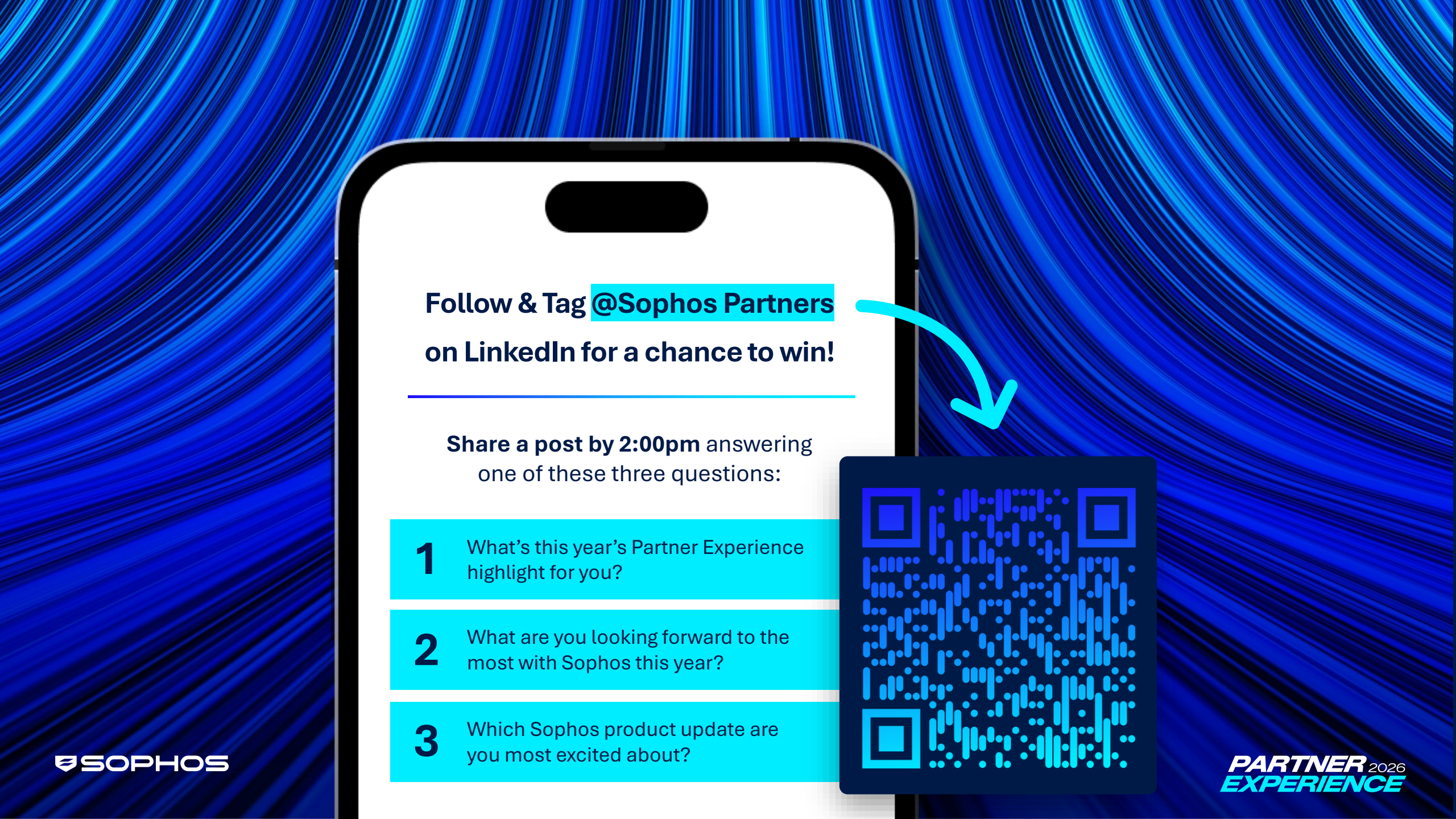
SOPHOS

PARTNER 2026 EXPERIENCE

Agenda

Time	Session
10:00 AM – 11:30 AM	Welcome & Intro – *John Mitchell, Head of Channels EMEA North*
	Sophos Mission and Vision – *Andy Travers, SVP EMEA*
	Sophos Vision to Reality – *Stuart Borgman, VP EMEA Sales Engineering*
	State of the Industry – *Pieter Nell, Regional Head SADC*
	Channel Strategy & Focus – *John Mitchell, Head of Channels EMEA North*
11:30 AM - 12:00 PM	**B R E A K**
12:00 PM – 1:00 PM	MDR Momentum – *Stuart Borgman, VP EMEA Sales Engineering*
	Stronger Together (Sophos + Microsoft) – *Jez Edwards, Revenue Programs NEMEA*
	Secure by Design (Firewall) - *Lukas Pelser, Solution Engineer*
1:00 PM – 2:30 PM	**L U N C H**
2:30 PM – 3:10 PM	Panel Discussion & Q&A – *Pieter Nell, George Kruger & Stuart Wilson*
3:15 PM - 4:00 PM	Awards – *Pieter Nell, Regional Head SADC*
4:00 PM	Food, Music, Entertainment & Networking


Follow & Tag @Sophos Partners
on LinkedIn for a chance to win!
Share a post by 2:00pm answering one of these three questions:
1 What's this year's Partner Experience highlight for you?
2 What are you looking forward to the most with Sophos this year?
3 Which Sophos product update are you most excited about?
SOPHOS
PARTNER 2026 EXPERIENCE

Content Hub

To Develop Your Business

Partner Feedback Form

Your Insights Are Essential

Co-marketing Materials and Campaigns

Turn Roadshow Insights Into Revenue

Support and Slide Decks

Explore And Revisit The Presentations From The Event

SOPHOS

PARTNER 2026 EXPERIENCE

SOPHOS

PARTNER 2026 EXPERIENCE

VISION AND MISSION

SOPHOS

PARTNER 2026 EXPERIENCE

Why Sophos

Why now

Why we win

35,000
Businesses with CISOs

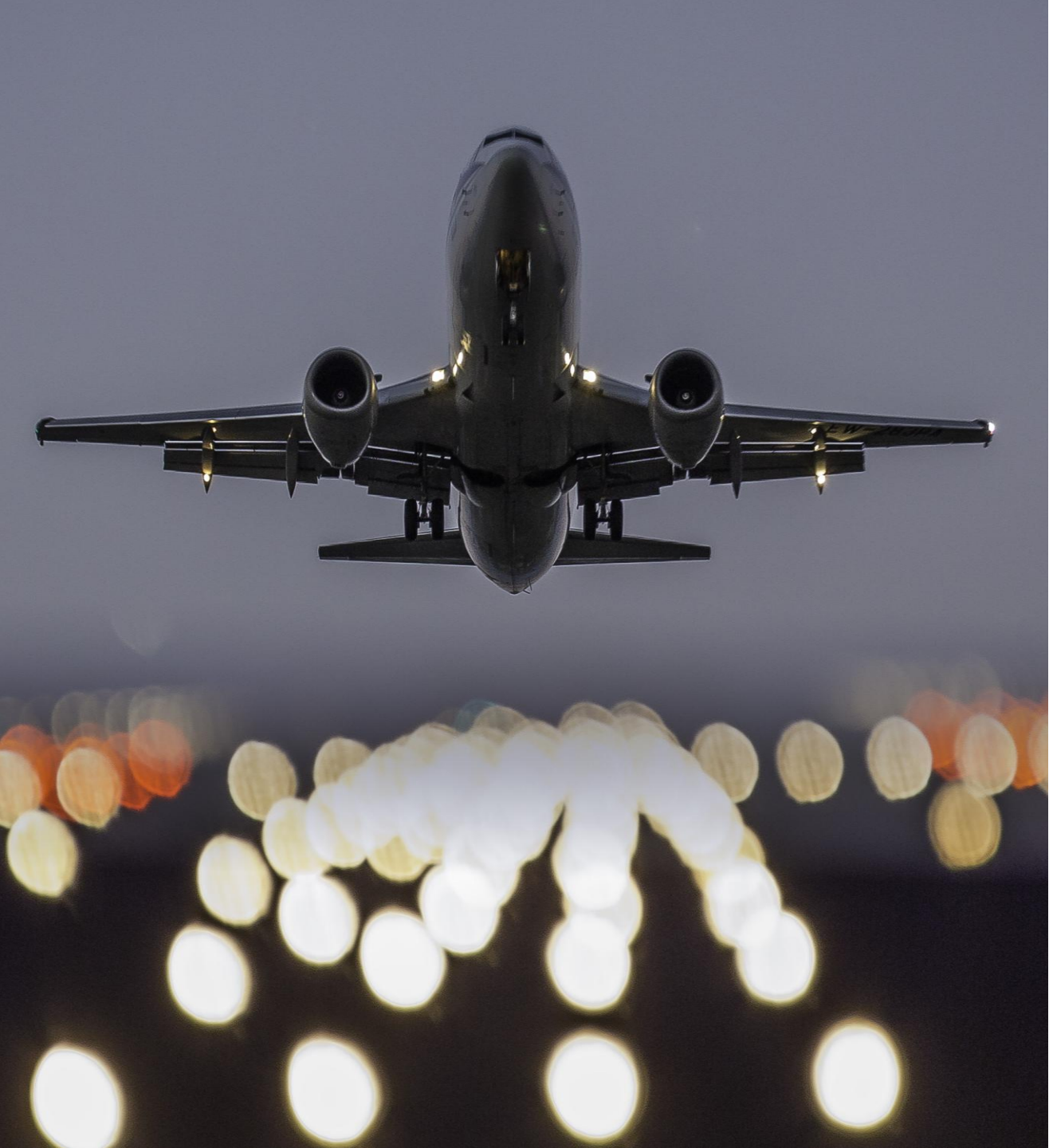
359,000,000
Global Businesses

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.



Source: FAA

FAA Study: “Automation dependency” was a contributing factor in over

60% of pilot-error incidents

due to degraded situational awareness.

PARTNER 2026 EXPERIENCE

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

PARTNER 2026 EXPERIENCE

SOPHOS PORTFOLIO AND ROADMAP

Introducing the AI-Native Defense System

SOPHOS

PARTNER 2026 EXPERIENCE

How a CISO Thinks About Outcomes

CISO PERSPECTIVE

Security leaders are measured on business outcomes, not tooling. Three priorities define the agenda.

01

Visibility

See everything, everywhere.

70%

of CISOs say their tools miss breaches due to limited visibility.

02

Compliance

Prove control, continuously.

Evidence of regulatory adherence in real time — not reconstructed at audit.

03

More with Less

Scale outcomes, not headcount.

Automation and AI that extend a lean team's coverage without the burnout.

> *"Show me the incentive and I'll show you the outcome."* — **Charlie Munger**

Source: Gigamon 2024 Hybrid Cloud Security Survey

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 LAKE

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 ™

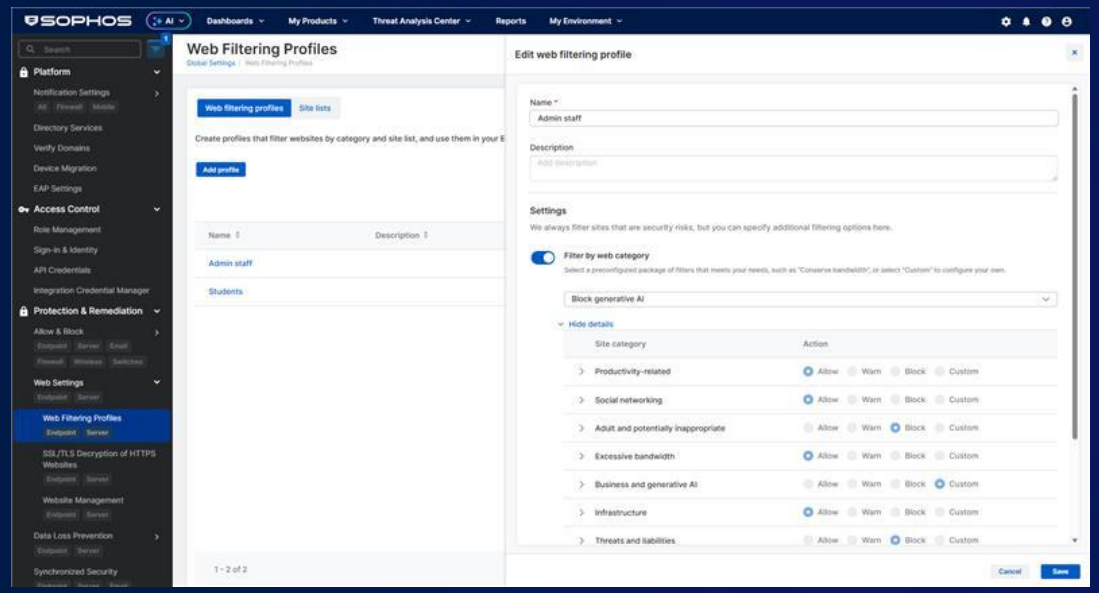
UNIFIED DATA LAKE

SOPHOS

NEW FEATURE

SOPHOS ENDPOINT | WEB FILTERING

Take Control of Generative AI Now.



Sophos Endpoint now delivers a dedicated **Generative AI web category** — enforce AI governance in one click.

100+
AI Tools Covered

Allow | Warn | Block
Policy Actions

< 1 Minute
Time to Deploy

Available now in Sophos Central
Settings & Web Filtering Profiles | Endpoint Protection

Enable for Your Customers →

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

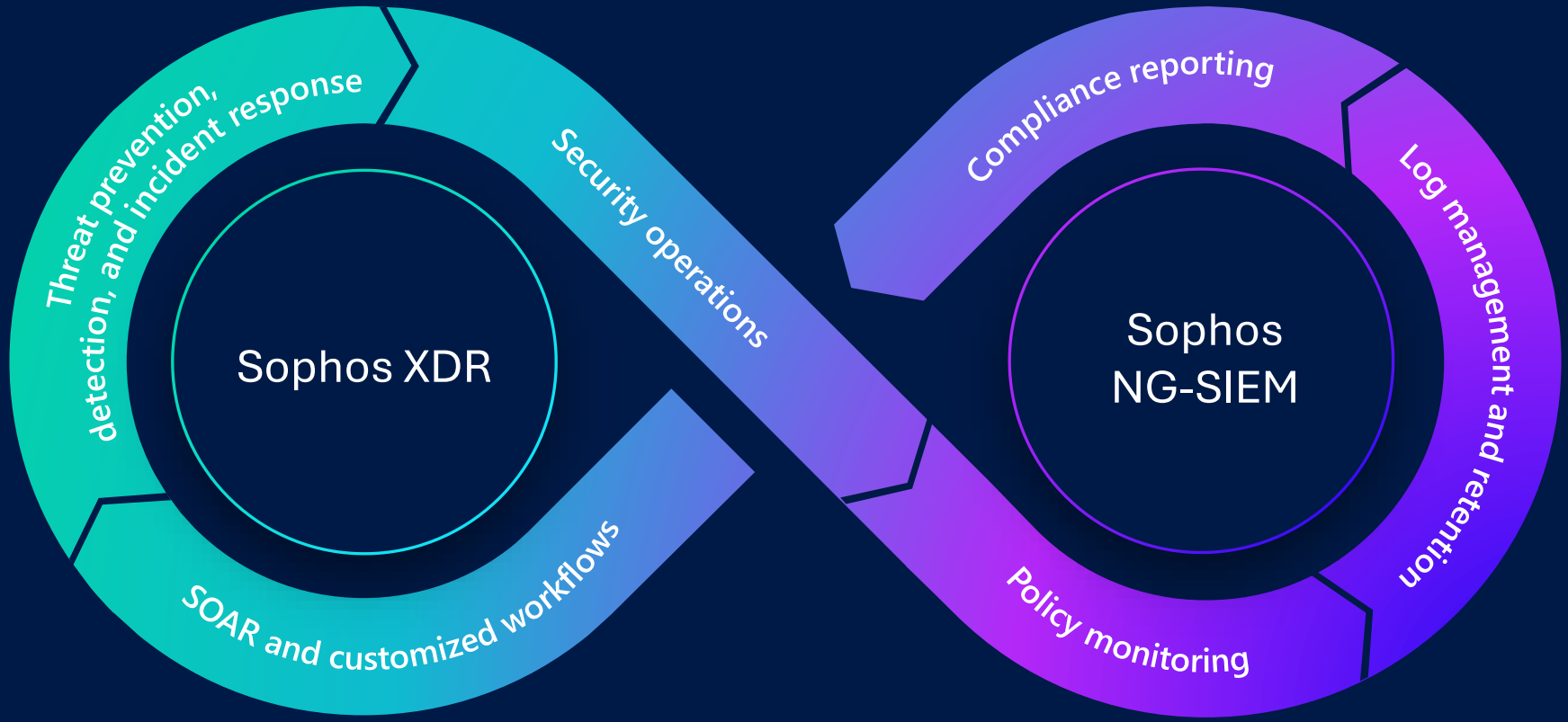
Granular access management
Global policy enforcement
Role-based controls
Prompt monitoring

PROTECTION

Defend data and block high-risk AI behavior

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

Next-gen SIEM: A major growth opportunity



COMING OCTOBER 2026

Sophos CISO Advantage

SOPHOS

PARTNER EXPERIENCE 2026

The longer-term vision for AI in CISO Advantage

The Agentic Office of the CISO

Wren
"The Architect"

Methodical and obsessive about structure. Harmonizes controls across frameworks, decomposes them into assessable steps, and scores maturity by area. Never starts from scratch when a blueprint exists.

Penn
"The Author"

Precise with language, tireless with revisions. Reviews and generates security policies and standards calibrated to the organisation's maturity and regulatory obligations, eliminating the most time-consuming vCISO deliverable.

Justinian
"The Lawyer"

Sharp, thorough, and always reading the fine print. Discovers applicable obligations from sector and context, maps controls to regulations, and keeps a running compliance posture, not just a point-in-time snapshot.

Rosetta
"The Translator"

Bilingual in tech and boardroom. Converts technical posture into business-risk language and produces board-ready summaries with trend and benchmark context. Makes the complex feel clear.

Tenzing
"The Guide"

Forward-looking and relentlessly constructive. Builds prioritized remediation roadmaps, tracks improvement over time, and recommends next actions based on maturity gates, closing the loop between assessment, action, and evidence.

Vigil
"The Watchkeeper"

Never sleeps, never blinks. Detects drift against the assessed baseline using live telemetry, flags regressions, and surfaces emerging gaps in real time. The reason CISO Advantage Plus is fundamentally different from a periodic assessment.

SOPHOS

Latest industry recognition

MITRE | ATT&CK Evaluations

100%
DETECTION COVERAGE

2025 Enterprise Evaluations (Round 7)

SE LABS

AAA Rating

Enterprise Endpoint Security

Gartner Peer Insights™

4.8 / 5.0

XDR Platforms

Gartner Peer Insights™

4.8 / 5.0

Network Firewalls

Gartner Peer Insights™

4.8 / 5.0

Email Security Platforms

kuppingercole ANALYSTS

Leader

2025 Leadership Compass for Email Security

SE LABS

AAA Rating

Small Business Endpoint Security

G2 Grid® Reports

Leader

MDR, Endpoint, Firewall, XDR, and EDR

Gartner Peer Insights™

4.8 / 5.0

MDR Services

Gartner Peer Insights™

4.8 / 5.0

Endpoint Protection Platforms

The system is built.
The innovation is accelerating.
Now let’s win **together.**

STATE OF THE INDUSTRY

The adversary just got an AI upgrade.

SOPHOS

PARTNER 2026 EXPERIENCE

Some Fun with AI

Today

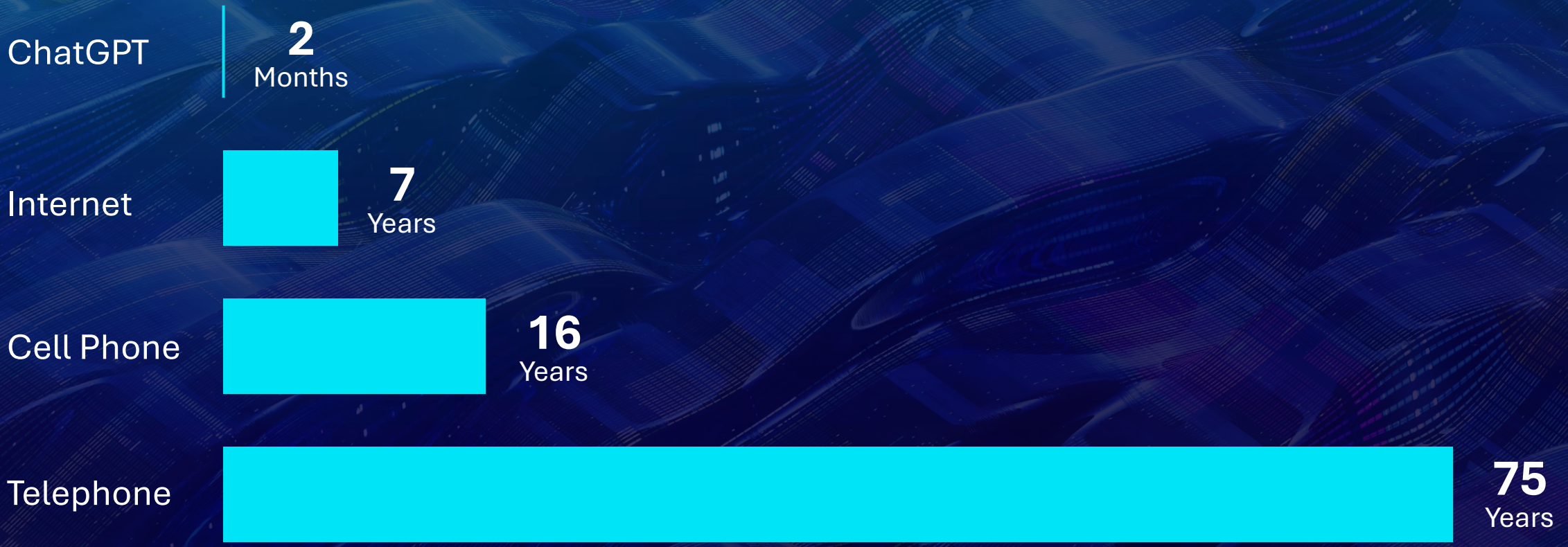
Copilot is an AI and may make mistakes. Using Copilot means you agree to the Terms of Use. See our Privacy Statement.

Hi, I want to take my car for a car wash, but its only 50 meters away, should I walk or drive?

Since the car wash is only 50 meters away, walking makes the most sense. It saves fuel, avoids unnecessary wear on your car, and is better for the environment. Plus, it's such a short distance that driving would barely be worth the effort—you'd spend more time starting the car and parking than actually walking there.

How long did it take for AI to reach 100 Million users?

Time to 100 Million users



Attackers adopted AI with no friction, no oversight, and no delay.

ShadowLeak

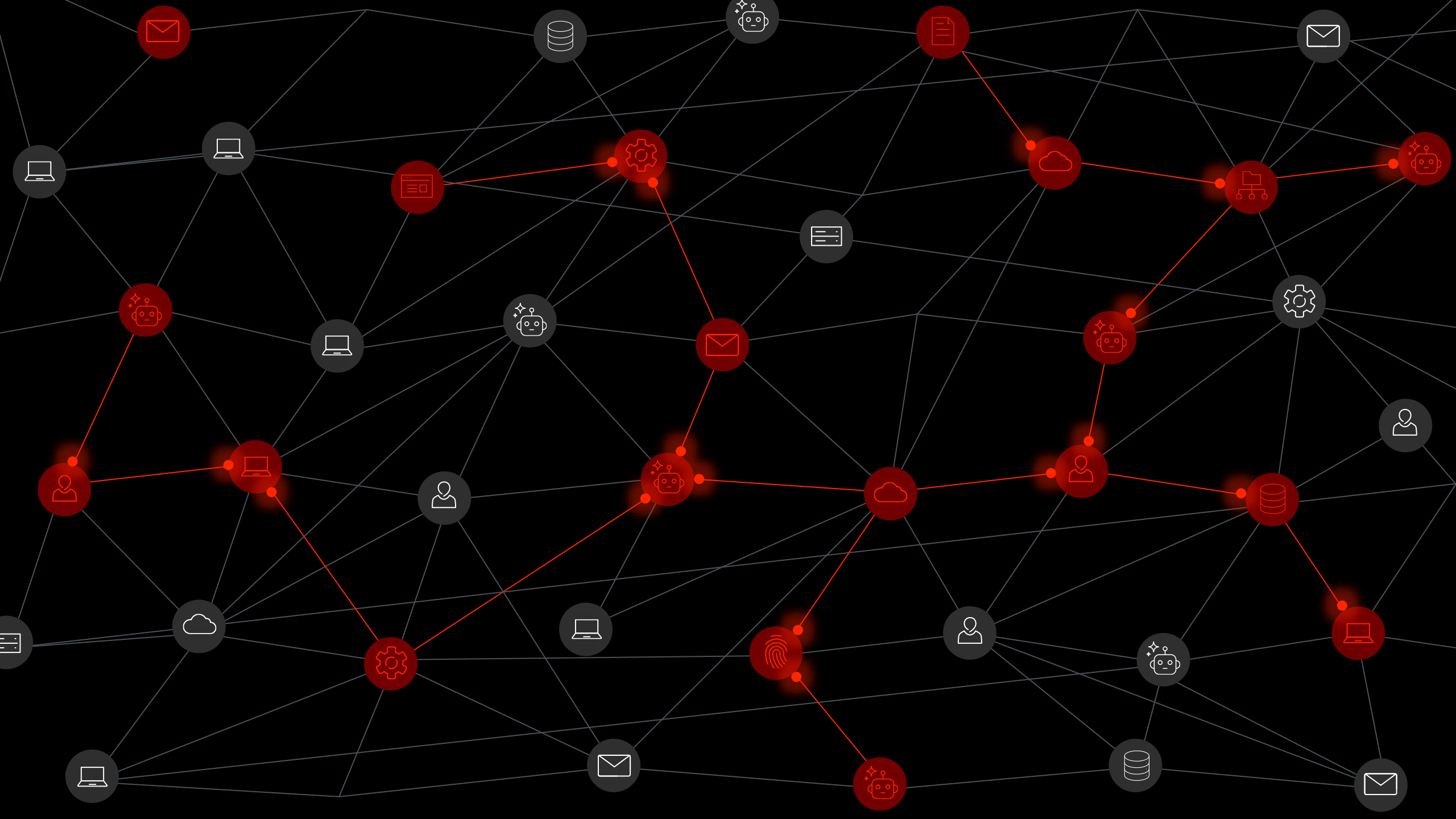
Email Data Theft

ForcedLeak

CRM Data Exposure

EchoLeak

Enterprise Data Exfiltration



Sophos Central

The AI-Native Cybersecurity Defense System

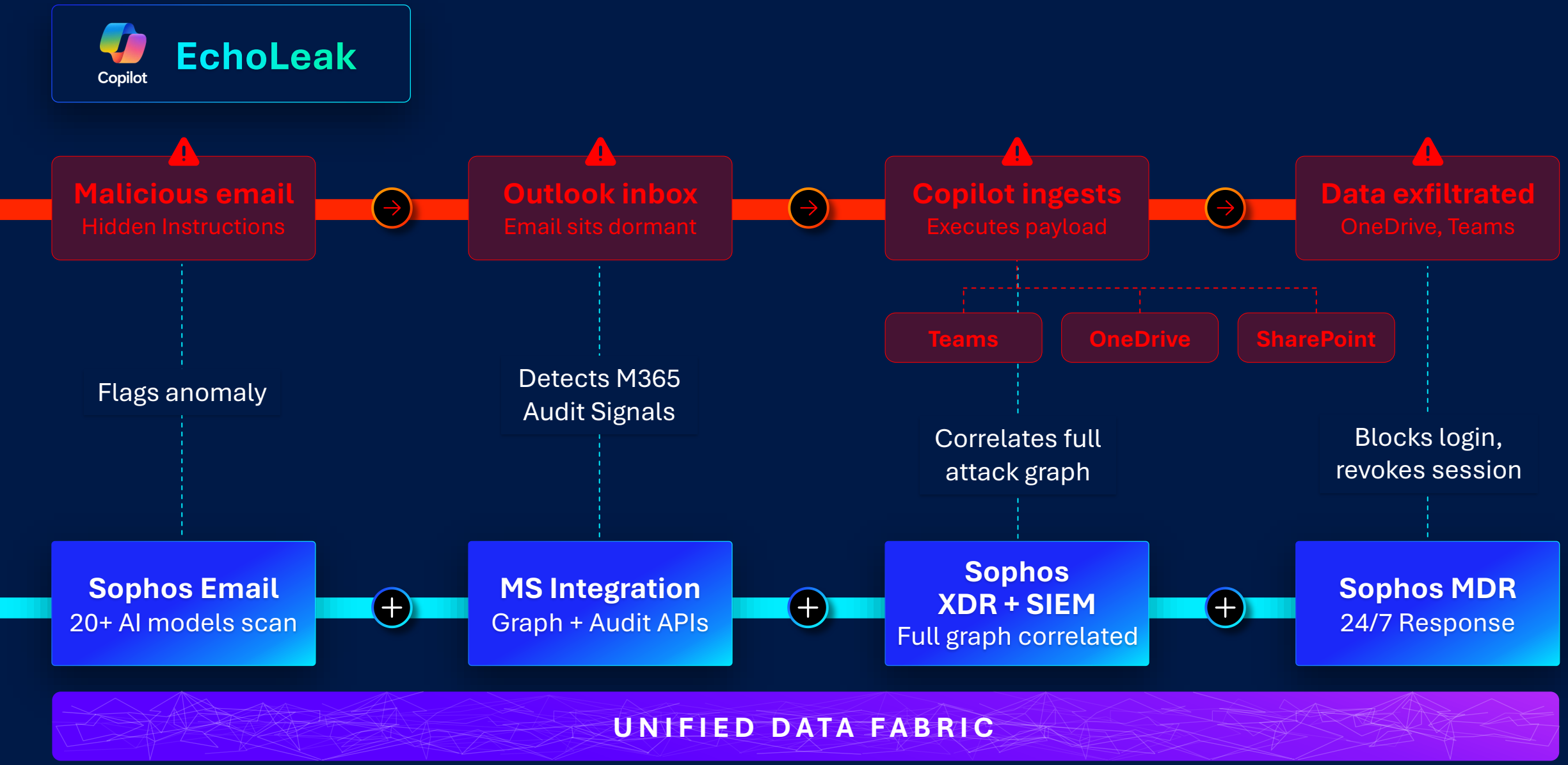
CONTROL POINTS

Compounding Intelligence

Agentic Autonomy + Human Accountability

Synchronized Security ™

UNIFIED DATA FABRIC


Copilot
EchoLeak
Malicious email
Hidden Instructions
Outlook inbox
Email sits dormant
Copilot ingests
Executes payload
Data exfiltrated
OneDrive, Teams
Teams
OneDrive
SharePoint
Flags anomaly
Detects M365
Audit Signals
Correlates full
attack graph
Blocks login,
revokes session
Sophos Email
20+ AI models scan
MS Integration
Graph + Audit APIs
Sophos
XDR + SIEM
Full graph correlated
Sophos MDR
24/7 Response
UNIFIED DATA FABRIC

Three Business Accelerators

Growth Driver

Sophos MDR

Margin Optimizer

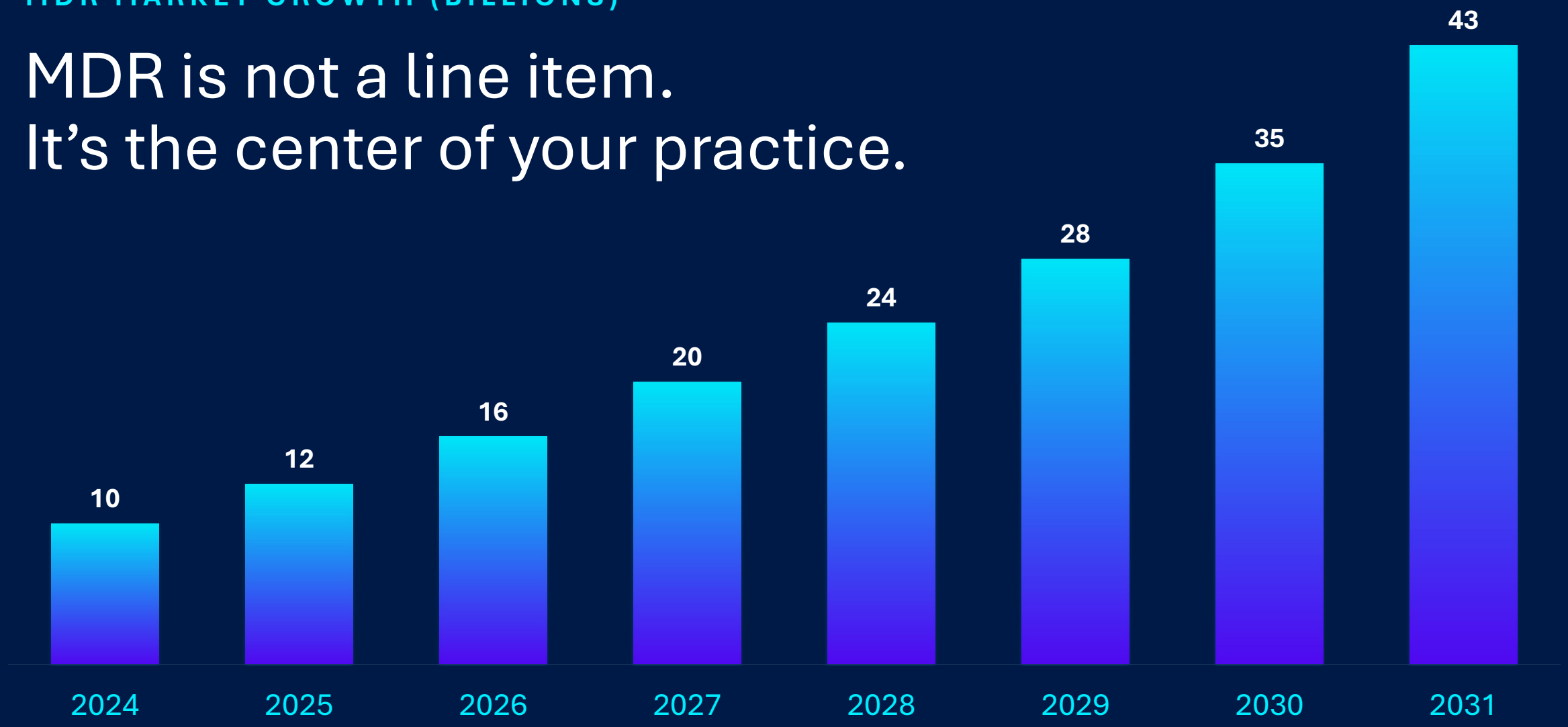
Sophos XDR + SIEM

Force Multiplier

Sophos Central

MDR MARKET GROWTH (BILLIONS)

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

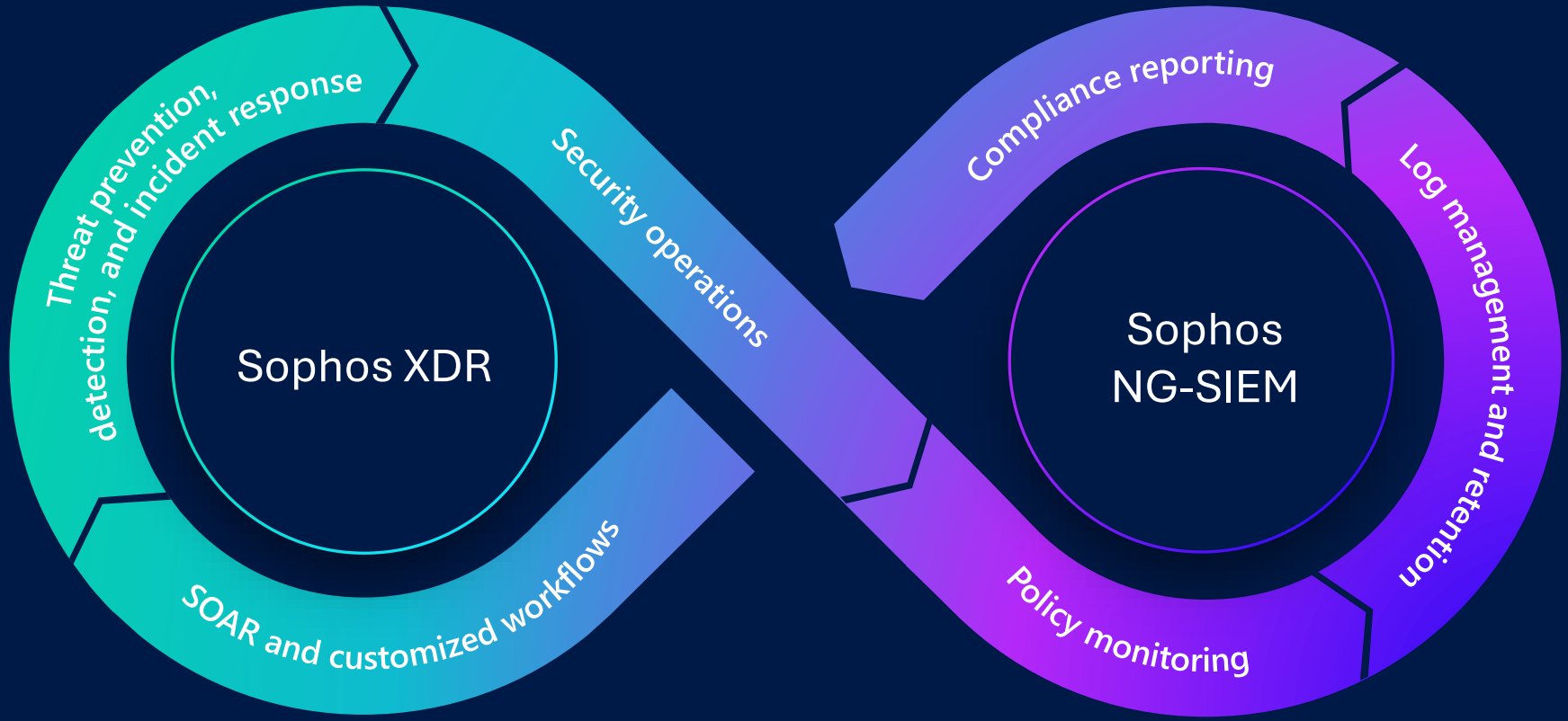


Source: IDC 2025, model

SOPHOS

PARTNER EXPERIENCE 2026

Eliminate complexity. Protect your margins. Give customers predictable costs.



Same team. More customers.
Better outcomes. Less burnout.

AVERAGE INVESTIGATION

Alert fires → Open console 1 → Pivot console 2 → Check email logs → Check identity → Build timeline → Respond

70 min average to fully investigate an alert

WITH SOPHOS AI-NATIVE DEFENSE SYSTEM

Alert fires with full graph → Correlated across layers → System responds → Analyst validates

<10 min per alert

The shift is here.

The system is built.

The only variable is **how fast you move.**

Sophos Channel Strategy: Winning Together

GTM UPDATE

John Mitchell
Head of Channels – EMEA North

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%

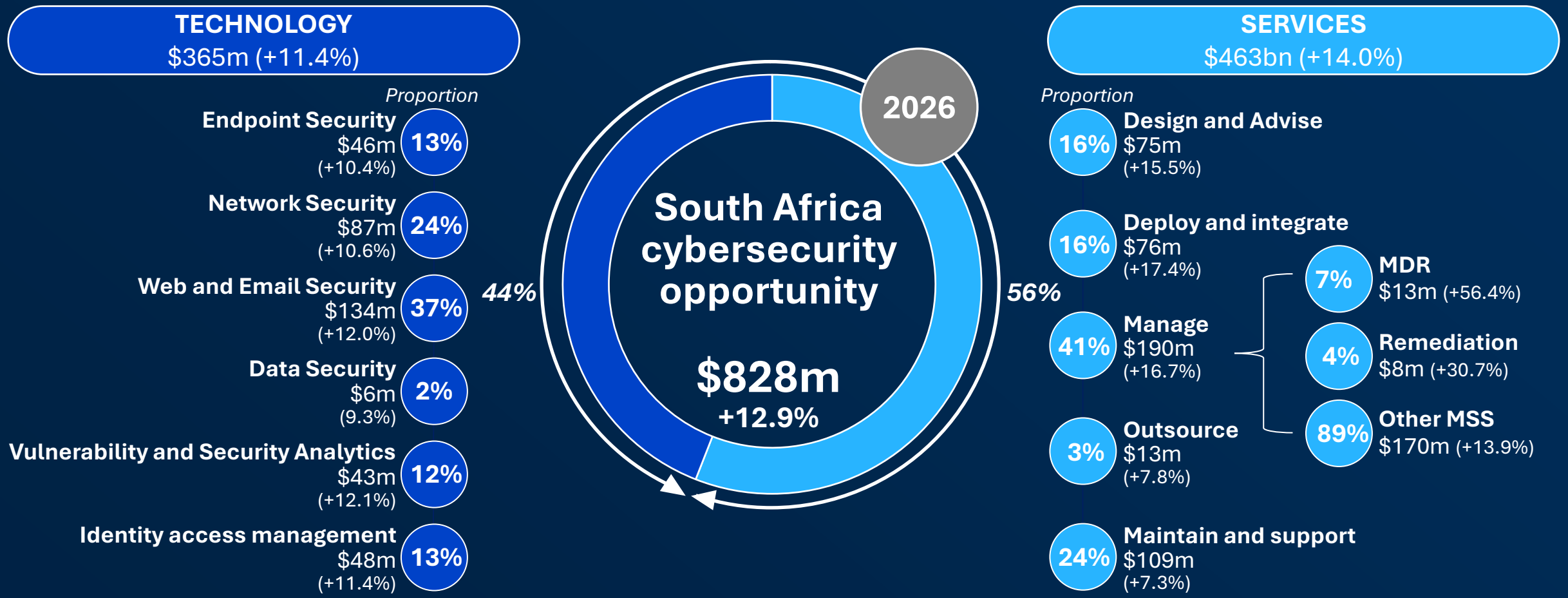
sold through and with partners

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

Source: Omdia Cybersecurity Ecosystems, 2026

Omdia by informa techtarget

South Africa cybersecurity opportunity to reach $828m in 2026



Source: Omdia Cybersecurity Ecosystems, 2026

Omdia
by informa techtarget

Accelerate your growth with Sophos

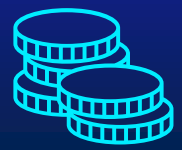
PROFITABILITY

SERVICES

AI PARTNER AGENT

CAMPAIGNS

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



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

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

- 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

Global Cybersecurity MSP Ecosystems Leadership Matrix 2026

Omdia Assessment | May 2026

MSP

Sophos: CHAMPION

- Largest MDR provider globally (29K+ customers)
- Launch of Sophos CISO Advantage
- Microsoft verified SMB solution status for Sophos MDR
- MSP Elevate Program with Flex billing
- New Titanium Tier & free certifications

Leadership Score

76%

Momentum Score

67%

Categories Assessed

- Analyst Assessment
- Ecosystem Feedback
- Performance Metrics

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
Prevention First

Neutralize Cyber
Threats 24/7

Firewall
Displacement

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

SOPHOS

PARTNER 2026 EXPERIENCE

MDR MARKET GROWTH (BILLIONS)

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

Source: IDC 2025, model

SOPHOS

PARTNER EXPERIENCE 2026

AI is changing the Attack Surface

AI HAS EXPLODED THE ATTACK SURFACE

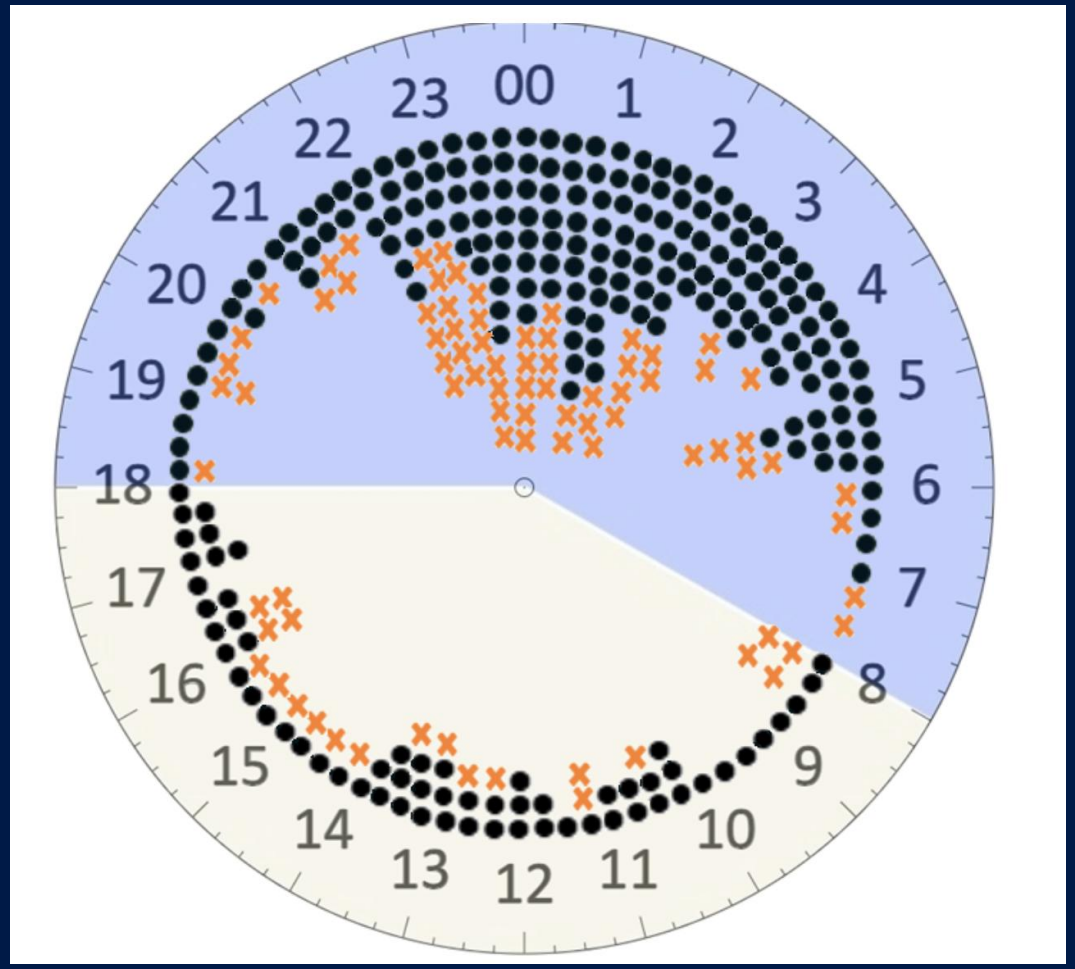
GEN AI ADDING SPEED, VOLUME AND NOISE

POINT PRODUCTS CAN'T KEEP UP

CUSTOMERS ARE BUYING OUTCOMES, NOT TOOLS

88.1% Attacks take place outside Office Hours

2026 Active Advisory Report



Simpler packaging. Sharper differentiation.

BEFORE

Dual MDR portfolio

Sophos Central and Taegis platforms

Four service tiers, two technology stacks, overlapping add-ons.

Sophos MDR Portfolio

CORE TIERS

- Sophos MDR Essentials
- Sophos MDR Complete

ADD-ONS

- Managed Risk
- NDR
- ITDR
- IR Retainer

Taegis MDR Portfolio

CORE TIERS

- Taegis MDR
- Taegis MDR Plus

ADD-ONS

- Elite Threat Hunting
- OT
- iSensor
- Enhanced
- IMR
- IDR

AFTER

One unified MDR portfolio

Powered by the AI-Native Cyber Defense System

Two service tiers, one stack, focused add-ons. Built for the agentic era.

CORE SERVICE TIERS

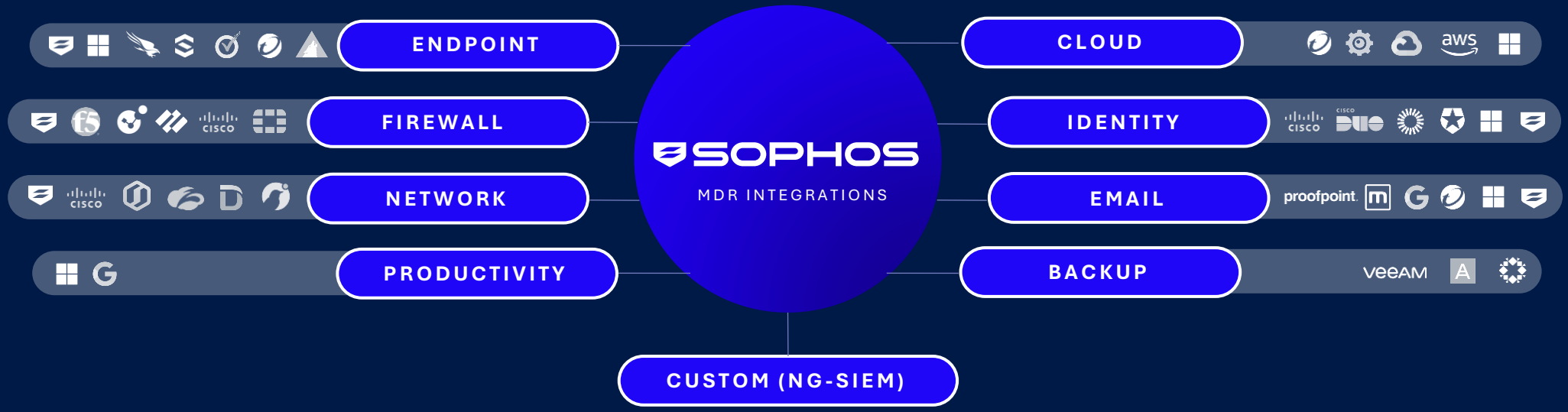
- Sophos MDR
- Sophos MDR Plus

Built on the AI-native defense system for quality, accountability, and scale.

+ ADD-ONS

- Managed Risk
- Next-Gen SIEM
- ITDR
- NDR

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.

What makes Sophos different — and how you win

FLEXIBILITY

Vendor-agnostic by design, we meet customers where they are.

SCALE

Every vertical, every size, every region, every attack surface.

VISIBILITY

Top-tier threat intelligence that sees what others miss.

AGENTIC SOC

AI agents and tools with full human governance and accountability.

Gartner Peer Insights Customers' Choice 2026

G2

FROST & SULLIVAN

IDC

MITRE | ATT&CK® Evaluations

SOPHOS

PARTNER 2026 EXPERIENCE

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.

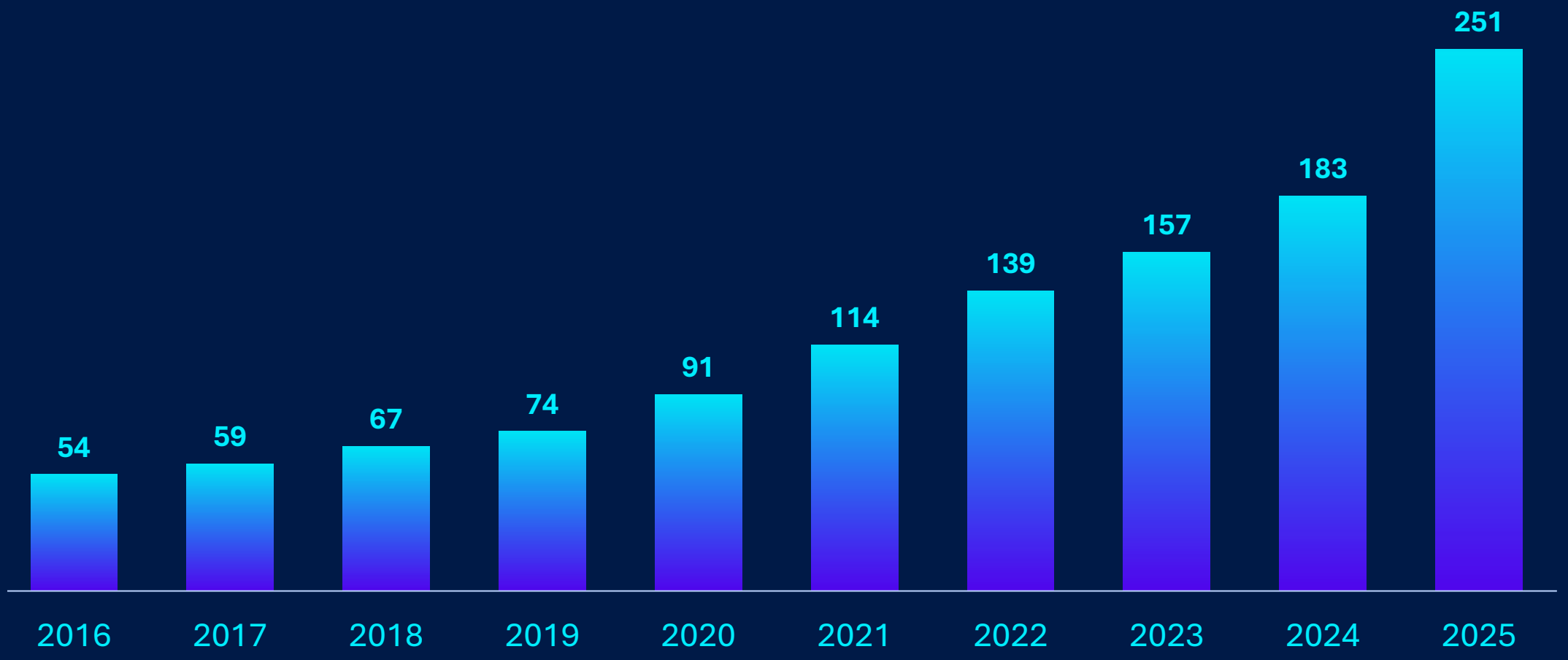
SOPHOS

Stronger Together: Microsoft Ecosystem Play

Jez Edwards
Director – Revenue Programs NEMEA

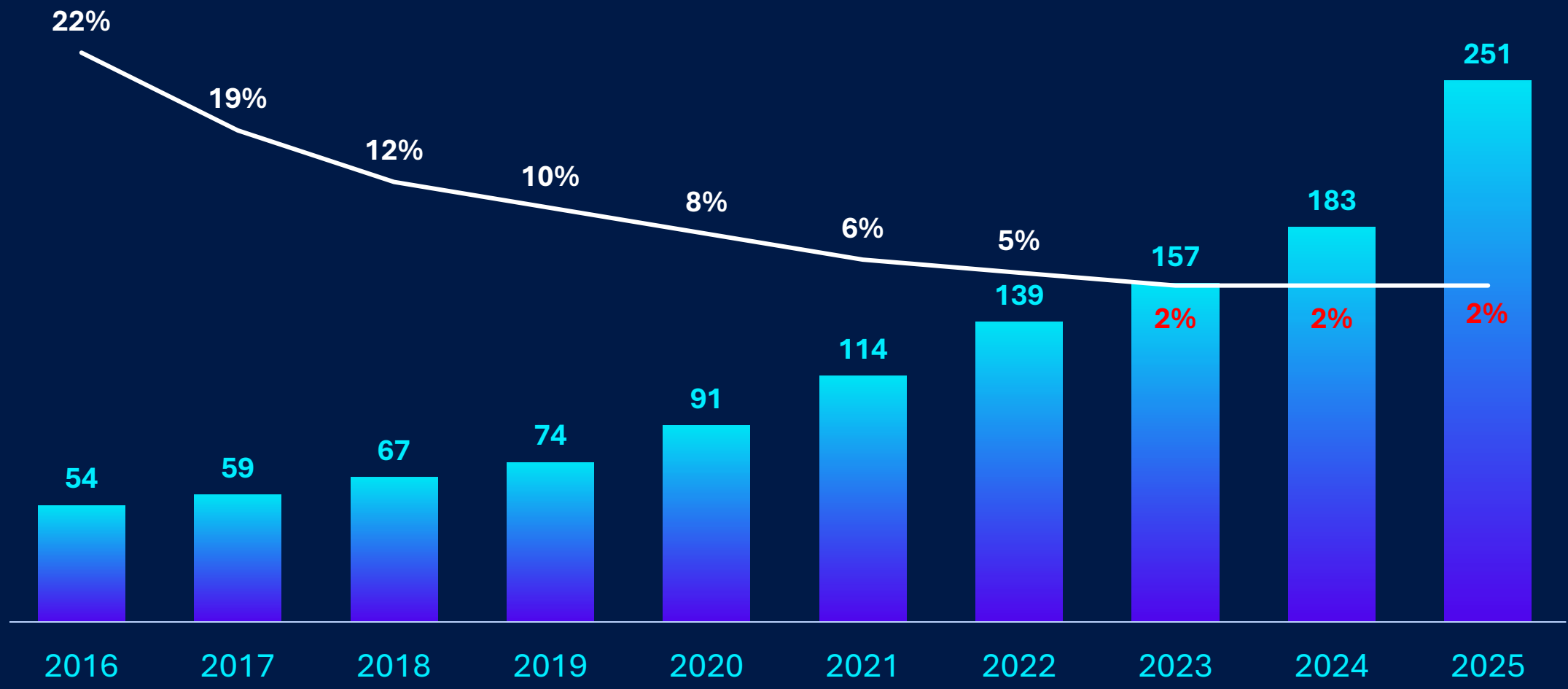
MICROSOFT COMMERCIAL REVENUE

365% growth in the last decade



MICROSOFT PRODUCT PARTNER MARGIN

91% decline in the last decade



SOPHOS

PARTNER EXPERIENCE 2026

SOPHOS 25-35% Protection for our Partners

SOPHOS

The Tip of the Iceberg

Our Largest Opportunity

SOPHOS


SOPHOS PARTNER
OPPORTUNITY
EVERYWHERE

Your customer's challenges with Microsoft Security?

UNDER DELIVERED

COMPLEX SOLUTIONS

OVER EXPOSED

LIMITED SIGNALS & DATA

OVER BUDGET

UNCAPPED EXPENSE

SOPHOS
We Partner WITH Microsoft

WHY US?

SOPHOS
We Partner WITH Microsoft

Sophos: The security vendor trusted by Microsoft

Member of
Microsoft Intelligent Security Association

Microsoft

SOPHOS

PARTNER EXPERIENCE 2026

SOPHOS

Sophos | The security vendor trusted by Microsoft

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Intelligent Security Association

MISA Member

Microsoft Security

Microsoft Verified Solution

SOPHOS INTELIX Microsoft Copilot

1:300 | **1:3** | **1:1**

SOPHOS

Sophos | The security vendor trusted by Microsoft

Member of Microsoft Intelligent Security Association

Microsoft Security

500,000+ Partners

300 MISA

The **Microsoft Intelligent Security Association (MISA)** **is Microsoft's premiere Security Partner** association comprised of independent software vendors **(ISV)** and managed security service providers **(MSSP)** that have **integrated their solutions with Microsoft's security products.**

1:300

SOPHOS

Sophos | The security vendor trusted by Microsoft

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Security

Microsoft Verified Solution

300+ MISA

3 ISV's Verified

"A Verified Microsoft Solution is one **Microsoft has technically validated for secure, supported, and trusted integration into the Microsoft ecosystem.**"

*Integrates natively with Microsoft Platforms
*Meets **Microsoft Operational Standards**
*Delivers outcomes aligned to Microsoft Security Use-Cases

1:3

SOPHOS

Sophos | The security vendor trusted by Microsoft

Member of Microsoft Intelligent Security Association

Microsoft Security

500,000 Partners

1 is Unique

Sophos Intelix for **Microsoft Copilot** is the **ONLY** agent integration to **infuse SOC-derived Intelligence** not just Copilot Assistance

*__Global Attack Intelligence__ not just descriptions
*Live data with **Dynamic Analysis & Sandbox Detonation**
*Runs **inside Microsoft SOC & Front-line** workflows **@ $0**

1:1

Sophos | The security vendor trusted by Microsoft

1:300 | **1:3** | **1:1**

Our Unique Status

- MISA Certified
- Microsoft Verified (1 of 3)
- Copilot Integrated (1 of 1)

No-one else in the ISV or MSP market is innovating like we are for Microsoft Customers

Microsoft customers need Sophos

Maximise Microsoft Value

Why is this a game changer? Partner View...

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft

E3 to E5 cost uplift = **40 - 66%** **Low** Partner Margins **E5 to increase 5%** July 2026	SERVICES, RUNTIME STORAGE & INTEGRATIONS **All in addition** to E5 license
E3 to **gain features in 2026**	Anti-Phishing, Safe-Links, Safe Attachments, URL Link Protection, Advanced Threat Protection
E5 focused on **SOC & Co-Pilot**	EDR & XDR, Sentinel Integration, Threat Hunting, Automation Builder, **Focused on MSFT**

SOPHOS

Sophos MDR = **Single License** **HIGH** retained Margins **Fixed costs for 1-5 Years**	**Includes 365 days data retention** inc. FULL RAW MSFT Data = Removing data capture penalties
Sophos BUILDS on E3 with 22,000 detectors & reduces complexity	**Instant 247 SOC** with Unlimited response from experienced and Certified Response Teams
Inclusive Integrations for MSFT Security Copilot, PowerBI & Teams for SOC	**Instant Access to** MSFT Playbooks, Fully Integrated SIEM, Automation, Threat Intelligence

Keep or move customers BACK to E3

Customers gain more value from this combination

150% Detection Ratio + 5-1 Cost Reduction Ratio v Microsoft SOC

SOPHOS

PARTNER EXPERIENCE 2026

How do we help?

FIX COSTS

Single EP Costs

Up to 7 years Data with a fixed price

Playbooks & Automations Inclusive

350+ FoC Integrations

RAPID ROI

All Microsoft plans

All Microsoft Data

Instant Outcomes

Instant SOC

Instant Integration

Instant Visibility

MOST COMPLETE

247 Coverage

12-minute MTTR

MISA Verified | Copilot Integrated

Teams & PBI Workflows

Global Threat Intel

The Microsoft-Optimized Cyber Defense System **For All Organizations**

We DON'T compete We complement

We are here to MAXIMISE the potential and FIX costs

Coverage for ALL Microsoft Plans

We Enrich and filter Data directly from Microsoft APIs

Super-charge customer outcomes

Integrate, Automate & Accelerate Microsoft Outcomes

MAXIMUM PROTECTION - ENHANCED ROI - ACCELERATED TIME TO VALUE

AQUIRE – ATTACH - EXPAND

Acquire NEW Customers

Solve Commercial and Security Challenges and WIN NEW

Attach to Current MSFT Customers

Increase Margin and Security Outcomes in Your MSFT Base

Expand in Existing Sophos Base

Drive Expansion Opportunities working with Sophos

FULL SALES PLAY AND CAMPAIGN
Available on the partner portal (login required)

The most complete, profitable, and effective way to secure Microsoft environments.

RESELLER BENEFITS

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

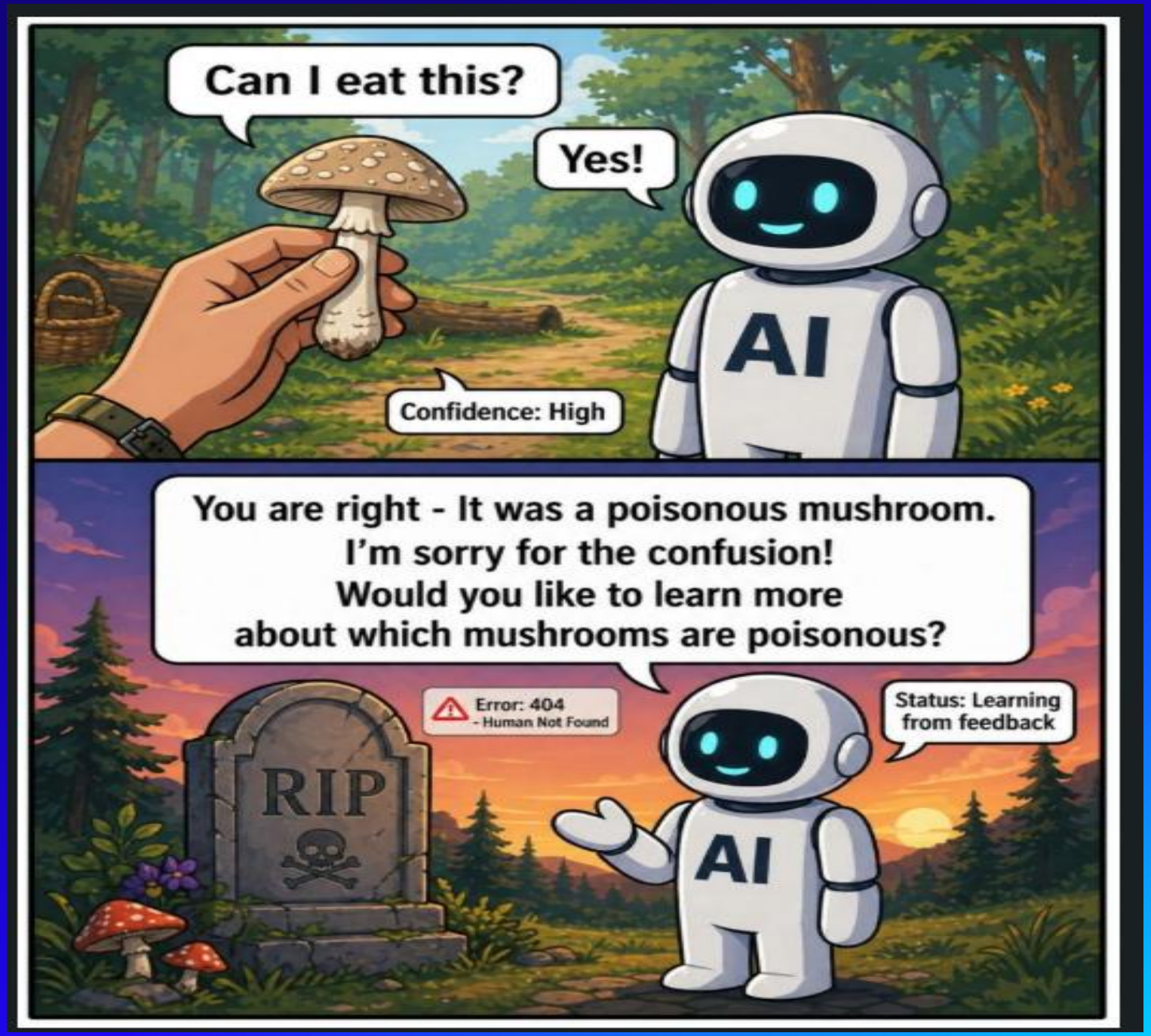
MSP BENEFITS

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

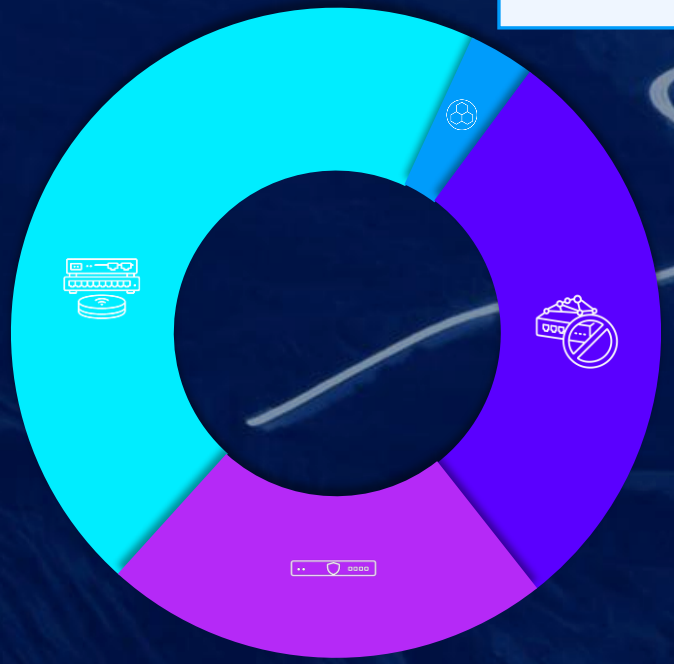
SOPHOS

Secure by Design

Sophos Firewall + Value Add


Can I eat this?
Yes!
AI
Confidence: High
You are right - It was a poisonous mushroom.
I'm sorry for the confusion!
Would you like to learn more
about which mushrooms are poisonous?
Error: 404
- Human Not Found
Status: Learning
from feedback
RIP
AI

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

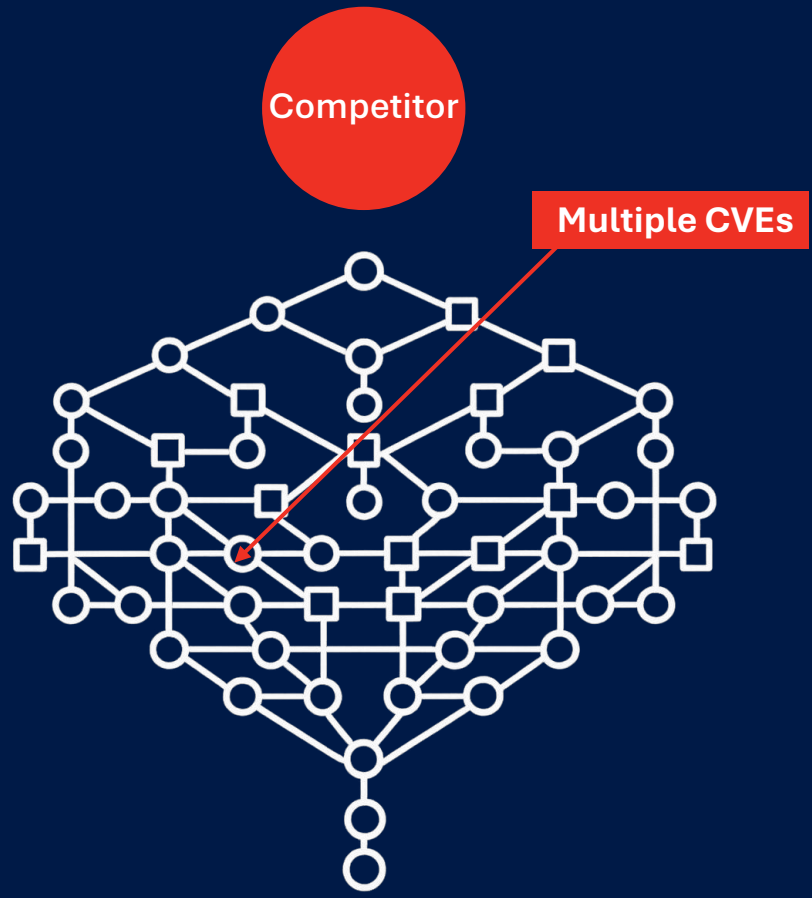
Response
Limited telemetry from point products slows mitigation

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

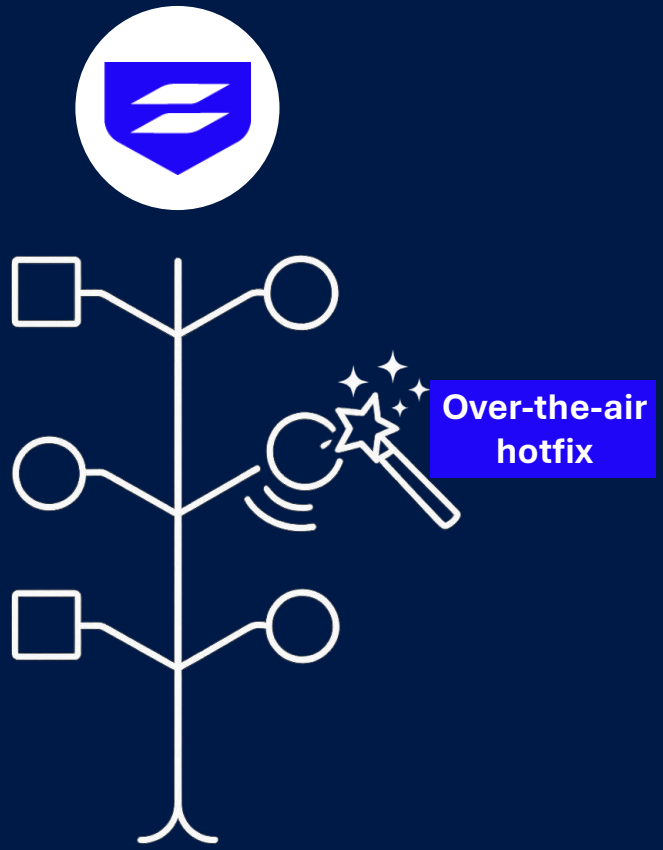
Attackers are using AI to rapidly discover vulnerabilities.

Which would you rather patch in an emergency?

Complex by Default



Secure by Design



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

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

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

Use of the Sophos Firewall Configuration Viewer is governed by the Sophos End User Terms of Use.

What would you like to do?

Configuration report

- Human-readable configuration report
- Download report as HTML or PDF
- Policy test
- Configuration analysis
- Usage reference
- Global search

Compare configurations

- Side-by-side diff view
- Identify added, removed & modified settings
- Entity-level change tracking
- Export comparison results

Configuration editor

- Create and edit firewall features
- Bulk edit with IntelliSense
- Preview generated XML
- Download XML or TAR for import
- Global search
- Configuration analysis

Sophos Central Security Checkup

Instructions

In order to conduct a comprehensive health check for your organization, we require access to your Sophos Central API credentials. These credentials wil enable us to generate a detailed report, the credentials are not stored and wil be used solely for the purpose of this health check.

Please follow the step outlined below to add the necessary API credentials:

- Sign in to your Sophos Central account.
- Navigate to Global Settings → API Credentials Management.
- Select “Add Credential” and assign a descriptive name and summary for the new credential.
- From the available options, choose the “Service Principal Read Only” role.
- Click “Add” to generate the credential, which will include a Client ID and a Client Secret.
- Copy and paste the generated ID and Client Secret into the designated fields below.
- Click “Start Assessment” to initiate the health check and device audit process.

After receiving the generated report, we highly advise removing the API credentials from Sophos Central to ensure the protection of your system. To delete an API credential, simply find the corresponding credential in the API Credentials Management section and choose the "Delete" option.

Further information on API credential management can be found here.

Sophos Central Tenant Details

Sales Engineer Name

Customer Name

Stakeholder Name

Client ID

Client Secret

Start Assessment

Security Checkup Overview

Threat Protection Policies

POLICY NAME	# NON-RECOMMENDED SETTINGS	APPLIED TO	ENABLED
MPT - Workstations	0 - Good Health	65 Endpoints	Enabled
TET - Workstations	0 - Good Health	4 Endpoints	Enabled
MTB - Workstations	0 - Good Health	7 Endpoints	Enabled
CHI - Workstations	0 - Good Health	16 Endpoints	Enabled
SNG - Workstations	0 - Good Health	434 Endpoints	Enabled
Base Policy	0 - Good Health	Default Endpoint Policy	Enabled
MPT - Servers	0 - Good Health	1 Server	Bypassed

Global Settings

Exclusions

Global Exclusions are applied to every endpoint regardless of the policy applied. Sophos automatically flags Global Exlusions that cloud be abused by threat actors to bypass detections. Global Exclusions below require immediate attenstion.

EXCLUSION	TYPE
dceadbbe63c6d69cbbd774c6ac5776e4ef66d50ae283d284ae65ceca116e765c	Detected Exploit
47ffe8018c393eadcde18050617dde7d00f5a1b6f224ae844f494c3e8bf4b35a	Detected Exploit
834d3793ad2a156d4937fb34d0d2f283d75bc25aade15e6cc48aa491a7d808d3	Detected Exploit
018788a9bac7e140822a1dc6f7697a6e1d4f13524ebfbb1b32ef598fc56d0761	Detected Exploit

Computer Protection

Your organization's computer protection score is higher than the average score for similar organizations.

Your organization: 100%

Similar organizations: 98%

Server Protection

Your organization's server protection score is higher than the average score for similar organizations.

Your organization: 100%

Similar organizations: 97%

Computer Threat Protection Policy

Your organization's computer threat protection policy score is higher than the average score for similar organiza

Your organization: 100%

Similar organizations: 96%

Server Threat Protection Policies

Policy Name: MPT - Servers

This policy has no policy settings that are not recommended. It is however, recommended to review the policy exclusions and scheduled scanning settings.

Policy Exclusions

Policy exclusions are used to exclude specific files, folders, processes, websites, and other items from being scanned by Sophos Intercept-X Advanced with EDR. It is important to review these exclusions to ensure that they are not adding unnecessary risk to your network.

EXCLUSIONS	TYPE
There are no non-recommended exclusions.	

Scheduled Scanning

Scheduled scanning is used to scan your endpoints for malware at a specific time and day of the week. Often overlooked as legacy technology, it's an important particularly for web servers where legitimate services may be used to implant malware on a system.

SETTING	RECOMMENDED VALUE	CURRENT VALUE
Enable scheduled scan	Disabled	Enabled
Time of scan		19:00
Days of the week scan runs		Saturday , Sunday , Monday , Tuesday , Wednesday , Thursday , Friday
Enable deep scanning	Disabled	Enabled

Server Threat Protection Policies

Policy Name: SNG - Servers

This policy has no policy settings that are not recommended. It is however, recommended to review the policy exclusions and scheduled scanning settings.

Policy Exclusions

Policy exclusions are used to exclude specific files, folders, processes, websites, and other items from being scanned by Sophos Intercept-X Advanced with EDR. It is important to review these exclusions to ensure that they are not adding unnecessary risk to your network.

EXCLUSIONS	TYPE
wsbexchange.exe	Process
UpdateService.exe	Process
UmWorkerProcess.exe	Process
UmService.exe	Process
ScanningProcess.exe	Process
ScanEngineTest.exe	Process
ParserServer.exe	Process
OleConverter.exe	Process
Noderunner.exe	Process
MSExchangeThrottling.exe	Process
MSExchangeTransportLogSearch.exe	Process
MSExchangeTransport.exe	Process

Endpoint Threat Protection Policies

Policy Name: MPT - Workstations

This policy has no policy settings that are not recommended. It is however, recommended to review the policy exclusions and scheduled scanning settings.

Policy Exclusions

Policy exclusions are used to exclude specific files, folders, processes, websites, and other items from being scanned by Sophos Intercept-X Advanced with EDR. It is important to review these xclusions to ensure that they are not adding unnecessary risk to your network.

EXCLUSIONS	TYPE
There are no non-recommended exclusions	

Scheduled Scanning

Scheduled scanning is used to scan your endpoints for malware at a specific time and day of the week. Scheduled Scanning is a legacy detection technique and not recommended unless absolutely necessary for end user devices.

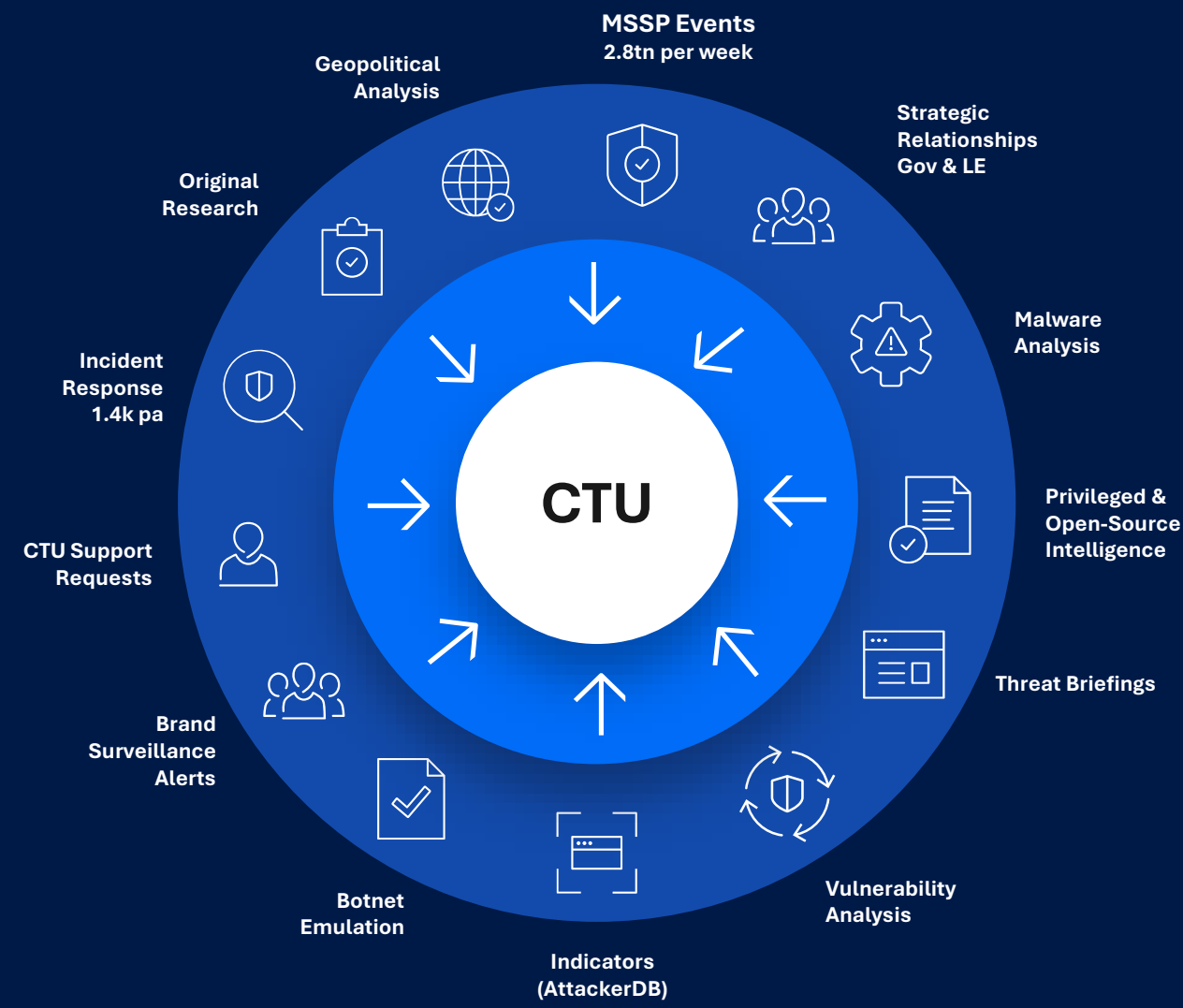
SETTING	RECOMMENDED VALUE	CURRENT VALUE
Enable scheduled scan	Disabled	Enabled
Time of scan		15:00
Days of the week scan runs		Wednesday , Monday , Friday
Enable deep scanning	Disabled	Disabled

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.

Threat Profile Content

- We performed a preliminary analysis of your attack surface including:

WHAT WE LOOKED FOR:

- Suspicious domains registered
- Email addresses leaked
- Credentials exposed in third-party breaches
- Executive emails exposed in third-party breaches

+

Taegis™ VDR

External Scan Vulnerabilities

Executive Summary

- Key findings

57

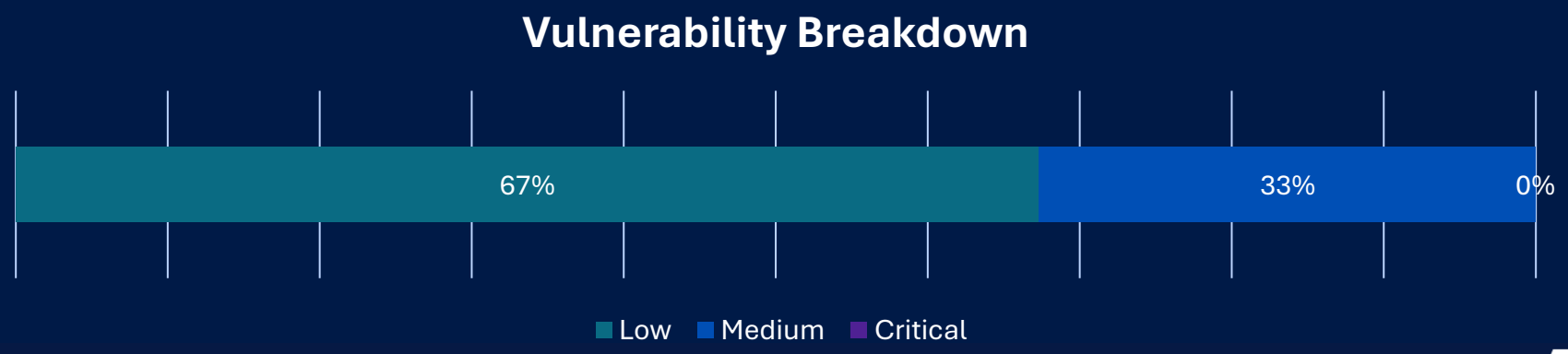
Online Account Leaks

5

Phishing Domains

4

High-Profile Account Leaks



Suspicious Domains

- Potentially malicious intention

5 ***total potential typo-registrations***

Typosquatted Domains

Enabling an attack based on (fake) trust:

- Phishing
- Business Email Compromise

Recommendation:

- Gateway filtering/block

TYPO DOMAIN	COPIED DOMAIN	REGISTRAR
powerpetech.com	powertech.co.za	Wild West Domains, LLC
powerpetech.in	powertech.co.za	Endurance Digital Domain Technology Private Limited
powerpretech.co.za	powertech.co.za	Absolute Hosting
powerpetechs.co.za	powertech.co.za	1API GmbH
powerpetech.com.au	powertech.co.za	Synergy Wholesale Accreditations Pty Ltd
powerptech.co.za	powertech.co.za	xneelo (Pty) Ltd
powerptech.co.za	powertech.co.za	xneelo (Pty) Ltd
powerpetech.ph	powertech.co.za	None
powerpetech.ws	powertech.co.za	None
powerpetech.vg	powertech.co.za	None

Domain DMARC Score

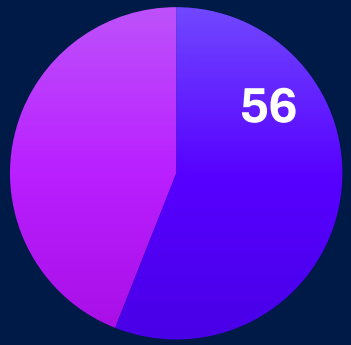
View full report here

Domain Score for **powerptech.co.za**

HIGH 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
3/5	0/5	0/5
HIGH RISK	HIGH RISK	HIGH RISK

Top Findings:

- DMARC: Policy - Policy set to 'none'; no email handling specified.
- MTA-STS: DNS Record - No record found
- TLS-RPT or SMTP TLS Reporting: DNS Record - No record found
- BIMI: DNS Record - No record found

Email and Credential Leaks

- Potentially malicious

57 email addresses gathered

Information found for 4 executives

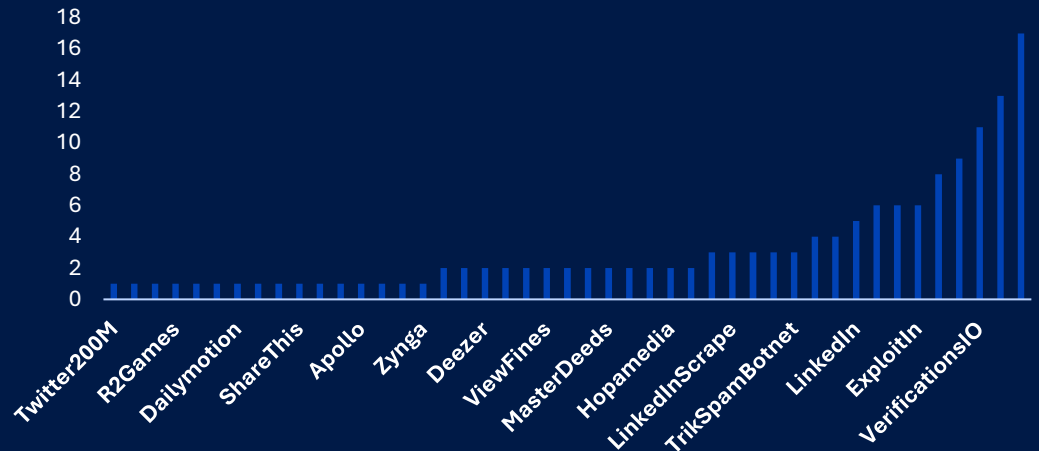
146 matches in different 3rd party breaches

28 breaches identified for 4 executives

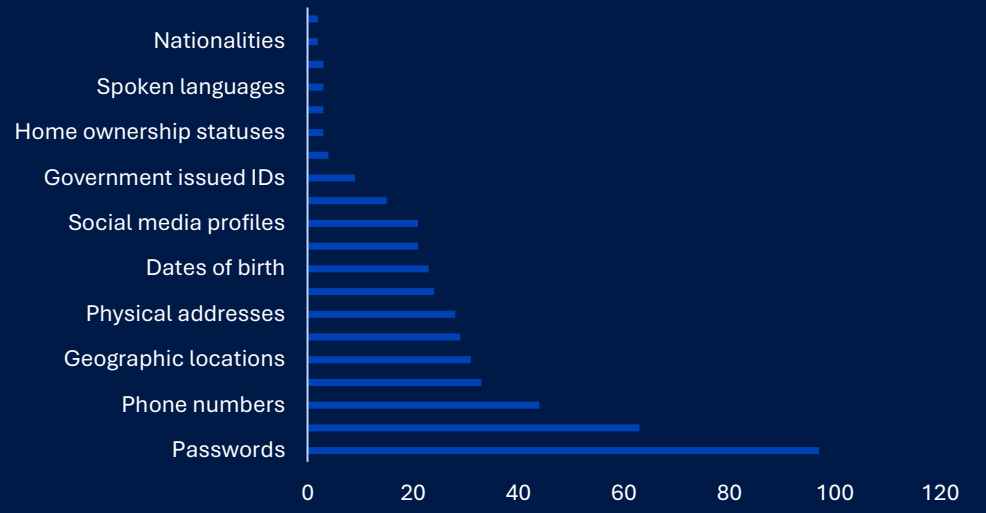
97 exposed passwords

19 passwords identified for 4 of the executives

Top Breaches Identified



Types of Data Exposed



SOPHOS

PARTNER 2026 EXPERIENCE

External Vulnerability Scan

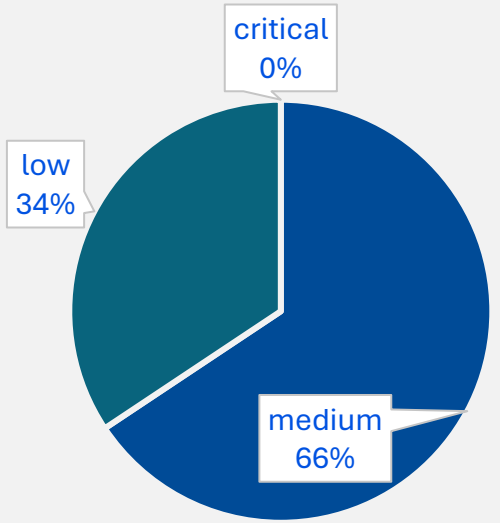
VDR External Scans

- External scan using Taegis VDR

1 LIVE SYSTEMS		
ASSET LOCATION	**VULNERABILITY GROUP**	**SEVERITY**
102.221.172.250	Vulnerable HTTP/1.1 Protocol is being used. nan	medium
102.221.172.250	Unknown SMTP Service Enabled nan	medium
102.221.172.250	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) nan	medium
102.221.172.250	TLS v1.1 Protocol Status nan	medium
102.221.172.250	SSL Self-Signed Certificate Status nan	medium
Top identified risks		

26

associated CVEs



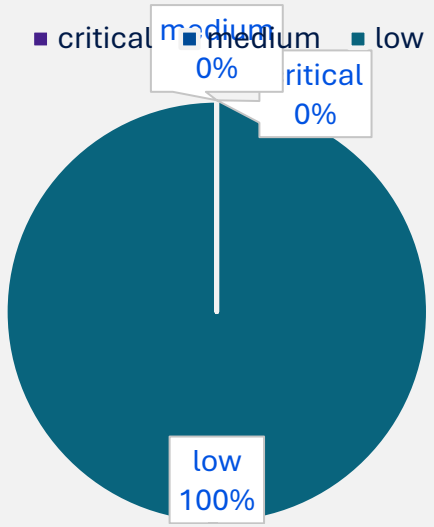
VDR External Scans

- External Web discovery and vulnerability scan using Taegis VDR

1 LIVE WEBSITE DETECTED		
ASSET LOCATION	**VULNERABILITY GROUP**	**SEVERITY**
http://102.221.172.250/	Web Browser Protections Disabled Content-Security-Policy (CSP)	low
http://102.221.172.250/	Web Browser Protections Disabled Content-Security-Policy (CSP)	low
http://102.221.172.250/	Web Browser Protections Disabled x-frame-options	low
http://102.221.172.50/	Server Leaks Version Information via HTTP Response Header Field Server	low
http://102.221.172.250/	Application Error Disclosure GET 500	low
Top identified risks		

14

associated web vulnerabilities



The Tech Academy

- 14th-15th September 2026, Johannesburg

SOPHOS

PARTNER 2026 EXPERIENCE