Sophos MDR

Das Ergebnis zählt - rundum sicher durch Cybersecurity als Service

Herbert Mayer
Senior Sales Engineer - Public

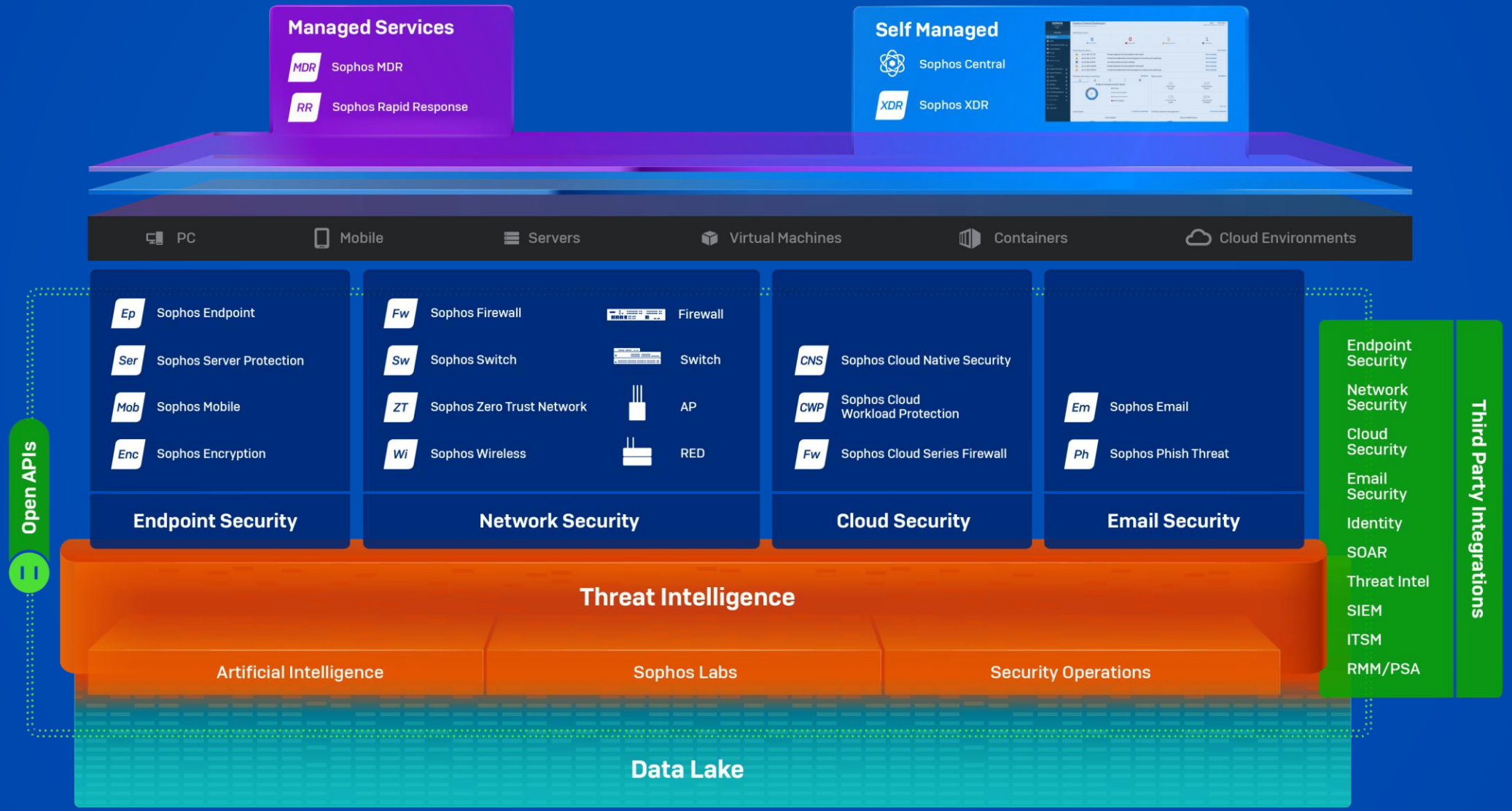
SOPHOS

Was ist Sophos Managed Detection and Response (MDR)?

24/7 Security Operations

- Threat Hunting
- Incident Response
- Proaktive Verbesserung der Sicherheit

SOPHOS Adaptive Cybersecurity Ecosystem



SOPHOS

Sophos MDR

Outcome-Focused Security™

Das Ergebnis zählt – rundum sicher durch Cybersecurity as a Service

Cyberangriffe nehmen in Umfang und Komplexität zu

Zwei Drittel der deutschen Unternehmen wurden 2021 mit Ransomware angegriffen. Der Schaden lag im Durchschnitt bei 1,7 Mio € [1].

Cybersecurity Werkzeuge sind teuer und kompliziert

Unternehmen setzen mehrere Dutzend unterschiedlicher Monitoring- und Sicherheitstools ein. IT-Sicherheits-Teams werden von Alarmen überflutet.

Cybersecurity Experten sind selten und teuer

Die Kosten für ein eigenes SOC liegen bei knapp 3 Mio € pro Jahr[2]

[1]The State of Ransomware 2022, Sophos; The Active Adversary Playbook 2022, Sophos

[2]Ponemon Institute: "The Economics of Security Operations Centers: What Is the True Cost for Effective Results?"

SOPHOS

Wie viele IT Security Spezialisten und welche Werkzeuge benötige ich?

GERINGERES RISIKO

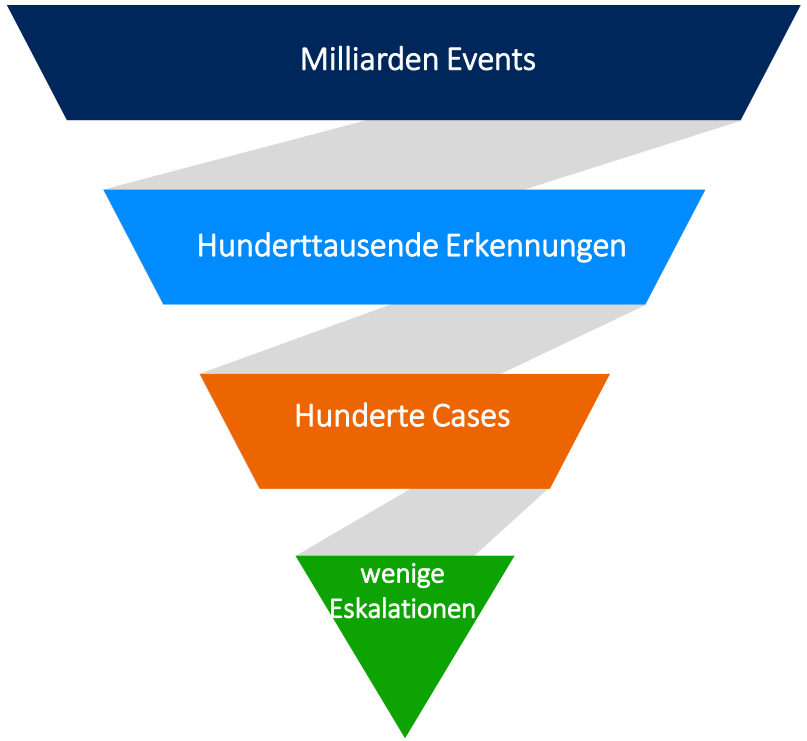
1.000+ fache Reduktion von Vorfällen, die eine genaue Betrachtung benötigen

HOHE EFFIZIENZ

12.000x Effizientere IT Security Teams

GERINGERE KOSTEN

5x Günstiger als das eigene SOC



Sophos MDR Spezialisten haben rund um die Uhr den Blick auf aktuell 12.000 Unternehmenskunden und nutzen Erkenntnisse über neue Bedrohungen über die Grenzen der Netzwerke hinweg. Eine Betrachtung auf eine einzige Infrastruktur lässt diesen entscheidenden Vorteil aus – vor allem bei zeitlich kritischen Ereignissen.

Ein eigenes SOC im 24/7 Betrieb ist mehr als 5x teurer gegenüber eines ver-gleichbaren Sophos MDR Complete Angebots. Das begründet sich in den Personalkosten für ein eigenes SOC Team und den Kosten für eine XDR und SIEM Plattform, Konnektoren, Threat Feeds, Playbooks, SOAR Werkzeugen, etc.

Sophos Vorteile: MDR und Cybersecurity

Mehr Organisationen vertrauen bei MDR auf Sophos, als auf jeden anderen Anbieter.

- Sophos liefert führende Cybersecurity-Produkte für **über 530.000 Kunden** weltweit
- Kein Anbieter wurde häufiger als **Gartner Leader** im Bereich Endpoint Security ausgezeichnet als Sophos
- Der am **besten bewertete** und am **häufigsten getestete** MDR-Service bei Gartner Peer Insights

Warum?

- **Breites Portfolio führender Next-Gen Produkte**
- **Adaptive Cybersecurity Ecosystem**
- **Sophos Central**
- **AI and Automation**
- **Sophos X-Ops Research**
- **A Proven, Trusted and Leading MDR Provider**

SOPHOS

SOPHOS MDR: Offen und flexibel

MDR Sophos MDR

Kompatibel mit Ihrer Umgebung
Wir nutzen Sophos Werkzeuge, die Werkzeuge anderer Anbieter – oder eine Kombination aus beiden

Kompatibel mit Ihren Anforderungen
Wir bieten komplettes Incident Response - oder Unterstützung für Ihr Team

Kompatibel mit Ihrem Unternehmen
Unser Team hat umfangreiche Erfahrung mit Angriffen auf Unternehmen aller Branchen

SOPHOS

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

Endpoint

Microsoft, CROWDSTRIKE, McAfee, SentinelOne, CHECK POINT, TREND MICRO, 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

Network

DARKTRACE, Forcepoint

Sophos MDR – Managed Detection and Response

Personal

Ich brauche Experten, um...

- meine Threat Response komplett zu verwalten
- die Threat Response meines Teams zu ergänzen
- um mein Team bei Bedrohungen zu alarmieren

Prozess

Erkannte Bedrohungsfälle benötigen...

- komplette Vorfallsbearbeitung (Incident Response)
- Eindämmung, damit mein Team sie eliminieren kann
- detaillierte Handlungsempfehlungen

Technologie

Ich möchte nutzen

- Sophos: bester Schutz, Erkennung und Reaktion
- Kombination aus Sophos und nicht-Sophos Tools
- keine Sophos Tools

Sichtbarkeit

Erkennt Bedrohungen mit Daten von...

- Endpoint
- Firewall
- Email
- Identity
- Public Cloud
- Network

Nahtlos integriert mit...

- XDR Sophos XDR
- Fw Sophos Firewall
- Em Sophos Email
- Mb Sophos Mobile
- Cld Sophos Cloud
- NDR Sophos NDR

Integrationen mit dem Service inkludiert:

Beliebige Antivirus- oder Endpoint-Schutz-plattform, inkl. Windows Defender

Weitere Integrationen zum Kauf verfügbar:

Nahezu jedes Schutzlösung, welche Bedrohungsdaten erzeugt und meldet

Sophos Servicestufen

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24/7 Überwachung, Bedrohungserkennung und Reaktion durch Experten	✓	✓	✓
Kompatibel mit Security-Werkzeugen anderer Hersteller	✓	✓	✓
Wöchentliches und monatliches Reporting	✓	✓	✓
Monatliches Briefing "Sophos MDR ThreatCast" zu aktuellen Bedrohungen	✓	✓	✓
Sophos Account Health Check – ist Sophos XDR richtig konfiguriert?		✓	✓
Proaktive Bedrohungssuche durch Experten		✓	✓
Stoppen und Eindämmen von Bedrohungen Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung, Reaktion) oder Sophos XDR Sensor (Erkennung, Reaktion)		✓	✓
Direkter Telefon-Support bei Vorfällen		✓	✓
Vollständiges Incident-Response: komplette Neutralisierung von Bedrohungen Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung und Reaktion)			✓
Ursachenanalyse – und wie können erneute Angriffe verhindert werden?			✓
Dedizierter Ansprechpartner beim Incident Response Team			✓

Sophos MDR nutzt Daten folgender Integrationen kostenfrei

Sophos XDR

Die einzige XDR-Plattform, die native Endpunkt-, Server-, Firewall-, Cloud-, E-Mail-, Mobil- und Microsoft-Integrationen vereint.

Sophos Firewall

Überwachung und Filterung des ein- und ausgehenden Netzwerkverkehrs, um aktuelle Bedrohungen zu stoppen, bevor sie Schaden anrichten.

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Azure Active Directory
- Microsoft Defender for Cloud Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365

Sophos Endpoint Protection

Blockieren Sie aktuelle Bedrohungen und erkennen Sie böswillige Verhaltensweisen - einschließlich Angreifern, die sich als legitime Benutzer ausgeben.

Sophos Network Detection and Response

Überwachen Sie kontinuierlich die Aktivitäten innerhalb Ihres Netzwerks, um verdächtige Aktionen zwischen Geräten zu erkennen, die sonst unbemerkt bleiben.

Third-Party Endpoint Protection

Kompatibel mit...

- Microsoft
- CrowdStrike
- SentinelOne
- Check Point
- Trend Micro
- BlackBerry (Cylance)
- McAfee
- Malwarebytes

Sophos Cloud

Sichern Sie Ihre Cloud Ressourcen und gewinnen Sie Transparenz über Ihre wichtigen Cloud-Dienste, einschließlich AWS, Azure und Google Cloud Platform.

Sophos Email

Schützen Sie Ihren Posteingang vor Malware und profitieren Sie von der fortschrittlichen KI, die gezielte Imitations- und Phishing-Angriffe.

90-Tage Datenhaltung

SOPHOS

Sophos MDR Add-On Integrationen für schnellste Reaktion

Firewall

Kompatibel mit...

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

Public Cloud

Kompatibel mit...

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

Identity

Kompatibel mit...

- Okta
- Duo

Network Security

Kompatibel mit...

- Darktrace
- Forcepoint
- McAfee (web gateway)

Email

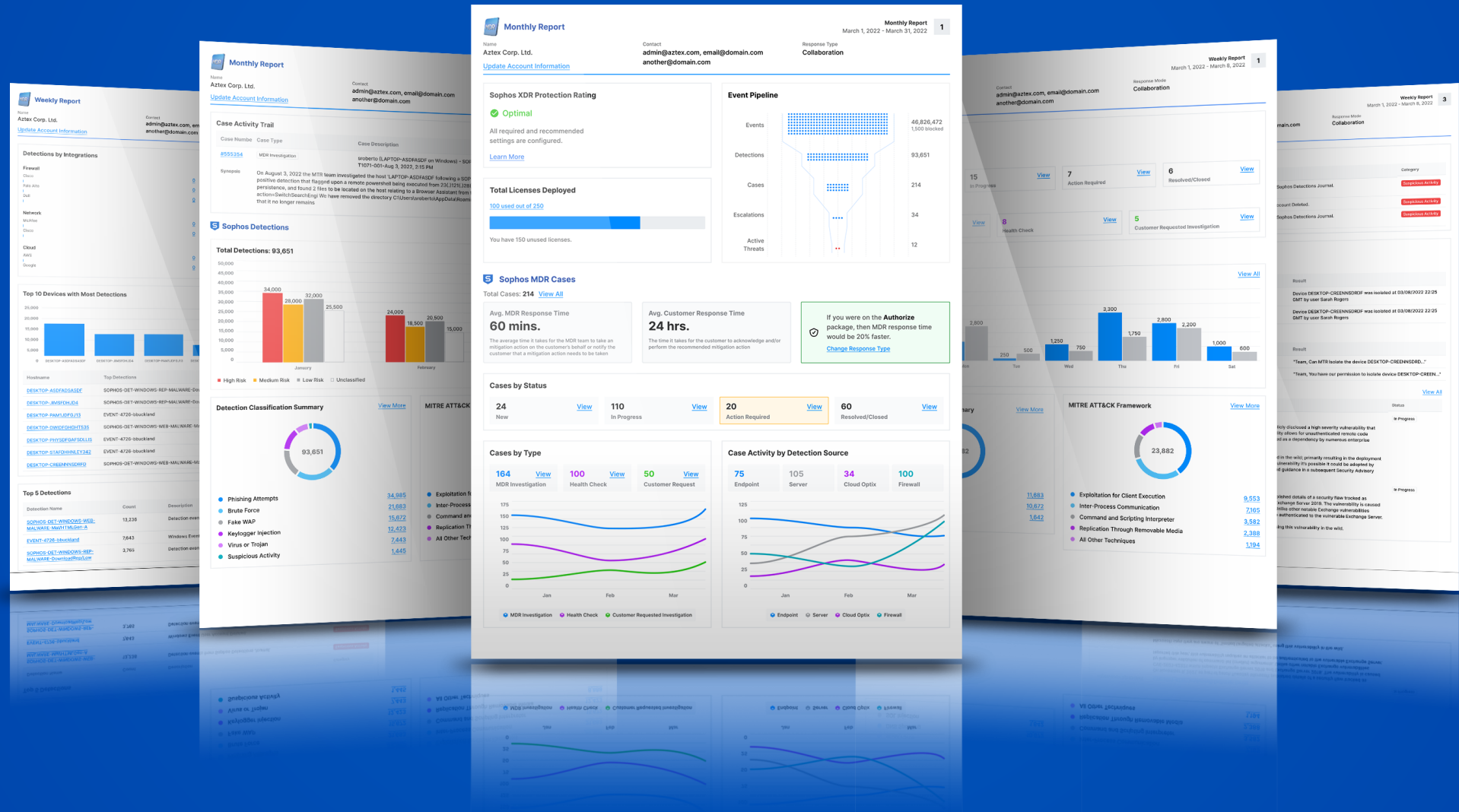
Kompatibel mit...

- Proofpoint
- Mimecast

1-Jahr Datenhaltung

Alle Integration Packs sind für Sophos MDR, Sophos MDR Complete und Sophos Threat Advisor verfügbar.
Die Datenhaltung ist für Sophos MDR und Sophos XDR erhältlich.
Alle Integration Packs müssen entsprechend der Anzahl der Sophos MDR-Lizenzen des Kunden erworben werden.

Managementtaugliche Cybersecurity Reports



SOPHOS

Gartner Peer Insights™

Der am **besten bewertete** und am **häufigsten getestete** MDR-Service bei Gartner Peer Insights

Sophos MDR

4.8	97%
Average Rating	Would Recommend

Based on 256 Reviews

SentinelOne	4.5
CrowdStrike	4.8*
Arctic Wolf	4.8*

Sophos Endpoint

4.8	95%
Average Rating	Would Recommend

Based on 539 Reviews

Microsoft	4.4
CrowdStrike	4.7
Trend Micro	4.6

Sophos Firewall

4.8	95%
Average Rating	Would Recommend

Based on 362 Reviews

Fortinet	4.6
Check Point	4.5
Palo Alto Networks	4.5

Reviews from last 12 months as of August 1, 2022
*Vendors with fewer than 50 customer reviews

SOPHOS

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."

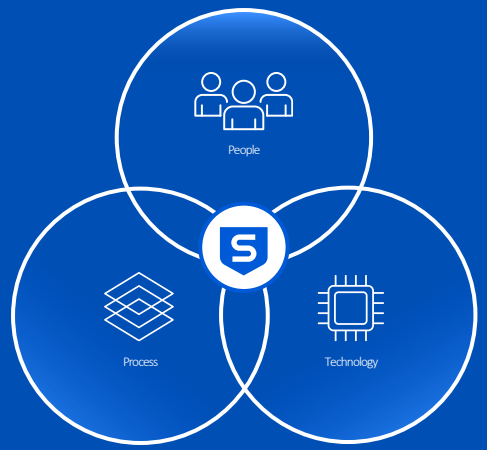
Scott Crawford, 451 Research
August 2022

451 Research

Die Lösung: Cybersecurity as a Service

MANAGED DETECTION AND RESPONSE

Das Ergebnis zählt - rundum sicher durch Cybersecurity as a Service



- Ihr ausgelagertes Security Operations Center (SOC)
- 24/7 Bedrohungserkennung und Reaktion
- Bedrohungssuche durch Experten
- Vollständiges Incident Response bei Angriffen
- Bestmögliches Ergebnis für Ihre IT-Sicherheit

SOPHOS

Sophos MDR

Outcome-Focused Security™

Das Ergebnis zählt – rundum sicher durch Cybersecurity as a Service

Kompatibel mit Ihrer Umgebung

Kompatibel mit ihren Anforderungen

Kompatibel mit Ihrem Unternehmen

Was kostet Sie Ihr Zögern?