Annex NET - Partnerský den

22.6.2023

SOPHOS

Annex NET - Partnerský den

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

22.6.2023

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

The State of Ransomware 2023

SOPHOS

The Hard Truth

66%
of organisations hit by ransomware

76%
of attacks successfully encrypted data

30%
Encrypted data was also stolen

70%
Used backups to restore data

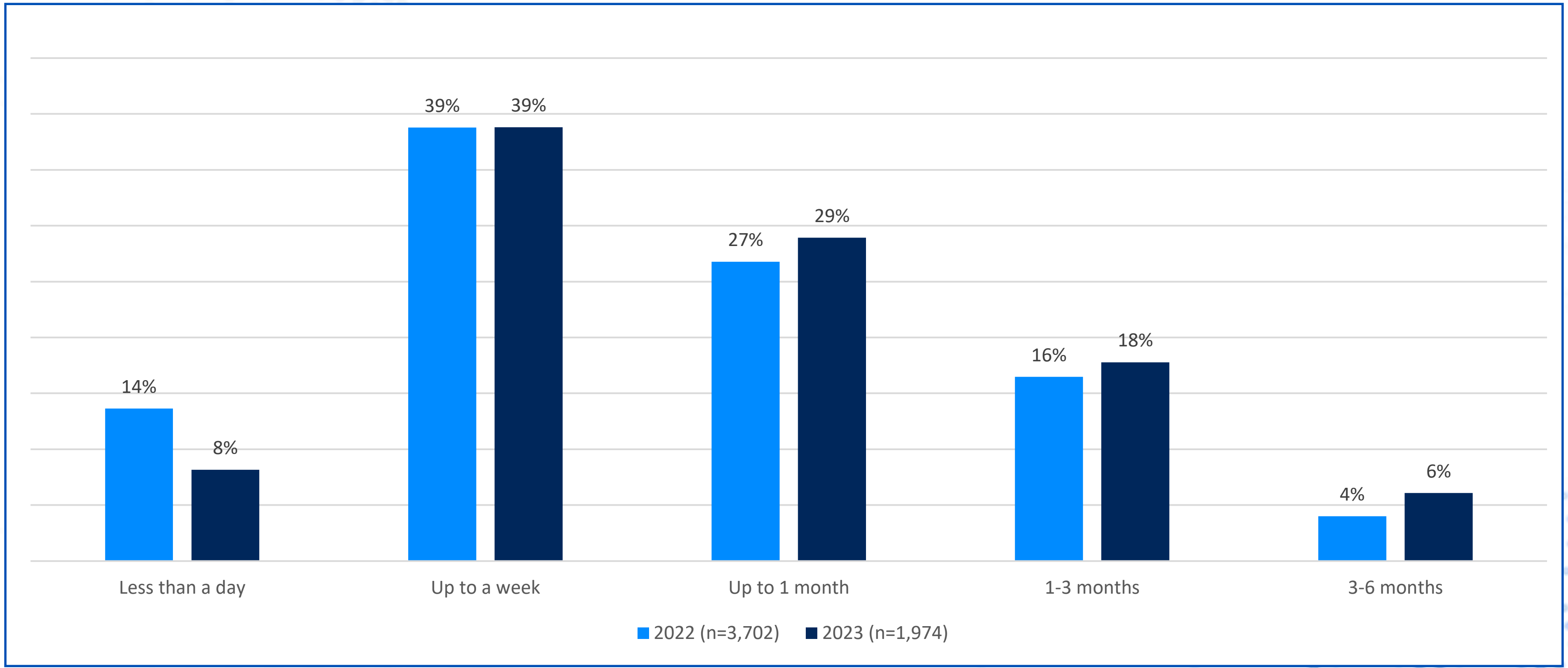
46%
of organisations paid the ransom

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*

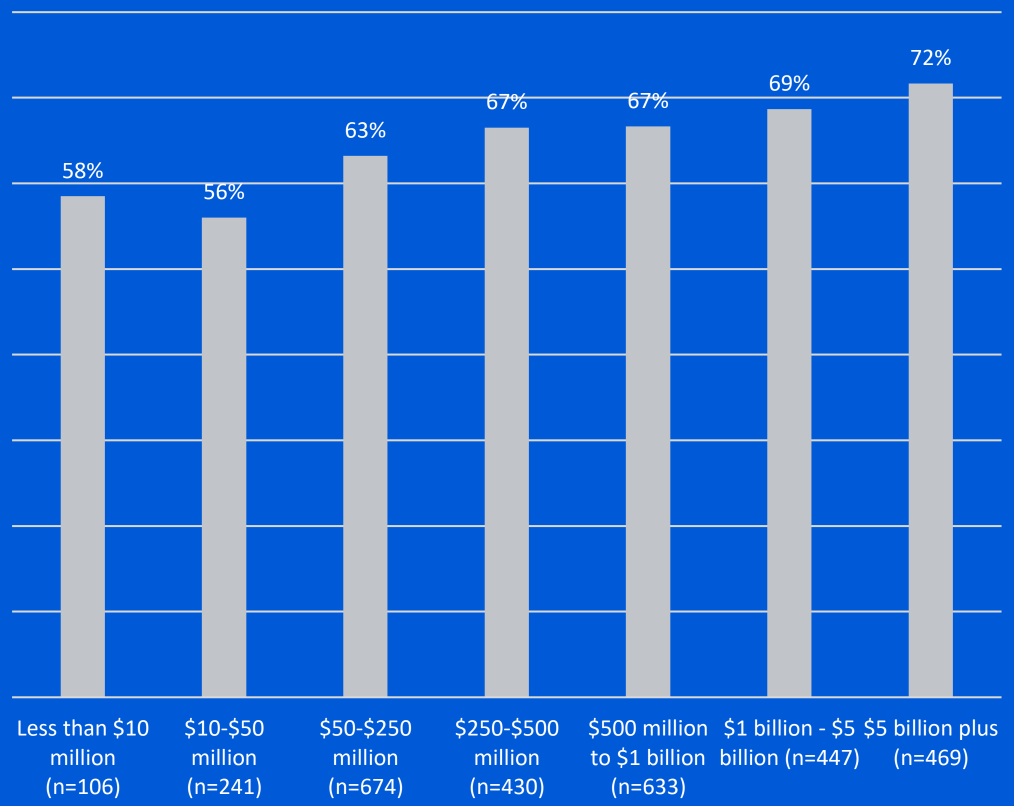
Rate of Ransomware Attacks: Revenue vs Size

- Number of employees had little impact on rate of ransomware attacks:

□ 100-250 employees:	62%
□ 250-500 employees:	62%
□ 501-1,000 employees:	62%
□ 1,001-3,000 employees:	73%
□ 3,001-5,000 employees:	63%

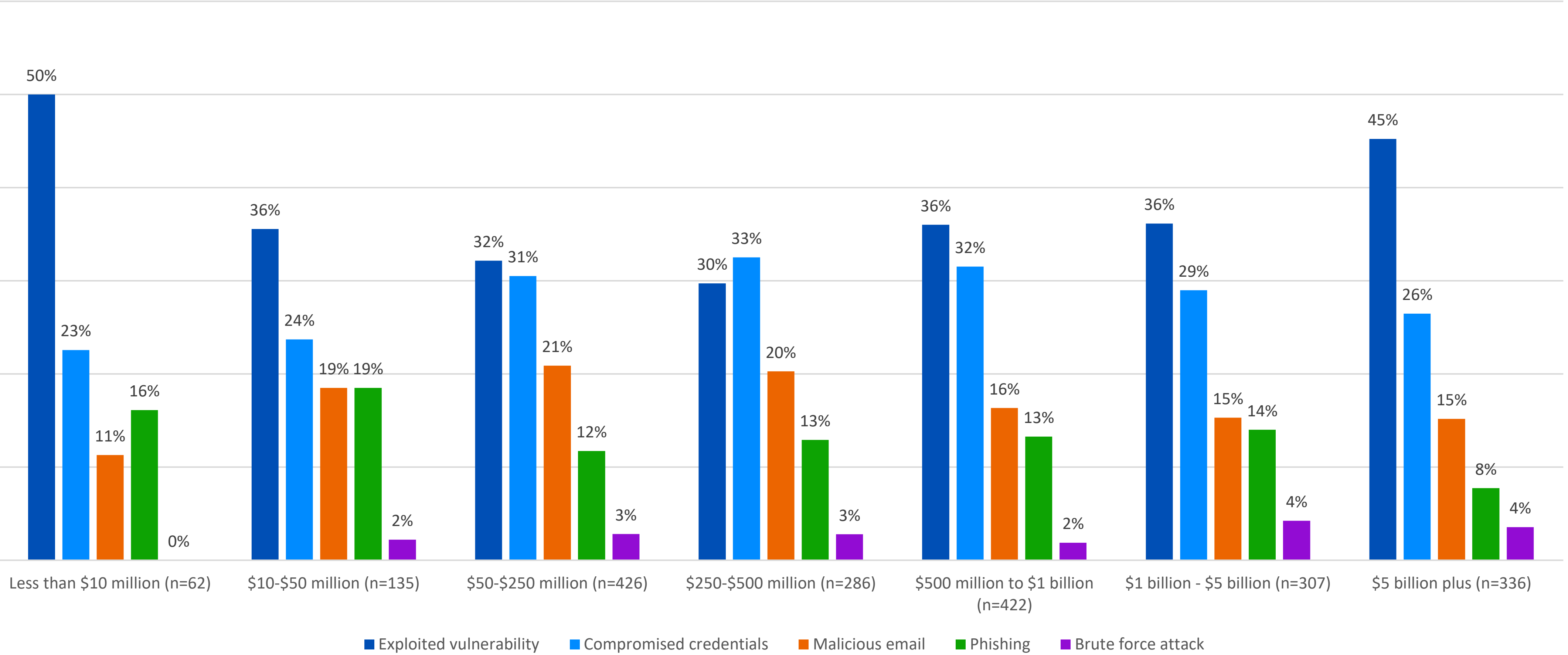
- There is a greater alignment between annual revenue and rate of attack, with the highest revenue organizations most likely to have been hit.

Percentage of Organizations Hit by Ransomware by Revenue



In the last year, has your organization been hit by ransomware? Yes. Base numbers in chart

Root Cause of Attack by Revenue



Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Impact of Insurance on Encrypted Data Recovery

Percentage of ransomware victims that recovered encrypted data

98%

With a standalone cyber policy

97%

With a wider insurance policy that includes cyber

84%

Without a cyber policy

Did your organization get any data back? n=1,497 organizations that were hit by ransomware in the last year and had data encrypted

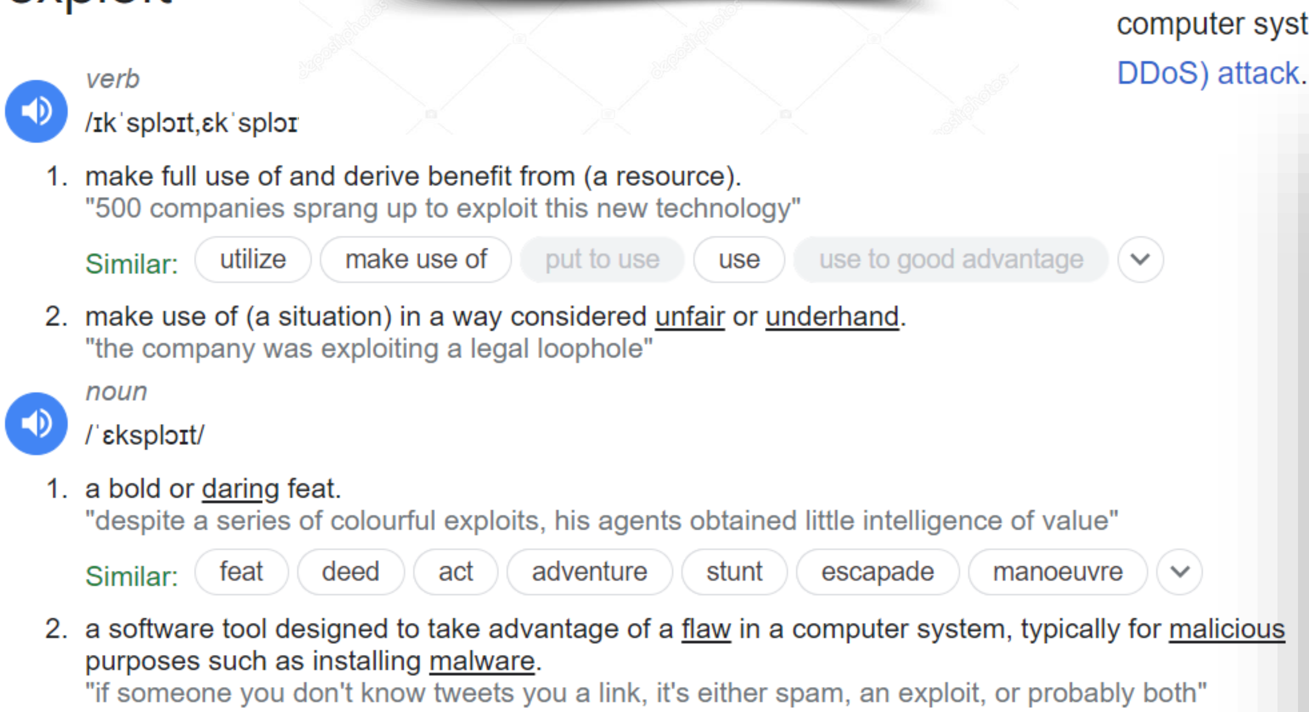
SOPHOS

Root Cause of Attack

36%	Exploited Vulnerability
29%	Compromised Credentials
18%	Malicious Email
13%	Phishing
3%	Brute Force Attack
1%	Download

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)

Exploit



exploit

verb

/ɪkˈsplɔɪt,ɛkˈsplɔɪ

1. make full use of and derive benefit from (a resource).
"500 companies sprang up to exploit this new technology"

Similar: utilize | make use of | put to use | use | use to good advantage

2. make use of (a situation) in a way considered unfair or underhand.
"the company was exploiting a legal loophole"

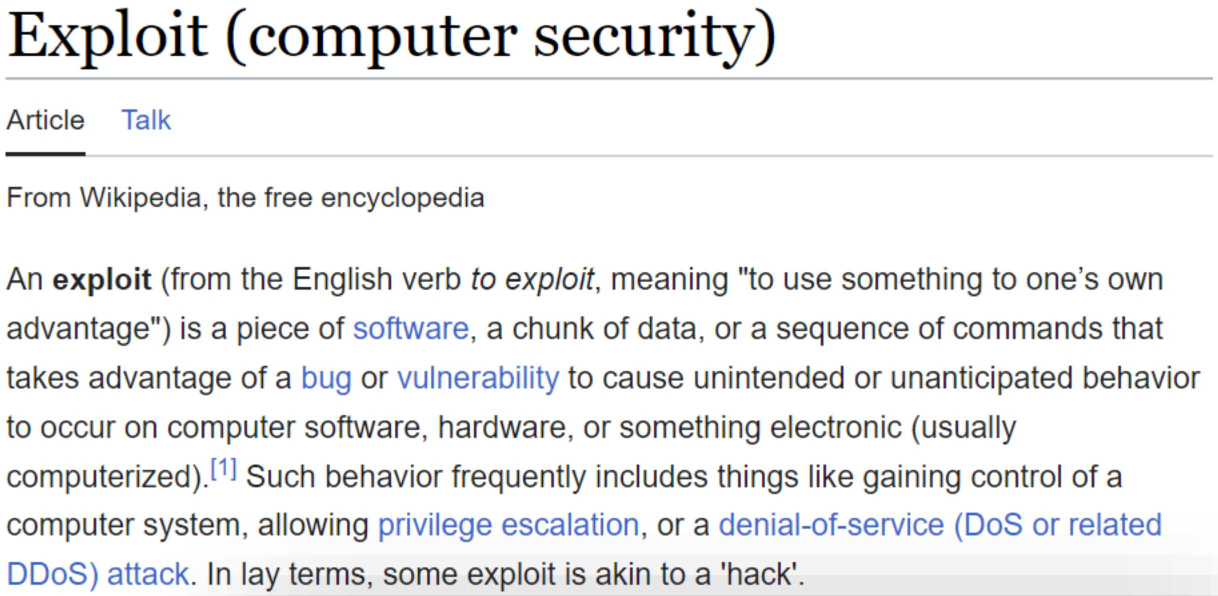
noun

/ˈɛksplɔɪt/

1. a bold or daring feat.
"despite a series of colourful exploits, his agents obtained little intelligence of value"

Similar: feat | deed | act | adventure | stunt | escapade | manoeuvre

2. a software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.
"if someone you don't know tweets you a link, it's either spam, an exploit, or probably both"



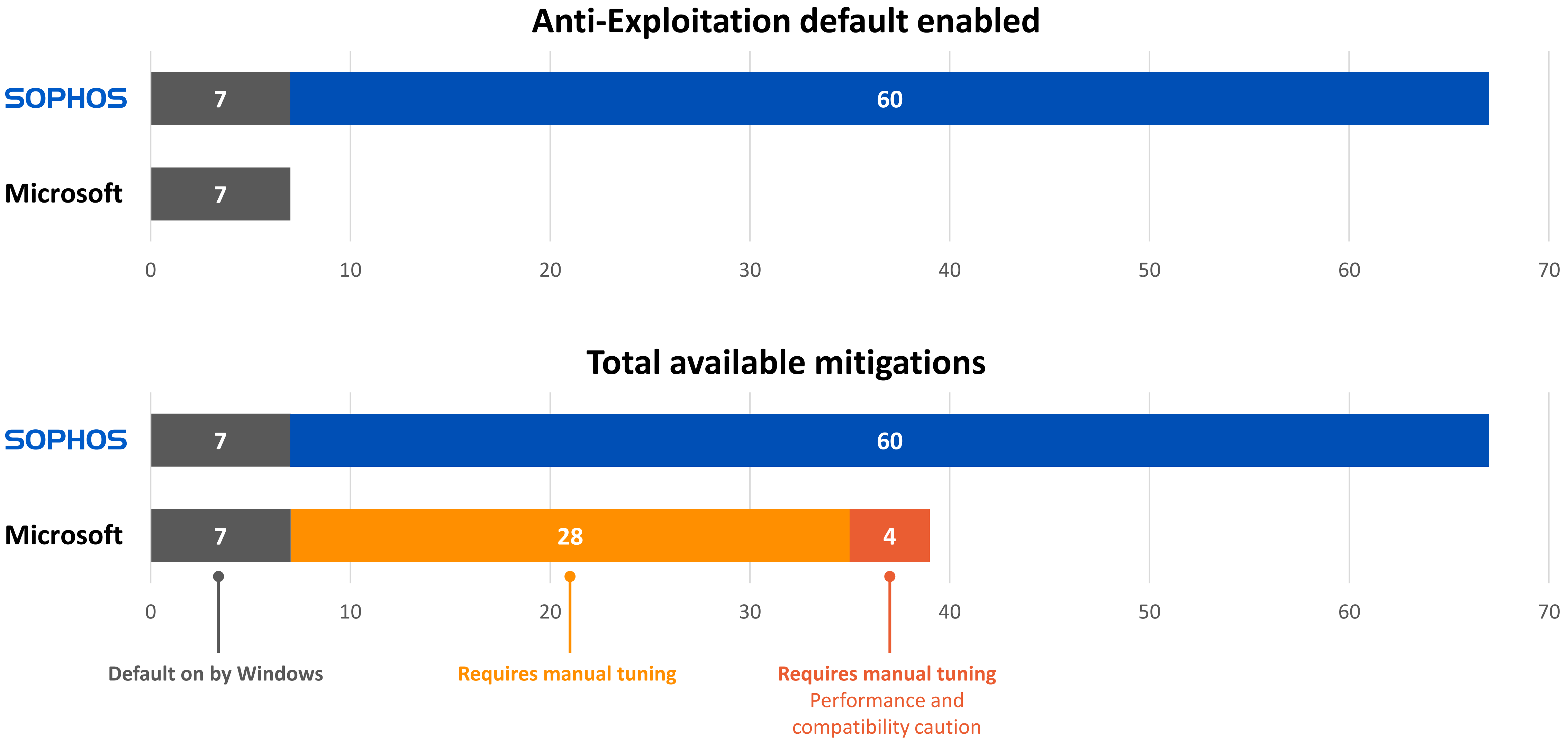
Exploit (computer security)

Article Talk

From Wikipedia, the free encyclopedia

An **exploit** (from the English verb *to exploit*, meaning "to use something to one's own advantage") is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).[1] Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack. In lay terms, some exploit is akin to a 'hack'.

Sophos Endpoint: Superior Exploit Prevention


Anti-Exploitation default enabled

Total available mitigations

Default on by Windows

Requires manual tuning

Requires manual tuning
Performance and
compatibility caution

More: https://sophos.com/microsoft

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[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

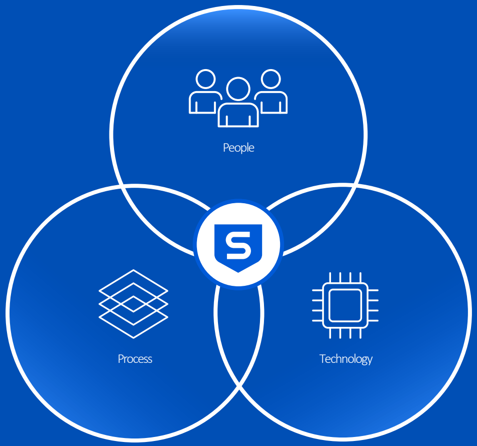
- The number of unfilled cybersecurity jobs worldwide **grew 350%** between 2013 and 2021
- In the US there are 1 million cybersecurity workers and **750,000 cybersecurity openings**
- Security Analysts cost $100-150K per year, and the annual cost to maintain a SOC is $2.86M[3]

[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

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

VANCOUVER CANUCKS

Sports and Hospitality
400 Employees

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

Manufacturing
200 Employees

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

GREATER EFFICIENCY

2X More efficient IT Teams

London South Bank University

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."

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."

LOWER COSTS

5X Less expensive than managing in-house

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."

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

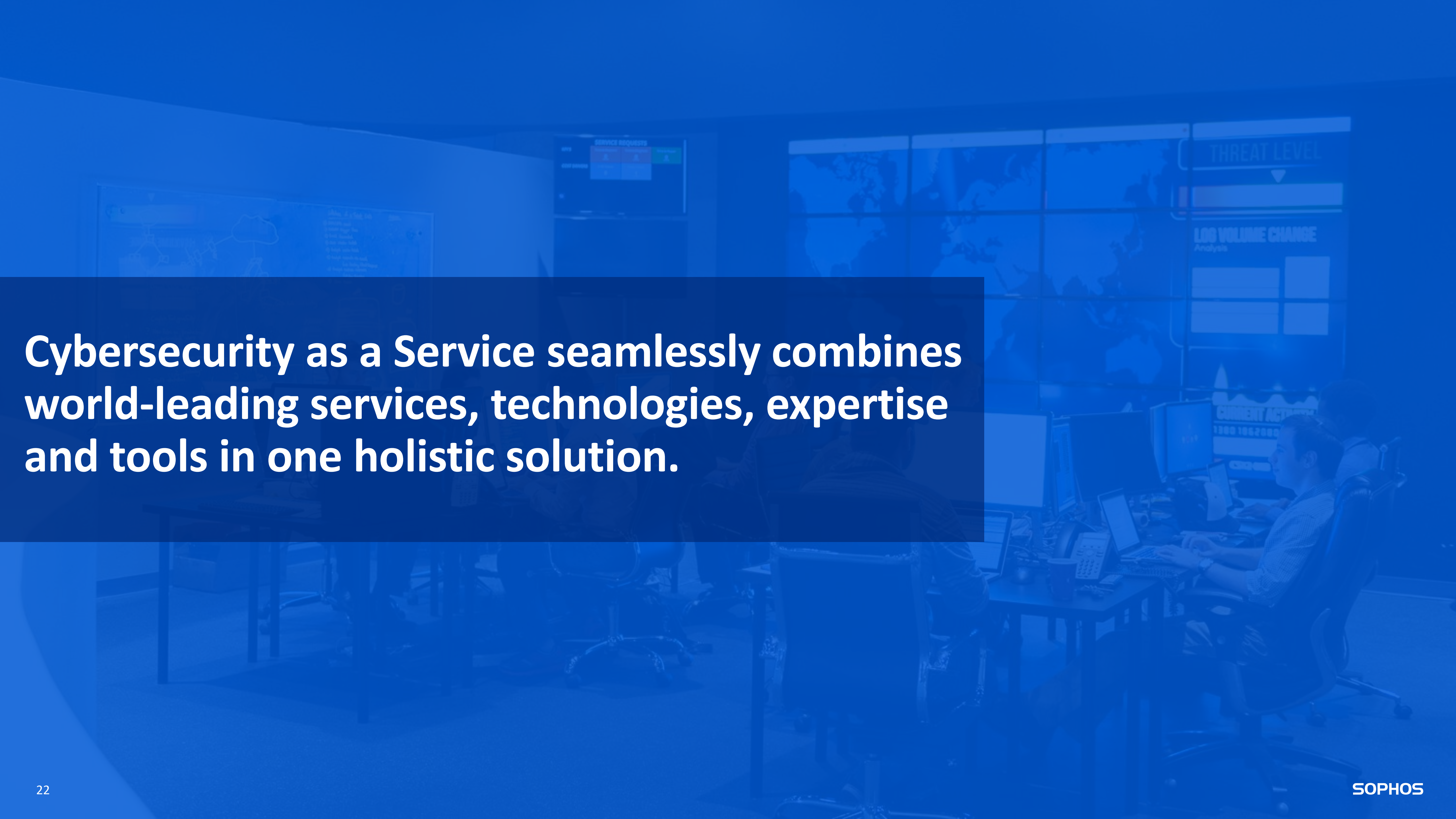
Adaptive Cybersecurity Ecosystem

Sophos Central

AI and Automation

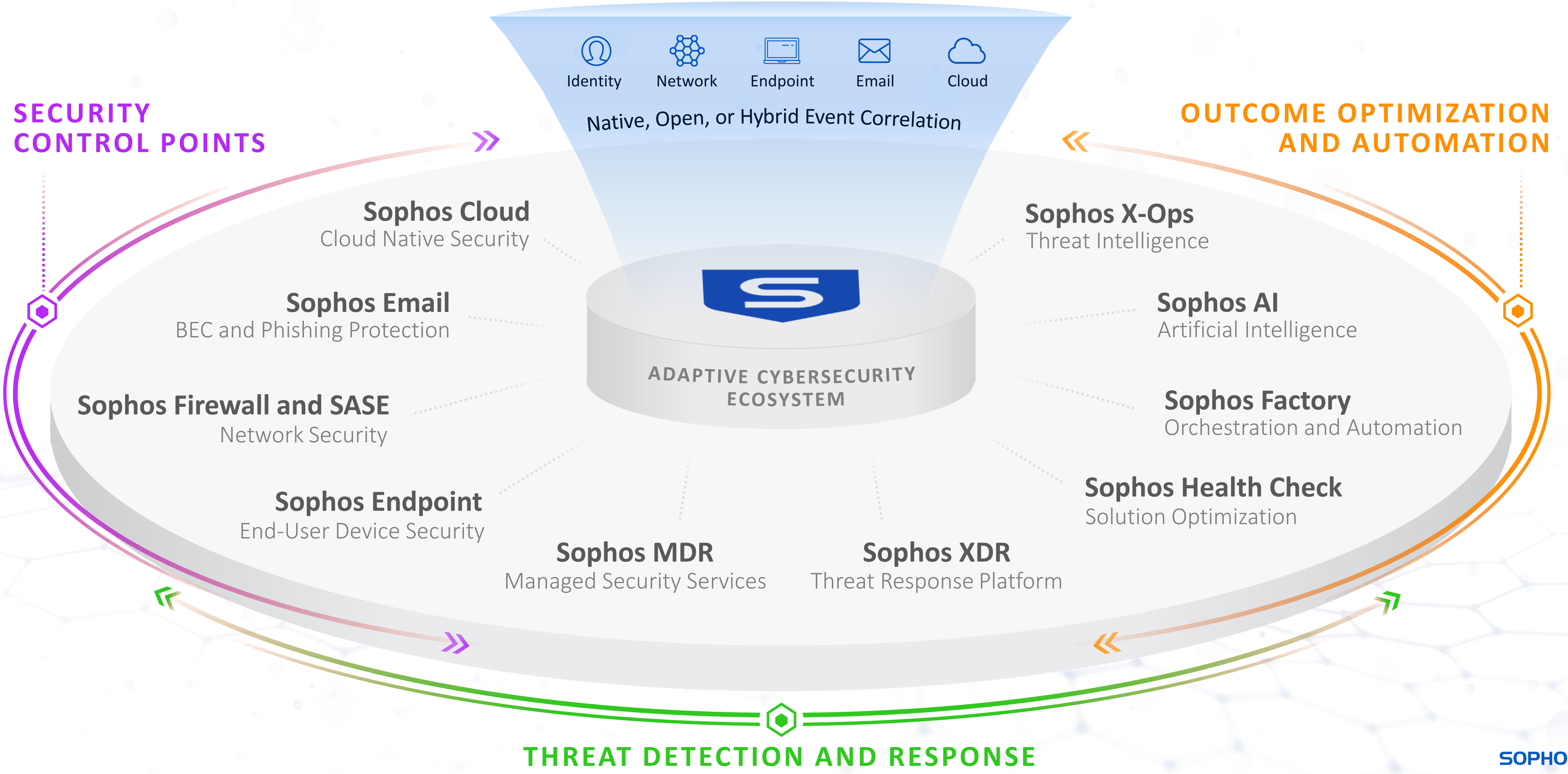
Sophos X-Ops Research

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



Identity

Network

Endpoint

Email

Cloud

Native, Open, or Hybrid Event Correlation

SECURITY CONTROL POINTS

OUTCOME OPTIMIZATION AND AUTOMATION

Sophos Cloud
Cloud Native Security

Sophos Email
BEC and Phishing Protection

Sophos Firewall and SASE
Network Security

Sophos Endpoint
End-User Device Security

Sophos MDR
Managed Security Services

Sophos XDR
Threat Response Platform

Sophos X-Ops
Threat Intelligence

Sophos AI
Artificial Intelligence

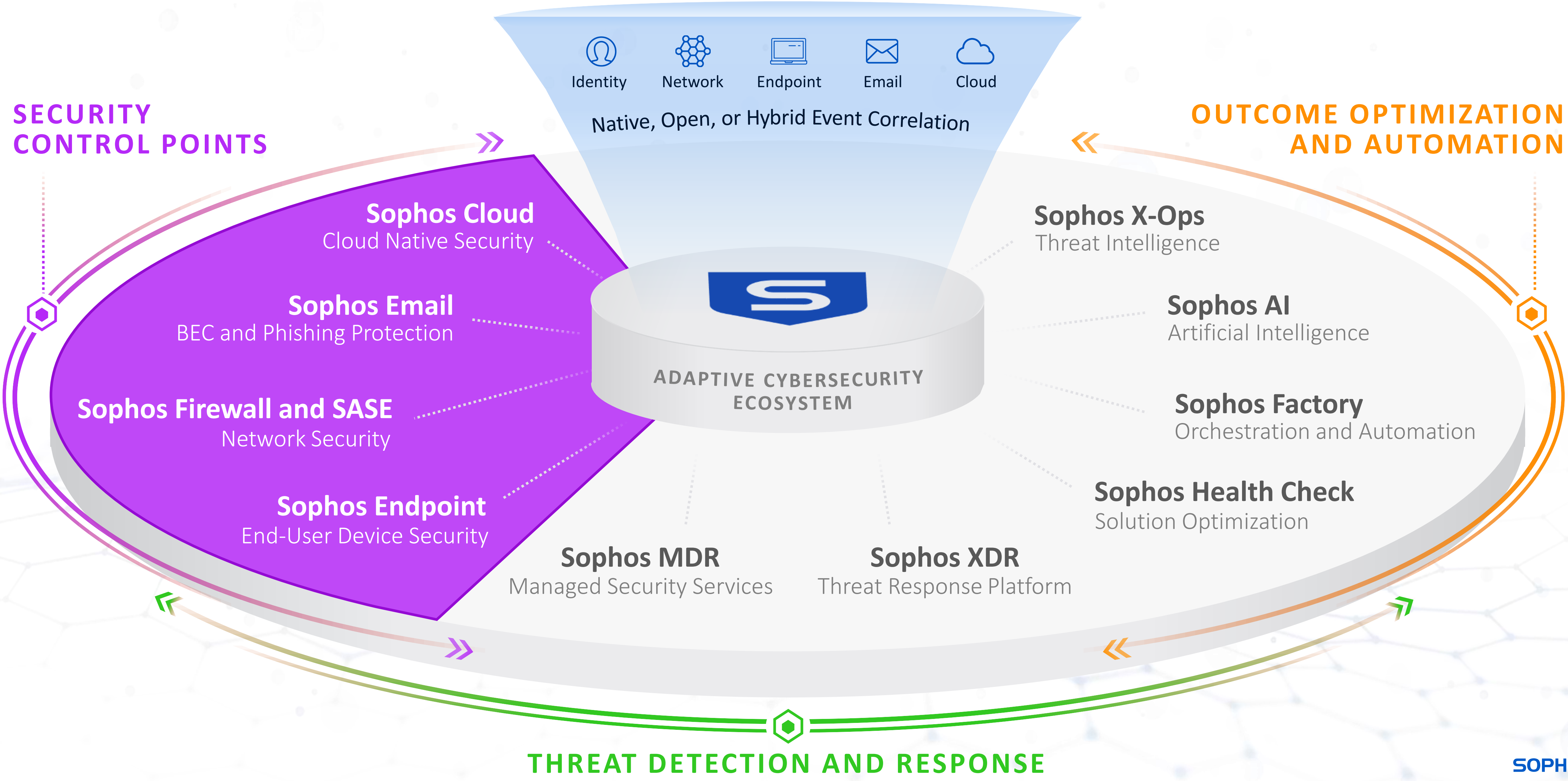
Sophos Factory
Orchestration and Automation

Sophos Health Check
Solution Optimization

ADAPTIVE CYBERSECURITY ECOSYSTEM

THREAT DETECTION AND RESPONSE

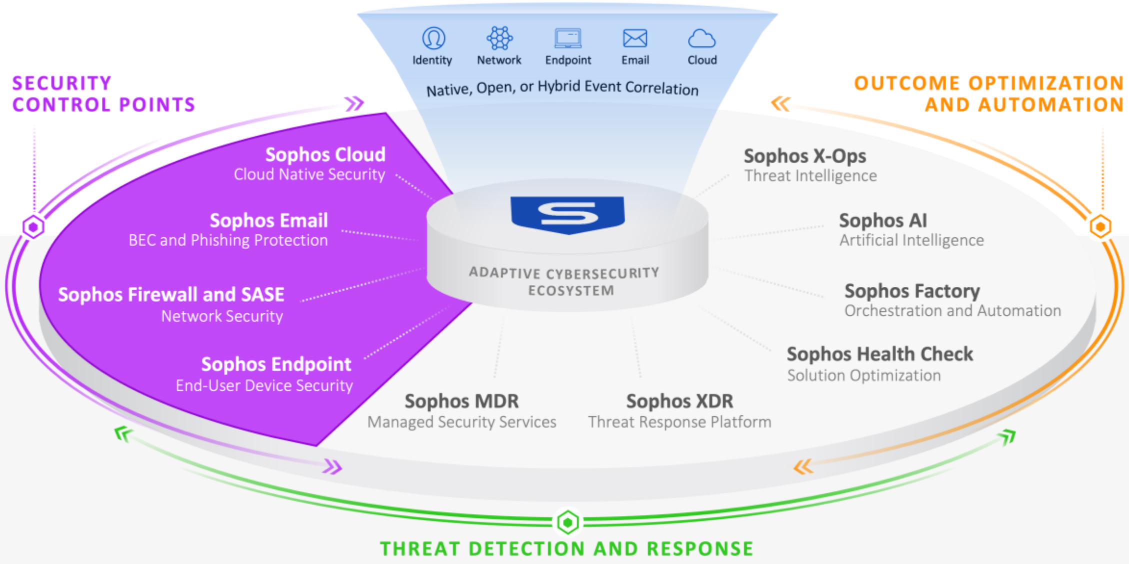
Delivering Optimal Cyber Security Outcomes

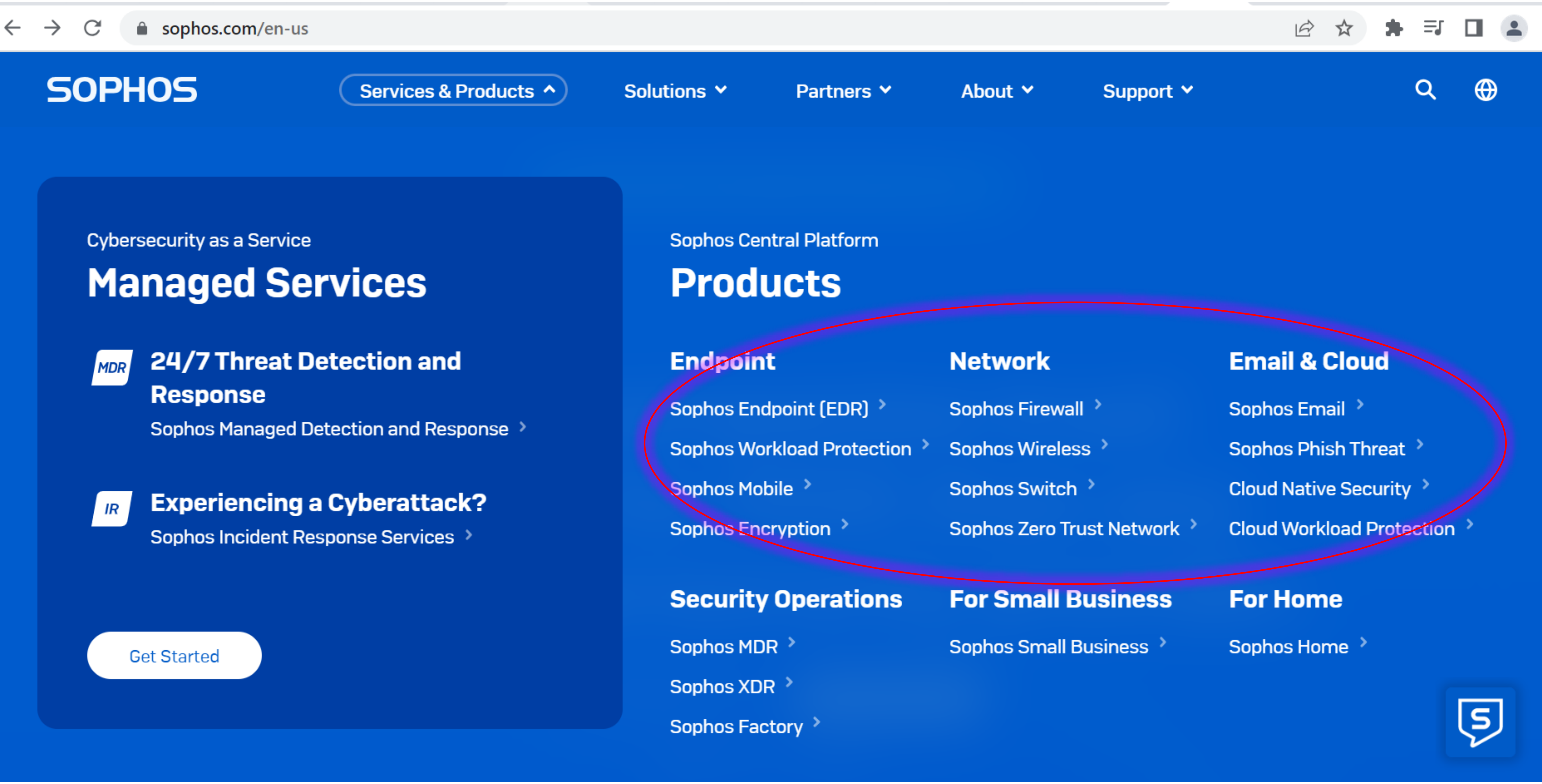


Security Control Points

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





Cybersecurity as a Service

Managed Services

24/7 Threat Detection and Response

MDR

Sophos Managed Detection and Response ›

Experiencing a Cyberattack?

IR

Sophos Incident Response Services ›

Sophos Central Platform

Products

Endpoint

- Sophos Endpoint (EDR) ›
- Sophos Workload Protection ›
- Sophos Mobile ›
- Sophos Encryption ›

Network

- Sophos Firewall ›
- Sophos Wireless ›
- Sophos Switch ›
- Sophos Zero Trust Network ›

Email & Cloud

- Sophos Email ›
- Sophos Phish Threat ›
- Cloud Native Security ›
- Cloud Workload Protection ›

Security Operations

- Sophos MDR ›
- Sophos XDR ›
- Sophos Factory ›

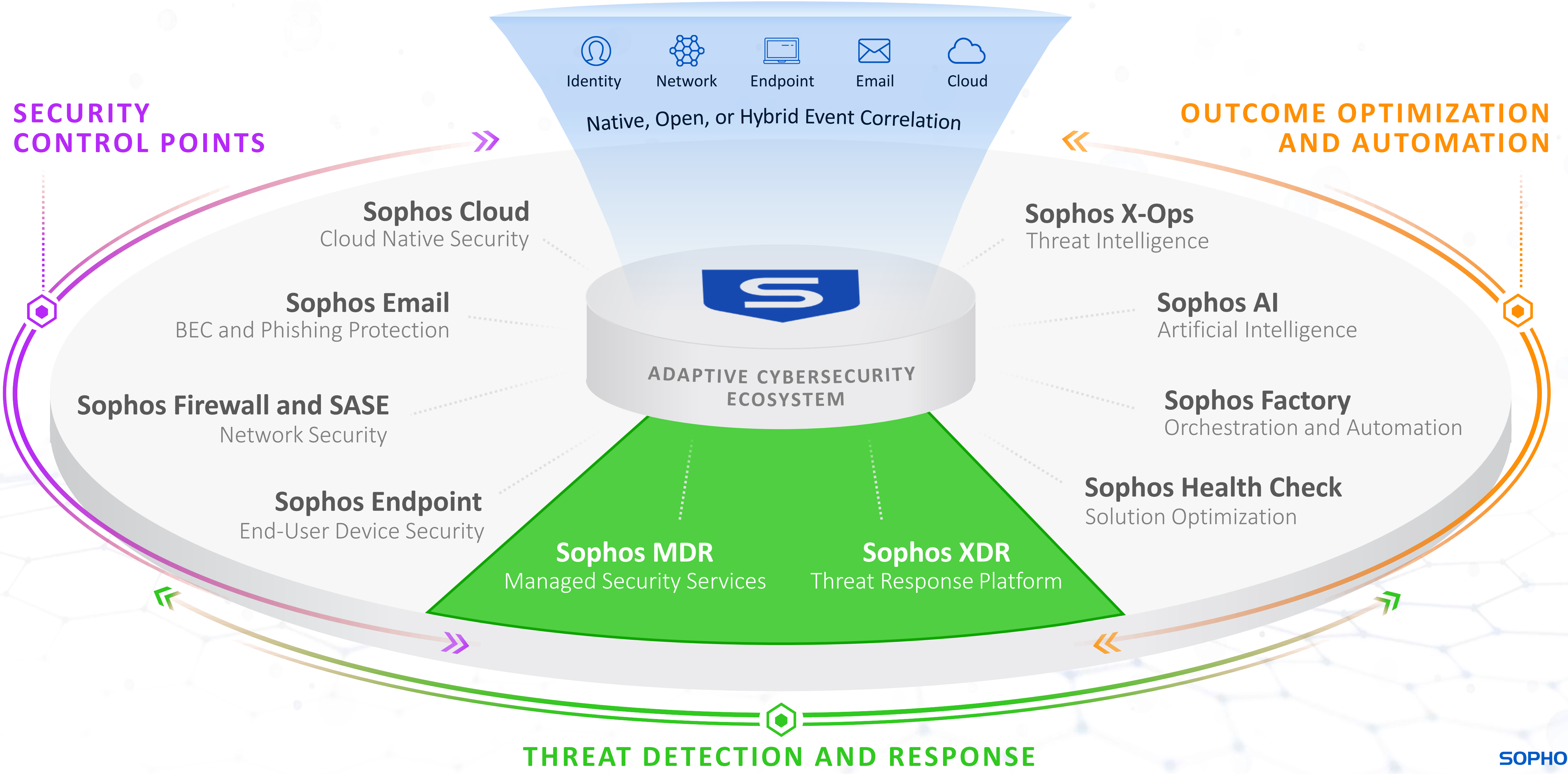
For Small Business

- Sophos Small Business ›

For Home

- Sophos Home ›

Delivering Optimal Cyber Security Outcomes



Identity

Network

Endpoint

Email

Cloud

Native, Open, or Hybrid Event Correlation

SECURITY CONTROL POINTS

Sophos Cloud
Cloud Native Security

Sophos Email
BEC and Phishing Protection

Sophos Firewall and SASE
Network Security

Sophos Endpoint
End-User Device Security

ADAPTIVE CYBERSECURITY ECOSYSTEM

OUTCOME OPTIMIZATION AND AUTOMATION

Sophos X-Ops
Threat Intelligence

Sophos AI
Artificial Intelligence

Sophos Factory
Orchestration and Automation

Sophos Health Check
Solution Optimization

Sophos MDR
Managed Security Services

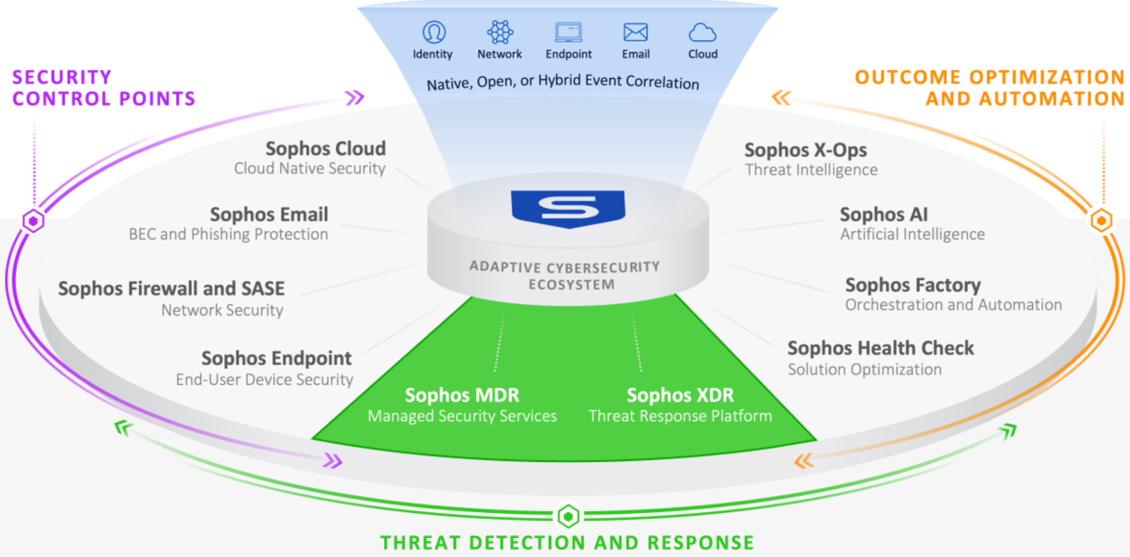
Sophos XDR
Threat Response Platform

THREAT DETECTION AND RESPONSE

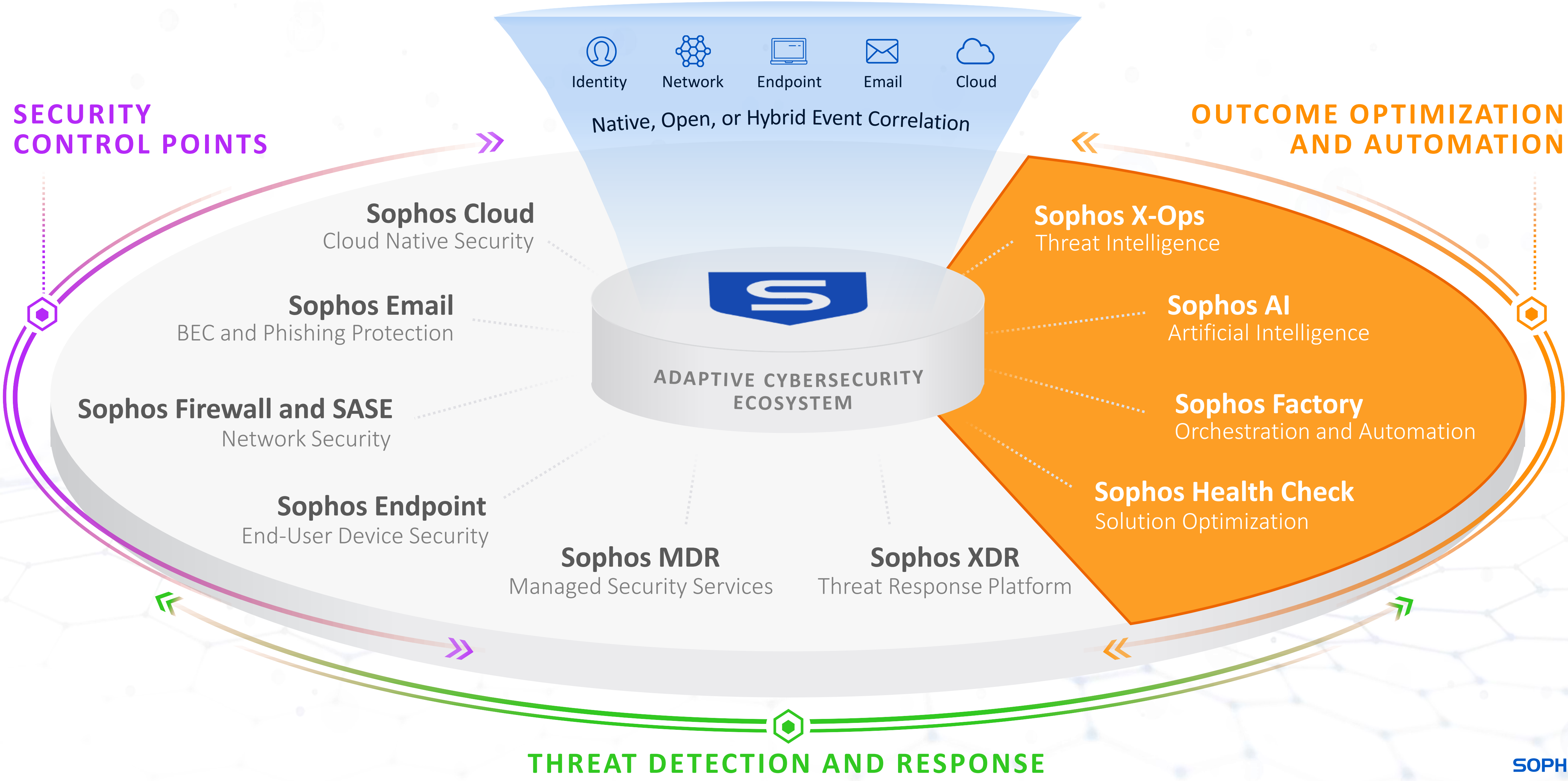
Threat Detection and Response

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



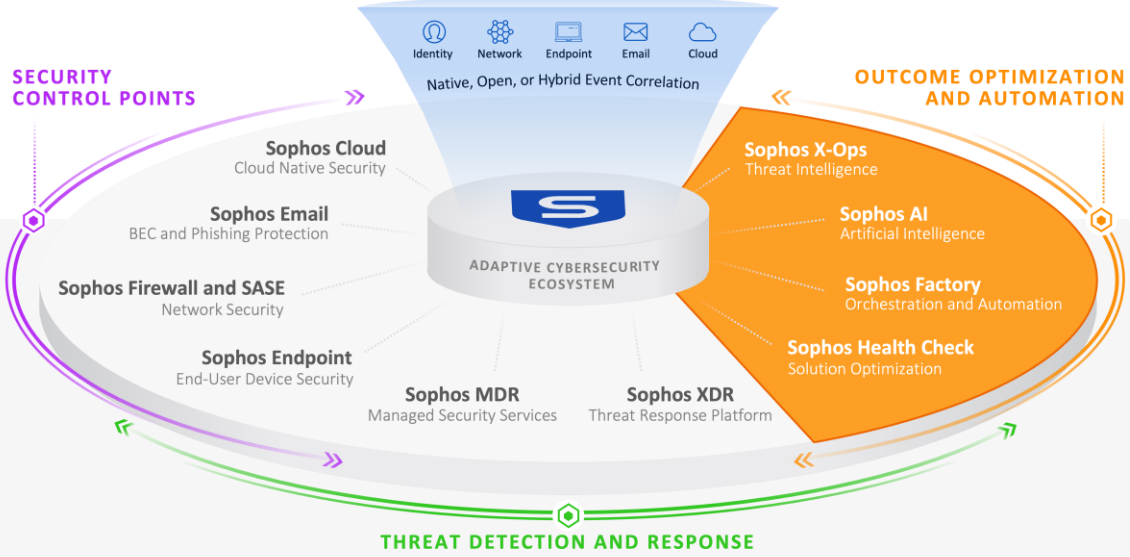
Delivering Optimal Cyber Security Outcomes



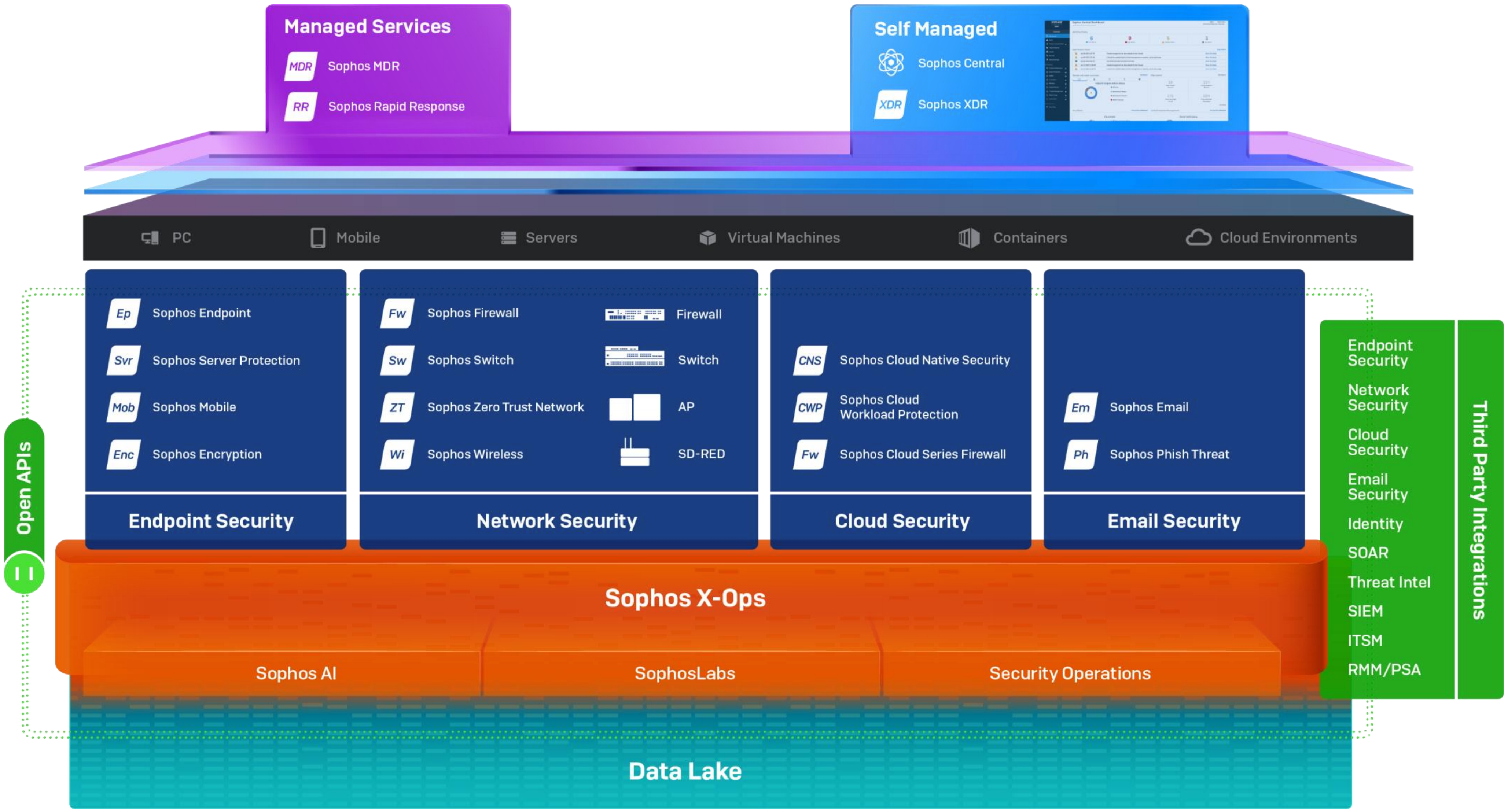
Outcome Optimization and Automation

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



Adaptive Cybersecurity Ecosystem



Managed Services

- MDR Sophos MDR
- RR Sophos Rapid Response

Self Managed

- Sophos Central
- XDR Sophos XDR

PC | Mobile | Servers | Virtual Machines | Containers | Cloud Environments

Endpoint Security

- Ep Sophos Endpoint
- Svr Sophos Server Protection
- Mob Sophos Mobile
- Enc Sophos Encryption

Network Security

- Fw Sophos Firewall — Firewall
- Sw Sophos Switch — Switch
- ZT Sophos Zero Trust Network — AP
- Wi Sophos Wireless — SD-RED

Cloud Security

- CNS Sophos Cloud Native Security
- CWP Sophos Cloud Workload Protection
- Fw Sophos Cloud Series Firewall

Email Security

- Em Sophos Email
- Ph Sophos Phish Threat

Open APIs

Sophos X-Ops

Sophos AI | SophosLabs | Security Operations

Data Lake

Third Party Integrations

- Endpoint Security
- Network Security
- Cloud Security
- Email Security
- Identity
- SOAR
- Threat Intel
- SIEM
- ITSM
- RMM/PSA

Sophos X-Ops Powers Products and Services

MDR
Sophos X-Ops
SOPHOS labs
AI

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

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

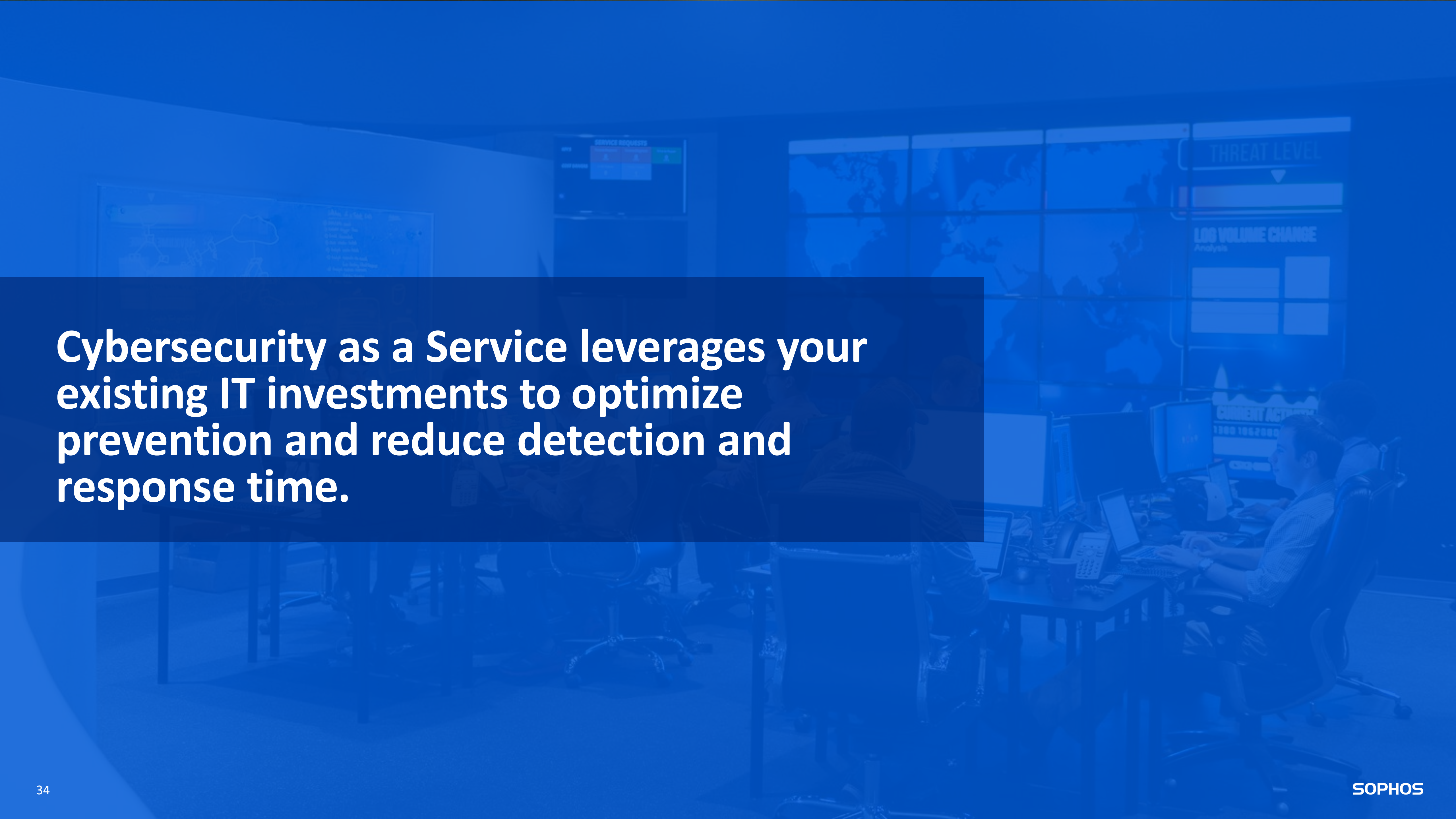
Cybersecurity as a Service

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

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

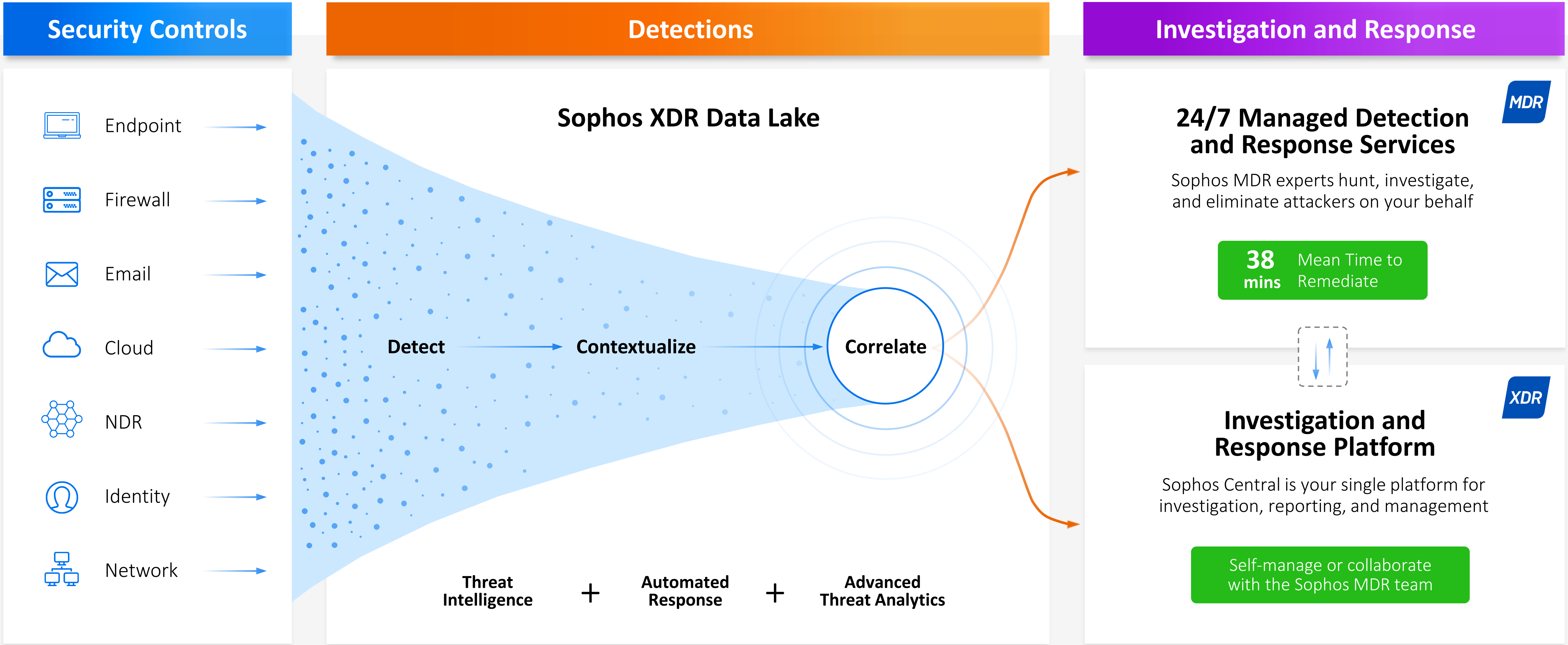
An **expert team** of cybersecurity professionals.

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



Security Controls

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identity
- Network

Detections

Sophos XDR Data Lake

Detect → Contextualize → Correlate

Threat Intelligence + Automated Response + Advanced Threat Analytics

Investigation and Response

MDR

24/7 Managed Detection and Response Services

Sophos MDR experts hunt, investigate, and eliminate attackers on your behalf

38 mins Mean Time to Remediate

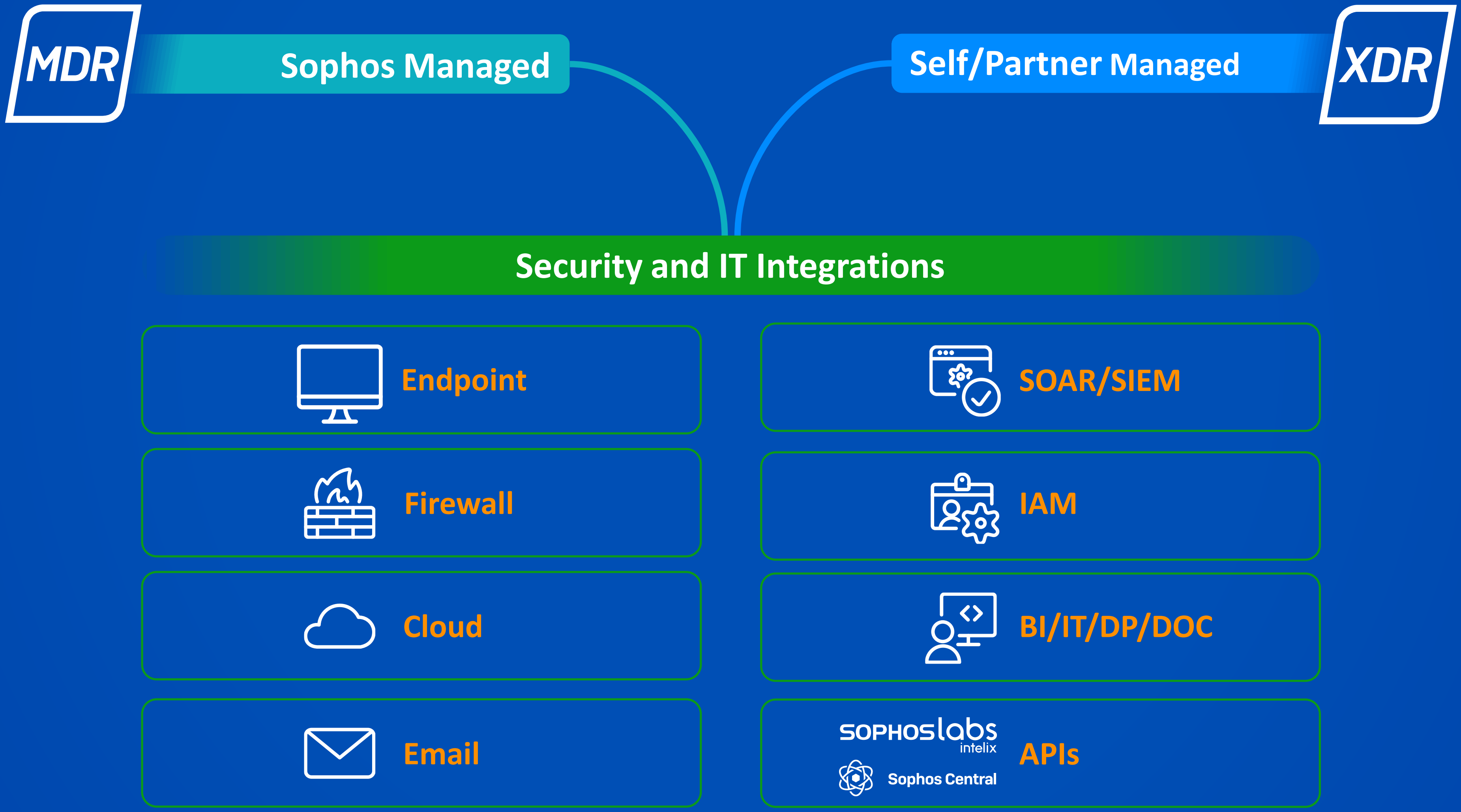
XDR

Investigation and Response Platform

Sophos Central is your single platform for investigation, reporting, and management

Self-manage or collaborate with the Sophos MDR team

Integrating With Your Existing IT Investments



MDR

Sophos Managed

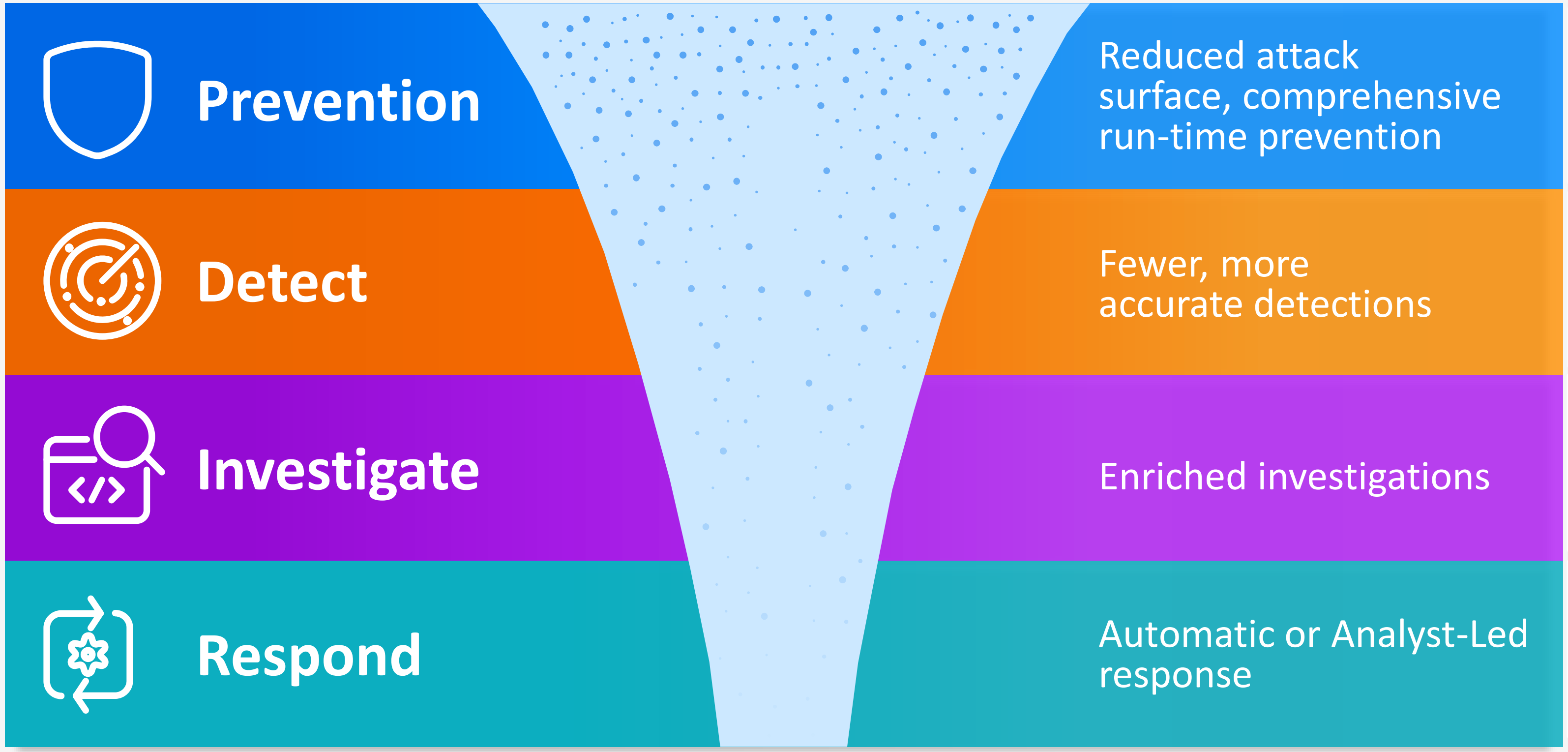
Self/Partner Managed

XDR

Security and IT Integrations

- Endpoint
- Firewall
- Cloud
- Email
- SOAR/SIEM
- IAM
- BI/IT/DP/DOC
- SOPHOSlabs intelix
Sophos Central — APIs

Optimize Prevention. Minimize Time to Detect and Respond



Prevention	Reduced attack surface, comprehensive run-time prevention	99.98% of threats blocked
Detect	Fewer, more accurate detections	MTTD <1 min
Investigate	Enriched investigations	MTTI <25 min
Respond	Automatic or Analyst-Led response	MTTR <12 min

Superior outcomes

(less risk, greater efficiency, lower costs)

Proven. Trusted.

Customer Growth One of Largest and Fastest-Growing MDR Service Providers	Industry Analysts 13-time Gartner Magic Quadrant Leader	3rd Party Testing Award-Winning Product and Services
554,000+ Customers 100+ million devices protected	**Leader: Endpoint Protection Platforms** Gartner Magic Quadrant	**Winner: Best Managed Security Services** Channel Partner Insight Awards
55,000+ Channel Partners 10,000+ MSPs	**Best Enterprise Endpoint Solution** SE Labs	**No. 1 Ranked MDR Service** Gartner Peer Insights
16,000+ MDR Customers Thousands of Investigations	**100% Protection/Usability Scores** AV-Test	**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

MDR
Sophos MDR

4.8
Average Rating

97%
Would Recommend

Based on 273 Reviews

SentinelOne	4.5
CrowdStrike	4.8*
Arctic Wolf	4.8*

Ep
Sophos Endpoint

4.8
Average Rating

95%
Would Recommend

Based on 385 Reviews

Microsoft	4.4
CrowdStrike	4.6
Trend Micro	4.5

Fw
Sophos Firewall

4.7
Average Rating

91%
Would Recommend

Based on 241 Reviews

Fortinet	4.7
Check Point	4.5
Palo Alto Networks	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

451 Research

The Evolution of Sophos Managed Detection and Response

September 7, 2022

SOPHOS

Managed Detection and Response (MDR)

A fully-managed, 24/7 service delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent

Gartner®

By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment and mitigation capabilities

MDR Sophos MDR

Threat Hunting

Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own

Threat Detection

Enabled by extended detection and response (XDR) capabilities that detect known threats and potentially malicious behaviors wherever your data reside

Incident Response

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

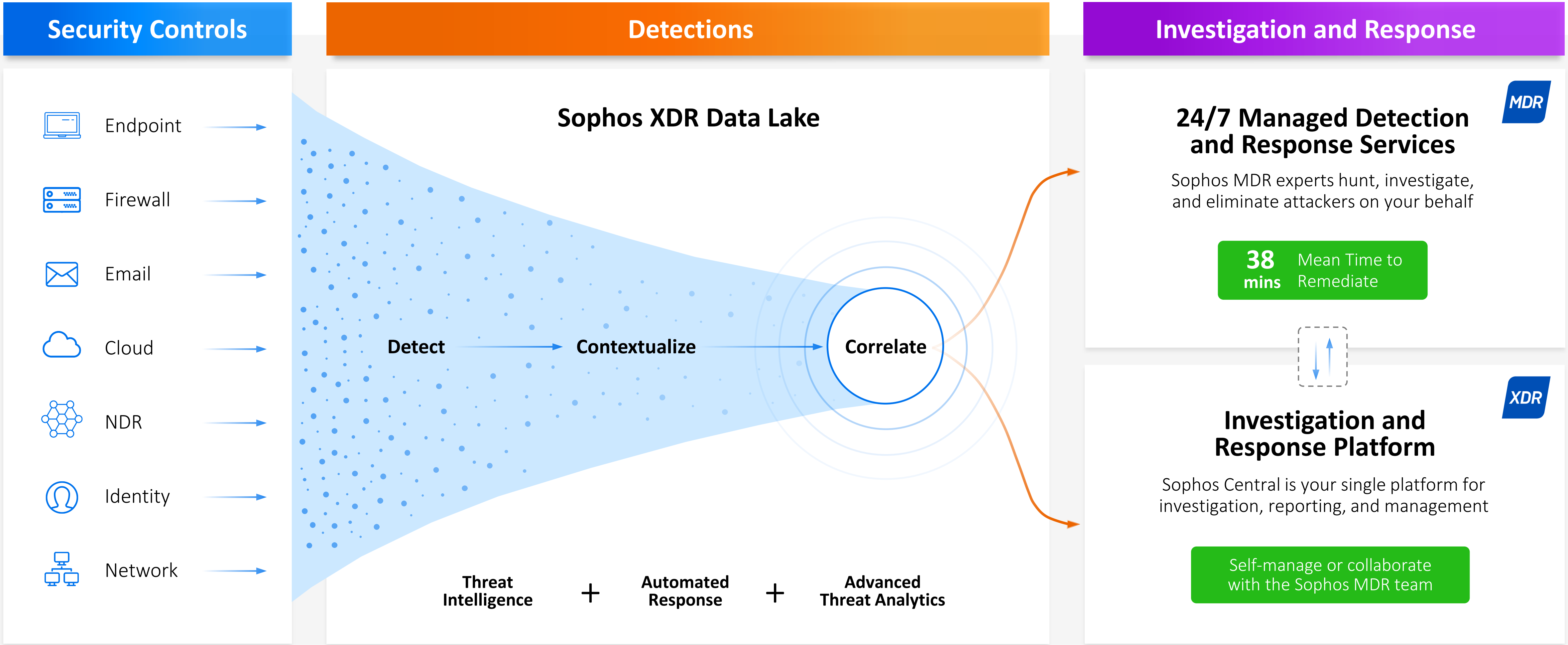
15,500+ MDR Customers

99.98% of threats automatically blocked*

Average Sophos MDR Threat Response Times

Time to Detect	Less than 1 Minute
Time to Investigate	Less than 25 Minutes
Time to Respond	Less than 12 Minutes

Security Operations Center: Managed By You or Us



Security Controls

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identity
- Network

Detections

Sophos XDR Data Lake

Detect → Contextualize → Correlate

Threat Intelligence + Automated Response + Advanced Threat Analytics

Investigation and Response

MDR

24/7 Managed Detection and Response Services

Sophos MDR experts hunt, investigate, and eliminate attackers on your behalf

38 mins Mean Time to Remediate

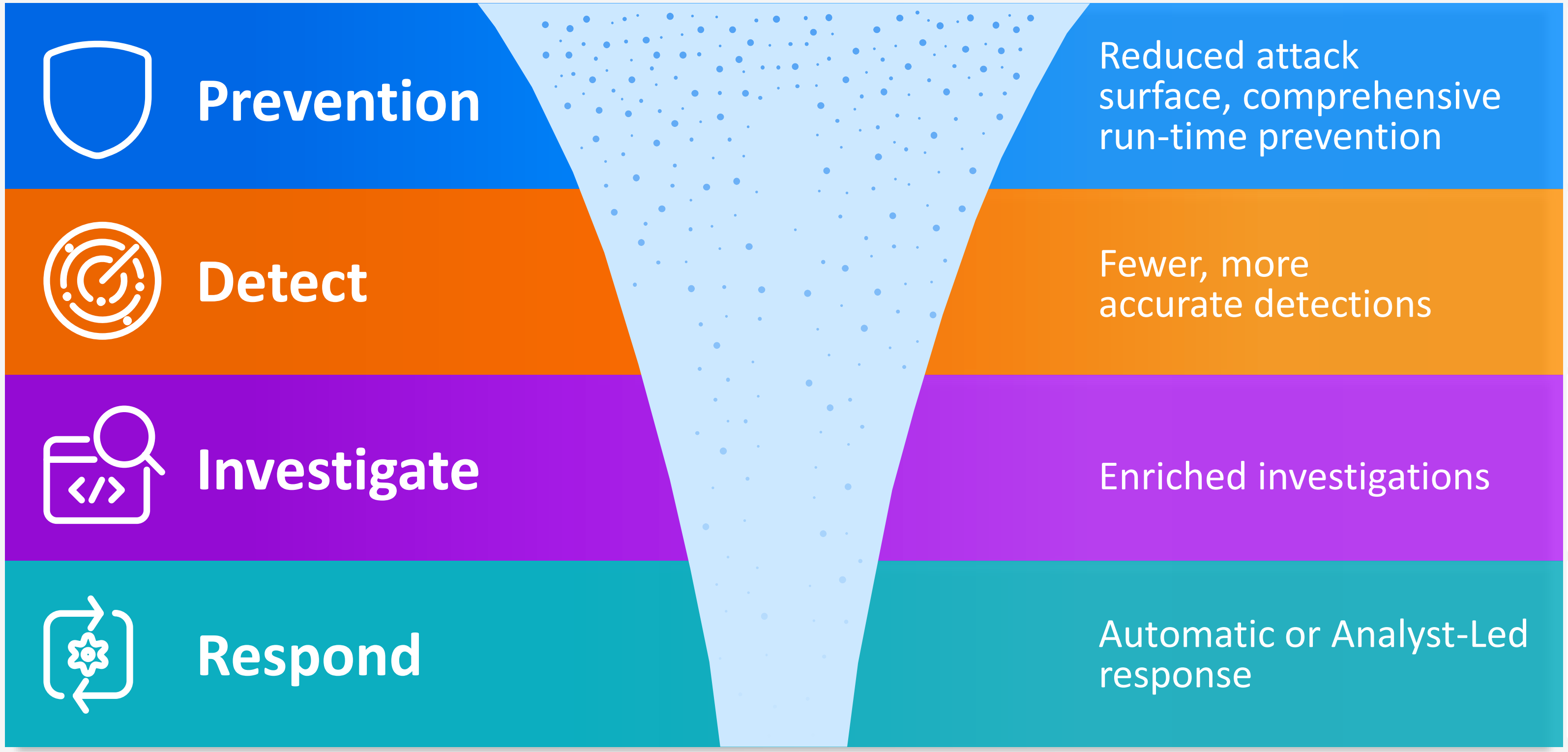
XDR

Investigation and Response Platform

Sophos Central is your single platform for investigation, reporting, and management

Self-manage or collaborate with the Sophos MDR team

Optimize Prevention. Minimize Time to Detect and Respond

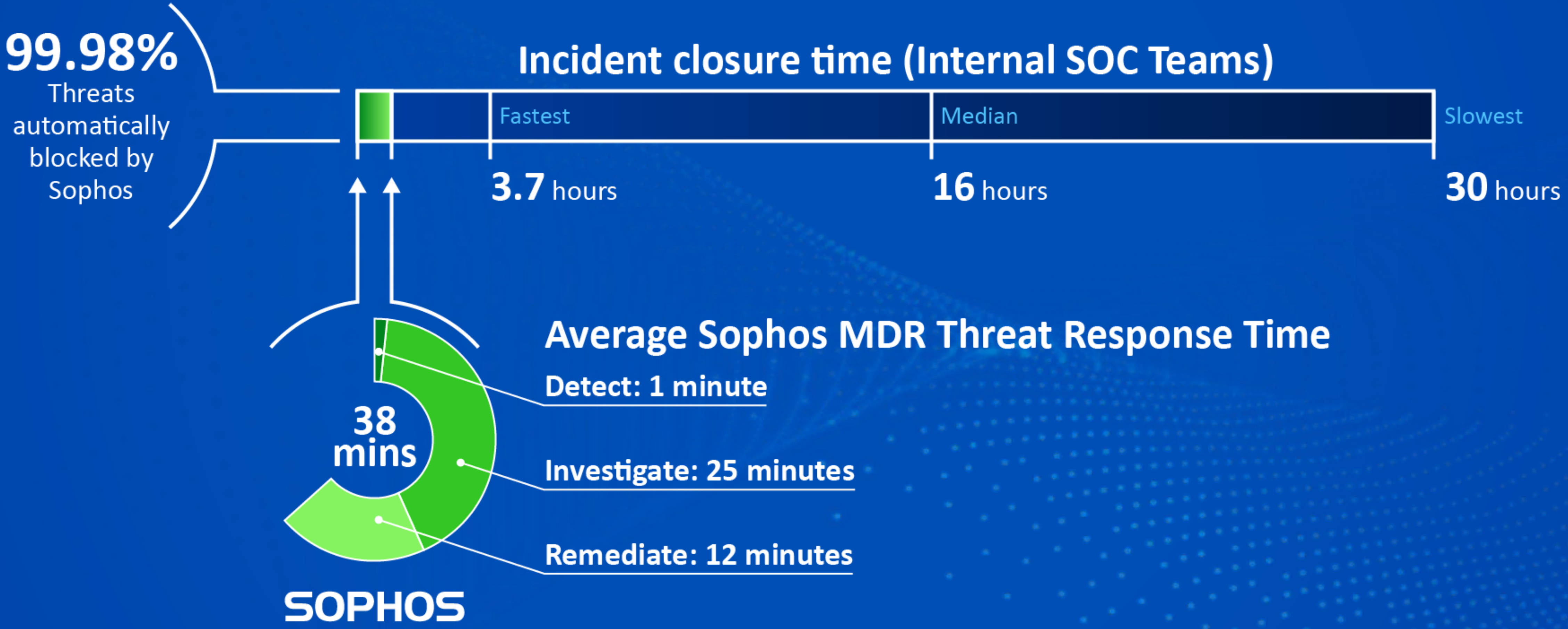


Prevention	Reduced attack surface, comprehensive run-time prevention	99.98% of threats blocked
Detect	Fewer, more accurate detections	MTTD <1 min
Investigate	Enriched investigations	MTTI <25 min
Respond	Automatic or Analyst-Led response	MTTR <12 min

Superior outcomes

(less risk, greater efficiency, lower costs)

Leading Detection and Response Times



99.98%
Threats automatically blocked by Sophos

Incident closure time (Internal SOC Teams)

Average Sophos MDR Threat Response Time

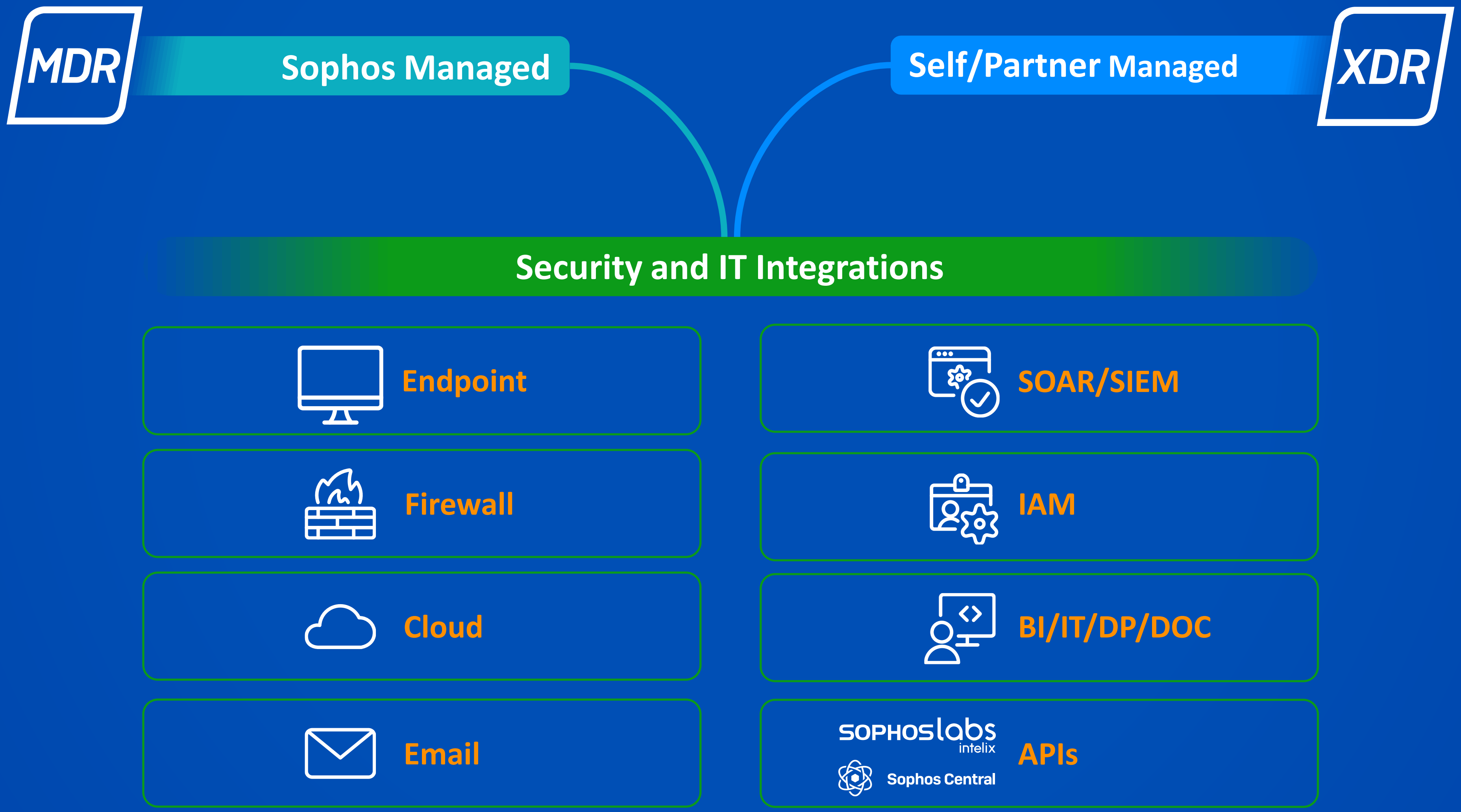
Detect: 1 minute

Investigate: 25 minutes

Remediate: 12 minutes

SOPHOS

Integrating With Your Existing IT Investments



MDR

Sophos Managed

Self/Partner Managed

XDR

Security and IT Integrations

- Endpoint
- Firewall
- Cloud
- Email
- SOAR/SIEM
- IAM
- BI/IT/DP/DOC
- SOPHOSlabs intelix, Sophos Central APIs

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

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

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.

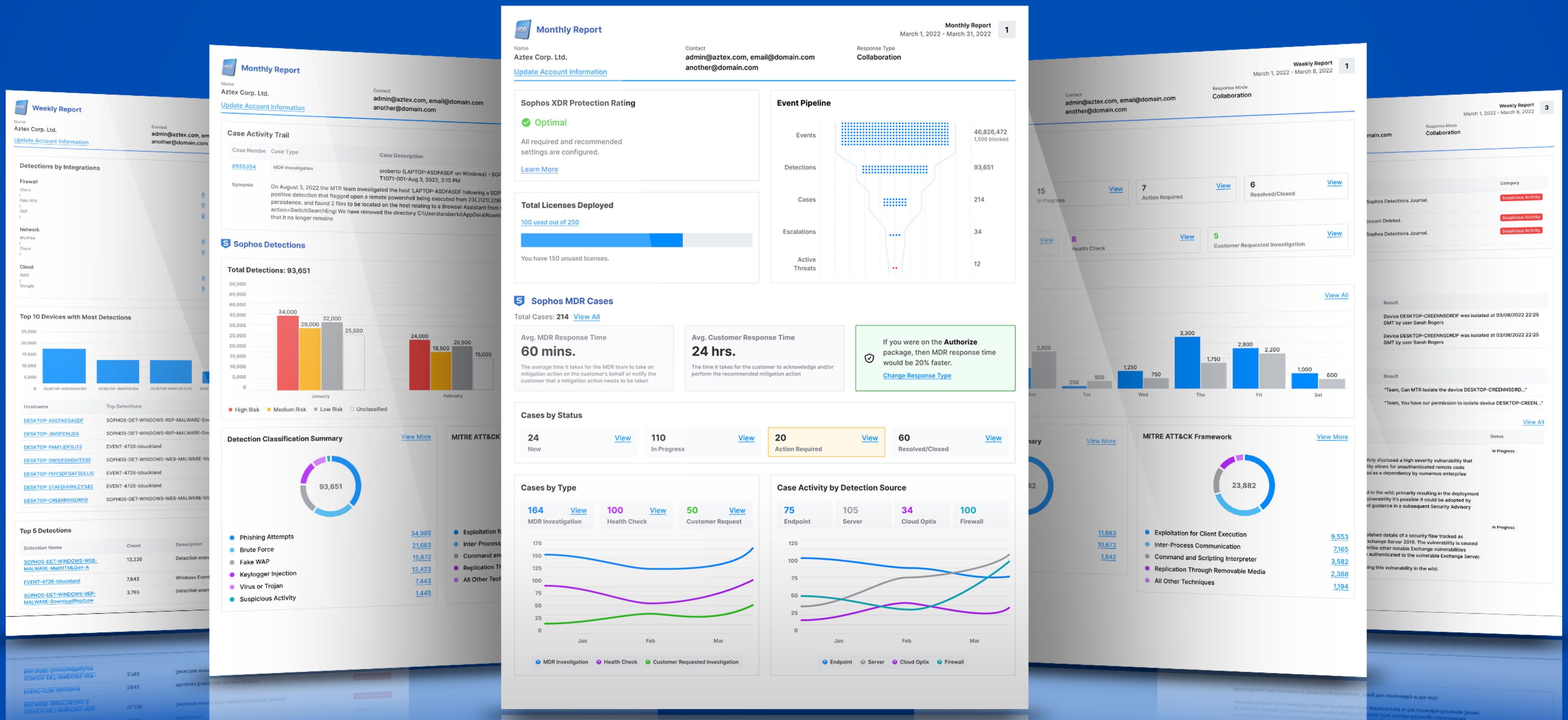
Identity

- Microsoft [Azure IDP, ATA]
- okta
- Duo
- ManageEngine

Network

- DARKTRACE
- Thinkst Canary
- Skyhigh Security

Monthly and Weekly Cybersecurity Reports



Monthly Report

Monthly Report
March 1, 2022 - March 31, 2022
1

Name
Aztex Corp. Ltd.
Update Account Information

Contact
admin@aztex.com, email@domain.com
another@domain.com

Response Type
Collaboration

Sophos XDR Protection Rating

Optimal

All required and recommended settings are configured.

Learn More

Total Licenses Deployed

100 used out of 250

You have 150 unused licenses.

Event Pipeline

Events	46,826,472 1,500 blocked
Detections	93,651
Cases	214
Escalations	34
Active Threats	12

Sophos MDR Cases

Total Cases: **214** View All

Avg. MDR Response Time
60 mins.
The average time it takes for the MDR team to take an mitigation action on the customer's behalf or notify the customer that a mitigation action needs to be taken

Avg. Customer Response Time
24 hrs.
The time it takes for the customer to acknowledge and/or perform the recommended mitigation action

If you were on the **Authorize** package, then MDR response time would be 20% faster.
Change Response Type

Cases by Status

24	New	View
110	In Progress	View
20	Action Required	View
60	Resolved/Closed	View

Cases by Type

164	MDR Investigation	View
100	Health Check	View
50	Customer Request	View

Case Activity by Detection Source

75	Endpoint
105	Server
34	Cloud Optix
100	Firewall

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 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 Uses full Sophos XDR agent (protection, detection and response) or Sophos XDR Sensor (detection and Response)		✓	✓
Direct call-in support during active incidents		✓	✓
Full-scale Incident Response: threats are fully eliminated Requires full Sophos XDR agent (protection, detection and response)			✓
Root Cause Analysis: performed to prevent future recurrence			✓
Dedicated Incident Response Lead			✓
Sophos Breach Protection Warranty			✓

Sophos MDR Included Integrations

XDR 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

Fw 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

Ep Sophos Endpoint Protection

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

Included in Sophos MDR and Sophos MDR Complete Pricing

Em 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

Cld 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 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

Sophos MDR Is Simple to Quote and Purchase

ORGANIZATION SIZE

How many users?	How many servers?
300	50

DATA RETENTION PERIOD

○ 90 Days (included)

● 1 Year

SERVICE TIER

● Sophos MDR Complete

○ Sophos MDR

○ Sophos Threat Advisor

○ Guided Onboarding

SOPHOS INTEGRATIONS

● XDR Sophos XDR

○ Em Sophos Email

○ Cld Sophos Cloud

○ Fw Sophos Firewall

● Ep Sophos Endpoint

● NDR Sophos NDR

THIRD-PARTY INTEGRATIONS

○ Endpoint Protection

○ Public Cloud

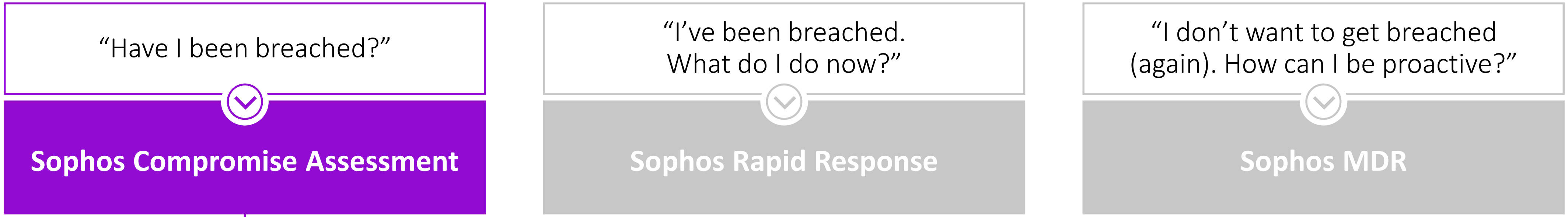
● Identity

● Firewall

○ Email

○ 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

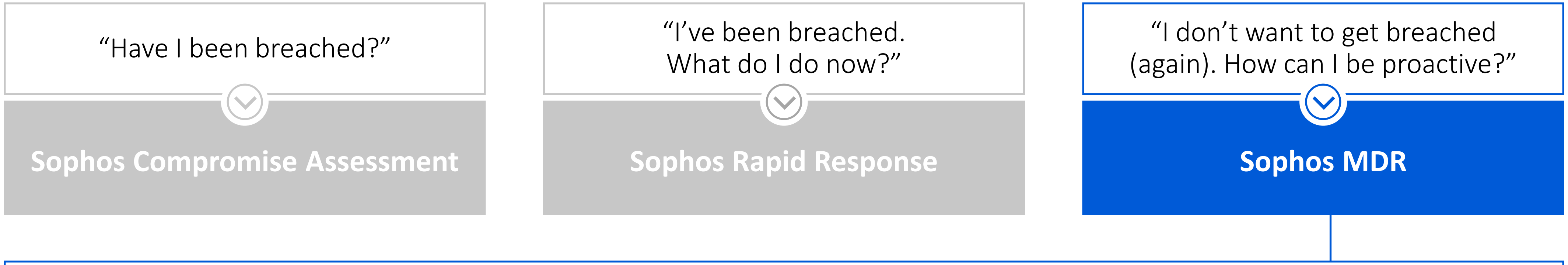
"I don't want to get breached (again). How can I be proactive?"

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?”

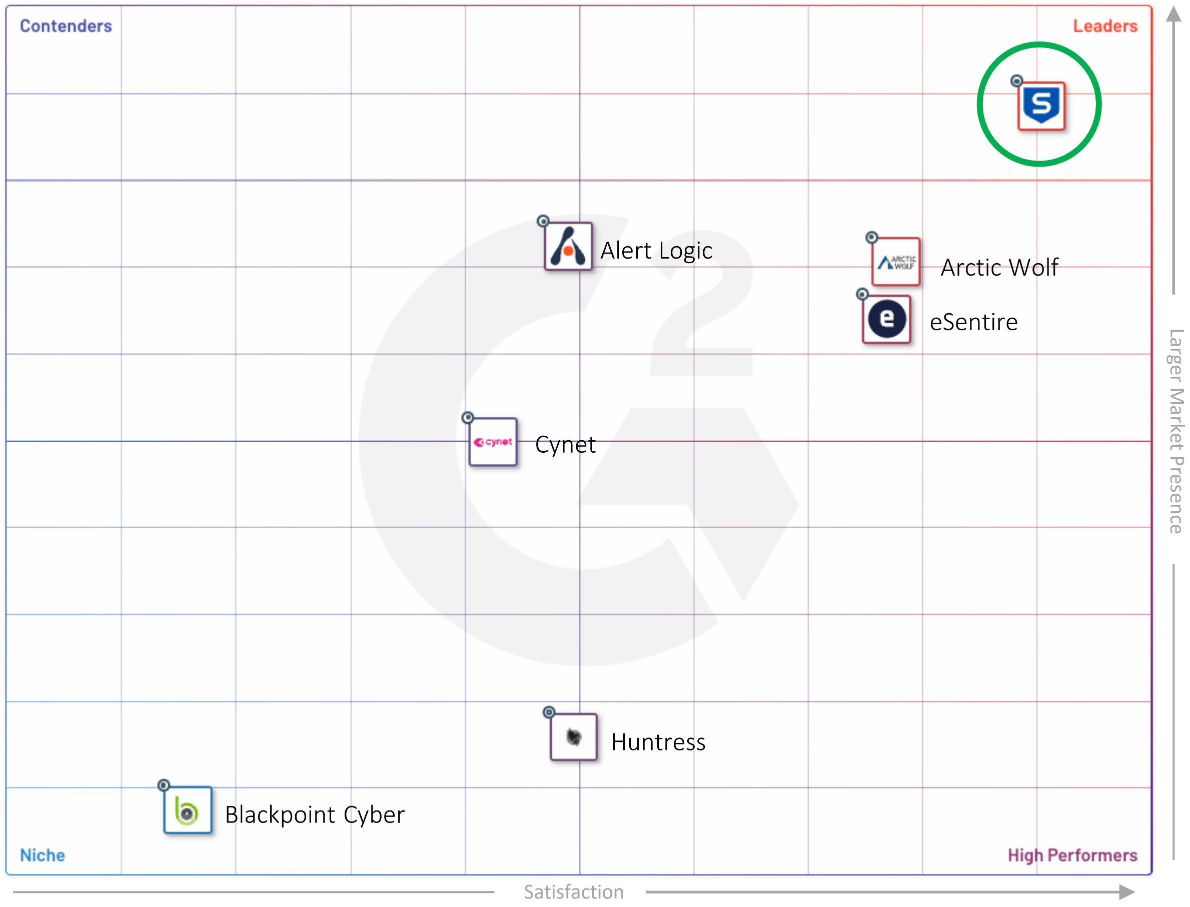
Sophos MDR

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

G2: MDR Service Ratings

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



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

Sophos MDR Sales Plays Are Live

MDR

Sales Play Objectives

- Upsell existing **Intercept X Advanced (CIXA-only)** customers to Sophos MTR Advanced prior to the launch of our expanded MDR service offering
- Upsell existing **Sophos XDR (CIXA-XDR)** to Sophos MDR Advanced prior to the launch of our expanded MDR service offering

Available Now on Sophos HUB

- K-12 Education (primary/secondary)
- Higher Education
- Retail
- Manufacturing
- Healthcare
- Financial Services
- Local Government
- Small Business

MDR Sophos MDR Sales Play Overviews (includes all 8 Industry Overviews)

Available Now: The State of Ransomware Report

- The State of Ransomware 2022 (includes data on all verticals and global regions)
- The State of Ransomware in Retail 2022
- The State of Ransomware in Education 2022 (includes lower education and higher education)
- The State of Ransomware in Financial Services 2022
- The State of Ransomware in Healthcare 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 as a Service

Sophos MDR: The Perfect Fit for VAR, MSP and MSSP Partners

Superior Business Outcomes for Partners

Expand Your Cybersecurity Portfolio

Extend your offerings with new services that integrate with and complement your existing security solutions.

Elevate Your Customers' Cyber Defenses

Enhance your customers' protection with 24/7 monitoring, investigation and neutralization support delivered by a global team of threat experts.

Grow Your Cybersecurity Revenue

Take advantage of the huge demand for MDR and other security services to win new customers and increase your existing customer footprint.

$1.2B

2022 total available market for Managed Detection and Response (MDR), growing over 20% YoY

Gartner Emerging Technologies-Adoption Growth Insights for MDR

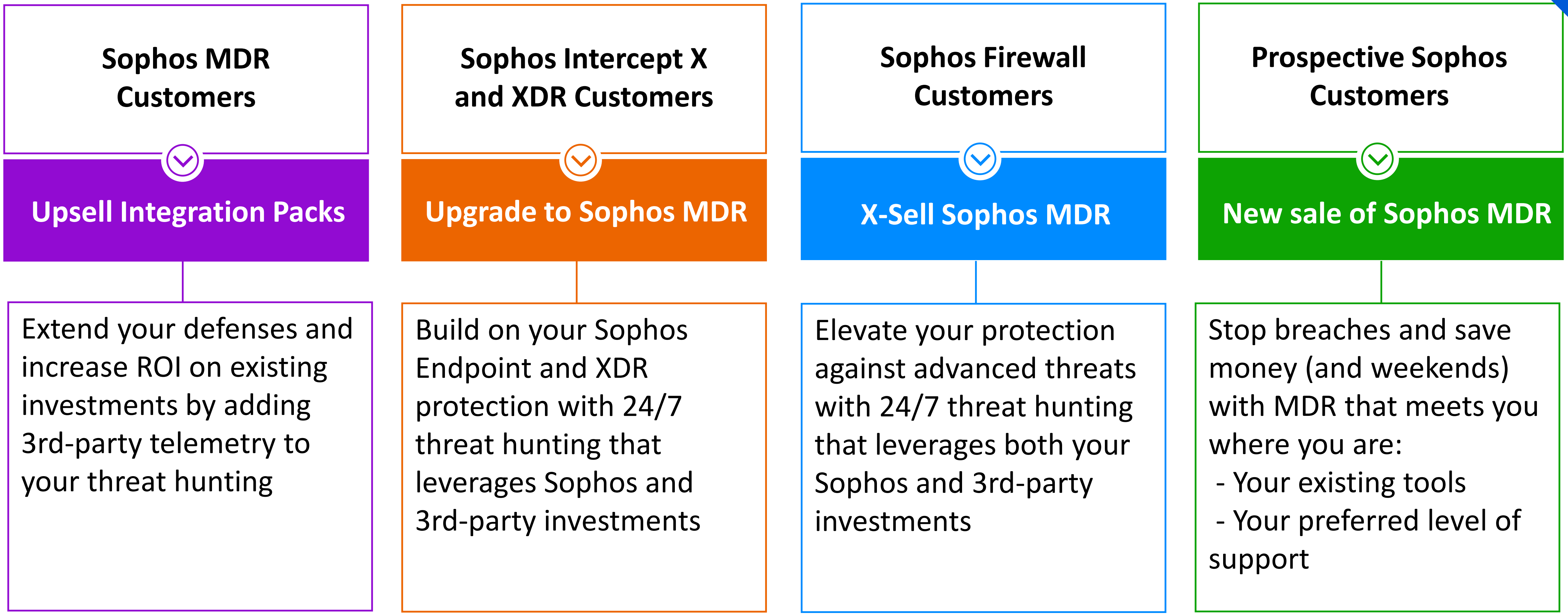
96%

Faster incident response time compared to internal SOC teams, enabling businesses to focus on strategic initiatives

3X

Partners that sell Sophos MDR services drive three times more revenue through increased customer lifetime value and retention

Primary Sales Plays for Sophos MDR



Sophos MDR Customers

Upsell Integration Packs

Extend your defenses and increase ROI on existing investments by adding 3rd-party telemetry to your threat hunting

Sophos Intercept X and XDR Customers

Upgrade to Sophos MDR

Build on your Sophos Endpoint and XDR protection with 24/7 threat hunting that leverages Sophos and 3rd-party investments

Sophos Firewall Customers

X-Sell Sophos MDR

Elevate your protection against advanced threats with 24/7 threat hunting that leverages both your Sophos and 3rd-party investments

Prospective Sophos Customers

New sale of Sophos MDR

Stop breaches and save money (and weekends) with MDR that meets you where you are:

- Your existing tools
- Your preferred level of support

Sophos MDR: Flexible Approach Based on Partner Needs

1

Resell Sophos Branded MDR

MDR

Offer an “instant SOC” fully staffed with the industry’s best cybersecurity operations talent (Sophos X-Ops engineers) with complete threat protection, active threat hunting, notification, remediation and reporting with the world’s most open and widely deployed MDR service.

2

For those who prefer to:

- *Maintain your own SOC*
- *Recruit, hire and retain threat hunting team*
- *Deliver incident response*

Use Sophos MDR to Extend Your Own Service

MDR

Use Sophos MDR in notification-only mode or leverage other capabilities to complement your existing team with skilled cybersecurity resources, expanded service hours, or extended service into new geographies as part of your own CSaaS delivery.

3

Staff

Data Center / SOC

Incident Response Process

… and who prefer to:

- *Deliver their own bespoke or vendor-provided MDR service*

Use Sophos XDR to Create Your Own Service

XDR

Build your own MDR service on a Sophos XDR foundation: Leverage the same Sophos technologies (AI, automation, threat intel, connectors, etc.) that power Sophos MDR.

MDR/CSaaS: A Better Way to Deliver Cybersecurity

Better for Customers

- Faster detection and response
- Less expensive than building and operating internal SOC
- More open and flexible than working with other vendors
- More affordable and simple to purchase, deploy, and manage than other vendors
- Better customer satisfaction

Better for Partners

- More strategic relationship with customer
- Better customer satisfaction rates
- Attractive subscription business model
- Enhanced retention rates
- Enhanced ability for cross-sell and upsell
- Differentiation and flexibility/open architecture to work alongside other vendors drives enhanced opportunity to attract new customers

Sophos MDR Fills a Key Gap in Any Partner Offering

VAR	MSP	MSSP		...with SOPHOS MDR
⚠	✓	✓	Managed Endpoint and Network Protection	✓
⚠	⚠	✓	Active Threat Hunting and XDR	✓
⚠	⚠	✓	Instant SOC	✓
⚠	⚠	✓	Full Incident Response	✓
⚠	⚠	⚠	Deep 3rd Party Product Coverage	✓
⚠	⚠	⚠	Worldwide Geographic Coverage	✓
⚠	⚠	⚠	24/7 Time Zone Coverage	✓
⚠	⚠	⚠	2nd Opinion XDR Toolset	✓
⚠	⚠	⚠	Cybersecurity Outcome Warranty	✓
⚠	⚠	⚠	Industry-Leading Human Expertise (Sophos X-Ops)	✓