Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Far fronte all’evoluzione dei cyberattacchi con un nuovo approccio alla sicurezza informatica

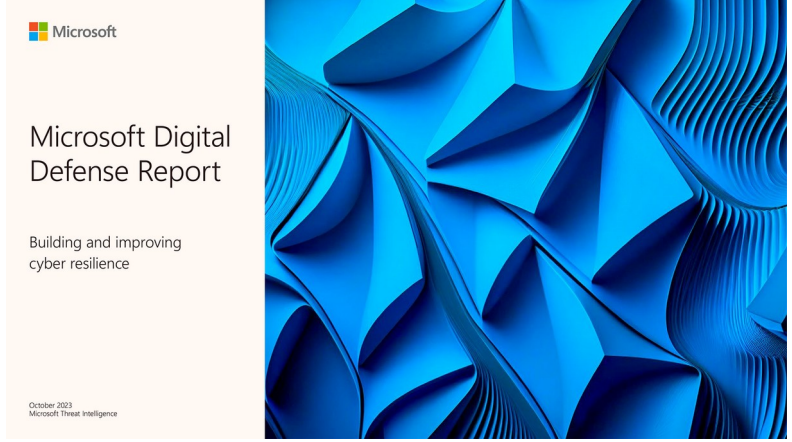
Walter Narisoni, Director Sales Engineer South EMEA, Sophos

Luca Bechelli, Clusit

19 marzo 2024 orario 12:00-13:00

Le cyber minacce

SOPHOS



L'80-90% di tutte le compromissioni ha origine da dispositivi non gestiti.

Il 70% delle organizzazioni che si sono imbattute in ransomware gestiti dall'uomo aveva meno di 500 dipendenti.

Source: https://www.microsoft.com/security/security-insider/microsoft-digital-defense-report-2023

Avversari attivi

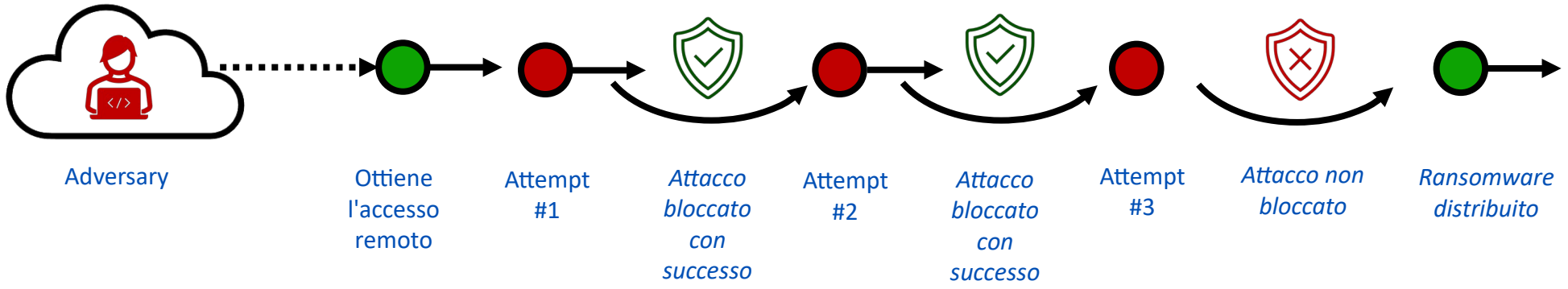
Avversari attivi

Implementano diversi approcci innovativi, tra cui:

- Sfruttare i punti deboli della sicurezza per penetrare nelle organizzazioni e spostarsi lateralmente
  - Incluse credenziali rubate, vulnerabilità prive di patch e configurazioni errate degli strumenti di sicurezza
- Abuso di strumenti IT legittimi per evitare di attivare rilevamenti
  - Inclusi PowerShell, PS Exec, e RDP
- Modificare i loro attacchi in tempo reale in risposta ai controlli di sicurezza

23%

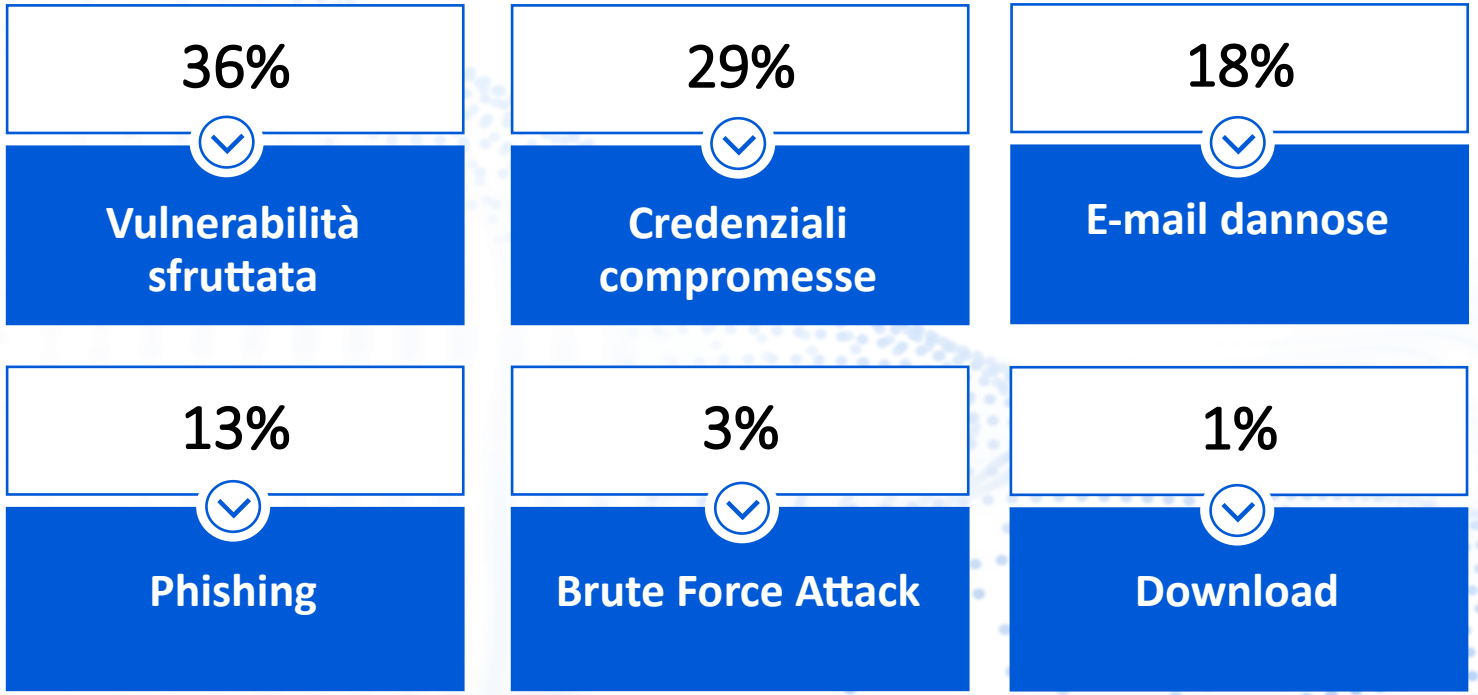
ha subito un attacco che ha coinvolto un avversario attivo nell'ultimo anno



Source: The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos

Gli avversari non irrompono.
Accedono.

Causa principale degli attacchi ransomware 2023



Source: The State of Ransomware 2023, Sophos. Responses from 1,974 organizations hit by ransomware in the last year

Credenziali rubate vendute sul dark web

Stolen Access Data For Sale

SOPHOS

Ref	Date Surfaced	Victim	Country/ Region	Industry	Details	Price (USD)	Samples
1	2-Jul-22	Not named	Indonesia	Banking	VPN access (user)	2,000	No
2	25-Jan-22	Not named	Hong Kong	Online shopping	RDP access to domain (user)	400	No
3	10-May-22	Not named	Singapore	Restaurants/hospitality	RDP access to domain (local admin)	2,500	No
4	11-Oct-21	Not named	Singapore	IT/Telecoms/Security	Local admin access to shared folders/drives, 2TB of data (bank statements, txns, IT, HR)	9,000	No
5	4-Jul-22	****	Mexico	Education	Citrix local admin access		
6	14-Jul-22	****	Turkey	Government	Access to gov account/email of Director of **** De		
7	7-Jul-22	Not named	Asia	Not known	Outlook accounts		
8	8-Jun-22	Not named	UK	Construction	RDP/VPN access		
9	22-Jun-22	****	Not known	Not known	50 Confluence accesses (CVE-2022-26134)		
10	23-Jun-22	Not named	Middle East	Pharmaceutical	Credentials to access Citrix Gateway and sites; dom creds; BloodHound files; backup creds; DA creds or ($5000 USD extra)		
11	15-Aug-21	Not named	Singapore	Transport/logistics	Access		
12	14-May-22	Not named	Canada	Education	VPN access		
13	19-Mar-22	****	Bangladesh	Military	Access to 3000 hosts, domain controller, database portals, emails		
14	18-Jul-22	Not named	Europe	Construction	Remote command-line access		
15	10-Jul-22	Not named	Brazil	IT/Telecoms/Security	RDP access		

Stolen Credentials For Sale

SOPHOS

Ref	Date surfaced	Name	Country/Region	Industry	# of records	Credentials	Price (USD)	Samples
1	27-Jul-22	****	Not known	N/A	50,000	Wordpress details: user rights, URL, username, password	10,000	No
2	23-Jul-22	Not named	Canada	N/A	1,200	Name, job title, address, phone number, SSN, email, gender, DOB, hiring details	15,000	Yes
3	15-Jul-22	Not named	Australia	N/A	1,000	Passports	3,000	No
4	25-Jun-22	****	China	Restaurant/ hospitality	54,00,000	Username, email, mobile number, gender, address	1000	Yes
5	6-Jun-22	Not named	UK	N/A	37,600	Scans of driver licences, passports, IDs	25,000	Yes
6	18-Jul-22	****	Germany	Retail	5,00,000	Email, name, DOB, password	Not known	Yes
7	27-Jul-22	****	Thailand	Insurance	32,80,000	369GB of data: customer records, agent data, ID card, DOB, name, address, mobile number, email, policy data	Not known	Yes
8	6-Jul-22	****	Argentina	Medical	1,20,00,000	Personal and medical data from a hospital	1,500	Yes
9	25-Jul-22	****	Spain	Gaming	2,814	Username, email, IP, password, salt	Not known	Yes
10	19-Jul-22	****	US	Gaming	6,90,00,000	Source code, database (DOB, IP, name, gender, email, passwords)	85,000	No
11	27-Jul-22	Not named	UK	N/A	500	Driving licences, passport, medical certificates	Not known	Yes
12	3-Apr-22	Not named	Singapore	Banking	17,01,940	Bank account database	3,500	No
13	11-Apr-22	****	Malaysia	Government	8,02,259	Data from election commission: name, ID, email, phone, DOB, address, password, selfie/card photo	2,000	Yes
14	6-May-22	****	Singapore	Telecoms	5,25,968	ID cards, selfies, other docs, possible accesses	20,000	No
15	1-May-22	****	Turkey	Religion	76,000	Email, password	250	Yes

Source: Sophos X-Ops

Mancanza di esperienza

93%

Trova impegnativa l'esecuzione di attività di sicurezza essenziali

71%
Trova difficile identificare i segnali dal rumore (cioè, su quali avvisi indagare)

75%
Trova difficile identificare la causa principale di un incidente

52%
Affermano che le minacce informatiche sono ora troppo avanzate per essere affrontate dalla propria organizzazione

66%
Affermano che la gestione degli incidenti di sicurezza ha avuto un impatto negativo su altri progetti IT

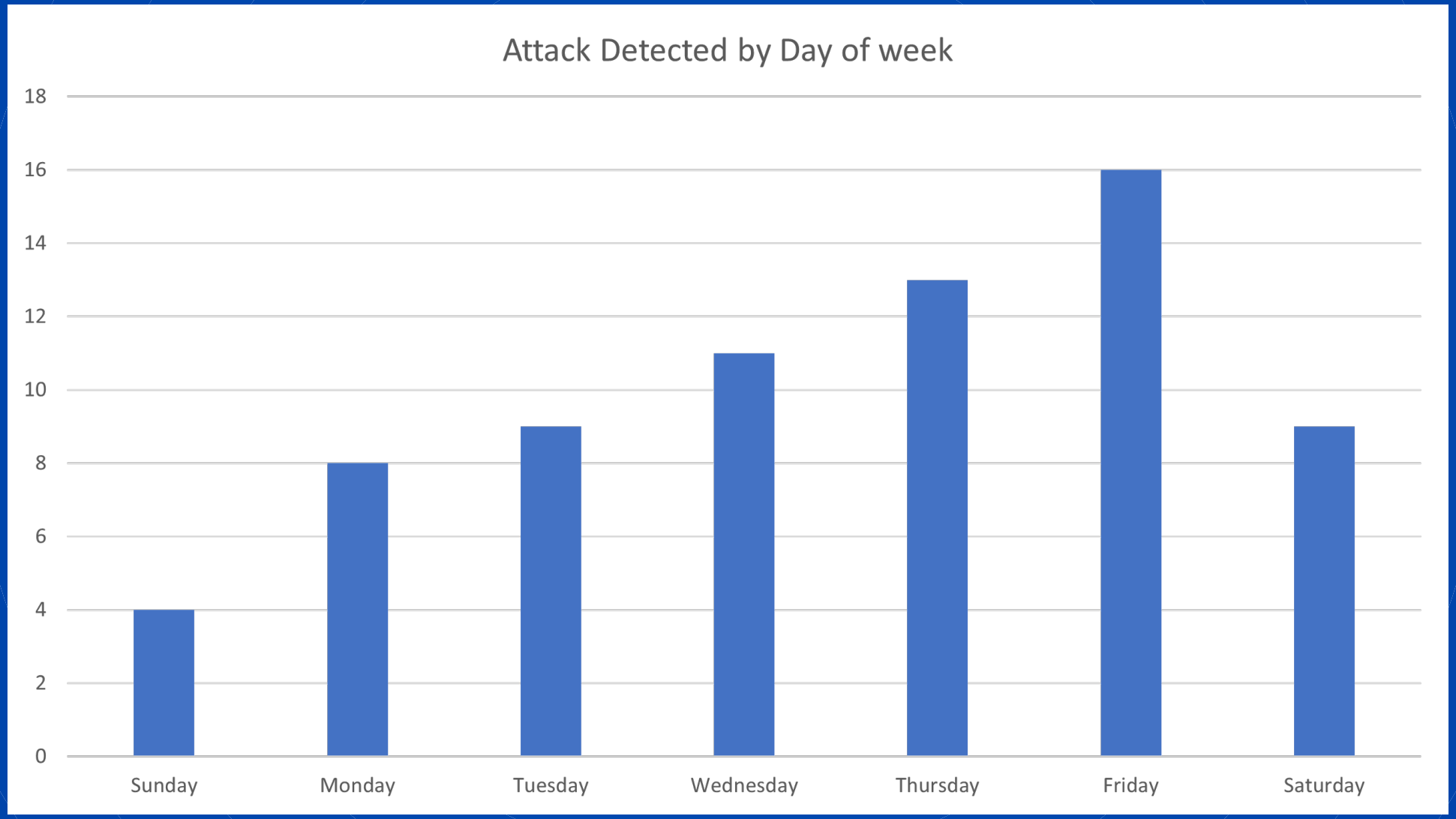
Source: The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos

Tempo di permanenza

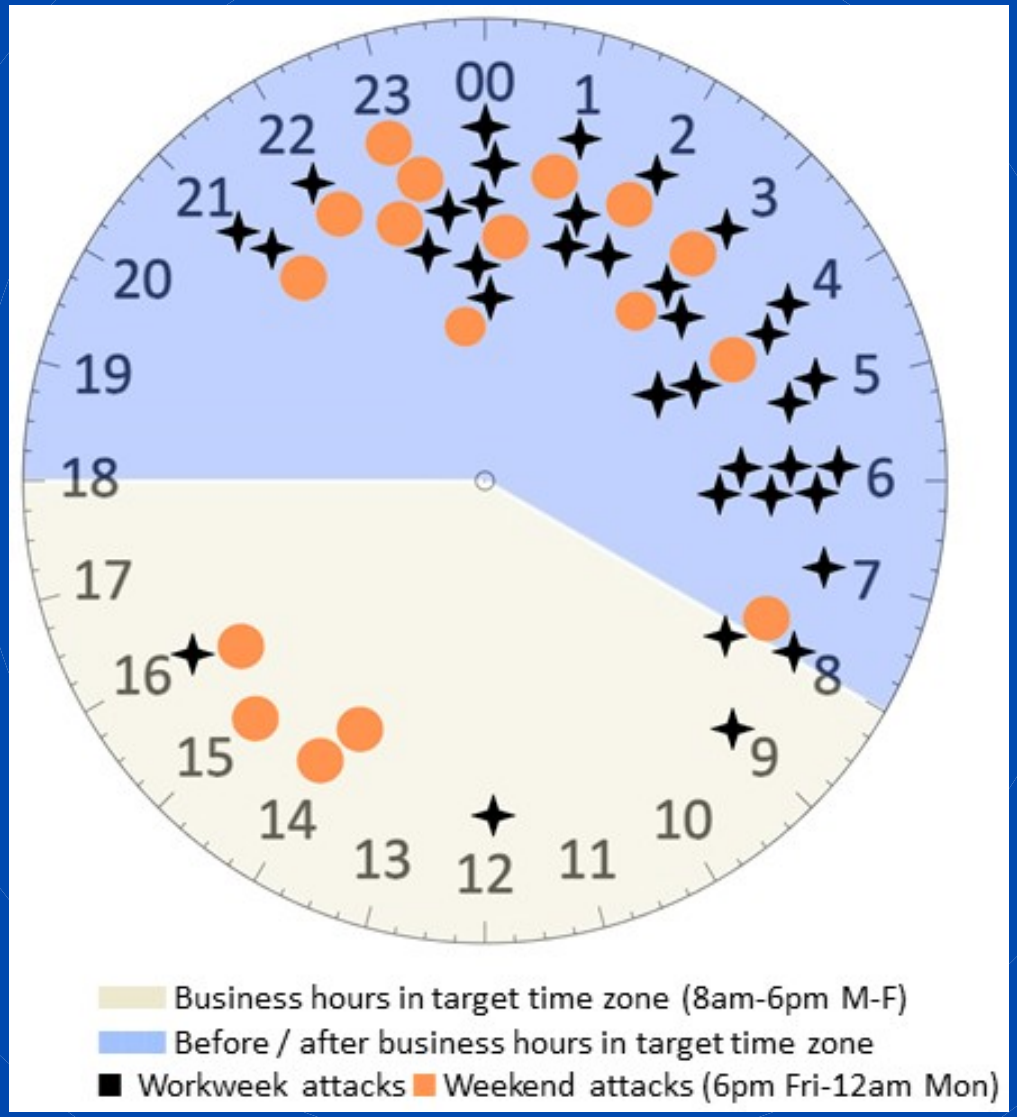
Tempo di permanenza del ransomware

SOPHOS

Attacco rilevato: giorno della settimana



Ora del giorno – ora locale



SOPHOS

Cinque attacchi più veloci

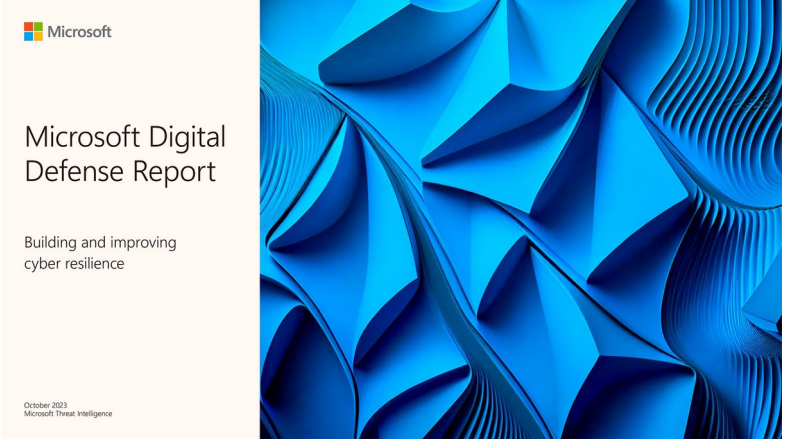
9 ore 7 minuti 30 secondi - Black Basta

5 ore 56 minuti 18 secondi - Blackbyte

2 ore 41 minuti 20 secondi - Blackbyte

2 ore 2 minuti 26 secondi - LockBit

1 ora 45 minuti 1 secondo - Royal



Microsoft Threat Intelligence ✓
@MsftSecIntel

RaaS affiliates continue to use techniques that minimize their footprint: 60% of attacks observed by Microsoft in the past year used remote encryption to evade process-based remediation, and 13% involved exfiltrating data for ransom without ever deploying a ransomware payload.

6:12 PM · Nov 3, 2023 · **1,442** Views

Il 60% degli attacchi ransomware gestiti dall'uomo ha utilizzato la cifratura remota.

Gli aggressori si stanno evolvendo per ridurre ulteriormente la loro impronta.

Source: https://www.microsoft.com/security/security-insider/microsoft-digital-defense-report-2023

L'87% degli incidenti ransomware ha avuto la cifratura remota

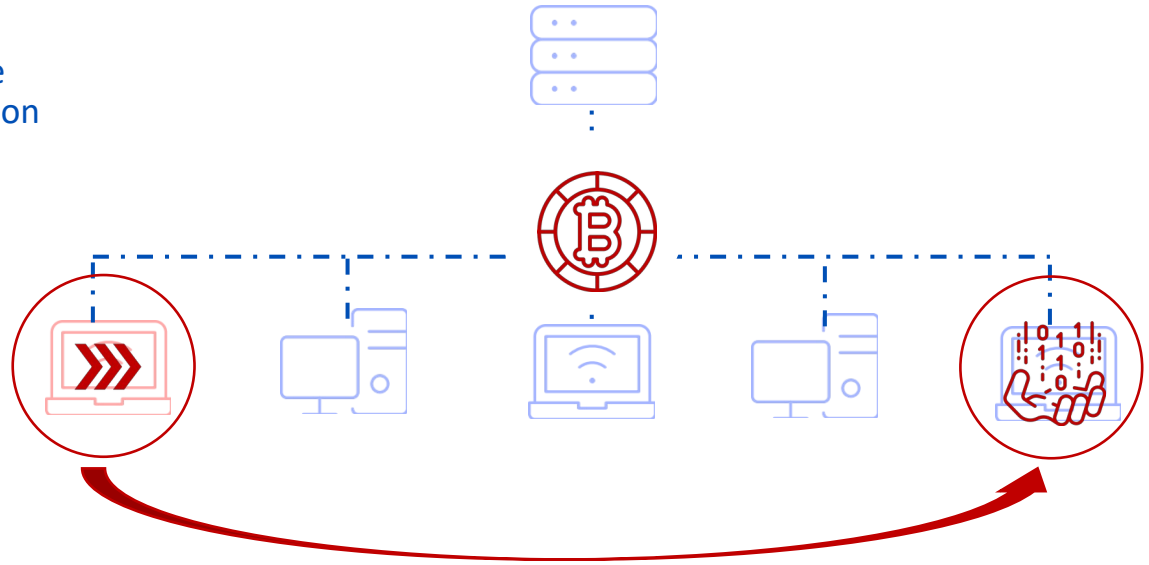
Il ransomware remoto è una minaccia crescente

Gli avversari compromettono un dispositivo e lo utilizzano per **crittografare in remoto i dati su altri dispositivi** sulla stessa rete.

La maggior parte delle soluzioni endpoint sono inefficaci poiché si concentrano sul rilevamento di file e processi dannosi sull'endpoint protetto.

Un singolo endpoint compromesso può esporre **l'intero patrimonio** al ransomware, anche se tutti gli altri dispositivi sono protetti.

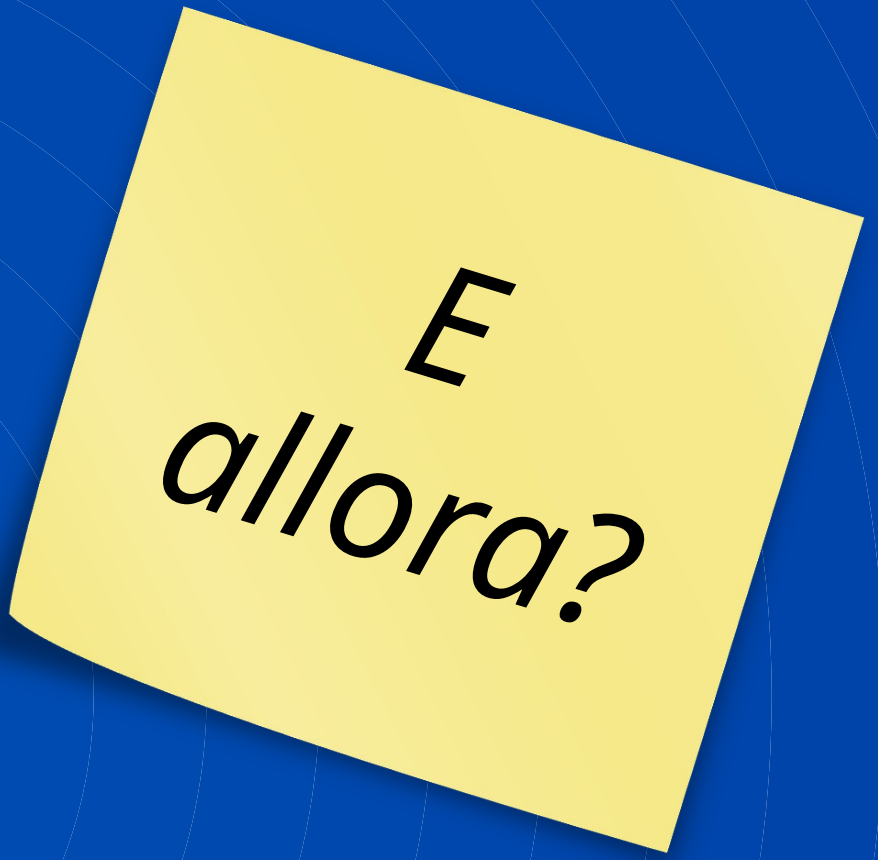
1. Compromettere un dispositivo non gestito o non protetto
2. Identificare i dispositivi protetti che desiderano crittografare sulla stessa rete
3. Esegue processi per crittografare in remoto i dispositivi protetti
4. Crifra i file su il dispositivi protetti
5. Invia una richiesta di riscatto alla vittima



SOPHOS

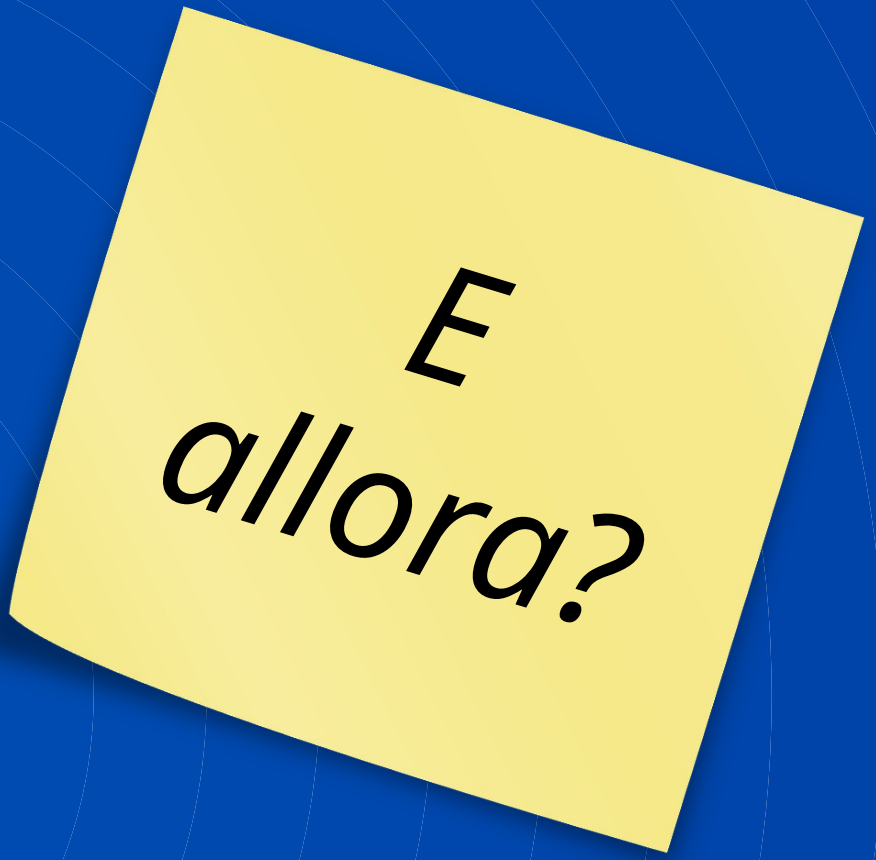
Secure. Monitor. Respond.

Aumenta l'attrito



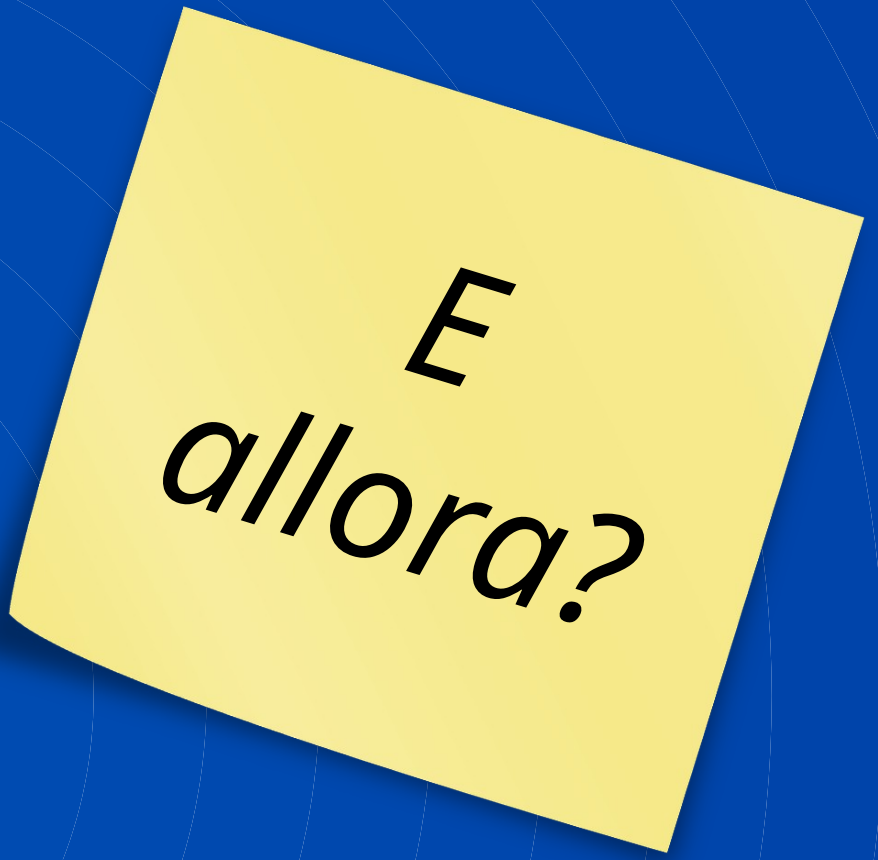
Secure. Monitor. Respond.

Aumenta l'attrito
Proteggi tutto!



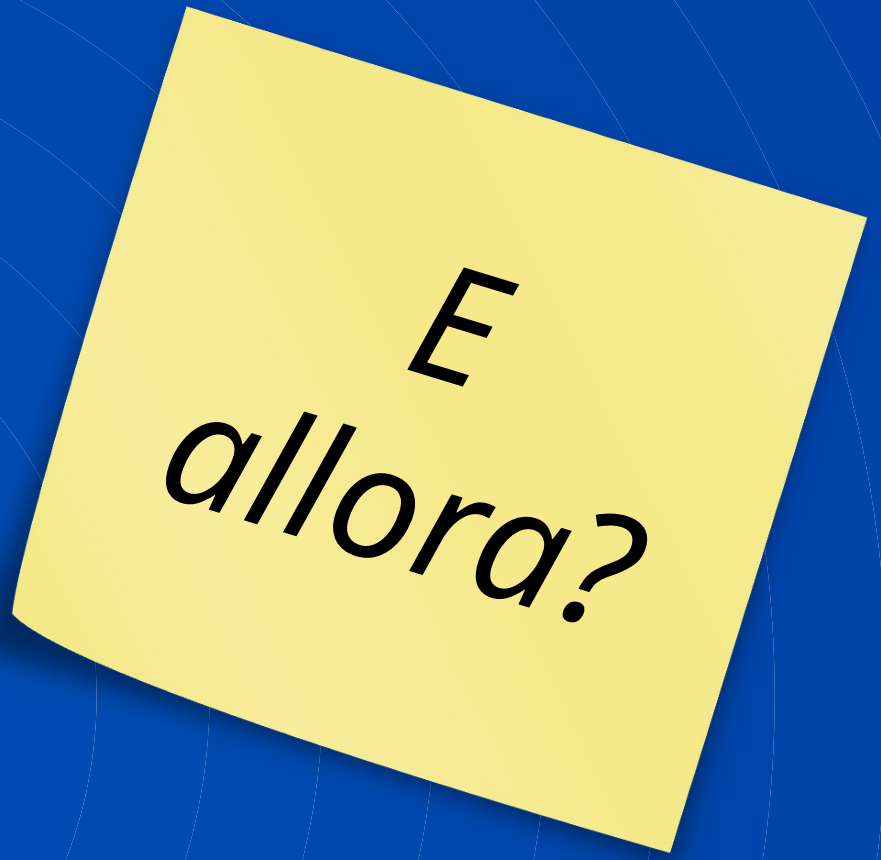
Secure. Monitor. Respond.

Aumenta l'attrito
Proteggi tutto!
Stai sempre attento



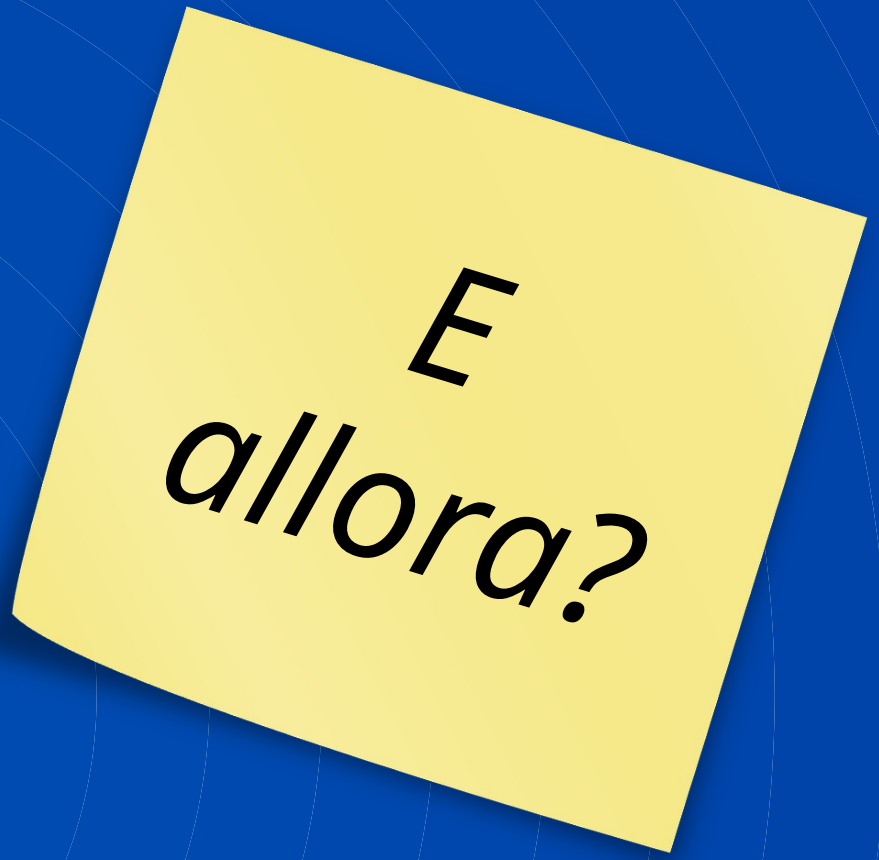
Secure. Monitor. Respond.

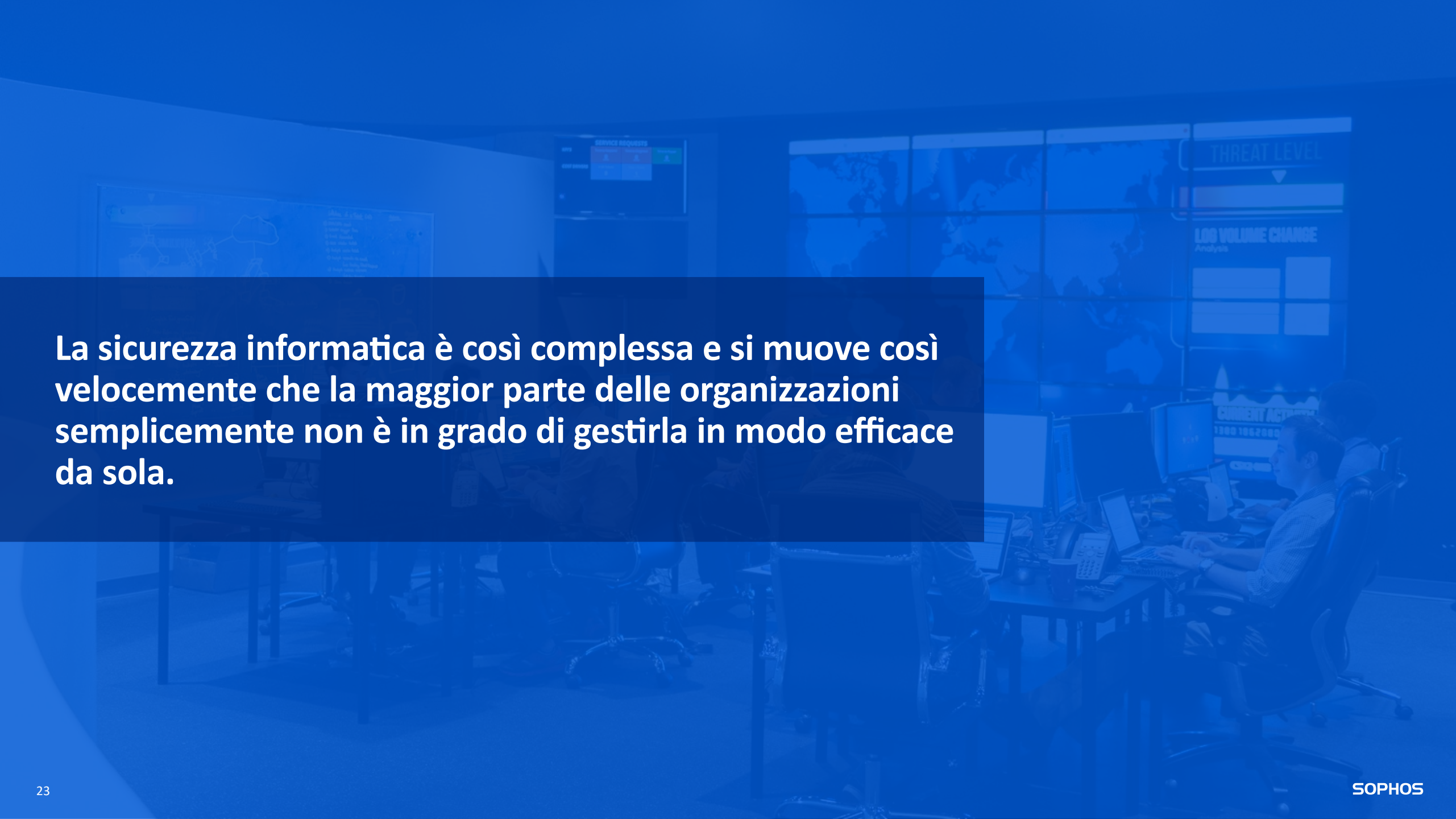
Aumenta l'attrito
Proteggi tutto!
Stai sempre attento
Preparati a indagare



Secure. Monitor. Respond.

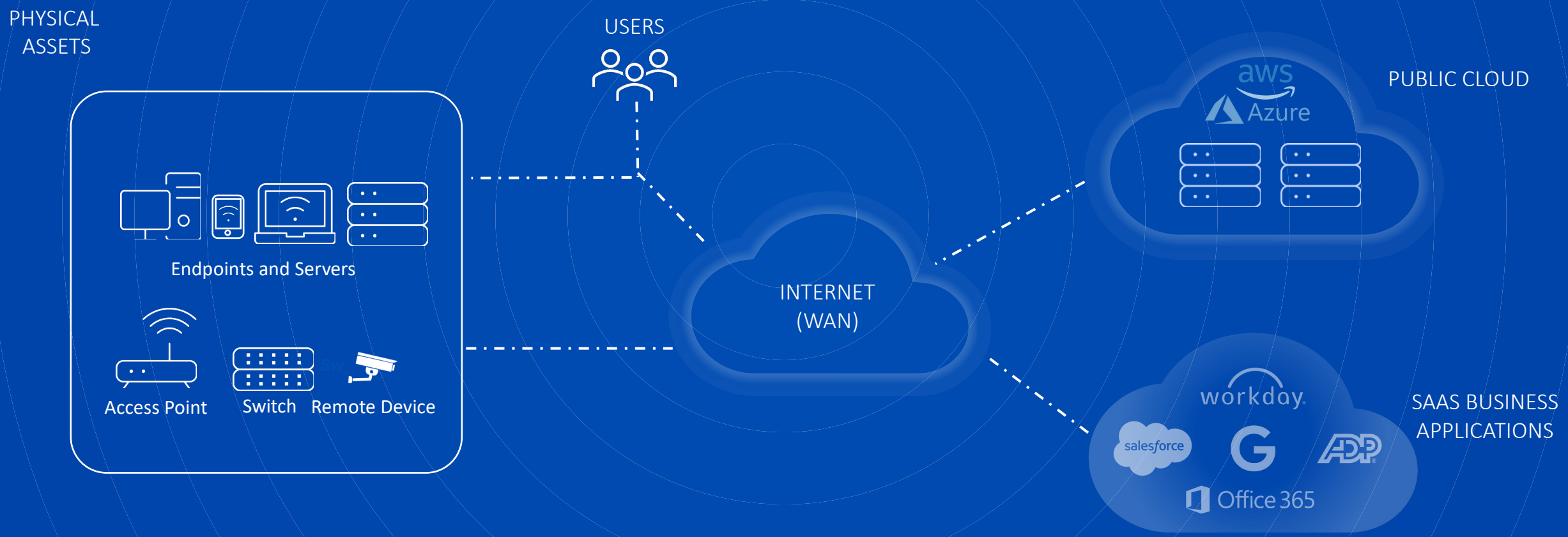
Aumenta l'attrito
Proteggi **tutto!**
Stai sempre attento
Preparati a indagare
Possiedi un piano





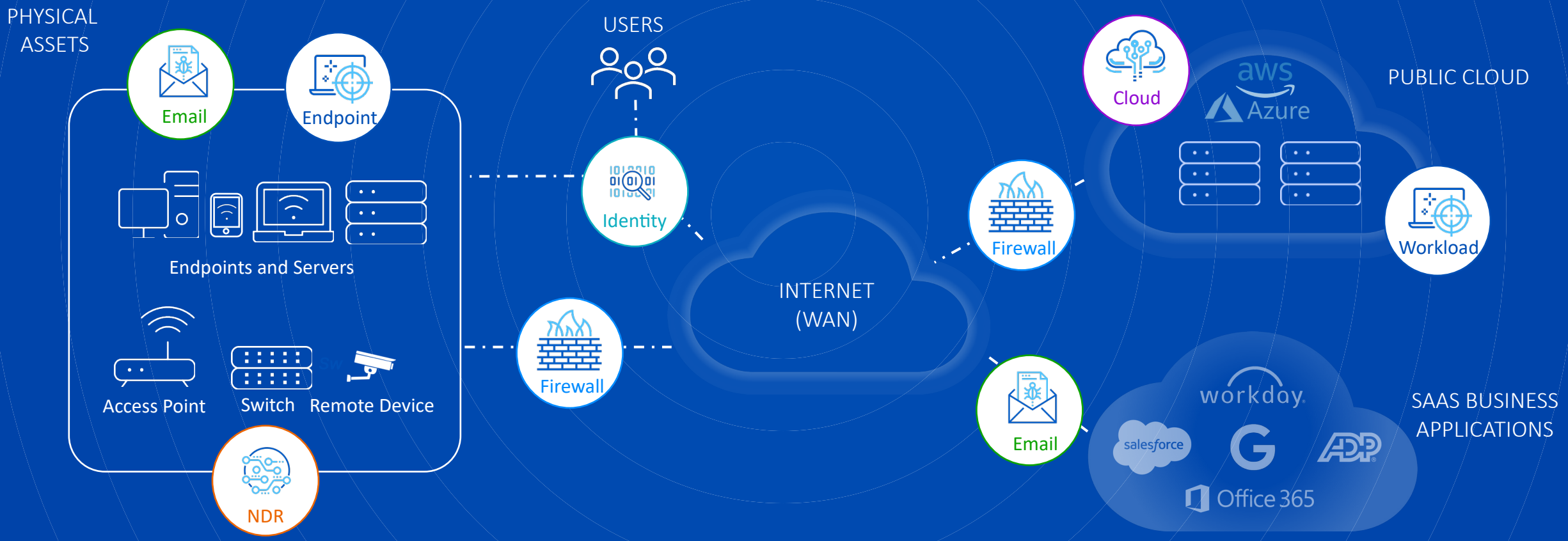
La sicurezza informatica è così complessa e si muove così velocemente che la maggior parte delle organizzazioni semplicemente non è in grado di gestirla in modo efficace da sola.

Gli ambienti odierni sono complessi e dispersi



SOPHOS

Gli strumenti di sicurezza sono distribuiti in tutto l'ambiente



SOPHOS

Sophos Managed Detection and Response (MDR)

Un servizio completamente gestito, 24 ore su 24, 7 giorni su 7, fornito da oltre 500 esperti di minacce specializzati nel rilevamento e nella risposta agli attacchi informatici che le soluzioni tecnologiche da sole non possono prevenire

Sophos MDR

Caccia alle minacce

La caccia proattiva alle minacce eseguita da analisti altamente qualificati scopre ed elimina rapidamente più minacce di quelle che i prodotti di sicurezza possono rilevare da soli

Rilevamento delle minacce

Abilitato da funzionalità estese di rilevamento e risposta (XDR) che rilevano minacce note e comportamenti potenzialmente dannosi ovunque risiedano i dati

Risposta agli incidenti

I nostri analisti rispondono alle minacce in pochi minuti, sia che tu abbia bisogno di una risposta completa agli incidenti o di assistenza per prendere decisioni più accurate

20.000+ clienti MDR

99,98% delle minacce bloccate *

Tempi medi di risposta alle minacce di Sophos MDR

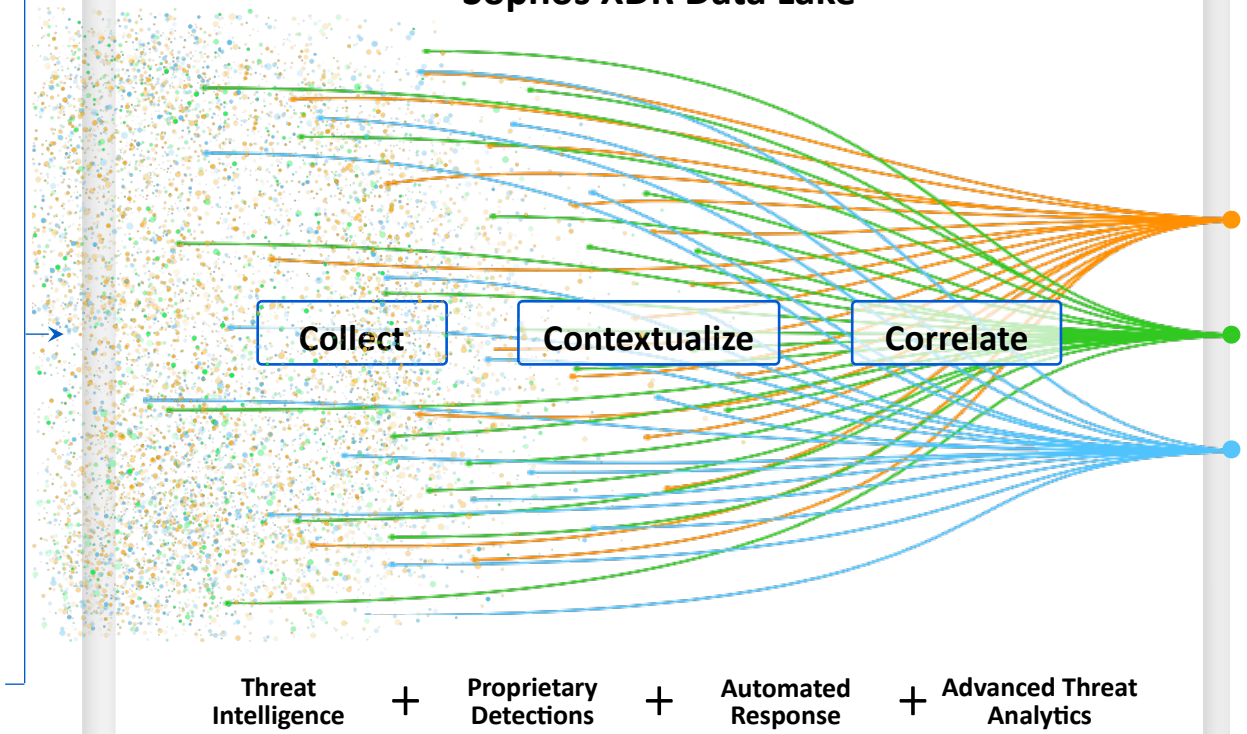
Tempo di rilevamento	Meno di 1 minuto
Tempo per investigare	Meno di 25 minuti
Tempo di Disposta	Meno di 12 minuti

Sophos MDR

Origini eventi di sicurezza Microsoft

- 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
- **Non-Microsoft Telemetry Sources**

Analisi delle minacce, correlazione e definizione delle priorità



Sophos MDR

Servizi gestiti di rilevamento e risposta 24 ore su 24, 7 giorni su 7

Risposta alle minacce guidata dall'uomo

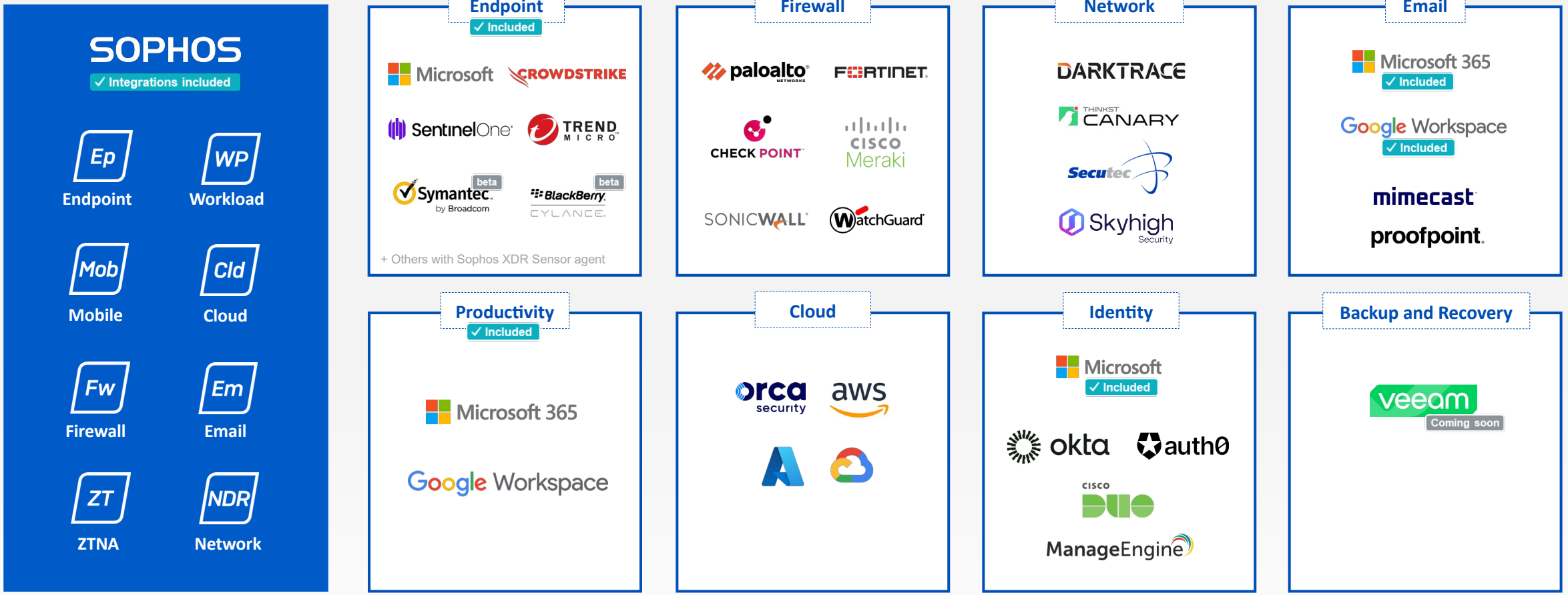
Proattiva
Caccia alle minacce

Indagine sulle minacce e analisi

Reportistica settimanale e mensile

Intelligence proprietaria sulle minacce

Visibilità su tutte le principali superfici di attacco



Le soluzioni Sophos Endpoint e Sophos Workload Protection sono incluse in Sophos XDR e MDR. Altre integrazioni di prodotti Sophos richiedono un abbonamento alla soluzione applicabile.

Le integrazioni di terze parti con Endpoint, Microsoft e Google Workspace sono incluse negli abbonamenti a Sophos XDR e MDR senza costi aggiuntivi. Gli Integration Pack per altre soluzioni non Sophos sono disponibili come abbonamenti aggiuntivi per ogni categoria di integrazione. La licenza si basa sul numero totale di utenti e server.

Updated: January 11, 2024

Sophos NDR

Dispositivi non protetti

Dispositivi non autorizzati

Minacce IoT/OT

Attacchi zero-day

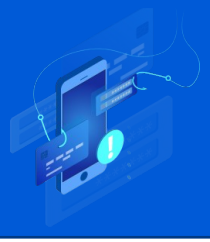
Minacce interne

La sicurezza degli endpoint

Intercept X adatta le tue difese in risposta a un attacco

Protezione preventiva

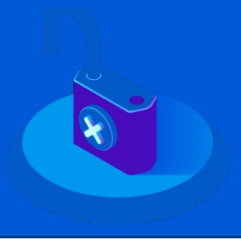
Delivery



Exploitation

Installation

Command



Actions

Pre-Breach

- Web Control
- Web Protection
- Intrusion Prevention System
- Peripheral Control
- Download Reputation

- Local Privilege Mitigation
- Application Lockdown
- Side Loading
- CTF Protocol
- Code Mitigations
- Memory Mitigations
- APC Mitigations

Post Breach

- Pre-execution Behavior
- Machine Learning
- Live Protection
- Anti-Malware
- Clean and Block
- AMSI
- Server Lockdown
- Process Protections
- PUA
- Application Control

- Credential Theft Protection
- Dynamic Shellcode
- Safe Browsing
- Malicious Traffic Detection

- Runtime Behavior Analysis
- Data Loss Prevention
- MFA Cookie
- Server FIM
- Anti-Ransomware
- Automatic + Manual client isolation

Blocca il ransomware sul nascere

Prevenzione del ransomware basata sul comportamento

Tecniche dei ransomware

Il ransomware si presenta in molte forme

Cifratura via sovrascrittura

Cifratura intermittente

Cifratura remota

Cifratura a livello di boot

Sophos Intercept X

Blocca il ransomware indipendentemente dalla fonte

Identifica le modifiche ai file indicative di ransomware

Rileva la crittografia da file, script o applicazioni attendibili

Termina il processo ed esegue il rollback dei file cifrati

Blocca il ransomware distribuito da altre macchine

Protezione adattiva dagli attacchi

Difese che si adattano dinamicamente a un attacco guidato dall'uomo

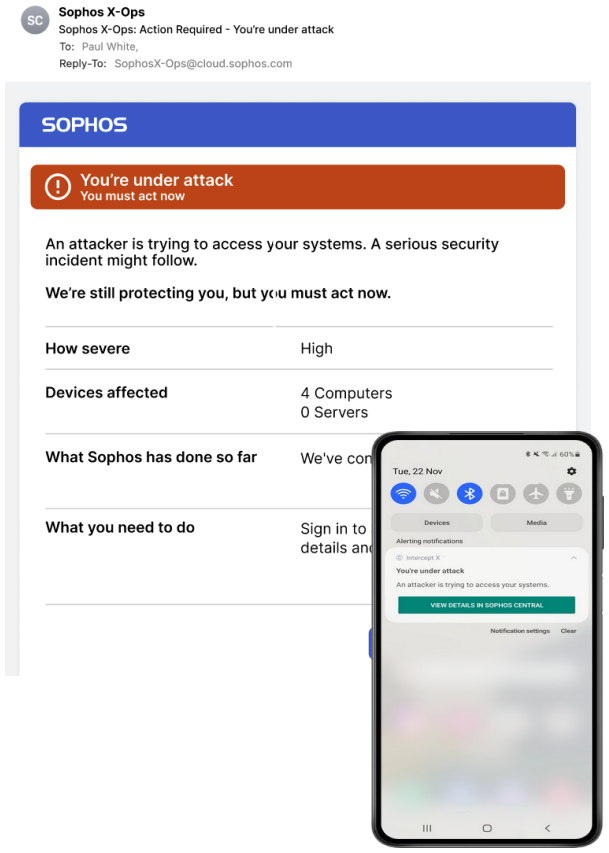
Se non viene ostacolato, un utente malintenzionato con le mani sulla tastiera ha maggiori possibilità di raggiungere i propri obiettivi

- Adaptive Attack Protection applica dinamicamente una protezione altamente aggressiva che interromperebbe le attività quotidiane

Difesa sensibile al contesto: Critical Attack Warning

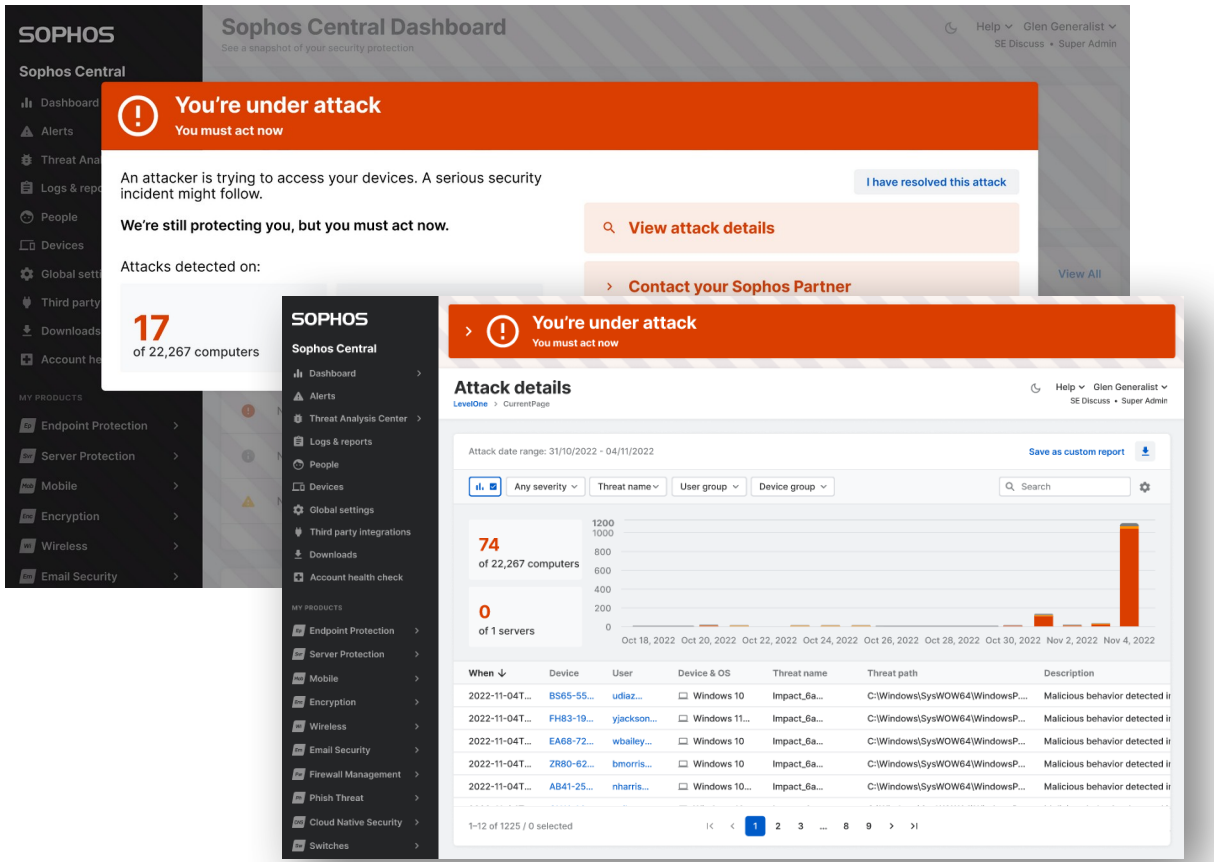
Notifica

Notifiche rapide al cliente via e-mail e cellulare



Informa

Fornisce il contesto e i dettagli dell'attacco



Risolve

Chiedi assistenza a Partner, Incident Response, o self-remediation

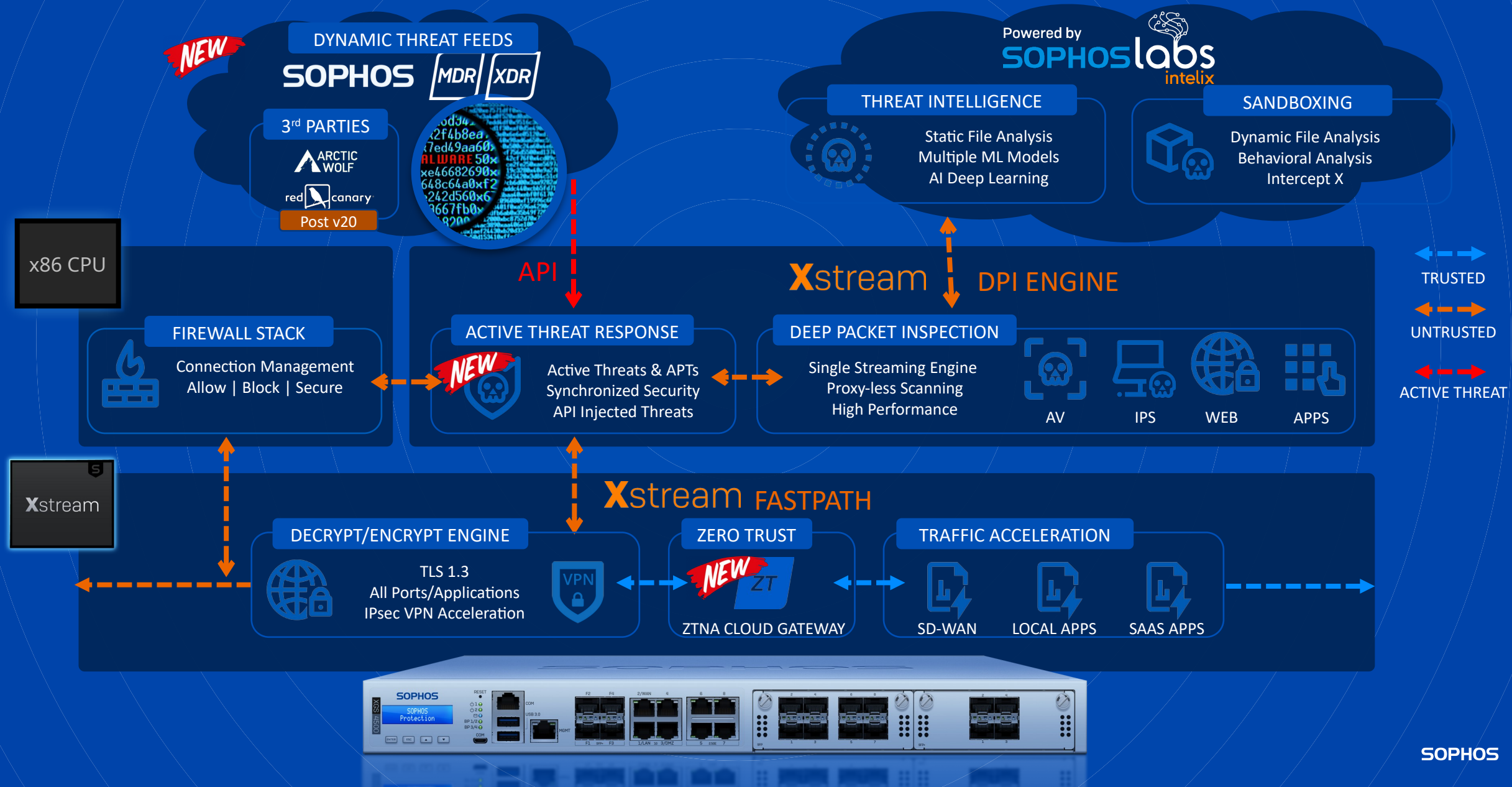
MDR

IR

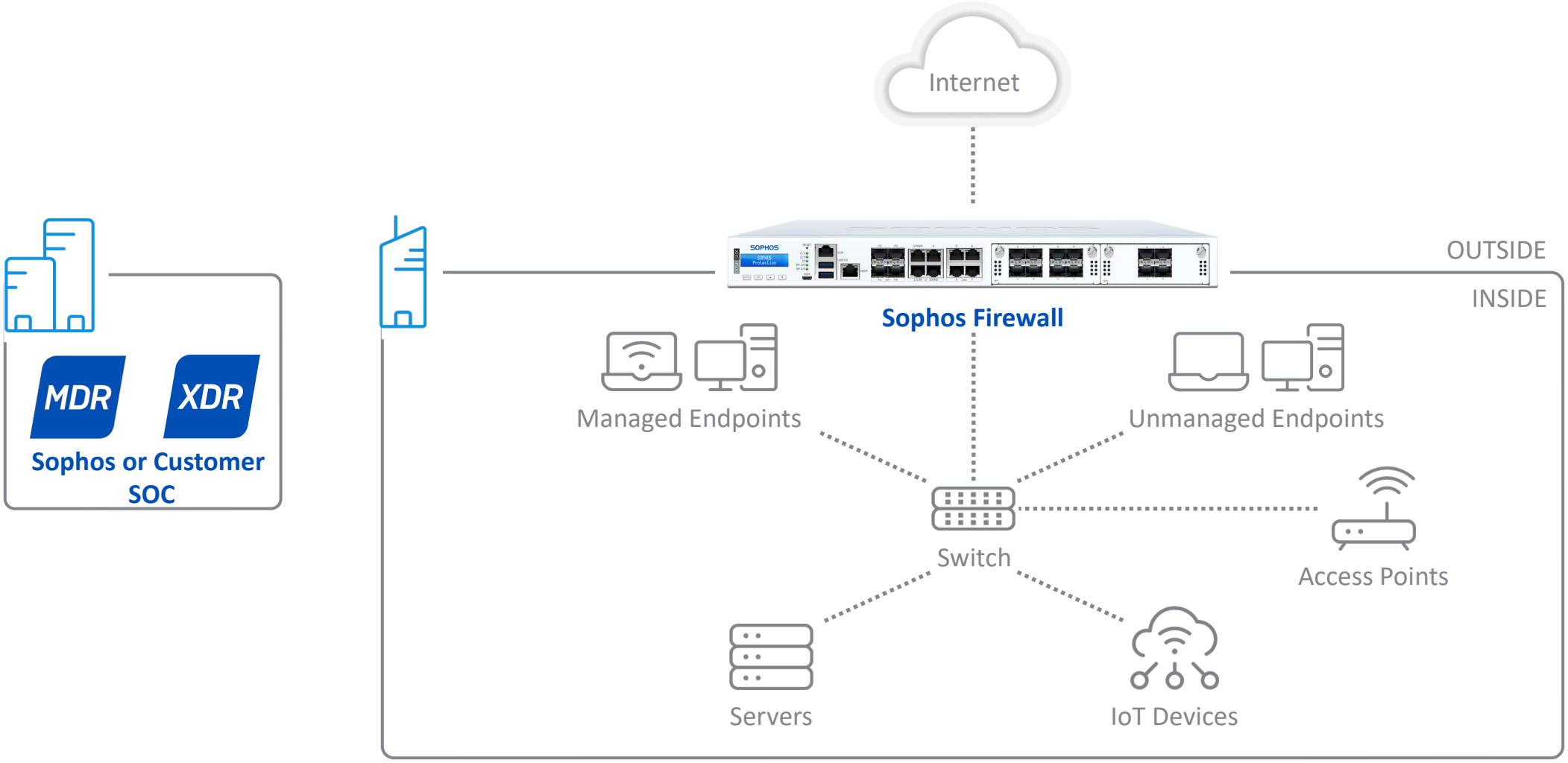
XDR

SOPHOS

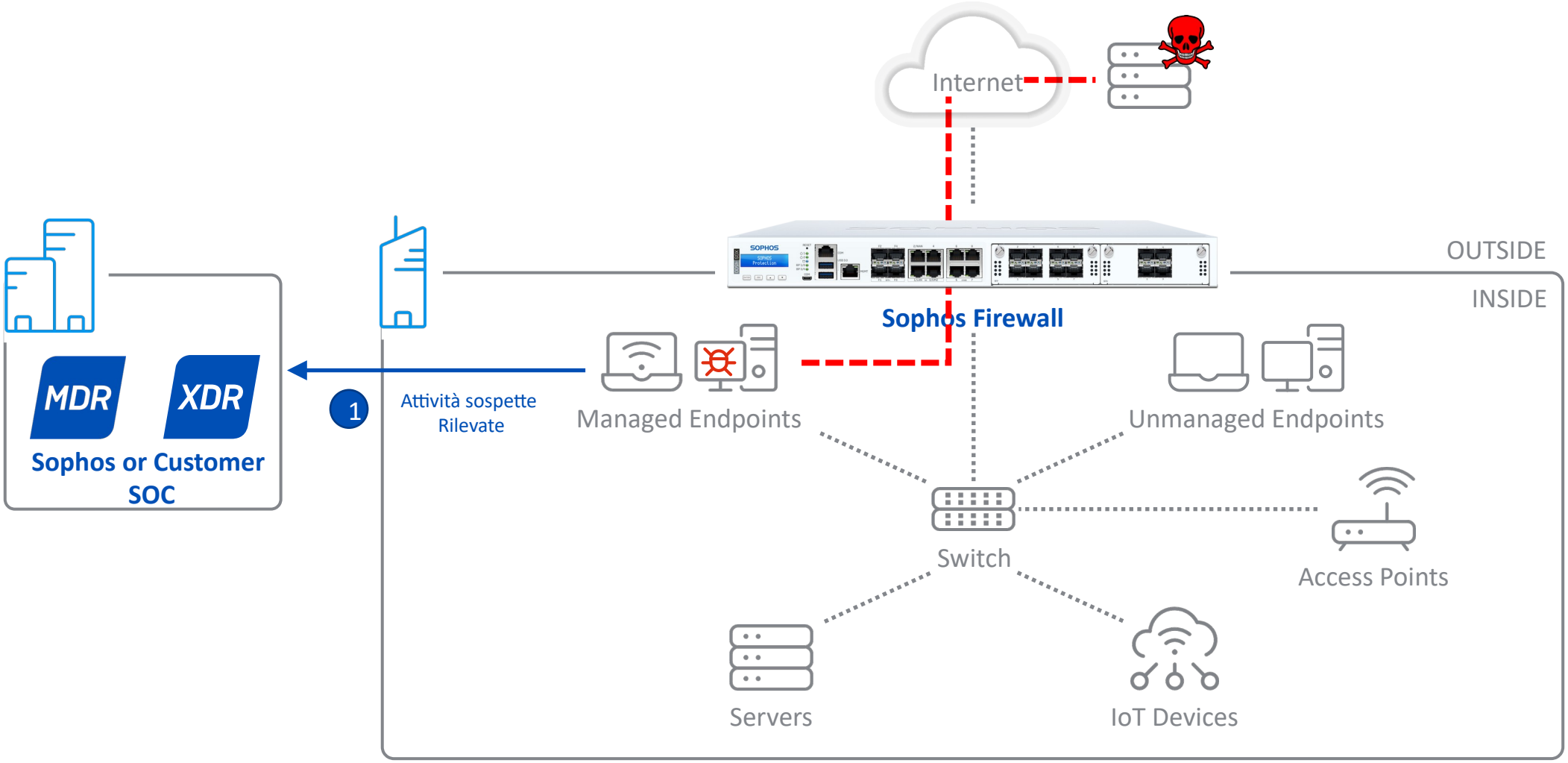
Architettura SFOS 20



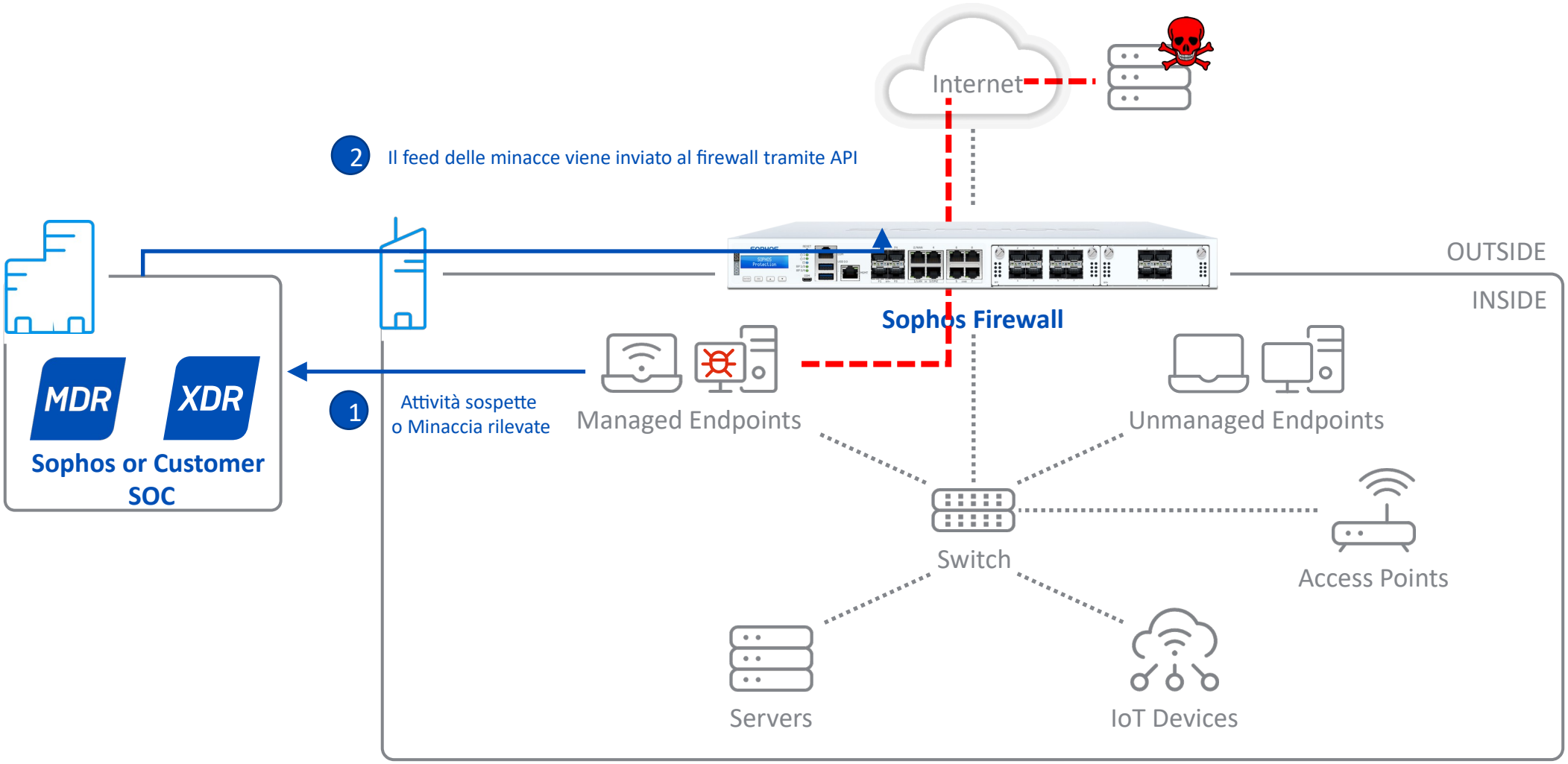
Active Threat Response in Azione (SFOS V20 release)



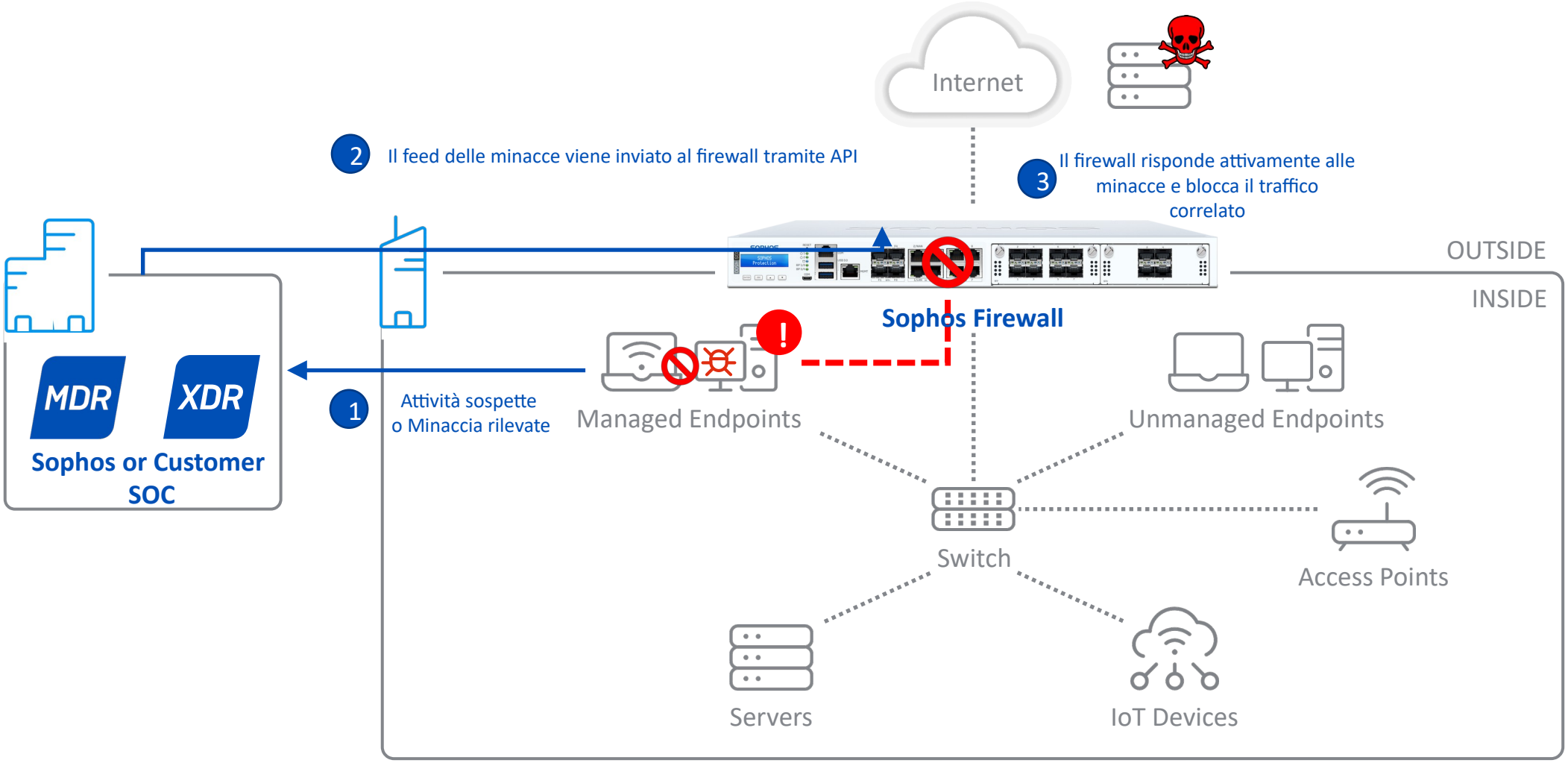
Active Threat Response in Azione



Active Threat Response in Azione



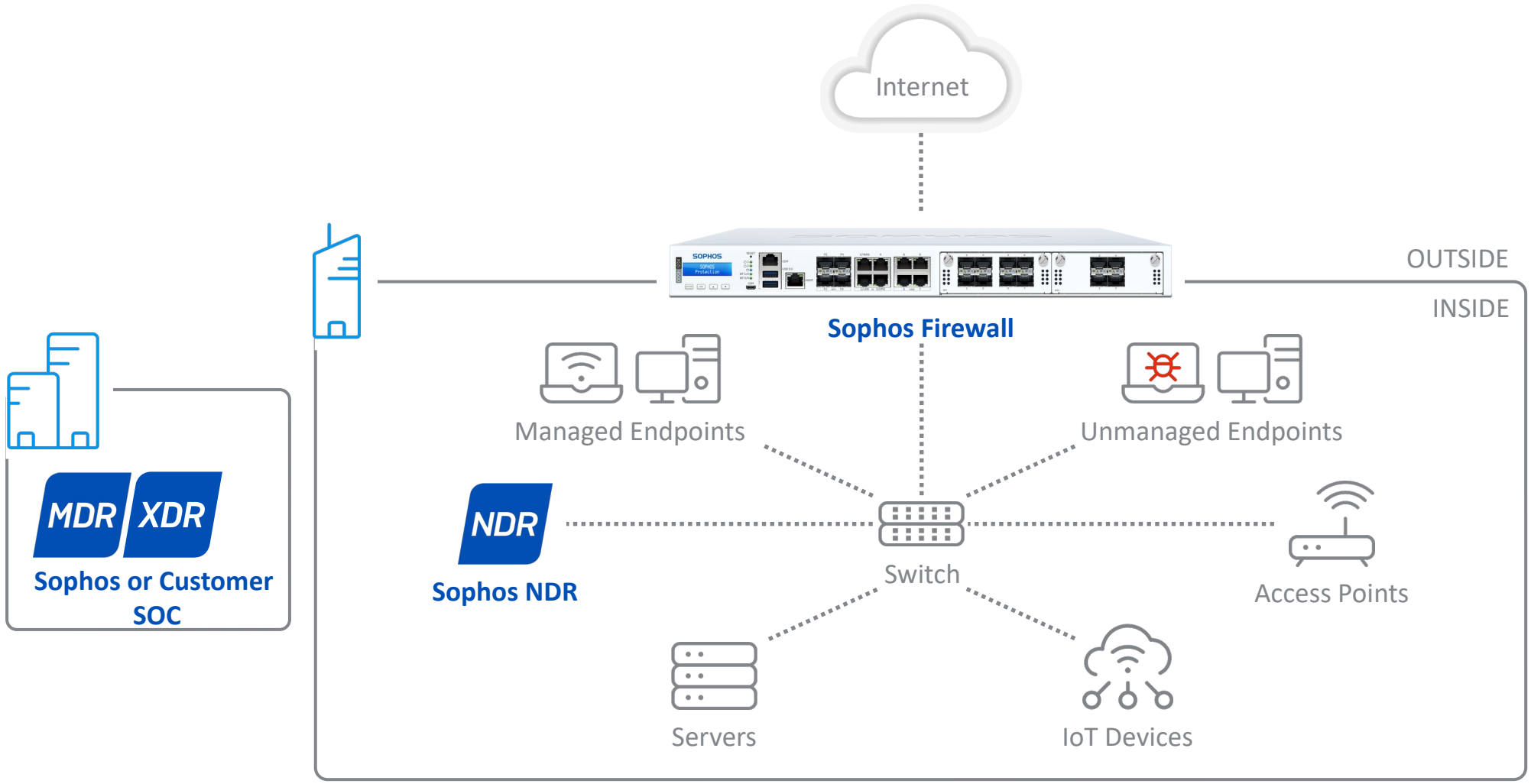
Active Threat Response in Azione



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

SOPHOS

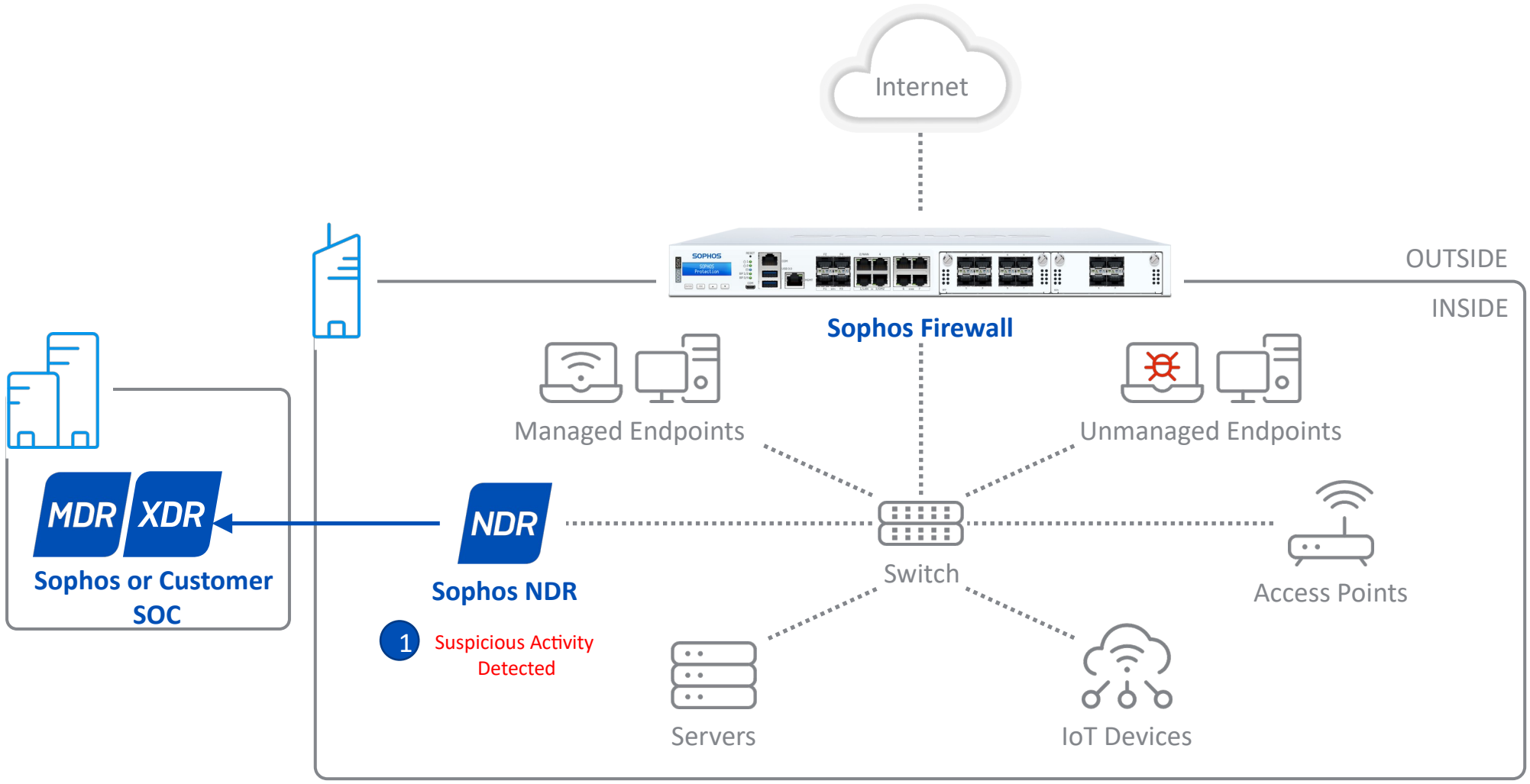
Active Threat Response con rilevamento avanzato NDR



La combinazione definitiva per il rilevamento e la risposta

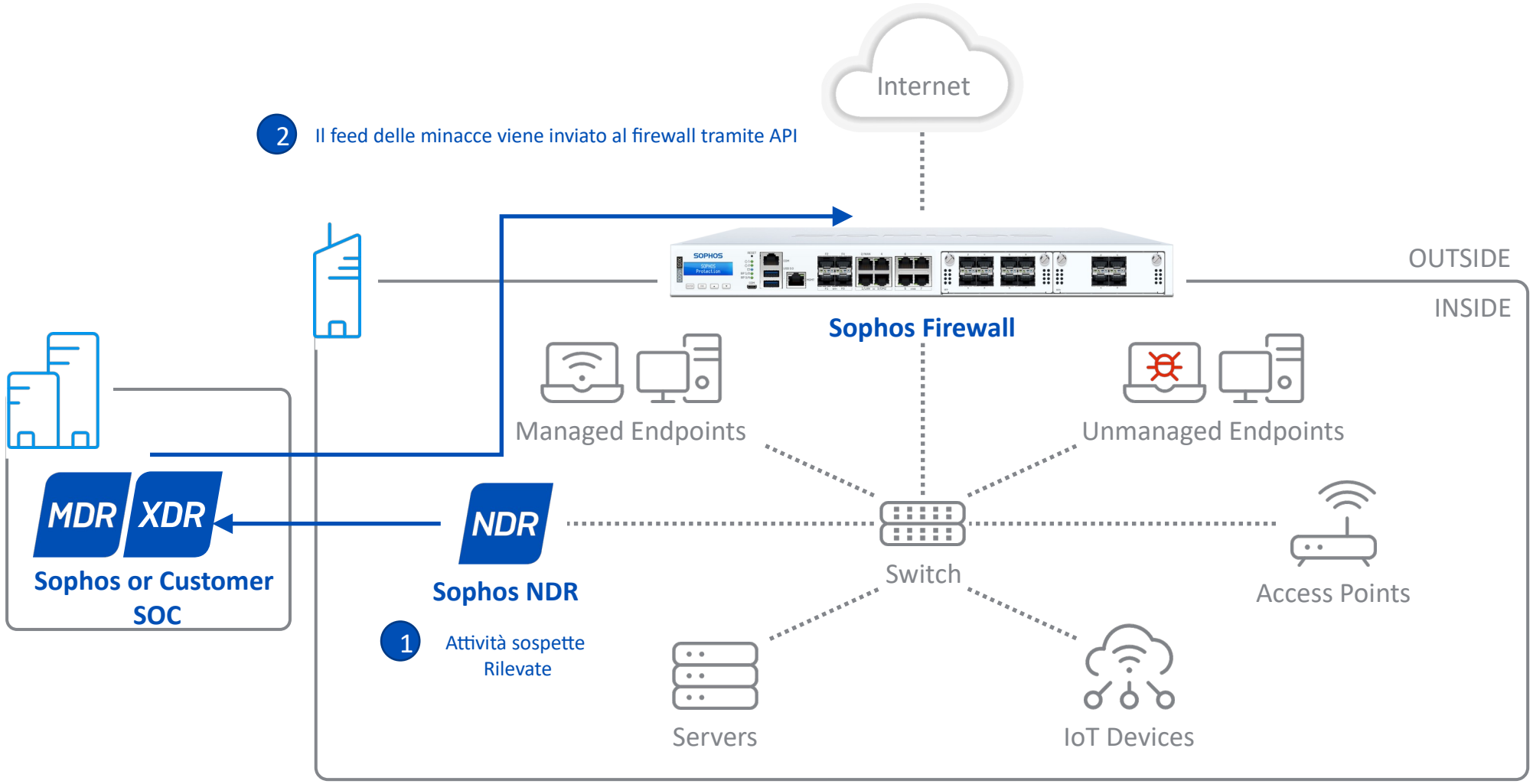
SOPHOS

Active Threat Response with NDR Enhanced Detection



The Ultimate Combination for Detection AND Response

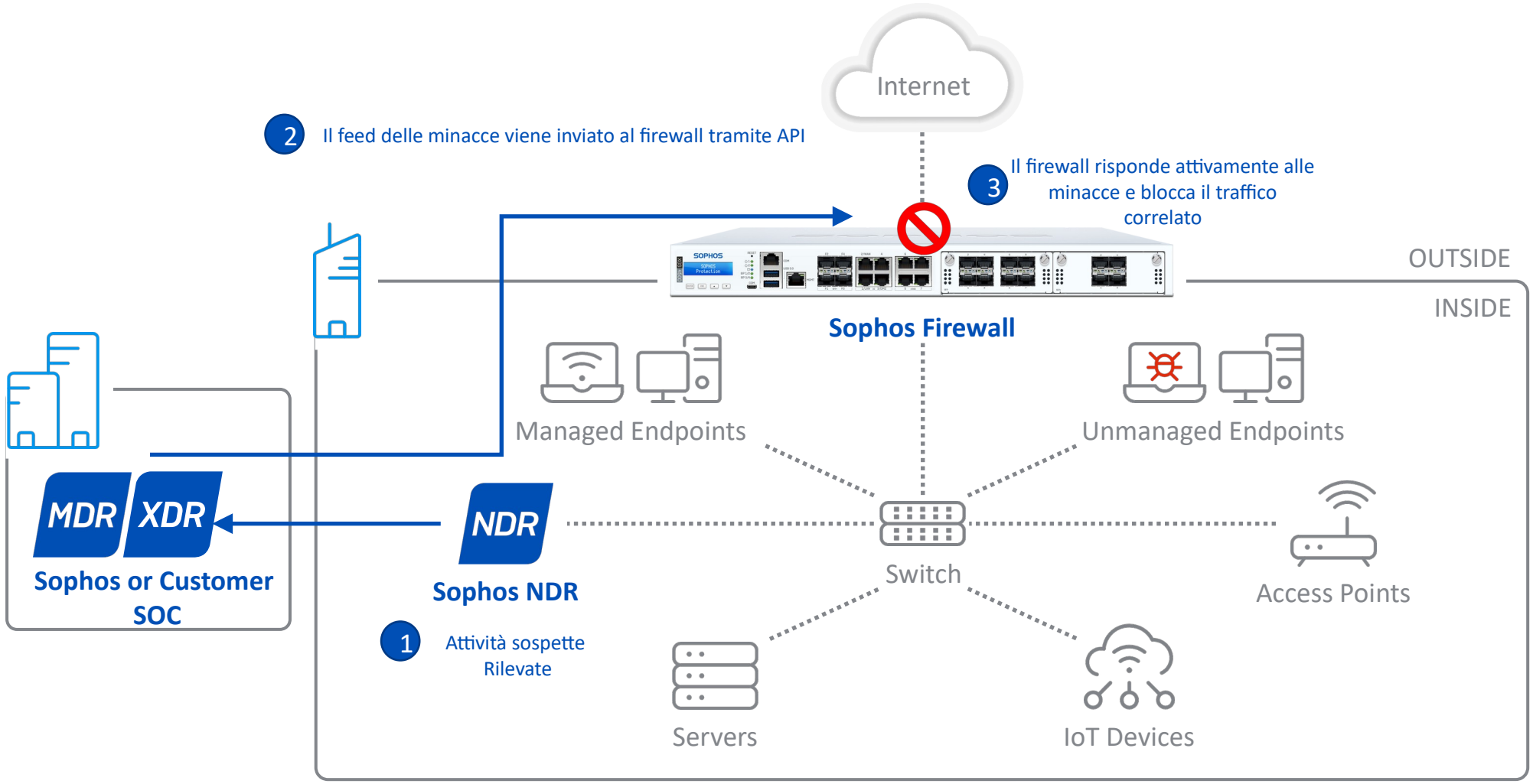
Active Threat Response con rilevamento avanzato NDR



The Ultimate Combination for Detection AND Response

SOPHOS

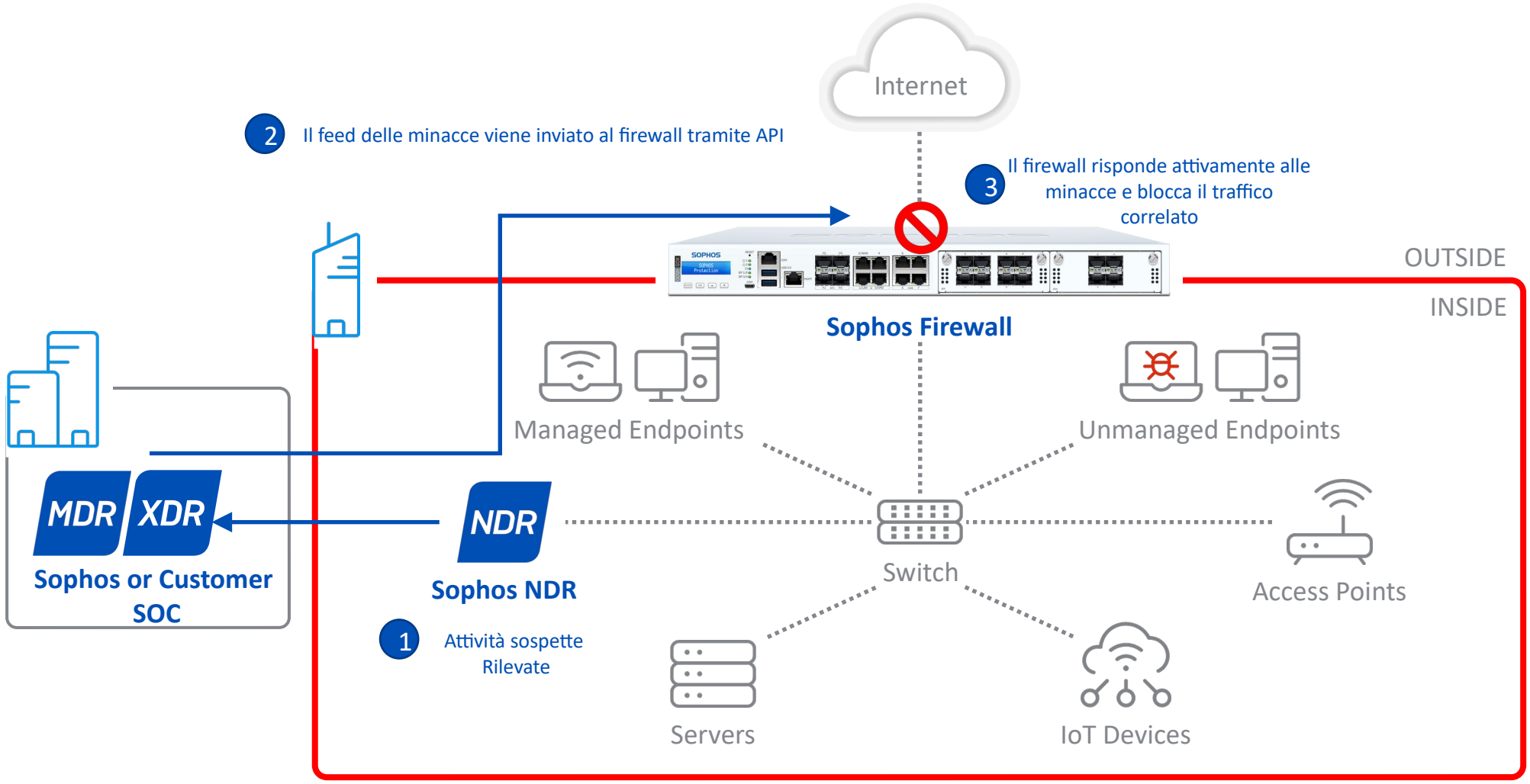
Active Threat Response con rilevamento avanzato NDR



The Ultimate Combination for Detection AND Response

SOPHOS

Active Threat Response con rilevamento avanzato NDR



The Ultimate Combination for Detection AND Response

SOPHOS

Connetti i tuoi dati di sicurezza per rilevare le minacce più rapidamente e bloccare più rapidamente gli avversari attivi

XDR

Sophos XDR semplifica la raccolta, l'arricchimento e la combinazione dei dati di sicurezza tra endpoint, firewall, cloud, identità, rete e prodotti e-mail. Filtra gli avvisi rumorosi e ridondanti, ottieni una visibilità completa da un'unica console e riduci il carico di lavoro con azioni di risposta automatizzate.

Blocca automaticamente l'accesso di avversari attivi alla tua rete

Fw

Sophos Firewall ora include Active Threat Response per bloccare automaticamente gli avversari attivi senza dover aggiungere regole del firewall. Utilizzando la threat intelligence e i dati di sicurezza in tempo reale provenienti da centinaia di migliaia di organizzazioni in tutto il mondo, Sophos Firewall blocca attacchi nuovi e inediti.

Rileva gli avversari attivi che tentano di spostarsi attraverso la tua rete

NDR

Sophos Network Detection and Response (NDR) rileva i modelli anomali di traffico di rete e i comportamenti associati a un avversario attivo. Sophos NDR monitora continuamente tutto il traffico di rete per rilevare nuove minacce, minacce interne e persino attacchi ai dispositivi IoT e OT.

SOPHOS

Cybersecurity as a Service