



Sophos MDR: Delivering superior security and business outcomes

Patrick Müller

Snr. Channel Account Executive Eastern Europe

07.10.2025

Sophos at a Glance



\$1.2B ARR

Total company ARR



35,000+

Sophos MDR Customers



600,000+

Total customers



300,000+

Sophos Endpoint Customers



105%

Next-Gen NIR



40,000+

Sophos XDR Customers



58,000+

Channel Partners

22,000 active partners



250,000+

Sophos Firewall Customers



100+

Strategic Partners

(Technology, services, etc.)



20,000+

Sophos Email Customers

MISSION: Enable MSPs to deliver better cybersecurity outcomes and accelerate growth and profitability.



The **largest provider** of Managed Detection and Response Services (MDR)



The only vendor named a **Gartner Customers' Choice** and **G2 Leader** for EPP, Firewall, and MDR



A top performer in the **MITRE ATT&CK Evals** for Enterprise Products and Managed Services



Industry-leading **compatibility** with virtually any environment or tech stack



The most expansive portfolio of world-class products and managed security services

Today's challenge

Allianz

Top 10

Allianz Ri:

Basierend auf
konnten.

Änderungen vor

Makro

Mangel an

Top 10 risks in Germany

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 454. Figures don't add up to 100% as up to three risks could be selected

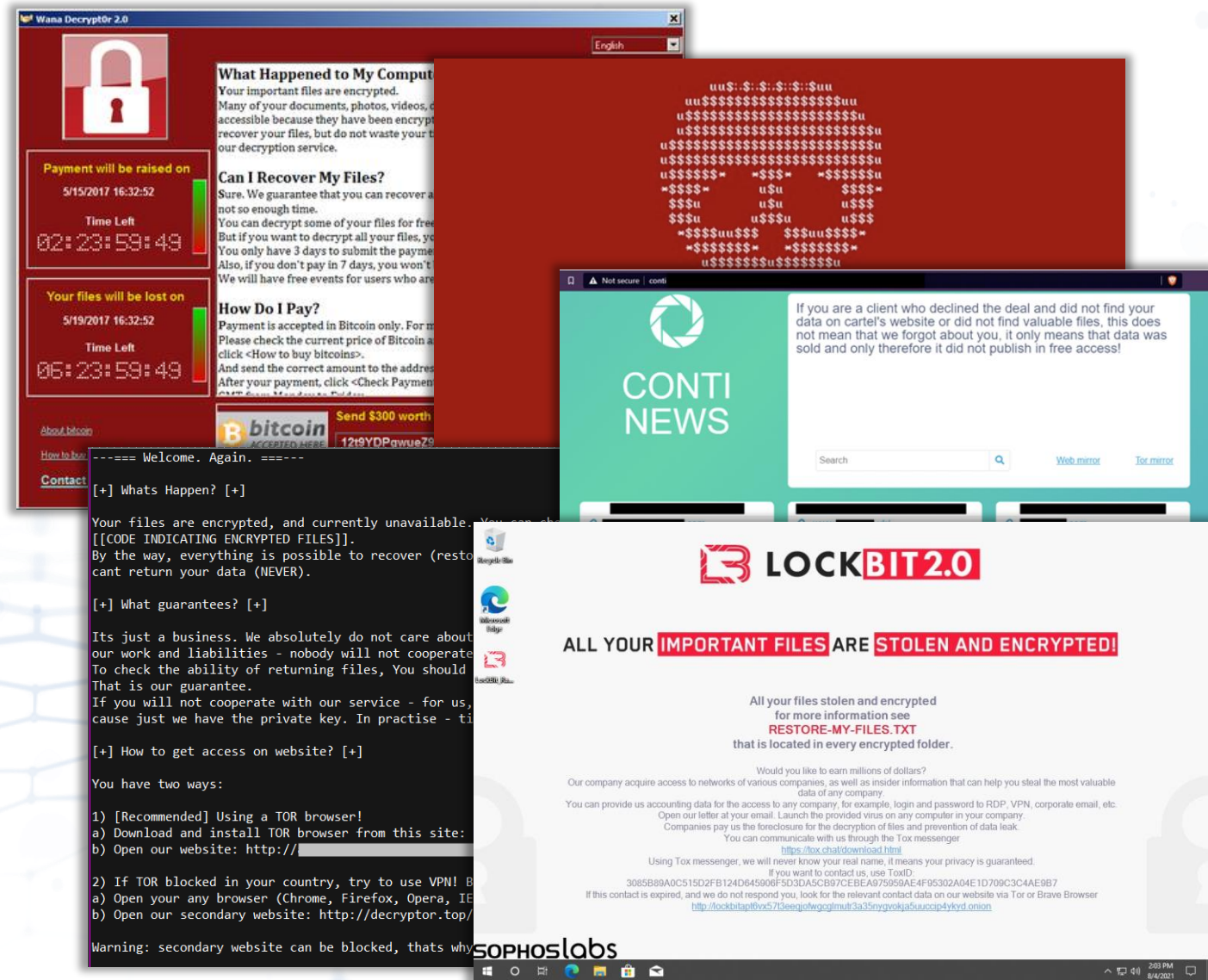
Rank		Percent	2023 rank	Trend
1	Cyber incidents (e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)	44%	2 (40%)	↑
2	Business interruption (incl. supply chain disruption)	37%	1 (46%)	↓
3	Changes in legislation and regulation (e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)	23%	4 (23%)	↑
4	Shortage of skilled workforce ¹	20%	6 (17%)	↑
5	Natural catastrophes (e.g., storm, flood, earthquake, wildfire, extreme weather events)	20%	5 (19%)	→
6	Climate change (e.g., physical, operational, and financial risks as a result of global warming)	19%	8 (17%)	↑
7	Energy crisis (e.g., supply shortage / outage, price fluctuations)	17%	3 (32%)	↓
8	Fire, explosion	16%	10 (13%)	↑
8	Political risks and violence (e.g., political instability, war, terrorism, coup d'état, civil commotion, strikes, riots, looting)	16%	NEW	↑
10	Macroeconomic developments (e.g., inflation, deflation, monetary policies, austerity programs)	15%	6 (17%)	↓

t werden

36%

Ransomware – 8 years in a row

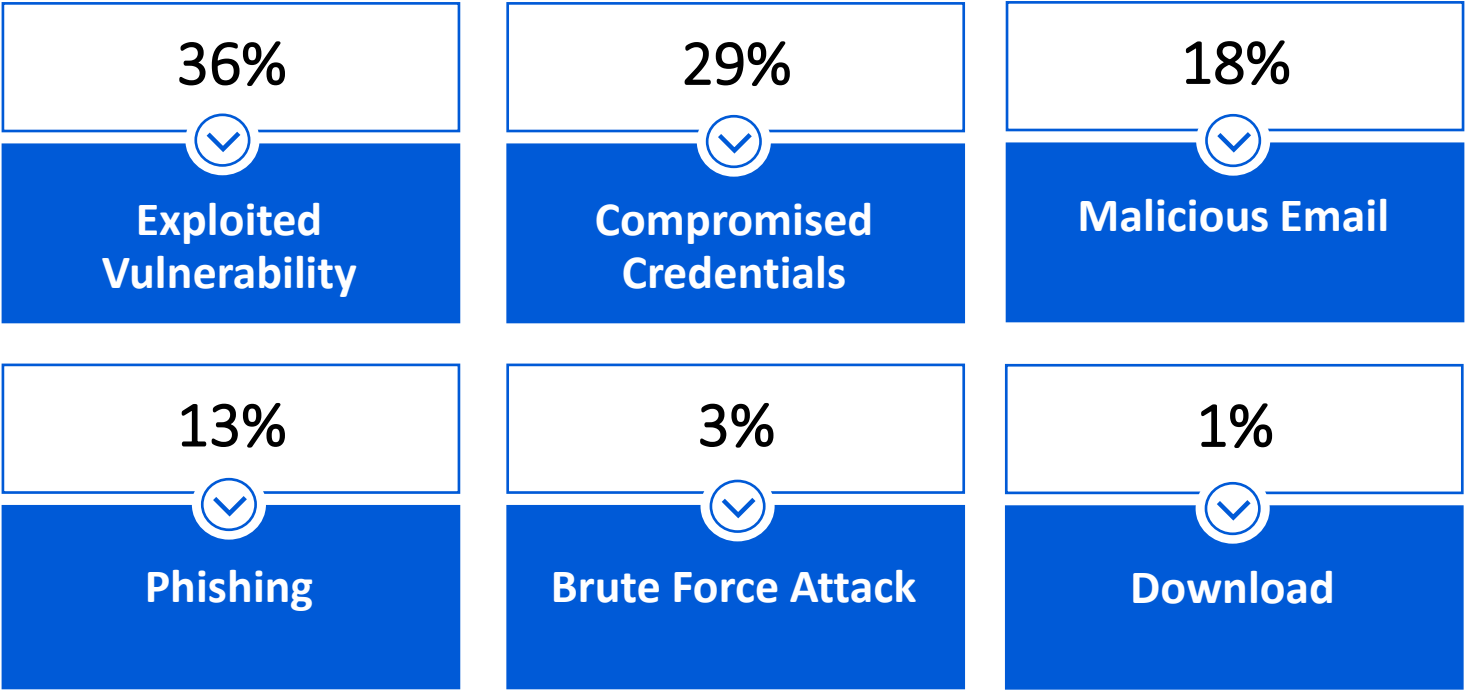
- Ransomware attacks remain successful
 - Organized crime
 - Professional setup
 - Groups focus on specific topics
 - Extortion (= Backup is not enough)
 - Remote Ransomware is a real threat
 - Not a lot of protection available (apart from Sophos)
- Mistakes were made
 - Sloppy approach with regards to IT Security
 - Budget spent on the right tools / services
 - Lacking Incident Response Plans
 - Belief that on-premise gives more control / security



Adversaries don't break in.
They login.



Root Cause of Ransomware Attacks 2023



Source: The State of Ransomware 2023, Sophos. Responses from 1,974 organizations hit by ransomware in the last year

Adversaries don't break in. They log in.

91%

Of ransomware attacks start outside
standard business hours

95%

Of successful cyber attacks involve
use of RDP by adversaries

16 Hours

Median time it takes attackers to
reach Active Directory

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

...and defenders are struggling to keep pace.

Cybercrime in Czech Republic

Cybercrime and Internet Offenses

	2019	2020	2021	2022	2023
Cybercrime and Internet Offences	8,417	8,073	9,518	18,554	21,337
% Change	23.5%	-4.1%	17.8%	195%	15%

Source: National Cyber and Information Security Agency (NUKIB) Report 2022

Examples:

University Hospital Brno estimates it suffered **150 million crowns** worth of damage after a 2020 cyber-attack.

The cost of a 2019 ransomware attack on a hospital in Benešov is estimated at **59 million crowns**



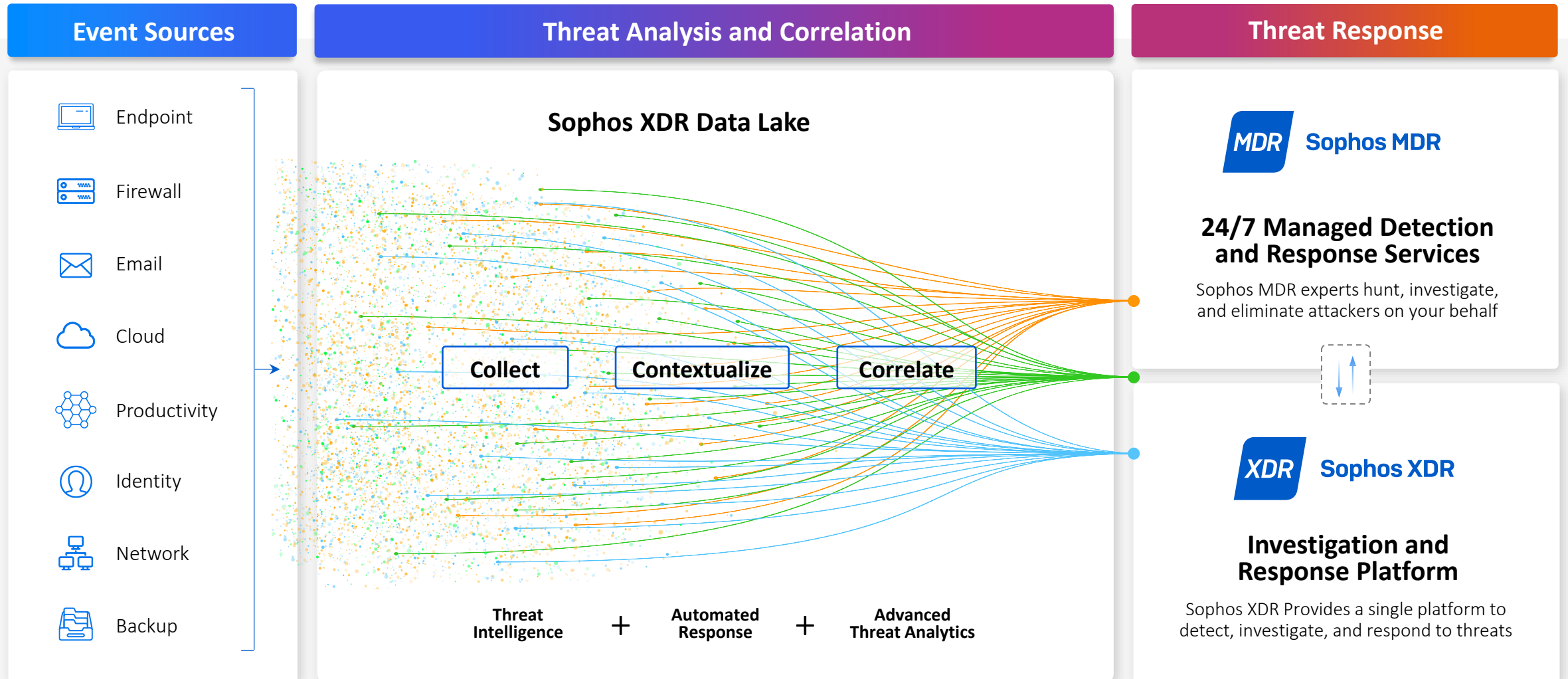
Gartner®

60% of organizations will use an MDR Service by 2025

Delivering Optimal Cyber Security Outcomes



Sophos Threat Detection and Response Platform



The logo consists of the letters 'MDR' in a bold, white, sans-serif font, enclosed within a white square that has a slight 3D effect with a shadow on the right side.

Sophos MDR

**Expert-led defense with
full-scale incident response**

MONITOR THREATS 24/7

Our highly skilled team of experts monitor, investigate, and respond to threats on your behalf.

ACCELERATE THREAT RESPONSE

We have an industry-leading average threat response time of 38 minutes—96% faster than the industry benchmark.

FULL-SCALE INCIDENT RESPONSE

Includes unmetered, full-scale IR—no hourly limits and no need to invoke an IR retainer or purchase additional DFIR services modules.

GET MORE ROI FROM SECURITY TECHNOLOGY

Our analysts can leverage your existing technology investments to detect and respond to threats.

SOPHOS MDR SERVICE OVERVIEW

**A flexible managed service that
meets you where you are**

Sophos MDR Service Tiers

Sophos MDR for
Microsoft Defender



Sophos MDR
Essentials

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

Integration Packs



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 by Broadcom beta

BlackBerry CYCLANCE beta

+ Others with Sophos XDR Sensor agent

Firewall

paloalto NETWORKS

FORTINET

CHECK POINT

CISCO Meraki

SONICWALL

WatchGuard

Network

DARKTRACE

THINKST CANARY

Secutec

Skyhigh Security

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.

Included Integrations



Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and third-party integrations.



Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm.



Microsoft Security Suite

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Cloud
- Microsoft Sentinel
- Microsoft Defender for Identity
- Azure Information Protection
- Microsoft Entra ID
- Microsoft 365 IAM



Sophos Endpoint Protection

Endpoint Prevention and EDR that stop advanced threats and detect malicious behaviors—including attackers mimicking legitimate users.



Sophos Network Detection and Response

Continuously monitor activity inside your network to detect suspicious actions and lateral attacker movement.



Google Security Suite

- Google System Defined Rules
- Alert Center
- Suspicious Activities
- Authentication
- Malware and Phishing
- Access Control
- User and Device Activity
- Data Control



Sophos Cloud

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform.



Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks.



Third-Party Endpoint Protection

Compatible with...

- Microsoft
- Symantec (Broadcom)
- CrowdStrike
- Trend Micro
- SentinelOne
- BlackBerry (Cylance)

+ Other solutions with Sophos XDR Sensor agent

Includes 90 days of data retention

Add-On Integrations



Firewall

Compatible with...

- Check Point
- Cisco
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard



Identity

Compatible with...

- Auth0
- Duo
- ManageEngine
- Okta

Microsoft integration included



Cloud

Compatible with...

- Orca Security

AWS, Azure and GCP integrations available via Sophos Cloud product



Network Security

Compatible with...

- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary



Email

Compatible with...

- Mimecast
- Proofpoint

Microsoft 365 and Google Workspace integrations included



Backup and Recovery

Compatible with...

- Veeam

Add-on Integration Packs and the Data Retention Pack are available for Sophos MDR and Sophos XDR
All Integration Packs are licensed based on the total number of Sophos MDR/XDR seats (users+servers)



1-Year Data Retention

24x7 Coverage from Seven Global SOC's



The **Sophos Breach Protection Warranty** covers up to **\$1 million** in response expenses



Included with new **Sophos MDR Complete** subscriptions – at no additional cost



Built-in automatically with **MSP Flex and term licenses**, both new customers and renewals



Comprehensive coverage: endpoints, servers, Windows, macOS, no geographic limits



Underwritten by Sophos, demonstrating our confidence in our protection



Includes Incident Response

MARKET PERFORMANCE

The **most used** and **highest rated**
MDR service in the world

The **only vendor** named 2023 Gartner Customers' Choice in each of these categories

2023

**Managed Detection
and Response**



2023

**Endpoint Protection
Platforms**



2023

Network Firewalls



2023

**Mobile Threat
Defense**



Gartner.
Peer Insights™

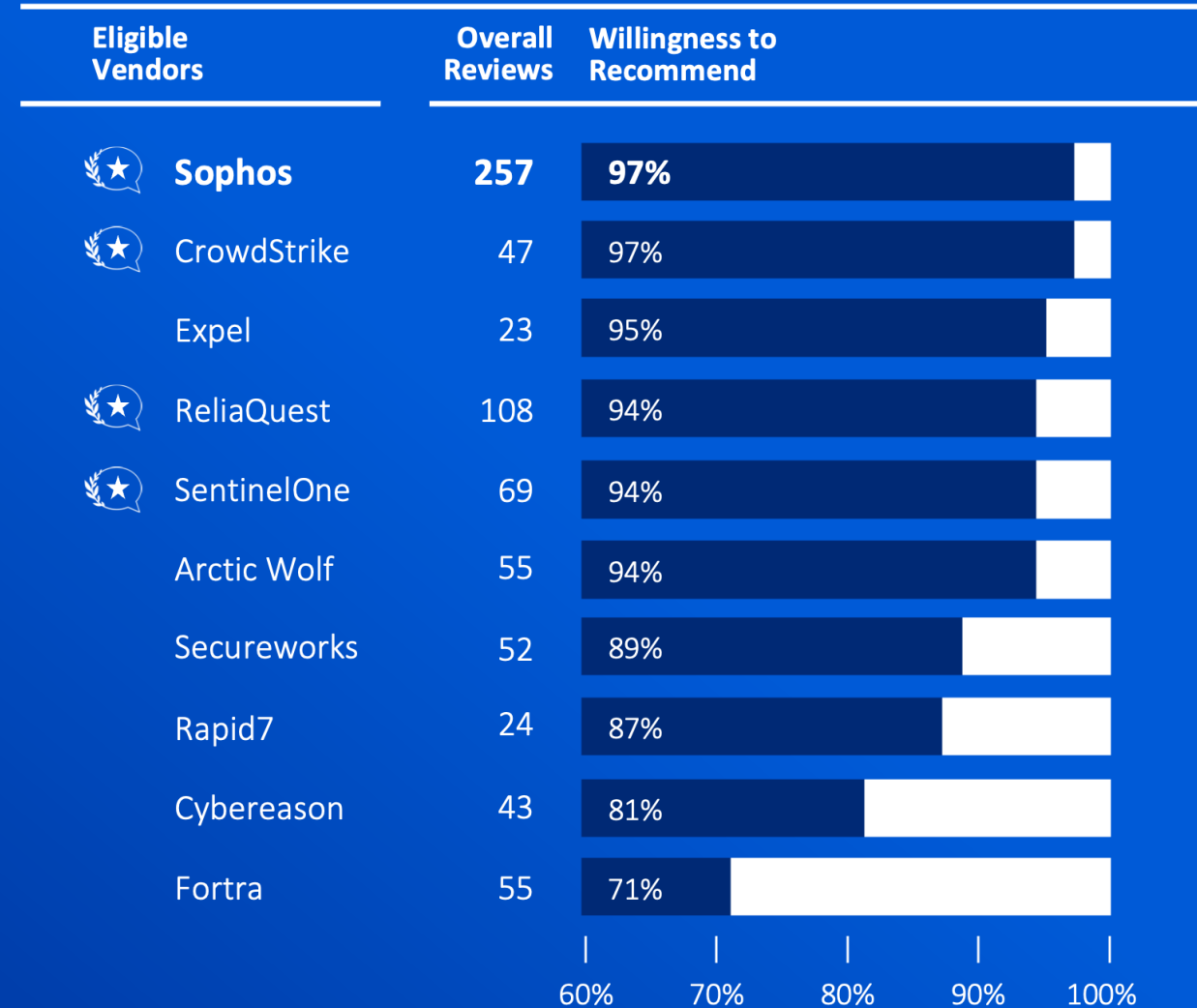


The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors 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 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



Gartner®

2025 Gartner Magic Quadrant for Endpoint Protection Platforms

Years as a Leader

 SOPHOS	16
 CROWDSTRIKE	6
 Microsoft	6
 SentinelOne	5
 paloalto NETWORKS	3

