



Sophos bringt Managed Detection and Response (MDR) für Microsoft Defender auf den Markt

Sophos MDR ist zusätzliche, wichtige Sicherheitsebene in Microsoft-Umgebungen

Wiesbaden, 18. Juli 2022 – Sophos hat seine Lösung [Sophos Managed Detection and Response \(MDR\) für Microsoft Defender](#) auf den Markt gebracht. Der vollständig verwaltete Service bietet Unternehmen, die Microsoft Security einsetzen, branchenweit die zuverlässigsten Threat-Response-Funktionen. Sophos MDR für Microsoft Defender ergänzt die Microsoft-Security-Suite mit Endpoint-, SIEM-, Identity-, Cloud- und anderen Lösungen um eine entscheidende Schutzebene, die rund um die Uhr vor Datenschutzverletzungen, [Ransomware](#) und anderen [Active-Adversary-Cyberangriffen](#) schützt.

„Standard-Sicherheitstechnologien allein reichen nicht aus, um ambitionierte Angreifer daran zu hindern, einen Weg für ihre Machenschaften zu finden, wie die Fälle unseres [Incident-Response-Teams](#) zeigen. Angreifer sind extrem hartnäckig, und Unternehmen benötigen eine menschliche Sicherheitsebene. Damit haben Unternehmen die Möglichkeit, Bedrohungen zu entdecken und das Verhalten von Angreifern, die versuchen, Sicherheits-Tools zu umgehen, zu erkennen und zu reagieren, um Angriffe schnell und präzise zu stoppen“, sagt Raja Patel, Senior Vice President of Products and Managed Services bei Sophos. „Anstatt Unternehmen zu zwingen, bestehende Technologien abzuschaffen und zu ersetzen, unterstützen wir sie mit dem, was, wie und wo sie es brauchen – unabhängig davon, welche Sicherheitslösungen sie bereits verwenden. Für Channel-Partner, die Microsoft Security-Angebote anbieten, ergeben sich enorme Möglichkeiten. Sie können sicherstellen, dass Kunden vollständig geschützt sind und die Investitionen in bestehende Implementierungen maximieren.“

Sophos MDR für Microsoft Defender integriert Telemetrie von einer Vielzahl von Microsoft Security-Tools. Im Gegensatz zu anderen MDR-Angeboten, die sich auf Microsoft Defender for Endpoint oder Microsoft Sentinel beschränken und nur minimale Threat-Response-Funktionen bieten, stärkt Sophos MDR die gesamte Microsoft Security Suite, einschließlich:

- Microsoft Defender für Endpoint
- Microsoft Defender für Identity
- Microsoft Defender für die Cloud
- Microsoft Defender für Cloud-Anwendungen
- Identitätsschutz (Azure Active Directory)
- Office 365 Sicherheits- und Compliance-Center
- Microsoft Sentinel
- Office 365 Verwaltungsaktivität

Die Telemetriedaten aus diesen Quellen werden automatisch konsolidiert, korreliert und mit den Erkenntnissen aus dem [Sophos Adaptive Cybersecurity Ecosystem](#) und der [Sophos X-Ops](#) Threat Intelligence Unit, die aus mehr als 500 Sicherheitsanalysten, Threat Hunttern, und anderen Spezialisten bei Sophos weltweit besteht, priorisiert. Dadurch ist das Sophos MDR Operations Team in der Lage, mehr Bedrohungen zu identifizieren und zu stoppen, als es Microsoft Security Tools oder andere Sicherheitstechnologien alleine könnten.

„Recherchen von IDC bestätigen, dass 65 Prozent der Unternehmen in den letzten zwölf Monaten einen signifikanten Ransomware-Vorfall hatten, trotz erheblicher Investitionen in Cybersicherheits-Tools. Grund dafür ist, dass oft nicht ein technologisches, sondern ein

menschliches Problem besteht. Die meisten IT- und Sicherheitsteams sind in der Regel überlastet, unterbesetzt und mit zu wenig Ressourcen ausgestattet. Sie sind nicht in der Lage, die tägliche Flut von Warnungen und Problemen zu sortieren und zu bearbeiten, um den gewünschten Schutz zu erhalten, den sie sich von ihren aktuellen Tool-Investitionen versprochen haben“, sagt Frank Dickson, Group Vice President für den Forschungsbereich Security and Trust bei IDC. „Unternehmen, die den Microsoft Security Stack einsetzen, können mit Sophos MDR die Ergebnisse erzielen, die sie sich von ihren bestehenden Cybersecurity-Investitionen erhoffen.“

„Unser Leitprinzip ist es, Kunden die bestmögliche Sicherheit zu liefern. Fortschritte bei Technologien wie Extended Detection and Response (XDR) und generative KI sorgen für mehr Effizienz im Sicherheitsbetrieb. Aber das menschliche Element bleibt eine entscheidende Komponente, um fortschrittliche Bedrohungen zu stoppen“, sagt Kieron Newsham, Chief Technologist - Cyber Security bei [Softcat](#). „Wir sind sehr zufrieden damit, wie Sophos MDR unseren Kunden hilft, den zunehmenden Fachkräftemangel und die wachsende Qualifikationslücke zu überwinden, um die bestmöglichen Cybersecurity-Ergebnisse zu erzielen, unabhängig von der Größe, Struktur oder den bisherigen Technologieinvestitionen des Kunden.“

Sophos MDR ist mit mehr als 17.000 Kunden aller Größen und Branchen das am weitesten verbreitete MDR-Angebot sowie die am besten und am häufigsten bewertete und getestete MDR-Lösung bei [Gartner Peer Insights](#) und [G2](#). Es ist der einzige MDR-Service, der sowohl für bestehende Sicherheitslösungen von Drittanbietern als auch für das Sophos Angebot bereitgestellt werden kann. Neben Microsoft können Unternehmen über den [Sophos Marketplace](#) auch Telemetriequellen von weiteren Anbietern integrieren, darunter Amazon Web Services (AWS), Google, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Okta, Darktrace und viele andere.

Verfügbarkeit

Sophos MDR für Microsoft Defender ist ab sofort für alle Sophos MDR-Essentials-Kunden verfügbar, die Sicherheitstechnologien der Microsoft 365 E3- und E5-Lizenzen verwenden. Das anpassbare Angebot mit verschiedenen Threat-Response-Optionen ist über den globalen Sophos Channel von Reseller-[Partnern](#) und [Managed Service Providern \(MSPs\)](#) erhältlich.

Über Sophos

Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.

Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen. Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.

Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.

Weitere Informationen unter: www.sophos.de

Pressekontakt:

Sophos

Jörg Schindler, PR-Manager Central & Eastern Europe

joerg.schindler@sophos.com, +49-721-25516-263

TC Communications

Arno Lücht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

Ariane Wendt +49-172-4536839

sophos@tc-communications.de