Lösungsbroschüre

Sophos Managed Detection and Response

24/7 Threat Detection and Response

Sophos MDR ist ein vollständig verwalteter 24/7-Service, der von Experten bereitgestellt wird. Die hochspezialisierten Experten erkennen Cyberangriffe auf Ihre Computer, Server, Netzwerke, Cloud Workloads, E-Mail-Konten, Backups etc. und ergreifen Reaktionsmaßnahmen.

Effektiver Schutz rund um die Uhr

Rund um die Uhr aktive Cybersecurity Operations sind für Unternehmen mittlerweile zwingend notwendig. Moderne Betriebsumgebungen sind jedoch hochkomplex und Cyberbedrohungen entwickeln sich permanent weiter. Das macht es Unternehmen zunehmend schwer, sich komplett selbst um das Erkennen und Bekämpfen von Cyberbedrohungen zu kümmern.

Mit Sophos MDR stoppen unsere Experten für Sie komplexe, manuell gesteuerte Angriffe. Wir beseitigen Bedrohungen, bevor diese Ihre Geschäftsabläufe stören oder sensible Daten gefährden können. Sophos MDR ist in verschiedenen Service-Leveln erhältlich und kann flexibel bereitgestellt werden – entweder über unsere proprietäre Technologie oder mit Ihren bereits bestehenden Cybersecurity-Technologien.

Cybersecurity als Komplett-Service

Sophos MDR nutzt umfassende MDR-Funktionalitäten (Managed Detection and Response), die Ihre Daten überall schützen, und leistet dadurch Folgendes:

- **Erkennt mehr Cyberbedrohungen als Sicherheitstools allein**
  Unsere Tools blockieren automatisch 99,98 % der Bedrohungen. So können sich unsere Analysten auf die Suche nach besonders versierten Angreifern konzentrieren, die nur geschulte Experten enttarnen und stoppen können.

  Reagiert schnell, damit Bedrohungen nicht Ihren Betrieb stören
  Bei einer Bedrohung erkennen, analysieren und reagieren unsere Experten innerhalb von Minuten – egal, ob Sie eine umfassende Reaktion auf Vorfälle oder Hilfe bei der Entscheidungsfindung benötigen.

  Ermittelt die Ursache von Bedrohungen, um künftige Vorfälle zu verhindern
  Wir ergreifen proaktiv Maßnahmen und geben Empfehlungen, um das Risiko für Ihr Unternehmen zu verringern. Weniger Vorfälle bedeuten weniger Störungen für Ihre IT- und Sicherheitsteams, Ihre Mitarbeiter und Ihre Kunden.

Kompatibel mit bereits vorhandenen Cybersecurity-Tools

Sie können selbst entscheiden: Nutzen Sie die starken Technologien aus unserem preisgekrönten Portfolio oder Ihre bereits bestehenden Cybersecurity-Technologien.

Die offene, KI-native Plattform von Sophos ist mit einer Vielzahl von Identity-, Netzwerk-, Firewall-, E-Mail-, Cloud-, Produktivitäts-, Backup- und Endpoint-Sicherheitslösungen kompatibel und bietet Microsoft- und Google-Workspace-Integrationen ohne Aufpreis.

Vorteile auf einen Blick

- Stoppen Sie Ransomware und andere komplexe, manuell gesteuerte Angriffe mithilfe eines 24/7-Expertenteams
- Maximieren Sie den Return on Investment Ihrer bestehenden Cybersecurity-Technologien
- Wählen Sie aus flexiblen Service-Leveln genau so viel Service, wie Sie in Ihrer individuellen Situation benötigen: komplette Incident Response durch Sophos, Zusammenarbeit unseres und Ihres Teams oder Benachrichtigungen und Tipps von uns, welche Reaktionsmaßnahmen wir empfehlen
- Sichern Sie sich bessere Konditionen bei Cyberversicherungen
- Ermöglichen Sie Ihren internen IT-Mitarbeitern, sich auf Projekte zu konzentrieren, die das Geschäft voranbringen

MDR – maßgeschneidert für Sie

Sophos MDR ist in verschiedenen Service-Leveln mit unterschiedlichen Reaktions-Optionen erhältlich – je nach Ihren individuellen Bedürfnissen: Überlassen Sie Ihre gesamte Reaktion auf Vorfälle komplett dem Sophos MDR Operations Team, bekämpfen Sie Cyberbedrohungen in enger Zusammenarbeit mit unserem Team oder lassen Sie sich nur benachrichtigen, sobald Bedrohungen erkannt wurden. Unser Team verschafft sich bei einem Angriff schnell Überblick. In allen Fällen können wir innerhalb von Minuten reagieren.

Wichtigste Funktionen

24/7 Threat Monitoring und Reaktion

Wir erkennen Bedrohungen und reagieren auf sie, bevor sie Ihre Daten kompromittieren oder Ausfallzeiten verursachen. Mit insgesamt sieben globalen Security Operations Centern (SOCs) ist Sophos MDR rund um die Uhr aktiv.

Kompatibilität mit anderen Anbietern

Sophos MDR kann Telemetriedaten von Endpoint-, Firewall-, Netzwerk-, Identitäts-, E-Mail-, Backup- Recovery und anderen Technologien von Drittanbietern integrieren.

Umfassende Incident Response

Wird eine akute Bedrohung erkannt, kann das Sophos MDR Operations Team per Remote-Zugriff umfangreiche Reaktionsmaßnahmen für Sie ergreifen, um den Angriff zu stören, einzudämmen und vollständig zu eliminieren. Mit einer Lizenz von MDR Complete erhalten Sie eine umfassende Reaktion auf Vorfälle ohne Obergrenze oder weitere Gebühren.

Reports und Datenaufbereitung

Mit Sophos Central erhalten Sie ein zentrales Dashboard für Echtzeit-Alerts, Reports und Verwaltung. Detaillierte Reports und Executive Dashboards bieten Einblick in Sicherheitsanalysen, Cyberbedrohungen und Ihren Sicherheitsstatus.

Endpoint- und Workload-Schutz inklusive

Sophos MDR-Analysten können Telemetrie von Ihrer bestehenden Endpoint-Protection-Lösung nutzen, um Bedrohungen zu erkennen und darauf zu reagieren, die auf Ihre Computer und Server abzielen. Alternativ können Sie zu Sophos Endpoint wechseln und erhalten ohne Aufpreis besseren Schutz.

Threat Hunting durch Experten

Proaktive Threat Hunts, die von hochqualifizierten Analysten durchgeführt werden, erkennen mehr Bedrohungen und beseitigen diese schneller als reine Security-Software. Unsere Experten können auch Telemetriedaten von Drittanbietern nutzen, um aktiv nach Bedrohungen zu suchen und Verhaltensweisen von Angreifern zu erkennen, die sich vor installierten Sicherheitsprogrammen verbergen konnten.

Direkter Telefon-Support

Ihr Team hat direkten Telefon-Zugriff auf unser Security Operations Center (SOC), um potenzielle Bedrohungen und aktive Vorfälle zu überprüfen. Das Sophos MDR Operations Team ist 24/7/365 erreichbar und wird von Support-Teams unterstützt, die weltweit auf 26 Standorte verteilt sind.

Dedizierter Ansprechpartner

Sie erhalten einen dedizierten Ansprechpartner, der mit Ihrem internen Team und externen Partnern zusammenarbeitet, sobald wir einen Vorfall bemerken. Dieser betreut Sie, bis der Vorfall behoben ist.

Ursachenanalyse

Wir geben Ihnen nicht nur proaktive Empfehlungen zur Verbesserung Ihres Sicherheitsstatus, sondern ermitteln auch anhand einer Ursachenanalyse, welche Probleme zu einem Vorfall geführt haben. Außerdem erhalten Sie eine ausführliche Anleitung zum Beseitigen von Sicherheits-Schwachstellen, damit diese in Zukunft nicht mehr ausgenutzt werden können.

Sophos Account Health Check

Wir überprüfen kontinuierlich die Einstellungen und Konfigurationen für von Sophos MDR verwaltete Endpoints und stellen sicher, dass diese mit optimaler Leistung arbeiten.

Eindämmung von Bedrohungen

Bei Kunden, die keine umfassende Reaktion auf Vorfälle durch Sophos MDR in Anspruch nehmen, kann das Sophos MDR Operations Team Maßnahmen zur Eindämmung von Bedrohungen ergreifen, um schädliche Aktivitäten zu stoppen und eine Ausbreitung zu verhindern. So werden interne Sicherheitsteams entlastet und schnelle Bereinigungsmaßnahmen ermöglicht.

Intelligence Briefings

Im Rahmen wöchentlicher Sophos MDR „ThreatBrief" Bulletins und monatlicher „ThreatCast"-Live-Webinare werden Kunden von Sophos MDR exklusiv über neueste Bedrohungsdaten und Security Best Practices informiert.

Breach Protection Warranty

Die Warranty ist in allen jährlichen (1–5 Jahre) und monatlichen Lizenzen von Sophos MDR Complete enthalten und deckt Kosten in Höhe von bis zu 1 Mio. US-Dollar für Reaktionsmaßnahmen ab. Die Warranty ist nicht in Stufen unterteilt und es gibt keine Mindestvertragslaufzeiten oder Anforderungen zum Kauf zusätzlicher Lizenzen.

Mit der Expertise von Sophos X-Ops

Sophos X-Ops verfügt über fundiertes Expertenwissen über das gesamte Angriffsumfeld. Unsere Expertenteams liefern Bedrohungsinformationen und entwickeln und implementieren kontinuierlich neue Erkennungsregeln für Sie, um Sie vor aktiven Angreifern zu schützen, die ihre Taktiken stetig weiterentwickeln.

Enthaltene Integrationen

Sicherheitsdaten aus den folgenden Quellen können zur Verwendung durch das Sophos MDR Operations Team ohne Aufpreis integriert werden. Telemetriequellen werden verwendet, um die Transparenz in Ihrer Umgebung zu erhöhen, neue Bedrohungserkennungen zu generieren, die Genauigkeit vorhandener Bedrohungserkennungen zu verbessern, Threat Hunts durchzuführen und zusätzliche Reaktionsmaßnahmen zu ermöglichen.

Sophos Endpoint

Blockieren Sie komplexe Bedrohungen und erkennen Sie schädliche Verhaltensweisen auf Ihren Endpoints.

Produkt im Preis von Sophos MDR enthalten

Workload Protection

Modernster Schutz und Bedrohungserkennung für Windows- und Linux-Server und -Container.

Produkt im Preis von Sophos MDR enthalten

Sophos Mobile

Schützen Sie Ihre iOS- und Android-Geräte und -Daten vor den neuesten Bedrohungen.

Produkt separat erhältlich; Integration ohne Aufpreis

Sophos Firewall

Überwachen und filtern Sie ein- und ausgehenden Netzwerkverkehr, um komplexe Bedrohungen zu stoppen, bevor sie Schaden anrichten können.

Produkt separat erhältlich; Xstream Protection Subscription erforderlich; ohne Aufpreis enthalten

Sophos Email

Schützen Sie Ihren Posteingang mit modernster KI vor Malware. Diese verhindert Phishing-Angriffe sowie gezielte Angriffe, bei denen eine falsche Identität vorgetäuscht wird.

Produkt separat erhältlich; Integration ohne Aufpreis

Sophos Cloud Optix

Verhindern Sie Cloud-Sicherheitsverstöße und gewinnen Sie Einblick in Ihre kritischen Cloud Services, einschließlich AWS, Azure und GCP.

Produkt separat erhältlich; Integration ohne Aufpreis

Sophos ZTNA

Ersetzen Sie Remote Access VPN durch „Least Privilege"-Zugriff, um Ihre Benutzer sicher mit Ihren Netzwerk-Anwendungen zu verbinden.

Produkt separat erhältlich; Integration ohne Aufpreis

Endpoint-Schutz anderer Anbieter

Integrationen umfassen:

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

Kompatibel mit anderen Endpoint-Protection-Lösungen mit dem Sophos „XDR Sensor"-Agent

Microsoft Security Tools

- Defender for Endpoint
- Defender for Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

90 Tage Datenspeicherung

Speichert Erkennungsdaten standardmäßig 90 Tage im Sophos Data Lake.

Microsoft Office 365 Management Activity

Liefern Informationen über Benutzer-, Admin-, System- und Richtlinienaktionen und -ereignisse, die über die Office 365-Verwaltungsaktivitäts-API erfasst werden.

Google Workspace

Erfasst Sicherheitstelemetrien von der Google Workspace Alert Center API.

Add-On-Integrationen

Durch den Erwerb sogenannter Integration Packs können Sicherheitsdaten aus den folgenden Drittanbieterquellen zur Verwendung durch das Sophos MDR Operations Team integriert werden. Telemetriequellen werden verwendet, um die Transparenz in Ihrer Umgebung zu erhöhen, neue Bedrohungserkennungen zu generieren, die Genauigkeit vorhandener Bedrohungserkennungen zu verbessern, Threat Hunts durchzuführen und zusätzliche Reaktionsmaßnahmen zu ermöglichen.

Sophos NDR

Überwachen Sie kontinuierlich die Aktivitäten in Ihrem Netzwerk und erkennen Sie verdächtige Aktionen zwischen Geräten, die sonst unbemerkt ablaufen.

Per SPAN Port Mirroring mit jedem Netzwerk kompatibel

Firewall

Integrationen umfassen:

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- Ubiquiti
- WatchGuard

Netzwerk

Integrationen umfassen:

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

Identity

Integrationen umfassen:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft-Integration ohne Aufpreis inbegriffen

E-Mail

Integrationen umfassen:

- Mimecast
- Proofpoint
- Trend Micro

Microsoft-365- und Google Workspace-Integrationen sind ohne Aufpreis enthalten

Cloud

Integrationen umfassen:

- Orca Security

AWS-, Azure- und GCP-Integrationen sind über das separat erhältliche Produkt „Cloud Optix“ verfügbar.

Sicherung und Wiederherstellung

Integrationen umfassen:

- Acronis
- Rubrik
- Veeam

1 Jahr Datenspeicherung

Erkennungsdaten werden 1 Jahr lang im Sophos Data Lake gespeichert

Add-on-Service

Sophos Managed Risk – basierend auf der Technologie von Tenable

Reduzieren Sie Cyber-Risiken mit proaktivem Vulnerability Management für Angriffsflächen als Service-Leistung. Sophos Managed Risk erkennt gefährliche Cybersecurity-Schwachstellen. So lassen sich Angriffe verhindern, bevor Ihr Geschäftsbetrieb gestört wird. Verfügbar als Add-on zu Sophos MDR.

Die Servicestufen von Sophos MDR

	Sophos MDR Essentials	Sophos MDR Complete
24/7 Threat Monitoring and Response durch Experten	✓	✓
Sophos Endpoint Protection und Sophos Workload Protection inklusive	✓	✓
Kompatibel mit Sicherheitsprodukten anderer Anbieter	✓	✓
Service-Einblicke und Reporting	✓	✓
Sophos Threat Intelligence Briefings	✓	✓
Sophos Account Health Check	✓	✓
Threat Hunting durch Experten	✓	✓
Eindämmung von Bedrohungen: die Angriffe werden gestoppt und eine Ausbreitung dadurch verhindert Bei Einsatz des vollständigen Sophos XDR Agent oder des Sophos „XDR Sensor" Agent	✓	✓
Direkter Telefon-Support bei akuten Vorfällen	✓	✓
Umfassende Reaktionsmaßnahmen bei Vorfällen: Bedrohungen werden vollständig eliminiert Vollständiger Sophos XDR Agent erforderlich	IR Service Add-on*	✓
Dedizierter Ansprechpartner	IR Service Add-on*	✓
Ursachenanalyse	IR Service Add-on*	✓
Breach Protection Warranty		✓
Microsoft- und Google-Workspace-Integrationen inklusive	✓	✓
Integrationen mit Firewall-, Netzwerk-, E-Mail-, Cloud-, Identity- und Backup-Lösungen anderer Anbieter	Add-on	Add-on
Sophos Network Detection and Response (NDR)	Add-on	Add-on
Sophos Managed Risk, powered by Tenable	Add-on	Add-on

* Eine jährliche Subscription für einen Sophos IR Services Retainer bietet Incident Response Services zum ermäßigten Preis. Greifen Sie im Ernstfall auf ein Team von Incident-Response-Experten zurück, die nach einem Sicherheitsvorfall schnell wieder den Geschäftsbetrieb wiederherstellen.

Guided Onboarding (optional)

Sophos MDR Guided Onboarding bietet Remote-Unterstützung beim Onboarding und ist gegen Aufpreis erhältlich. Der Service leistet praktischen Support für eine reibungslose und effiziente Bereitstellung, stellt sicher, dass Konfigurationen Best Practices entsprechen, und bietet Trainings, um den Wert Ihrer Investition in unseren MDR-Service zu maximieren. Sie erhalten einen dedizierten Ansprechpartner von Sophos Professional Services, der Sie während der ersten 90 Tage betreut und sicherstellt, dass Ihre Implementierung erfolgreich verläuft. Sophos MDR Guided Onboarding umfasst:

Tag 1 – Implementierung

- Projektstart
- Konfiguration von Sophos Central und Prüfen der Funktionen
- Aufbau und Test des Bereitstellungsprozesses
- Konfiguration von MDR-Integrationen
- Konfiguration von Sophos NDR-Sensor(en)
- Unternehmensweite Bereitstellung

Tag 30 – MDR-Training

- Schulung, in der Sie lernen, wie ein SOC zu denken und zu handeln
- Suche nach Indicators of Compromise
- Einsatz der MDR-Plattform für administrative Zwecke
- Erstellen von Abfragen für zukünftige Analysen

Tag 90 – Bewertung des Sicherheitsstatus

- Überprüfen der aktuellen Richtlinien auf Best-Practice-Empfehlungen
- Besprechen von ungenutzten Funktionen, die zusätzlichen Schutz bieten könnten
- Sicherheitsbewertung nach dem NIST Framework
- Abschlussbericht mit Empfehlungen zu Maßnahmen, die zur Erhöhung der Sicherheit getroffen werden sollten

Darum entscheiden sich Kunden für Sophos MDR

Sophos ist ein etablierter Marktführer im Bereich Managed Detection and Response und erhält regelmäßig unabhängige Auszeichnungen, die dies untermauern.

IDC

Leader im IDC MarketScape 2024 in der Kategorie „Worldwide Managed Detection and Response Services“

Gartner peerinsights™

Im „Voice of the Customer Report for Managed Detection and Response“ 2024 von Gartner® zur „Customers‘ Choice“ gekürt

G2 Leader

Im Winter-Report 2025 für Managed Detection and Response von G2 Grid® von Kunden zum „Overall Leader“ gekürt

FROST & SULLIVAN

Ein Leader im Frost Radar Report für Global Managed Detection and Response 2024

MITRE | ATT&CK® Evaluations

Ein „Strong Performer“ bei den MITRE ATT&CK Evaluations für Managed Services

Weitere Informationen unter

sophos.de/mdr

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2025-02-03 BRDE (PS)

SOPHOS