Defender for Business Deep Dive

- Peter Schmidt
- Cloud Architect @ NeoConsulting
- Twitter @petsch
- Blog: www.msdigest.net
- MVP, MCM, MCT

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC — VIRTUAL SUMMIT —

Defender for Business Deep Dive

- Morten Thomsen
- Cloud Security Architect, APENTO
- Twitter: @Thomsen79
- Mail: mth@apento.com
- Cerfitified: Enterprise Administrator expert
- MCT

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC — VIRTUAL SUMMIT —

Agenda

- Introduction
- Defender for Business
- Getting Started with onboarding
- Demo
- Summary

300% increase in identity attacks over the past year[3]

Phishing and stolen credentials (hacking) are among the top threat action varieties in breaches for SMBs[2]

+300% Ransomware attacks in the past year, with more than 50% targeted at small businesses [6]

[1] Source: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ based on MSFT internal study
2.2020 Verizon Data Breach Investigations Report
3. MSFT Internal research

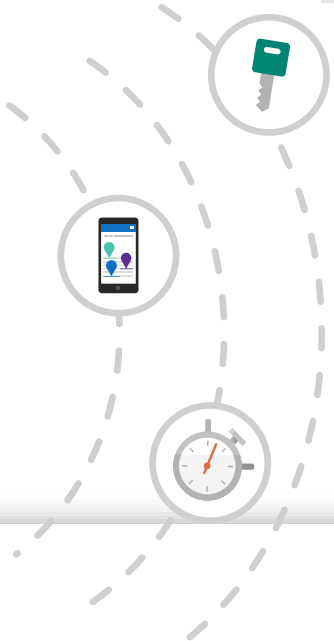
Protect against ransomware

Devices are protected with Microsoft Defender. Microsoft Defender provides multi-layered protection – with Threat and Vulnerability Management thwarting attacks before they occur and EDR and Automated Investigation and Response defending against manual and targeted attacks.

80% of SMBs list ransomware as a top concern.[1]

In 2020 the average cost of downtime associated with ransomware attacks rose[1] **94%**

Microsoft Defender for Business



Microsoft Defender for Business protects against ransomware in 3 ways:

Threat & Vulnerability Management thwarts attacks before they occur

Protection against targeted ransomware attacks with EDR

Automated Investigation and Response provides post-breach protection

[1]*Source: Datto's 2020 Global State of the Channel Ransomware Report, statistics pulled from a survey of more than 1,000 MSPs around the world.*

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

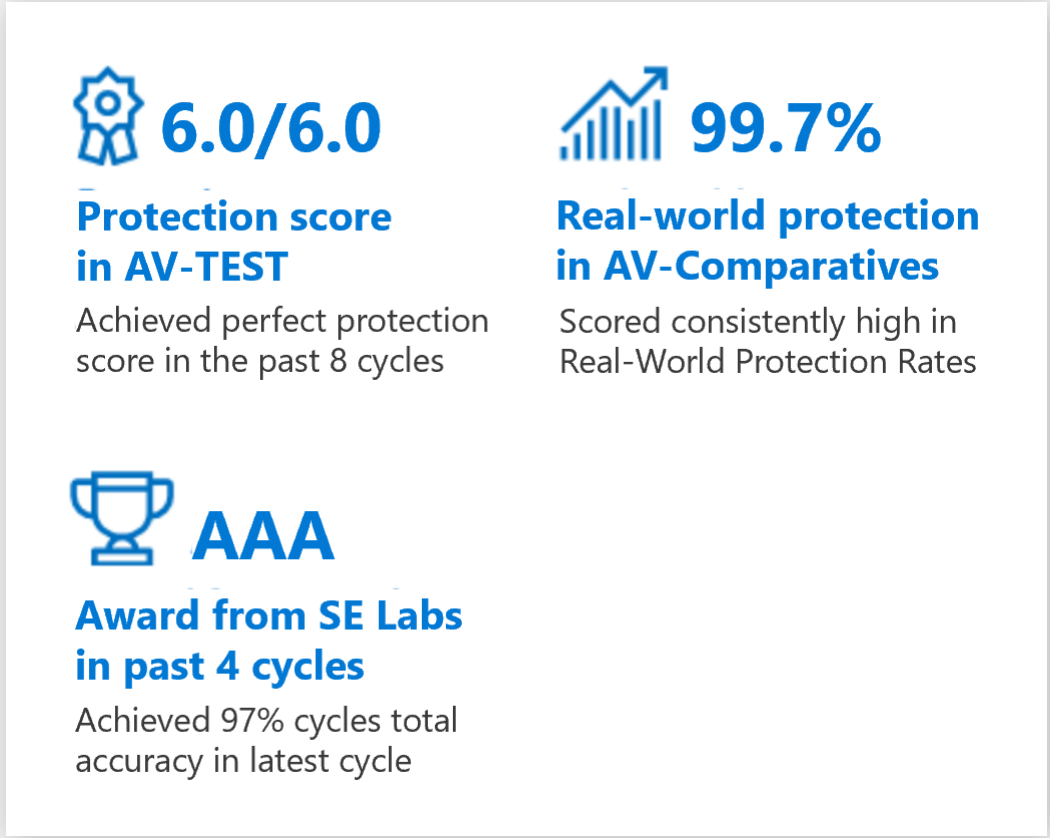
Streamline onboarding with wizard-driven set up and recommended security policies activated out-of-the-box to quickly secure devices.

Cost-effective

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

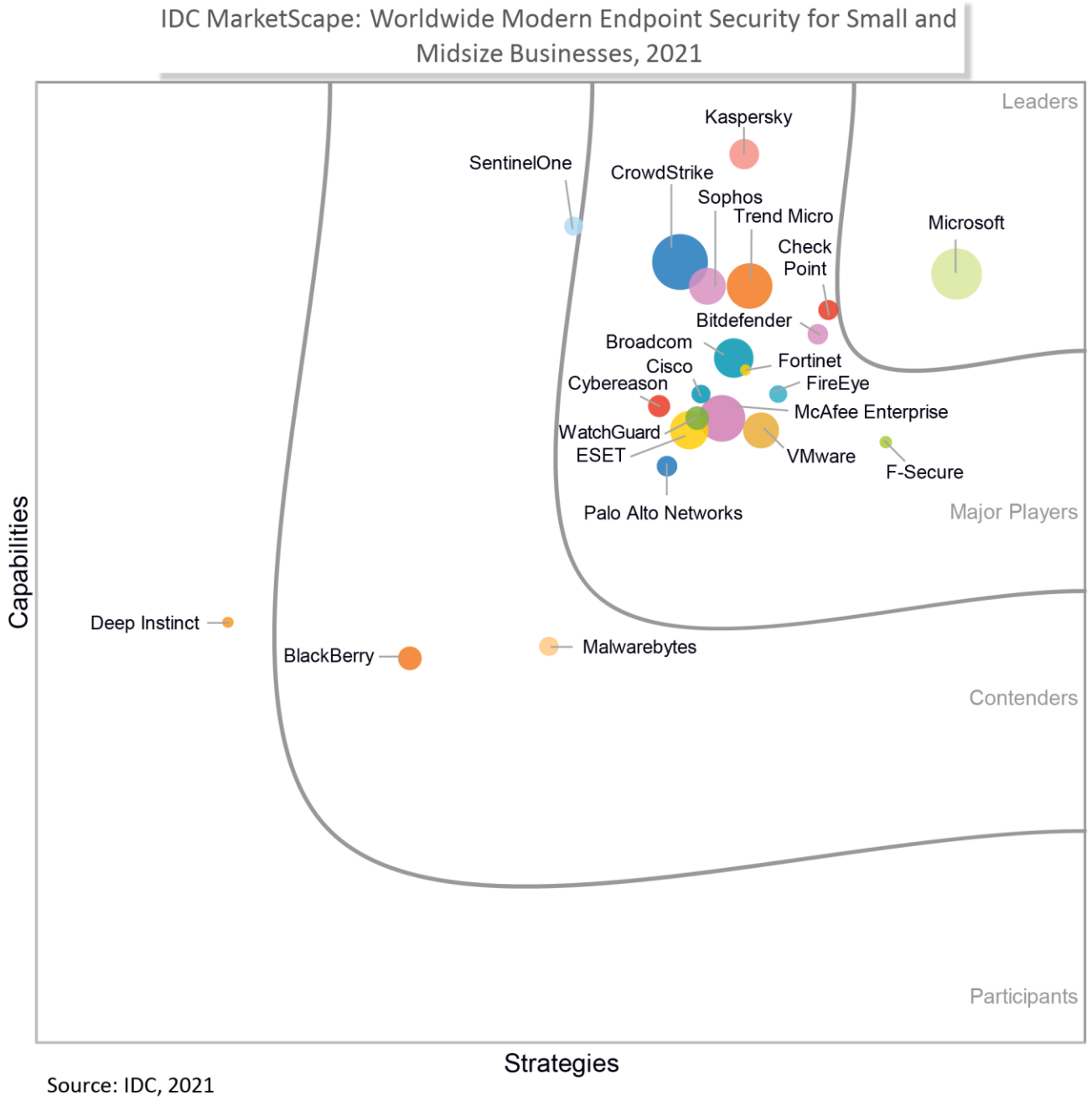
Microsoft Defender consistently rated top AV

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



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

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



Source: IDC, 2021

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

Delivering endpoint security across platforms

Windows macOS

Endpoints

iOS

Mobile device OS

Windows 365

Azure Virtual Desktop

Virtual desktops

Defender for Business Licensing options

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 ($22pupm)

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

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

Enterprise-grade protection for SMBs

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

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

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

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

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Centralized management	✔	✔	✔
Simplified client configuration	✔		
Threat and Vulnerability Management	✔		✔
Attack Surface Reduction	✔	✔	✔
Next-Gen Protection	✔	✔	✔
Endpoint Detection and Response	✔[2]		✔
Automated Investigation and Response	✔[2]		✔
Threat Hunting and 6-months data retention			✔
Threat Analytics	✔[2]		✔
Cross platform support for Windows, MacOS, iOS, and Android	✔	✔	✔
Microsoft Threat Experts			✔
Partner APIs	✔	✔	✔
Microsoft 365 Lighthouse for viewing security incidents across customers	✔[3]		

[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	●		●

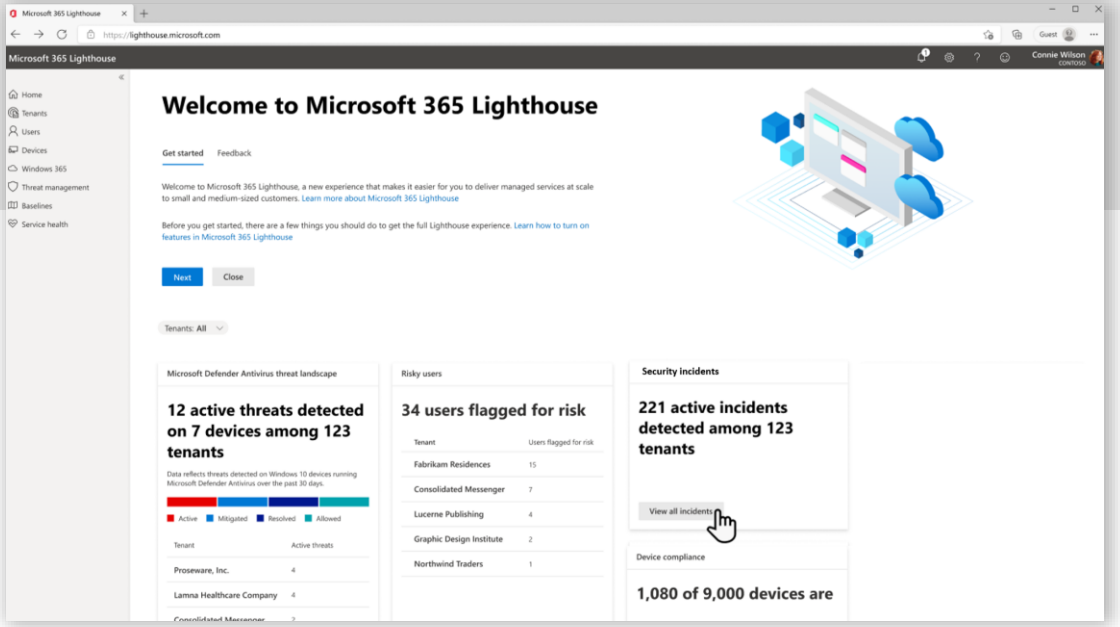
Detailed product comparison

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)	●	●	●

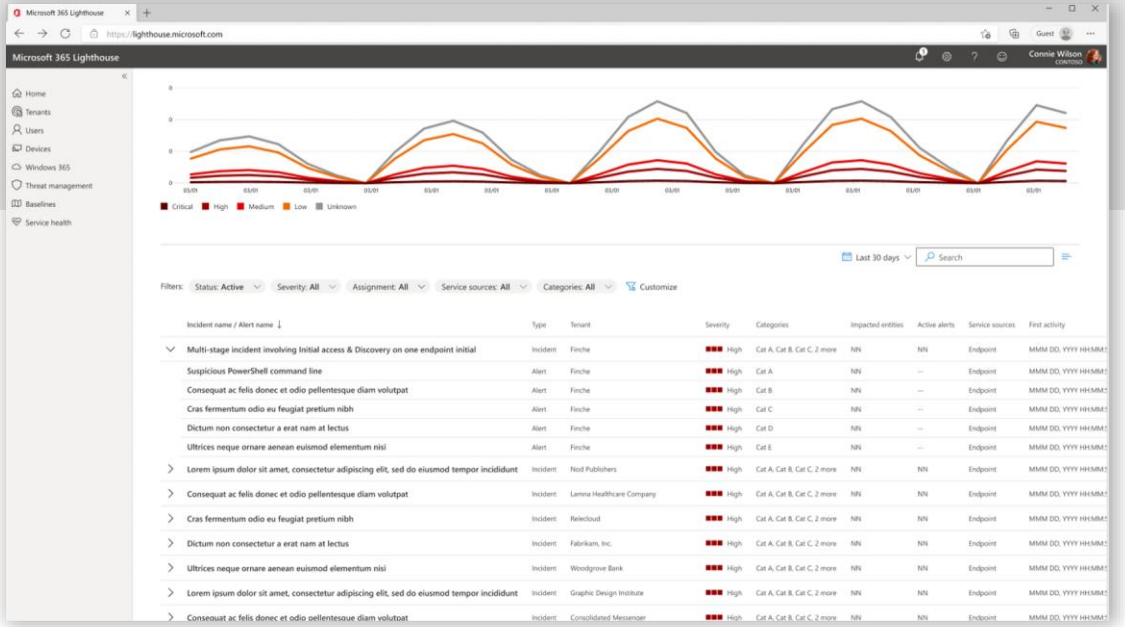
Public Preview

Microsoft 365 Lighthouse with Defender for Business and Microsoft Business Premium

View security incidents and alerts from Defender for Business in the dashboard and get the detail from the Incidents queue. Additional security management capabilities are planned on the roadmap.



Security incident summary on the Home dashboard



Incident queue highlighting security incidents and alert details

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

Welcome to Microsoft Defender for Business

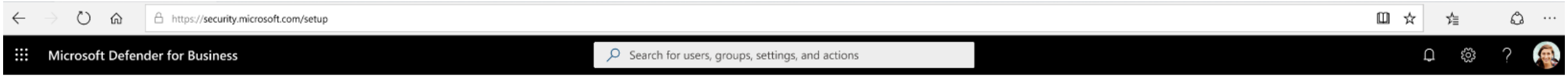
Welcome to Microsoft Defender for Business, where you can monitor and manage security across your devices. Learn more about Microsoft Defender for Business

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 Close



- 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
AG Admin group 1	Security admin
Amanda Johnson	Security reader

+ Add assignment

RECOMMENDATION

Why give access to people in your organization?
By giving access to people, you provide your security team with the permissions they need to perform their tasks.

Continue

Skip

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

- 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
jonathan.wolcott@contoso.com	Alerts & Vulnerabilities
Type email address	Select notification type

+ Add recipients

RECOMMENDATION

Why set up your email notification now?
email notifications, users will be informed in real time about any alerts or vulnerabilities that might be putting your organization at risk.

Back

Continue

Skip

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

How do you want to onboard your devices?

We noticed that you have devices enrolled in Microsoft Endpoint Manager.

Choose devices to onboard to Defender for Business. This process will establish a connection between Defender for Business and Endpoint Manager. You can add other OS devices later. Learn more about onboarding options

- (•) All devices (recommended)
  - Onboards all Windows devices that are enrolled in Endpoint Manager
  - Any new devices added to your org in the future will be automatically onboarded
- ( ) Devices you select

  Choose which Windows devices you want to onboard to Defender for Business.
  You can add more devices manually in the future.

RECOMMENDATION

Why onboard your devices now?

Onboarding now helps ensure that your organization's devices are more secure and less vulnerable to malware, attacks, and threats.

Back

Continue

https://security.microsoft.com/setup

Microsoft Defender for Business

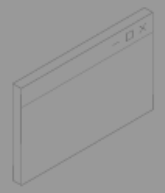
Search for users, groups, settings, and actions

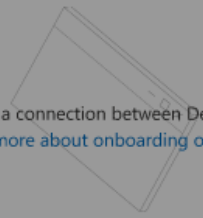
- Assign user permissions
- Set up email notifications
- **Add Windows devices**
- Apply security settings
- Finish

How do you want to onboard your device

We noticed that you have devices enrolled in Microsoft Endpoint Manager.

Choose devices to onboard to Defender for Business. This process will establish a connection between Defender for Business and Endpoint Manager. You can add other OS devices later. Learn more about onboarding options





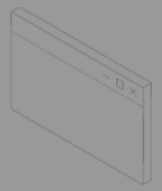
○ All devices (recommended)

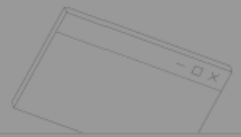
- Onboards all Windows devices that are enrolled in Endpoint Manager
- Any new devices added to your org in the future will be automatically onboarded

◉ Devices you select

Choose which Windows devices you want to onboard to Defender for Business.
You can add more devices manually in the future.

+ Choose devices





Back

Continue

Choose devices to onboard

68 items

Search

Device name ↓	OS type
☑ ComputerPII_4b5ebbef2a951814	Windows server
☑ ComputerPII_4b5ebbef2a9518149ac88c98a0	Windows client
☑ ComputerPII_4b5ebbef2a9518149	Windows server
☑ ComputerPII_4b5ebbef2a9518149ac	Windows client
☐ ComputerPII_4b	Windows client
☐ ComputerPII_4b5ebbef2a9518149ac8	Windows client
☐ ComputerPII_4b5ebbef2a	Windows client
☐ ComputerPII_4b5ewe	Windows server
☐ ComputerPII_4b5ebb	Windows client
☐ ComputerPII_4b5ebb	Windows client
☐ ComputerPII_4b5ebb	Windows server
☐ ComputerPII_4b5ebbef	Windows client
☐ ComputerPII_4b5ebbef2	Windows client
☐ ComputerPII_4b5ebbef2	Windows client
☐ ComputerPII_4b5ebbef23	Windows client
☐ ComputerPII_4b5ebbef2a	Windows client

Add devices | Cancel

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

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

Configure your security settings

We noticed that you are using Microsoft Endpoint Manager (MEM) to manage your security settings and policies.

If you choose to switch to simplified configuration process in Microsoft Defender for Business (MDB), our recommended security policies and settings will be created and applied to your onboarded devices. Learn more about your configuration options

Select your preferred configuration management process:

Use the simplified configuration
Switch to managing security settings and policies in MDB

Continue using MEM
Keep using MEM to manage security settings and policies

To avoid policies conflicts please remove the following policies detected MEM:

- Antivirus dev IL
- Next generation protection
- Microsoft Edge Baseline
- Next generation protection management
- Microsoft 10 Security Baseline

When you have finished, choose '**Continue**' to proceed.

RECOMMENDATION

Why use simplified configuration?
Microsoft Defender for Business will create default security policies and settings for all devices, helping ensure devices are protected from day one.

Back

Continue

MDB Recommended Security Policies

Next Generation Protection

- Antivirus
- Antimalware
- Scanning of removable drives
- Daily quick scans
- Security intelligence updates
- Security intelligence checks

Firewall

- Outbound connections from devices are allowed
- Devices connected to org network, all inbound connections are blocked
- Devices connected to public or private network, all inbound connections are blocked

https://aka.ms/mdb-docs

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

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

You're almost done..

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

Assign user permissions

Assign Security reader and admin roles:

Security reader (2)

Amanda Johnson

IG IT group 1

Security admin (2)

AG Admin group 1

Set up email notifications

Set up email notifications for these recipients:

jonathan.wolcott@contoso.com - Alerts & vulnerabilities

kondoeloremipsum@contoso.com - Alerts

JanedoeLoremipsum@contoso.com - Vulnerabilities

Devices to add

Onboard your organization's devices to Microsoft Defender for Business

Security settings to apply

Microsoft Defender for Business will apply default security policies and settings to your devices

Back

Submit

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

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

You're all set

Your setup is complete.

System dashboard

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

Go to System dashboard

Device configuration

View or edit your device security settings and policies

Go to Device configuration

Onboard other OS devices

Onboard devices of additional operating systems

Go to Device onaboarding

Done

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

Without MEM

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

Choose a method to onboard devices

This step onboard **Windows devices** and enrolls seamlessly 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

- **Local script**

  If you're onboarding a few devices, you can choose this method.
  Learn more about onboarding with local script

- **Microsoft Endpoint Manager**
- **Group Policy**
- **VDI onboarding script**

RECOMMENDATION

Why onboard your devices?
Onboarding your organization's devices now helps ensure that those devices are more secure and less vulnerable to malware, attacks, and threats.

Back

Continue

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

Without MEM

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

Configure your 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

Using the built-in security configuration will:

- Configure your default security policies and settings
- Apply your settings and policies to Windows devices

To start the process, choose '**Continue**' and relax while we set things up.
You can always edit your settings later in Device configuration.

RECOMMENDATION

Why use automatic configuration?

You save time and effort with default security policies and settings that help protect your organization's devices from day one. We take the guesswork out with built-in policies and settings that are based on industry best practices.

Back

Continue

Skip

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

Without MEM

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

You're almost done..

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

Assign user permissions

Assign Security reader and admin roles:

Security reader (2)

Amanda Johnson

IG IT group 1

Security admin (2)

AG Admin group 1

Set up email notifications

Set up email notifications for these recipients:

jonathan.wolcott@contoso.com - Alerts & vulnerabilities

kondoeloremipsum@contoso.com - Alerts

JanedoeLoremipsum@contoso.com - Vulnerabilities

Devices to add

Onboard your organization's devices to Microsoft Defender for Business

Security settings to apply

Microsoft Defender for Business will apply default security policies and settings to your devices

Back

Submit

https://security.microsoft.com/setup

Microsoft Defender for Business

Search for users, groups, settings, and actions

Without MEM

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

You're all set

Your setup is complete.

System dashboard

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

Go to System dashboard

Device configuration

View or edit your device security settings and policies

Go to Device configuration

Onboard other OS devices

Onboard devices of additional operating systems

Go to Device onaboarding

Done

NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

RECAST SOFTWARE

DEMO

Microsoft Defender for Business

Defender for Business Summary

NORDIC
– VIRTUAL SUMMIT –

- Provides layered protection – more than just antivirus
- Brings enterprise grade security to customers and partners who manage customer security
- Is well awarded and considered best-in-class by third-party testers and influential analysts
- Creates a security solution whose experience is tailored to SMBs
- Integrates with Microsoft 365 Lighthouse
- Exposes partner APIs

A big thanks to our sponsors

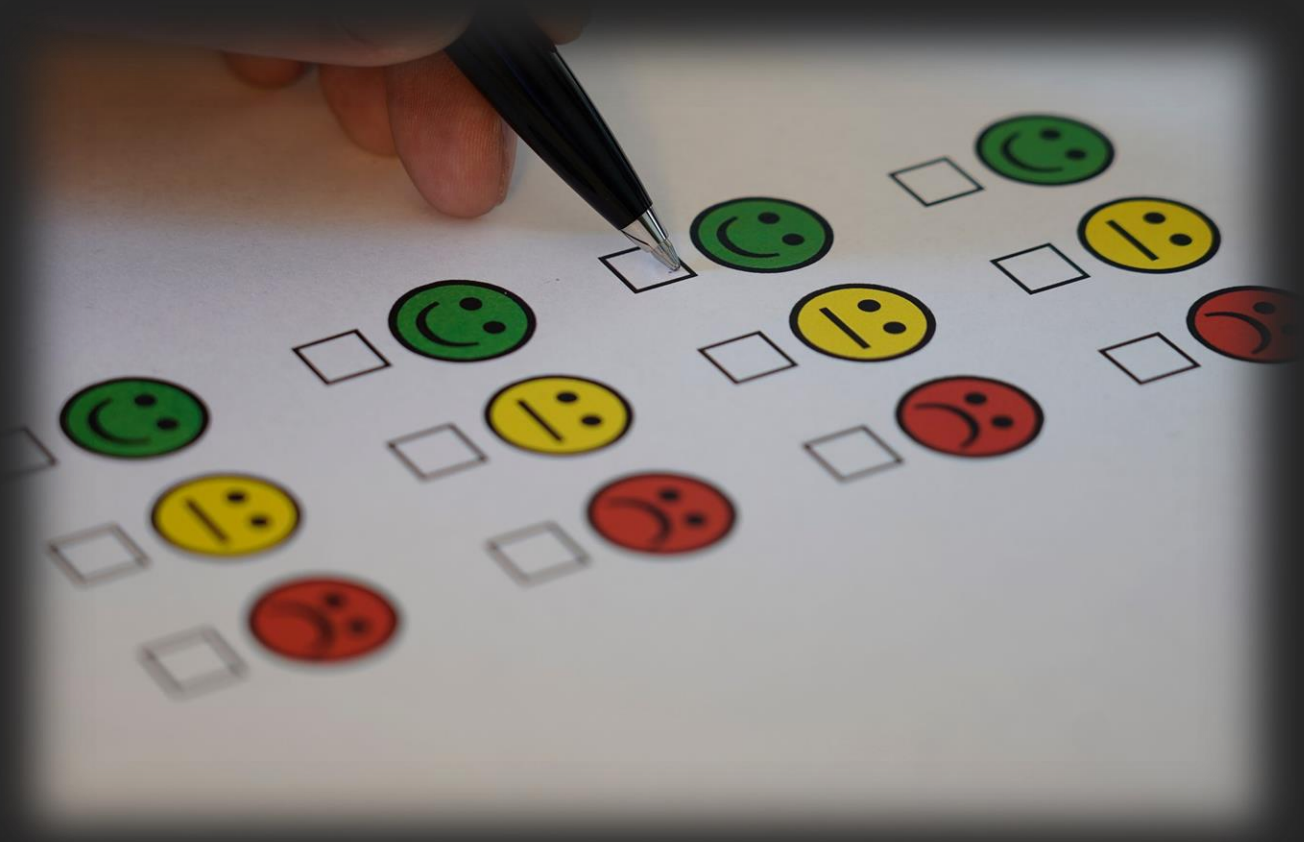
NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

RECAST SOFTWARE

Thank you!

Please remember to fill out the evals!



NORDIC
– VIRTUAL SUMMIT –