Sophos MDR for Microsoft Defender

Threat Response aus Expertenhand für Microsoft-Umgebungen

Sophos Managed Detection and Response (MDR) for Microsoft Defender erweitert Ihr Team um hochqualifizierte Experten, die Microsoft-Sicherheitswarnmeldungen 24/7 für Sie überwachen, analysieren und darauf reagieren.

Schöpfen Sie Ihre Investition in Microsoft Security voll aus

Viele Unternehmen und Organisationen haben in die Microsoft Security Suite investiert. Sie verfügen jedoch nicht über ausreichend interne Expertise, um die Vielzahl der Microsoft-Produkttechnologien effektiv zu nutzen oder täglich Hunderte von Sicherheitswarnmeldungen zu bearbeiten:

- Der weltweite Mangel an Cybersecurity-Experten hat 3,4 Mio.[1] erreicht.
- 71 % der Security-Teams finden es angesichts der Datenflut von ihren Sicherheitsprogrammen schwierig, Sicherheitswarnmeldungen angemessen zu priorisieren[2].
- Unternehmen und Organisationen mit einem dedizierten Security Operations Team brauchen im Mittel 16 Stunden, um auf Bedrohungen zu reagieren, sodass Angreifer viel Zeit für ihre Aktivitäten im Netzwerk haben[3].

Sophos MDR for Microsoft Defender bietet die leistungsstärksten Threat-Detection-, Threat-Hunting- und Threat-Response-Funktionen für Microsoft-Umgebungen. Unsere Analysten überwachen, untersuchen und reagieren 24/7 auf Microsoft-Sicherheitswarnmeldungen. Dabei ergreifen sie sofortige Reaktionsmaßnahmen und stoppen bestätigte Bedrohungen in durchschnittlich nur 38 Minuten – 96 % schneller als der Branchenstandard.

Erkennen und stoppen Sie Bedrohungen jenseits von Microsoft Defender

Mit Sophos MDR for Microsoft Defender erkennen und analysieren unsere Microsoft-Sicherheitsexperten Bedrohungen und reagieren auf diese mithilfe von Sicherheitsdaten von den folgenden Microsoft-Produkten:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- 0365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity

Darüber hinaus bilden unsere proprietären Erkennungen, erstklassigen Bedrohungsinformationen und Threat Hunting durch ein Expertenteam zusätzliche Schutzebenen, sodass mehr Bedrohungen erkannt und gestoppt werden können als mit Microsoft Security-Tools allein.

Für noch mehr Transparenz und Schutz können Unternehmen und Organisationen auch Sicherheitstools und Telemetriequellen einbeziehen, die nicht von Microsoft stammen – von Sophos-Lösungen oder anderen Anbietern wie Palo Alto Networks, Fortinet, Check Point, AWS, Google, Okta und Darktrace.

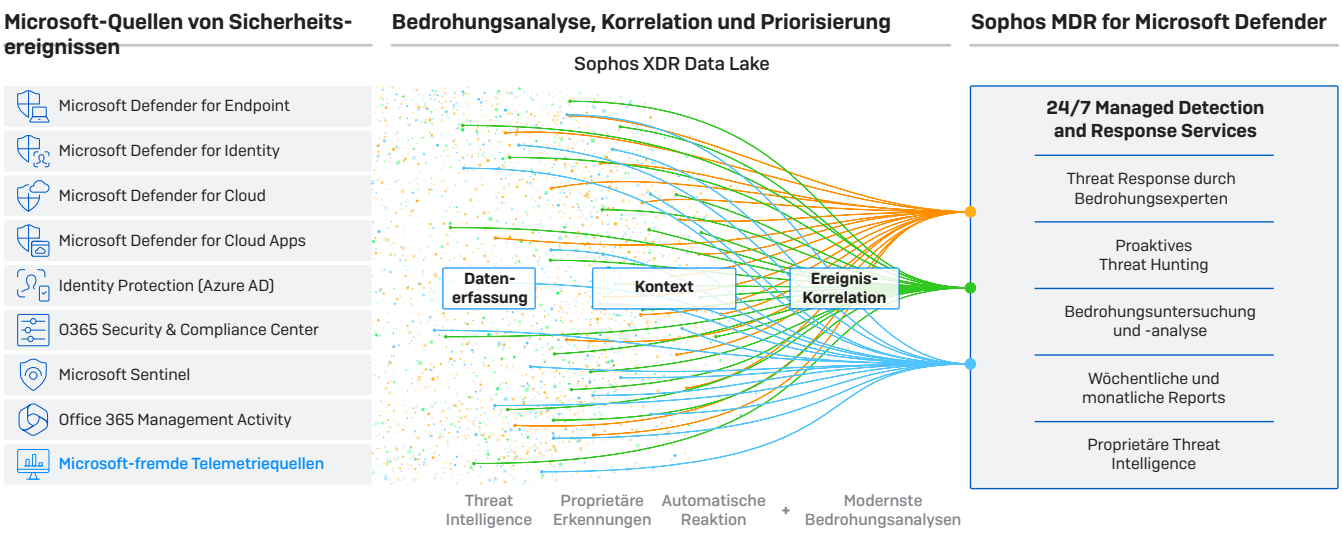
Vorteile auf einen Blick

- Analysten von Sophos MDR überwachen und untersuchen Microsoft-Sicherheitswarnmeldungen 24/7 und reagieren darauf, indem sie sofortige Maßnahmen ergreifen, um bestätigte Bedrohungen zu stoppen
- Die Servicefunktionen gehen über Microsoft Defender for Endpoint und Microsoft Sentinel hinaus und decken die gesamte Microsoft-Security-Plattform ab
- Wird eine akute Bedrohung erkannt, kann das Sophos MDR Operations Team umfangreiche Threat-Response-Maßnahmen für Sie ergreifen
- Proprietäre Sophos-Erkennungen, Bedrohungsinformationen und Threat Hunting durch ein Expertenteam bilden zusätzliche Schutzebenen
- Integrieren Sie Tools und Telemetriequellen, die nicht von Microsoft stammen, um Angriffe auf Ihr Netzwerk, Ihre Benutzer und Ihre Kunden zu stoppen

1 2022 Cybersecurity Workforce Study, (ISC)2
2 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen, Sophos
3 Gartner Cybersecurity Business Value Benchmark Database, 2022

SOPHOS

Sophos MDR for Microsoft Defender: Wichtigste Funktionen



24/7 Threat Monitoring

Unsere Microsoft-Security-Experten erkennen und stoppen Bedrohungen, bevor sie Ihre Daten gefährden oder Betriebsunterbrechungen verursachen können. Mit insgesamt sechs globalen Security Operations Centern (SOCs) ist Sophos rund um die Uhr aktiv.

Threat Response durch Bedrohungsexperten

Das Sophos MDR-Team kann umfangreiche Threat-Response-Maßnahmen für Sie ergreifen, um Angreifer zu stören, einzudämmen und zu eliminieren. u. a.:

- Isolieren von Hosts mit Sophos Central
- Anwenden hostbasierter Firewall-IP-Blöcke
- Beenden von Prozessen
- Erzwungenes Abmelden von Benutzersitzungen
- Deaktivieren von Benutzerkonten
- Entfernen schädlicher Artefakte
- Hinzufügen schädlicher Hashes zu blockierten Elementen in Sophos Central

Proaktives Threat Hunting durch Bedrohungsexperten

Im Rahmen von proaktiven Threat Hunts durch hochqualifizierte Analysten werden Bedrohungen aufgedeckt und schnell beseitigt. Außerdem werden ggf. Verhaltensweisen von Angreifern erkannt, die sich vor installierten Sicherheitsprogrammen verbergen konnten.

Kompatibel mit Microsoft-fremden Tools

Um Angriffe in Ihrer gesamten Umgebung zu erkennen und zu stoppen, kann Sophos MDR auch auf Sicherheitstools und Telemetriequellen anderer Anbieter als Microsoft zurückgreifen.

Wöchentliche und monatliche Reports

Echtzeit-Warnmeldungen, Reporting und Verwaltungsoptionen stehen in Sophos Central zur Verfügung. Gleichzeitig bieten wöchentliche und monatliche Reports Einblick in Sicherheitsanalysen, Cyberbedrohungen und den Sicherheitsstatus Ihres Unternehmens oder Ihrer Organisation.

Monatliche Threat Intelligence Briefings

Der vom Sophos MDR-Team durchgeführte „Sophos MDR ThreatCast" ist ein monatliches Briefing, bei dem Sie über neueste Bedrohungsdaten und Security Best Practices informiert werden.

Proprietäre Erkennungen

Die in die Sophos-Plattform integrierten proprietären Erkennungen, modernen Bedrohungsanalysen und erstklassigen Bedrohungsinformationen bilden zusätzliche Schutzebenen, sodass mehr Bedrohungen erkannt werden können als mit Microsoft Security-Tools allein.

Weitere Informationen unter:

sophos.de/microsoft-defender

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

23-07-10 DS-DE (DD)

SOPHOS