ICT POWER.IT

Microsoft

#POWERCON2022

Microsoft Defender for Endpoint: oltre Windows

Riccardo Corna

Microsoft MVP | Senior Consultant @ Microsys

rc@itspecialist.cloud

Agenda

- Microsoft Defender for Endpoint: panoramica
- Cross Platform Protection
  - Linux
  - macOS
  - Android
  - iOS

Cos’è Microsoft Defender for Endpoint?

“È una piattaforma di sicurezza degli endpoint aziendali progettata per consentire alle reti aziendali di bloccare, rilevare, analizzare e rispondere a minacce avanzate”

Dove siamo oggi?

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

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

Forrester names Microsoft a Leader in 2020 Enterprise Detection and Response Wave.

Our antimalware capabilities consistently achieve high scores in independent tests.

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

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

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

✓ Best Product Hardware Security

✓ Market Leader Endpoint Security

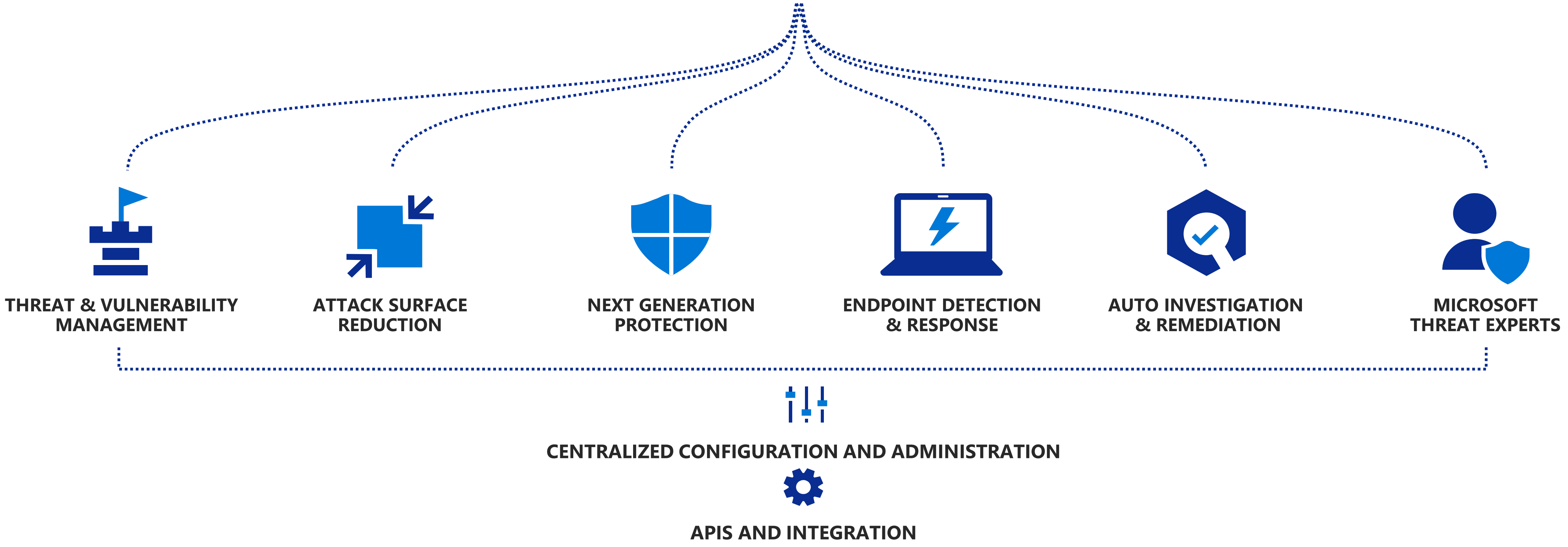
✓ Editor's Choice Extended Detection and Response (XDR)

✓ Most Innovative Malware Detection

✓ Cutting Edge Email Security

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

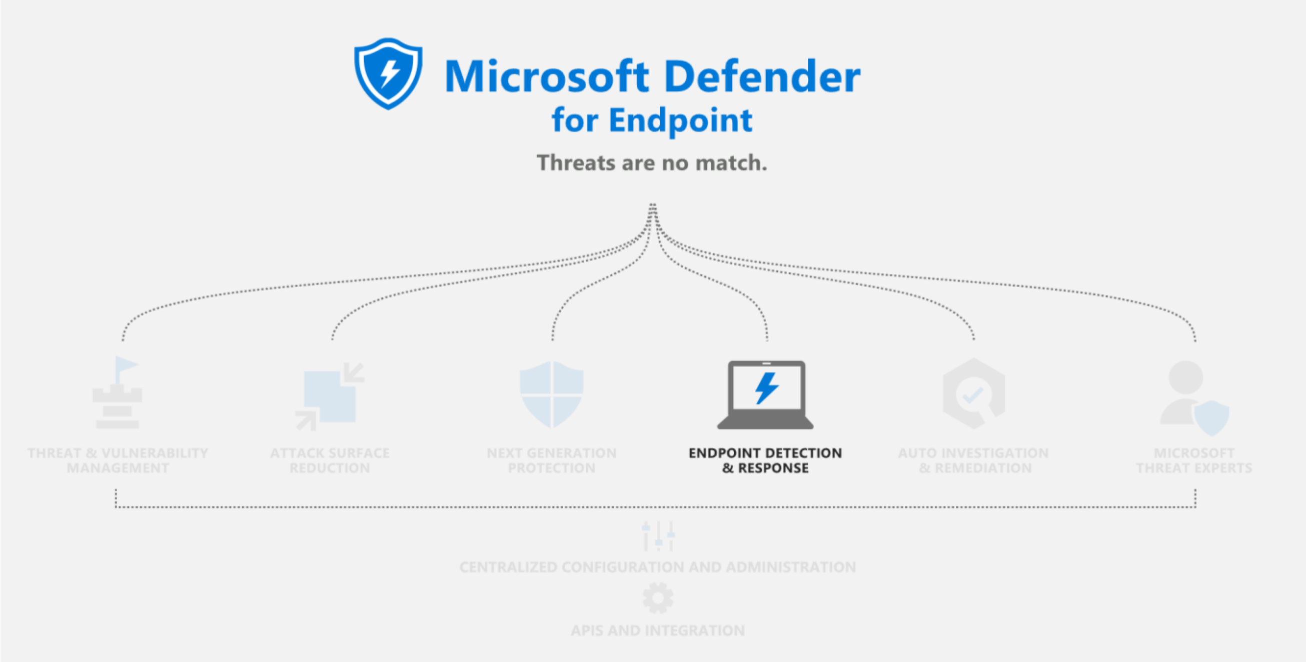
Endpoint Detection & Response

Quali problemi risolve?

- La quantità di attacchi e delle loro tipologie rende complesso capire se è accaduto qualcosa e “cosa è avvenuto quando”

Come li risolve

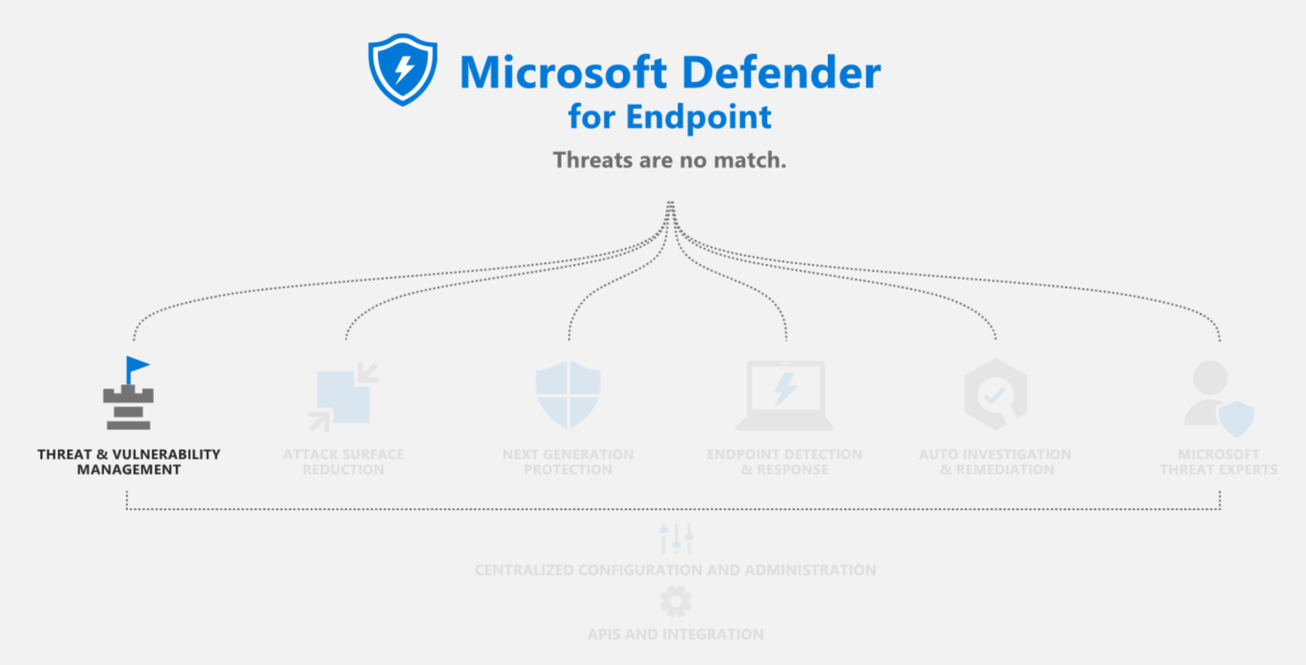
- Correlazione di alert
- Analisi comportamentale lungo 6 mesi di dati
- Disponibilità di azioni di reazione


Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION

Threat & Vulnerability Management

Quali problemi risolve?

- Conoscenza incompleta dei software installati sul parco endpoint
- Mancanza di informazioni sulle versioni installate dei software
- Configurazioni errate o incomplete sugli endpoint
- Processi di remediation/aggiornamento manuali e lunghi



Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION

Come li risolve

- Discovery, valutazione, prioritizzazione e correzione delle vulnerabilità e delle errate configurazioni degli endpoint.

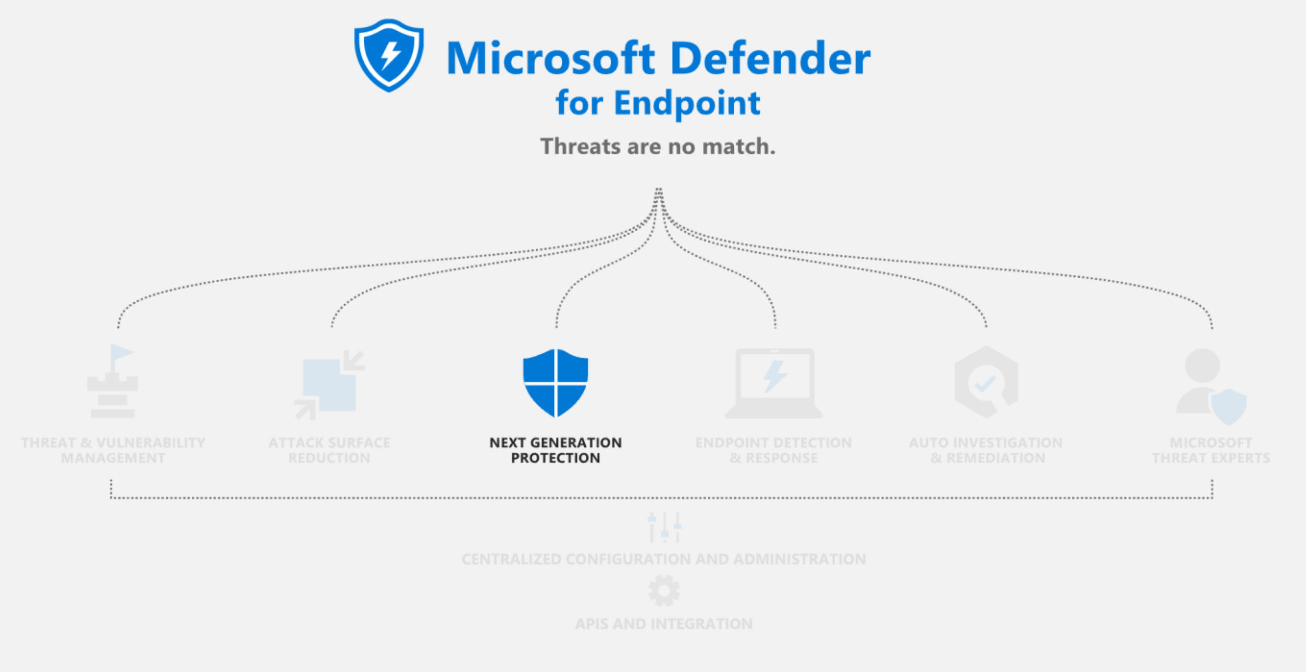
Next Generation Protection

Quali problemi risolve?

- In soluzioni classiche, nonostante un continuo aggiornamento delle firme AV, è impossibile rimanere al passo del numero di minacce che emerge quotidianamente

Come li risolve:

- Focus sul comportamento di un file/processo oltre che sui classici parametri di un file/processo sospetti [hash, etc]



Microsoft Defender
for Endpoint
Threats are no match.

THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

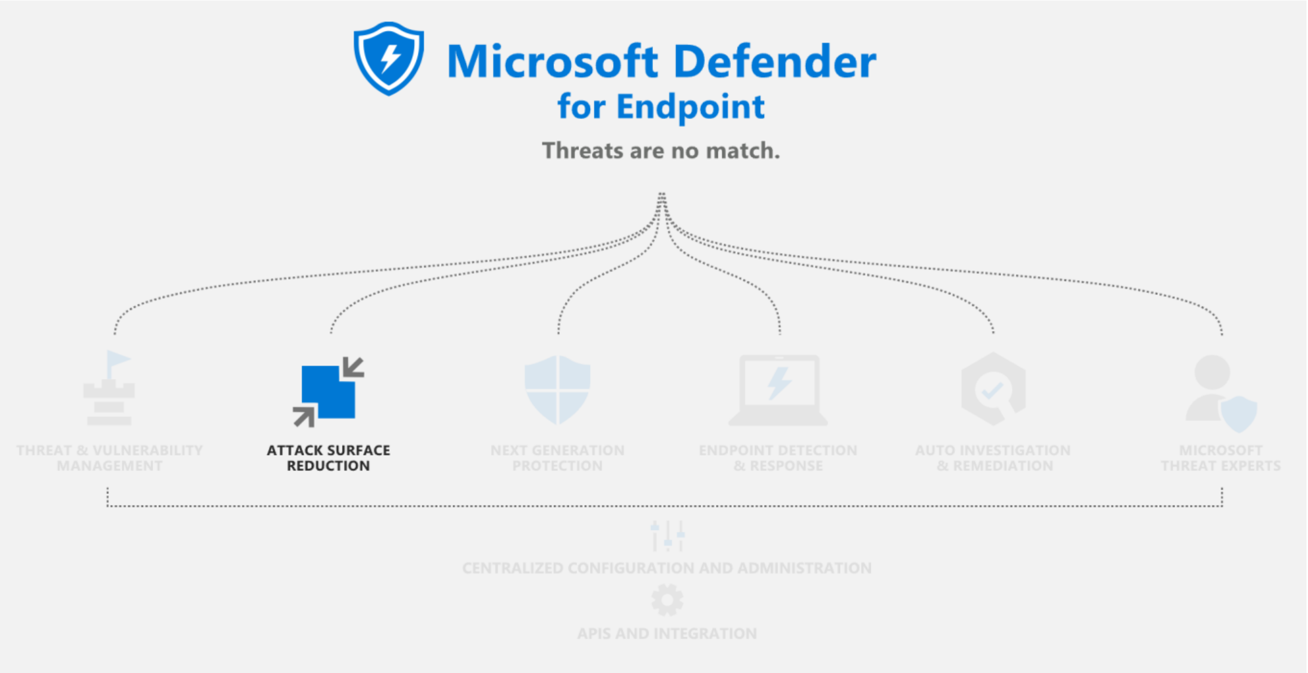
CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

Attack Surface Reduction

Quali problemi risolve?

- In un contesto con endpoint multi-piattaforma e in cui il perimetro [rete] non è più l'unico da sorvergliare, diventa difficile disegnare ed implementare una strategia di hardening.
- Non è sempre semplice misurare lo stato di avanzamento della distribuzione delle azioni di hardening


Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION

Come li risolve

- Rilevando, sulla base dei risultati di Threat & Vulnerability Management, quali sono le precise azioni da implementare sugli endpoint per ridurre rischio e superficie d'attacco, con una fotografia completa degli stati di avanzamento dell'hardening.

Cross Platform Protection

Windows macOS

Endpoints and servers

iOS

Mobile device OS

Windows 365

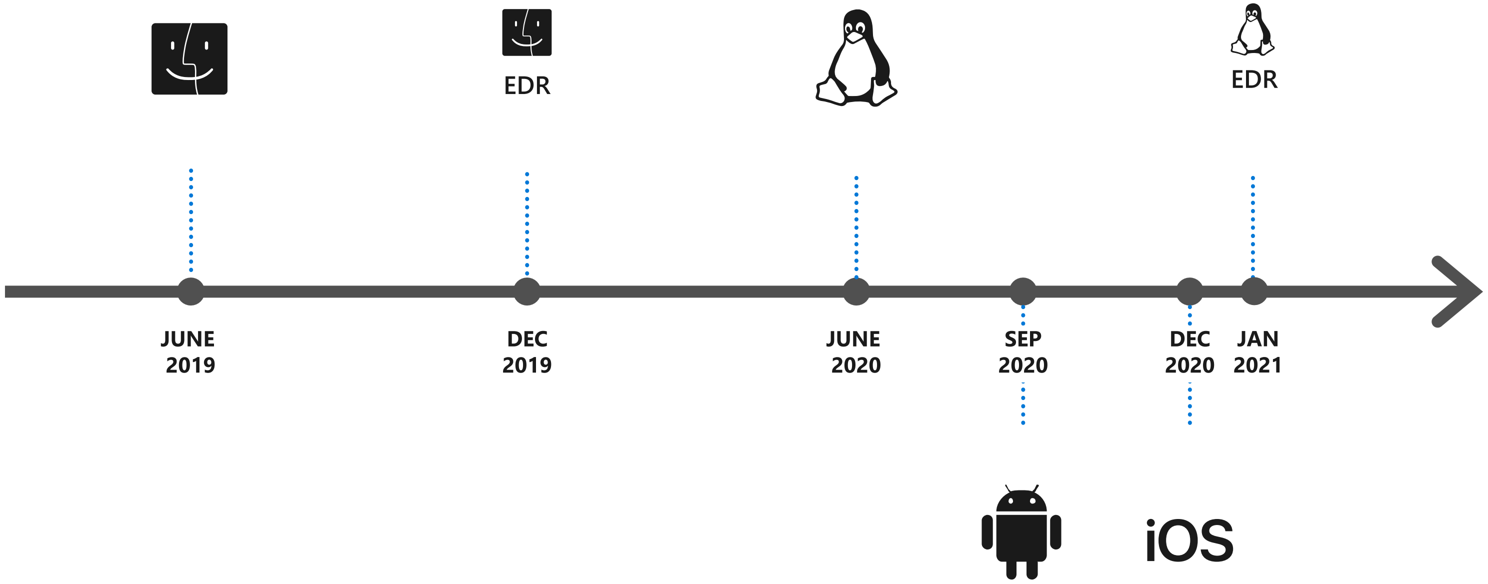
Azure Virtual Desktop

Virtual desktops

Cisco
HP Enterprise
Juniper Networks
Palo Alto Networks

Network devices

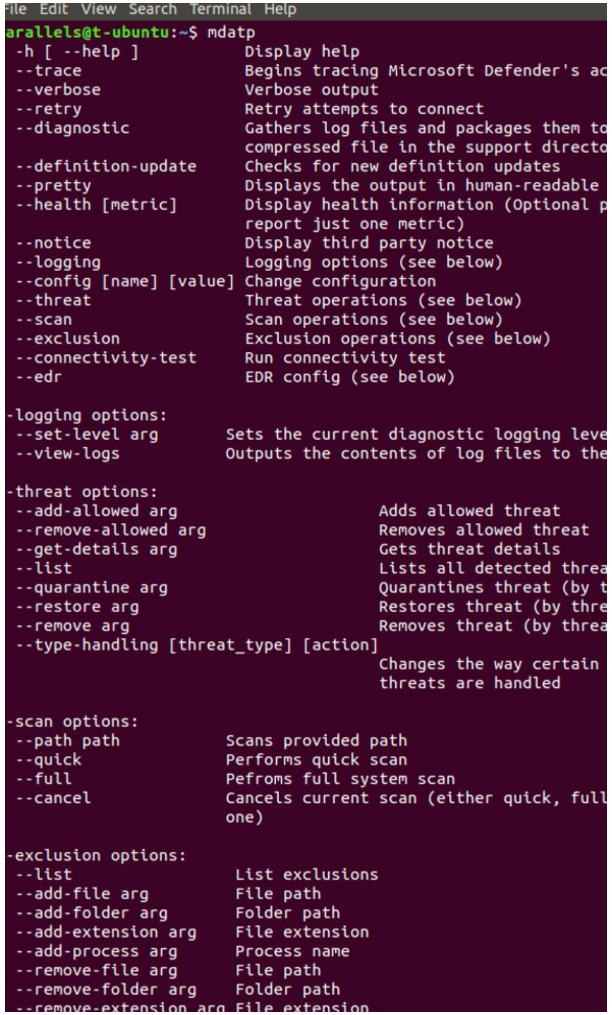
Cross Platform Protection - Journey



Microsoft Defender for Endpoint - Linux

Features:

- AV prevention
- Full command line experience (scanning, configuring, agent health)
- Potentially unwanted app protection
- Passive Mode (Manual)
- Live Response
- TVM
- Arc Enabled



```
arallels@t-ubuntu:~$ mdatp
 -h [ --help ]           Display help
 --trace                 Begins tracing Microsoft Defender's ac
 --verbose               Verbose output
 --retry                 Retry attempts to connect
 --diagnostic            Gathers log files and packages them to
                         compressed file in the support directo
 --definition-update     Checks for new definition updates
 --pretty                Displays the output in human-readable
 --health [metric]       Display health information (Optional p
                         report just one metric)
 --notice                Display third party notice
 --logging               Logging options (see below)
 --config [name] [value] Change configuration
 --threat                Threat operations (see below)
 --scan                  Scan operations (see below)
 --exclusion             Exclusion operations (see below)
 --connectivity-test     Run connectivity test
 --edr                   EDR config (see below)

-logging options:
 --set-level arg       Sets the current diagnostic logging leve
 --view-logs           Outputs the contents of log files to the

-threat options:
 --add-allowed arg                     Adds allowed threat
 --remove-allowed arg                  Removes allowed threat
 --get-details arg                     Gets threat details
 --list                                Lists all detected threa
 --quarantine arg                      Quarantines threat (by t
 --restore arg                         Restores threat (by thre
 --remove arg                          Removes threat (by threa
 --type-handling [threat_type] [action]
                                       Changes the way certain
                                       threats are handled

-scan options:
 --path path           Scans provided path
 --quick               Performs quick scan
 --full                Pefroms full system scan
 --cancel              Cancels current scan (either quick, full
                       one)

-exclusion options:
 --list                 List exclusions
 --add-file arg         File path
 --add-folder arg       Folder path
 --add-extension arg    File extension
 --add-process arg      Process name
 --remove-file arg      File path
 --remove-folder arg    Folder path
 --remove-extension arg File extension
```

In the Microsoft Defender Security Center, you'll see basic alerts and machine information.

Antivirus alerts:

- ✓ Severity
- ✓ Scan type
- ✓ Device information (hostname, machine identifier, tenant identifier, app version, and OS type)
- ✓ File information (name, path, size, and hash)
- ✓ Threat information (name, type, and state)

Device information:

- ✓ Machine identifier
- ✓ Tenant identifier
- ✓ App version
- ✓ Hostname
- ✓ OS type
- ✓ OS version
- ✓ Computer model
- ✓ Processor architecture
- ✓ Whether the device is a virtual machine

Microsoft Defender for Endpoint - Mac

The first step in our cross-platform journey

Threat prevention

- Realtime MW protection for Mac OS
- Malware detection alerts visible in the Microsoft Defender for Endpoint console
- Device control – removable storage protection
- Potentially unwanted app protection

Rich cyber data enabling attack detection and investigation

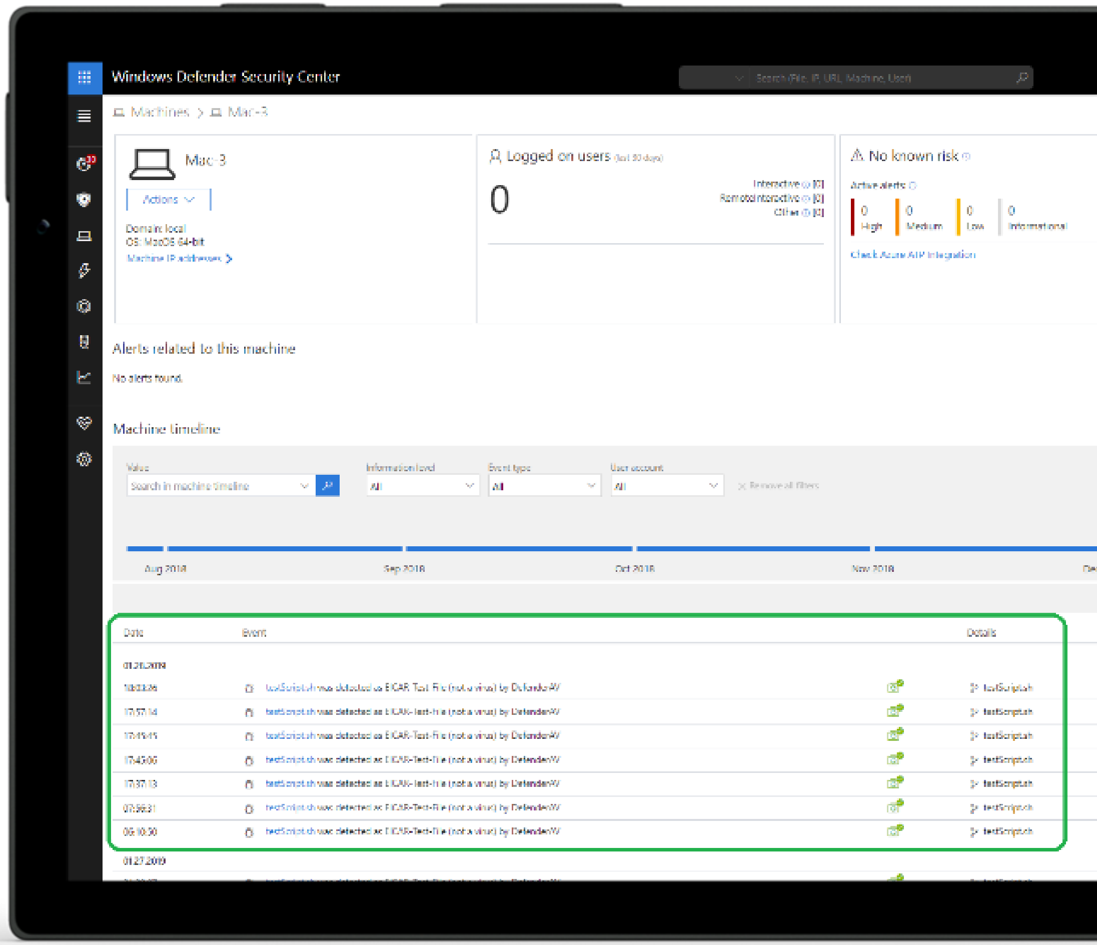
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Cloud-delivered protection
- Live response

Enterprise Grade

- Lightweight deployment & onboarding process
- Performant, none intrusive
- Aligned with compliance, privacy & data sovereignty requirements
- Passive mode (Manual)

Seamlessly integrated with Microsoft Defender for Endpoint capabilities

- Detection dictionary across the kill chain
- 6 months of raw data on all machines inc Mac OS
- Reputation data for all entities being logged
- Single pane of glass across all endpoints Mac OS
- Advanced hunting on all raw data including Mac OS
- Custom TI
- API access to the entire data model inc Mac OS
- SIEM integration
- Compliance & Privacy
- RBAC



Domain: local
OS: MacOS 64-bit

Alerts related to this machine

No alerts found.

Machine timeline

Date	Event	Details
01.28.2019		
18:03:26	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:57:14	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:45:45	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:43:06	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
17:37:13	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
07:56:31	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
06:10:30	testScript.sh was detected as EICAR-Test-File (not a virus) by DefenderAV	testScript.sh
01.27.2019		

Panoramica delle minacce su mobile

Phishing

85% of phishing attacks seen on mobile devices take place outside of email

90% of data breaches start from a phishing attack

Malicious apps

46% of organizations had at least one employee download a malicious mobile application

>5M New malware added for Android. From ransomware to financial trojans

Vulnerable device

90% Android devices are running out-of-date version of OS

30% iOS devices are running out-of-date version of OS

Jailbroken/Rooted device

6% of all organizations have a jailbroken/rooted device

Perché proteggere i dispositivi mobile?

Productivity has gone mobile

- Corporate data is being increasingly accessed on mobile outside the corporate perimeter
- COVID-19 has hastened the pace of mobile adoption within enterprises

So have the attackers

- Mobile phishing attempts grew by more than 65% in the last year
- Security concerns are #1 inhibitor to BYOD adoption in the enterprises

MDM isn’t enough

- MDM & MAM are management tools for administration of mobile devices
- Only MTD can detect and block mobile cybersecurity threats from harming an organization

Microsoft Defender for Endpoint - Android

Web Protection

- Anti-phishing
- Block unsafe network connections
- Custom indicators: allow/block URLs
- Tamper protection
- TVM
- Microsoft Tunnel

Malware Scan

- Alerts for malware, PUA
- Files scan
- Storage and memory peripheral scans

Single Pane of Glass Reporting

- Alerts for phishing
- Alerts for malicious apps
- Auto-connection for reporting in Microsoft Defender Security Center

Conditional Access

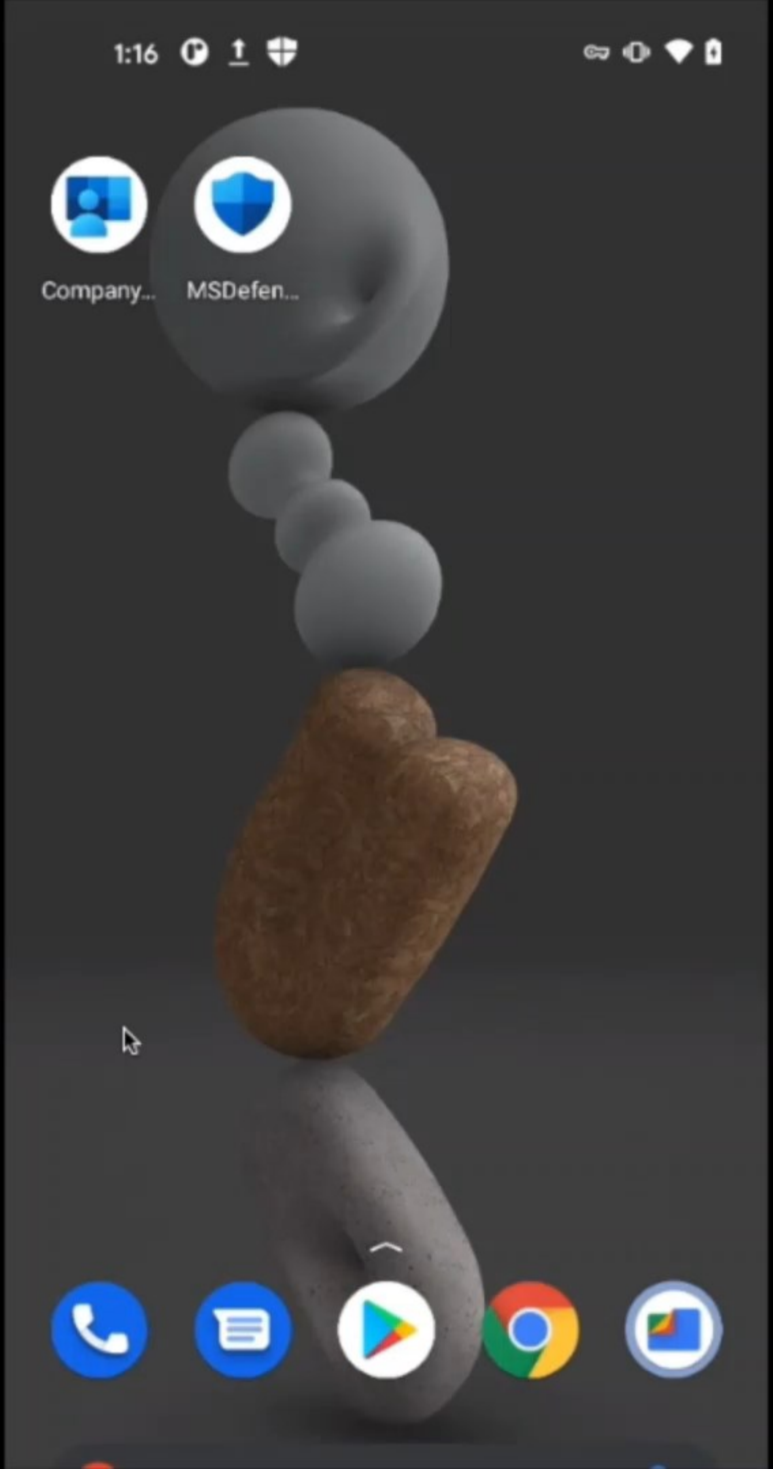
- Block risky devices
- Mark devices non-compliant

Supported Configurations

- Device Administrator
- Android Enterprise (Work Profile)

Licensed by Microsoft

- Included in per user licenses that offer Microsoft Defender for Endpoint
- Part of the 5 qualified devices for eligible licensed users
- Reach out to your account team or CSP


1:16
Company...
MSDefen...

Microsoft Defender for Endpoint - iOS

Web Protection

- Anti-Phishing
- Block unsafe network connections
- Custom Indicators: allow/block URLs
- Tamper protection
- TVM
- Microsoft Tunnel

Single Pane of Glass Reporting

- Alerts for phishing
- Auto connection for reporting in Microsoft Defender Security Center

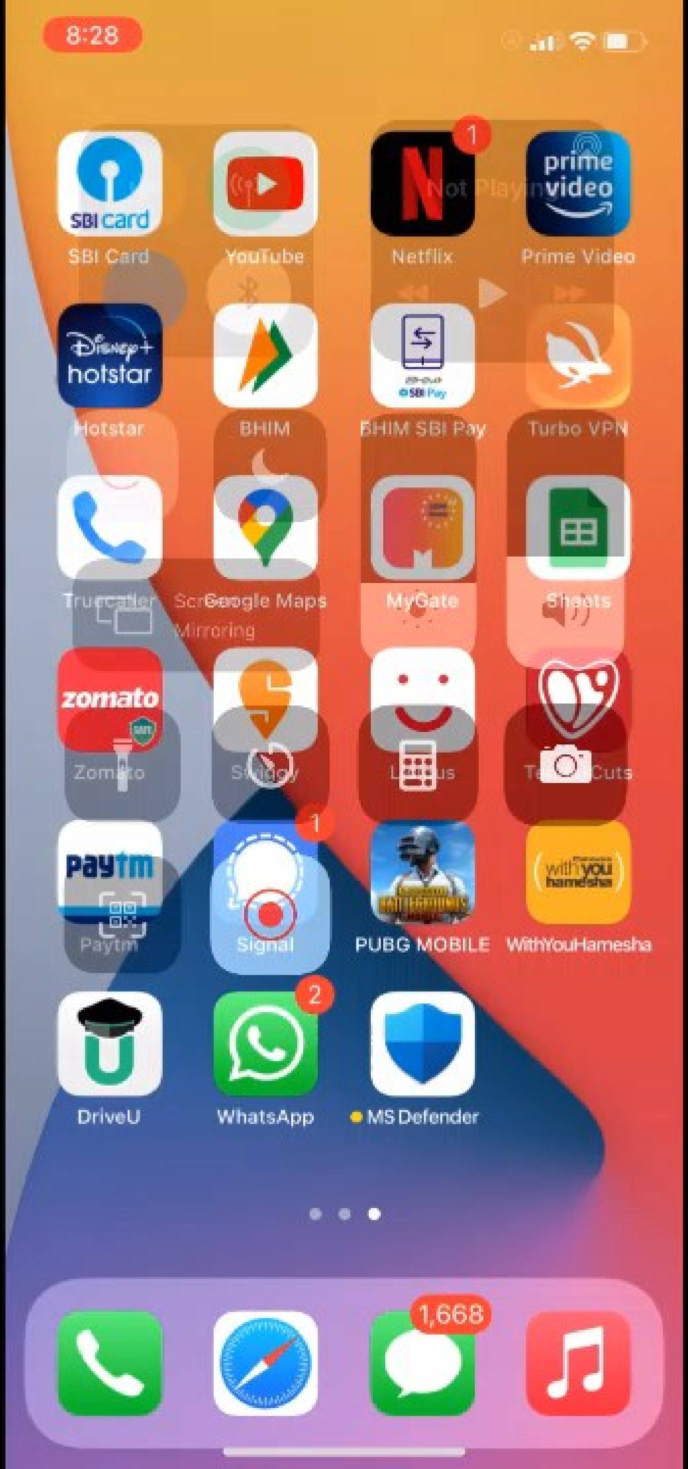
Supported Configurations

- Supervised
- Unsupervised

Licensed by Microsoft

- Included in per user licenses that offer Microsoft Defender for Endpoint
- Part of the 5 qualified devices for eligible licensed users
- Reach out to your account team or CSP

Onboarding


8:28
SBI Card
YouTube
Netflix
Prime Video
Hotstar
BHIM
BHIM SBI Pay
Turbo VPN
Truecaller
Google Maps
Screen Mirroring
MyGate
Sheets
Zomato
Swiggy
Lenskart
TeaCuts
Paytm
Signal
PUBG MOBILE
WithYouHamesha
DriveU
WhatsApp
MS Defender
1,668

Anti - Phishing

Threat and Vulnerability Management for Android and iOS

What’s available

→Vulnerability Assessment of OS - Android and iOS

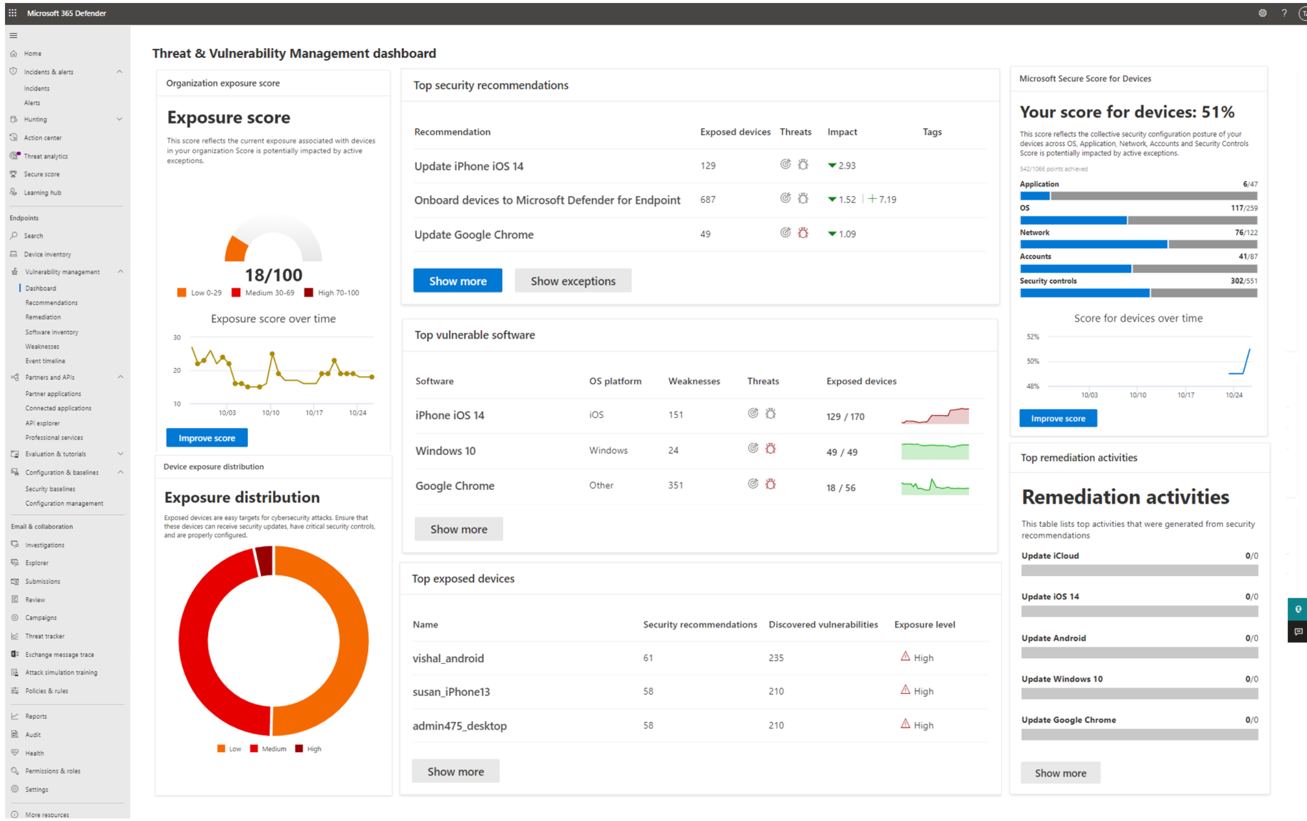
→Vulnerability Assessment of apps - Android

→Exposure Score

→Security Recommendations based on vulnerability assessment

→Software Inventory - Android

→Native integration with all other TVM features – weaknesses page, advanced hunting, events and notifications



Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization Score is potentially impacted by active exceptions.

18/100

🟧 Low 0-29 🟥 Medium 30-69 🟥 High 70-100

Exposure score over time

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Update iPhone iOS 14	129		▼2.93	
Onboard devices to Microsoft Defender for Endpoint	687		▼1.52 | +7.19	
Update Google Chrome	49		▼1.09	

Top vulnerable software

Software	OS platform	Weaknesses	Threats	Exposed devices
iPhone iOS 14	iOS	151		129 / 170
Windows 10	Windows	24		49 / 49
Google Chrome	Other	351		18 / 56

Top exposed devices

Name	Security recommendations	Discovered vulnerabilities	Exposure level
vishal_android	61	235	⚠ High
susan_iPhone13	58	210	⚠ High
admin475_desktop	58	210	⚠ High

Microsoft Secure Score for Devices

Your score for devices: 51%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.

542/1066 points achieved

Application	6/47
OS	117/259
Network	76/122
Accounts	41/87
Security controls	302/551

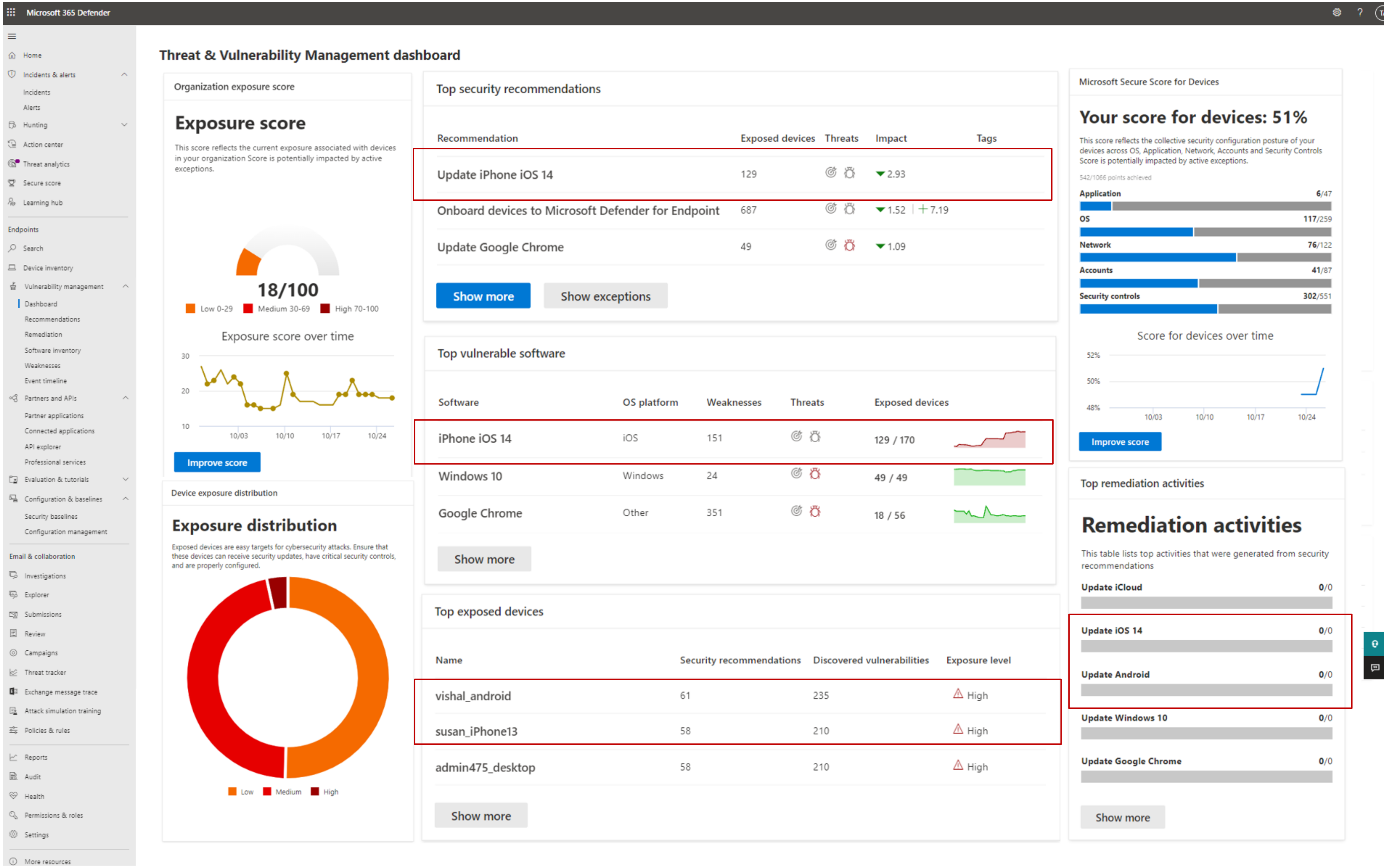
Score for devices over time

Top remediation activities

Remediation activities

This table lists top activities that were generated from security recommendations

Update iCloud	0/0
Update iOS 14	0/0
Update Android	0/0
Update Windows 10	0/0
Update Google Chrome	0/0



Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization Score is potentially impacted by active exceptions.

18/100

🟧 Low 0-29 🟥 Medium 30-69 🟥 High 70-100

Exposure score over time

Improve score

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

🟧 Low 🟥 Medium 🟥 High

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Update iPhone iOS 14	129		▼ 2.93	
Onboard devices to Microsoft Defender for Endpoint	687		▼ 1.52 | + 7.19	
Update Google Chrome	49		▼ 1.09	

Show more Show exceptions

Top vulnerable software

Software	OS platform	Weaknesses	Threats	Exposed devices
iPhone iOS 14	iOS	151		129 / 170
Windows 10	Windows	24		49 / 49
Google Chrome	Other	351		18 / 56

Show more

Top exposed devices

Name	Security recommendations	Discovered vulnerabilities	Exposure level
vishal_android	61	235	⚠ High
susan_iPhone13	58	210	⚠ High
admin475_desktop	58	210	⚠ High

Show more

Microsoft Secure Score for Devices

Your score for devices: 51%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.

542/1066 points achieved

Application	6/47
OS	117/259
Network	76/122
Accounts	41/87
Security controls	302/551

Score for devices over time

Improve score

Top remediation activities

Remediation activities

This table lists top activities that were generated from security recommendations

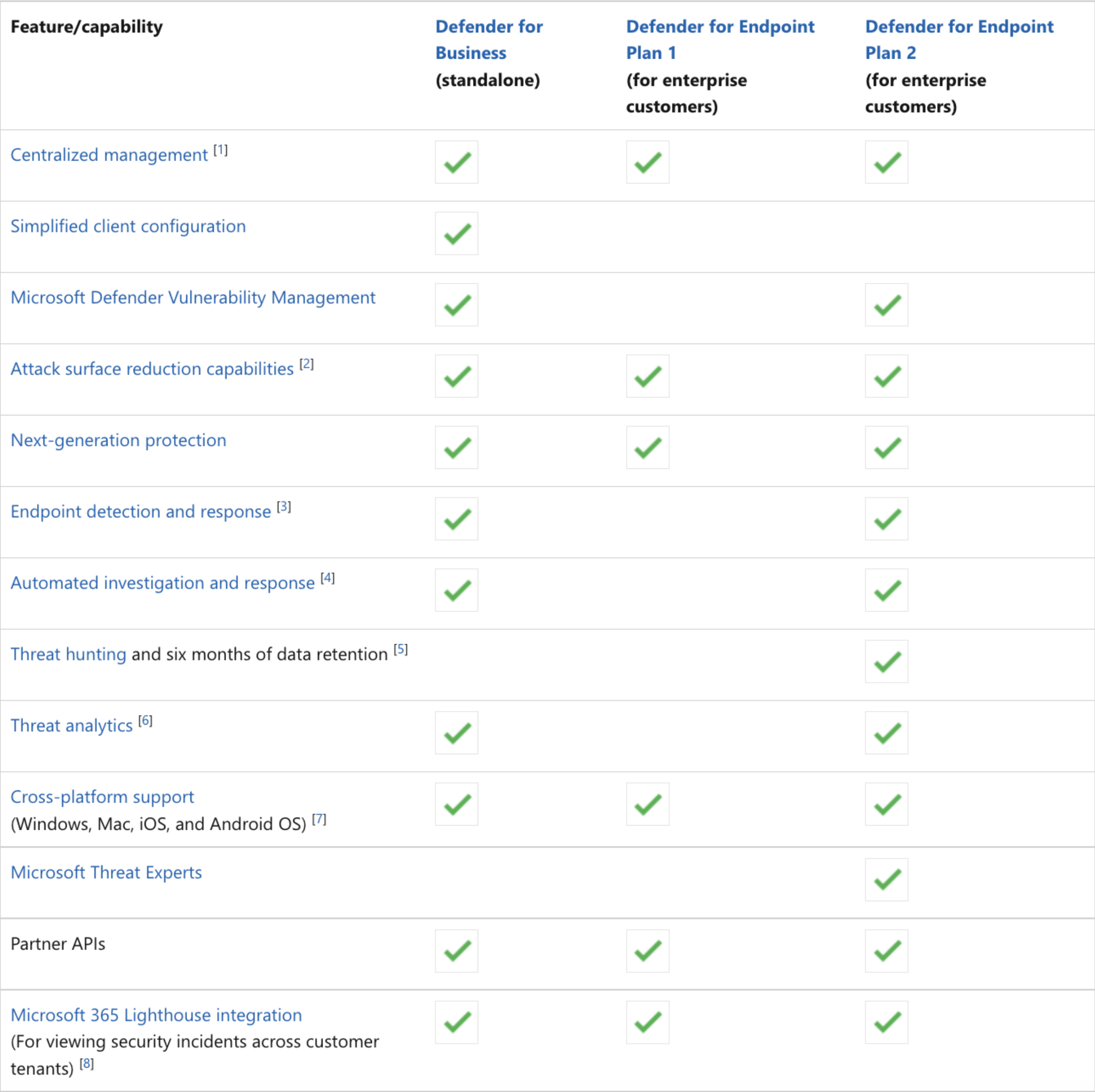
Update iCloud	0/0
Update iOS 14	0/0
Update Android	0/0
Update Windows 10	0/0
Update Google Chrome	0/0

Show more

Riassunto finale delle funzionalità

Capabilities	Windows	🐧	macOS	🤖	iOS
Threat & Vulnerability Management - Cyber Security Posture Provides real-time visibility and recommend ways to improve your overall security posture and reduce risk to your organization.	●	●	●	●	●
ASR controls ASR rules, Network protection, Device control, App control	●	◔	◐		
Industry certified AV Consistent top scores on AV-Test, AV-Comparatives and SE Labs independent testing	●	●	●	●	●
Endpoint Detection & Response - EDR Monitors behaviors, applies machine learning, and security analytics to spot attacks	●	●	●	◐	◐
Response and Self- Healing Automatically investigate alerts and remediate complex threats in minutes, without human intervention	●	◐	◐		
Managed Hunting services - MDR A service that provides your Security Operations Centers with deep knowledge, expert level threat monitoring, analysis, and support to identify critical threats in your unique environment.	●	●	●	●	●
Built in contextual TI based on industry TI driven reports that helps you assess the impact of threats to your environment and provide recommendation on how contain them	●	●	●	●	●
Management console Unified security management, including security configuration, recommendation and prioritization	●	◐	◐	●	●

Comparazione dei piani di MDE



Feature/capability	Defender for Business (standalone)	Defender for Endpoint Plan 1 (for enterprise customers)	Defender for Endpoint Plan 2 (for enterprise customers)
Centralized management [1]	✓	✓	✓
Simplified client configuration	✓		
Microsoft Defender Vulnerability Management	✓		✓
Attack surface reduction capabilities [2]	✓	✓	✓
Next-generation protection	✓	✓	✓
Endpoint detection and response [3]	✓		✓
Automated investigation and response [4]	✓		✓
Threat hunting and six months of data retention [5]			✓
Threat analytics [6]	✓		✓
Cross-platform support (Windows, Mac, iOS, and Android OS) [7]	✓	✓	✓
Microsoft Threat Experts			✓
Partner APIs	✓	✓	✓
Microsoft 365 Lighthouse integration (For viewing security incidents across customer tenants) [8]	✓	✓	✓

Volete quotidianamente contenuti come questi?

Siete appassionati di security e di tecnologie Microsoft?

SEGUITECI! 😉

Microsoft Security Italian Users Group

ITSpecialist.cloud

Grazie

Riccardo Corna
Microsoft MVP – Senior Consultant @ Microsys
rc@itspecialist.cloud