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 und E-Mail-Konten und ergreifen Reaktionsmaßnahmen.

Cybersecurity as a Service

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.

Leistungen von Sophos MDR

Sophos MDR nutzt umfassende XDR-Funktionalitäten (Extended 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 vorhandenen Cybersecurity-Tools

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

Sophos MDR ist kompatibel mit Sicherheitstelemetrie von Anbietern wie Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace etc. Die Telemetriedaten werden automatisch konsolidiert, korreliert und priorisiert, mithilfe des Sophos Adaptive Cybersecurity Ecosystem (ACE) und der Sophos X-Ops Threat Intelligence Unit.

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

SOPHOS

MDR – maßgeschneidert für Sie

Sophos MDR ist in verschiedenen Service-Leveln mit unterschiedlichen Reaktions-Optionen erhältlich – je nach Ihren individuellen Bedürfnissen: Unsere Experten können die Bedrohungserkennung und -bekämpfung komplett für Sie übernehmen, mit Ihrem Team zusammenarbeiten oder Sie nur benachrichtigen, wenn wir Bedrohungen erkennen. In allen Fällen können wir innerhalb von Minuten reagieren.

Wichtigste Funktionen

24/7 Threat Monitoring and Response

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

Kompatibilität mit anderen Anbietern

Sophos MDR kann Telemetriedaten von Endpoint-, Firewall-, Identitäts-, E-Mail- und anderen Sicherheitstechnologien von Drittanbietern als Teil von Sophos ACE integrieren.

Umfassende Reaktion auf Vorfälle

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.

Wöchentliche und monatliche Reports

Mit Sophos Central erhalten Sie ein zentrales Dashboard für Echtzeit-Warnmeldungen, Reports und Verwaltung. Wöchentliche und monatliche Reports bieten Einblick in Sicherheitsanalysen, Cyberbedrohungen und Ihren Sicherheitsstatus.

Sophos Adaptive Cybersecurity Ecosystem

Sophos ACE verhindert automatisch schädliche Aktivitäten und ermöglicht uns, nach schwachen Bedrohungssignalen zu suchen, bei denen zum Erkennen, Analysieren und Beseitigen der Gefahr ein manuelles Eingreifen nötig ist.

Threat Hunting aus Expertenhand

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 XDR 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 Aktionen zu stoppen und eine Ausbreitung zu verhindern. So werden interne Sicherheitsteams entlastet und schnelle Bereinigungsmaßnahmen ermöglicht.

Intelligence Briefings: „Sophos MDR ThreatCast“

Der vom Sophos MDR Operations Team durchgeführte „Sophos MDR ThreatCast“ ist ein monatliches Briefing, bei dem Kunden von Sophos MDR exklusiv über neueste Bedrohungsdaten und Security Best Practices informiert werden.

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.

Service-Level

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24/7 Threat Monitoring and Response durch Experten	✓	✓	✓
Kompatibel mit Sicherheitsprodukten anderer Anbieter	✓	✓	✓
Wöchentliche und monatliche Reports	✓	✓	✓
Monatliches Intelligence Briefing: „Sophos MDR ThreatCast“	✓	✓	✓
Sophos Account Health Check		✓	✓
Threat Hunting durch Experten		✓	✓
Eindämmung von Bedrohungen: Angriffe werden gestört, um eine Ausbreitung zu verhindern Vollständiger Sophos XDR Agent (Schutz, Erkennung und Reaktion) oder Sophos XDR Sensor (Erkennung und Reaktion) erforderlich		✓	✓
Direkter Telefon-Support bei akuten Vorfällen		✓	✓
Umfassende Reaktionsmaßnahmen bei Vorfällen: Bedrohungen werden vollständig eliminiert Vollständiger Sophos XDR Agent (Schutz, Erkennung und Reaktion) erforderlich			✓
Ursachenanalyse			✓
Dedizierter Ansprechpartner			✓
Breach Protection Warranty Übernimmt Kosten für Reaktionsmaßnahmen in Höhe von bis zu 1 Mio. US-Dollar			✓

In Sophos MDR 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 XDR

Kombiniert als einzige XDR-Plattform native Endpoint-, Server-, Firewall-, Cloud-, E-Mail-, Mobile- und Microsoft-Integrationen.

Im Preis für Sophos MDR und Sophos MDR Complete enthalten

Sophos Firewall

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

Produkt separat erhältlich; ohne Aufpreis integriert

Microsoft-Graph-Sicherheit

- Microsoft Defender für Endpunkt
- Microsoft Defender für Cloud
- Microsoft Defender für Cloud-Apps
- Microsoft Defender für Identität
- Identity Protection (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Security and Compliance Center
- Azure Information Protection

Sophos Endpoint

Blockieren Sie komplexe Bedrohungen und erkennen Sie schädliche Verhaltensweisen – darunter Angreifer, die legitime Benutzer imitieren.

Im Preis für Sophos MDR und Sophos MDR Complete enthalten

Sophos Email

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

Produkt separat erhältlich; ohne Aufpreis integriert

Office 365 Verwaltungsaktivität

Liefert Informationen über Benutzer-, Admin-, System- und Richtlinienaktionen und -ereignisse aus Office-365- und Azure-Active-Directory-Protokollen

Sophos Cloud

Verhindern Sie Cloud-Sicherheitsverstöße und gewinnen Sie Transparenz über Ihre kritischen Cloud Services, einschließlich AWS, Azure und Google Cloud Platform.

Produkt separat erhältlich; ohne Aufpreis integriert

90 Tage Datenspeicherung

Speichert Daten von allen Sophos-Produkten und Drittanbieter-Produkten (nicht Sophos) im Sophos Data Lake.

Endpoint-Schutz von Drittanbietern

Kompatibel mit ...

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

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 Network Detection and Response

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

Kompatibel mit ...

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

Identität

Kompatibel mit ...

- Okta
- Duo
- ManageEngine

Public Cloud

Kompatibel mit ...

- AWS Security Hub
- AWS CloudTrail
- Orca Security
- Google Cloud Platform Security

E-Mail

Kompatibel mit ...

- Proofpoint
- Mimecast

Netzwerk

Kompatibel mit ...

- Darktrace
- Tinkst Canary
- Skyhigh Security

1 Jahr Datenspeicherung

Sophos MDR Guided Onboarding

Unser Sophos MDR Guided Onboarding ist gegen Aufpreis erhältlich und bietet Remote-Unterstützung beim Onboarding. 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 – XDR-Training

- Schulung, in der Sie lernen, wie ein SOC zu denken und zu handeln
- Suche nach Indicators of Compromise
- Einsatz der XDR-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

Weitere Information unter
sophos.de/mdr

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

23-01-24 DS-DE (PC)

SOPHOS