



netgo Partner Feature

Sophos

Cybersecurity 24/7 dank Managed Detection and Response von Sophos



Sophos MDR Managed Detection & Response

24/7 Fully-Managed Service aus
Expertenhand

Cybersecurity as a Service mit netgo und Sophos

Cybersecurity ohne Managed Detection & Response? Nicht mehr denkbar. MDR-Dienste bieten eine kontinuierliche Überwachung rund um die Uhr, wodurch Bedrohungen jederzeit erkannt und bekämpft werden können.

Dank hochqualifizierter Sicherheitsexperten sind MDR-Services besonders interessant für Unternehmen ohne eigene interne Ressourcen in diesem Bereich. Durch schnelle Reaktionszeiten minimieren MDR-Dienste die Zeit, die ein Angreifer im Netzwerk verbringen kann, und verringern so den Schaden.

Neben der reaktiven Bedrohungsabwehr verfolgt MDR auch proaktive Ansätze, indem Schwachstellen und potentielle Bedrohungen im Netzwerk identifiziert werden, bevor sie ausgenutzt werden können. Somit gewährleistet MDR eine umfassende Sicherheitslösung, die kontinuierliche Überwachung, spezialisiertes Fachwissen und schnelle Reaktionszeiten kombiniert, um Cyberbedrohungen effektiv zu bekämpfen und die Sicherheit der Unternehmensinfrastruktur zu stärken.

Sophos MDR Managed Detection & Response setzt hier an und bietet Unternehmen moderne, professionelle Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen als Fully-Managed-Service. Der Service bietet rund um die Uhr Überwachung, Bedrohungserkennung und Reaktion durch das Sophos-Expertenteam.

Darüber hinaus ist das MDR kompatibel mit Cybersecurity-Tools anderer Hersteller und umfasst eine proaktive Bedrohungssuche durch Experten. Somit können Bedrohungen erfolgreich gestoppt und eingedämmt werden. Sophos MDR nutzt umfassende XDR-Funktionalitäten (Extended Detection and Response), die eine weitreichende Analyse und Reporting erst ermöglichen.

Die steigende Anzahl von Cyber-Angriffen erhöht nicht nur den Bedarf an Prävention, sondern erfordert auch eine effektive Abwehr von Angriffen innerhalb von Organisationen. Hierfür bedarf es einer Vielzahl interner Fachkräfte und Tools – nicht selten mangelt es in Unternehmen jedoch genau an dieser Stelle. Deshalb ist ein 24/7 verfügbares Managed Detection and Response (MDR) unabdingbar.

Das Sophos MDR schützt Sie rund um die Uhr gegen hochkomplexe Bedrohungen als Fully-Managed-Service. Das Expertenteam spürt dabei proaktiv potentielle Bedrohungen und Vorfälle auf, kümmert sich um Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen und gibt konkrete Ratschläge für die Ursachenbekämpfung.

Ihre Vorteile von Sophos MDR Managed

Der große Vorteil für Unternehmen, die sich für Sophos MDR entscheiden: Es werden keine internen IT-Ressourcen benötigt, um Angriffe zu verhindern und es besteht die Gewissheit, dass hochqualifizierte Experten sich rund um die Uhr mit dem Schutz vor Cyberangriffen befassen.

- **99,98 % der Bedrohungen werden automatisch blockiert** - die Analysten fokussieren sich auf besonders komplexe Angriffe, die nur ein geschultes Auge erkennen kann.
- **Schnelle Reaktion**, damit die Betriebsabläufe nicht gestört werden.
- **Ursachenermittlung** künftiger Bedrohungen und Empfehlungen zur Risiko-Minimierung

Die wichtigsten Funktionen von Sophos MDR Managed Detection & Response

Sophos MDR wird in verschiedenen Optionen angeboten und kann auf Ihre individuellen Bedürfnisse zugeschnitten werden. Lassen Sie sich gerne zu den unterschiedlichen Service-Levels beraten. Grundsätzlich werden die folgenden Funktionen angeboten:

- **24/7 Threat Monitoring and Response:** Rund um die Uhr aktiv mit sieben globalen Security Operations Centern (SOCs) -, Identitäts-, E-Mail-, Backup- Recovery und anderen Technologien von Drittanbietern
- **Kompatibilität mit anderen Anbietern:** Integration von Endpoint-, Firewall-, Netzwerk-, Identitäts-, E-Mail-, Backup- Recovery und anderen Technologien von Drittanbietern
- **Umfassende Reaktion auf Vorfälle:** Direkte Reaktionsmaßnahmen per Remote-Zugriff, um Angriffe zu stören, einzudämmen und vollständig zu eliminieren
- **Wöchentliche und monatliche Reports:** Zentrales Dashboard für Echtzeit-Warnmeldungen, Reports und Verwaltung
- **Sophos Adaptive Cybersecurity Ecosystem:** Automatisches Verhindern schädlicher Aktivitäten
- **Threat Hunting aus Expertenhand:** Proaktive Bedrohungserkennung und -beseitigung durch hochqualifizierte Analysten
- **Direkter Telefon-Support:** 24/7/365 Erreichbarkeit und direkter Telefon-Zugriff auf Security Operations Center
- **Dedizierter Ansprechpartner:** Betreuung, bis der Vorfall behoben ist
- **Ursachenanalyse:** Ermittlung der Probleme, die zum Vorfall geführt haben
- **Sophos Account Health Check:** Kontinuierliche Überprüfung der Einstellungen und Konfigurationen für von Sophos MDR verwaltete Endpoints
- **Eindämmung von Bedrohungen:** Maßnahmen zur Eindämmung von Bedrohungen für Kunden, die keine Reaktion auf Vorfälle durch Sophos MDR nutzen
- **Monatliche Intelligence Briefings:** „**Sophos MDR ThreatCast**“: Einblick in aktuelle Bedrohungsdaten und Security Best Practices
- **Breach Protection Warranty:** Die Warranty wird automatisch auf alle Neukäufe und Renewals von jährlichen Sophos MDR Complete Subscriptions gewährt, außerdem beim Erwerb von Integrationspaketen für Sophos MDR Complete. Mit diesen Paketen können Sicherheitsexperten die Erkennung und Reaktion durch die Integration von Daten der Sicherheitslösungen von Drittanbietern beschleunigen. Die Warranty deckt Geräte, Endpoints und Server unter Windows und macOS ab und ist in allen Ländern verfügbar, in denen wir tätig sind.

Integration in bestehende Systeme

Sicherheitsdaten aus folgenden Quellen können ohne Aufpreis integriert werden:

- Sophos Endpoint, Workload Protection, Sophos Mobile, Sophos Firewall, Sophos Email, Sophos Cloud und Sophos ZTNA
- Endpoint-Schutz von Drittanbietern
 - Microsoft
 - CrowdStrike
 - SentinelOne
 - Trend Micro
 - BlackBerry (Cylance)
 - Broadcom (Symantec)
- Microsoft Security Tools
 - Defender for Endpoint
 - Defender for Cloud
 - Defender for Cloud Apps
 - Defender for Identity
 - Microsoft Entra ID
 - Azure Sentinel
 - Office 365 Security and Compliance Center

Sicherheitsdaten aus folgenden Drittanbieterquellen können durch den Erwerb von Integration Packs integriert werden:

- Sophos NDR
- Firewall: Kompatibel mit Check Point, Cisco Firepower, Cisco Meraki, Fortinet, Palo Alto Networks, SonicWall, WatchGuard
- Netzwerk: Kompatibel mit Cisco Umbrella, Darktrace, Secutec, Skyhigh Security, Thinkst Canary
- Identity: Kompatibel mit Auth0, Duo, ManageEngine, Okta
- E-Mail: Kompatibel mit Proofpoint, Mimecast
- Public Cloud: Kompatibel mit AWS Security Hub, AWS Cloud Trail, Orca Security
- Sicherung und Wiederherstellung: Kompatibel mit Veeam

Sophos MDR Managed Detection & Response: Ihr All-Inclusive-Service für ein bestmögliches Ergebnis in der IT-Sicherheit.

- ✓ Profitieren Sie von einer proaktiven Bedrohungssuche
- ✓ Reagieren Sie schneller auf Bedrohungen dank 24/7 Erkennung und Reaktion durch Analysten
- ✓ Erkennen Sie mehr Bedrohungen als mit gängigen Security-Tools

get in touch

www.netgo.de

in f @ X y <