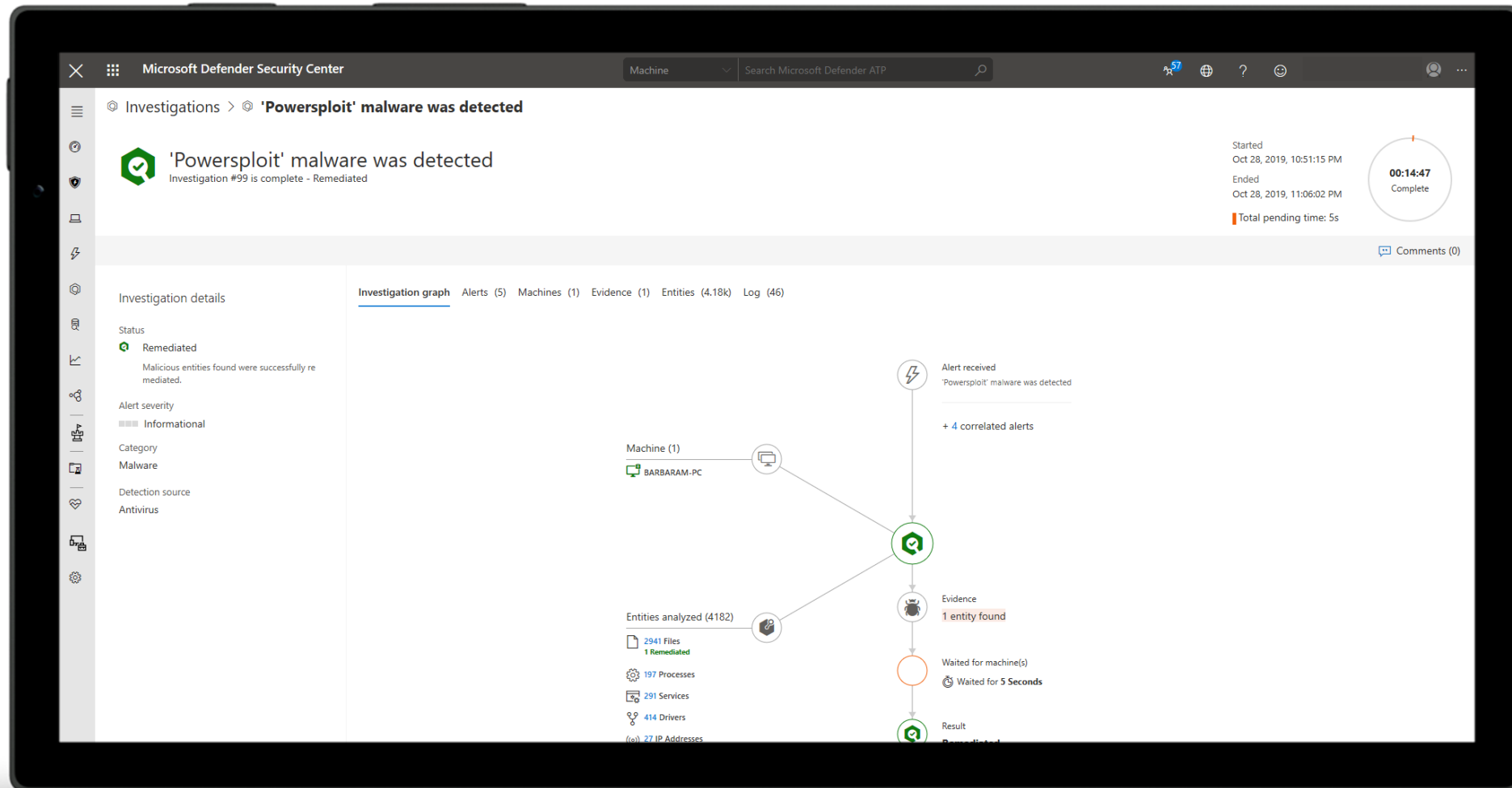
Triggering alert

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

Detection Source

- Any
- AutomatedInvestigation (9)
- Antivirus (4)
- EDR (2)
- OfficeATP (2)

Investigation graph



Centralized Administration & Configuration



Security Management

Assess, configure and respond to changes in your environment



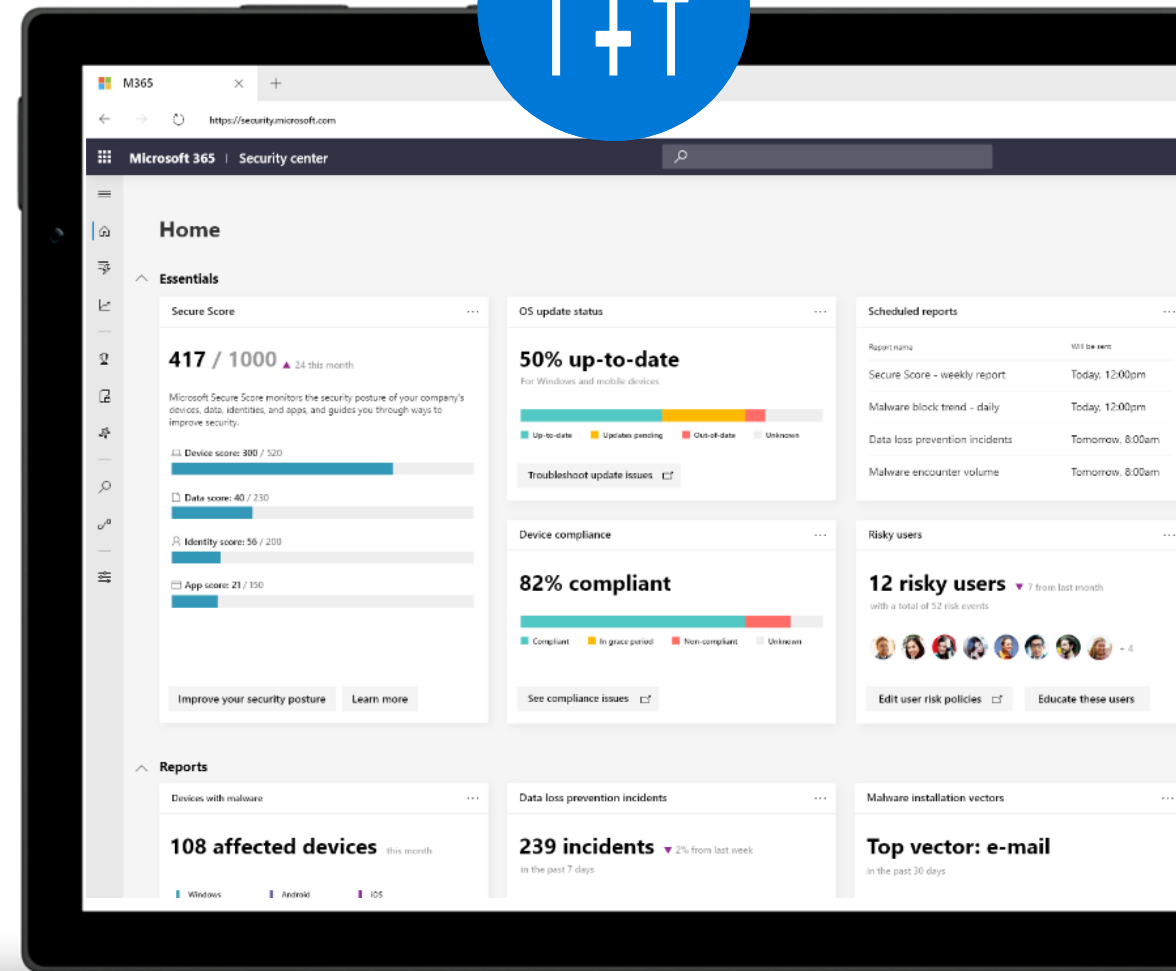
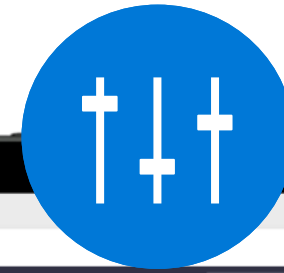
Centrally assess & configure your security



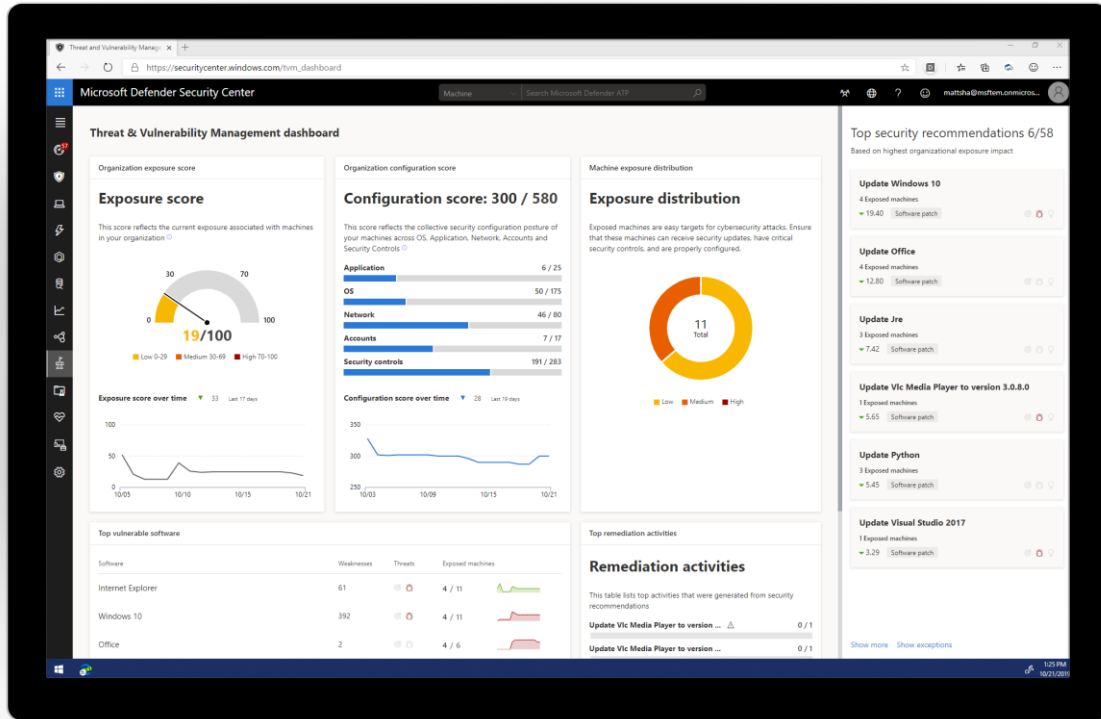
Variety of reports and dashboards for detailed monitoring and visibility



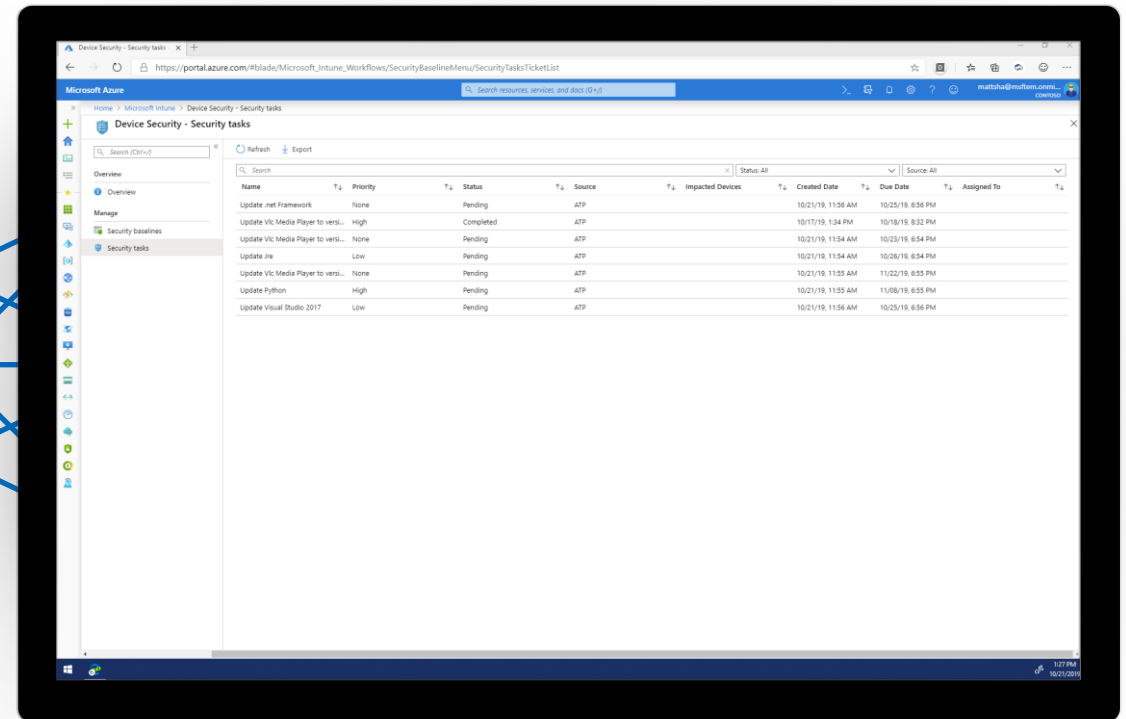
Seamless integration between policy assessment and policy enforcement



Seamless integration



Microsoft Defender for Endpoint
Policy Assessment



Microsoft Intune
Policy Enforcement

DEMO

SMB Onboarding - Microsoft 365 x

https://security.microsoft.com/smb-onboarding?tid=1d5a26...

Microsoft 365 Defender

- Home
- Incidents
- Actions & submissions
- Threat analytics
- Secure score
- Learning hub
- Partner catalog
- Assets
- Devices
- Endpoints
- Vulnerability management
- Tutorials
- Configuration management
- Email & collaboration
- Policies & rules
- Cloud apps

Welcome to Microsoft Defender for Business

Welcome to Microsoft Defender for Business, which helps you monitor and manage security across your organization. Learn more about Microsoft Defender for Business.

Let's set this up!

We'll walk you through the steps of the setup process.

- Assign user permissions
- Set up email protection
- Onboard and manage Windows devices

[Get started](#)

[Elevate your endpoint security with Microsoft Defender for Business \(cloudguides.com\)](https://cloudguides.com)

Links

- [What is Microsoft Defender for Business? | Microsoft Learn](#)
- [Microsoft Defender for Business: la soluzione antimalware Microsoft per la PMI - ICT Power](#)
- [Compare Microsoft endpoint security plans | Microsoft Learn](#)
- [Compare security features in Microsoft 365 plans for small and medium-sized businesses | Microsoft Learn](#)
- [Microsoft Defender for Endpoint demonstration scenarios | Microsoft Learn](#)

Grazie



/nicolaferrini.it



@nicolaferrini



/nicolaferrini