

SOPHOS MDR

24/7 Cybersecurity with Ransomware and
Breach Prevention

Stelios Gerardis

Sales Manager NSS

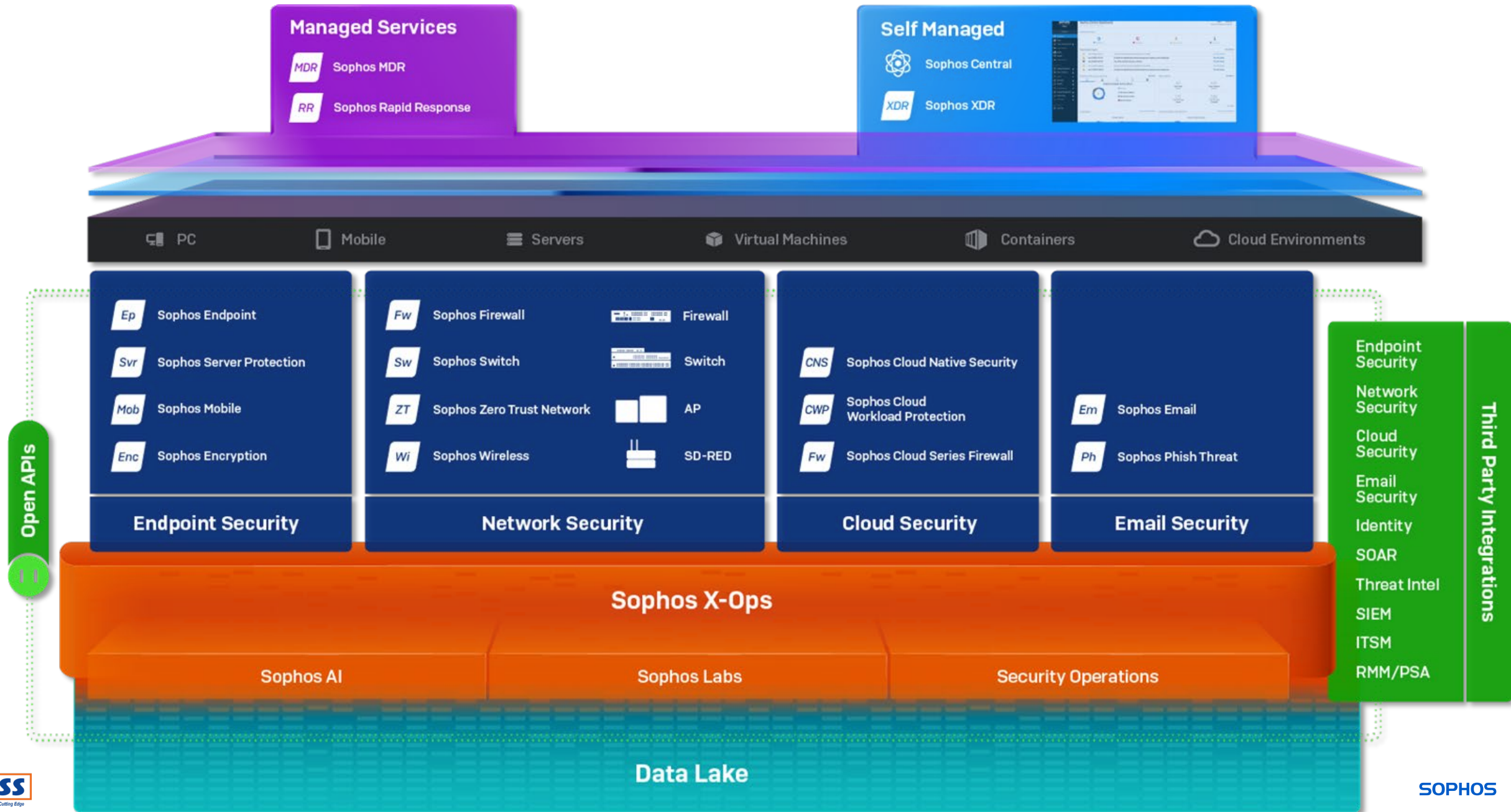
April 2024



SOPHOS

CYBERSECURITY IS SO COMPLEX,
SO DIFFICULT, AND MOVES SO FAST
THAT MOST ORGANIZATIONS
SIMPLY CAN'T MANAGE IT EFFECTIVELY
ON THEIR OWN.

Adaptive Cybersecurity Ecosystem



The Cybersecurity Challenge

Cybersecurity is so complex, so difficult, and moves so fast that most organizations simply can't manage it effectively on their own.

Cyberthreats Are Accelerating in Volume and Sophistication



- 57% of organizations report an increase in the number of attacks over the past year¹
- **78% increase** in the number of organizations hit by ransomware last year¹
- “It’s nearly impossible for organizations to outrun threat actors and keep themselves, their customers, and employees safe” – IDG

Cybersecurity Tools Are Overwhelmingly Costly and Complex



- The average organization has more than **46 cybersecurity monitoring tools** in place
- Most sec ops teams are **drowning in alerts**
- The average organization spends \$7.5K on cybersecurity per employee²

Hiring and Retaining Cybersecurity Experts Has Become Fiercely Competitive



- The number of unfilled cybersecurity jobs worldwide **grew 350%** between 2013 and 2021
- In the US there are 1 million cybersecurity workers and **750,000 cybersecurity openings**
- Security Analysts cost \$100-150K per year, and the annual cost to maintain a SOC is \$2.86M³

¹The State of Ransomware 2024, Sophos; The Active Adversary Playbook 2024, Sophos

²Statista: <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

³Ponemon Institute: "The Economics of Security Operations Centers: What Is the True Cost for Effective Results?"

The Solution: Cybersecurity as a Service

MANAGED DETECTION AND RESPONSE

**Superior security outcomes
delivered as a service**

The diagram consists of three overlapping white circles on a blue background. The top circle is labeled 'People' and contains an icon of three stylized human figures. The bottom-left circle is labeled 'Process' and contains an icon of a stack of three horizontal lines. The bottom-right circle is labeled 'Technology' and contains an icon of a microchip. In the center, where all three circles overlap, is a shield-shaped icon with a white 'S' on a blue background.

- ✓ **Instant Security Operations Center (SOC)**
- ✓ **24/7 Threat Detection and Response**
- ✓ **Expert-Led Threat Hunting**
- ✓ **Full-Scale Incident Response Capabilities**
- ✓ **Superior Cybersecurity Outcomes**

Superior Outcomes with Cybersecurity as a Service

LESS RISK

GREATER EFFICIENCY

LOWER COSTS

85% Reduction in incidents that require investigation

2X More efficient IT Teams

5X Less expensive than managing in-house



Sports and Hospitality
400 Employees

"We can't stop everything that comes in, that's why we rely on Sophos."



Education
20,000 Employees

"We've managed to free up significant operational hours that have allowed our teams to focus on initiatives that have increased student satisfaction."

DETMOLD GROUP

Manufacturing
3,000 Employees

"Sophos provides the equivalent coverage and workload of six full time staff for the cost of less than one."



Manufacturing
200 Employees

Sophos Identified and neutralized a Cuba ransomware attack, preventing data exfiltration and extortion.

IPSA
Independent Parliamentary Standards Authority

Government
70 Employees

"It frees us up to do more interesting and more development-style work rather than just day-to-day security."



Supermarket Chain
13,000 Employees

With Sophos, our IT team saves 4-6 hours/day and used that extra time to reduce attack surface and up-skill staff.

Sophos MDR Is the Best of Both Worlds

BRING-YOUR-OWN-TECHNOLOGY MDR

Provides MDR services using the customer's existing cybersecurity tools

- ✔ Can collect security data from multiple sources
- ⚠ Limited ability to perform manual response actions
- ⚠ Typically provide "guidance" only, leaving customer to implement

Representative vendors



SINGLE VENDOR MDR

Provides MDR services as an overlay on top of vendor's own cybersecurity tools

- ✔ Cybersecurity tools and MDR services are integrated
- ⚠ Requires customer to rip and replace existing cybersecurity tools
- ⚠ Limited to actions that can be taken by the one set of cybersecurity tools

Representative vendors



Sophos MDR

The only service that combines the strengths of both delivery models

- No need to replace existing cybersecurity tools
- Delivered using our integrated tools, third-party tools, or any combination of the two
- Customized service levels from detailed notification to full-scale incident response

The Sophos Advantage: MDR and Cybersecurity

More than 20,000 organizations trust Sophos for MDR which is more than any other vendor



Sophos defends more than **600,000 organizations** and more than **100 million users** worldwide



No vendor has been **named a Gartner Leader** in endpoint security more times than Sophos



The **highest rated** and **most reviewed** MDR Service on Gartner Peer Insights

Why?



Broad Portfolio of Leading Next-Gen Products



Adaptive Cybersecurity Ecosystem



Sophos Central



AI and Automation



Sophos X-Ops Research



A Proven, Trusted and Leading MDR Provider

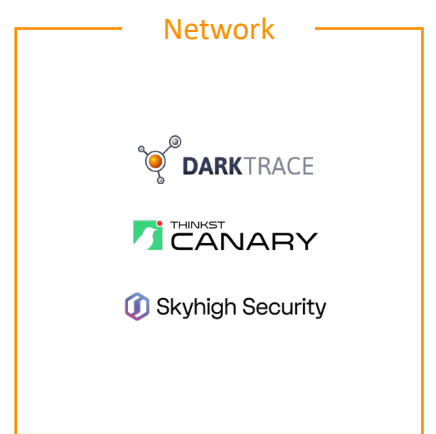
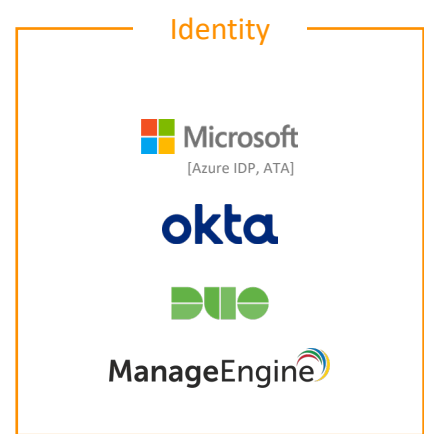
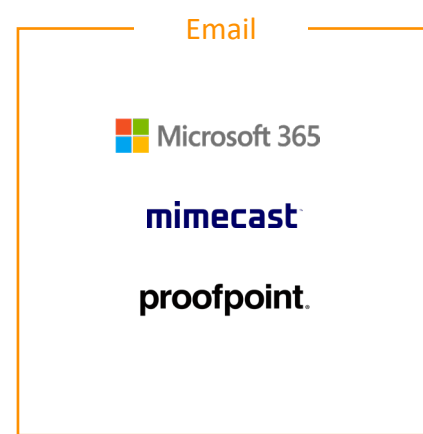
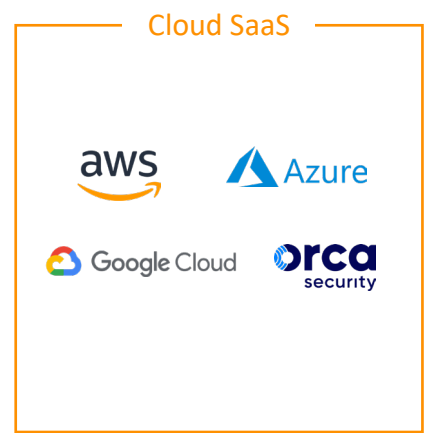
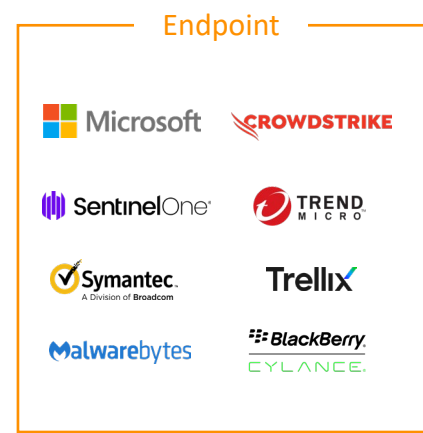
Sophos MDR: Industry-Leading Openness and Flexibility



Compatible with your environment
We can use our tools, another vendor's tools or any combination of the two

Compatible with your needs
Whether you need full-scale incident response or assistance making more accurate decisions

Compatible with your business
Our team has deep experience hunting threats targeting organizations in every industry



Sophos X-Ops Powers MDR with Leading Threat Intelligence

Security Professionals

Sophos team sharing queries, tools, and techniques from CISO to frontline



MDR SecOps Analysts

Discovering new IOCs and hunting methods, in-the-wild impact



Sophos X-Ops

500+ experts across threat intel, analysis, data engineering, data science, threat hunting, adversary tracking, and incident response, staffing 6 global SOCs in every major theater

SophosLabs Researchers

Providing deep analysis of files, email, behaviors, URLs, IOCs, and DPI

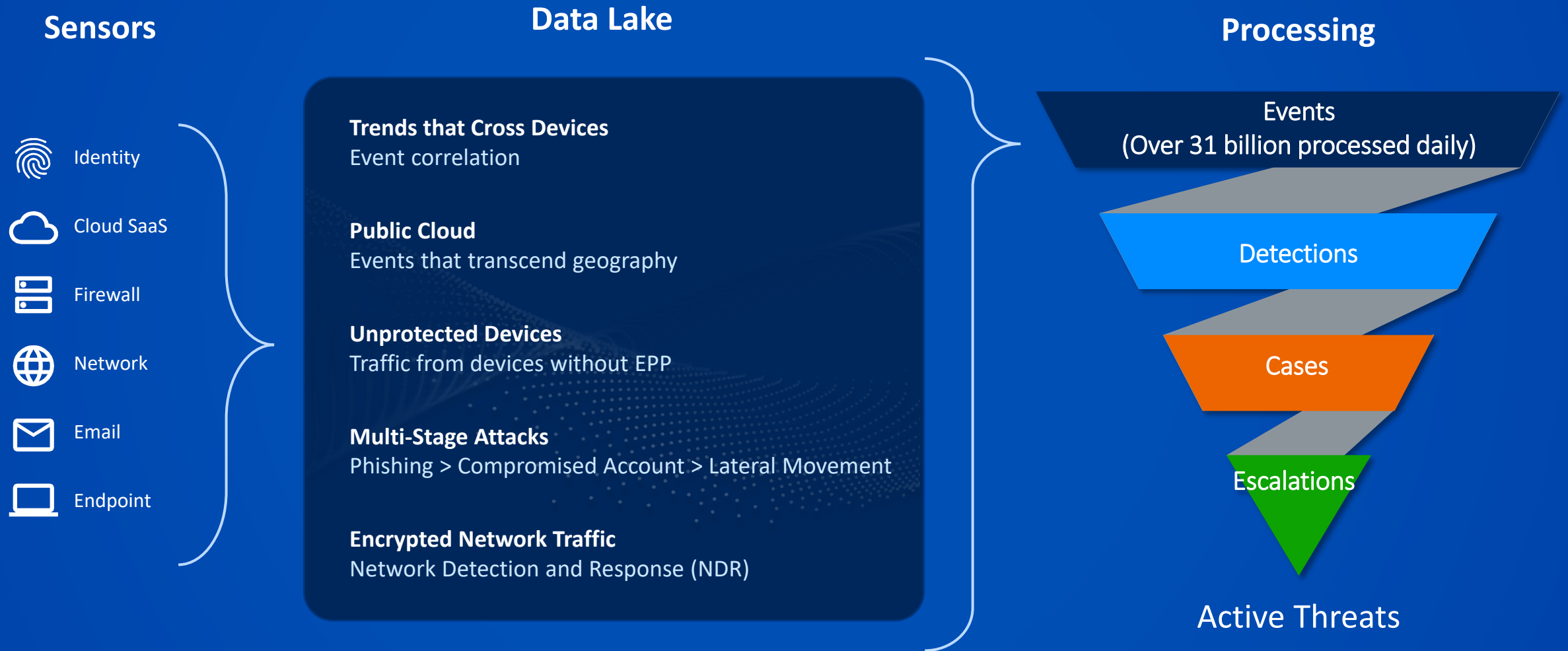


Sophos AI Data Scientists

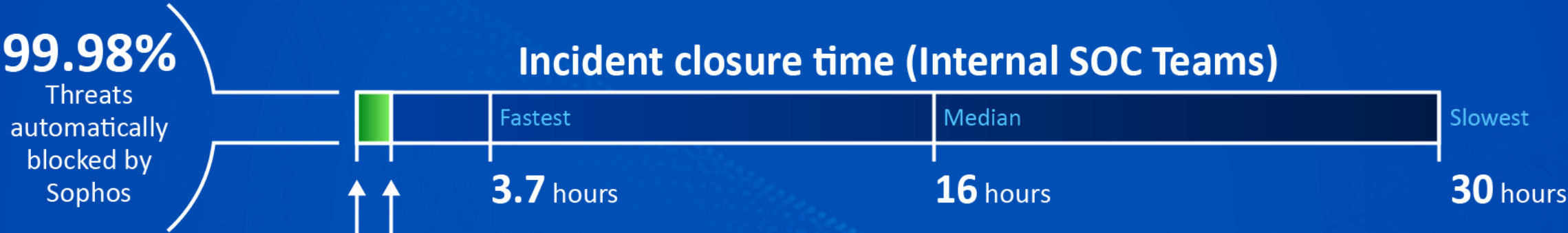
Development and insights on advanced ML models, automation and detection for MDR and Sophos products



Broad, Advanced Telemetry Allows Sophos to See More

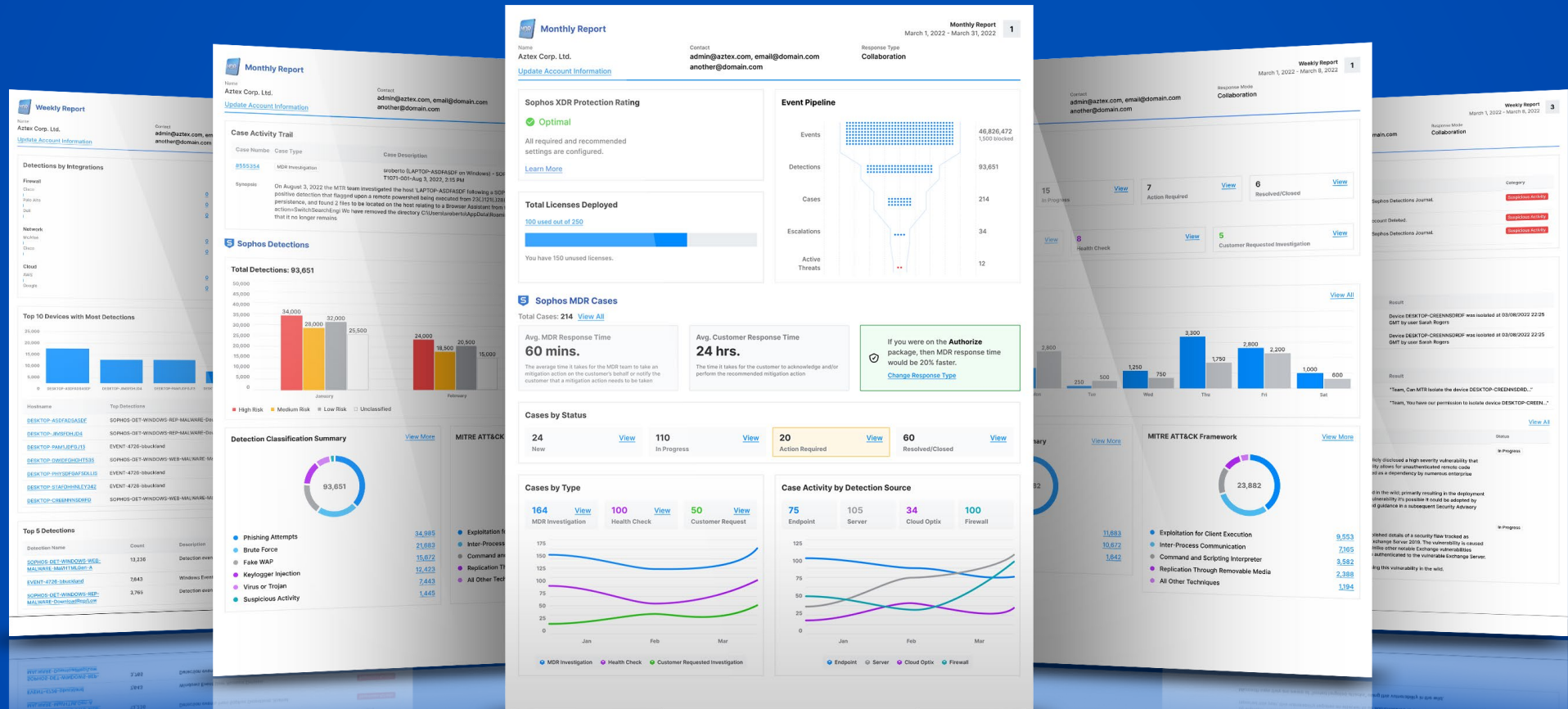


Leading Detection and Response Times



SOPHOS

Monthly and Weekly Cybersecurity Reports



Response Modes

You choose the best way
for our MDR team
to work alongside you

Notify

We notify you about the detection and provide detail to help you in prioritization and response

Collaborate

We work with your internal team or external point(s) of contact to respond to the detection

Authorize

We handle containment and neutralization actions and will inform you of the action(s) taken

You do it on your own

You do step 1,2,3, I'll do 4,5,6

You guys see it, you do it

(interchangeable – someone gets sick or goes on vacation, just switch mode with us)
(collaborate – after hours – we'll do it for you when you're not around)

MDR That Meets You Where You Are

People

I need an expert team to...

Completely manage threat response

Co-manage threat response with my team

Alert my team to threats that require action

Process

Confirmed threats require...

Full-scale incident response: threat is eliminated

Containment so my team can eliminate them

A detailed alert with remediation guidance

Technology

I want to use...

Sophos: best protection, detection, and response

A combination of Sophos and non-Sophos tools

Non-Sophos tools only

Visibility

Detect threats using data from...

Endpoint

Firewall

Email

Identity

Public Cloud

Network

Sophos solutions integrated at no additional cost

 Sophos XDR

 Sophos Firewall

 Sophos Email

 Sophos Endpoint


 Sophos Cloud

 Sophos NDR

Non-Sophos solutions integrated at no additional cost

 Any endpoint protection platform, including Windows Defender

Add-on integrations available for purchase:

 Virtually any security tool that generates threat detection data

Sophos Service Tiers

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24/7 expert-led threat monitoring and response	✓	✓	✓
Compatible with non-Sophos security products	✓	✓	✓
Weekly and monthly reporting	✓	✓	✓
Monthly intelligence briefing: "Sophos MDR ThreatCast"	✓	✓	✓
Sophos Account Health Check		✓	✓
Expert-led threat hunting		✓	✓
Threat Containment: attacks are interrupted, preventing spread <small>Uses full Sophos XDR agent (protection, detection and response) or Sophos XDR Sensor (detection and Response)</small>		✓	✓
Direct call-in support during active incidents		✓	✓
Full-scale Incident Response: threats are fully eliminated <small>Requires full Sophos XDR agent (protection, detection and response)</small>			✓
Root Cause Analysis: performed to prevent future recurrence			✓
Dedicated Incident Response Lead			✓

Sophos MDR Included Integrations

Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and Microsoft integrations

Included in Sophos MDR and Sophos MDR Complete Pricing

Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm

Product sold separately; integrated at no additional charge

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Identity Protection (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Security and Compliance Center
- Azure Information Protection

Sophos Endpoint Protection

Block advanced threats and detect malicious behaviors—including attackers mimicking legitimate users

Included in Sophos MDR and Sophos MDR Complete Pricing

Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks

Product sold separately; integrated at no additional charge

Office 365 Management Activity

Provides information on user, admin, system, and policy actions and events from Office 365 and Azure Active Directory activity logs

Sophos Cloud

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform

Product sold separately; integrated at no additional charge

90-Days Data Retention

Retains data from all Sophos products and any third-party (non-Sophos) products in the Sophos Data Lake

Third-Party Endpoint Protection

Compatible with...

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- Trellix
- BlackBerry (Cylance)
- Symantec (Broadcom)
- Malwarebytes

Add-On Integrations



Sophos Network Detection and Response

Continuously monitor activity inside your network to detect suspicious actions occurring between devices that otherwise are unseen

Compatible with any network via SPAN port mirroring



Firewall

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall



Identity

- Okta
- Duo
- ManageEngine



Public Cloud

- AWS Security Hub
- AWS CloudTrail
- Orca Security
- Google Cloud Platform Security



Email

- Proofpoint
- Mimecast



Network

- Darktrace
- Thinkst Canary
- Skyhigh Security



1-Year Data Retention

Sophos Breach Protection Warranty

THE WARRANTY PROVIDES UP TO \$1 MILLION IN RESPONSE EXPENSES FOLLOWING A RANSOMWARE INCIDENT IN AN ENVIRONMENT PROTECTED BY SOPHOS MDR COMPLETE

Clear

Warranty is...

Included automatically with purchases of Sophos MDR Complete term licenses

Available in all countries where Sophos operates*

No warranty tiers that restrict coverage

No additional licenses required to qualify

Comprehensive

Warranty covers...

Devices running Windows and macOS

Endpoints and servers

1-, 2-, and 3- year subscription licenses

Both new and renewing customers

Coverage

Warranty pays...

Up to \$1,000 per breached machine

Up to \$1 million total response expenses

Up to \$100,000 ransom (as part of per device limit)

Covers multiple incurred expenses including data breach notification, PR, legal and compliance

**Excludes embargoed countries*

For full details and conditions of the warranty see www.sophos.com/legal.

Sophos Security Services

“Have I been breached?”



Sophos Compromise Assessment

“I’ve been breached.
What do I do now?”



Sophos Rapid Response

“I don’t want to get breached
(again). How can I be proactive?”



Sophos MDR

**The fastest, most
effective means of
identifying ongoing or
past attacker activity
in your environment**



Delivered by an expert team of threat hunters and response specialists who confirm if an attacker is operating undetected in your environment



Identifies the scope of the threat and quantifies the potential risk of a widespread security incident



Receive a written report with technical documentation and a non-technical executive summary detailing evidence of attacker activity



Immediately shift from threat assessment to threat neutralization with Sophos Rapid Response

Sophos Security Services

“Have I been breached?”



Sophos Compromise Assessment

“I’ve been breached.
What do I do now?”



Sophos Rapid Response

“I don’t want to get breached
(again). How can I be proactive?”



Sophos MDR

Emergency incident response to rapidly eliminate active threats and monitor for reoccurrence



Delivered by a 24/7 team of remote incident response experts, threat intelligence analysts, and threat hunters



Rapid deployment enables threat responders to take immediate action to triage, contain, and eliminate active threats



45 days of ongoing threat monitoring and response from the Sophos MTR team ensures any recurrence of the threat is handled immediately



Fixed-fee pricing determined by the number of users and servers in your environment keeps remediation costs predictable

Sophos Security Services

“Have I been breached?”



Sophos Compromise Assessment

“I’ve been breached.
What do I do now?”



Sophos Rapid Response

“I don’t want to get breached
(again). How can I be proactive?”



Sophos MDR

**24/7 threat hunting,
investigation, and
response delivered by
an expert team as a
fully-managed service**



Enabled by extended detection and response (XDR) capabilities that provide complete security coverage wherever your data reside



Proactive threat hunts performed by highly-trained analysts uncover more malicious behavior than security products can detect on their own



Analysts respond to threats in minutes whether you need full-scale incident response or assistance making more accurate decisions

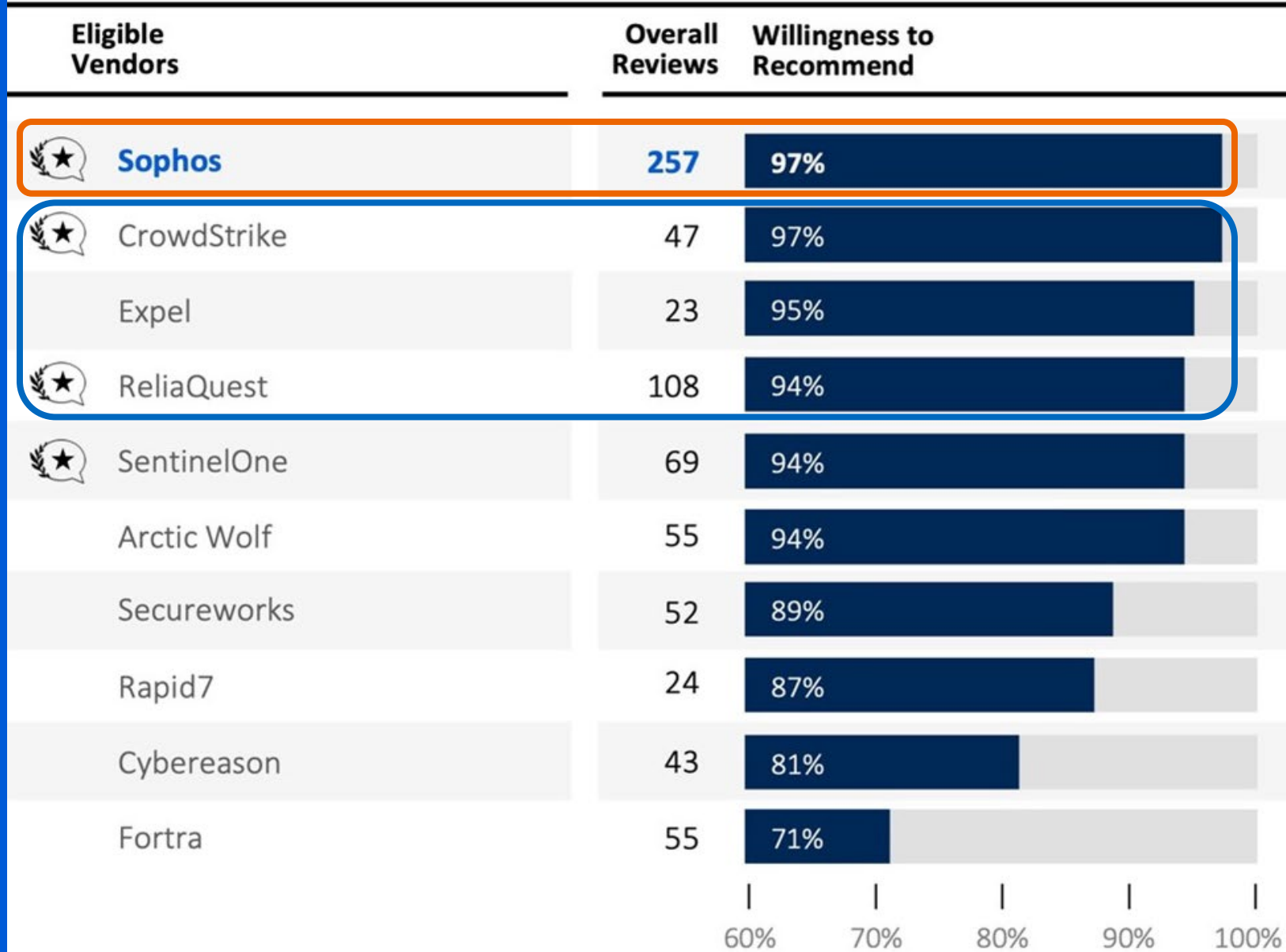


Identifies the root cause of threats and provides recommendations to prevent future incidents and reduce risk to your business

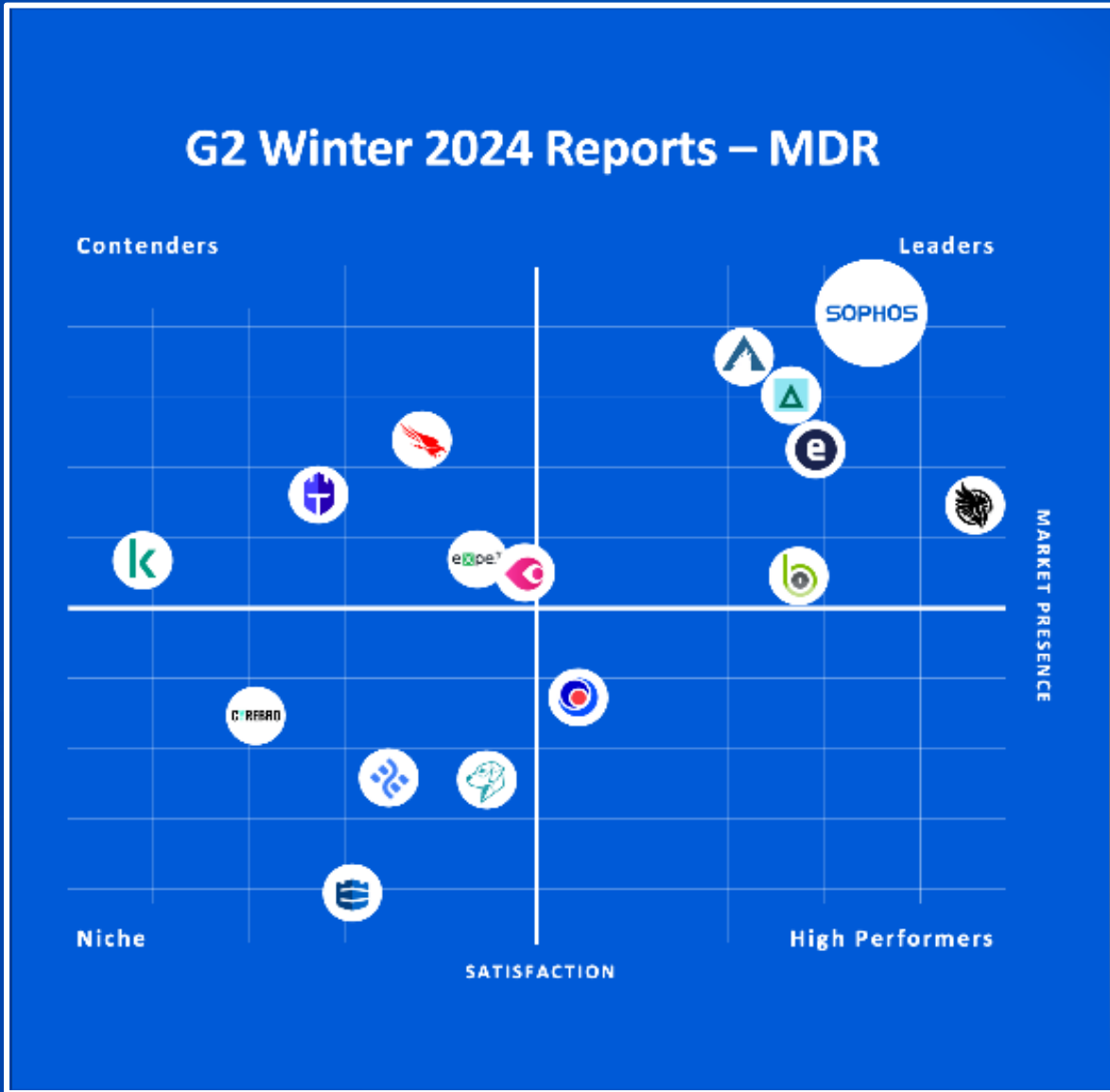
Gartner® Peer Insights™

Sophos earned a **97% “Willingness to Recommend”** score—*no other service provider scored higher*—and had **more customer reviews** than the other three Customers’ Choice selections combined.

Gartner Peer Insights “Voice of the Customer” Managed Detection and Response Services



G2: Delivering Defense in Depth for Today's Businesses



Sophos MDR is a **Leader** in the Overall



Rated the **Top Vendor** in the 2024 G2 Grid®

Winter 2024 G2 Grid® for Managed Detection and Response

NO OTHER CYBERSECURITY VENDOR COMES CLOSE

Over 19,500 organizations are now actively protected by Sophos MDR Security Operations analysts.

The team has investigated 179,783 cases in 2023 that's one case every three minutes!

With 3x more MDR customers than any other cybersecurity vendor, Sophos has the experience to deliver the best possible cybersecurity outcomes.

Value Added Distributor



<https://nss.gr>