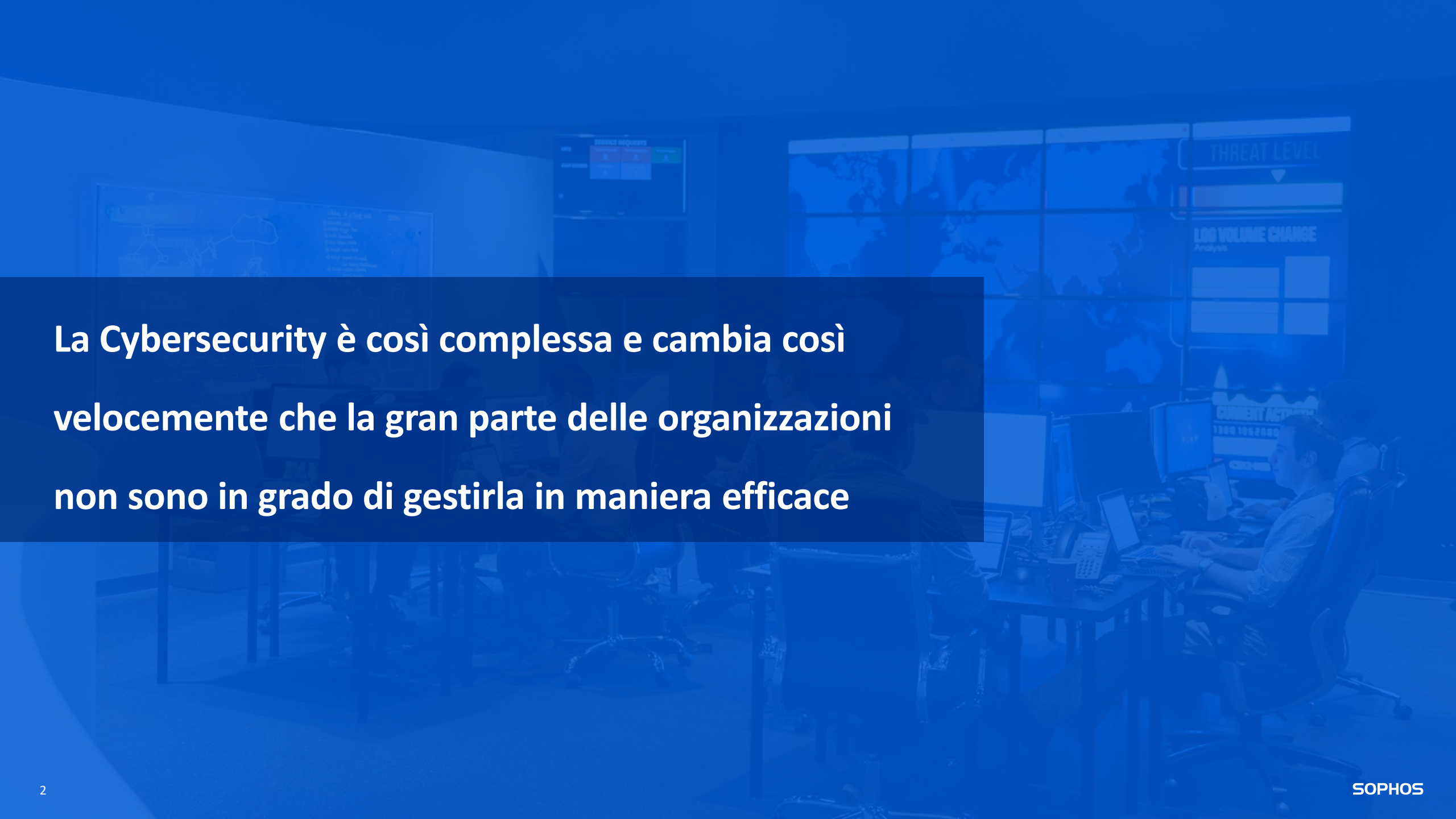
Npo SISTEMI
A RICOH COMPANY

SIMPLIFY
THROUGH
TECHNOLOGIES

SOPHOS

NPO SISTEMI ACADEMY - INNOVATION STATION

Protezione Senza Compromessi: Resilienza, Efficienza e Conformità con Sophos

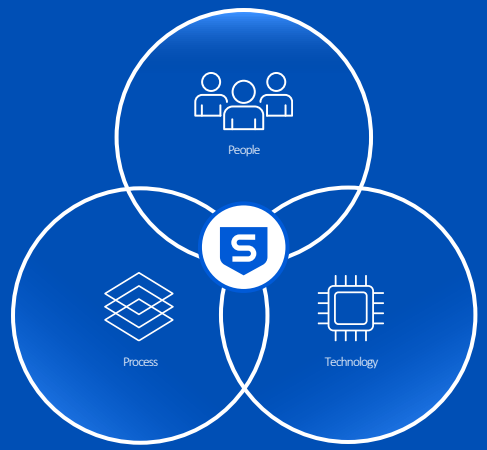


La Cybersecurity è così complessa e cambia così velocemente che la gran parte delle organizzazioni non sono in grado di gestirla in maniera efficace

Cybersecurity as a Service

MANAGED DETECTION AND RESPONSE

Risultati di sicurezza superiori forniti come servizio



- **Security Operations Center (SOC) istantaneo**
- **24/7 Threat Detection and Response**
- **Threat Hunting guidata da esperti**
- **Capacità di gestione completa dell'Incident Response**
- **Massimizza i risultati nella Cybersecurity**

Managed Detection and Response

Un servizio completamente gestito, 24 ore su 24,
7 giorni su 7, fornito da esperti specializzati nel rilevamento
e nella risposta agli attacchi informatici che le soluzioni
tecnologiche da sole non possono prevenire

SOPHOS

MDR – Design del servizio

Persone

Ho bisogno di un team di esperti per …

- Gestire completamente la risposta alle minacce
- Co-gestire la risposta alle minacce con il mio team
- Allertare il mio team sulle minacce da gestire

Processi

Le minacce identificate richiedono…

- Full-scale incident response: Minaccia debellata
- Contenimento, così che il mio team elimini la minaccia
- Analisi dettagliate con guida alla rimozione

Tecnologia

Voglio utilizzare…

- Sophos: miglior protezione, rilevamento e risposta
- Combinazione di strumenti Sophos e non Sophos
- Solo strumenti di terze parti

Visibilità

Rilevamento minacce usando i dati di…

- Endpoint
- Firewall
- Backup and Recovery
- Email
- Identity
- Public Cloud
- Network

Integrazioni incluse con le soluzioni Sophos, tra cui:

- XDR Sophos XDR
- Fw Sophos Firewall
- Em Sophos Email
- Mob Sophos Mobile
- Cld Sophos Cloud
- NDR Sophos NDR

Integrazioni Non-Sophos incluse nel servizio:

Qualsiasi soluzione di endpoint protection.
Microsoft 365 activity e MS Graph

Add-on disponibili in acquisto

Firewall
Email
Identity
Cloud
Network
Sophos NDR

SOPHOS

How We Sell Detection and Response Solutions

	Strongest Endpoint Protection	Detection and Response	Extendable with NDR and Integrations	24/7 Managed Service	Full-scale Incident Response
MDR	✓	✓ Sophos managed	✓	✓	✓
XDR — Sophos XDR license includes EDR features	✓	✓ Self-managed tools	✓		IR Retainer Add-on
Ep	✓				IR Retainer Add-on

MDR Service Insights: New Dashboard Widgets

New dashboard widgets highlight the human effort the Sophos MDR team undertakes on behalf of customers and partners

Threat hunt and intel effort

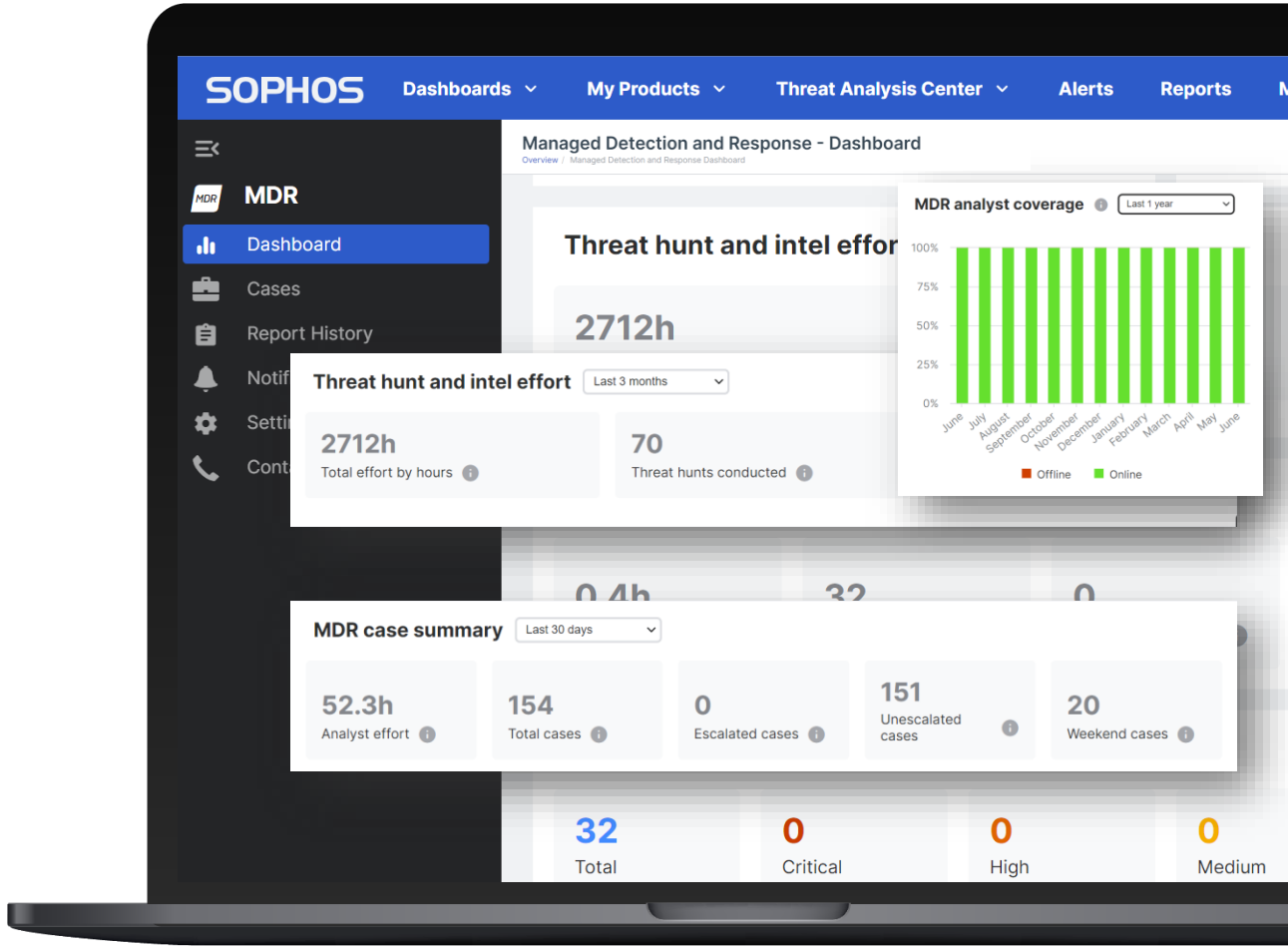
The combined effort of Sophos' threat hunting and intelligence teams proactively searching for threats and tracking adversary activities, including the number of threat hunts conducted and new detection rules created based on threat hunts

MDR case summary

The effort and time spent by MDR analysts conducting detailed investigations on the customer's detections and cases

MDR analyst coverage

Analysts' online status and availability in each 24-hour period, ensuring continuous coverage to protect customers 24/7

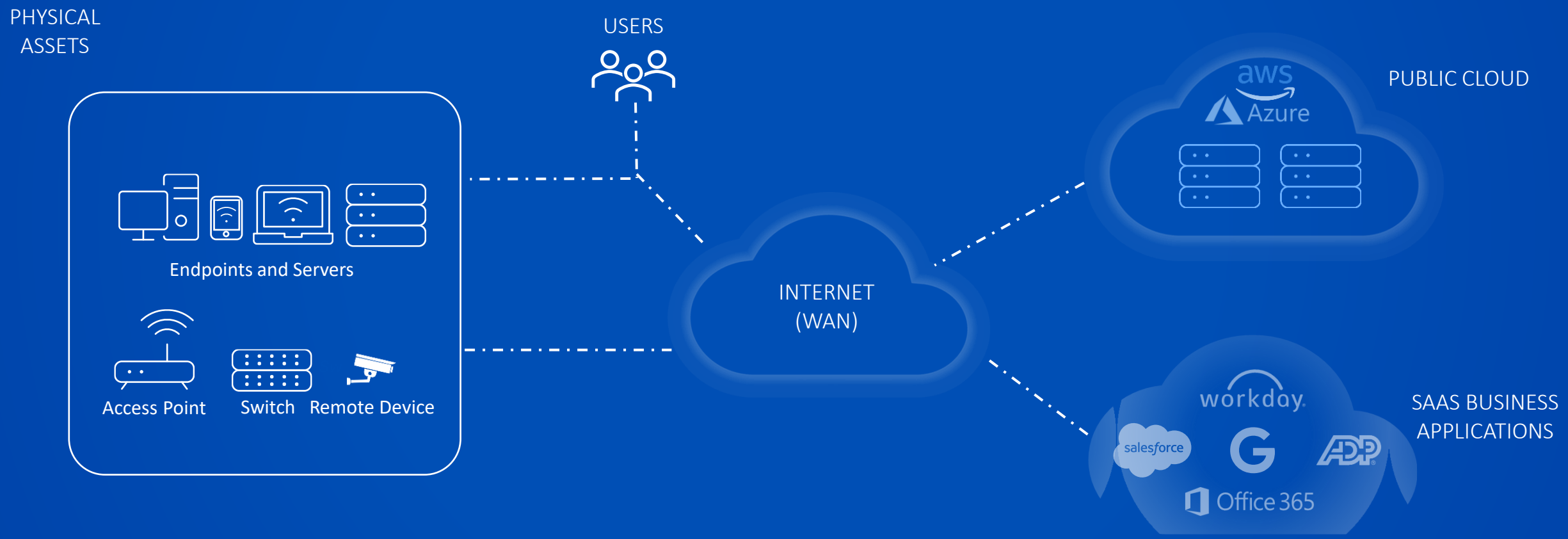


Visibilità

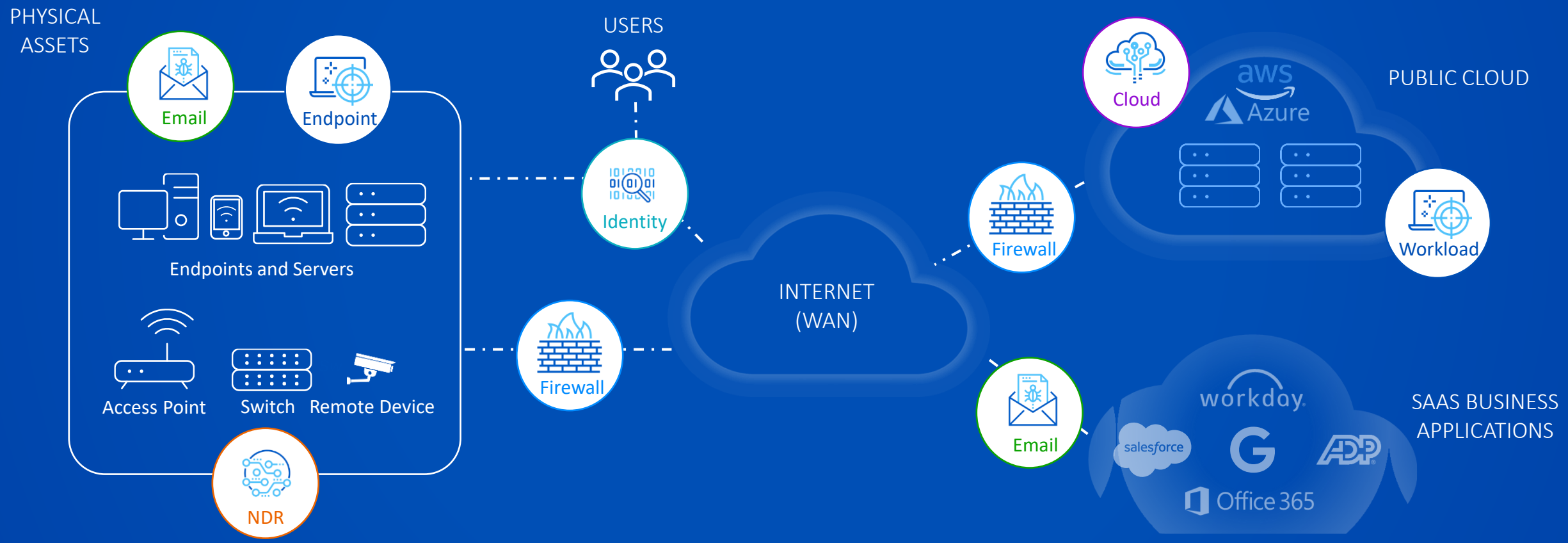
Elemento chiave per la threat detection

SOPHOS

L’infrastruttura IT è complessa e distribuita



Gli strumenti di sicurezza sono distribuiti all'interno dell'ambiente

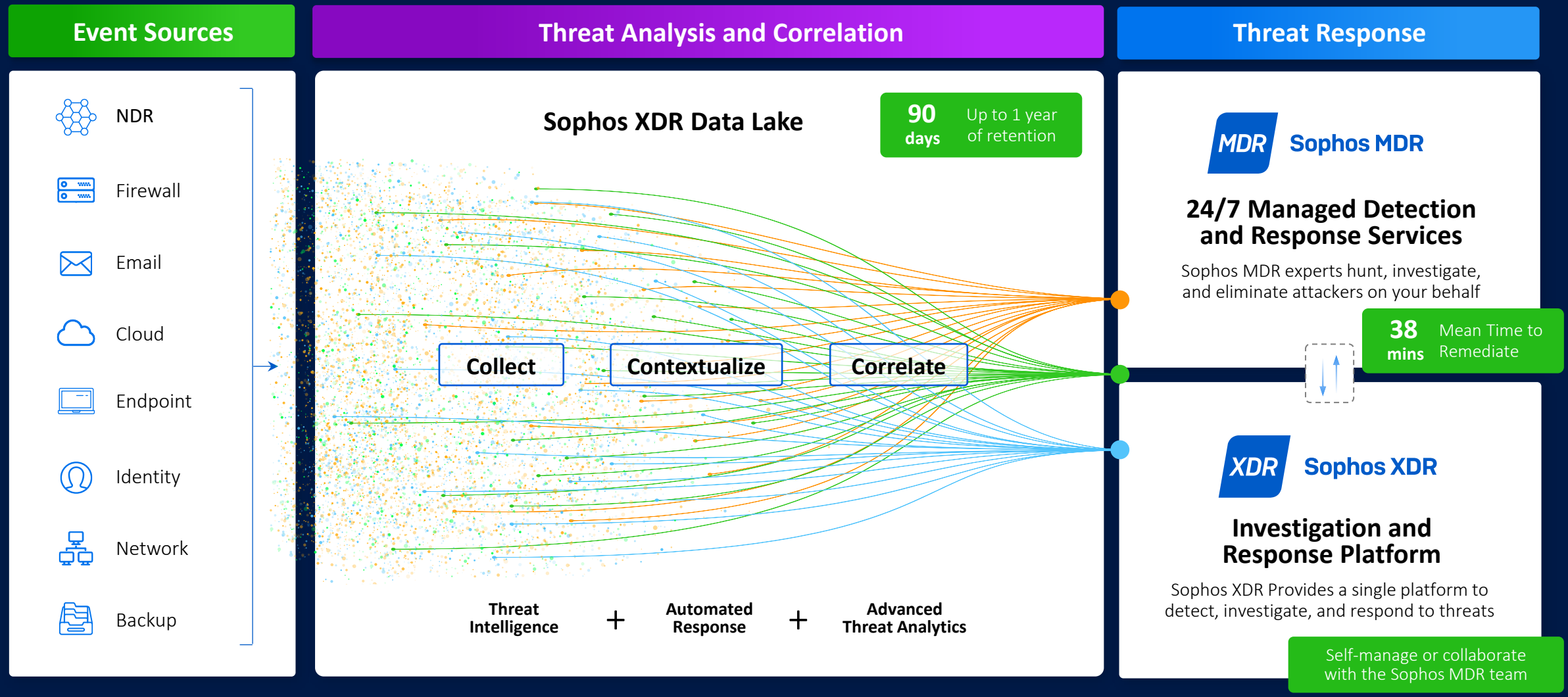


Value of Integrated Insights

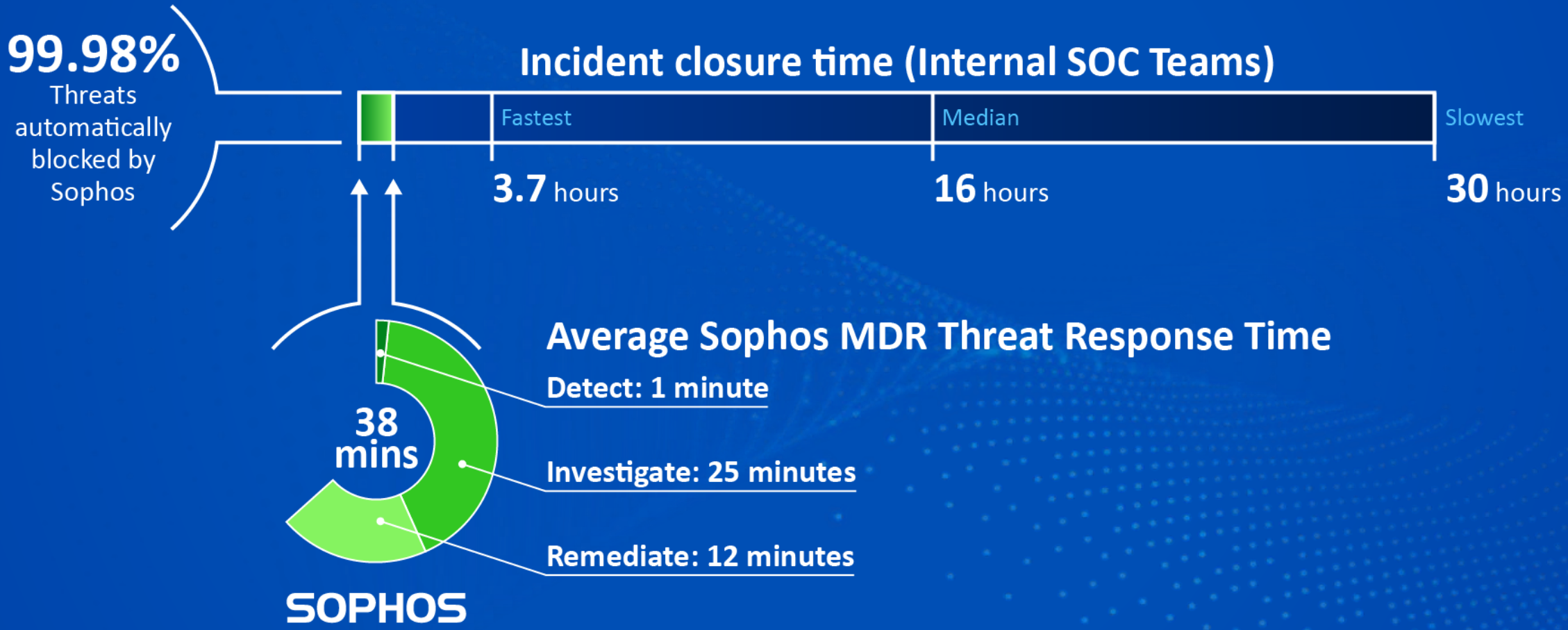
Top 5 MITRE Tactics discoverable with 3rd party telemetry

FIREWALLS	IDENTITY	EMAIL SECURITY	PUBLIC CLOUD	NETWORK
C&C	Credential Access	Initial Access	Persistence	C&C
Execution	Persistence	Persistence	Discovery	Execution
Discovery	Defence Evasion	Impact	Privilege Escalation	Initial Access
Initial Access	Initial Access	Collection	Initial Access	Discovery
Credential Access	Privilege Escalation	Execution	Credential Access	Exfiltration

Sophos Threat Detection and Response



Leading Detection and Response Times – Gartner benchmark



Sophos MDR

Creato dall'acquisizione di RookSecurity e DarkBytes

Lanciato nell'Ottobre 2019

+3.000.000 endpoint monitorati

7 centri MDR global Servizio 24/7 con contatti diretti

Include +500 esperti SophosAI, SophosLabs, Sophos MDR

Service Level Target

Tempo target per creazione caso	2 minuti dalla Detection
Tempo target per le azioni di risposta	30 minuti dalla creazione del caso

Incremento medio mensile dei clienti MDR	1000
MDR Dati medi elaborati al giorno	38.420.700.453
MDR Media dei rilevamenti al giorno	358.360.119
MDR Media manuale gestita dal cacciatore di minacce, casi al giorno	357
MDR Media di escalation al risponditore di minacce al giorno	47
MDR Media minacce attive gestite al giorno	1
Tempo medio di chiusura dell'incidente	38 min
Gartner Peer Insight review Tasso MDR (1-5)	4,8
Posizionamento su analista G2 per soluzioni Endpoint Protection, EDR, XDR, Firewall e MDR	Leader

Sophos protegge oltre 630,000 clienti su oltre 121 paesi

Sophos MDR Mission

Sophos MDR garantisce la massima serenità, grazie alla consapevolezza di poter contare sull'aiuto di un team composto da esperti di threat hunting, analisi delle minacce e capacità di risposta agli incidenti di sicurezza

30,000+ Clienti MDR

99.98% delle minacce bloccate in automatico*

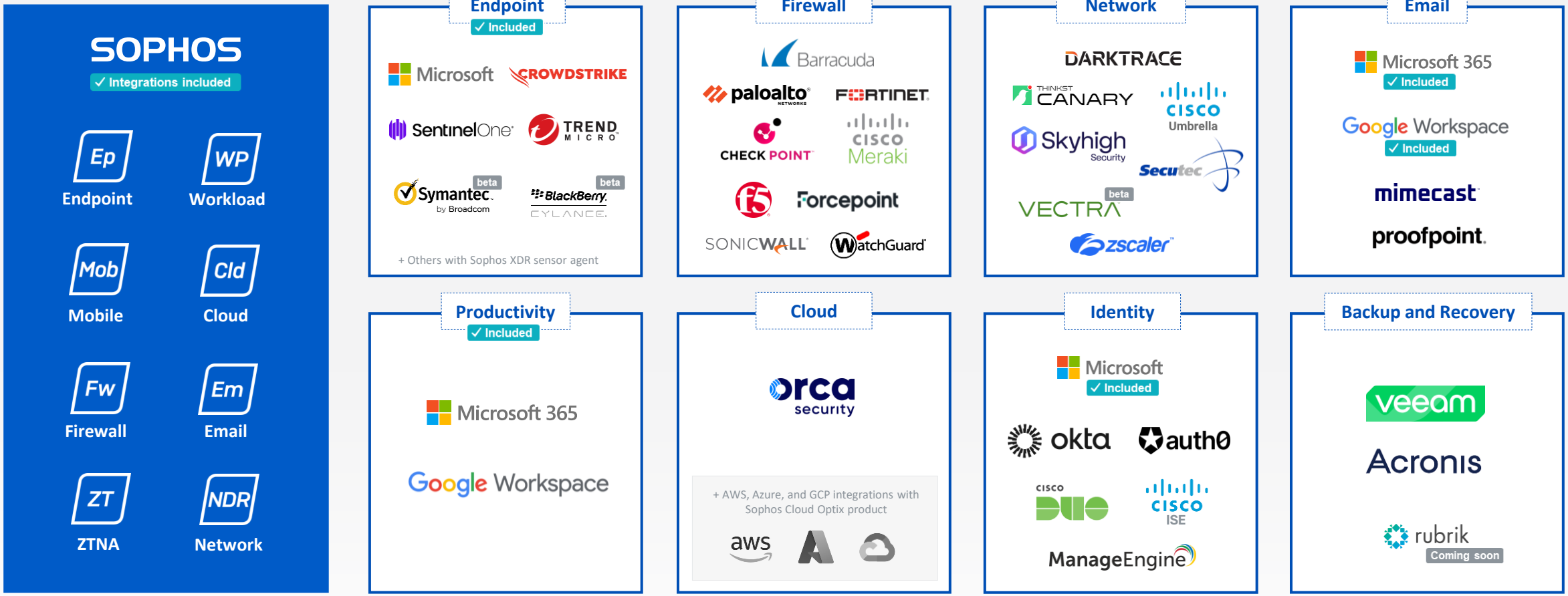
Media dei tempi di risposta del servizio MDR

Tempo Rilevamento	Meno di 1 Minuto
Tempo Investigazione	Meno di 25 Minuti
Tempo Risposta	Meno di 12 Minuti

Incident Response inclusa senza extra costi* con MDR complete

SOPHOS

Visibility Across All Key Attack Surfaces



Sophos Endpoint and Sophos Workload Protection solutions are included with Sophos XDR and MDR. Other Sophos integrations require an applicable subscription for the Sophos product.

Third-party Endpoint, Microsoft, and Google Workspace integrations are included with Sophos XDR and MDR subscriptions at no additional charge. Integration Packs for other non-Sophos solutions are available as add-on subscriptions for each integration category. Licensing is based on the total number of users and servers.

Updated July 9, 2024


SOPHOS
Secureworks®

Portfolio Expansion

Endpoint Protection
Sophos Endpoint provides more options and new opportunities

Identity Threat Detection and Response (ITDR)
Taegis identity detections enhance Sophos detection and response

Extended Detection and Response (XDR)
Taegis XDR benefits from the scale and diversity of Sophos telemetry

Security Advisory Services
Expanded set of advisory services is delivered by elite teams of experts

Managed Detection and Response (MDR)
World-class MDR services that address every security operations use case

Exposure Management
Taegis VDR and VMS complement Sophos Managed Risk

Security information and event management (SIEM)
Next-Gen SIEM for security operations and regulatory compliance

Network Detection and Response (NDR)
iSensor and Sophos NDR provide options for any use case

Included Integrations

Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and third-party integrations.

Sophos Firewall

Monitor and filter network traffic to stop threats before they have a chance to cause harm. Xstream Protection subscription required.

Microsoft Security Suite

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP
- Office 365 Management Activity

Sophos Endpoint

Endpoint Prevention and EDR that stop advanced threats and detect malicious behaviors—including attackers mimicking legitimate users.

Sophos Network Detection and Response

Continuously monitor activity inside your network to detect suspicious actions and lateral attacker movement.

Google Security Suite

- Google System Defined Rules
- Suspicious Activities
- Malware and Phishing
- User and Device Activity
- Alert Center
- Authentication
- Access Control
- Data Control

Sophos Cloud Optix

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform.

Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks.

Third-Party Endpoint Protection

Compatible with...

- Microsoft
- CrowdStrike
- SentinelOne
- Symantec (Broadcom)
- Trend Micro
- BlackBerry (Cylance)

+ Other solutions with the Sophos XDR sensor agent

Includes 90 days of data retention

Add-Ons

Firewall

Compatible with...

- Barracuda
- Check Point
- Cisco
- F5
- Forcepoint
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard

Identity

Compatible with...

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft integration included

Cloud

Compatible with...

- Orca Security

Integrations with AWS, Azure and GCP are available via the Sophos Cloud Optix product, sold separately

Network Security

Compatible with...

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

Email

Compatible with...

- Mimecast
- Proofpoint

Microsoft 365 and Google Workspace integrations included

Backup and Recovery

Compatible with...

- Acronis
- Veeam

Data retention

1-year retention add-on

Sophos Managed Risk

Powered by Tenable

Add-on service for Sophos MDR

Integration Packs and the Data Retention Pack are available for Sophos MDR and Sophos XDR. All Integration Packs are licensed based on the total number of Sophos MDR/XDR seats (users+servers).
Sophos Managed Risk is available as an add-on service for Sophos MDR only.

SOPHOS

Microsoft - Custom Platform Detections Based on Audit Logs

Microsoft Security Event Sources

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- O365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity (6.1k MDR, 5.1k XDR)
- Non-Microsoft Telemetry Sources

UNIFIED AUDIT LOGS

Microsoft Platform Detections

Inbox Rules

- Special characters in the rule name
- Moving emails to suspicious folders + mark as read
- BEC keywords (subject/email body)
- 6 character or less rule name, delete and mark as read

Suspicious

- Application consent
- User-agent strings

Impact

- Disabling Unified Audit Log ingestion

Session

- Multiple suspicious chrome user agent strings
- Multiple OS user agent strings

Extend MS Graph API

- MS-SEC-GRAPH-UNFAMILIAR-SIGN-IN-PROPERTIES
- MS-SEC-GRAPH-ANONYMOUS-IP-ADDRESS

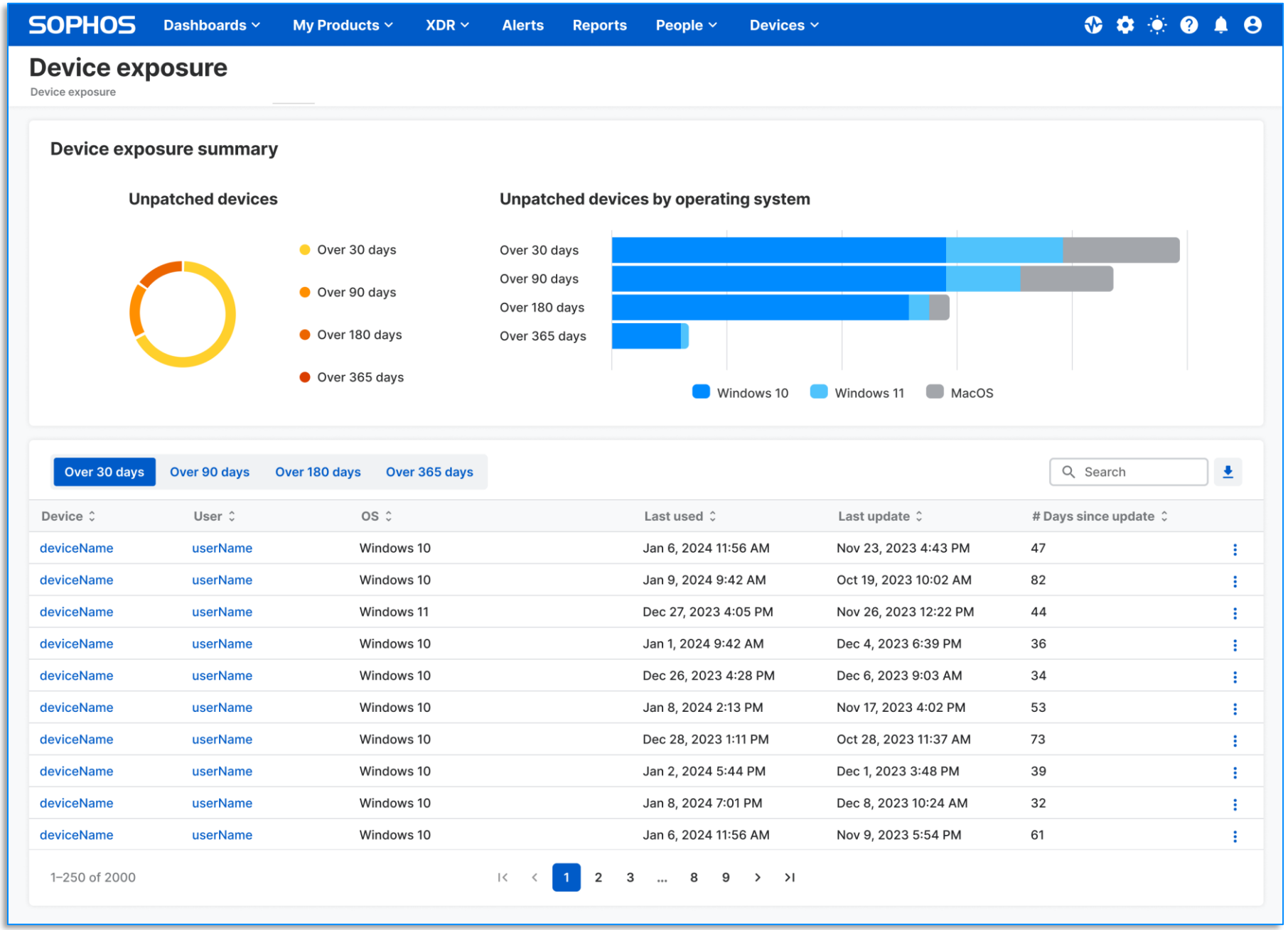
SAAS-M365

- Transport-rule-external-RedirectMessageTo-or-BlindCopyTo (not case creating)
- Authentication-OfficeHome-Sus-Linux-Chrome-UserAgent

Device Exposure and Managed Risk

Device Exposure will be included at no extra cost for XDR and MDR customers

	Product Offering **Device Exposure**	Service Offering **Managed Risk**
Highlight missing OS patches	✓	✓
Leverage X-Ops threat insight	✓	✓
Customer reports/visualizations	✓	✓
OS and application vulnerabilities		✓
Risk prioritization		✓
Build vs Partner	Build	Powered by Partner
Licensing	XDR, MDR	Add-on license
Sales Motion	• Deflect key sales objections • On-ramp for Managed Risk	• Competitive feature sure • Extensive estate visibility


SOPHOS
Dashboards
My Products
XDR
Alerts
Reports
People
Devices
Device exposure
Device exposure
Device exposure summary
Unpatched devices
Over 30 days
Over 90 days
Over 180 days
Over 365 days
Unpatched devices by operating system
Over 30 days
Over 90 days
Over 180 days
Over 365 days
Windows 10
Windows 11
MacOS
Over 30 days
Over 90 days
Over 180 days
Over 365 days
Search
Device
User
OS
Last used
Last update
Days since update
deviceName userName Windows 10 Jan 6, 2024 11:56 AM Nov 23, 2023 4:43 PM 47
deviceName userName Windows 10 Jan 9, 2024 9:42 AM Oct 19, 2023 10:02 AM 82
deviceName userName Windows 11 Dec 27, 2023 4:05 PM Nov 26, 2023 12:22 PM 44
deviceName userName Windows 10 Jan 1, 2024 9:42 AM Dec 4, 2023 6:39 PM 36
deviceName userName Windows 10 Dec 26, 2023 4:28 PM Dec 6, 2023 9:03 AM 34
deviceName userName Windows 10 Jan 8, 2024 2:13 PM Nov 17, 2023 4:02 PM 53
deviceName userName Windows 10 Dec 28, 2023 1:11 PM Oct 28, 2023 11:37 AM 73
deviceName userName Windows 10 Jan 2, 2024 5:44 PM Dec 1, 2023 3:48 PM 39
deviceName userName Windows 10 Jan 8, 2024 7:01 PM Dec 8, 2023 10:24 AM 32
deviceName userName Windows 10 Jan 6, 2024 11:56 AM Nov 9, 2023 5:54 PM 61
1–250 of 2000
1
2
3
...
8
9

Sophos Managed Risk | Use Cases

Powered by tenable

1 | ATTACK SURFACE VISIBILITY

Mitigate risk by knowing precisely what you own

2 | CONTINUOUS RISK MONITORING

Extend your team with vulnerability experts

3 | PRIORITIZE VULNERABILITIES

Understand which vulnerabilities to fix first

4 | IDENTIFY NEW RISKS FAST

Know when new critical exposures affect your apps

PHASE 1

External Attack Surface Management (EASM)

- Scans identify vulnerabilities impacting internet-facing assets, services, and apps
- Available as an add-on for Sophos MDR customers only, later this year also for XDR

PHASE 2

Internal Attack Surface Management (IASM)

- Scans identify vulnerabilities impacting assets within the organization's network such as servers and endpoints
- Available as an add-on for Sophos MDR customers only, later this year also for XDR
- Will be included as free upgrade for Managed Risk purchaser

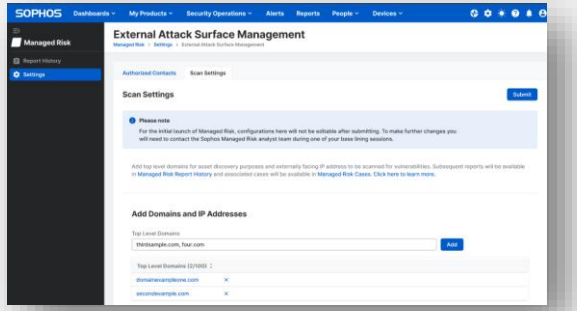
Sophos Managed Risk

Powered by tenable

Quick and easy on-boarding

Guided setup gets you up and running in minutes

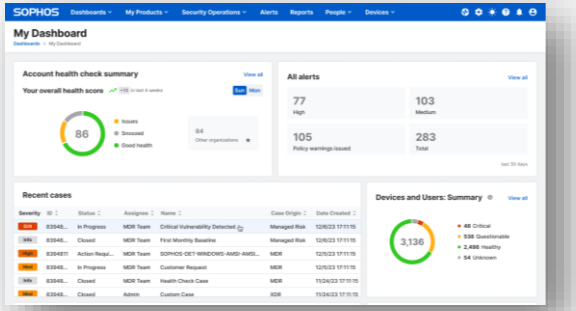
1. Provide authorized contact details
2. Enter external IP addresses and domain names
3. Specify day and time for weekly scan
4. Schedule baseline review with the Sophos team



Integrated with Sophos MDR

Fully managed service delivered by threat experts

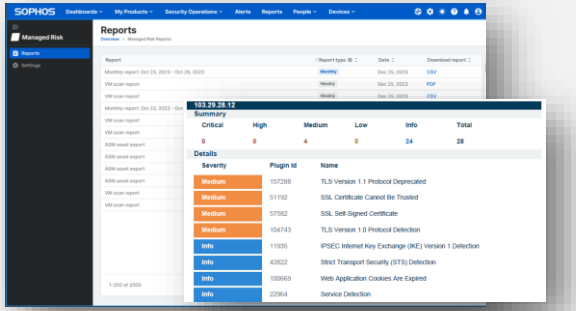
- Schedule reviews with Sophos Managed Risk
- Auto-created cases for **critical vulnerabilities**
- Create cases to discuss with Sophos Managed Risk
- Cases visible alongside MDR in Sophos Central's Threat Analysis Center



Comprehensive engagment

Access to vulnerability data in Sophos Central

- Detailing your discovered internet-facing assets
- Vulnerabilities prioritized based on risk to your organization
- Links to vulnerability documentation for further information and remediation guidance
- Monthly executive summary reports and meetings

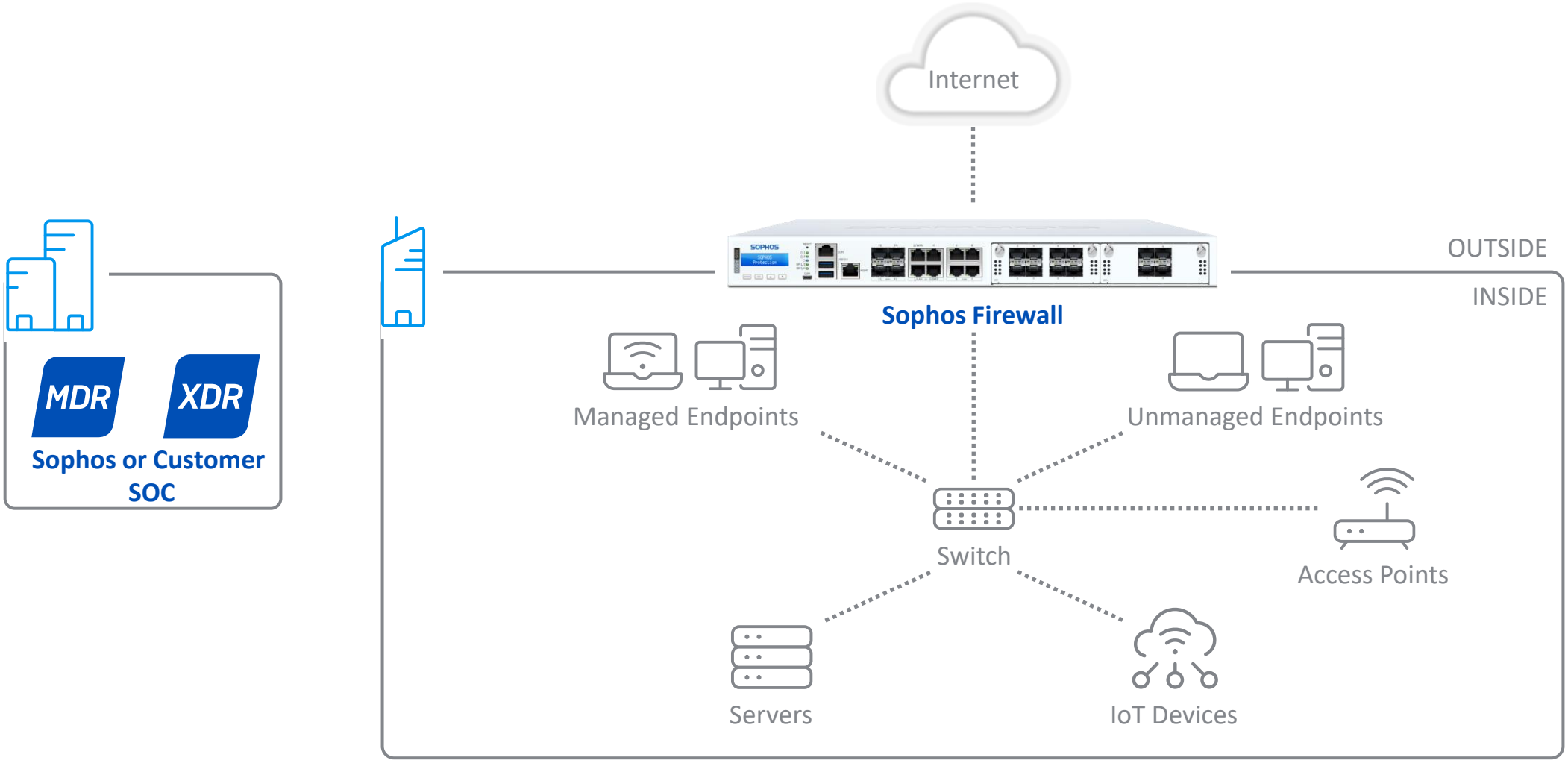


Network Threat Response

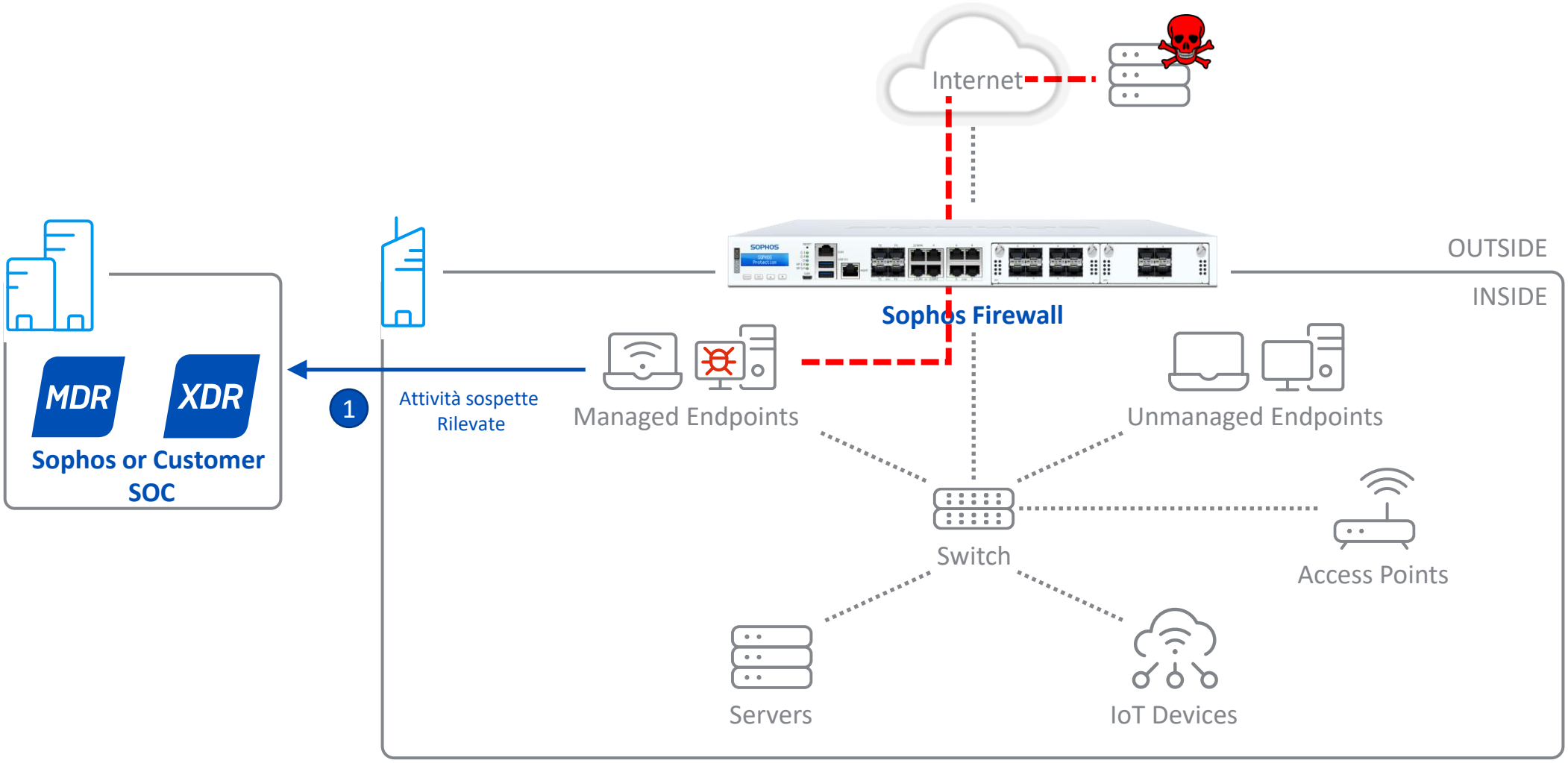
Se l’attacco arriva da un dispositivo non gestito?

SOPHOS

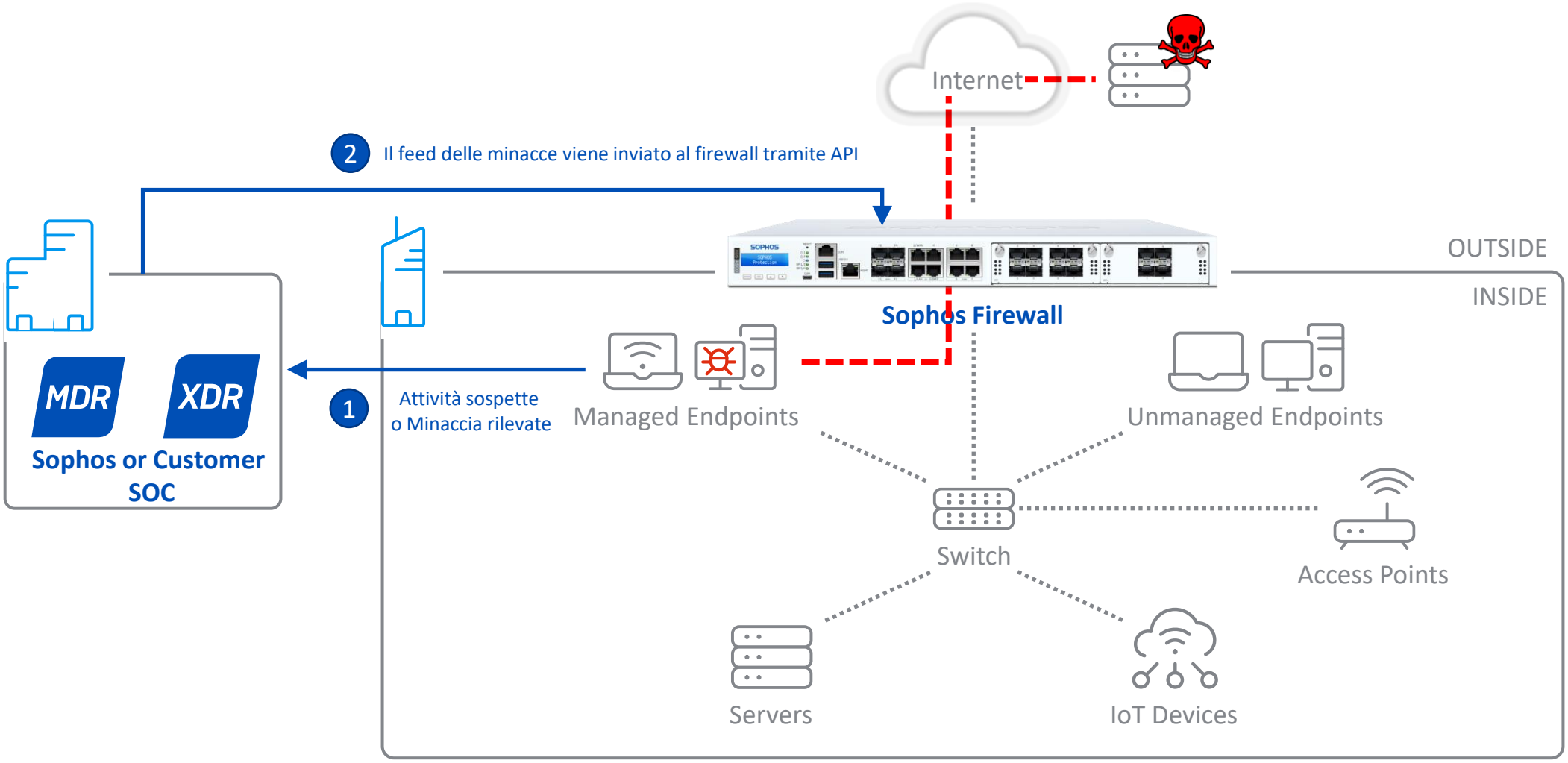
Active Threat Response in Azione (SFOS V20 release)



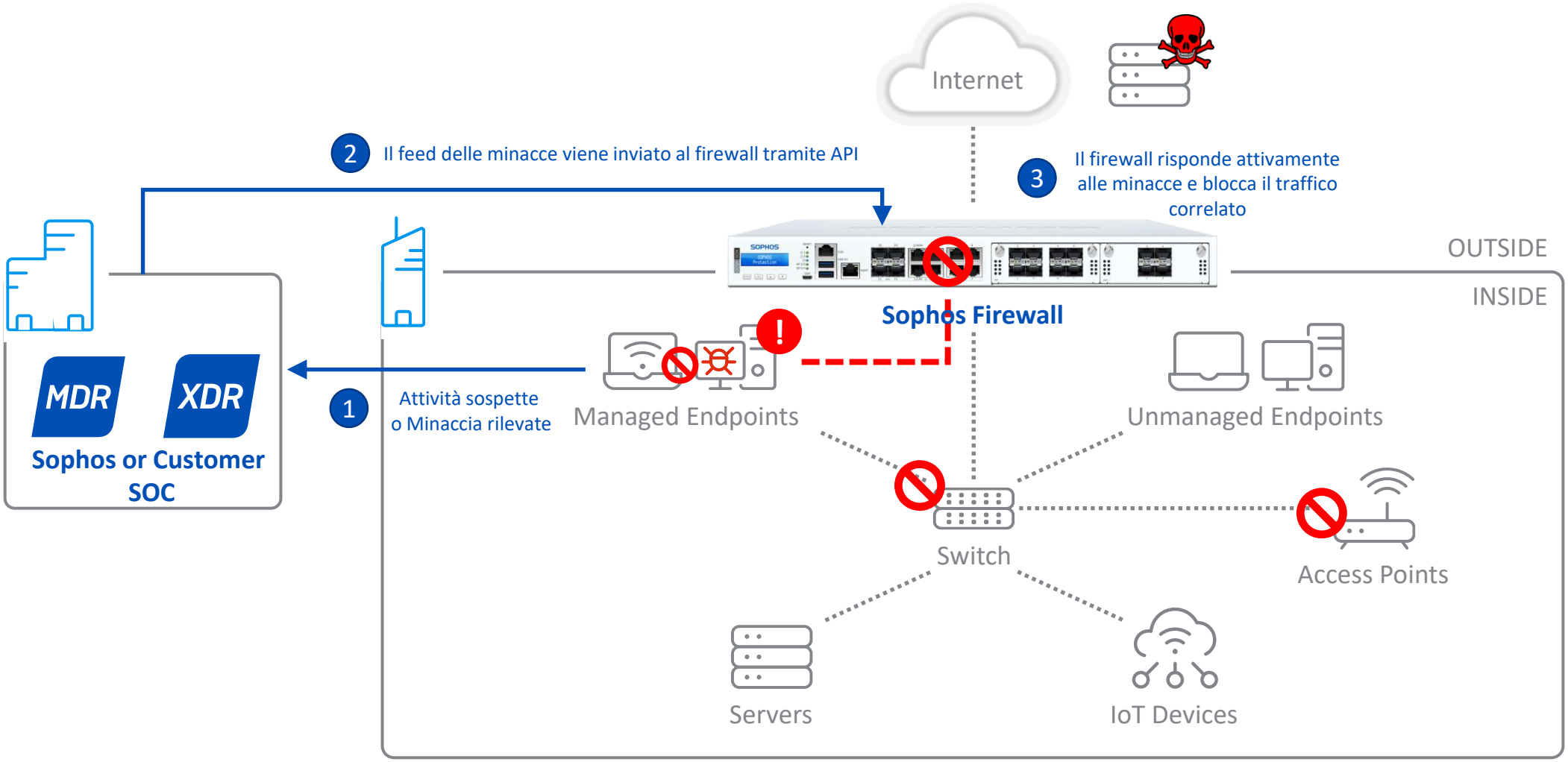
Active Threat Response in Azione



Active Threat Response in Azione

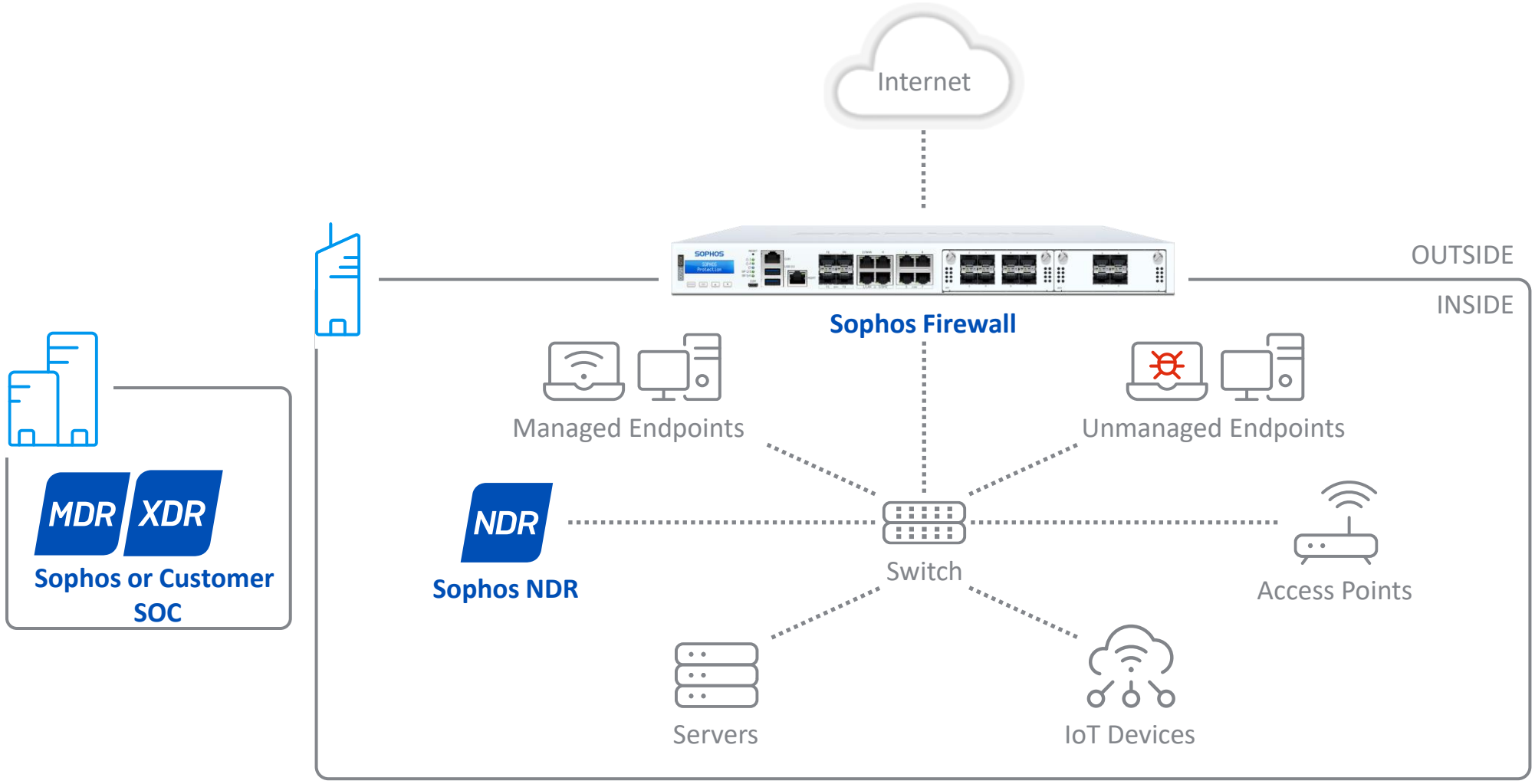


Active Threat Response in Azione



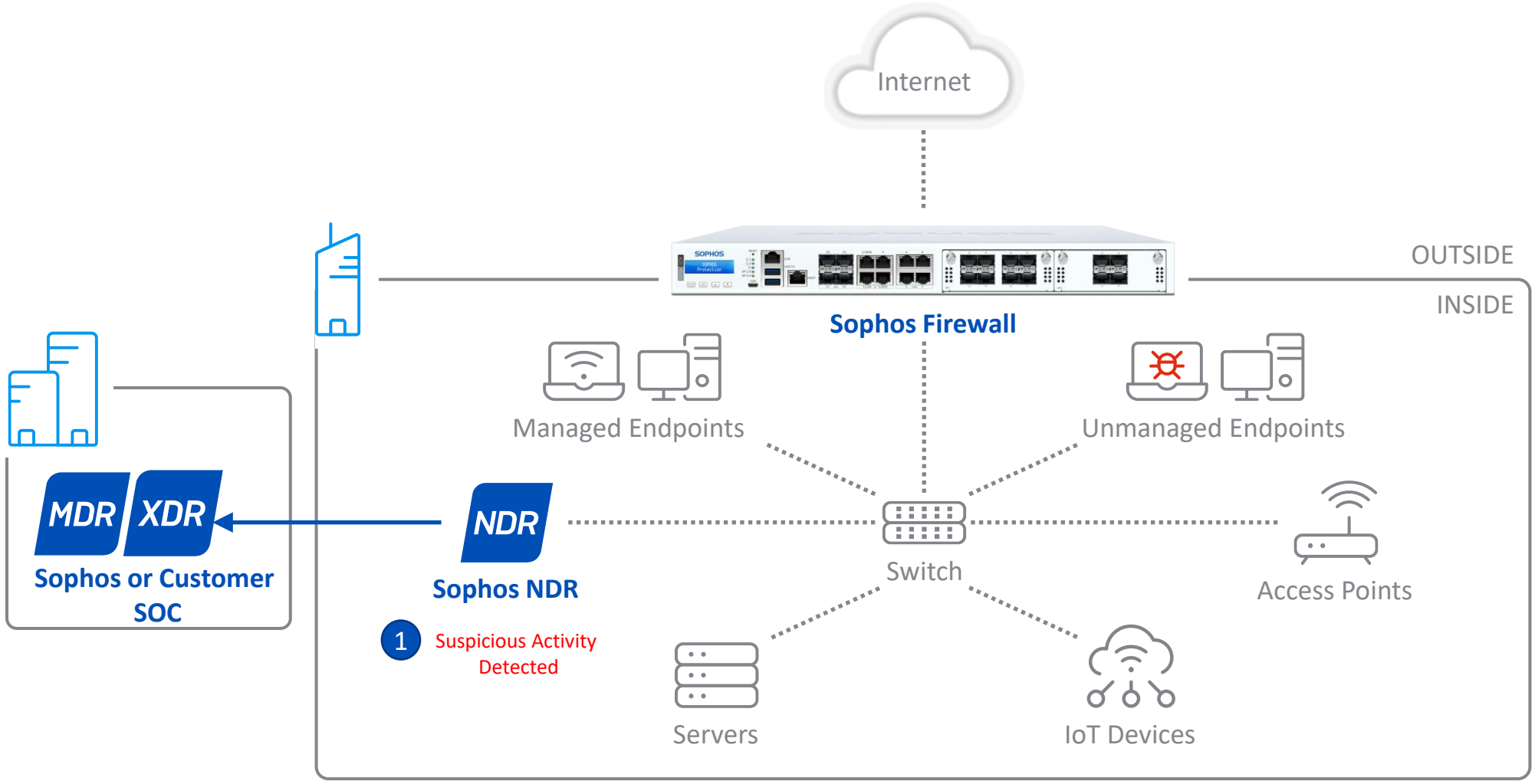
Risposta immediata: non è richiesta alcuna configurazione delle regole del firewall

Active Threat Response con rilevamento avanzato NDR



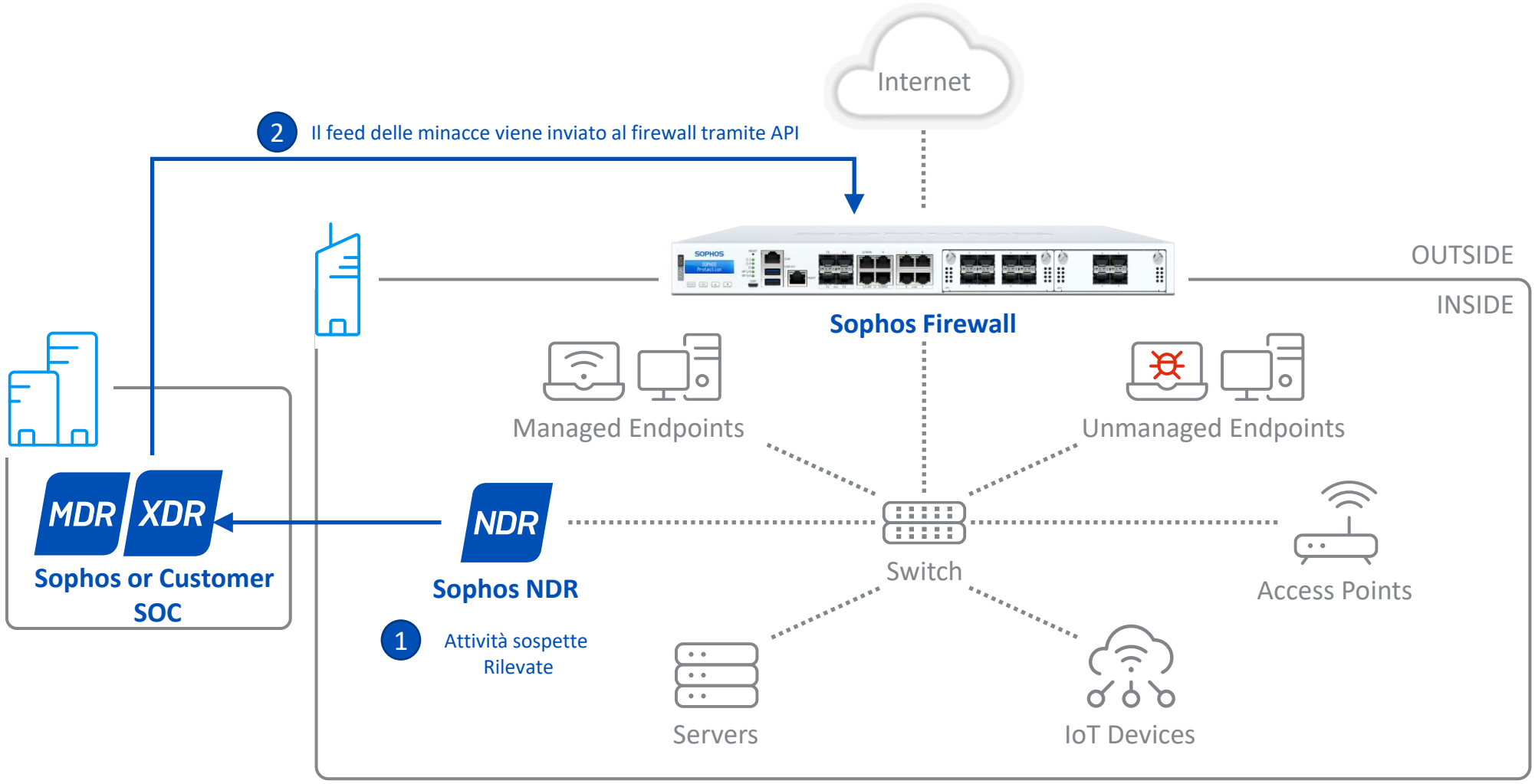
La combinazione definitiva per il rilevamento e la risposta

Active Threat Response with NDR Enhanced Detection



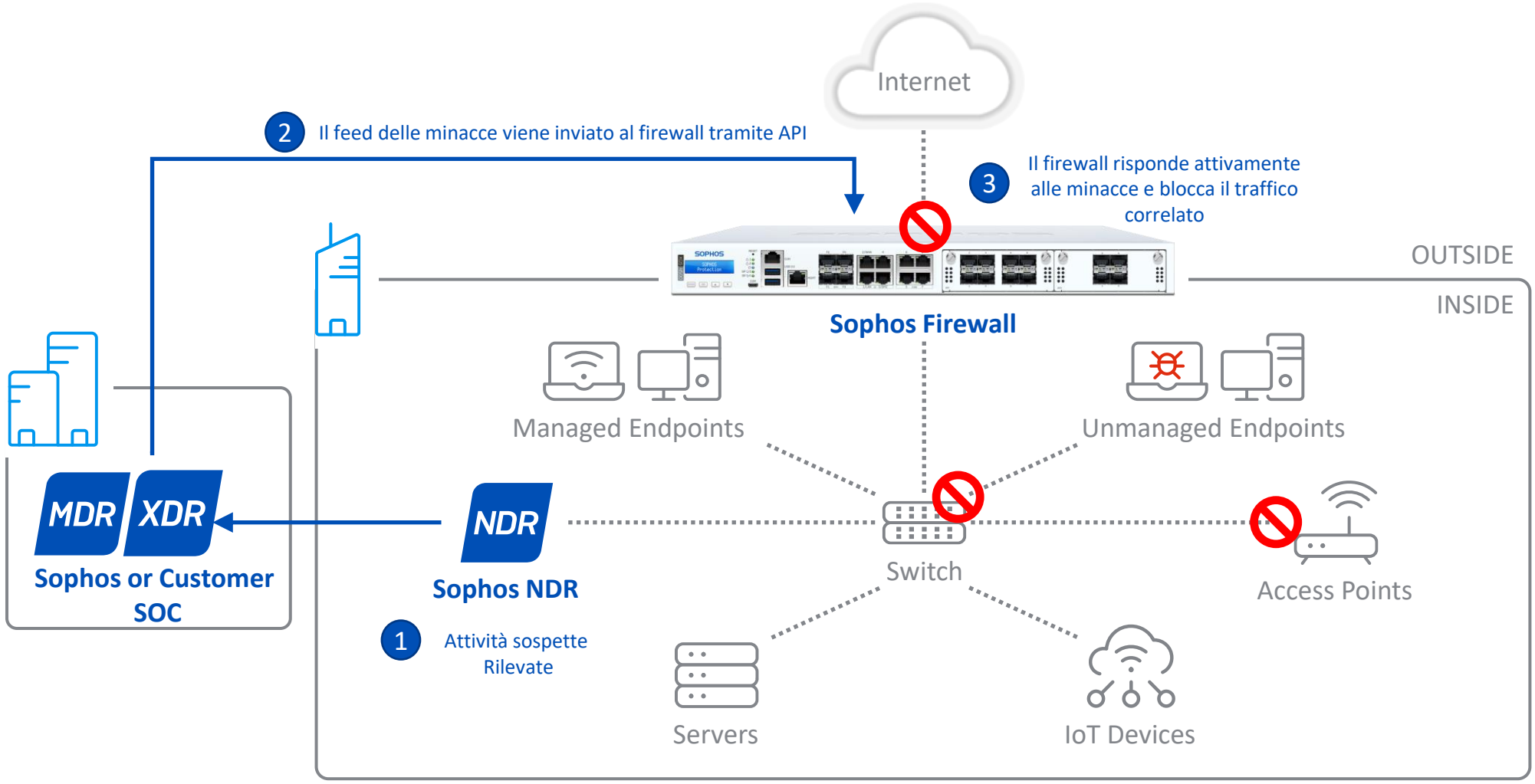
The Ultimate Combination for Detection AND Response

Active Threat Response con rilevamento avanzato NDR



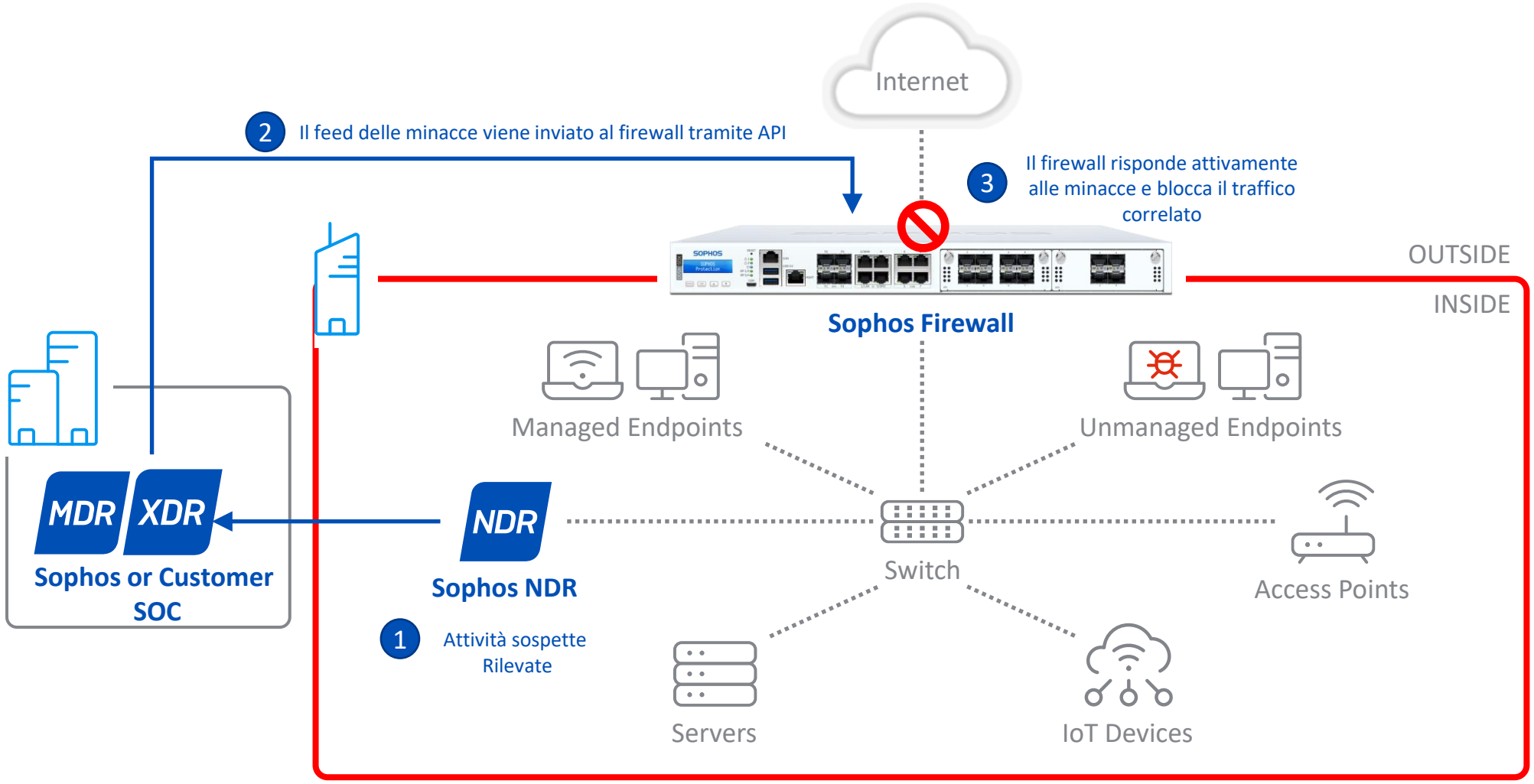
The Ultimate Combination for Detection AND Response

Active Threat Response con rilevamento avanzato NDR



The Ultimate Combination for Detection AND Response

Active Threat Response con rilevamento avanzato NDR



The Ultimate Combination for Detection AND Response

Active Threat Response

For Switch and AP6

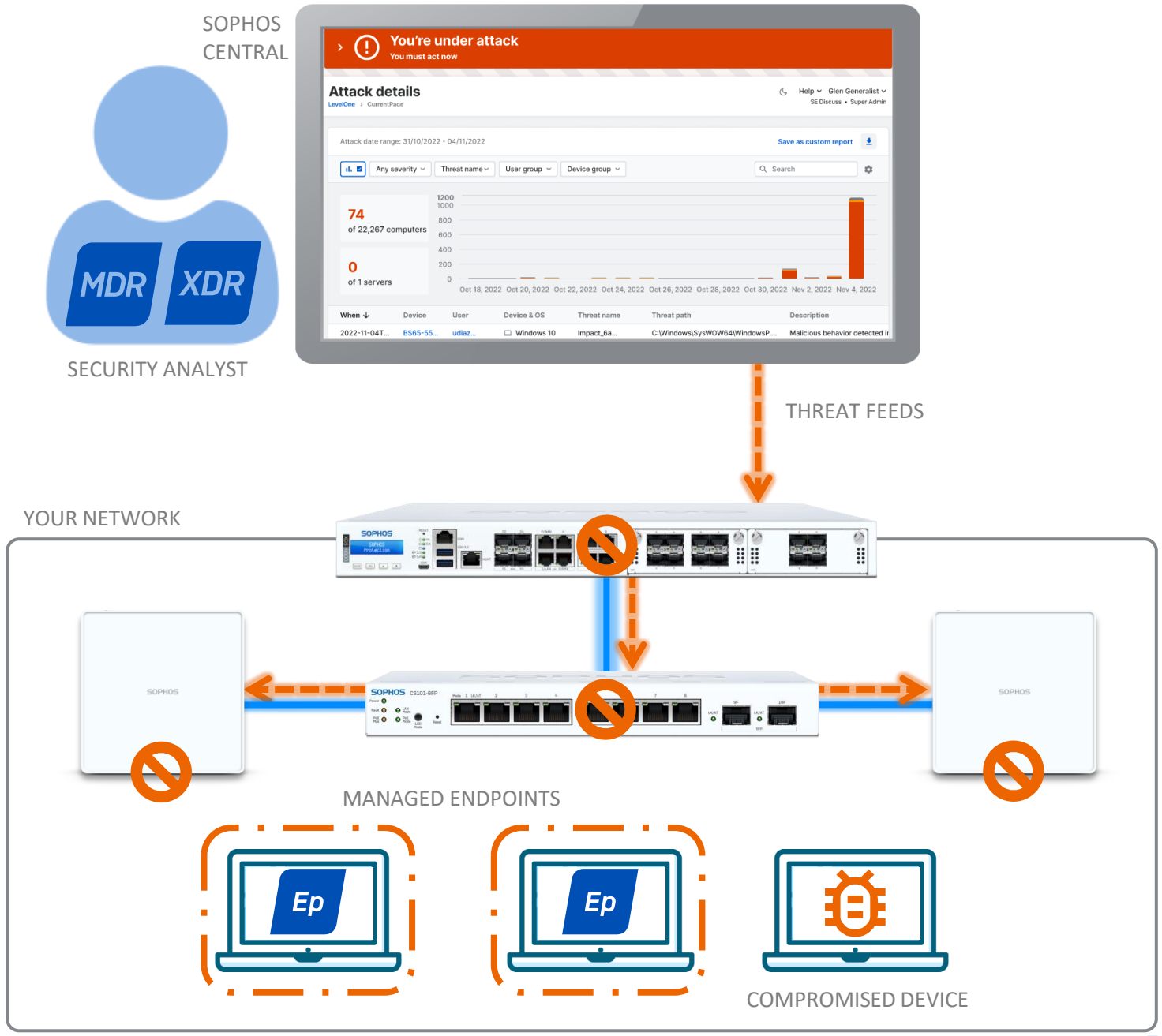
Cross-Product Automation

- MDR/XDR Analysts can trigger a response via Sophos Central Threat Feed API
- Works with Sophos Firewall, Switch, AP6

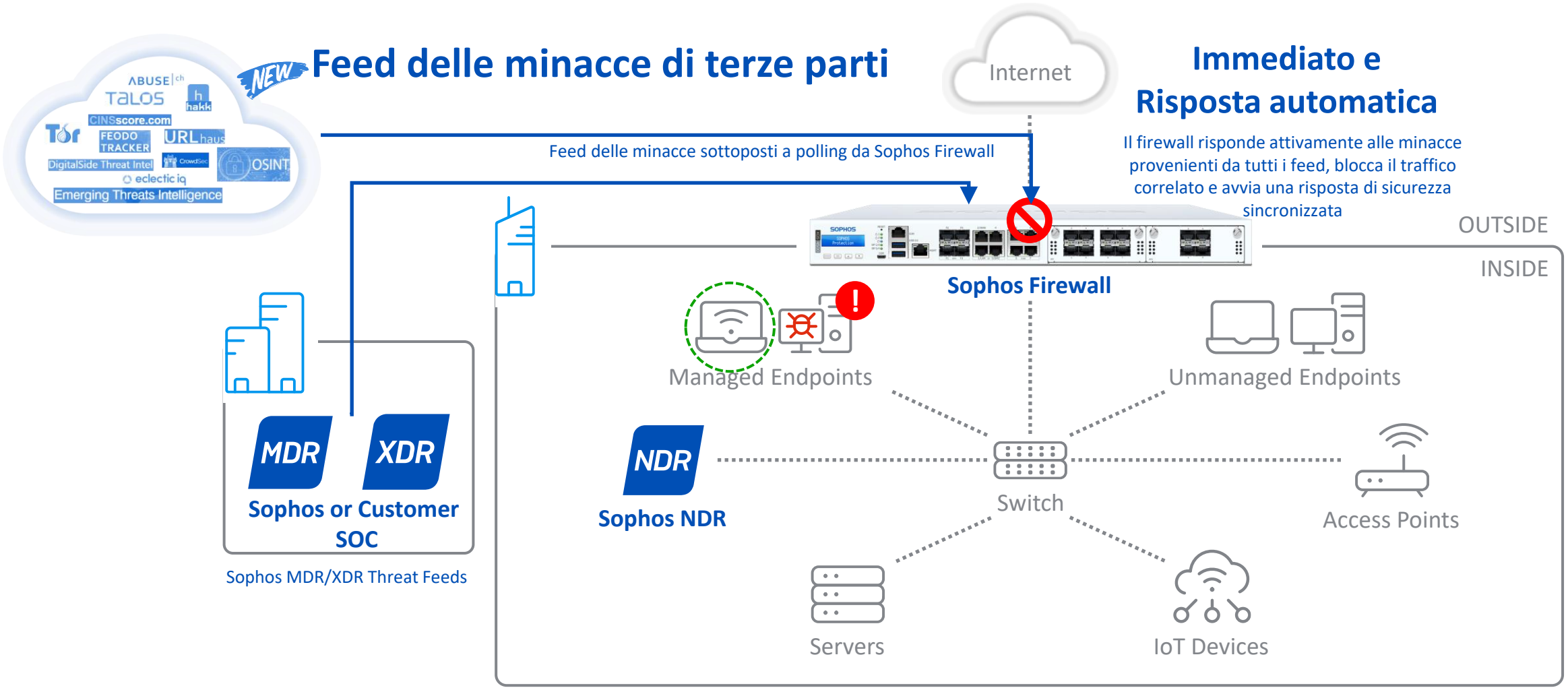
Automatic Response

- Firewall automatically blocks threats from communicating to other parts of the network
- Firewall automatically coordinates with managed endpoints to block traffic from compromised hosts
- ZTNA automatically prevents connections to applications

NEW Switch and AP6 automatically block compromised device at the access layer – completely isolating them - even within the same LAN segment



Estensione di Active Threat Response



Threat Response Demo

Sophos MDR Threat Case

Detecting Business Email Compromise (BEC) using Microsoft Audit Logs

ACTIVITY:

Adversary

9:07 p.m. UTC

The attack beings with a phishing email sent to [USER 1].

The attacker uses Evilginx, an open-source (man-in-the-middle) MITM framework used for phishing login credentials and session cookies, to obtain [USER 1's] username, password, and authorization tokens.

The attacker then uses the intercepted authorization tokens to circumvent [CUSTOMER's] multi-factor authentication (MFA).

ACTIVITY:

Adversary

10:19 p.m. UTC

The attacker creates an email forward rule in [USER 1's] inbox.

Impersonating [USER 1], the attacker sends a request to [ADMIN 1] to validate the attacker's IP address, granting the attacker access to a Microsoft Dev Box in Azure.

The attacker begins post-initial access activities.

SOURCE:

Microsoft Audit Logs

10:20 p.m. UTC

Sophos XDR detects the creation of new inbox rules for [USER 1's] Microsoft 365 email account that contain only special characters.

An additional detection identifies that multiple IPs and user agents were being used within the same session, indicating [USER 1's] account and session have been compromised through a man-in-the-middle attack.

SOURCE:

Sophos Endpoint

10:20 p.m. UTC

Sophos MDR analysts investigate endpoint telemetry associated with [USER 1] and identify malicious behaviors and artifacts, including tools such as Mimikatz and BloodHound—two tools commonly used by attackers to steal sensitive data and escalate privileges within a network.

ACTIVITY:

Sophos MDR Threat Response

10:26 p.m. UTC

Sophos MDR analyst isolates the compromised host and suspends [USER 1's] account to contain the attack.

Sophos MDR analyst advises [CUSTOMER] and [CUSTOMER PARTNER] to reset the credentials of the compromised user.

Sophos MDR analysts conduct full-scale incident response to determine initial access and remove all malicious artifacts used in the attack.

NIS2 How MDR can help

NIS2

By delivering 24/7 threat detection, investigation and response across the full security environment, Sophos MDR supports organisations working towards the NIS2 Directive; primarily assisting with Chapter IV of the NIS2 Directive, Cybersecurity Risk-Management Measures And Reporting Obligations

NIS2 Requirement	Sophos MDR
Chapter IV, Article 21, Cybersecurity risk-management measures	
2. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems… based on a) policies on risk analysis and information system security;	24/7 threat detection and response identifies and neutralizes advanced cyber-attacks that technology alone cannot stop
2. b) incident handling	Continuously monitors signals from across the security environment, including network, email, firewall, identity, endpoint, and cloud technologies, enabling us to quickly and accurately detect and respond to potential cybersecurity events. Full incident response service is included as standard, providing 24/7 coverage delivered by IR experts. Includes full root cause analysis and reporting. Our average time to detect, investigate and respond is just 38 minutes.

NIS2

By delivering 24/7 threat detection, investigation and response across the full security environment, Sophos MDR supports organisations working towards the NIS2 Directive; primarily assisting with Chapter IV of the NIS2 Directive, Cybersecurity Risk-Management Measures And Reporting Obligations

NIS2 Requirement	Sophos MDR
Chapter IV, Article 21, Cybersecurity risk-management measures	
2. c) business continuity, such as backup management and disaster recovery, and crisis management	Ensures the information security aspect of business continuity management with 24/7 detection of and response to security incidents across the IT environment, leveraging human expertise, AI, and advanced technologies.
2. d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Delivers expert threat hunting and remediation as a fully managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Our threat-hunting experts monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities and protect personal data wherever it resides. Sophos NDR generates high-caliber actionable signals across the network infrastructure to optimize cyber defenses. Sophos MDR proactively responds to vulnerability disclosure by the client. On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation

NIS2

By delivering 24/7 threat detection, investigation and response across the full security environment, Sophos MDR supports organisations working towards the NIS2 Directive; primarily assisting with Chapter IV of the NIS2 Directive, Cybersecurity Risk-Management Measures And Reporting Obligations

NIS2 Requirement	Sophos MDR
Chapter IV, Article 21, Cybersecurity risk-management measures	
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	Investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk levels and prioritize response.
2. i) human resources security, access control policies and asset management;	Threat-hunting experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities by regularly reviewing records of information system activity, such as audit logs, access logs, access reports, and security incident tracking reports.

NIS2

By delivering 24/7 threat detection, investigation and response across the full security environment, Sophos MDR supports organisations working towards the NIS2 Directive; primarily assisting with Chapter IV of the NIS2 Directive, Cybersecurity Risk-Management Measures And Reporting Obligations

NIS2 Requirement	Sophos MDR
Chapter IV, Article 23, Reporting obligations	
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: **d) a final report not later than one month after the submission of the incident notification under point (b), including the following:** **(i) a detailed description of the incident, including its severity and impact;**	On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation
(ii) the type of threat or root cause that is likely to have triggered the incident;	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops. Full root cause analysis by Sophos MDR enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.

MDR Livelli di servizio

Servizio completo con garanzia 1 MLN $

	Sophos MDR	Sophos MDR Complete
24/7 Monitoraggio delle minacce e risposta guidata da esperti	✓	✓
Compatibile con tecnologia non-Sophos	✓	✓
Reportistica live, settimanale e mensole	✓	✓
Meenting mensile di aggiornamento sulle ultime minacce "Sophos MDR ThreatCast"	✓	✓
Revisione continua delle impostazioni di Sicurezza di Sophos Central	✓	✓
Threat Hunting guidato da esperti	✓	✓
Contenimento delle minacce, interruzione degli attacchi, blocco della diffusione Possibilità di utilizzare l'agent full Intercept X con XDR (protezione e detection and response) o solo l'agent Sophos XDR Sensor	✓	✓
Canale telefonico diretto durante gli incidenti attivi	✓	✓
Incident Response completa: minaccia completamente eliminata Richiede la protezione completa installata Intercept X con XDR (protection, detection and response)		✓
Individuare la fonte degli attacchi: Per prevenire futuri attacchi		✓
Incident Response Leader dedicato		✓

SLA for MDR Complete: Tempo di risposta garantito, 60 minuti per il 90% dei casi di alta priorità. Misurato su base mensile

MDR Livelli di servizio

	Sophos MDR	Sophos MDR Complete
24/7 Monitoraggio delle minacce e risposta guidata da esperti	✓	✓
Compatibile con tecnologia non-Sophos	✓	✓
Reportistica live, settimanale e mensole	✓	✓
Meenting mensile di aggiornamento sulle ultime minacce "Sophos MDR ThreatCast"	✓	✓
Revisione continua delle impostazioni di Sicurezza di Sophos Central	✓	✓
Threat Hunting guidato da esperti	✓	✓
Contenimento delle minacce, interruzione degli attacchi, blocco della diffusione Possibilità di utilizzare l'agent full Intercept X con XDR (protezione e detection and response) o solo l'agent Sophos XDR Sensor	✓	✓
Canale telefonico diretto durante gli incidenti attivi	✓	✓
Incident Response completa: minaccia completamente eliminata Richiede la protezione completa installata Intercept X con XDR (protection, detection and response)		✓
Individuare la fonte degli attacchi: Per prevenire futuri attacchi		✓
Incident Response Leader dedicato		✓

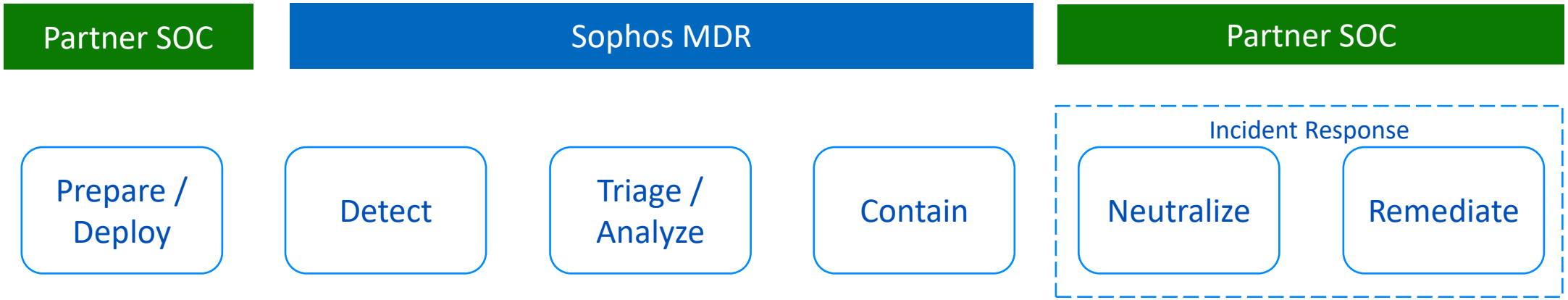
Attività coadiuvate dal Key Partner MDR

MDR Livelli di servizio

	Sophos MDR	Sophos MDR Complete
24/7 Monitoraggio delle minacce e risposta guidata da esperti	✓	✓
Compatibile con tecnologia non-Sophos	✓	✓
Reportistica live, settimanale e mensole	✓	✓
Meenting mensile di aggiornamento sulle ultime minacce “Sophos MDR ThreatCast”	✓	✓
Revisione continua delle impostazioni di Sicurezza di Sophos Central	✓	✓
Threat Hunting guidato da esperti	✓	✓
Contenimento delle minacce, interruzione degli attacchi, blocco della diffusione Possibilità di utilizzare l’agent full Intercept X con XDR (protezione e detection and response) o solo l’agent Sophos XDR Sensor	✓	✓
Canale telefonico diretto durante gli incidenti attivi	✓	✓
Incident Response completa: minaccia completamente eliminata Richiede la protezione completa installata Intercept X con XDR (protection, detection and response)	✓	
Individuare la fonte degli attacchi: Per prevenire futuri attacchi	✓	
Incident Response Leader dedicato	✓	

Attività erogate dal Key Partner MDR

Partner Services + Sophos MDR – MDR vs MDR Complete



MDR Complete (per l'IR Sophos non può agire direttamente su tutta l'infrastruttura del cliente). Il Deploy non è gestito da Sophos

MDR (per ottenere la migliore combinazione tra
Threat hunting e risposta agli incidenti).
Il Key Partner MDR gestisce il deploy e l'Incident response (guidato dal team Sophos MDR)

Scenario: Attacco Phishing mirato

Scanrio di attacco
L'utente apre l'email di phishing mirato e clicca sl link che henera il download di uno script malevolo

MITRE | ATT&CK®

TACTIC	Initial Access	Execution	Defense Evasion	Persistence
TECHNIQUE	Spearphishing Link	Malicious File	Process Injection	Schedule Task

▲ RILEVAMENTO INIZIALE

Sophos MDR

Azioni di contenimento della minaccia

- Isolamento dei dispositive coinvolti
- Rimozione del file malevoli
- Rimozione dei task programmatic dall'hacker
- Notifica al Key Partner MDR delle azioni intraprese e fornisce la procedura di remediation complete guidata

MDR\Key Partner MDR

Incident Response e analisi della causa iniziale

- Individuazione dell'email di phishing mirato e dell'URL che portato all'esecuzione dell'attacco
- Verifica se altri utenti hanno ricevuto lo stesso attacco di phishing mirato
- Crea il resoconto sull'incidente per il cliente coadiuvato dalle informazioni e linee guida fornite da Sophos MDR

Key Partner MDR

Remediation Guidance

- Blocco del mittente malevolo sul Sistema di posta\antispam del cliente
- Reset delle credenziali degli utenti eventualmente coinvolti nell'attacco

Servizio MDR integrato tra vendor e partner

MDR	MSSP		Key Partner MDR + SOPHOS MDR
✓	⚠	Visibilità globale sulle minacce grazie alla telemetria di +650.000 clienti	✓
✓	⚠	Threat-hunting proattivo e non solo monitoraggio reattivo	✓
⚠	✓	Network Operation Center	✓
⚠	✓	Gestione IT e Incident response completa sull'ambiente del cliente	✓
⚠	✓	Un servizio che parli la stessa lingua del cliente	✓
✓	⚠	Copertura globale del servizio per clienti multi-sede	✓
✓	⚠	Team unico: Security Operation, Threat Labs, AI scientist e Automation	✓
✓	⚠	Livelli target di servizio: 2 min detection 30 min response	✓
✓	✓	Integrazione dei dati dei vari strumenti di security	✓
⚠	✓	Interventi on-site	✓

Soluzione integrata

Sulla base delle specifiche esigenze mostrate dal cliente, ad oggi prevediamo il seguente pacchetto di offerta:

Sophos MDR

- Detection < 1 minuto
- Analysis < 25 minuti
- Containment < 12 minuti
- Time-Frame 7x24
- Full Remote
- Service Coverage: All Events

Security Operation Manager

- Persona esperta dedicata
- Full remote
- First Contact
- Time-Frame 5x8

Continuous Vulnerability Assessment

- Vulnerability Assessment trimestrale
- Team Offensive dedicato
- Report executive
- Report di dettaglio delle vulnerabilità
- Azioni di remediation consigliate

Supporto on Demand

- Supporto per esigenze specifiche (Recovery, System Configuration, Interventi on-site)

Security Operation Manager

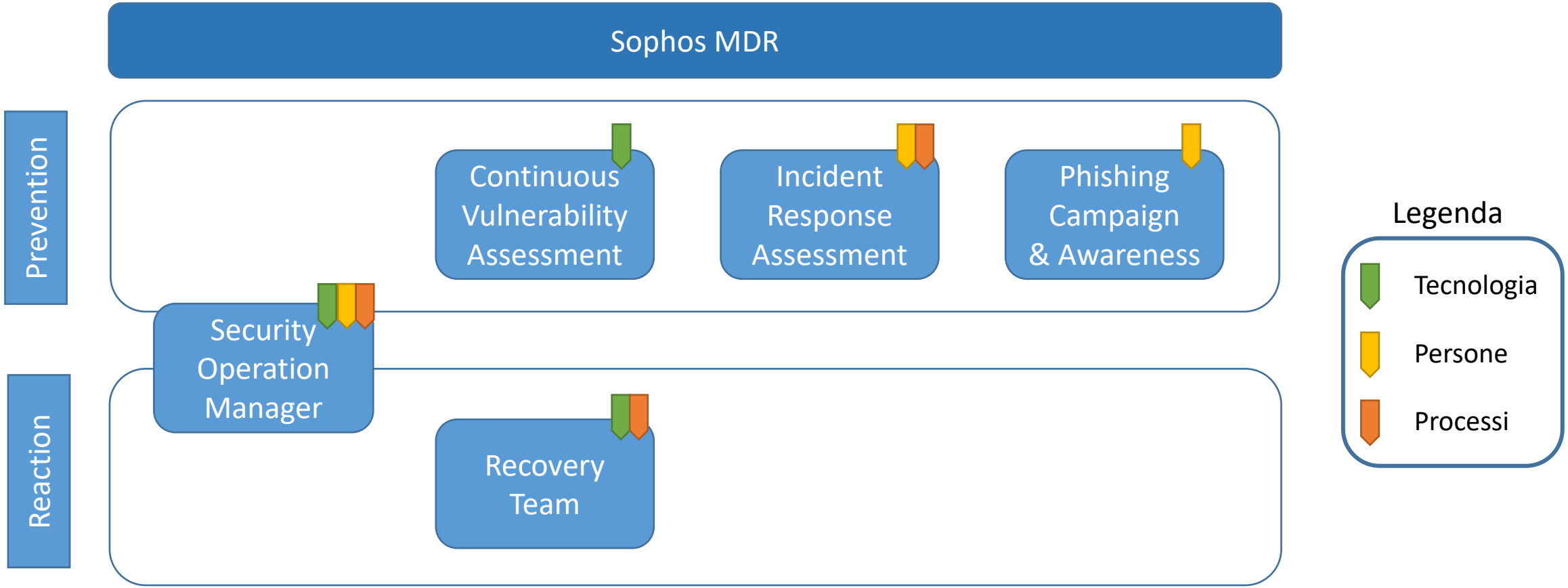
E’ uno specialista esperto e competente in ambito Security Operations che coordina le attività di Response e funge da intermediario tra il cliente ed il servizio MDR.

Ruolo del Security Operation Manager (SOM)

- Interfacciarsi col servizio Sophos MDR per qualsiasi evento rilevato o richiesta di investigazione;
- Conoscere il Business del cliente ed allinearne le esigenze col servizio MDR così da limitare i falsi positivi;
- Pianificare e coordinare le attività di Recovery, sia attraverso l’ingaggio del Response Team che di eventuali fornitori terzi owner del servizio impattato.
- Descrivere e riportare dettagliatamente rischi ed eventuali impatti.
- Supportare il cliente nel proporre azioni mitigatorie a correzione del vettore d’attacco.
- Supporto in lingua italiana (nativa) e inglese (professionale)

Managed Services

I servizi professionali sono proposti in formato modulare. E' possibile attivare uno più servizi sia in fase iniziale che a servizio avviato. Ogni servizio contribuisce a vario titolo ad aumentare le sicurezza delle 3 dimensioni d'impresa.



Q&A

Indirizzo: Viale Martesana, 12 - 20055 Vimodrone (MI)

Telefono: +39 02 925961

Sito web: www.nposistemi.it

Indirizzo email: info_marketing@nposistemi.it