



Sophos MDR

Delivering Superior Security Outcomes Through
Cybersecurity as a Service

George Kapaniris
Executive Director, NSS

December 6, 2023



Affordable Cutting Edge

SOPHOS

Sophos at a Glance

- Global leader in cybersecurity as a service, AI-enabled endpoint, network, email, and cloud security
- HQ in Oxford, UK
- 4,124 employees
- Over \$1.1 billion (CC) in billings in FY23
- Over 562,000 customers
- Over 100 million users
- Over 450,000 active next-gen firewalls
- One of world's largest and fastest-growing MDR providers, with over 18,000 customers
- Over 25,000 active partners and over 6,000 active MSPs
- Global revenue strength: 51% EMEA, 37% Americas, 12% APJ

A Recognized Market Leader

Endpoint Security

Gartner

13-time Gartner
Magic Quadrant Leader

Leader:
Endpoint Protection Platforms
Gartner Magic Quadrant

Best Enterprise
Endpoint Solution
SE Labs

Customers' Choice for EPP
Gartner Peer Insights

Network Security

FORRESTER®

Award-Winning
Network Appliances

Customers' Choice
for Network Firewalls
Gartner Peer Insights

Best in Network Security
*CRN Annual Report Card
(ARC) Awards*

Editors Choice:
Sophos Firewall
IT Pro

Managed Services



One of Largest and Fastest-Growing
MDR Service Providers

Winner:
Best Managed Security Services
Channel Partner Insight Awards

Best Managed Detection and Response
Services
CRN

Average 4.8 / 5
Customer Rating
Gartner Peer Insights

Sophos Channel Program

CRN

Top-Rated
Global Partner Programs

Best in endpoint,
network, XDR, MDR
ChannelPro Readers Choice Awards

Security Vendor of the Year
Channel Partner Insight

5-Star Rating
CRN Partner Program Guide

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.


G2 REPORTS | SPRING 2023

A Leader in 36 categories



The only solution
named a Leader in every
major category

- MDR** Managed Detection and Response
- XDR** Extended Detection and Response
- EDR** Endpoint Detection and Response
- Fw** Network Firewall
- Ep** Endpoint Protection



**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 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 2022, Sophos; The Active Adversary Playbook 2022, 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?"

Superior Outcomes with Cybersecurity as a Service

LESS RISK

85% Reduction in incidents that require investigation



Sports and Hospitality
400 Employees

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

GREATER EFFICIENCY

2X More efficient IT Teams



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."

LOWER COSTS

5X Less expensive than managing in-house



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.



Government
70 Employees

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



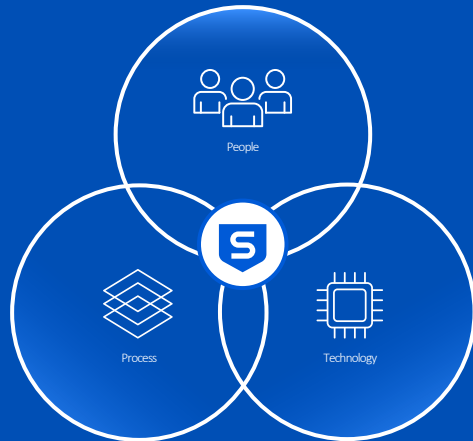
Supermarket Chain
13,000 Employees

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

The Solution: Cybersecurity as a Service

MANAGED DETECTION AND RESPONSE

Superior security outcomes
delivered 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**

Gartner® Peer Insights™

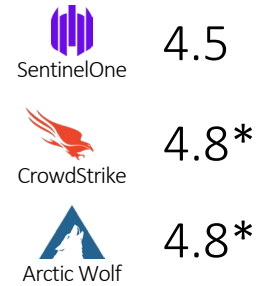
The **highest rated** and **most reviewed** solutions across MDR, Endpoint, and Firewall



4.8
Average Rating

97%
Would Recommend

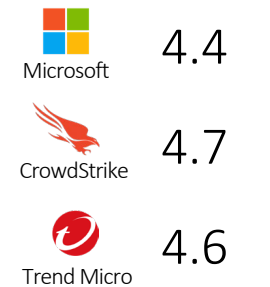
Based on 256 Reviews



4.8
Average Rating

95%
Would Recommend

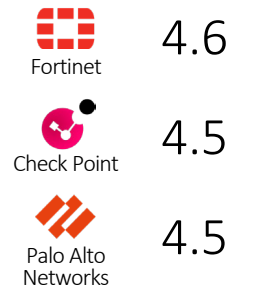
Based on 539 Reviews



4.8
Average Rating

95%
Would Recommend

Based on 362 Reviews



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.

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



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.



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

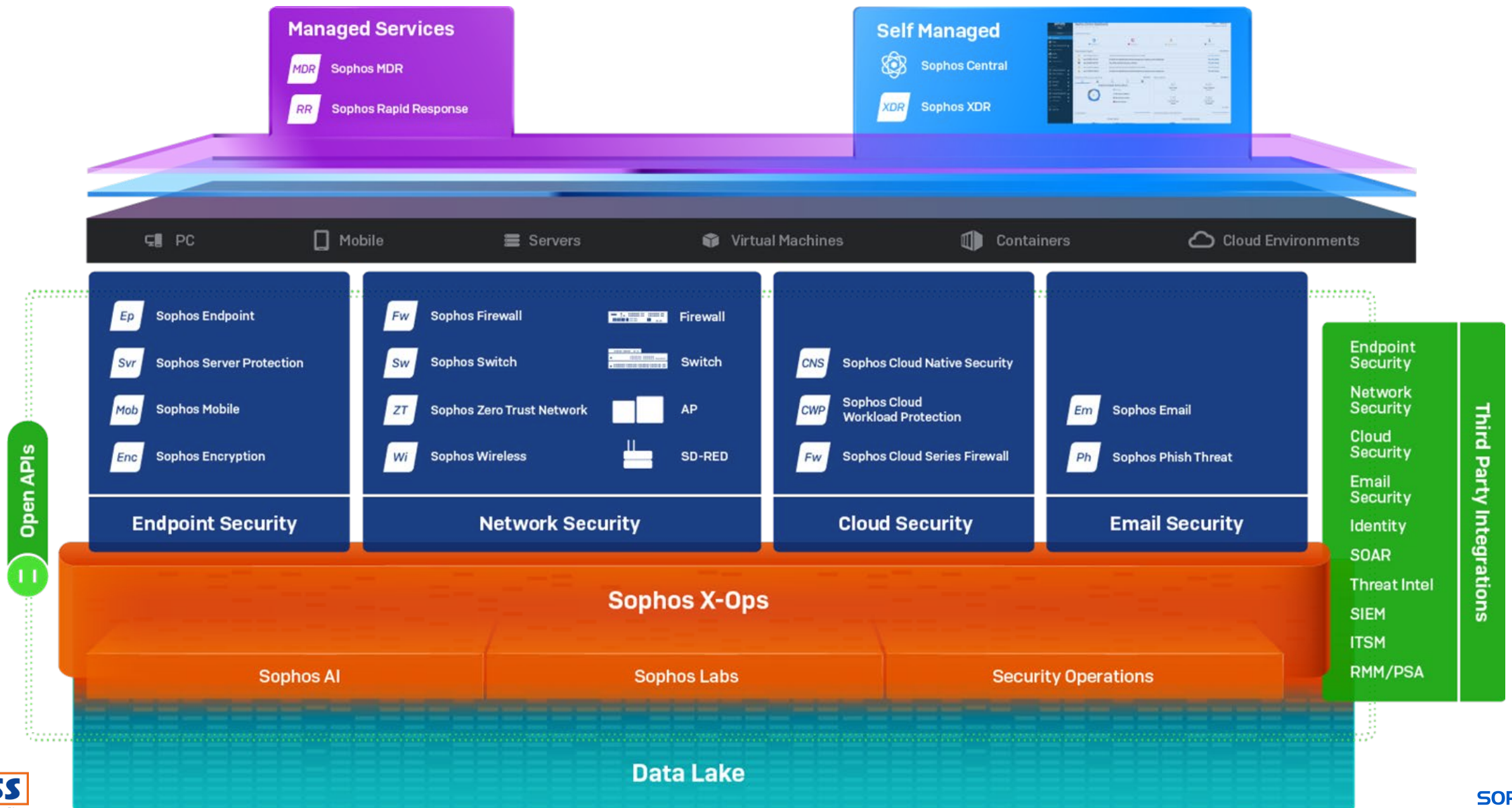


Sophos X-Ops Research



A Proven, Trusted and Leading MDR Provider

Adaptive Cybersecurity Ecosystem



Sophos MDR: Industry-Leading Openness and Flexibility



Compatible with your environment

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

Compatible with your needs

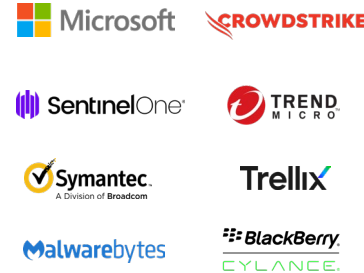
Whether you need full-scale incident response or assistance making more accurate decisions

Compatible with your business

Our team has deep experience hunting threats targeting organizations in every industry



Endpoint



Firewall



Cloud SaaS



Email



Identity












Network



Non-Microsoft Telemetry Sources

Microsoft Security Event Sources

-  Microsoft Defender for Endpoint
-  Microsoft Defender for Identity
-  Microsoft Defender for Cloud
-  Microsoft Defender for Cloud Apps
-  Identity Protection (Azure AD)
-  O365 Security & Compliance Center
-  Microsoft Sentinel
-  Office 365 Management Activity
-  **Non-Microsoft Telemetry Sources**

Sophos

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

Endpoint



Firewall



Network



Email

mimecast
proofpoint.

Identity

okta
duo
ManageEngine

Public Cloud

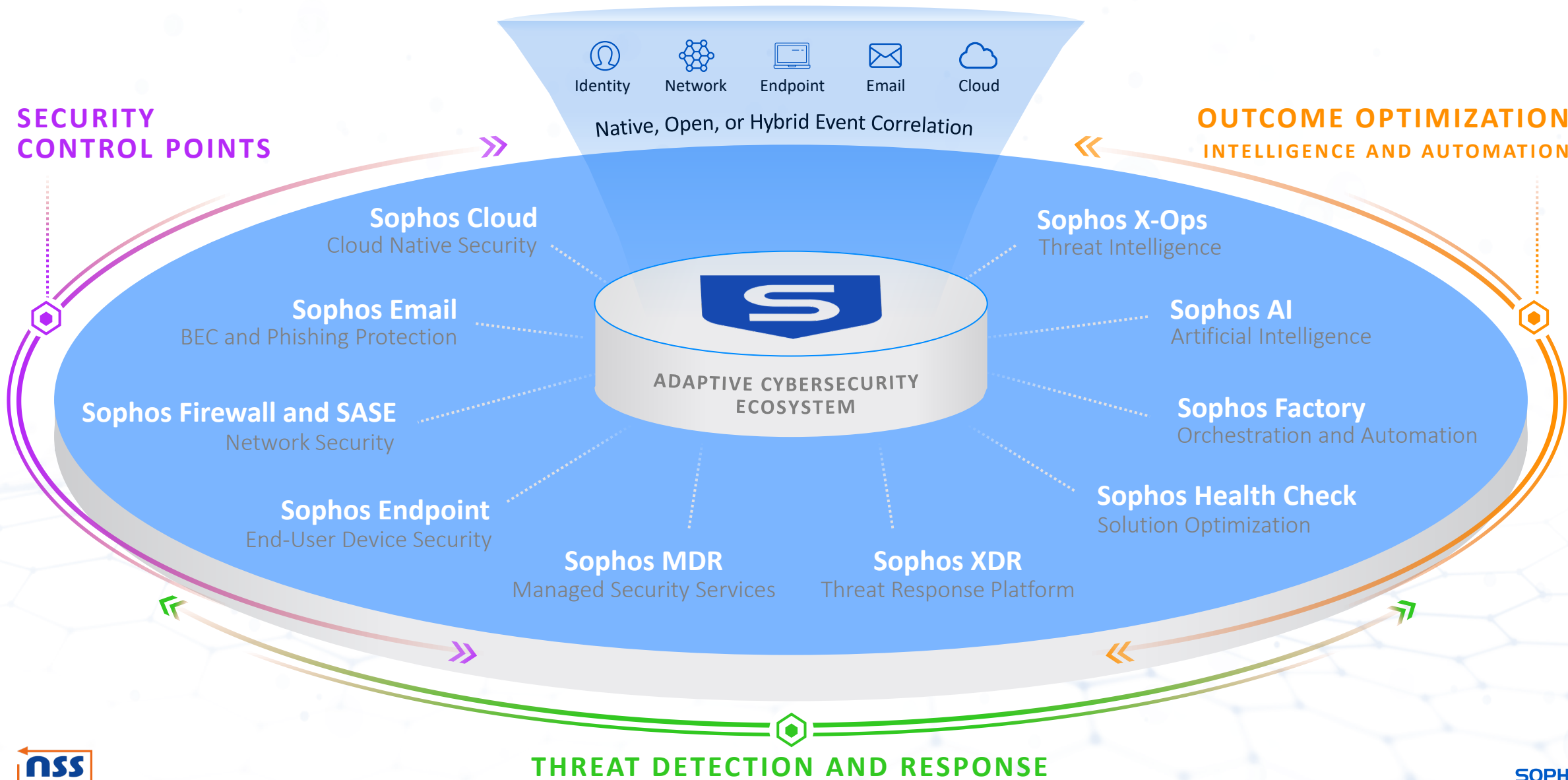
aws
orca security

Productivity

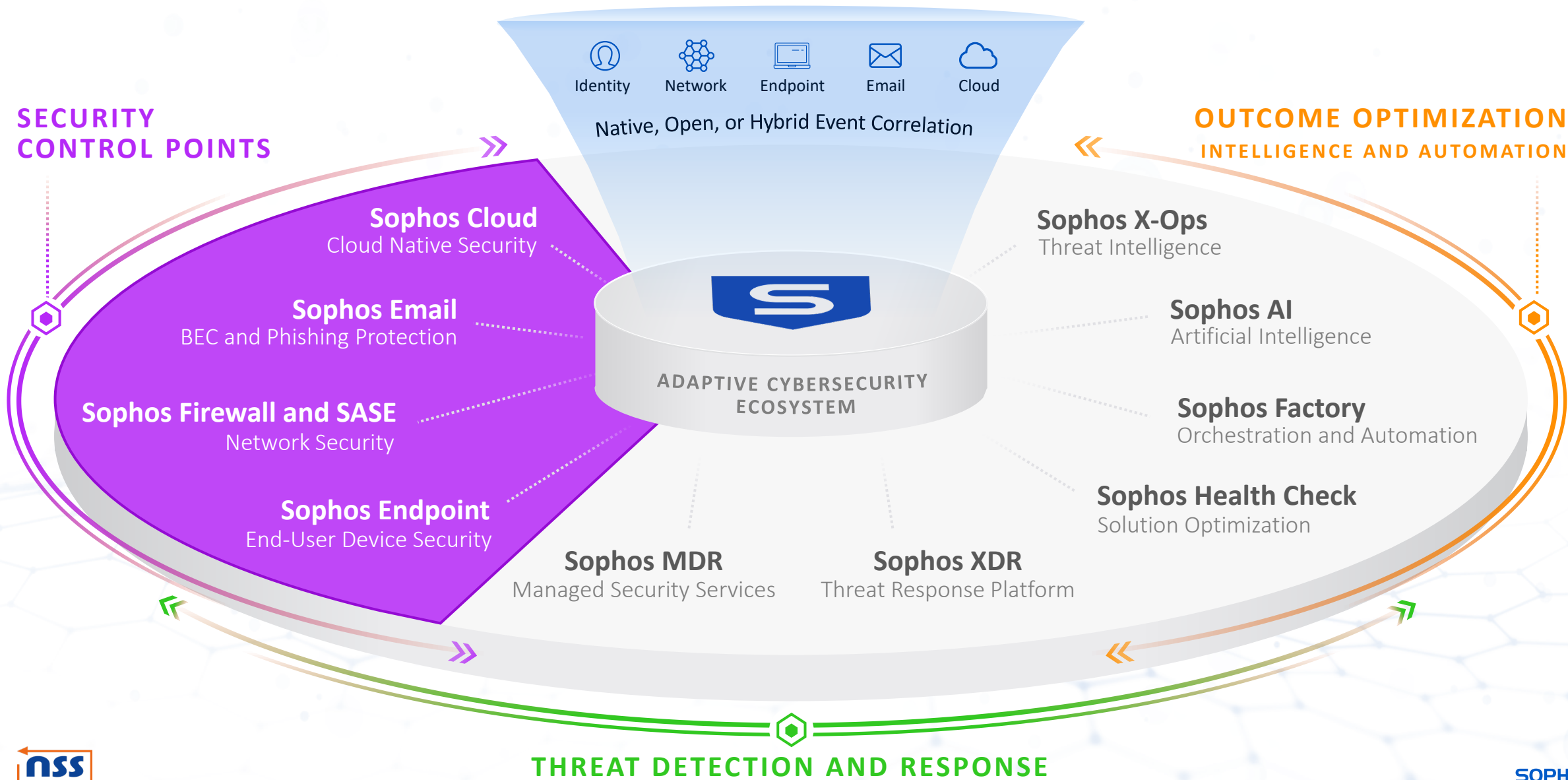
Google
Workspace

Sophos, Microsoft, Endpoint, and Productivity Integrations are included at no additional cost.
Other integration packs are chargeable add-ons.

Delivering Optimal Cyber Security Outcomes



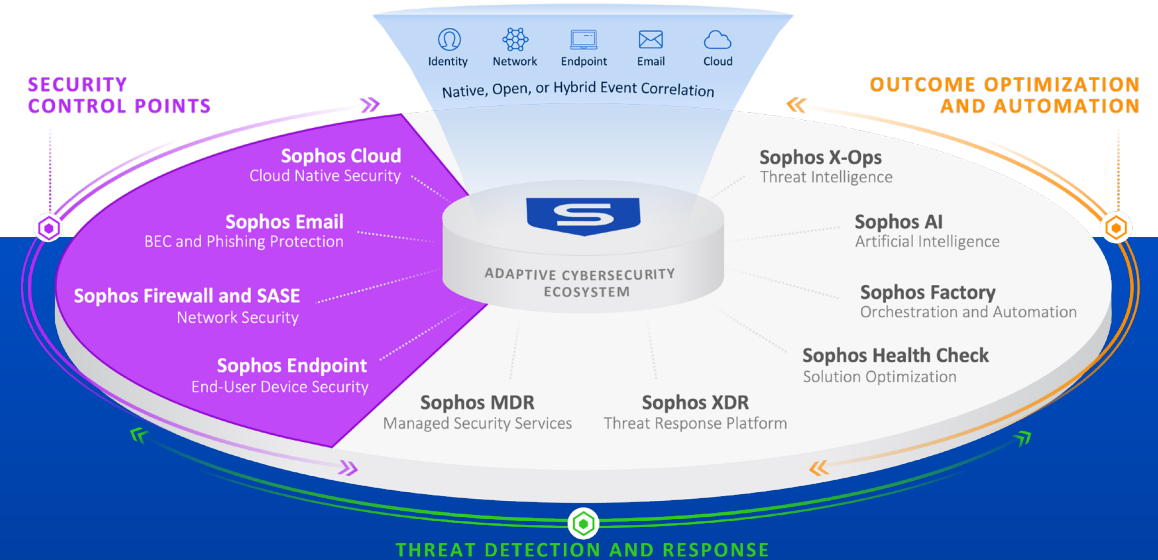
Delivering Optimal Cyber Security Outcomes



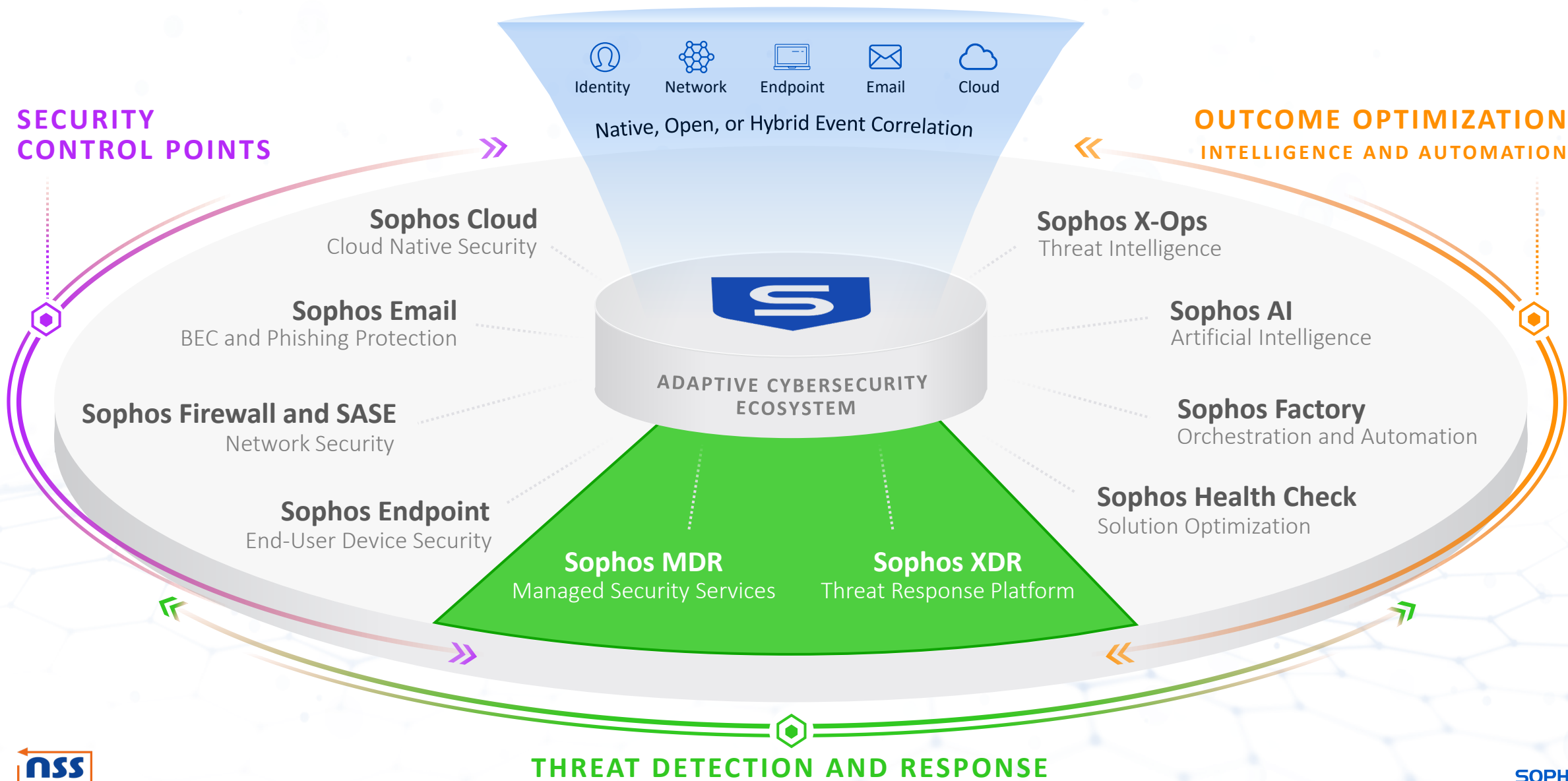
Security Control Points

Newly Released Innovations

- Adaptive Attack Protection
- Account Health Check Scoring
- New SD-WAN capabilities in Network Security
- Firewalls double the VPN performance
- New high-end XGS Series firewall hardware
- Zero Trust Network Access (ZTNA) as a Service
- Sophos Email adds integrated mail flow rules and spam control slider



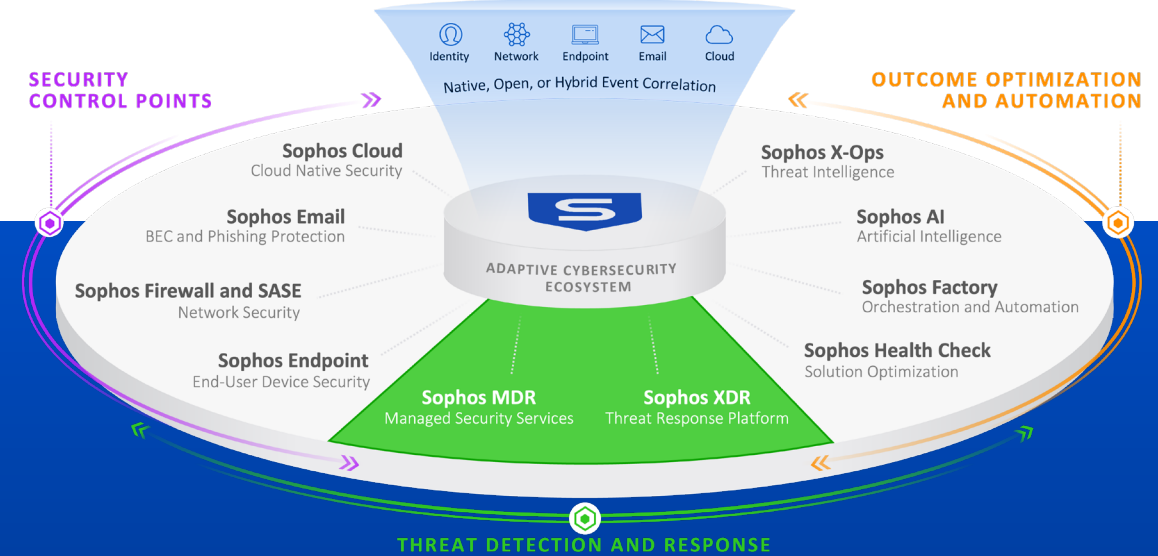
Delivering Optimal Cyber Security Outcomes



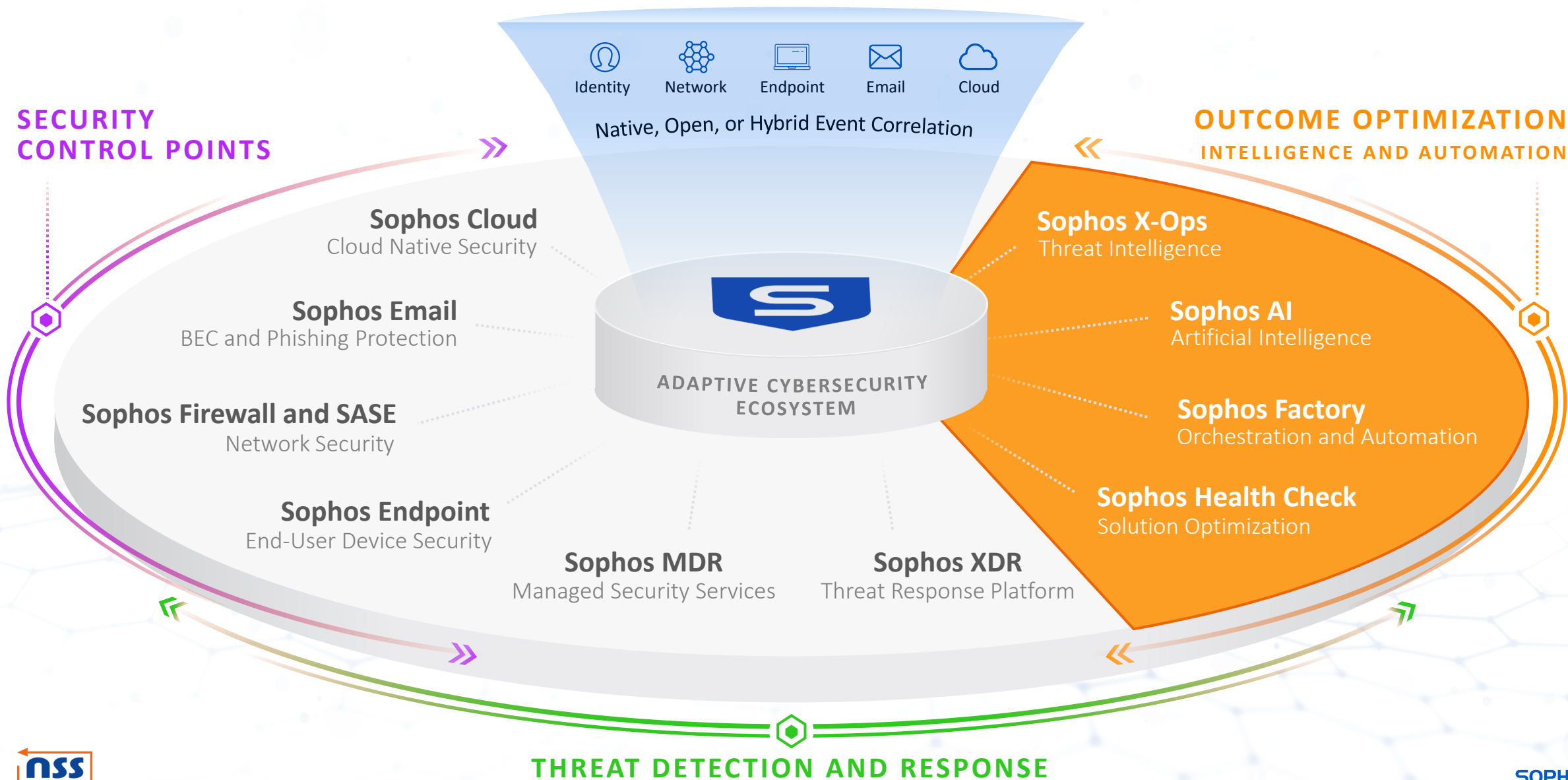
Threat Detection and Response

Newly Released Innovations

- MDR service for Sophos and third-party environments
- MDR Essentials for Microsoft Defender environments
- Detection across endpoints, servers, firewalls, network traffic, cloud, email, and identity tools
- Network Detection and Response (NDR)
- Full-scale Incident Response (IR) and new IR retainer
- Market leading response time
- \$1M Breach Protection Warranty



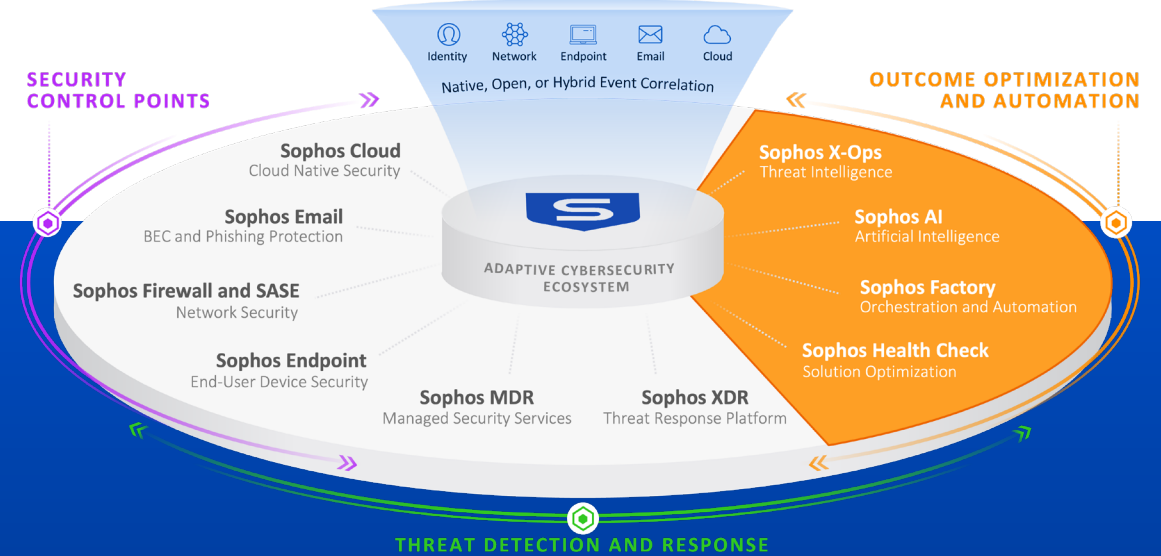
Delivering Optimal Cyber Security Outcomes



Outcome Optimization and Automation

Newly Released Innovations

- New anti-exploitation and anti-ransomware techniques
- New ML models for enhanced threat detection
- Improved ML models to prevent email impersonation
- Sophos Intelix integrations with MISP, ThreatQuotient, CompTIA ISAO, Cyber Threat Alliance, and OpenCTI



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



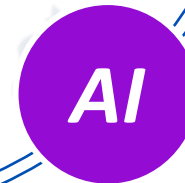
Sophos X-Ops

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

Sensors



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

Events
(Over 31 billion processed daily)

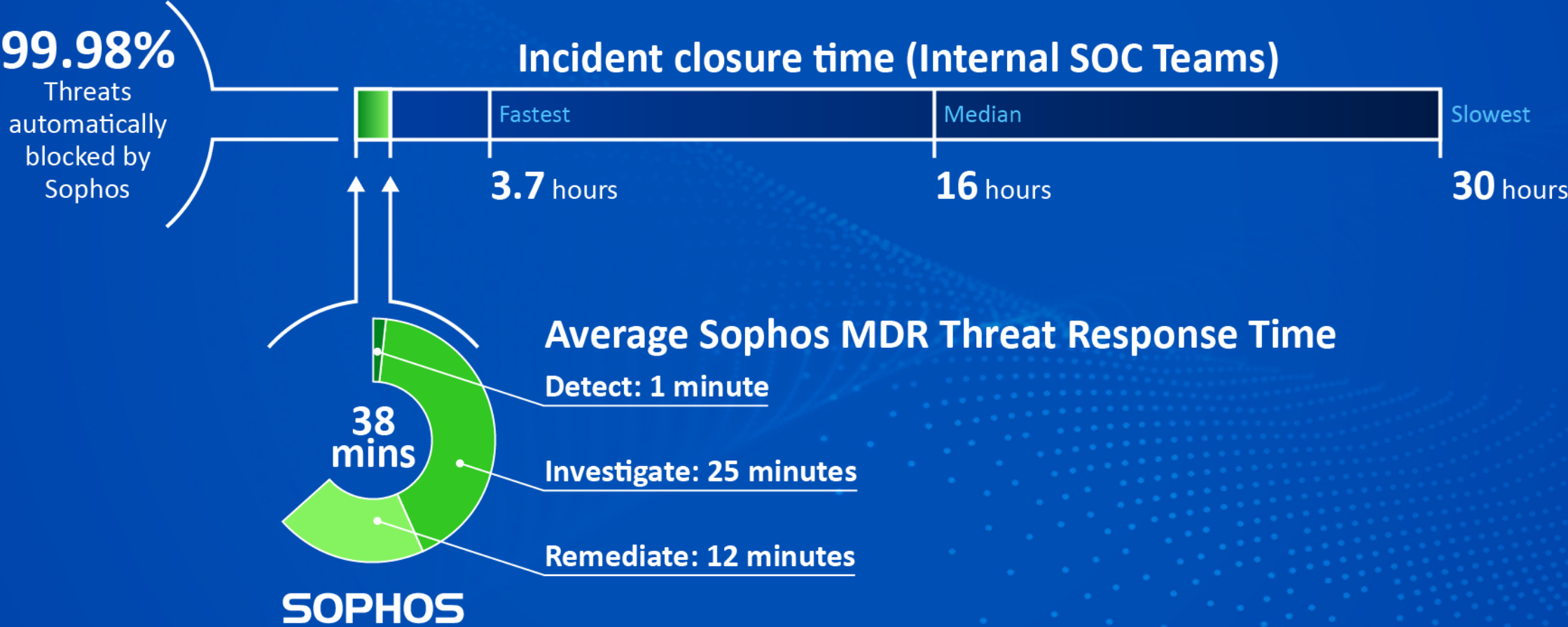
Detections

Cases

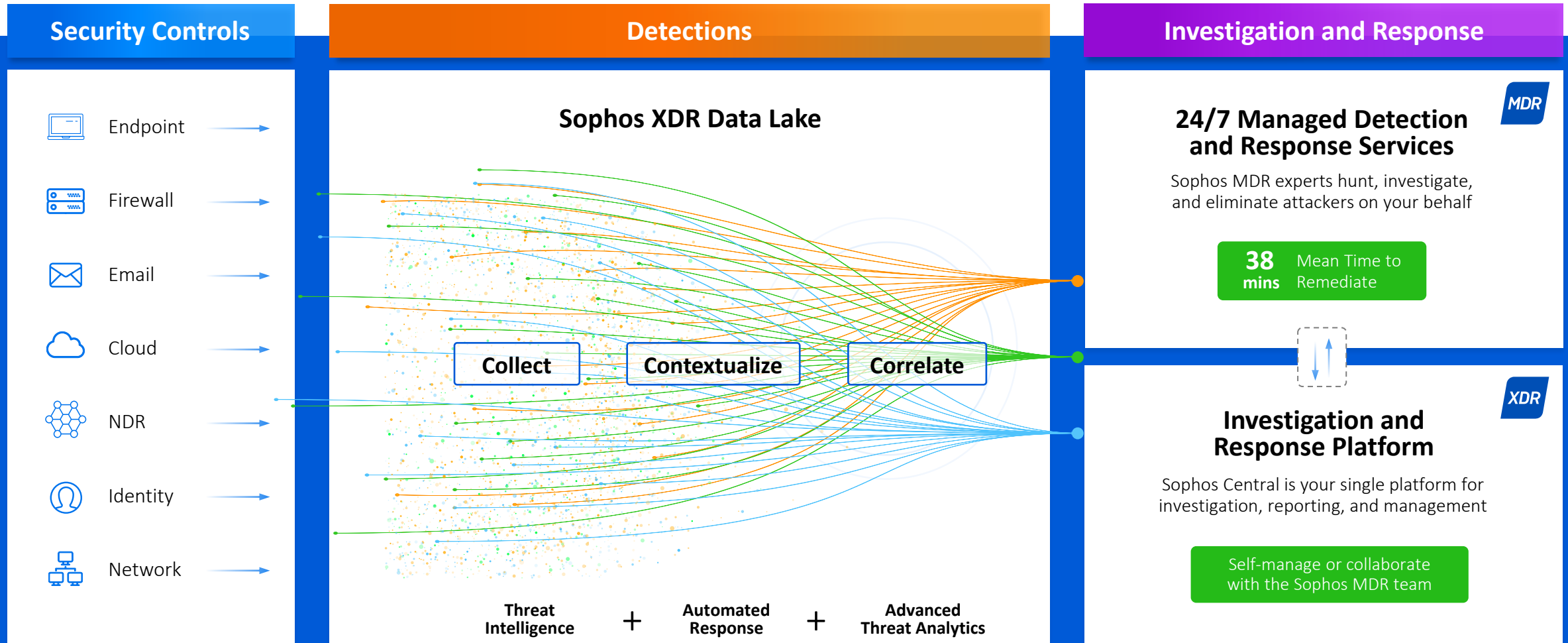
Escalations

Active Threats

Leading Detection and Response Times



Security Operations Center: Managed By You or Us



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 Essential	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 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

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 MDR Is Simple to Quote and Purchase

ORGANIZATION SIZE

How many users?

300

How many servers?

50

DATA RETENTION PERIOD

☐ 90 Days
(included)

☒ 1 Year

SERVICE TIER



Sophos MDR Complete



Sophos MDR



Sophos Threat Advisor



Onboarding Plus Package

SOPHOS INTEGRATIONS



XDR

Sophos XDR



Fw

Sophos Firewall



Em

Sophos Email



Ep

Sophos Endpoint



Cld

Sophos Cloud



NDR

Sophos NDR

THIRD-PARTY INTEGRATIONS



Endpoint Protection



Firewall



Public Cloud



Email



Identity



Network Security

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

Cybersecurity as a Service Is the Future of Cybersecurity

“Nobody has enough people to do security...you have to deliver it as a service. It’s not enough to sell software because most buyers don’t have the people who can use it. We see a huge interest in managed security services - because this whole security market is becoming far too complicated for the average organization.”

*Peter Firstbrook, Gartner
Venturebeat, March 2022*

Gartner

“The threat landscape is simply too big and too complex. Cybersecurity as a service is a critical tool for organizations to be able to mitigate that as much as they possibly can.”

*Scott Crawford, 451 Research
August 2022*



Visit our booth at the expo area

Thank You



Value Added Distributor



Affordable Cutting Edge