

RESOL/E

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.

/ 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

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.

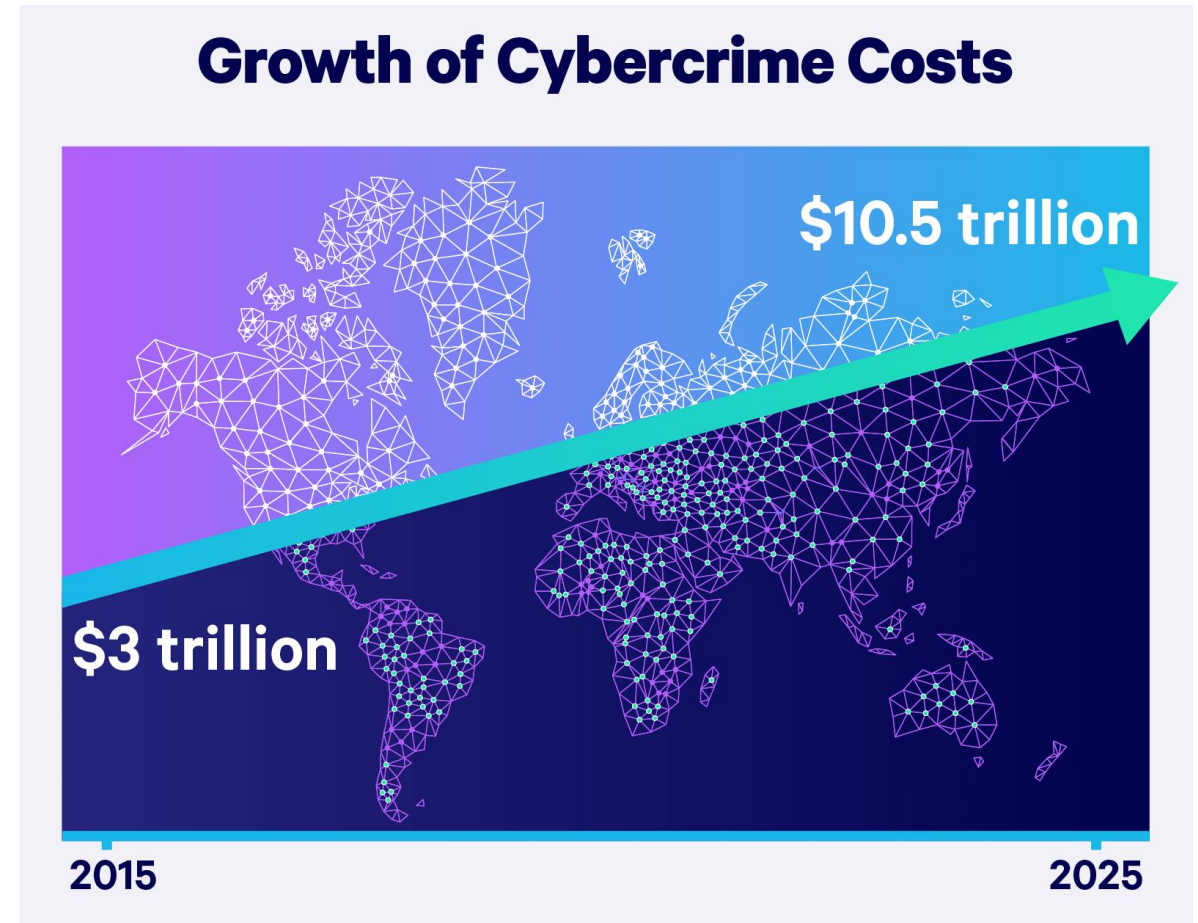
Vista la progressiva digitalizzazione dei processi, la Cyber security serve a preservare l'intero ecosistema aziendale che sempre più è formato da uno scenario ibrido.

01. CYBER SECURITY

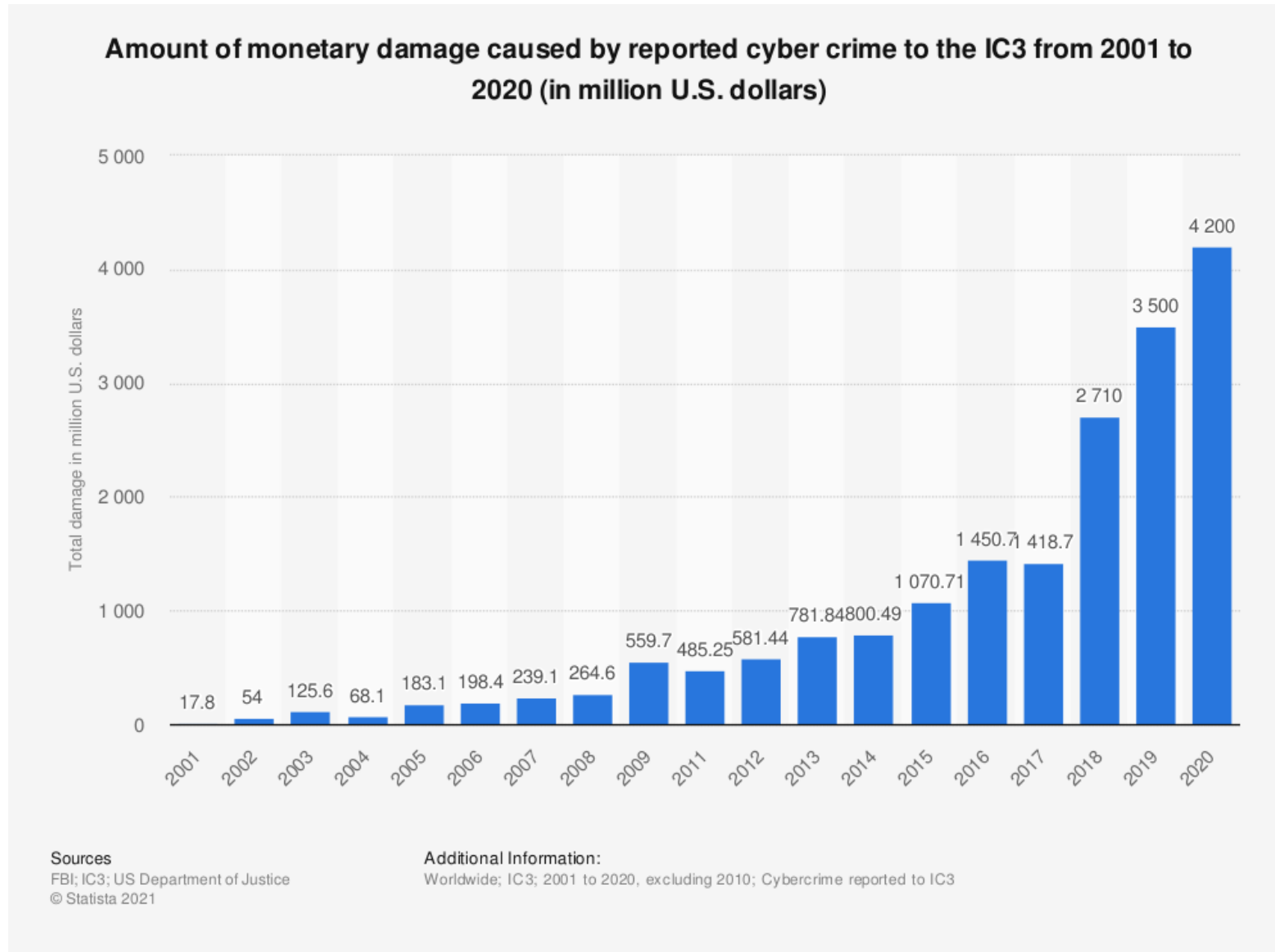
Perché oggi la Cyber Security è Importante?

/ 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



/ Perché la cybersecurity è importante?



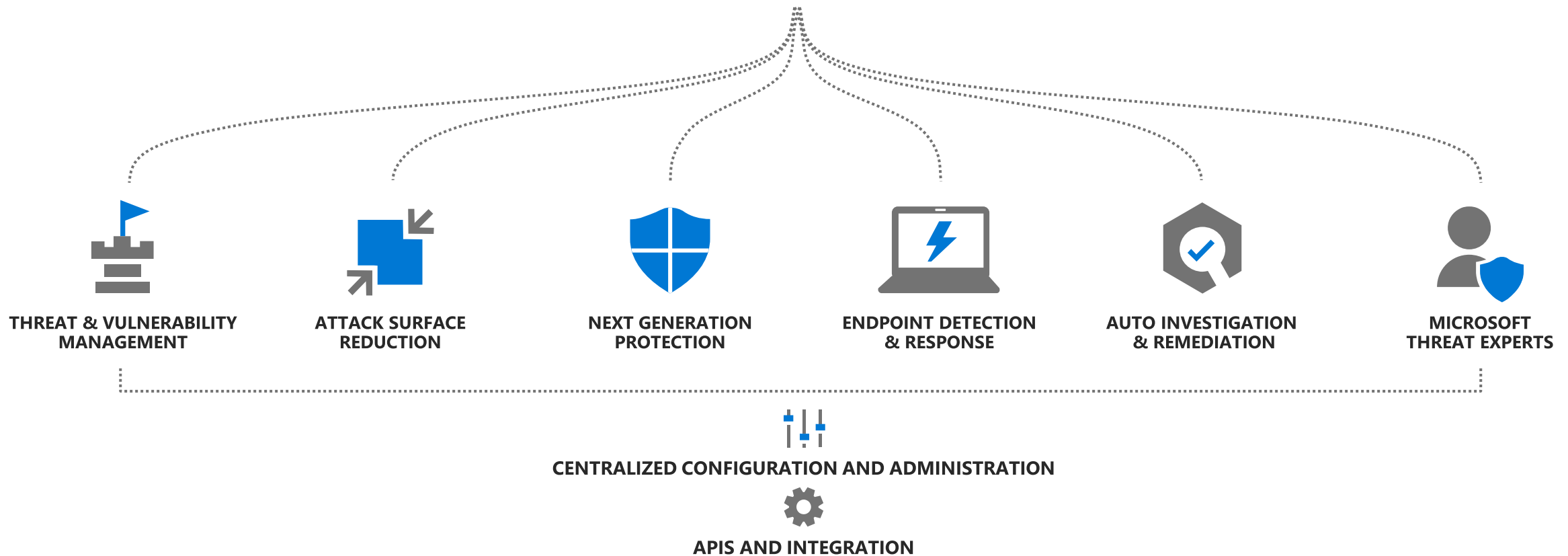
02. MICROSOFT DEFENDER FOR ENDPOINT

**Proteggere i clients con
una soluzione moderna**



Microsoft Defender for Endpoint

Threats are no match.



/ 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**.

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



Our antimalware capabilities consistently achieve **high scores in independent tests**.

/ Microsoft Defender for Endpoint



 Windows



macOS



iOS

 Windows 365
 Azure Virtual Desktop



Cisco
Juniper Networks

HP Enterprise
Palo Alto Networks

Endpoints and servers

Mobile device OS

Virtual desktops

Network devices

/ Microsoft Defender for Endpoint



 Windows



macOS



iOS

 Windows 365
 Azure Virtual Desktop



Cisco
Juniper Networks

HP Enterprise
Palo Alto Networks

Endpoints and servers

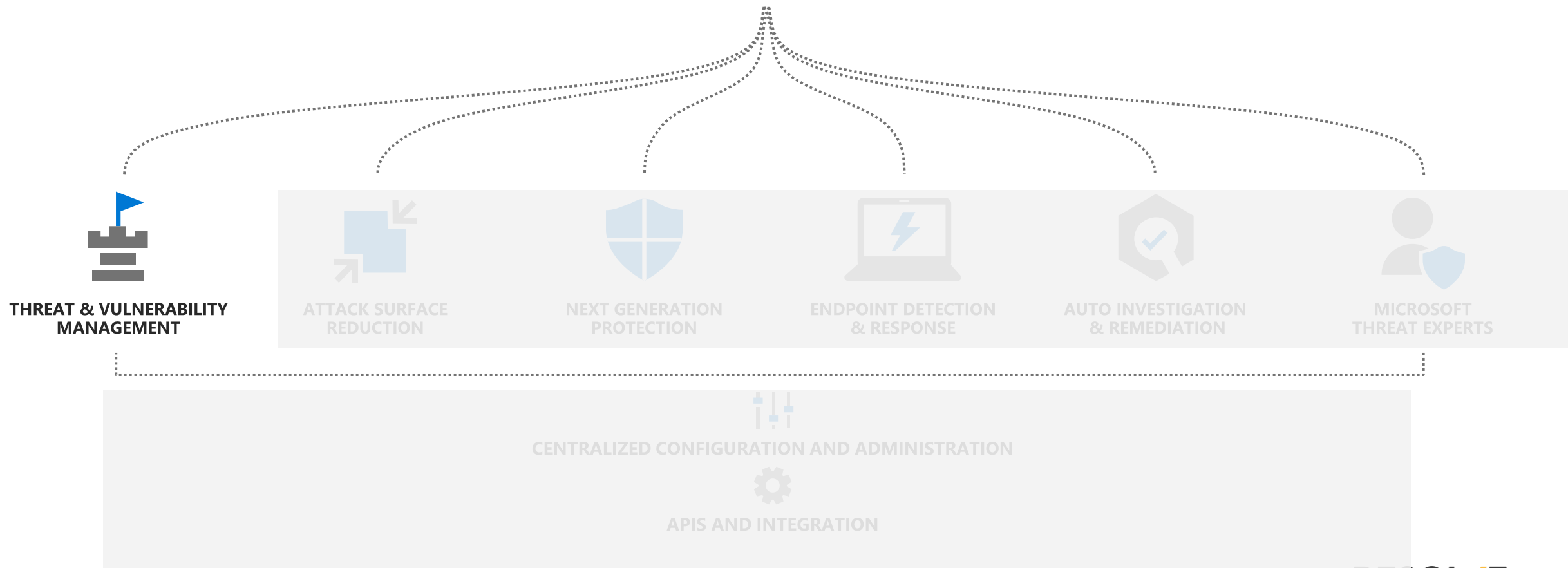
Mobile device OS

Virtual desktops

Network devices



Microsoft Defender for Endpoint



/ Microsoft Defender for Endpoint

Threat & Vulnerability Management

Un approccio risk-based per migliorare la gestione delle vulnerabilità

1



Continuous real-time discovery

2

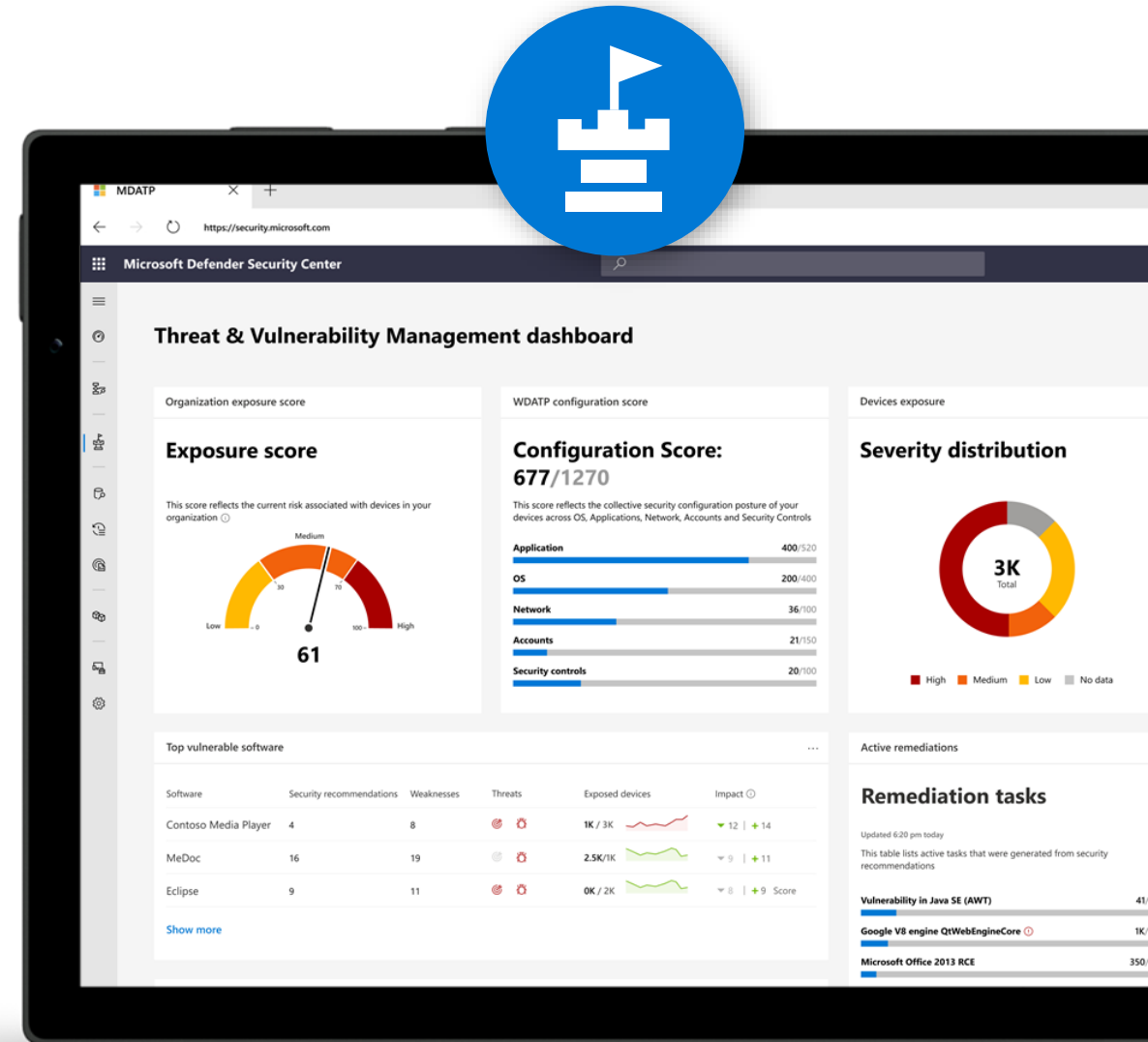


Context-aware prioritization

3

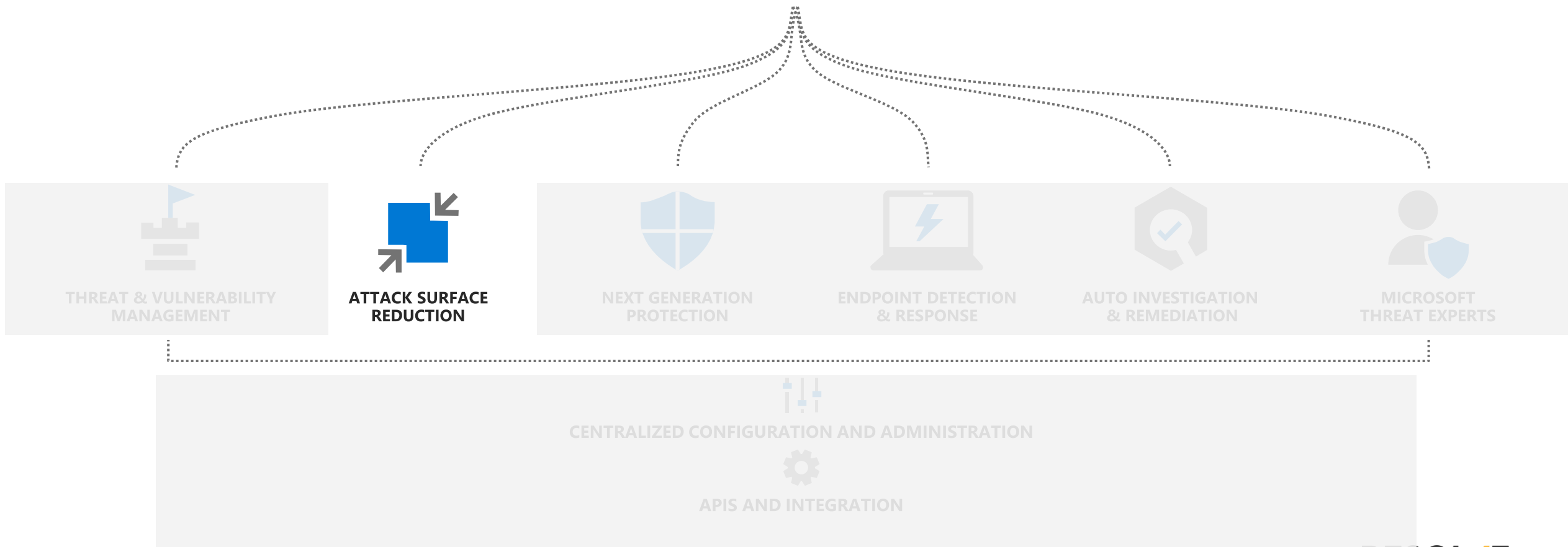


Built-in end-to-end remediation process





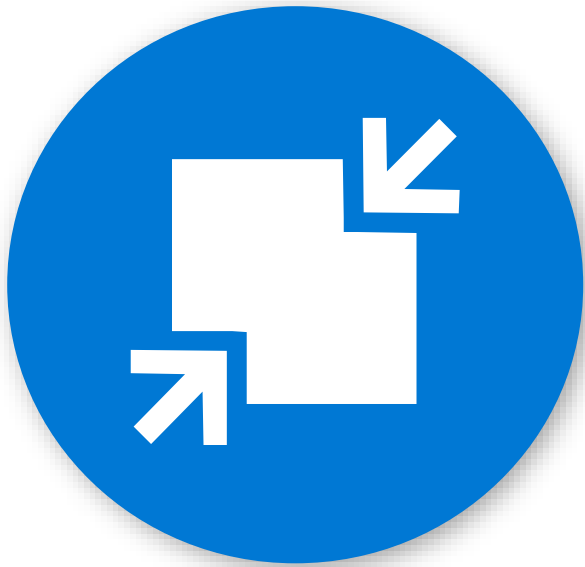
Microsoft Defender for Endpoint



/ 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

/ Microsoft Defender for Endpoint

Attack Surface Reduction

Easy button:
turn on block

The screenshot displays the Microsoft 365 Security console interface. The main heading is "Monitoring & reports > Attack surface reduction rules". Below this, there are tabs for "Detections", "Configuration" (which is selected), and "Rule status".

A prominent message states: "Five rules can be turned on for 80% of your devices with no user impact. Based on your audit data over the last 14 days." Below this message are two buttons: "View details" and "Dismiss".

Below the message, there is a section titled "Device configuration overview". It shows three categories: "Rules in audit only" with a count of 324, "Some or all rules in block" with a count of 525, and "Off" with a count of 22.

To the right of the "Device configuration overview" section is a link: "Identify and fix devices with limited protection due to missing prerequisites or misconfigured rules. [Learn about prerequisites](#)".

Below the counts, there is an "Export" button and a table with the following columns: Device name, Domain, OS, User, ASR support, Overall configuration, and Rules in block.

The table contains three rows of data:

Device name	Domain	OS	User	ASR support	Overall configuration	Rules in block
CONT_PC_1	Workgroup	Windows 10	UserName1	Partial	Rules in audit only	0
CONT_PC_2	AAD joined	Windows 10	UserName2 + 1 more	Full	Some or all rules in block	4
CONT_PC_3	Workgroup	Windows 10	UserName3 + 2 more	None	Off	0

On the right side of the console, there is a sidebar with the heading "Five rules can be turned on for 80% of your devices with no user impact". Below this, it says "Based on your audit data over the last 14 days".

The sidebar lists several rules with "Learn more" links:

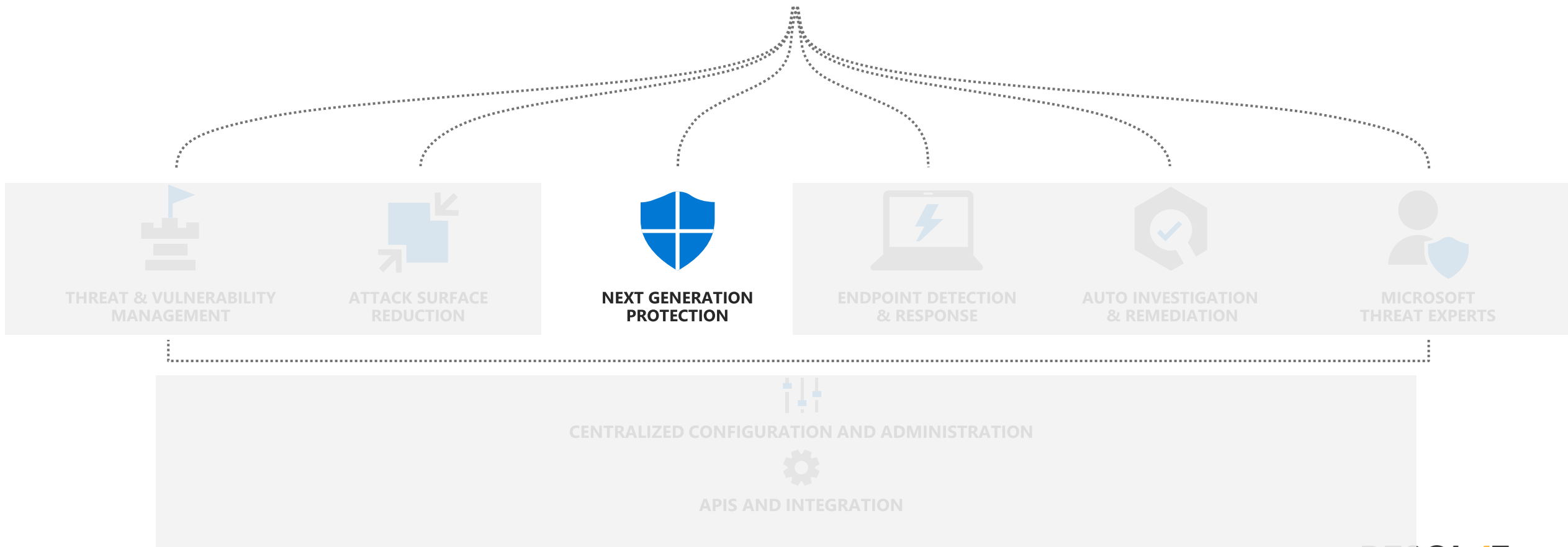
- Office apps injecting into other processes
- Office apps/macros creating executable content
- Office apps launching child processes
- Win32 imports from Office macro code
- Obfuscated js/vbs/ps/macro code

At the bottom of the sidebar, it says "Devices" and "2,354 devices". Below this, it says "80% of your total devices with Windows Defender Advanced Threat Protection".

At the bottom of the sidebar, there are two buttons: "Get script to implement" and "Submit Intune ticket".



Microsoft Defender for Endpoint



/ 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

/ 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

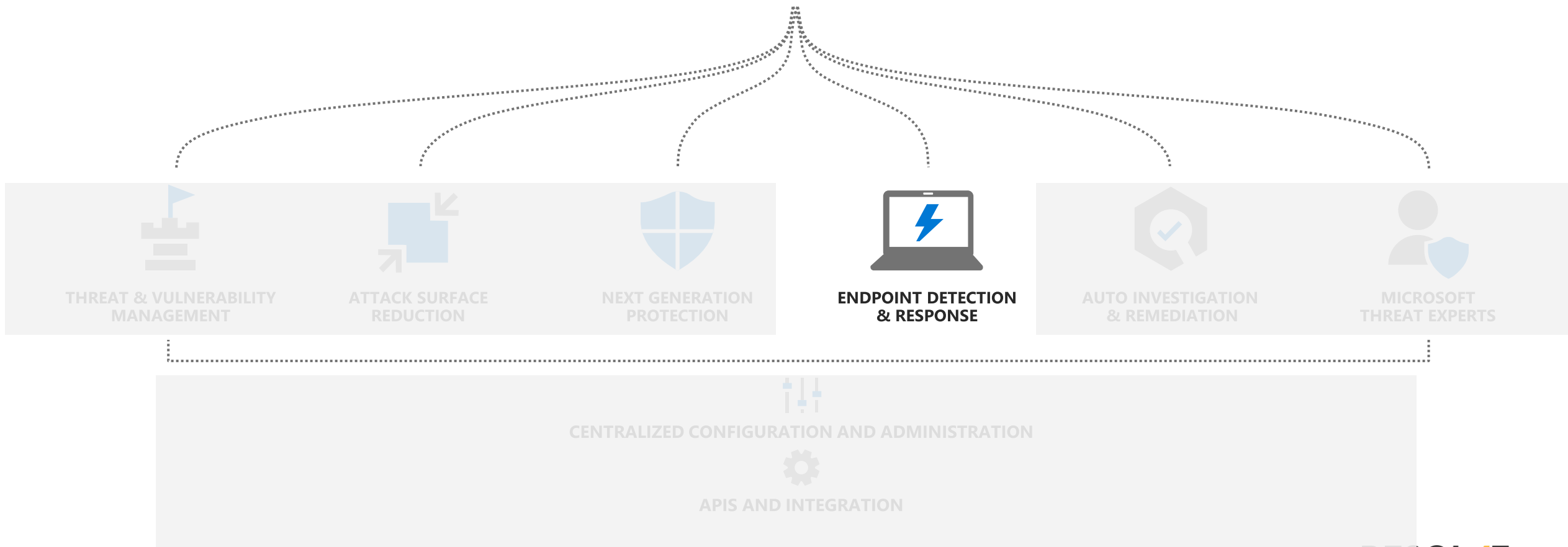


Network monitoring

Catches malicious network activities



Microsoft Defender for Endpoint



/ 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

Click on a URL



Installation



Persistence



Reconnaissance



Exploitation



C&C channel



Privilege escalation



Lateral movement



46% of compromised systems had no malware on them



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



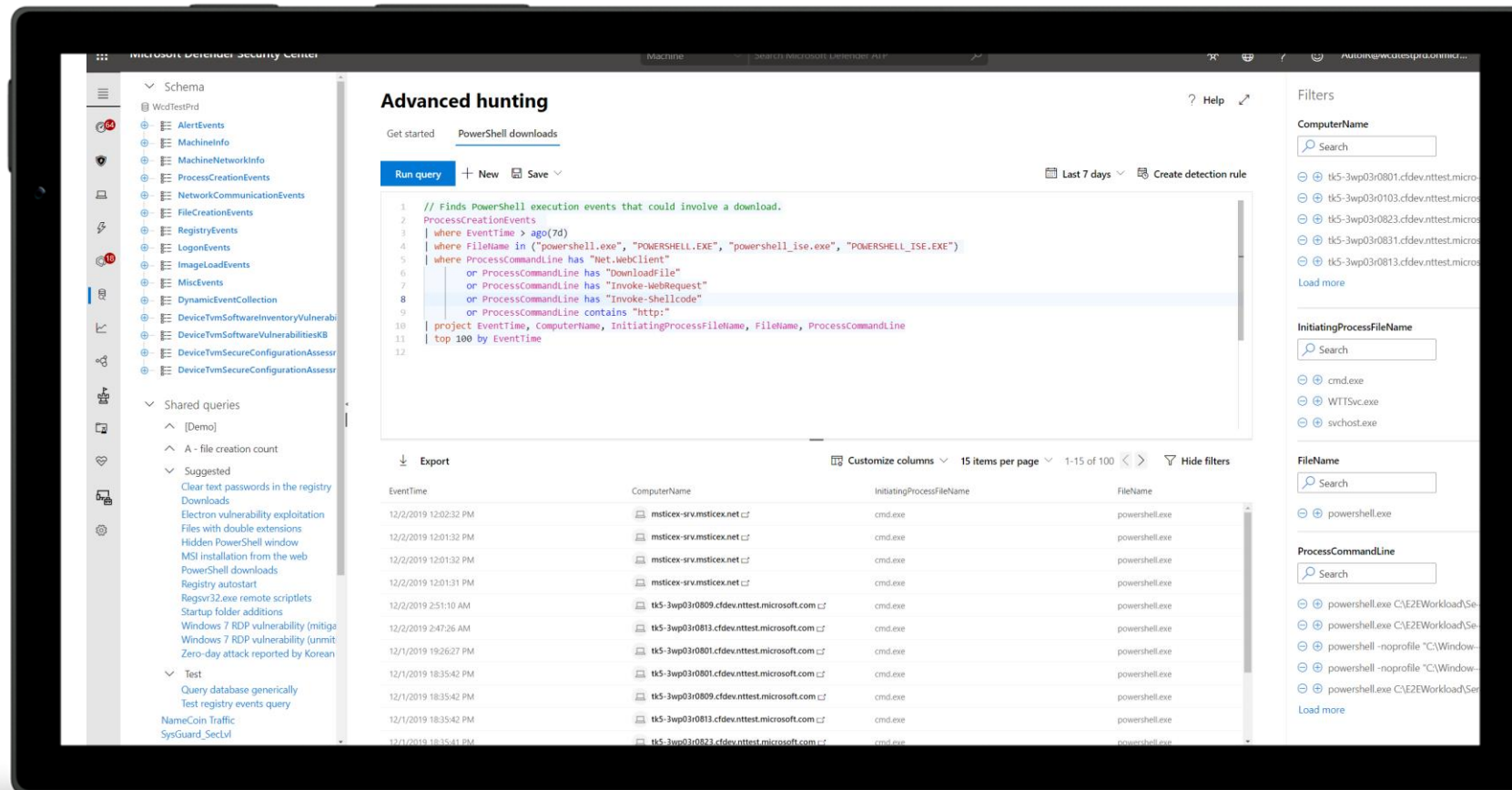
Collecting evidence and alerts, even from 1 infected device, can be a long time-consuming process



Living off the land - Attackers use evasion-techniques

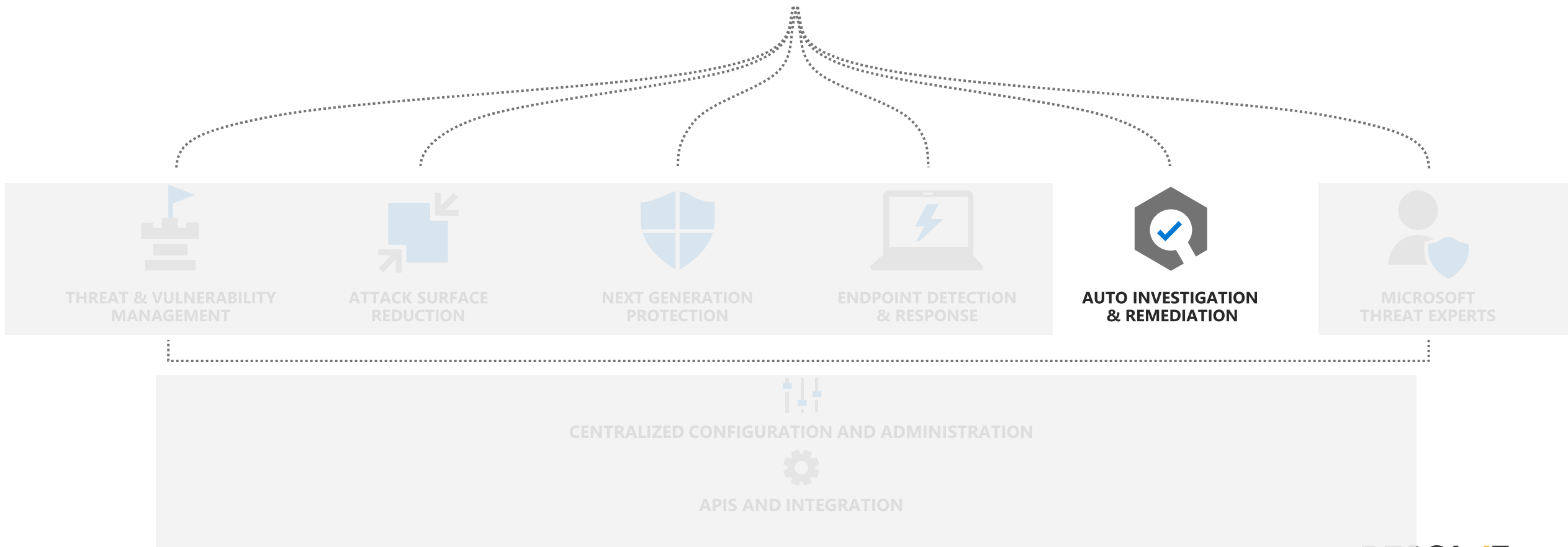
/ Microsoft Defender for Endpoint

Advanced hunting with custom detection and custom response





Microsoft Defender for Endpoint



/ Microsoft Defender for Endpoint



More threats, more alerts
leads to analyst fatigue



Alert investigation
is time-consuming



Expertise is expensive



Manual remediation
requires time

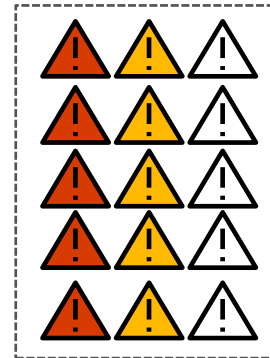


Talent shortage in
cybersecurity



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

Alert queue

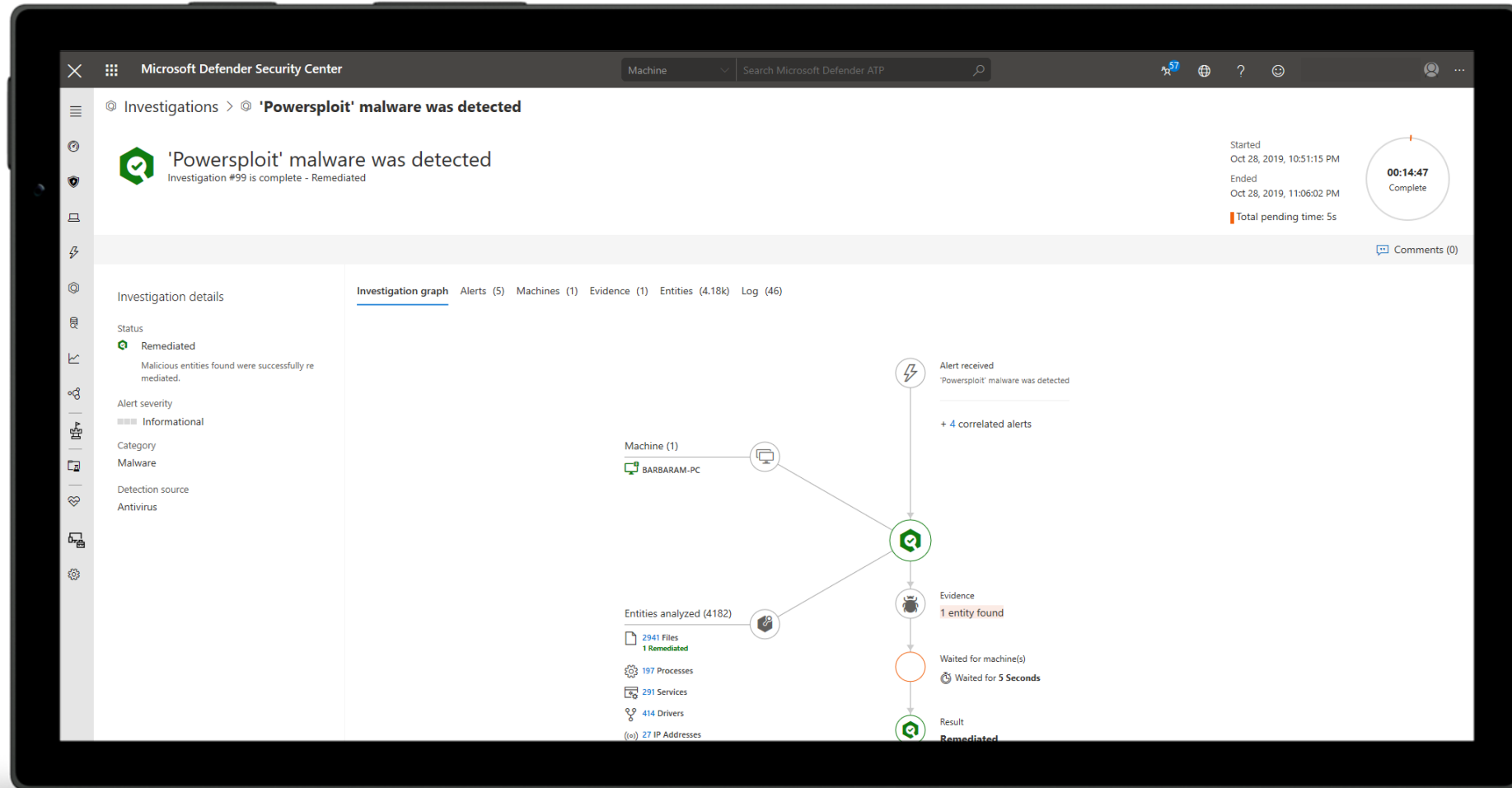


Analyst 1



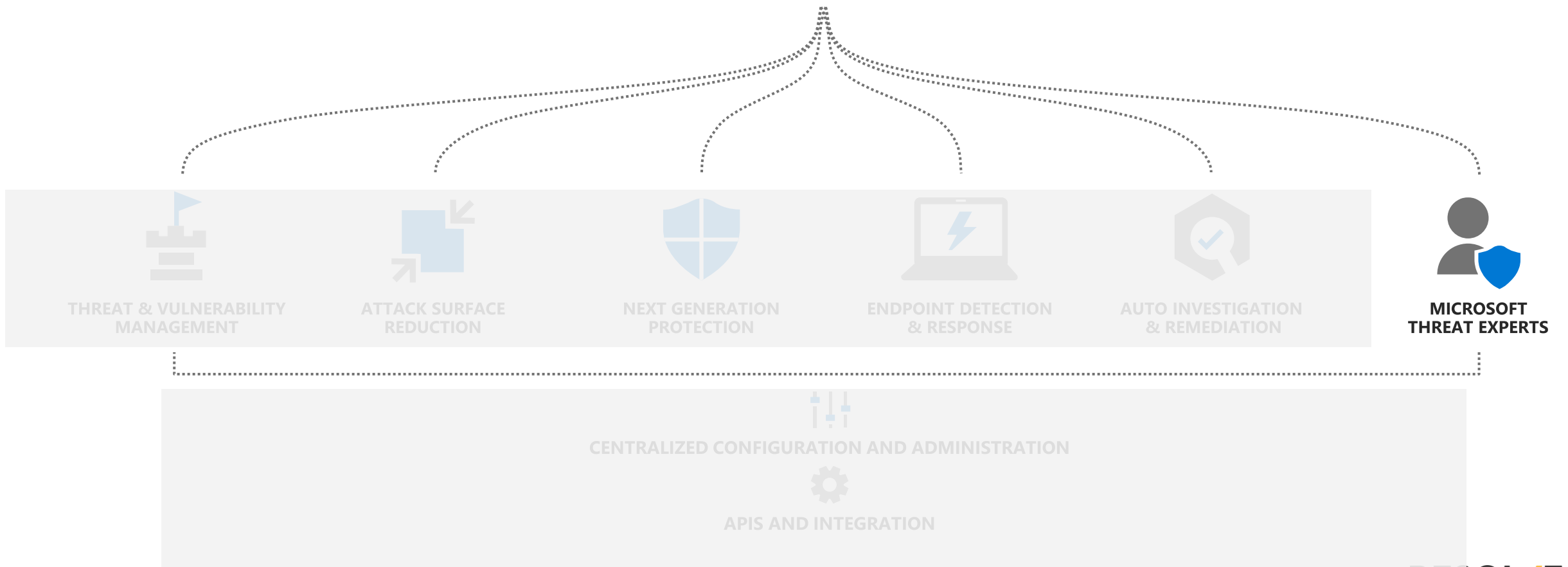
Analyst 2

/ Microsoft Defender for Endpoint





Microsoft Defender for Endpoint



/ Microsoft Defender for Endpoint

Microsoft Defender Security Center

File

Search Microsoft Defender ATP

Analyst@contoso.com

Alerts > Detection of file linked to adversary with supp...

Microsoft Threat Experts

BARIUM

Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Severity: High

Category: Execution

Detection source: Microsoft Threat Experts

Automated investigation is not applicable to alert type

Alert context

desktop-c7ud4hh

janedoe

First activity: 9.10.2019 | 23:43:38

Last activity: 9.10.2019 | 23:43:38

Description

Executive summary

This alert provides additional context for an alert you have received, [Windows Defender AV detected "Winnti" high-severity malware](#). We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action [here](#). While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

Timeline of observed events

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

Impacted machines

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f1508b76e9a22	Impacted machine 1

Recommended actions

Recommendation summary

- Fully investigate the machine in question
- Practice the principle of least-privilege a Restricting local administrative privileges
- Enforce strong, randomized local admini
- If you have any questions about this alert select 'Consult a threat expert'.
- If you need immediate help from Micros
- Examine the Indicators of Compromise (I

Indicators of Compromise

IOC

Install (2).exe [\[explore\]](#)

InstallConfig.exe [\[explore\]](#)

InstallLauncher.exe [\[explore\]](#)

881ba9b12040d4576b5e09de73e5eb33de2e [\[explore\]](#)

ab16cd1b09e5157791a568456a12659aae92 [\[explore\]](#)

131.107.147.82 [\[explore\]](#)

Microsoft Threat Experts - Trial

Your Experts on Demand trial version expires in 41 days from your Microsoft Threat Experts enrolment. Contact your Microsoft representative to get a full subscription.

Learn more about [Microsoft Threat Experts - Experts on Demand](#)

Consult a threat expert

Get Microsoft Threat Experts advice and insights about suspicious activities in your organization.

Ensure that the portal page for the alert or machine in question is in view while providing information for this inquiry.

Note: This and other relevant information will be shared with Microsoft Threat Experts to enable the best response to your inquiry.

Inquiry topic *

https://securitycenter.windows.com/alert/da637073841040265613_-882982118

Thank you for sending this Threat Expert alert. Can you help us investigate this threat further including whether you think we were targeted, and whether this and other machines in our company were compromised?

Email *

Enter the email address you'd like Microsoft Threat Experts to send their reply

Analyst@contoso.com

Submit

[Privacy statement.](#)

RESOL/E

03. AZURE SENTINEL

Modernizzare le operazioni di sicurezza con Azure Sentinel

Azure Sentinel

SIEM



Multi-cloud



Partnerships

Cloud native, any data, any entity



Cloud native



Any data



AI



Automation

Modernizzare il SOC con Azure Sentinel

THE INTELLIGENT, CLOUD-NATIVE SIEM



Scales to support your growing digital estate



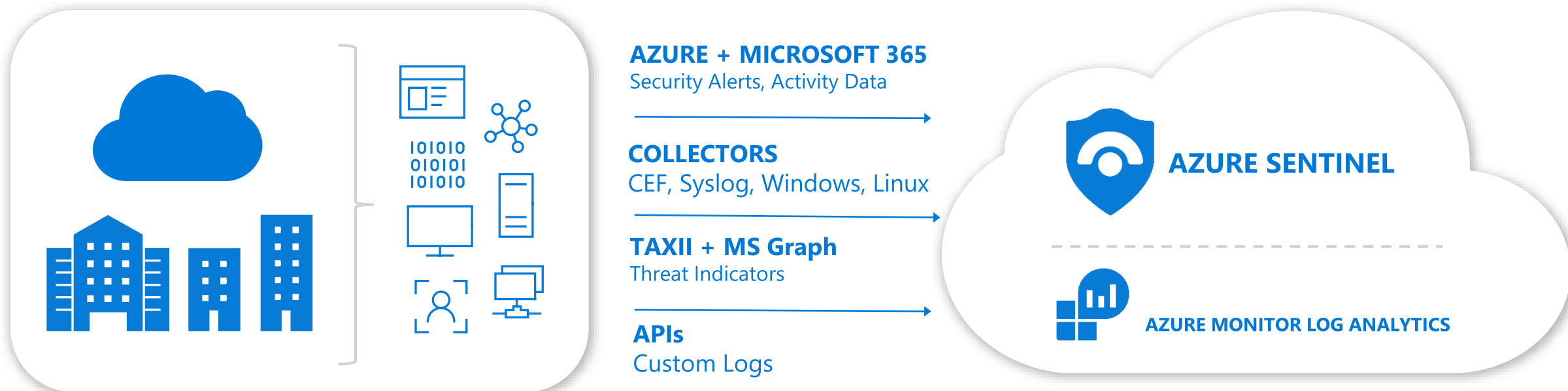
Offers improved threat detection



Uses AI and automation to increase efficiency



Raccogli i dati nel cloud da qualsiasi fonte





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

The screenshot displays the Microsoft Sentinel 'Active rules' page. At the top, there's a 'Create' button and a 'Refresh' button. A '51 Active rules' badge is shown. A 'RULES BY SEVERITY' bar chart indicates 12 High, 26 Medium, 9 Low, and 4 Informational rules. Below this, a search bar and filters for 'SEVERITY: All', 'TYPE: All', and 'TACTICS: All' are present. A table lists various rules, including 'Known Phosphorus group domains', 'Create incidents based on Azure Act...', 'Advanced Multistage Attack...', 'Create incidents based on A...', 'Create incidents based on Microsoft ...', 'Known Strontium group domains', 'Create incidents based on Azure Adv...', 'Suspect application consent', 'SharePointFileOperation via devices ...', 'Process execution frequency anomaly', 'Office policy tampering', 'Anomalous sign-in location by user ...', 'Brute force attack against Azure Portal', 'High count of failed logons by a user', 'SSH Potential Brute Force', 'Base64 encoded Windows process c...', 'Malformed user agent', and 'Rare high NXDomain count'. The 'Known Phosphorus group domains' rule is highlighted, showing it is 'IN USE', 'Scheduled', and requires 'DNS (Pr... +2)' data sources. A sidebar on the right provides details for this rule, including its description, required data sources (DNS (Preview), DnsEvents, VMConnection, Cisco ASA, CommonSecurityLog, Palo Alto Networks, CommonSecurityLog), tactics (Command and Control), and a KQL rule query. A 'Create rule' button is at the bottom of the sidebar.

Known Phosphorus group domains

High SEVERITY | **Scheduled DETECTION TYPE**

Description
Matches domain name IOCs related to Phosphorus group activity with CommonSecurityLog, DnsEvents and VMConnection dataTypes. References: <https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/>.

Required data sources

- DNS (Preview)
- DnsEvents
- VMConnection
- Cisco ASA
- CommonSecurityLog
- Palo Alto Networks
- CommonSecurityLog

Tactics

- Command and Control

Rule query

```
let timeframe = 1d;  
let DomainNames = dynamic(["yahoo-verification.org", "s  
accounts-web-mail.com", "customer-certificate.com", "se  
yahoo-verification.net", "yahoo-verify.net", "outlook-v
```

Create rule

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

Microsoft Azure (Preview) Report a bug Search resources, services, and docs (G+)

Home > Azure Sentinel > User Entity Behavior Analytics - CyberSecuritySoc

cybersecuritysoc

Entity	Score	Count	Entity ID	Entity Name
cboehmsa	0	0	1 e82b6fce-5774-4bde-9532-922a0f984ccf	cboehmsa@seccxp.ninja.onmicrosoft.com
sridhper@microsoft.com	0	0	1 Odd4a385-2ff9-4fcb-9798-f748c832b74a	sridhper@microsoft.com
aatpservice	0	0	2 699d5012-a2ff-4202-8751-640c869425bb	aatpservice@seccxp.ninja

Incidents Breakdown: Jeff@seccxp.ninja

Severity: All Status: All Owner: All

The query returned no results.

Anomalies Breakdown: Jeff@seccxp.ninja

Anomaly Name: All Tactic: All IP Address: Enter value Location: Enter value Uncommon For The User: <unset> Peers Uncommon Activity: <unset>

Search

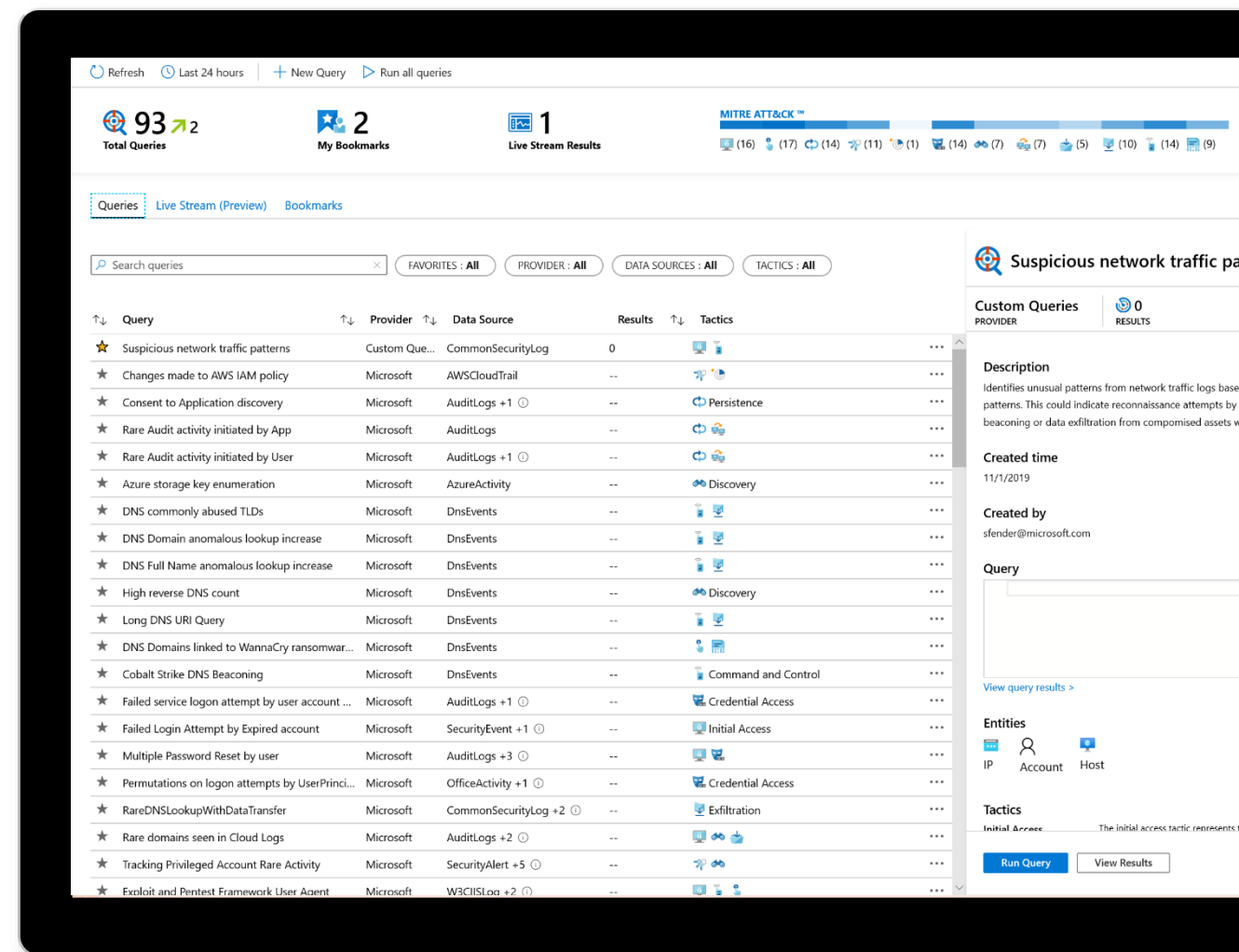
TimeGenerated	AnomalyName	Tactic	Technique	SubTechnique	Description	Username	UserPri
8/16/2020, 8:44:35 PM	Anomalous Geo Location Logon	Initial Access	Brute Force	Password Guessing	Adversaries may steal the credentials of a specific user or se	Jeff	Jeff@sec
8/16/2020, 8:53:21 PM	Anomalous Account Creation	Persistence	Create Account		Adversaries may create a cloud account to maintain access	Jeff	Jeff@sec
8/16/2020, 8:55:19 PM	Anomalous Role Assignment	Persistence	Account Manipulation		Adversaries may manipulate accounts to maintain access to	Jeff	Jeff@sec
8/17/2020, 14:27:08 PM	Anomalous Login to Device	Lateral Movement	Valid Accounts		Adversaries may steal the credentials of a specific user or se	Jeff	Jeff@sec
8/17/2020, 14:34:48 PM	Anomalous Resource Access	Lateral Movement	Remote Services	Remote Desktop Protocol	Adversary may be trying to move through the environment	Jeff	Jeff@sec



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





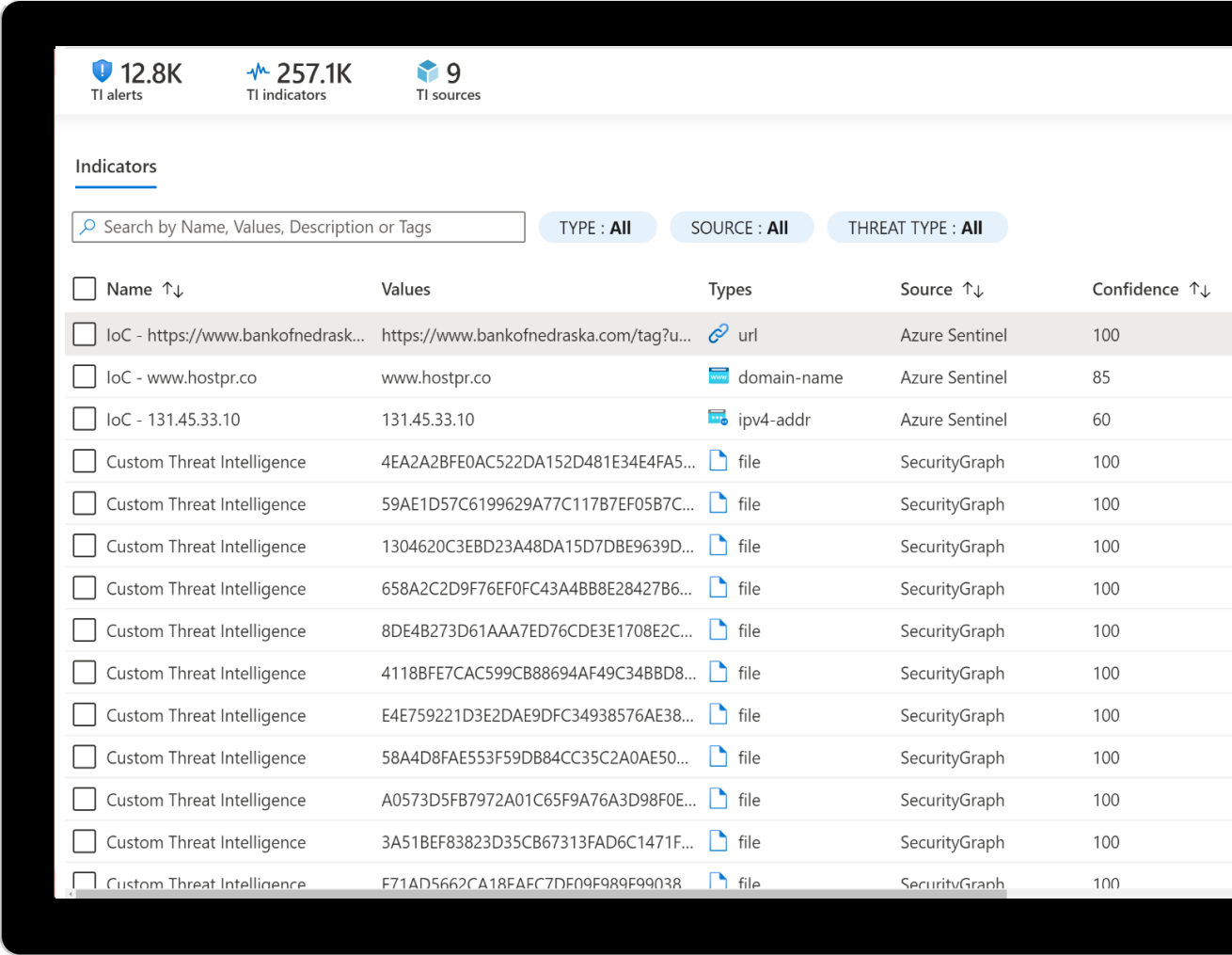
Intelligenza

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





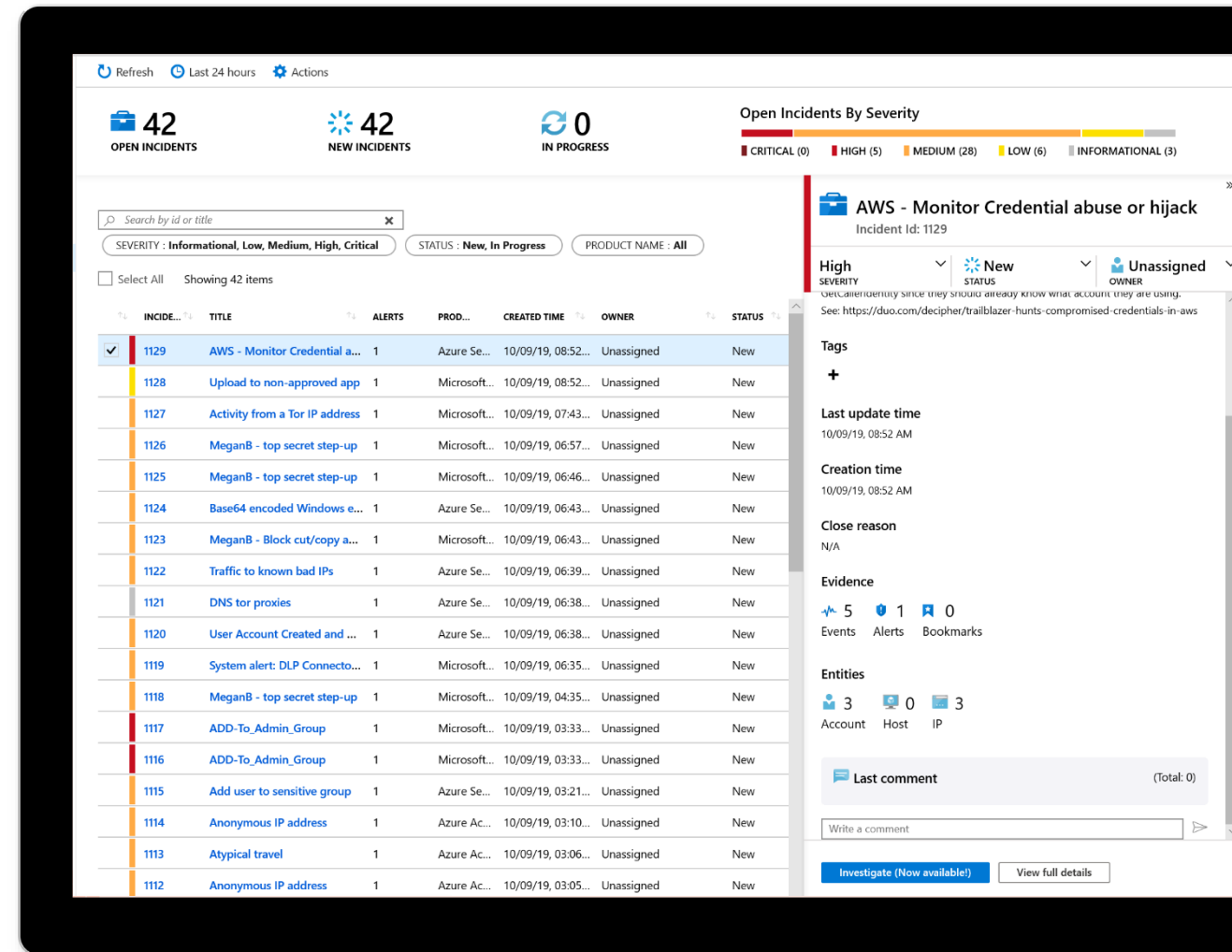
Avvia e monitora le indagini dagli incidenti di sicurezza processati e prioritari

Use incident to collect related alerts, events, and bookmarks

Manage assignments and track status

Add tags and comments

Trigger automated playbooks



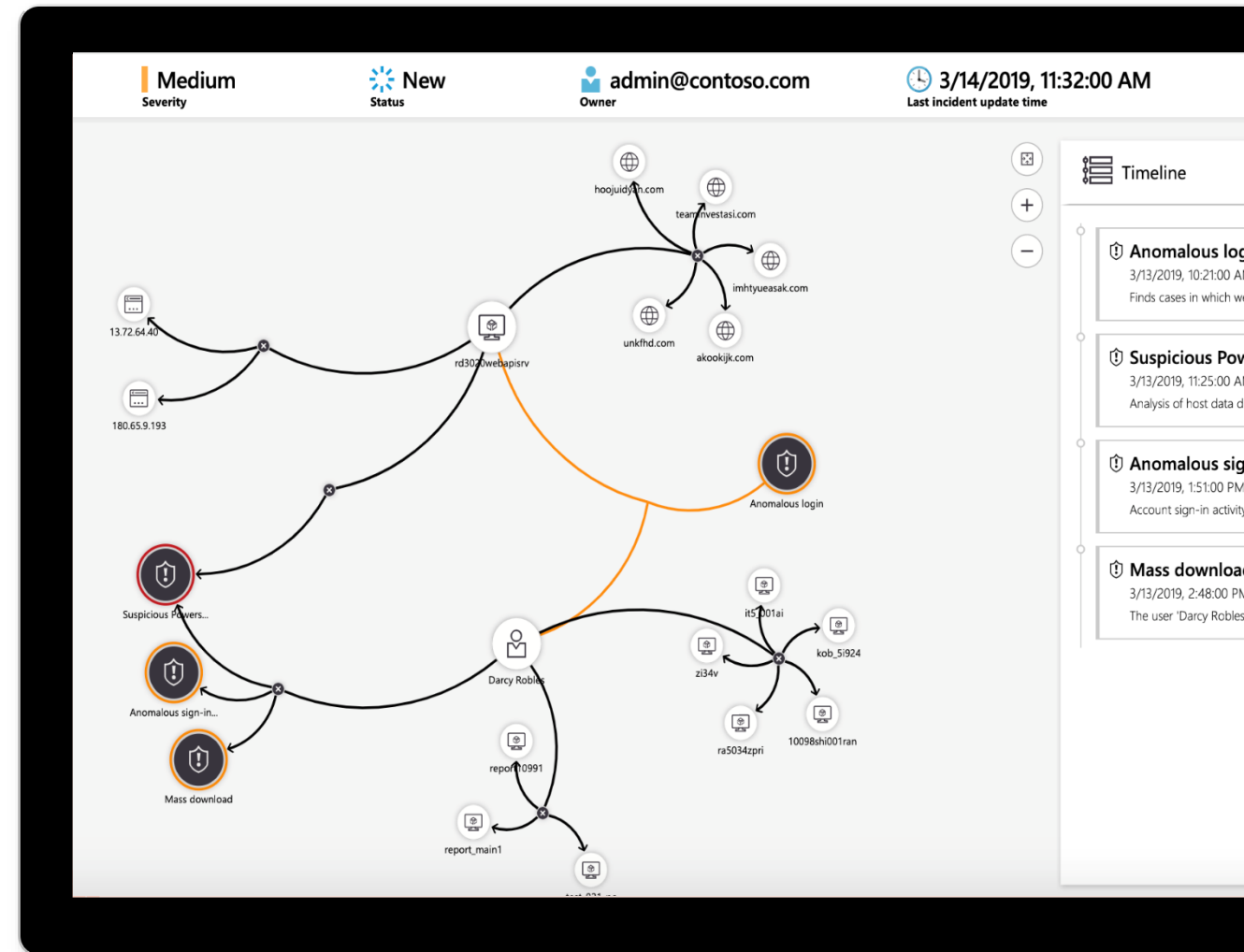
Visualizza l'intero attacco

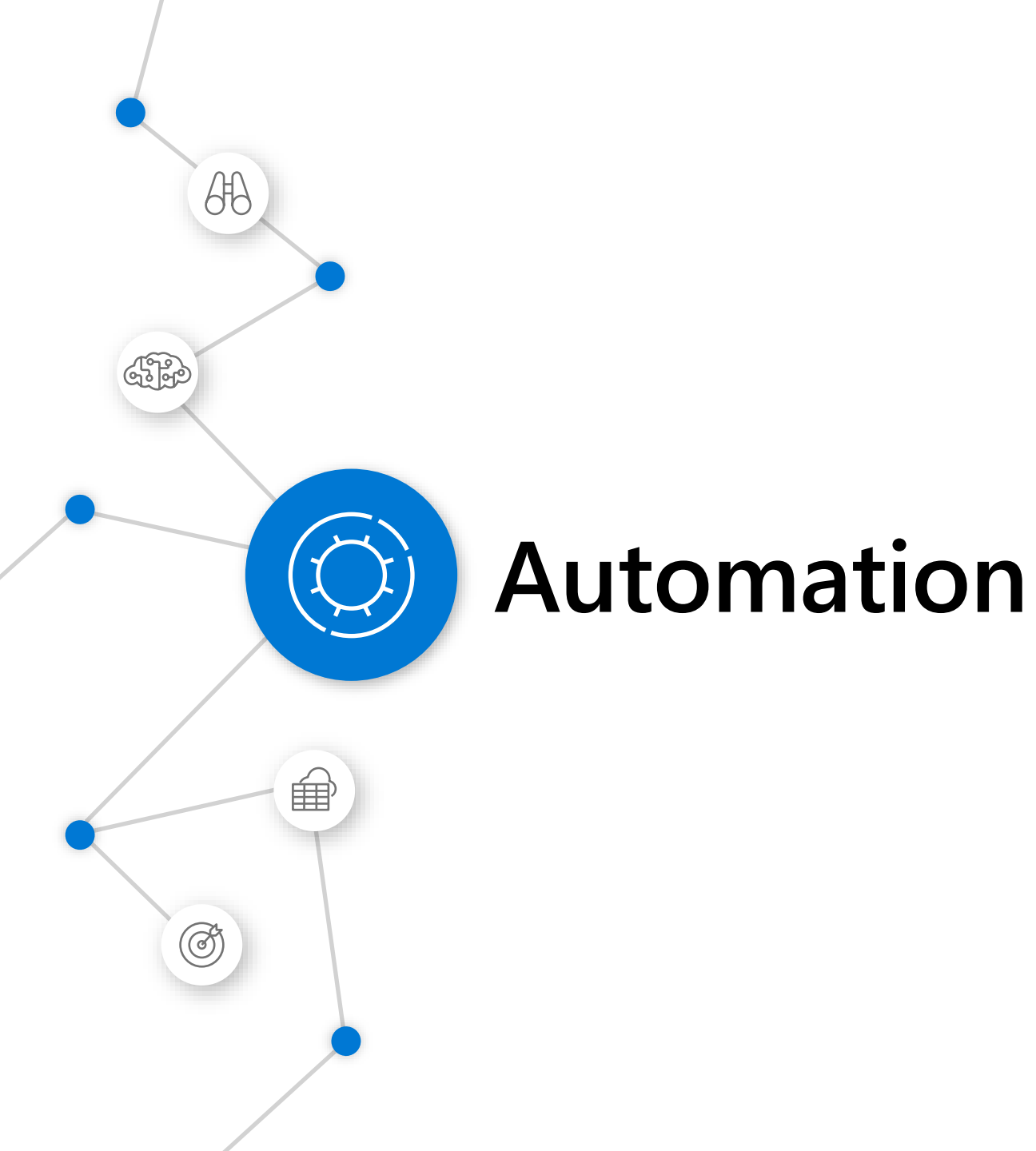
Navigate the relationships between related alerts, bookmarks, and entities

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





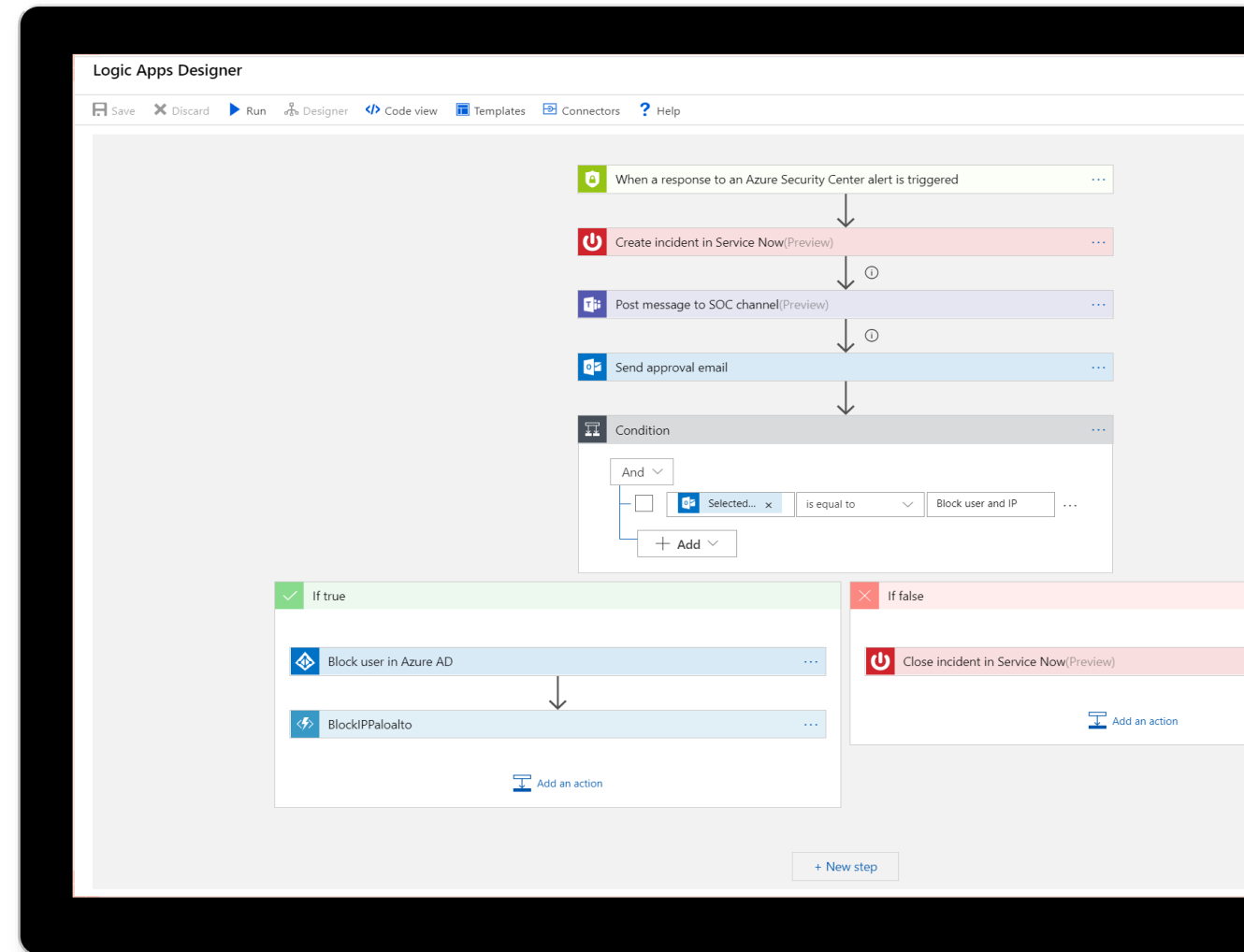
Automatizza e orchestra le operazioni di sicurezza usando le Azure Logic Apps

Build automated and scalable playbooks that integrate across tools

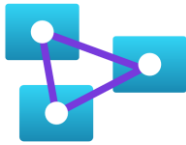
Choose from a library of samples

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

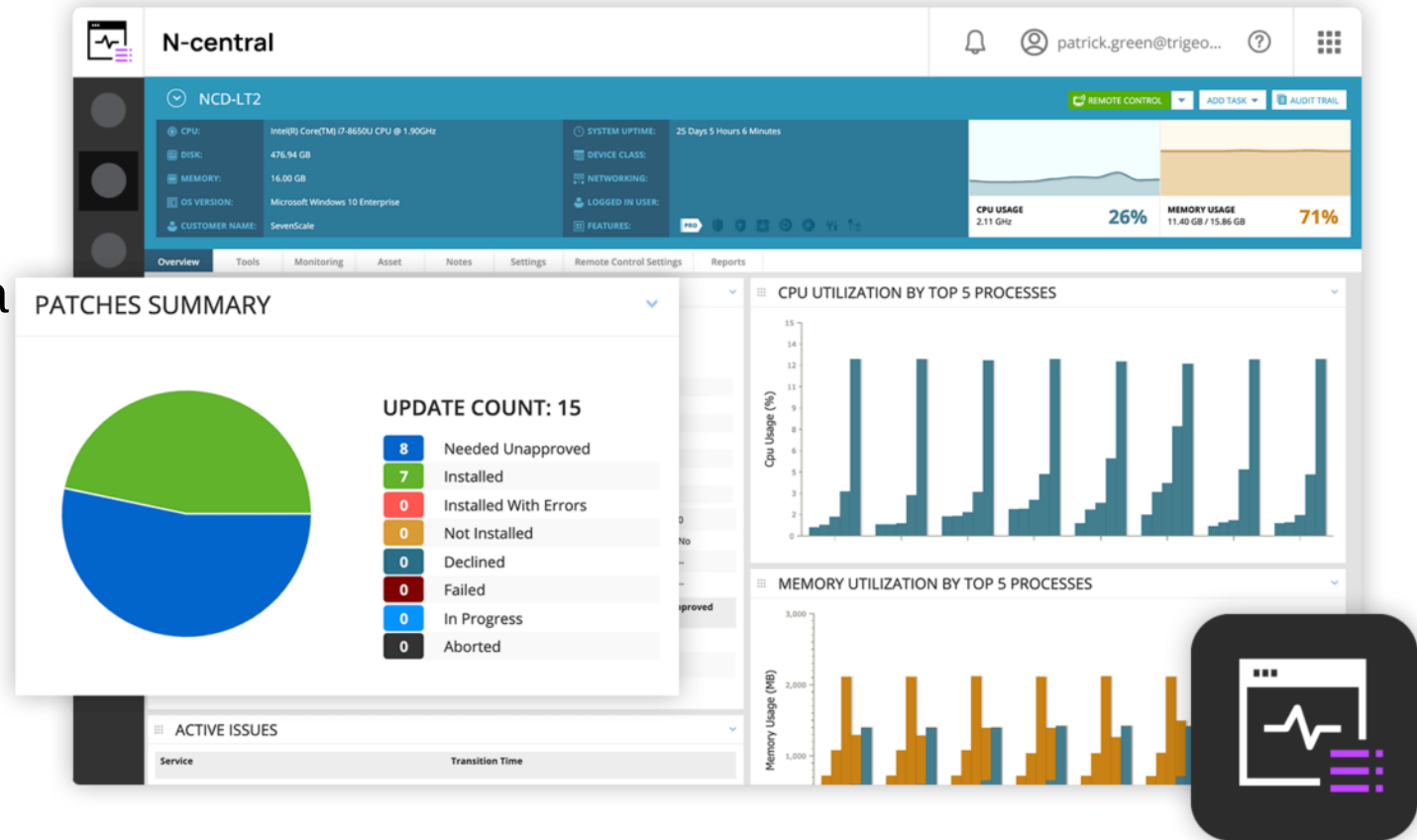
Block an IP Address
Block User Access
Trigger Conditional Access
Isolate Machine

04. N-CENTRAL

**Modernizzare il
monitoraggio della
propria infrastruttura**

/ N-Central

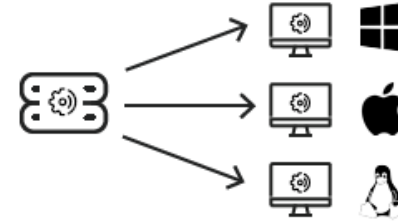
- Disponibile come soluzione on-premise o in hosting
- Visibilità e gestione semplificate ed efficienti da una singola dashboard
- Avvisi proattivi con funzionalità di riparazione automatica
- Potenti strumenti di automazione per la gestione globale o granulare



/ N-Central

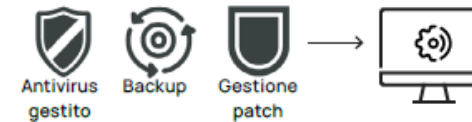
1 INTEGRAZIONE AUTOMATIZZATA

- 1 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.



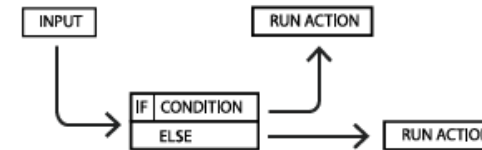
2 CONFIGURAZIONE AUTOMATIZZATA

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



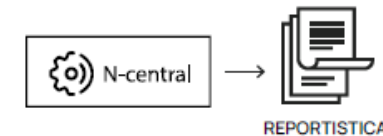
3 MANUTENZIONE AUTOMATIZZATA

- 3 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

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



/ N-Central

WALK2TALK_5525

Views

Active Issues

All Devices

Job Status

NetPath

Topology Maps

Dashboards

Device - ESX Hosts

Device - Network Devices

Device - Printers

Device - Servers

Device - Workstations

Manage - Antivirus

Manage - Patch Status

Manage Dashboards

Actions

Add/Import Devices

Add Customer

Domain User Management

Download Agent/Probe

Export Last Recovery Point

File Transfer

Patch Approvals

Push Third Party Software

ACTIVE ISSUES

ACKNOWLEDGE NOTIFICATIONS

EDIT DEVICES

DELETE SERVICES

SERVICE MONITORING

ADD NOTE

ADD TASK

EXPORT

Filter by No Filter in all Sites with all services

Customer	Site	Remote Control	Tools	Device/Probe	Device Class	Service	Status	Transition
☐	Ergon	--		SRVDPM1	Servers - Windows	Guest Status (Hyper-V) - SRV...		2021-Sep-2
☐	Ergon	--		SRVDPM1	Servers - Windows	Guest Status (Hyper-V) - SRV...		2021-Sep-2
☐	Ergon	--		SRVDPM1	Servers - Windows	Guest Status (Hyper-V) - SRV...		2021-Sep-2
☐	Ergon	--		SRVDPM1	Servers - Windows	Guest Status (Hyper-V) - Win...		2021-Sep-2
☐	Ergon	--		SRVDPM1	Servers - Windows	Memory		2021-Sep-2
☐	Ergon	--		SRVDPM1	Servers - Windows	Veeam Failed Jobs		2021-Sep-2
☐	Ergon	--		SRVGEN02	Servers - Windows	Windows UAC Status		2021-Sep-2
☐	Ergon	--		SRVGEN02	Servers - Windows	Disk - C:		2021-Sep-2
☐	Ergon	--		SRVGEN03	Servers - Windows	Memory		2021-Oct-0
☐	Ergon	--		SRVGEN03	Servers - Windows	Windows Backup		2021-Sep-2
☐	Ergon	--		SRVGENSQL2	Servers - Windows	SQL Memory Manager - MSS...		2021-Sep-2
☐	Ergon	--		SRVGENSQL2	Servers - Windows	SQL Memory Manager - NAV		2021-Sep-2
☐	Ergon	--		SRVGENSQL2	Servers - Windows	SQL Server - Buffer Manager...		2021-Oct-0

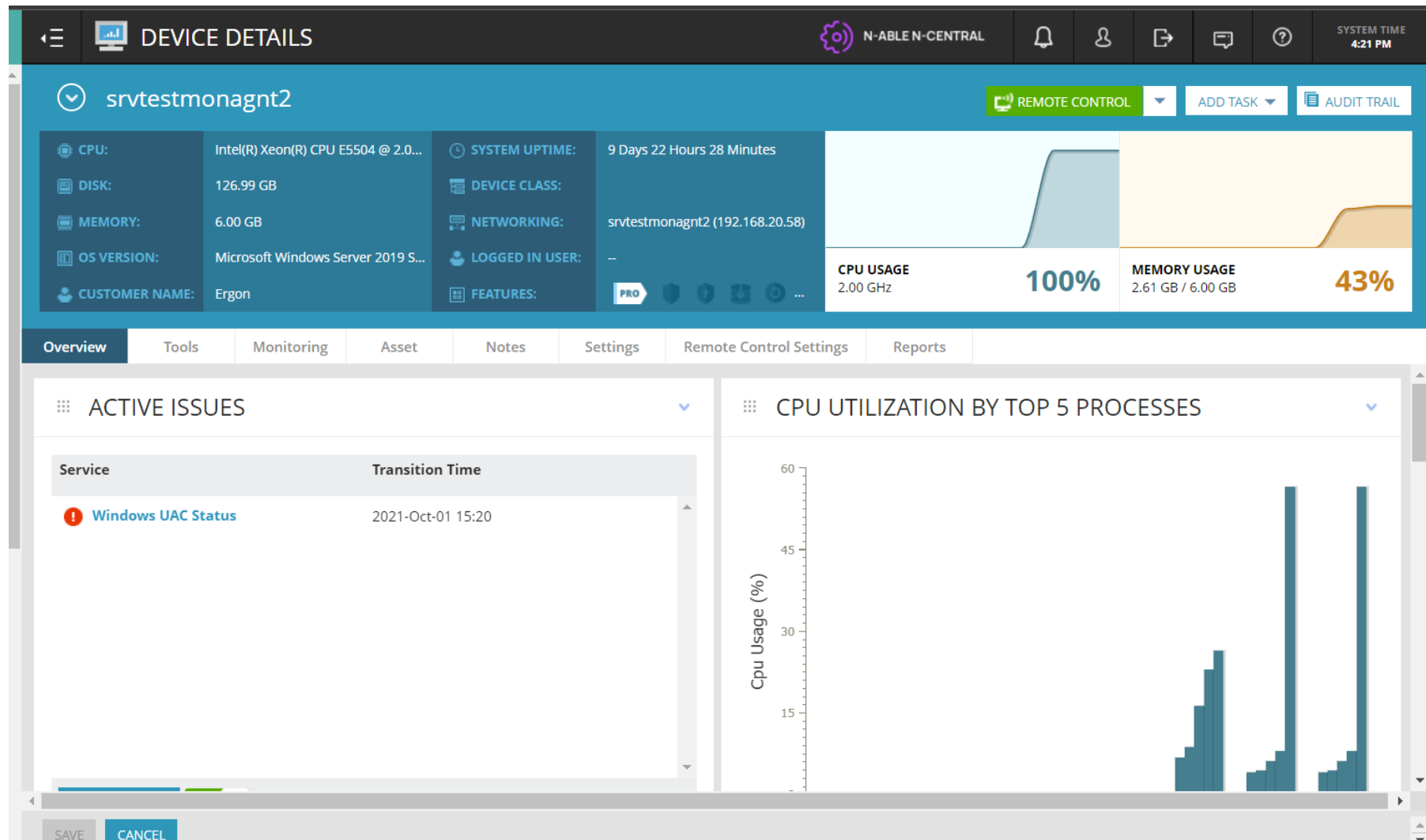
REFRESH NOW

ON

Refresh in: 10 minutes

Selected: 0 Total: 113

/ N-Central



/ N-Central

The screenshot displays the N-Central web interface for a device named 'srvtestmonagnt2'. The top navigation bar includes a back arrow, a device icon, the title 'DEVICE DETAILS', the N-ABLE N-CENTRAL logo, and various utility icons like a bell, user profile, share, chat, and help. The system time is shown as 4:22 PM.

The main content area features a header with a dropdown arrow, the device name 'srvtestmonagnt2', and buttons for 'REMOTE CONTROL', 'ADD TASK', and 'AUDIT TRAIL'. Below this, a dashboard provides key system information:

- CPU:** Intel(R) Xeon(R) CPU E5504 @ 2.0...
- DISK:** 126.99 GB
- MEMORY:** 6.00 GB
- OS VERSION:** Microsoft Windows Server 2019 S...
- CUSTOMER NAME:** Ergon
- SYSTEM UPTIME:** 9 Days 22 Hours 30 Minutes
- DEVICE CLASS:**
- NETWORKING:** srvtestmonagnt2 (192.168.20.58)
- LOGGED IN USER:** -
- FEATURES:** PRO, shield, lock, power, etc.

Two line graphs show usage trends: CPU usage (peaking at 78%) and memory usage (peaking at 40%). Below the graphs, specific usage values are listed: CPU usage is 2.00 GHz at 78%, and memory usage is 2.43 GB / 6.00 GB at 40%.

A horizontal menu below the dashboard includes tabs for Overview, Tools (selected), Monitoring, Asset, Notes, Settings, Remote Control Settings, and Reports. The 'Tools' tab is active, showing a sub-menu with Services, Processes, Registry, Applications, Startup Applications, Printers, Command Prompt, File System, and Task Execution. The 'Command Prompt' option is selected, displaying a terminal window with the following output:

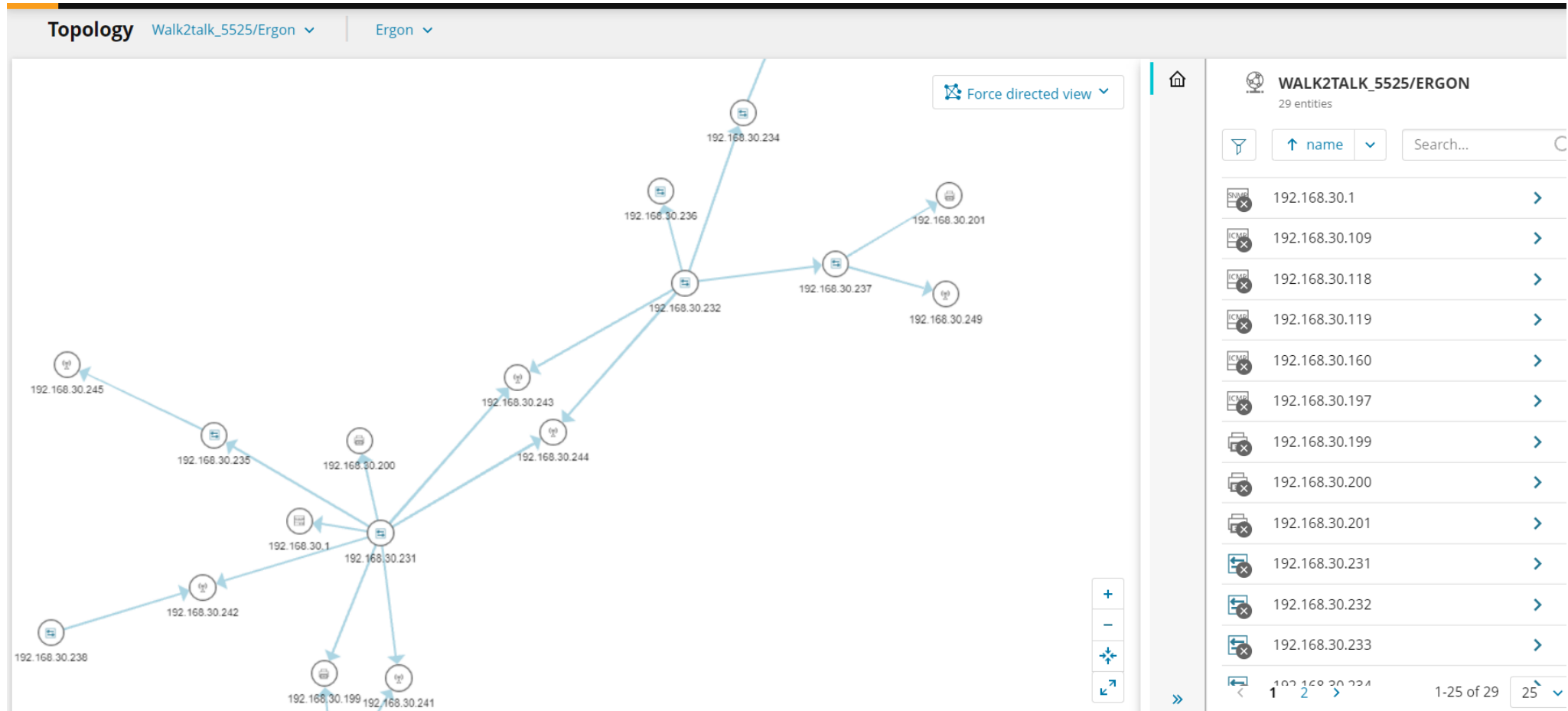
```
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : gruppogenesis.local
    Link-local IPv6 Address . . . . . : fe80::38e5:19ff:c0da:852%5
    IPv4 Address. . . . . : 192.168.20.58
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.1

C:\Windows\system32>
```

/ N-Central



/ N-Central

REPORTS - ASSET SITE

SYSTEM TIME
4:26 PM

Company Name: Demo

Report: Asset Site

Created on: 2021-Oct-04 16:25

ASSET SITE

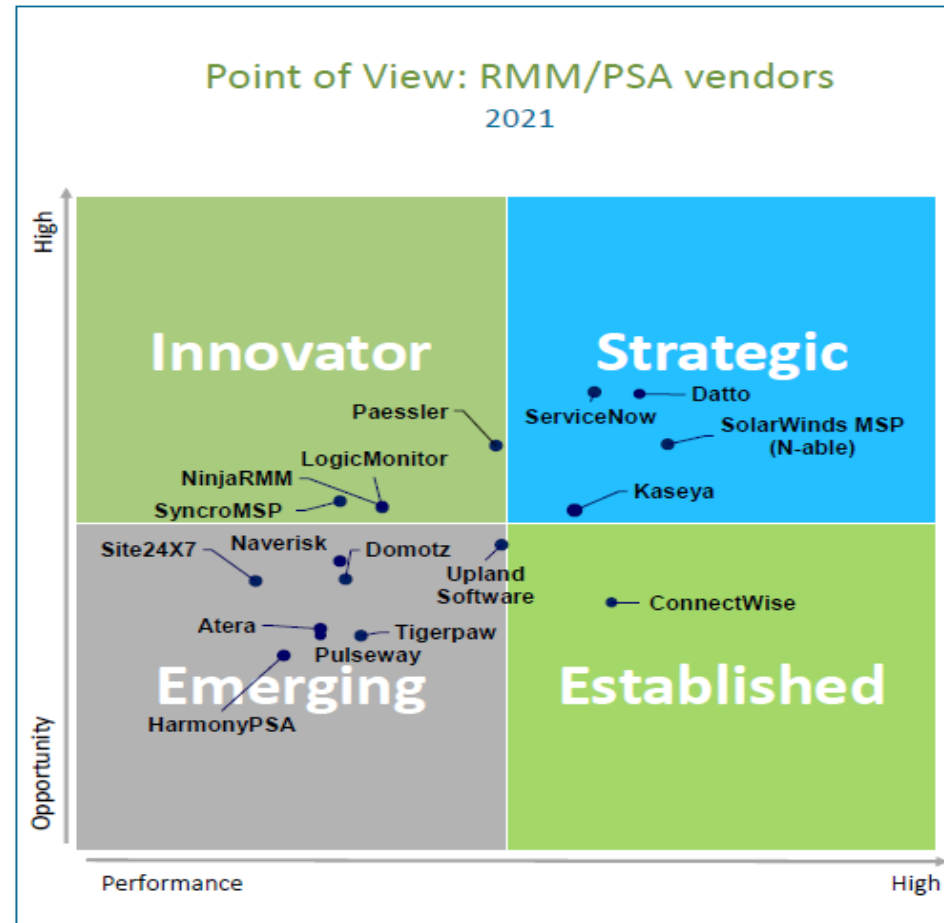
Site	Property	Description	Instances	Devices
--	Memory by amount	3.50 GB	3	vm-ubnt-1 vm-ubntcef VM-WINSERV2 vm-ubnt-1
--	Memory by amount	8.00 GB	3	vm-win10corso vm-winserv1 vm-win10-1
--	Operating system by version	Microsoft Windows 10 Pro	2	vm-win10corso vm-win10-1
--	Operating system by version	Ubuntu 18.04 LTS x64 Edition	1	vm-ubntcef
--	Operating system by version	Microsoft Windows Server 2019 Datacenter x64 Edition	2	VM-WINSERV2 vm-winserv1
--	Operating system by version	Other Operating System	1	vm-ubnt-1
--	Hard drives by capacity	< 100 GB	4	VM-WINSERV2 vm-win10corso vm-winserv1 vm-win10-1
--	Hard drives by capacity	100GB to 200GB	4	vm-winserv1 vm-win10-1 vm-win10corso VM-WINSERV2
--	CPU by speed	2290 MHz to 2390 MHz	4	vm-win10corso vm-winserv1 vm-win10-1

Total: 14

EXPORT

EMAIL

MSP tech stack



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. Cisco Meraki per una nuova rete Cloud Managed

01 Dicembre 2021

DIGITAL COMPLIANCE. Proteggi i dati della tua azienda

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

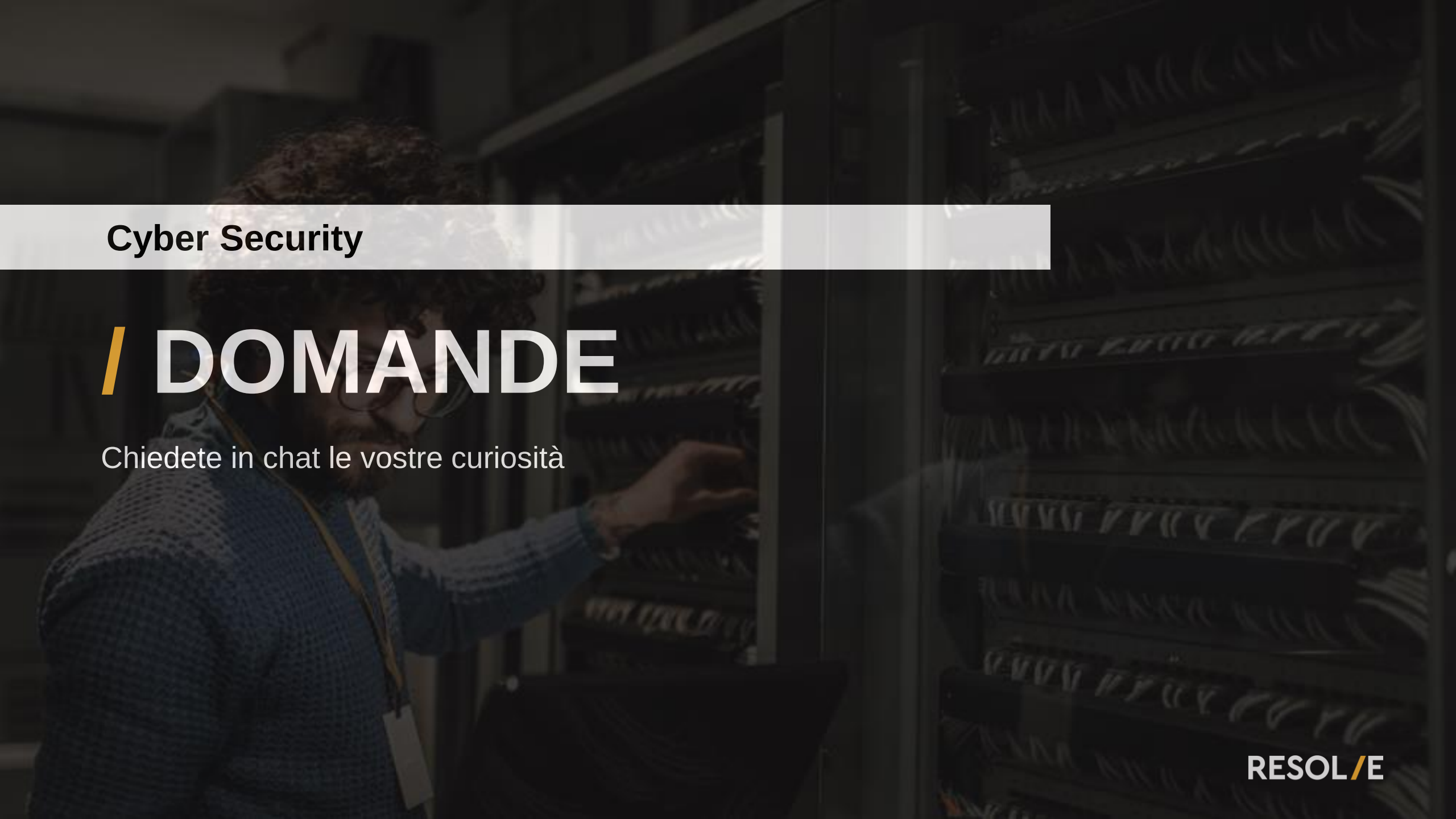
Managing Microsoft Teams - NOVEMBRE: 15-19-22-25-30

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

RESOL/E

by ErgonGroup