



Cybersecurity as a service Protezione avanzata e gestita

Letterio La Spada

Senior Channel Sales Engineer

Ottobre 2025





Cybersecurity as a service Protezione avanzata e gestita

Letterio La Spada

Senior Channel Sales Engineer

Ottobre 2025



**Cosa definisce una minaccia
informatica moderna?**

Definizione di una minaccia moderna

Threat

=

Intent

+

Opportunity

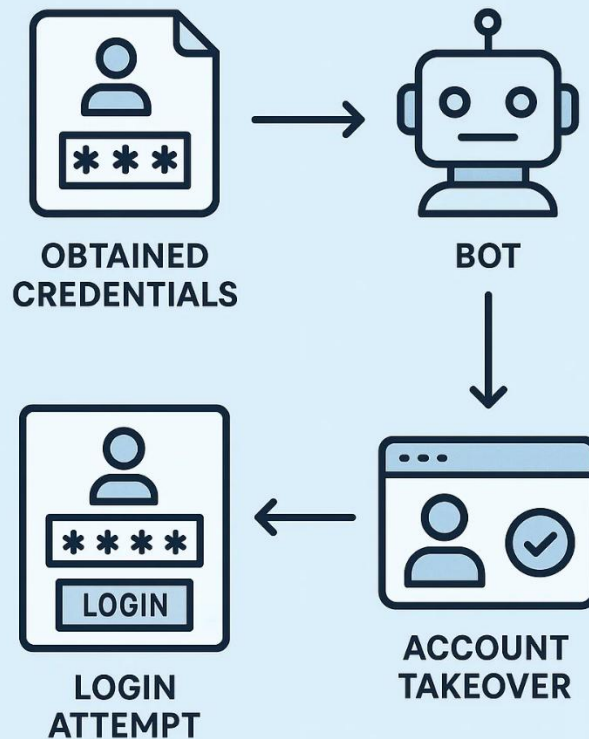
+

Capability

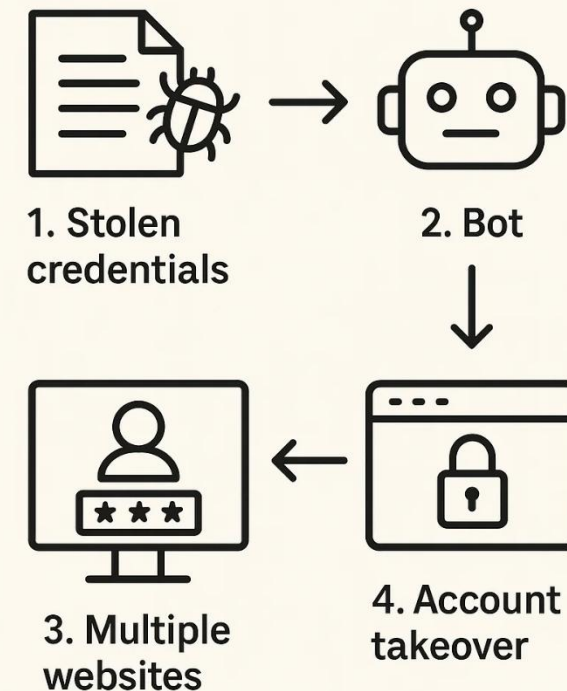
Credential Stuffing

Utilizzo delle violazioni esistenti per ottenere l'accesso iniziale – Ancora utilizzato nel 2025

HOW CREDENTIAL STUFFING WORKS



HOW CREDENTIAL STUFFING WORKS



Typical Targets

- **RDP**
- **VPN**
- **M365**
- **WEBSITES**

+700% YoY

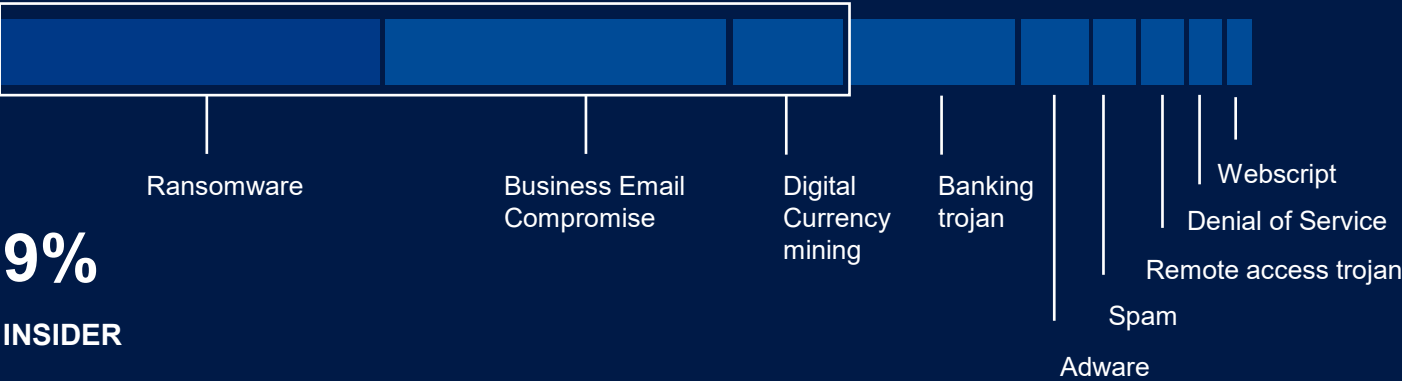
Intento

79%

Degli incidenti che investighiamo sono **motivati da ragioni finanziari**

79%

FINANCIALLY-MOTIVATED



9%

INSIDER



12%

NATION-STATE



Il panorama delle minacce moderne non lascia spazio a errori



Velocità

Tempo mediano impiegato da un utente malintenzionato per ottenere l'accesso come amministratore di dominio

11 ore



Aumento

Aumento annuale degli strumenti "living-off-the-land" utilizzati negli attacchi

126%

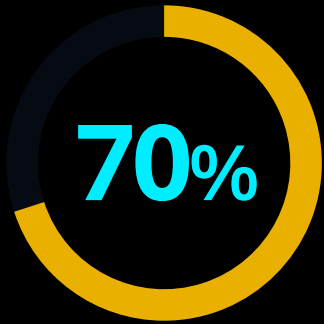


Sofisticazione

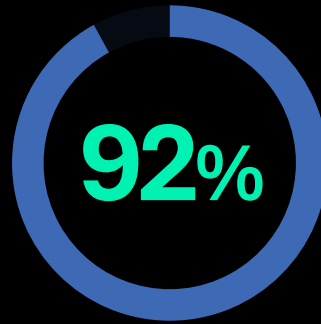
Percentuale di attacchi in cui gli avversari hanno effettuato l'accesso con credenziali valide

56%

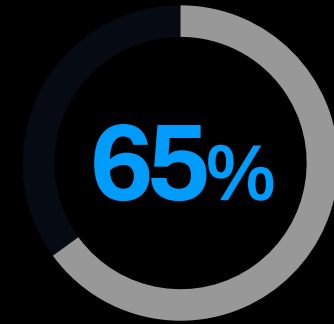
Ricerca sulle minacce Sophos X-Ops Active Adversary report 2025



In 2024 Microsoft “observed remote encryption in 70% of successful attacks”¹
(up from 60% in 2023)

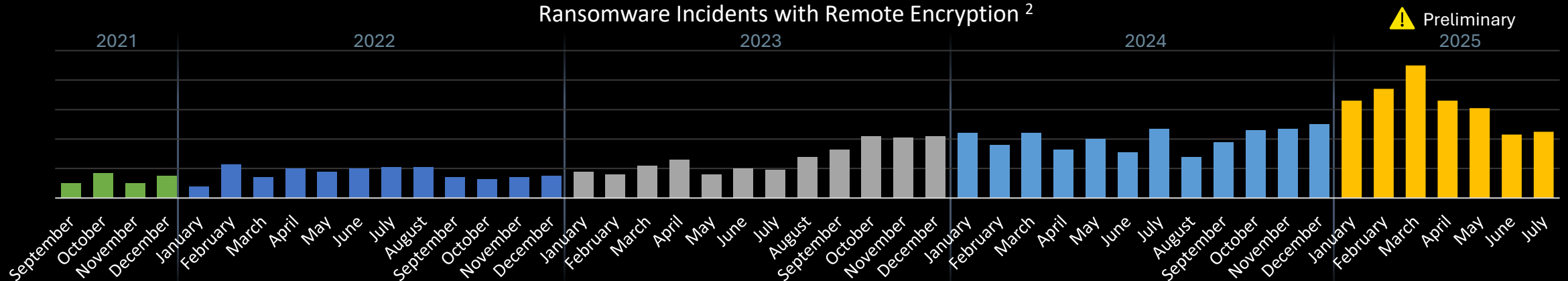


“with 92% originating from unmanaged devices in the network”¹
(up from 80% in 2023)



In H1 2025, Sophos saw a 65% increase over full-year 2024²
(up from a 50% increase in 2024 over 2023)

Ransomware Incidents with Remote Encryption²



¹ Microsoft Digital Defense Report 2024 ² Sophos data

E' necessaria una strategia di Cybersecurity multilivello

Enhance security controls

1

Detection

Endpoint,
network
(behavioral)

2

Prevention

Patching,
multi-factor
authentication

3

Resilience

Hardening Active
Directory to secure
the domain

4

Response

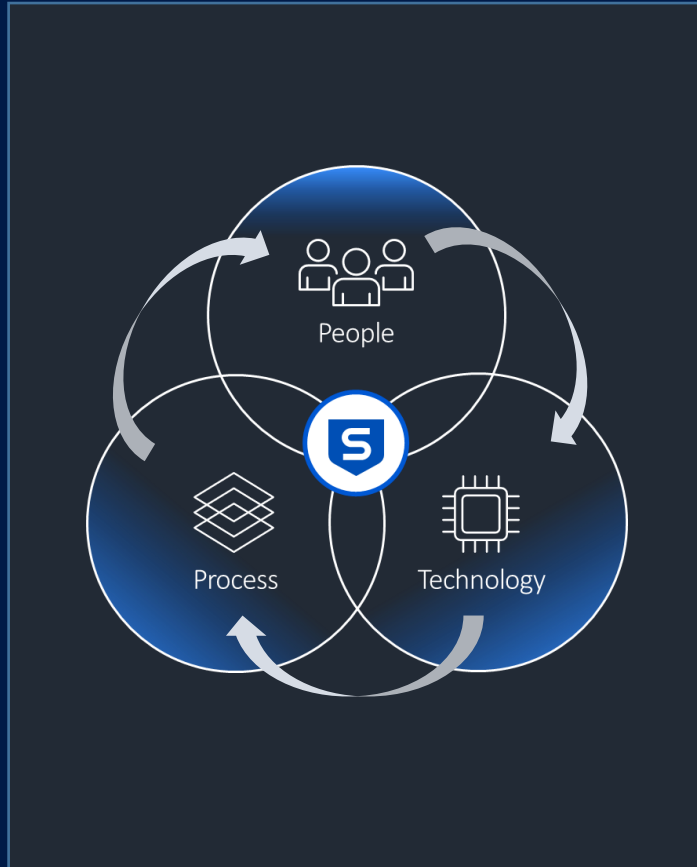
Have a plan,
practice it, involve
the entire business,
and be left of
“boom”

5

Recovery

Offline
backups

Le nuove domande da porsi



**Sei in grado di rispondere
alle cyberminacce mentre
dormi?**

parte delle
organizzazioni non
dispongono
delle
competenze
e umane
per
bloccare
da sole le
minacce

88%

of ransomware attacks
start during evenings,
nights or weekends

Sophos Active Adversary Report 2025

7 days

is the average attacker
dwell time – the window
to detect and stop a
major cyber attack

Sophos Active Adversary Report 2025

63%

of ransomware victims
say they lacked the
human expertise needed
to stop the attack

Sophos State of Ransomware Report 2025



MDR
riduce
drasticamente il
rischio di
incorrere in
minacce
avanzate
che gli
strumenti
da soli non
possono

88%

of ransomware attacks
start during evenings,
nights or weekends

Sophos Active Adversary Report 2025

7 days

is the average attacker
dwell time – the window
to detect and stop a
major cyber attack

Sophos Active Adversary Report 2025

63%

of ransomware victims
say they lacked the
human expertise needed
to stop the attack

Sophos State of Ransomware Report 2025

**24/7
coverage**



8 Global SOC's

**38
minutes**

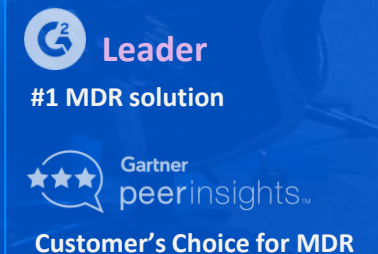
is the average Sophos MDR
response time - the team
stops 231 advanced attacks
every single day

**100's
of experts**

with deep knowledge
across all aspects of
security operations

Managed Detection and Response (MDR)

Un servizio 24/7 completamente gestito, erogato da esperti specializzati nel rilevamento e nella risposta ai cyberattacchi che le soluzioni tecnologiche da sole non sono in grado di prevenire.



Cybersecurity as a service = MDR

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

 Email

 Identity

 Public Cloud

 Network

Integrazioni incluse con le soluzioni Sophos, tra cui:

 **Sophos XDR**

 **Sophos Firewall**

 **Sophos Email**

 **Sophos Mobile**

 **Sophos Cloud**

 **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

La Sophos Breach Protection Warranty Offre Fino a 1 Milione di \$ Per Coprire Le Spese Correlate Alla Risposta Agli Incidenti



Inclusa senza costi aggiuntivi nelle nuove subscription annuali (a termine) di **Sophos MDR Complete**



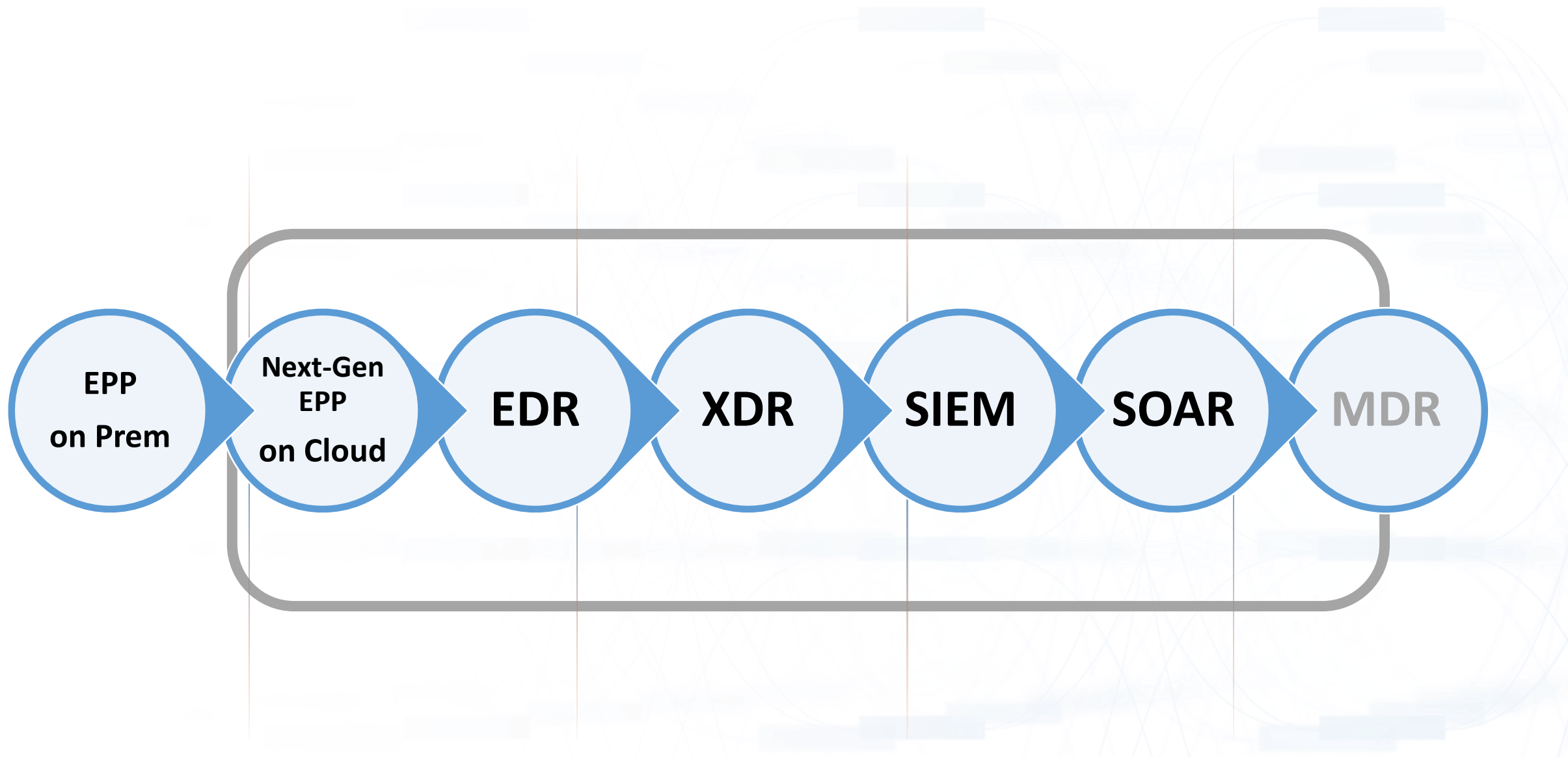
Integrata automaticamente nelle **licenze di 1, 2 e 3 anni**, sia per i nuovi clienti che per i rinnovi



Copertura completa: endpoint, server, Windows, macOS, nessuna limitazione geografica



Copertura fornita direttamente da Sophos, a dimostrazione della fiducia che riponiamo nella nostra protezione



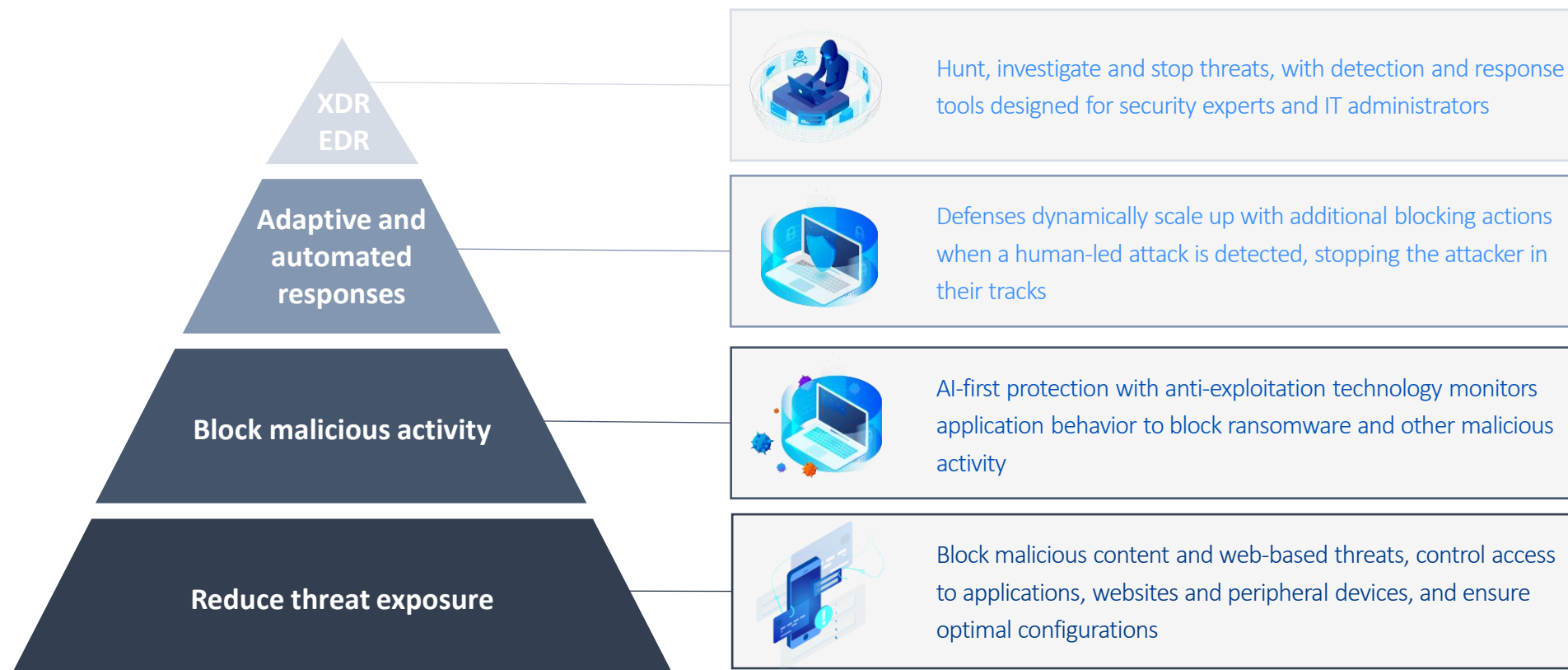
Soluzioni = Protection, Detection and Response

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

NB: Detection is not Protection!

Perchè MDR e non un next-gen Endpoint?

Sophos Endpoint adatta le difese al contesto di attacco ma da solo non basta



SERVICES

MANAGED SERVICES

MDR

Emergency
Incident ResponseVulnerability
ManagementIncident Response
Retainer

ADVISORY SERVICES

Penetration
TestingSecurity
AssessmentsRed Team
ExercisesIncident
Readiness

PLATFORM

CONTROLS

Endpoint

Firewall

Identity

Email

Network

Cloud

INTEGRATIONS

Broad Ingest
350+ Integrations

SECURITY OPERATIONS

XDR

SIEM

EDR

ITDR

NDR

Playbooks
and SOAR AI-Assisted Workflows and Experiences

SOPHOS X-OPS THREAT INTELLIGENCE

THREAT INTELLIGENCE

Adversary
TrackingThreat
ResearchIncident and
Case DataMalware
Analysis

AI, AUTOMATION & ENGINEERING

Adaptive Attack
ProtectionEarly Warning
SystemSecurity
AnalyticsDetection
Engineering

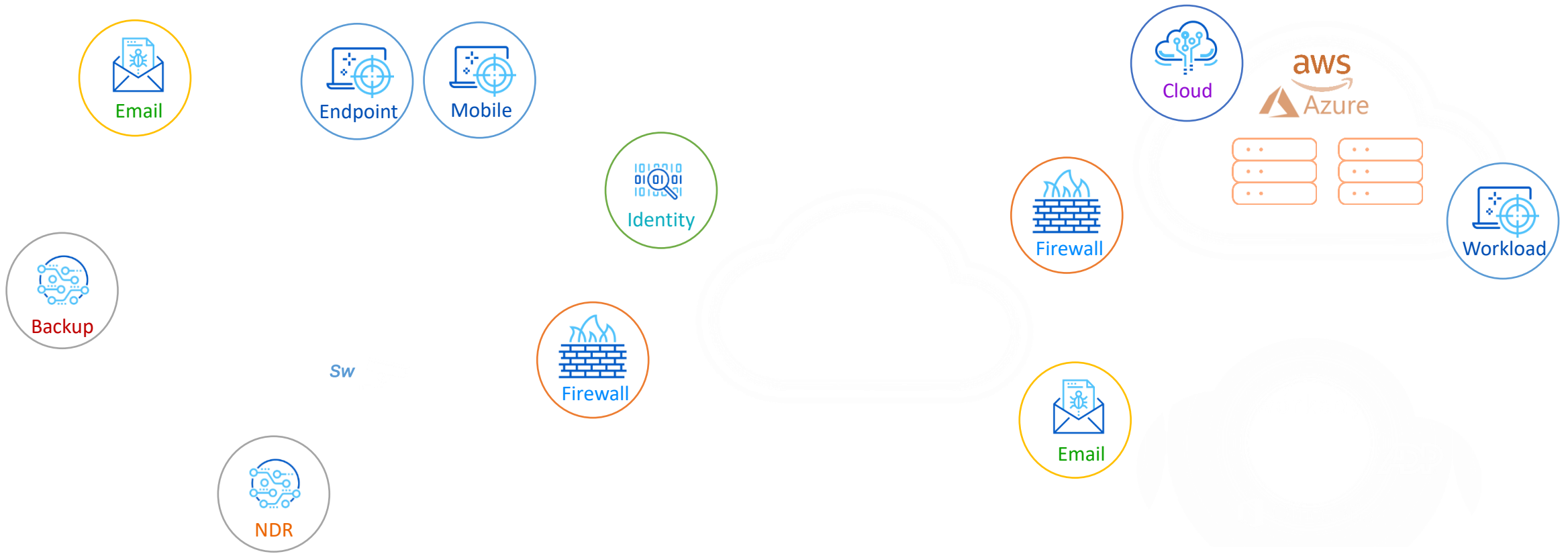
DATA LAKE

Sophos MDR livelli di servizio

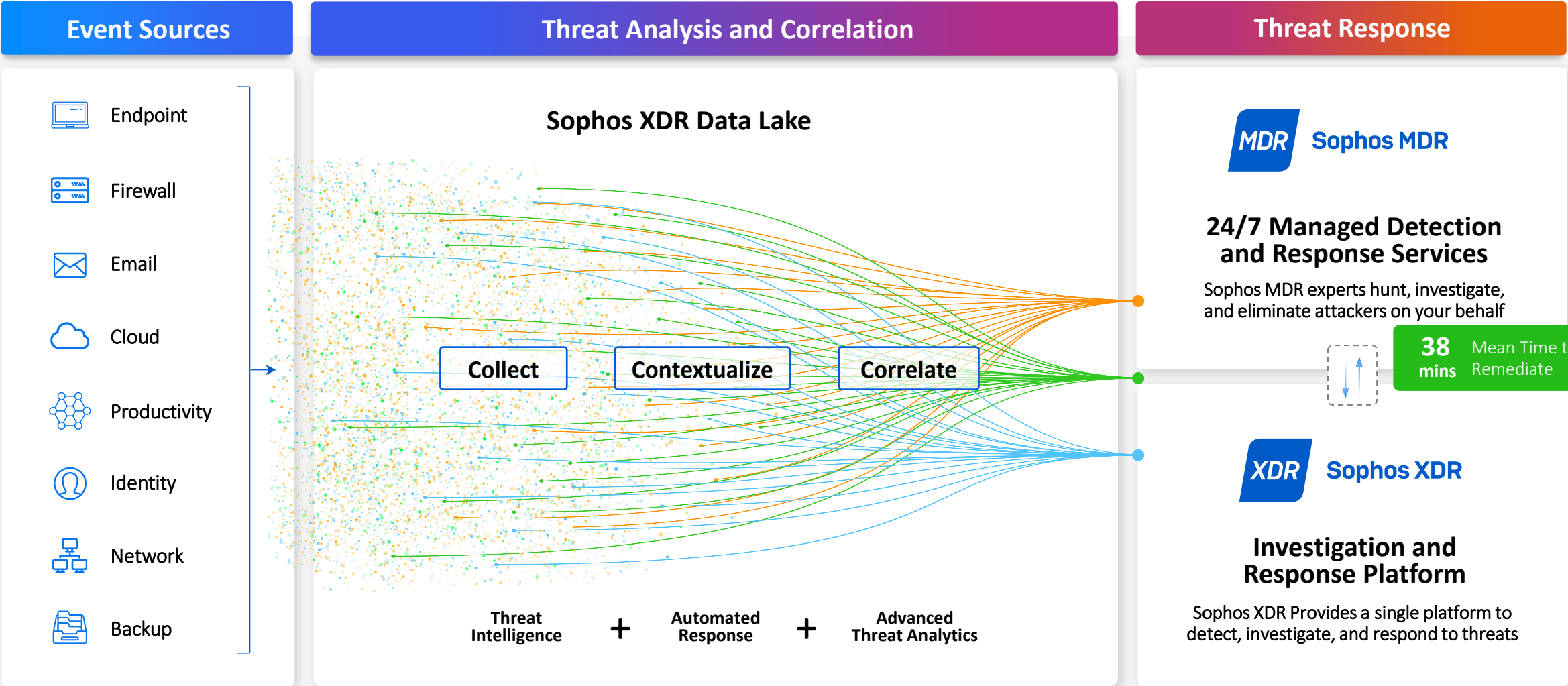
	Sophos MDR for Microsoft Defender	
	SOPHOS MDR Essentials	SOPHOS MDR Complete
24/7 expert-led threat monitoring and response	✓	✓
Compatible with non-Sophos security products (Microsoft and Google integrations included)	✓	✓
Sophos Endpoint and Sophos XDR solutions included	✓ *	✓
Comprehensive reporting and “MDR ThreatCast” intelligence briefings	✓	✓
Sophos account health check	✓	✓
Expert-led threat hunting	✓	✓
Threat response: active attacks are stopped and contained Using the Sophos XDR endpoint agent or Sophos XDR sensor	✓	✓
Direct call-in support during active incidents	✓	✓
Root cause analysis: performed to prevent future recurrence		✓
Full-scale incident response: threats are fully eliminated Requires the Sophos XDR endpoint agent		✓
Dedicated incident response lead		✓
Sophos breach protection warranty		✓
Sophos Incident Response Services Retainer Discount on hourly Emergency IR service for extended capabilities (e.g., on-site support, ransom negotiations, digital forensics)	+ Add-on	+ Add-on
Sophos Managed Risk Vulnerability management powered by Tenable technology and delivered as a service	+ Add-on	+ Add-on

✓ Attività
 ✓ erogate dal
 ✓ Key Partner
 ✓ MDR

* Option to use Sophos Endpoint or any non-Sophos endpoint protection solution with MDR Essentials

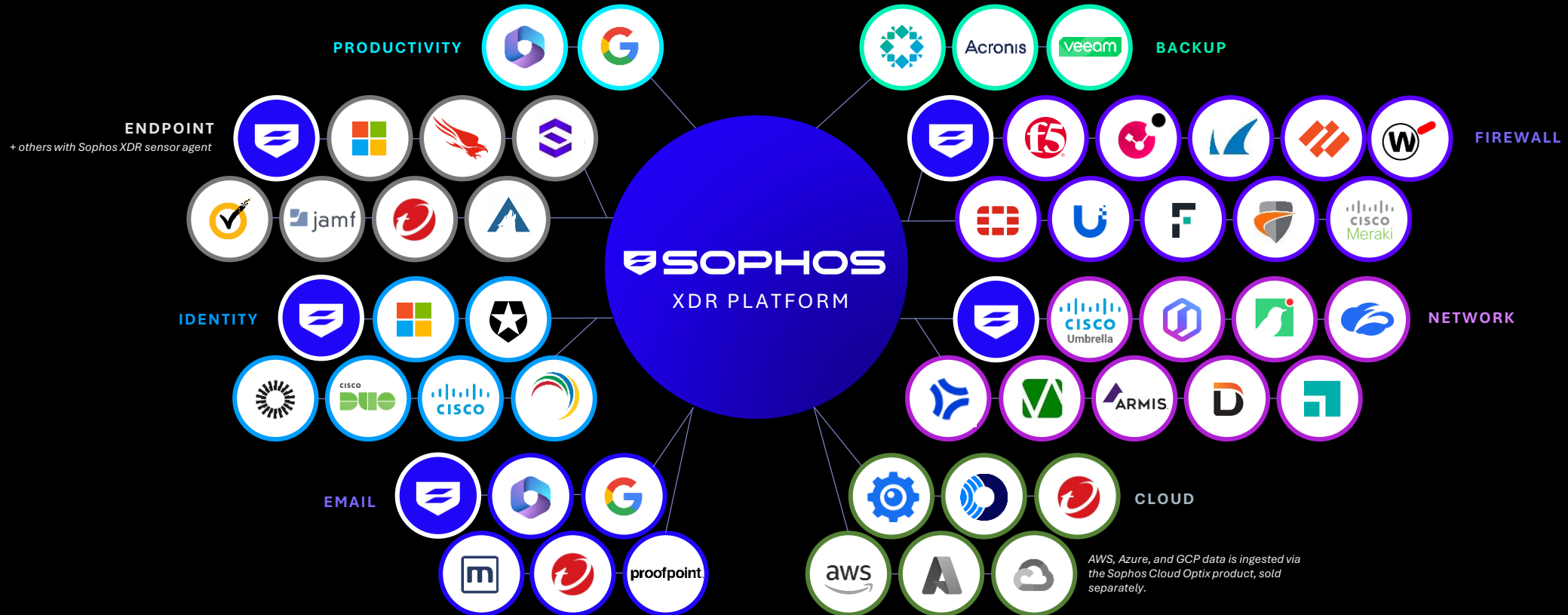


Sophos Threat Detection and Response Platform



Visibilità su tutte le superfici di attacco

I nostri analisti possono sfruttare gli investimenti tecnologici esistenti per rilevare e rispondere alle minacce.



TUTTE LE INTEGRAZIONI SONO INCLUSE SENZA COSTI AGGIUNTIVI!

Valore elevato per ogni piano di Microsoft 365 Business

MICROSOFT TELEMETRY BY LICENSE									
Microsoft	M365 Business Basic	M365 Business Standard	M365 Business Premium	E3	Entra ID P1	Entra ID P2	Defender for Endpoint P1	Defender for Endpoint P2	E5
Office 365 Mgmt. Activity	✓	✓	✓	✓	✓	✓	✓	✓	✓
Defender for Office 365			✓	✓					✓
Defender for Identity									✓
Defender for Cloud Apps									✓
Microsoft 365 Defender									✓
Defender for Endpoint			✓	✓			✓	✓	✓
Entra ID Protection						✓			✓

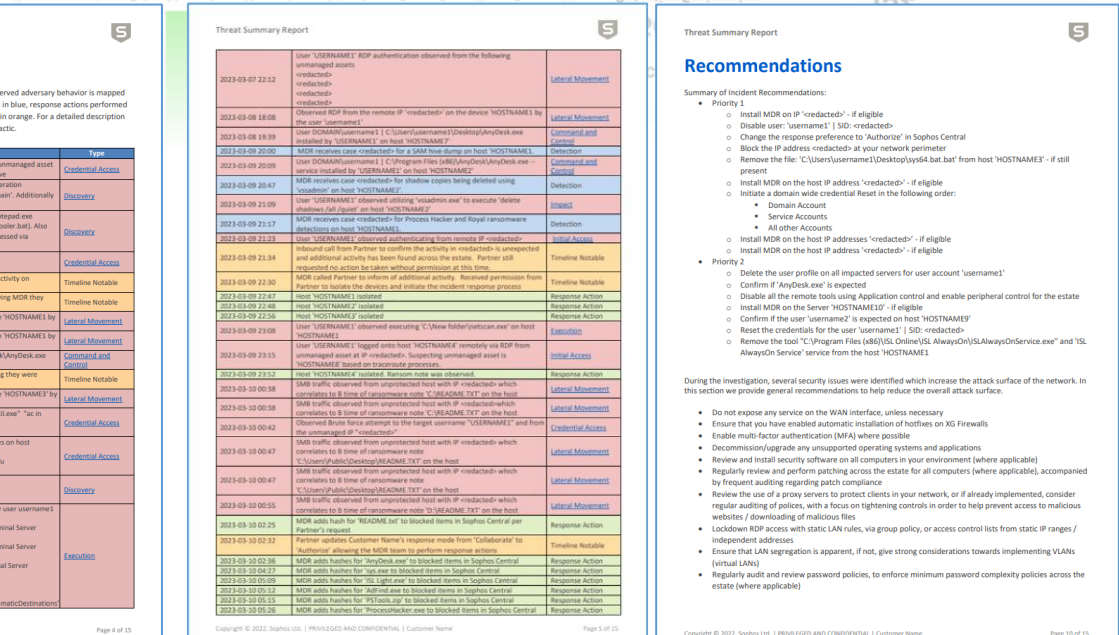
Sophos MDR SOC

Microsoft data is...

- correlated with data from other sources
- enriched with Sophos threat intelligence
- used to create Sophos proprietary detections

Sophos XDR Platform

Management > Managed Detection and Response - Dashboard

 Sophos Managed Detection and Response

Customer Name
CASE: 1-12345
DATE:

Executive Summary

On March 5, 2023, 20:00 UTC, the Sophos Managed Detection & Response (MDR) team responded to detection triggered for credentials dumping within estate Customer name on host "HOSTNAME". MDR observed the user "username1" accessing reg.exe via command line to save HKLM\SAM hive at file path "c:\temp\sam.save", which was detected and cleaned by Sophos Intercept X. This activity was detected by MDR which led to case <redacted> being automatically generated. The MDR team escalated the observed activity to the Partner team at 21:49 UTC.

On March 6, 15:59 UTC, the MDR team escalated additional activity for a detection triggered on host "HOSTNAME1" related to network enumeration commands. MDR observed the user "username1" executing net1 and nistest commands on the host along with creation of "C:\ProgramData\New" folder to drop multiple files such as netscan.exe. MDR contacted Partner successfully at 15:45 UTC to explain the activity and informed that this was similar to the previously escalated activity for host "HOSTNAME1".

On March 9, 21:34 UTC, MDR observed the Partner team for a detection that triggered for credential dumping on host "HOSTNAME1", which was previously escalated in case "redacted". MDR observed user "username1" saving file HKLM\System\SystemKey.hv on the host which was detected and cleaned by Sophos Intercept X. MDR observed AnyDesk installation and access by the user "username1", where a window "shadow copy, along with the file "C:\Users\username1\Desktop\username1.exe" was created. MDR observed the user "username1" findings discussed over a call with the Partner team. The MDR team requested permission to take action in an attempt to neutralize the threat actor. The threat actor's response preference was to "Collaborate". Partner provided approval for the MDR team to isolate 4 threat actors, "HOSTNAME1", "HOSTNAME2", "HOSTNAME3", and "HOSTNAME4". From March 5 to March 9, the threat actor performed reconnaissance and discovery, installed remote utility tools such as AnyDesk and Isight, attempted to execute ransomware binary.exe, and dropped ransomware on multiple hosts. Due to the ransomware note, the threat actors bypassed the Raytheon ransomware group.

During the investigation across Customer Name's estate, the MDR team observed the threat actor accessed the host `*HOSTNAME1` remotely on March 5 between 14:30 UTC to 22:20 UTC from unmanaged IPs <redacted>. This host is believed to be an access point as it successfully authenticated compromised user 'username1' in the estate. The MDR team had limited visibility across the estate as Customer Name only had MDR Complete licenses for servers. Additionally, there were many unprotected servers at the time of the incident.

On March 9, the MDR team reviewed the estate for ransomware notes and identified 172 impacted servers. On March 10, 02:32 UTC, Partner updated Customer Name's response mode from 'Collaborate' to 'Authorize', allowing the MDR team to take action. At this time, MDR began adding malicious file hashes to Sophos Central's blocked items list.

The last notable activity performed by the threat actor was on March 9 on hosts 'HOSTNAME1', 'HOSTNAME2' and 'HOSTNAME3'. At this time, the MDR team has not observed additional signs of compromise or suspicious activity across the Customer Name estate.

Timeline of Key Events (UTC)

The table below establishes the key events in the active incident timeline. Observed adversary behavior is mapped to a MITRE Tactic highlighted in red, Sophos technology detections highlighted in blue, response actions performed by the Sophos MIDR team in green, and all other timeline notables highlighted in orange. For a detailed description on the adversary behavior, refer to [MITRE ATT&CK Details](#) for the associated tactic.

Date	Detailed Event	Type
2023-03-19 13:39	User "USERNAME" logged onto host "HOSTNAME" from an unmanaged esp client connected via the SAMBA service to \\hostname.local	Credential Access
2023-03-19 14:40	User "USERNAME" initiated multiple recursive/reenumuration commands. User initiated net user "Domain Admin"/Domain Admin. Additionally received "Host: Guest" and net view results.	Discovery
2023-03-19 14:48	"User:ADMIN" accessed multiple files from C:\Program Files folder (e.g. examples, TestNetworkClient.bat, HOSTNAME.MSI, Setup, Notepad.exe). Also viewed file C:\Users\Administrator\AppData\Local\Foxit\Foxit Reader\Foxit Reader.exe	Discovery
2023-03-19 15:59	Received new HKEYSYSTEM\System\CurrentControlSet\Services\HypervisorPlatform\SysStart registry save HKEYSYSTEM Sysprep.log	Credential Access
2023-03-20 21:49	Mimikatz output of cme credexec for credential dump activity on HOSTNAME	Timeline Noteable
2023-03-23 22:30	Partner requested to conduct cme credexec on machine HOSTNAME MDR they own	Timeline Noteable
2023-03-26 08:21	Observed RDP from the remote IP "credacted" on the device "HOSTNAME" by the user "useradmin"	Lateral Movement
2023-03-26 14:31	Observed Remote Desktop ("credacted") on the device "HOSTNAME" by the user "useradmin"	Lateral Movement
2023-03-26 14:40	Observed Remote Desktop ("C:\Program Files\Ansys\AnsysDesktop.exe installed by user "USERAME" on host "HOSTNAME3")	Sensitive Data Control
2023-07-01 00:36	Partner requested to conduct cme credexec on device HOSTNAME3	Timeline Noteable
2023-07-01 10:15	Observed RDP from the remote IP "credacted" on the device "HOSTNAME" by the user "useradmin"	Lateral Movement
2023-07-01 10:25	Observed rdpm hit on host "C:\Windows\system32\cmdutils.exe" "ac in test" "net user /add /fullname /password: /c /d /m /n /w /r /p /q /f /t /u /c /P:ProgramFiles(x86)\Ansys\AnsysDesktop.exe"	Credential Access
2023-07-01 20:26	Observed commands used to dump Domain Password hashes on host "HOSTNAME3": "C:\Windows\system32\cmdutils.exe" "ac in test" "net user /add /fullname /password: /c /d /m /n /w /r /p /q /f /t /u /c /P:ProgramFiles(x86)\Ansys\AnsysDesktop.exe" ping request initiated by user username@domain.com ping HOSTNAME3 -n 1 ping domain local -n 1	Credential Access
2023-07-07 12:15	C:\Users\UserName\Desktop\Payload.ps1 was created by user username@domain.com The following contents were included in the file: "reg delete \"CURRENT_USER\\Software\\Microsoft\\Terminal Server Client\\Default\" /v /f /t /y "reg delete \"CURRENT_USER\\Software\\Microsoft\\Terminal Server Client\\Default\" /v \"REG_CURRENT_USER\\Software\\Microsoft\\Terminal Server Client\\Default\" /f /t /y attrib +x %UserProfile%\documents\Default.rpt cd %UserProfile%\documents\default.rpt if \$? { cd %SystemRoot%\system32; powershell Invoke-AutomaticDestinations	Discovery
2023-07-20 21:24		Sensitive Data Control

	Unr "USERNAME1" RDP authentication observed from the following unmanaged assets <redacted>	
--	--	--

2023-03-08 18:08	Observed RDP from remote IP "victims" on the host "VICTIM1" by the user "victims1"	Lateral Movement
2023-03-08 18:39	User DOMAIN\useradmin [C:\Users\useradmin\Desktop\AnyDesk.exe installed on victim host "VICTIM1"	Command and Control
2023-03-08 20:00	MDM receives call "victims1" for a SAM hash dump on host "VICTIM1"	Command and Control
2023-03-09 00:20	MDM receives call "victims1" (C:\Program Files\WinSxS\AnyDesk\AnyDesk.exe and services installed on victim host "VICTIM1"	Command and Control
2023-03-09 20:47	MDM receives call "victims1" for shadow copies being deleted using "vssadmin.exe /deleteall"	Detection
2023-03-09 22:00	User "VICTIM1" observed "vssadmin.exe" to execute "Delete shadow\All" against an "vssadmin" process and Royal remanence detections on host "VICTIM1"	Detection
2023-03-09 23:17	MDM receives call "victims1" for "Process Hacker and Royal remanence shadow\All" on host "VICTIM1"	Detection
2023-03-21 21:11	User "VICTIM1" observed authenticating from remote IP "victims1" on victim host "VICTIM1"	Initial Access
2023-03-21 23:34	Internal call from remote IP "victims1" to victim host "VICTIM1" and additional actions have been found across the site. Partner still requested no action be taken without permission at this time	Timeline Notable
2023-03-28 22:36	Host "VICTIM1" observed "vssadmin.exe" to execute "Delete shadow\All" on host "VICTIM1"	Timeline Notable
2023-03-28 22:40	MDM receives call "victims1" for "Process Hacker and Royal remanence shadow\All" on host "VICTIM1"	Timeline Notable
2023-03-28 22:48	Host "VICTIM1" observed "vssadmin.exe" to execute "Delete shadow\All" on host "VICTIM1"	Response Action
2023-03-29 23:26	Host "VICTIM1" observed "vssadmin.exe" to execute "Delete shadow\All" on host "VICTIM1"	Response Action
2023-03-29 04:08	User "VICTIM1" observed "vssadmin.exe" to execute "Delete shadow\All" on host "VICTIM1"	Response Action
2023-03-29 13:15	User "VICTIM1" logged onto "VICTIM1" remotely via RDP from unmanaged asset at "victims1". Subjected unmanaged asset "victims1" to "VICTIM1" based on transitive progression.	Initial Access
2023-03-29 17:52	Host "VICTIM1" observed "vssadmin.exe" to execute "Delete shadow\All" on host "VICTIM1"	Response Action
2023-03-30 00:38	SMB traffic observed from unpatched host with IP "victims1" which correlates to a time of remanence note "C:\WINDOWS" on the host "VICTIM1"	Response Action
2023-03-30 08:08	SMB traffic observed from unpatched host with IP "victims1" which correlates to a time of remanence note "C:\WINDOWS" on the host "VICTIM1"	Lateral Movement
2023-03-30 02:42	Observed Brute force attempt to the target username "VICTIM1" and the correlation to a time of remanence note "C:\WINDOWS" on the host "VICTIM1"	Credential Access
2023-03-30 00:47	SMB traffic observed from unpatched host with IP "victims1" which correlates to a time of remanence note "C:\WINDOWS" on the host "VICTIM1"	Lateral Movement
2023-03-30 00:47	SMB traffic observed from unpatched host with IP "victims1" which correlates to a time of remanence note "C:\WINDOWS" on the host "VICTIM1"	Lateral Movement
2023-03-30 00:55	SMB traffic observed from unpatched host with IP "victims1" which correlates to a time of remanence note "C:\WINDOWS" on the host "VICTIM1"	Lateral Movement
2023-03-30 02:25	MDM has had "README.txt" blocked items in Sophos Central on Partner's request	Response Action
2023-03-30 02:32	Partner and customer team's response mode from "Collaborator" to "Authorizer" allowing the MDM team to perform response actions	Timeline Notable
2023-03-30 26:36	MDM has had "AnyDesk.exe" to blocked items in Sophos Central	Response Action
2023-03-30 02:27	MDM has had "AnyDesk.exe" to blocked items in Sophos Central	Response Action
2023-03-30 05:09	MDM has had "AnyDesk.exe" to blocked items in Sophos Central	Response Action
2023-03-30 05:15	MDM has had "AnyDesk.exe" to blocked items in Sophos Central	Response Action
2023-03-30 05:15	MDM has had "AnyDesk.exe" to blocked items in Sophos Central	Response Action

Recommendations

Summary of Incident Recommendations:

- **Priority 1**
 - Install MDR on host address '`<redacted>`' - if eligible
 - Disable user '`\\servername\`' SID - `<redacted>`
 - Change the response permission to 'Authorized' in Sophos Central
 - Block the IP address '`<redacted>`' at your network perimeter
 - Remove user '`C:\Users\<redacted>\Desktop\psys64.bat`' from host '`HOSTNAME`' - if still present
 - Install MDR on the host IP address '`<redacted>`' - if eligible
 - Initiate a domain wide credential reset in the following order:
 - Domain Account
 - Service Accounts
 - All other Accounts
 - Install MDR on the host IP address '`<redacted>`' - if eligible
 - Install MDR on the host IP address '`<redacted>`' - if eligible
- **Priority 2**
 - Delete the user profile on all impacted servers for user account '`\\servername\`'
 - Confirm if 'AnyDesk.exe' is expected
 - Disable all the remote tools with Application control and enable peripharal control for the estate
 - Install MDR on the server '`HOSTNAME`' - if eligible
 - Confirm if the user '`\\servername\`' is expected on host '`HOSTNAME`'
 - Reset the credential for the user '`\\servername\`' SID - `<redacted>`
 - Remove the tool '`C:\Program Files\6809\SQL\AlwaysOn\AlwaysOn\SQLAlwaysOnService.exe`' and '`SQLAlwaysOnService\service\bin\SQLAlwaysOnService.exe`' from host '`HOSTNAME`'

During the investigation, several security issues were identified which increase the attack surface of the network. In this section we provide general recommendations to help reduce the overall attack surface.

- Do not expose any service on the WAN interface, unless necessary
- Ensure that you have enabled automatic installation of hostesses on XG Firewalls
- Enable multi-factor authentication (MFA) where possible
- Decommission/upgrade any non-compliant operating systems and applications
- Review and install security software on all computers in your environment (where applicable)
- Regularly review and perform patching across the estate for all network computers, (where applicable), accompanied by frequent auditing regarding patch compliance
- If any of a group of users is not permitted to access any network, or if already implemented, consider regular auditing of policies, with a focus on tightening controls in order to help prevent access to malicious websites / downloading of malicious files
- Lockdown RDP access with static LAN ranges, via group policy, or access control lists from static IP ranges / independent addresses
- Ensure that LAN segregation is apparent, i.e., give strong considerations towards implementing VLANs (virtual LANs)
- Regularly audit and review password policies, to enforce minimum password complexity policies across the estate (where applicable)

Actions	Description
---------	-------------

Cosa può fare Sophos MDR con Sophos e i prodotti di terze parti

Microsoft 365 response actions now available



Block/enable user sign-in

Sophos MDR analysts can lock down a user's account to prevent an adversary from accessing Microsoft 365 services and Azure resources using stolen credentials. Following clean-up, access to the user's account can be restored in seconds.



Terminate current user sessions

By immediately revoking all currently active sessions for a specific user, Sophos MDR analysts can quickly eject an attacker who has already gained access to an account and remove their ability to reuse any stolen session tokens.

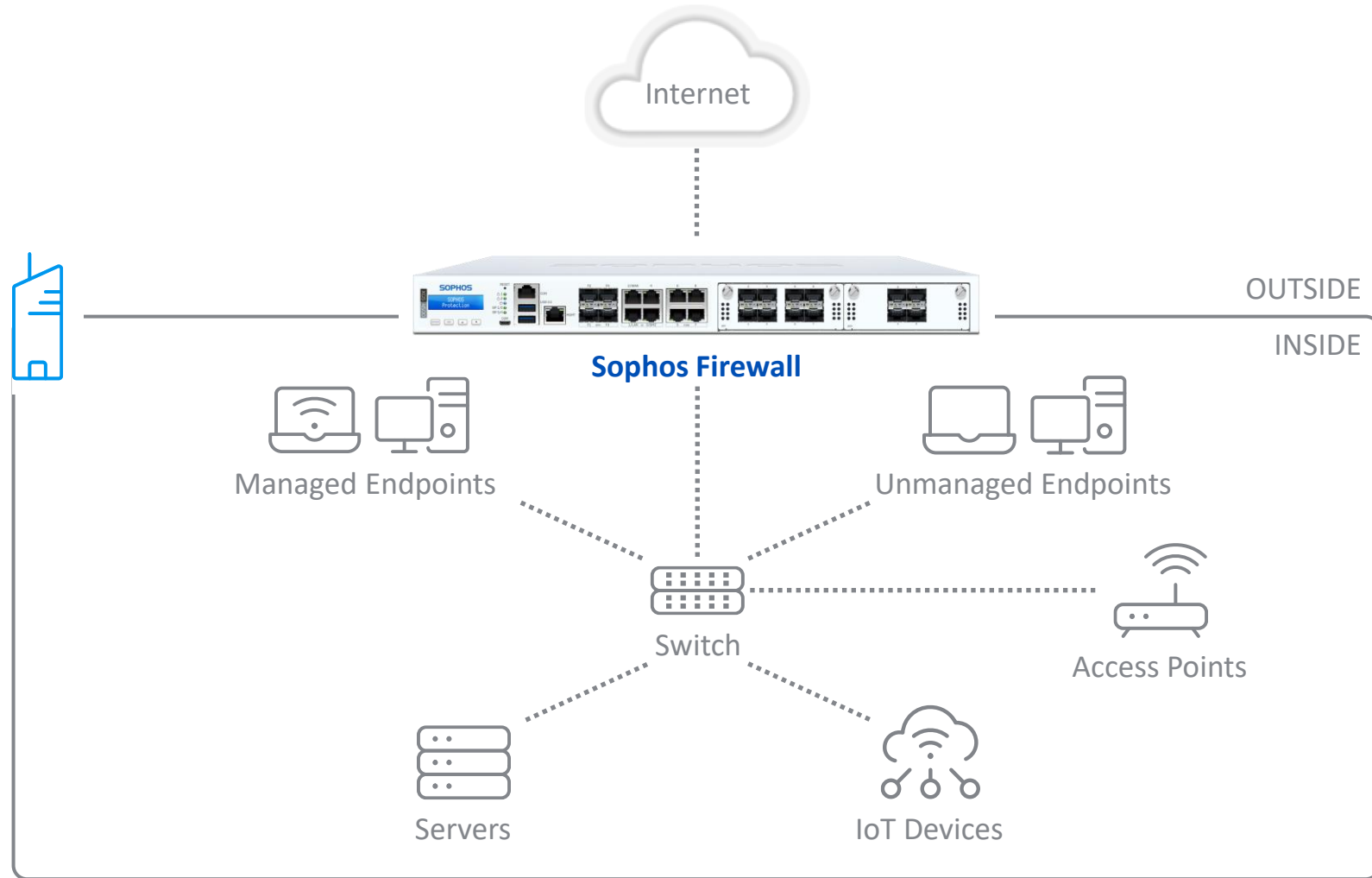
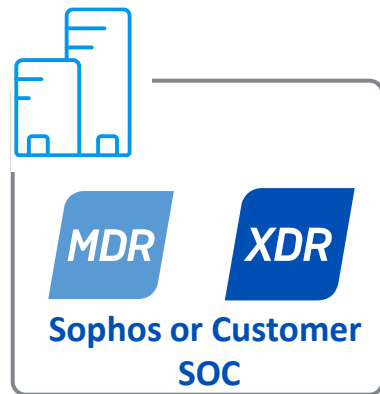


Disable suspicious inbox rules

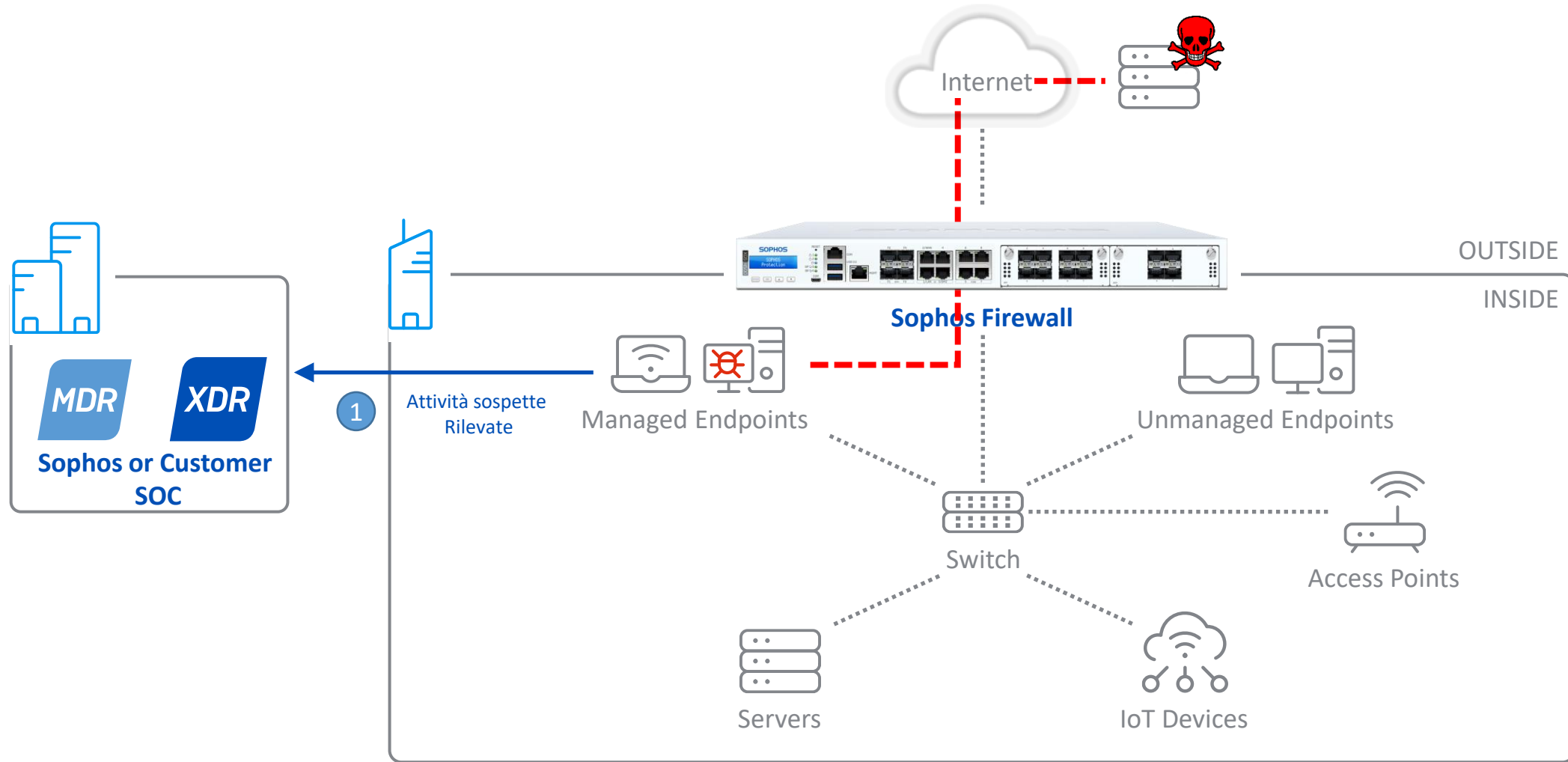
Attackers routinely set up inbox rules in Microsoft 365 for business email compromise attacks in order to move, obfuscate, or delete emails that could otherwise alert the user. Sophos MDR analysts can disable specific inbox rules to regain control.



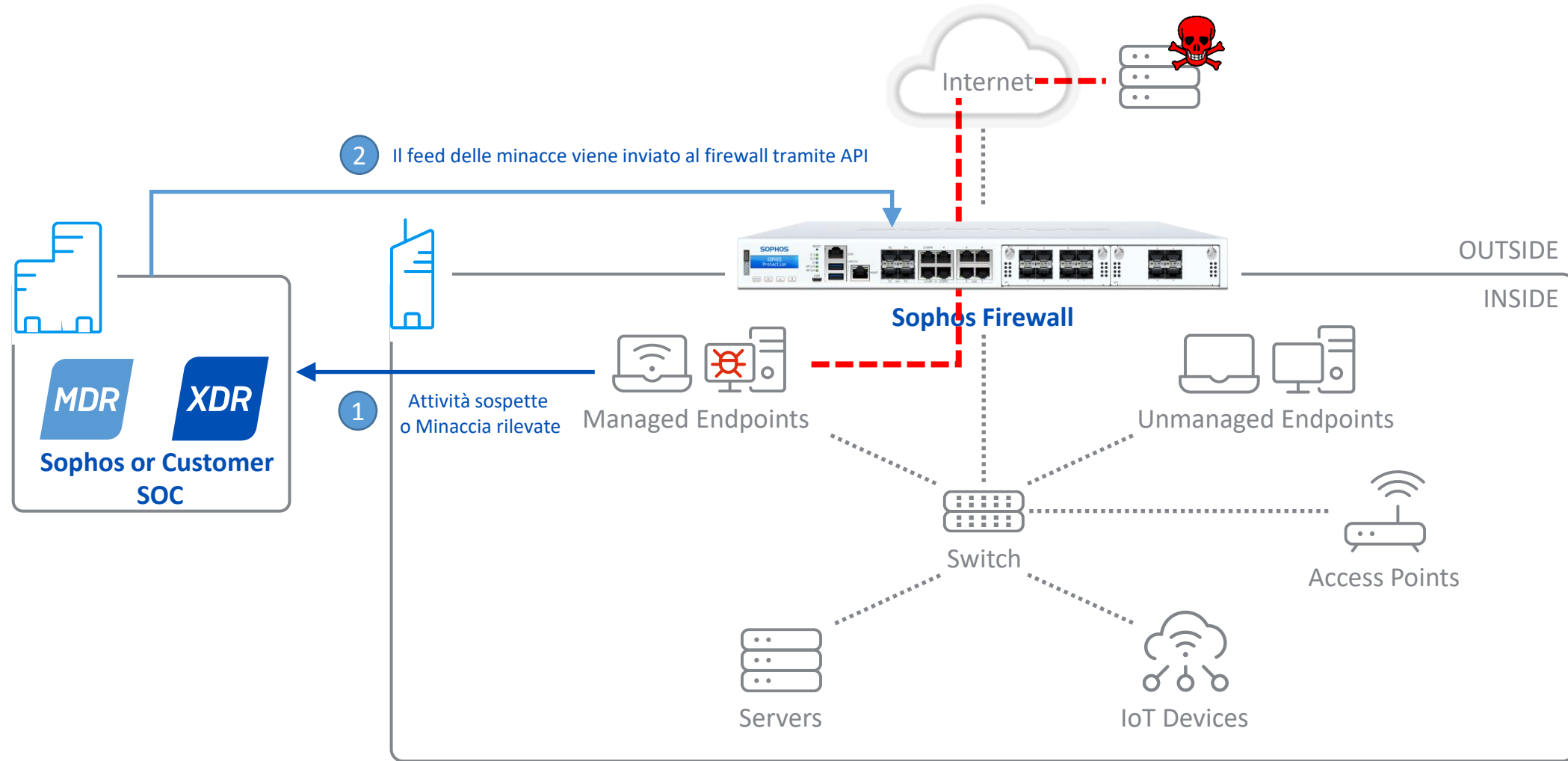
Active Threat Response in Azione (SFOS V20 release)



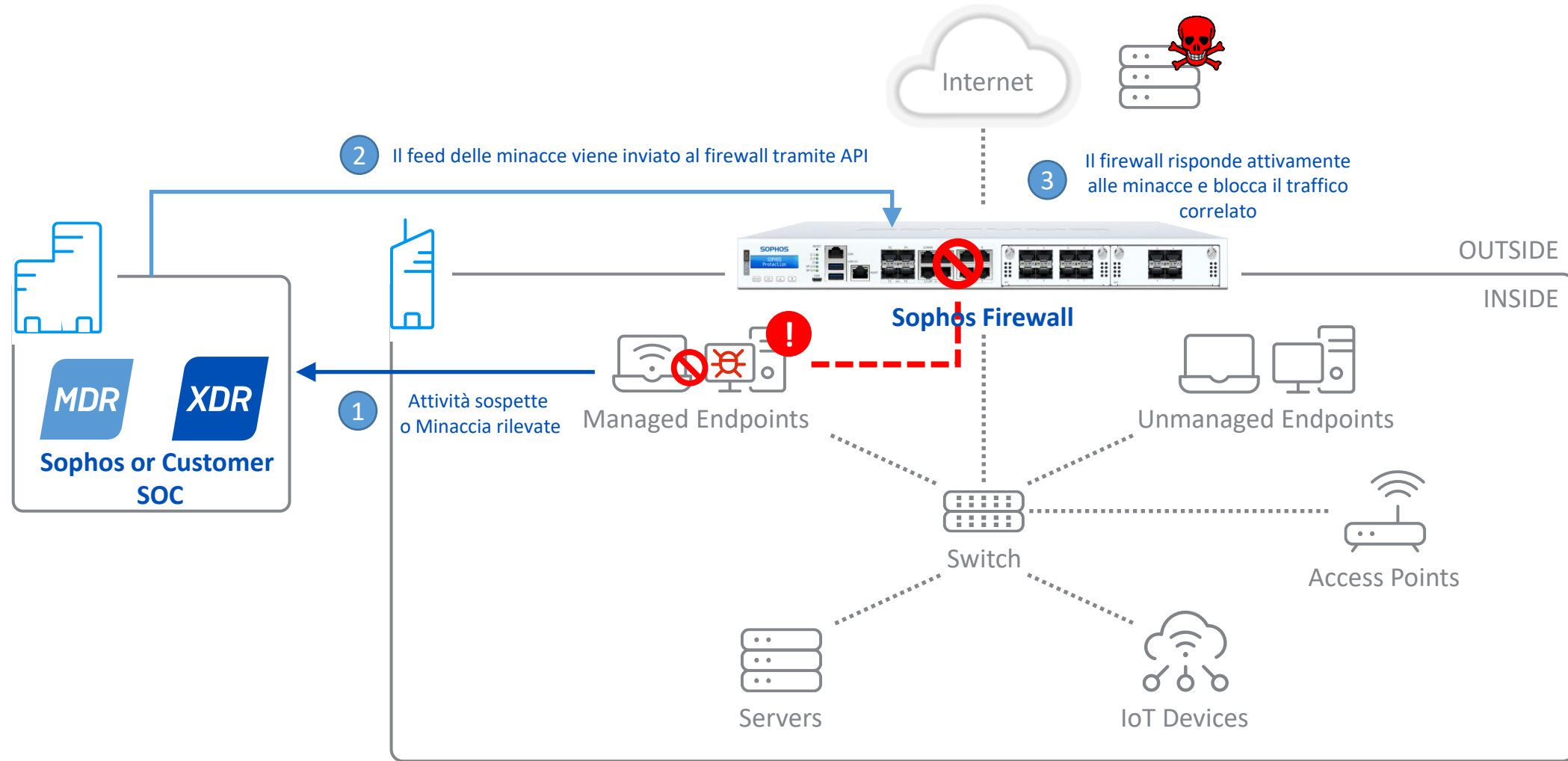
Active Threat Response in Azione



Active Threat Response in Azione

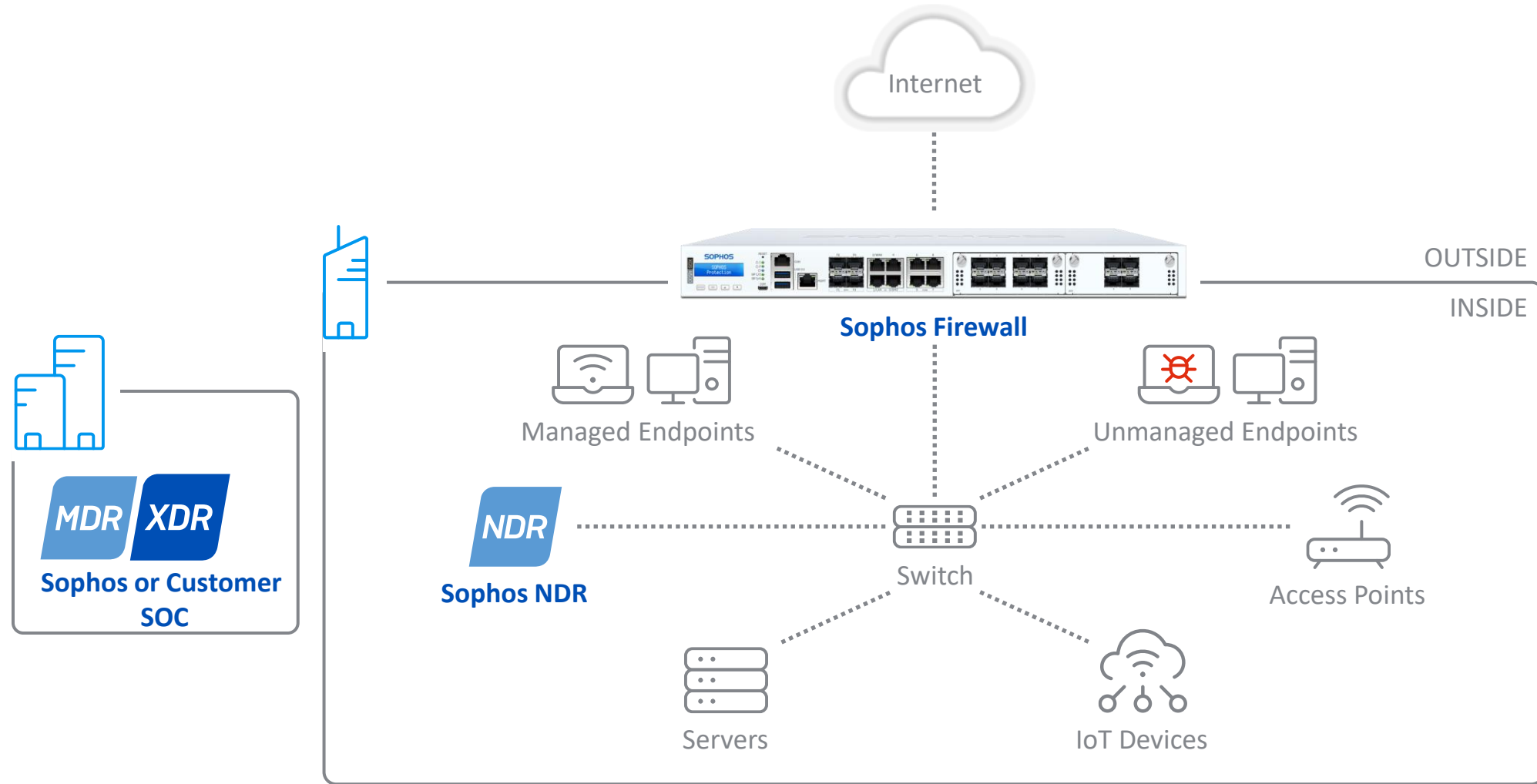


Active Threat Response in Azione



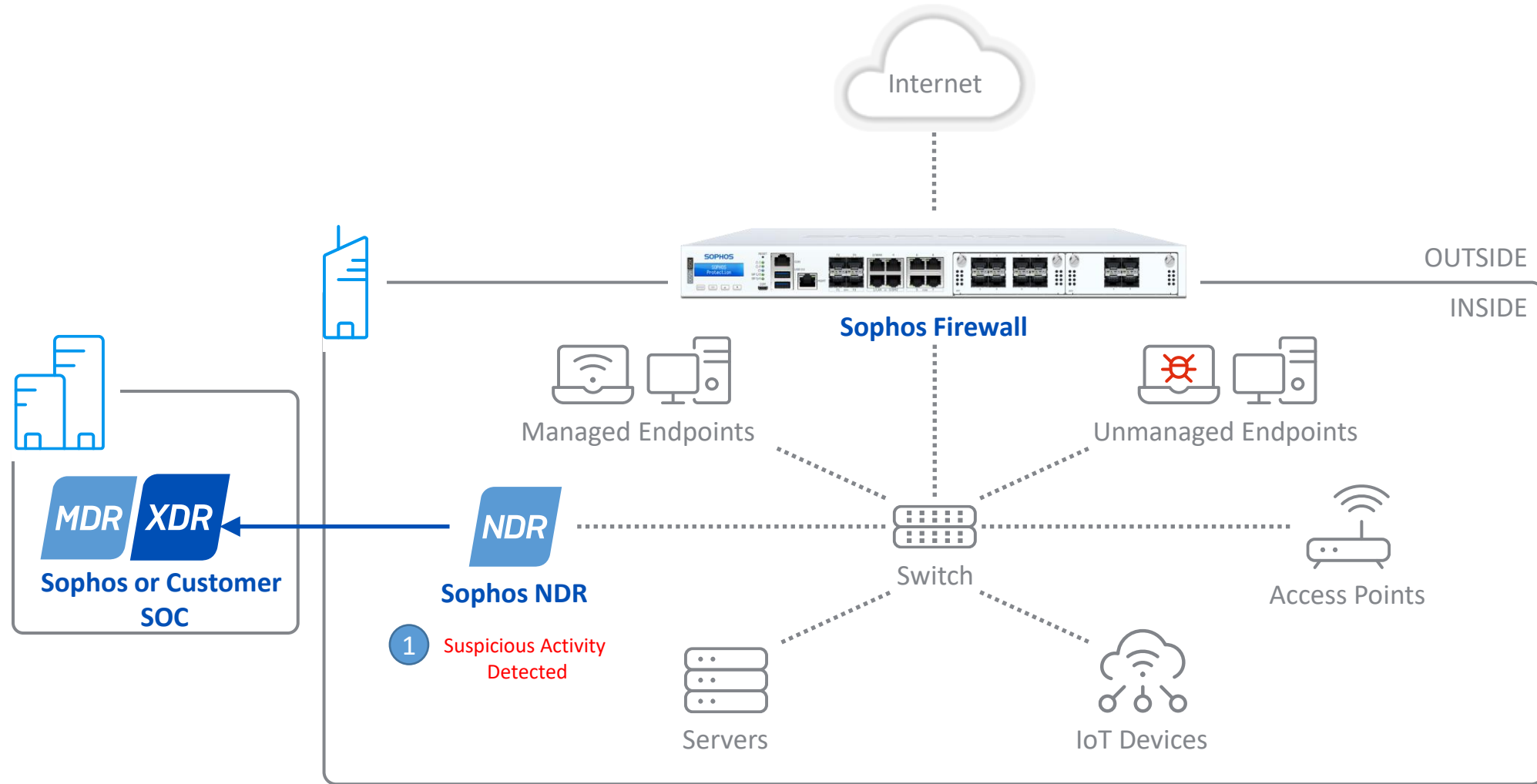
Risposta immediata: non è richiesta alcuna configurazione delle regole del firewall

Active Threat Response con rilevamento avanzato NDR



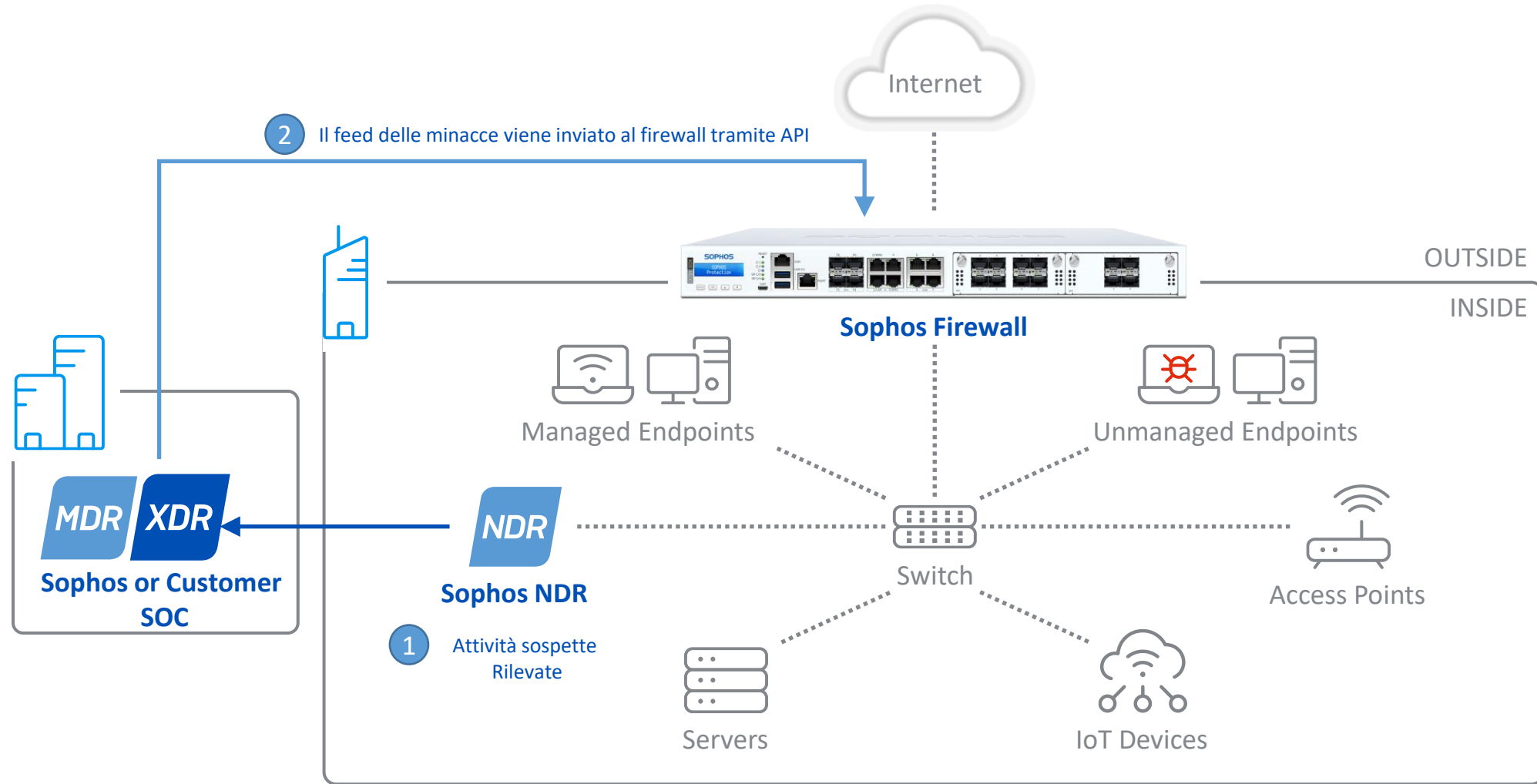
La combinazione definitiva per il rilevamento e la risposta

Active Threat Response with NDR Enhanced Detection



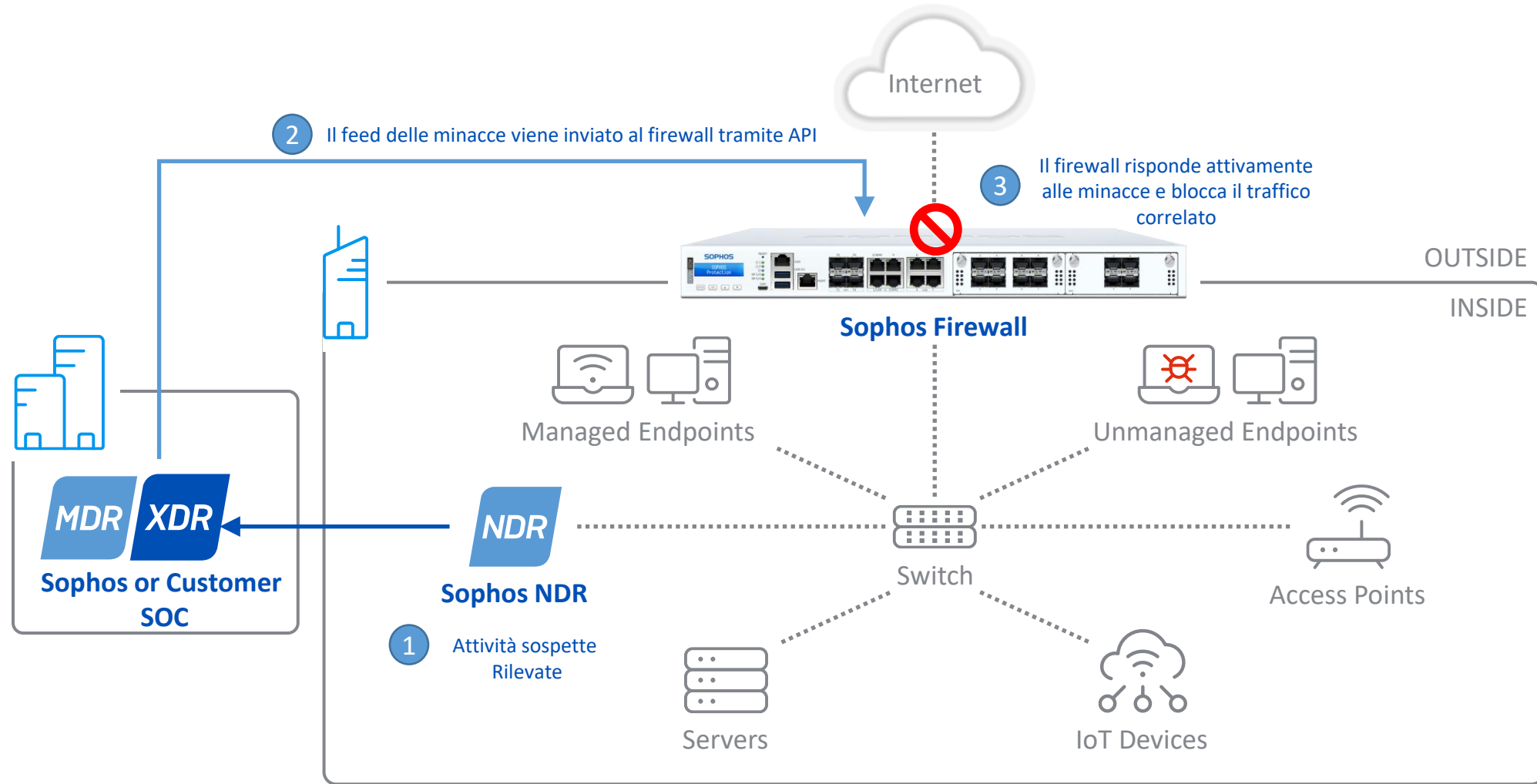
The Ultimate Combination for Detection AND Response

Active Threat Response con rilevamento avanzato NDR



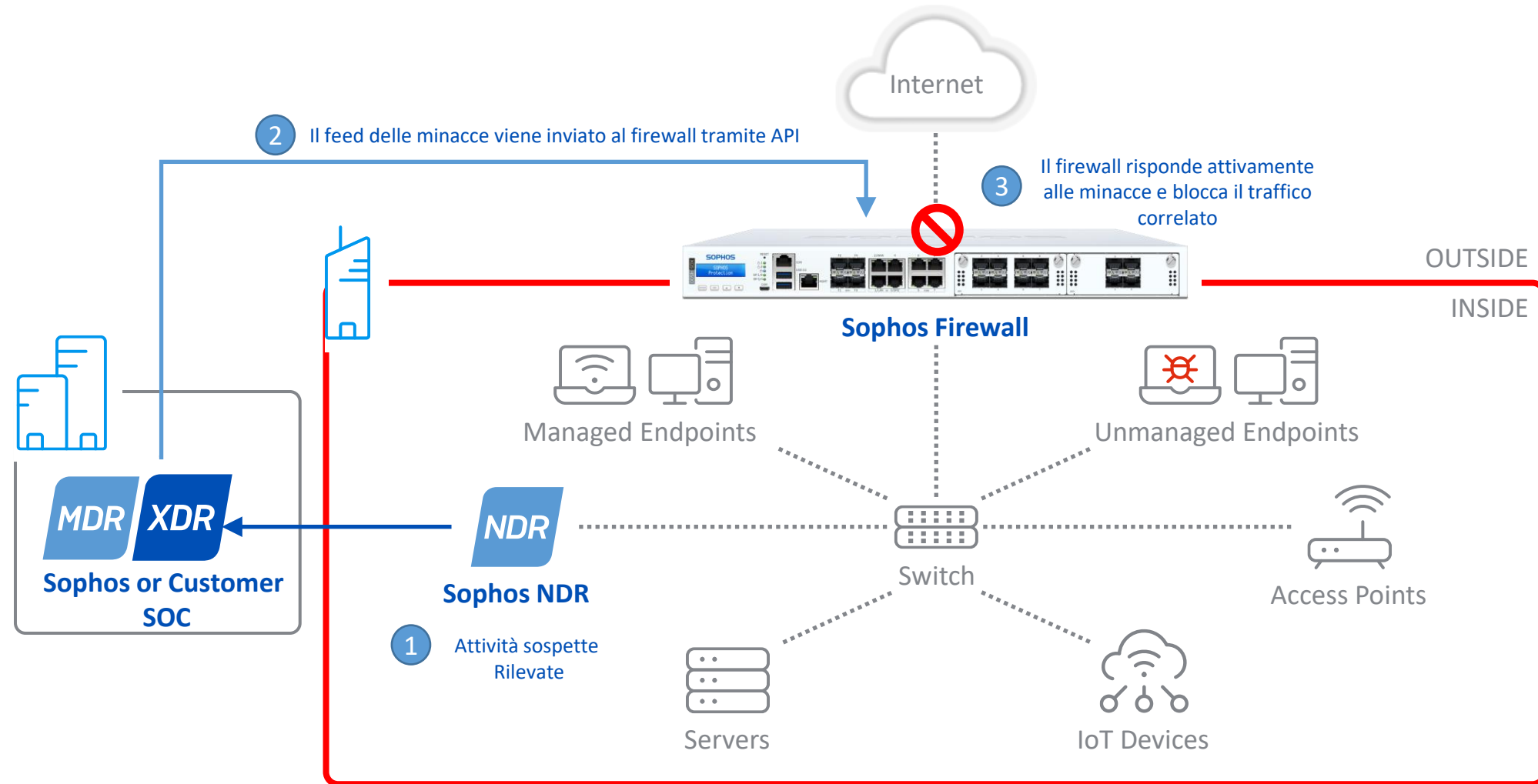
The Ultimate Combination for Detection AND Response

Active Threat Response con rilevamento avanzato NDR



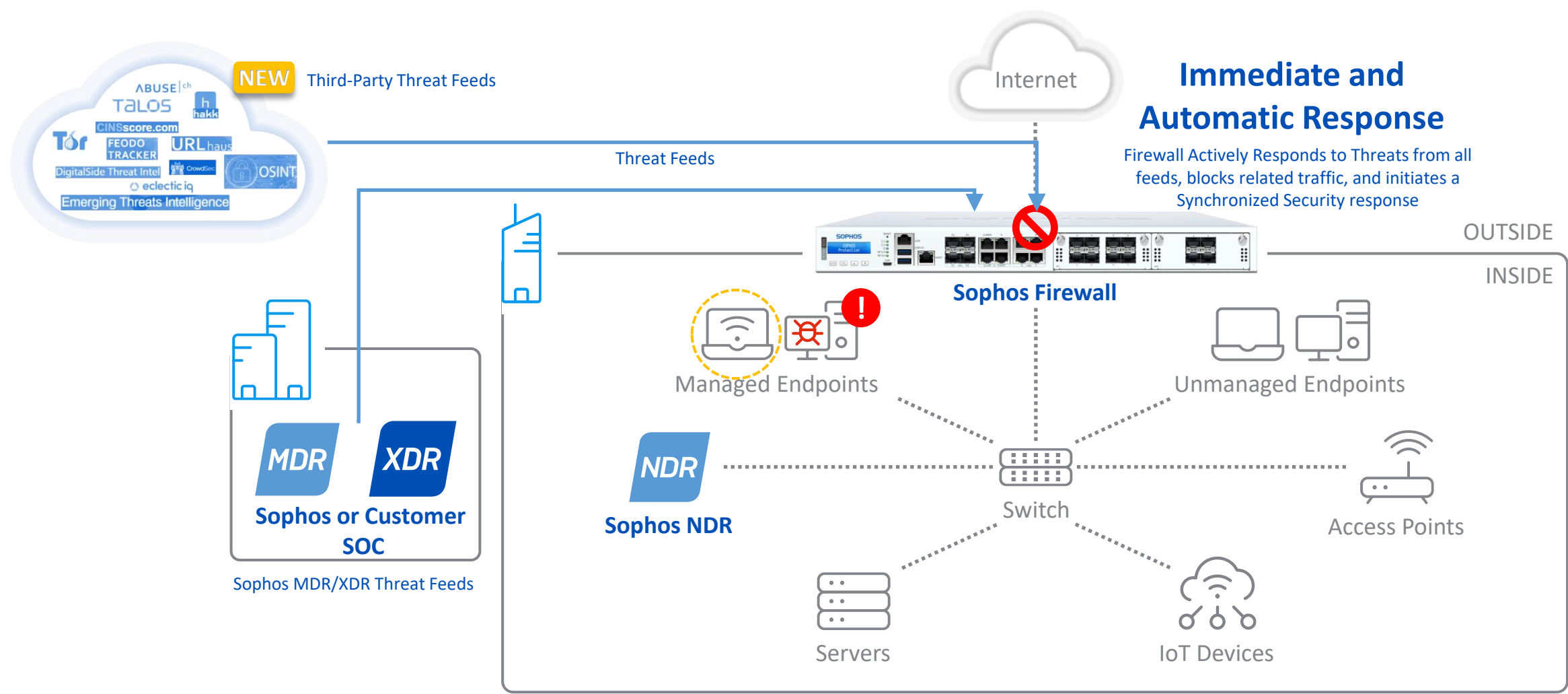
The Ultimate Combination for Detection AND Response

Active Threat Response con rilevamento avanzato NDR



The Ultimate Combination for Detection AND Response

Extending Active Threat Response



Vantaggi della Cybersecurity as a service - Sophos MDR

24/7/365

**RANSOMWARE AND BREACH
PREVENTION SERVICES**

Fully Managed by a
Team of Experts



Blocca gli attacchi avanzati guidati dall'uomo, incluso il ransomware

Our expert team stops advanced human-led attacks on your behalf, neutralizing threats before they can disrupt business operations or compromise sensitive customer data



Concentrati sulla crescita della tua attività

We monitor, detect, and respond to threats, enabling you and your IT support to focus on strategic initiatives that drive growth for your business



Dormi meglio sapendo che ci pensiamo noi

Proactive 24/7/365 threat monitoring, investigation, and response performed by a team of highly-trained analysts means you can relax knowing we have your back



Immunità di comunità

Sophos delivers MDR for over 33,000 organizations, giving us greater visibility into attacks targeting one customer and apply intel from that customer to proactively defend everyone else



Sfrutta la tua protezione esistente

Sophos MDR leverages signals from your Sophos Intercept X Endpoint protection to identify and investigate suspicious activities that may require human intervention

Problemi complessi – semplificati!

ORGANIZATION SIZE

How many users?

300

How many servers?

50

DATA RETENTION PERIOD

☐ 90 Days (included)

☒ 1 Year

SERVICE TIER

☒ **Sophos MDR Complete**

☐ **Sophos MDR Essentials**

☐ Guided Onboarding

SOPHOS INTEGRATIONS

☒ **XDR** Sophos XDR

☐ **Fw** Sophos Firewall

☐ **Em** Sophos Email

☒ **Ep** Sophos Endpoint

☐ **Cld** Sophos Cloud

☒ **NDR** Sophos NDR

THIRD-PARTY INTEGRATIONS

☐ Endpoint

☒ Firewall

☒ Microsoft

☐ Cloud

☐ Email

☐ Google Workspace

☒ Identity

☐ Network

☐ Backup

Un servizio con elevate standard globale, declinato dal tuo partner di fiducia



Key Partner **SOPHOS**



✓	⚠	Visibilità globale sulle minacce grazie alla telemetria di +600.000 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	✓

**Servizio MDR complete arricchito dai
servizi di threat response del partner**

Azioni di risposta in base al livello di servizio combinato tra Sophos ed il partner

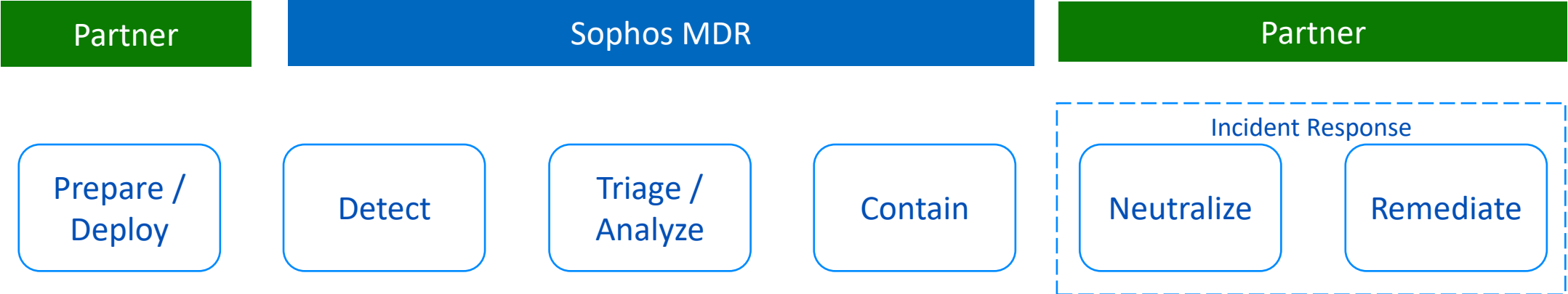
THREAT RESPONSE	INCIDENT RESPONSE	IDENTIFICARE	ACT: Identificare dove si è verificato un incidente, come è stato rilevato, l'ambito e l'impatto sul business. RECOMMEND: Azioni dei clienti per aumentare le informazioni	SOPHOS MDR COMPLETE
		CONTENERE	ACT: Isolare, se possibile, i problemi e i sistemi interessati per evitare ulteriori danni. Rimuovi tutti i malware e gli artefatti. RECOMMEND: Azioni sulle tecnologie gestite dal cliente	
		NEUTRALIZZARE	ACT: Identificare e rimuovere l'accesso ai sistemi interessati da parte dei Threat Actor tramite Root Cause Analysis RECOMMEND: Azioni dei clienti per rafforzare l'ambiente	
		AGGIORNARE	ACT: Verificare che tutti gli endpoint siano stati rinforzati RECOMMEND: Determinare un piano per mitigare il rischio di attacchi futuri con gli stessi metodi e migliorare il monitoraggio	Partner Security Operation

**Servizio MDR essential arricchito dai
servizi di cybersecurity del partner**

Azioni di risposta in base al livello di servizio combinato tra Sophos ed il partner

THREAT RESPONSE	INCIDENT RESPONSE	IDENTIFICARE	ACT: Identificare dove si è verificato un incidente, come è stato rilevato, l'ambito e l'impatto sul business. RECOMMEND: Azioni dei clienti per aumentare le informazioni	SOPHOS MDR COMPLETE
		CONTENERE	ACT: Isolare, se possibile, i problemi e i sistemi interessati per evitare ulteriori danni. Rimuovi tutti i malware e gli artefatti. RECOMMEND: Azioni sulle tecnologie gestite dal cliente	
		NEUTRALIZZARE	ACT: Identificare e rimuovere l'accesso ai sistemi interessati da parte dei Threat Actor tramite Root Cause Analysis RECOMMEND: Azioni dei clienti per rafforzare l'ambiente	
		AGGIORNARE	ACT: Verificare che tutti gli endpoint siano stati rinforzati RECOMMEND: Determinare un piano per mitigare il rischio di attacchi futuri con gli stessi metodi e migliorare il monitoraggio	
				Partner Security Operation

Partner MDR + 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 (dedicato al Key Partner MDR, per ottenere un servizio combinato tra Threat hunting e risposta agli incidenti).
Il Key Partner MDR gestisce il deploy e l'Incident response (guidato dal team Sophos MDR)

Come quantificare il ROI: l'impatto dei prodotti e dei servizi di cybersecurity sulle richieste di risarcimento assicurativo in ambito informatico

-97.5%

Una ricerca rivela che il valore delle richieste di risarcimento per la cyber-assicurazione avanzate dalle aziende che utilizzano i servizi MDR è, in media, inferiore del 97,5% rispetto a quelle delle organizzazioni che si affidano alla sola protezione degli endpoint

Flessibilità elevata – un servizio che supporta il tuo business

Expand to New Geographies



Grow your business by adding service coverage in new states or countries

Support New Environments



Add Resources



Virtually expand your team with expert operators and analysts

MDR

Extend Service Hours



Move to a 24/7/365 operation by partnering with a team that works in all regions and every time zone

Top Cybersecurity Controls

The key to insurability, mitigation, and resilience



Multifactor authentication for remote access and admin/privileged controls



Endpoint Detection and Response (EDR)



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections



End-of-life systems replaced or protected



Vendor/digital supply chain risk management

Maggiore aderenza alle compliance con Sophos MDR



Compliance con ISO/IEC 27001:2013 grazie a monitoraggio H24, rilevamento minacce, investigazione e risposta attiva



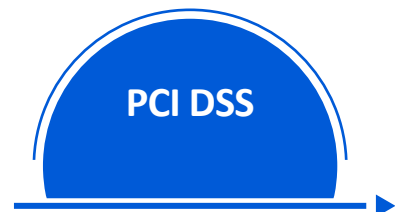
Supporto alla conformità NIS2: gestione del rischio e obblighi di reporting con MDR 24/7



Risposta rapida agli incidenti per mitigare impatti e garantire compliance GDPR



Difesa gestita 24/7 per soddisfare i requisiti del NIST Framework



Conformità alla PCI DSS v4: Sophos MDR soddisfa i requisiti chiave della sezione 10.4



Trattare dati di carte di credito implica responsabilità e conformità PCI DSS



Conformità al DORA semplificata grazie alla difesa gestita e alla risposta proattiva di Sophos MDR

MDR Service

Caso reale di attacco a un cliente 365

Sophos MDR Threat Case

Rilevamento della compromissione della posta elettronica aziendale (BEC) utilizzando i log di controllo Microsoft

ACTIVITY:

Adversary

9:07 p.m. UTC

L'attacco avviene con un'e-mail di phishing inviata a [UTENTE 1].

L'aggressore utilizza Evilginx, un framework MITM open source (man-in-the-middle) utilizzato per le credenziali di accesso al phishing e i cookie di sessione, per ottenere nome utente, password e token di autorizzazione [USER 1].

L'utente malintenzionato utilizza quindi i token di autorizzazione intercettati per eludere l'autenticazione a più fattori (MFA) [CLIENTE].

ACTIVITY:

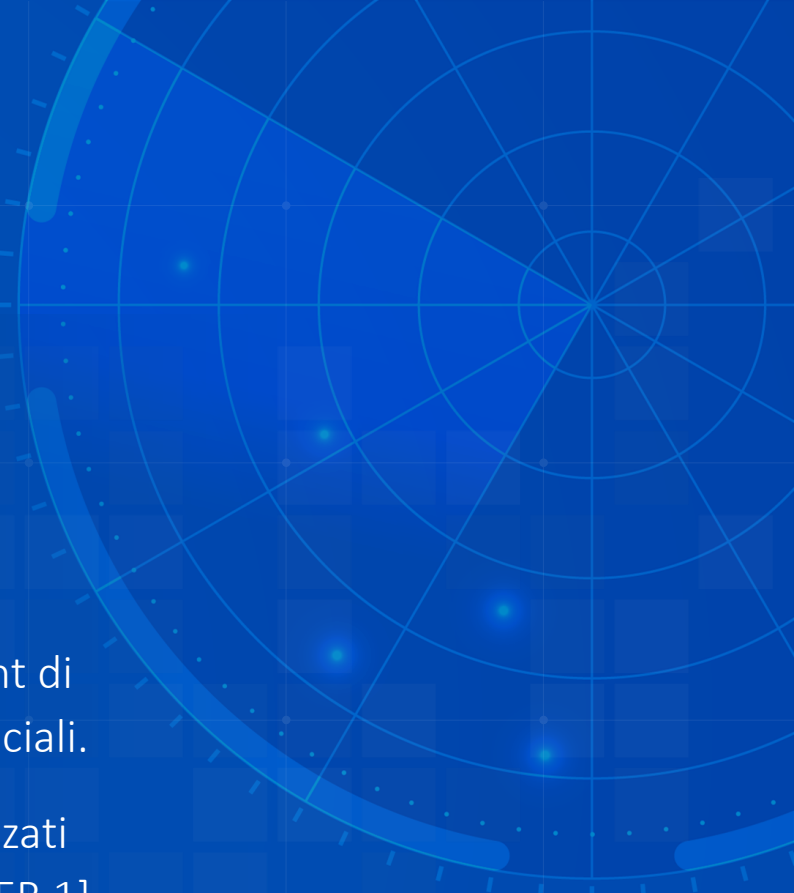
Adversary

10:19 p.m. UTC

L'utente malintenzionato crea una regola di inoltro e-mail nella casella di posta di [USER 1].

Impersonando [USER 1], l'utente malintenzionato invia una richiesta a [ADMIN 1] per convalidare l'indirizzo IP dell'utente malintenzionato, concedendo all'utente malintenzionato l'accesso a un Microsoft Dev Box in Azure.

L'utente malintenzionato inizia le attività successive all'accesso iniziale.



SOURCE:

Microsoft Audit Logs

10:20 p.m. UTC

Sophos XDR rileva la creazione di nuove regole di posta in arrivo per l'account di posta elettronica Microsoft 365 [USER 1] che contengono solo caratteri speciali.

Un ulteriore rilevamento identifica che più IP e agenti utente sono stati utilizzati all'interno della stessa sessione, indicando che l'account e la sessione di [USER 1] sono stati compromessi attraverso un attacco man-in-the-middle.



SOURCE:

Sophos Endpoint

10:20 p.m. UTC

Gli analisti di Sophos MDR indagano sulla telemetria degli endpoint associata a [UTENTE 1] e identificano comportamenti e artefatti dannosi, inclusi strumenti come Mimikatz e BloodHound, due strumenti comunemente utilizzati dagli aggressori per rubare dati sensibili e aumentare i privilegi all'interno di una rete.

ACTIVITY:

Sophos MDR Threat Response

10:26 p.m. UTC

L'analista MDR di Sophos isola l'host compromesso e sospende l'account [USER 1] per contenere l'attacco.

L'analista Sophos MDR consiglia a [CLIENTE] e [PARTNER CLIENTE] di reimpostare le credenziali dell'utente compromesso.

Gli analisti di Sophos MDR conducono una risposta agli incidenti su vasta scala per determinare l'accesso iniziale e rimuovere tutti gli artefatti dannosi utilizzati nell'attacco.

GRAZIE!

