ICT POWER.IT

Microsoft

#POWERCON2023

Difendersi in Modo Proattivo: Microsoft Defender for Endpoint e Cloud Apps

Guido Imperatore

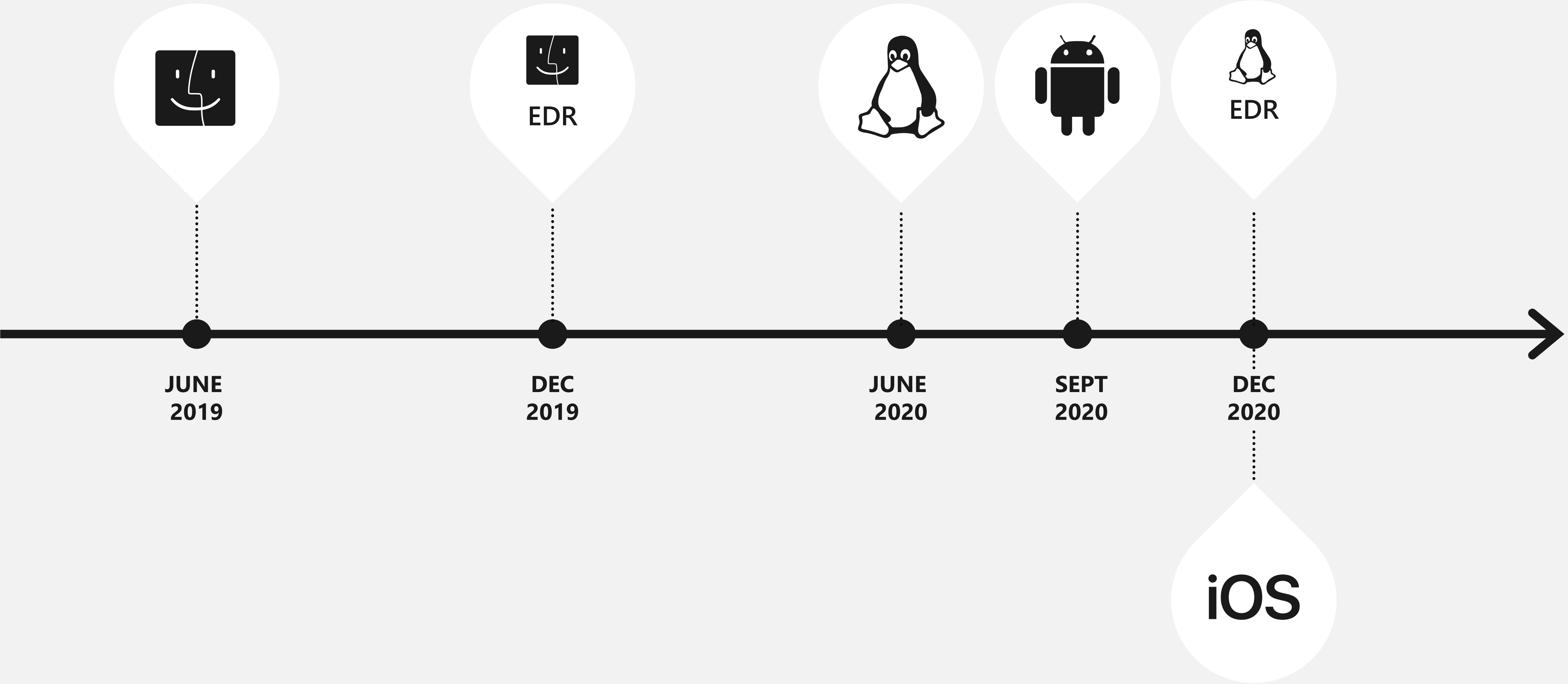
Microsoft Solution Specialist @ Project Informatica - WeAreProject
guido.imperatore@project.it

f /guido.imperatore
@GuidoImpe
in /guidoimperatore

Agenda

- Timeline Defender for Endpoint
- Funzionalità Defender for Endpoint
- Licensing
- Integrazione Defender for Endpoint e Cloud Apps
- Demo Integrazione MDE e Cloud Apss

Delivering industry leading endpoint security across platforms



JUNE 2019

EDR

DEC 2019

JUNE 2020

SEPT 2020

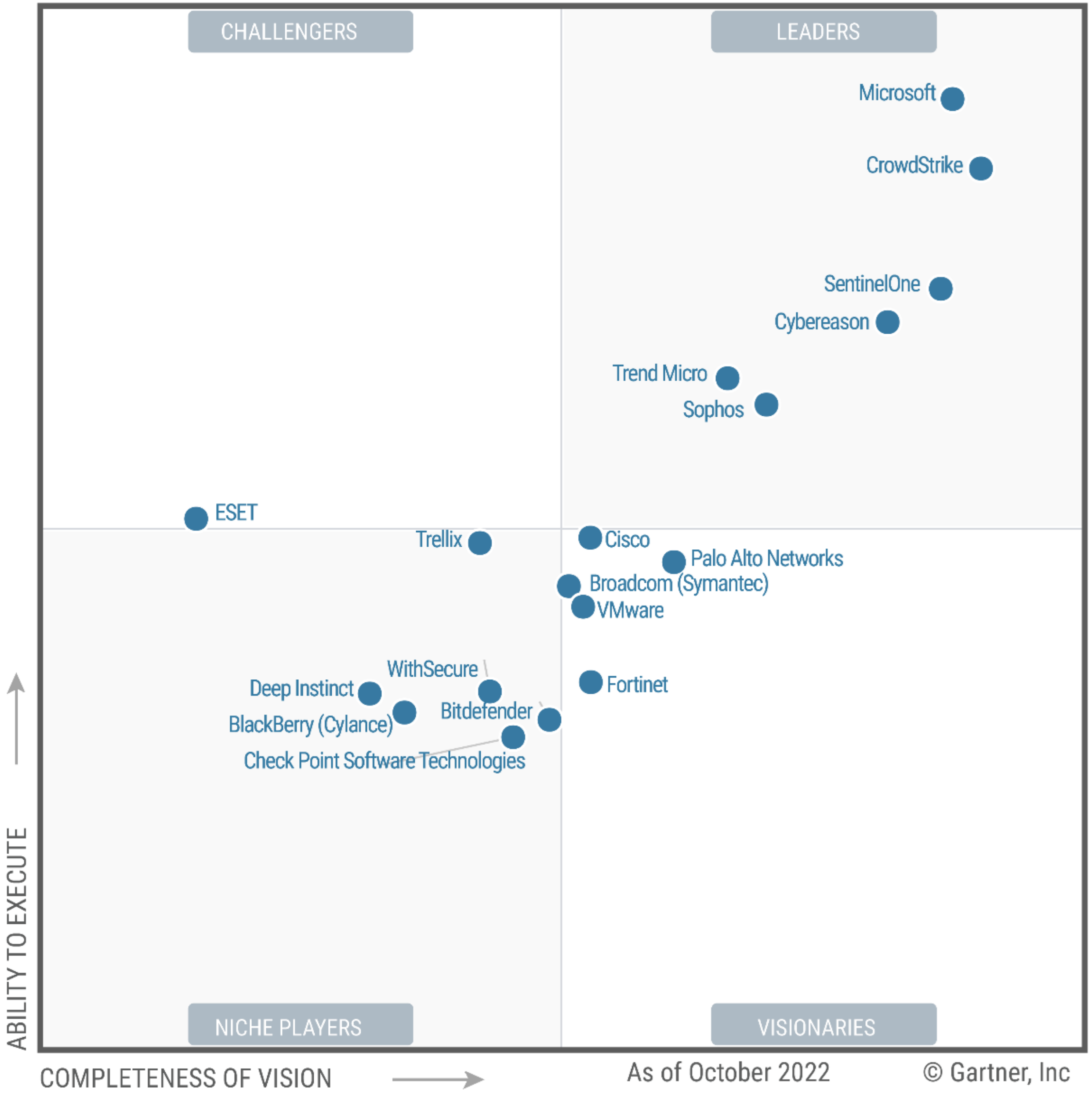
EDR

DEC 2020

iOS

General availability dates

Figure 1: Magic Quadrant for Endpoint Protection Platforms



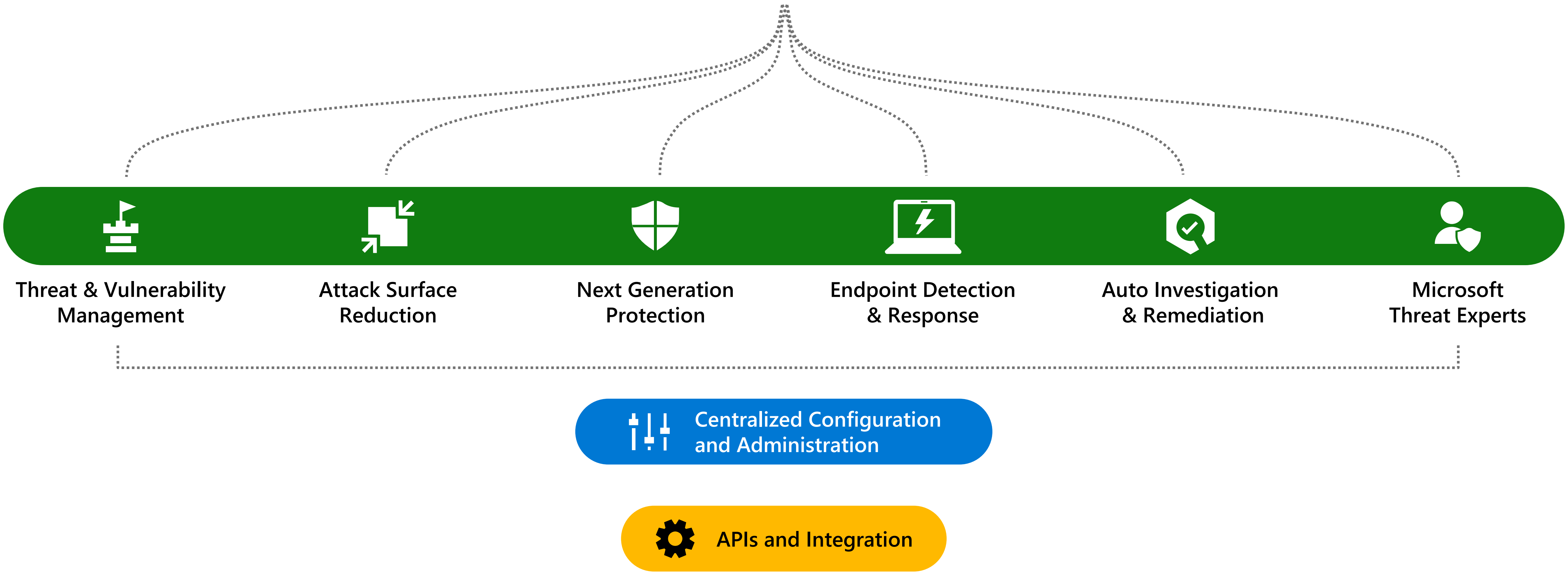
As of October 2022 © Gartner, Inc

Source: Gartner (December 2022)

Microsoft Defender for Endpoint: Leader Gartner per la terza volta consecutiva

Microsoft Defender for Endpoint

Threats are no match.



Threat & Vulnerability Management

Attack Surface Reduction

Next Generation Protection

Endpoint Detection & Response

Auto Investigation & Remediation

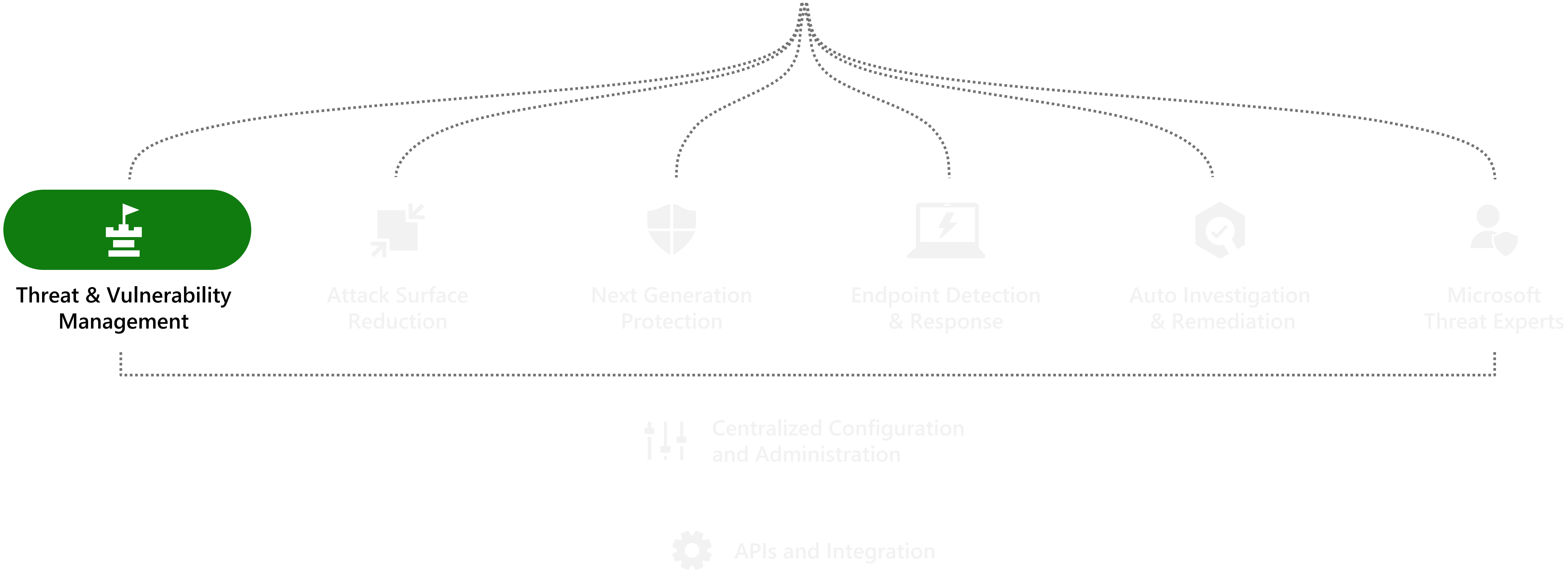
Microsoft Threat Experts

Centralized Configuration and Administration

APIs and Integration

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

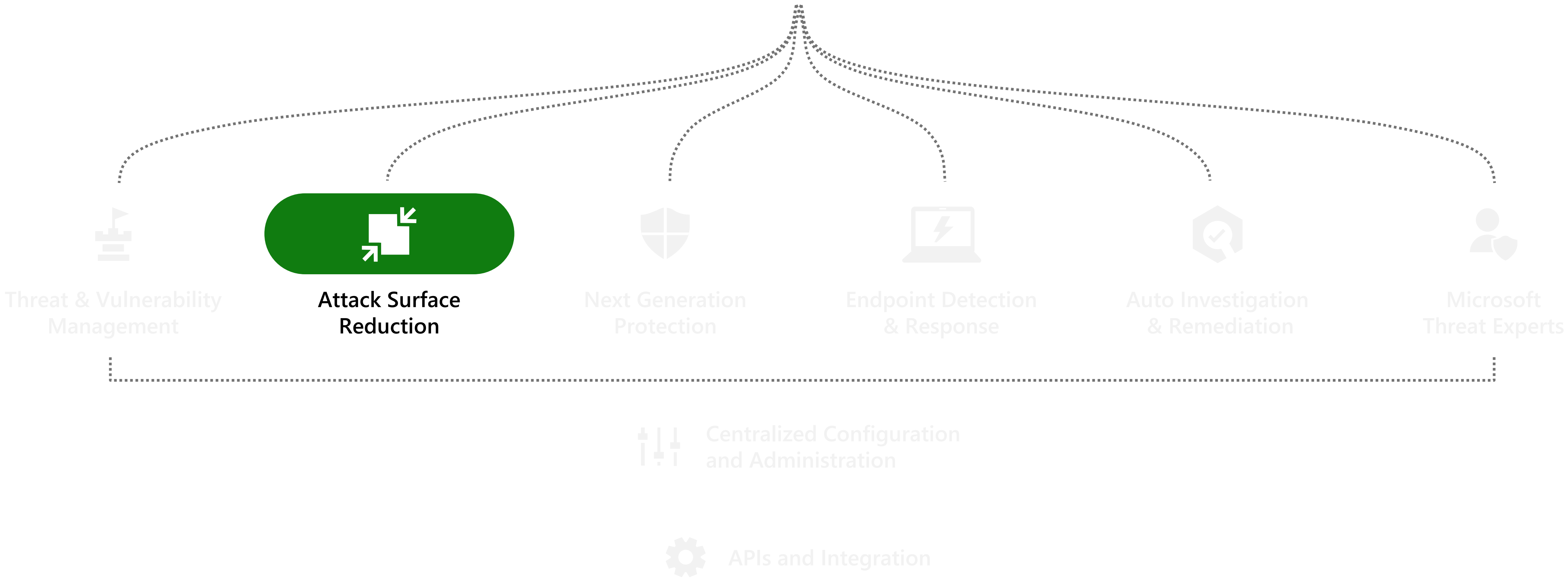
Threat & Vulnerability Management

Cosa rileva TVM?

- Quali dispositivi sono conformi e configurati correttamente
- Quali dispositivi sono vulnerabili contro CVE-XXX
- I dispositivi sono attivi con zero-day?
- Quali dispositivi non sono conformi e configurati con errori
- Quali dispositivi non sono configurati correttamente con AV
- Dispositivi senza Tamper Protection
- Dispositivi con una versione datata di .net framework
- Dispositivi in cui l'account amministratore predefinito non è disabilitato

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

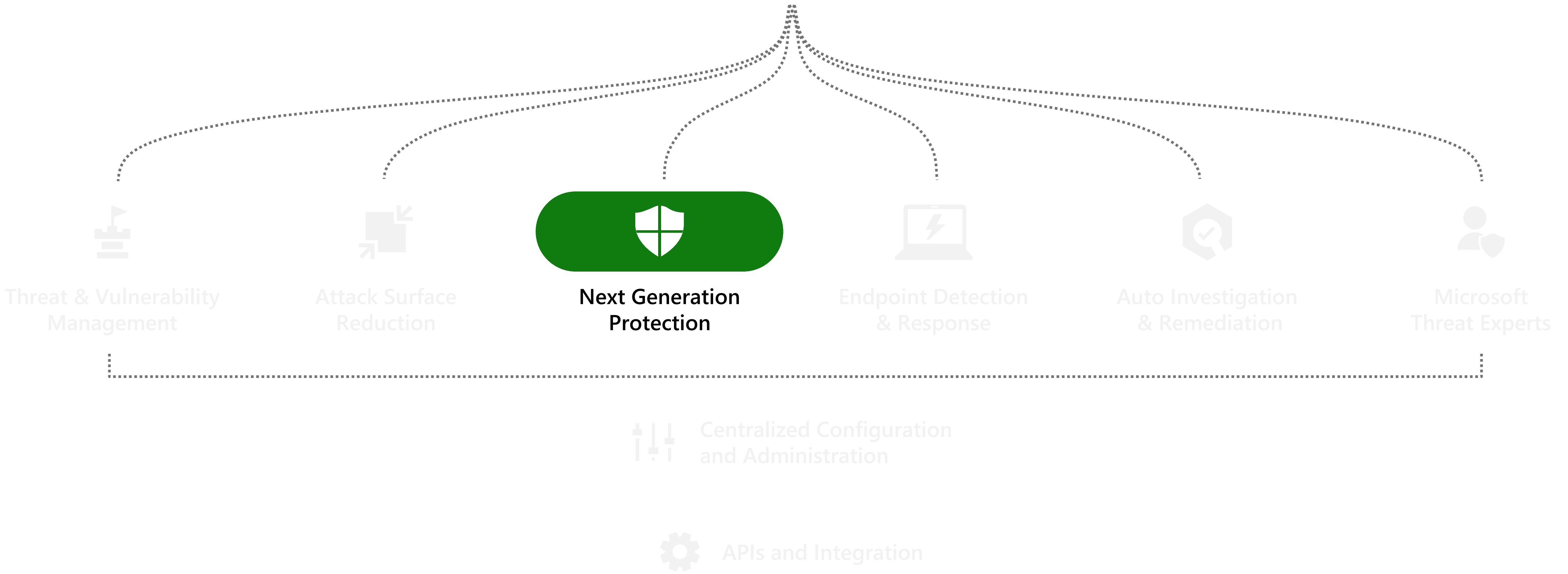
Attack Surface Reduction

Come si comporta ASR?

- Riceve le analisi svolte da TVM
- Attraverso delle regole blocca eventuale codice malevolo
- Attraverso delle regole blocca contenuto attivo in allegati E-mail
- Attraverso delle regole blocca esecuzione di comandi per impedire Lateral Movement

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

Next Generation Protection

Come si comporta NGP?

⃠ Ineffective

Static signatures:
focus on a file

- Hashes
- Strings
- Emulators

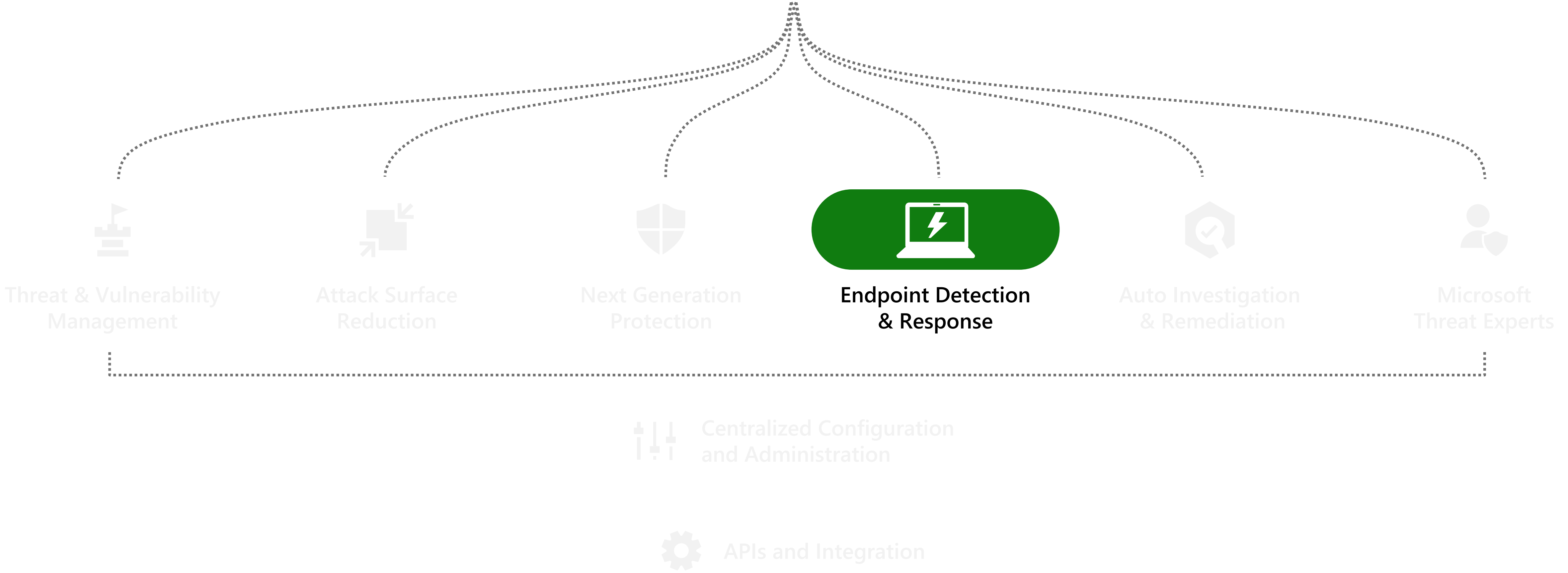
✓ Effective

Dynamic heuristics:
focus on *run-time behaviors*

- Behavior monitoring
- Memory scanning
- AMSI
- Command-line scanning

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

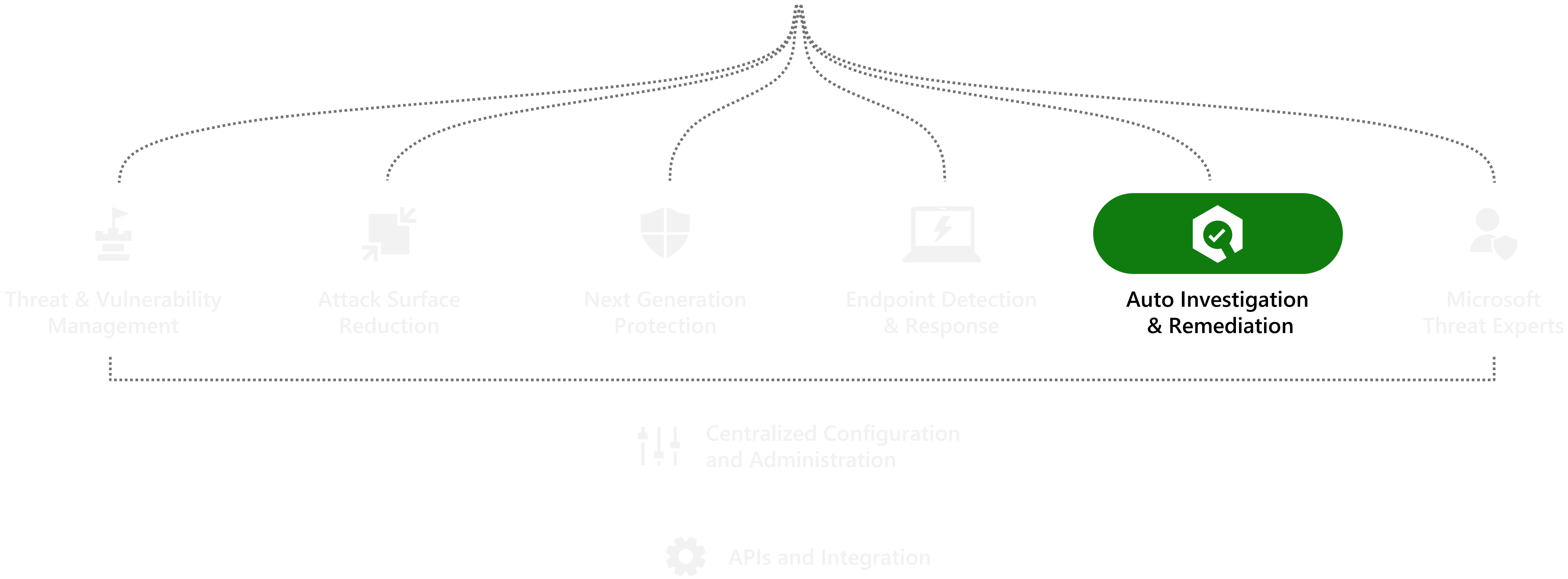
Endpoint Detection & Response

Come si comporta EDR?

- Correlazione di Eventi
- Dispone di Alert fino a 6 mesi
- Analisi comportamentale
- Dispone di modalità blocco e di audit

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

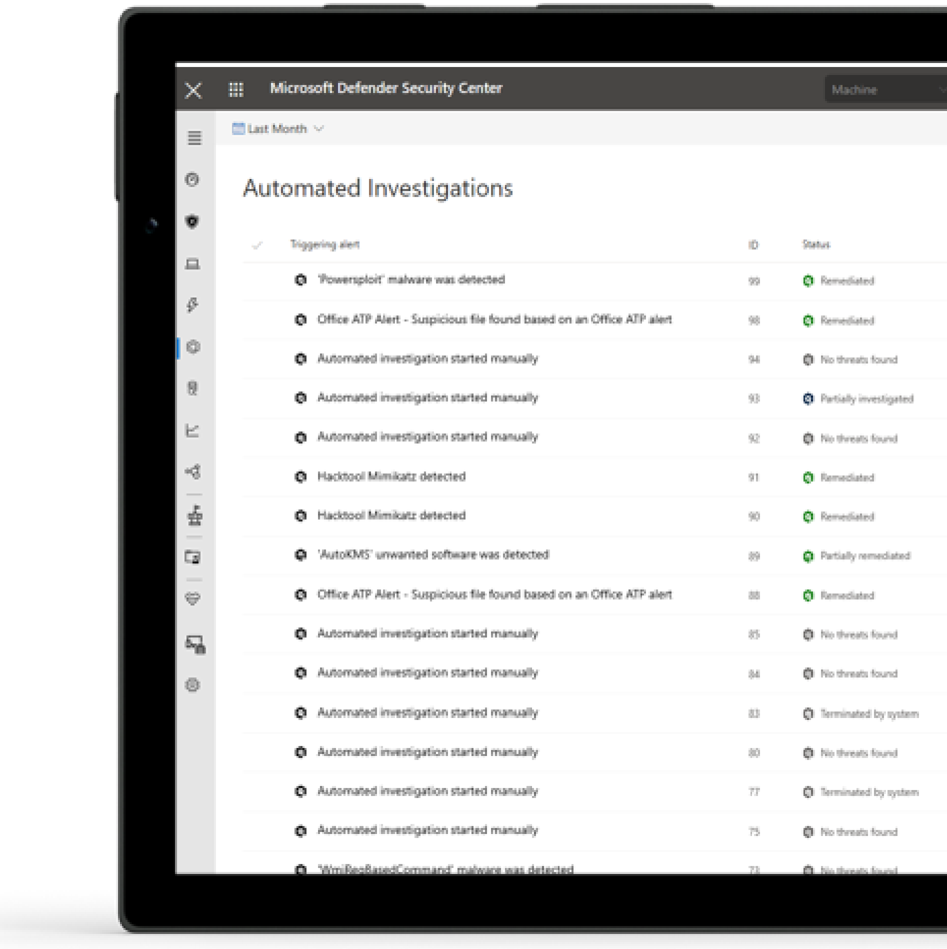
APIs and Integration

Autoinvestigation & Remediation

Come si comporta AIR?

Passaggi di un Cyber Analist in caso di compromissione/Alert:

- Determinare quale alert richiede la sua attenzione
- Eseguire Remediation necessaria
- Decidere gli step successiva per fa si che non accada in futuro

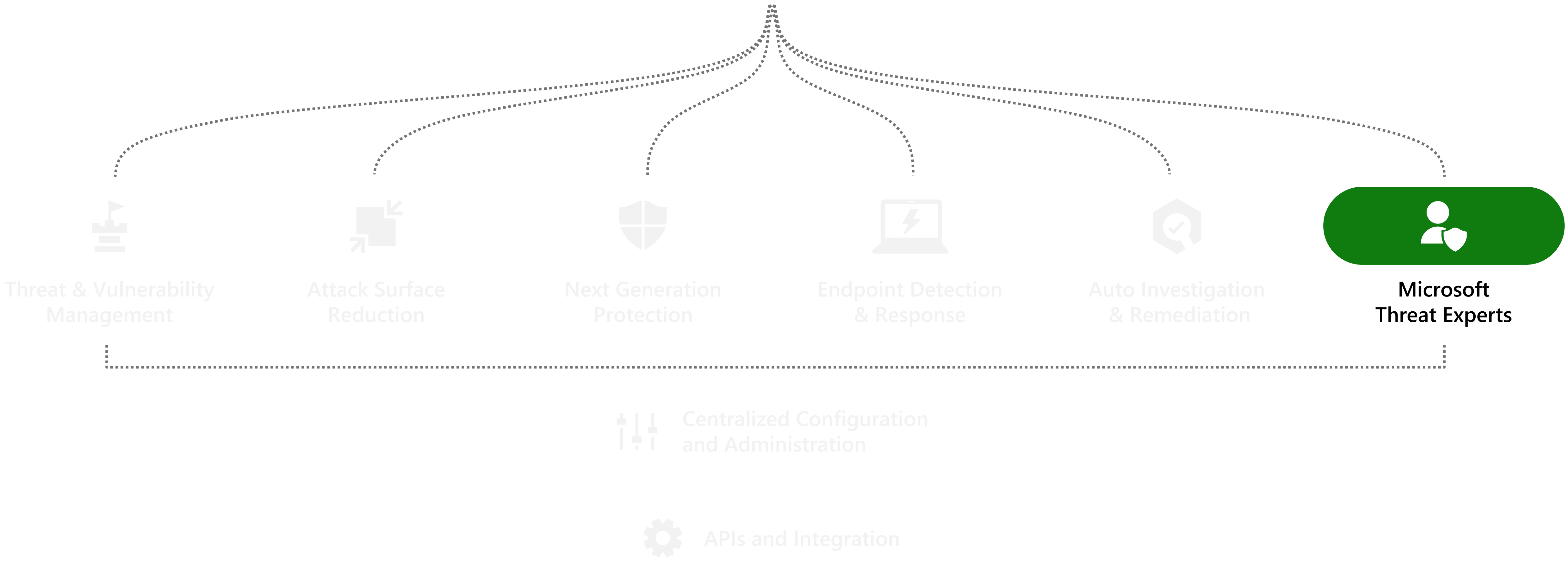


Automated Investigations

Triggering alert	ID	Status
'Powersploit' malware was detected	99	Remediated
Office ATP Alert - Suspicious file found based on an Office ATP alert	98	Remediated
Automated investigation started manually	94	No threats found
Automated investigation started manually	93	Partially investigated
Automated investigation started manually	92	No threats found
Hacktool Mimikatz detected	91	Remediated
Hacktool Mimikatz detected	90	Remediated
'AutoKMS' unwanted software was detected	89	Partially remediated
Office ATP Alert - Suspicious file found based on an Office ATP alert	88	Remediated
Automated investigation started manually	85	No threats found
Automated investigation started manually	84	No threats found
Automated investigation started manually	83	Terminated by system
Automated investigation started manually	80	No threats found
Automated investigation started manually	77	Terminated by system
Automated investigation started manually	75	No threats found
'WmiRegBasedCommand' malware was detected	73	No threats found

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

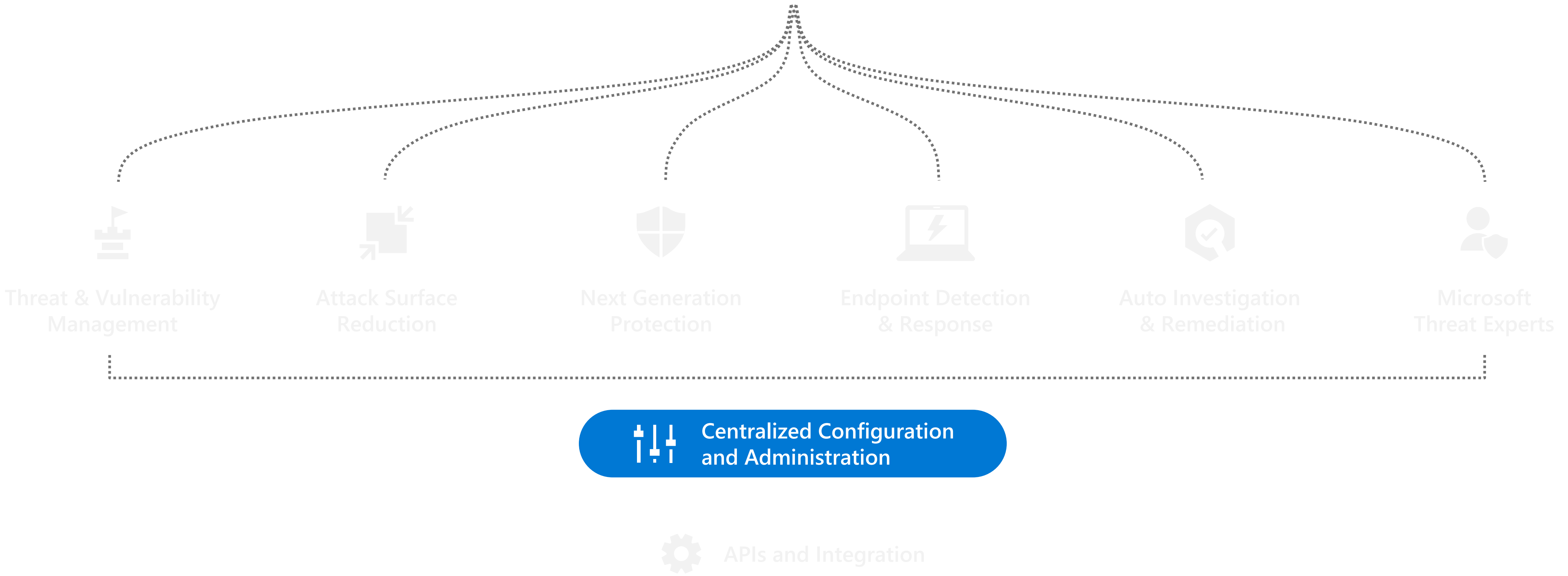
Microsoft Threat Experts

A cosa serve questa componente?

- Monitoraggio e analisi delle minacce, riducendo i tempi di permanenza degli attaccanti e i rischi per l'azienda
- IA addestrata da Etichal Hacker per scoprire e dare priorità agli attacchi noti e sconosciuti
- Identificare i rischi più importanti, aiutando i SOC a massimizzare tempo ed energia
- Microsoft mette a disposizioni i propri analisti per casi particolarmente complessi

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

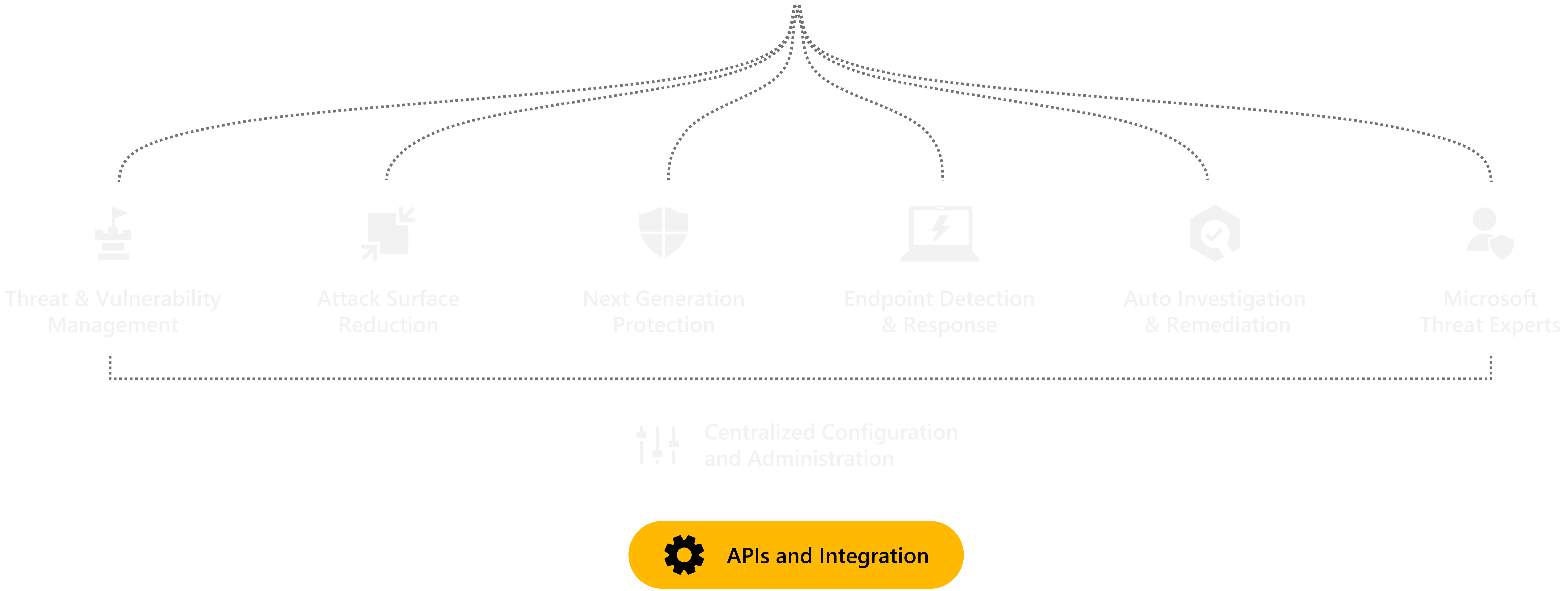
Centralized Configuration and Administration

APIs and Integration

Microsoft Defender

for Endpoint

Threats are no match.



Threat & Vulnerability Management

Attack Surface Reduction

Next Generation Protection

Endpoint Detection & Response

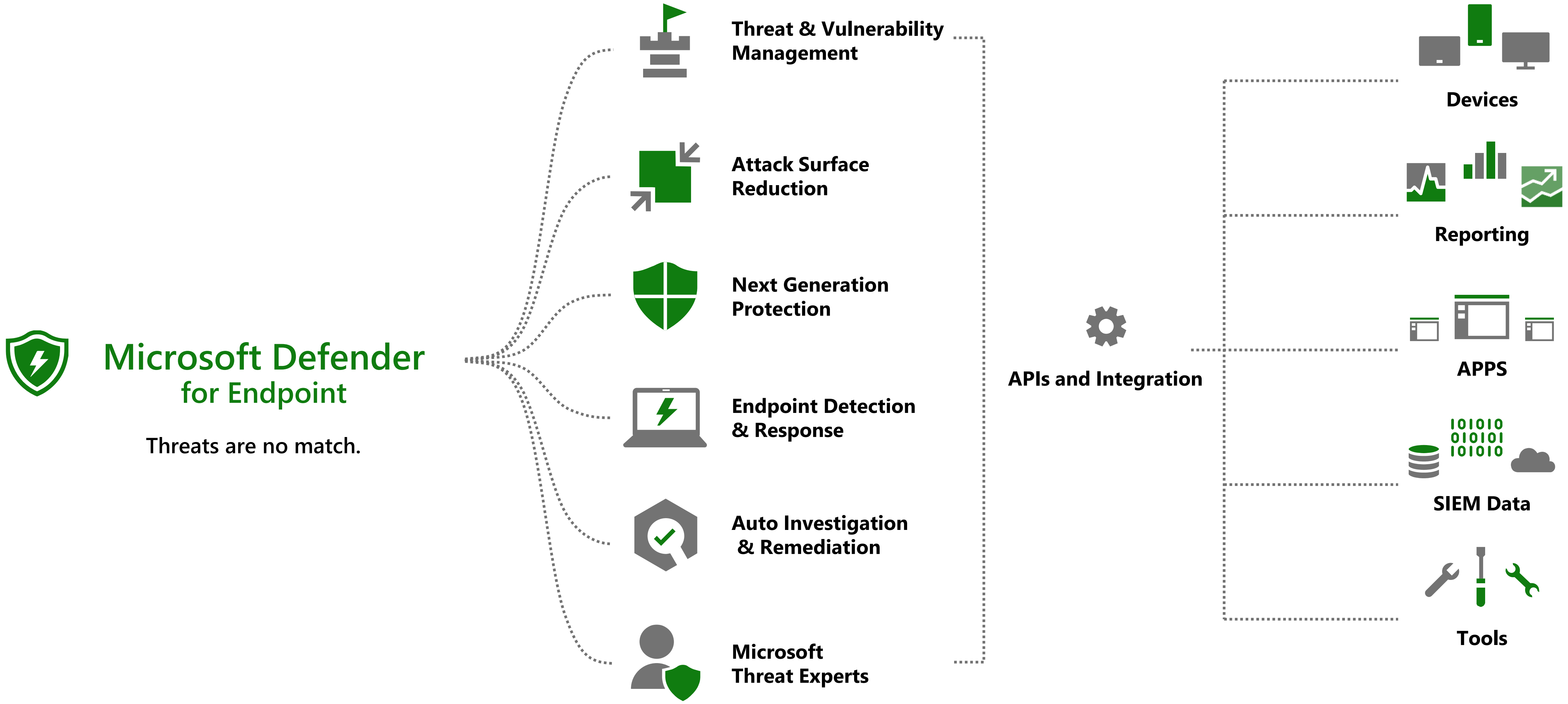
Auto Investigation & Remediation

Microsoft Threat Experts

Centralized Configuration and Administration

APIs and Integration

Connecting with the platform



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

APIs and Integration

Devices

Reporting

APPS

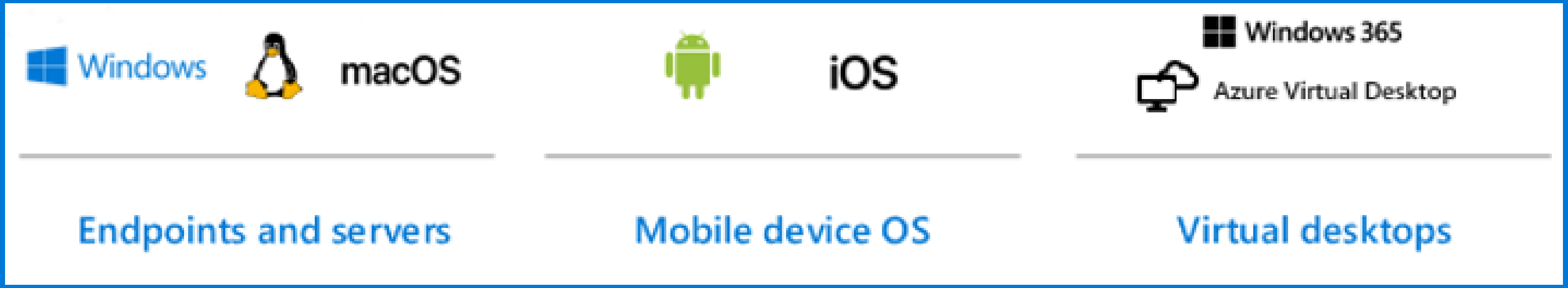
SIEM Data

Tools

Defender For Endpoint Cross Platform

Sistemi Operativi: Microsoft Defender for Endpoint

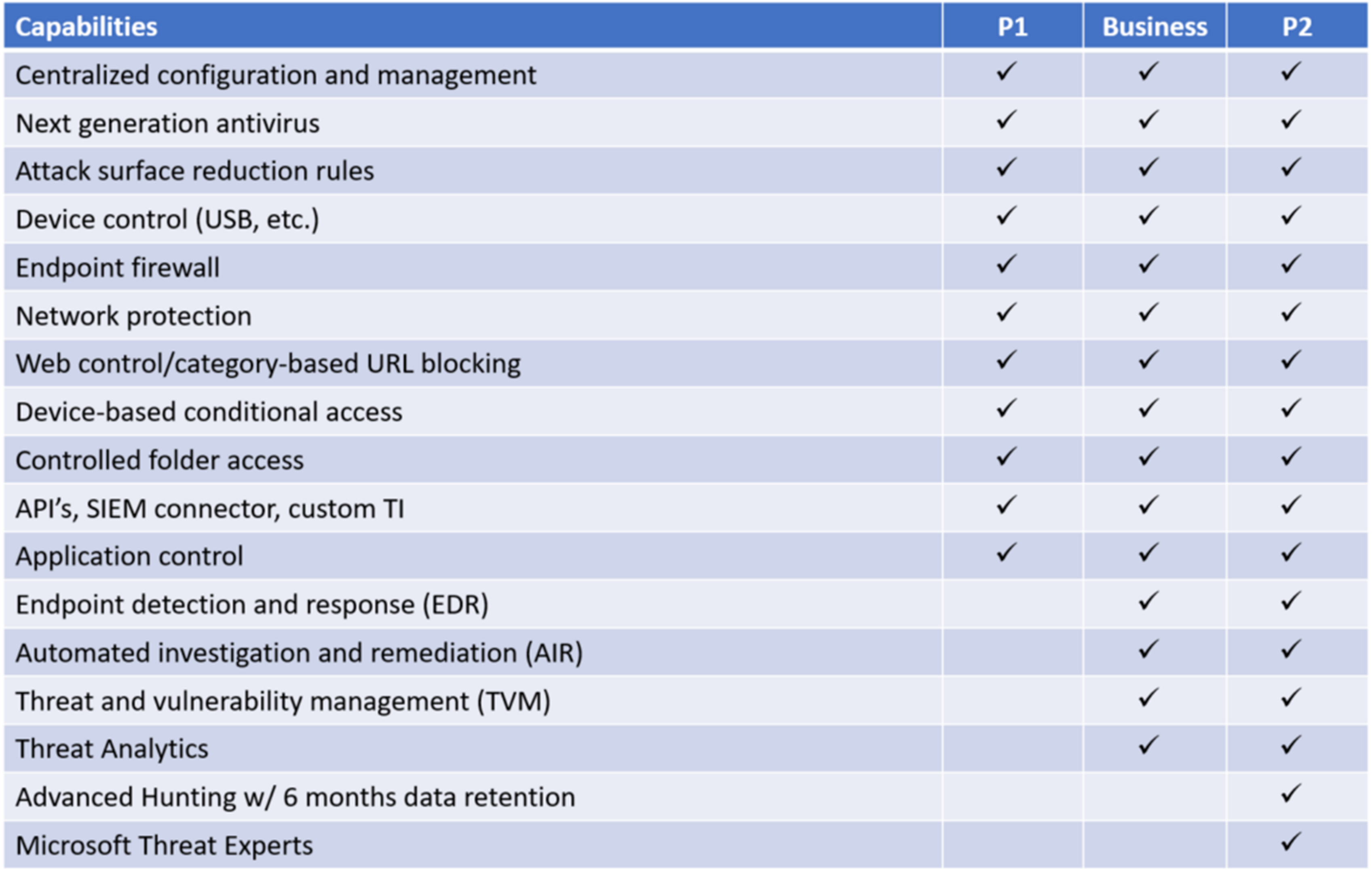
- Windows
- MacOS
- Linux
- iOS
- Android
- Windows 365
- Azure Virtual Desktop



Licensing Defender for Endpoint

Microsoft Defender
for Endpoint

- Defender for Endpoint P1
- Defender for Endpoint P2
- Defender for Business
- Defender for Server



Capabilities	P1	Business	P2
Centralized configuration and management	✓	✓	✓
Next generation antivirus	✓	✓	✓
Attack surface reduction rules	✓	✓	✓
Device control (USB, etc.)	✓	✓	✓
Endpoint firewall	✓	✓	✓
Network protection	✓	✓	✓
Web control/category-based URL blocking	✓	✓	✓
Device-based conditional access	✓	✓	✓
Controlled folder access	✓	✓	✓
API's, SIEM connector, custom TI	✓	✓	✓
Application control	✓	✓	✓
Endpoint detection and response (EDR)		✓	✓
Automated investigation and remediation (AIR)		✓	✓
Threat and vulnerability management (TVM)		✓	✓
Threat Analytics		✓	✓
Advanced Hunting w/ 6 months data retention			✓
Microsoft Threat Experts			✓

Integrazione Defender for Endpoint con Defender for Cloud Apps

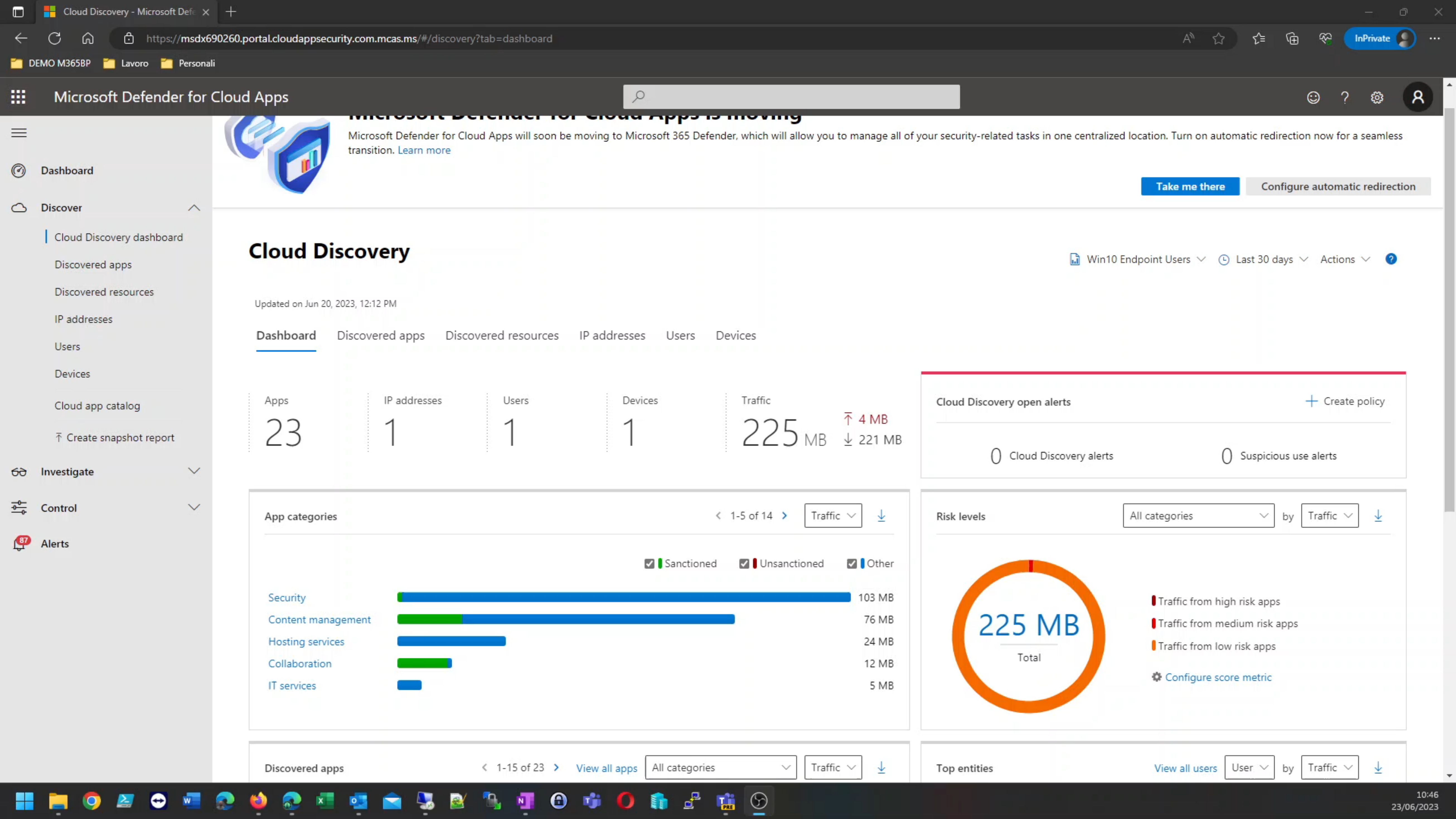
Cosa è Microsoft Defender for Cloud Apps ?

- **Visibilità**: rilevazione di tutti i servizi cloud; assegnazione a ognuno di una classificazione del rischio; identificazione di tutti gli utenti e di tutte le app di terze parti in grado di accedere all’ambiente

- **Sicurezza dei dati**: identificare e controllare le informazioni sensibili (DLP); rispondere alle etichette di riservatezza sul contenuto

- **Protezione dalle minacce**: funzioni di controllo di accesso adattivo, analisi del comportamento degli utenti e delle entità (User and Entity Behavior Analytics o UEBA); attenuazione degli effetti del malware

- **Conformità**: disponibilità di report e dashboard che illustrino la governance del cloud; assistenza nella realizzazione della conformità alle norme di residenza dei dati e ai requisiti normativi



Cloud Discovery - Microsoft Defe

https://msdx690260.portal.cloudappsecurity.com.mcas.ms/#/discovery?tab=dashboard

InPrivate

DEMO M365BP | Lavoro | Personali

Microsoft Defender for Cloud Apps

- Dashboard
- Discover
  - Cloud Discovery dashboard
  - Discovered apps
  - Discovered resources
  - IP addresses
  - Users
  - Devices
  - Cloud app catalog
  - Create snapshot report
- Investigate
- Control
- Alerts 87

Microsoft Defender for Cloud Apps is moving

Microsoft Defender for Cloud Apps will soon be moving to Microsoft 365 Defender, which will allow you to manage all of your security-related tasks in one centralized location. Turn on automatic redirection now for a seamless transition. Learn more

Take me there | Configure automatic redirection

Cloud Discovery

Win10 Endpoint Users | Last 30 days | Actions

Updated on Jun 20, 2023, 12:12 PM

Dashboard | Discovered apps | Discovered resources | IP addresses | Users | Devices

Apps	IP addresses	Users	Devices	Traffic
23	1	1	1	225 MB ↑ 4 MB ↓ 221 MB

Cloud Discovery open alerts — + Create policy

0 Cloud Discovery alerts

0 Suspicious use alerts

App categories — 1-5 of 14 — Traffic

☑ Sanctioned ☑ Unsanctioned ☑ Other

Category	Traffic
Security	103 MB
Content management	76 MB
Hosting services	24 MB
Collaboration	12 MB
IT services	5 MB

Risk levels — All categories by Traffic

225 MB

Total

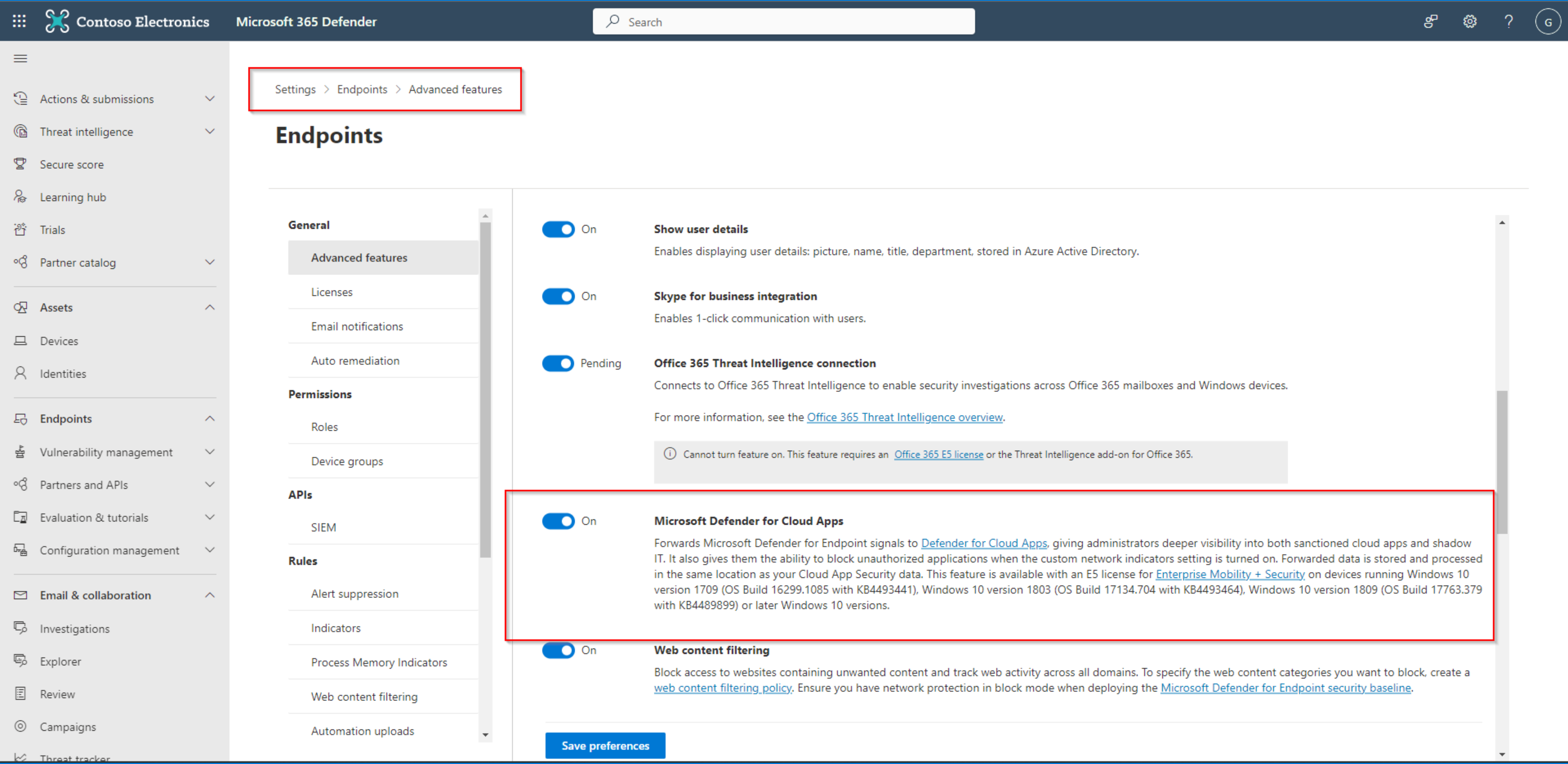
- Traffic from high risk apps
- Traffic from medium risk apps
- Traffic from low risk apps

Configure score metric

Discovered apps — 1-15 of 23 — View all apps — All categories — Traffic

Top entities — View all users — User by Traffic

10:46
23/06/2023



Settings > Endpoints > Advanced features

Endpoints

On **Show user details**

Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.

On **Skype for business integration**

Enables 1-click communication with users.

Pending **Office 365 Threat Intelligence connection**

Connects to Office 365 Threat Intelligence to enable security investigations across Office 365 mailboxes and Windows devices.

For more information, see the Office 365 Threat Intelligence overview.

ⓘ Cannot turn feature on. This feature requires an Office 365 E5 license or the Threat Intelligence add-on for Office 365.

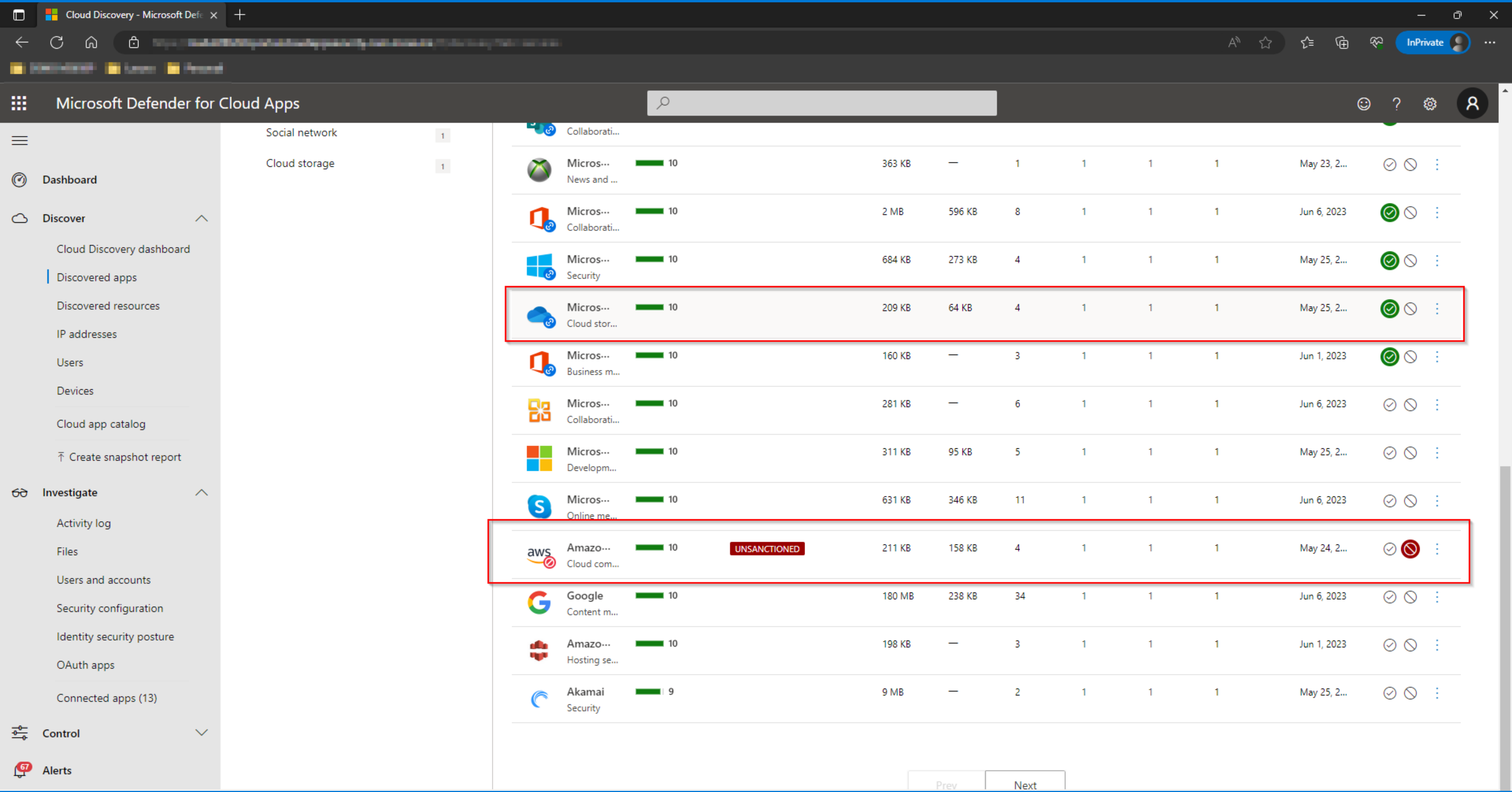
On **Microsoft Defender for Cloud Apps**

Forwards Microsoft Defender for Endpoint signals to Defender for Cloud Apps, giving administrators deeper visibility into both sanctioned cloud apps and shadow IT. It also gives them the ability to block unauthorized applications when the custom network indicators setting is turned on. Forwarded data is stored and processed in the same location as your Cloud App Security data. This feature is available with an E5 license for Enterprise Mobility + Security on devices running Windows 10 version 1709 (OS Build 16299.1085 with KB4493441), Windows 10 version 1803 (OS Build 17134.704 with KB4493464), Windows 10 version 1809 (OS Build 17763.379 with KB4489899) or later Windows 10 versions.

On **Web content filtering**

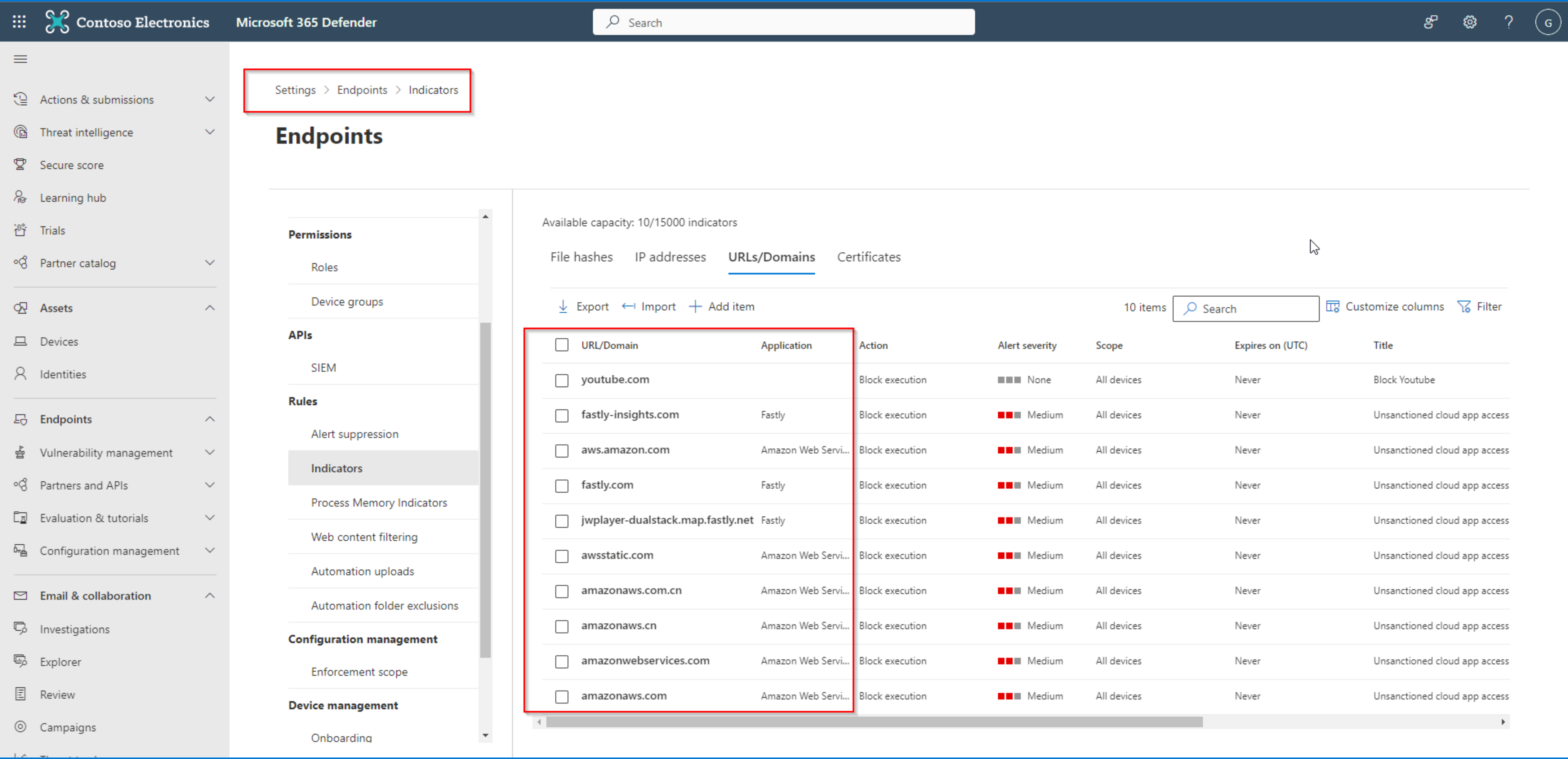
Block access to websites containing unwanted content and track web activity across all domains. To specify the web content categories you want to block, create a web content filtering policy. Ensure you have network protection in block mode when deploying the Microsoft Defender for Endpoint security baseline.

Save preferences



Social network	1								
Cloud storage	1								

Collaborati...									
Micros... News and ...	10		363 KB	—	1	1	1	1	May 23, 2...
Micros... Collaborati...	10		2 MB	596 KB	8	1	1	1	Jun 6, 2023
Micros... Security	10		684 KB	273 KB	4	1	1	1	May 25, 2...
Micros... Cloud stor...	10		209 KB	64 KB	4	1	1	1	May 25, 2...
Micros... Business m...	10		160 KB	—	3	1	1	1	Jun 1, 2023
Micros... Collaborati...	10		281 KB	—	6	1	1	1	Jun 6, 2023
Micros... Developm...	10		311 KB	95 KB	5	1	1	1	May 25, 2...
Micros... Online me...	10		631 KB	346 KB	11	1	1	1	Jun 6, 2023
Amazo... Cloud com...	10	UNSANCTIONED	211 KB	158 KB	4	1	1	1	May 24, 2...
Google Content m...	10		180 MB	238 KB	34	1	1	1	Jun 6, 2023
Amazo... Hosting se...	10		198 KB	—	3	1	1	1	Jun 1, 2023
Akamai Security	9		9 MB	—	2	1	1	1	May 25, 2...



Settings > Endpoints > Indicators

Endpoints

Available capacity: 10/15000 indicators

10 items

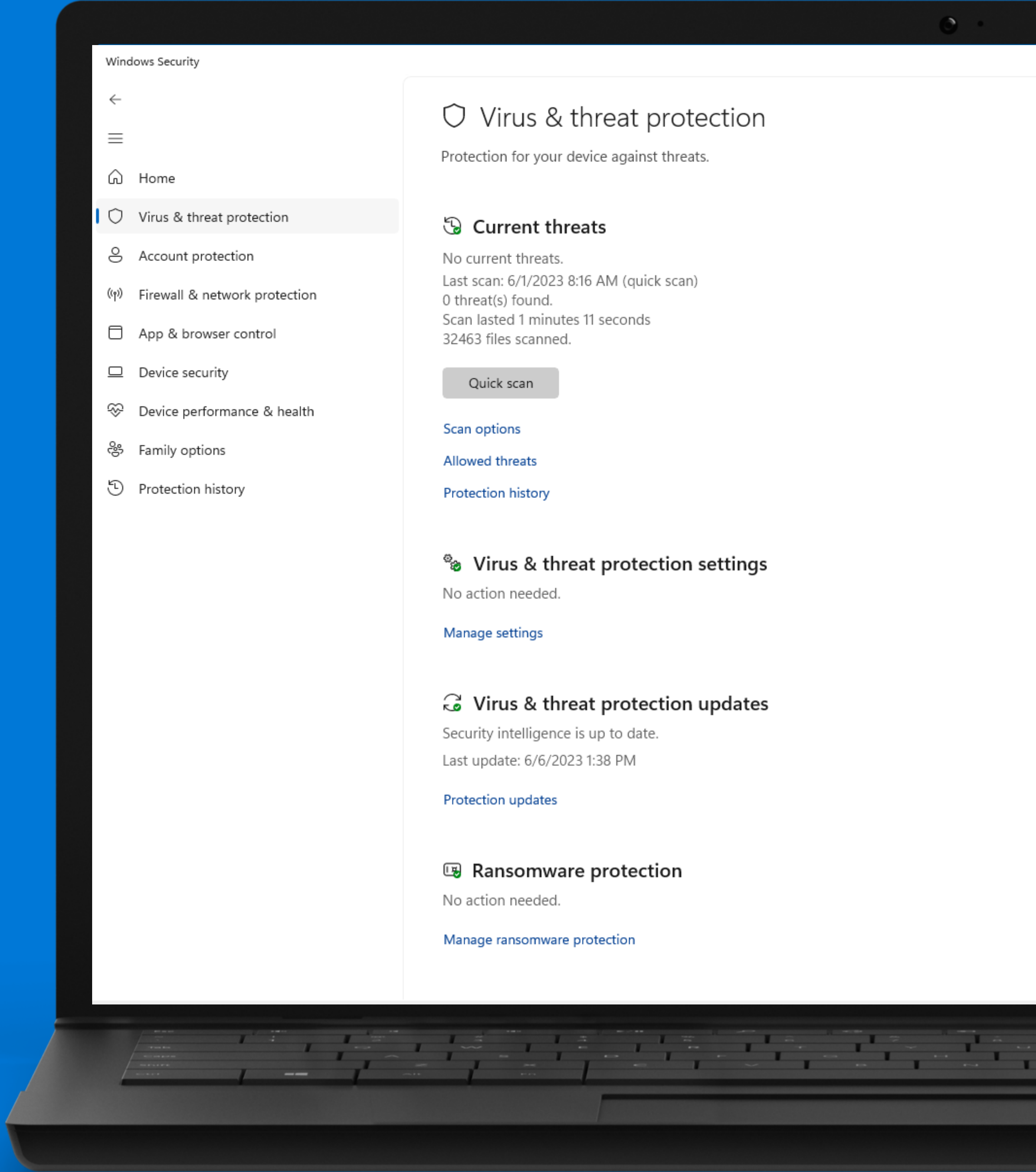
	URL/Domain	Application	Action	Alert severity	Scope	Expires on (UTC)	Title
□	youtube.com		Block execution	■■■ None	All devices	Never	Block Youtube
□	fastly-insights.com	Fastly	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	aws.amazon.com	Amazon Web Servi...	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	fastly.com	Fastly	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	jwplayer-dualstack.map.fastly.net	Fastly	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	awsstatic.com	Amazon Web Servi...	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	amazonaws.com.cn	Amazon Web Servi...	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	amazonaws.cn	Amazon Web Servi...	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	amazonwebservices.com	Amazon Web Servi...	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access
□	amazonaws.com	Amazon Web Servi...	Block execution	■■■ Medium	All devices	Never	Unsanctioned cloud app access

Funziona con tutti i Browser ?

- Microsoft Edge (Smartscreen)
- Altri Browser di Terze Parti (Network Protection in Block Mode)

DEMO

Defender for Endpoint



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 6/1/2023 8:16 AM (quick scan)
0 threat(s) found.
Scan lasted 1 minutes 11 seconds
32463 files scanned.

Virus & threat protection settings

No action needed.

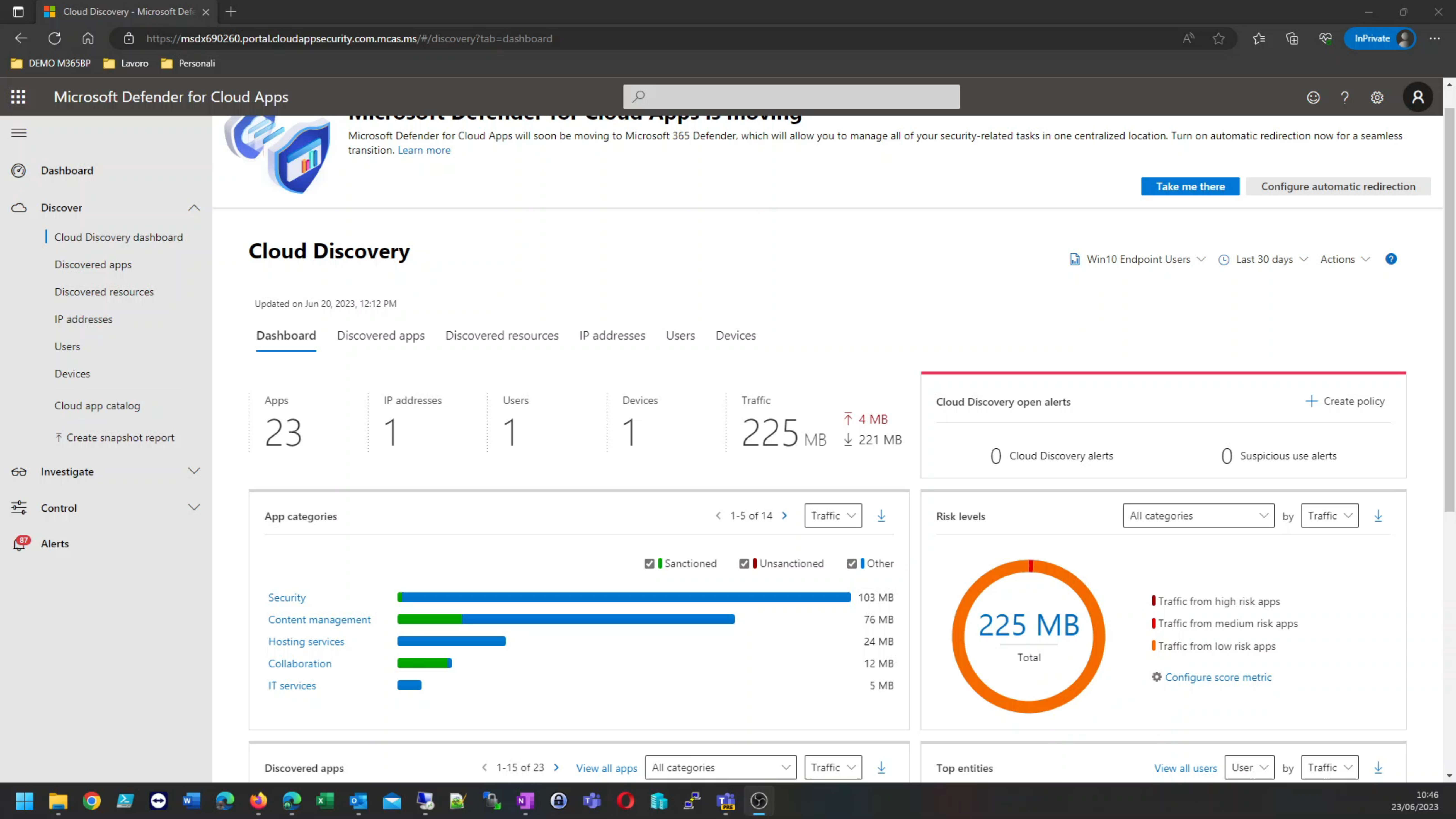
Virus & threat protection updates

Security intelligence is up to date.

Last update: 6/6/2023 1:38 PM

Ransomware protection

No action needed.


Cloud Discovery - Microsoft Defe
https://msdx690260.portal.cloudappsecurity.com.mcas.ms/#/discovery?tab=dashboard
InPrivate
DEMO M365BP
Lavoro
Personali
Microsoft Defender for Cloud Apps
Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Devices
Cloud app catalog
Create snapshot report
Investigate
Control
87
Alerts

Microsoft Defender for Cloud Apps is moving

Microsoft Defender for Cloud Apps will soon be moving to Microsoft 365 Defender, which will allow you to manage all of your security-related tasks in one centralized location. Turn on automatic redirection now for a seamless transition. Learn more

Take me there
Configure automatic redirection

Cloud Discovery

Win10 Endpoint Users · Last 30 days · Actions

Updated on Jun 20, 2023, 12:12 PM

Apps	IP addresses	Users	Devices	Traffic
23	1	1	1	225 MB ↑ 4 MB ↓ 221 MB

Cloud Discovery open alerts

0 Cloud Discovery alerts

0 Suspicious use alerts

App categories

1-5 of 14 · Traffic

☑ Sanctioned ☑ Unsanctioned ☑ Other

Security	103 MB
Content management	76 MB
Hosting services	24 MB
Collaboration	12 MB
IT services	5 MB

Risk levels

All categories by Traffic

225 MB
Total
Traffic from high risk apps
Traffic from medium risk apps
Traffic from low risk apps
Configure score metric

Discovered apps

1-15 of 23 · View all apps · All categories · Traffic

Top entities

View all users · User by Traffic

ICT POWER.IT

Microsoft

Grazie

Guido Imperatore

Microsoft Solution Specialist @ Project Informatica - WeAreProject

Guido.imperatore@project.it

/guido.imperatore

@GuidoImpe

guidoimpera
tore