Microsoft

Microsoft Defender for Business overview

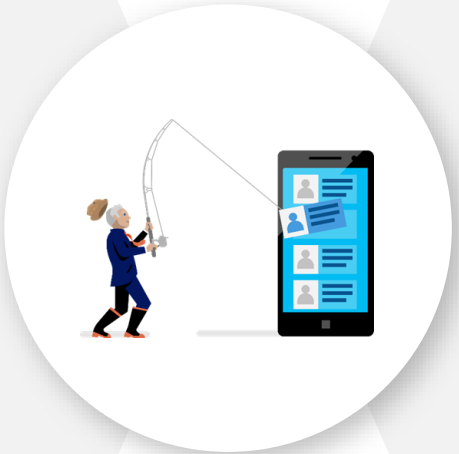
Peter Schmidt & Ronni Pedersen

SMBs are increasingly a target of cyberattacks like ransomware

COVID-19 exploited by malicious cyber actors

"...groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails."

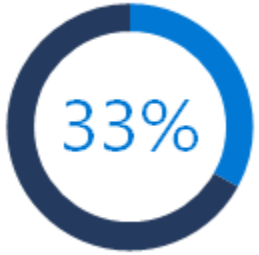
Department of Homeland Security, April 8, 2020, CISA Alert (AA20-099A)



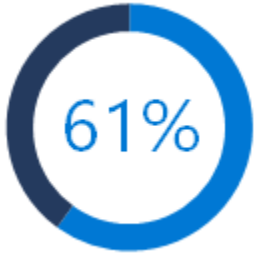
Increase in ransomware attacks

"... small businesses comprise approximately one-half to three-quarters of the victims of ransomware," he said. Overall, ransomware attacks have been up almost 300% in the past year, he said. "

Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report



1/3rd of all cyberattacks are targeted at small businesses.[1]



of small businesses that experienced a recent cyberattack were not able to operate.[2]

$108K

average cost of a SMB data breach.[3]

Source: 1 Introduction to the 2020 DBIR | Verizon Enterprise Solutions, 2 Microsoft commissioned Forrester Research, 2020, 3 Kaspersky Global Corporate IT Security Risks Survey, 2019

Microsoft Defender for Business

Elevate your security

Elevate your security with enterprise-grade endpoint protection specially built for businesses with up to 300 employees.

Enterprise-grade protection

Security for all your devices with next-gen protection, endpoint detection and response, and threat and vulnerability management.

Easy to use

Streamline onboarding with wizard-driven set up and recommended security policies activated out-of-the-box to quickly secure devices.

Cost-effective

Endpoint security that keeps you productive and works with your IT without compromising budget.

Read the preview blog: https://aka.ms/MDB-PreviewBlog; Sign up for the Preview at https://aka.ms/MDB-Preview

How to purchase Microsoft Defender for Business at General Availability

Microsoft Defender Business ($3pupm)

Enterprise-grade endpoint security

Per user license

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

Microsoft 365 Business Premium ($20pupm)

Comprehensive productivity and security solution

Per user license

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

+

Coming soon! Microsoft Defender for Business

Microsoft Defender for Office 365 Plan 1

Intune

Azure AD Premium Plan 1

Azure Information Protection Premium P1

Exchange Online Archiving

Autopilot

Azure Virtual Desktop license

Windows 10/11 Business

Shared Computer Activation

Note that not all capabilities may be available in preview.

1) As standalone SKU, upto 300 users

Entitlement for use on up to 5 devices

Generally available H1 2022

2) Included as part of Microsoft 365 Business Premium, upto 300 users

Microsoft Defender for Business will roll out to new and existing M365 Business Premium customers, post GA

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

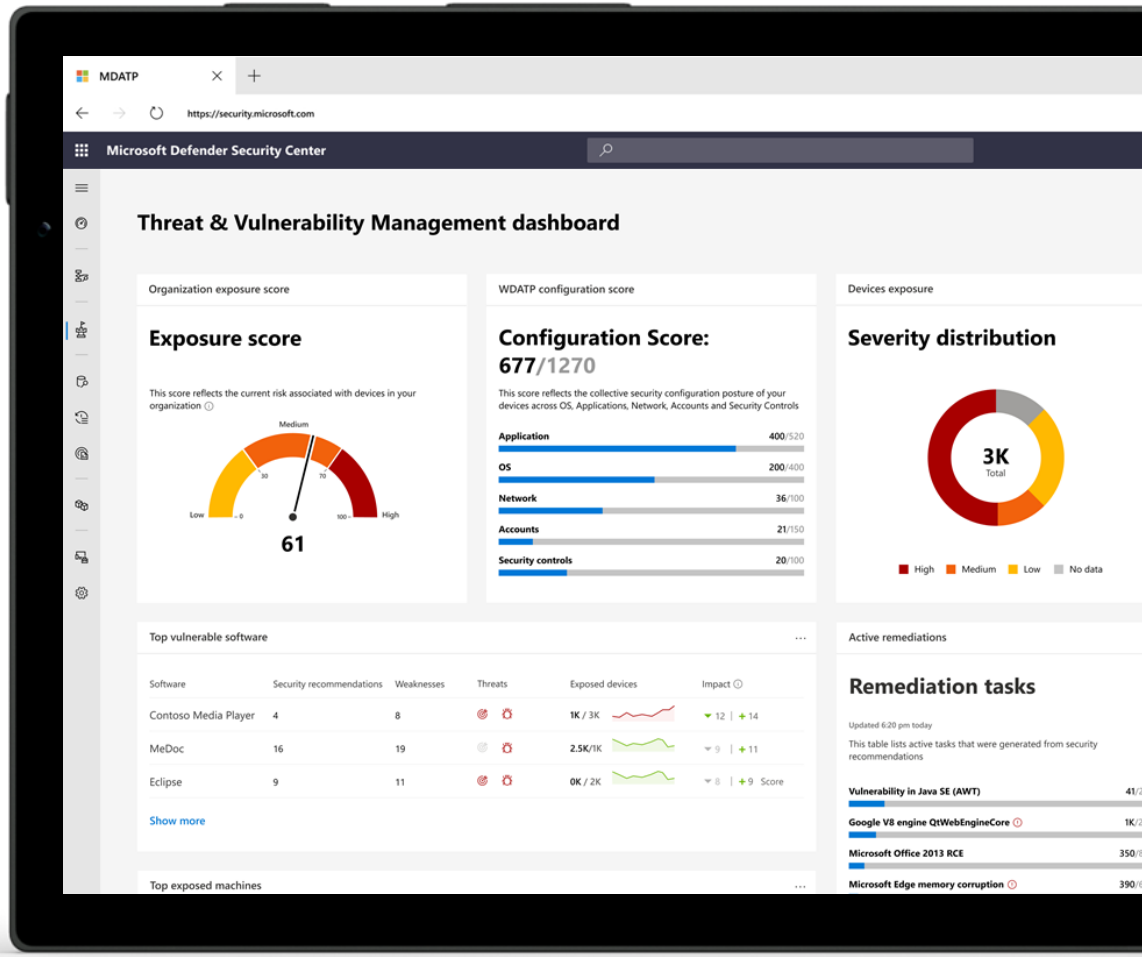
APIs and Integration

*Not all capabilities available at time of preview

Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

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

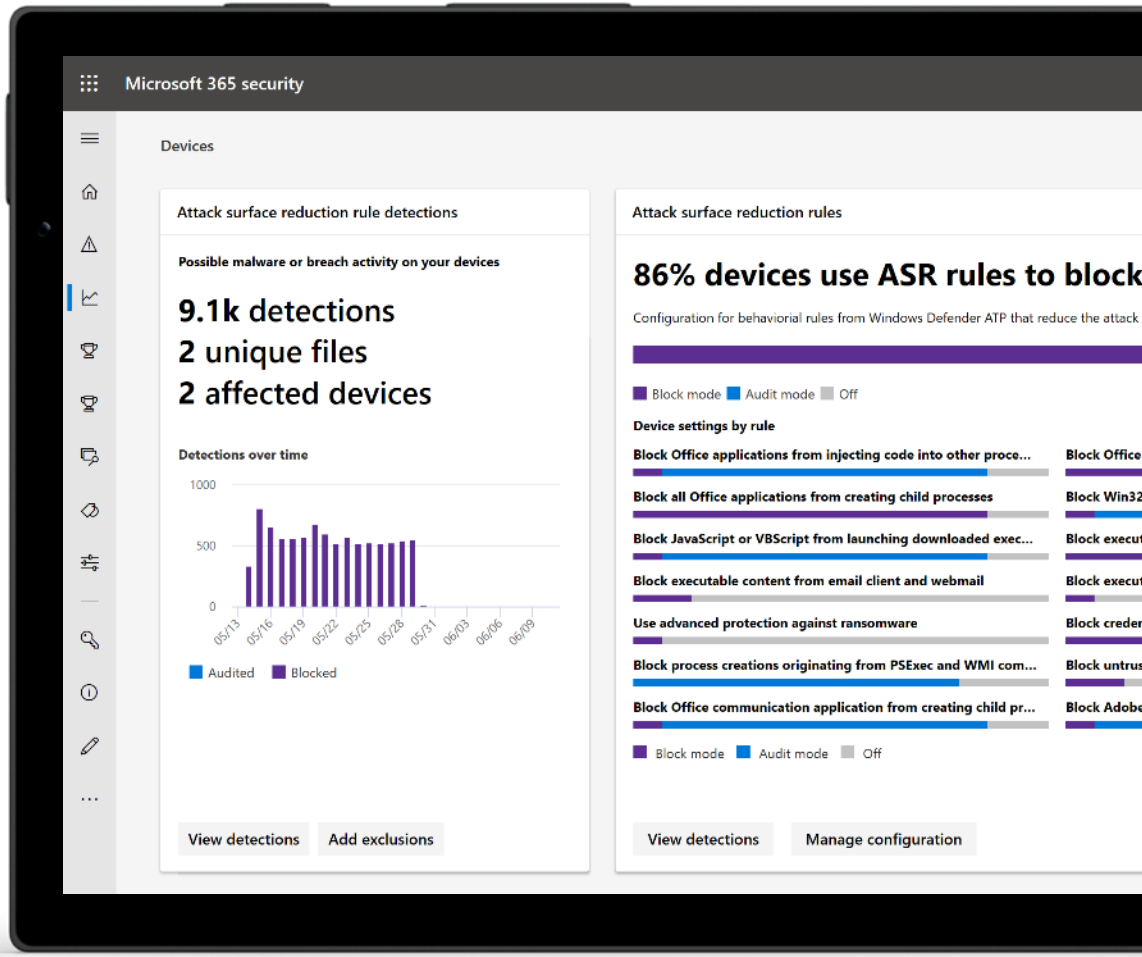


*Not all capabilities available at time of preview

Attack Surface Reduction

Protect against 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

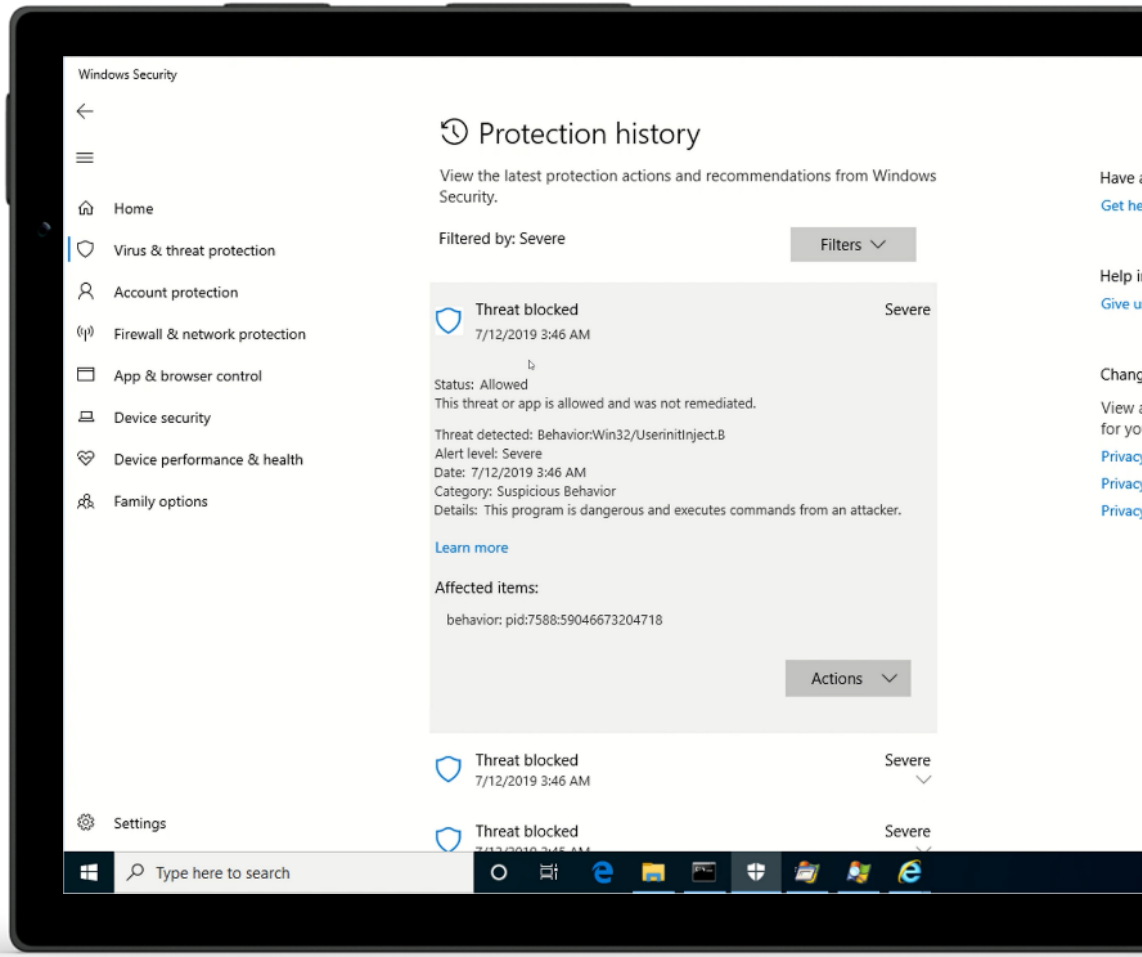


*Not all capabilities available at time of preview

Next Generation Protection

Helps block and tackle sophisticated threats and malware

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

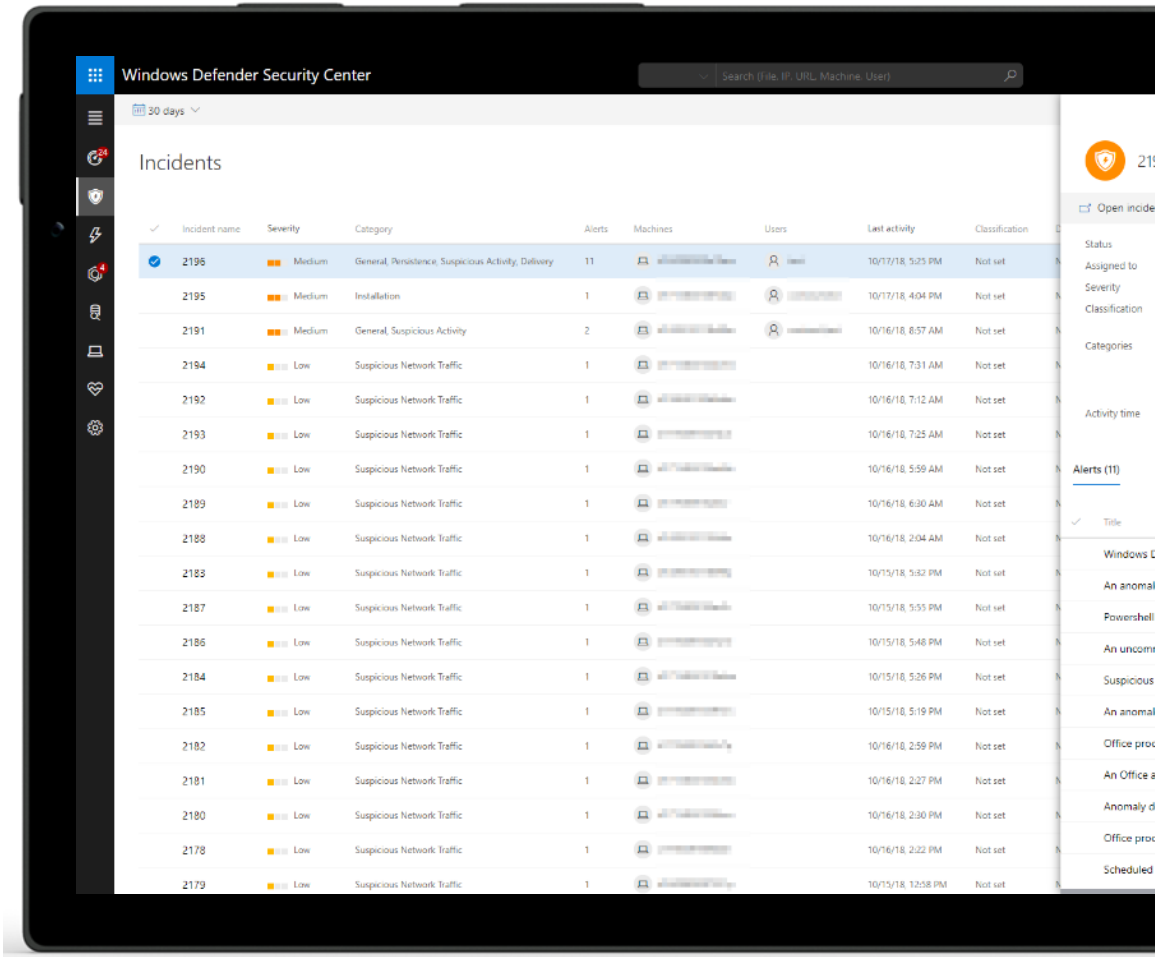


*Not all capabilities available at time of preview

Endpoint Detection & Response

Detect and investigate advanced persistent attacks

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

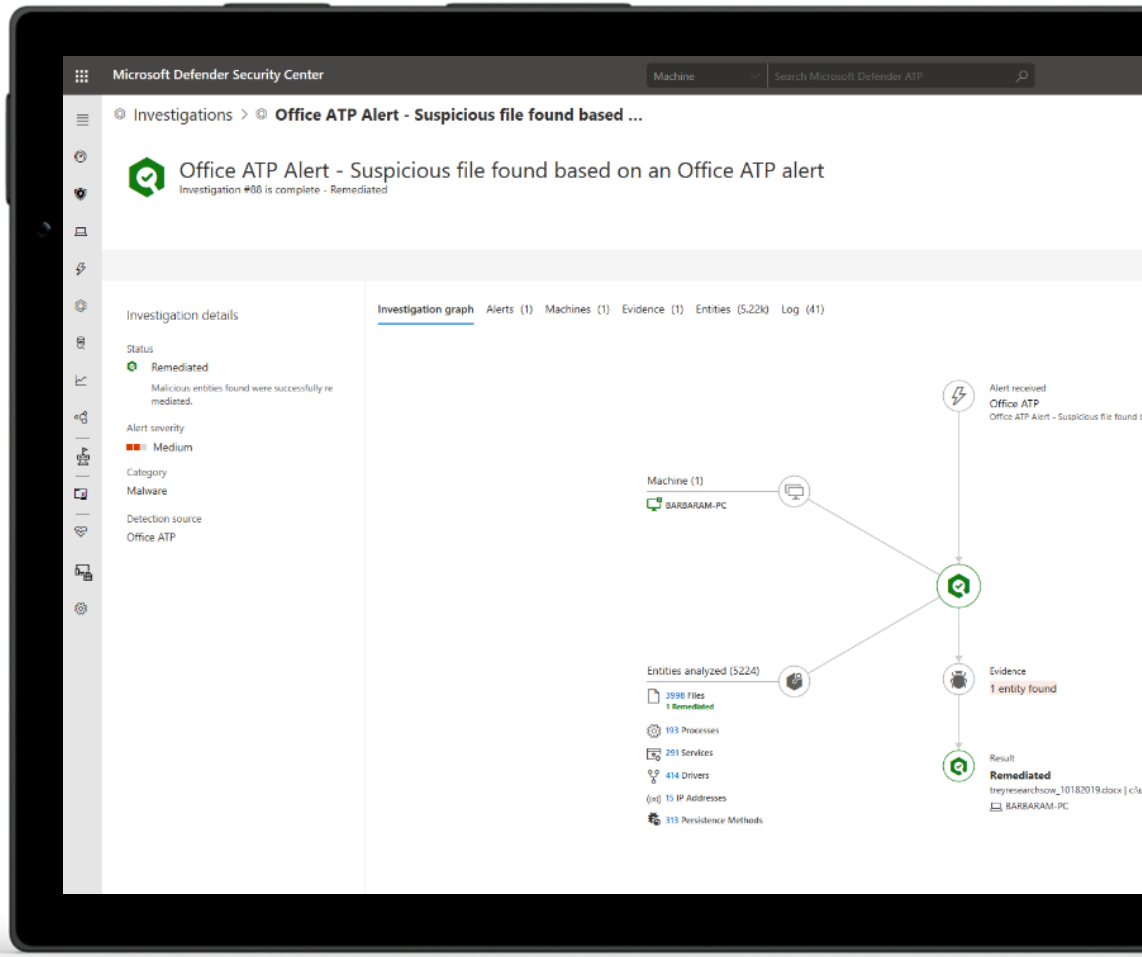


*Not all capabilities available at time of preview

Auto Investigation & Remediation

Automatically investigates alerts and helps to remediate complex threats

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

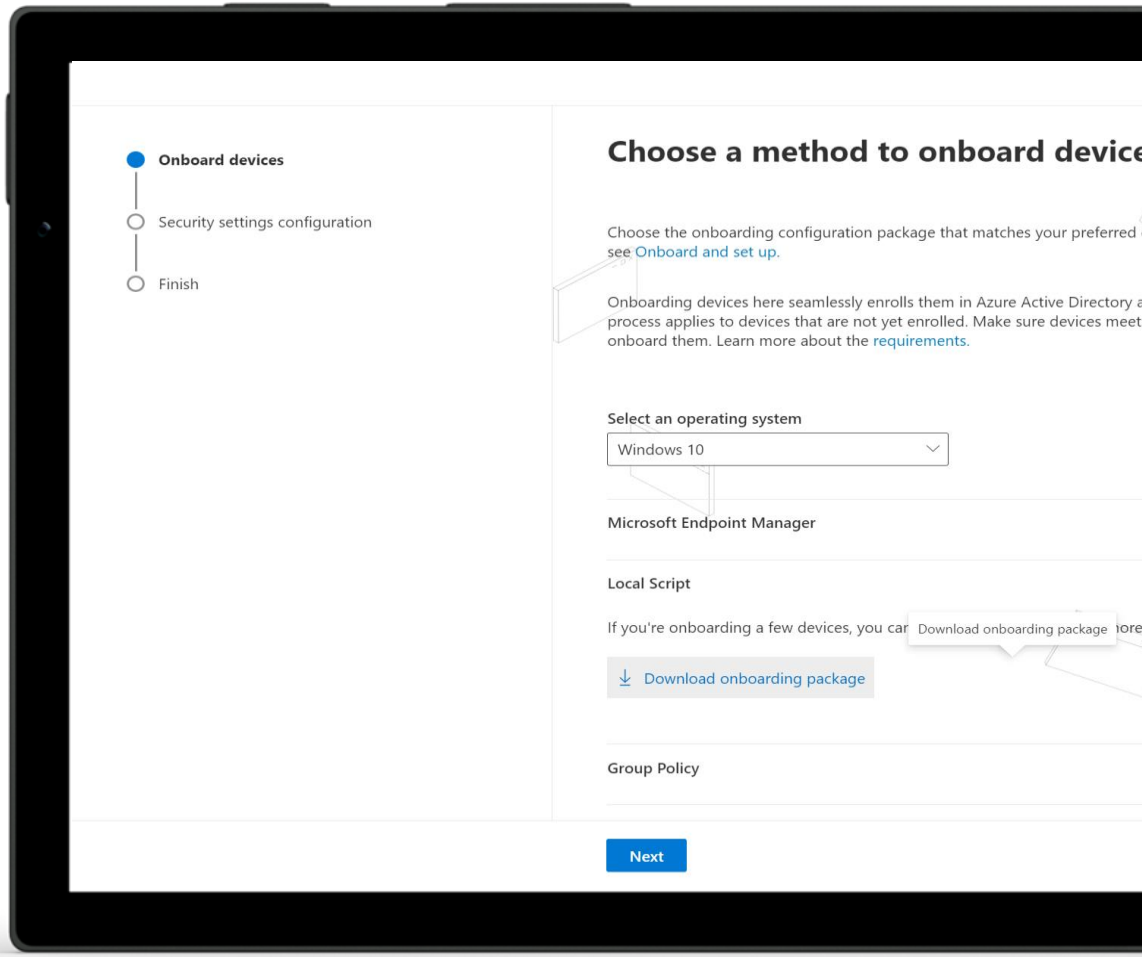


*Not all capabilities available at time of preview

Simplified Onboarding and Administration

Wizard-driven onboarding and easy to use management controls

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



*Not all capabilities available at time of preview

Delivering endpoint security across platforms

Windows macOS

Endpoints

iOS

Mobile device OS

Windows 365

Azure Virtual Desktop

Virtual desktops

*Not all capabilities available at time of preview

Product Comparison: Defender for Business brings enterprise=grade capabilities to SMBs

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	Microsoft Defender for Business (currently in preview, will Included with M35BP post GA)	Microsoft Defender for Endpoint Plan 1 (Included with M365 E3, currently in preview)	Microsoft Defender for Endpoint Plan 2 (Included with M365 E5)
Centralized management	✔	✔	✔
Simplified client configuration	✔		
Threat and Vulnerability Management	✔		✔
Attack Surface Reduction	✔	✔	✔
Next-Gen Protection	✔	✔	✔
Endpoint Detection and Response	✔[2]		✔
Automated Investigation and Response	✔[2]		✔
Threat Hunting and 6-months data retention			✔
Threat Analytics	✔[2]		✔
Cross platform support for Windows, MacOS, iOS, and Android	✔	✔	✔
Microsoft Threat Experts			✔
Partner APIs for exporting to SIEM	✔	✔	✔
Microsoft 365 Lighthouse for partners for viewing security incidents across customers	✔[3]		

Note that not all capabilities may be available in preview

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

Detailed product comparison

Capabilities	MDB	MDE P1	MDE P2
Threat & Vulnerability			
Microsoft secure score	●		●
Vulnerability management (visibility into software and vulnerabilities)	●		●
Vulnerability remediation based on Intune integration	●		●
Attack Surface Reduction			
Advanced vulnerability and zero-day exploit mitigations	●	●	●
Attack Surface Reduction rules	●	●	●
Application Control	●	●	●
Network Firewall	●	●	●
Device Control (e.g.: USB)	●	●	●
Network protection	●	●	●
Device-based conditional access	●	●	●
Web Control / Category-based URL Blocking	●	●	●
Ransomware mitigation	●	●	●
Next Gen Protection			
Advanced cloud protection (deep inspection and detonation) BAFS	●	●	●
Monitoring, analytics and reporting for Next Generation Protection capabilities	●	●	●
Endpoint Detection and Response			
Behavioral-based detection (post-breach)	●		●
Rich investigation tools			●
Custom detections			●
6-month searchable data per endpoint			●
Advanced hunting			●
Evaluation Lab			●
Manual response actions - (Run AV scan, Machine isolation, File stop and quarantine)	●	●	●
Live response	●		●

*Not all capabilities available at time of preview

Detailed product comparison

Capabilities	MDB	MDE P1	MDE P2
Automatic Investigation and Remediation			
Default automation levels	●		●
Customized automation levels			●
Centralized Management			
Role-based access control	●	●	●
Simplified client configuration	●		
Reporting	●	●	●
API's			
SIEM Connector		●	●
API's (Response, Data collection)		●	●
Partner applications		●	●
Threat Intelligence			
Threat Analytics	●		●
Custom Threat Intelligence	●	●	●
Sandbox			●
3rd party Threat Intelligence Connector			●
Partner Support			
APIs (For Partners)	●	●	●
RMM Integration	●		
MSP Support (Multi-tenant API, multi tenant authentication)	●	●	●
Microsoft Threat Expert			
Targeted attack notification			●
Collaborate with Experts, on demand			●
Platform support			
Windows Client	●	●	●
MacOS	●	●	●
Mobile (Android, iOS)	●	●	●

*Not all capabilities available at time of preview

Get started with Microsoft Defender for Business

Read the preview blog:
https://aka.ms/MDB-PreviewBlog

Sign up for the Defender for Business Preview: https://aka.ms/MDB-Preview
(Preview roll out starts now, and will expand in phases in the coming months leading upto General Availability)

Review the Tech Documentation:
https://aka.ms/MDB-Docs

Preview sign up process for Customers

Sign up Process:

- ✓ **Preview will roll out in phases; first to an initial set of customers and partners in the coming weeks and will be expanded as we get closer to GA in the coming months.**
- ✓ To register your name for the preview, please sign-up at https://aka.ms/MDB-Preview.
- ✓ Customers can sign directly; IT partners can also deploy to their customers.
- ✓ Preview trial will last 90-days from activation
- ✓ Need to be signed into your tenant with the Global Administrator role to activate it.

IT Partners wishing to deploy preview trial to customer tenants

- ✓ You can activate Defender for Business preview trial license to up to 25 tenants each with 300 user subscription licenses each.
- ✓ Using the same preview license code, you can also deploy it to your own tenants for self-testing.

IMPORTANT - Partners must have each customer process the customer flow and accept the End-user license agreement on their own before partners can deploy MDB to their environment.

After you've signed up

- ✓ **We'll onboard partners in phases, so some customers and partners will start receiving onboarding codes in the coming weeks while others may have to wait for us to expand capacity as we march to General Availability in the coming months.**
- ✓ Visit Microsoft Defender for Business documentation for information about how to onboard devices, configure settings, and ongoing security management.

Evaluering: https://forms.office.com/r/Tsqs7AKrKY