

SOPHOS

El reto de la ciberseguridad para la Administración Pública

Álvaro Fernández

Director Comercial

Mayo 2025

SOPHOS

Why isn't cybersecurity working?







Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



Peter Firstbrook | Gartner

Distinguished VP Analyst

“ Nadie tiene suficiente gente para ocuparse de la ciberseguridad... **hay que ofrecerla como un servicio**. No basta con vender software **porque la mayoría de los compradores no cuentan con las personas que puedan explotarlo**. Vemos un enorme interés en los servicios de seguridad gestionados, porque la ciberseguridad se está volviendo demasiado complicada para la mayoría de las organizaciones. ”

3.4 Million

The global shortage of cybersecurity practitioners currently needed

(ISC)², 2022 Cybersecurity Workforce Study

71%

Of security teams struggle with too many noisy alerts from their tools

Sophos, The State of Cybersecurity 2023

16 Hours

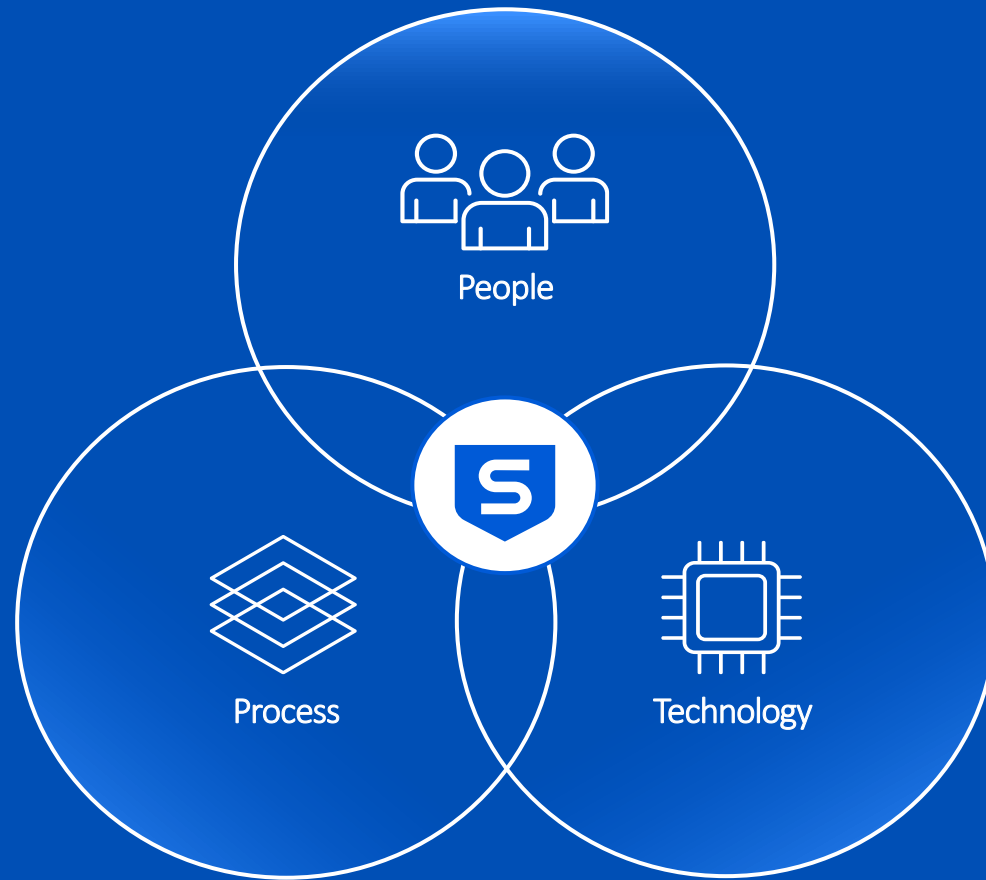
Median threat response time for orgs with dedicated Security Teams

Gartner, Cybersecurity Business Value Benchmark database

Conversaciones del día a día...

- *“Hace días que no abro la consola de gestión.”*
- *“No me da tiempo a analizar todas las alertas.”*
- *“No queremos gestionarlo...” / “Prefiero que lo gestioneis vosotros”*
- *“Me faltan recursos, especialmente en CiberSeguridad.”*
- *“Se encarga un compañero que ahora está de baja.”*

Cybersecurity delivered as a service



How Sophos Delivers Cybersecurity as a Service



MANAGED SECURITY SERVICES



Sophos MDR Complete



Sophos MDR Essentials



Sophos MDR for Microsoft Defender



Sophos IR Services



Sophos NDR



Sophos Managed Risk



A COMPREHENSIVE AND EXTENSIBLE PLATFORM



Sophos Adaptive Cybersecurity Ecosystem



Sophos Central



SECURITY SOLUTIONS AND CONTROL POINTS



Sophos XDR



Sophos Firewall



Sophos Email



Sophos Endpoint



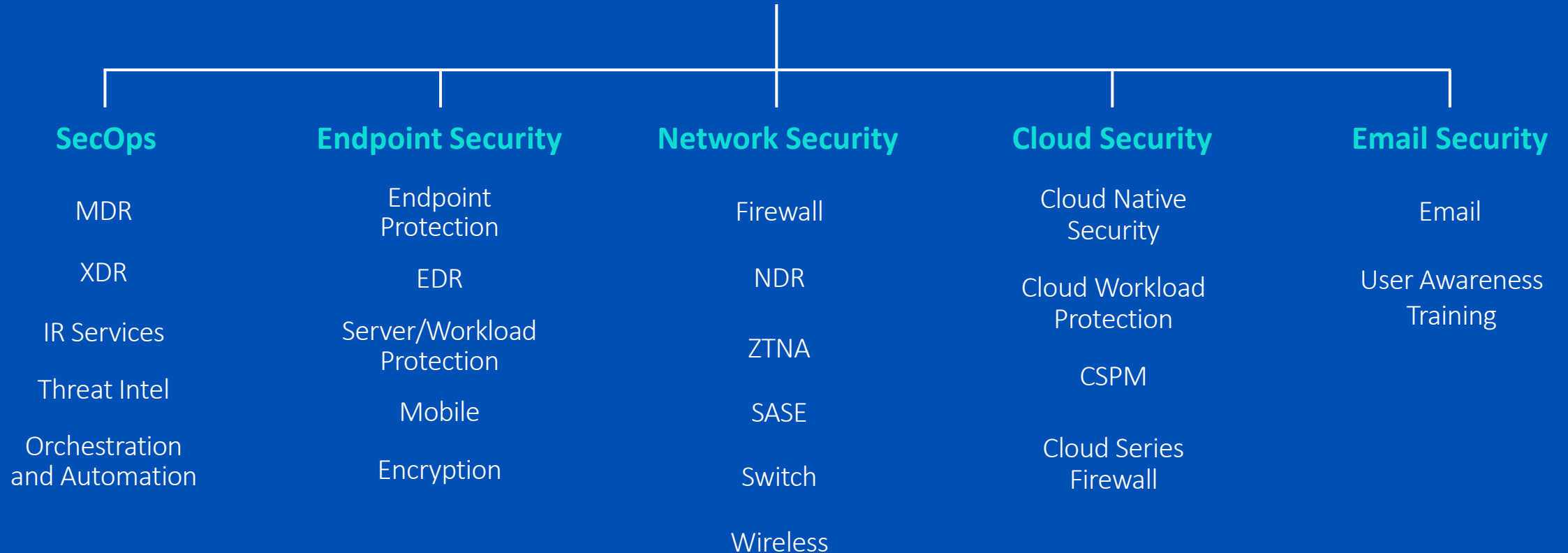
Sophos Cloud



Sophos Factory



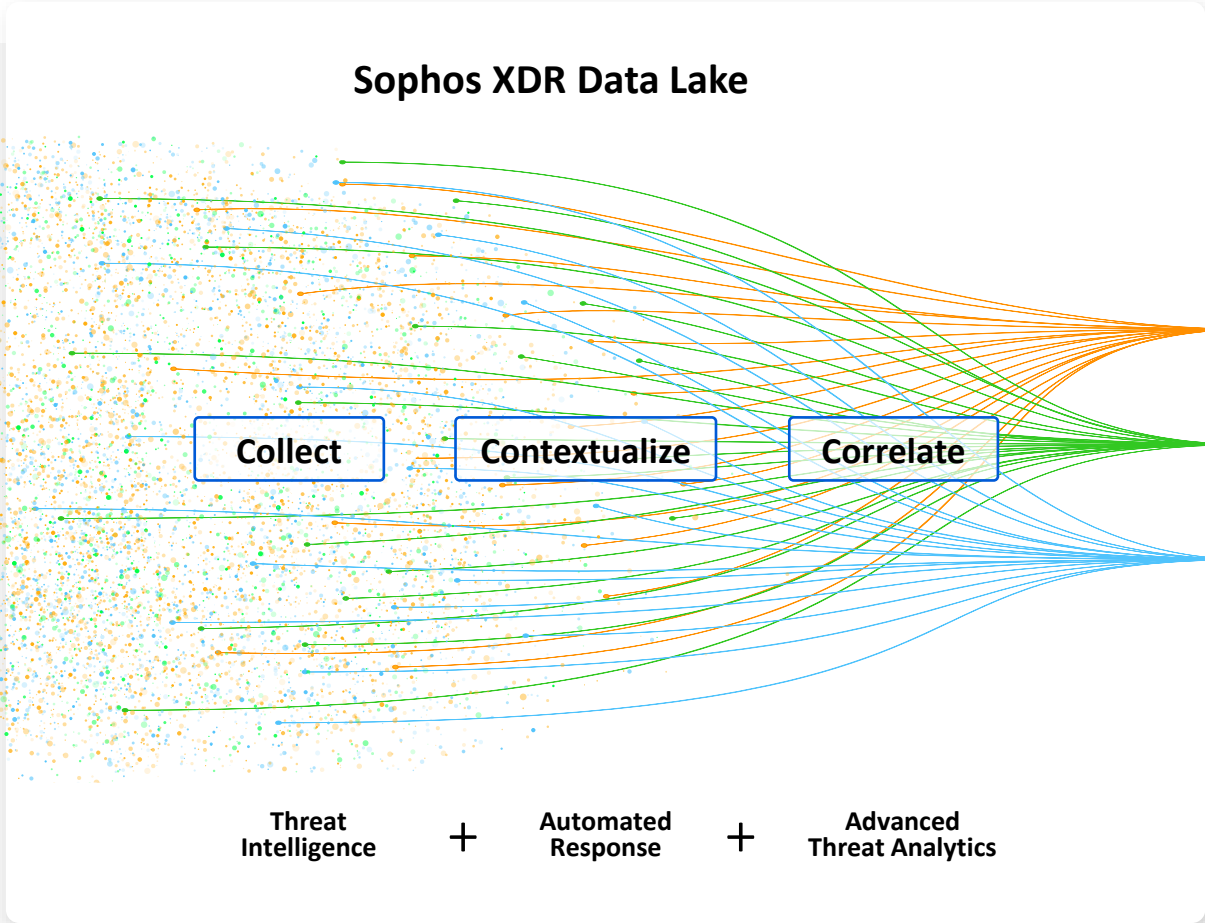
Sophos Central



Event Sources

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

Threat Analysis and Correlation



Sophos MDR Complete

- 24/7 Managed Detection and Response Services**
- Full-Scale Incident Response
 - Root Cause Analysis and Remediation
 - \$1M Breach Protection Warranty
 - Proactive Threat Hunting
 - Expert-Led Threat Investigation

Visibility Across All Key Attack Surfaces

SOPHOS
 ✓ Integrations included

Ep
Endpoint

WP
Workload

Mob
Mobile

Cld
Cloud

Fw
Firewall

Em
Email

ZT
ZTNA

NDR
Network

Endpoint
 ✓ Included

Microsoft **CROWDSTRIKE**

SentinelOne **TREND MICRO**

Symantec^{beta} by Broadcom **BlackBerry**^{beta} CYLANCE

+ Others with Sophos XDR Sensor agent

Firewall

paloalto NETWORKS **FORTINET**

CHECK POINT **CISCO Meraki**

SONICWALL **WatchGuard**

Network

DARKTRACE

THINKST **CANARY** **Securtec**

Skyhigh Security **CISCO Umbrella**

Email

Microsoft 365
 ✓ Included

Google Workspace
 ✓ Included

mimecast
proofpoint.

Productivity
 ✓ Included

Microsoft 365

Google Workspace

Cloud

orca security **aws**

A **Cloud**

Identity

Microsoft
 ✓ Included

okta **auth0**

CISCO **Duo**

ManageEngine

Backup and Recovery

veeam

Sophos Endpoint and Sophos Workload Protection solutions are included with Sophos XDR and MDR. Other Sophos product integrations require a subscription to the applicable solution.

Third-party Endpoint, Microsoft, and Google Workspace integrations are included with Sophos XDR and MDR subscriptions at no additional charge. Integration Packs for other non-Sophos solutions are available as add-on subscriptions for each integration category. Licensing is based on the total number of users and servers.

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 Microsoft Defender

Add-on integrations available for purchase:

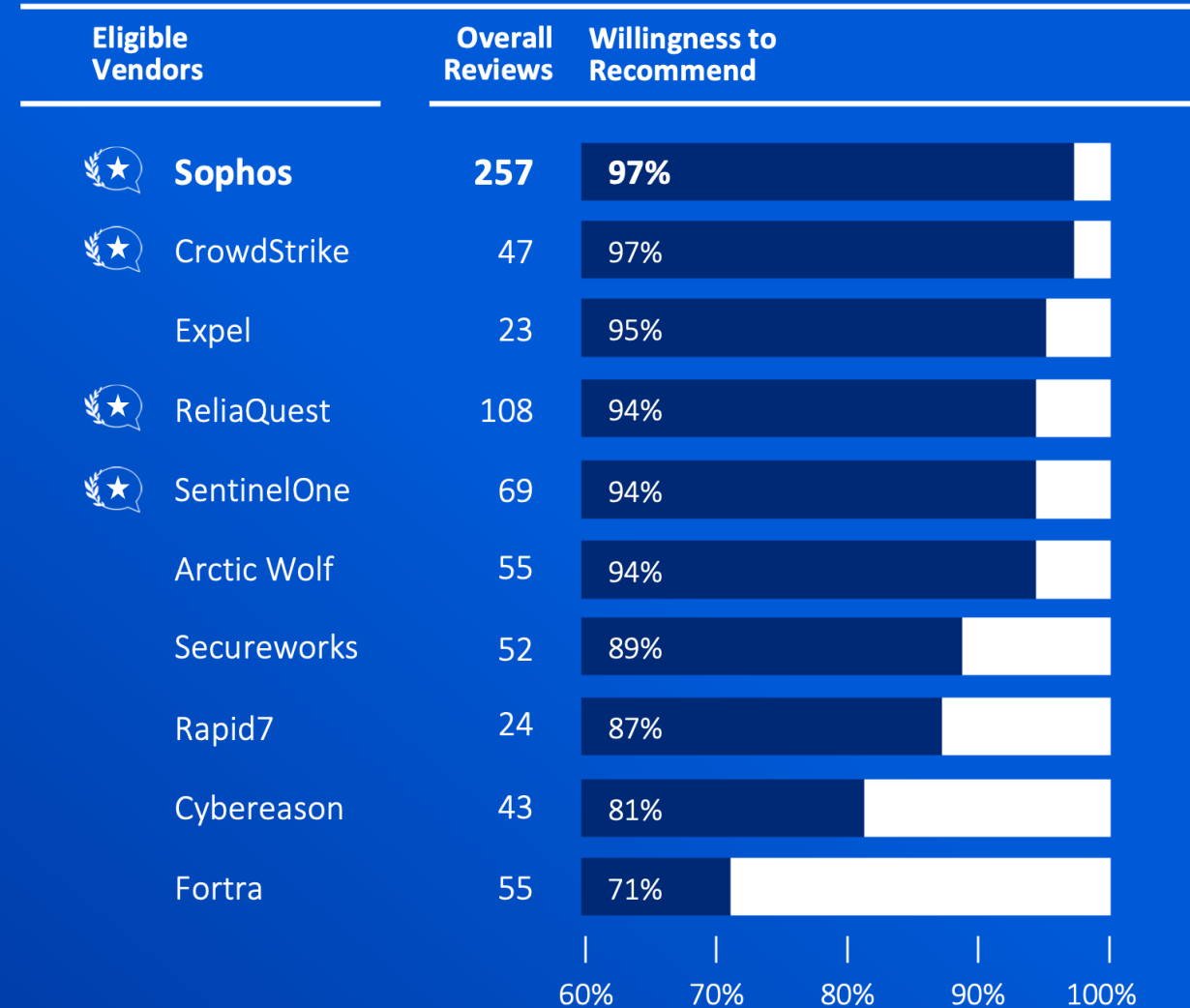


Virtually any security tool that generates threat detection data



Sophos earned the highest rating and had more reviews than any other MDR vendor.

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

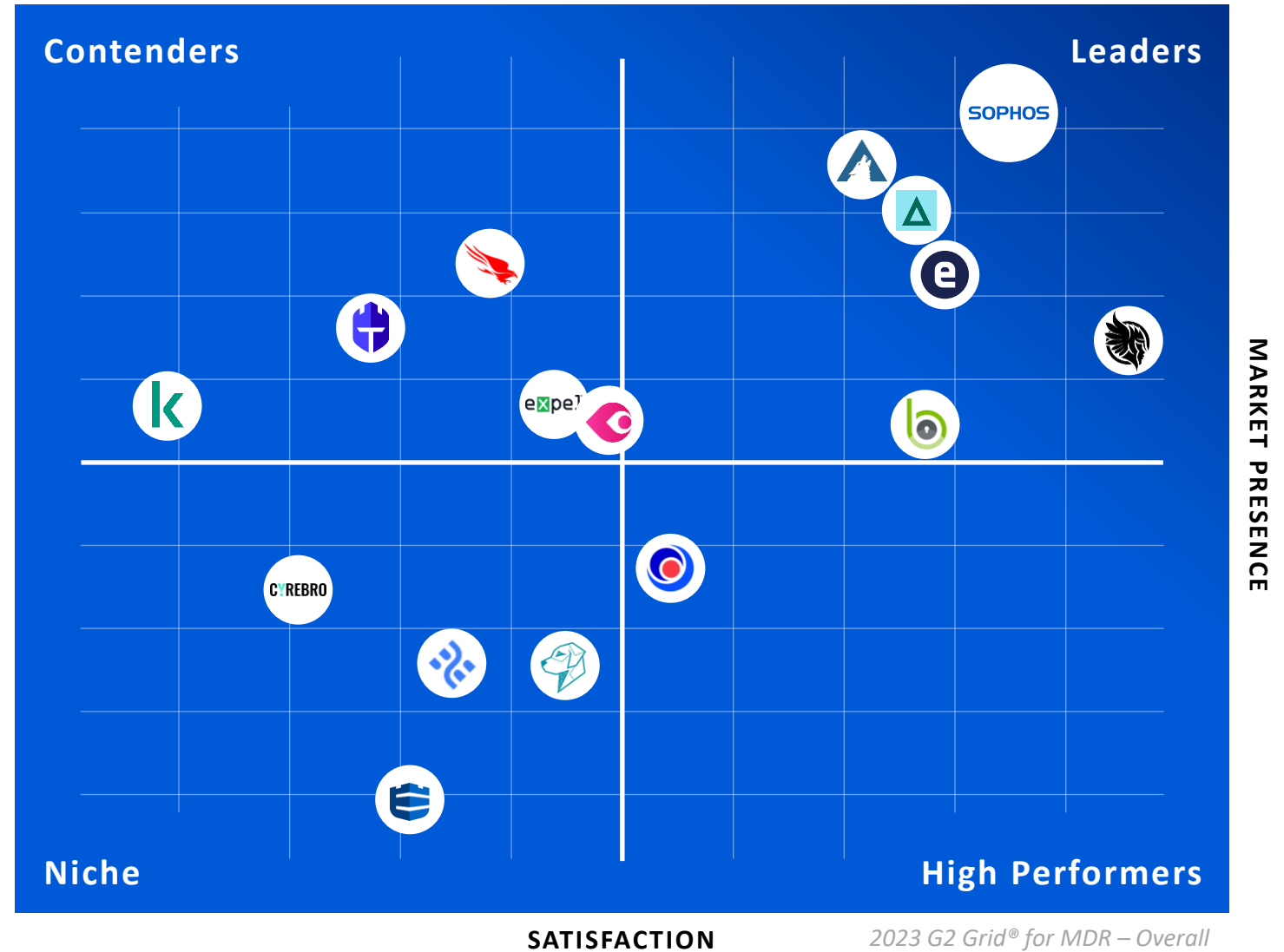


Sorted by Willingness to Recommend

As of May 2023

G2 REPORTS | WINTER 2023

The Top-Rated MDR Service



2023 G2 Grid® for MDR - Overall

SOPHOS

Cybersecurity as a Service