



# SOPHOS

## Kybernetická bezpečnost jako služba

Mgr. Ondrej Vlach  
Senior Distribution Account Executive – SOPHOS Eastern Europe

14.9.2023

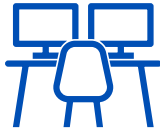
**SOPHOS**

**Cybersecurity has become too complex for most organizations to manage effectively.**

# Findings from an Independent Survey of IT Professionals



**3,000**  
respondents



**100-5,000**  
employees



**14**  
countries



**<\$10M - \$5B+**  
Annual revenue



**Jan-Mar 23**  
research conducted

Learn More  
[www.sophos.com/ransomware2023](http://www.sophos.com/ransomware2023)

The State of  
Ransomware  
2023

# The Hard Truth

**66%**

of organisations hit by  
ransomware

**76%**

of attacks successfully  
encrypted data

**30%**

Encrypted data was  
also stolen

**46%**

of organisations paid  
the ransom

**70%**

Used backups to  
restore data

**97%**

Got Encrypted Data Back

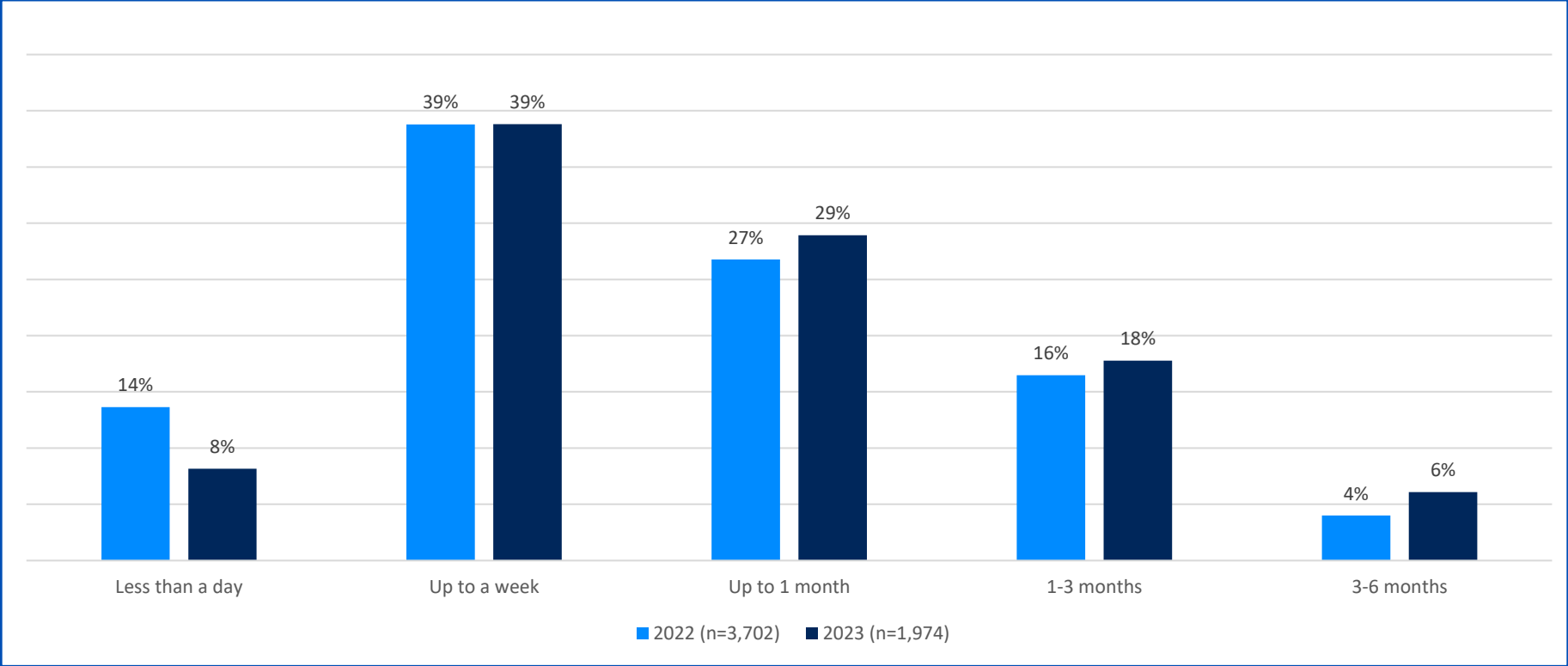
**\$1.54m**

Average Ransom Payments

**\$1.82m**

Average ransomware  
recovery cost

# Recovery Time 2022 vs. 2023



How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart

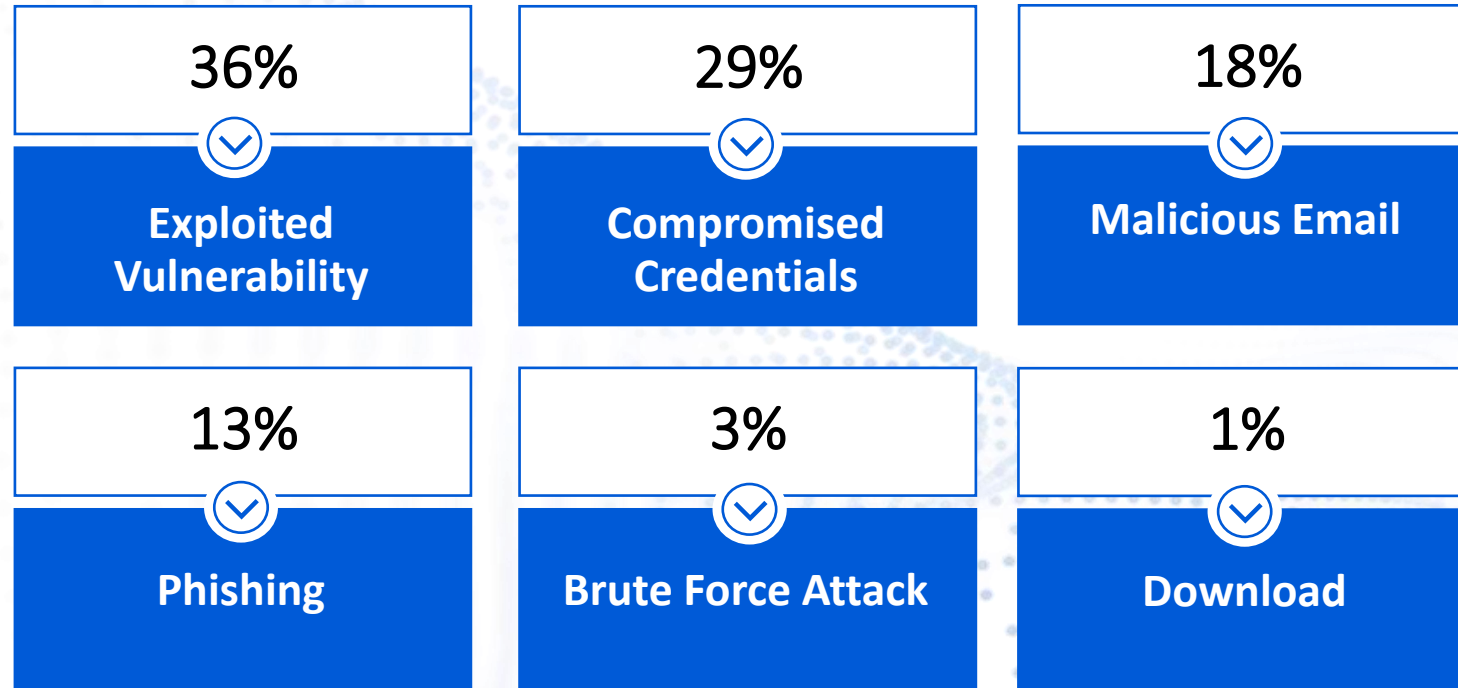
# Business Impact

**84%**

Of organizations hit by  
ransomware said the  
attack caused them to  
lose business/revenue

*Did the ransomware attack cause your organization to lose business/revenue? Yes, we lost a lot of business/ revenue, Yes, we lost a little business/ revenue. n=1.523 private sector organizations that were hit by ransomware*

# Root Cause of Attack



7 Do you know the root cause of the ransomware attack your organization experienced in the last year? If you were hit more than once, think about the most significant attack (n=1,974 organizations hit by ransomware in the last year)

# Recommendations

## Strengthen Defensive Shields

- Protection against the most common attack vectors
- Adaptive technologies that respond automatically to an attack
- 24/7 threat detection, investigation and response

## Optimize Attack Preparation

- Taking regular backup
- Practicing recovering data from backups
- Maintaining an up-to-date incident response plan

## Maintain Good Security Hygiene

- Timely patching
- Regularly reviewing security tool configuration





**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<sup>1</sup>
- **78% increase** in the number of organizations hit by ransomware last year<sup>1</sup>
- “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<sup>2</sup>

## 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<sup>3</sup>

<sup>1</sup>The State of Ransomware 2022, Sophos; The Active Adversary Playbook 2022, Sophos

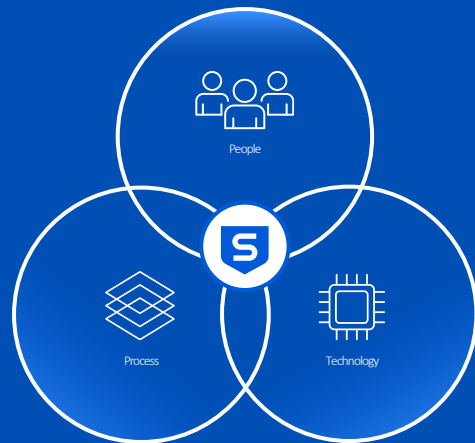
<sup>2</sup>Statista: <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

<sup>3</sup>Ponemon 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**



- ✓ **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

**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 Sophos Advantage

**More organizations trust Sophos for MDR than any other vendor.**



Sophos delivers leading cybersecurity outcomes for over **554,000 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**



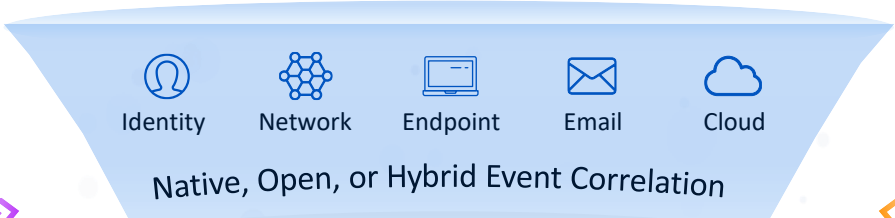
**A Proven, Trusted and Leading MDR Provider**





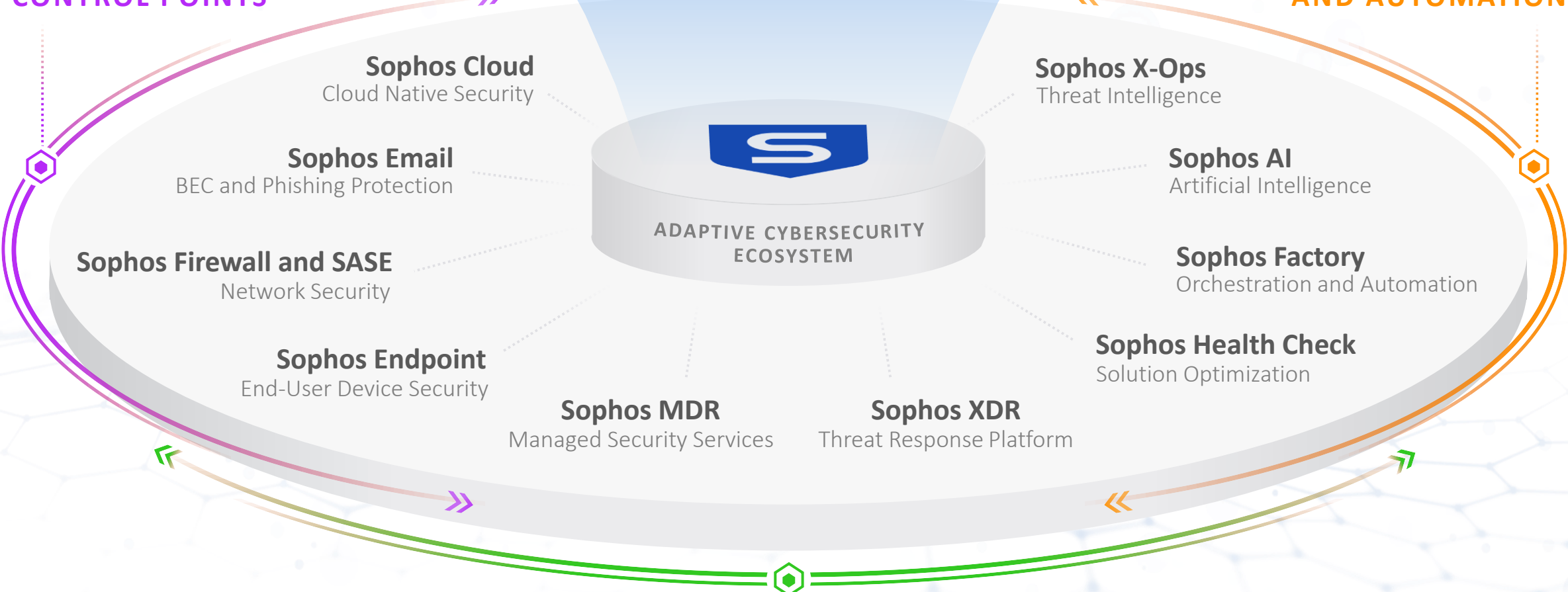
**Cybersecurity as a Service seamlessly combines world-leading services, technologies, expertise and tools in one holistic solution.**

# Delivering Optimal Cyber Security Outcomes



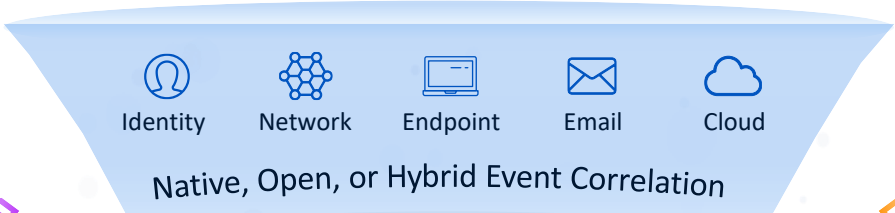
**SECURITY CONTROL POINTS**

**OUTCOME OPTIMIZATION AND AUTOMATION**

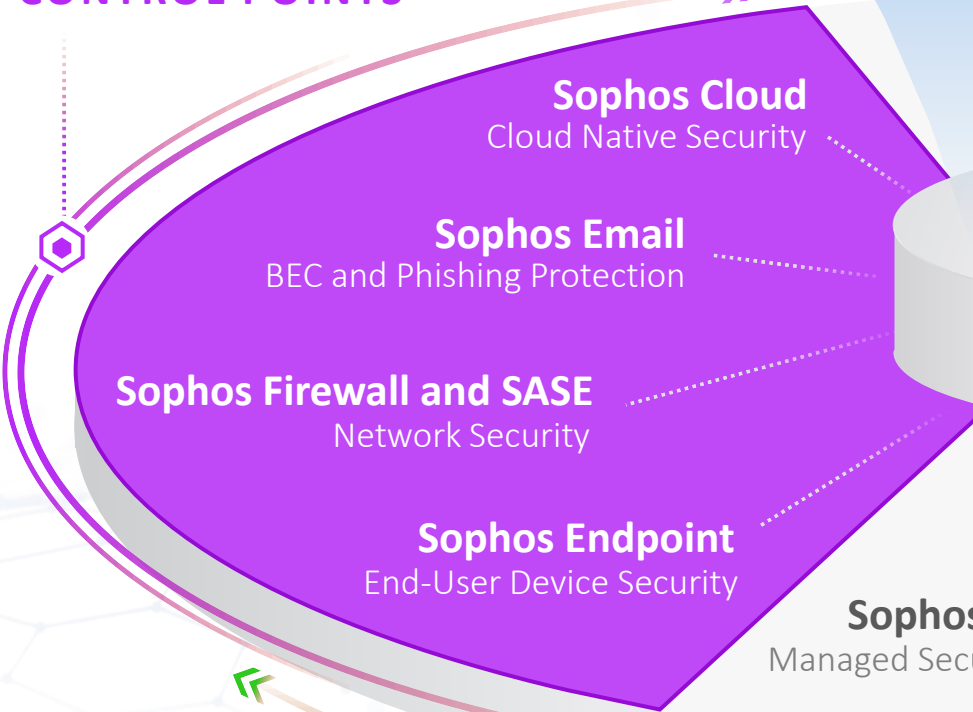


**THREAT DETECTION AND RESPONSE**

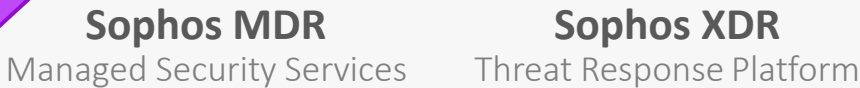
# Delivering Optimal Cyber Security Outcomes



## SECURITY CONTROL POINTS



## OUTCOME OPTIMIZATION AND AUTOMATION



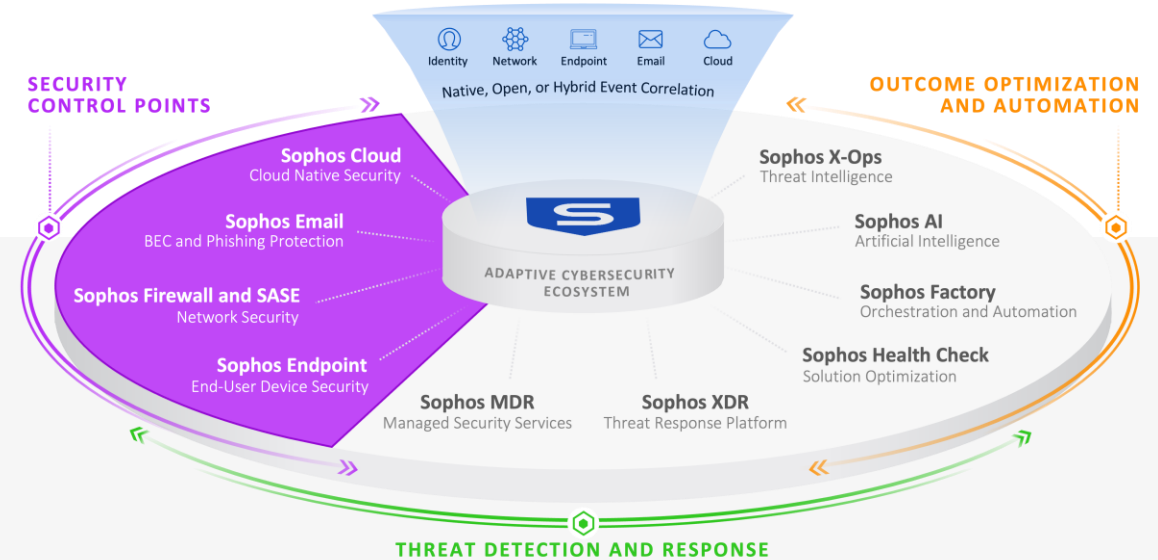
## THREAT DETECTION AND RESPONSE



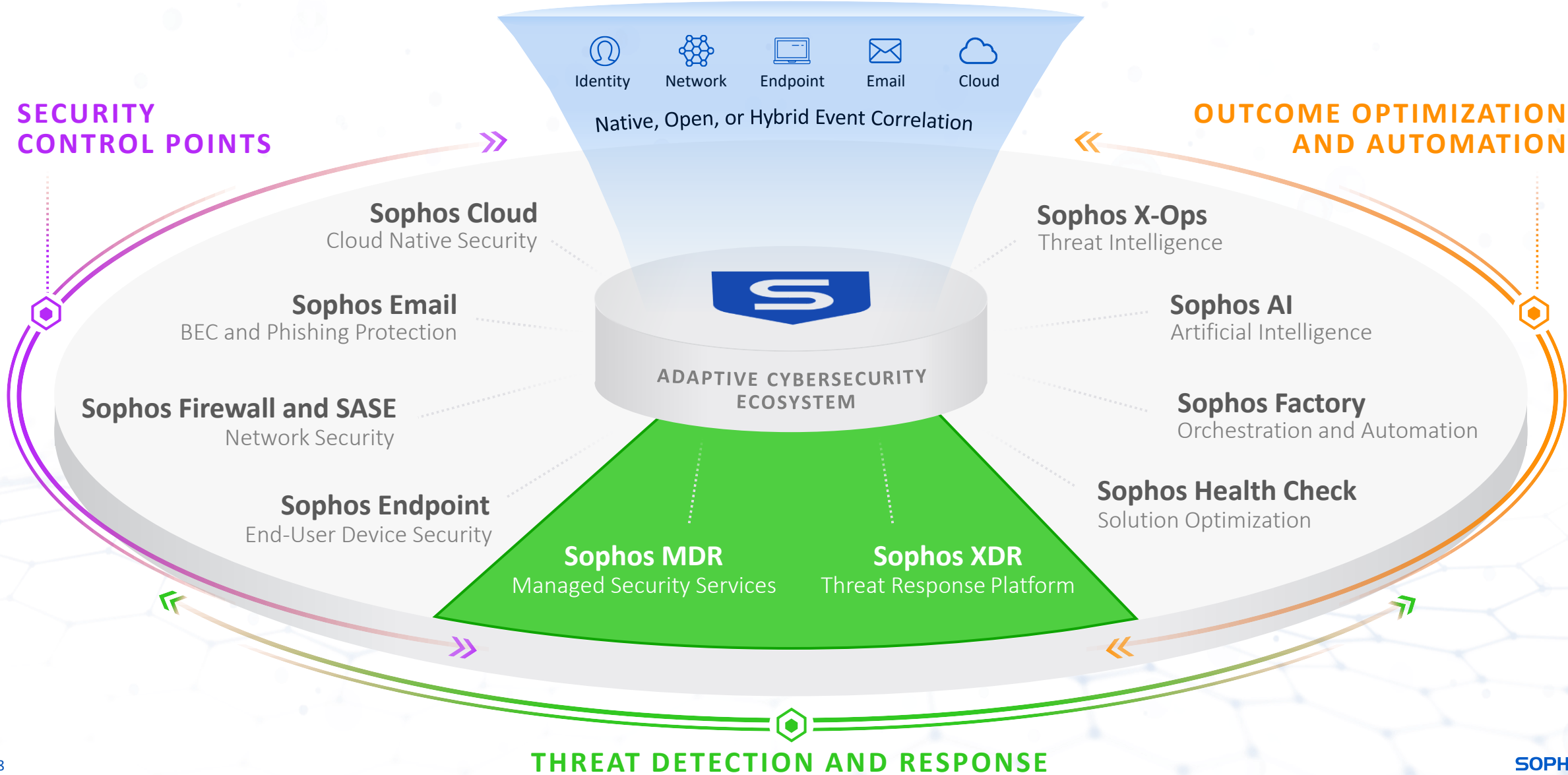
# Security Control Points

## Newly Released Innovations

- Adaptive Attack Protection
- Account health check
- Network security add new SD-WAN capabilities
- 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



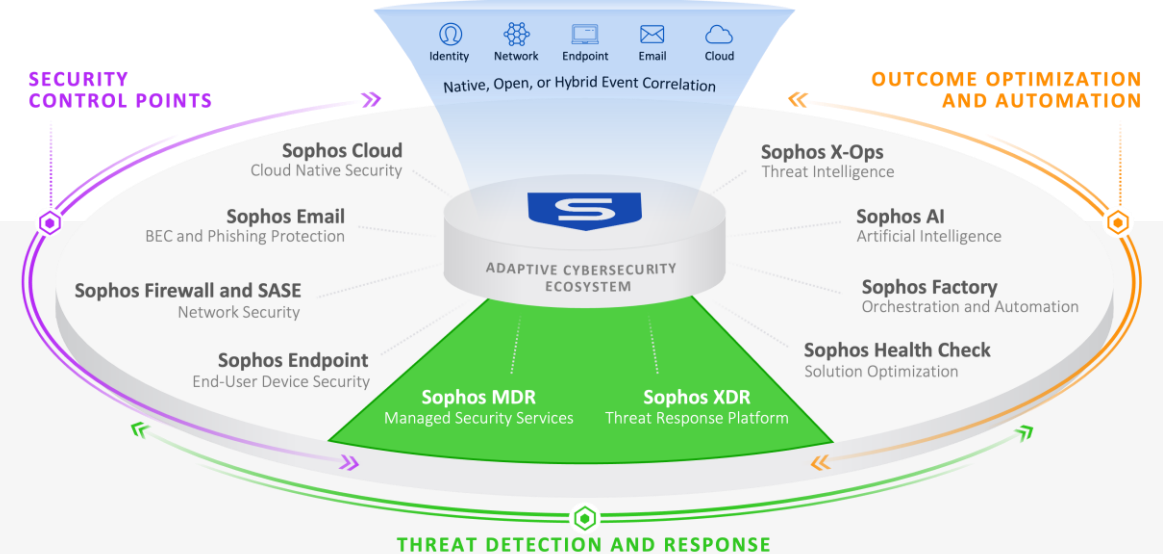
# Delivering Optimal Cyber Security Outcomes



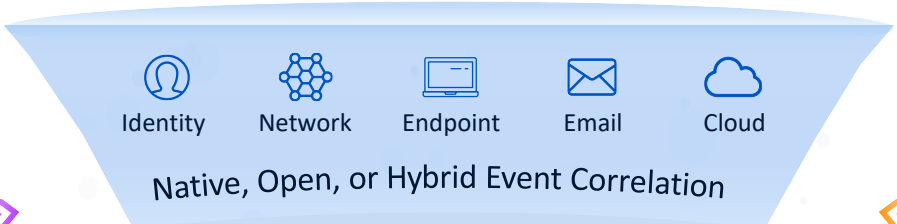
# Threat Detection and Response

## Newly Released Innovations

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

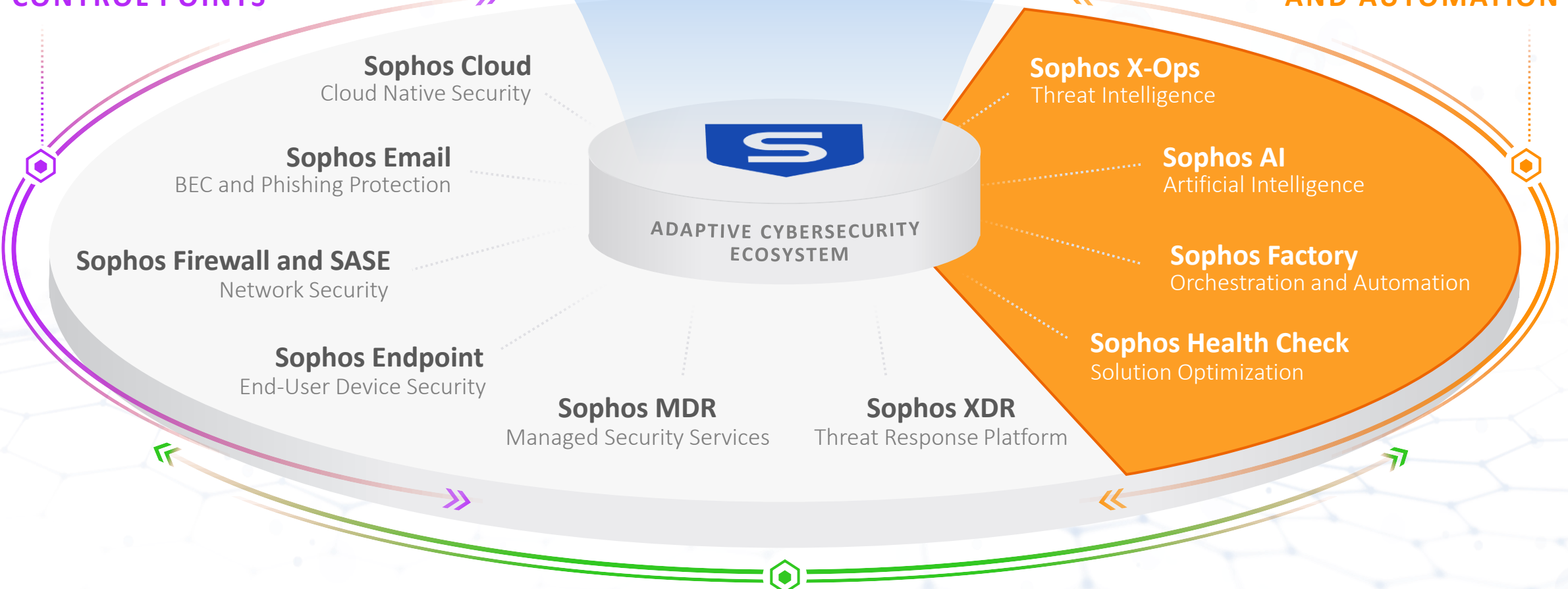


# Delivering Optimal Cyber Security Outcomes



## SECURITY CONTROL POINTS

## OUTCOME OPTIMIZATION AND AUTOMATION

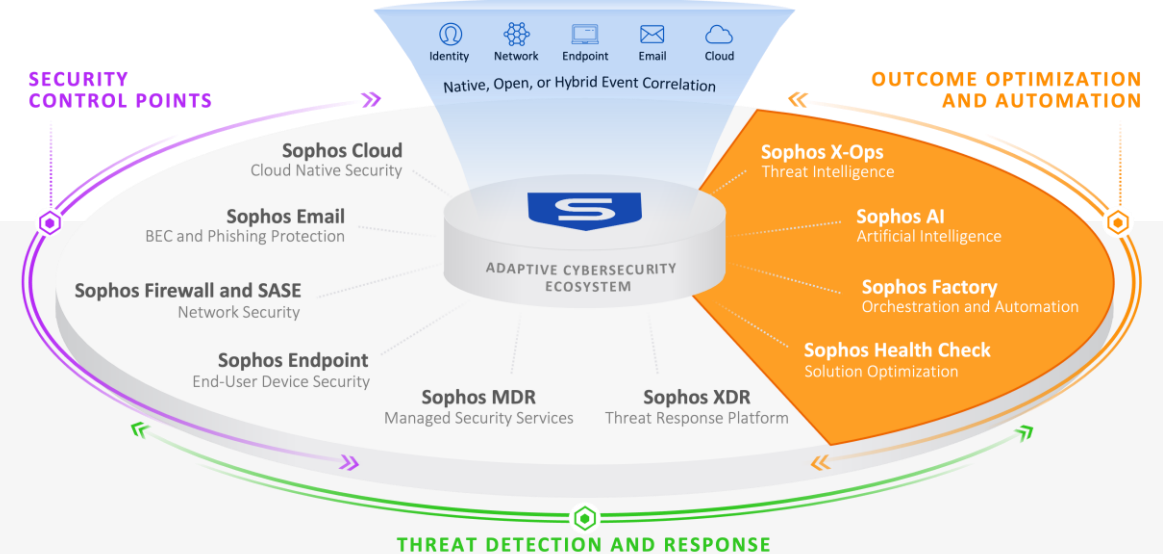


## THREAT DETECTION AND RESPONSE

# 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 Products and Services

## 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

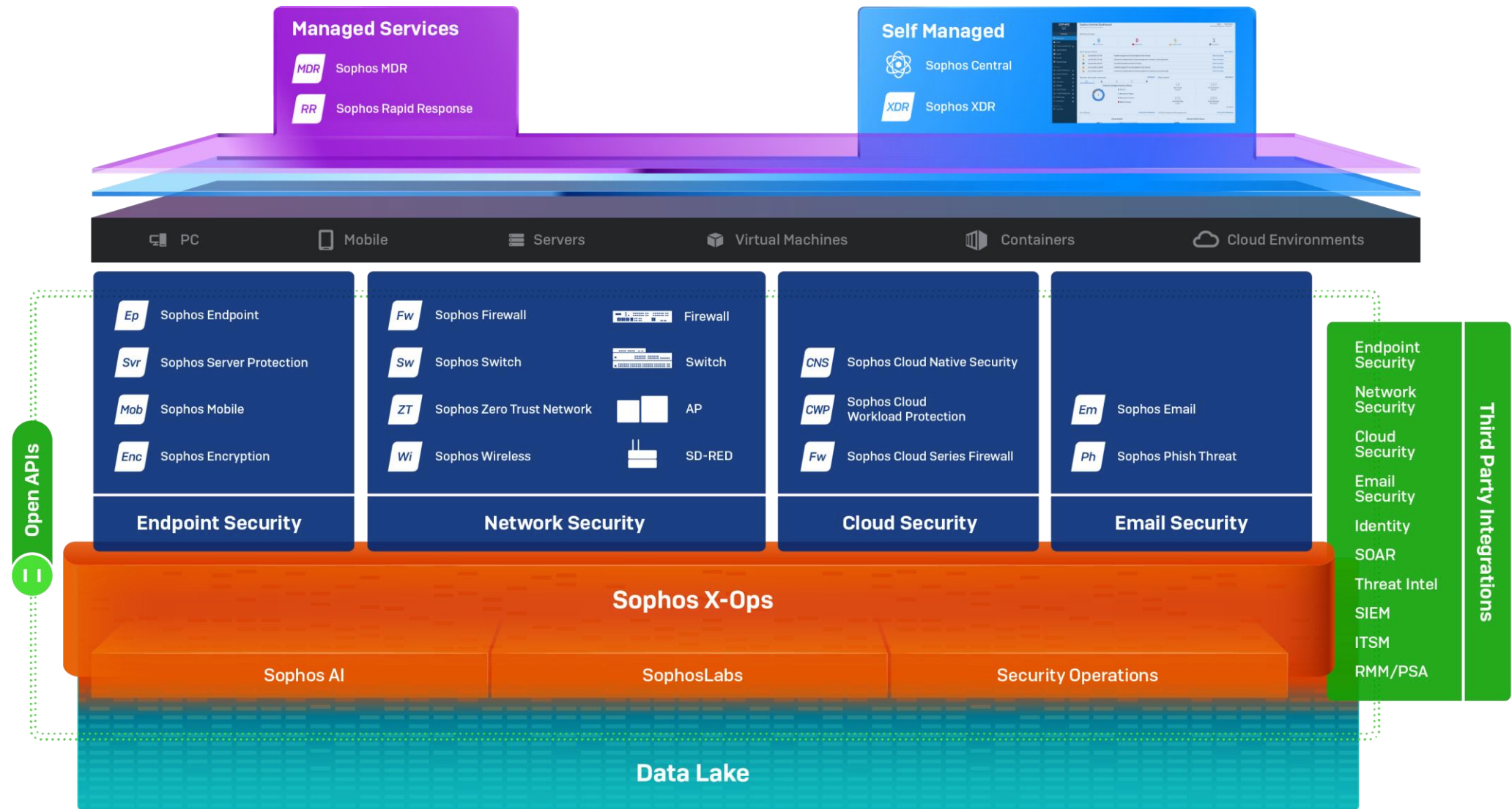


## Sophos AI Data Scientists

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



# Adaptive Cybersecurity Ecosystem





# Cybersecurity as a Service



Instant **Security Operations Center**:  
Managed by us, by you, or both.



World-class integrated **cybersecurity defenses** that work with what you already have.



An **expert team** of cybersecurity professionals.



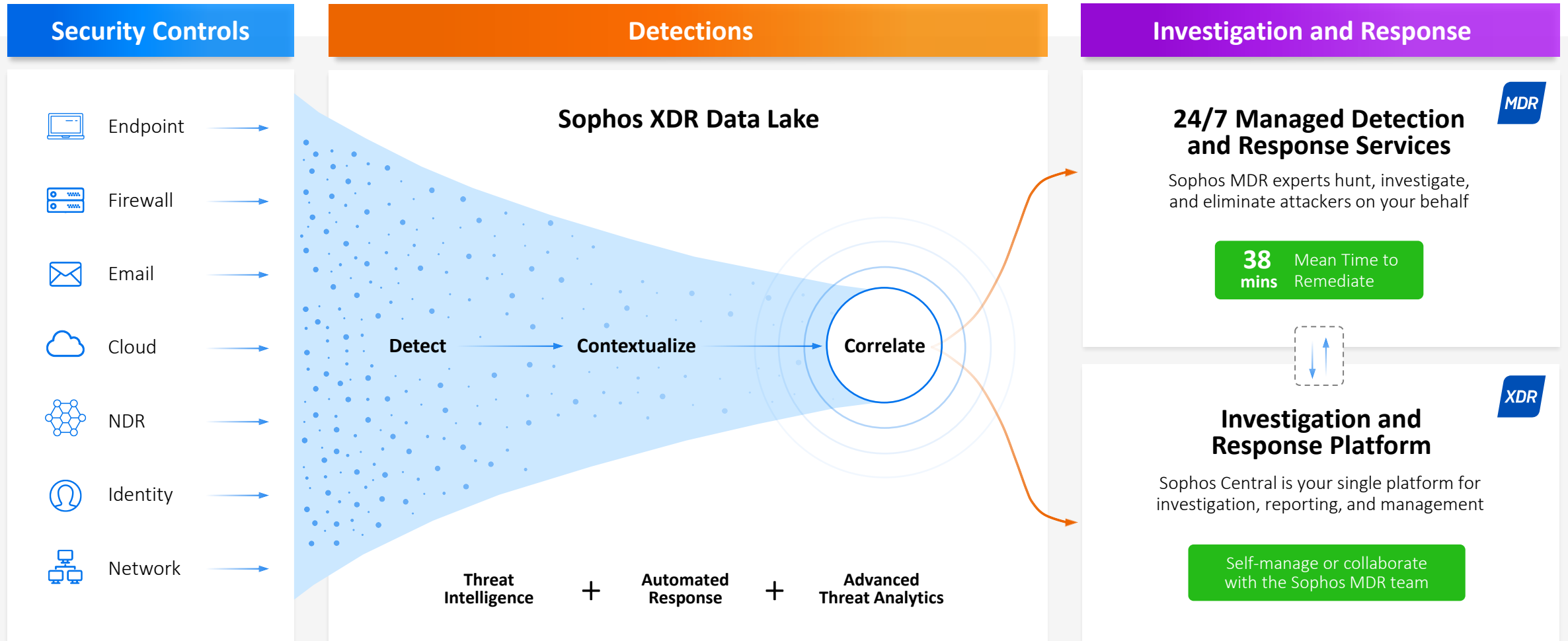
Managed through an **intuitive cloud-based security platform**.



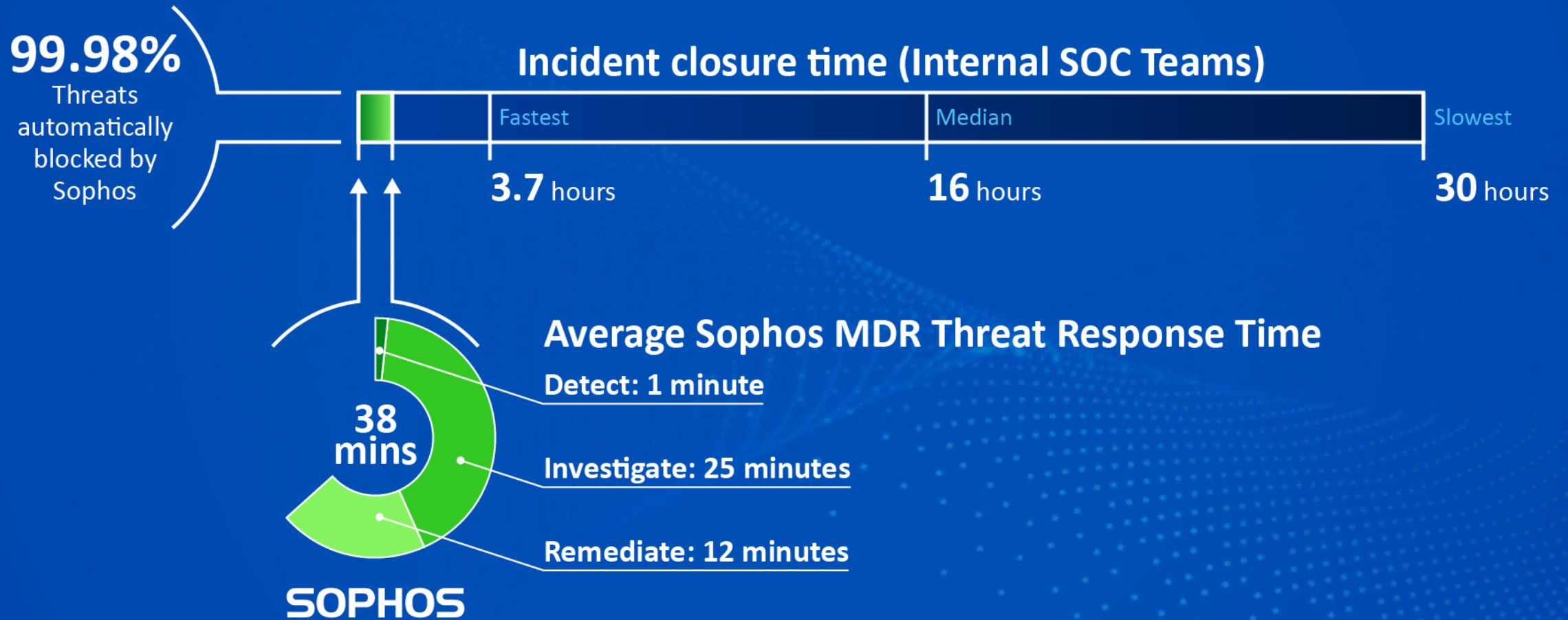


**Cybersecurity as a Service leverages your existing IT investments to optimize prevention and reduce detection and response time.**

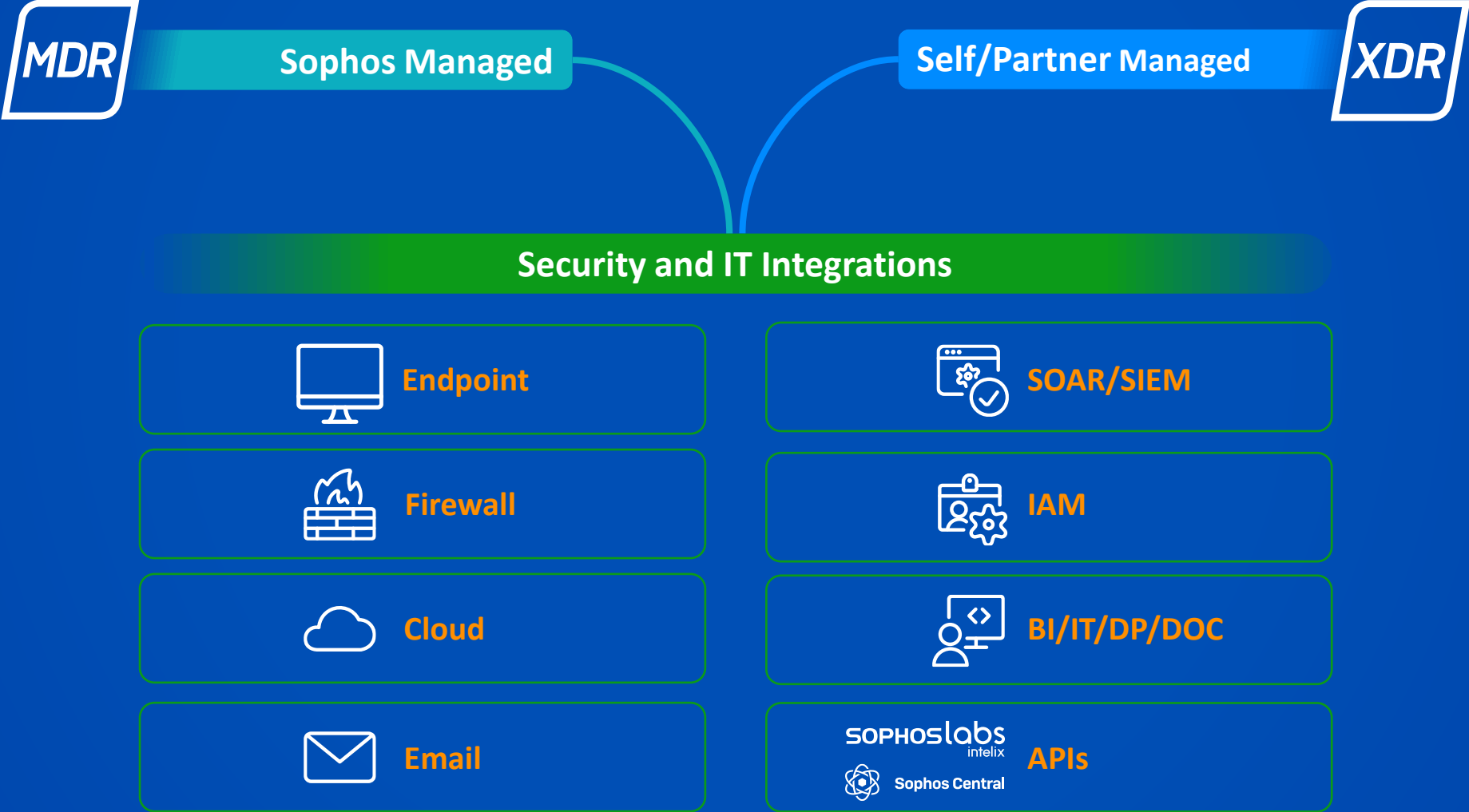
# Security Operations Center: Managed By You or Us



# Leading Detection and Response Times



# Integrating With Your Existing IT Investments



# Proven. Trusted.

## Customer Growth

One of Largest and Fastest-Growing  
MDR Service Providers

**554,000+ Customers**  
100+ million devices protected

**55,000+ Channel Partners**  
10,000+ MSPs

**16,000+ MDR Customers**  
Thousands of Investigations

## Industry Analysts

13-time Gartner  
Magic Quadrant Leader

**Leader: Endpoint Protection Platforms**  
Gartner Magic Quadrant

**Best Enterprise Endpoint Solution**  
SE Labs

**100% Protection/Usability Scores**  
AV-Test

## 3<sup>rd</sup> Party Testing

Award-Winning  
Product and Services

**Winner: Best Managed Security Services**  
Channel Partner Insight Awards

**No. 1 Ranked MDR Service**  
Gartner Peer Insights

**Customers' Choice for EPP and Firewall**  
Gartner

As mentioned in Gartner® Peer Insights™ Based on reviews in the last 12 months as of March 23, 2023

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.

# Gartner Peer Insights™

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



4.8

Average Rating

97%

Would Recommend

Based on 273 Reviews



4.8

Average Rating

95%

Would Recommend

Based on 385 Reviews



4.7

Average Rating

91%

Would Recommend

Based on 241 Reviews



4.5



4.8\*



4.8\*



4.4



4.6



4.5



4.7



4.5



4.5

Reviews from last 12 months as of March 23, 2023

\*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.



# 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*



# Sophos: Delivering Superior Security Outcomes Through Cybersecurity as a Service



## Stop Advanced Human-led Attacks, Including Ransomware

Our expert team stops advanced human-led attacks on your behalf, neutralizing threats before they can disrupt business operations or compromise sensitive customer data.



## Focus on Growing Your Business

We monitor, detect, and respond to threats, enabling you and your IT team to focus on strategic initiatives that drive growth for your business.



## Community Immunity

Sophos delivers cybersecurity for over 530,000 organizations, giving us greater visibility into both widespread and targeted attacks, with systems to operationalize novel threat intelligence to proactively defend all our customers.



## Build on Your Existing Protection

Sophos MDR leverages signals from across your existing ecosystem to identify and investigate suspicious activities that may require human intervention.



## Sleep Better Knowing We Have You Covered

Proactive 24/7/365 threat monitoring, investigation, and response performed by a team of highly-trained expert analysts means you can relax knowing we “have your back”.



**SOPHOS**  
Cybersecurity delivered.

# 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

# Sophos MDR: Industry-Leading Openness and Flexibility

## **MDR** Sophos MDR

### Compatible with your environment

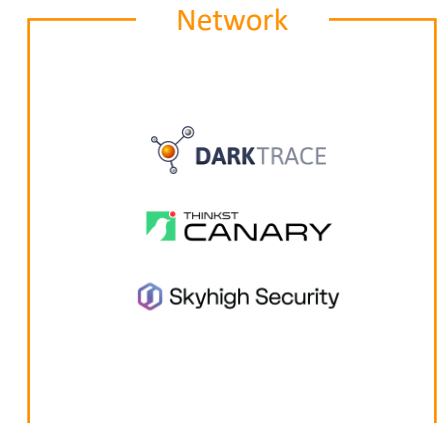
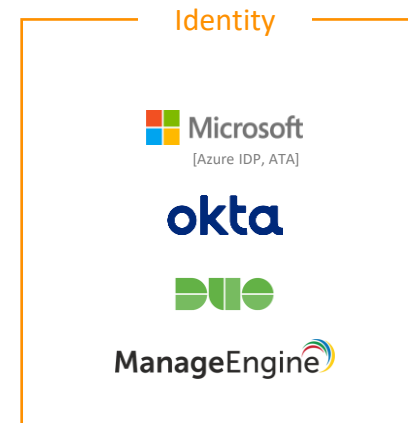
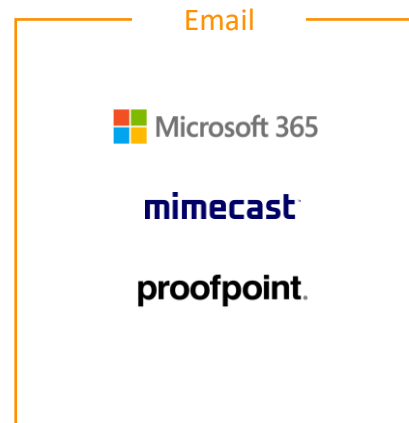
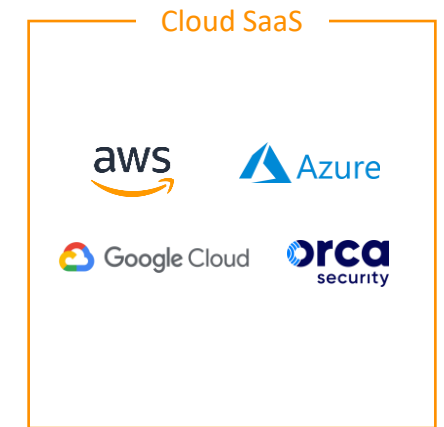
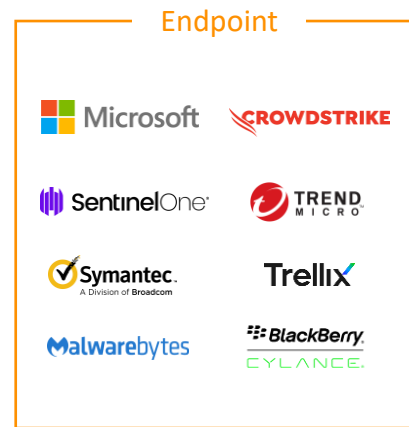
We can use our tools, another vendor's tools or any combination of the two

### 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



# Monthly and Weekly Cybersecurity Reports

The image displays several overlapping screenshots of Sophos cybersecurity reports for Aztec Corp. Ltd. The reports are organized into sections:

- Weekly Report (March 1, 2022 - March 6, 2022):** Shows 'Detections by Integrations' with a bar chart for Firewall, IPS, and Network. It also lists 'Top 10 Devices with Most Detections' and 'Top 5 Detections' with a table of detection names and counts.
- Monthly Report (March 1, 2022 - March 31, 2022):**
  - Sophos XDR Protection Rating:** Shows an 'Optimal' status with 46,826,472 events blocked and 1,300 detections.
  - Event Pipeline:** A funnel chart showing 46,826,472 events, 93,651 detections, 214 cases, 34 escalations, and 12 active threats.
  - Total Licenses Deployed:** A bar chart showing 100 licenses used out of 250.
  - Sophos MDR Cases:** Shows a total of 214 cases with an average response time of 60 minutes.
  - Cases by Status:** A bar chart showing 24 new, 110 in progress, 20 action required, and 60 resolved/closed cases.
  - Cases by Type:** A line chart showing trends for MDR Investigation, Health Check, and Customer Requested Investigation.
  - Case Activity by Detection Source:** A line chart showing activity for Endpoint, Server, Cloud Optix, and Firewall.
  - Mitre ATT&CK Framework:** A donut chart showing 23,882 detections across various categories like 'Exploitation for Client Execution' and 'Inter-Process Communication'.

# 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		✓	✓
<b>Threat Containment: attacks are interrupted, preventing spread</b> <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		✓	✓
<b>Full-scale Incident Response: threats are fully eliminated</b> <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			✓

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

# 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 Breach Protection Warranty



At Sophos, we make your cybersecurity our responsibility. The Sophos Breach Protection Warranty is included at no additional charge with our Sophos MDR Complete subscription. It covers up to \$1 million in response expenses for qualifying customers.

## Trusted Protection for Complete Peace of Mind

More organizations trust Sophos for MDR than any other security vendor. With the Sophos Breach Protection Warranty, Sophos MDR Complete customers enjoy the reassurance and peace of mind that comes with having financial coverage if a breach happens.

## Clear, Comprehensive Coverage

- Automatically provided – no need to apply
- Included with one-, two-, and three-year subscriptions
- Included with new and renewal license purchases
- Covers endpoints, servers, and devices running Windows and macOS
- No warranty tiers that restrict coverage
- No additional license purchase requirements

## Included with Sophos MDR Complete

The warranty is included automatically and at no additional charge with new purchases or renewals of Sophos MDR Complete annual subscriptions. There are no warranty tiers, minimum contract terms, or additional purchase requirements.

## Up to \$1 Million in Response Expenses

The warranty covers response expenses following a ransomware incident within an environment protected by Sophos MDR Complete:

- Up to \$1,000 per breached machine
- Up to \$1 million in total response expenses
- Up to \$100,000 ransom payment (as part of per-device limit)

Reflecting the reality of today's operating environments, breached machines include endpoints, servers, and Windows and macOS devices. The warranty covers a wide range of incurred expenses, including data breach notification, PR, legal, and compliance.

## Warranty Overview

- Up to \$1 million in total response expenses
- Up to \$100,000 for ransom payment (as part of per-device limit)
- Up to \$1,000 per breached machine
- Covers a range of incurred expenses, including data breach notification, PR, legal, and compliance

For full terms and conditions of the warranty, visit [www.sophos.com/legal](http://www.sophos.com/legal)

# 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



Guided Onboarding

## SOPHOS INTEGRATIONS



Sophos XDR



Sophos Firewall



Sophos Email



Sophos Endpoint



Sophos Cloud



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 MDR 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