Microsoft

CSP Masters Program in person series
Technical training

Microsoft Defender for Business

Microsoft Defender for Business

Microsoft Defender
for Business

Elevate your security

Threat & Vulnerability Management

Attack Surface Reduction

Next Generation Protection

Endpoint Detection & Response

Auto Investigation & Remediation

Simplified Onboarding and Administration

APIs and Integration

Delivering endpoint security across platforms

Windows macOS

Endpoints and servers[2]

iOS

Mobile device OS[1]

Windows 365

Azure Virtual Desktop

Virtual desktops

[1] iOS, and Android requires Microsoft Intune. Intune is included in Microsoft 365 Business Premium. [2]Add-on server support now available in preview. Please see Documentation for more detail.

Microsoft Defender for Business is included in Business Premium

Microsoft Defender Business ($3pupm)[1]

Enterprise-grade endpoint security

Per user license

- ✓ Next generation protection
- ✓ Cross-Platform support (iOS, Android, Windows, MacOS)[2]
- ✓ Endpoint Detection and Response
- ✓ Threat and Vulnerability Management
- ✓ ...and more

Microsoft 365 Business Premium ($22pupm)[1]

Comprehensive productivity and security solution

Per user license

Microsoft 365 Business Standard ($12.50)[1]
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

Licensing options

1. **As standalone SKU, up to 300 users**
   Entitlement for use on up to 5 devices
2. **Included as part of Microsoft 365 Business Premium, up to 300 users.**
3. **Add-on Server offering now available in preview.**

[1]price is subject to change based on subscription term, currency and region

[2]iOS, and Android requires Microsoft Intune. Intune is included in Microsoft 365 Business Premium. Please see Documentation for more detail.

Product comparison – Endpoint security

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

Available as a standalone endpoint security and as part of Microsoft 365 Business Premium

Defender for Business servers add-on is now in preview

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

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 Firewall and Antivirus configuration for Windows	✔		
Threat and Vulnerability Management	✔		✔
Attack Surface Reduction	✔	✔	✔
Next-Gen Protection	✔	✔	✔
Endpoint Detection and Response	✔[1]		✔
Automated Investigation and Remediation	✔[1]		✔
Threat Hunting and 6-months data retention			✔
Threat Analytics	✔[1]		✔
Cross platform support for Windows, MacOS, iOS[3], and Android[3] clients	✔	✔	✔
Windows server and Linux server	(Add-on) Microsoft Defender for Business server in preview	✔[4]	✔[4]
Microsoft Threat Experts			✔
Partner APIs	✔	✔	✔
Microsoft 365 Lighthouse for viewing security incidents across customers	✔[2]		

[1] Optimized for SMB. [2] Additional capabilities planned. [3]Requires Microsoft Intune. Intune is included in Microsoft 365 Business Premium. [4]Requires separate server license. Please see Documentation for more detail.

Defender for Business

brings enterprise grade endpoint security to Microsoft 365 Business Premium

		PRE MDB	WITH MDB	
		Microsoft 365 Business Premium[3]	Microsoft 365 Business Premium[3]	Microsoft Defender for Business (MDB)[3]
eDiscovery and Audits	eDiscovery	•	•	
	Litigation Hold	•	•	
	Email Archiving	•	•	
Information Protection	Information Rights Management	•	•	
	File classification/labeling	•	•	
	File tracking and revocation	•	•	
Data Loss Prevention	Message Encryption	•	•	
	Data Loss Prevention	•	•	
	Data App Security	•	•	
Email and Collaboration Security	Safe links	•	•	
	Safe Attachments	•	•	
	Anti-phishing	•	•	
Device management	Windows device setup & management	•[1]	•[1]	
	Device health analytics	•	•	
	Mobile Device Management	•	•	
	Mobile App Management	•	•	
Identity and Access Management and Security	Risk based Conditional access	•	•	
	Multi-factor authentication	•	•	
Endpoint Security	Centralized management	•	•	•
	Simplified client configuration		•	•
	Next-gen protection	Win10	•	•
	Attack Surface Reduction	Win10[1]	•	•
	Network Protection		•	•
	Web Category blocking		•	•
	Endpoint detection and response		•	•
	Cross platform support (iOS/Android/Mac)		•[4]	•[4]
	Automated investigation and response		•[2]	•[2]
	Threat and vulnerability		•	•
	Threat intelligence		•[2]	•[2]

[1]Limited. [2] Optimized for SMB.

[3] Microsoft Defender for Business is available in Microsoft 365 Business Premium and as a standalone SKU. Read the blog post to learn more.

[4] iOS, and Android requires Microsoft Intune. Intune is included in Microsoft 365 Business Premium. Please see Documentation for more detail.

Gartner®

Microsoft Security—a Leader in 5 Gartner Magic Quadrant reports

Access Management

Cloud Access Security Brokers

Enterprise Information Archiving

Endpoint Protection Platforms

Unified Endpoint Management

*Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021

*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020

*Gartner "Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020

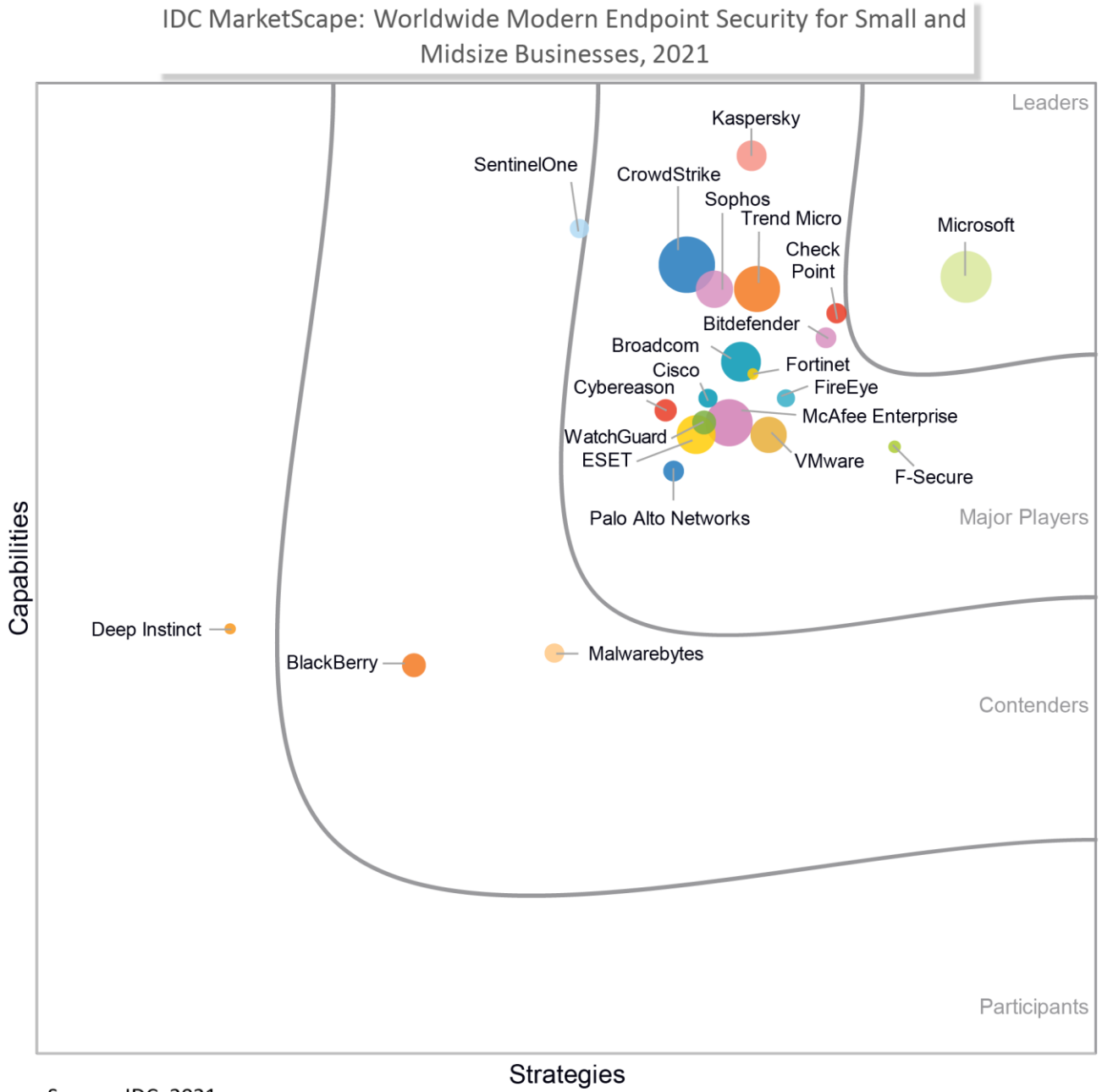
*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021

*Gartner "Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Chris Silva, Tom Cipolla, August 2021

Microsoft the only Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessmenthttps://idcdocserv.com/US48304721
IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of information and communication technology (ICT) suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market, and business execution in the short term. The Strategy score measures alignment of vendor strategies with customer requirements in a three to five-year timeframe. Vendor market share is represented by the size of the icons.

Microsoft named a Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses - Microsoft Security Blog

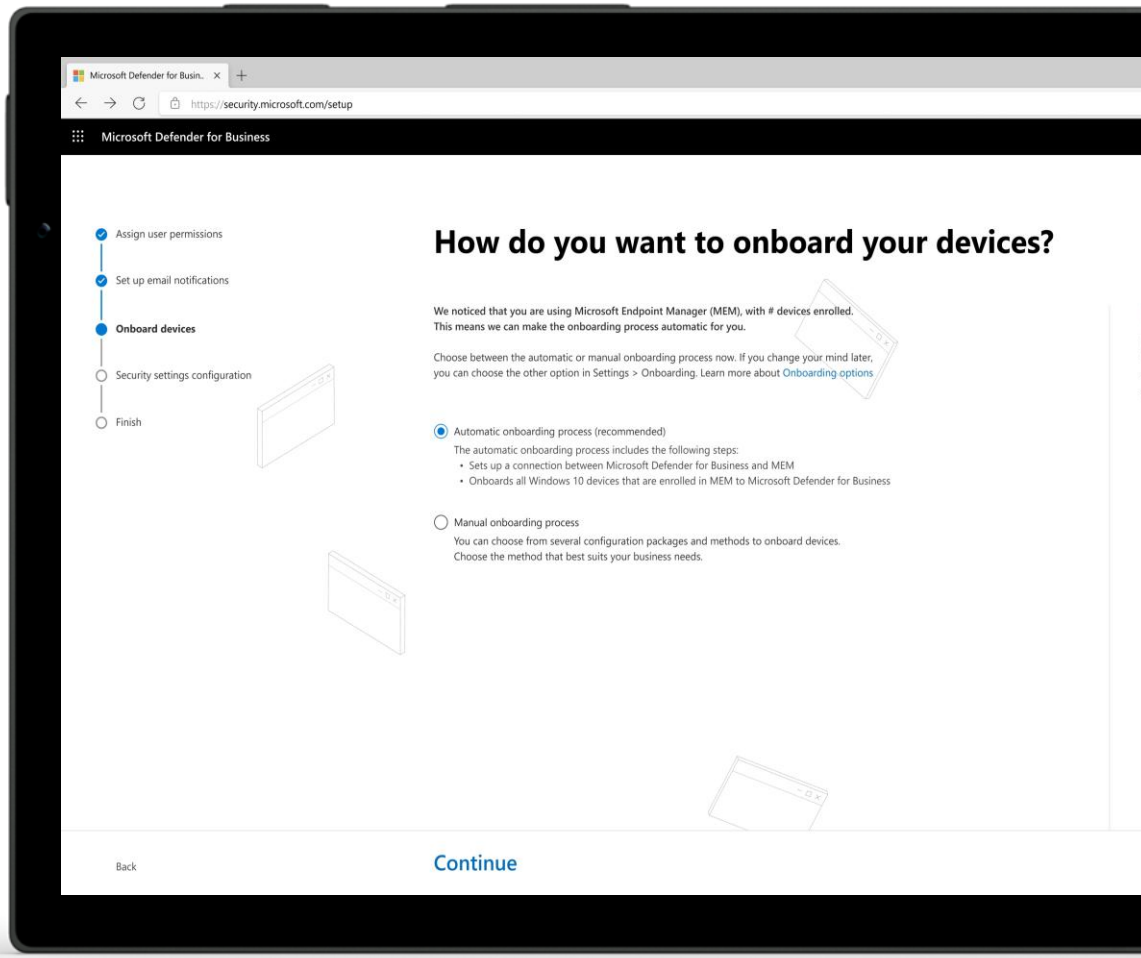


Source: IDC, 2021

Simplified Onboarding and Administration

Wizard-driven onboarding and easy to use management controls

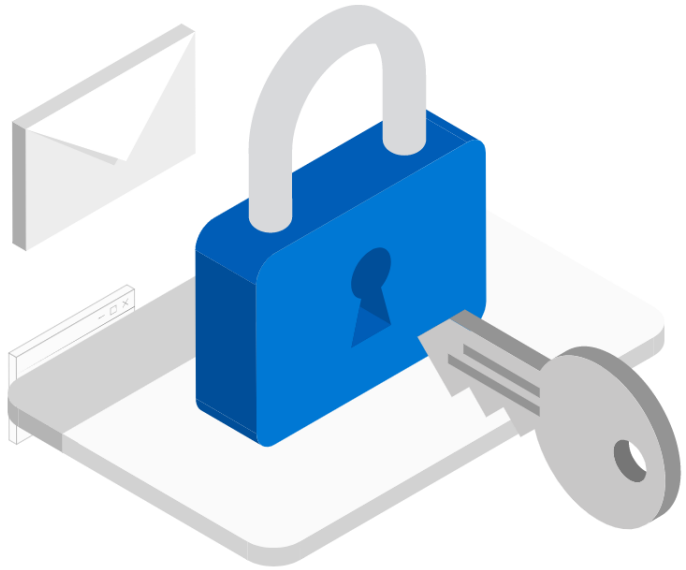
1. Onboard new Windows devices in a few simple steps
2. Recommended security policies activated out-of-the-box
3. Action-oriented dashboard help prioritize tasks



iOS, and Android requires Microsoft Intune. Intune is included in Microsoft 365 Business Premium. Please see Documentation for more detail.

Initial setup

Home
Incidents
Incidents & alerts
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Endpoints
Device inventory
Vulnerability management
Tutorials
Configuration management
Email & collaboration
Real-time detections



Welcome to Microsoft Defender for Business

Welcome to Microsoft Defender for Business, where you can monitor and manage security across your devices. Learn more about Microsoft Defender for Business

Let's set this up!

We'll walk you through these steps of the setup process:

- Assign user permissions
- Set up email notifications
- Onboard and configure Windows devices

Get started

- **Assign user permissions**
- Set up email notifications
- Add Windows devices
- Apply security settings
- Finish

Let's give people access

Select users or groups to assign the Security Reader or Security Admin role.
You can edit role assignments later in Microsoft Azure Active Directory (Azure AD)

Users can be assigned as:

- **Security Administrators** can view security information and reports, and manage security settings
- **Security Readers** can view security information and reports

Learn more about these roles

Name	Role
Type user or group name	Select role

+ Add role assignment

Continue

Skip

Cancel

- Assign user permissions
- Set up email notifications
- Add Windows devices
- Apply security settings
- Finish

Let's give people access

Select users or groups to assign the Security Reader or Security Admin role.
You can edit role assignments later in Microsoft Azure Active Directory (Azure AD)

Users can be assigned as:

- **Security Administrators** can view security information and reports, and manage security settings
- **Security Readers** can view security information and reports

Learn more about these roles

Name	Role
MA MOD Administrator	Security admin
AV Adele Vance	Security reader

+ Add role assignment

Continue

Skip Cancel

- Assign user permissions
- **Set up email notifications**
- Add Windows devices
- Apply security settings
- Finish

Set up email notifications

Specify an email address and select the type of notifications you want users to receive.
This action creates rules that you can edit later in your email notification settings.

Email notification types

Alerts
Get email notifications when any type of alert is triggered on devices.

Vulnerabilities
Get email notifications when certain exploit or vulnerability events occur, such as a new public exploit.

Recipients	Notification type
admin@M365B345200.onmicrosoft.com	Select notification type

Alerts
Vulnerabilities
Alerts & vulnerabilities

+ Add recipients

Back | Continue | Skip | Cancel

- Assign user permissions
- Set up email notifications
- **Add Windows devices**
- Apply security settings
- Finish

Choose a method to onboard devices

Onboard **Windows devices** to seamlessly enroll the devices in Azure Active Directory and Microsoft Endpoint Manager. You can add other OS devices later.

To get started, choose the preferred deployment method. Learn more about onboarding devices

Onboarding method

- Microsoft Endpoint Manager
- Local Script
- Group Policy
- VDI onboarding scripts

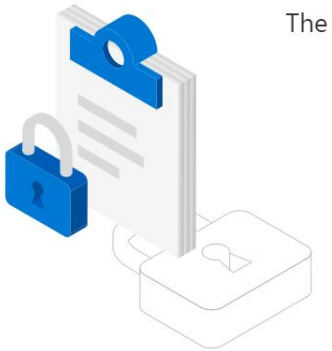
Back | Continue | Cancel

- Assign user permissions
- Set up email notifications
- Add Windows devices
- **Apply security settings**
- Finish

Apply security settings

Let us do the work for you

Microsoft Defender for Business includes default policies with recommended settings that can be applied to Windows devices. Learn more about security configuration settings



The recommended configuration will include:

- Next generation protection policies for antivirus and threat protection
- Firewall policies to block or allow network traffic

To start the process, choose '**Continue**' You can always edit your settings later in **Device configuration**

Back | Continue | Skip | Cancel

- Assign user permissions
- Set up email notifications
- Add Windows devices
- Apply security settings
- **Finish**

You're almost done..

Review the details below. When you're ready, select Submit to finish setting up your preferences.

Roles and permissions

Security reader (1)

AV Adele Vance

Security admin (1)

MA MOD Administrator

Email notifications

Set up email notifications for these recipients:

admin@M365B345200.onmicrosoft.com - Alerts & vulnerabilities

Devices to add

Onboard your organization's devices to Microsoft Defender for Business

Back Submit Cancel

- Assign user permissions
- Set up email notifications
- Add Windows devices
- Apply security settings
- Finish

Hold on while we set this up

Sit back, this may take a few seconds..

Done

- Assign user permissions
- Set up email notifications
- Add Windows devices
- Apply security settings
- Finish

You're all set

Here are some steps you can take to get started.

System dashboard

Visit your system dashboard to see real-time status of your organization

Go to System dashboard

Device configuration

View or edit device security policies

Go to Device configuration

Onboard more devices

Add more devices, including devices with non-Windows operating systems

Go to device onboarding

Done

Enable features

Event timeline
Tutorials
Configuration management
Email & collaboration
Real-time detections
Review
Exchange message trace
Policies & rules
Reports
Audit
Health
Permissions
Settings
More resources
Customize navigation

Endpoints

General
Data retention
Email notifications
Advanced features
Auto remediation

APIs
SIEM

Rules
Alert suppression
Indicators
Web content filtering

This section provides a set of advanced features you can enable.
These features require integration with other products. You need to verify that these settings are enabled to use the features.

On — Automated Investigation
Enables the automation capabilities for investigation and response.

On — Live Response
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.

On — Live Response for Servers
Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.

On — Live Response unsigned script execution
Enables using unsigned PowerShell scripts in Live Response.

Save preferences

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Endpoint security | Microsoft Defender for Endpoint

Search (Ctrl+/)

All devices
Security baselines
Security tasks

Manage

Antivirus
Disk encryption
Firewall
Endpoint detection and response
Attack surface reduction
Account protection
Device compliance
Conditional access

Monitor

Assignment failures (preview)

Setup

Microsoft Defender for Endpoint

Help and support

Help and support

Refresh | Save | Discard | Delete

The Microsoft Defender for Endpoint connector is active for Windows, iOS, and Android but a risk assessment is not included in a compliance policy for these platforms. To protect devices on these platforms, click here to set up a compliance policy with the Machine Risk Score settings configured in the Microsoft Defender for Endpoint section.

Connection status	Last synchronized
Enabled	6/13/2022, 10:51:31 AM

Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations	Off / On

MDM Compliance Policy Settings

Connect Android devices to Microsoft Defender for Endpoint	Off / On
Connect iOS devices to Microsoft Defender for Endpoint	Off / On
Connect Windows devices to Microsoft Defender for Endpoint	Off / On
Enable App Sync for iOS/iPadOS Devices	Off / On
Send full application inventory data on personally-owned iOS/iPadOS Devices	Off / On
Block unsupported OS versions	Off / On

Onboarding

Event timeline
Tutorials
Configuration management
Email & collaboration
Real-time detections
Review
Exchange message trace
Policies & rules
Reports
Audit
Health
Permissions
Settings
More resources
Customize navigation

Endpoints

Alert suppression
Indicators
Web content filtering

Configuration management

Enforcement scope

Device management

Onboarding
Offboarding

Network assessments

Assessment jobs

Select operating system to start onboarding process:

Windows 10 and 11

1. Onboard a device

First device onboarded: Incomplete

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read Onboard and set up.

Deployment method

Local Script (for up to 10 devices)

You can configure a single device by running a script locally.
Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above.
For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see Configure devices using a local script section in the Microsoft Defender for Endpoint guide.

Select operating system to start onboarding process:

Windows 10 and 11

1. Onboard a device

First device onboarded: Incomplete

Onboard devices to Microsoft Defender for Endpoint using the onboarding confi
matches your preferred deployment method. For other device preparation instruc
set up.

Deployment method

- Local Script (for up to 10 devices)
- Group Policy
- Microsoft Endpoint Configuration Manager current branch and later
- Mobile Device Management / Microsoft Intune
- VDI onboarding scripts for non-persistent devices

ices

for

section in the Microsoft Defender for Endpoint guide.

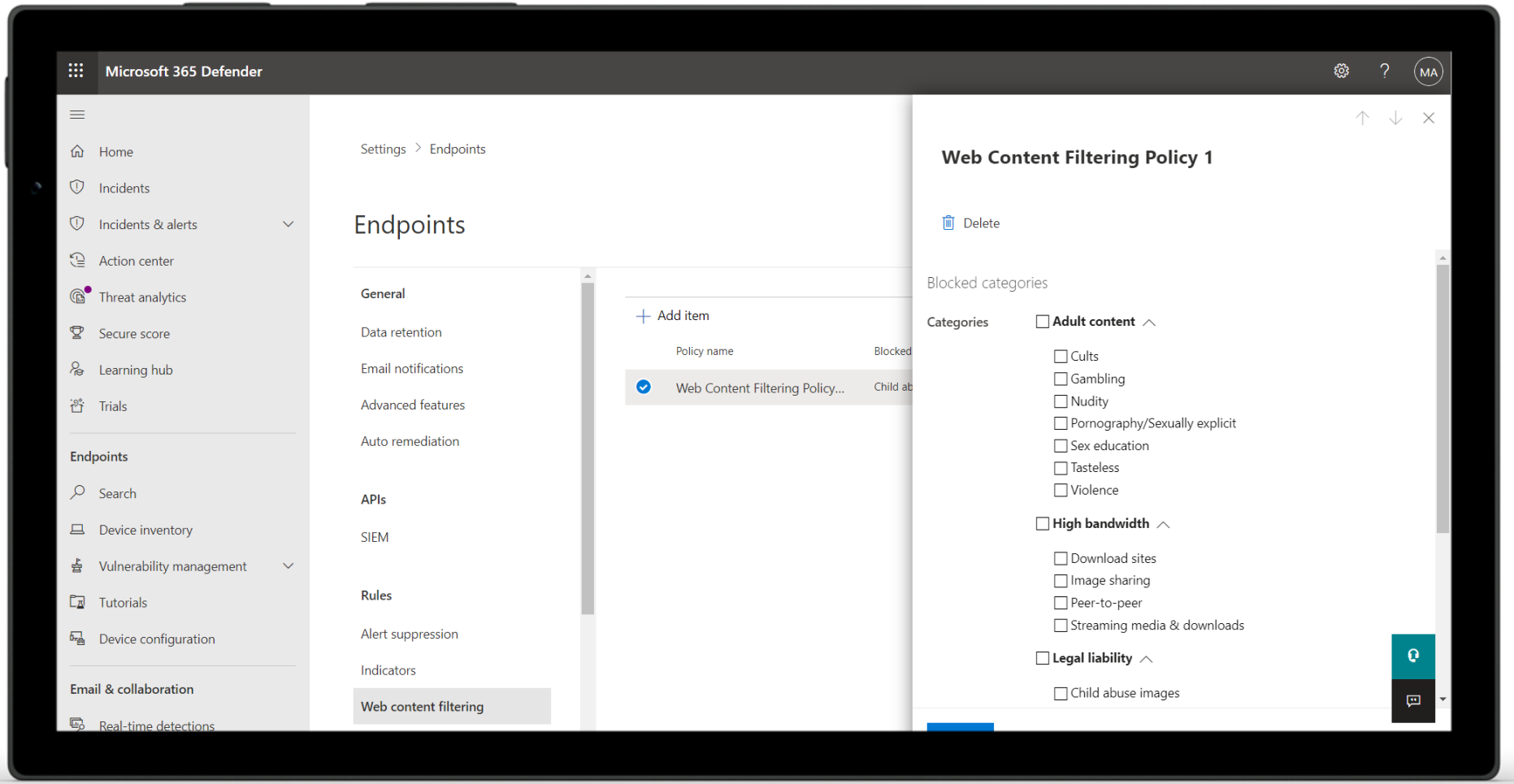
Select operating system to start onboarding process:

Windows 10 and 11

- Windows 7 SP1 and 8.1
- Windows 10 and 11
- Windows Server 2008 R2 SP1
- Windows Server 2012 R2 and 2016
- Windows Server 1803, 2019 and 2022
- macOS
- Linux Server
- iOS
- Android

DEMO

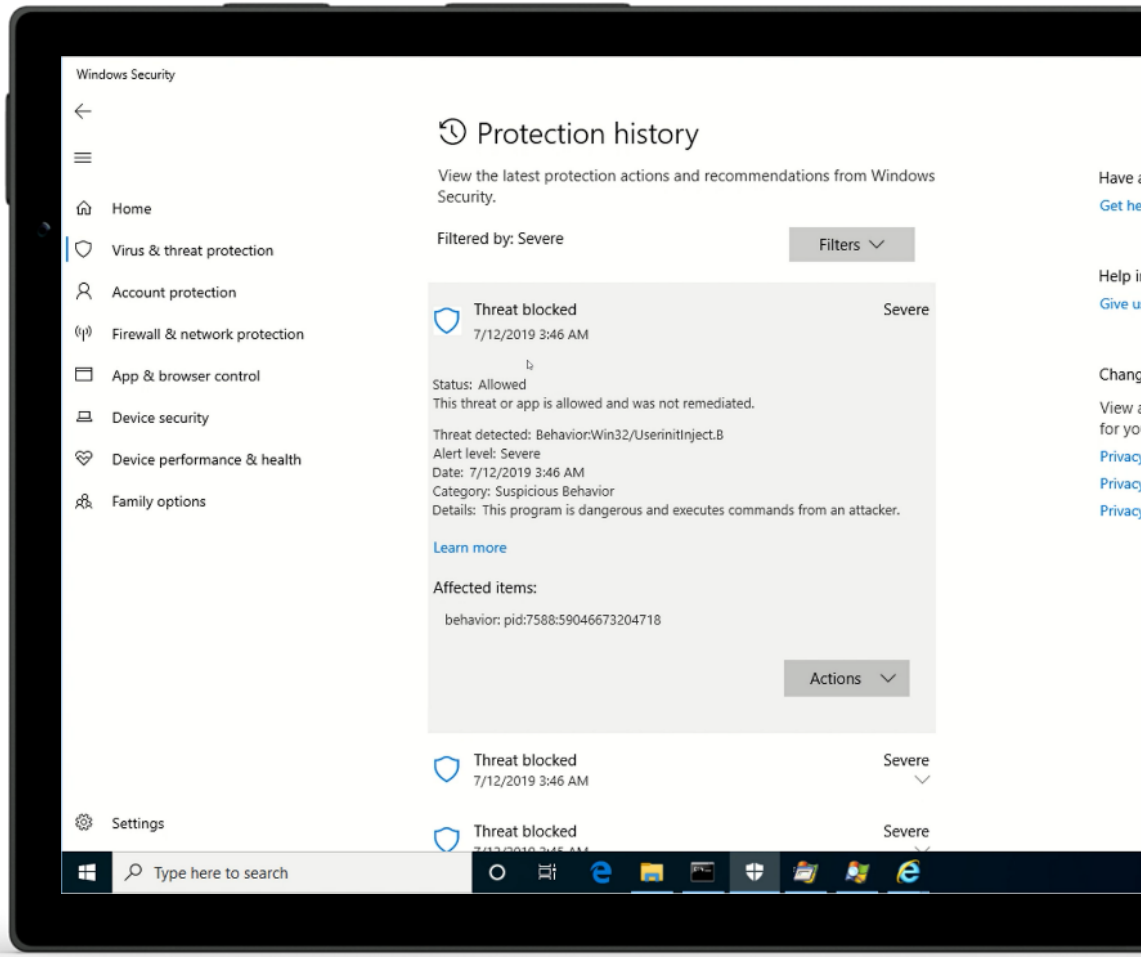
Web content filtering configuration



Next Generation Protection

Helps block and tackle sophisticated threats and malware

1. Behavioral based real-time protection
2. Blocks file-based and fileless malware
3. Stops malicious activity from trusted and untrusted applications



Microsoft Defender for Business next generation protection engines

Metadata-based ML
Stops new threats quickly by analyzing metadata

Behavior-based ML
Identifies new threats with process trees and suspicious behavior sequences

AMSI-paired ML
Detects fileless and in-memory attacks using paired client and cloud ML models

File classification ML
Detects new malware by running multi-class, deep neural network classifiers

Detonation-based ML
Catches new malware by detonating unknown files

Reputation ML
Catches threats with bad reputation, whether direct or by association

Smart rules
Blocks threats using expert-written rules

ML
Spots new and unknown threats using client-based ML models

Behavior monitoring
Identifies malicious behavior, including suspicious runtime sequence

Memory scanning
Detects malicious code running in memory

AMSI integration
Detects fileless and in-memory attacks

Heuristics
Catches malware variants or new strains with similar characteristics

Emulation
Evaluates files based on how they would behave when run

Network monitoring
Catches malicious network activities

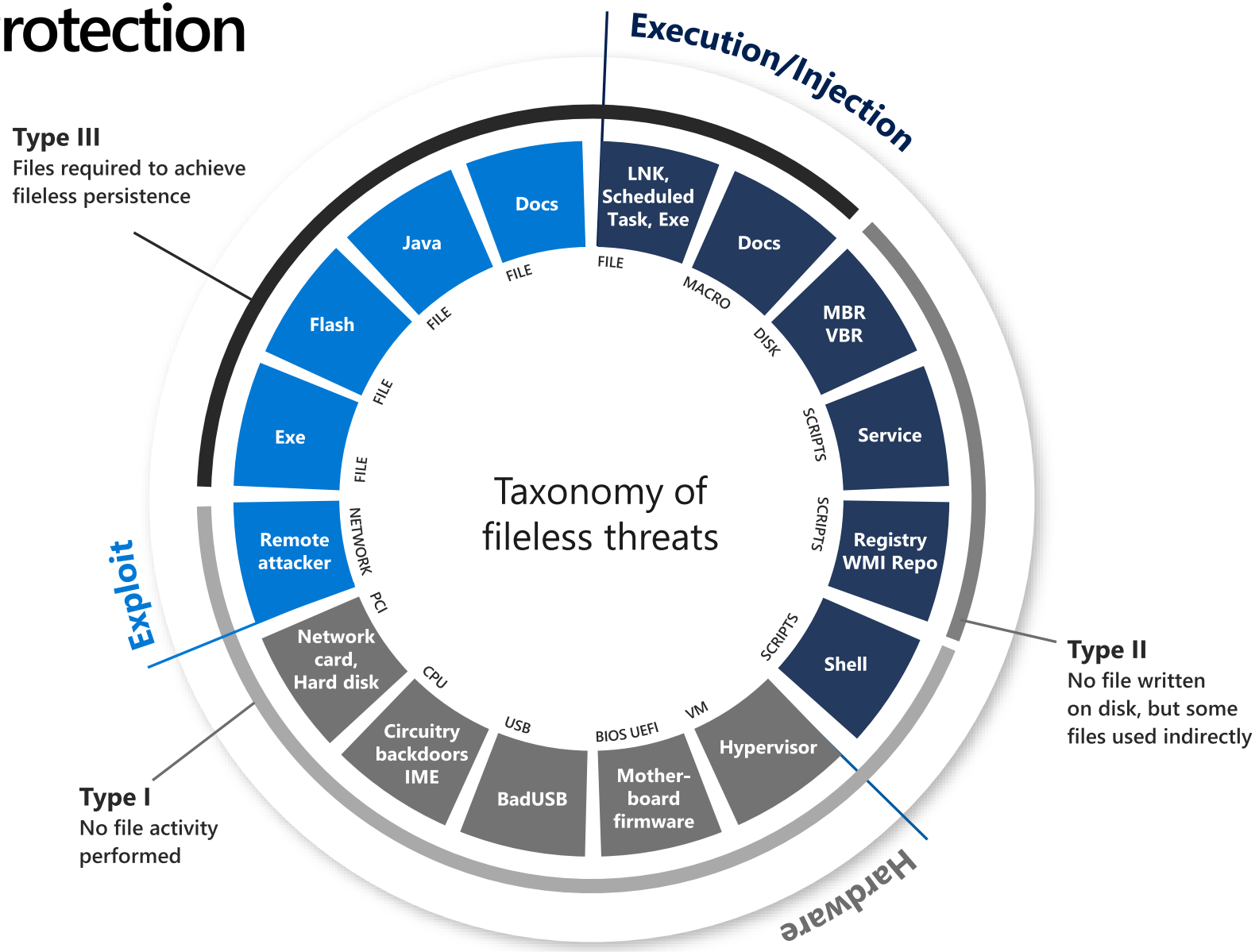
Innovations in Fileless Protection

→Dynamic and in context URL analysis to block call to malicious URL

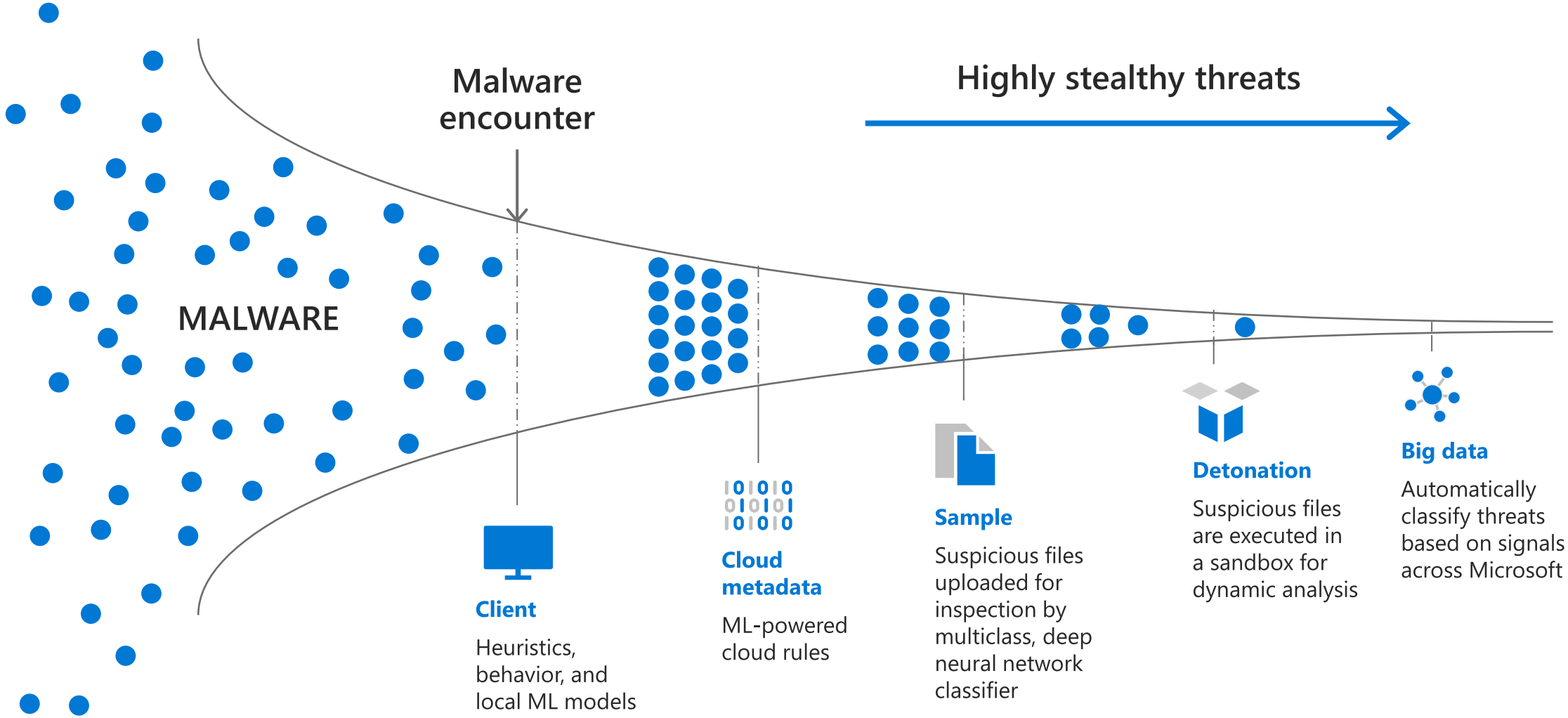
→AMSI-paired machine learning uses pairs of client-side and cloud-side models that integrate with Antimalware Scan Interface (AMSI) to perform advanced analysis of scripting behavior

→DNS exfiltration analysis

→Deep memory analysis



Microsoft Defender for Business' NGP protection pipeline



Dynamic: behavior monitoring

Monitors activity on:

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

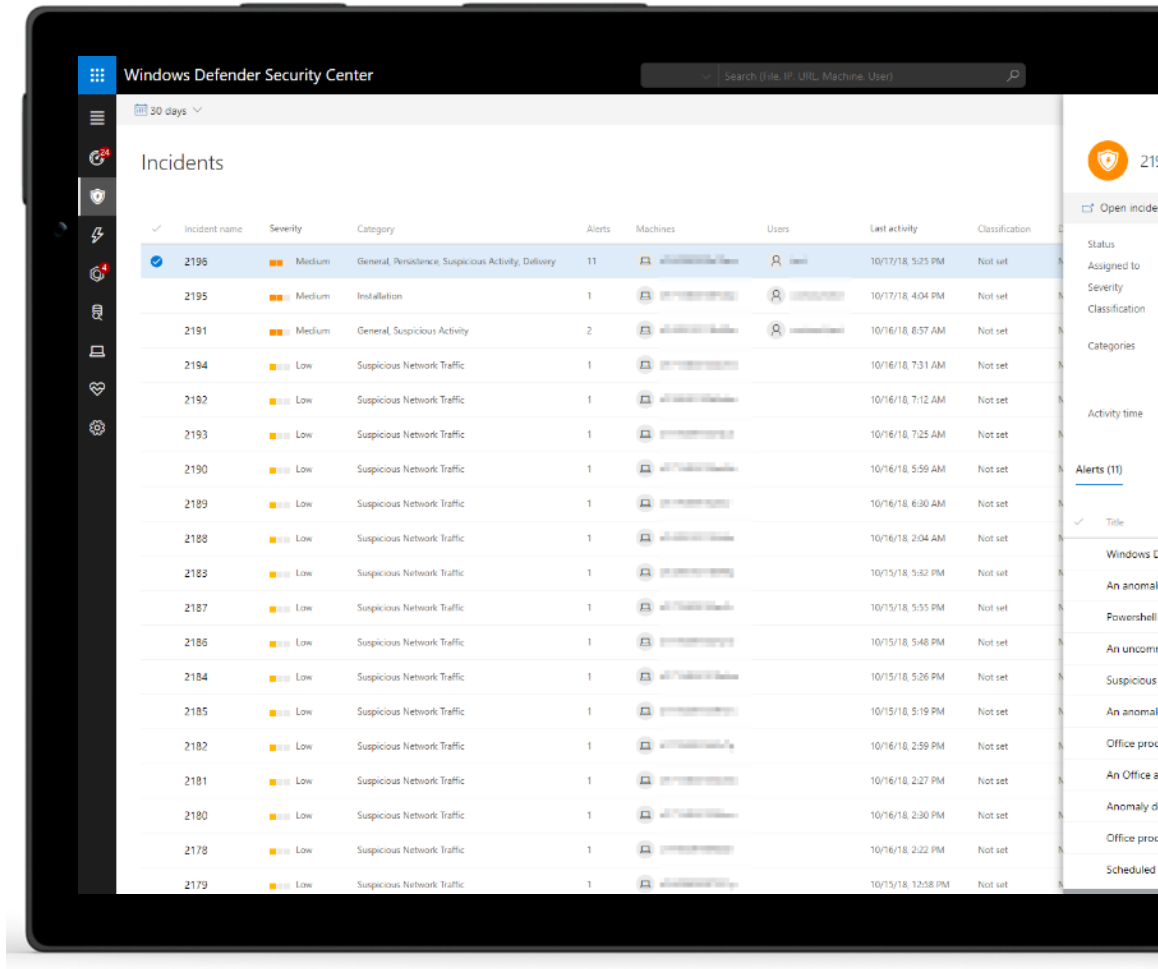
Heuristics can:

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

Endpoint Detection & Response

Detect and investigate advanced persistent attacks

1. Behavioral-based detection
2. Manual response actions for a device or file
3. Live response to gain access to devices



Incidents

Narrate the end-to-end attack story

Reconstructing the story

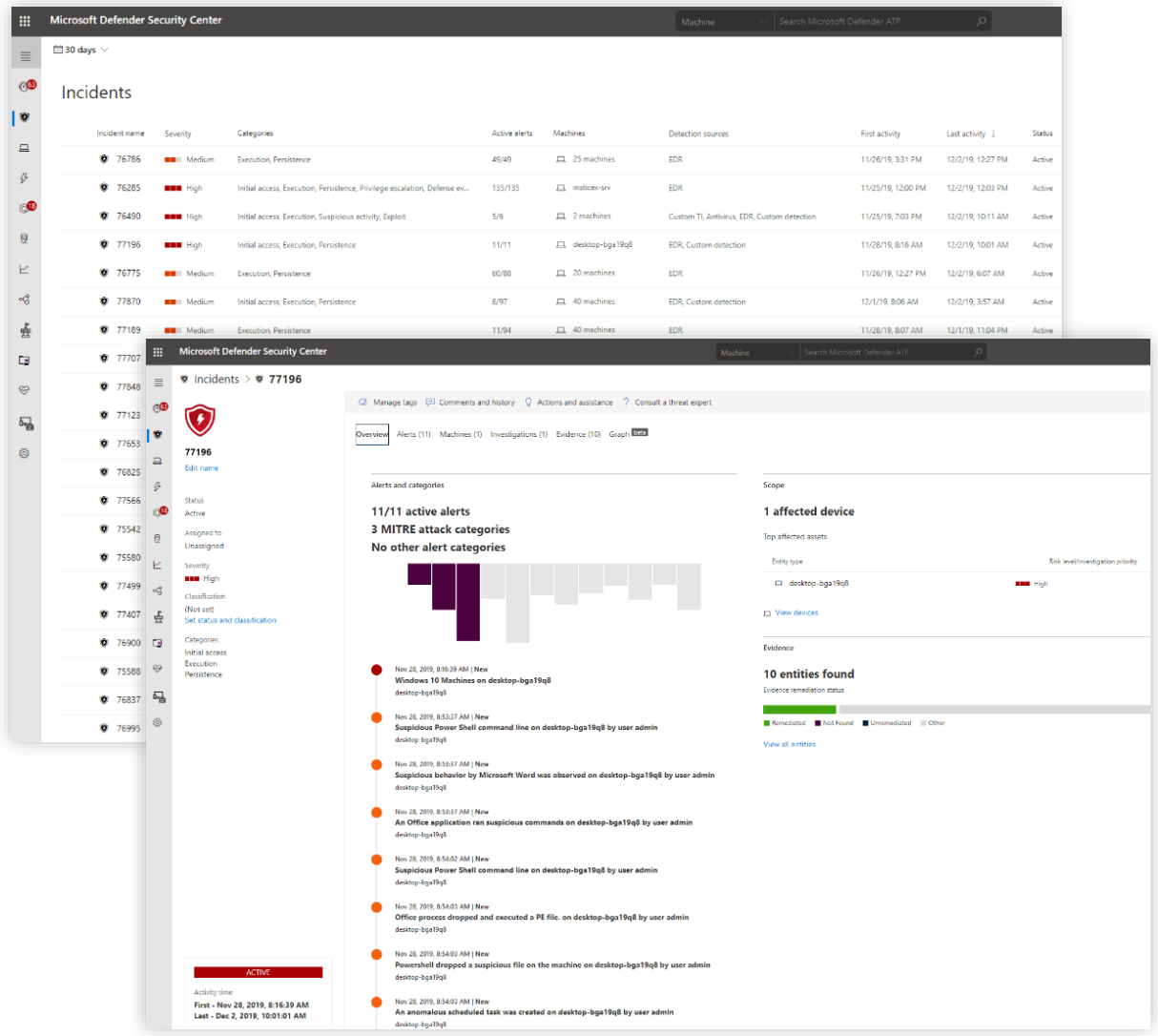
The broader attack story is better described when relevant alerts and related entities are brought together.

Incident scope

IT Admins receive better perspective on the purview of complex threats containing multiple entities.

Higher fidelity, lower noise

Effectively reduces the load and effort required to investigate and respond to attacks.



Live Response

→Real-time live connection to a remote system

→Leverage Microsoft Defender for Business Auto IR library (memory dump, MFT analysis, raw filesystem access, etc.)

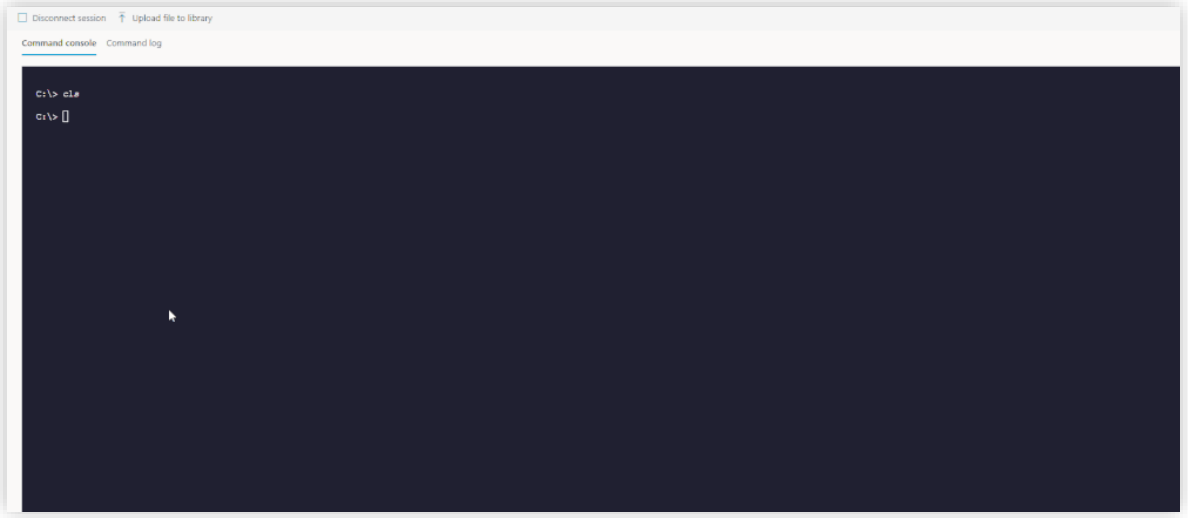
- Extended remediation command + easy undo

→Full audit

→Extendable (write your own command, build your own tool)

→RBAC+ Permissions

→Git-Repo (share your tools)



Threat Analytics

Delivering insight on major threats to your organization

Threat to posture view

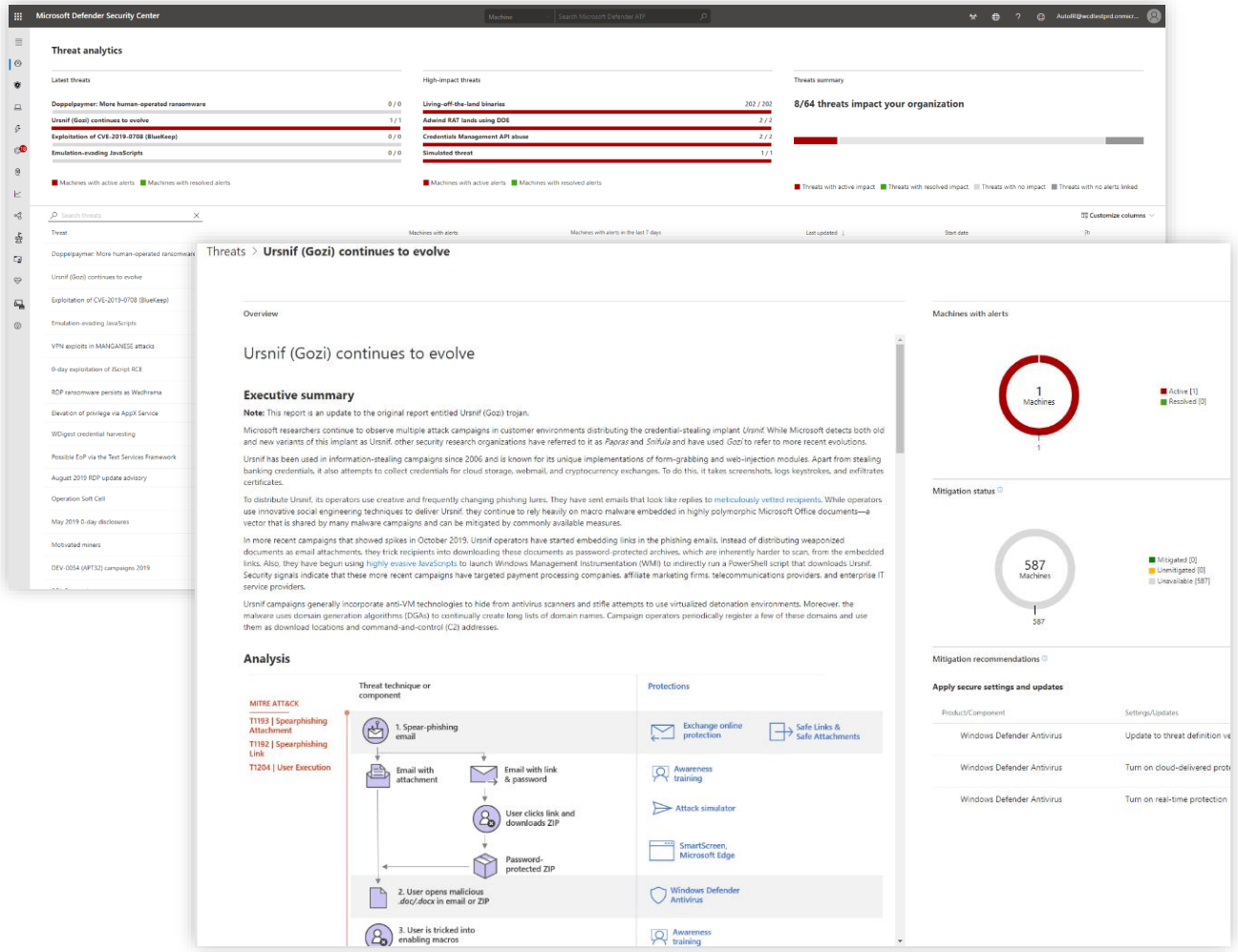
See how you score against significant and emerging campaigns with interactive reports.

Identify unprotected systems

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

Get guidance

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

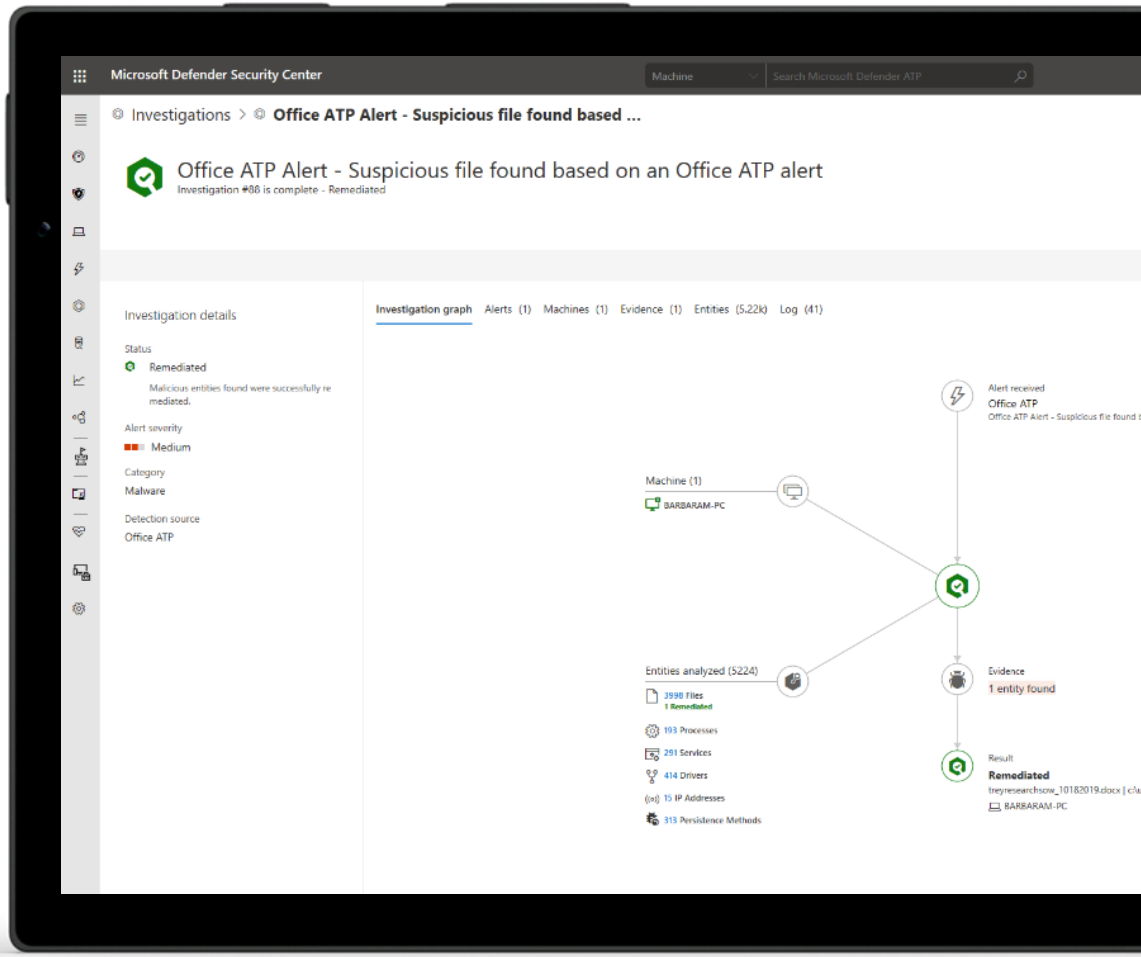


DEMO

Auto Investigation & Remediation

Automatically investigates alerts and helps to remediate complex threats

1. Mimics the ideal steps analysts would take
2. Tackles file or memory-based attacks
3. Scales security operations with 24x7 automated responses



What Is Microsoft Defender for Business Auto IR?

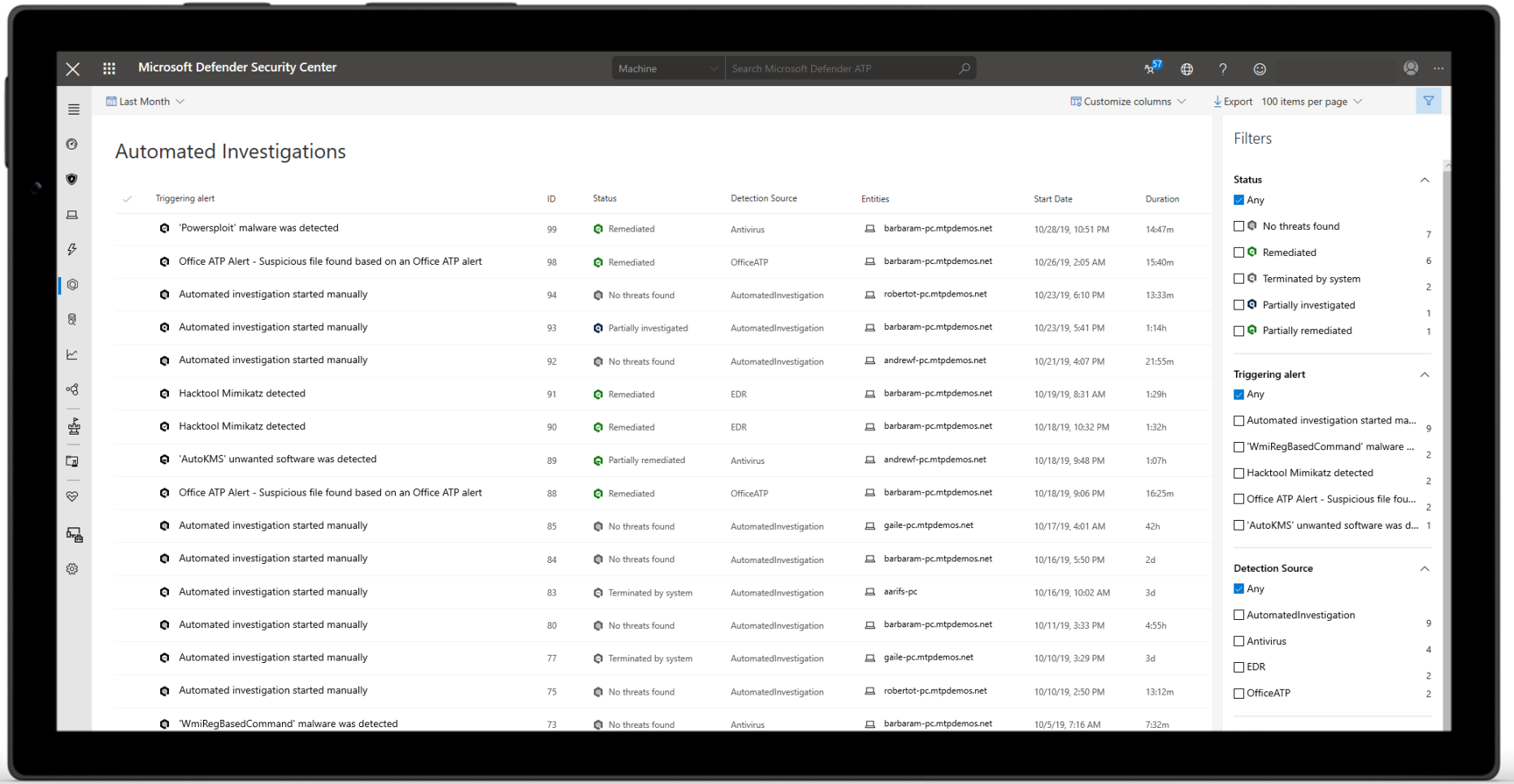
Security automation is…
mimicking the *ideal steps* a human would take *to investigate and remediate* a cyber threat

Security automation is not…
if machine has alert → auto-isolate

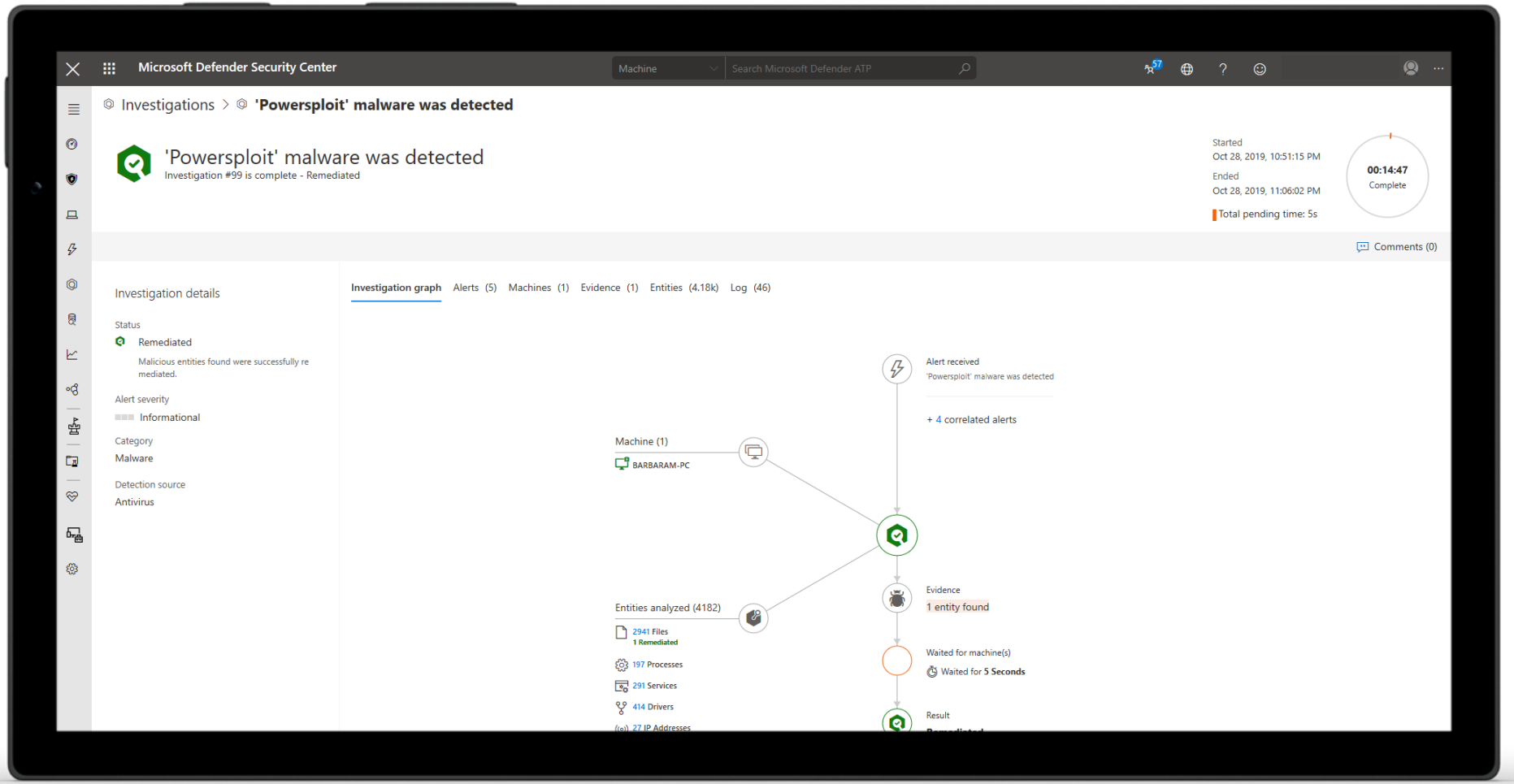
When we look at the steps an analyst is taking as when investigating and remediating threats we can identify the following high-level steps:

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

Auto investigation queue



Investigation graph



Partner APIs - Connecting with the platform

Microsoft Defender for Business

Elevate your security

Threat & Vulnerability Management

Attack Surface Reduction

Next Generation Protection

Endpoint Detection & Response

Auto Investigation & Remediation

APIs and Integration

Devices

Reporting

Apps

SIEM Data

Tools

DEMO

Built on the foundation of an industry leader in endpoint security

Gartner names Microsoft a Leader in 2021 Endpoint Protection Platforms Magic Quadrant.

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

Forrester names Microsoft a Leader in 2021 Endpoint Security Software as a Service Wave.

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

IDC names Microsoft a Leader for Modern Endpoint Security for Enterprise and Small and Midsize Businesses

Our antimalware capabilities consistently achieve high scores in independent tests.

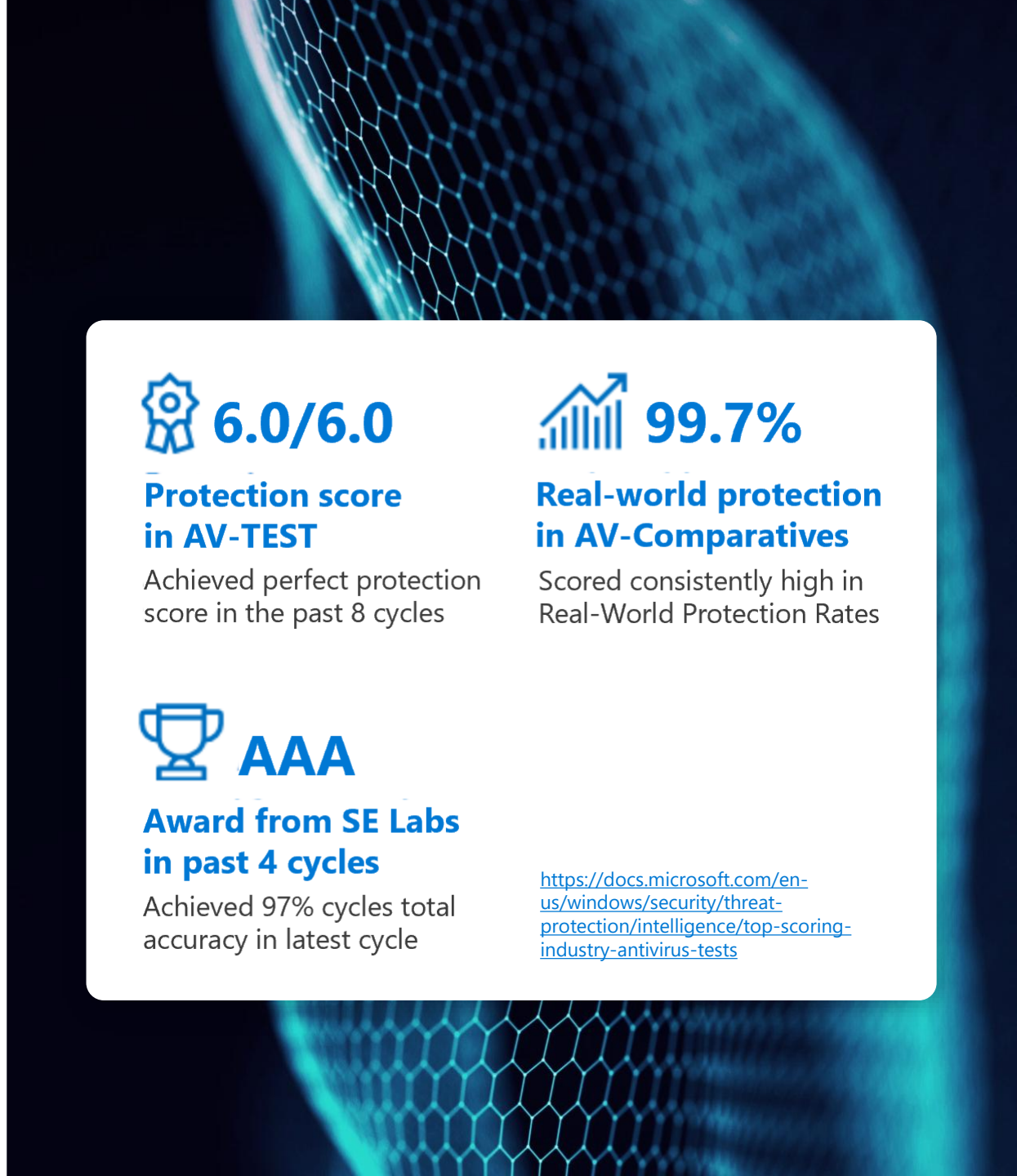
Microsoft won six security awards with Cyber Defense Magazine at RSAC 2021:

- Best Product Hardware Security
- Market Leader Endpoint Security
- Editor's Choice Extended Detection and Response (XDR)
- Most Innovative Malware Detection
- Cutting Edge Email Security

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment, Doc #US48306021. November 2021

Microsoft Defender consistently rated top AV

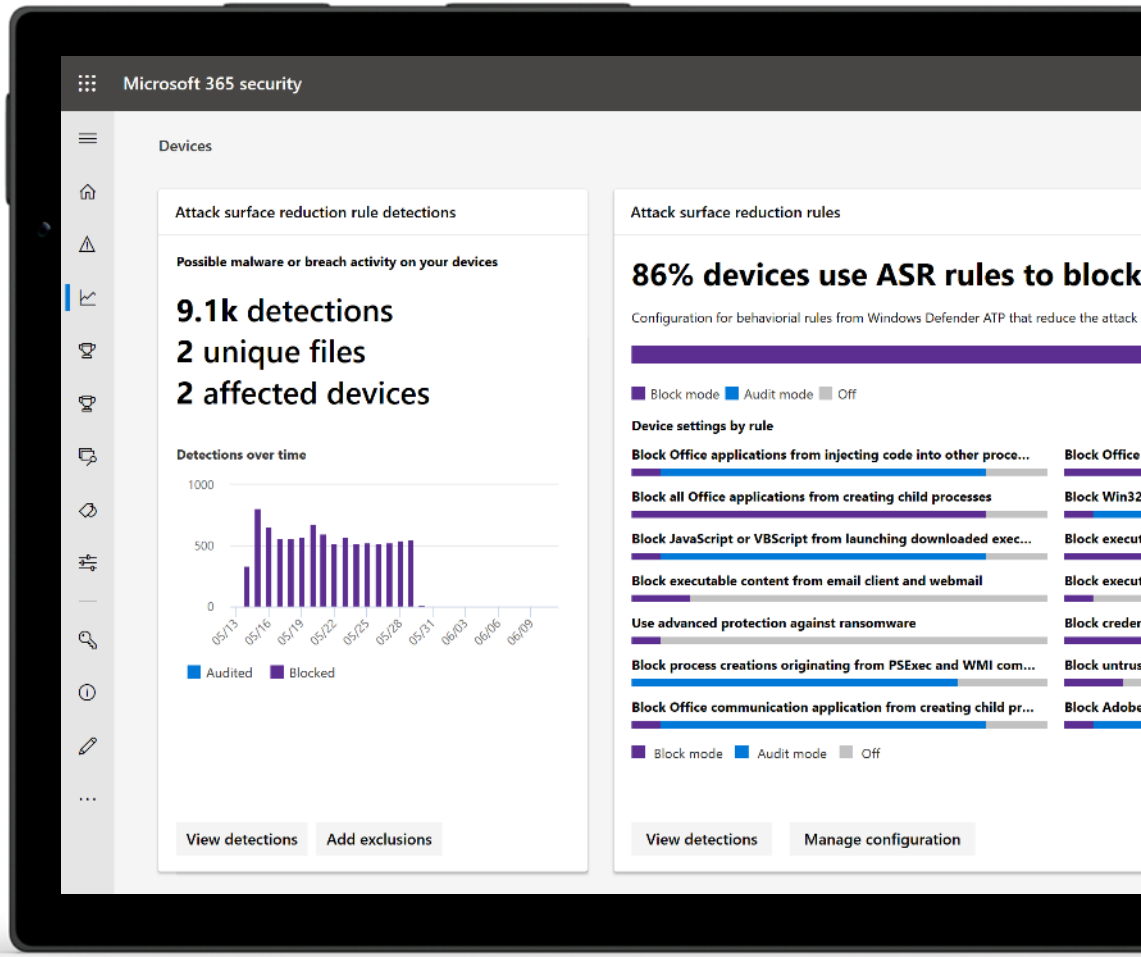
1. **AV-TEST**: Protection score of 6.0/6.0 in the latest test
2. **AV-Comparatives**: Protection rating of 99.7% in the latest test
3. **SE Labs**: AAA award in the latest test
4. **MITRE**: Industry-leading optics and detection capabilities



Attack Surface Reduction

Protect against risks by reducing the surface area of attack

1. System hardening without disruption
2. Customization that fits your business
3. 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

Attack surface reduction (ASR) rules help to control entry points to your Windows devices using cloud intelligence, 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

DEMO