
SOPHOS
PARTNER 2026
EXPERIENCE

SOPHOS

Agenda

Agenda

Horario	Sesión
11:30h	Registro y Bienvenida
11:45h	Visión y Estrategia de Sophos
12:00h	De la visión a la realidad: innovaciones en la plataforma y novedades del Roadmap
12:25h	Estrategia de Canal de Sophos: Triunfando juntos
12:50h	AWS & Sophos: Acelerando tus ventas
13:30h	**CÓCTEL & NETWORKING**
15:00h	El auge de la detección y respuesta gestionadas & Endpoint
15:30h	Juntos somos más fuertes: la estrategia del ecosistema de Microsoft
15:50h	Seguridad desde el diseño: la próxima generación de protección mediante Firewall
17:00h	Actividad Exclusiva
19:00h	**PARTNER AWARDS & COCKTAIL**


aws
INGRAM MICRO
SOPHOS
PARTNER 2026 EXPERIENCE
ALSO
TD SYNNEX
veeam

¡No pierdas tu acreditación!

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

PARTNER 2026 EXPERIENCE

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE

SOPHOS


Noche y cena para dos
Noche y cena para dos
smartbox
2 PERSONAS | +1100 ESTANCIAS
1 NOCHE, DESAYUNO, CENA Y/O SPA
Hoteles gastronómicos
Masías
Casas rurales
Haciendas
¡Y mucho más!
Tripadvisor
Tripadvisor traveler rating
Puntuación media de nuestros colaboradores en España

Agenda

Horario	Sesión
11:30h	Registro y Bienvenida
11:45h	Visión y Estrategia de Sophos
12:00h	De la visión a la realidad: innovaciones en la plataforma y novedades del Roadmap
12:25h	Estrategia de Canal de Sophos: Triunfando juntos
12:50h	AWS & Sophos: Acelerando tus ventas
13:30h	**CÓCTEL & NETWORKING**
15:00h	El auge de la detección y respuesta gestionadas & Endpoint
15:30h	Juntos somos más fuertes: la estrategia del ecosistema de Microsoft
15:50h	Seguridad desde el diseño: la próxima generación de protección mediante Firewall
17:00h	Actividad Exclusiva
19:00h	**PARTNER AWARDS & COCKTAIL**

Naveed Malik

EMEA MSP Senior Director

Jason Ellis

EMEA VP Channel

Dermot Hayden

EMEA Distribution Director

SOPHOS

PARTNER 2026 EXPERIENCE

Visión y Estrategia de Sophos

Álvaro Fernández

Iberia Sales Director

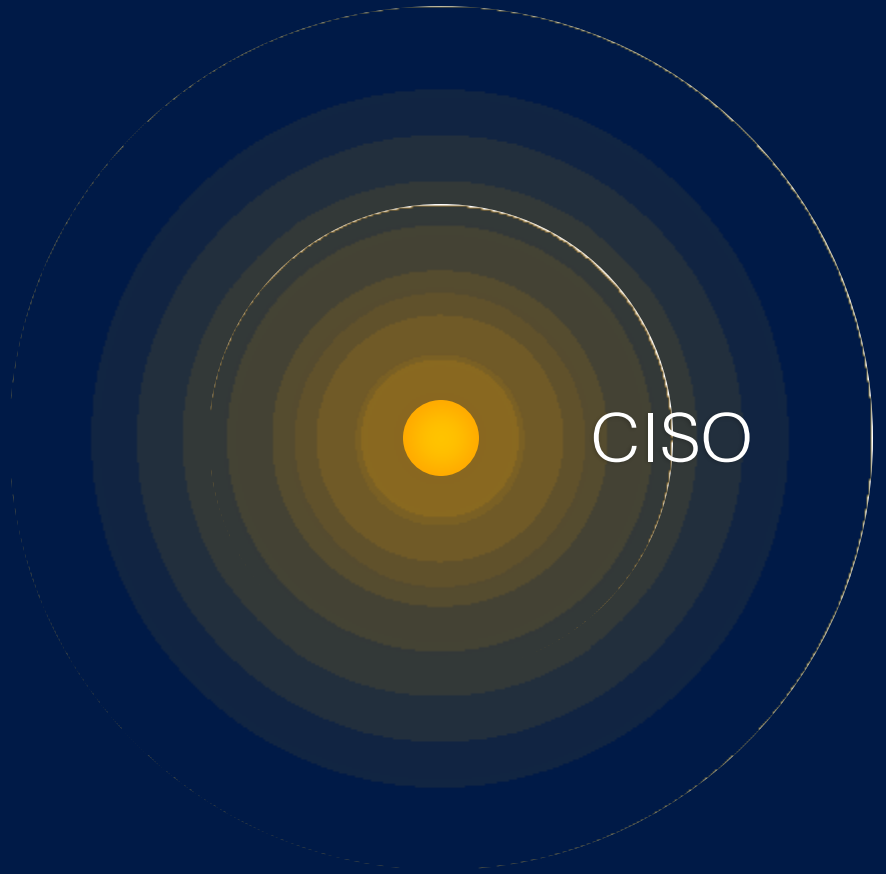
VISION AND MISSON

Why we exist.

Why Sophos

Why now

Why we win


CISO

10,000

OUR VISION

A world where the most trusted cybersecurity is also the most accessible.

OUR MISSION

Erase the cybersecurity poverty line and democratize resilience by driving advances in technology and services, AI, and global threat intelligence.

Sophos Strategy

Portfolio

Build for the most demanding environments. Make it accessible to everyone.

Channel

Scale through partners as the operating model, not just the route to market.

Customer

Make outcomes the product and the system the proof.

Operating Model

AI is the multiplier. People remain strategic and accountable.

Culture

Build things that matter. Be people worth trusting. We are a company of builders.

SOPHOS	Proof Point
Scale that compounds into intelligence	600,000+ customers; every threat feeds the system
Human judgment at the control point	MDR analysts supervise AI, own critical decisions, and preserve trust
A defense system, not a stack	One architecture; detection anywhere triggers response everywhere
The strongest first line of defense	Autonomous protection stops threats before they become incidents
The most complete Microsoft security integration	Proprietary detection rules; surfacing threats that MSFT misses

Why Sophos

We have identified the root cause

Why now

We have named the inflection

Why we win

We have built the system


SOPHOS

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

PARTNER EXPERIENCE 2026

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE

SOPHOS

De la visión a la realidad: innovaciones en la plataforma y novedades del Roadmap

Alberto R Rodas

Iberia SE Manager

SOPHOS PORTFOLIO AND ROADMAP

Introducing the AI-Native Defense System

SOPHOS

PARTNER 2026 EXPERIENCE

WHAT WE'LL COVER…

- The architecture of the industry's first AI-native defense system, and why differentiated in the market.
- The FY27 innovations that expand your opportunity, from Next-gen SIEM to Secure AI to CISO Advantage.
- Why together we **are positioned to** to build the best Cyber Security outcomes with both our SMB and Enterprise customers.

SOPHOS

SOPHOS CENTRAL

Managed by Customers | Managed by Partners | Managed by Sophos

SERVICES

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

THREAT PREVENTION AND CONTROLS

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Cloud

INTEGRATIONS

350+ Third Party Integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

THREAT INTELLIGENCE

SOPHOS X-OPS

- Adversary Tracking
- Threat Research
- Breach Forensics
- Malware Analysis
- Industry Collaboration

AI, AUTOMATION & ENGINEERING

- Adaptive Attack Protection
- Critical Attack Warning
- Security Analytics
- Detection Logic
- Threat Protection

UNIFIED DATA FABRIC

AI-NATIVE DEFENSE SYSTEM

Sophos Central

The AI-Native Cybersecurity Defense System

CONTROL POINTS

Native and third-party

Compounding Intelligence

Agentic autonomy + human accountability

Synchronized Security™

UNIFIED DATA FABRIC

SOPHOS

	✕ Product Stacks (What they sell)	✓ Defense System (What we built)
Data	Aggregated from siloed products	Single unified data fabric, real-time
AI Role	Feature layer bolted on top	AI *is* the architecture; remove it and the system must function differently
Response	Manual or playbook-driven automation across consoles	Synchronized; detection automatically triggers response everywhere
Intelligence	Static per-product models	Compounds across 600K+ organizations
Integration	Assembled via acquisitions	Native inside. Open outside. 350+ integrations

SOPHOS

Two Leaders. One architecture. The most complete defense system in cybersecurity.

Unified XDR and Next-gen SIEM

Fully integrated into Sophos Central. One platform, one experience.

Upgraded MDR Services

Combines the operational expertise of Sophos MDR and Taegis MDR.

Sophos X-Ops + Counter Threat Unit

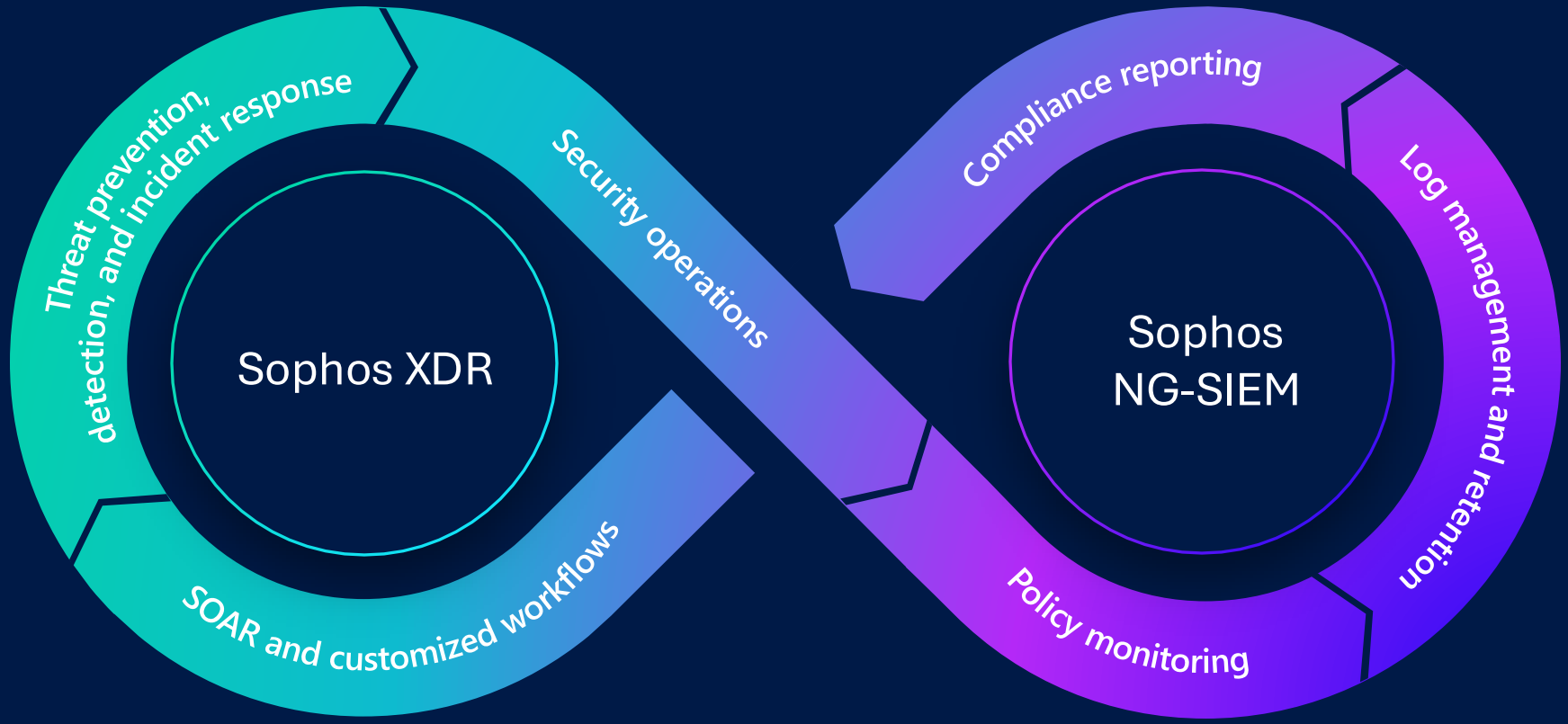
Sophos threat research + Secureworks CTU = threat tracking across every layer

350+ Integrations and growing...

Open integration framework inherited from the Taegis platform

SOPHOS

Next-gen SIEM: A major growth opportunity



SOPHOS

Secure AI: Protecting the new attack surface

VISIBILITY

See every AI tool across the environment

Shadow AI discovery
AI usage dashboard
Endpoint + Network + Browser multi-layer detection

CONTROL

Enforce AI policy without slowing innovation

Granular access management
Global policy enforcement
Role-based controls
Prompt monitoring

PROTECTION

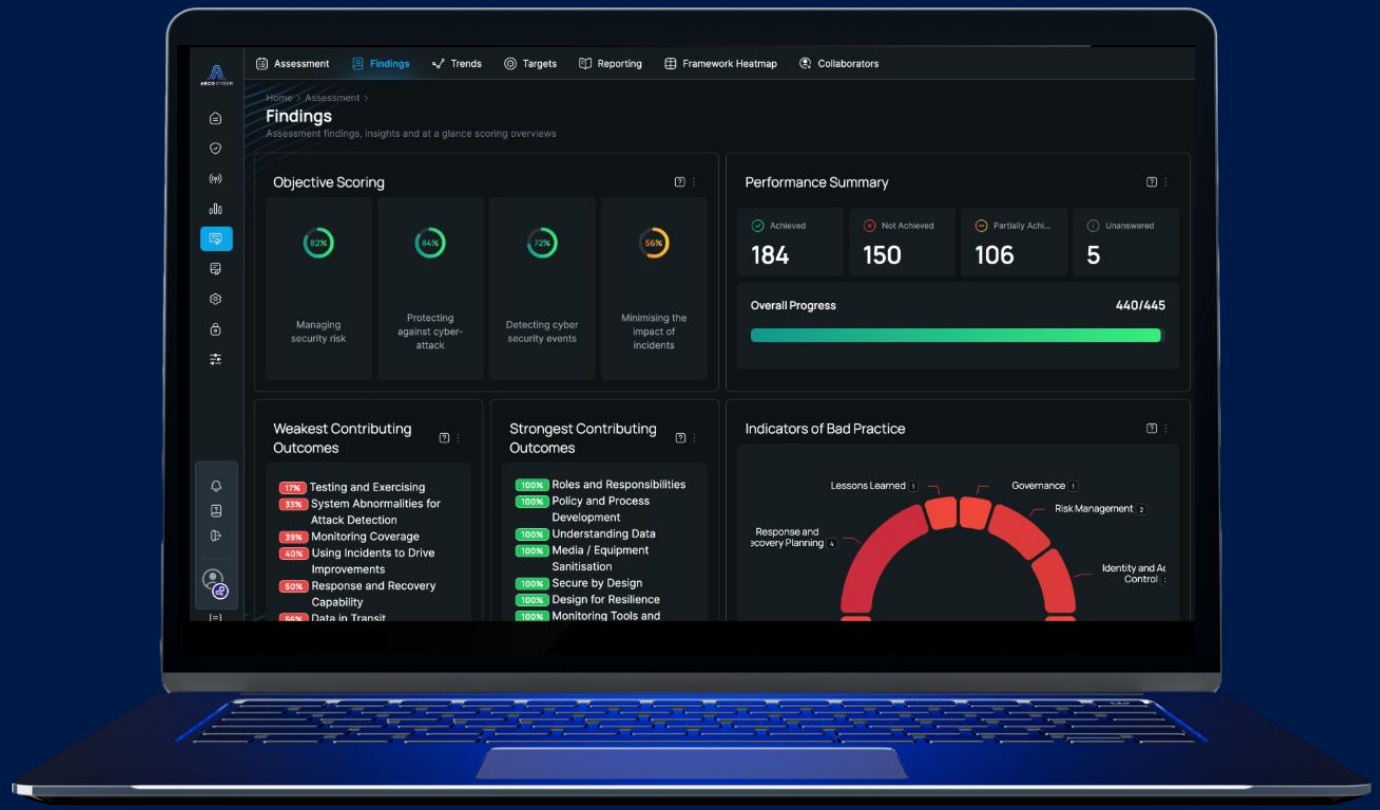
Defend data and block high-risk AI behavior

Input sanitization
Output interception
DLP for AI prompts
MDR-managed AI risk 24/7

SOPHOS

COMING OCTOBER 2026

Sophos CISO Advantage



SOPHOS

SOPHOS

Protection	Endpoint, Firewall, Email, Cloud, Workspace Protection	*The strongest first line of defense in the industry.*
Detection & Response	XDR, NG-SIEM, EDR, NDR, ITDR, SOAR	*Displace Splunk/Sentinel. Already integrated.*
Managed Services	MDR, Incident Response, Vulnerability Management	*37K+ MDR customers. World's largest operation.*
Advisory Services	Security Services Retainer	*On-demand expertise with built-in flexibility.*
Secure AI Coming in July	Visibility, Control, Protection for AI adoption	*Secure the new attack surface.*
CISO Advantage Coming in October	Risk assessment, compliance, peer benchmarking	*Strategic leadership and risk management as a service*

SOPHOS

The system is built.
The innovation is accelerating.
Now we go win **together.**


SOPHOS

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE

Estrategia de Canal de Sophos: Triunfando juntos

Manuel Alonso

Iberia Channel Director

Thank you!

RECORD HIGH

Incredible 60,000 partner projects closed via deal reg in past 12 months

MARKET SHARE

Sophos MDR is the number 1 MDR solution in Europe, Middle & Africa

RECORD YEAR

2025 saw record new customer wins thanks to our partners

NUMBER 1

Sophos MSP partners grew 26% and exceeds 3500 active partners

Partners drive every stage of the customer journey

2026
EMEA cybersecurity opportunity

$99.57bn ↑ +11.6%

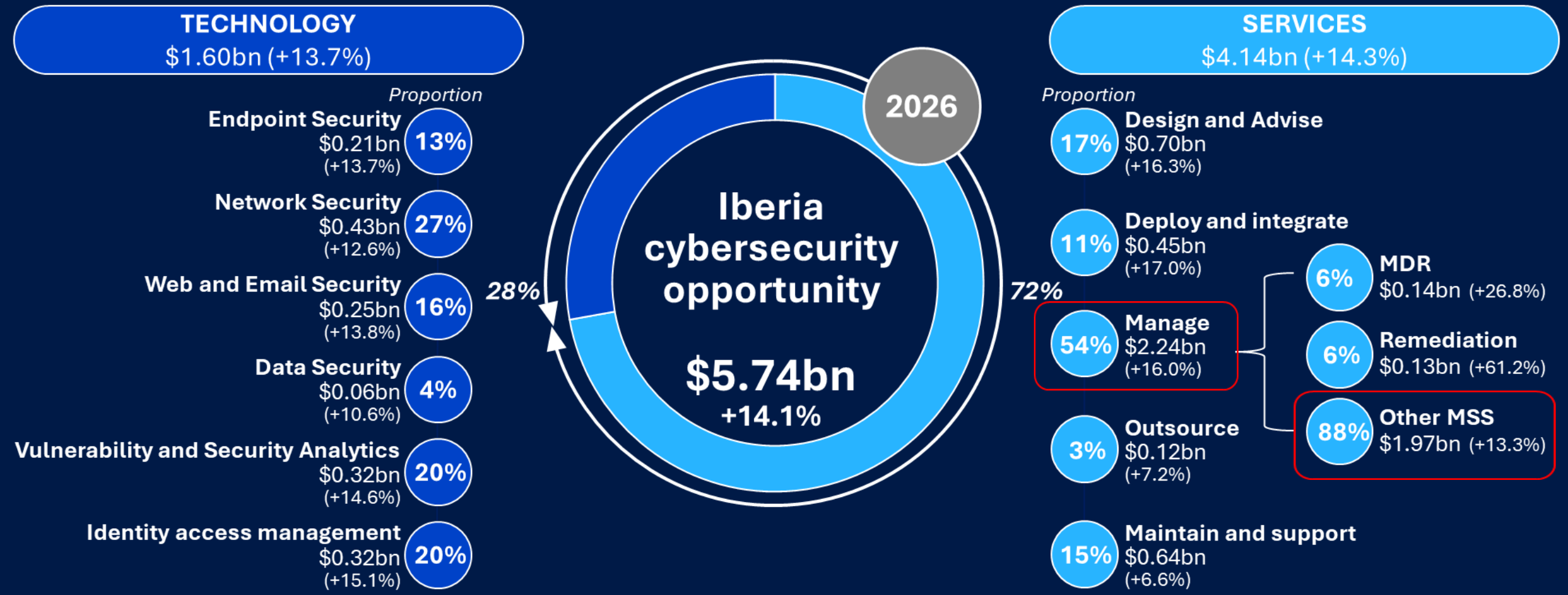
>90%

sold through and with partners

- Advise and design **12%**
- Sell technology **32%**
- Deploy and integrate **7%**
- Maintain and support **10%**
- Manage and outsource **39%**

Source: Omdia Cybersecurity Ecosystems, 2026

Iberia cybersecurity opportunity to reach $5.74bn in 2026



Source: Omdia Cybersecurity Ecosystems, 2026

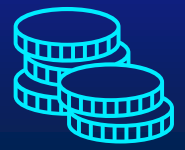
SOPHOS

PARTNER 2026 EXPERIENCE

Accelerate your growth with Sophos

PROFITABILITY

- Award winning partner program managing $1B of projects
- **NEW:** Deal reg extended to all opportunities
- Extra 10% for new customer wins extended



SERVICES

- **NEW:** Teaming agreements available this quarter
- Defined engagement, long term protection

AI PARTNER AGENT

- Stand out with our new **Sophos Sales Professional certification**
- Check out “Win with Sophos” training series

CAMPAIGNS

- Earn $$ every time you sell Sophos !!
- We pay you for closing 5k+ Deal reg opportunities
- Terms apply

Accelerate your growth with Sophos

PROFITABILITY

SERVICES (MSP)

AI PARTNER AGENT

CAMPAIGNS

MSP

For Partners who deliver Sophos security as part of a managed IT service, protecting customers day-to-day with simple, flexible, usage-based billing. Best suited to MSPs managing security alongside broader IT services for SMB and Mid-Market customers.

- Sophos Central at the heart of MSP Efficiency
- Usage Based Aggregated Billing – aligns costs and revenue
- MDR Bundles for MSPs – differentiation and scale
- Integrates seamlessly with RMM & PSA systems

Manage $6.84bn (+10.9%)

Source: Omdia Cybersecurity Ecosystems, 2026

More Choice. More Control.
One Powerful Sophos MSP Program.

MSP

Partnerships require valid Sophos reseller and MSP agreements

Partner-owned license entitlements

MSP FLEX

Deliver Sophos cybersecurity solutions on a flexible, usage-based model.

REQUIREMENTS

- **Complete your sales certification (SC01)**
- **Get approval for monthly billings with Disti of choice**
- **Use PSA/RMM tools and provide Level 1 support to your managed customers**

Consumption-based billing in arrears

MSP ELEVATE

Unlock exclusive MSP rewards: MDR bundles, 40% off hardware, free training, growth incentives and more.

REQUIREMENTS

- **Meet the requirements of MSP Flex**
- **Minimum monthly spend of $2,000 USD (or local currency equivalent)**
- **12-month participation period**

Accelerated discounts and benefits

Accelerate your growth with Sophos

PROFITABILITY

SERVICES (MSSP)

AI PARTNER AGENT

CAMPAIGNS

MSSP

For Partners provide security as a core, specialist service, delivering advanced threat detection and response such as MDR, often with 24/7 monitoring and security operations.

- Scale without building a platform
- Build MDR/XDR services faster (MTTR)
- Deliver outcomes, not just alerts
- Drive operational efficiency and resilience
- **NEW:** Certified Training available

$5.92bn (+7.8%)

Source: Omdia Cybersecurity Ecosystems, 2026

Accelerate your growth with Sophos

PROFITABILITY

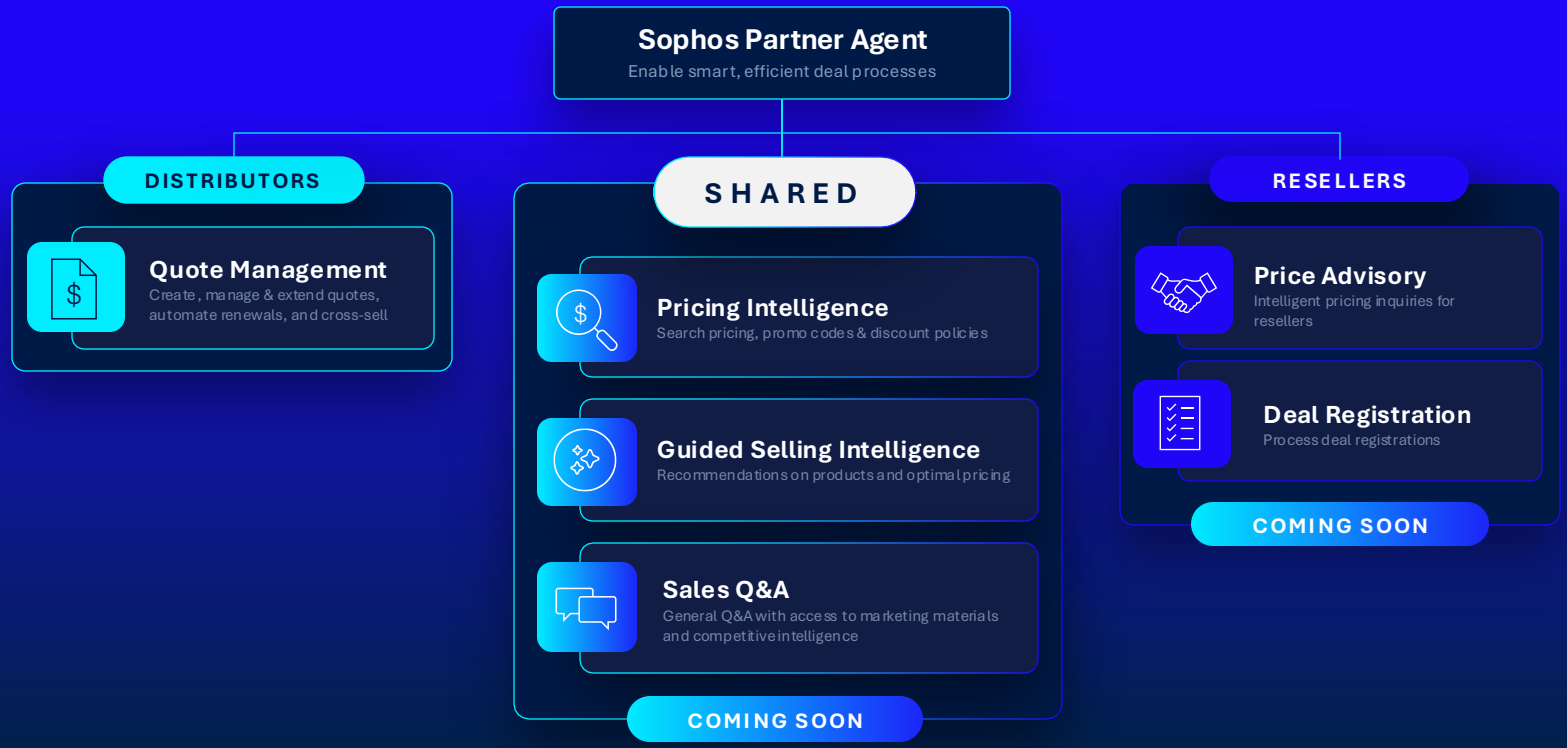
SERVICES (MSP)

AI PARTNER AGENT

CAMPAIGNS

Introducing the Sophos Partner Agent

A unified AI-powered experience to simplify and accelerate partner deal workflows



SOPHOS

PARTNER 2026 EXPERIENCE

What's Next

Expanding capabilities to drive even greater partner impact

AVAILABLE NOW

Distributors:

- Quote management (renew, upgrades & cross-sell)
- Pricing intelligence

COMING SOON IN H1

All Partners:

- Guided Selling
- Sales Q&A
- Price Intelligence
- Access directly within your Microsoft Teams environment

Distributors:

- Expanded quote management capabilities (new, amend & extend)

Resellers:

- Price Advisory
- Deal Registration

This is just the beginning of a **smarter, more connected** partner experience.

SOPHOS

PARTNER 2026 EXPERIENCE

Accelerate your growth with Sophos

PROFITABILITY

SERVICES

AI PARTNER AGENT

CAMPAIGNS

Sophos + Microsoft Stronger Together

Sophos Endpoint Prevention First

Neutralize Cyber Threats 24/7

Firewall Displacement "Secure by Design"

- Purpose built marketing campaigns from execution to pipeline
- Awareness – Consideration - Decision
- Speak to your Account Manager or Distributor for details

¡Gracias!

CRECIENDO JUNTOS

+1,100 Arquitectos certificados a día de hoy!

CONSTRUYENDO JUNTOS

+50 Actividades de co-marketing!

GANANDO JUNTOS

+6,200 oportunidades ganadas juntos en los últimos 12 meses!

SOPHOS

PARTNER 2026 EXPERIENCE


SOPHOS
PARTNER 2026
EXPERIENCE

AWS & Sophos acelerando tus ventas

Manuel Alonso

Iberia Channel Director

SOPHOS

Jose Rayo

Snr. Manager – EMEA
Software Partnership
AWS

Modera:

Ruth Velasco

Marketing Director
EMEA South
SOPHOS

SOPHOS

PARTNER 2026 EXPERIENCE

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

PARTNER EXPERIENCE 2026

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE


SOPHOS
PARTNER 2026
EXPERIENCE

Agenda

Horario	Sesión
11:30h	Registro y Bienvenida
11:45h	Visión y Estrategia de Sophos
12:00h	De la visión a la realidad: innovaciones en la plataforma y novedades del Roadmap
12:25h	Estrategia de Canal de Sophos: Triunfando juntos
12:50h	AWS & Sophos: Acelerando tus ventas
13:30h	**CÓCTEL & NETWORKING**
15:00h	El auge de la detección y respuesta gestionadas & Endpoint
15:30h	Juntos somos más fuertes: la estrategia del ecosistema de Microsoft
15:50h	Seguridad desde el diseño: la próxima generación de protección mediante Firewall
17:00h	Actividad Exclusiva
19:00h	**PARTNER AWARDS & COCKTAIL**

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

PARTNER 2026 EXPERIENCE

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE

SOPHOS

Endpoint Innovation to MDR Expansion: From Prevention to Outcomes

Javier Donoso

Senior Sales Engineer

AI just made the endpoint the front line

AI DIDN'T JUST INCREASE ATTACK VOLUME,
IT COLLAPSED THE TIME WINDOW TO REACT.

SOPHOS

PARTNER 2026 EXPERIENCE

Recognized by analysts, customers and 3rd party tests

for continuous innovation

Gartner

16x [illegible]der

Ma[illegible]int
P[illegible]ion Pl[illegible]s

MITRE | ATT&CK®

100%

Detection coverage in MITRE ATT&CK® Enterprise 2025 Evaluation (Round 7)

G2 Grid® Reports

Leader

MDR, Endpoint, Firewall, XDR, and EDR

SE LABS

AAA Rating

Enterprise Endpoint Security

SE LABS

AAA Rating

Small Business Endpoint Security

Gartner Peer Insights Customers' Choice™

Endpoint Protection Platforms

SOPHOS

PARTNER EXPERIENCE 2026

Sophos Named a Leader in the 2026 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

Positioned as a Leader for the 17th Consecutive Report

May 27, 2026

SOPHOS

PARTNER 2026 EXPERIENCE

Recognized by analysts, customers and 3rd party tests

for continuous innovation

Gartner

17x Leader

Magic Quadrant for Endpoint Protection Platforms

MITRE | ATT&CK®

100%

Detection coverage in MITRE ATT&CK® Enterprise 2025 Evaluation (Round 7)

G2 Grid® Reports

Leader

MDR, Endpoint, Firewall, XDR, and EDR

SE LABS

AAA Rating

Enterprise Endpoint Security

SE LABS

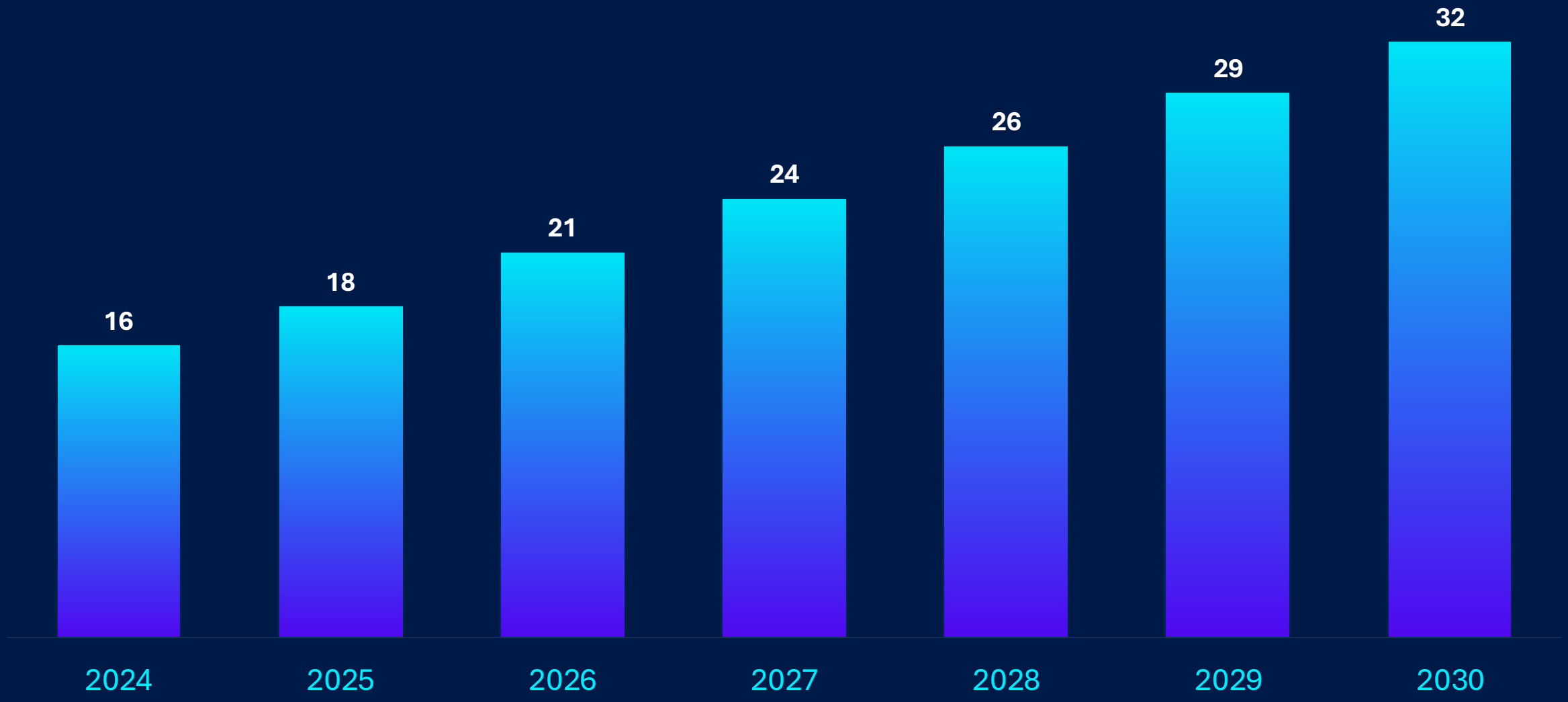
AAA Rating

Small Business Endpoint Security

Gartner Peer Insights Customers' Choice™

Endpoint Protection Platforms

ENDPOINT MARKET GROWTH (BILLIONS)



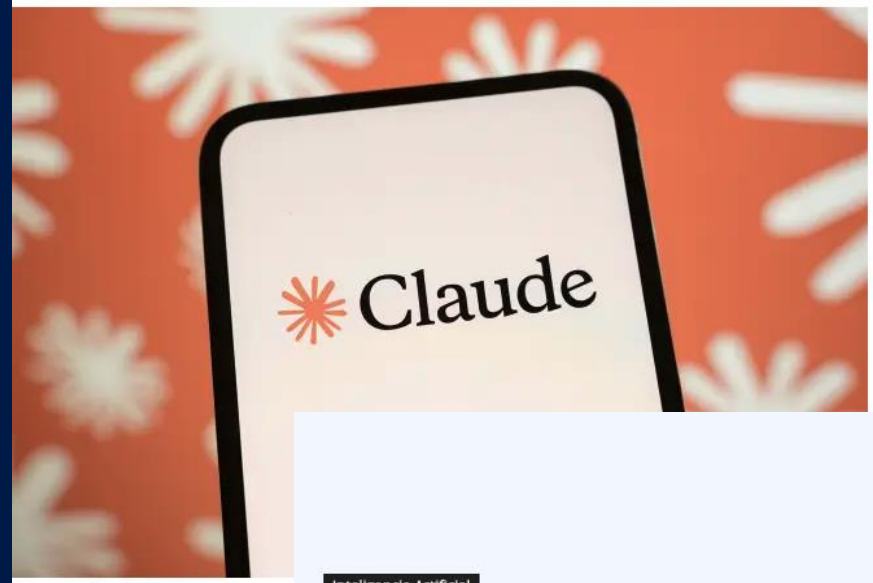
Source: Gartner, March 2026 model


LEAKED // CLASSIFIED
CAPYBARA TIER // BEYOND OPUS
CLAUDE MYTHOS
Step-change AI model with unprecedented cybersecurity capabilities. What it means for defenders.
ANTHROPIC

Tecnología

Qué es Claude Mythos y por qué esta IA provocó una cumbre urgente en Wall Street

El nuevo modelo de Anthropic se especializa en detectar fallos de ciberseguridad



El logo de Claude. Getty

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIMAS NOTICIAS

INTELIGENCIA ARTIFICIAL >

E Anthropic oculta su nuevo modelo de IA, Mythos, por ser demasiado peligroso

La compañía ha optado por ceder estrictamente su acceso a unas docenas de empresas escogidas para que lo usen para proteger su 'software'

TECNOLOGÍA

La IA más avanzada de Anthropic …a que, de …o lo podrán usar 40 …s de seguridad

…almente en marzo, supera en un 25% …de seguridad informática. Anthropic …igroso para el público general y lo …cios seleccionados bajo el programa

Inteligencia Artificial

abril 13, 2026

Claude Mythos no es el peligro, es la señal de lo que viene

Realizado por **Nyria**

1752

Compartir

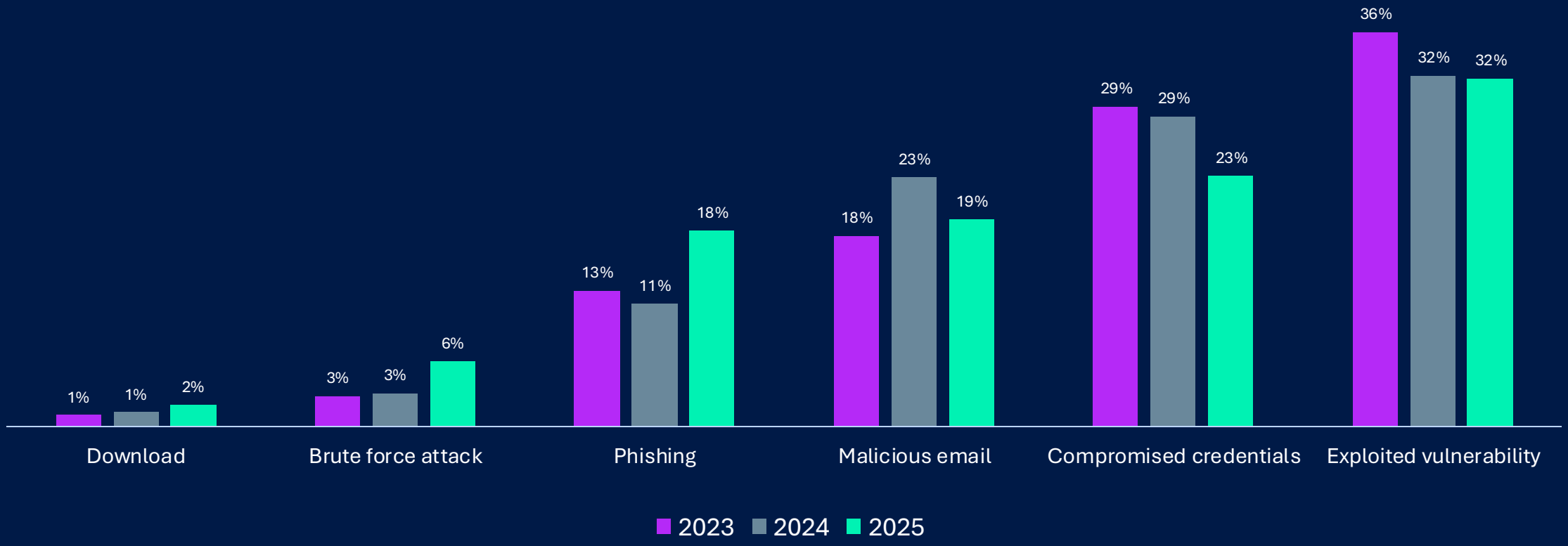
PARTNER 2026 EXPERIENCE

The vulnerability flood is here. Here's what it means – and how to prepare

We can't control the pace of AI-driven vulnerability discovery, but we can control how fast we respond.

Technical Root Cause of Attacks

For the third year running, exploited vulnerabilities are the top-reported root cause of ransomware attacks



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=3,400 (2025), 2,974 (2024), 1974 (2023).

Prevent threats from executing

CryptoGuard

STOP RANSOMWARE THAT
OTHER SOLUTIONS MISS

- Monitors files for malicious encryption
- Blocks local and remote attacks
- Automatic rollback of affected files
- Stops remote ransomware
- Doesn't depend on indicators of "bad"
- Master Boot Record (MBR) protection

Adaptive Attack Protection

BLOCK THE ATTACKER'S NEXT
MOVE BEFORE IT HAPPENS

- Detects "Hands-on-Keyboard" attacks
- Dynamically strengthens protections
- Blocks malicious actions / behaviors
- Prevents lateral movement
- Powered by Sophos X-Ops researchers
- Includes customizable controls

Anti-Exploitation

REDUCE YOUR ATTACK SURFACE
AND THREAT EXPOSURE

- Zero-day attack protection
- Real-time scanning
- Web protection
- Identify unpatched devices
- Protection for Office applications
- Pre-configured—no tuning required

Reduce exposure to attack

Web Protection and Control

Stops threats at the delivery stage by preventing users from being diverted to malware delivery or phishing websites. Block access to undesirable or inappropriate content, such as adult and gambling websites.

Peripheral Control

Monitor and block access to removable media, Bluetooth, and mobile devices to prevent certain hardware from connecting to your endpoints and network.

Application Control

Block potentially vulnerable or unsuitable applications or applications used for nefarious purposes using Sophos' pre-defined categories, simplifying the process of monitoring and management.

Data Loss Prevention

Monitors and restrict the transfer of files containing sensitive data.

For example, prevent employees from sending confidential files home using web-based email.

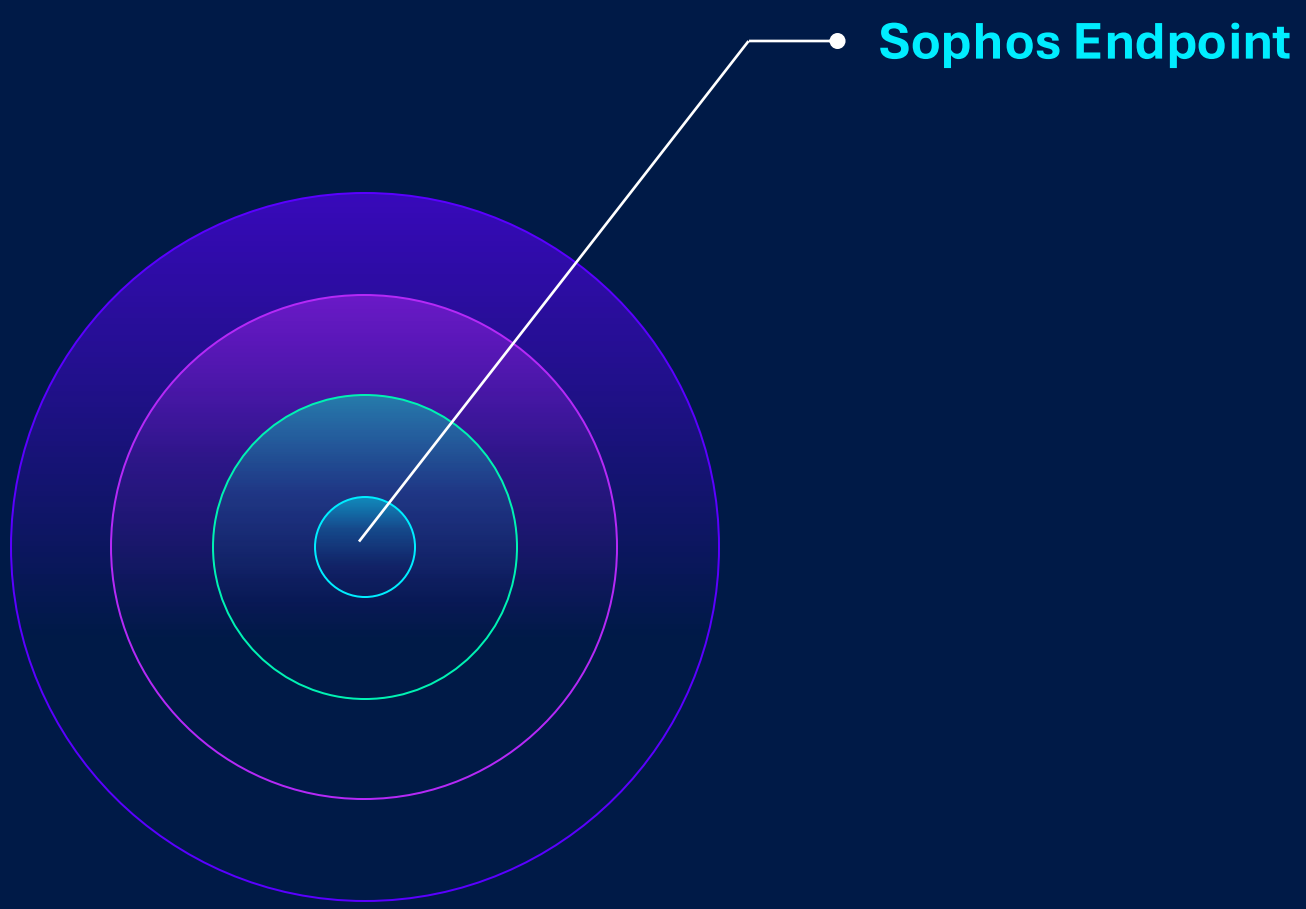
THE THREAT HAS BECOME AI-NATIVE
YOUR DEFENSE NEEDS TO BE AI-NATIVE TOO

MODERN PROTECTION FOR MODERN THREATS

PROTECTION AND PERFORMANCE

ADAPT WITH ADVERSARIAL BEHAVIOR IN REAL-TIME

Path to growth and profitability



PRE-ATT&CK

Recon | Weaponize

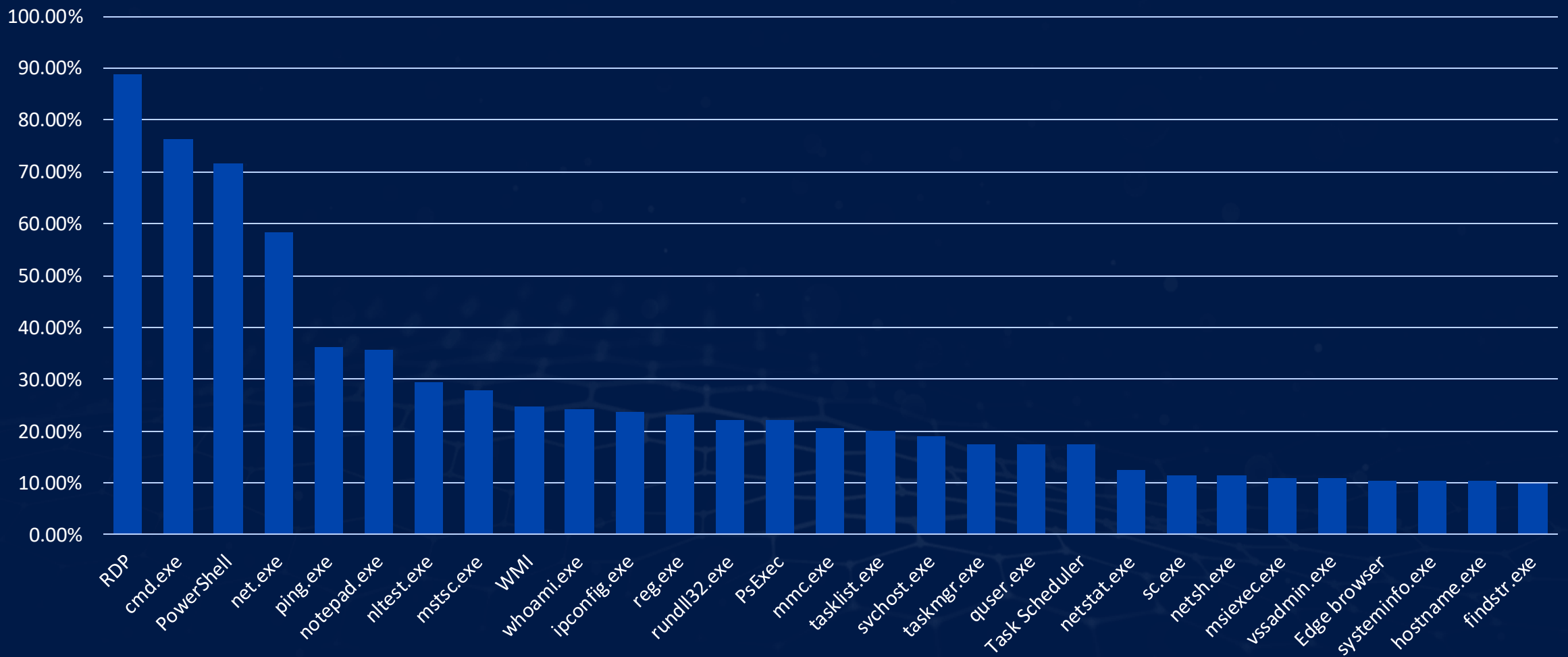
- Priority Definition
- Target Selection
- Information Gathering
- Weakness Identification
- Adversary SecOps
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

Deliver | Exploit | Control | Execute | Maintain

- Initial Access
- Execution
- Persisitance
- Privlege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command & Control
- Impact

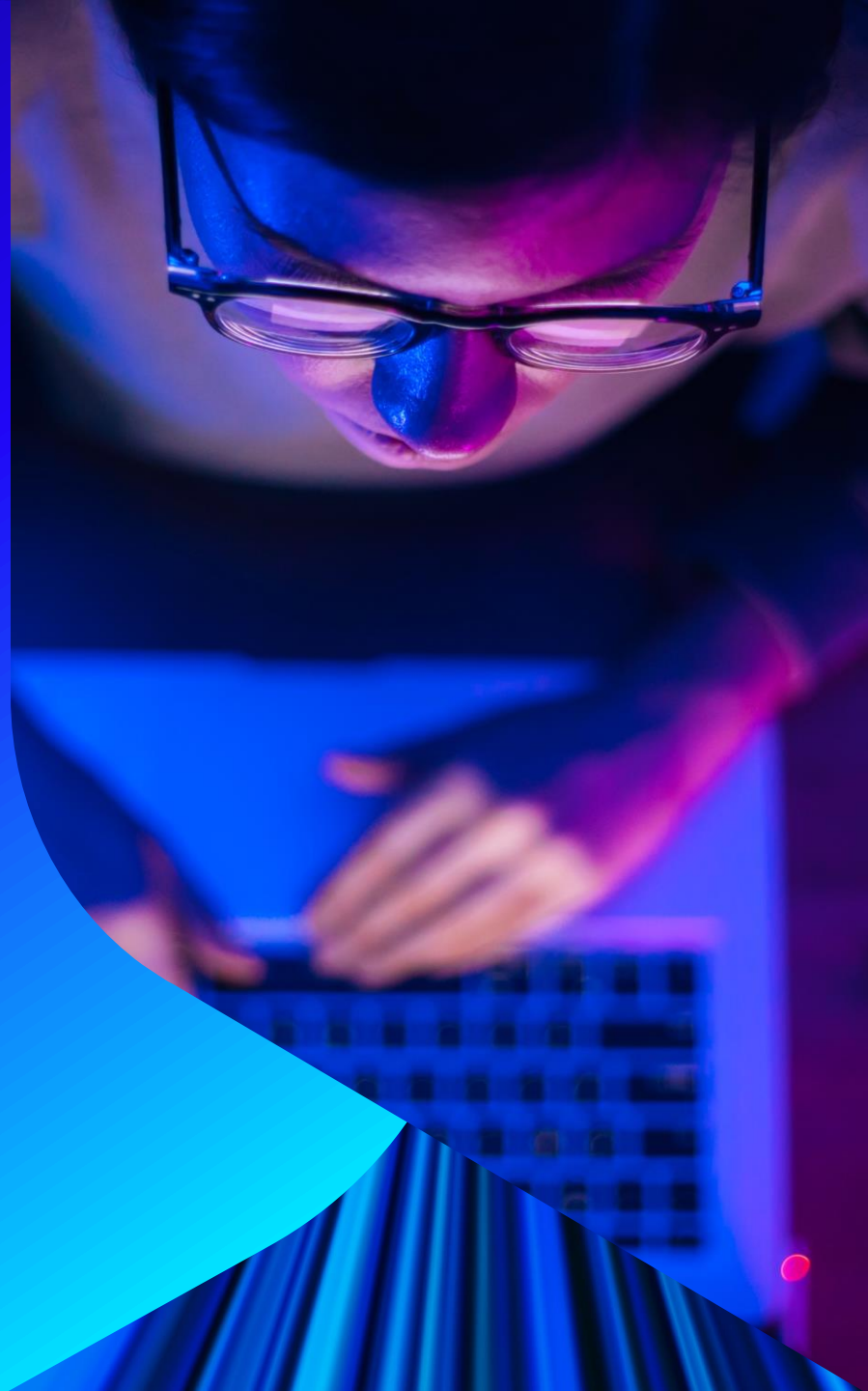
LOLBin prevalence (2025)

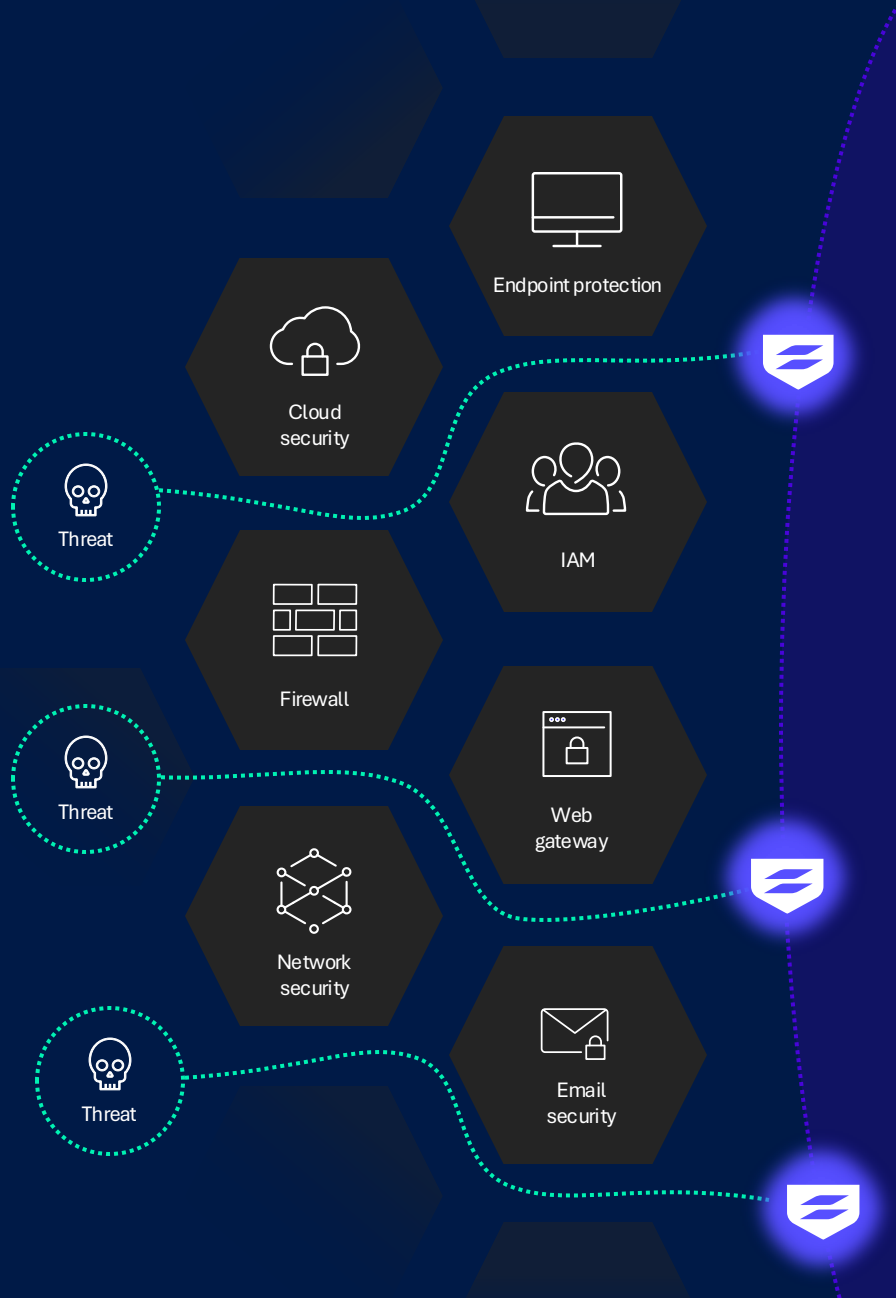


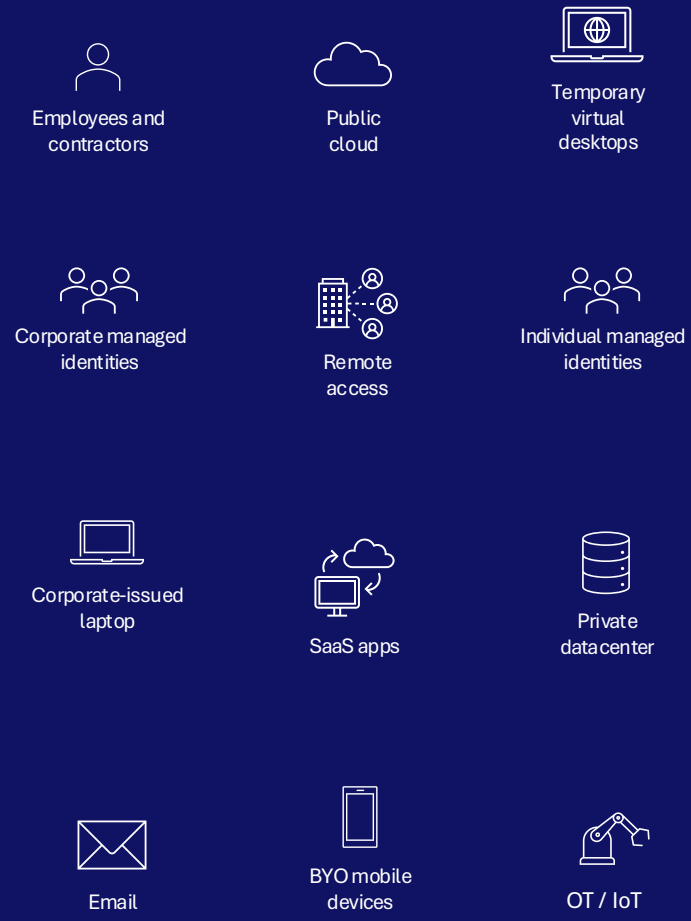
SOPHOS

Sophos XDR

eXtended Detection and Response







XDR protects the modern attack surface

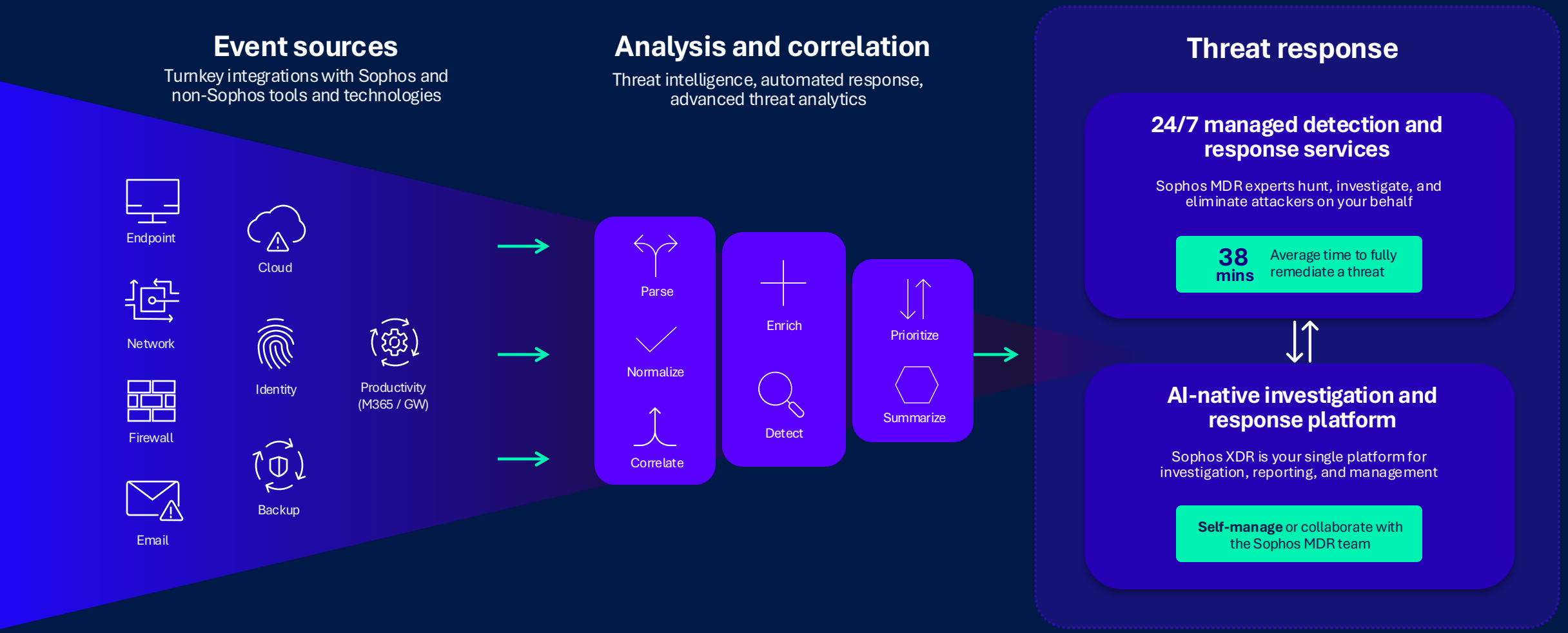
Sophos XDR covers the gaps in point-security controls that adversaries attempt to exploit.

Our AI-native open platform unifies information from multiple security products to automate and accelerate threat detection, investigation, and response in ways that isolated point solutions cannot.

SOPHOS

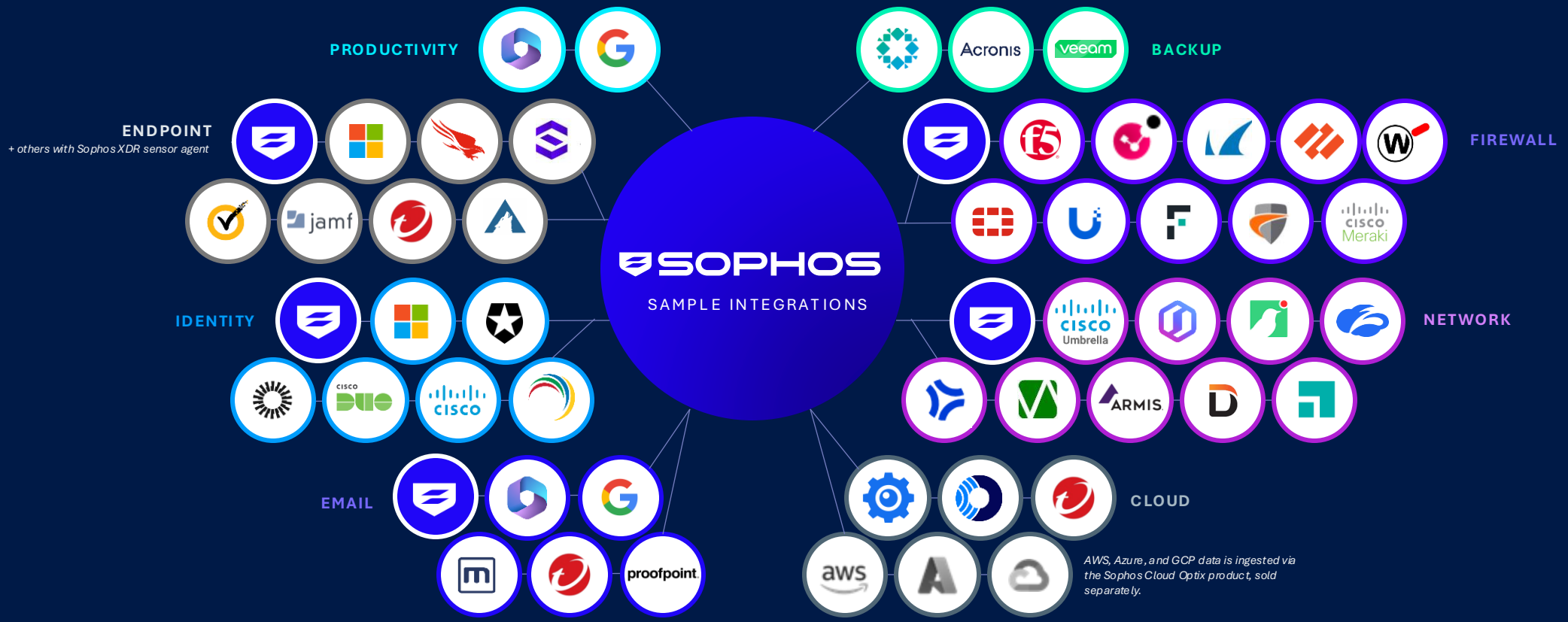
PARTNER 2026 SOPHOS

AI-powered prevention, detection, and response platform



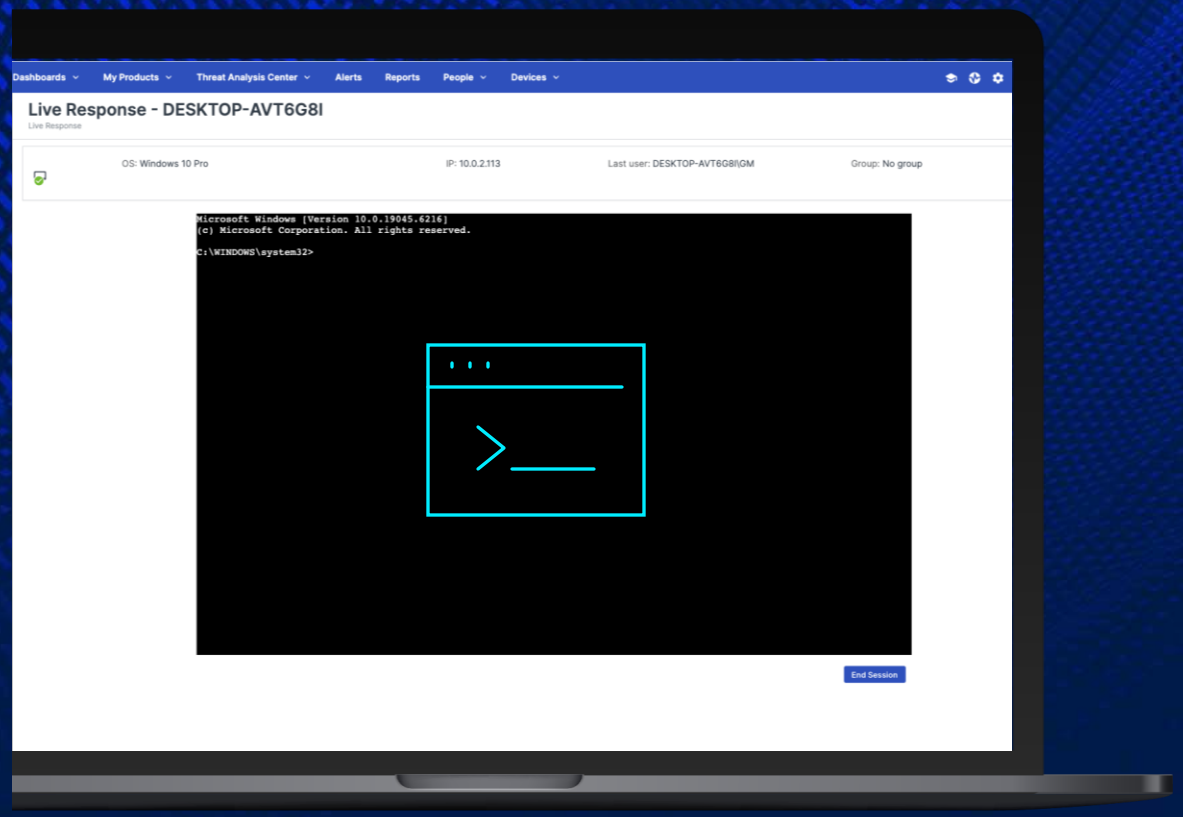
Visibility across all attack surfaces

Our analysts can leverage your existing technology investments to detect and respond to threats.



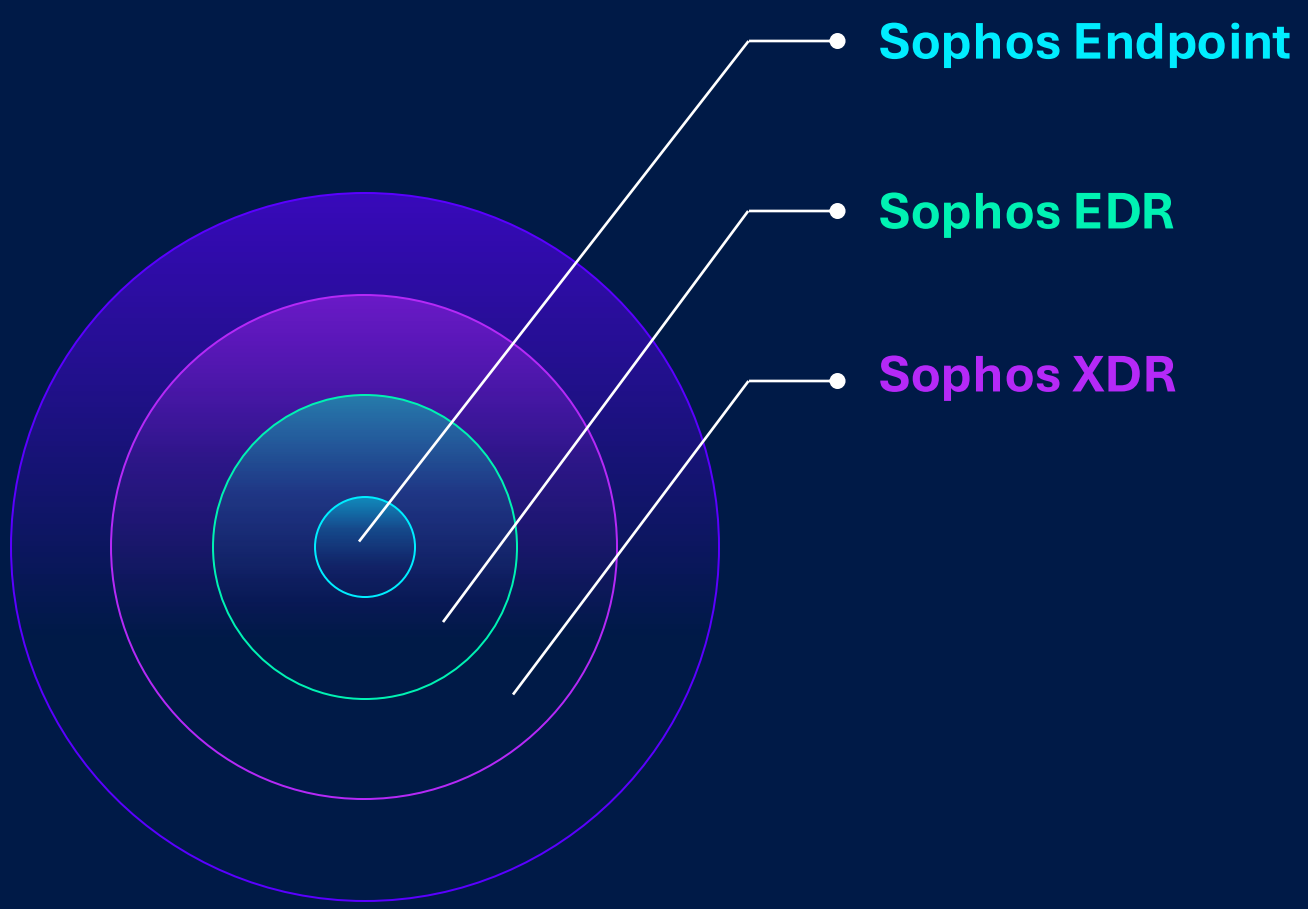
A representative sample of integrations included with Sophos MDR.

Live Response



- **A direct, secure, and audited** connection to your devices to investigate and remediate possible issues
- Remotely access devices to
  - Install and uninstall software
  - Run scripts and programs
  - Edit configuration files
  - Shutdown / reboot
  - Run third-party forensic tools
  - And more

Path to growth and profitability



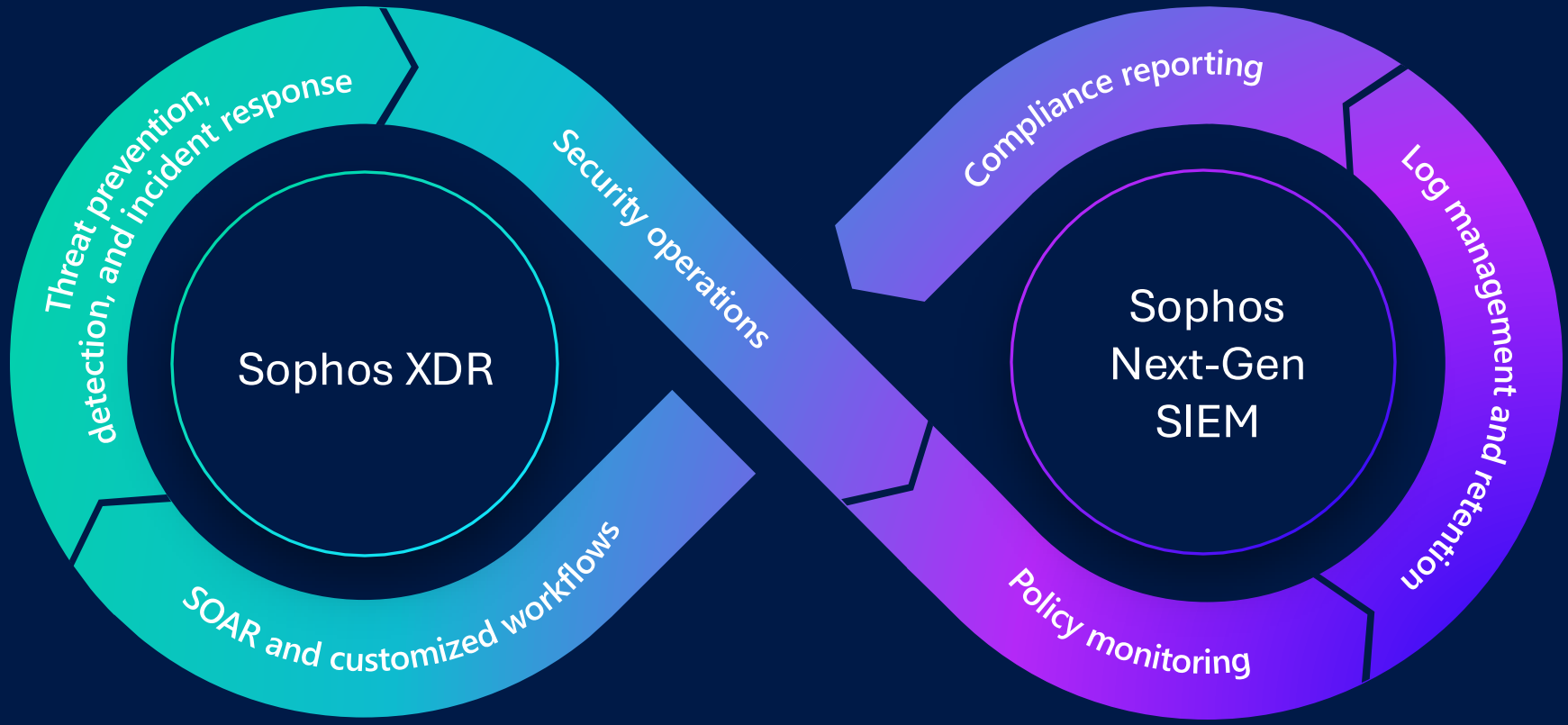
SOPHOS

PRE-GA

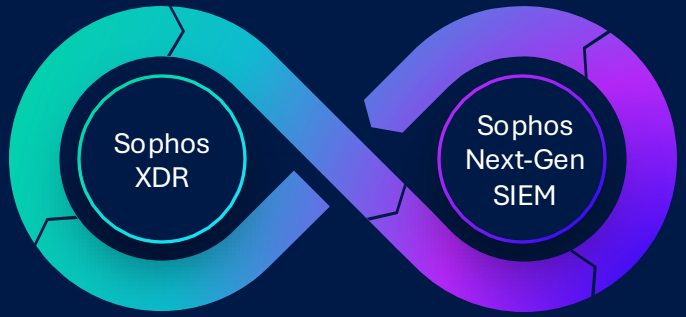
SOPHOS NEXT-GEN SIEM

Extend your Sophos XDR with Next-Gen SIEM.

Sophos XDR with Next-Gen SIEM



Sophos Next-Gen SIEM



SECURITY OPERATIONS

DETECT | INVESTIGATE | RESPOND

Open, vendor-agnostic system
Integrate your IT and security tools for full visibility and powerful response actions.

Superior protection built-in
Block more threats upfront to free-up analysts to focus on what matters most.

Powerful threat detection
Identify multi-stage, multi-vector attacks with comprehensive detectors and customizable detection rules.

AI-native SOC
Accelerate analyst workflows and decision-making with AI architecture.

Automation (SOAR)
Respond to threats and automate common tasks like ticketing.

Integrated threat intelligence
Stay ahead of emerging threats with actionable intelligence at your fingertips.

COMPLIANCE

RETAIN | REPORT | PROVE

Flexible data integrations
Ingest data that meets your organization's unique needs.

Extended, long-term telemetry
Retain multi-domain telemetry for up to 10 years.

Predictable data retention at scale
Retention through simple endpoint-based pricing.

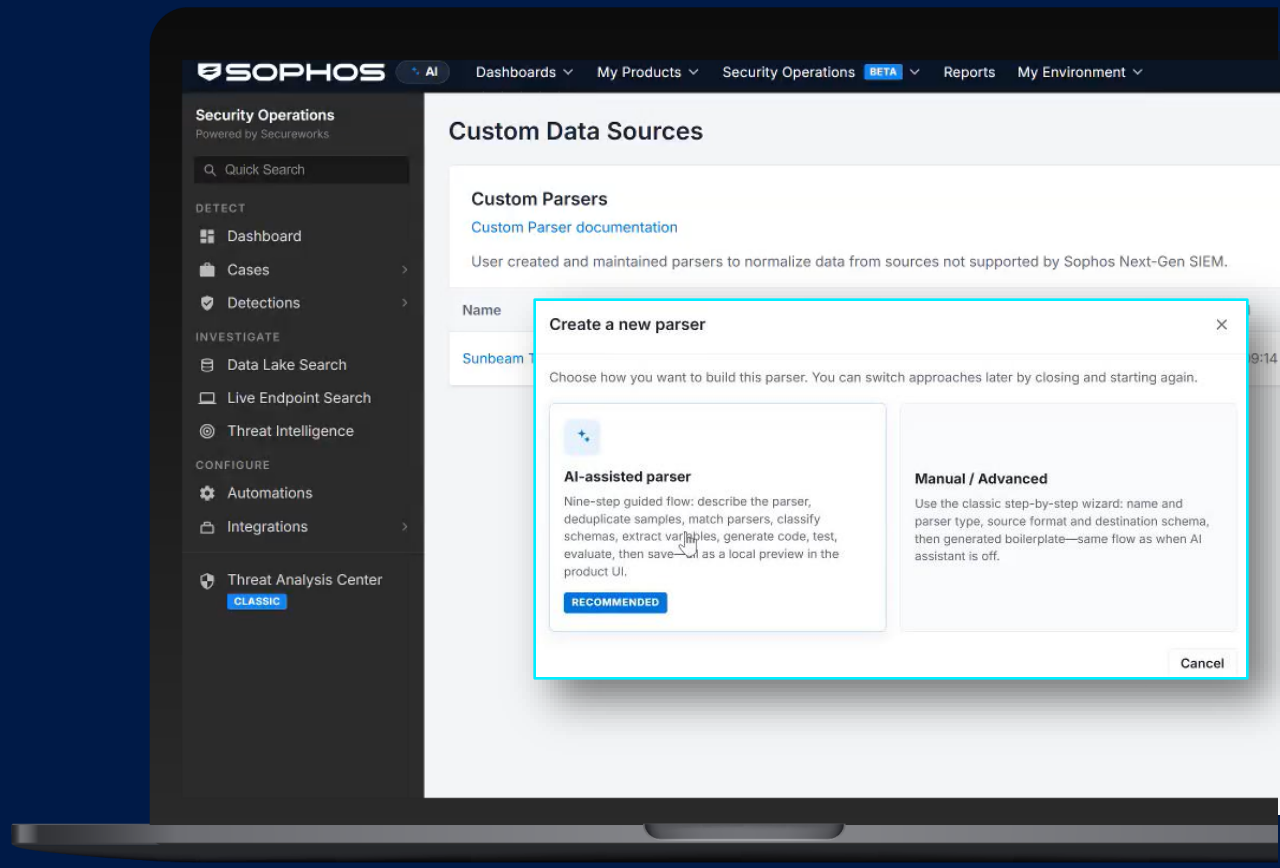
Reliable security and compliance data
Ingest both threat-related and compliance-focused data.

UNIFIED CONTEXT LAKE

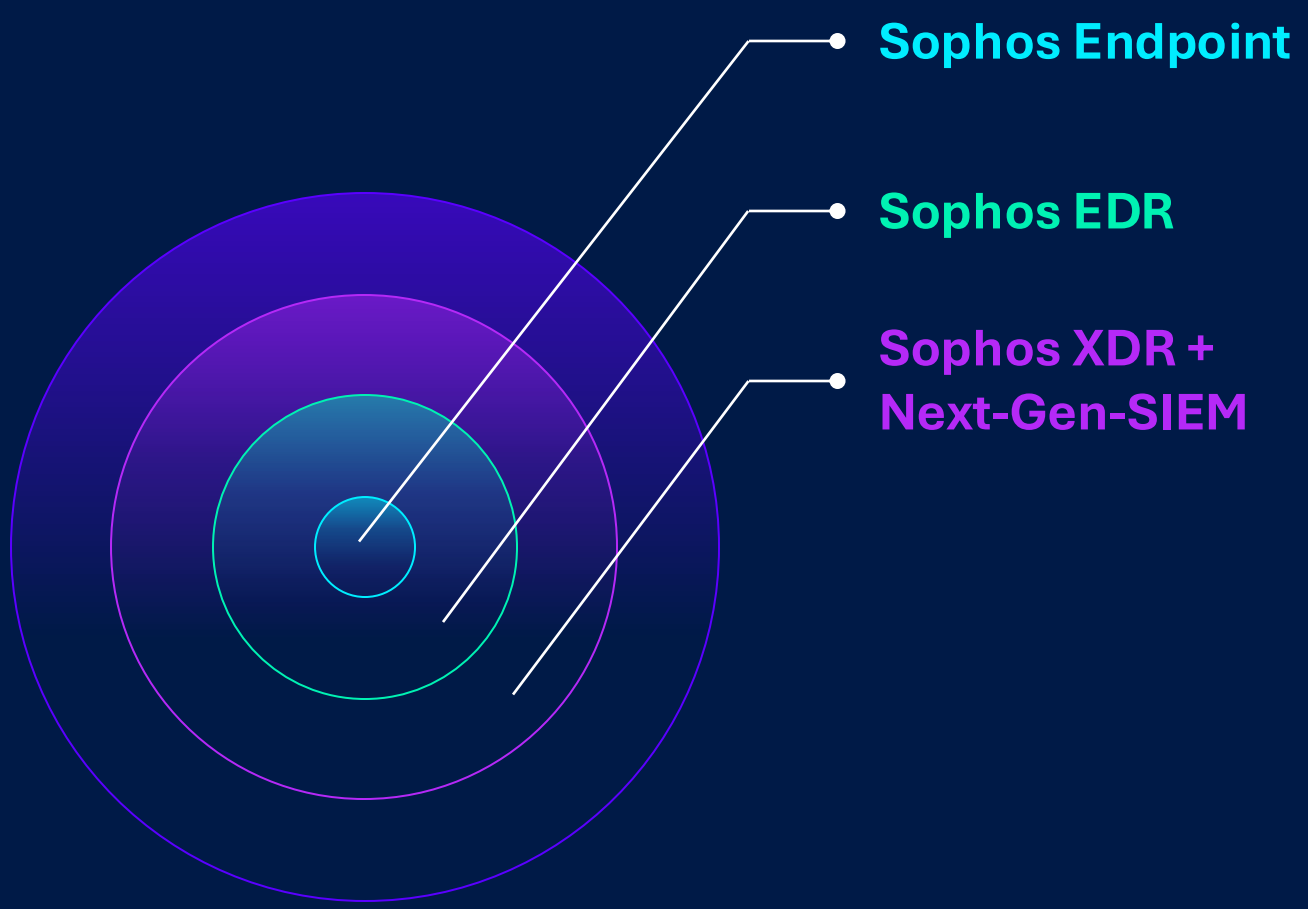
Custom integrations + AI-assisted data parsers

Ingest data unique to your environment with custom integrations, including legacy systems, regional tools, and internal applications.

- Enables a single search model and prevents data sprawl across disparate systems.
- Parsers turn raw data into structured fields aligned to Sophos schemas.
- AI-assisted parsers generate logic based on examples, enabling faster customizations.

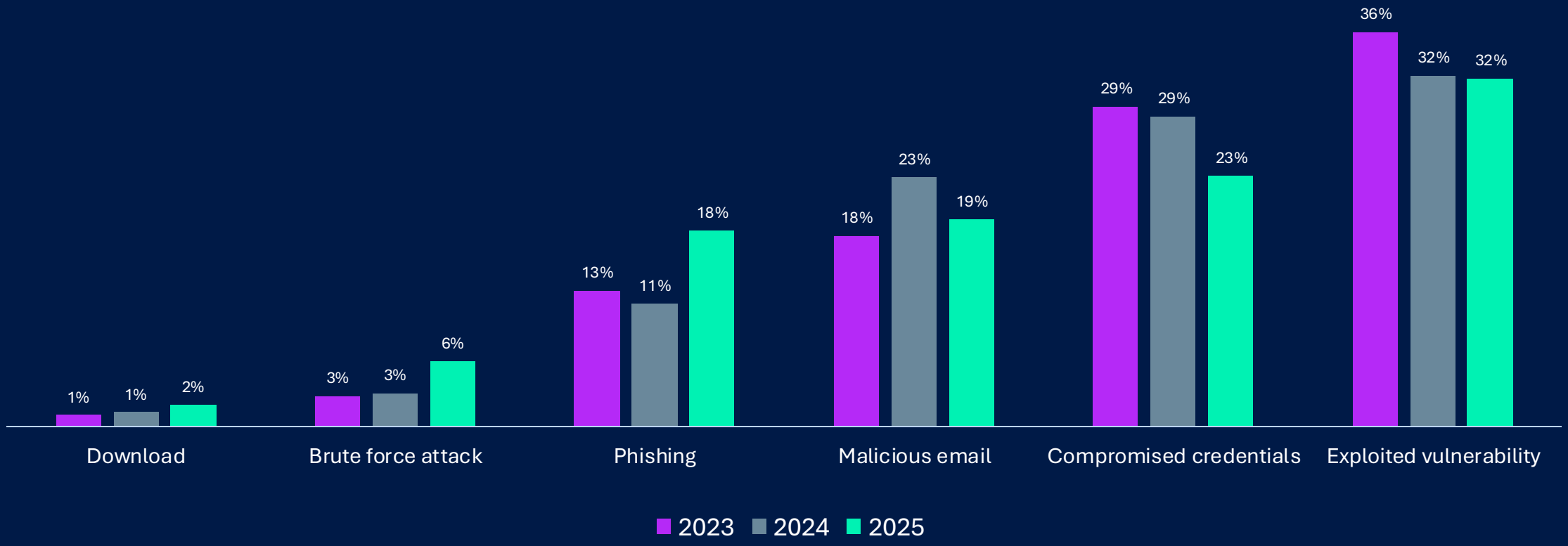


Path to growth and profitability



Technical Root Cause of Attacks

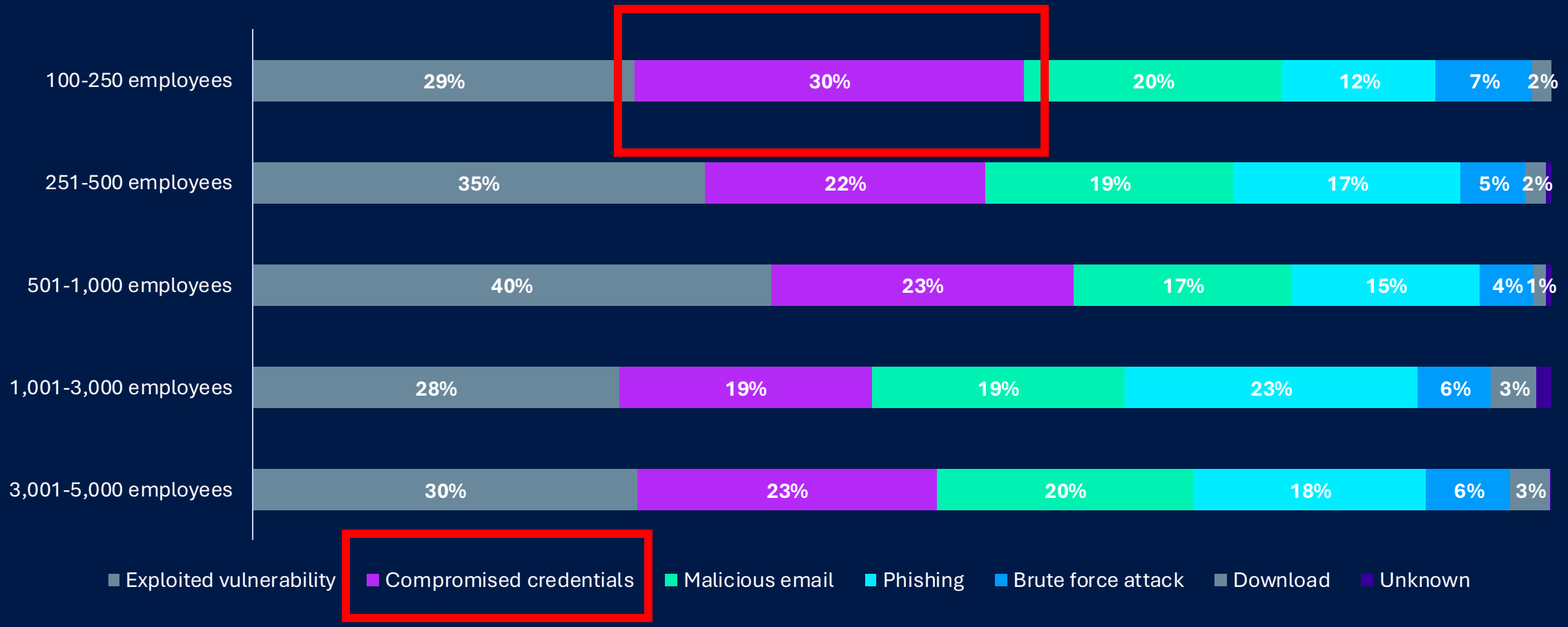
For the third year running, exploited vulnerabilities are the top-reported root cause of ransomware attacks



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=3,400 (2025), 2,974 (2024), 1974 (2023).

Technical Root Cause of Attacks | Company Size

Perceived root cause varies based on organization size, although exploited vulnerabilities are the most common cause for all segments except the 100-250 employees, where compromised credentials tops the list.



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=3,400 (2025)

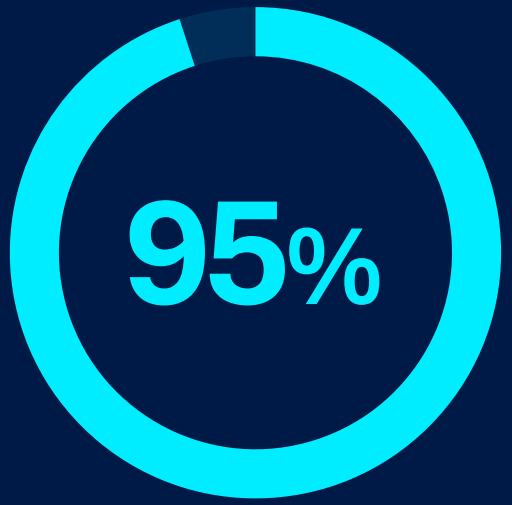
SOPHOS

Sophos ITDR

Identity Threat Detection and Response

SOPHOS

PARTNER EXPERIENCE



IAM misconfigurations

95% of organizations have a critical Microsoft Entra ID identity misconfiguration.

Source: incident response engagements conducted by Sophos

Identity-based attacks

90% of organizations experienced an identity breach in the past year.

Source: IDSA Trends in Securing Digital Identities, 2024

Leaked and stolen credentials

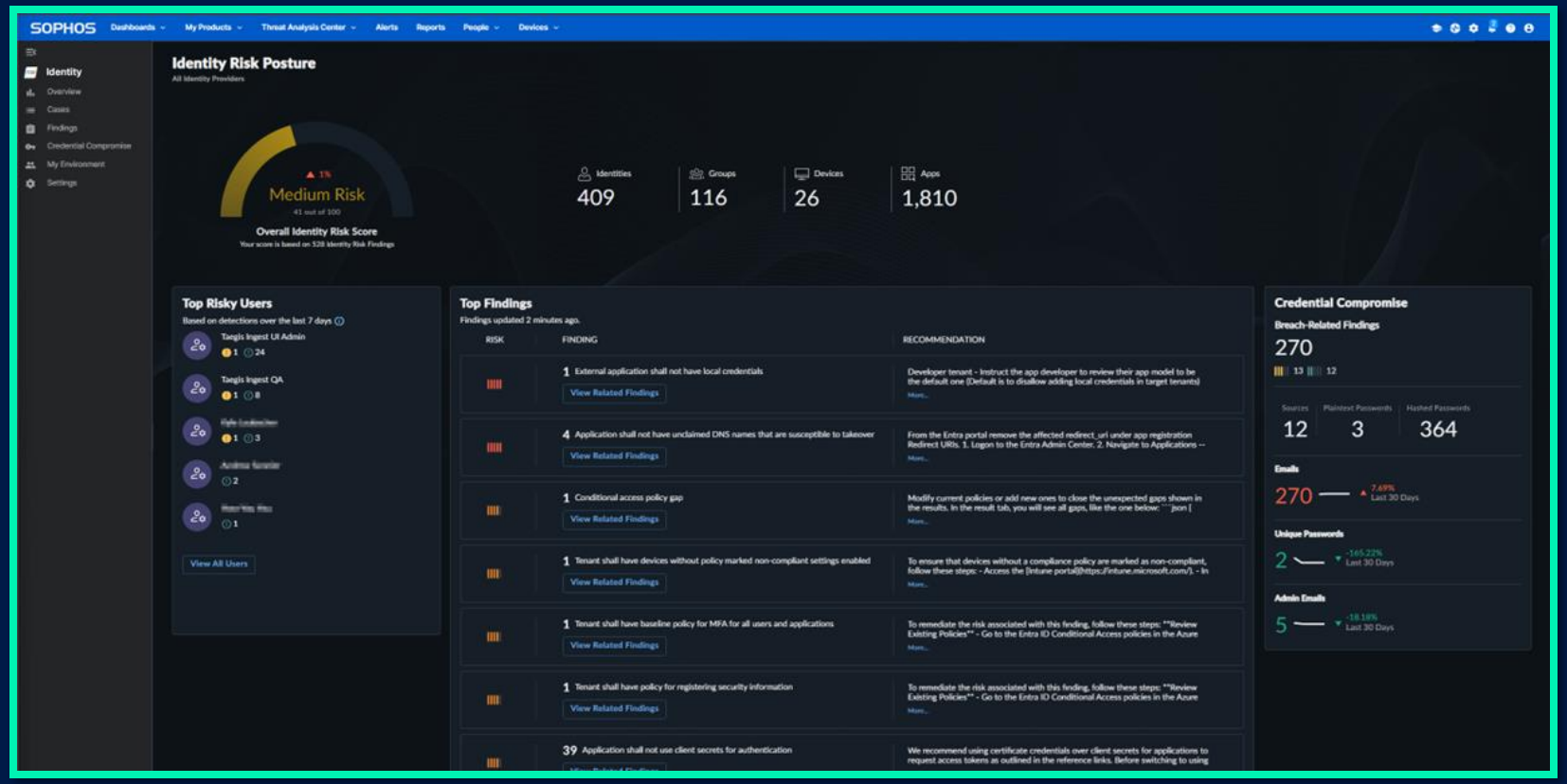
The number of stolen credentials for sale on the dark web has more than doubled in the past year.

Source: Sophos X-Ops Counter Threat Unit (CTU) data, June 2024 – June 2025

Reduces the identity attack surface

Continuously scans Microsoft Entra ID for identity misconfigurations and risks

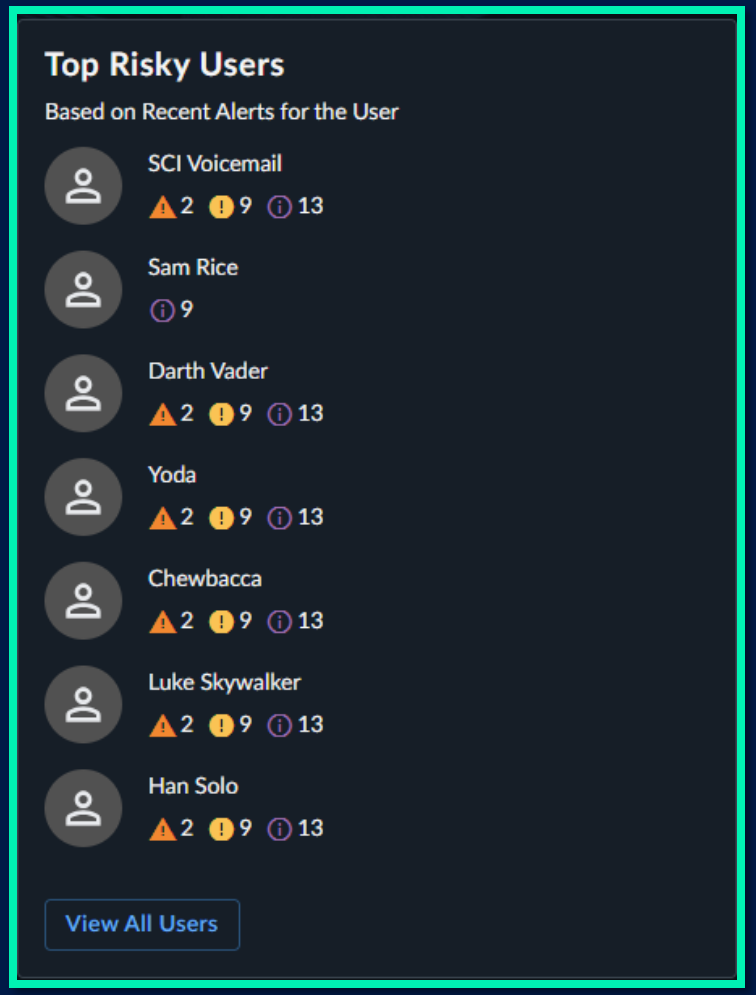
- Produces a prioritized list of “Findings” that pose a risk to your organization with recommended actions
- Provides an identity posture score to help you understand risk and benchmark over time
- Automatically performs 80+ identity posture checks



Identifies risky user behaviors

Highlights abnormal activity associated with the use of stolen credentials

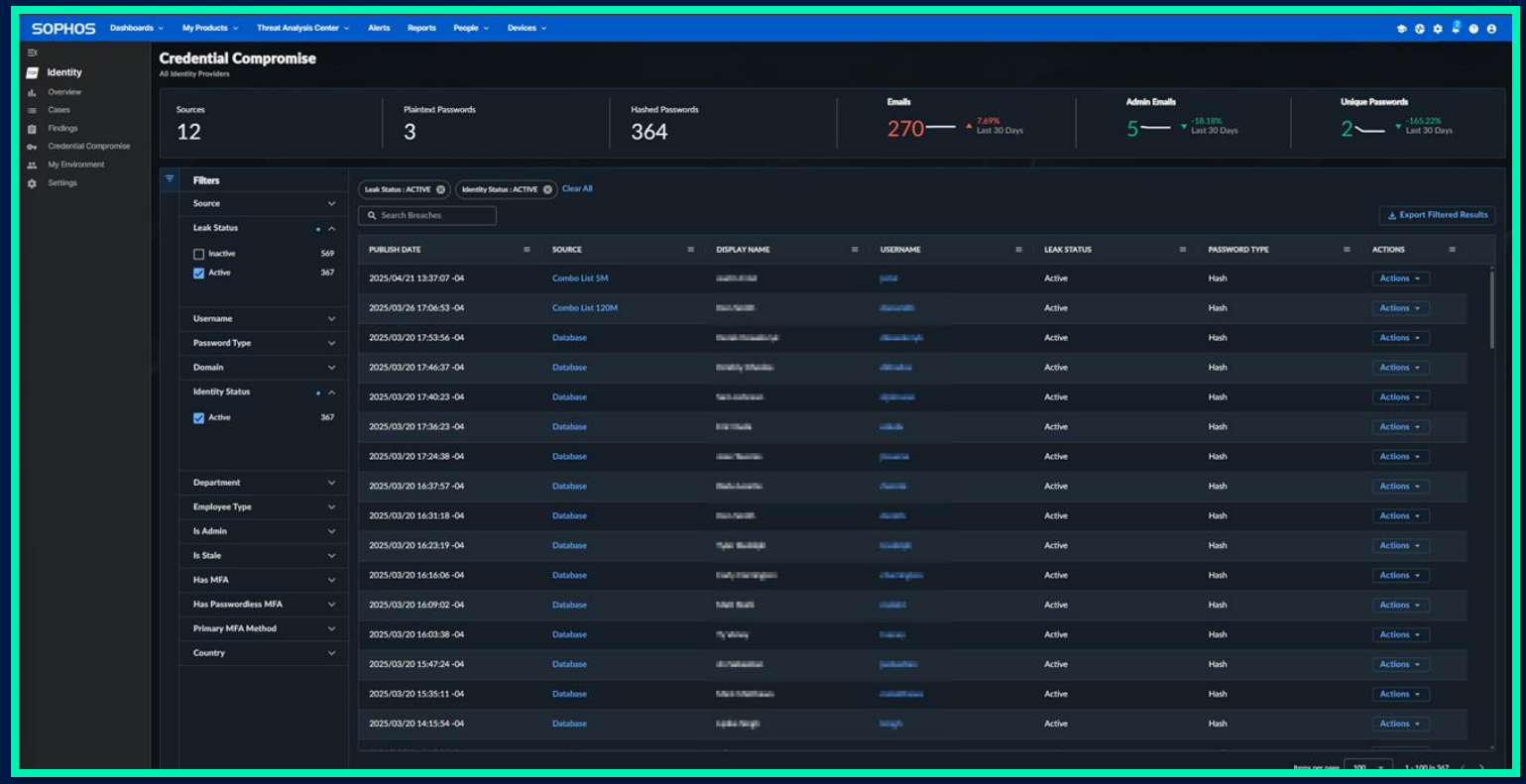
- Provides a list of users that have been recently involved in Sophos security alerts
- Enables quick analysis from within the identity details page
- Highlights abnormal activity such as:
  - Unseen IP address for tenant
  - Unseen ASN for tenant
  - Unseen IP address for user
  - Unseen ASN address for user
  - Unseen user agent



Minimizes stolen credential risk

Monitors and alerts when credentials have been exposed

- Finds credentials leaked on the dark web and within breach databases
  - Reduces the risk of credential stuffing attacks and credential misuse
- Provides insights and trends around:
  - The number of breaches
  - Unique passwords breached
  - Types of breaches observed
  - Admin accounts
- Explore historical leak data using the Credential Compromise explorer
- Correlates with last password change time and MFA configuration for improved accuracy



Reducing Identity Risk with Sophos ITDR

A powerful new add-on for Sophos MDR and Sophos XDR

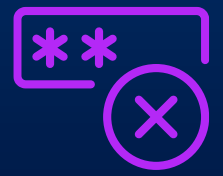
Protects against identity threats

Detect and responds to sophisticated identity-based threats

Reduces the identity attack surface

Continuously scans Microsoft Entra ID for identity security gaps

Minimizes stolen credential risk



Monitors and alerts when credentials have been exposed

Identifies risky user behaviors

Monitors for abnormal activity associated with stolen credentials

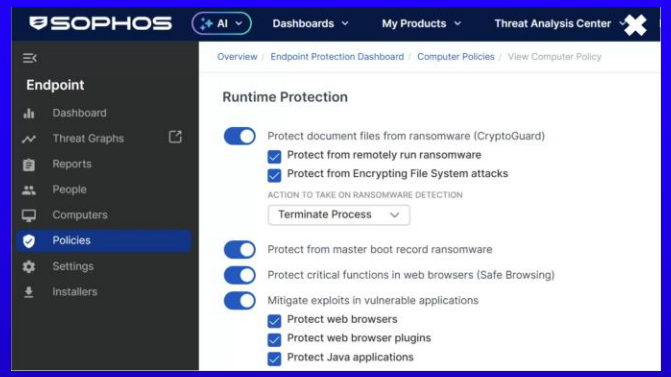
MDR/XDR

Identity Threat Detection and Response (ITDR) Add-on

Path to growth and profitability

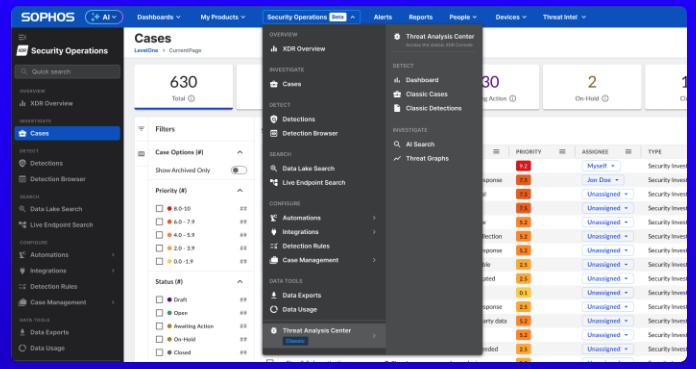
Sophos Platform and Services

Endpoint



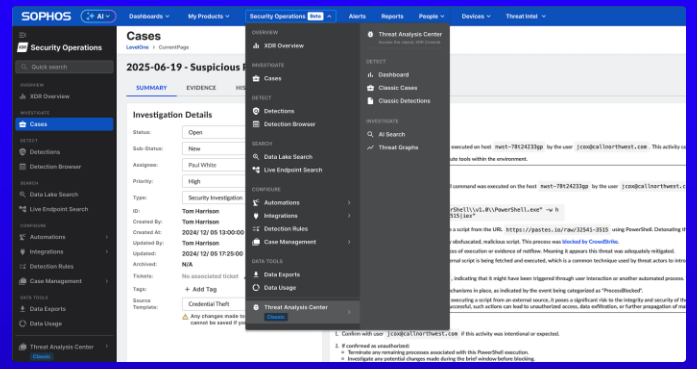
Sophos Endpoint delivers unparalleled defense against advanced cyberattacks with best-in-class endpoint security to over 300,000 organizations worldwide .

EDR/XDR + NGSIEM + ITDR



XDR is a cybersecurity technology and architecture that integrates and correlates telemetry and threat data from multiple security layers — including endpoints, networks, email, identities, and productivity tools — into a unified platform. XDR enhances visibility, accelerates threat detection, and enables faster incident investigation and response across previously siloed systems

MDR

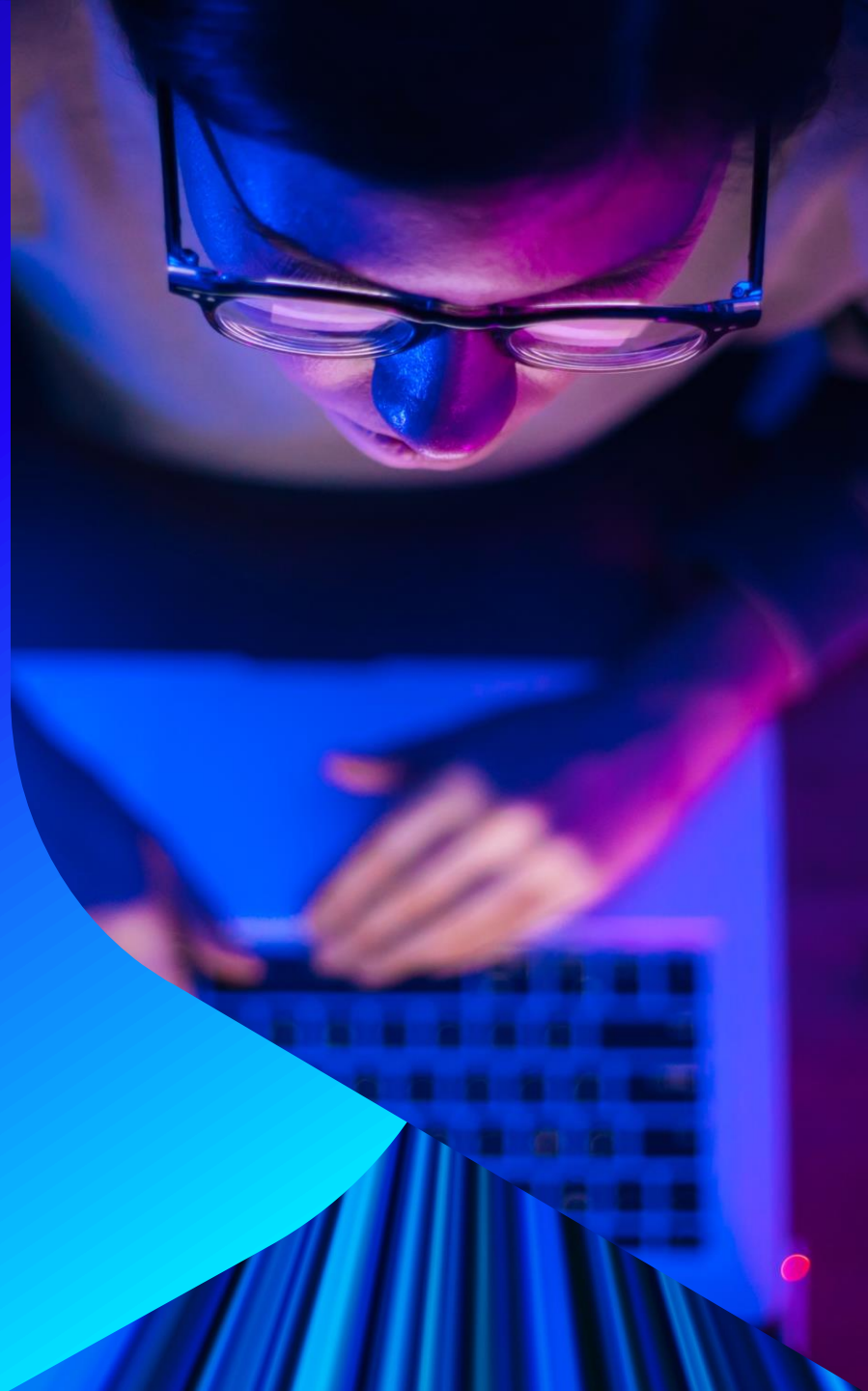


Sophos MDR is the world's most trusted 24/7 managed detection and response service, delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent, across your entire IT ecosystem.

SOPHOS

Sophos MDR

Managed Detection and Response



24/7 global analyst coverage from nine regional hubs

Sophos MDR | Industry-leading advanced cyber defense

Monitor for advanced threats 24/7

Our highly skilled experts hunt for, detect, triage, investigate, and respond to threats on your behalf, delivered by 8 global Security Operations Centers (SOCs).

Detect threats across your environment

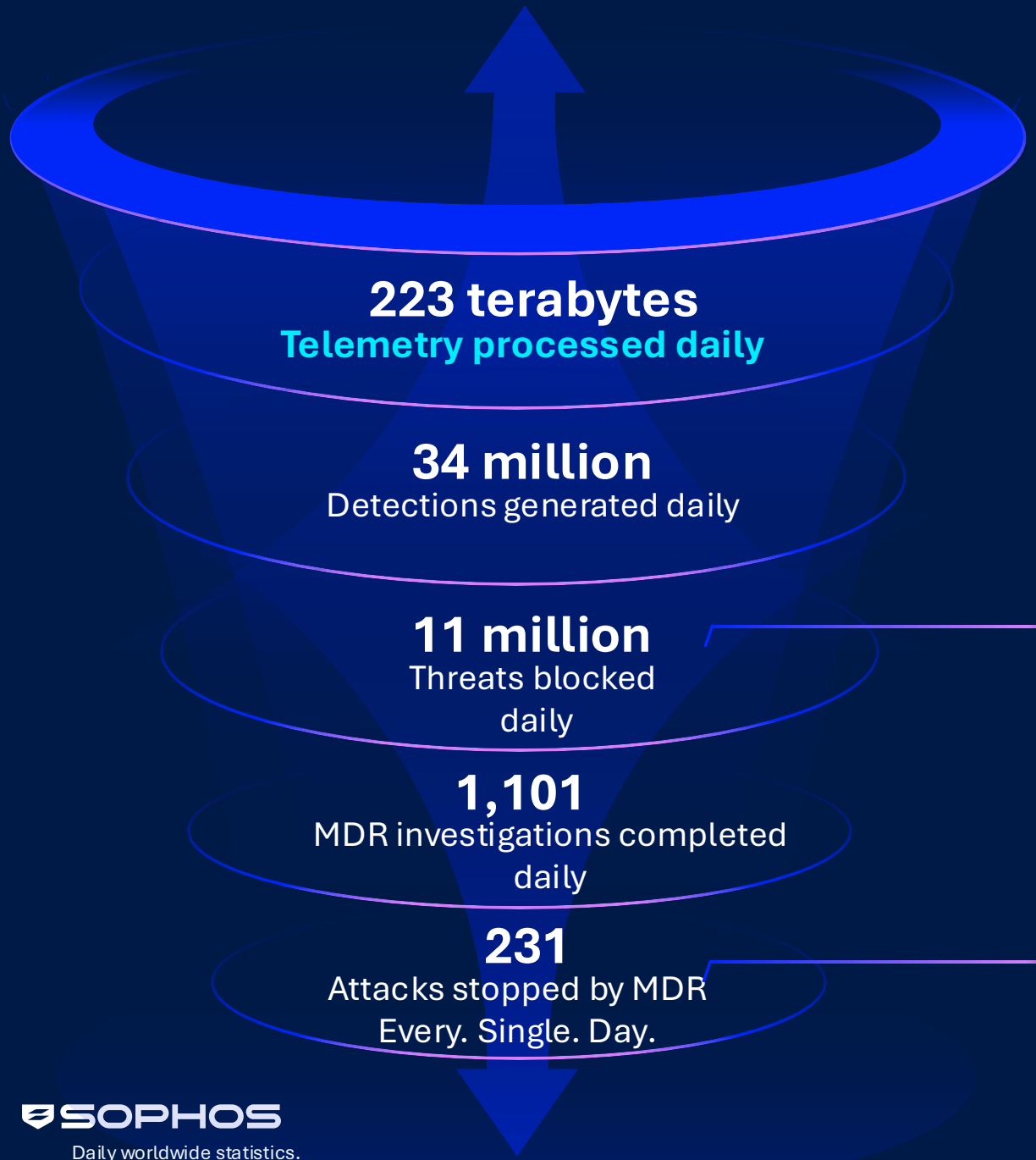
We leverage telemetry from your IT and cybersecurity solutions to identify suspicious activity at the earliest possible opportunity – and increase return on your security investments.

Respond to attacks before they can progress

We have an industry-leading average threat response time of 38 minutes — 96% faster than the industry benchmark for in-house SOC teams.

Neutralize adversaries and identify root cause

Unmetered full Incident Response (IR) coverage with no hourly limits. Active threats are neutralized and root cause identified to improve security posture.



Sophos MDR is built on the largest AI-native open platform

Our unique **prevention-first** approach reduces breaches and improves detection and response outcomes.

Learnings from investigations and attacks stopped by Sophos MDR **drive enhancements** to proactive protection.

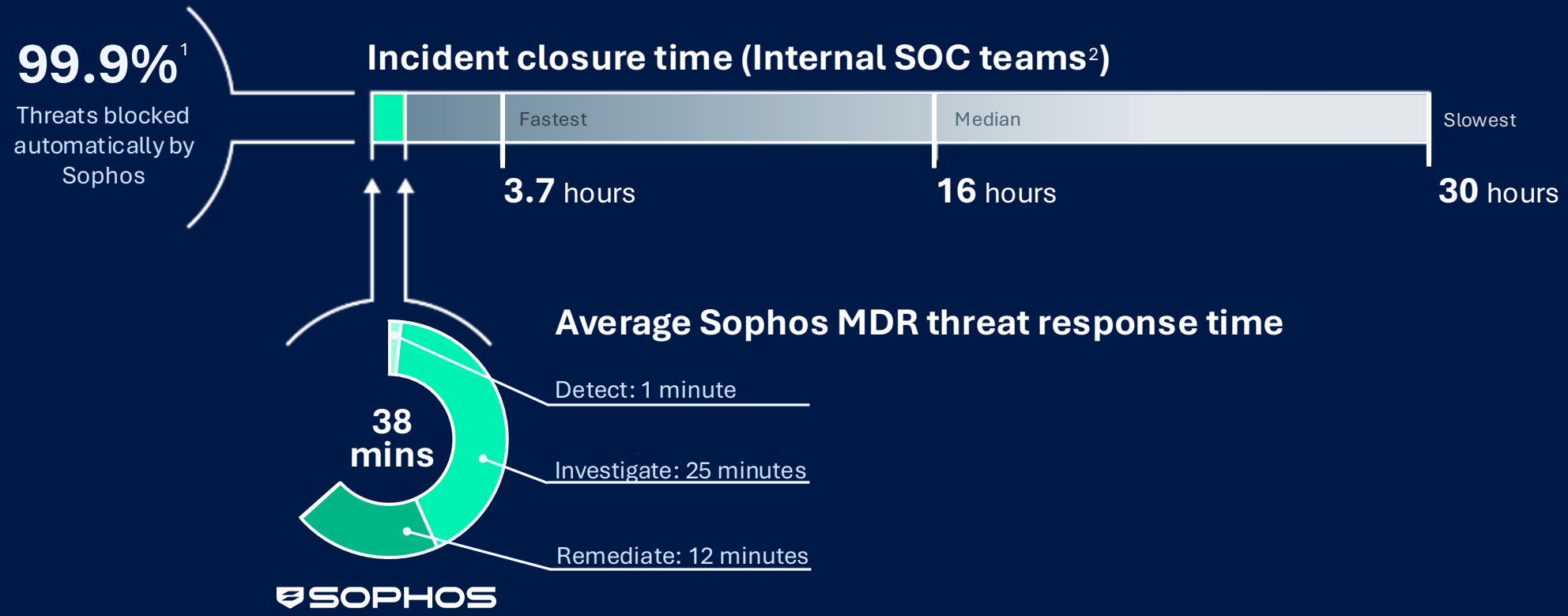
SOPHOS

Daily worldwide statistics.

PARTNER 2026 SOPHOS

Leading detection and response times

Sophos MDR analysts **respond to threats in minutes** — whether you need full-scale incident response or assistance making more accurate decisions.



[1] 99.93% based on average AV-Test scores on Windows over a six-month period (Sep 2024 – Feb 2025). | [2] Gartner Cybersecurity Business Value Benchmark data.

Sophos MDR

40,000 +
Customers Globally

A vast, diverse customer base provides unparalleled intelligence and proactive threat defense.

1,101
Investigations completed daily

Our highly skilled experts monitor, triage, investigate, and respond to threats on your behalf.

231
Advanced attacks stopped every day

Learnings from attacks stopped by Sophos MDR drive enhancements to proactive protection.

Global analyst coverage

Tested. Recognized. Trusted.

Gartner Peer Insights Customers' Choice 2024
Customers' Choice

MITRE ATT&CK®
Top Performer

FROST & SULLIVAN
Leader

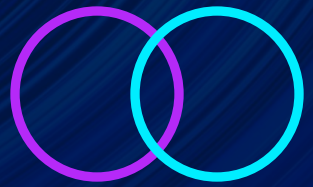
Gartner Peer Insights™
Highest-Rated

G2 Grid® Reports
Highest-Rated

SOPHOS

PARTNER EXPERIENCE 2026

Sophos is your partner for growth



Your SOC
+
Our SOC

Your SOC
=
Our SOC

Your SOC
+
Our system

RESOURCES AVAILABLE ON THE PARTNER PORTAL (LOGIN REQUIRED)

SOPHOS

PARTNER 2026 EXPERIENCE

Flexible service tiers

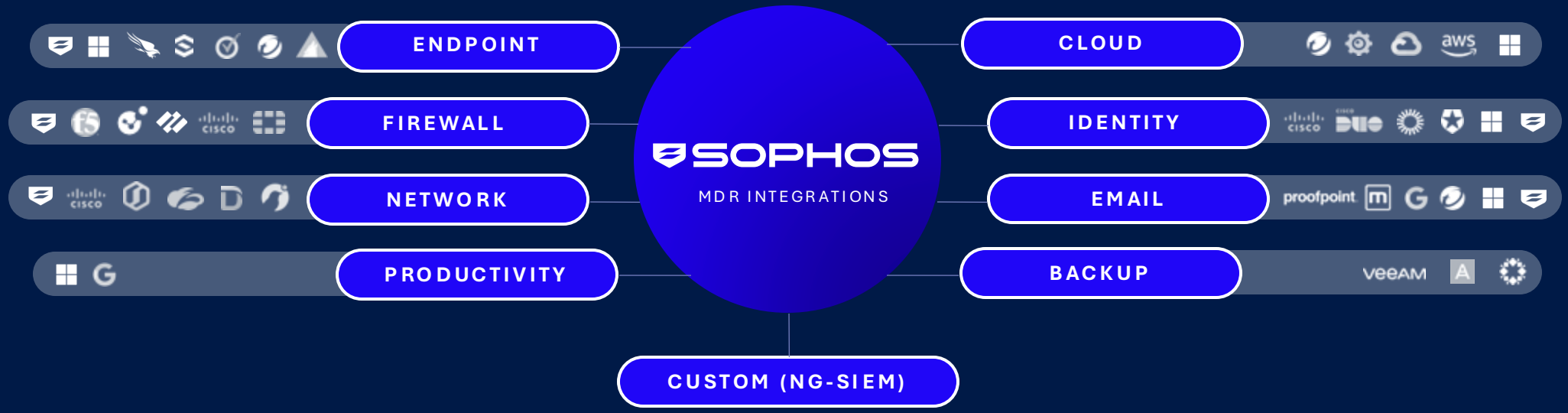
	SOPHOS MDR	SOPHOS MDR PLUS
24/7 expert-led threat monitoring and response	✓	✓
Detection and response across your entire IT environment Includes integrations with endpoint, network, firewall, cloud, identity, email, productivity, backup solutions	✓	✓
Sophos Endpoint and Sophos XDR technology included	Option to use Sophos Endpoint (included) or any third-party endpoint solution	✓
Comprehensive reporting and intelligence briefings	✓	✓
Proactive threat hunting	✓	✓
Threat response: active attacks are stopped and contained Using the full Sophos Endpoint agent or the Sophos Endpoint "XDR sensor" (included)	✓	✓
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 full Sophos Endpoint agent (included)	-	✓
Dedicated incident response lead	-	✓
Sophos breach protection warranty	-	✓

MDR MARKET GROWTH (BILLIONS)

MDR is not a line item.
It’s the center of your practice.

Source: IDC 2025, model

Vendor-agnostic. Partner-centric.



SELL FLEXIBLE SOLUTIONS

Sell Sophos MDR with the solutions you already offer to your customers.

LAYER SERVICES

Offer services around data integrations and automated response workflows.

INCREASE DEAL SIZES

Expand MDR opportunities with ITDR, NDR, Next-Gen SIEM, and more.

Sell with confidence across every segment

Win new business. Retain customers. Expand accounts. Across your entire customer base.

COMMERCIAL
1-99 seats

Security outcomes without security staff.

Highly targeted, limited staff, and unable to monitor 24/7 — creating immediate demand for MDR.

High urgency — fast close. Delivers strong recurring revenue with low overhead.

MID-MARKET
100-1000 seats

24/7 defense across a growing attack surface.

Small teams overwhelmed by alerts and complexity need a trusted provider to own security operations outcomes.

Natural security operations upsell from endpoint and firewall. Clear expansion path as customers grow.

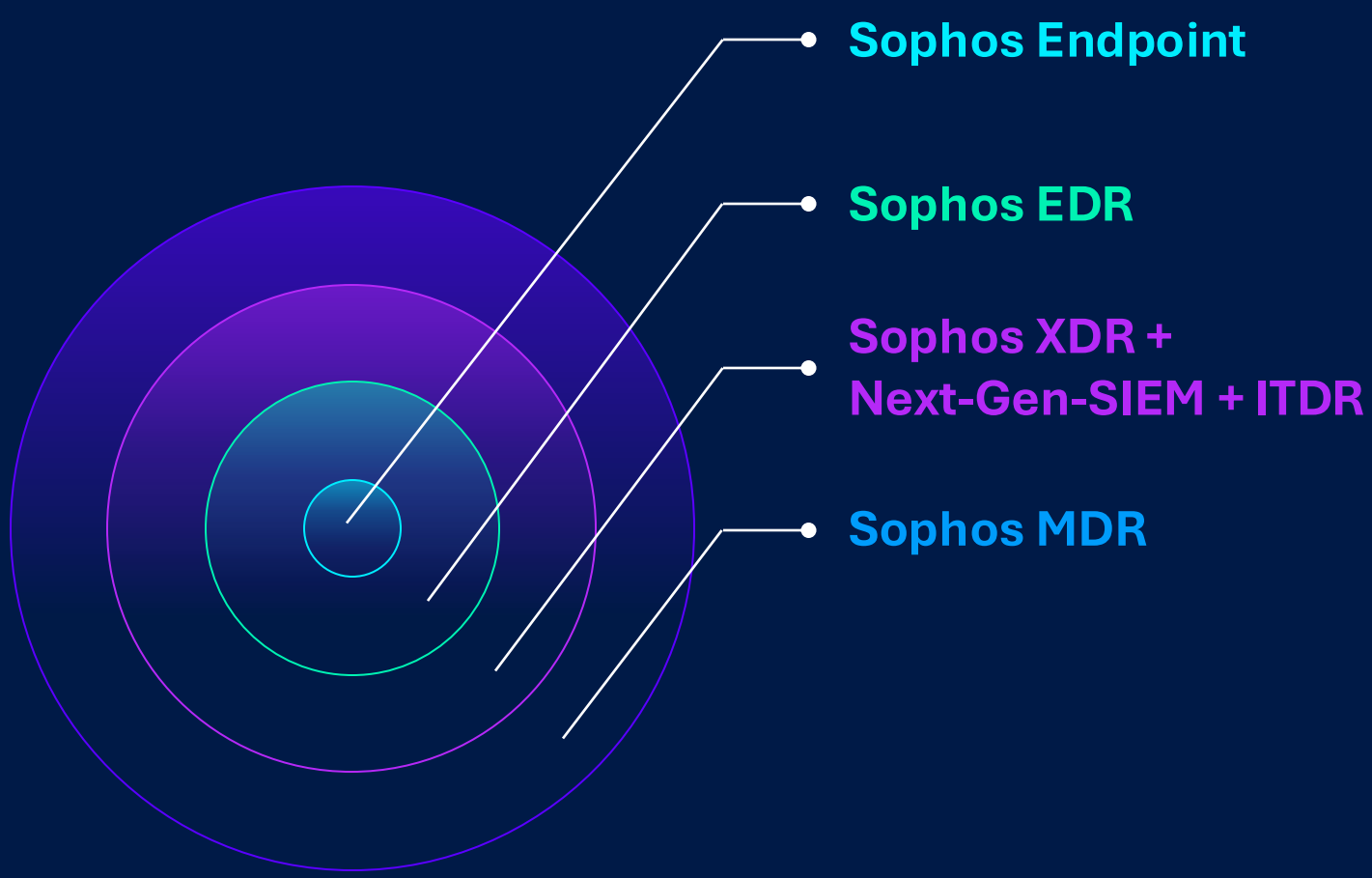
ENTERPRISE
1000+ seats

AI-native MDR for complex, multi-layer environments.

Organizations running multiple solutions struggling with visibility, compliance, and operational overhead.

Larger deals — longer cycles. Target customers with fragmented stacks and compliance requirements.

Path to growth and profitability



SOPHOS

Threat Profile Assessment

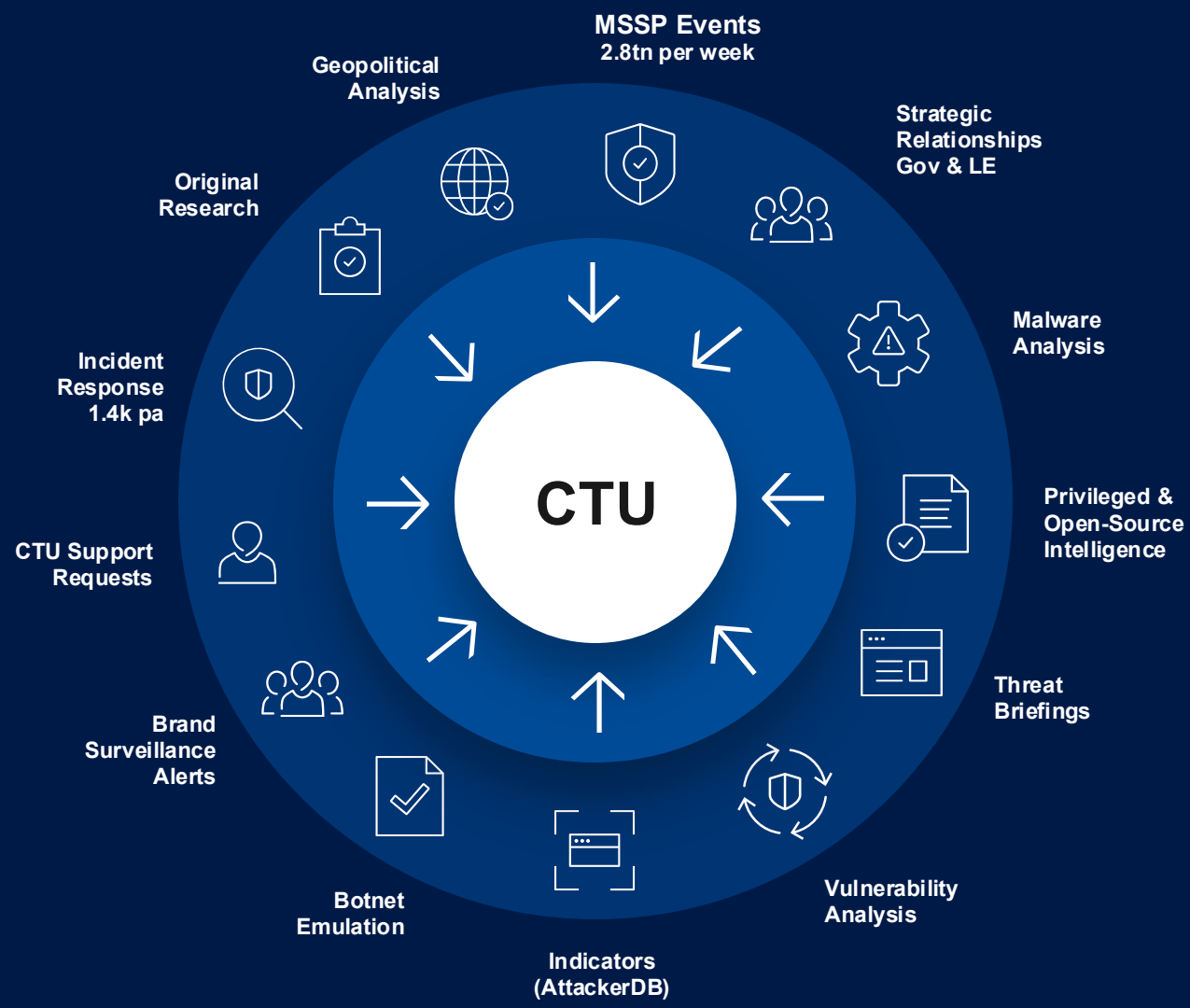
OSINT and Threat Intelligence

OSINT stands for **open-source intelligence**

Includes:

- Information found in media
- Images
- Public forums / job ads
- Public conferences

CTU collects threat data such as: Endpoint telemetry, Incident Response and Targeted Threat Hunting engagements, Third Party / OSINT news reports, Botnet Tracking, Dark Web as well as other CTU research initiatives.



Suspicious Domains

- Potentially malicious intention

6 ***total potential typo-registrations***

TYPO DOMAIN	COPIED DOMAIN	REGISTRAR
d0minio.com	dominio.com	Register.com - Network Solutions, LLC
dominlo.com	**dominio.com**	Network Solutions, LLC
…	**dominio.com**	OVH, SAS
	dominio.com	None
	dominio.com	None
	dominio.com	None

Typosquatted Domains

Enabling an attack based on (fake) trust:

- Phishing
- Business Email Compromise

Recommendation:

- Gateway filtering/block

Domain DMARC Score

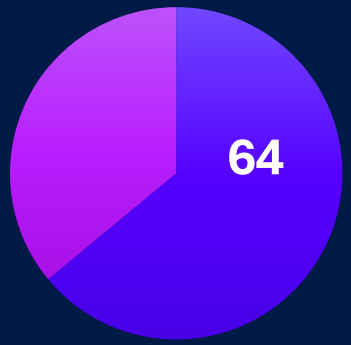
View full report here

Domain Score for **dominio.net**

MODERATE RISK

You've got some measures in place to shield recipients from harmful emails coming from your domain. But there's opportunity to strengthen your domain's security even more. Taking these steps can boost trust in your brand, keep your business and stakeholders safe from cyberattacks, and help ensure emails are delivered effectively.

Overall Score

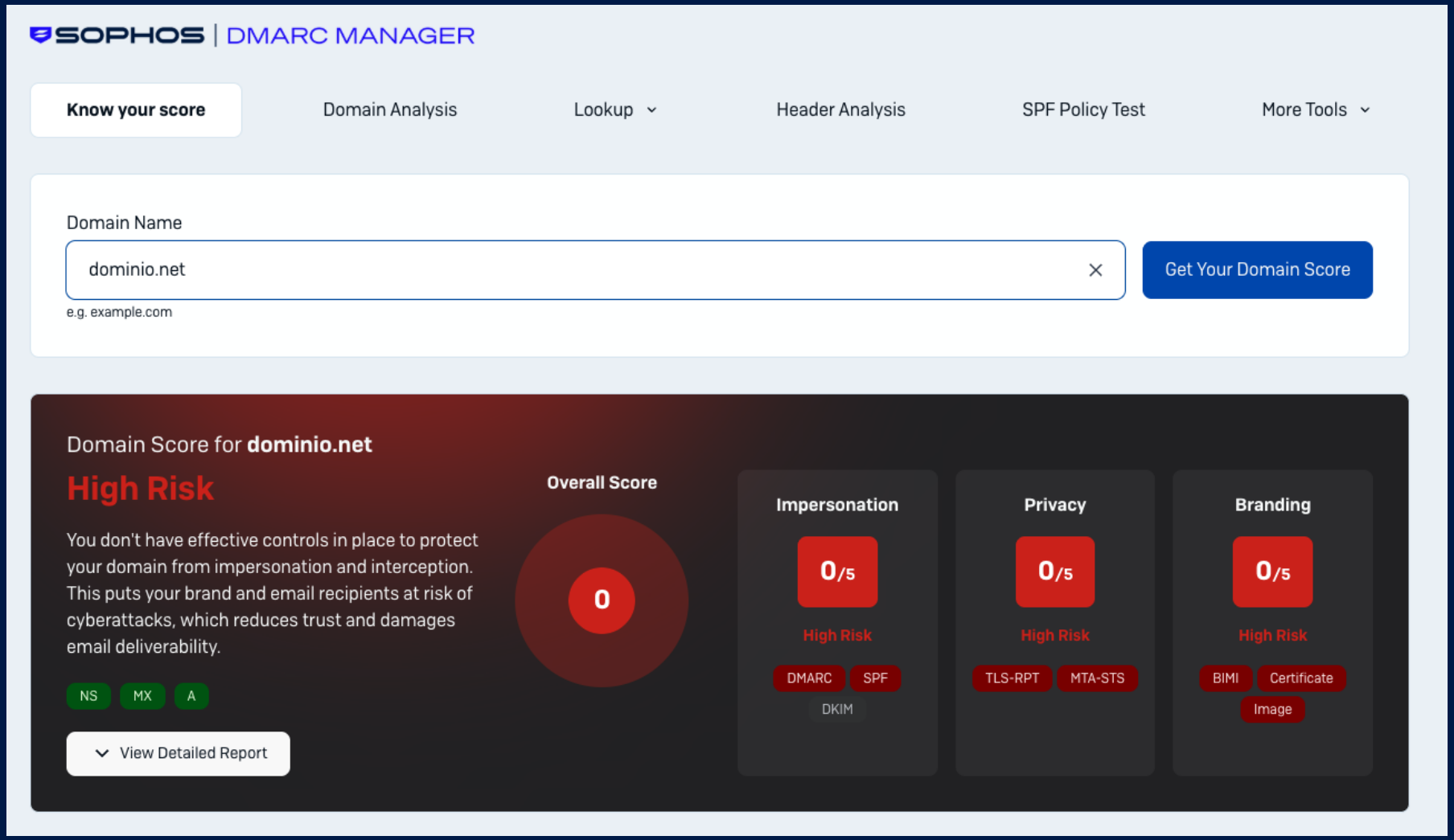


Impersonation	Privacy	Branding
4/5	0/5	0/5
MODERATE RISK	HIGH RISK	HIGH RISK

Top Findings:

- DMARC: Policy - Policy set to 'quarantine'; accept all email as possibly valid. Emails are considered suspicious.
- MTA-STS: DNS Record - No record found
- TLS-RPT or SMTP TLS Reporting: DNS Record - No record found
- BIMI: DNS Record - No record found

Sophos DMARC MANAGER



https://tools.sophosdmarc.com/

Email and Credential Leaks

- Potentially malicious

40 email addresses gathered

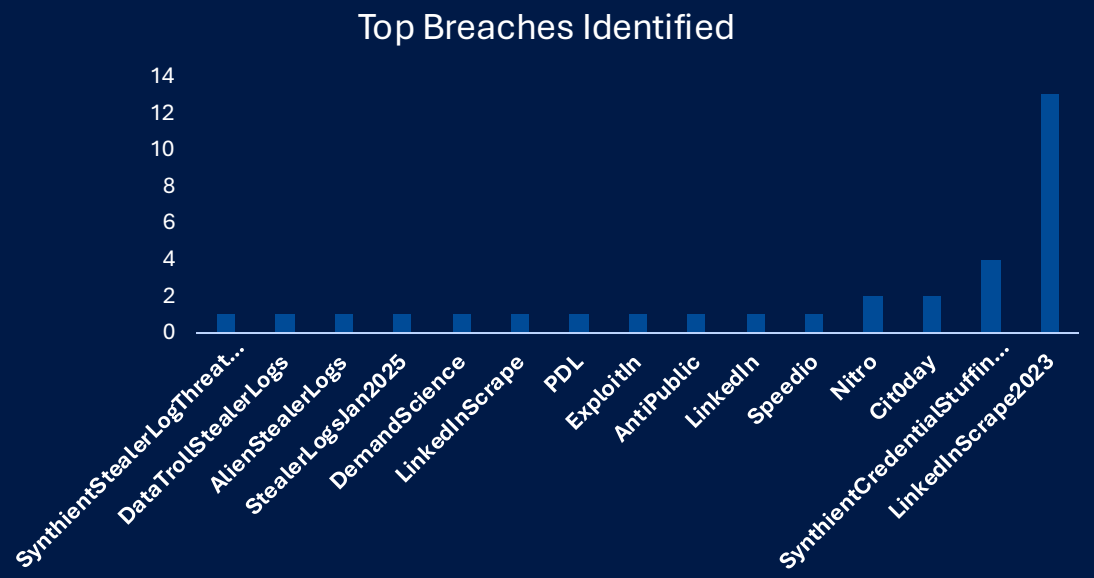
Information found for 2 executives

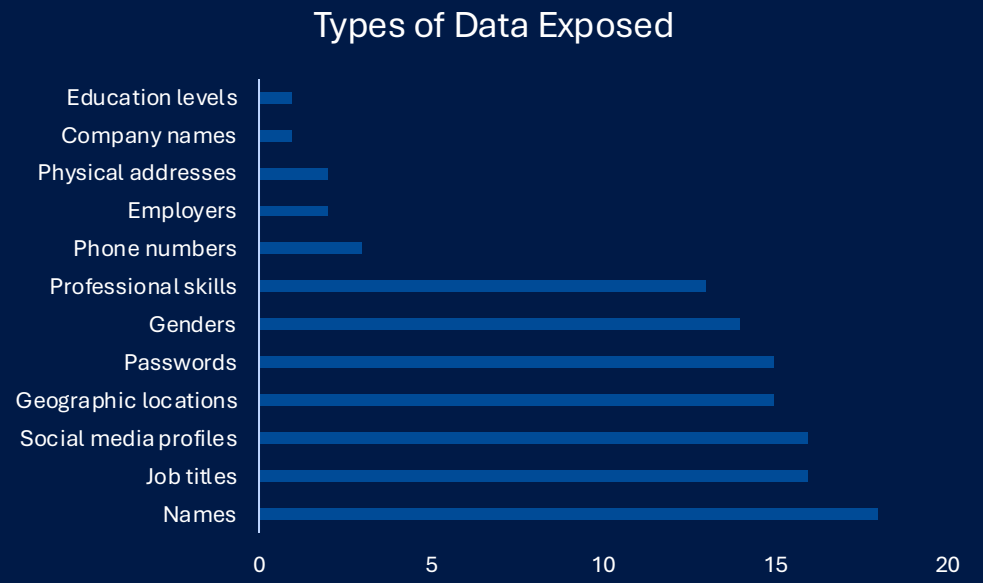
32 matches in different 3rd party breaches

7 breaches identified for 2 executives

15 exposed passwords

5 passwords identified for 2 of the executives





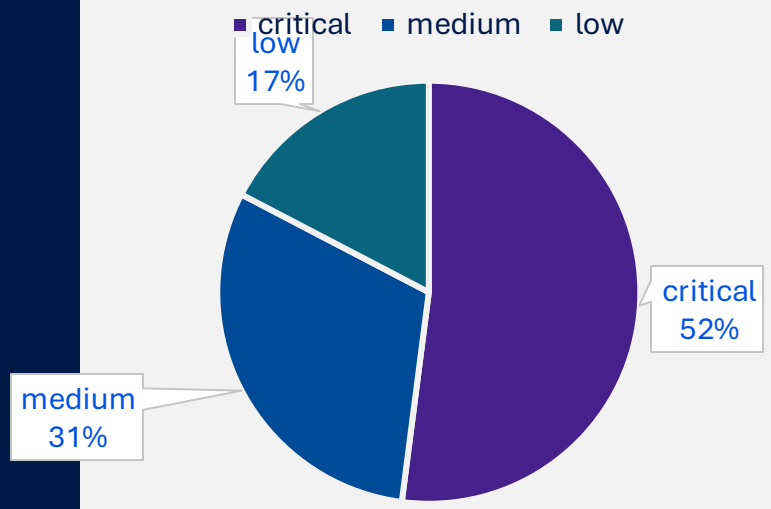
VDR External Scans

- External scan using Taegis VDR

6 LIVE SYSTEMS		
ASSET LOCATION	**VULNERABILITY GROUP**	**SEVERITY**
X.X.Y.Y	Software Outdated Cisco IOS 12.2 (OS EOL)	critical
X.X.Y.Y	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) nan	critical
X.X.Y.Y	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) nan	critical
X.X.Y.Y	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) nan	critical
X.X.Y.Y	Vulnerable HTTP/1.1 Protocol is being used. nan	critical
Top identified risks		

273

associated CVEs



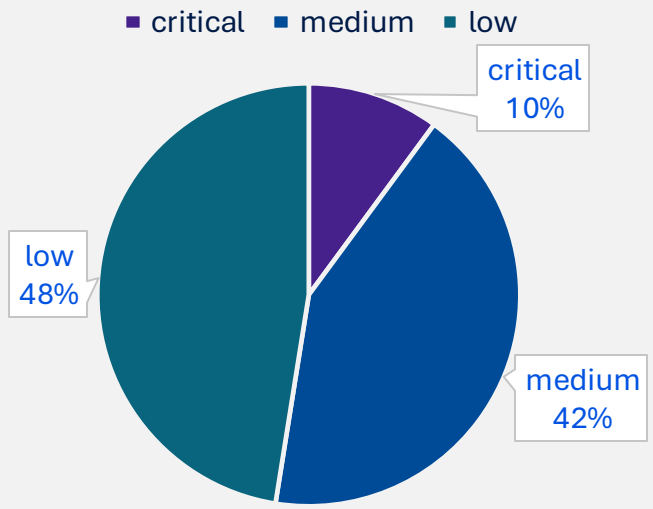
VDR External Scans

- External Web discovery and vulnerability scan using Taegis VDR

1 LIVE WEBSITE DETECTED		
ASSET LOCATION	**VULNERABILITY GROUP**	**SEVERITY**
https://X.X.Y.Y/	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) nan	critical
https://X.X.Y.Y/	SSL/TLS: Vulnerable Cipher Suites for HTTPS nan	critical
https://X.X.Y.Y/	SSL/TLS: Weak Cipher Suites nan	medium
https://X.X.Y.Y/	Web Browser Protections Disabled Content-Security-Policy (CSP)	medium
https://X.X.Y.Y/	Web Browser Protections Disabled x-frame-options	medium
Top 5 identified risks		

19

associated web vulnerabilities



Threat Profile Requeriments

- Valued Cx users >= 200
- One shot

Path to growth and profitability

Sophos Endpoint

Sophos EDR

Sophos XDR +
Next-Gen-SIEM + ITDR

Sophos MDR

*Sophos THREAT PROFILE

SERVICE OVERVIEW

SOPHOS MANAGED RISK

Powered by tenable®

SOPHOS

PARTNER EXPERIENCE 2026

Comprehensive attack surface vulnerability management

Powered by Tenable technology, Sophos Managed Risk delivers both external and internal attack surface management (EASM and IASM) in a single managed service. Discover your entire digital footprint and define your critical assets to focus on what matters most.

External Attack Surface Management (EASM)

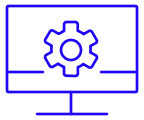
Discovers internet-facing assets and the exposures they may present.

Internal Attack Surface Management (IASM)

Discovers risks posed by internal assets (e.g., computers, servers, network devices, and more) using authenticated and unauthenticated vulnerability scanning.

DEFINED CRITICAL ASSETS

Service onboarding



Day 1: Onboarding

An intuitive wizard in Sophos Central guides you through the simple steps to provide your authorized contacts and schedule automated scans.

Day 30: Baseline review

An initial baseline review meeting enables the Sophos team to understand what's important to your organization and review the results of your first scans.

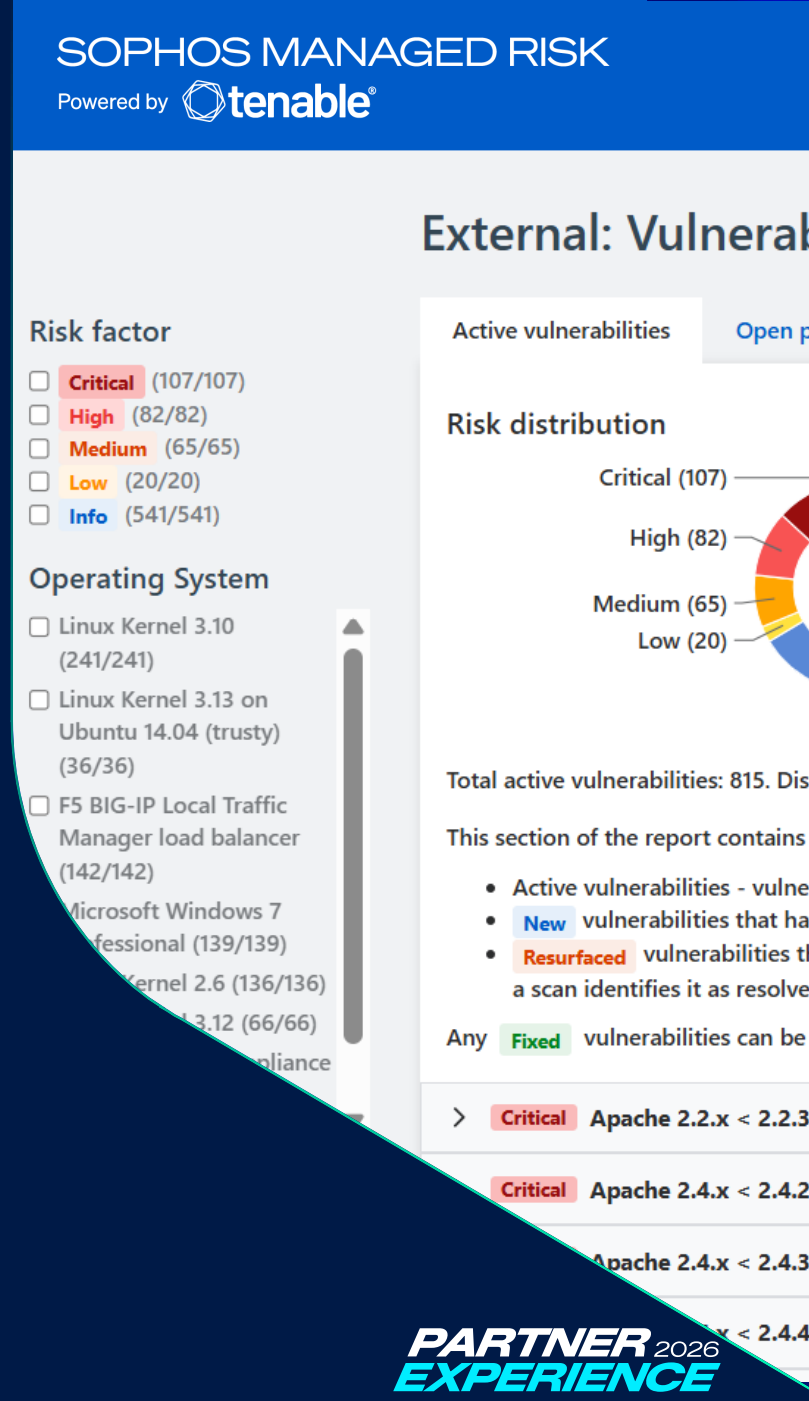
Quarterly reviews

Live meetings with the Sophos Managed Risk team to review recent findings, learn about the current exploitation landscape, and agree remediation priorities.

Comprehensive reporting

Stay informed and plan your remediation actions.

- Eliminate blind spots with external attack surface, internal discovery, and vulnerability scan reports.
- Comprehensive vulnerability scan results, prioritized by risk to your organization, with focus on your defined critical assets.
- Links to vulnerability documentation for additional information and remediation guidance.
- Interactive reports provide vulnerability data in an intuitive view.



SOPHOS

PARTNER EXPERIENCE 2026

Collaborates with Sophos MDR

Sophos Managed Detection and Response + Sophos Managed Risk

- Sophos Managed Risk and MDR teams share data to deliver superior outcomes for your business.
- View your Sophos Managed Risk and Sophos MDR cases together in a single view.
- Engage with Sophos Managed Risk experts by raising cases in your Sophos console.
- Review findings and receive expert guidance on the current exploitation landscape.

Gartner peerinsights™
A Gartner "Customers' Choice" vendor for MDR

G2
Rated a Leader in MDR by customers

MITRE | ATT&CK® Evaluations
A top performing vendor in MITRE ATT&CK Evaluations

FROST & SULLIVAN
A Leader in the 2025 Frost Radar for MDR

SOPHOS

Sophos Managed Risk is an add-on for Sophos MDR.

PARTNER 2026 EXPERIENCE

Simple and predictable pricing.

Sophos MDR add-on****

Available for Sophos MDR customers to purchase as an add-on service.

Simple licensing model

Includes both internal and external scanning in a single, streamlined subscription.

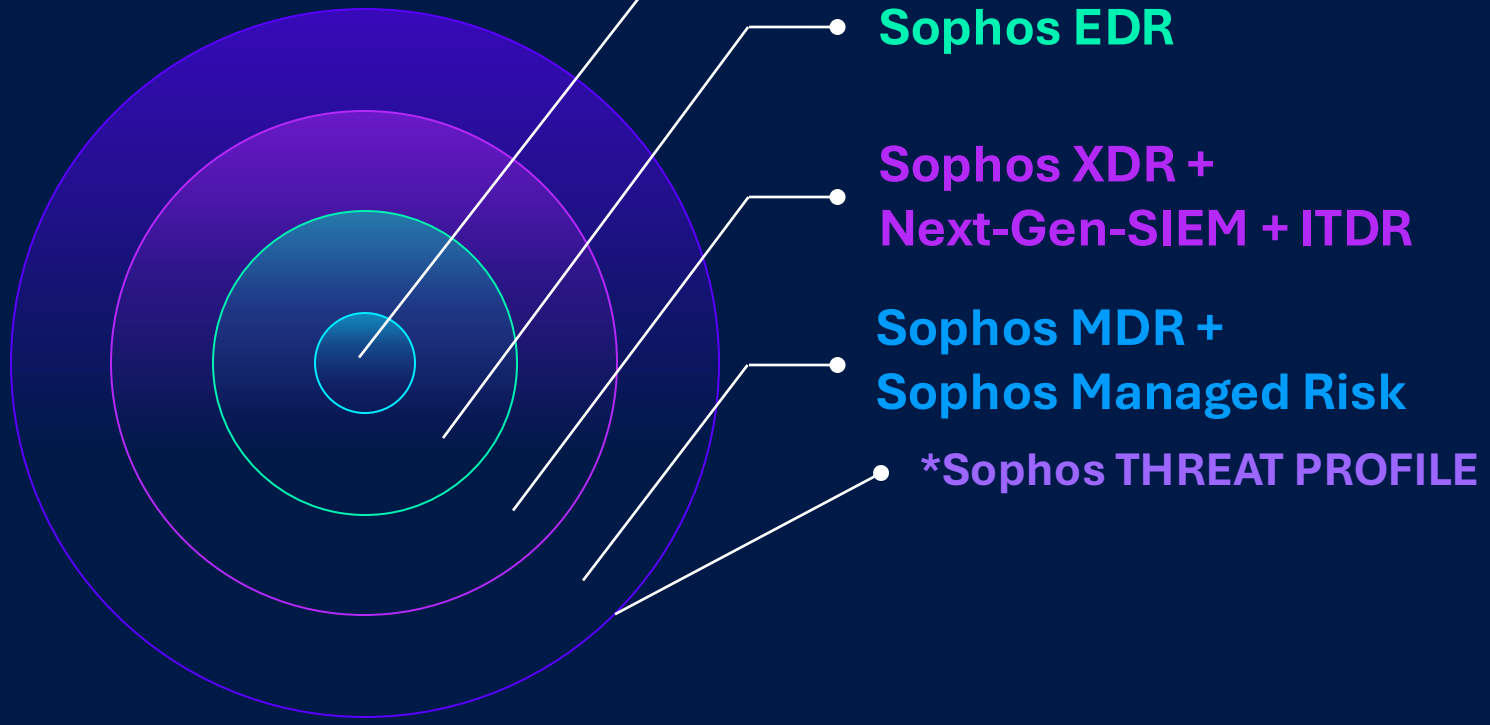
Term subscription

Volume-based pricing with built-in discounts based on the number of units.

Flexible service tiers

	SOPHOS MDR	SOPHOS MDR PLUS
24/7 expert-led threat monitoring and response	✓	✓
Detection and response across your entire IT environment Includes integrations with endpoint, network, firewall, cloud, identity, email, productivity, backup solutions	✓	✓
Sophos Endpoint and Sophos XDR technology included	Option to use Sophos Endpoint (included) or any third-party endpoint solution	✓
Comprehensive reporting and intelligence briefings	✓	✓
Proactive threat hunting	✓	✓
Threat response: active attacks are stopped and contained Using the full Sophos Endpoint agent or the Sophos Endpoint "XDR sensor" (included)	✓	✓
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 full Sophos Endpoint agent (included)	-	✓
Dedicated incident response lead	-	✓
Sophos breach protection warranty	-	✓
Sophos Managed Risk — powered by Tenable Vulnerability and attack surface management delivered as a managed service	⊕	⊕
Sophos Identity Threat Detection and Response (ITDR) Neutralize identity-based threats before they can impact your business	⊕	⊕

Path to growth and profitability



The world just got faster

No time to compromise on protection

The endpoint and MDR market is growing: Grab your share

Clear path to growth and profitability

RESOURCES AVAILABLE ON THE PARTNER PORTAL (LOGIN REQUIRED)

SOPHOS

PARTNER 2026 EXPERIENCE


SOPHOS

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

PARTNER 2026 EXPERIENCE

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE

SOPHOS

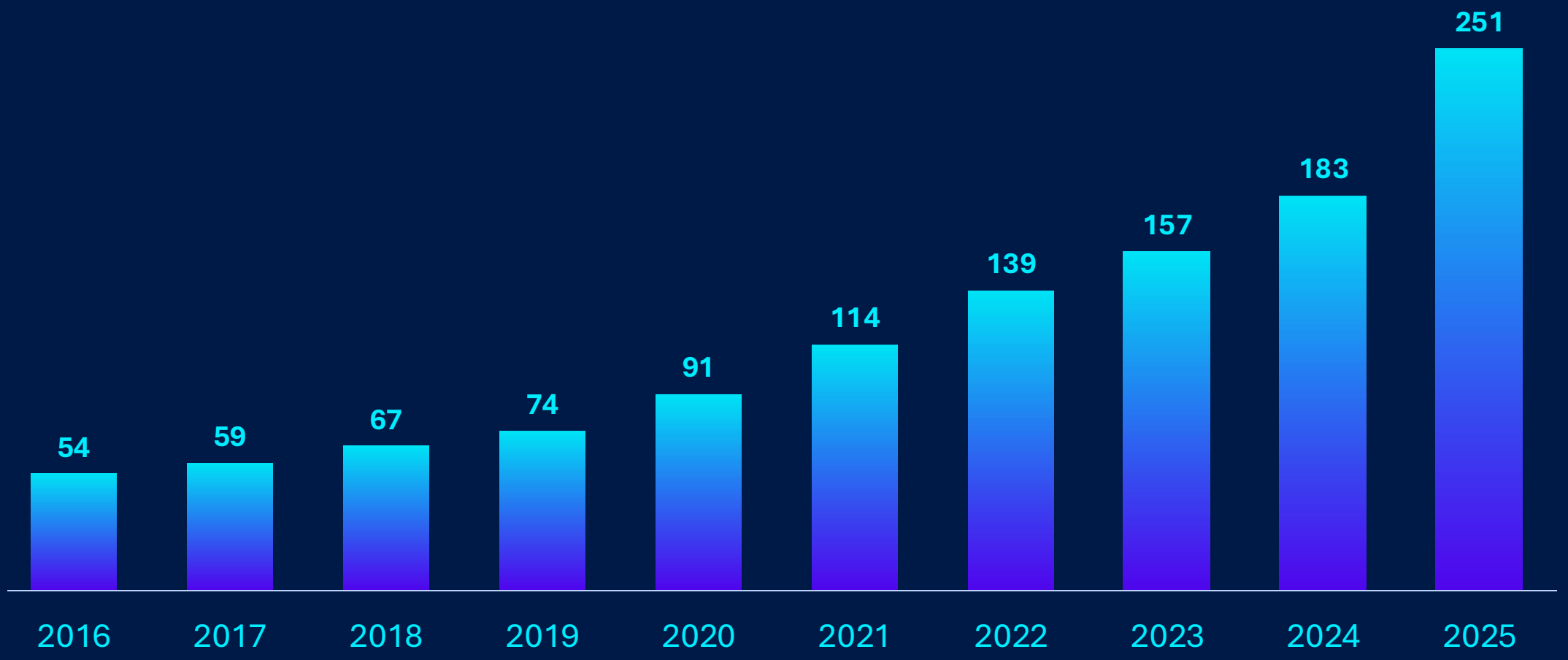
Stronger Together: Microsoft Ecosystem Play

Óscar López

Senior Sales Engineer

MICROSOFT COMMERCIAL REVENUE

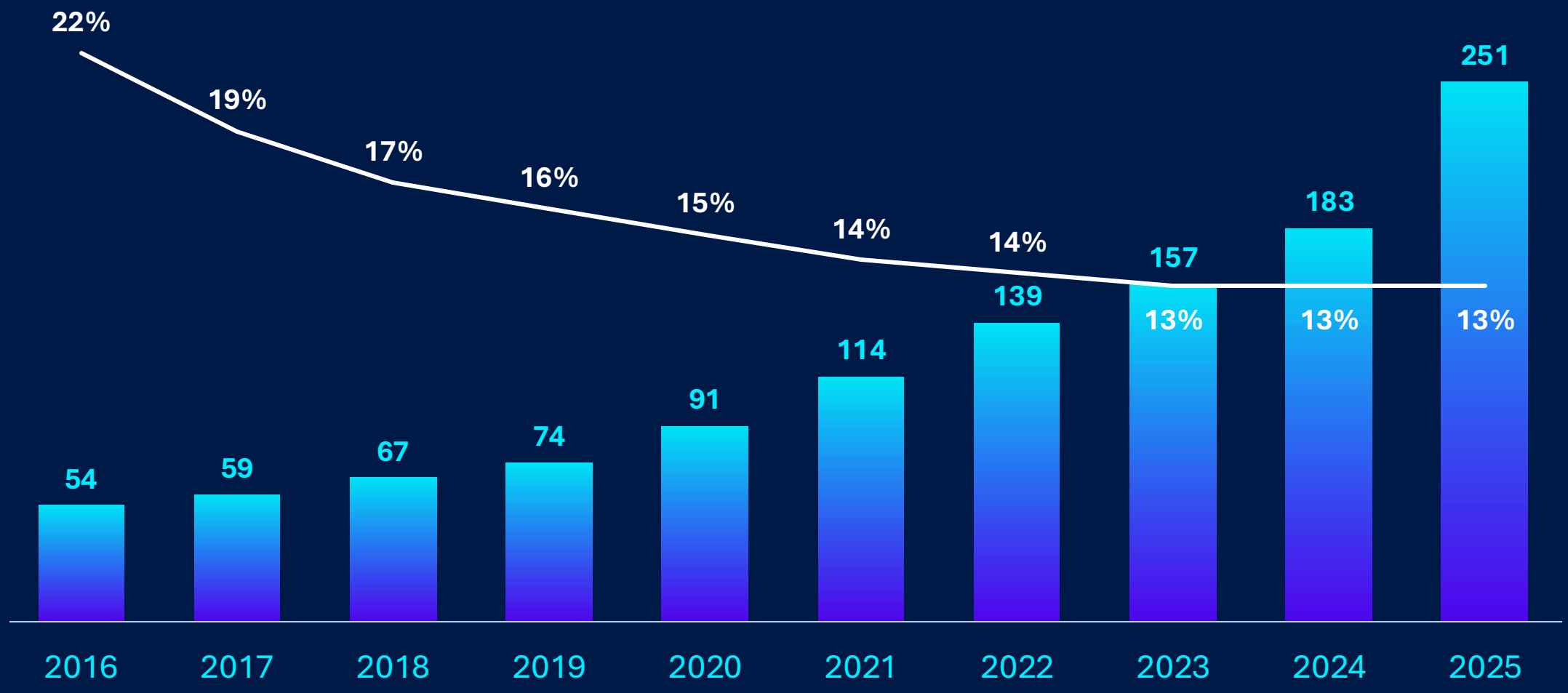
365% Crecimiento en la última década



Source: Stockanalysis.com

MARGEN DE PARTNERS DE MICROSOFT

41% menos en la última década



Source: Stockanalysis.com
Partner margin Indicative trend based on industry sources (Cloudmore, IDC, Steve Mordue/Forceworks, Volpi Capital).

Sophos: El proveedor de seguridad en el que Microsoft confía

Member of
Microsoft Intelligent Security Association

Microsoft

EXPERIENCE

El Sistema de Defensa Cibernética Optimizado para Microsoft

MÁS COMPLETO

MÁS RENTABLE

MÁS EFECTIVO

Complementando a Microsoft, no reemplazando

EXPERIENCE

El Sistema de Defensa Cibernética Optimizado para Microsoft

MÁS COMPLETO

Todos los planes de Microsoft

Full security portfolio

Endpoint, EDR, XDR, MDR, NG SIEM, ITDR, Email, Firewall, Services

MÁS RENTABLE

Márgenes más altos

Opciones de venta flexibles

Release Sentinel consumption costs

MÁS EFECTIVO

600,000+ Entornos

12-minute MTTR

MISA Verified | Copilot Integrated

Customer Acquisition

Microsoft Customer Attach

(Sophos and non-Sophos)

Sophos + Microsoft Bundles

FULL SALES PLAY AND CAMPAIGN AVAILABLE ON THE PARTNER PORTAL (LOGIN REQUIRED)

El Sistema de Defensa Cibernética Optimizado para Microsoft

Para todas las organizaciones

Commercial
1 - 99 seats

Immediate risk reduction

Sophos Endpoint, Sophos MDR, Sophos Email, Sophos Firewall

Mid-Market
100 - 1,000 seats

Synchronized defenses

Sophos MDR, Sophos ITDR, Sophos Firewall

Enterprise
1,000 seats

Capacity, resilience, budget efficacy

Sophos MDR, Sophos Next-Gen SIEM add-on, Sophos EMS

RANSOMWARE, IDENTITY THREATS, BEC

CYBER RISK

EXPERIENCE

La forma más completa, rentable y eficaz de proteger los entornos Microsoft.

RESELLER BENEFITS

- Larger deal sizes
- Higher margins
- Competitive differentiation
- Long-term account growth

MSP BENEFITS

- Higher MRR
- Stronger protection
- Reduced overheads
- Standardize and scale

Microsoft pone la plataforma...

...Sophos la monetiza


SOPHOS

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

PARTNER 2026 EXPERIENCE

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE

SOPHOS

Secure by Design: The Next Generation of Firewall Protection

Meet our speakers

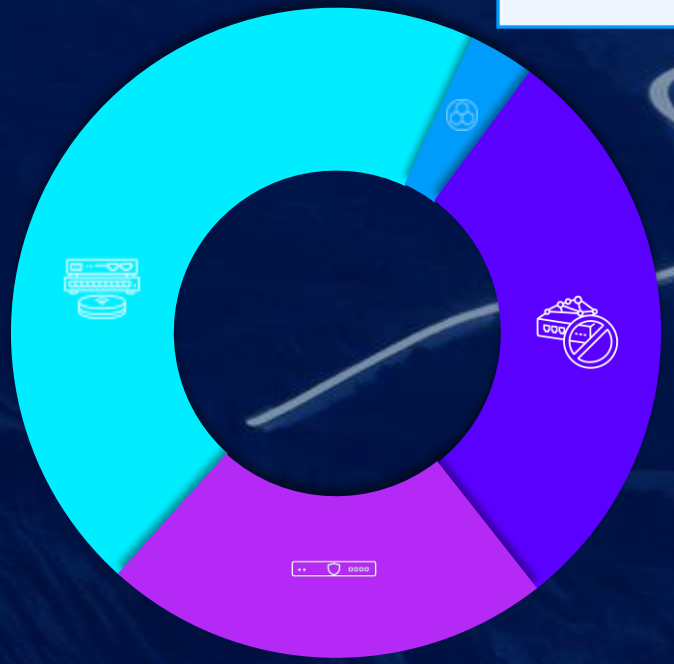
Ivan Mateos

Senior Sales Engineer

SOPHOS

PARTNER 2026 EXPERIENCE

Our Partners are at different places in their network journey...



UTM (SG) ONLY

MULTIPLE NETWORK PRODUCTS

NO NETWORK PRODUCTS

FIREWALL ONLY

But all face the same challenges...

But all face the same challenges...

Security
Frequent attacks on edge devices challenge your response capacity

The AI Conundrum
Visibility gaps slow AI adoption/ benefits, while attackers profit

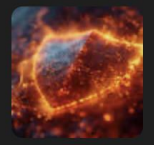
Response
Limited telemetry from point products slows mitigation

Complexity
Tool sprawl due to too many vendors, consoles, and agents

Firewalls are under attack

SecurityWeek

Hundreds of FortiGate Firewalls Hacked in AI-Powered Attacks: AWS



Threat actors have been hacking FortiGate firewalls via exposed ports and weak credentials with the help of AI.

1 week ago

GBHackers News

Hackers Launch Massive SonicWall Firewall Attack Using 4,000+ IP Addresses

Hackers are actively mapping SonicWall firewalls worldwide, launching more than 84000 SonicOS scanning sessions from over 4000 unique IP...

9 hours ago

ET Edge Insights

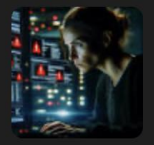
90% of ransomware attacks are exploiting firewalls: How attackers hide among routine IT changes - ET Edge

The modern ransomware attack no longer begins with a dramatic breach. It begins quietly with a login that looks routine, a firewall rule...

5 days ago

Cybersecurity Insiders

Ransomware attack makes customer file lawsuit against SonicWall Firewall Vulnerability



Explore how a ransomware attack led to a customer lawsuit over a SonicWall firewall vulnerability, what it means for security and steps to...

5 days ago

Cisco Blogs

Double Defense: Cisco Secure Firewall 10.0 Confronts Encrypted Traffic and Emerging Attack Challenges

Discover how Cisco Secure Firewall 10.0 boosts visibility and protection against modern threats, from encrypted attacks to AI-driven...

3 weeks ago

Cybersecurity Dive

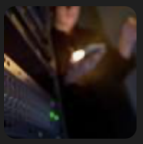
SonicWall investigating possible zero-day related to firewall attacks

Researchers recently warned about a surge in Akira ransomware attacks linked to a potential SonicWall vulnerability.

Aug 5, 2025

The Hacker News

Cisco Warns of New Firewall Attack Exploiting CVE-2025-20333 and CVE-2025-20362



In addition to the two vulnerabilities, Cisco has shipped patches for a high-severity DoS bug (CVE-2025-20343, CVSS score: 8.6) in Identity...

Nov 6, 2025

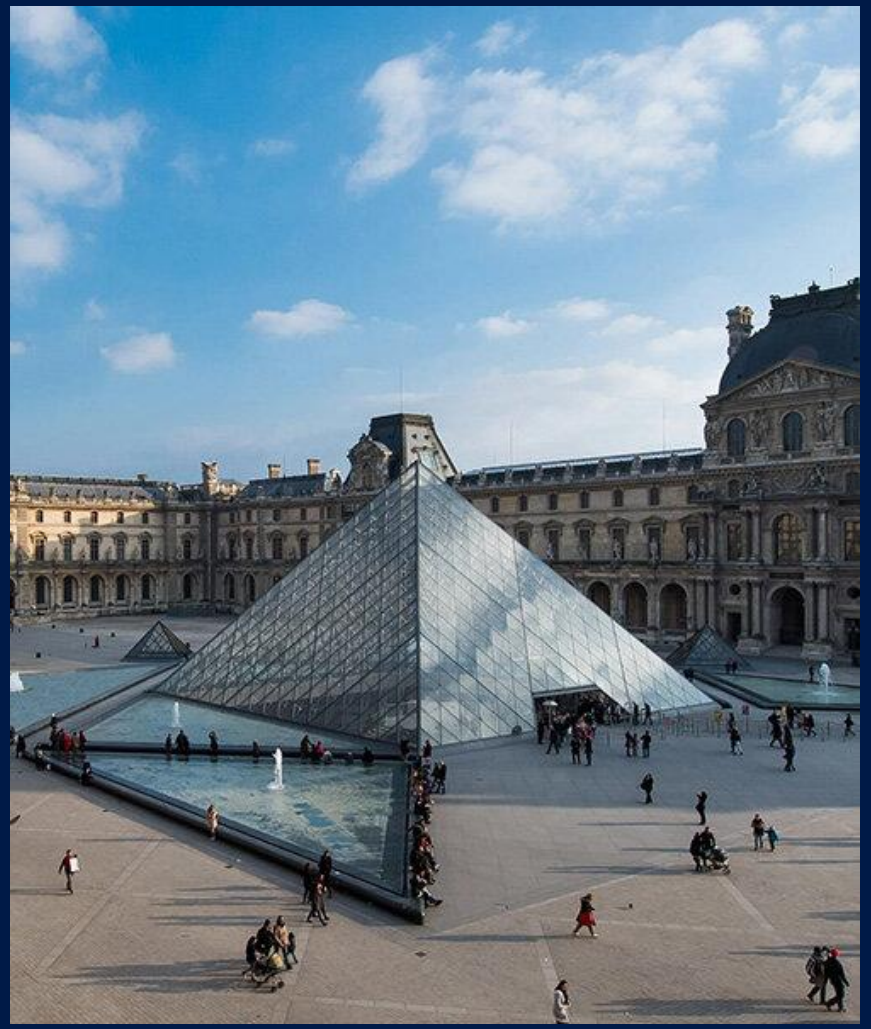
CISO Series

Cybersecurity News: Australia BadCandy warning, Cisco firewall attack, Aardvark eats bugs

Australia warns of BADCANDY Attacks Exploiting Cisco IOS XE. The Australian Signals Directorate (ASD) is warning of cyber attacks targeting...

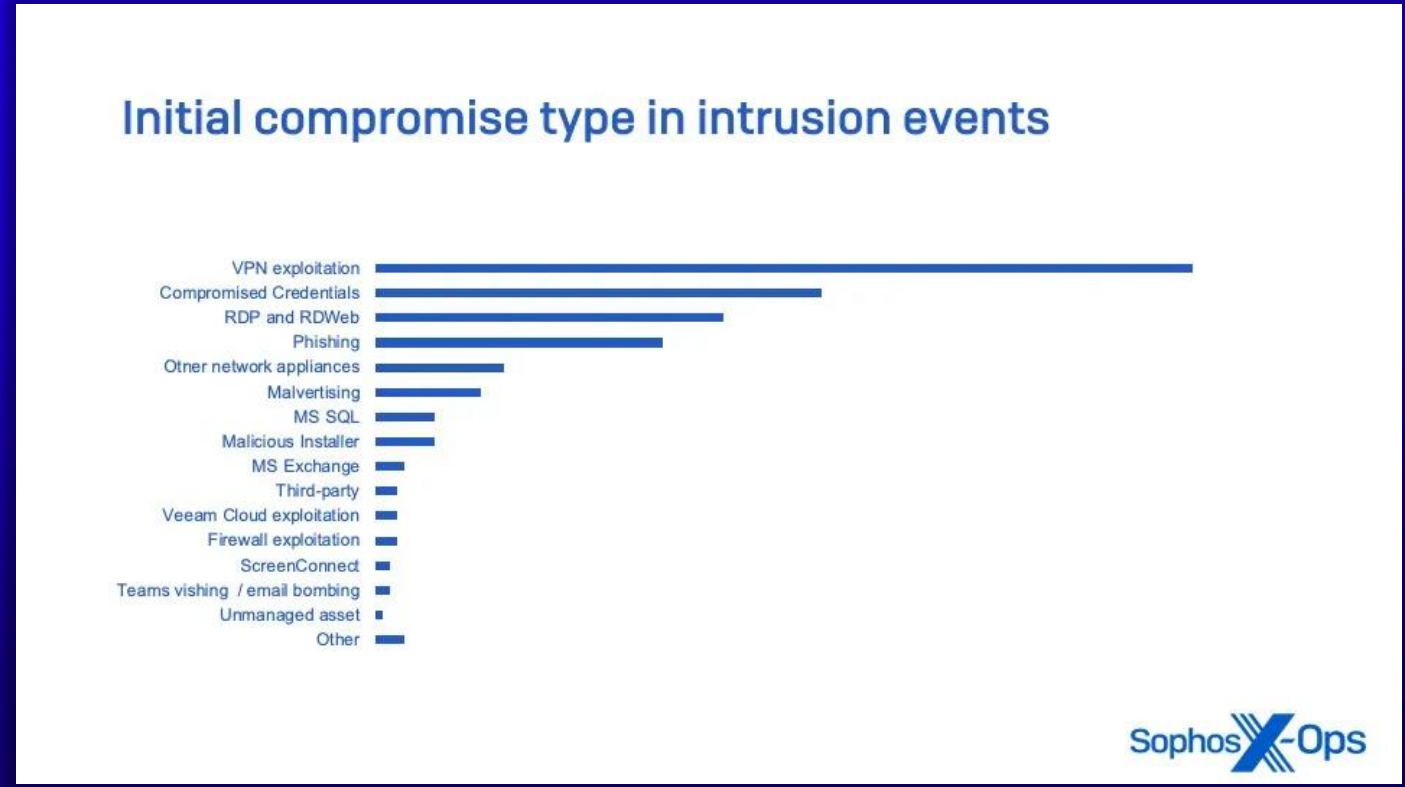
Nov 3, 2025

How safe are your most valuable assets?



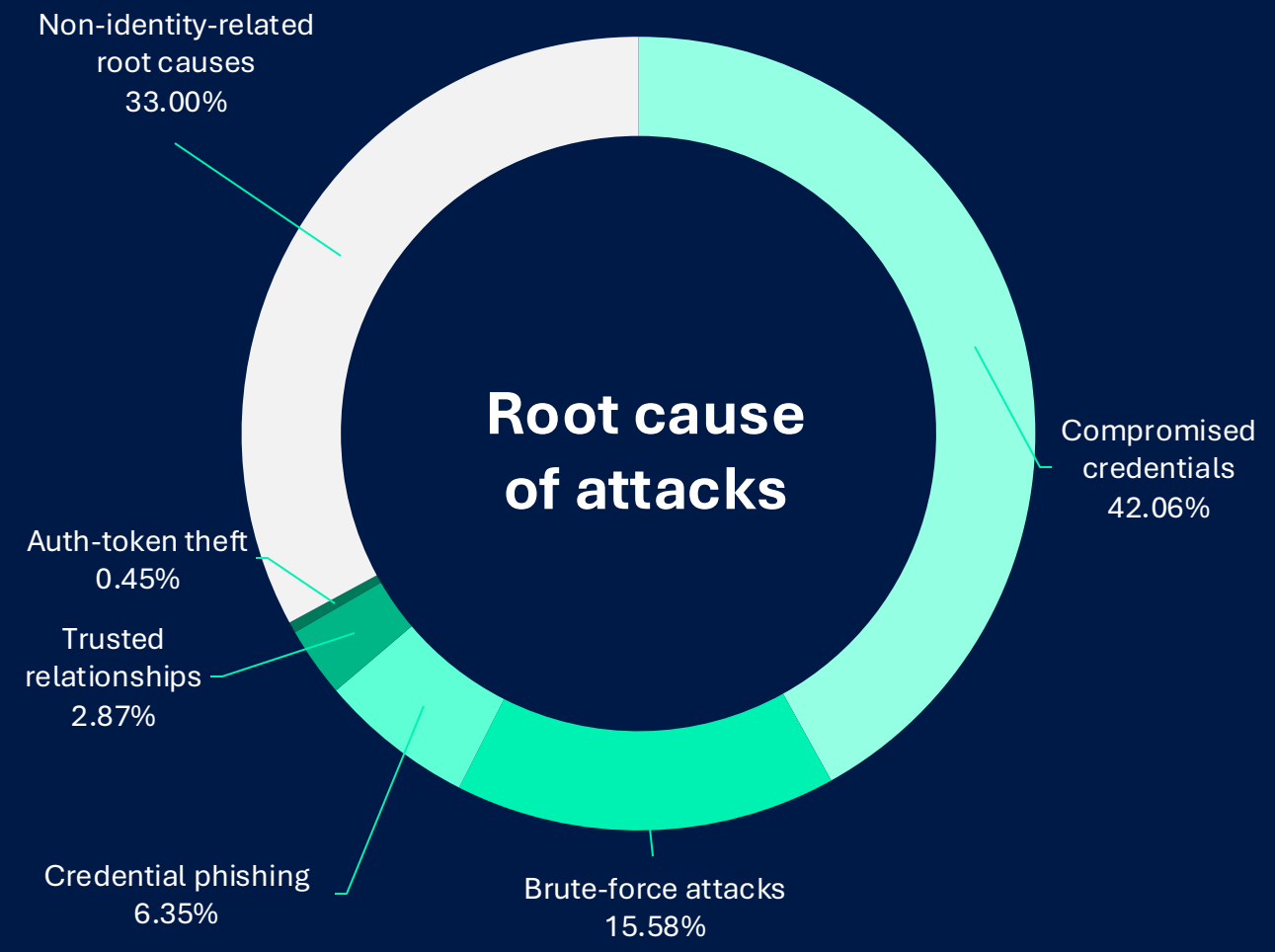
Firewalls are in a **privileged position**

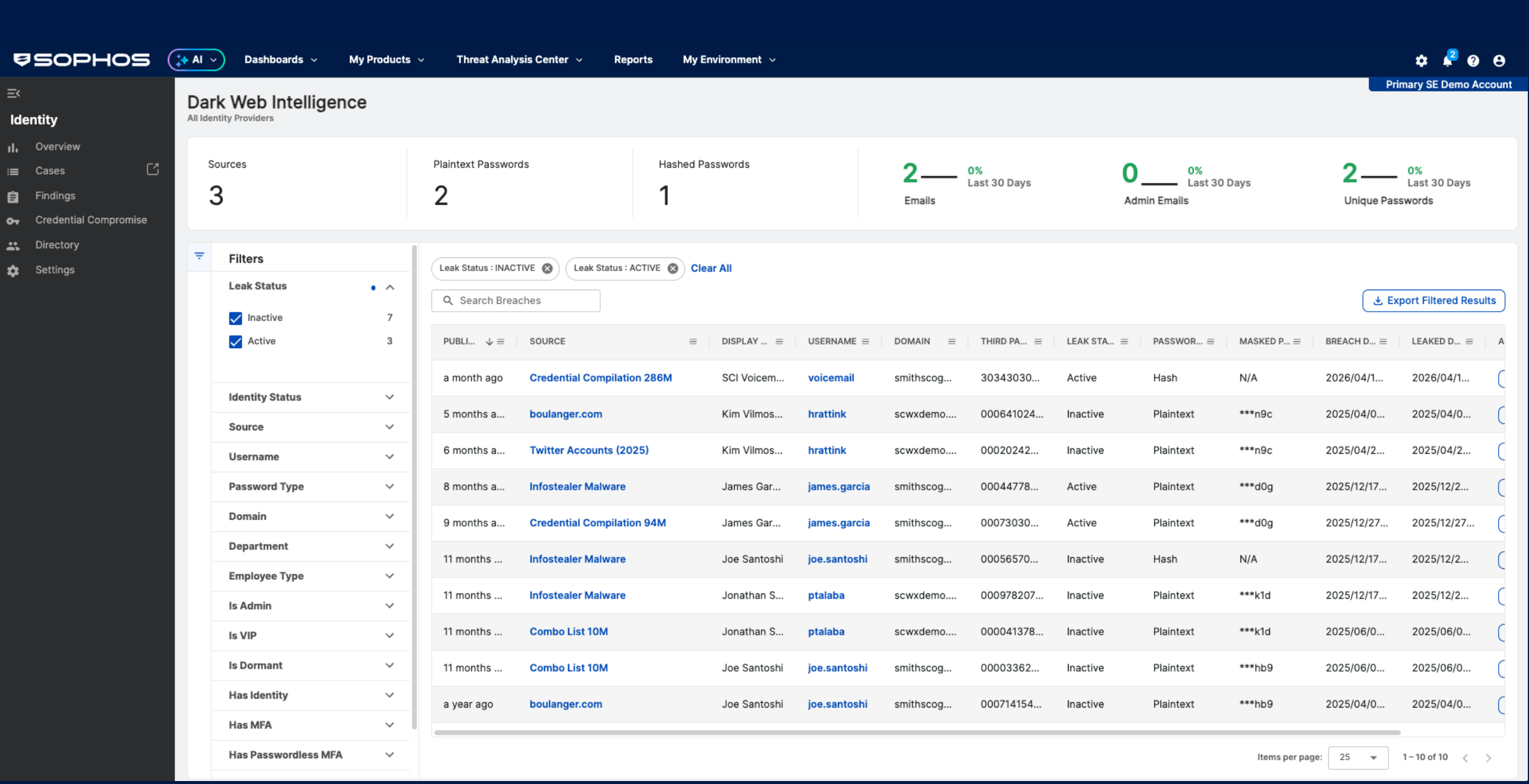
Vulnerabilities become a high-impact entry point



67%

of incidents started with compromised identity




SOPHOS
AI
Dashboards
My Products
Threat Analysis Center
Reports
My Environment
Primary SE Demo Account
Identity
Overview
Cases
Findings
Credential Compromise
Directory
Settings
Dark Web Intelligence
All Identity Providers
Sources
3
Plaintext Passwords
2
Hashed Passwords
1
2
0%
Last 30 Days
Emails
0
0%
Last 30 Days
Admin Emails
2
0%
Last 30 Days
Unique Passwords
Filters
Leak Status
Inactive 7
Active 3
Identity Status
Source
Username
Password Type
Domain
Department
Employee Type
Is Admin
Is VIP
Is Dormant
Has Identity
Has MFA
Has Passwordless MFA
Leak Status : INACTIVE
Leak Status : ACTIVE
Clear All
Search Breaches
Export Filtered Results
PUBLI...
SOURCE
DISPLAY ...
USERNAME
DOMAIN
THIRD PA...
LEAK STA...
PASSWOR...
MASKED P...
BREACH D...
LEAKED D...
a month ago
Credential Compilation 286M
SCI Voicem...
voicemail
smithscog...
30343030...
Active
Hash
N/A
2026/04/1...
2026/04/1...
5 months a...
boulanger.com
Kim Vilmos...
hrattink
scwxdemo....
000641024...
Inactive
Plaintext
***n9c
2025/04/0...
2025/04/0...
6 months a...
Twitter Accounts (2025)
Kim Vilmos...
hrattink
scwxdemo....
00020242...
Inactive
Plaintext
***n9c
2025/04/2...
2025/04/2...
8 months a...
Infostealer Malware
James Gar...
james.garcia
smithscog...
00044778...
Active
Plaintext
***d0g
2025/12/17...
2025/12/2...
9 months a...
Credential Compilation 94M
James Gar...
james.garcia
smithscog...
00073030...
Active
Plaintext
***d0g
2025/12/27...
2025/12/27...
11 months ...
Infostealer Malware
Joe Santoshi
joe.santoshi
smithscog...
00056570...
Inactive
Hash
N/A
2025/12/17...
2025/12/2...
11 months ...
Infostealer Malware
Jonathan S...
ptalaba
scwxdemo....
000978207...
Inactive
Plaintext
***k1d
2025/12/17...
2025/12/2...
11 months ...
Combo List 10M
Jonathan S...
ptalaba
scwxdemo....
000041378...
Inactive
Plaintext
***k1d
2025/06/0...
2025/06/0...
11 months ...
Combo List 10M
Joe Santoshi
joe.santoshi
smithscog...
00003362...
Inactive
Plaintext
***hb9
2025/06/0...
2025/06/0...
a year ago
boulanger.com
Joe Santoshi
joe.santoshi
smithscog...
000714154...
Inactive
Plaintext
***hb9
2025/04/0...
2025/04/0...
Items per page:
25
1 – 10 of 10
SOPHOS
PARTNER 2026
EXPERIENCE

CVEdetails.com
powered by SecurityScorecard

CVE id, product, vendor...

New/Updated CVEs

213 CVEs created, **531** CVEs updated since yesterday

1146 CVEs created, **2362** CVEs updated in the last 7 days

6430 CVEs created, **100872** CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
7	9	22

Recent EPSS score changes

>5%	>10%	>50%
0	0	0

Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	1949
1-2	102
2-3	1072
3-4	2754
4-5	18524
5-6	45802
6-7	44525
7-8	64910
8-9	36028
9+	46148
Total	261814

Weighted Average CVSS Score: 7.6

** For CVEs published in the last 10 years*

Vulnerabilities by type & year

Firewalls remain vulnerable long after patches are released

322 days

Median time between a vendor publishing an advisory or patch and an attacker exploiting that flaw.

SECURE BY DESIGN

PLEDGE

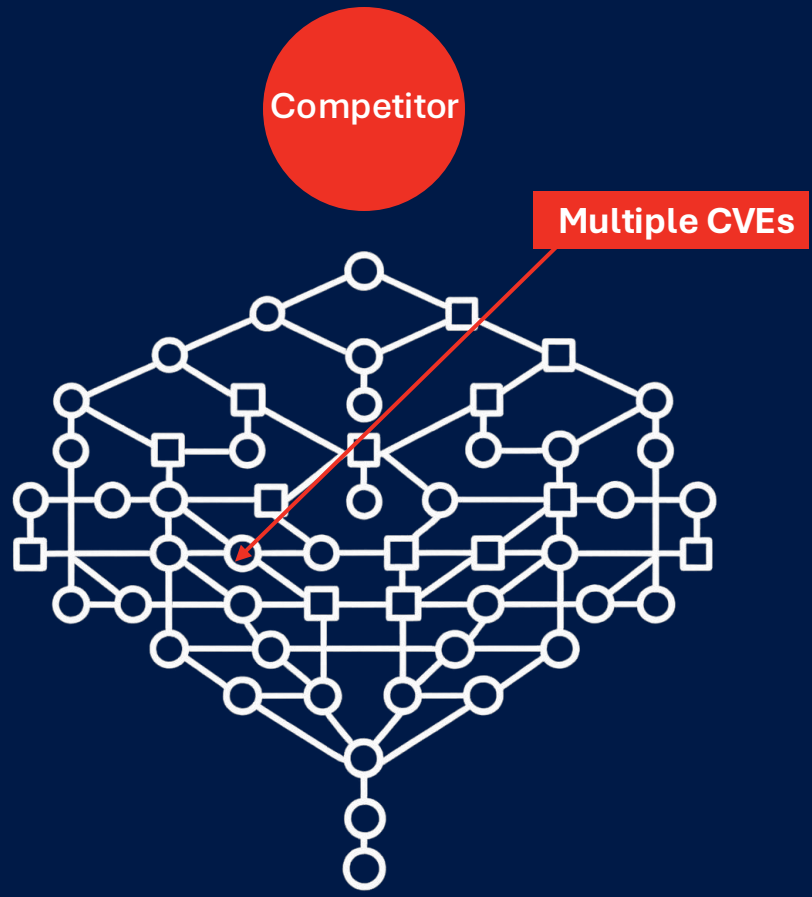
GOALS

- MULTIFACTOR AUTHENTICATION (MFA)
- DEFAULT PASSWORDS
- REDUCING ENTIRE CLASSES OF VULNERABILITY
- SECURITY PATCHES
- VULNERABILITY DISCLOSURE POLICY
- COMMON VULNERABILITIES AND EXPOSURES (CVE)
- EVIDENCE OF INTRUSIONS

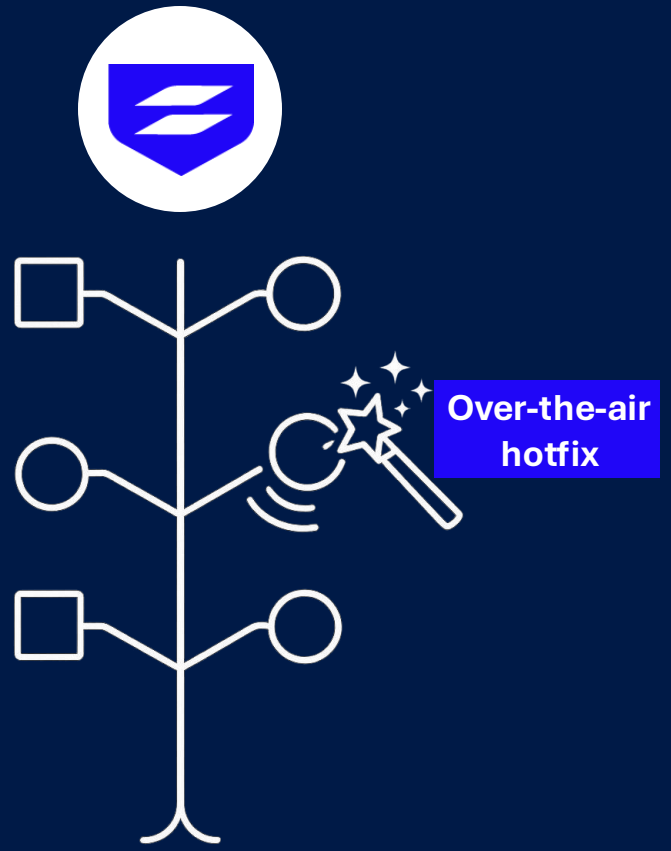
Attackers are using AI to rapidly discover vulnerabilities.

Which would you rather patch in an emergency?

Complex by Default



Secure by Design



A new Era of AI-driven attacks

DRAMATICALLY CHANGING THE THREAT LANDSCAPE

Anthropic Claude Mythos:

- A new AI model to discover exploitable software vulnerabilities
- In just 7 weeks of testing, Mythos discovered over 2000 previous unknown zero-day vulnerabilities
- It can autonomously identify vulnerabilities and generate working exploits across all operating systems at machine speed
- It presents a huge opportunity but also an enormous risk

Ya está aquí GPT-5.5-Cyber ¿Qué supone para los defensores que trabajan en primera línea?

El lanzamiento de GPT-5.5 por parte de OpenAI el 7 de mayo y la vista previa limitada de GPT-5.5-Cyber ponen la IA de vanguardia en manos de defensores verificados. Como miembro del programa Trusted Access for Cyber, Sophos está utilizando estos modelos para perfeccionar lo que ya tenemos en marcha: un SOC autónomo que resuelve más de la mitad de los casos sin intervención humana, y una arquitectura de endpoints diseñada específicamente para detener los ataques de día cero generados por IA.

Mayo 11, 2026

Escrito por John Peterson

The vulnerability flood is here. Here's what it means – and how to prepare

We can't control the pace of AI-driven vulnerability discovery, but we can control how fast we respond.

April 9, 2026 |  Written by Ross McKerchar

MSP Survey: Firewall Security Vulnerability - Impact on Partner

Source: Sophos MSP Survey

Together, We Share the Responsibility

Partner

Secure by Design

Over-the-air hotfixes, proactive monitoring, health check, securely encrypted backups and updates, etc.

Your Benefits

Accelerated, proactive remediation with no additional overhead, monetizable health check, increased trust

Visibility and Control

Synchronized Security cross-product integration and automated response, visibility into AI usage, support for remote and hybrid working scenarios, network stack

Your Benefits

Cross-sell opportunities via ecosystem, chance to support customers' AI-adoption and zero-trust transitions, Workspace Protection greenfield

Constantly Adding Value

Many new releases introduce new features and improved performance at no extra cost, e.g., NDR Essentials, DNS Protection, Active Threat Response

Your Benefits

Demonstrate customer ROI over the full lifecycle of the product, easier to position higher-value bundle and incentivize upgrades, helps with customer retention

The new AI era

Speed
Accelerated speed of discovery and attack

Scale
Unprecedented vulnerabilities and patching

Scope
Dramatic lowers the barrier of entry for adversaries

Protecting your network and a Secure by Design firewall is more important than it ever has been.

A Strong Value Proposition For All Market Segments

Commercial

1 - 99 seats

All-in-one, no-compromise protection at an attractive price point

Network-in-a-Box
(Sophos Firewall, switches, wireless)

Mid-Market

100 - 1,000 seats

Consolidate, simplify, and save
Best protection and performance
Constantly adding value

Consolidate, Simplify, and Save
(Firewall with SD-WAN, Access, Workspace, Email)

Distributed Enterprise

1,000 seats

Powerful performance and protection
Integrated detection and response
Unified management

Sophos Firewall with NDR and purpose-built MDR/XDR integration with Active Threat Response and Sync Security

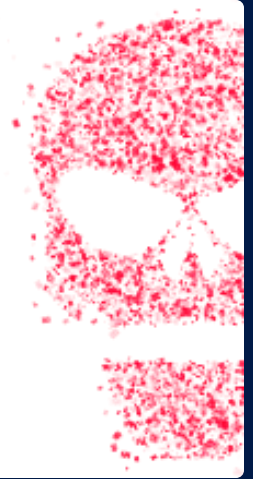
Sophos Firewall v22 | Secure By Design taken to a new level

Secure By Design
Hardened against attacks

Automated Hotfixes

Eliminate patch fatigue

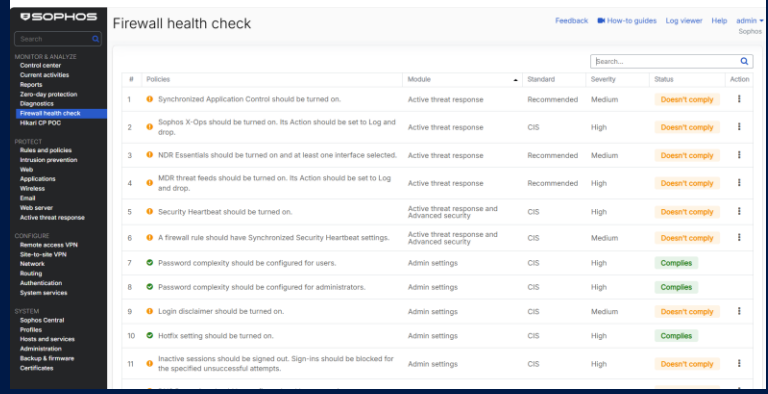
Over-the-air security patches applied automatically with no down time



Health Check

Mitigate the risk of misconfiguration

Continuously monitors dozens of configurations against best-practices



Proactive Monitoring
by Sophos

Continuously monitoring system integrity to identify and respond to attacks sooner

MFA/ZTNA
Prevent attacks with compromised credentials

- ✓MFA integrated across all areas of the firewall
- ✓ZTNA gateway integrated into the firewall makes deployment easy

Secure Xstream Architecture
Eliminate entire classes of vulnerabilities

- ✓ Hardened kernel
- ✓ Secure control plane
- ✓ Process isolation

SOPHOS

PARTNER 2026 EXPERIENCE

Competitive Firewall Displacement

HW + LICENSES + SERVICES
AND REDUCE ADMIN OVERHEAD

Sell the Full Stack

INCL. WORKSPACE PROTECTION
MANAGED FROM A SINGLE CONSOLE

MDR Cross-sell

SELL MDR/EP TO FW CUSTOMERS
SELL FW TO MDR/EP CUSTOMERS

SOPHOS

Config Studio

View, edit, compare, test, and analyze your Sophos Firewall configurations. Your data stays private. All processing happens locally on your endpoint.

Get started

What would you like to do?

Configuration report

- Human-readable report
- Export to HTML or PDF
- Policy test and analysis
- Global search

Compare configurations

- Side-by-side diff view
- Track added and removed settings
- Entity-level change tracking
- Export comparison results

Configuration editor

- Visual rule and object editor
- Bulk edit with IntelliSense
- Preview generated XML
- Download XML or TAR

Migrate to Sophos Firewall

- Sophos Firewall and Sophos UTM
- SonicWall, FortiGate, and Palo Alto
- Runs entirely in your browser

Competitive Firewall Displacement

HW + LICENSES + SERVICES
AND REDUCE ADMIN OVERHEAD

Sell the Full Stack

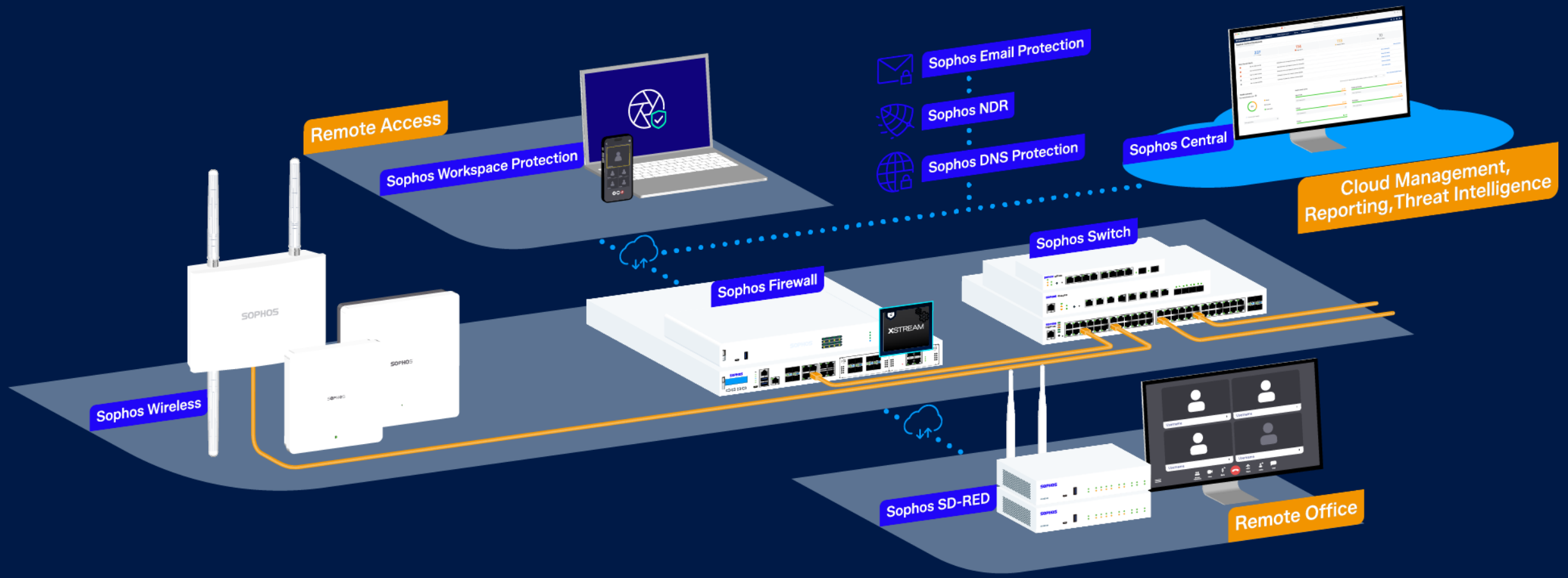
INCL. WORKSPACE PROTECTION
MANAGED FROM A SINGLE CONSOLE

MDR Cross-sell

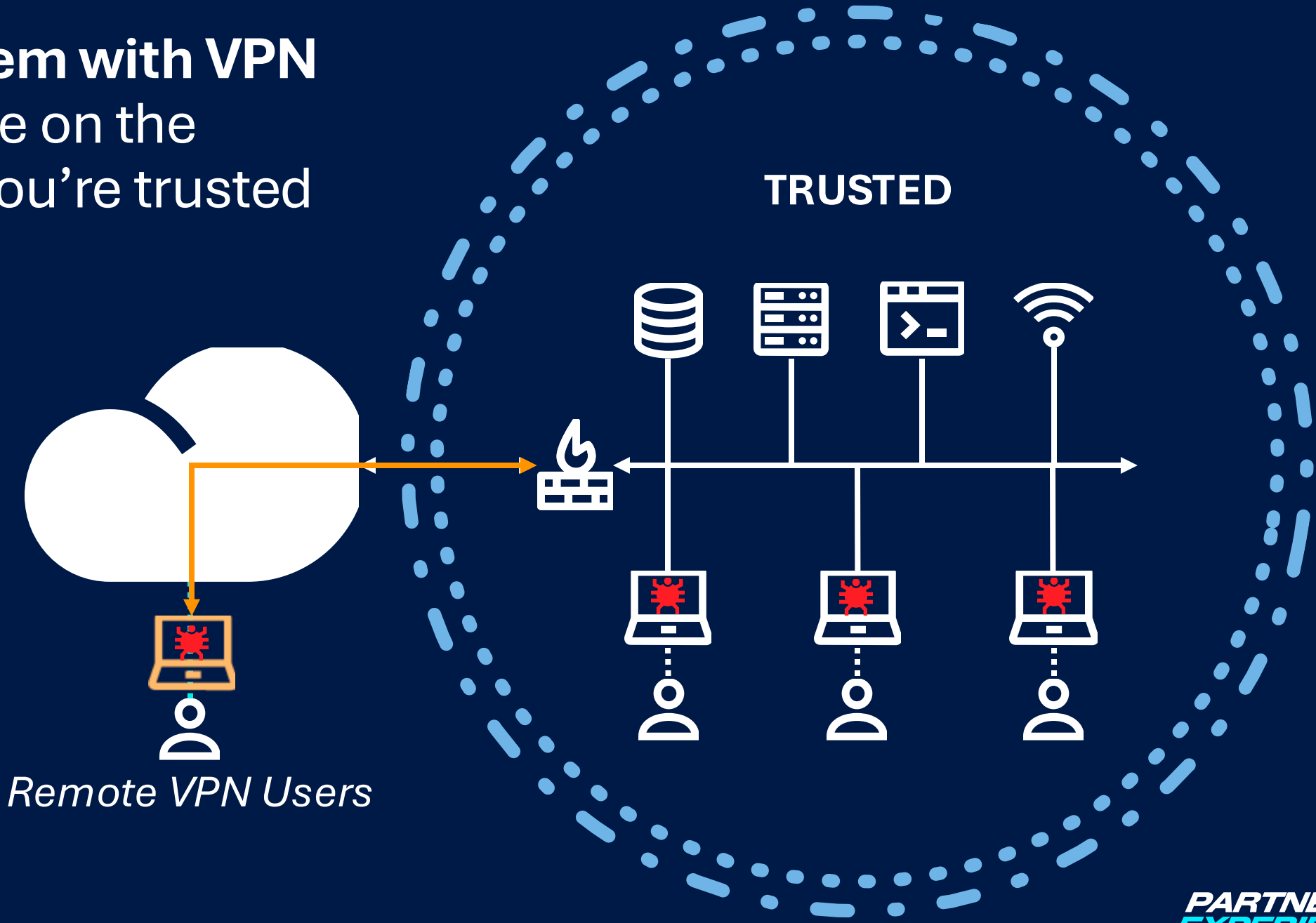
SELL MDR/EP TO FW CUSTOMERS
SELL FW TO MDR/EP CUSTOMERS

Sophos Network Security

Much more than a firewall

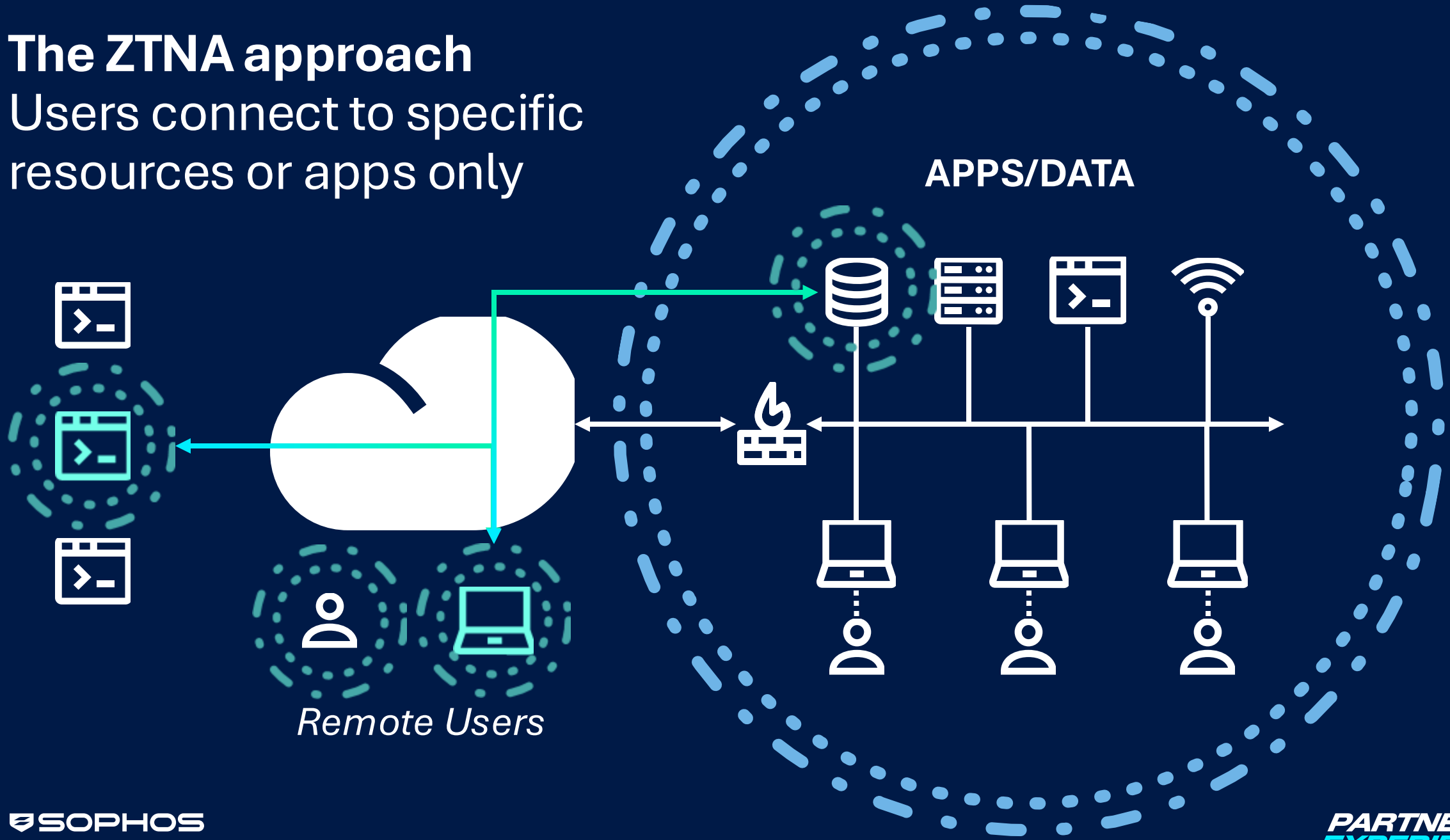


The problem with VPN
once you're on the network, you're trusted



The ZTNA approach

Users connect to specific resources or apps only



Sophos Workspace Protection – What You Get:

ZTNA

- In-browser integration
- RDP and SSH support
- Device posture assessment including Synchronized Security

SaaS Control

- Application usage monitoring and controls
- Data controls and data boundary

Secure Web & DNS

- Web and DNS Policy Engine
- Sophos Threat Intel
- DNS Protection
- User/Device Policy

Hardened Browser

- Improves security against browser exploits/attacks without the heavy RBI experience

Data Loss Controls

- Cut / Copy & Paste
- Screen Capture
- Print / Save
- Download & Upload
- Data Redaction

Email Monitoring

- Detection of malicious URLs injected via email
- Detection of phishing messages delivered to end users

Sophos Central

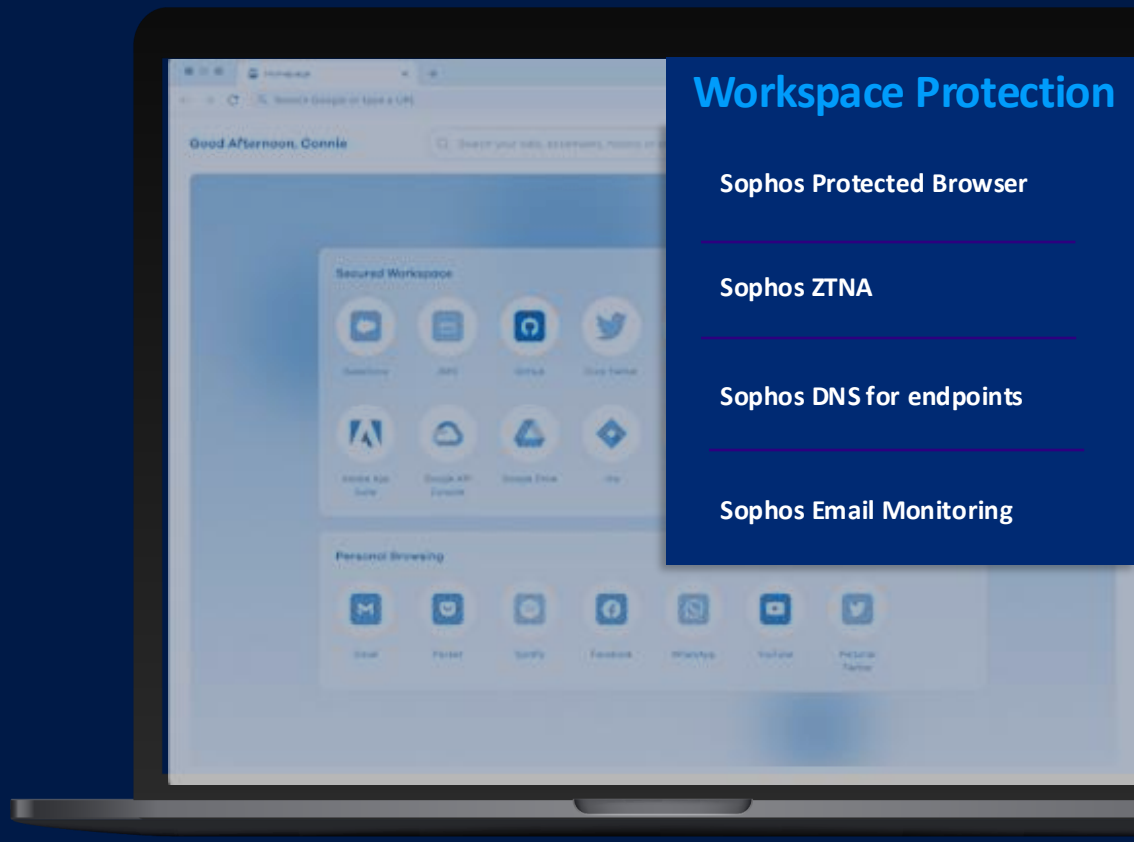
- Management of Protected Browser
- Integration with Central Directory Services
- Synchronized Security Support

Sophos Cloud

- Sophos SXL URL/Domains, Intelix file upload/downloads
- Integrated with Sophos Datalake
- ZTNA data plane integration

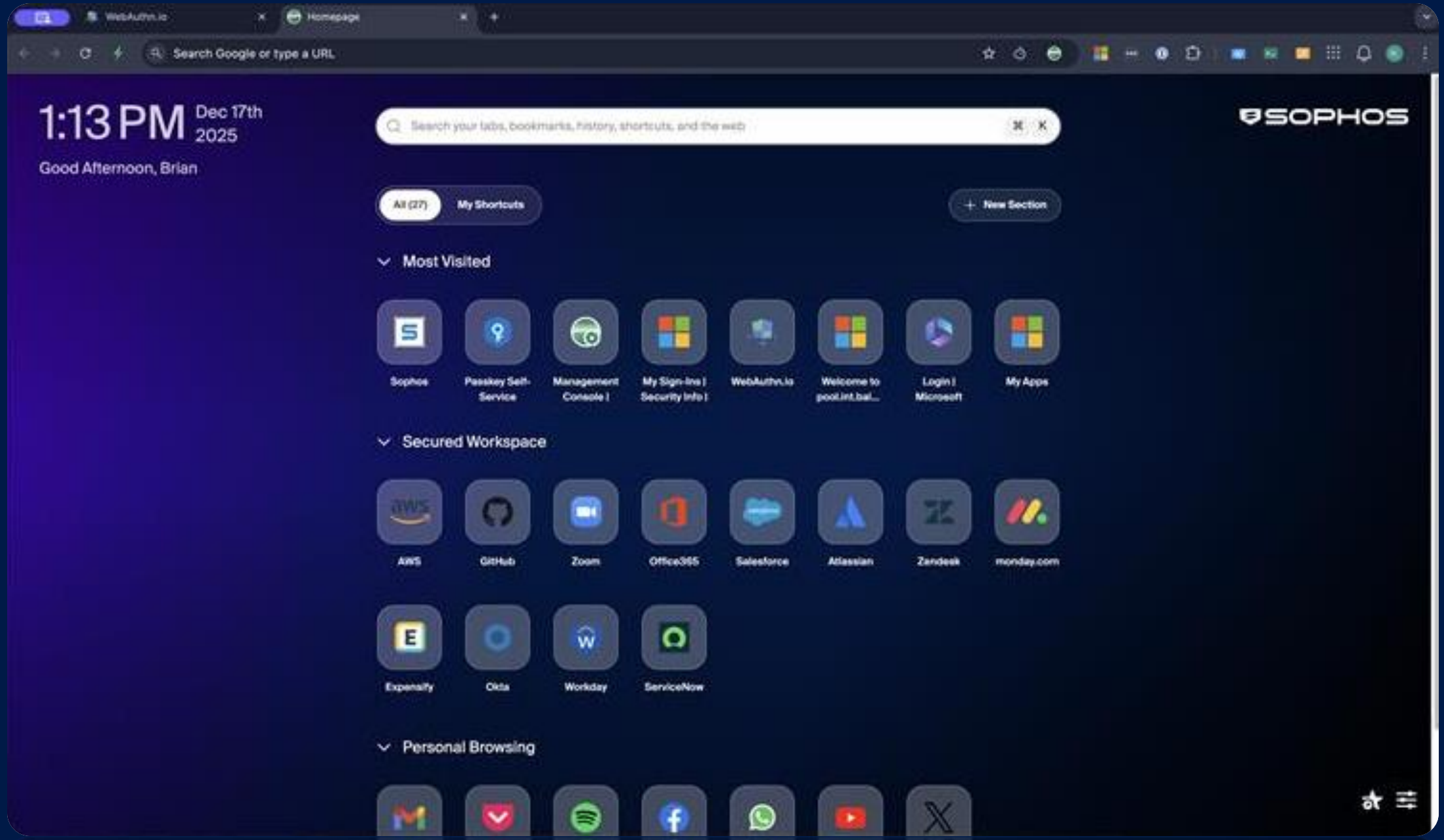
Deployment

- Easy installation in 30 seconds by end users
- Managed or unmanaged devices
- Windows, Mac, browser support
- DNS for Windows



SOPHOS

PARTNER 2026 EXPERIENCE



SOPHOS

PARTNER EXPERIENCE 2026

Sophos Protected Browser

Powered by Island

Island Chromium Browser

- Island Data, web, and SaaS app control features
- Simple and familiar user experience
- Easy installation

Sophos Protection and Management

- Sophos Central management, logging, reporting
- Sophos threat intelligence (web and content inspection)
- Integrated Sophos ZTNA for web apps, SSH, RDP

The Hacker News

Fortinet Patches Actively Exploited CVE-2026-35616 in FortiClient EMS

Fortinet Patches Actively Exploited CVE-2026-35616 in FortiClient EMS ... Fortinet has released out-of-band patches for a critical security flaw...

hace 1 mes

BleepingComputer

Hackers exploit newly patched Fortinet auth bypass flaws

CVE-2025-59718 is a FortiCloud SSO authentication bypass affecting FortiOS, FortiProxy, and FortiSwitchManager. It is caused by improper...

16 dic 2025

The Hacker News

Fortinet Warns of Active Exploitation of FortiOS SSL VPN 2FA Bypass Vulnerability

Fortinet on Wednesday said it observed "recent abuse" of a five-year-old security flaw in FortiOS SSL VPN in the wild under certain...

25 dic 2025

BleepingComputer

Hackers breach Fortinet FortiGate devices, steal firewall configs

The campaign started last week, on January 15, with the attackers exploiting an unknown vulnerability in the devices' single sign-on (SSO)...

22 ene 2026

SecurityWeek

SonicWall Urges Immediate Patching of Firewall Vulnerabilities

SonicWall Urges Immediate Patching of Firewall Vulnerabilities. The bugs could be exploited to bypass security controls, access restricted...

hace 4 semanas

Cybersecurity Dive

Patch bypass allows hackers to exploit prior flaw in SonicWall SSL-VPN

... in SonicWall SSL-VPN. Researchers said a wave of attacks began in February targeting firewalls that appeared to be protected. Published May 19, 2026.

hace 1 semana

Help Net Security

Exploited SonicWall zero-day patched (CVE-2025-40602)

SonicWall has patched a local privilege escalation vulnerability (CVE-2025-40602) affecting its Secure Mobile Access (SMA) 1000 appliances...

17 dic 2025

CyberSecurityNews

Hackers Actives Scanning SonicWall Firewall Interfaces - 597,000 Sessions Observed

A surge in scans targeting SonicWall firewall interfaces has raised concerns about possible pre-disclosure vulnerability reconnaissance.

hace 2 días

Content Hub

Para desarrollar tu negocio

¡Danos tu feedback! Encuesta

Tu opinion es muy importante para nosotros

Materiales de Co-marketing y Campañas

Convierte los insights del Roadshow en ingresos

Soporte y Presentaciones

Explora y vuelve a consultar las presentaciones y recursos del evento.

SOPHOS

PARTNER 2026 EXPERIENCE

Sigue & Menciona @Sophos Partners en LinkedIn para tener la oportunidad de ganar

Publica antes de las 17:00pm
respondiendo a unas de estas tres preguntas:

1. ¿Qué está siendo lo más destacado para ti de la jornada Partner Experience de este año?
2. ¿Qué oportunidad de colaboración o solución de Sophos puede impulsar más tu negocio este año?
3. ¿Qué innovación de Sophos crees que tendrá mayor impacto en tu negocio y el de tus clientes?

SOPHOS

PARTNER 2026 EXPERIENCE


SOPHOS
PARTNER 2026
EXPERIENCE


SOPHOS