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 sie 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 reine Sicherheitstools**
  Unsere Tools blockieren automatisch 99,98 % der Bedrohungen. Dadurch können sich unsere Analysten auf die gezielte Suche nach besonders versierten Angreifern konzentrieren, die nur von entsprechend geschulten Experten enttarnt und gestoppt werden können.
- **Reagiert schnell, damit Bedrohungen nicht Ihren Unternehmensbetrieb 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 bestehenden 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.

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			✓

Kostenfreie Integrationen

Sicherheitsdaten aus den folgenden Quellen können zur Verwendung durch das Sophos MDR Operations Team kostenlos 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.

Sophos Firewall

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

Microsoft-Graph-Sicherheit

- Microsoft Defender für Endpunkt
- Microsoft Defender für Cloud
- Microsoft Defender für Identität
- Azure Active Directory
- Microsoft Defender für Cloud-Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365

Sophos Endpoint

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

Sophos Network Detection and Response

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

Endpoint-Schutz von Drittanbietern

Kompatibel mit ...

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

Sophos Cloud

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

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.

90 Tage Datenspeicherung

Die Produkte Sophos XDR und Sophos Endpoint Protection sind im Sophos MDR-Service enthalten.
Die Produkte Sophos Firewall, Sophos Cloud, Sophos Email und Sophos NDR müssen vor der Integration in den Sophos MDR-Service erworben und bereitgestellt werden.

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 und die Genauigkeit vorhandener Bedrohungserkennungen zu verbessern, Threat Hunts durchzuführen und zusätzliche Reaktionsmaßnahmen zu ermöglichen.

Firewall

Kompatibel mit ...

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

Cloud

Kompatibel mit ...

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

Identität

Kompatibel mit ...

- Okta
- Duo

Netzwerk-Security

Kompatibel mit ...

- Darktrace
- Forcepoint
- McAfee (Web Gateway)

E-Mail

Kompatibel mit ...

- Proofpoint
- Mimecast

1 Jahr Datenspeicherung

Onboarding Plus Package für Sophos MDR

Unser Onboarding Plus Package ist ein remote geführter Onboarding-Service für Kunden von Sophos MDR. Sie erhalten einen dedizierten Ansprechpartner aus dem „Sophos Professional Services"-Team. Ihr Ansprechpartner unterstützt bei Onboarding und Planung, bei Bereitstellung und Training und führt einen Health Check durch, um sicherzustellen, dass Sie den größten Nutzen aus unseren Best Practices ziehen. Onboarding Plus umfasst:

Tag 1 – Implementierung – Planung und Durchführung:

- Projektstart
- Konfiguration von Sophos Central
- Überprüfen der Funktionen von Sophos Central
- Aufbau und Test des Bereitstellungsprozesses
- Unternehmensweite Bereitstellung von Sophos Central

Tag 30 – XDR-Training

- Schulung, in der Sie lernen, wie ein SOC zu denken und zu handeln
- Suche nach IOCs
- Erstellen von Abfragen für zukünftige Analysen

Tag 90 – XDR-Training

- Überprüfen Ihrer aktuellen Sicherheitsrichtlinien und ggf. Aktualisierung
- Bestimmen, mit welchen Funktionen Ihr Cyberschutz ggf. weiter verbessert werden kann
- Erhalt schriftlicher Dokumentation mit Empfehlungen von unserem Health Check

Weitere Informationen unter
sophos.de/mdr

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

22-10-17 DS-DE (DD)

SOPHOS