Sophos MDR

Delivering Superior Security Outcomes Through Cybersecurity as a Service

Stelios Gerardis
Sales Manager NSS

April 2023

nss
Affordable Cutting Edge

SOPHOS

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

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 year[1]
- **78% increase** in the number of organizations hit by ransomware last year[1]
- "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 employee[2]

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 $2.86M[3]

[1]The State of Ransomware 2022, Sophos; The Active Adversary Playbook 2022, Sophos
[2]Statista: https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[3]Ponemon Institute: "The Economics of Security Operations Centers: What Is the True Cost for Effective Results?"

The Solution: Cybersecurity as a Service

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

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

ARCTIC WOLF, red canary, eSENTIRE, expel, Secureworks

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

CROWDSTRIKE, SentinelOne, Microsoft, RAPID7, cybereason

MDR 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

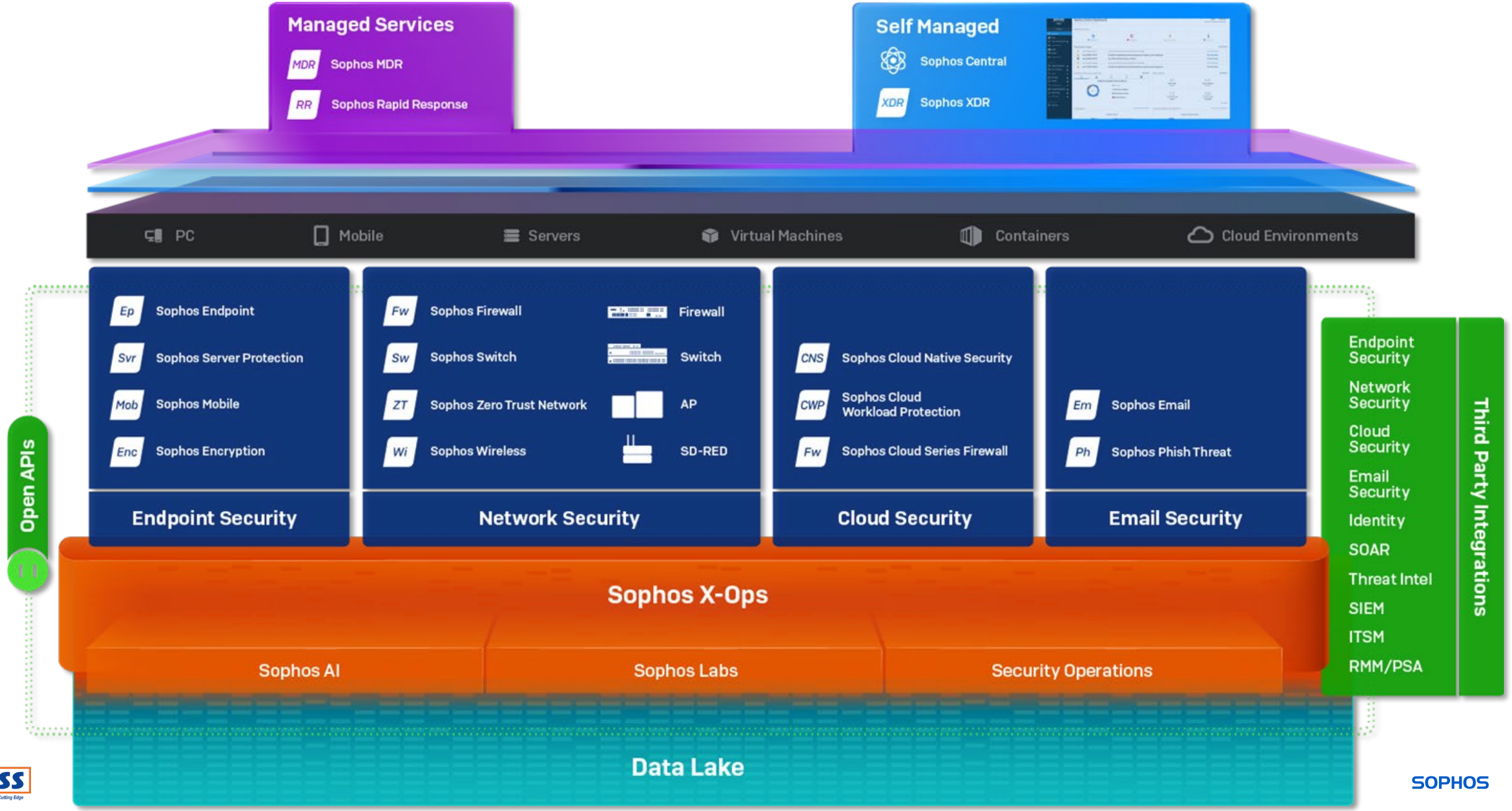
More organizations trust Sophos for MDR than any other vendor. 12000 customers

- Sophos delivers leading cybersecurity outcomes for over **530,000 customers** globally
- 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**

Adaptive Cybersecurity Ecosystem



Sophos MDR: Industry-Leading Openness and Flexibility

Sophos MDR

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

- XDR Sophos XDR
- Fw Sophos Firewall
- Cld Sophos Cloud
- NDR Sophos NDR
- Em Sophos Email
- Ep Sophos Endpoint

Endpoint

Microsoft, CROWDSTRIKE, SentinelOne, TREND MICRO, Symantec (A Division of Broadcom), Trellix, Malwarebytes, BlackBerry CYLANCE

Firewall

paloalto NETWORKS, FORTINET, CHECK POINT, CISCO, SONICWALL

Cloud SaaS

aws, Azure, Google Cloud, orca security

Email

Microsoft 365, mimecast, proofpoint

Identity

Microsoft [Azure IDP, ATA], okta, DUO, ManageEngine

Network

DARKTRACE, THINKST CANARY, Skyhigh Security

Broad, Advanced Telemetry Allows Sophos to See More

Sensors

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

Data Lake

Trends that Cross Devices
Event correlation

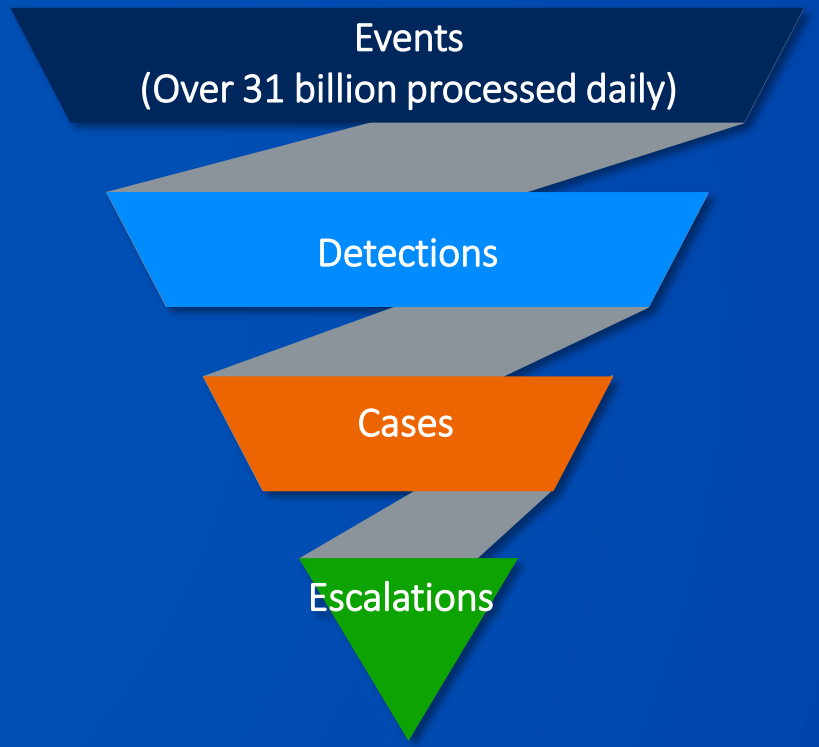
Public Cloud
Events that transcend geography

Unprotected Devices
Traffic from devices without EPP

Multi-Stage Attacks
Phishing > Compromised Account > Lateral Movement

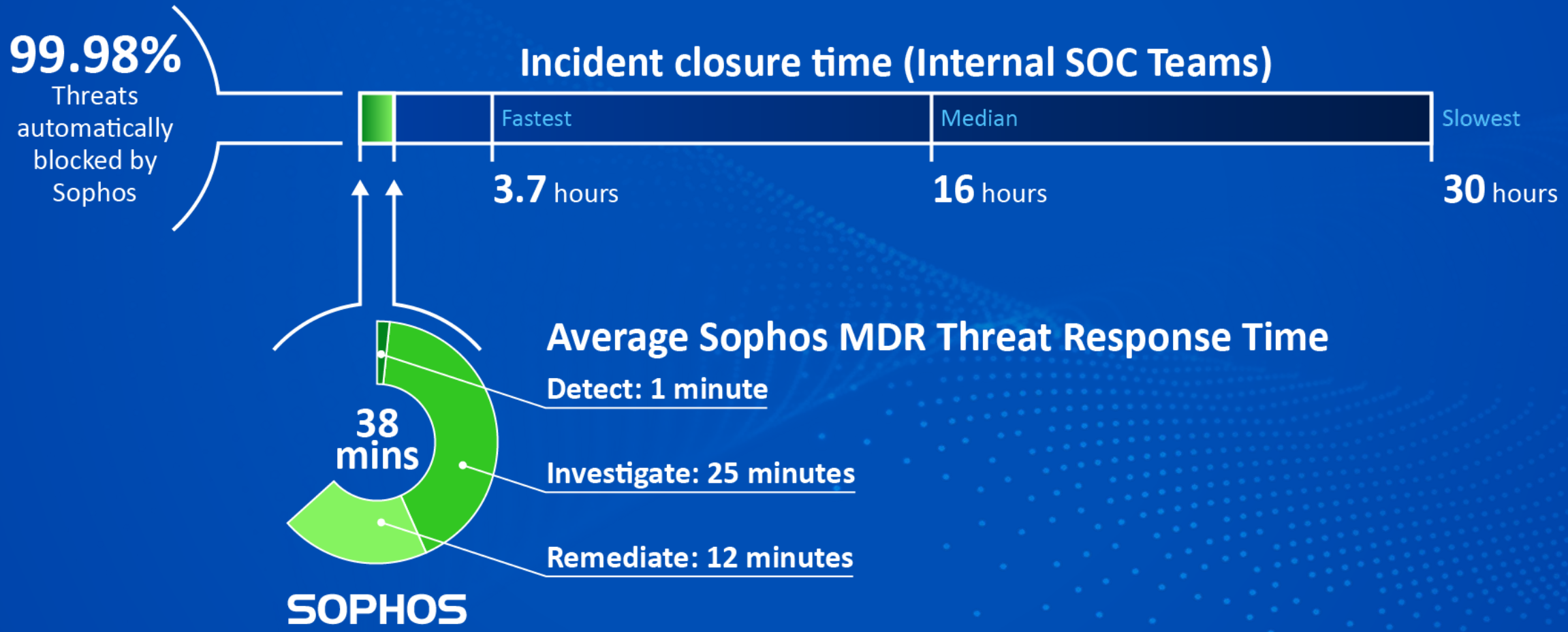
Encrypted Network Traffic
Network Detection and Response (NDR)

Processing

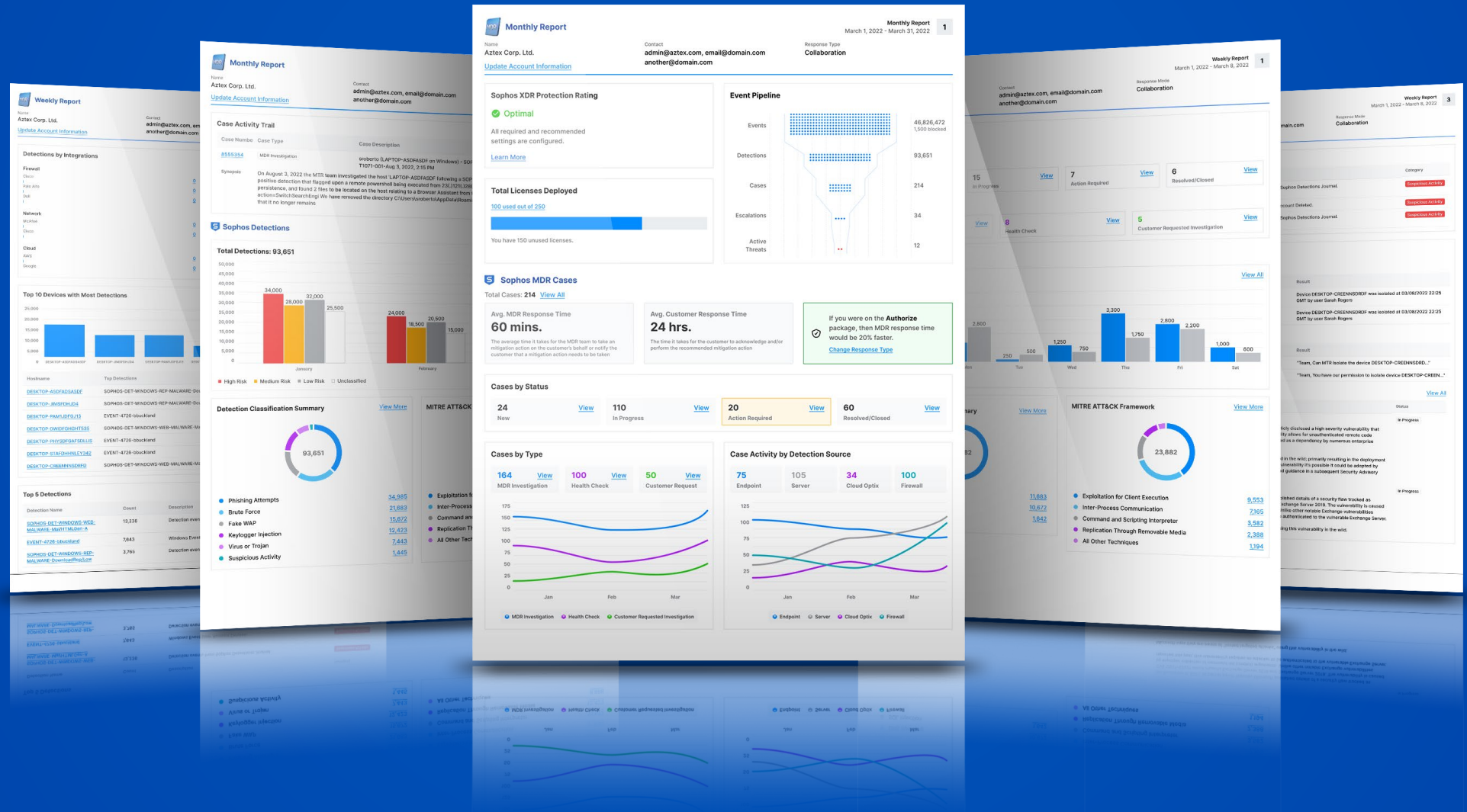


Active Threats

Leading Detection and Response Times



Monthly and Weekly Cybersecurity Reports



nss Affordable Cutting Edge

SOPHOS

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

- XDR Sophos XDR
- Fw Sophos Firewall
- Em Sophos Email
- Ep Sophos Endpoint
- Cld Sophos Cloud
- NDR 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 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 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

All Integration Packs are available for Sophos MDR, Sophos MDR Complete, and Sophos Threat Advisor
All Integration Packs need to be purchased based on the number of Sophos MDR seats for that customer

Sophos Security Services

"Have I been breached?"	"I've been breached. What do I do now?"	"I don't want to get breached (again). How can I be proactive?"
Sophos Compromise Assessment	**Sophos Rapid Response**	**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?"	"I've been breached. What do I do now?"	"I don't want to get breached (again). How can I be proactive?"
Sophos Compromise Assessment	**Sophos Rapid Response**	**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?"	"I've been breached. What do I do now?"	"I don't want to get breached (again). How can I be proactive?"
Sophos Compromise Assessment	**Sophos Rapid Response**	**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™

The **highest rated** and **most reviewed** solutions across MDR, Endpoint, and Firewall

Sophos MDR

4.8	97%
Average Rating	Would Recommend

Based on 256 Reviews

SentinelOne	4.5
CrowdStrike	4.8*
Arctic Wolf	4.8*

Sophos Endpoint

4.8	95%
Average Rating	Would Recommend

Based on 539 Reviews

Microsoft	4.4
CrowdStrike	4.7
Trend Micro	4.6

Sophos Firewall

4.8	95%
Average Rating	Would Recommend

Based on 362 Reviews

Fortinet	4.6
Check Point	4.5
Palo Alto Networks	4.5

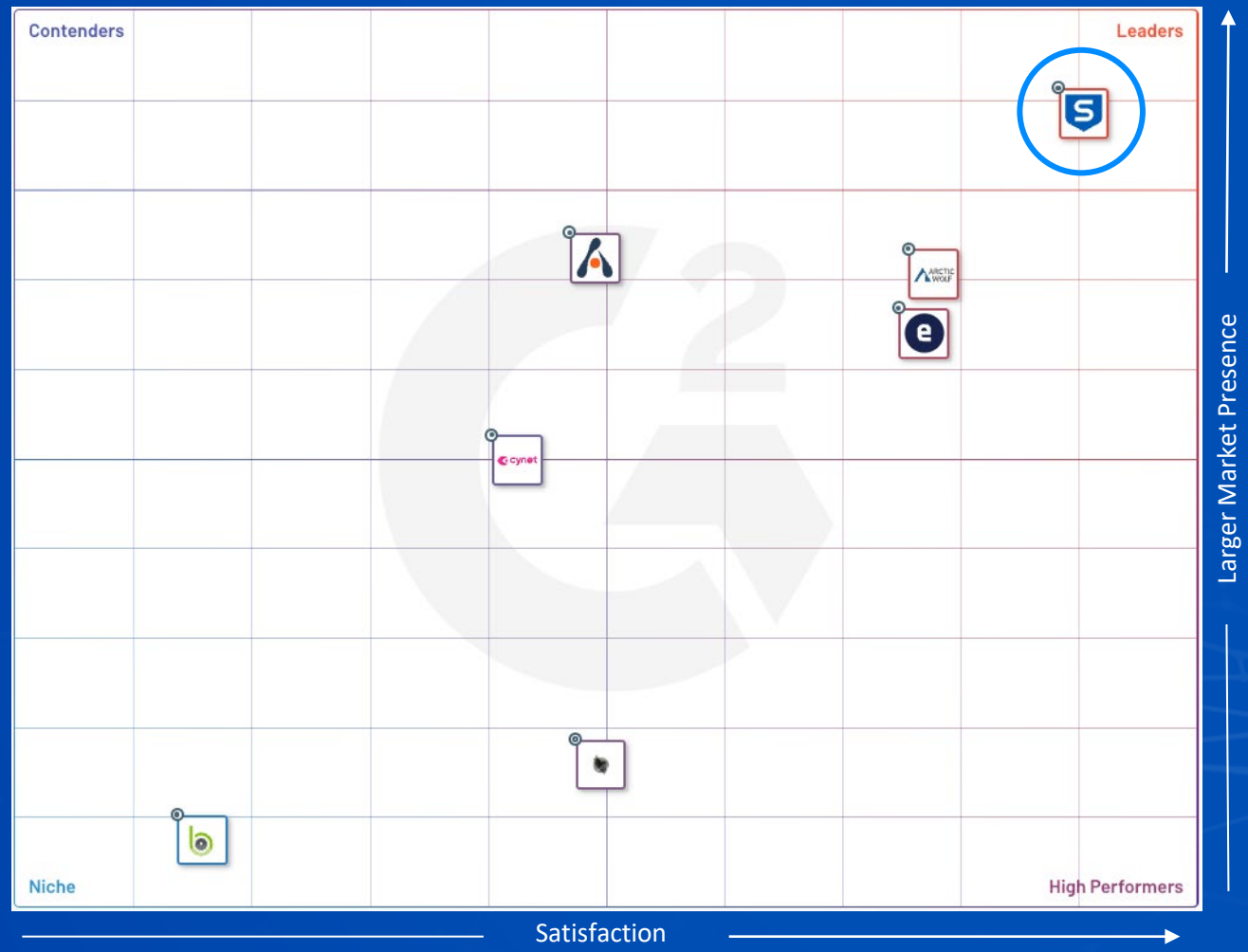
Reviews from last 12 months as of August 1, 2022
*Vendors with fewer than 50 customer reviews

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

NSS Affordable Cutting Edge

SOPHOS

G2: A Leader in MDR Service Ratings



Sophos MDR is a **Leader** in the Overall, Mid-Market, and Enterprise segments

Rated the **Top Vendor** in the 2022 G2 Grid® for MDR Services serving the midmarket

2022 G2 Grid® for Managed Detection and Response (MDR) - Midmarket

Value Added Distributor

Affordable Cutting Edge

SOPHOS

Cybersecurity delivered.

sales@nss.gr
211 8000 330