bechtle × SOPHOS

Le SOC 24x7 Next Gen compatible *avec vos solutions de cyber-sécurité existantes.*

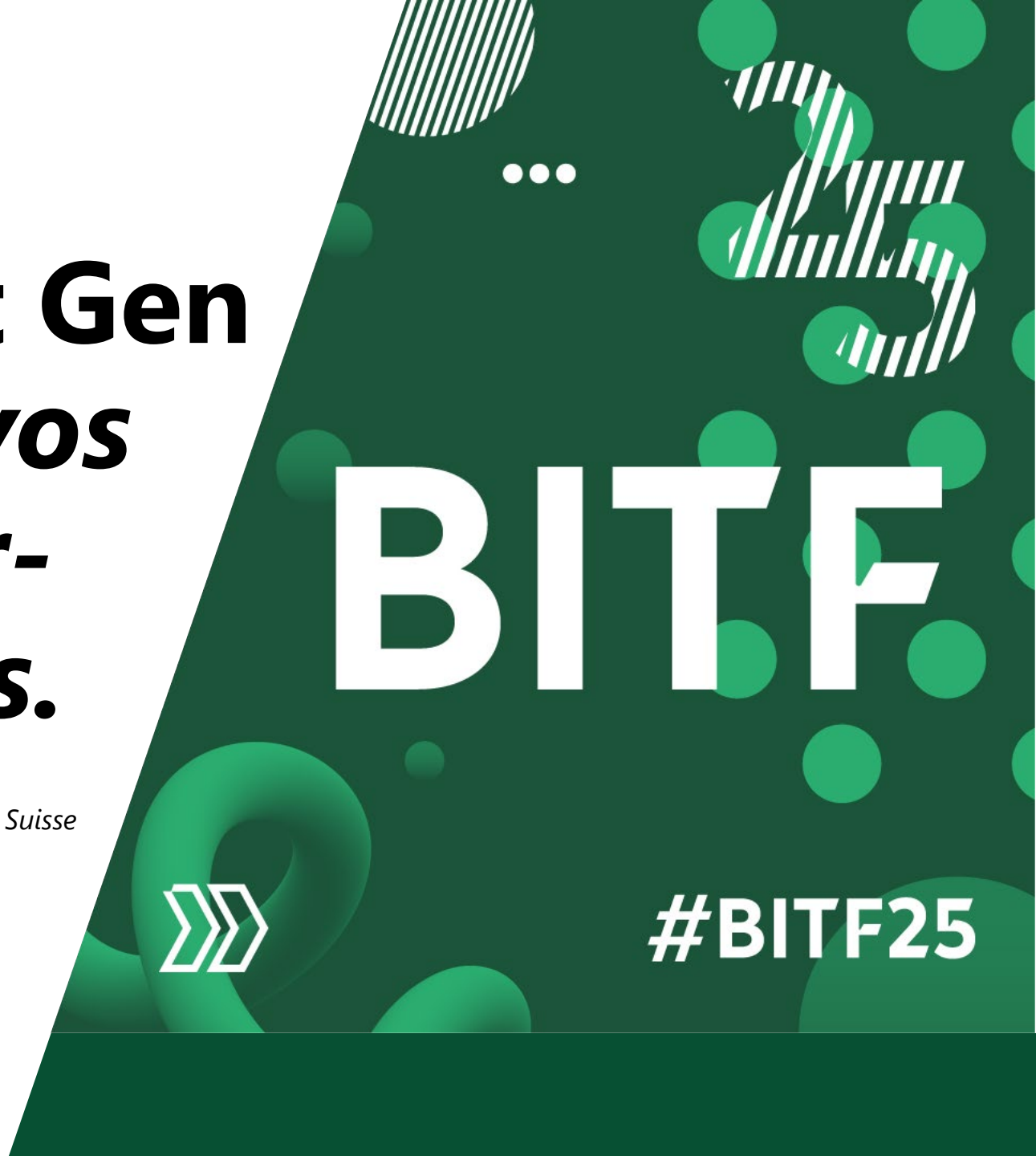
Claudio Guerrieri – *Business Development Manager Network & Security, Bechtle Suisse*

Michel Rueger – *Senior Sales Engineer, Sophos*

Renaud Schweingruber – *Senior Enterprise Account Executive, Sophos*

Bechtle IT Forum, Lausanne.

24.06.2025

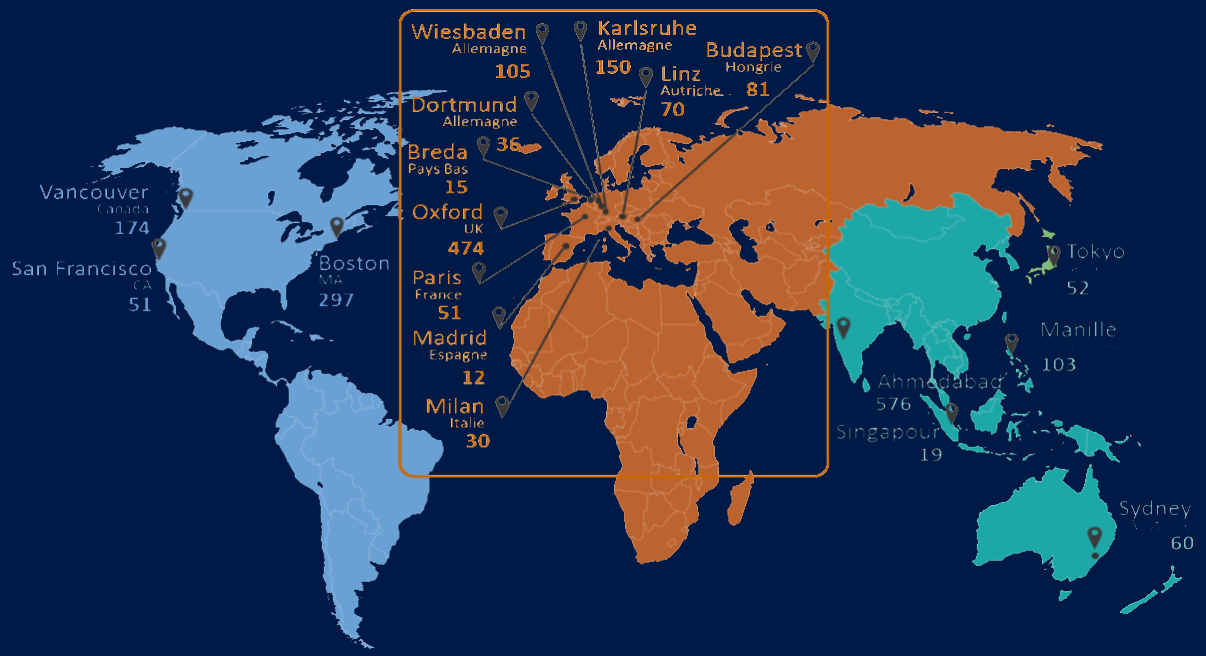


Sophos en un coup d'œil

1985
FONDÉ A
OXFORD, Royaume-Uni

Siège
OXFORD, Royaume-Uni

5'000+
EMPLOYÉS
(APPROX.)



600,000+
Clients

25,000+
Partenaires actifs

100+
Partenaires stratégiques
(Technologie, services, etc.)

350+
Intégrations tierces

30,000+
Clients Sophos MDR

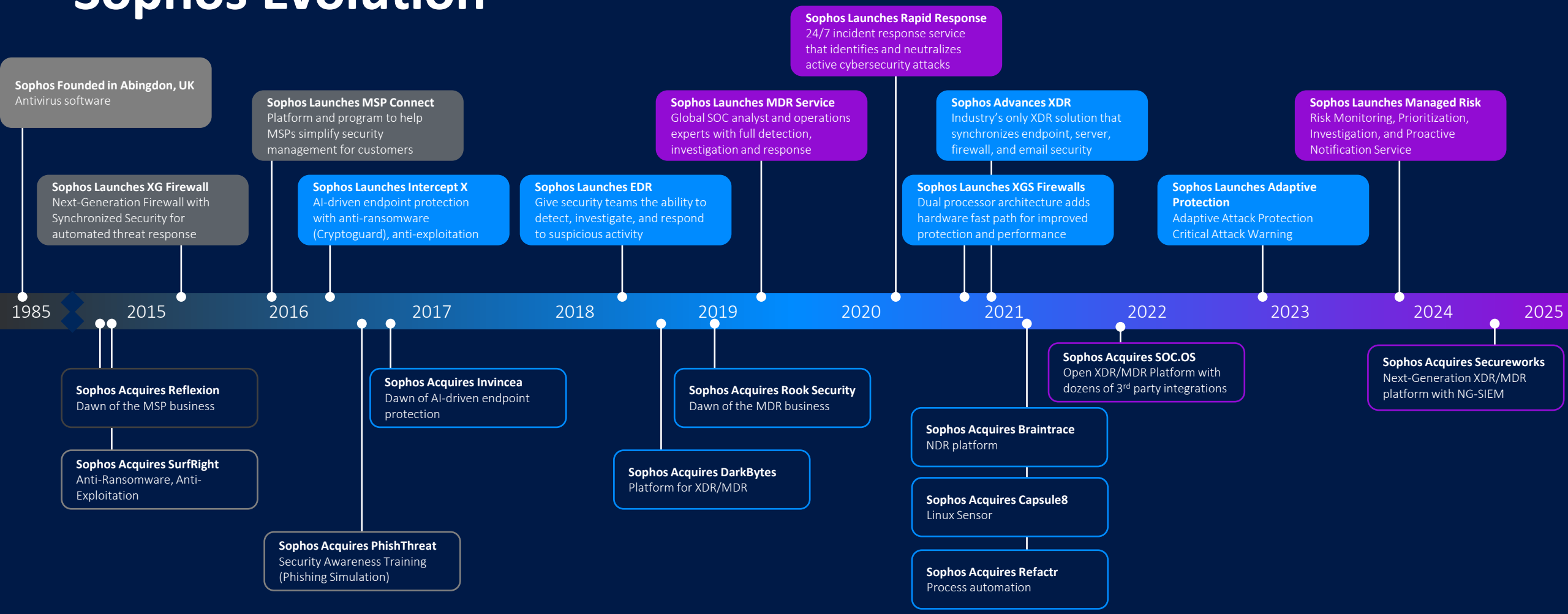
300,000+
Clients Sophos Endpoint

45,000+
Clients Sophos XDR

300,000+
Clients Sophos Firewall

SOPHOS / Secureworks

Sophos Evolution



2015 – Present: Crypto fuels a ransomware explosion

2017 – Present: Detection and Response and AI Revolution

2019 – Present: Cybersecurity Divide drives the shift to Services

SOPHOS

Cybermenaces en Suisse romande

SOPHOS

Les adversaires ne s'introduisent pas. Ils se connectent.

La valeur des données en tant que « monnaie » ne cesse de croître

Les pirates utilisent les données et identifiants volés **via divers canaux**

Les attaquants privilégient comme cible les PME disposant de **peu de ressources de sécurité**

Les PME ont tendance à **peu segmenter les accès aux données, applications et ressources**

Identifiants volés en vente sur le Dark Web

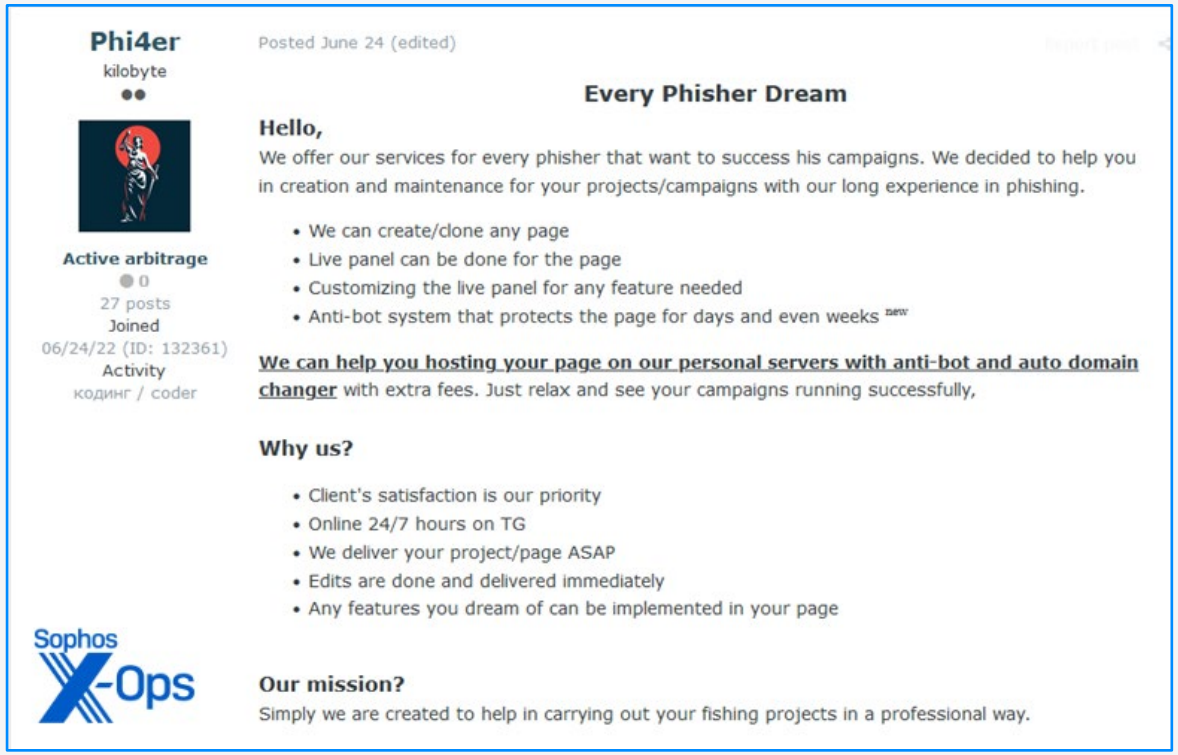
Stolen Access Data For Sale

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	2,000	No
6	14-Jul-22	****	Turkey	Government	Access to gov account/email of Director of **** Department	Not known	No
7	7-Jul-22	Not named	Asia	Not known	Outlook accounts	8,500	No
8	8-Jun-22	Not named	UK	Construction	RDP/VPN access	500	No
9	22-Jun-22	****	Not known	Not known	50 Confluence accesses (CVE-2022-26134)	2,000	Yes
10	23-Jun-22	Not named	Middle East	Pharmaceutical	Credentials to access Citrix Gateway and sites; domain creds; BloodHound files; backup creds; DA creds on request ($5000 USD extra)	5,000	No
11	15-Aug-21	Not named	Singapore	Transport/logistics	Access	Not known	No
12	14-May-22	Not named	Canada	Education	VPN access	500	No
13	19-Mar-22	****	Bangladesh	Military	Access to 3000 hosts, domain controller, database, web portals, emails	20,000	No
14	18-Jul-22	Not named	Europe	Construction	Remote command-line access	2,700	No
15	10-Jul-22	Not named	Brazil	IT/Telecoms/Security	RDP access	1,500	No

Source: Sophos X-Ops

Cybercrime as a Service: un marché bien organisé



Phi4er
kilobyte
●●

Active arbitrage
0
27 posts
Joined
06/24/22 (ID: 132361)
Activity
кодинг / coder

Posted June 24 (edited)

Every Phisher Dream

Hello,

We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks new

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

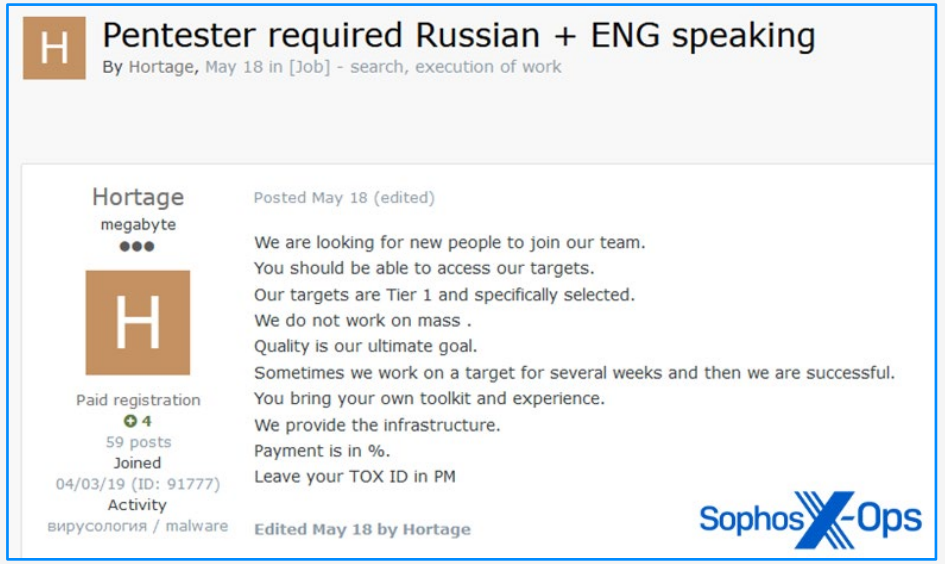
Why us?

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Our mission?

Simply we are created to help in carrying out your fishing projects in a professional way.

Sophos X-Ops



H

Pentester required Russian + ENG speaking

By Hortage, May 18 in [Job] - search, execution of work

Hortage
megabyte
●●●

H

Paid registration
4
59 posts
Joined
04/03/19 (ID: 91777)
Activity
вирусология / malware

Posted May 18 (edited)

We are looking for new people to join our team.
You should be able to access our targets.
Our targets are Tier 1 and specifically selected.
We do not work on mass .
Quality is our ultimate goal.
Sometimes we work on a target for several weeks and then we are successful.
You bring your own toolkit and experience.
We provide the infrastructure.
Payment is in %.
Leave your TOX ID in PM

Edited May 18 by Hortage

Sophos X-Ops

dripper
HDD-drive
Пользователь

Joined: May 19, 2022
Messages: 44
Reaction score: 6

Jun 23, 2022

Sophos X-Ops

I am looking for pentesting job.

I have experience in AV Bypass on your docx/xlsx and bins
I can do lateral movement for you
I can code for you in C/Cpp python NIM
I have experience make crypts and loaders

More details in PM.

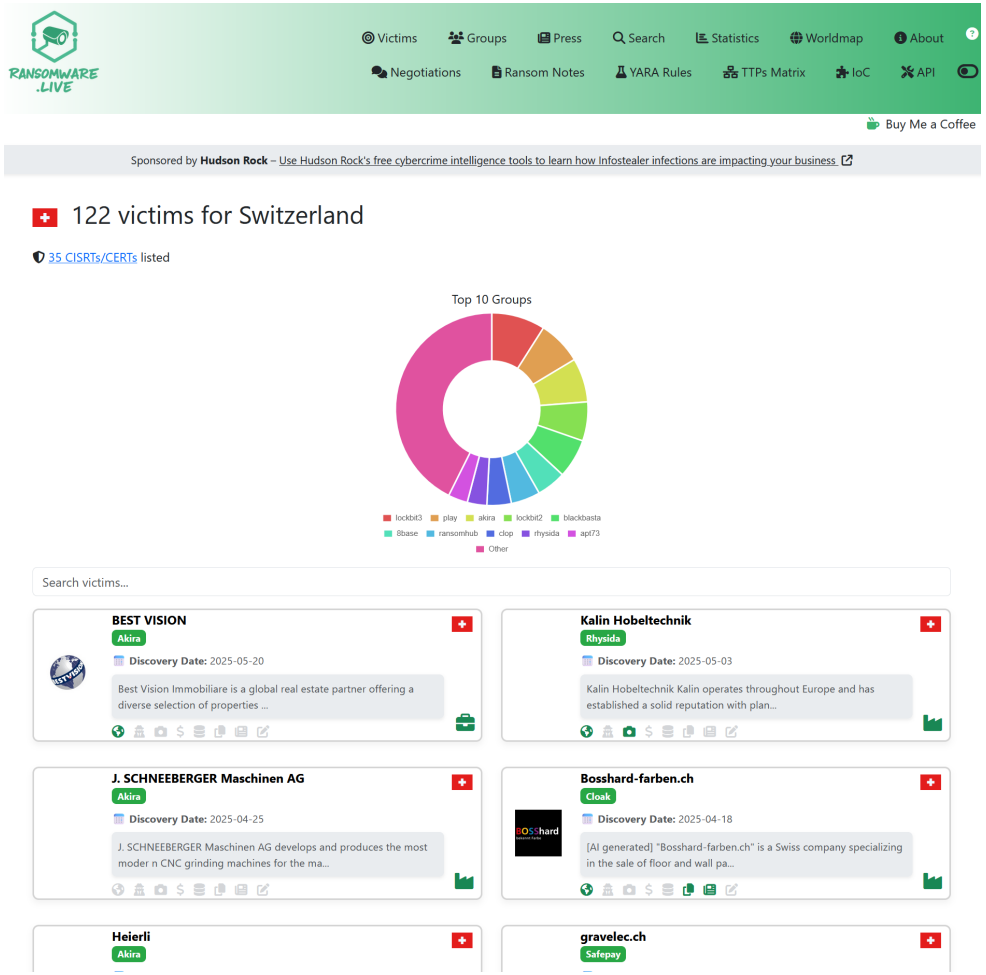
Make damage memorable.

Source: Sophos X-Ops

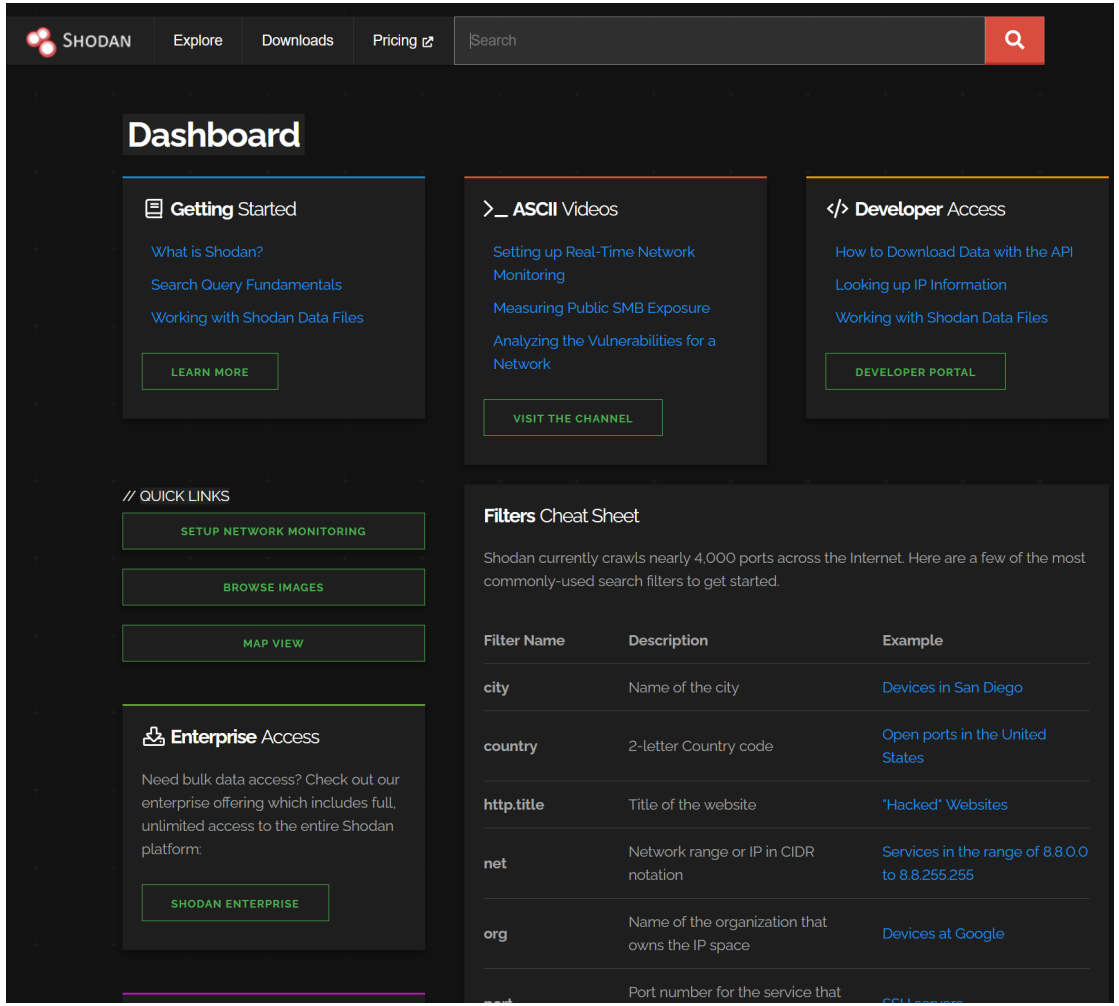
Ne nous croyez pas sur parole !

SOPHOS

Exemples récents



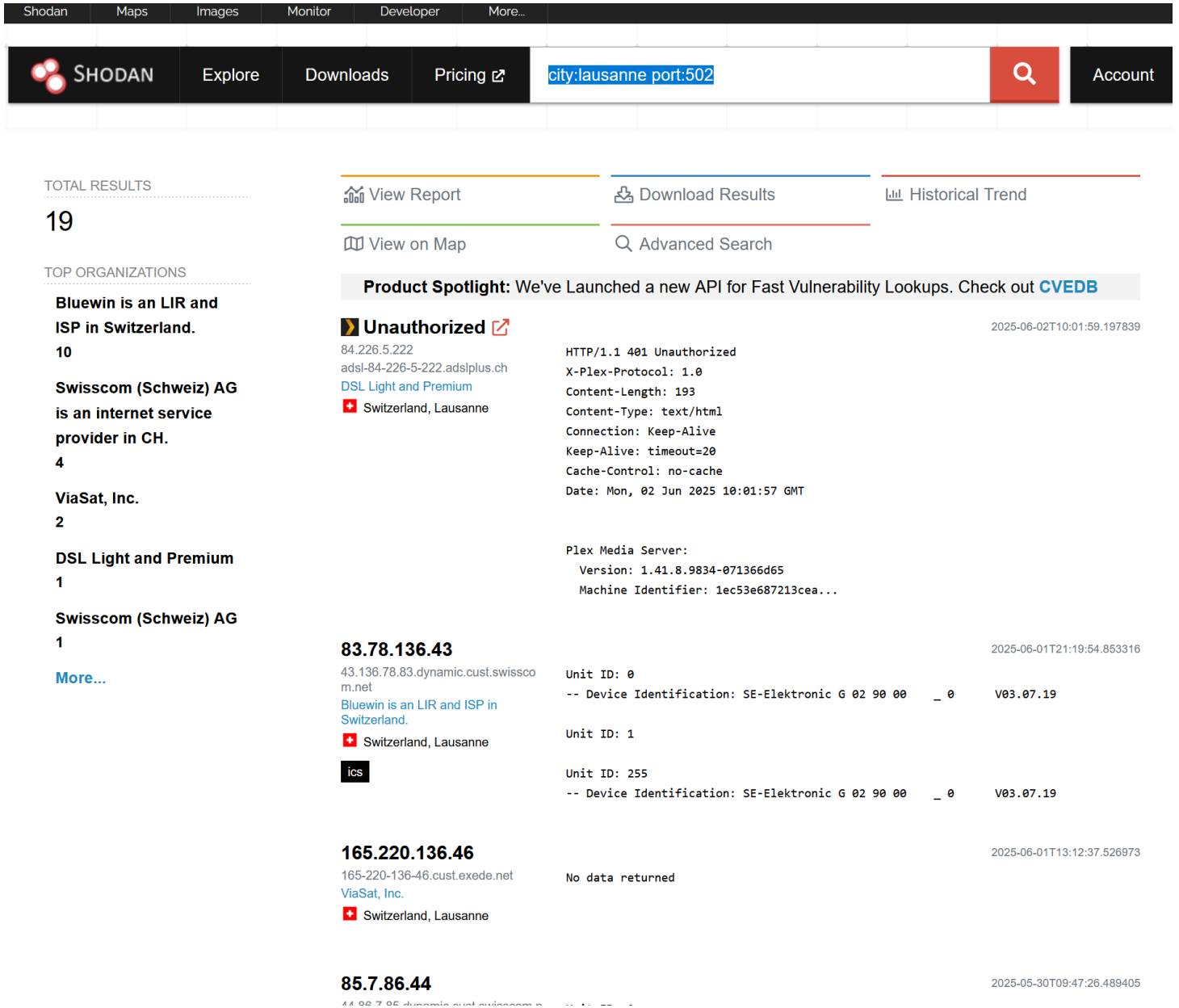
https://www.ransomware.live/country/CHE



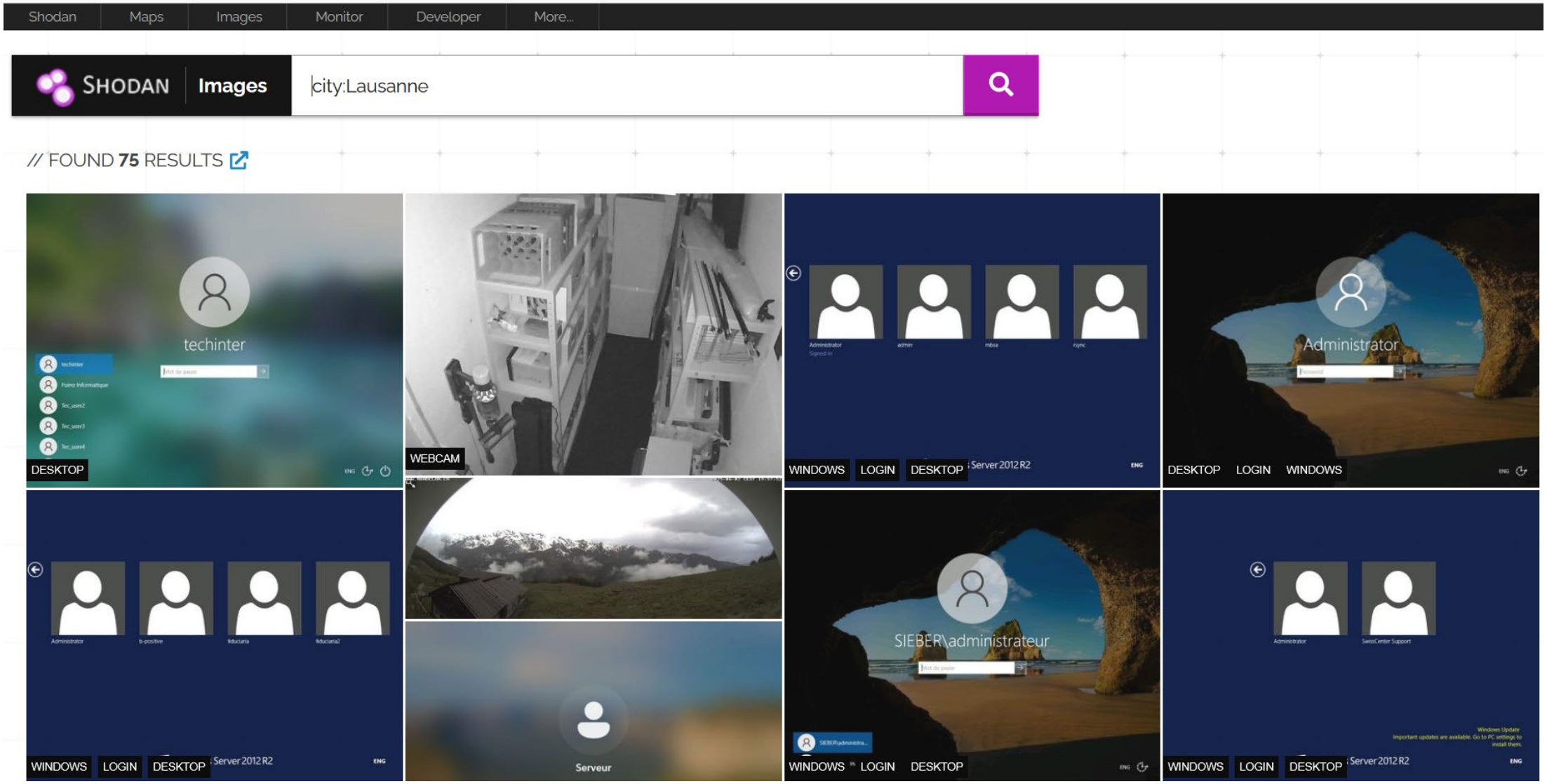
https://www.shodan.io

SOPHOS

Exemples récents

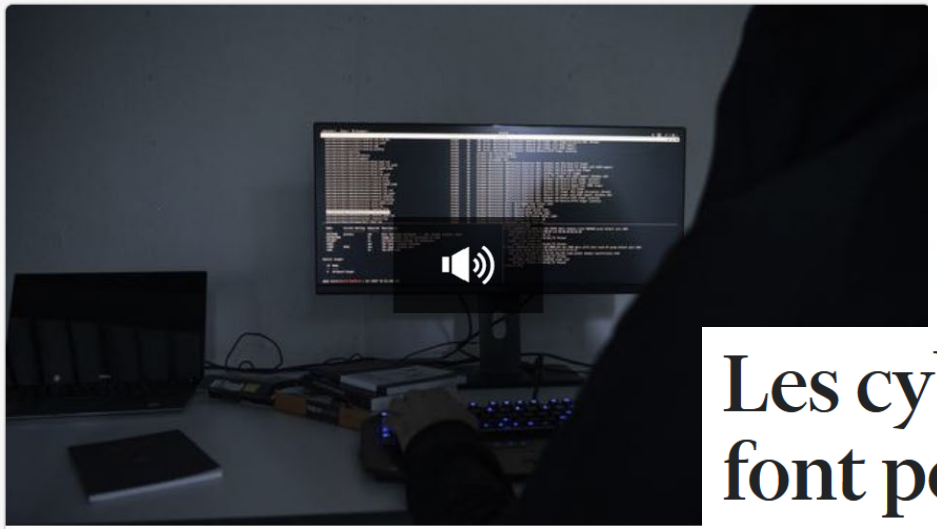


Exemples récents



SOPHOS

Revue de presse



Les PME suisses et les parti ont un faux sentiment de sé face aux cyberattaques

Suisse
Aujourd'hui à 14:42

Toutes les huit minutes, l'Office fédéral de la cybersécurité reçoit une annonce de menace

à 18:14

Les cyberarnaques financières font perdre des millions aux entreprises romandes. Pourquoi font-elles encore de tels dégâts?

Dans les cantons de Vaud et Neuchâtel, 66 sociétés viennent d'être touchées, avec des pertes cumulées de 12,5 millions d'euros. Une petite partie de l'argent volé a pu être récupérée et des interpellations ont eu lieu en Israël. Le fléau est massif

SOPHOS

Problématique majeure des équipes IT et de sécurité

Manque de visibilité

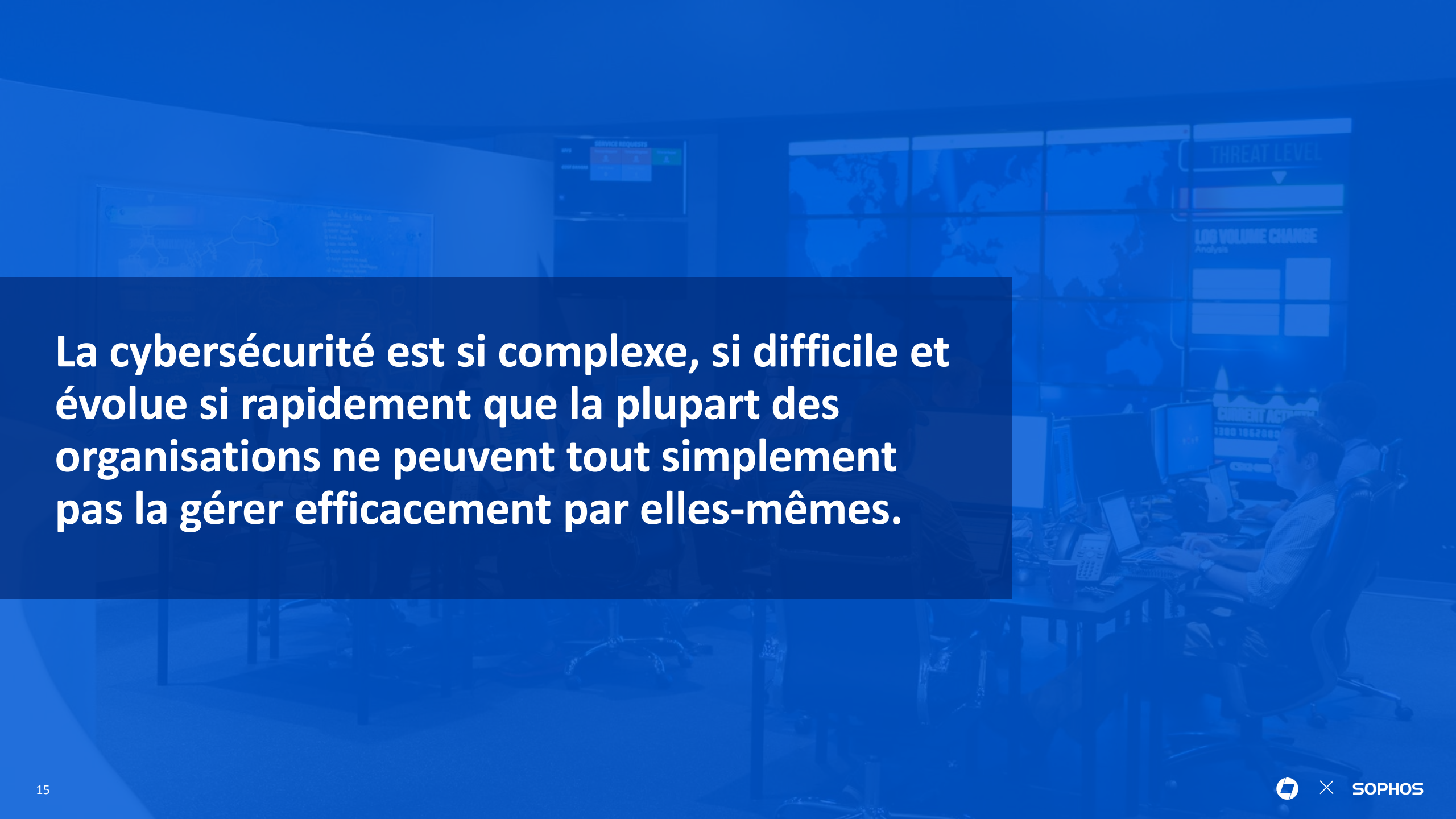
68% *des violations de sécurité sont détectées 30 jours après*

Manque de temps

26% *du temps du team IT pour gérer des problèmes liés à la sécurité*

Manque de resources

2/3 *mentionnent un budget de sécurité insuffisant*



La cybersécurité est si complexe, si difficile et évolue si rapidement que la plupart des organisations ne peuvent tout simplement pas la gérer efficacement par elles-mêmes.


SOPHOS

Un Security Operation Center (SOC) 24h/24, 7j/7 pour investiguer et neutraliser les menaces

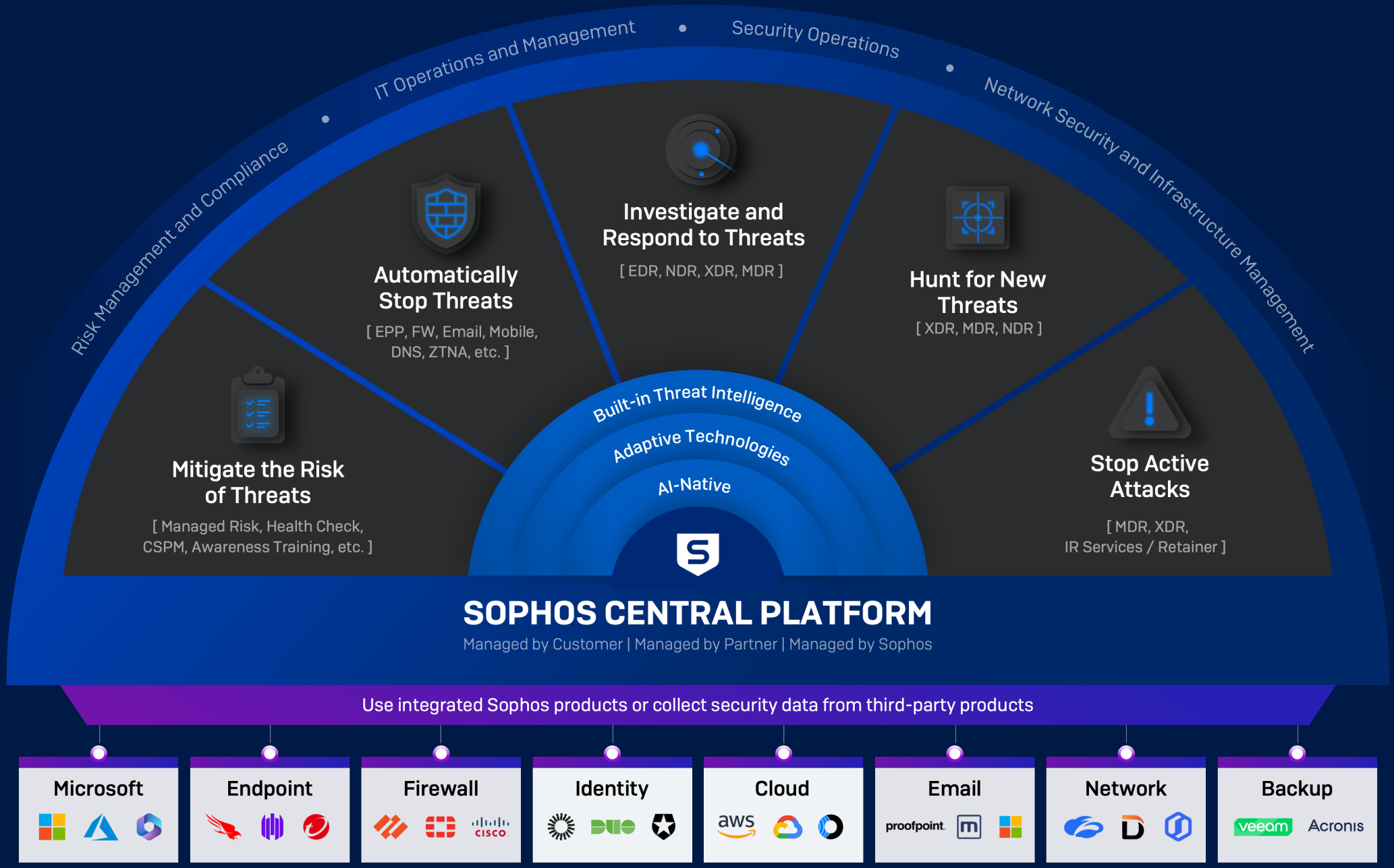
Michel Rueger
Snr. Sales Engineer, Sophos

15.05.2025

SOPHOS

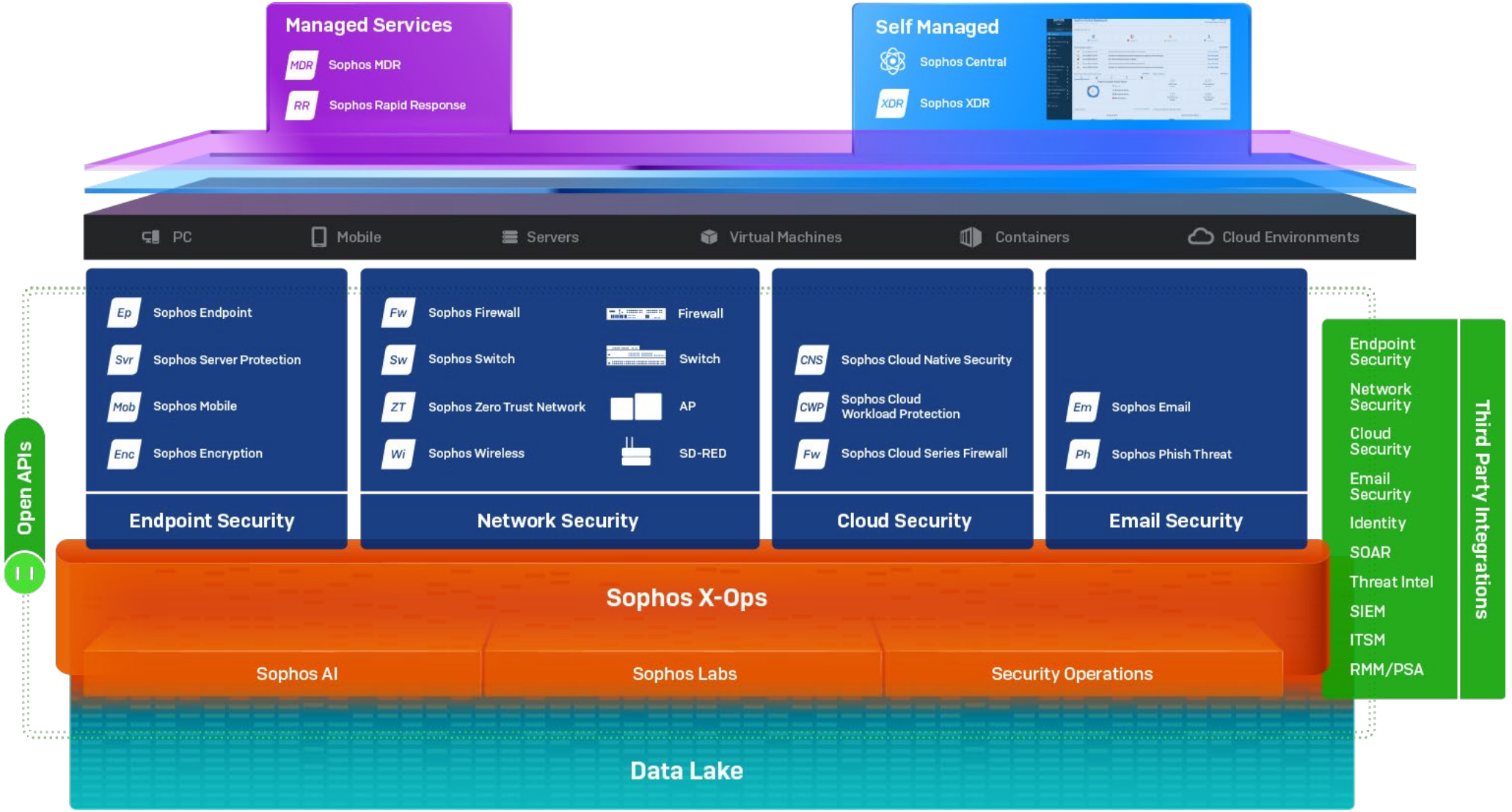
La Sécurité comme un Eco-système

SOPHOS


Risk Management and Compliance
IT Operations and Management
Security Operations
Network Security and Infrastructure Management
Mitigate the Risk of Threats
[Managed Risk, Health Check, CSPM, Awareness Training, etc.]
Automatically Stop Threats
[EPP, FW, Email, Mobile, DNS, ZTNA, etc.]
Investigate and Respond to Threats
[EDR, NDR, XDR, MDR]
Hunt for New Threats
[XDR, MDR, NDR]
Stop Active Attacks
[MDR, XDR, IR Services / Retainer]
Built-in Threat Intelligence
Adaptive Technologies
AI-Native
SOPHOS CENTRAL PLATFORM
Managed by Customer | Managed by Partner | Managed by Sophos
Use integrated Sophos products or collect security data from third-party products
Microsoft
Endpoint
Firewall
Identity
Cloud
Email
Network
Backup
aws
proofpoint
veeam
Acronis

SOPHOS

Adaptive Cybersecurity Ecosystem



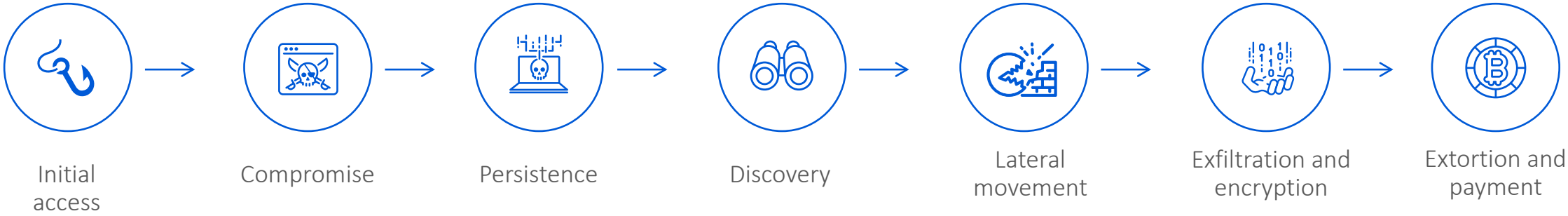
A typical ransomware attack

59% of **organizations hit by ransomware** in the last year

94% of victims said their **backups were targeted**

32% of encrypted data attacks also involved **data theft**

$2.0M Average (median) **ransom paid**



91% of attacks began **outside regular business hours**

57% of compromise attempts **were successful**

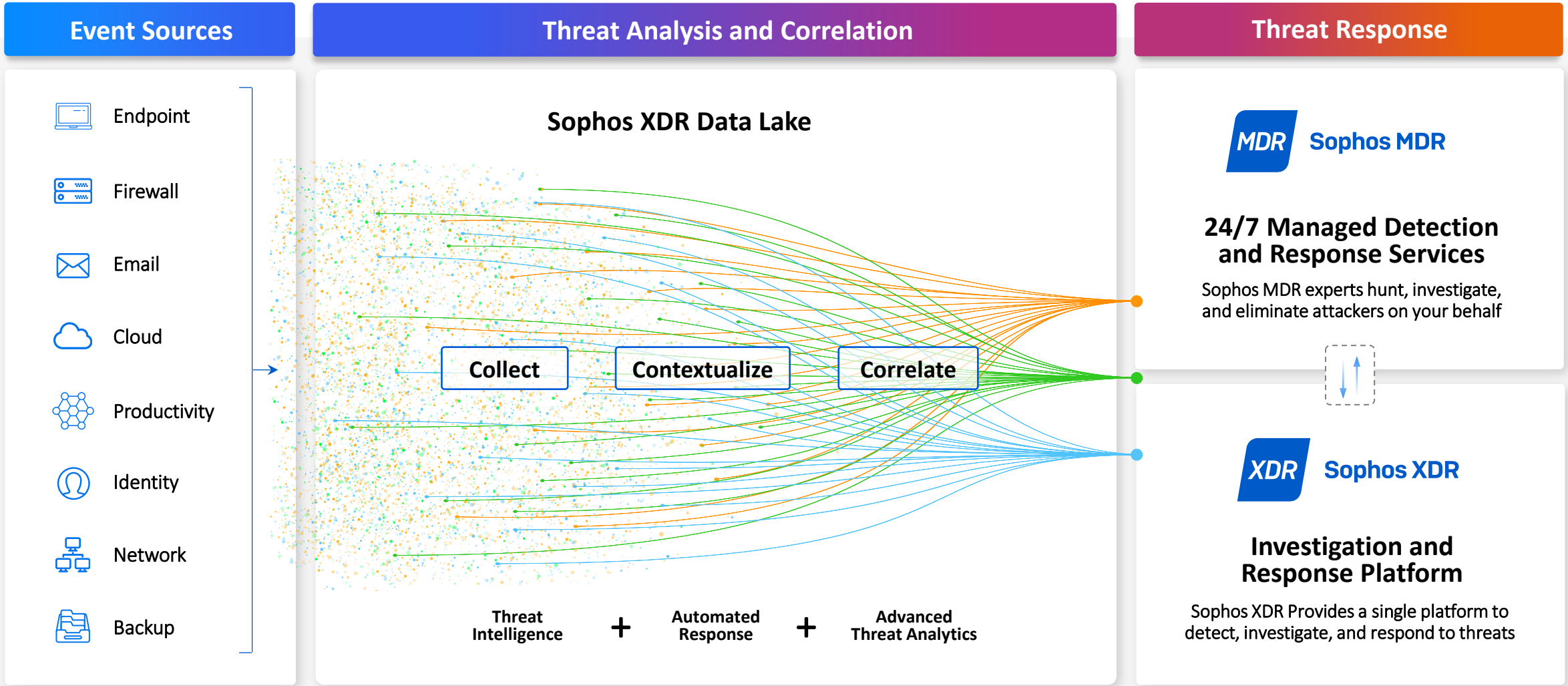
70% of attacks resulted in **data encryption**

56% of victims **paid the ransom**

Sources: The State of Ransomware 2024 – Sophos, Stopping Active Adversaries: Lessons From The Cyber Frontline- Sophos

SOPHOS

Sophos Threat Detection and Response Platform



Sophos Endpoint

Que fait Sophos Endpoint pour vous ?

Protection contre les menaces connues et inconnues grâce à des technologies sophistiquées

SOPHOS

D
do-not-reply@central.sophos.com
September 13, 2024 at 13:53

[HIGH] Alert for Sophos Central [Primary SE Demo Account]: We detected ransomware

To:

Reply-To: do-not-reply@central.sophos.com

This email alert was generated by Sophos Central. Do not reply to this email.

SOPHOS CENTRAL

Sophos Central Event Details for Primary SE Demo Account

What happened: We detected ransomware trying to encrypt files.

Where it happened: Win11-1

Path: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

What was detected: CryptoGuard

User associated with device: WIN11-1\Sophos

How severe it is: High

What Sophos has done so far: We have blocked the ransomware's file-system access. If the computer is a Windows workstation or server, we clean up the ransomware automatically. If it's a Mac, you need to clean up manually.

What you need to do:

- For Windows computers:
  1. If automatic sample submission isn't enabled, send us a sample of the ransomware. We'll classify it and update our rules: if it's malicious, Sophos Central will block it in future.
  2. Go to Sophos Central, go to **Alerts**, and mark the alert as resolved.

- For Macs:
  1. Move the computer temporarily to a network where it is not a risk to other computers. Go to the computer. On the Endpoint UI, select the Events tab and expand the event entry to show the path of the ransomware. If its confirmed to be malicious, remove it manually.
  2. Go to Sophos Central and select the device's Status tab. In the Alerts section, mark the alert as resolved.

Sophos Central Dashboard

See a snapshot of your security protection

1119	945	166	8
Total Alerts	High Alerts	Medium Alerts	Low Alerts

Most Recent Alerts

View all Alerts

⚠	Mar 19, 2025 12:01 AM	Policy non-compliance: Malware Protection	IntelMacMini\administr...	IntelMacMini	Show full details
●	Mar 18, 2025 5:24 PM	Manual malware cleanup required: 'Troj/PSDL-B' at 'C:\Users\Sophos\App...	WIN11-3-LR\Sophos	Win11-3-LR	Show full details
●	Mar 18, 2025 5:09 PM	Manual malware cleanup required: 'ATK/AtomicRed-A' at 'C:\Users\Sopho...	WIN11-4\Sophos	Win11-4	Show full details
●	Mar 18, 2025 4:31 PM	Manual malware cleanup required: 'Mal/T1010-A' at 'C:\Users\Sophos\Ap...	WIN11-4\Sophos	Win11-4	Show full details
●	Mar 18, 2025 4:30 PM	Manual malware cleanup required: 'ML/PE-A' at 'C:\threat\seed\Highscor...	WIN11-2\Sophos	Win11-2	Show full details

Go to Account Health Check

Health summary

Show scores for organizations with a similar number of devices 1-49

Your overall health score

Health check scores

Protection installed 100

Tamper protection 88

Threat Analysis Center

DETECT
Dashboard
Cases
Detections
Device Exposure

INVESTIGATE
Search
AI Search
Threat Graphs
Live Discover

SETTINGS
Integrations
Configured
Marketplace
Detection Rules
Preferences

Summary

Detection name: CryptoGuard

Root cause: outlook.exe

Possible data involved: 12 business files

Where: On Win11-1 that belongs to Jim Halpert

When: Detected on Mar 5, 2025 11:32 AM

Suggested next steps

Set a status for the threat graph — Priority: High — Status: New

Isolate this device while you investigate

Scan the device

Run a Live Discover query

Analyze | Graph record

Filters: Processes | Other files | Business files | Network connections | Registry keys — Show full graph

Et ensuite?

Qui d’autre a reçu cet email ?
Qui d’autre a ouvert la pièce jointe ?
Un attaquant est-il toujours connecté à votre réseau ?

Sophos XDR

Que fait Sophos XDR pour vous?

Ep +

XDR

Capacités de détection et de réponse avec télémétrie unifiée à partir de plusieurs technologies de sécurité sur une seule plateforme

SOPHOS

Threat Analysis Center

DETECT
Dashboard
Cases
Detections
Device Exposure

INVESTIGATE
Search
AI Search
Threat Graphs
Live Discover

SETTINGS
Integrations
Configured
Marketplace
Detection Rules
Preferences

Case Details

CryptoGuard investigation

#2-517300 High Investigating

Owner	Created	Assigned	Last updated
Andrew Mundell	Mar 30, 2025, 03:31 PM	Mar 30, 2025, 03:31 PM	Mar 30, 2025, 03:31 PM

Overview | Detections | Notebook | History | Respond | AI Assistant

Information

Case type	Investigation
Origin	
Detection count	23

MITRE Tactic(s)

TA0002	12
TA0004	6
TA0005	13
TA0011	1
TA0040	2

Case Summary

Sophos AI Analysis Insert

The Case Summary analysis provided by Sophos AI Assistant features are generated by a Third-Party Generative Artificial Intelligence tool ("GenAI Tool"). By using these features, you agree that (i) the output is generated by the GenAI Tool with no warranty from Sophos as to its accuracy/reliability/appropriateness, and you are solely responsible for verifying its accuracy, (ii) you will comply with the GenAI Tool Use Policy, (iii) Sophos disclaims all liabilities for your use of or reliance on the output, (iv) the output does not represent Sophos's views; and (v) all personal data are processed in accordance with the Sophos Privacy Notice.

Impacted Entities

Show filters

Type	Name	SophosLabs Intelix

No results found

Threat Analysis Center

DETECT
Dashboard
Cases
Detections
Device Exposure

INVESTIGATE
Search
AI Search
Threat Graphs
Live Discover

SETTINGS
Integrations
Configured
Marketplace
Detection Rules
Preferences

Threat Analysis Center - Live Discover

Overview / Threat Analysis Center Dashboard / Live Discover

Designer Mode
Lets you create or edit queries

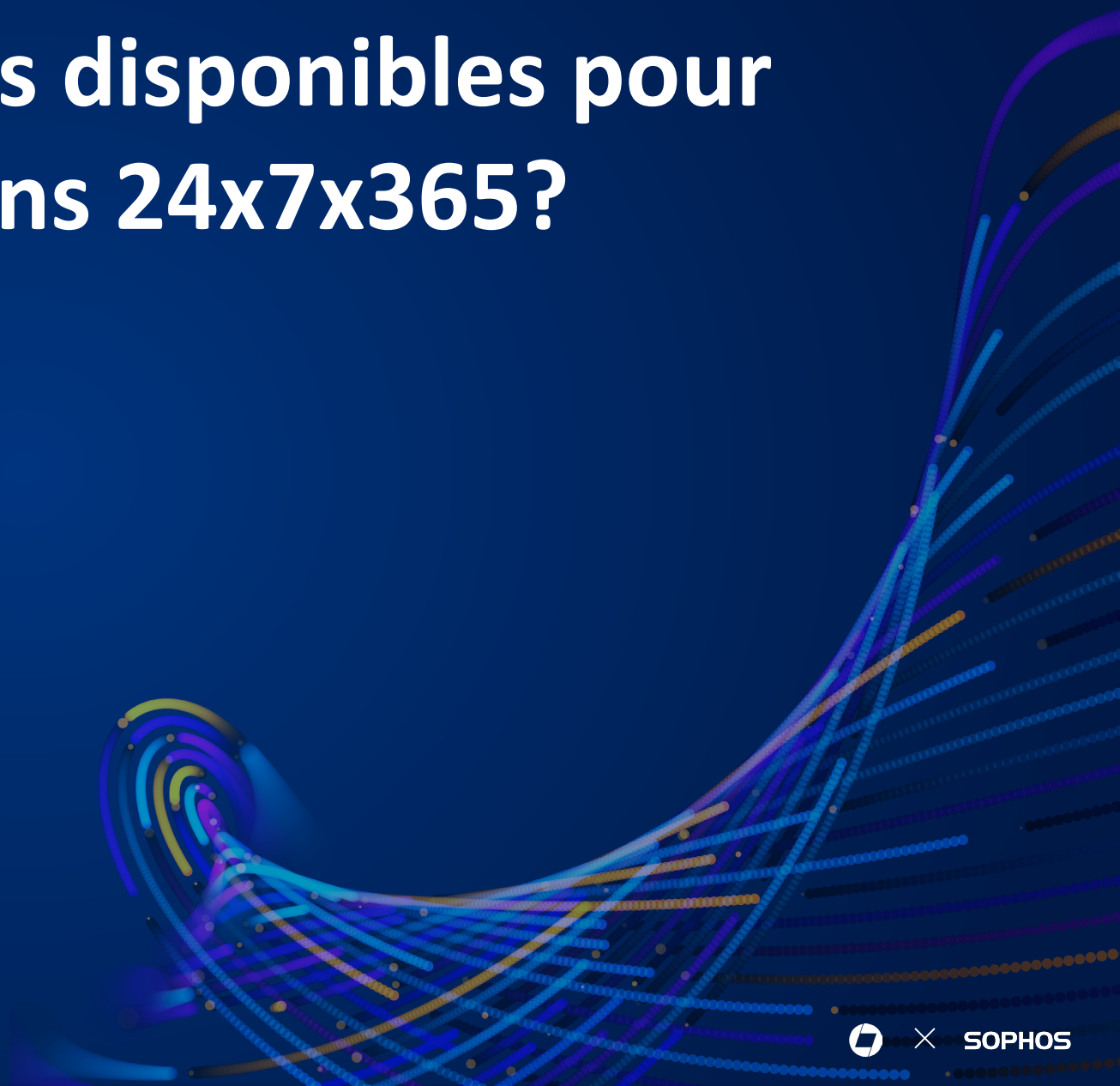
Query : Select One - 0 Categories, 0 Queries

All Queries | Endpoint Queries | Data Lake Queries

Queries that get data from devices or from the Data Lake
Endpoint queries get data from devices that are currently connected. Data Lake queries get data from the Data Lake that your devices upload their data to.

Search

Avez-vous les personnes disponibles pour réaliser ces investigations 24x7x365?



Sophos MDR

Que fait Sophos MDR pour vous?

Ep + XDR +

MDR

Un service managé qui fournit aux clients un SOC 24h/24, 7j/7 et 365j/an pour neutraliser les menaces et les adversaires actifs

D do-not-reply@central.sophos.com

To:
Reply-To: do-not-reply@central.sophos.com

September 13, 2024 at 13:53

This email alert was generated by Sophos Central. Do not reply to this email.

SOPHOS
CENTRAL

CASE ID: 2342522-007

//Analysis
We gave completed an investigation of a detection related to Microsoft Word spawning the MSHTA application on machine “Win11-1”. During the investigation we determined that a malicious attachment “deltaflightitinerary.docm” was received by 4 users, and first opened on “Win11-1” by user “Jim Halpert”. The same file was opened on ”Win10-5” by user “Michael Scott”.

When executed, the MSHTA application connected to an IP address [210-52-109-110] and attempted to download an an HTA file which appears to have been poisoned with a Meterpreter reverse shell command and control agent.

...

D do-not-reply@central.sophos.com

To:
Reply-To: do-not-reply@central.sophos.com

September 13, 2024 at 13:53

//Response actions

As your MDR response mode is “Authorize”, we have taken the following response actions:

1. Terminated malicious PowerShell processes on Win11-1 and Win10-5
2. Blocked attacker C2 IP address [210-52-109-110] on your Sophos protected endpoints
3. Initiated and confirmed status of clawback of the 4 emails received

//Recommendations

We recommend taking the following actions / steps to further contain this threat and limit future attack potential:

1. Block the attacker C2 IP address on your network firewall
2. Consider updating your email filtering policies to restrict incoming attachments with the capacity to execute applications, e.g. .docm files
3. Consider using Application Control to limit the use of applications that are not needed in your environment, e.g. the Microsoft HTML Application / MSHTA
4. Consider anti-phishing training for the users who opened this attachment (Jim Halpert and Michael Scott)

Sophos MDR

Chasse aux menaces

Les recherches proactives de menaces effectuées par des analystes hautement qualifiés permettent de découvrir et d'éliminer rapidement plus de menaces que les produits de sécurité ne peuvent en détecter par eux-mêmes.

Détection des menaces

Les capacités étendues de détection et de réponse (XDR) permettent de détecter les menaces connues et les comportements potentiellement malveillants, quel que soit l'endroit où se trouvent vos données.

Réponse aux incidents

Nos analystes répondent aux menaces en quelques minutes, que vous ayez besoin d'une réponse complète à un incident ou d'une aide pour prendre des décisions plus précises.

Plus de 30'000 clients MDR

99,98 % des menaces sont automatiquement bloquées*

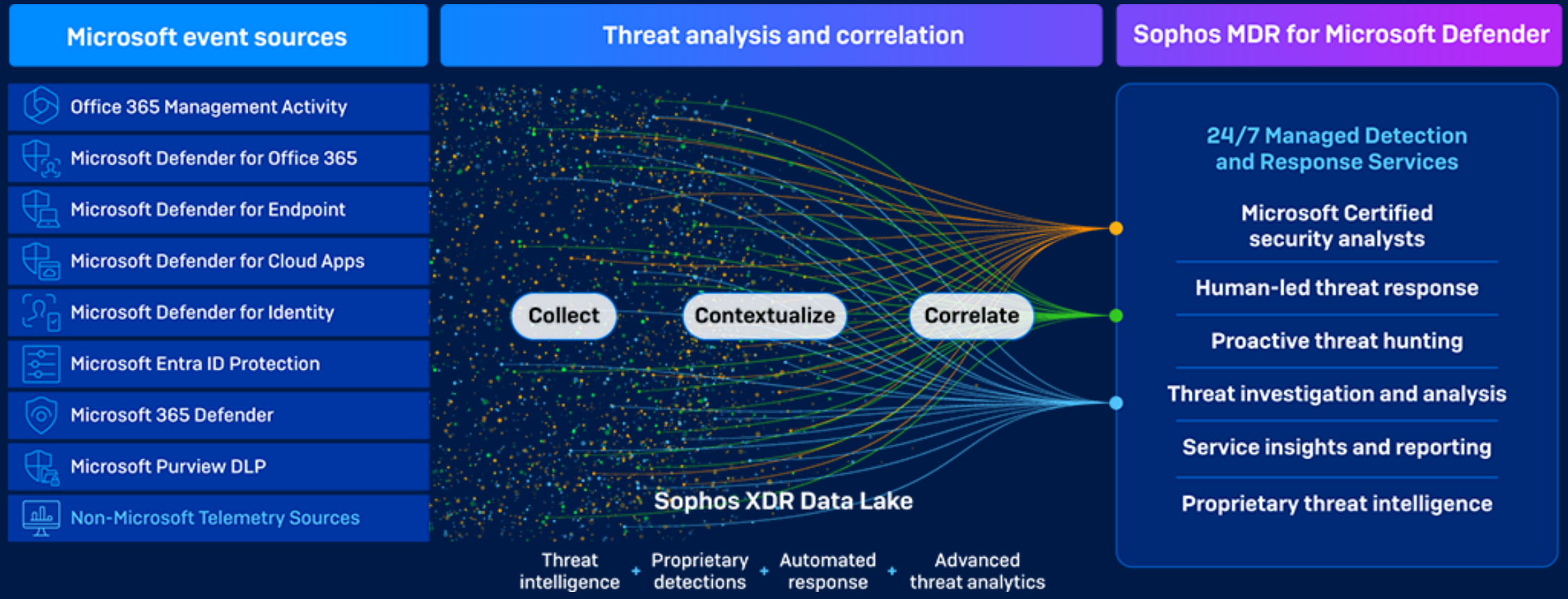
Temps de réponse moyen aux menaces de Sophos MDR

Temps de détection	Moins d'une minute
Il est temps d'enquêter	Moins de 25 minutes
Le temps de répondre	Moins de 12 minutes

SOPHOS

Sophos MDR pour Microsoft Defender

Élargissez votre équipe avec des experts certifiés Microsoft qui surveillent et examinent l'activité 24 h/24, 7 j/7 et exécutent des actions de réponse immédiates dirigées par l'homme pour neutraliser les menaces.



Sophos MDR pour Microsoft Defender

Prend en charge une gamme complète de solutions Microsoft

Intégrations incluses sans frais supplémentaires

Microsoft Certified Security Operations Analysts

Détections propriétaires pour tous les plans M365

Conserve la protection MS-Defender

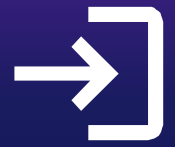
NEW

Actions de réponse pour Microsoft 365

Actions de réponses Microsoft 365 par les analystes Sophos

Block / enable user sign-in

Verrouille le compte d'un utilisateur pour empêcher l'accès aux services M365 et aux ressources Azure à l'aide d'informations d'identification volées. Rétablit l'accès des utilisateurs en quelques secondes.



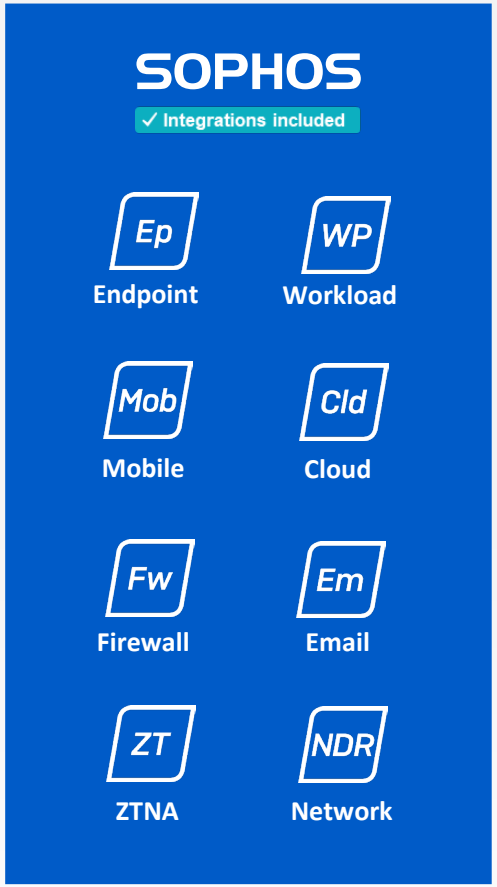
Terminate active user sessions

Révoque les sessions en cours pour qu'un utilisateur spécifique puisse éjecter un attaquant et supprime sa capacité à réutiliser les jetons de session volés.

Disable suspicious inbox rules

Les adversaires créent des règles de boîte de réception dans les attaques de compromission d'e-mail professionnel. Les analystes peuvent désactiver des règles de boîte de réception spécifiques pour reprendre le contrôle.

Visibility across all key attack surfaces



Endpoint ✓ Included

Microsoft · CROWDSTRIKE · SentinelOne · TREND · Symantec by Broadcom (beta) · BlackBerry CYLANCE (beta) · jamf

+ Others with Sophos 'XDR Sensor' agent

Firewall

Barracuda · paloalto NETWORKS · FORTINET · CHECK POINT · CISCO Meraki · f5 · Forcepoint · SONICWALL · WatchGuard

Network

DARKTRACE · THINKST CANARY · CISCO Umbrella · Skyhigh Security · Secutec · VECTRA (beta) · zscaler

Email ✓ Included

Microsoft 365 · Google Workspace · mimecast · TREND · proofpoint.

Productivity

Microsoft 365 ✓ Included

Google Workspace ✓ Included

Cloud

orca security

+ AWS, Azure, and GCP integrations with Sophos Cloud Optix product

aws · A · cloud

Identity

Microsoft ✓ Included · okta · auth0 · CISCO DUO · CISCO ISE · ManageEngine

Backup and Recovery

Acronis · rubrik · veeam

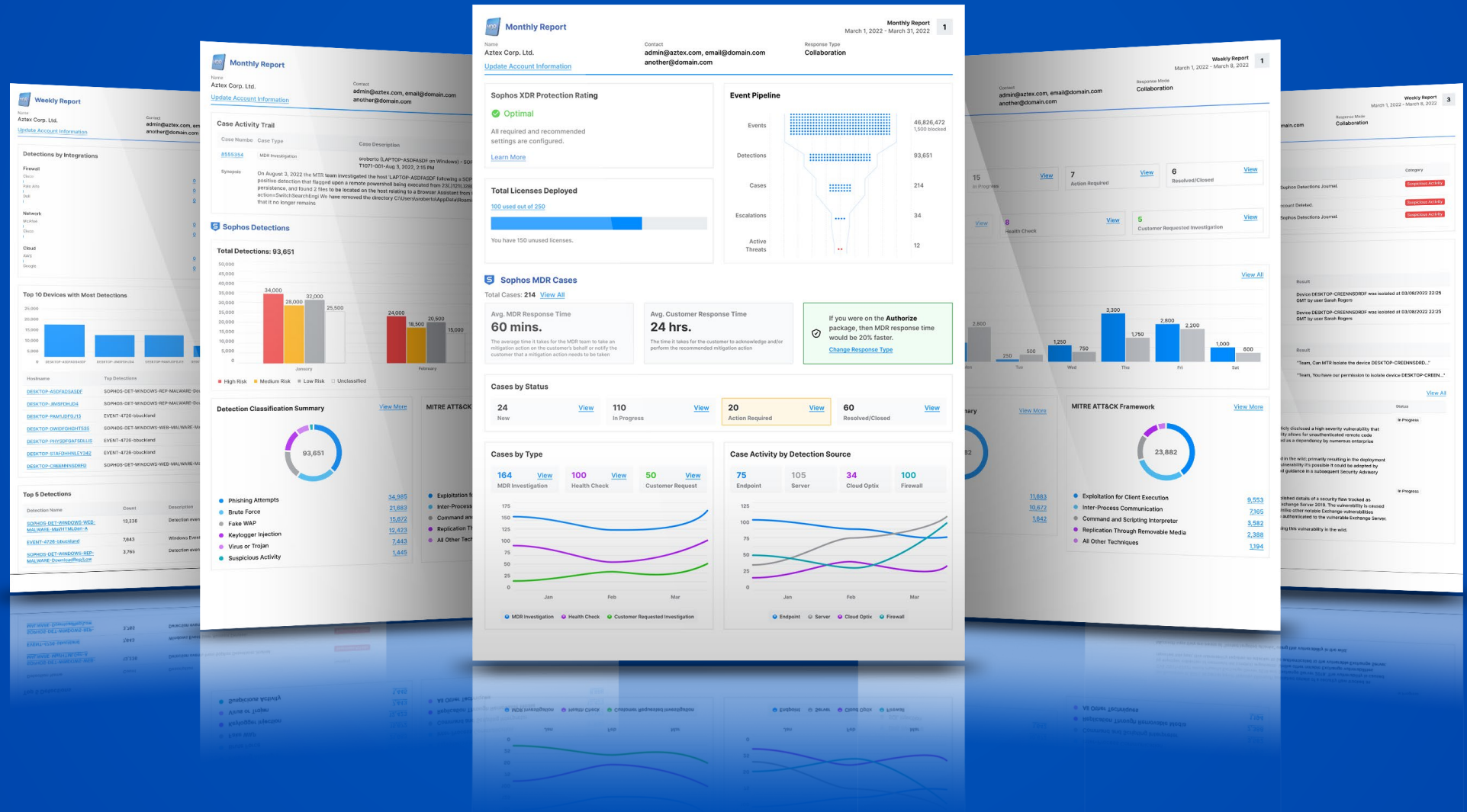
Sophos Endpoint and Sophos Workload Protection solutions are included with Sophos XDR and MDR. Other Sophos integrations require an applicable subscription for the Sophos product.

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 February 26, 2025

SOPHOS

Monthly and Weekly Cybersecurity Reports



Guided On-Boarding (Add-On)

Session **One**

Deployment and Implementation

- Ensures the Sophos Endpoint Agent is installed on all protected devices
- Ensures deployment is successful

Session **Two**

MDR/XDR Training

- How to navigate Sophos Central
- How to use XDR features
- How to respond to cases and work with the MDR team

Session **Three**

Security Posture Assessment

- Ensure your environment is the most secure it can be based on your requirements
- 3 objectives of the assessment
  - Sophos Central Configuration review
  - NIST Cybersecurity Framework Assessment
  - EASM scan and Dark Web Scan

Ep

Protection contre les menaces connues et inconnues grâce à des technologies sophistiquées

XDR

Capacités de détection et de réponse avec télémétrie unifiée à partir de plusieurs technologies de sécurité sur une seule plateforme

MDR

Un service managé qui fournit aux clients un SOC 24h/24, 7j/7 et 365j/an pour neutraliser les menaces et les adversaires actifs

Clear and Simple Packaging

Strongest protection included at all license levels.

	Sophos Endpoint	Sophos XDR	Sophos MDR
Next-Gen Threat Protection Web Protection, Deep Learning anti-malware	✓	✓	✓
Malicious Activity Blocking Anti-ransomware, Exploit Protection, Context-Sensitive Defenses	✓	✓	✓
Threat Exposure Reduction Web Control, Peripheral, Application, DLP	✓	✓	✓
Detection and Response Detections, Hunts, Investigations, Response		✓	✓
Visibility Across Key Attack Surfaces Sophos and 3rd Party Integrations		✓	✓
Managed Detection and Response 24/7 Expert-led Monitoring and Response			✓

Mobile

Intercept X for Mobile
Threat Defence

Central Mobile Standard
Device Management

Central Mobile Advanced
Threat Defence + Device Management

Encryption

Central Device Encryption
Managed Full Disk Encryption

Sophos Managed Risk

Powered by tenable

Sophos Managed Risk

Attack Surface Visibility

tenable

Comprenez tous les actifs et leurs vulnérabilités associées, puis déterminez la priorité de correction en fonction de l'évaluation des risques.

Risk Assessment

tenable

Fournissez de manière proactive des indicateurs clés de performance concis aux équipes de direction et de gestion des risques organisationnels afin d'évaluer l'exposition aux risques.

Risk Monitoring

SOPHOS

Utilisez des outils, des personnes et des processus pour surveiller en permanence la surface d'attaque et concentrer les efforts sur la prévention des attaques probables.

Threat Response

SOPHOS

Une équipe d'experts hautement qualifiés fournissant des services de surveillance, d'enquête, de chasse aux menaces et de réponse aux incidents 24 heures sur 24, 7 jours sur 7.

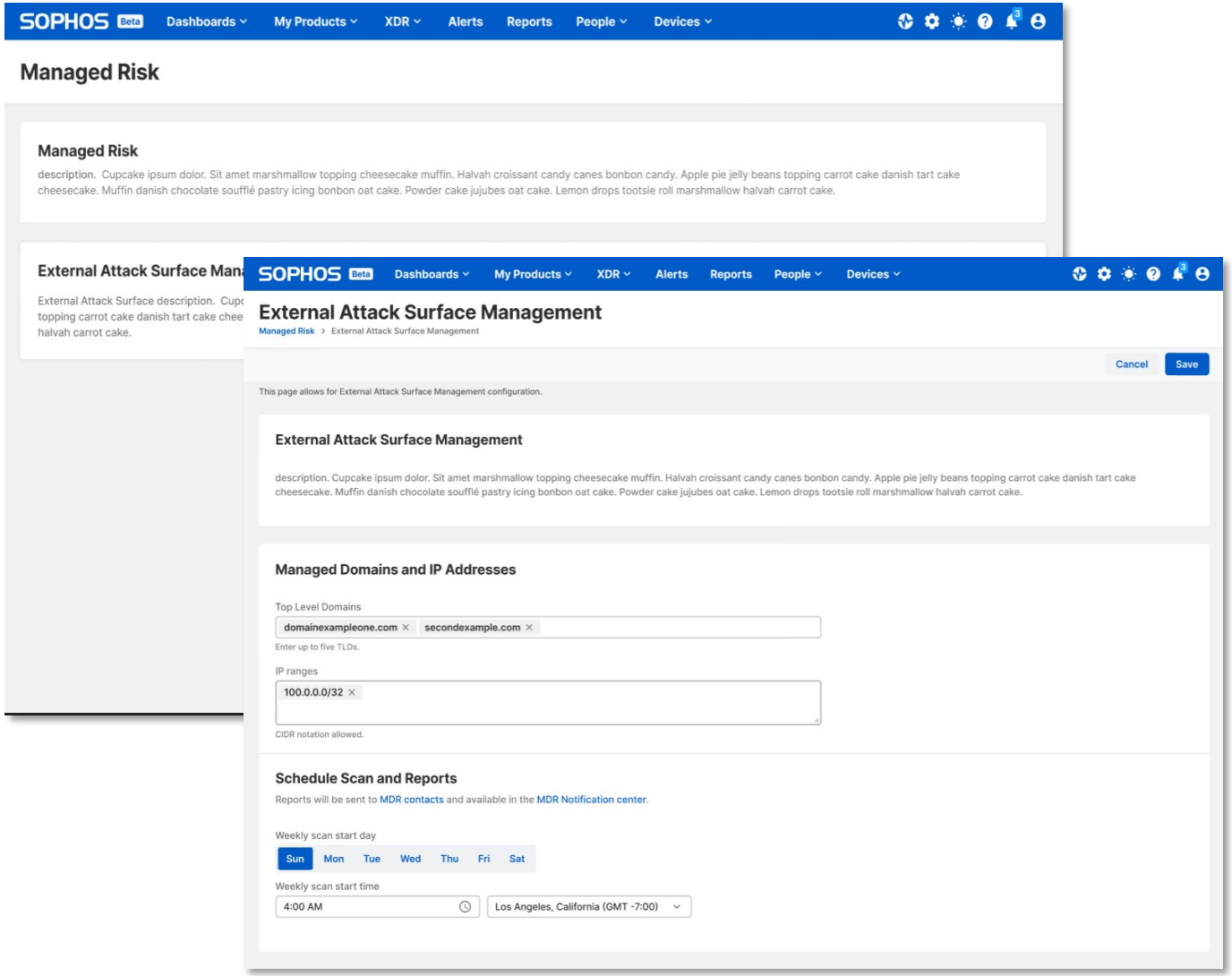
Sophos Managed Risk | Use Cases

1 | ATTACK SURFACE VISIBILITY
Mitigate risk by knowing what you own

2 | CONTINUOUS RISK MONITORING
Extend your team with vulnerability experts

3 | PRIORITIZE VULNERABILITIES
Know what to patch and why

4 | IDENTIFY NEW RISKS FAST
Get alerted to new critical vulnerabilities



tenable × SOPHOS

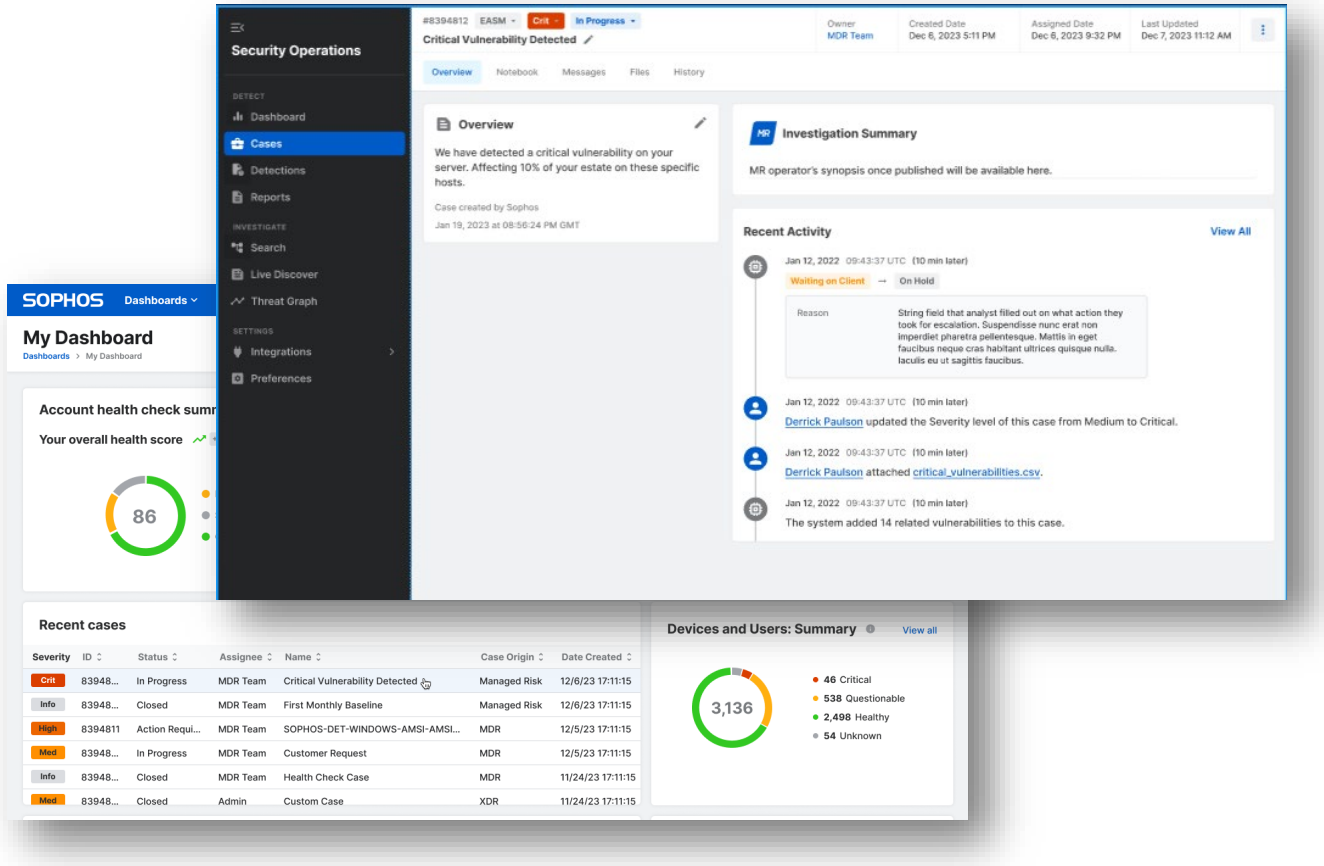
Sophos Managed Risk

Powered by tenable®

Collaborates with Sophos MDR

Fully managed service delivered by threat experts

- Schedule reviews to discuss findings, guidance on the current exploitation landscape, and recommendations for priority remediation
- Create cases to consult with the Sophos Managed Risk team
- View Managed Risk cases alongside your Sophos MDR cases in your Threat Analysis Center



SOPHOS

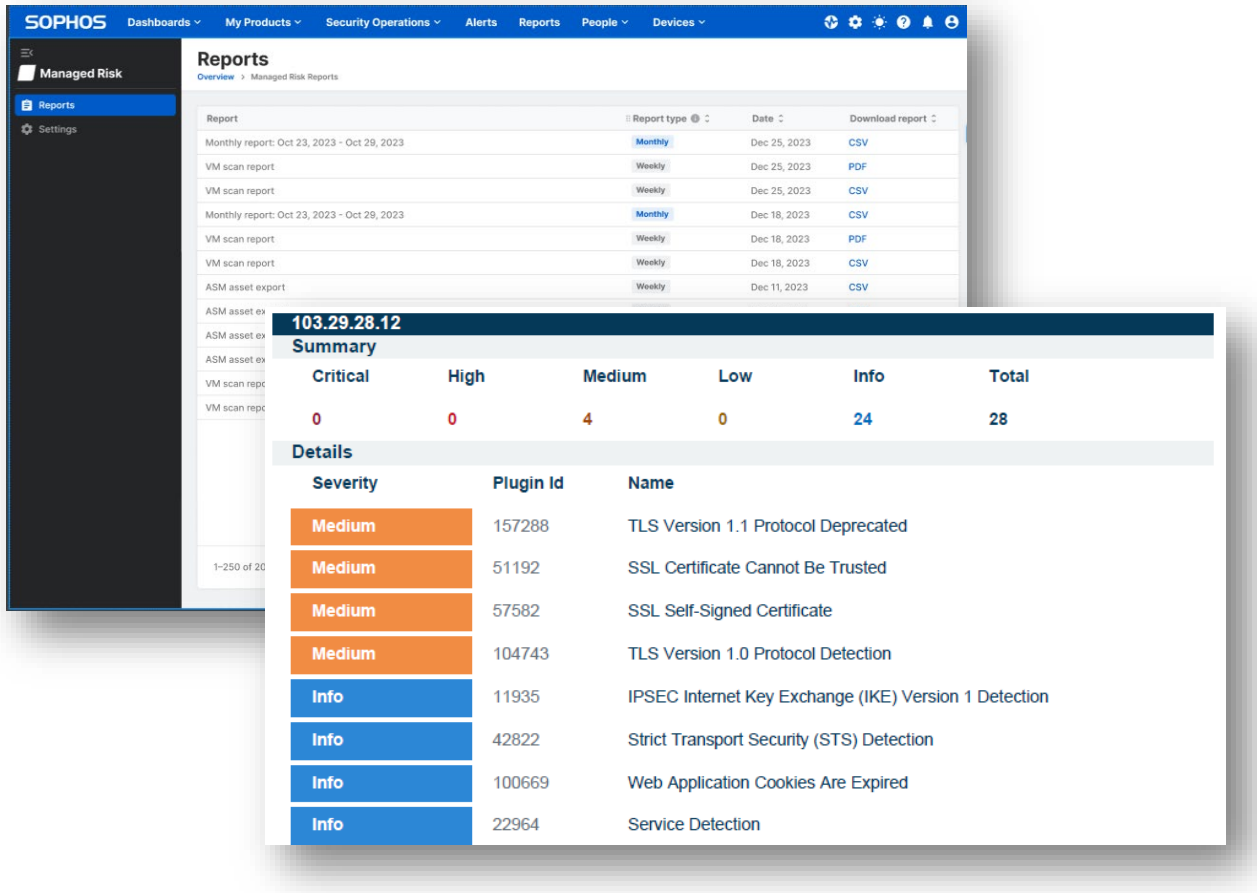
Sophos Managed Risk

Powered by tenable®

Comprehensive reporting

Access to vulnerability data in Sophos Central

- External attack surface reports detail your discovered internet-facing assets
- Comprehensive vulnerability scan reports, prioritized based on risk to your organization
- Links to vulnerability documentation for further information and remediation guidance

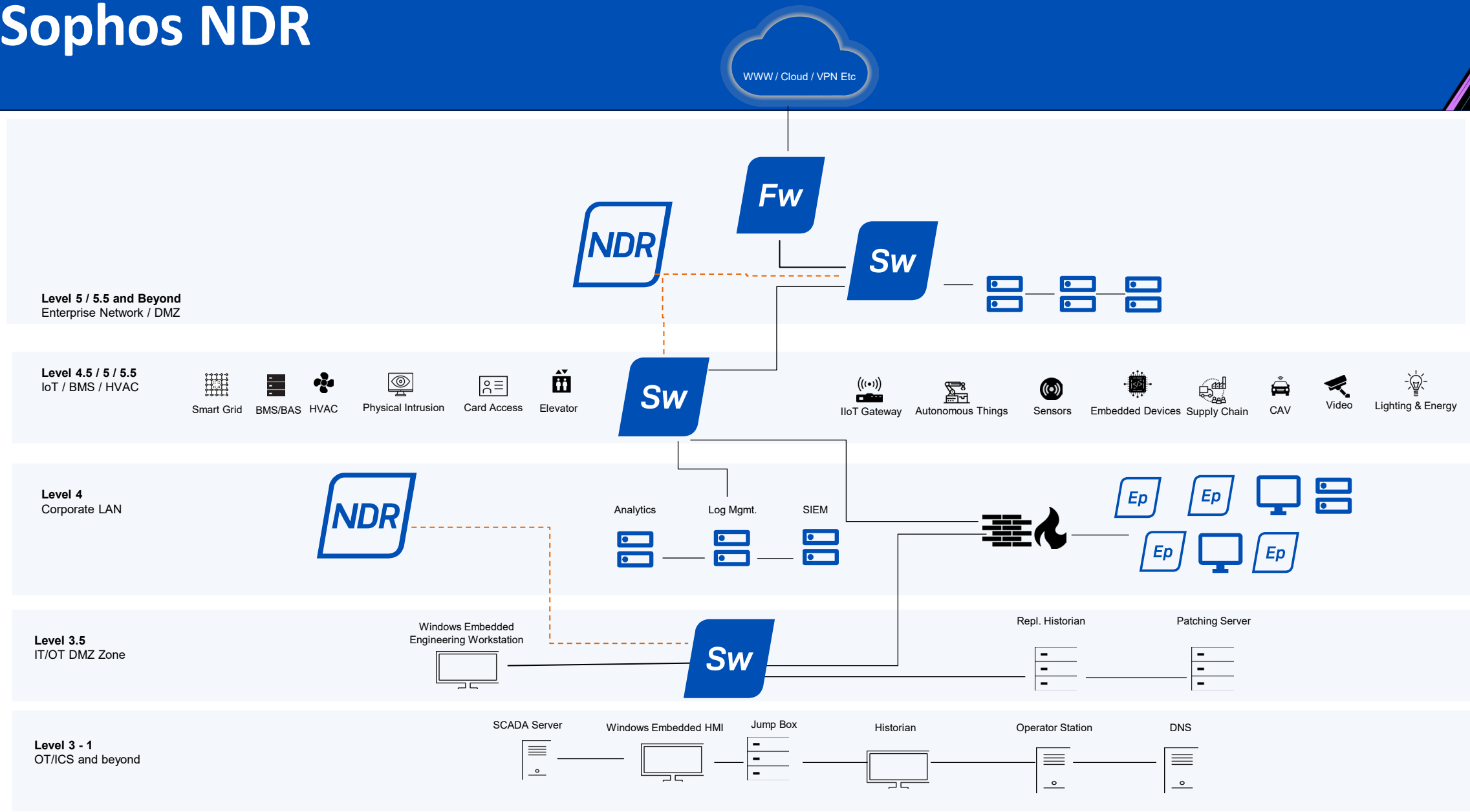


SOPHOS

Sophos NDR

SOPHOS

Sophos NDR


WWW / Cloud / VPN Etc
Fw
NDR
Sw
Level 5 / 5.5 and Beyond
Enterprise Network / DMZ
Level 4.5 / 5 / 5.5
IoT / BMS / HVAC
Smart Grid
BMS/BAS
HVAC
Physical Intrusion
Card Access
Elevator
Sw
IIoT Gateway
Autonomous Things
Sensors
Embedded Devices
Supply Chain
CAV
Video
Lighting & Energy
Level 4
Corporate LAN
NDR
Analytics
Log Mgmt.
SIEM
Ep
Ep
Ep
Ep
Level 3.5
IT/OT DMZ Zone
Windows Embedded
Engineering Workstation
Sw
Repl. Historian
Patching Server
Level 3 - 1
OT/ICS and beyond
SCADA Server
Windows Embedded HMI
Jump Box
Historian
Operator Station
DNS

Top Sophos NDR use cases

Unsecured Devices

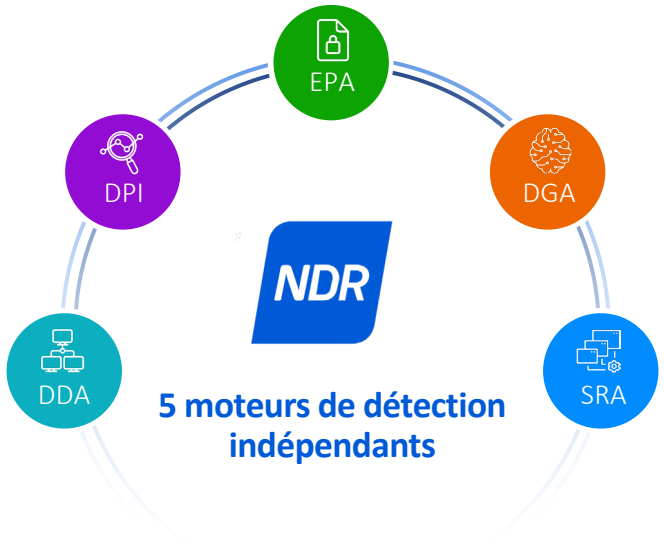
Unauthorized Devices

IoT/OT Threats

Zero-Day attacks

Insider Threats

Sophos NDR: Étendre la visibilité sur le trafic réseau



DDA — Device Detection Analytics

Identifie la communication des équipements réseaux qui ne sont pas gérés par Sophos, ce qui inclu les périphériques non-autorisés et/ou potentiellement malveillants.

DGA — Domain Generation Algorithms

Intelligence artificielle en 'deep learning' intégrant une mémoire à long terme pour prédire des noms de domaine générés automatiquement grâce à un algorithme.

DPI — Deep Packet Inspection

Détecte les Indices de compromission (IOC) parmi le trafic en clair et le trafic chiffré afin d'identifier les acteurs et les TTP (Tactiques, Techniques et Procédures)

SRA — Session Risk Analytics

Moteur logique puissant qui utilise des règles qui alertent sur un facteur de risque basé sur des sessions (Certificats TLS auto-signé, transfert d'application binaire, etc.)

EPA — Encrypted Payload Analytics

Détecte les serveurs de C&C zéro-Day et les nouvelles variantes de malware en se basant sur des patterns découverts dans les sessions réseaux (taille de paquets, sens du flux réseau et intervalles de temps).

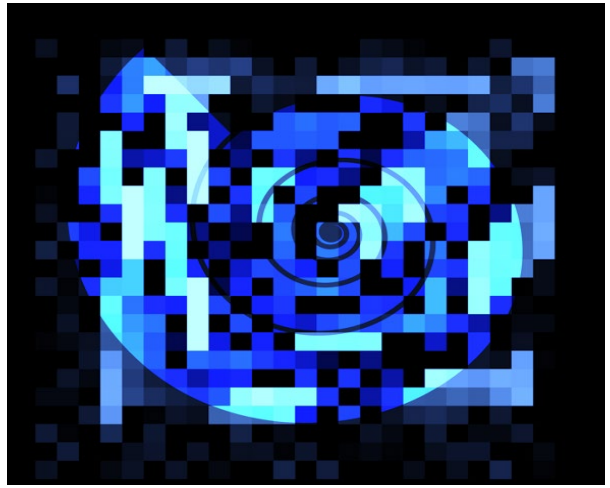
Encrypted Payload Analytics

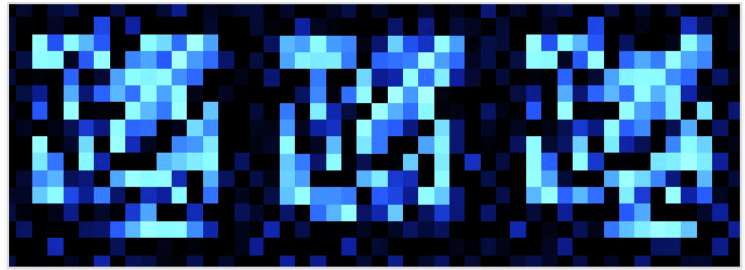
Sophos NDR

Sophos NDR extracts important information about the encrypted payload packets. Known in the NDR industry as the **Sequence of Packet Length and Interarrival Time (SPLIT)**, each packet has a payload size, direction, and arrival time.

```
[127, 0, -1382, -37, 0, 134, -59, 389, 1354, 0, 1354, 1354, 1354, 0, 1354, 1354, 233, 0, 0, 0, -789, 0, 389, 1354, 1354, 1354, 1354, 1354, 1354, 233, 0, 0]
[0, 0, -2746, -69, 585, 23241, -179643, 2559, 47, -171964, 652, 39, 12, -184557, 640, 37, 12, -52793, -116186, -5, 490, -427740, 214454, 796707, 307, 25, 9, 7, 7, 8, 8, -203697, -5948]
```

```
0, 0, 25, 0, 51, 0, 178, 0, 0, 0, 0, 0, 0, 0, 0, 0, 25, 0,
76, 204, 204, 128, 51, 0, 0, 0, 0, 102, 76, 128, 178, 102, 0,
0, 0, 153, 0, 204, 0, 102, 0, 26, 25, 0, 76, 204, 102, 0, 0,
26, 0, 51, 127, 230, 229, 230, 0, 0, 76, 204, 204, 102, 229,
76, 25, 0, 76, 102, 127, 26, 102, 76, 0, 26, 0, 51, 0, 230,
0, 128, 25, 0, 76, 153, 127, 230, 102, 153, 25, 0, 76, 76,
127, 230, 102, 76, 25, 0, 76, 51, 127, 153, 102, 153, 0, 26,
0, 76, 0, 0, 0, 51, 25, 0, 76, 153, 127, 230, 102, 102, 25,
0, 76, 76, 127, 204, 102, 178, 0, 0, 51, 51, 76, 153, 76,
153, 0, 26, 0, 26, 0, 153, 0, 204, 0, 26, 0, 51, 0, 128, 0,
76, 0, 0, 0, 26, 0, 178, 0, 51, 0, 0, 178, 153, 204, 153,
229, 128, 0, 26, 0, 76, 0, 230, 0, 76, 0, 26, 76, 76, 204,
26, 229, 204, 25, 26, 76, 102, 127, 153, 102, 0, 25, 0, 76,
153, 127, 26, 102, 128, 25, 0, 76, 76, 127, 102, 102, 128,
25, 0, 76, 51, 127, 76, 102, 153, 25, 0, 76, 51, 127, 0, 102,
230, 25, 0, 76, 51, 127, 0, 102, 230, 0, 0, 51, 51, 76, 51,
76, 76, 0, 0, 0, 51, 0, 51, 0, 76, 0, 26, 0, 76, 0, 26, 0, 76
```





Cobalt Strike Beacon

(Limb, J. (2021). *Identifying Network Applications Using Images Generated from Payload Data and Time Data. US Patent 11,159,560.* Washington, DC: U.S.)

SOPHOS

The First MDR-Focused Firewall

with purpose-built active threat detection and response capabilities

SOC

MDR

XDR

SOPHOS X-OPS

APTs
Active C2s

3rd PARTIES

Domains
Bad IPs
IPS

SOPHOS NDR

NDR

AI Analysis
of TLS & DNS

SOPHOS DNS

DNS
Protection

SOPHOS vCISO

Threat Intel
and
Fortification

"Ross in a Box"

SECURE BY DESIGN

Proactively monitored by Sophos
Containerized OS
Hardened access
Over-the-Air updates

ADVANCED AI DETECTIONS

Multiple AI threat intel sources:
MDR | XDR | NDR | EDR
- Sophos or Third Party -
Direct feeds to the Firewall

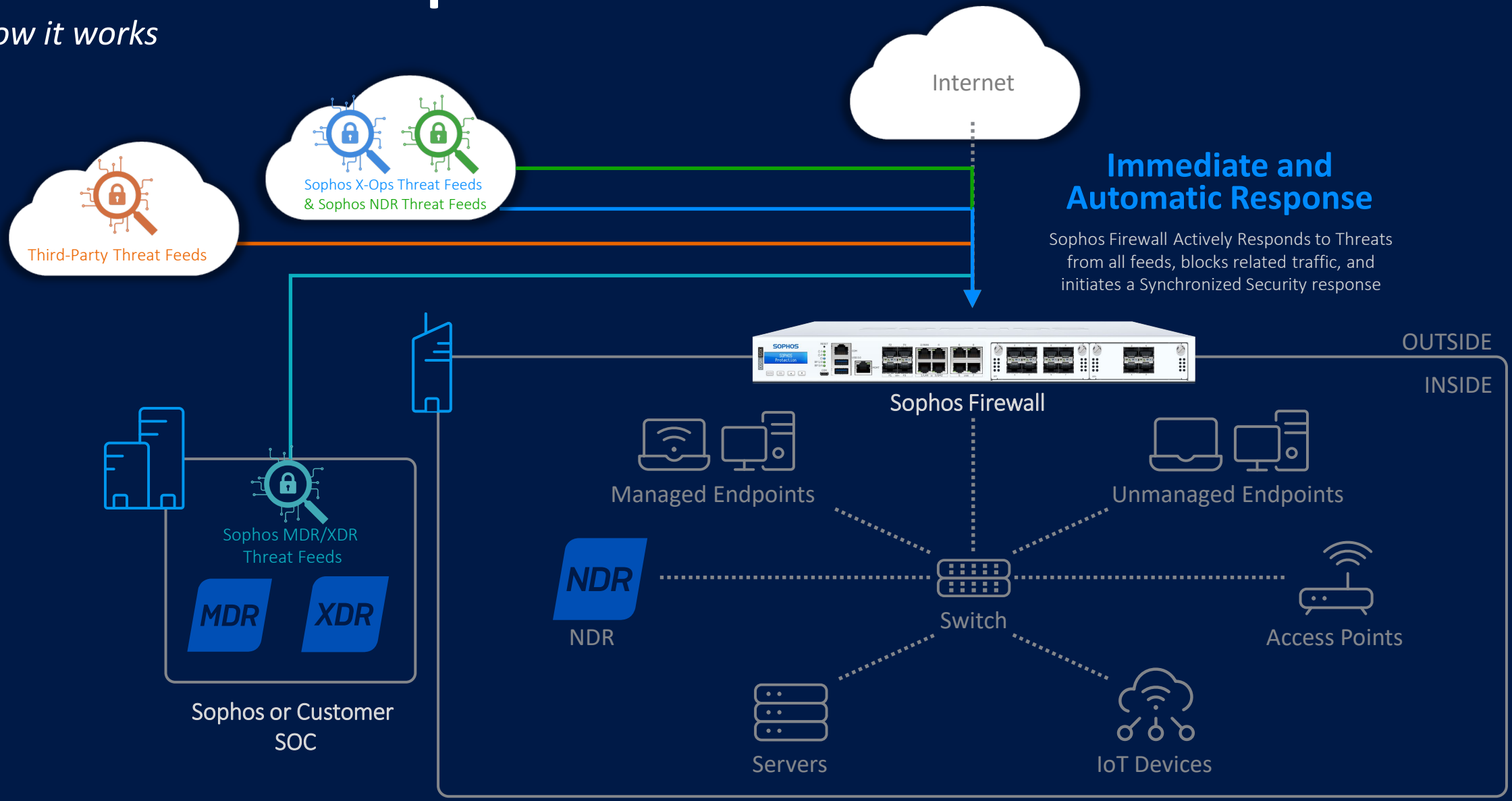
ACTIVE THREAT RESPONSE

Auto response to active threats
with Synchronized Security and
Lateral Movement Protection

SOPHOS

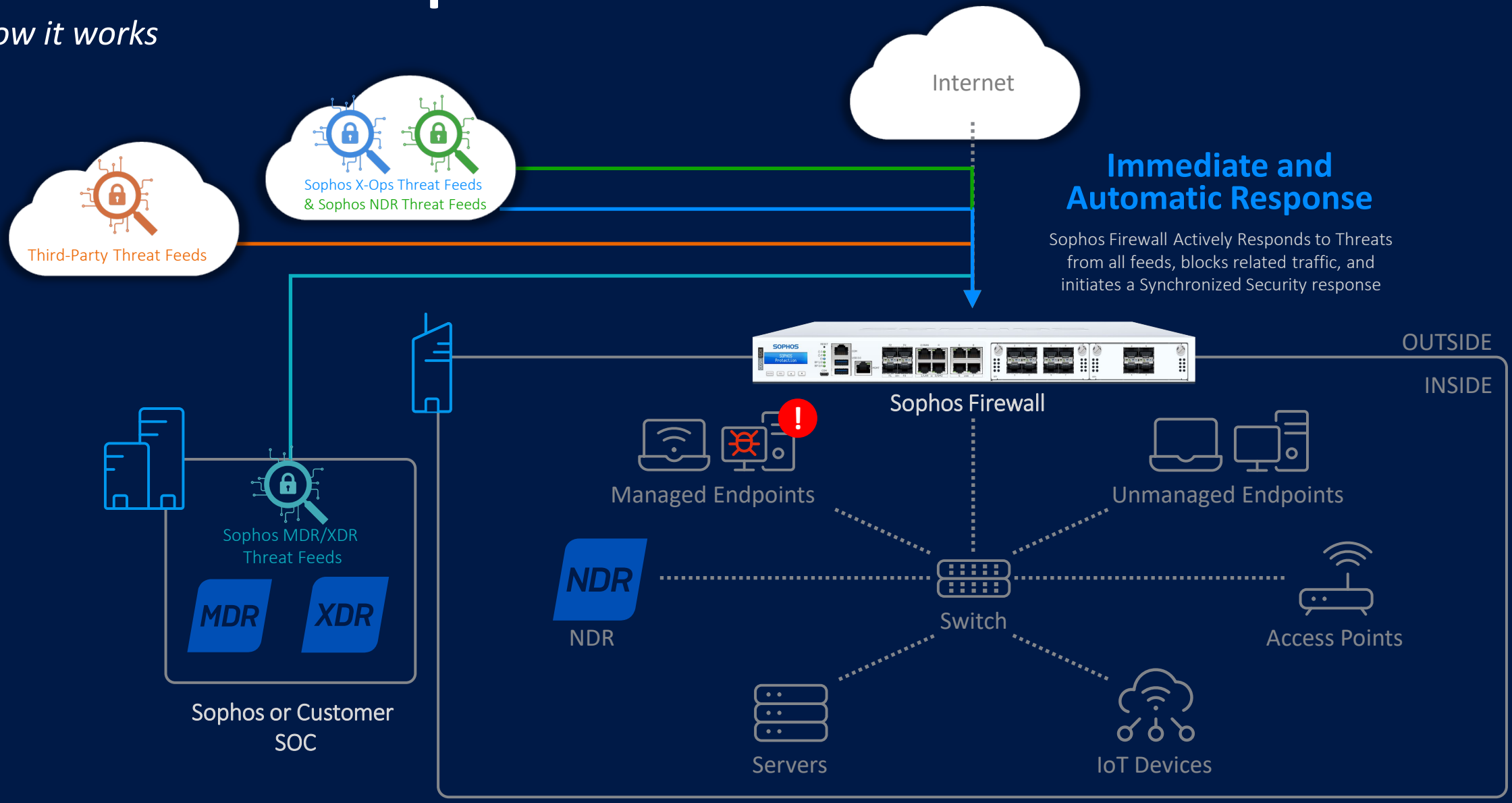
Active Threat Response

How it works



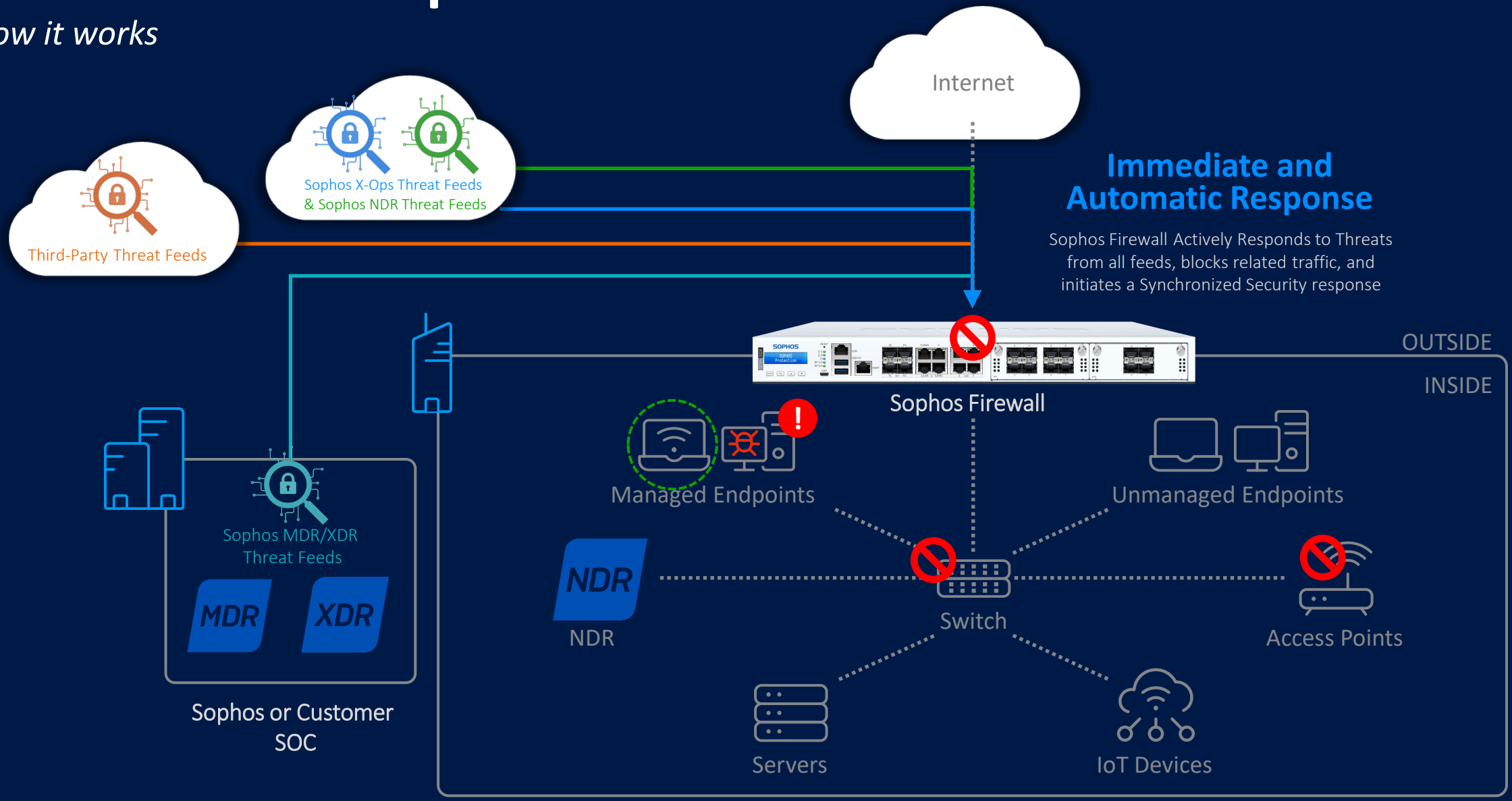
Active Threat Response

How it works



Active Threat Response

How it works



Gartner®

D’ici à 2026, plus de 60 % des organisations utiliseront des services MDR fournis directement par les éditeurs de solutions de sécurité.

SOPHOS

Cybersecurity Assessment.

Bechtle Suisse SA vous propose la mise à disposition des consultants de cybersécurité pour objectif l'analyse de votre niveau de sécurité et la définition de votre feuille de route.

Les consultants ont une connaissance de toutes les bonnes pratiques de cybersécurité et maîtrisent l'identification des vulnérabilités. Ils vous accompagnent pour :

- **Identifier les lacunes de sécurité** par rapport aux normes et standards de sécurité ;
- **Détecter les vulnérabilités de votre système** à travers des outils d'analyse ;
- **Analyser votre niveau et dresser une feuille de route sur 5 ans** afin d'augmenter votre niveau de protection face aux menaces en évolution continuelle.

L'Assessment est composé des 4 phases suivantes :

- **Phase 1 – Initialisation** : Organisation du projet, validation des intervenants et des prérequis pour l'installation des outils de détection des vulnérabilités
- **Phase 2 – Questionnaire de sécurité** : Workshop de diagnostic de votre niveau de sécurité actuel (entretiens et déroulement d'un questionnaire avec votre responsable informatique ou de sécurité)
- **Phase 3 – Audit technique** : Installation et configuration des outils de détection des vulnérabilités, puis recueil et analyse des résultats
- **Phase 4 – Feuille de route** : Proposition d'une feuille de route et estimation des budgets et ressources nécessaires pour sa mise en oeuvre, validation et présentation des résultats à la Direction

Merci!

Des questions ? Contactez-nous :
it-forum.ch@bechtle.com


bechtle