



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



iOS



Windows 365
Azure Virtual Desktop

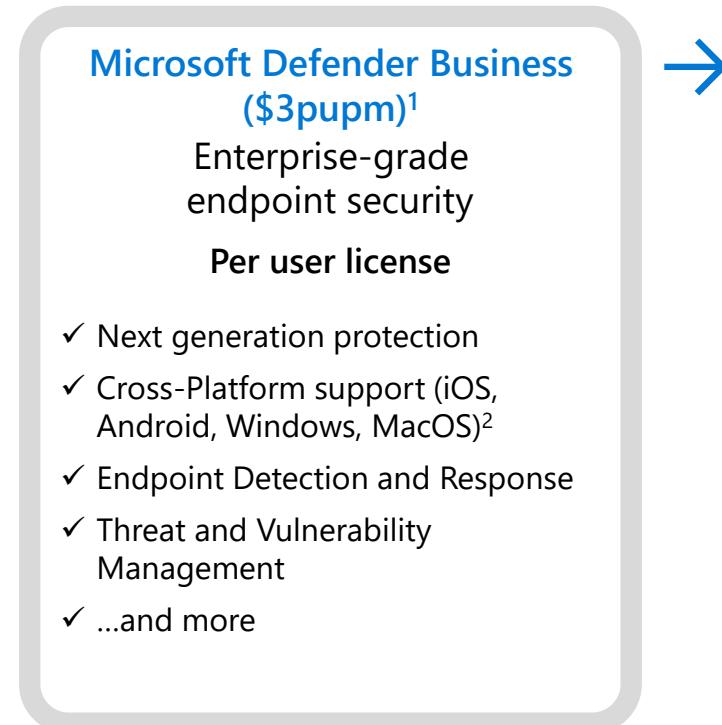
Endpoints and servers²

Mobile device OS¹

Virtual desktops

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

Microsoft Defender for Business is included in Business Premium



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](#).

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

²iOS, 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	Endpoint capabilities\SKU	< 300 seats	> 300 seats	
		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. ³Requires Microsoft Intune. Intune is included in Microsoft 365 Business Premium. ⁴Requires separate server license. Please see [Documentation](#) for more detail.

Defender for Business

brings enterprise grade endpoint security to Microsoft 365 Business Premium

brings enterprise grade endpoint security to Microsoft 365 Business Premium

¹Limited. 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.

		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	•	•	
Identity and Access Management and Security	Mobile App Management	•	•	
	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	• ⁴
	Automated investigation and response	• ²	• ²	• ²
	Threat and vulnerability	•	•	•
	Threat intelligence	• ²	• ²	• ²



Microsoft Security— a Leader in 5 Gartner Magic Quadrant reports



*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

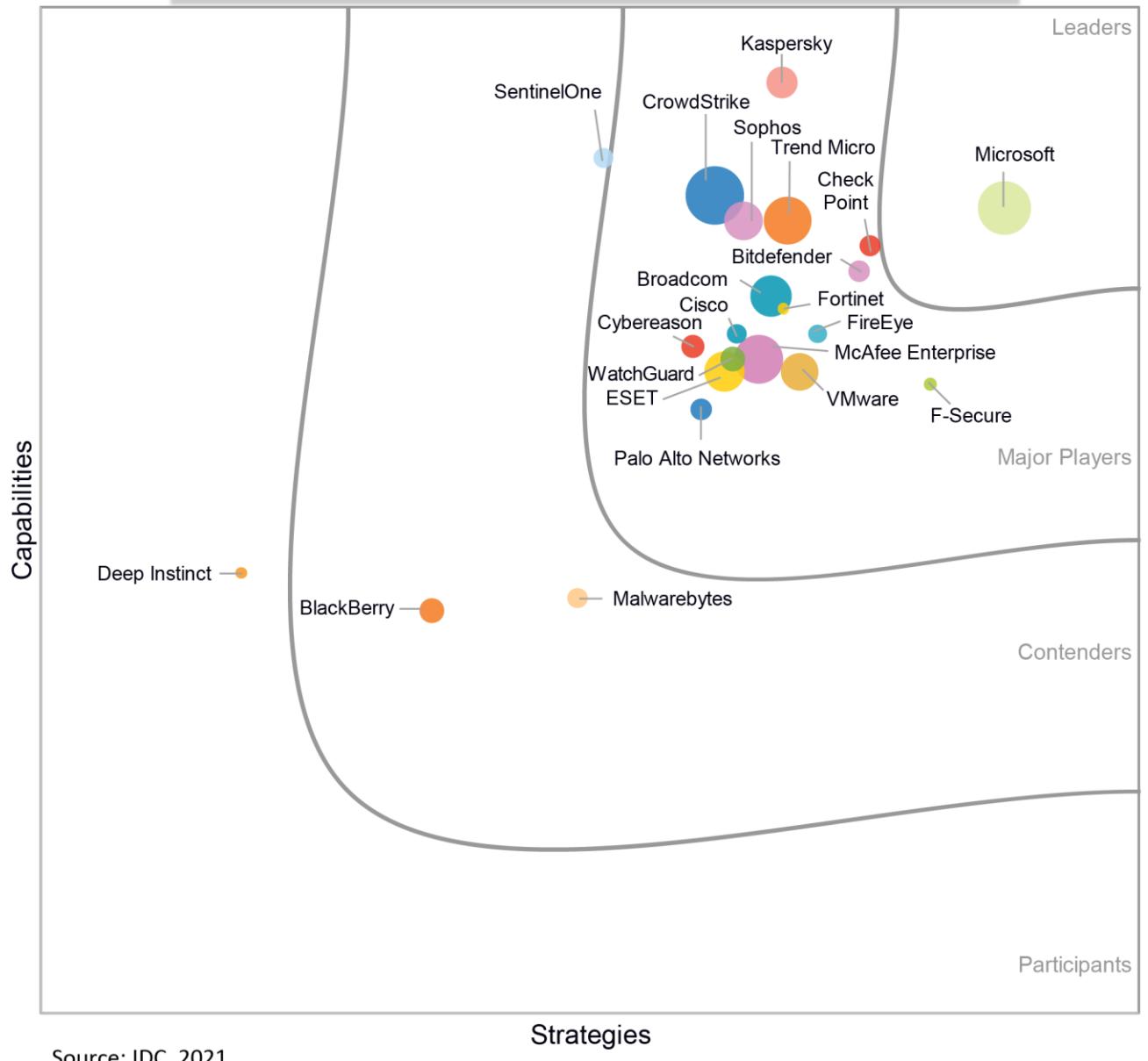
These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

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 Assessment <https://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](#)

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses, 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.

How do you want to onboard your devices?

We noticed that you are using Microsoft Endpoint Manager (MEM), with # devices enrolled. This means we can make the onboarding process automatic for you.

Choose between the automatic or manual onboarding process now. If you change your mind later, you can choose the other option in Settings > Onboarding. Learn more about [Onboarding options](#).

Automatic onboarding process (recommended)
The automatic onboarding process includes the following steps:

- Sets up a connection between Microsoft Defender for Business and MEM
- Onboards all Windows 10 devices that are enrolled in MEM to Microsoft Defender for Business

Manual onboarding process
You can choose from several configuration packages and methods to onboard devices. Choose the method that best suits your business needs.

Back Continue

Initial setup



Home

Incidents

Incidents & alerts



Actions & submissions



Threat analytics

Secure score

Learning hub

Trials

Endpoints



Device inventory

Vulnerability management



Tutorials

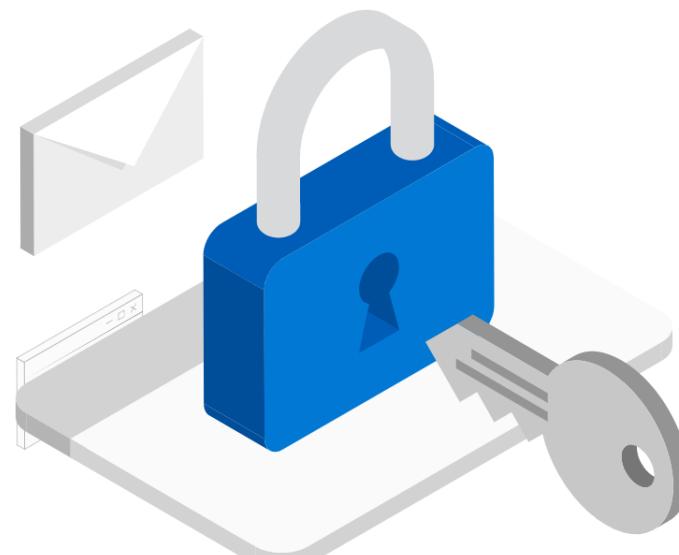
Configuration management



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

Type user or group name

Role

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
MOD Administrator	Security admin
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

+ Add recipients

Notification type



Alerts

Vulnerabilities

Alerts & vulnerabilities

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

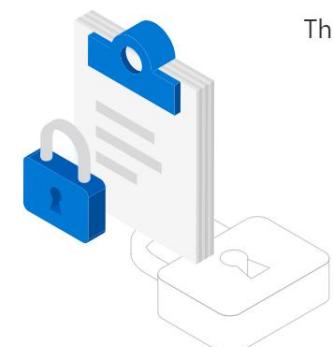
Cancel

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



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)

Adele Vance

Security admin (1)

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

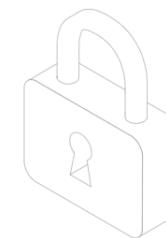


Back

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..



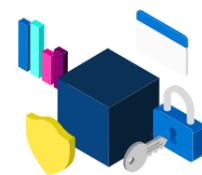
Done



- 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

Settings > Endpoints

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 > Endpoint security



Endpoint security | Microsoft Defender for Endpoint

X

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Search (Ctrl+ /)

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.

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

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

On

MDM Compliance Policy Settings

Connect Android devices to Microsoft Defender for Endpoint

On

Connect iOS devices to Microsoft Defender for Endpoint

On

Connect Windows devices to Microsoft Defender for Endpoint

On

Enable App Sync for iOS/iPadOS Devices

On

Send full application inventory data on personally-owned iOS/iPadOS Devices

On

Block unsupported OS versions

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

Settings > Endpoints

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 config
matches your [preferred deployment method](#). For other device preparation instruc
[set up](#).

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

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

The screenshot shows the Microsoft 365 Defender web interface. The left sidebar is titled "Microsoft 365 Defender" and includes sections for Home, Incidents, Threat analytics, Secure score, Learning hub, Trials, Endpoints, Search, Device inventory, Vulnerability management, Tutorials, Device configuration, Email & collaboration, and Real-time detections. The "Endpoints" section is currently selected. The main content area is titled "Settings > Endpoints" and shows the "Endpoints" configuration page. On the left of this page, there are sections for General (Data retention, Email notifications, Advanced features, Auto remediation), APIs, SIEM, Rules (Alert suppression, Indicators), and Web content filtering (which is highlighted in gray). In the center, there is a table titled "Add item" with columns for "Policy name" and "Blocked". A row is selected with the value "Web Content Filtering Policy..." under "Policy name". On the right, the "Web Content Filtering Policy 1" configuration is displayed, showing a "Delete" button and a list of "Blocked categories" under "Categories". The "Adult content" category is expanded, showing sub-categories like Cults, Gambling, Nudity, Pornography/Sexually explicit, Sex education, Tasteless, and Violence. Other collapsed categories include "High bandwidth" (Download sites, Image sharing, Peer-to-peer, Streaming media & downloads) and "Legal liability" (Child abuse images).



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

The screenshot shows the Windows Security app interface. On the left, a sidebar lists options: Home, Virus & threat protection (selected), Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main area is titled "Protection history" with the sub-header "View the latest protection actions and recommendations from Windows Security." It is filtered by "Severe". A list of threats blocked is shown:

Threat blocked	Date	Status
7/12/2019 3:46 AM	Severity: 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.
7/12/2019 3:46 AM	Severity: 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.
7/12/2019 3:46 AM	Severity: 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.

At the bottom, there is a search bar "Type here to search" and a taskbar with various icons.



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



Cloud



Client



ML

Spots new and unknown threats using client-based ML models



Behavior monitoring

Identifies malicious behavior, including suspicious runtime sequence



Memory scanning

Detects malicious code running in memory



AMSI integration

Detects fileless and in-memory attacks



Heuristics

Catches malware variants or new strains with similar characteristics



Emulation

Evaluates files based on how they would behave when run

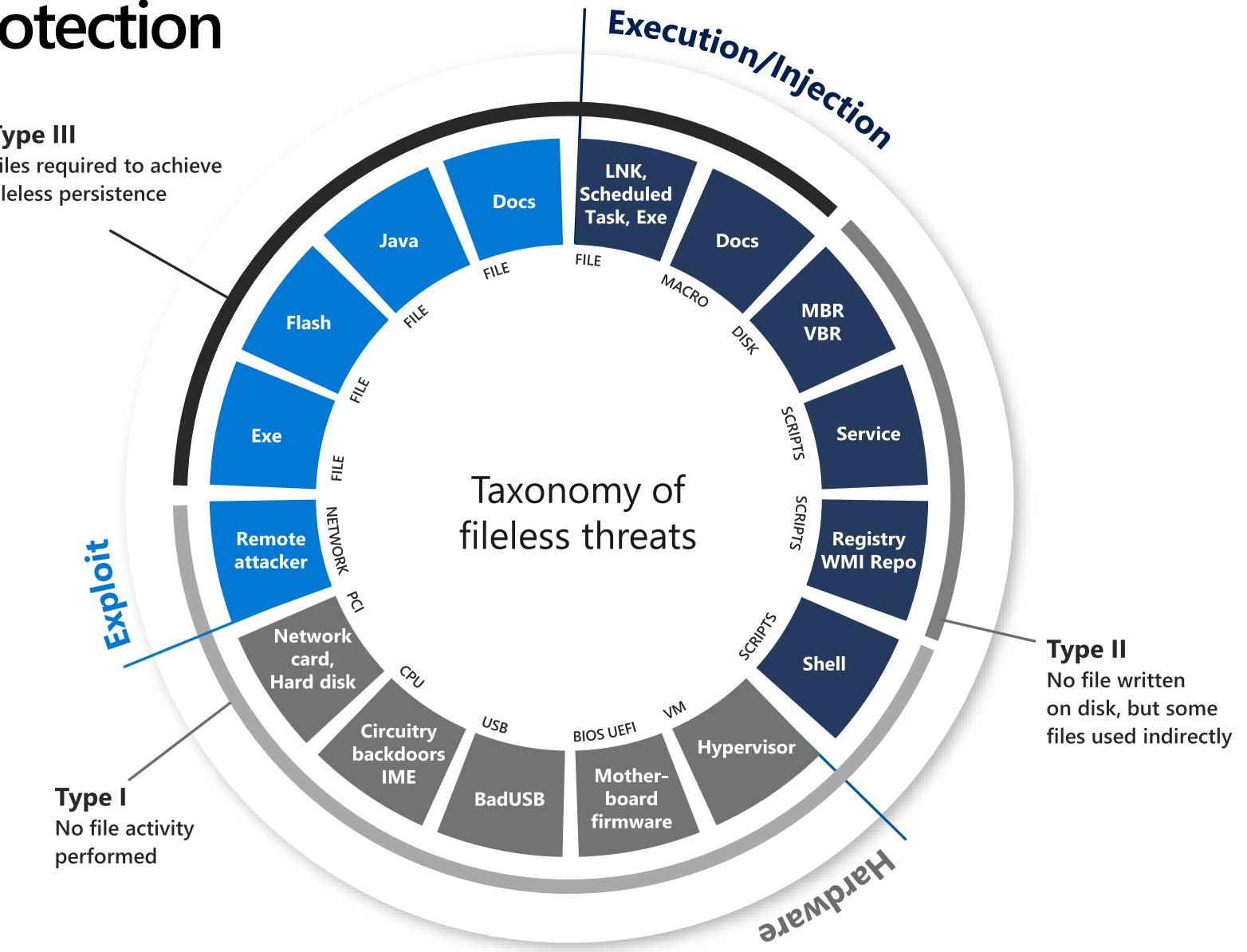


Network monitoring

Catches malicious network activities

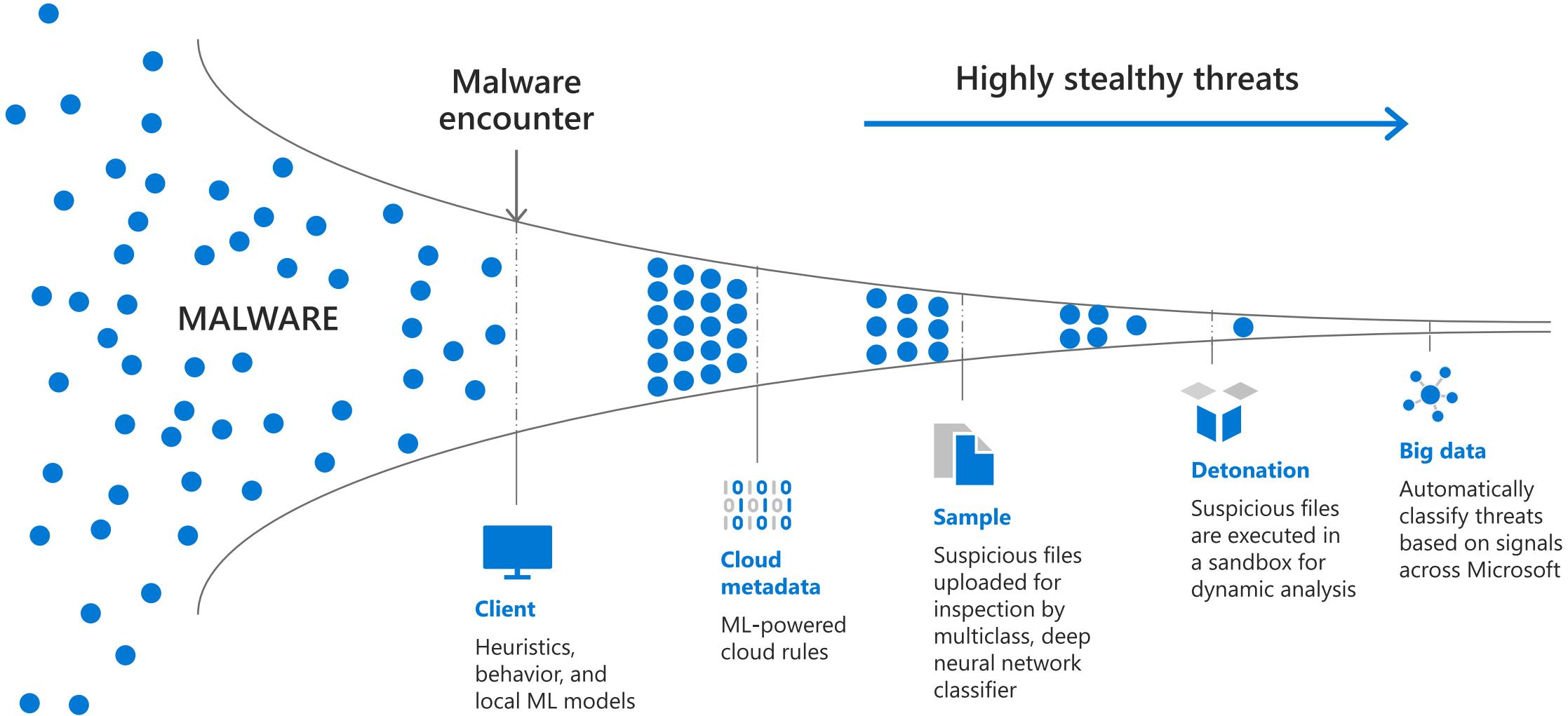
Innovations in Fileless Protection

- Dynamic and in context URL analysis to block call to malicious URL
- AMSI-paired machine learning uses pairs of client-side and cloud-side models that integrate with Antimalware Scan Interface ([AMSI](#)) to perform advanced analysis of scripting behavior
- DNS exfiltration analysis
- Deep memory analysis





Microsoft Defender for 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

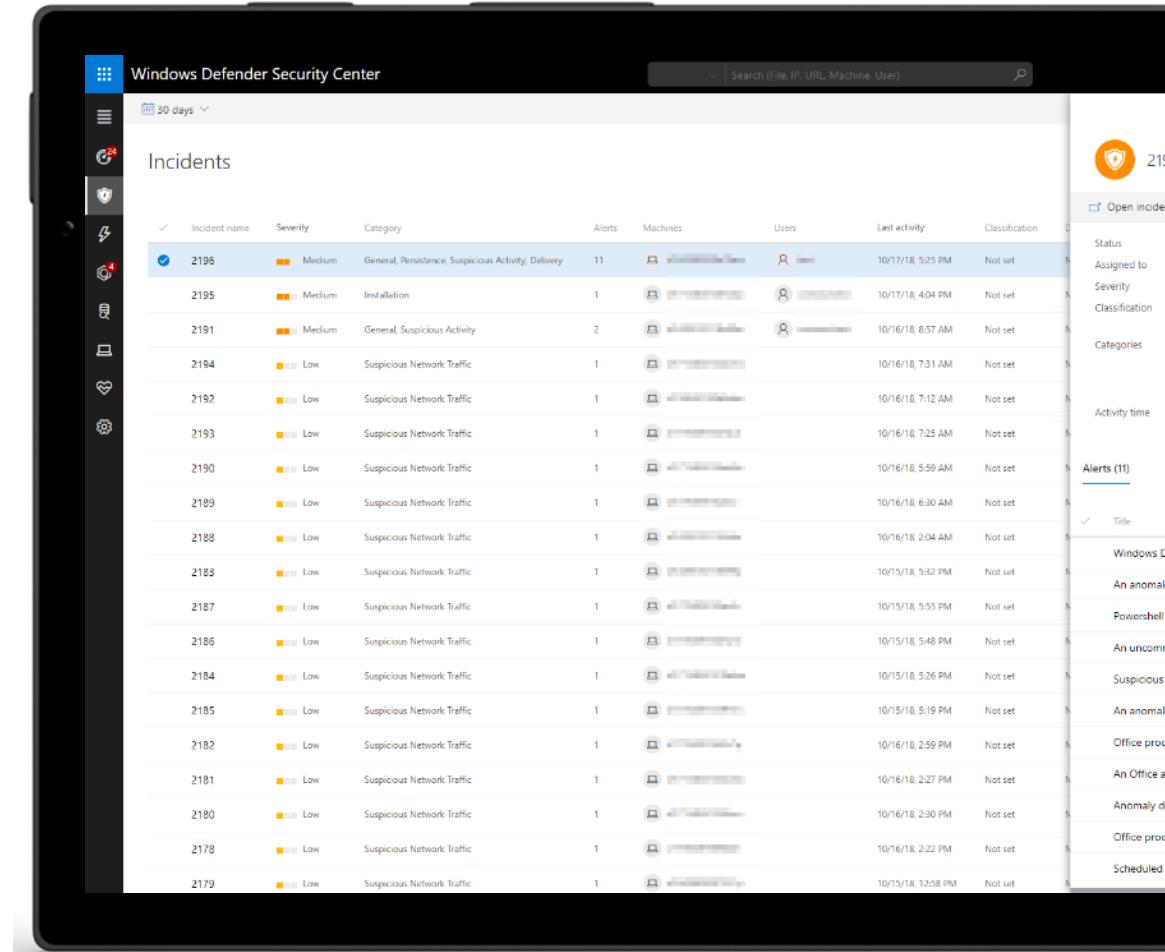
Behavioral-based detection

2

Manual response actions for a device or file

3

Live response to gain access to devices



A screenshot of the Windows Defender Security Center interface. The main area shows a list of 'Incidents' with 2199 entries. The columns include Incident name, Severity, Category, Alerts, Machines, Users, Last activity, Classification, and Status. Most incidents are labeled as 'Medium' severity and 'Suspicious Network Traffic'. On the right side, there are various navigation links and status indicators, such as 'Open incident' (2199), 'Alerts (11)', and 'Windows Defender Protection (11)'.

Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification	Status
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]	[redacted]	10/16/18, 7:31 AM	Not set	N
2192	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 7:12 AM	Not set	N
2193	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 7:25 AM	Not set	N
2190	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 5:59 AM	Not set	N
2189	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 6:20 AM	Not set	N
2188	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 2:04 AM	Not set	N
2183	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/15/18, 5:52 PM	Not set	N
2187	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/15/18, 5:55 PM	Not set	N
2186	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/15/18, 5:48 PM	Not set	N
2184	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/15/18, 5:26 PM	Not set	N
2185	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/15/18, 5:19 PM	Not set	N
2182	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 2:59 PM	Not set	N
2181	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 2:27 PM	Not set	N
2180	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 2:30 PM	Not set	N
2178	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/16/18, 2:22 PM	Not set	N
2179	Low	Suspicious Network Traffic	1	[redacted]	[redacted]	10/15/18, 12:58 PM	Scheduled	N



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.

The screenshot displays the Microsoft Defender Security Center interface. The top navigation bar includes 'Machine' and a search bar for 'Search Microsoft Defender ATP'. Below the navigation is a table titled 'Incidents' showing a list of detected threats over a 30-day period. The table columns include 'Incident name', 'Severity', 'Categories', 'Active alerts', 'Machines', 'Detection sources', 'First activity', 'Last activity', and 'Status'. Below the table, a specific incident is selected (ID 77196). The right pane provides a detailed view of this incident, including 'Alerts and categories' (11 active alerts, 3 MITRE attack categories), 'Scope' (affected device: desktop-bga19q8), and 'Evidence' (10 entities found, remediation status: Remediated, Not Found, Unremediated, Other). The bottom of the detailed view shows a timeline of recent activities on the machine.

Incident name	Severity	Categories	Active alerts	Machines	Detection sources	First activity	Last activity	Status
76785	Medium	Execution, Persistence	46/49	25 machines	EDR	11/26/19, 3:31 PM	12/2/19, 1:27 PM	Active
76285	High	Initial access, Execution, Persistence, Privilege escalation, Defense evasion	135/135	1 machine	EDR	11/25/19, 12:00 PM	12/2/19, 12:03 PM	Active
76490	High	Initial access, Execution, Suspicious activity, Exploit	5/6	2 machines	Custom TI, Antivirus, EDR, Custom detection	11/25/19, 7:03 PM	12/2/19, 10:11 AM	Active
77196	High	Initial access, Execution, Persistence	11/11	1 machine	EDR, Custom detection	11/28/19, 8:16 AM	12/2/19, 10:01 AM	Active
76775	Medium	Execution, Persistence	60/68	20 machines	EDR	11/26/19, 12:27 PM	12/2/19, 6:07 AM	Active
77870	Medium	Initial access, Execution, Persistence	8/97	40 machines	EDR, Custom detection	12/1/19, 8:06 AM	12/2/19, 3:57 AM	Active
77189	Medium	Execution, Persistence	11/94	40 machines	EDR	11/28/19, 8:07 AM	12/1/19, 11:04 PM	Active
77707								

Incident Details for ID 77196:

Alerts and categories:
11/11 active alerts
3 MITRE attack categories
No other alert categories

Scope:
Affected device: desktop-bga19q8

Evidence:
10 entities found

Entity type: desktop-bga19q8

Risk level/investigation priority: High

Timeline of recent activities:

- Nov 28, 2019, 8:56:39 AM | New Windows 10 Machines on desktop-bga19q8
- Nov 28, 2019, 8:56:37 AM | New Suspicious Power Shell command line on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:56:37 AM | New Suspicious behavior by Microsoft Word was observed on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:56:37 AM | New An Office application ran suspicious commands on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New Suspicious Power Shell command line on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New Office process dropped and executed a PE file. on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New Powershell dropped a suspicious file on the machine on desktop-bga19q8 by user admin
- Nov 28, 2019, 8:54:02 AM | New An anomalous scheduled task was created on desktop-bga19q8 by user admin

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



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.)

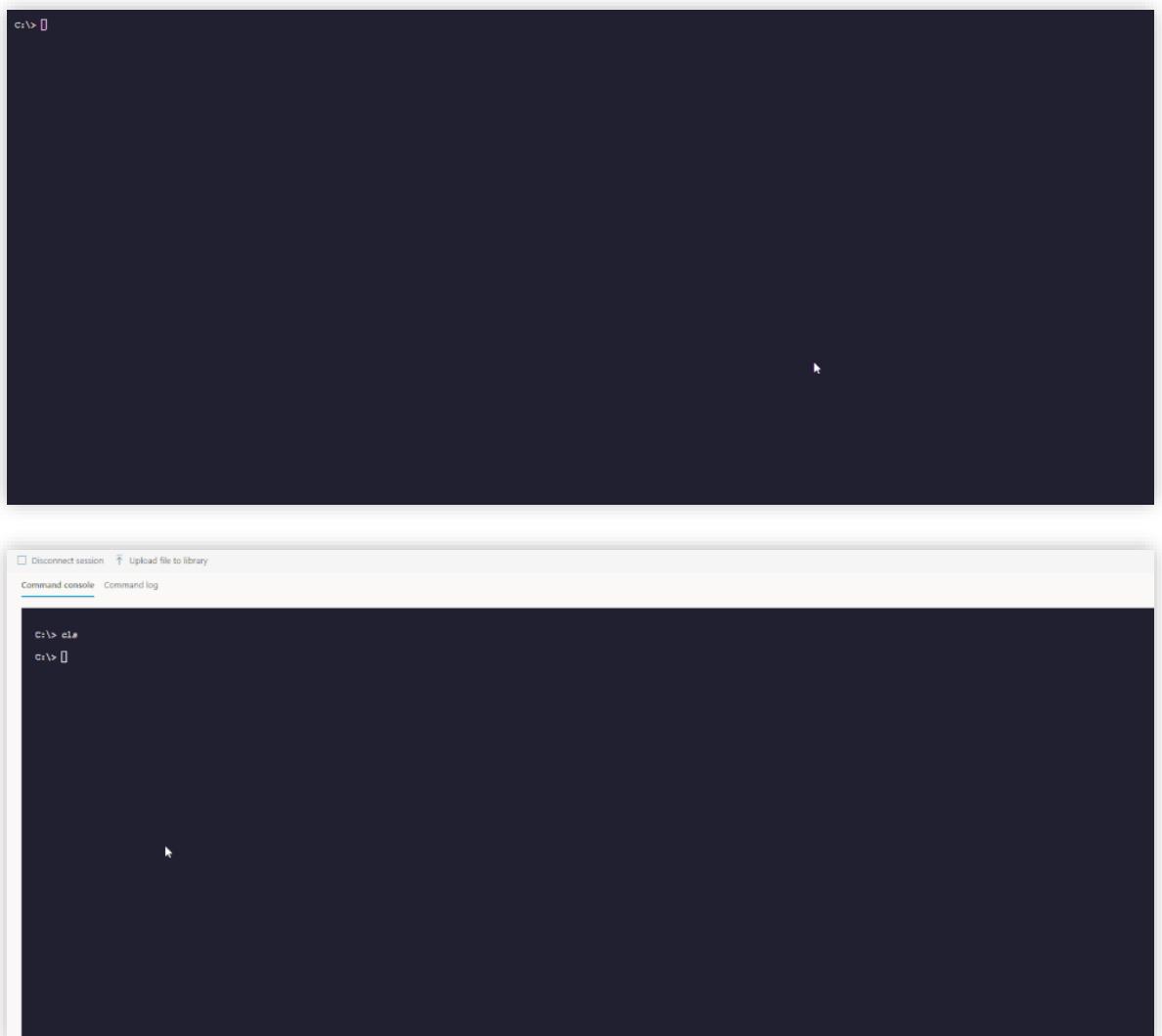
- Extended remediation command + easy undo

→ 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.

The screenshot displays the Microsoft Defender Security Center interface, specifically the Threat analytics section. It shows a summary of threats across the organization, including a count of 8/64 threats impacting the organization. The interface includes sections for Latest threats, High-impact threats, and Threats summary. A detailed report for the Ursnif (Gozi) threat is shown, providing an overview, executive summary, and analysis of threat techniques and protections. The analysis section details a spear-phishing attack flow involving Exchange online protection, Safe Links & Safe Attachments, Awareness training, Attack simulator, SmartScreen, Microsoft Edge, Windows Defender Antivirus, and Awareness training. The interface also tracks machine status with 1 active machine and 587 total machines, and provides mitigation status and recommendations for Windows Defender Antivirus settings.

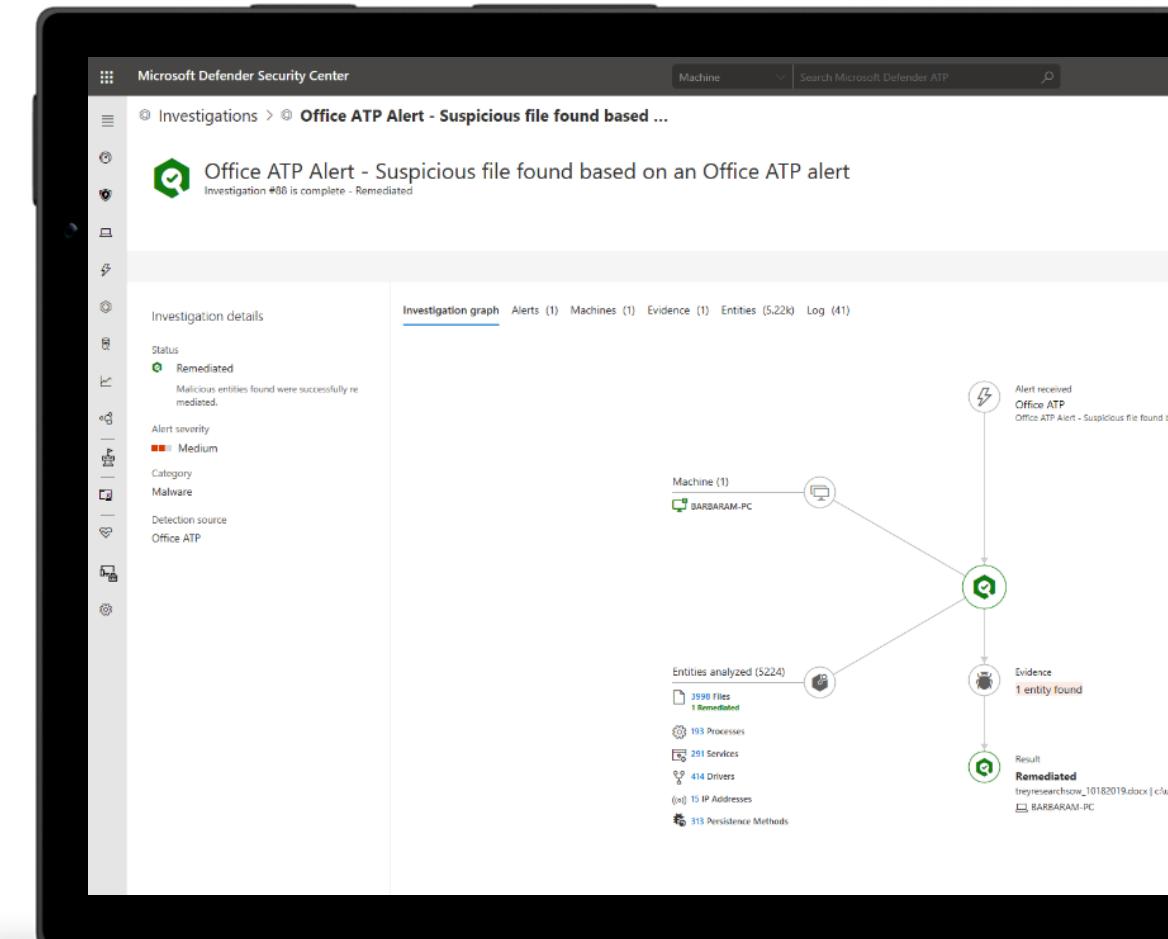
DEMO



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

Microsoft Defender Security Center

Last Month

Automated Investigations

Triggering alert	ID	Status	Detection Source	Entities	Start Date	Duration
'Powersploit' malware was detected	99	Remediated	Antivirus	bararam-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	bararam-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	bararam-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	bararam-pc.mtpdemos.net	10/19/19, 8:31 AM	1:29h
Hacktool Mimikatz detected	90	Remediated	EDR	bararam-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	bararam-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	bararam-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	bararam-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	bararam-pc.mtpdemos.net	10/5/19, 7:16 AM	7:32m

Customize columns Export 100 items per page

Filters

Status

Any

No threats found 7

Remediated 6

Terminated by system 2

Partially investigated 1

Partially remediated 1

Triggering alert

Any

Automated investigation started ma... 9

'WmiRegBasedCommand' malwar... 2

Hacktool Mimikatz detected 2

Office ATP Alert - Suspicious file fou... 2

'AutoKMS' unwanted software was d... 1

Detection Source

Any

AutomatedInvestigation 9

Antivirus 4

EDR 2

OfficeATP 2



Investigation graph

Microsoft Defender Security Center

Machine | Search Microsoft Defender ATP

Investigations > 'Powersploit' malware was detected

'Powersploit' malware was detected
Investigation #99 is complete - Remediated

Started Oct 28, 2019, 10:51:15 PM
Ended Oct 28, 2019, 11:06:02 PM
Total pending time: 5s

00:14:47 Complete

Comments (0)

Investigation details

- Status: Remediated (Malicious entities found were successfully remediated.)
- Alert severity: Informational
- Category: Malware
- Detection source: Antivirus

Investigation graph

Alert received: 'Powersploit' malware was detected + 4 correlated alerts

Machine (1): BARBARAM-PC

Entities analyzed (4182):

- 2941 Files (1 Remediated)
- 197 Processes
- 291 Services
- 414 Drivers
- (o) 27 IP Addresses

Evidence: 1 entity found

Waited for machine(s)
Waited for 5 Seconds

Result: Remediated

```
graph TD; Alert((Alert received: 'Powersploit' malware was detected + 4 correlated alerts)) --> Machine((Machine (1): BARBARAM-PC)); Machine --> Entities((Entities analyzed (4182))); Entities --> Evidence((Evidence: 1 entity found)); Evidence --> Result((Result: Remediated))
```



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

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner content described herein (the "Gartner Content") represent(s) research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. ("Gartner"), and are not representations of fact. Gartner Content speaks as of its original publication date (and not as of the date of this [type of filing]), and the opinions expressed in the Gartner Content are subject to change without notice. GARTNER and MAGIC QUADRANT are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

[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

 **6.0/6.0**

**Protection score
in AV-TEST**

Achieved perfect protection score in the past 8 cycles

 **AAA**

**Award from SE Labs
in past 4 cycles**

Achieved 97% cycles total accuracy in latest cycle

<https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/top-scoring-industry-antivirus-tests>



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

The screenshot displays the Microsoft 365 security interface with the following details:

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

A bar chart showing detections from May 13 to June 9. The Y-axis ranges from 0 to 1000. The X-axis shows dates from 05/13 to 06/09. The legend indicates:

- Audited (blue)
- Blocked (purple)

Date	Audited	Blocked
05/13	~100	~100
05/16	~400	~400
05/19	~300	~300
05/22	~400	~400
05/25	~300	~300
05/28	~400	~400
06/01	~300	~300
06/04	~400	~400
06/07	~300	~300
06/09	~400	~400

Attack surface reduction rules

86% devices use ASR rules to block

Configuration for behavioral rules from Windows Defender ATP that reduce the attack surface.

Rule Description	Mode
Block Office applications from injecting code into other processes	Block mode
Block all Office applications from creating child processes	Block mode
Block JavaScript or VBScript from launching downloaded executables	Block mode
Block executable content from email client and webmail	Block mode
Use advanced protection against ransomware	Block mode
Block process creations originating from PSEXEC and WMI commands	Block mode
Block Office communication application from creating child processes	Block mode

Device settings by rule

Rule	Block mode	Audit mode	Off
Block Office applications from injecting code into other processes	High	Low	Low
Block all Office applications from creating child processes	High	Low	Low
Block JavaScript or VBScript from launching downloaded executables	High	Low	Low
Block executable content from email client and webmail	High	Low	Low
Use advanced protection against ransomware	High	Low	Low
Block process creations originating from PSEXEC and WMI commands	High	Low	Low
Block Office communication application from creating child processes	High	Low	Low

View detections | **Add exclusions**

View detections | **Manage configuration**



Attack Surface Reduction

Resist attacks and exploitations

HW based isolation

Isolate access to untrusted sites

Application control

Isolate access to untrusted Office files

Exploit protection

Host intrusion prevention

Network protection

Exploit mitigation

Controlled folder access

Ransomware protection for your files

Device control

Block traffic to low reputation destinations

Web protection

Protect your legacy applications

Ransomware protection

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