



Bessere Abwehr von Cyberbedrohungen und vereinfachte Verwaltung für Sophos Endpoint Security

Adaptive Active Adversary Protection, Erweiterungen beim Schutz vor Linux-Malware, Health Check-Funktionen, integrierter ZTNA-Agent und mehr.

Wiesbaden, 9. März 2023 – Sophos stellt mehrere Weiterentwicklungen seines [Endpoint-Security-Portfolios](#) zum verbesserten Schutz vor fortschrittlichen Cyberbedrohungen und zum optimierten Sicherheitsmanagement von Endpoints vor. Dazu gehören unter anderem die neue Adaptive Active Adversary Protection, Verbesserungen beim Schutz vor Linux-Malware, Account Health Check-Funktionen sowie ein integrierter [Zero Trust Network Access](#) (ZTNA)-Agent für Windows- und macOS-Geräte.

„Ransomware ist nach wie vor eine der am weitesten verbreiteten und schädlichsten Cyberbedrohungen für Unternehmen und jetzt ist nicht der richtige Zeitpunkt, um die Wachsamkeit zu vernachlässigen, nur weil die Zahl der Angriffe vermeintlich abnimmt. Vielmehr sollten Unternehmen ihre Abwehrmaßnahmen verstärken. Angriffe sind heute komplexer und schwieriger zu erkennen. Dies erfordert fortschrittliche Sicherheitstechniken, die eine schnelle Erkennung und Anpassung bieten“, sagt Raja Patel, Senior Vice President of Products bei Sophos.

Die neuen Sophos-Endpoint-Innovationen sind:

Adaptive Active Adversary Protection: Adaptive Active Adversary Protection ist ein zentraler Bestandteil der "Shields Up"-Methode von Sophos und verschafft Verteidigern zusätzliche Zeit, um auf aktuelle, gezielte Angriffe zu reagieren. Sophos Intercept X aktiviert sofort Verteidigungsmaßnahmen, sobald es ein "Hands-on-Keyboard"-Eindringen am Endpoint erkennt. Dadurch wird einem Angreifer die Möglichkeit genommen, weitere Aktionen durchzuführen. Es reduziert die Angriffsfläche und Angriffe werden unterbrochen beziehungsweise eingedämmt noch bevor das Reaktionsteam eingreift. Zudem stellt es die erforderlichen Erkenntnisse zur Verfügung, die für eine vollständige Behebung des Angriffs nötig sind.

Verbesserter Schutz vor Linux-Malware: On-Access-Malware-Scans und Quarantänefunktionen verbessern die Echtzeit-Prävention für Linux-Umgebungen. Die neuen Funktionen ergänzen [Sophos Intercept X Advanced for Server](#), einschließlich der Erkennung von und Reaktion auf Container-Escapes, Cryptominer, Datenvernichtung und Kernel-Exploits.

Health Check: Die intuitive Echtzeitüberwachung von Sicherheitskonfigurationen und Richtlinieneinstellungen bietet die Möglichkeit, mit einem einzigen Mausklick automatisch zu den empfohlenen Einstellungen zurückzukehren, um die Sicherheitslage zu optimieren. Die Bewertungen stellen beispielsweise sicher, dass auf den Geräten die erforderlichen Sicherheitskomponenten ausgeführt werden, dass die Richtlinien den empfohlenen Einstellungen folgen, dass der Manipulationsschutz aktiv ist oder dass Ausnahmen keine Angriffsfläche bieten.

Integrierter ZTNA-Agent für Windows- und macOS-Geräte: Sophos Intercept X ist eine Endpoint-Protection-Lösung mit einem modularen ZTNA-Agenten. Unternehmen können

jetzt ihren Sophos-ZTNA-Schutz für ganze Unternehmen ausweiten, ohne einen zusätzlichen Agenten einsetzen zu müssen.

Schneller, schlanker Agent: Der neue Agent verringert den Speicherbedarf auf Windows um 40 Prozent und senkt die Anzahl der Prozesse um mehr als 30 Prozent. Sophos hat außerdem eine neue Option für den Einsatz von XDR-Sensoren (Extended Detection and Response) eingeführt, der ca. 80 Prozent schlanker als der bisherige Full-Agent ist.

Das vollständig integrierte Portfolio an Endpoint-, Netzwerk- und Cloud-Lösungen sowie Managed Security Services von Sophos ist Teil des [Sophos Adaptive Cybersecurity Ecosystem](#). Die Lösungen werden durch Threat Intelligence von [Sophos X-Ops](#) unterstützt, um einen schnelleren und kontextbezogenen Schutz, Erkennung und Reaktion zu ermöglichen.

Verfügbarkeit

Das Sophos Endpoint Security-Portfolio ist ab sofort exklusiv über den weltweiten Sophos Channel bei [Partnern](#) und [Managed Service Providern](#) (MSPs) erhältlich. Neue Software-Management-Optionen ermöglichen es Unternehmen, genau zu steuern, welche Versionen der Sophos Endpoint-Software auf bestimmten Geräten eingesetzt werden. Zusätzlich gibt es neue Support-Pakete mit fester Laufzeit für Windows-Computer und -Server, die im Laufe des Jahres auch für macOS und Linux zur Verfügung stehen werden.

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 [in](#) und [t](#)

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