



Sophos MDR startet mit umfangreichem Service-Portfolio

Sophos Marketplace ermöglicht die Integration von Fremdhersteller-Technologien sowohl für sein Managed Detection & Response Programm als auch andere Lösungen aus dem Sophos Cybersecurity-Ökosystem

Sophos Breach Protection Warranty schützt Kunden bis zu einer Summe von 1 Millionen Dollar

Wiesbaden 30. November 2022 – Nach der Vorankündigung zur it-sa 2022 gibt Sophos heute die allgemeine Verfügbarkeit von Sophos Managed Detection and Response (MDR) mit neuen, branchenweit einzigartigen Funktionen zur Erkennung und Reaktion auf Bedrohungen bekannt. Sophos ist der erste Endpoint-Security-Anbieter, der herstellerunabhängige Telemetriedaten von Sicherheitstechnologien anderer Unternehmen in sein MDR-Angebot integriert und damit eine beispiellose Transparenz und Erkennung in unterschiedlichen Betriebsumgebungen ermöglicht. Im Zusammenhang mit den neuen MDR-Services stellt Sophos zudem seinen neuen Sophos Marketplace und die Sophos Breach Protection Warranty vor.

Der Bedarf an MDR-Diensten und spezialisierten Verteidigern war noch nie so groß wie heute, wie die neue Studie [„LockBit 3.0 'Black' Attacks and Leaks Reveal Wormable Capabilities and Tooling“](#) von [Sophos X-Ops](#) zeigt. Die Untersuchung analysiert Taktiken, Techniken und Prozeduren (TTPs), die von [LockBit](#), einer der derzeit am stärksten verbreiteten Ransomware-Banden verwendet werden. Weiterhin beleuchtet die Studie, wie die jüngste Version der Ransomware wurmfähige Funktionen hinzufügt und legitime Pentesting-Tools verwendet, um die Erkennung zu umgehen.

In einem zweiten Bericht mit dem Titel [„Detection Tools and Human Analysis Lead to a Security Non-Event“](#) beschreibt Sophos X-Ops einen realen Einsatz von Sophos MDR, bei dem es um den Diebstahl von Zugangsdaten geht – eine weitere Technik, die es Angreifern ermöglicht, sich als legitime Benutzer auszugeben. In diesem Fall kombinierte das Sophos MDR-Team seine Threat Hunting Intelligence mit Informationen aus der Security Appliance eines Drittanbieters, um einen Angriff zu vereiteln.

„Die einzige Möglichkeit, die immer versteckter agierenden Angreifer zuverlässig auszuschalten, ist eine 24/7-Überwachung, die auf Signale aus einer Vielzahl von Ereignisquellen aufbaut und verwertbare Bedrohungsdaten zum Verhalten von Angreifern in Echtzeit einsetzt“, so Joe Levy, Chief Technology and Product Officer bei Sophos. „Unternehmen haben es schwer, mit gut finanzierten Angreifern Schritt zu halten, die ihre Fähigkeit zur Umgehung von Verteidigungstechnologien ständig weiterentwickeln und industrialisieren. Sophos MDR kann dieser Entwicklung Einhalt gebieten, bevor sie zu einer Datenverletzung, Ransomware oder einer anderen Art von kostspieliger Kompromittierung führt. Leider stellt Ransomware nach wie vor eine der größten Bedrohungen für Unternehmen dar, wie der Sophos [2023 Threat Report](#) zeigt. Mit unserer MDR-Offensive setzen wir neue Maßstäbe dafür, wie Cybersecurity as a Service bereitgestellt werden kann, um eine bessere und schnellere Erkennung und Reaktion zu realisieren.“

Branchenführende Managed Detection & Response inkl. neuem Sophos Marketplace

Sophos ist der erste Anbieter von Endpoint Security, der MDR sowohl für sein eigenes Produktportfolio als auch für die bestehenden Sicherheitsimplementierungen von Endanwendern anbietet. Zur Unterstützung des Channels hat Sophos den [Sophos Marketplace](#) eingeführt. Dieses offene Ökosystem umfasst mehr als 75 Technologie-Integrationen, darunter Amazon Web Services (AWS), Check Point, CrowdStrike, Darktrace, Fortinet, Google, Microsoft, Okta, Palo Alto Networks, Rapid7 und viele andere. Dank des erweiterten Einblicks in diese Integrationen und unterschiedlichen Betriebsumgebungen können die Experten von Sophos Angriffe schneller und präziser erkennen und abwehren, unabhängig von den vorhandenen Sicherheitslösungen der Kunden.

Zusätzlich zu Sophos MDR bietet der Sophos Marketplace Drittanbieter-Integrationen für das Sophos Portfolio an Services, Produkten und Technologien. Telemetriedaten werden automatisch konsolidiert, korreliert und mit den Erkenntnissen aus dem [Sophos Adaptive Cybersecurity Ecosystem](#) und der Sophos X-Ops Threat Intelligence Unit priorisiert.

Erweiterte Sicherheit für Kunden

Sophos unterstützt seine MDR-Kunden mit der neuen [Sophos Breach Protection Warranty](#). Unternehmen, die durch Sophos MDR Complete geschützt sind, können damit im Fall der Fälle bis zu 1 Million US-Dollar an Reaktionskosten abdecken. Die Breach Protection Warranty wird ausschließlich von Sophos übernommen und deckt Endpoints (Windows- und Mac-Geräte) sowie Server ab. Im Gegensatz zu Konkurrenzangeboten gibt es hier keine Einstufungen oder Laufzeitbeschränkungen für aktive Kunden. Diese Sophos Breach Protection Warranty ist automatisch in allen Käufen und Verlängerungen von Sophos MDR Complete-Jahresabonnements über das globale Sophos Partnernetzwerk enthalten.

Verfügbarkeit



Mehr als 13.000 Unternehmen nutzen bereits den MDR-Service von Sophos, bei dem Expertenteams rund um die Uhr Bedrohungen aufspüren, erkennen und darauf reagieren. Das neueste Angebot mit Funktionen zur Integration von Drittanbietern ist ab sofort verfügbar. Der Service lässt sich mit verschiedenen Stufen und Optionen für die Reaktion auf Bedrohungen anpassen. Kunden können wählen, ob das Sophos MDR-Team eine umfassende Reaktion auf Vorfälle durchführen, Unterstützung bei bestätigten Bedrohungen leisten oder detaillierte Alert-Benachrichtigungen liefern soll, die ihre Security Operations Teams selbst verwalten können.

Zusätzliche Ressourcen

- Mehr über den [Sophos Marketplace](#), der Integrationen für das gesamte Sophos Portfolio bietet, einschließlich Sophos MDR, Sophos Central, Sophos Factory und Sophos Cloud Optix
- Die [Sophos Breach Protection-Warranty](#)
- Die Bedrohungslandschaft und Trends, die sich voraussichtlich auf die Cybersicherheit auswirken werden, im [Threat Report 2023](#)
- [Sophos X-Ops](#) und seine bahnbrechende Bedrohungsforschung durch Abonnement der Sophos X-Ops Blogs
- Verweildauer von Angreifern und Einblicke in Taktiken, Techniken und Verfahren (TTPs) im Sophos [Active Adversary Playbook 2022](#)
- Die weltweite Verbreitung und Auswirkung von Ransomware im [State of Ransomware 2022](#) Report
- Ransomware nach Namen im [Ransomware Threat Intelligence Center](#)

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos_info

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 Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

Ariane Wendt +49-172-4536839

sophos@tc-communications.de