



## Sophos integriert Cloud-Security in Endpoint- und Server-Schutz

Sophos stattet seinen Endpoint- und Server-Schutz Sophos Intercept X Advanced for Server standardmäßig und ohne zusätzliche Kosten mit einem Cloud Security Posture Management aus. In allen aktuellen Versionen von Intercept X Advanced for Server sind jetzt die Standardfunktionen von Sophos Cloud Optix, der Security-Lösung speziell für Cloud-Umgebungen, integriert.

Einer der wichtigsten Gründe, weshalb jetzt die Kernfunktionen von Sophos Cloud Optix in Intercept X for Server inkludiert sind, ist die Tatsache, dass mittlerweile über 60 Prozent der Angriffe auf cloudbasierte Daten und Webanwendungen auf Fehlkonfigurationen in den Cloud-Umgebungen zurückzuführen sind.

Cloud Optix identifiziert über automatisierte Scans unsichere Konfigurationen sowie mit Hilfe von künstlicher Intelligenz verdächtige Zugriffe und ungewöhnlichen Netzwerkverkehr in Cloud-Umgebungen. Die Scans werden mit CIS Benchmarks verglichen, die auf einer von der Community erstellten und gepflegten Reihe von Best Practices für die Cloud-Sicherheit basieren. Schwachstellen werden erkannt und Abwehrmaßnahmen priorisiert, damit Security-Teams mit Hilfe kontextbezogener Warnungen schneller reagieren können.

In Verbindung mit Sophos Central profitieren Kunden zudem von einer neuen nahtlosen Integration, die Server automatisch aus der Central Admin-Konsole entfernt, wenn Cloud-Server-Instanzen in AWS- und Azure-Umgebungen gestoppt oder gelöscht werden.



Die wichtigsten Funktionen sind:

- **Cloud-Asset-Inventarisierung:** Diese Funktion zeigt ein detailliertes Inventar der gesamten Cloud-Infrastruktur (z. B. IAM-Rollen, Sicherheitsgruppen, gemeinsam genutzter Speicher, Datenbanken, Serverless, Container, etc.), wodurch die zeitaufwändige manuelle Zusammenstellung über AWS, Azure und GCP hinweg entfällt.
- **Access and Traffic Anomaly Detection:** Ungewöhnliche Anmeldeversuche und verdächtige Traffic-Muster werden automatisch erkannt und die Teams alarmiert.
- **Sicherheits-scans:** Tägliche und bedarfsgesteuerte Scans überwachen die Cloud-Umgebung, um deren Sicherheitszustand zu gewährleisten. Warnungen werden automatisch nach Risikostufe priorisiert und Administratoren erhalten detaillierte Informationen und Anweisungen zur Lösung des Problems.
- **Security Best Practice:** Diese Funktion erkennt, wenn Cloud-Konten und die Konfiguration der bereitgestellten Ressourcen nicht den Sicherheits-Best-Practices mit den Richtlinien des Center for Internet Security (CIS) Benchmark entsprechen.
- **Alert Management Integrationen:** E-Mail-Benachrichtigungen werden an die Sicherheitsverantwortlichen gesendet, wenn ein manuelles Eingreifen erforderlich ist.

Die neuen Funktionen stehen allen Kunden mit einer Intercept X Advanced for Server oder Intercept X Advanced for Server with EDR-Laufzeitlizenz ohne zusätzliche Kosten über Sophos Central zur Verfügung. Kunden, die Sophos Central nutzen und diese neue Funktionalität testen möchten, können eine Testversion über die Sophos Central Konsole starten. Kunden, die noch nicht mit Sophos Central arbeiten, können sich für eine Trial-Version unter [Sophos.com](https://www.sophos.com) registrieren.

### **Neu: 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

### **Pressekontakt:**

Sophos

Jörg Schindler, PR-Manager Central & Eastern Europe

[joerg.schindler@sophos.com](mailto: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](mailto:sophos@tc-communications.de)