RESOLVE

by ErgonGroup

WEBINAR

CYBER SECURITY

L'infrastruttura informatica per monitorare e salvaguardare i dati

MER 20.10 | 16:00 – 17:00

RESOL/E

/ CHI SONO

SPEAKER

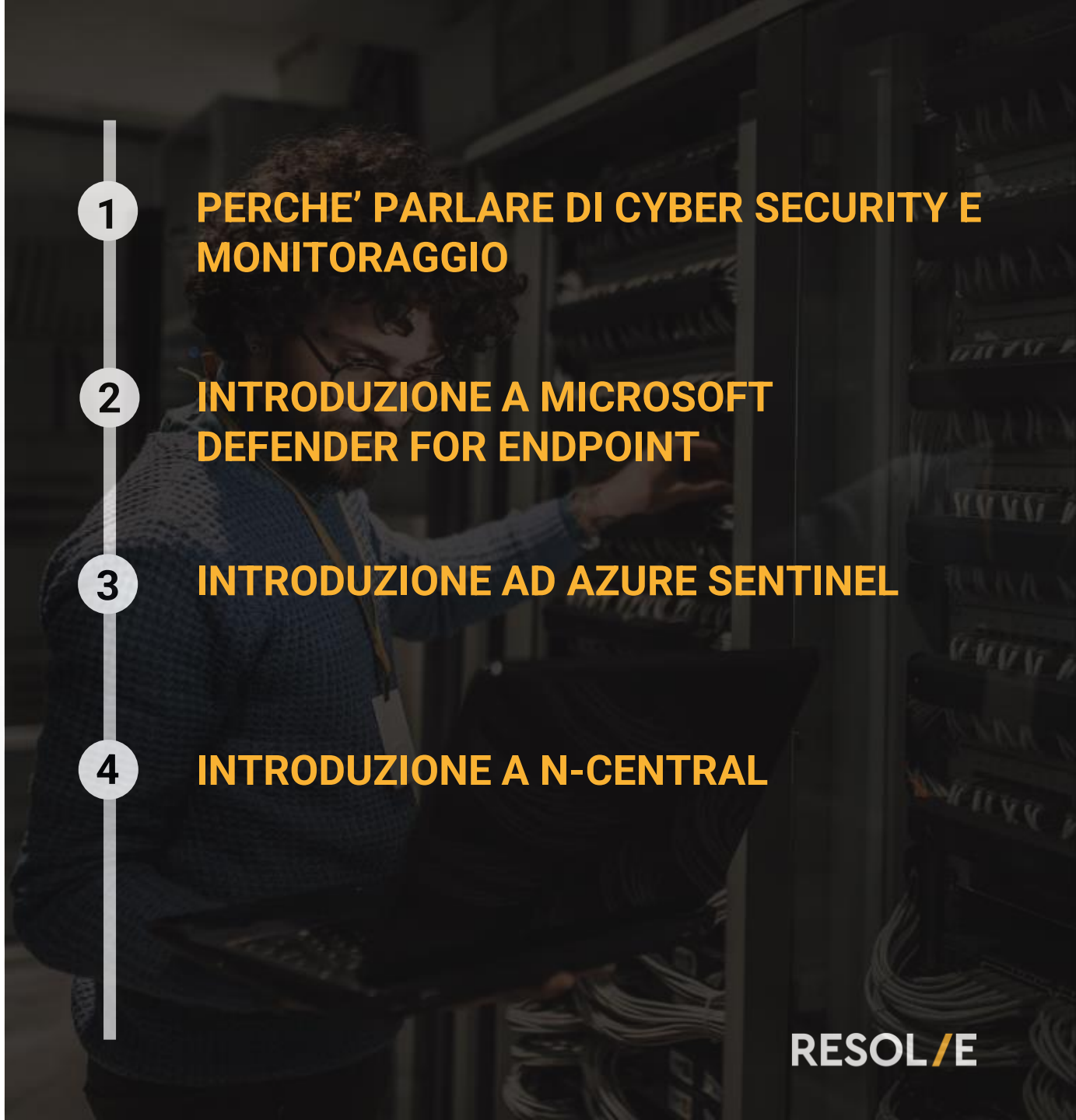
EMANUEL MARCON

System Architect @Resolve Digital - walk2talk

Ha fatto della sua passione il suo lavoro. Emanuel opera da anni all'interno del settore IT, affiancando le aziende con **percorsi di consulenza strategica** volti ad introdurre innovazione e sviluppo. Infatti, è costantemente alla ricerca di nuove tecnologie per dare modo alle aziende di crescere con cognizione di causa utilizzando le tecnologie più performanti a disposizione sul mercato. È proprio per questo motivo che, con passione, supporta le aziende con configurazioni tailor-made ideate in base alle loro esigenze specifiche.

RESOL/E

/ AGENDA



1. PERCHE’ PARLARE DI CYBER SECURITY E MONITORAGGIO
2. INTRODUZIONE A MICROSOFT DEFENDER FOR ENDPOINT
3. INTRODUZIONE AD AZURE SENTINEL
4. INTRODUZIONE A N-CENTRAL

RESOL/E

01. CYBER SECURITY

Cos’è oggi la Cyber Security

La Cyber security è l’insieme degli strumenti, delle competenze e dei comportamenti che permettono a un’organizzazione di «avere una barriera» tra il mondo esterno ed i propri dati in formato digitale.

Vista la progressiva digitalizzazione dei processi, la Cyber security serve a preservare l’intero ecosistema aziendale che sempre più è formato da uno scenario ibrido.

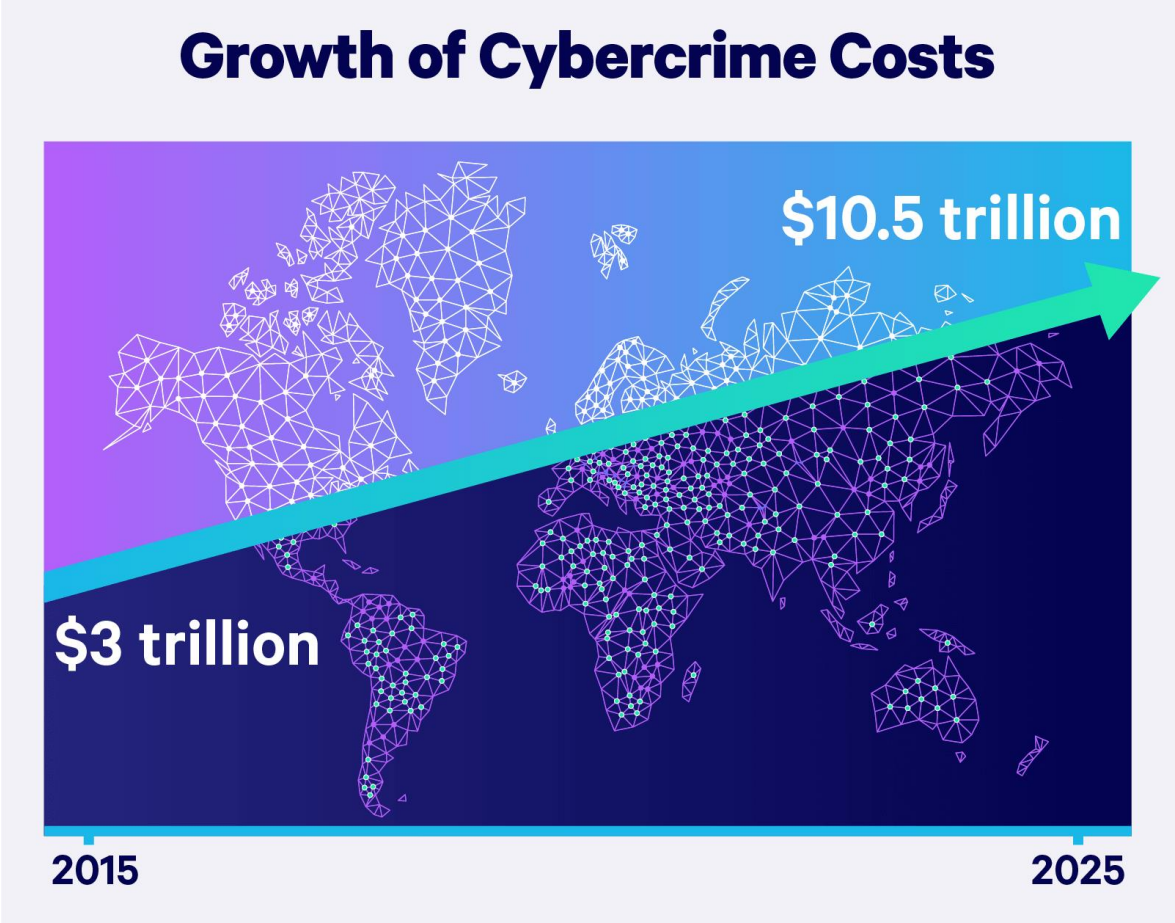
RESOLVE

01. CYBER SECURITY

Perché oggi la Cyber Security è Importante?

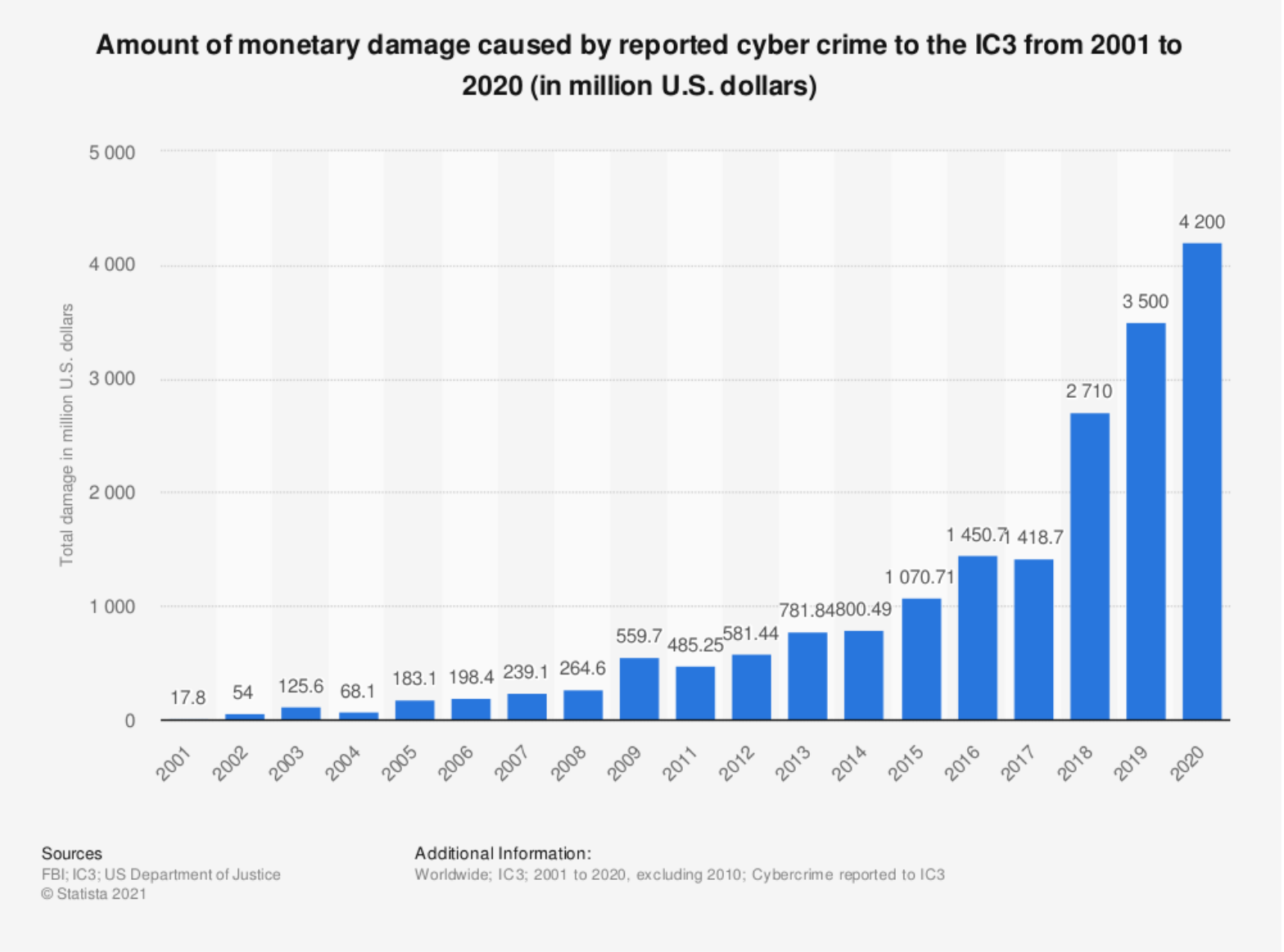
/ Perché la cybersecurity è importante?

- C'è un attacco hacker ogni 39 secondi
- Il 43% degli attacchi informatici prende di mira le piccole imprese
- Il 95% delle violazioni della sicurezza informatica sono dovute a errori umani
- Il 98% degli attacchi informatici si basa sull'ingegneria sociale



RESOL/E

/ Perché la cybersecurity è importante?



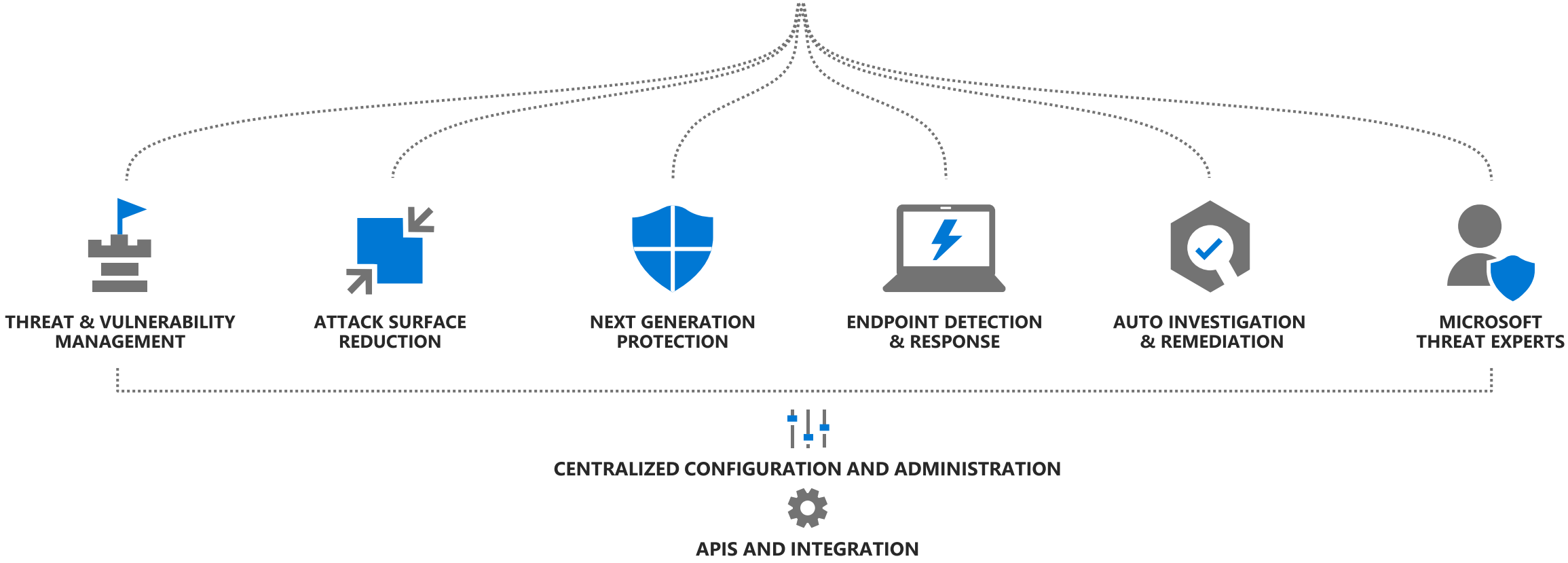
RESOL/E

02. MICROSOFT DEFENDER FOR ENDPOINT

Proteggere i clients con una soluzione moderna

Microsoft Defender
for Endpoint

Threats are no match.



RESOLVE

/ Microsoft Defender for Endpoint

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

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

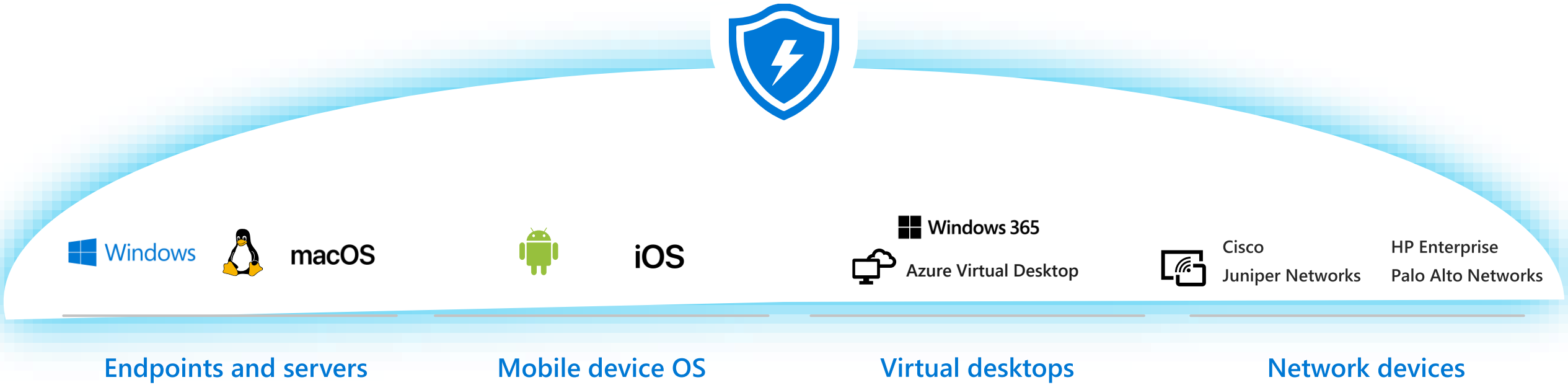
Our antimalware capabilities consistently achieve high scores in independent tests.

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

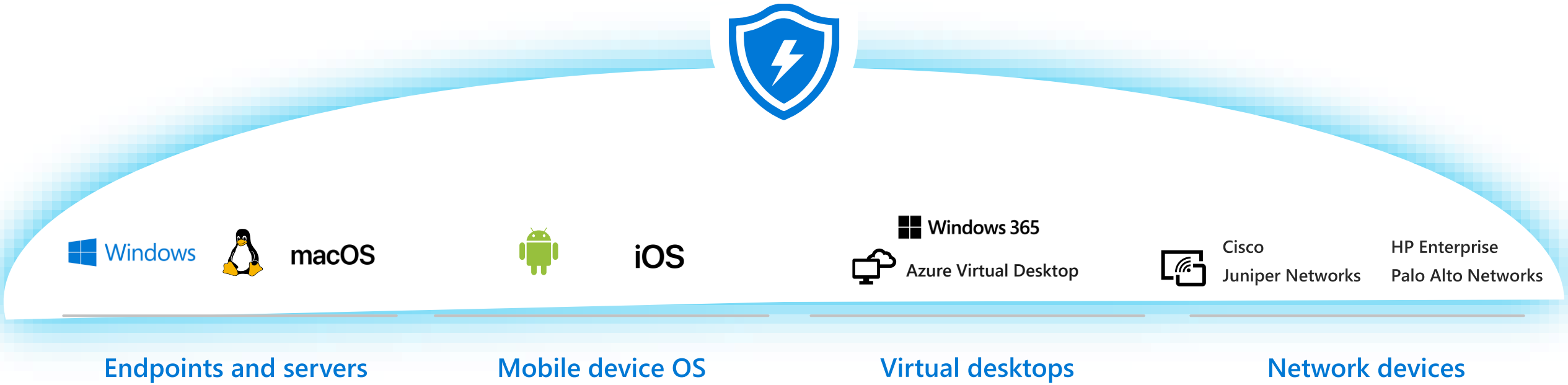
RESOL/E

/ Microsoft Defender for Endpoint



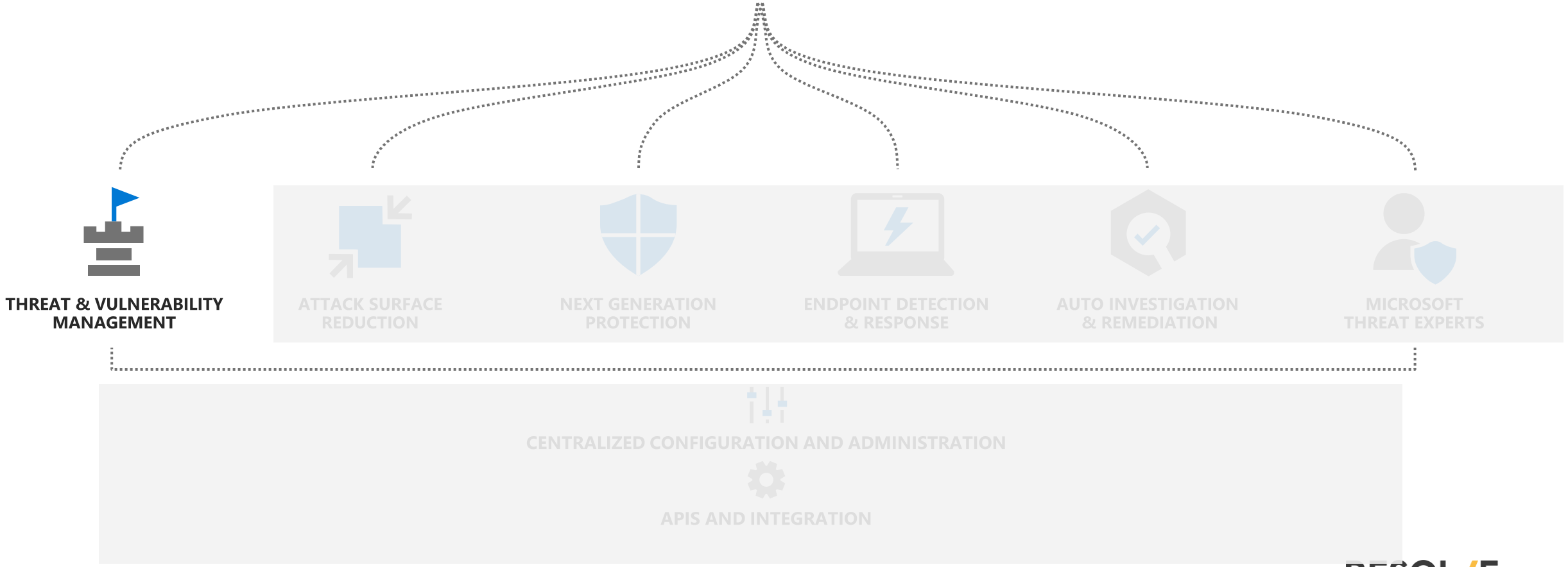
RESOL/E

/ Microsoft Defender for Endpoint



RESOL/E

Microsoft Defender
for Endpoint



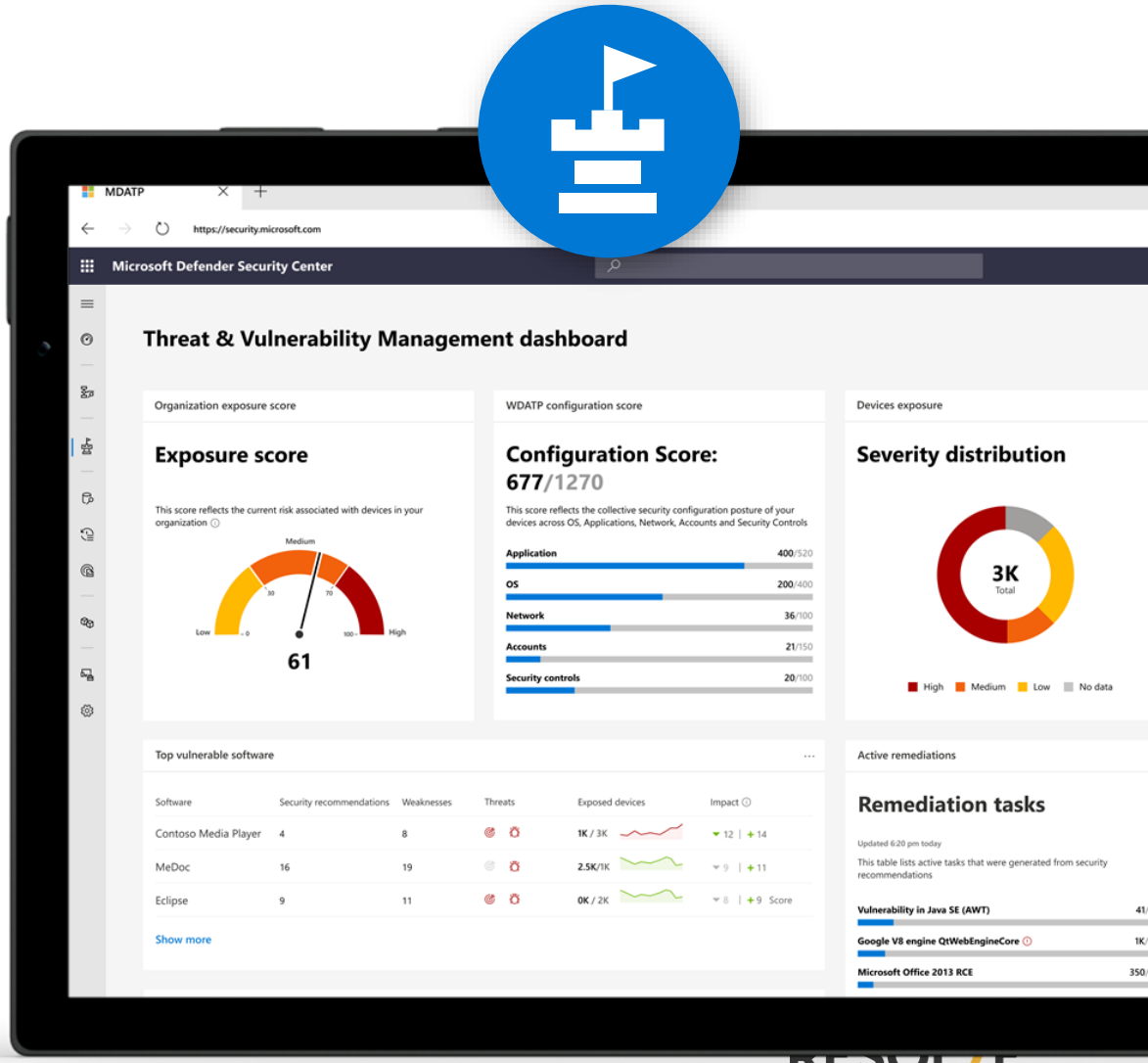
RESOL/E

/ Microsoft Defender for Endpoint

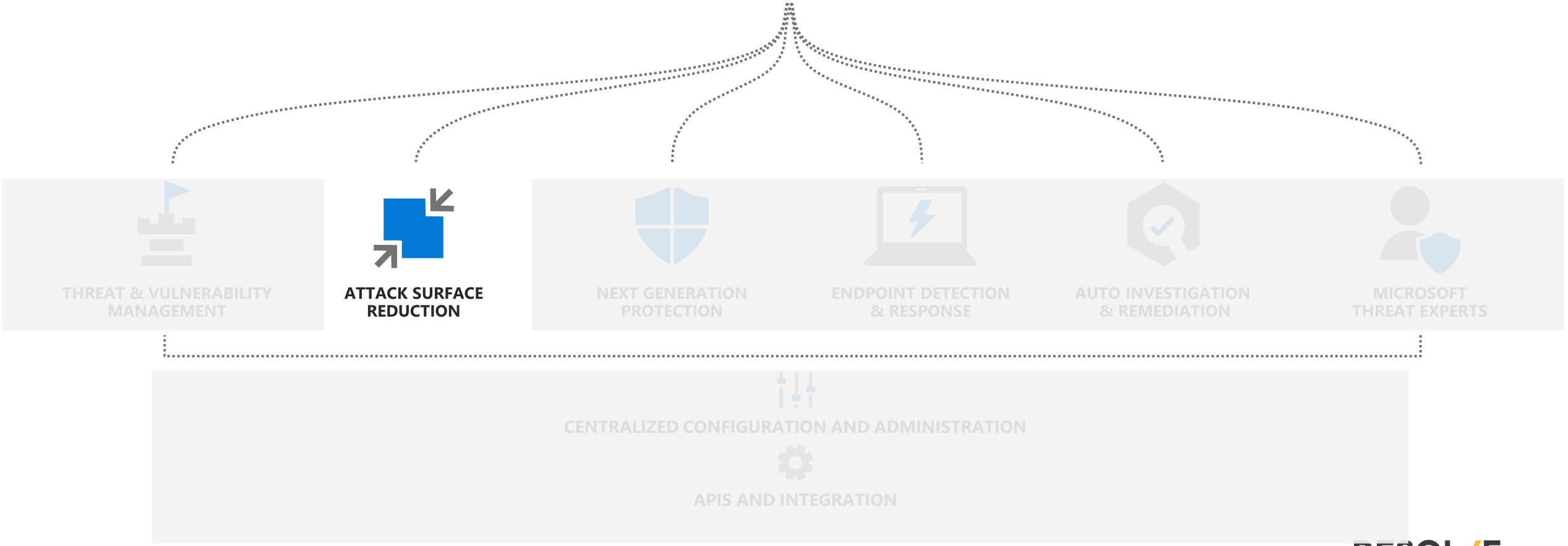
Threat & Vulnerability Management

Un approccio risk-based per migliorare la gestione delle vulnerabilità

1. Continuous real-time discovery
2. Context-aware prioritization
3. Built-in end-to-end remediation process



Microsoft Defender
for Endpoint

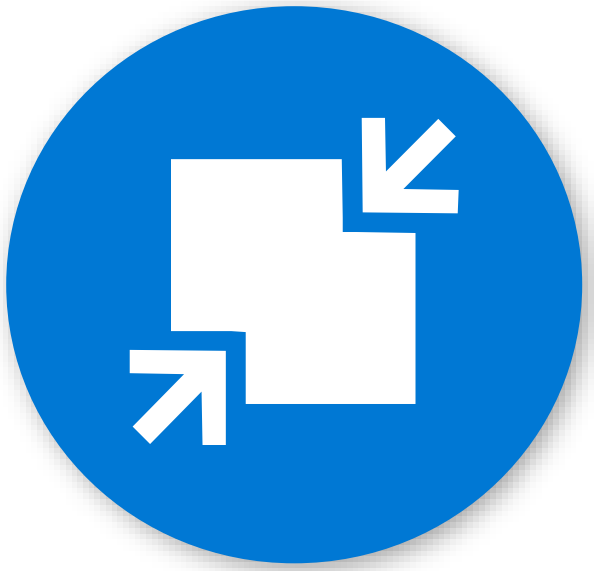


RESOL/E

/ Microsoft Defender for Endpoint

Attack Surface Reduction

Resist attacks and exploitations



HW based isolation

Application control

Exploit protection

Network protection

Controlled folder access

Device control

Web protection

Ransomware protection

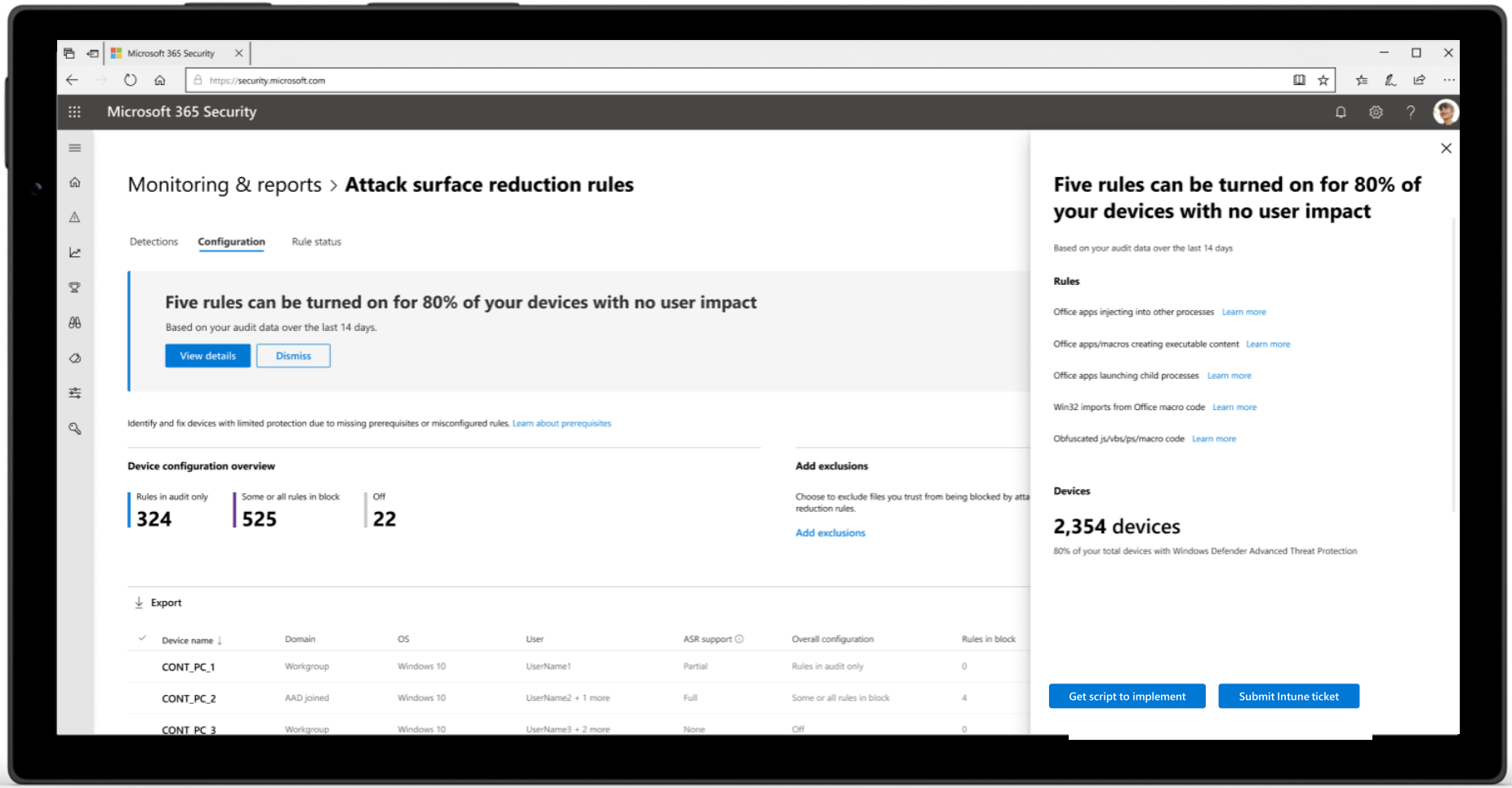
- Isolate access to untrusted sites
- Isolate access to untrusted Office files
- Host intrusion prevention
- Exploit mitigation
- Ransomware protection for your files
- Block traffic to low reputation destinations
- Protect your legacy applications
- Only allow trusted applications to run

RESOL/E

/ Microsoft Defender for Endpoint

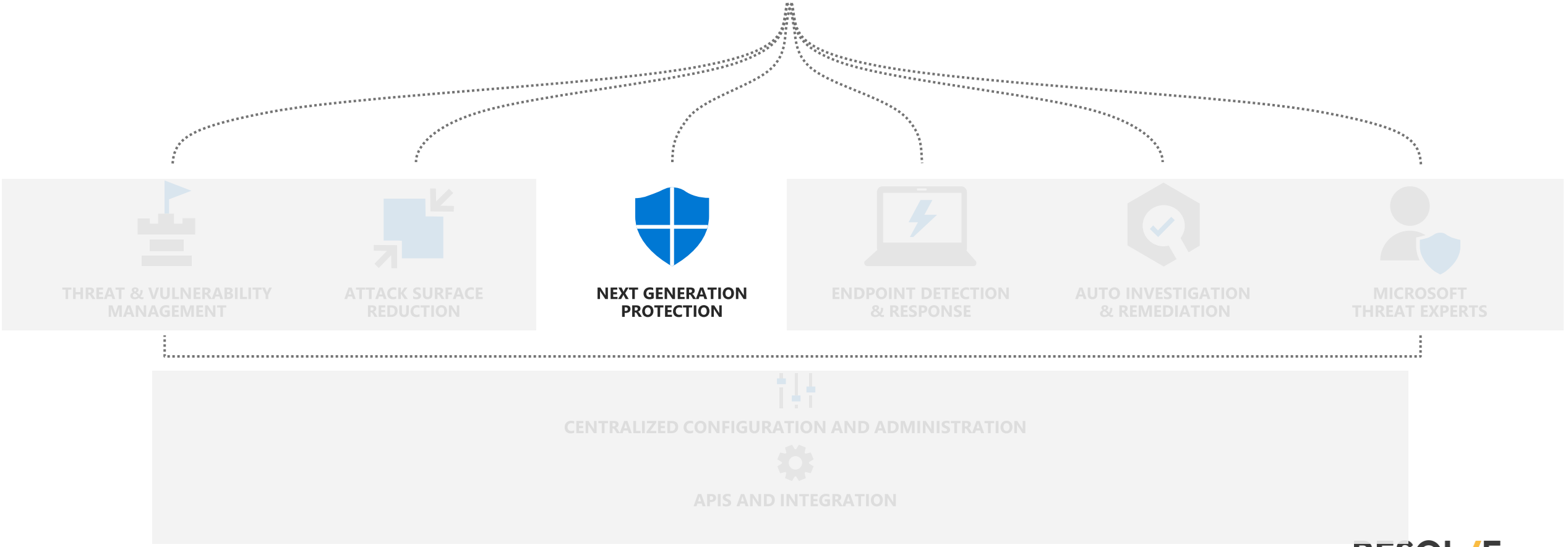
Attack Surface Reduction

Easy button:
turn on block



RESOL/E

Microsoft Defender
for Endpoint



RESOL/E

/ Microsoft Defender for Endpoint

Static vs Dynamic

Static signatures: focus on a file

Hashes

Strings

Emulators

Ineffective

Dynamic heuristics: focus on *run-time behaviors*

Behavior monitoring

Memory scanning

AMSI

Command-line scanning

Effective

RESOL/E

/ Microsoft Defender for Endpoint

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

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

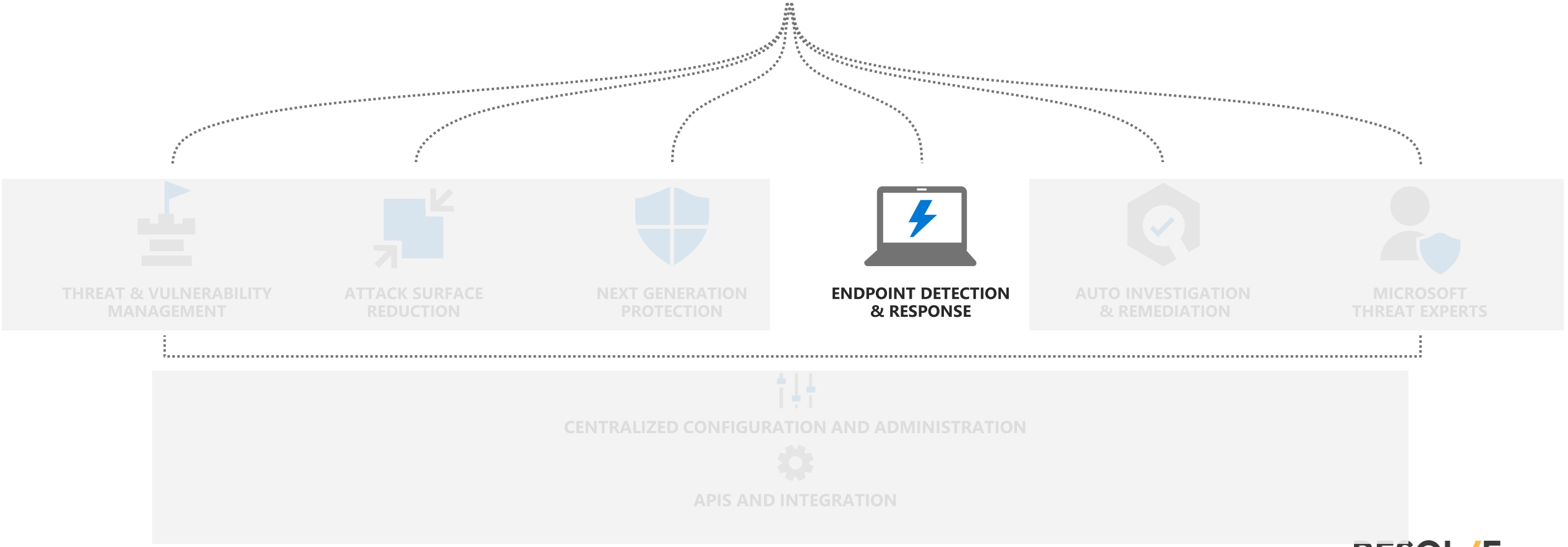
Heuristics
Catches malware variants or new strains with similar characteristics

Emulation
Evaluates files based on how they would behave when run

Network monitoring
Catches malicious network activities

RESOL/E

Microsoft Defender
for Endpoint

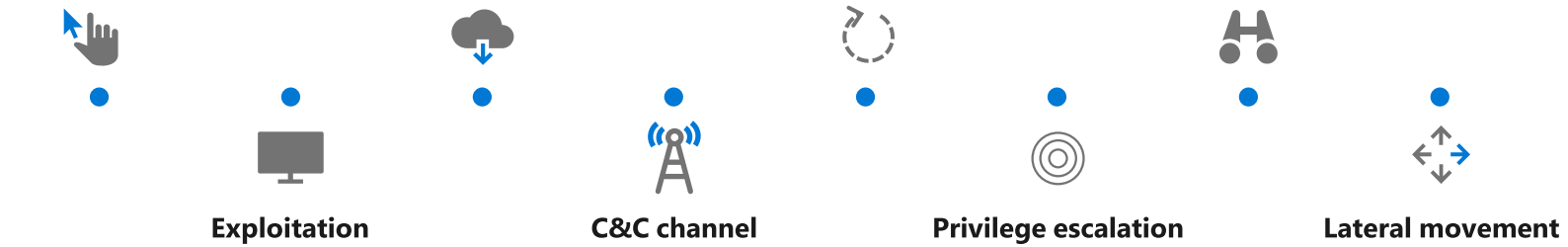


RESOLVE

/ Microsoft Defender for Endpoint

Key customer pain points

As attacks become more complex and multi-staged, it's difficult to make sense of the threats detected



46% of compromised systems had no malware on them

Following an advanced attack across the network and different sensors can be challenging

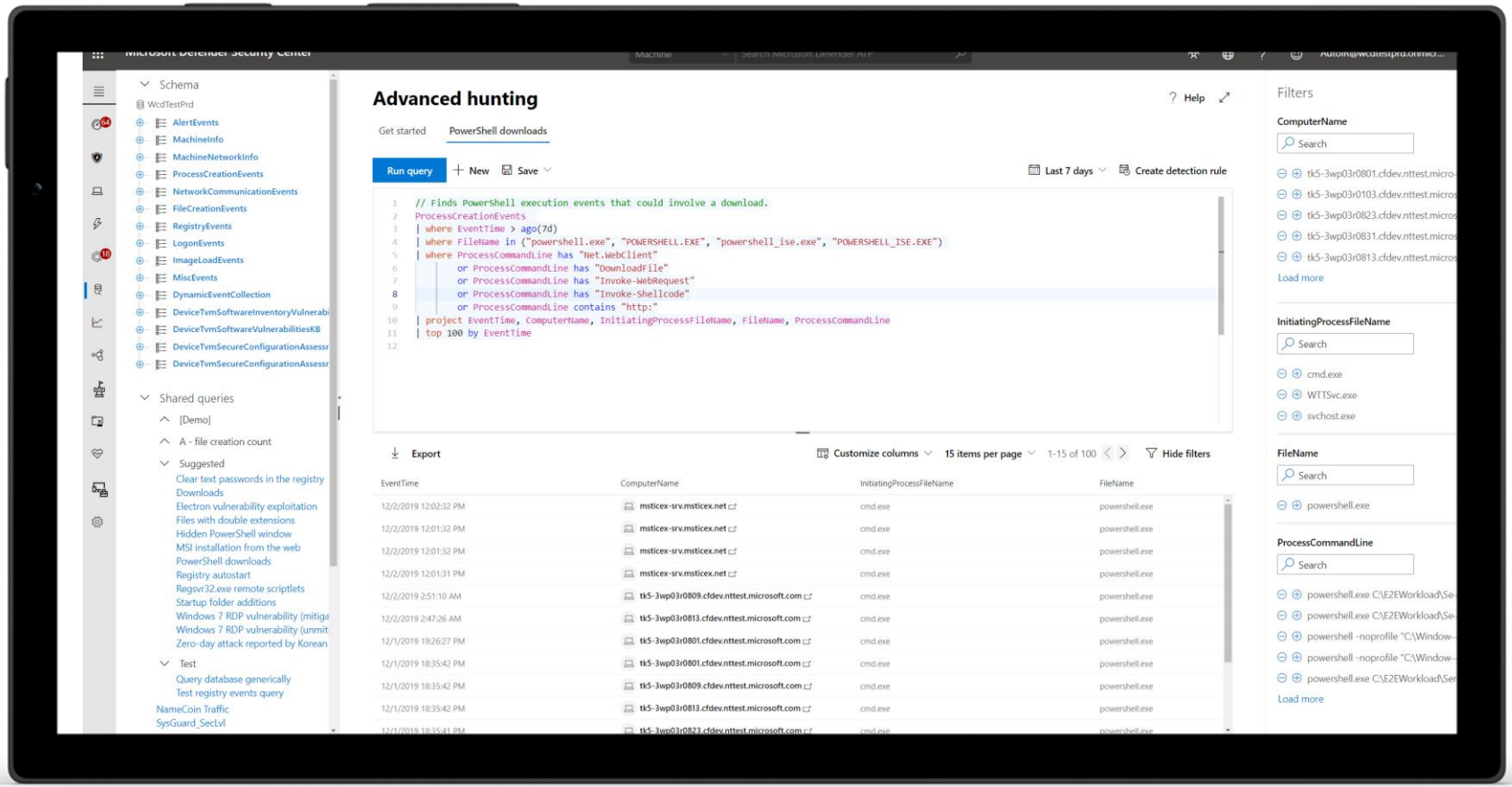
Collecting evidence and alerts, even from 1 infected device, can be a long time-consuming process

Living off the land - Attackers use evasion-techniques

RESOL/E

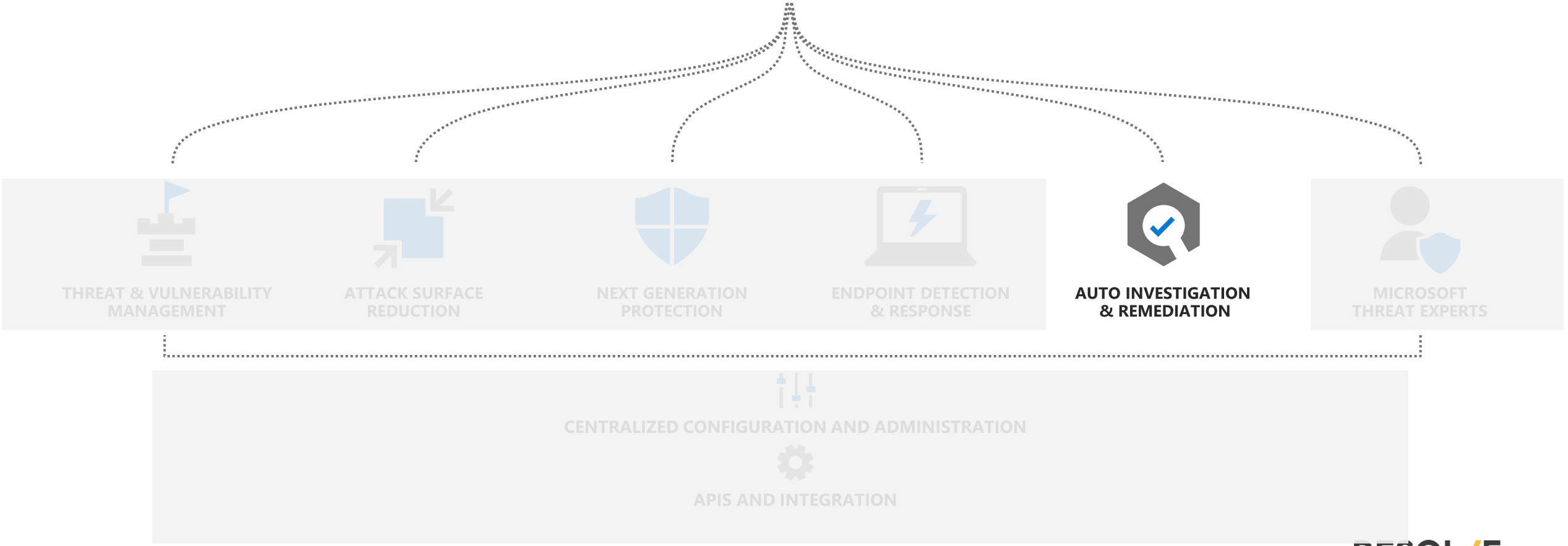
/ Microsoft Defender for Endpoint

Advanced hunting with custom detection and custom response



RESOLVE

Microsoft Defender
for Endpoint

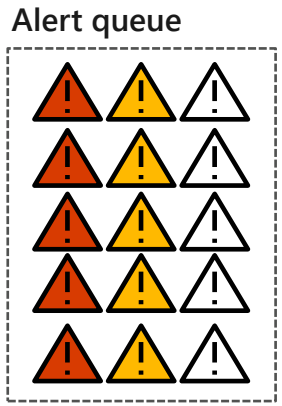


RESOL/E

/ Microsoft Defender for Endpoint

- More threats, more alerts leads to analyst fatigue
- Alert investigation is time-consuming
- Expertise is expensive
- Manual remediation requires time
- Talent shortage in cybersecurity

Gli Analisti normalmente sono impegnati dall'indagine e dalla risoluzione degli avvisi manuali

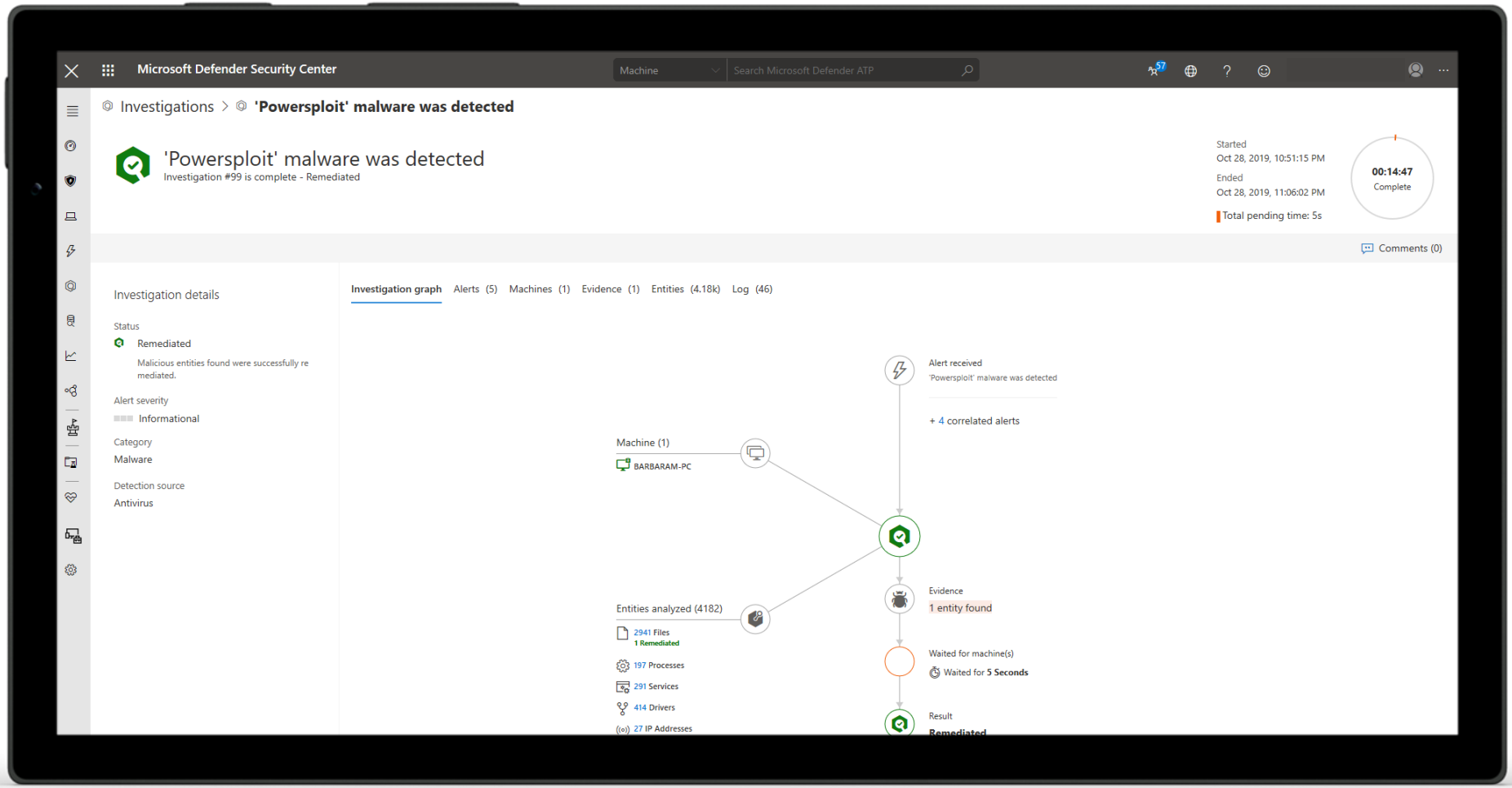



Analyst 1


Analyst 2

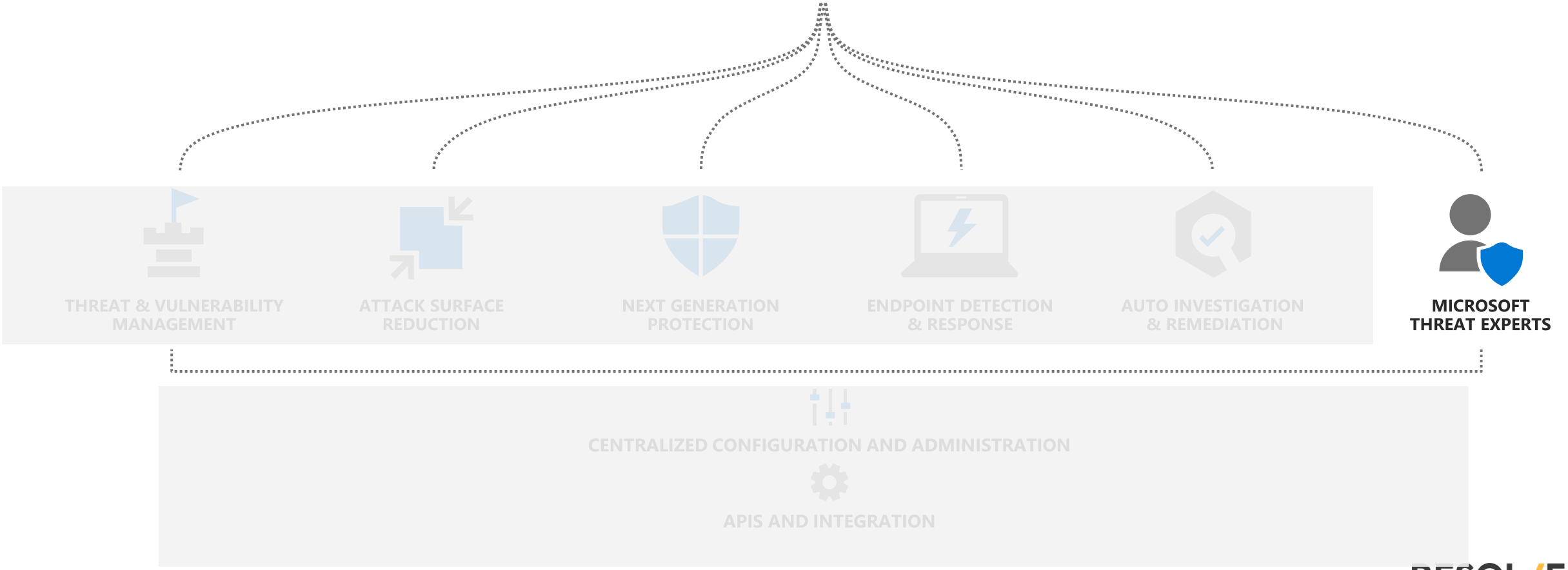
RESOL/E

/ Microsoft Defender for Endpoint



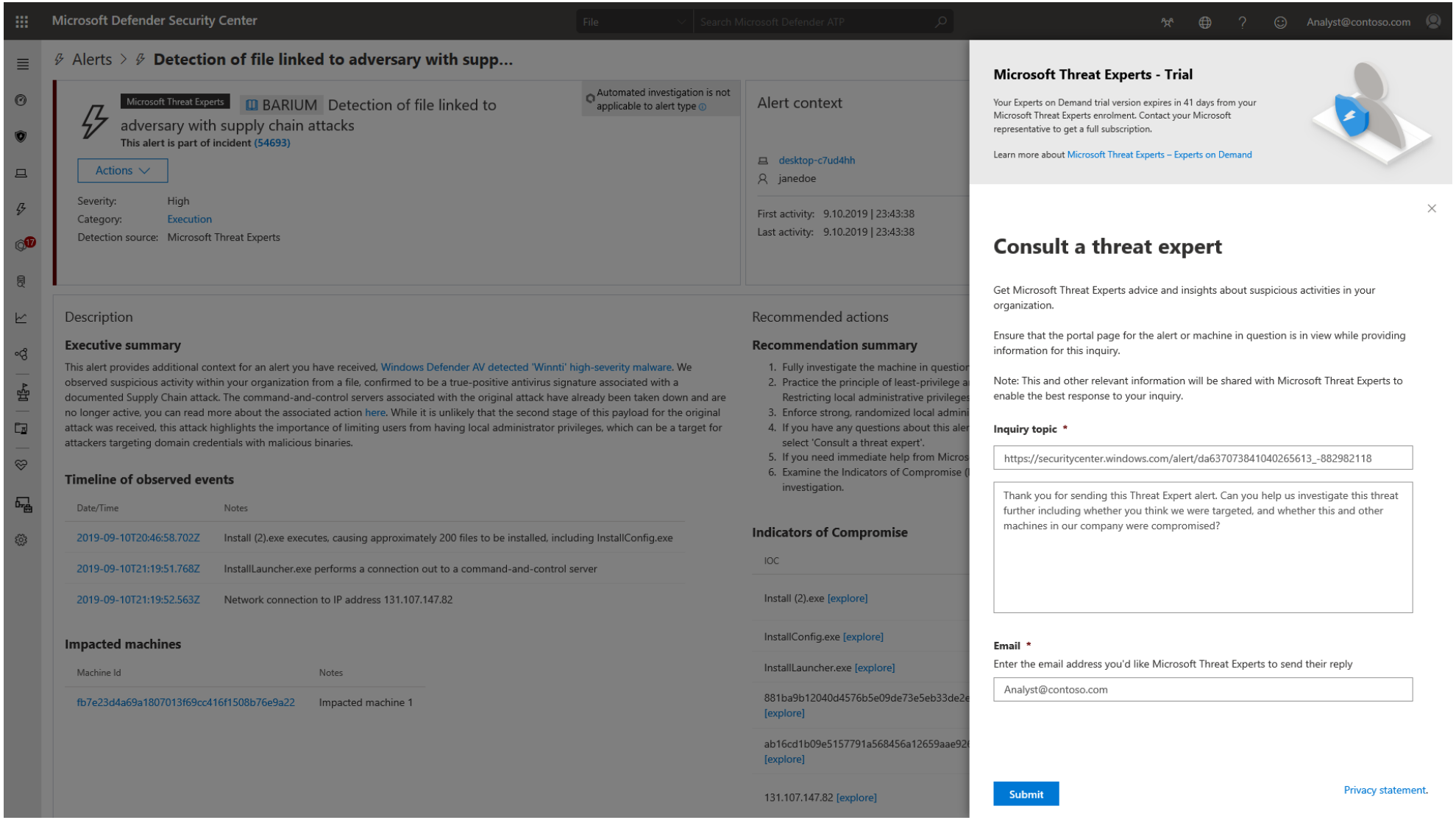
RESOLVE

Microsoft Defender
for Endpoint



RESOL/E

/ Microsoft Defender for Endpoint



RESOL/E

03. AZURE SENTINEL

Modernizzare le operazioni di sicurezza con Azure Sentinel

Azure Sentinel

Multi-cloud

SIEM

Cloud native, any data, any entity

Partnerships

Cloud native

Any data

AI

Automation

RESOLVE

Modernizzare il SOC con Azure Sentinel

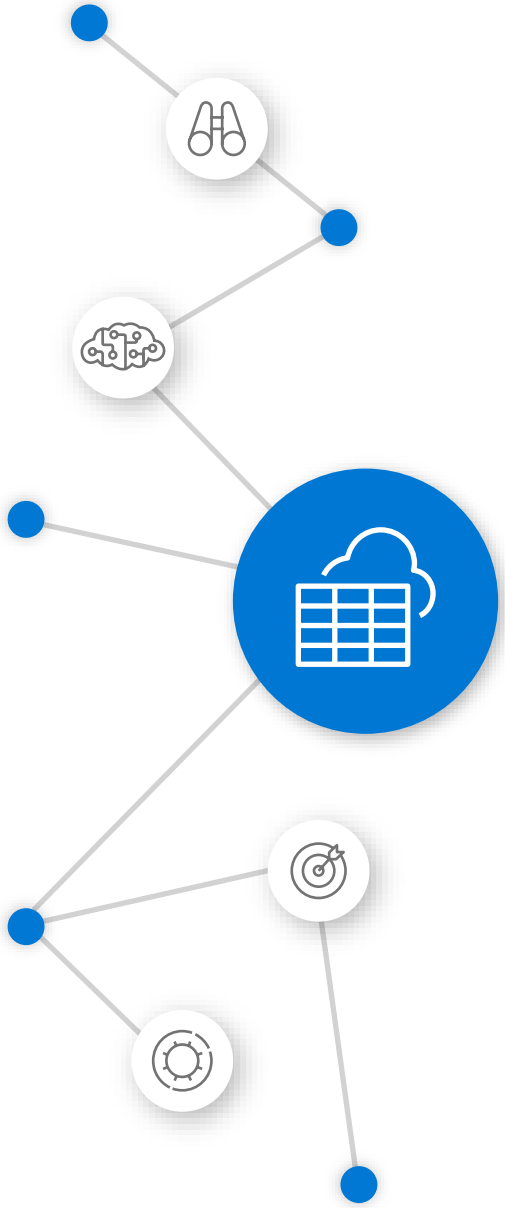
THE INTELLIGENT, CLOUD-NATIVE SIEM

Scales to support your growing digital estate

Offers improved threat detection

Uses AI and automation to increase efficiency

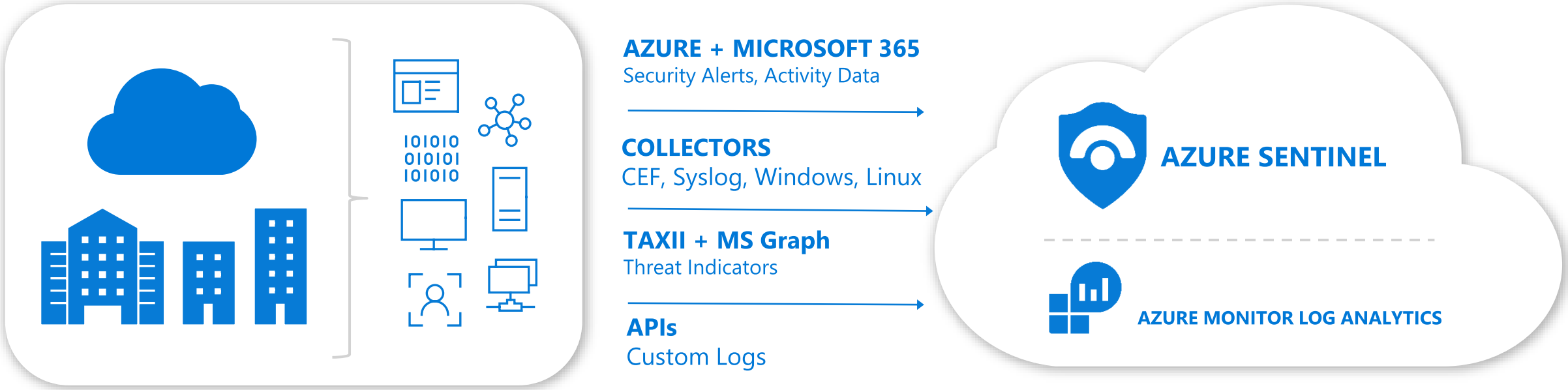
RESOL/E

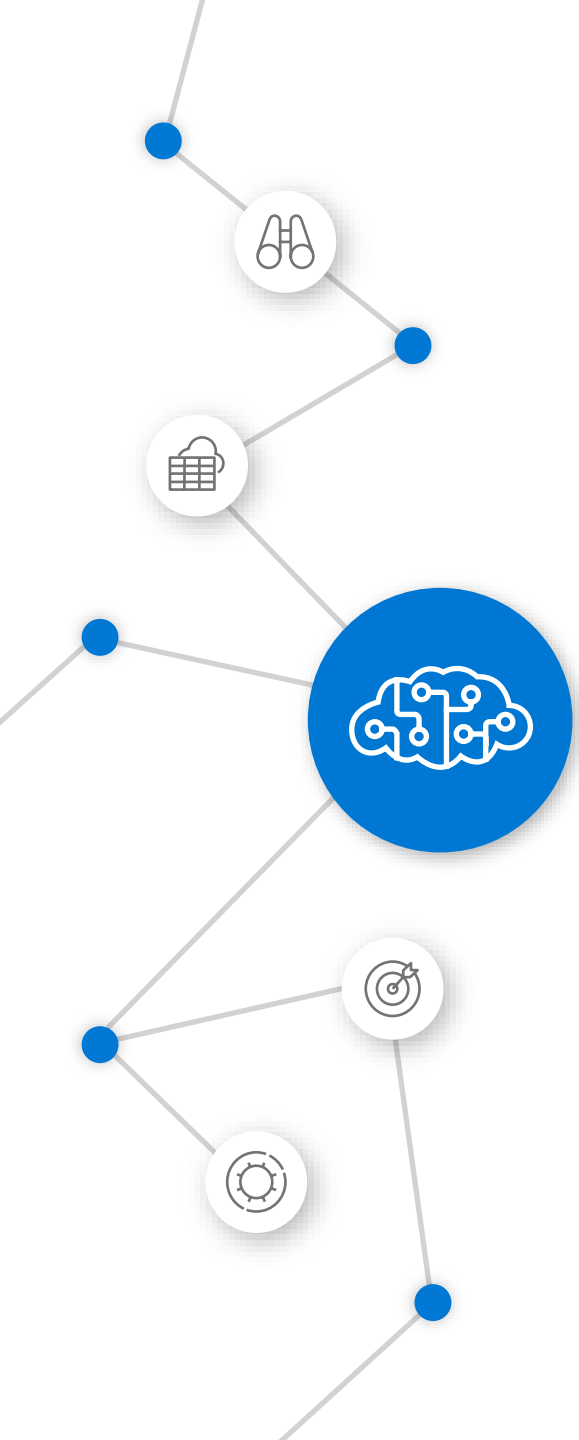


Visibilità

RESOLVE

Raccogli i dati nel cloud da qualsiasi fonte





Analytics

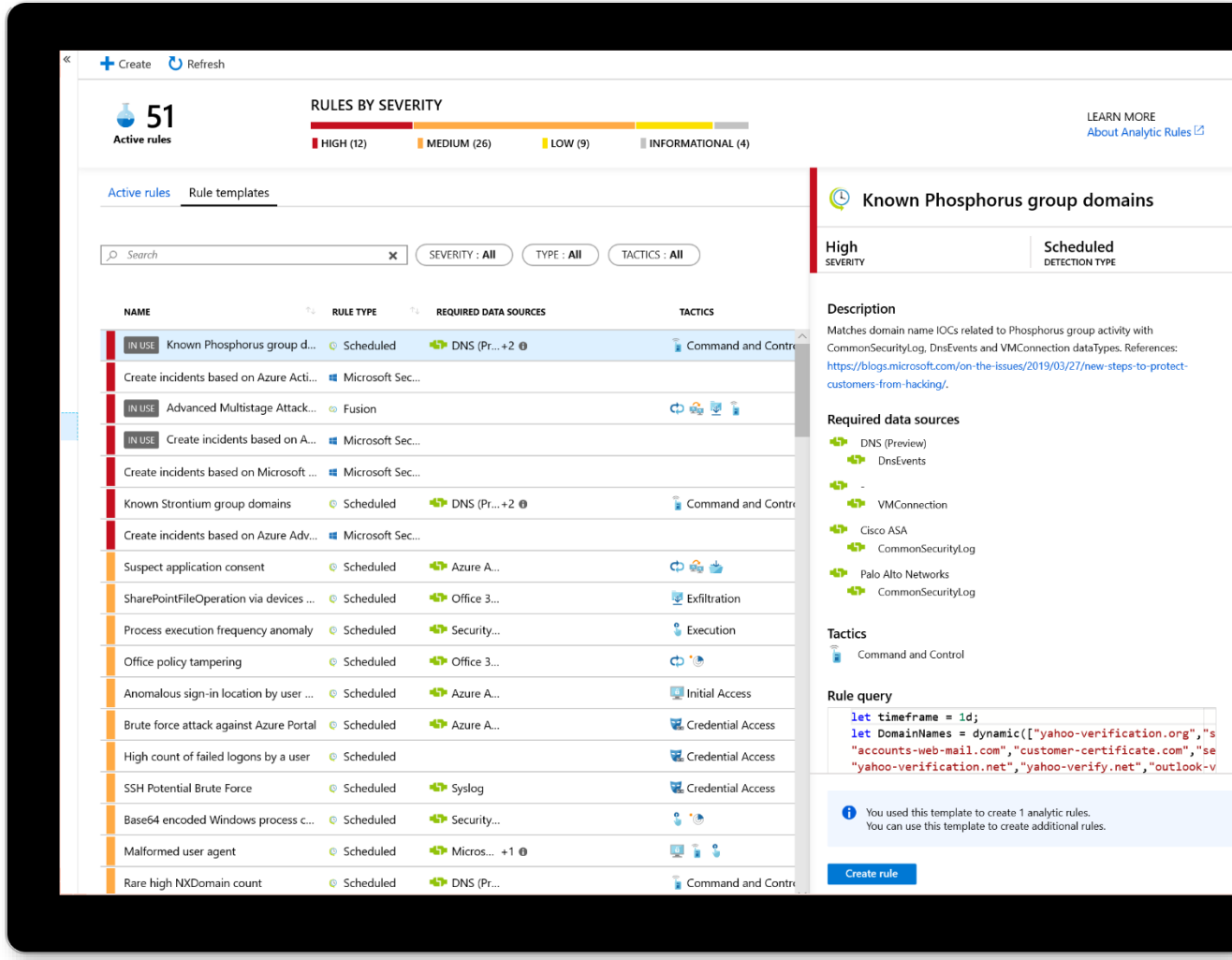
Sfrutta un'ampia libreria o crea regole custom

Choose from more than 100 built-in analytics rules

Customize and create your own rules using KQL queries

Correlate events with your threat intelligence and now with Microsoft URL intelligence + network data

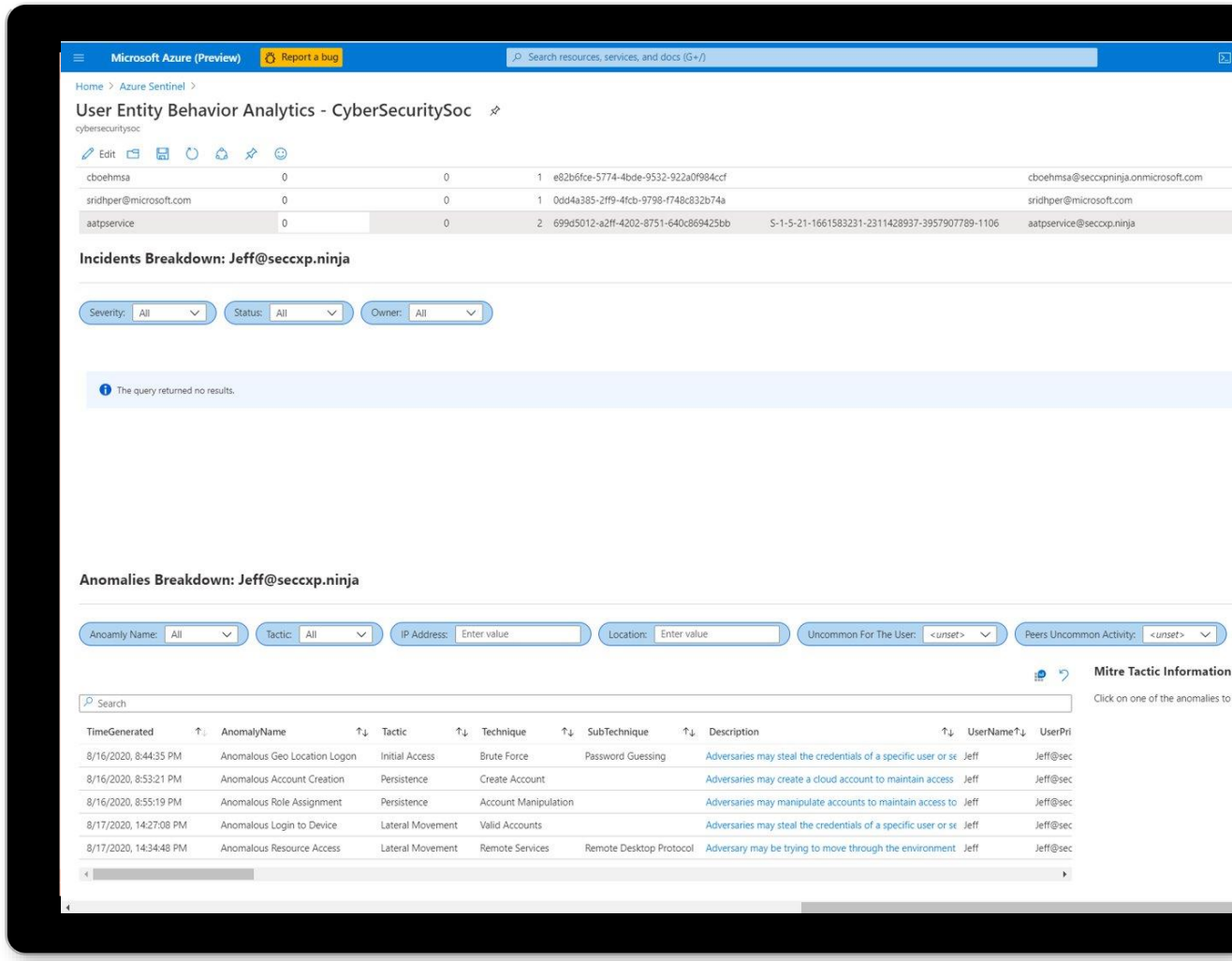
Trigger automated playbooks



Migliora il rilevamento delle minacce interne e sconosciute con l'analisi del comportamento di utenti ed entità

Use behavioral insights to detect anomalies, understand the relative sensitivity of entities, and evaluate potential impact

Get baseline behavioral profiles of entities across time and peer group horizons



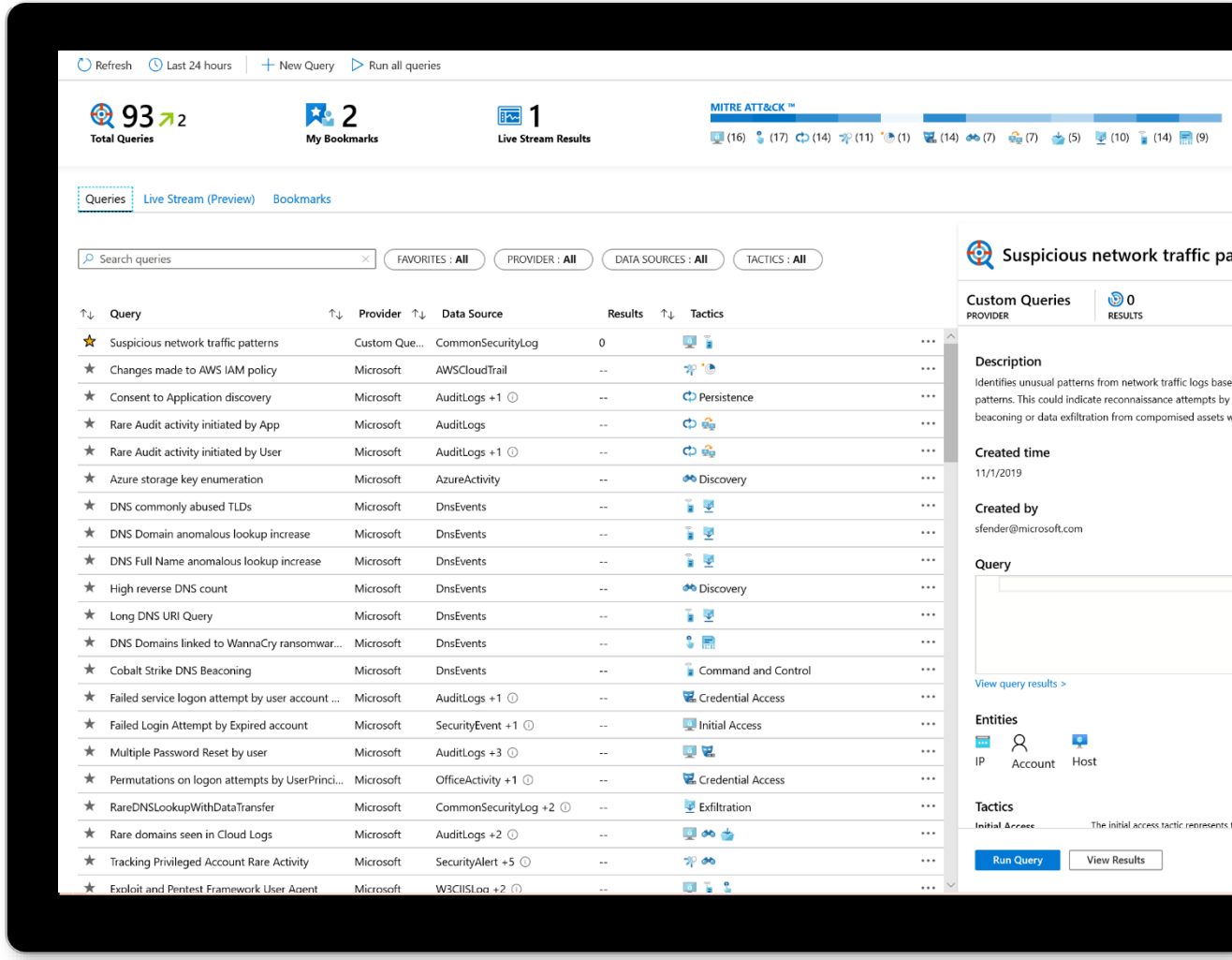
Powered by the proven Microsoft User and Entity Behavior Analytics (UEBA) engine

Ricerca

Inizia a ricercare i dati con query veloci e flessibili

Run built-in threat hunting queries - no prior query experience required

Customize and create your own hunting queries using KQL



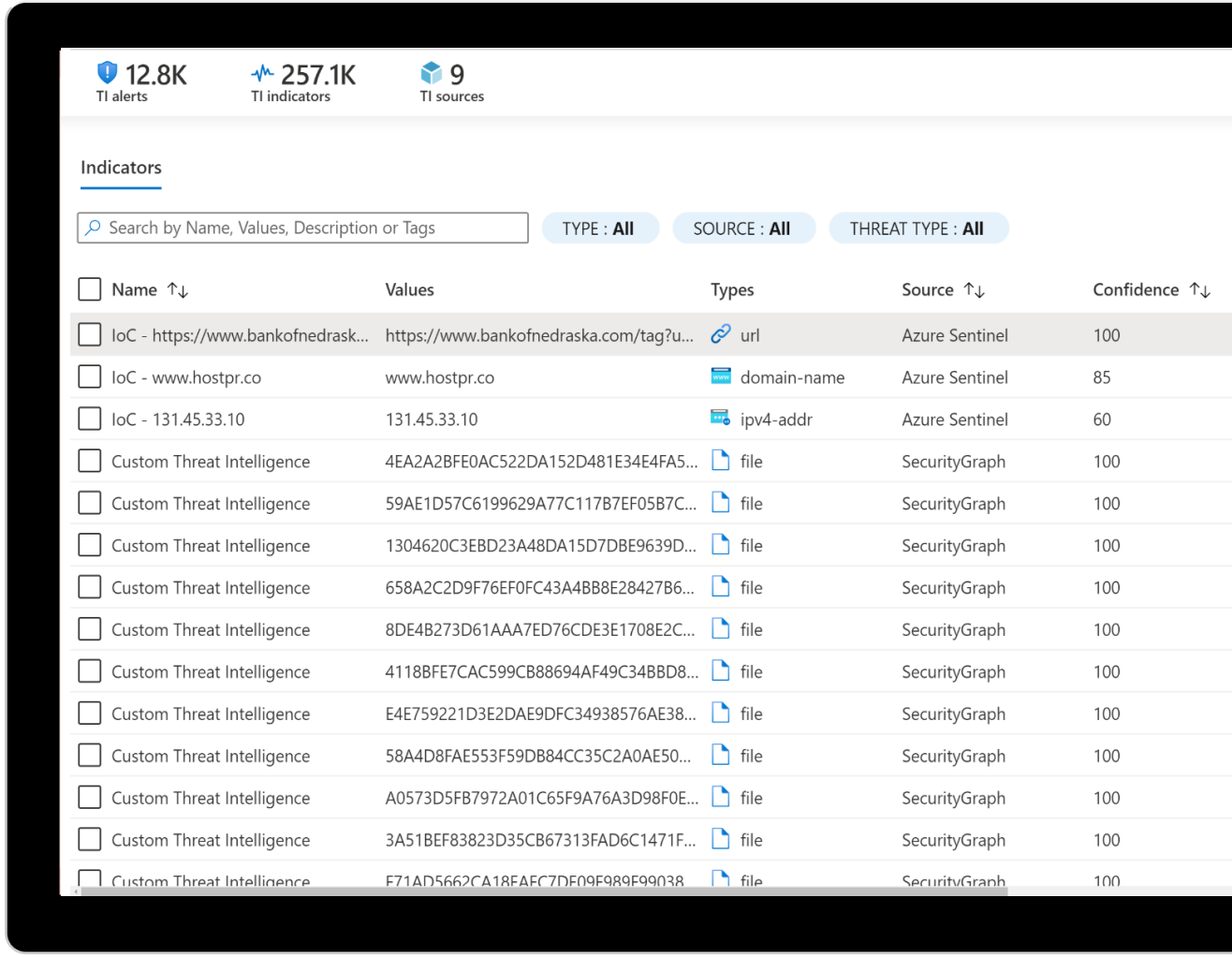
Intelligenza

Monitora e gestisci l'intelligence sulle minacce

Create, view, search, filter, sort, and tag all your threat indicators in a single pane

Use alert metrics to help understand top threats targeting your organization

Use automation playbooks for leading threat intelligence providers to enrich alerts



Incidenti

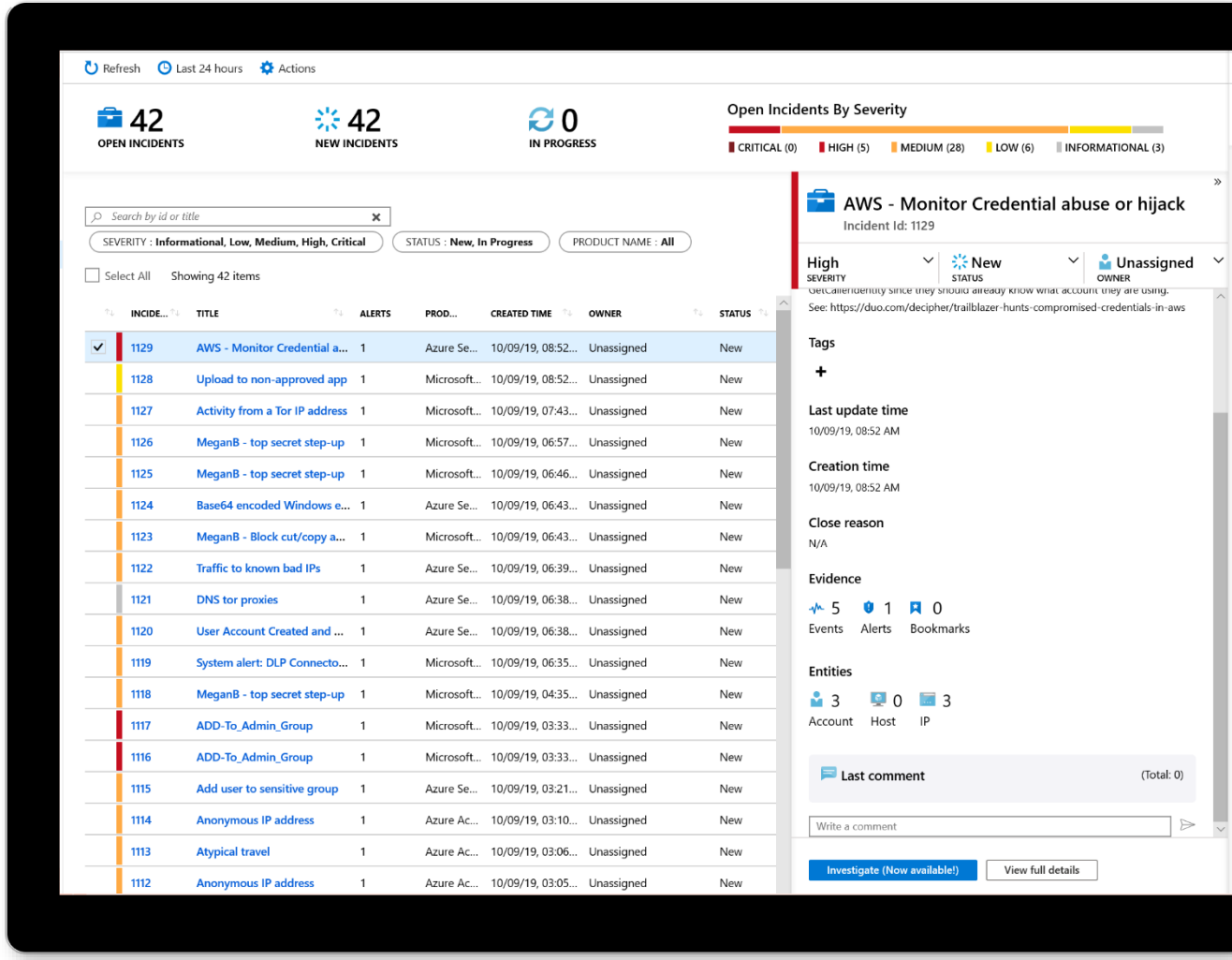
Avvia e monitora le indagini dagli incidenti di sicurezza processati e prioritari

Use incident to collect related alerts, events, and bookmarks

Manage assignments and track status

Add tags and comments

Trigger automated playbooks



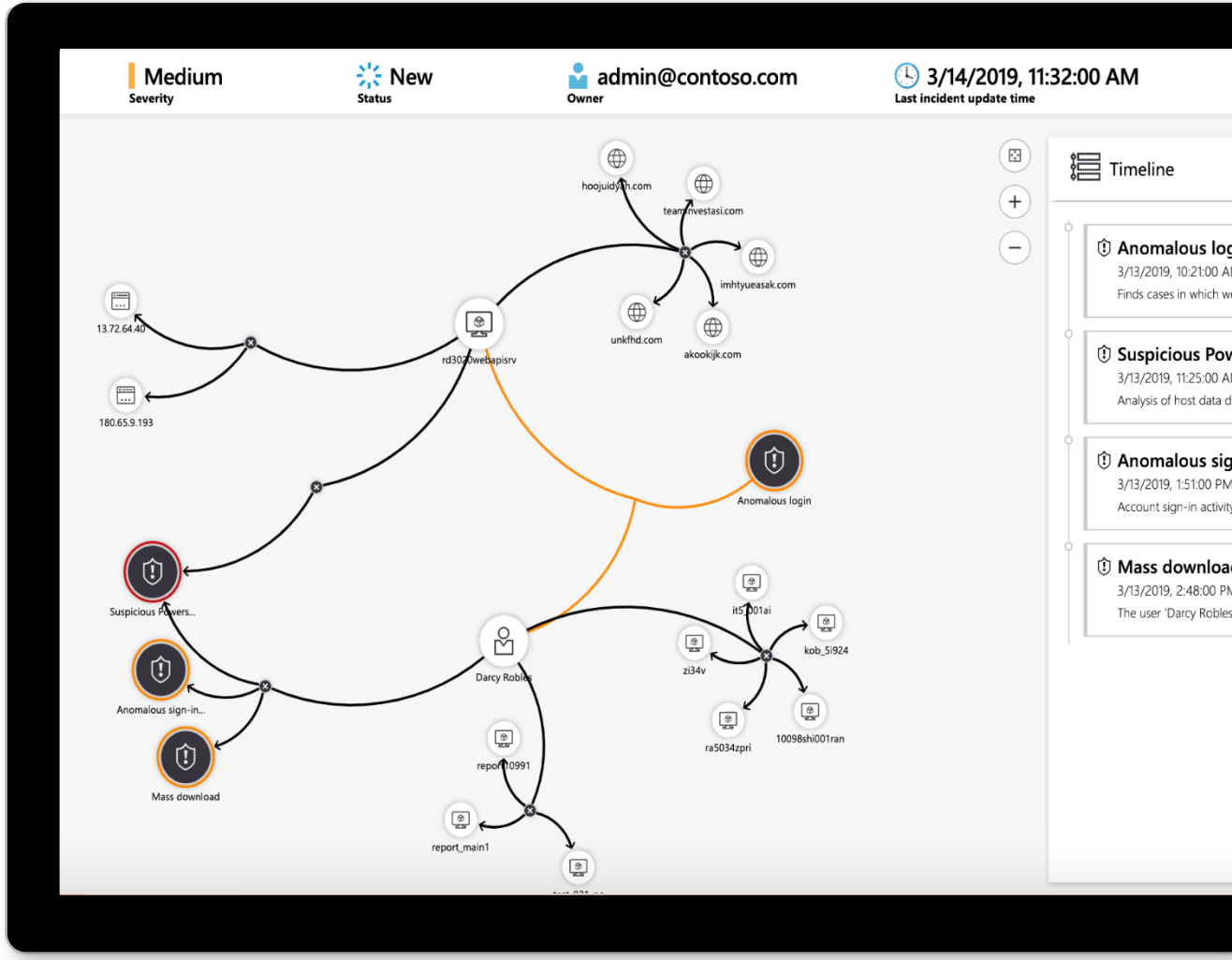
Visualizza l’intero attacco

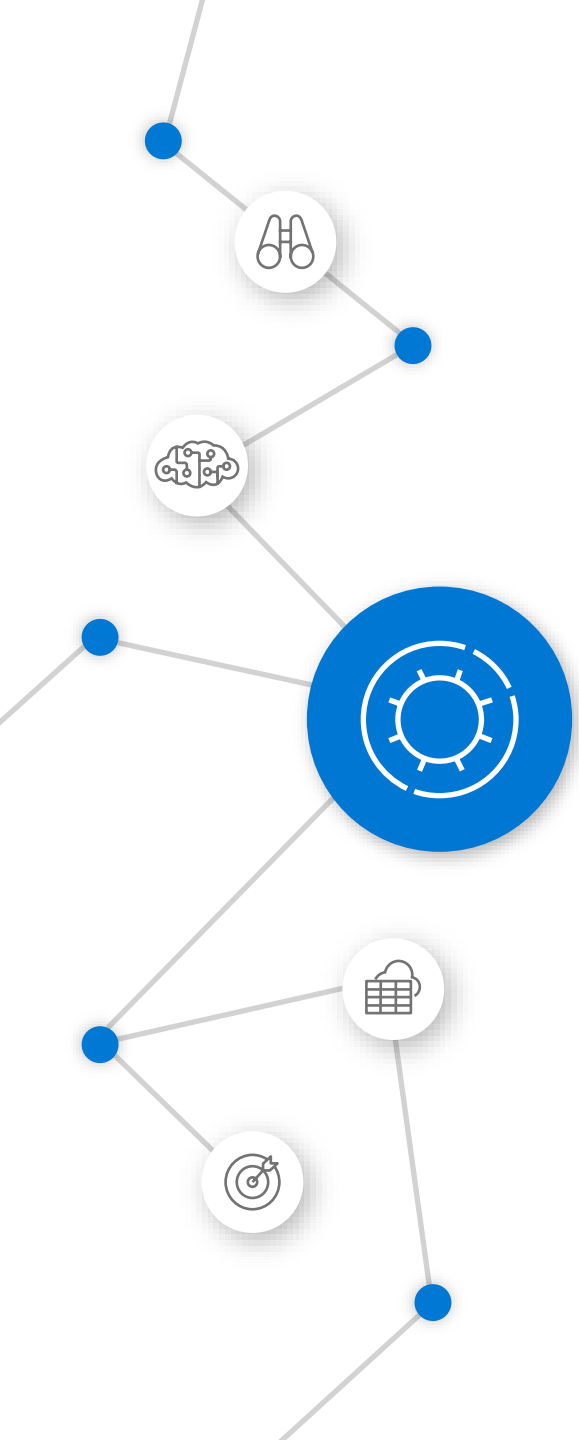
Navigate the relationships between related alerts, bookmarks, and entities

Expand the scope using exploration queries

View a timeline of related alerts, events, and bookmarks

Gain deep insights into related entities – users, domains, and more





Automation

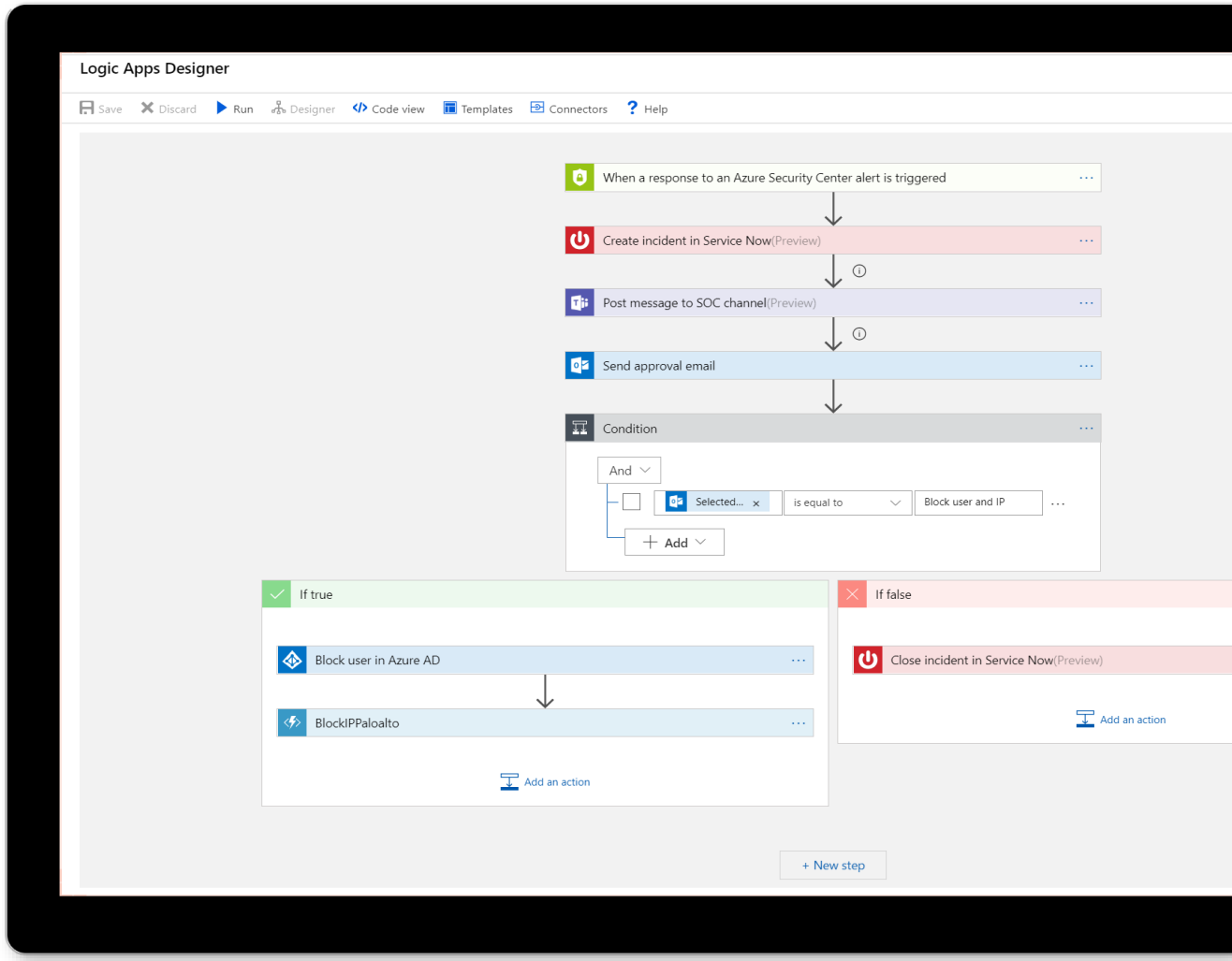
Automatizza e orchestra le operazioni di sicurezza usando le Azure Logic Apps

Build automated and scalable playbooks that integrate across tools

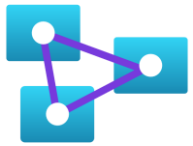
Choose from a library of samples

Create your own playbooks using 200+ built-in connectors

Trigger a playbook from an alert or incident investigation



Esempio di Playbook



Incident Management

Assign an Incident to an Analyst

Open a Ticket (ServiceNow/Jira)

Keep Incident Status in Sync

Post in a Teams or Slack Channel

Enrichment + Investigation

Lookup Geo for an IP

Trigger Defender ATP Investigation

Send Validation Email to User

Remediation

Block an IP Address

Block User Access

Trigger Conditional Access

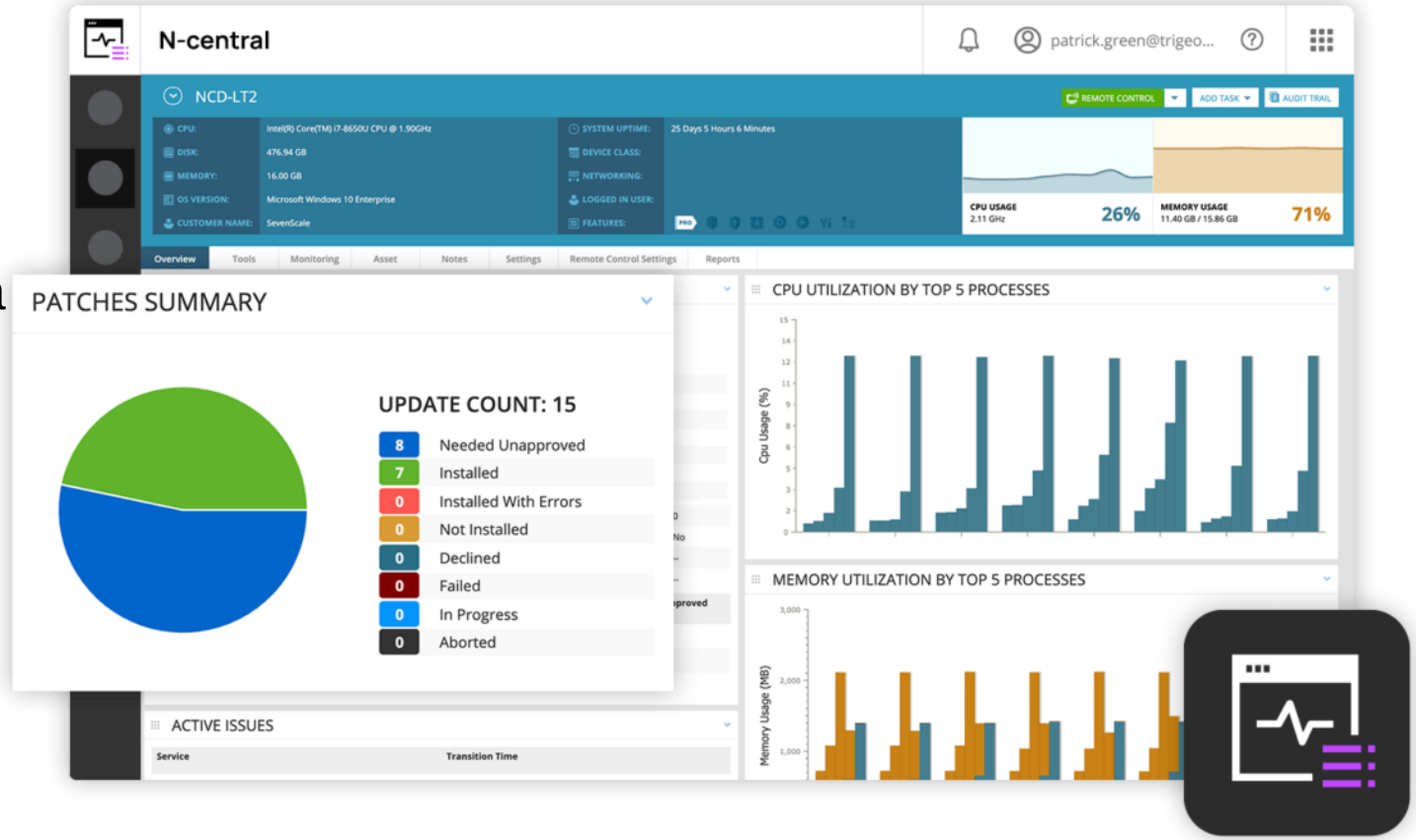
Isolate Machine

04. N-CENTRAL

Modernizzare il monitoraggio della propria infrastruttura

/ N-Central

- Disponibile come soluzione on-premise o in hosting
- Visibilità e gestione semplificate ed efficienti da una singola dashboard
- Avvisi proattivi con funzionalità di riparazione automatica
- Potenti strumenti di automazione per la gestione globale o granulare

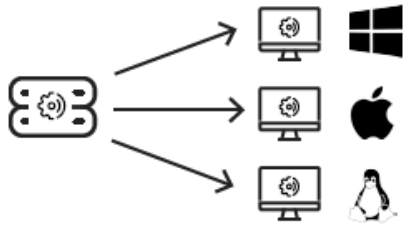


RESOL/E

/ N-Central

1 INTEGRAZIONE AUTOMATIZZATA

N-central è in grado di individuare e integrare automaticamente i dispositivi dei vostri utenti finali e di applicare le best practice per il monitoraggio.

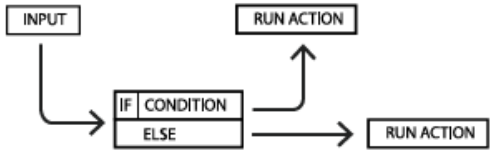


2 CONFIGURAZIONE AUTOMATIZZATA

Installazione automatica di antivirus e patch e configurazione automatica del backup.

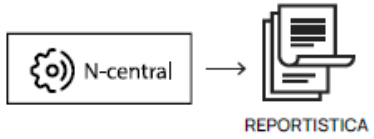
3 MANUTENZIONE AUTOMATIZZATA

Utilizzate la nostra ampia libreria di script o create il vostro in tutta facilità con un'interfaccia drag-and-drop; non è necessaria alcuna esperienza pregressa di programmazione o scripting.



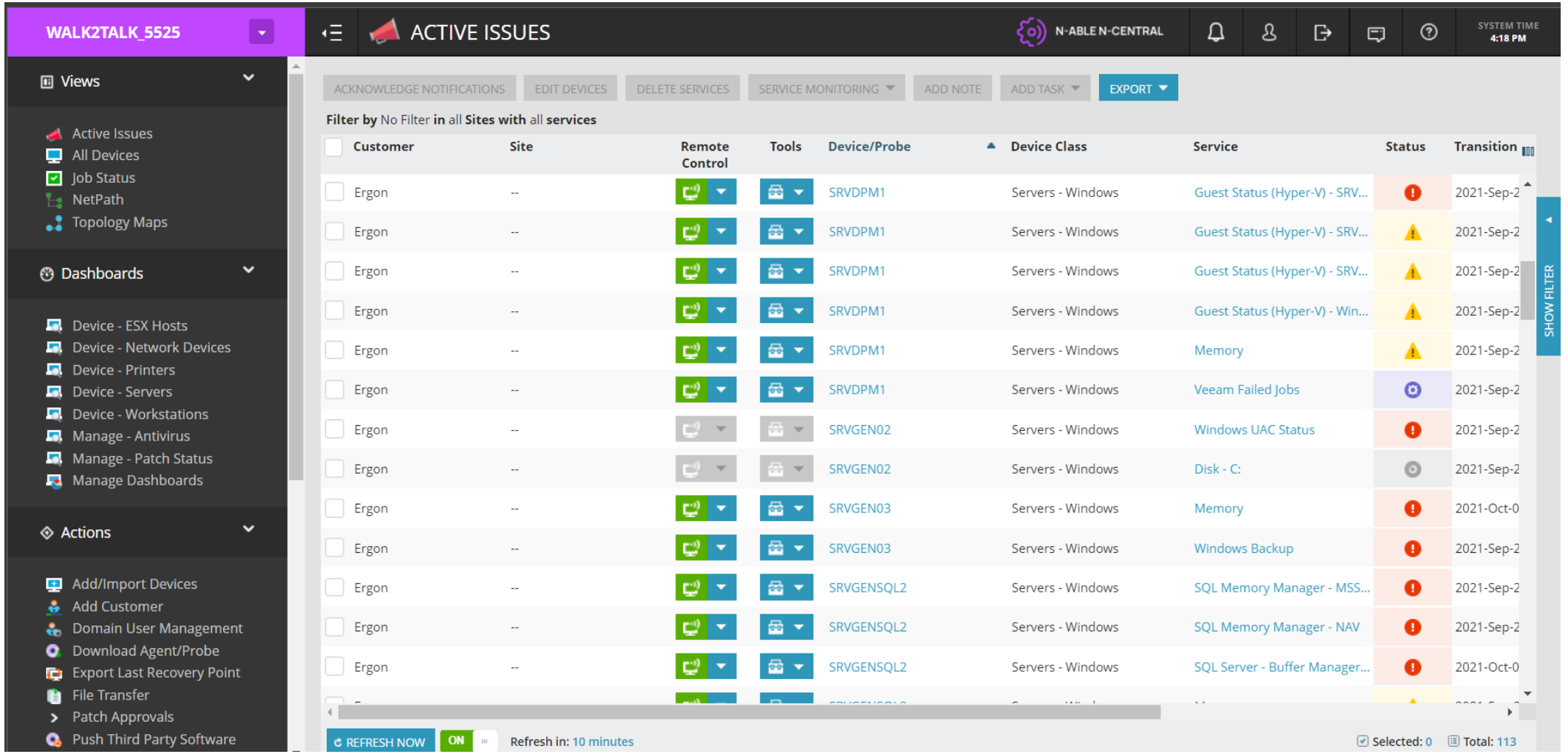
4 REPORTISTICA AUTOMATIZZATA

Dimostrate alle parti interessate e alla dirigenza il valore del vostro lavoro.



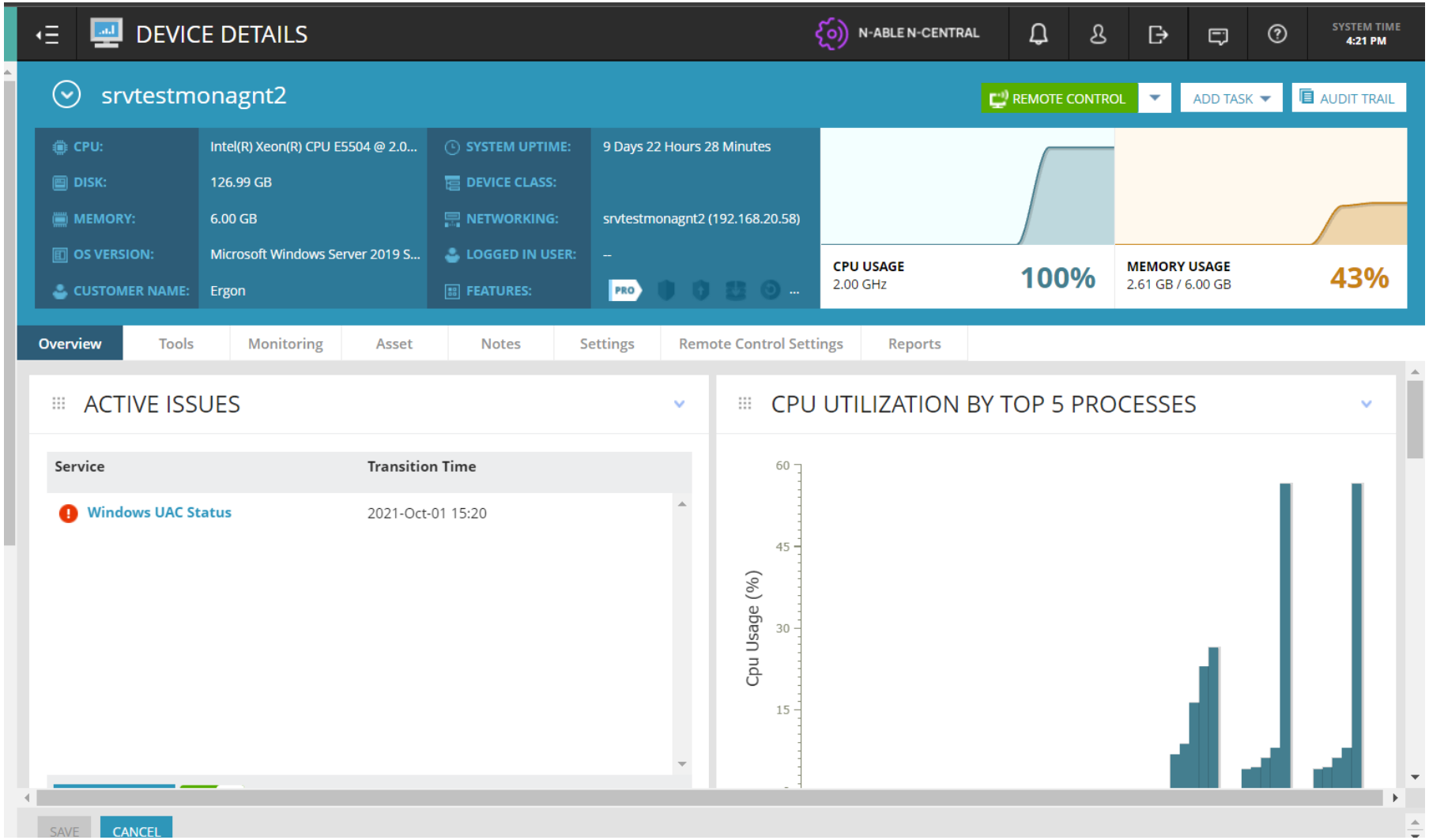
RESOL/E

/ N-Central



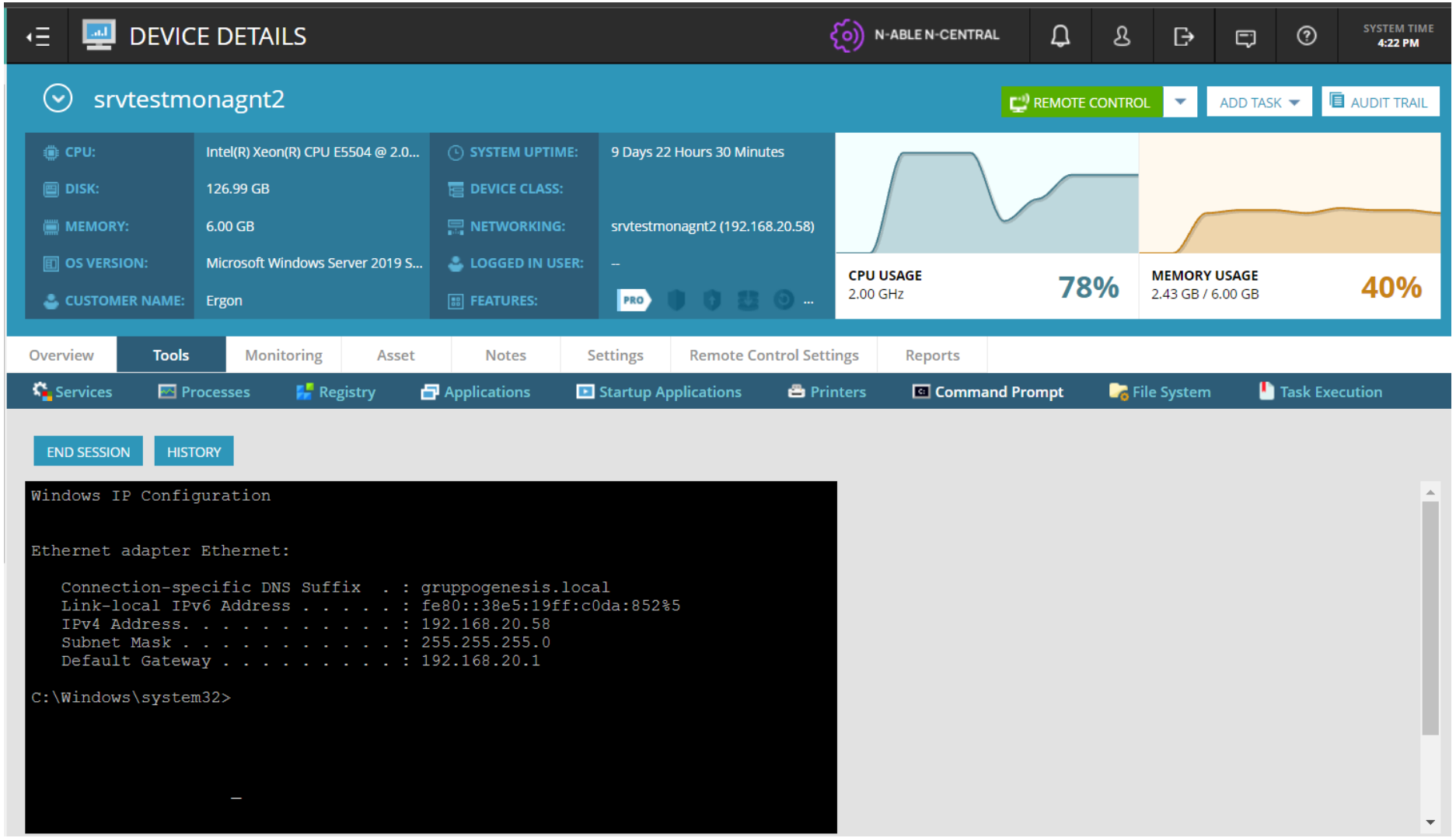
RESOL/E

/ N-Central



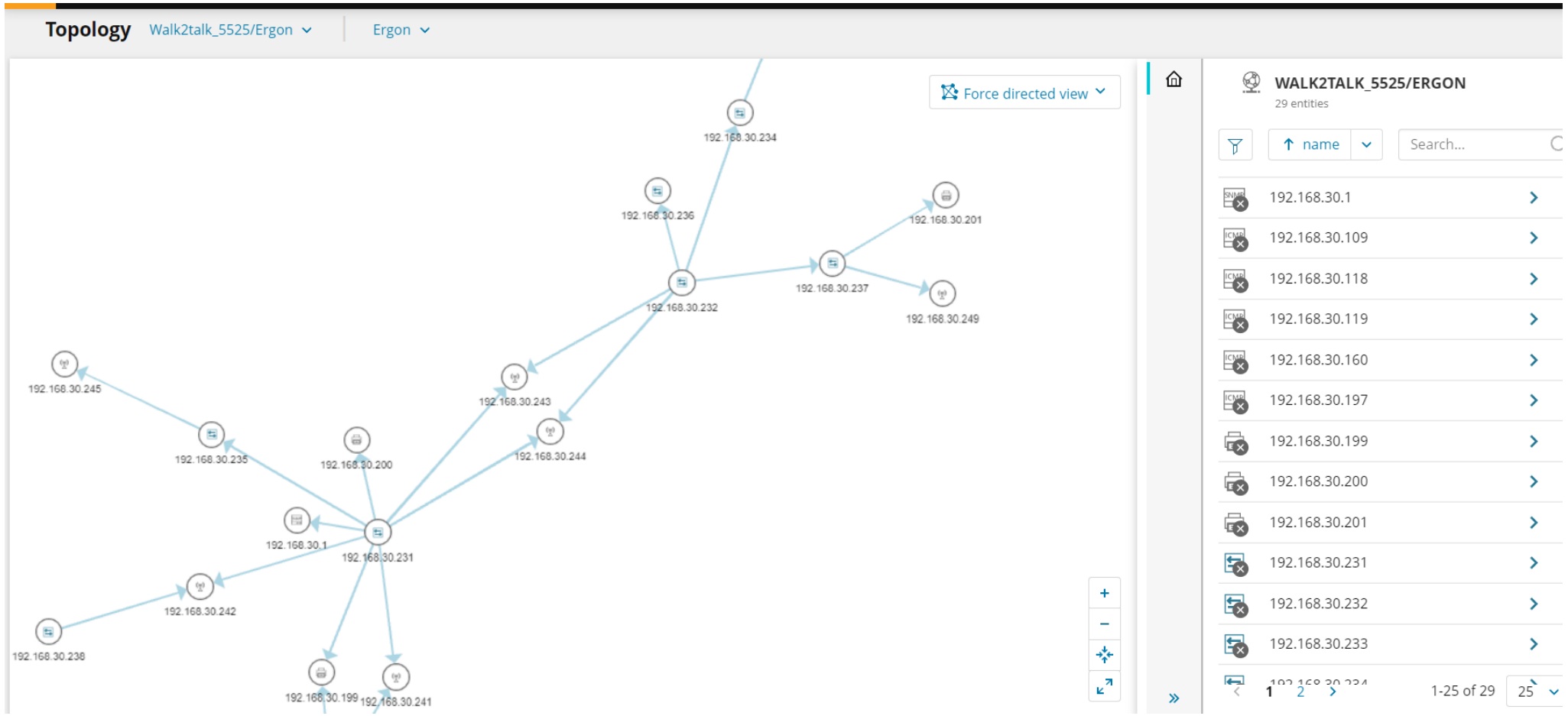
RESOL/E

/ N-Central



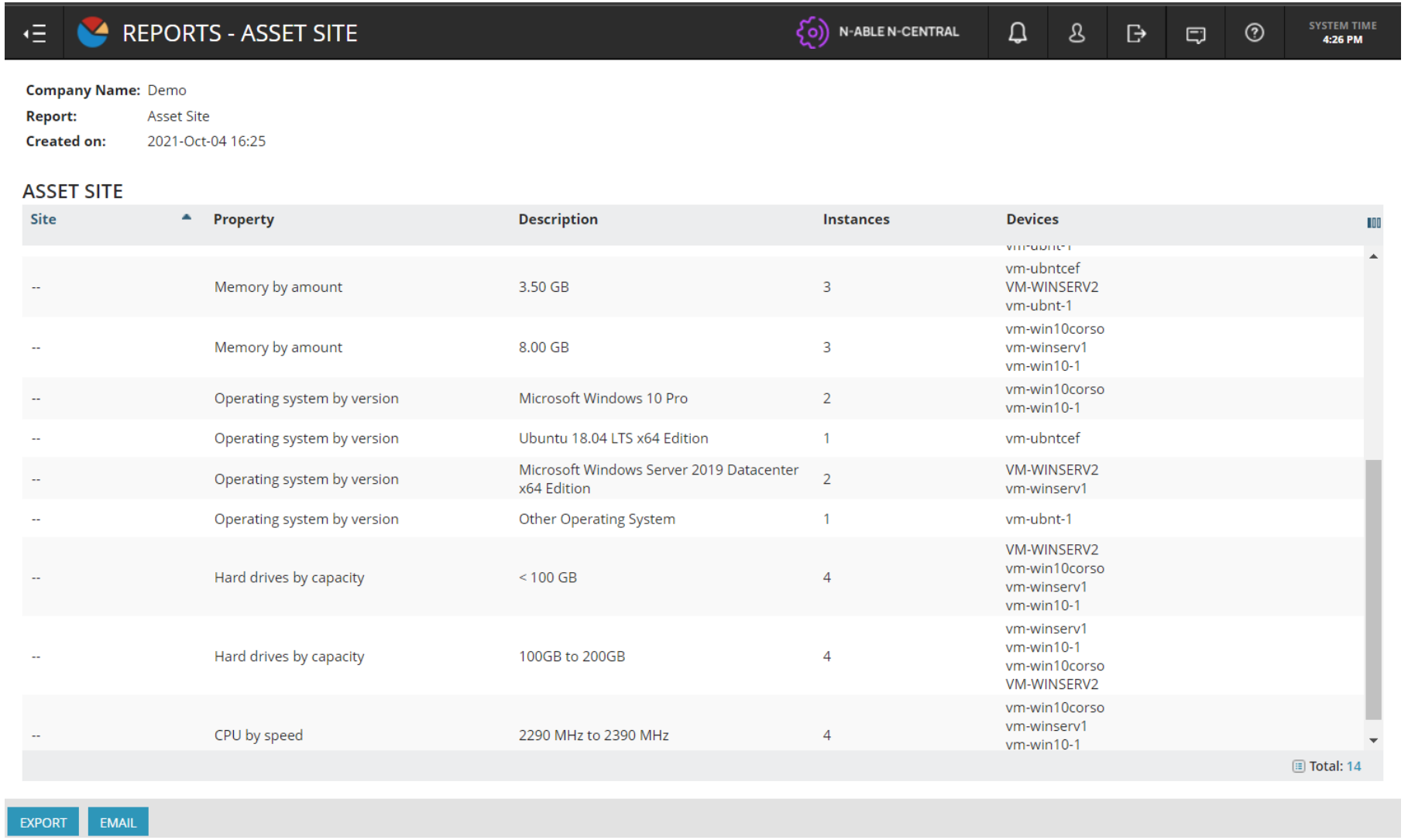
RESOL/E

/ N-Central



RESOL/E

/ N-Central



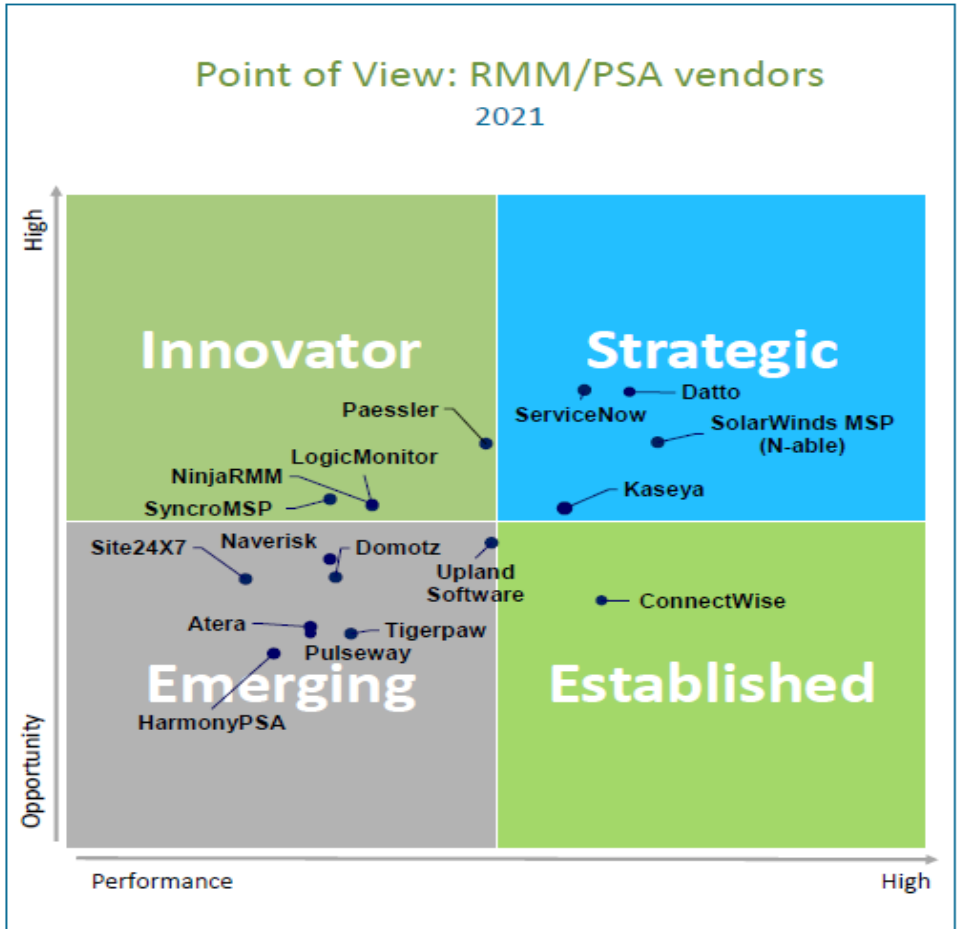
RESOL/E

/ N-Central

Managed Services Analysis
March 2021

canalys

MSP tech stack



RESOL/E

CICLO DI WEBINAR

Cloud Conference Italia 2021

8 eventi online IN DIRETTA dedicati alle novità tecnologiche di casa Microsoft

28 Ottobre 2021
CLOUD PC. Creare computer virtuali all'interno dell'infrastruttura IT

03 Novembre 2021
HYBRID WORK. Microsoft Teams, Logitech, Barco e Microsoft Surface per creare e gestire sale riunioni

10 Novembre 2021
CLOUD TRANSITION. Passare al Modern Desktop con Microsoft 365

17 Novembre 2021
CENTRALINO IN CLOUD. La Modern Collaboration passa da Microsoft Teams e Nfon

24 Novembre 2021
MODERN NETWORK. Cisko Meraki per una nuova rete Cloud Managed

01 Dicembre 2021
DIGITAL COMPLIANCE. Proteggi i dati della tua azienda

RESOL/E

PROMO ISCRIZIONE CORSI

10% di sconto su tutti i nostri corsi

Administering a SQL Database Infrastructure - NOVEMBRE: 09-17-23

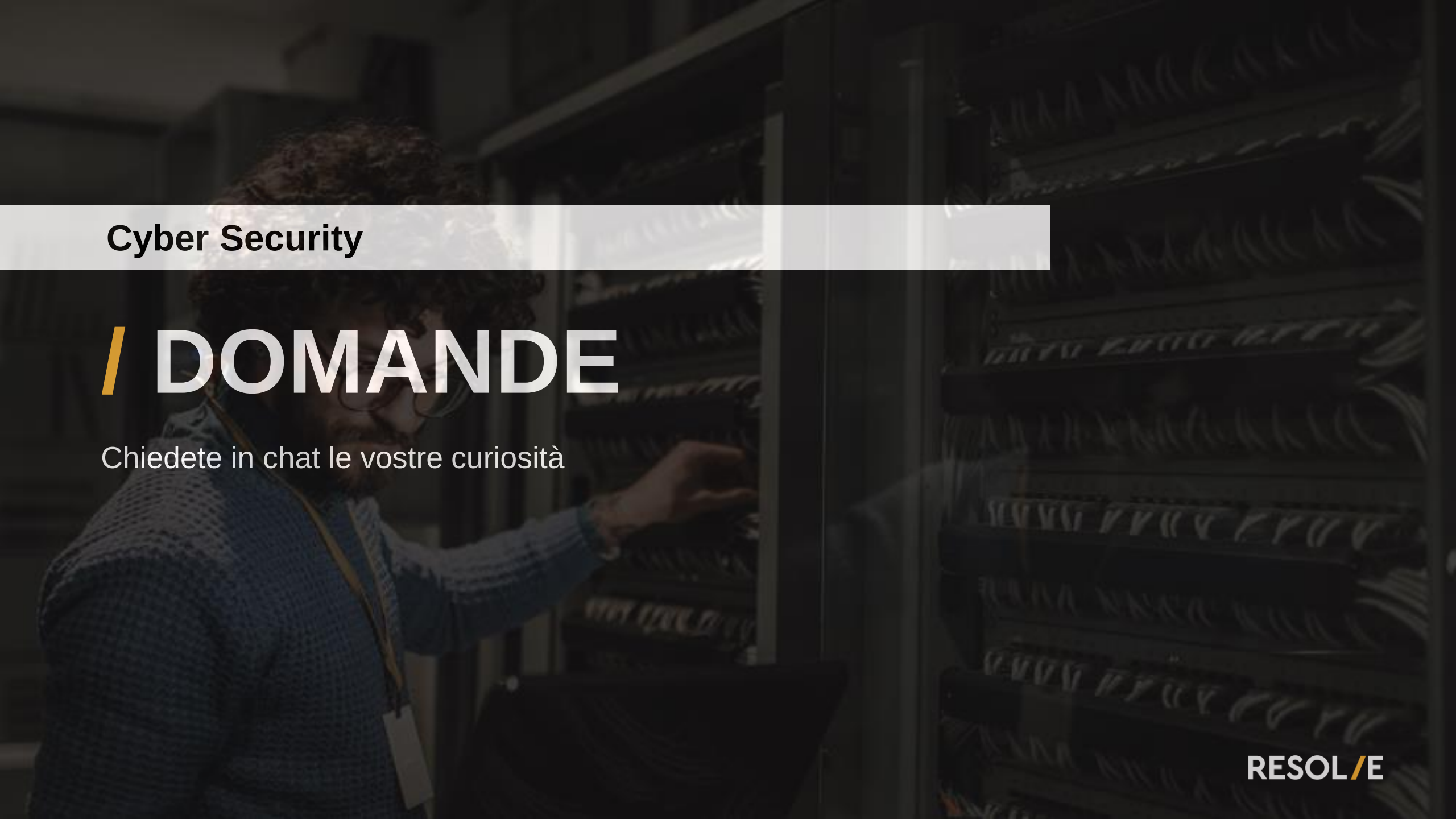
Office 365 Administrator - NOVEMBRE: 09-11-16-18-23

Managing Microsoft Teams - NOVEMBRE: 15-19-22-25-30

Power BI - NOVEMBRE: 23-29-30

Managing Modern Desktops - NOVEMBRE: 30 DICEMBRE: 02-13-15-17

DAX – Data Analysis Expressions - DICEMBRE: 02-06-13-14



Cyber Security

/ DOMANDE

Chiedete in chat le vostre curiosità

RESOL/E

RESOLVE

by ErgonGroup