

# Sophos Cloud Optix

## Eine Kombination aus leistungsstarker KI und Automation vereinfacht Ihre Cloud Security

Der agentenlose SaaS-basierte Service von Sophos Cloud Optix kombiniert exzellentes Sicherheits-Know-how mit leistungsstarker Künstlicher Intelligenz. So überwachen Sie Ihre Sicherheit in der Cloud und automatisieren die Compliance mit einer leicht zu bedienenden Benutzeroberfläche für effiziente Prozessgestaltung.

### Highlights

- ▶ Einrichtung des agentenlosen SaaS-basierten Services in wenigen Minuten
- ▶ Inventory Management über mehrere Cloud-Anbieter hinweg
- ▶ Komplette Visualisierung der Netzwerktopologie und des Datenverkehrs
- ▶ KI-basierte Erkennung von Anomalien im Benutzerverhalten und Datenverkehr
- ▶ Kontinuierliche Überprüfung der Compliance
- ▶ Fertig nutzbare Compliance-Richtlinien
- ▶ Korrelation von Warnmeldungen zur schnelleren Bereinigung
- ▶ Erkennung von Änderungen an kritischen Einstellungen
- ▶ Kontinuierliche Überprüfung von Infrastructure-as-Code-Vorlagen

### Alles im Blick. Alles geschützt.

Automatische Erkennung Ihrer Unternehmens-Assets in Umgebungen von Amazon Web Services (AWS), Microsoft Azure und der Google Cloud Platform (GCP). So kann Ihr Team innerhalb weniger Minuten auf Sicherheitsrisiken reagieren und diese bereinigen – mit kontinuierlicher Überwachung der Assets, vollständiger Visualisierung der Netzwerktopologie und des Datenverkehrs einschließlich eingehendem, ausgehendem und internem Datenverkehr.

### Proaktive Cloud Compliance

Durch die vermehrte Nutzung von Cloud-Anwendungen wird das Thema Compliance immer schwieriger: Welche Compliance-Prozesse sind notwendig und wie können sie umgesetzt werden? Cloud Optix verringert Kosten und Aufwand für Governance, Risikomanagement und Compliance – durch fertig nutzbare Vorlagen, anpassbare Richtlinien und Tools zur Zusammenarbeit.

### Schnellere Compliance-Prozesse

Überwachen Sie kontinuierlich die Compliance mit benutzerdefinierten oder fertig nutzbaren Vorlagen für Standards wie CIS, DSGVO, SOC2, HIPAA ISO 27001 und PCI DSS.

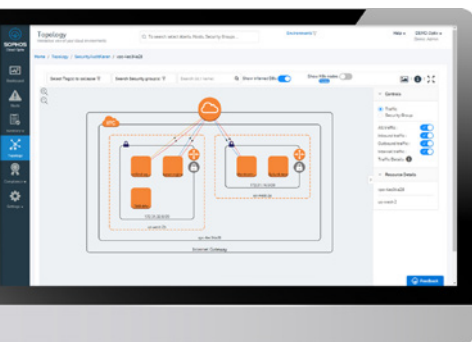
### Einfache Zusammenarbeit

Verwalten und kontrollieren Sie die Compliance, um sicherzustellen, dass wichtige Tasks nie verloren gehen, auch nicht während eines Releases – durch die Integration von Fremdanbieter-Tools wie JIRA und ServiceNow.

### KI-basierte Sicherheitsanalysen und -überwachung

Cloud Optix überwacht Ihre Sicherheit kontinuierlich und verarbeitet Daten über Ihre Cloud-Assets, Konfigurationen und Netzwerkverkehr. KI-basierte, intelligente Warnmeldungen ermöglichen kürzere Reaktionszeiten auf Vorfälle und eine schnellere Beseitigung von Sicherheitsrisiken, mit automatisierter Priorisierung und Kontext-Informationen.

- ▶ Kontinuierliche Überwachung des Cloud Workload Inventory (Amazon Simple Storage Service (S3), Sicherheitsgruppen, Benutzerzugriffsschlüssel usw.), der Konfigurationen und der Protokolle der Sicherheitsgruppen
- ▶ Erkennen von Anomalien im Benutzerverhalten, um komplexe automatisierte Bedrohungen zu finden, die aus gestohlenen Benutzerzugriffsschlüsseln oder unautorisiertem Zugriff durch Mitarbeiter resultieren
- ▶ Prognose zum Datenverkehr basierend auf Ihren Sicherheitseinstellungen; potenzielle Schwachstellen werden verhindert, bevor es zum Angriff kommt
- ▶ Schutzmaßnahmen, um versehentliche oder böswillige Änderungen in der Netzwerkkonfiguration zu verhindern, zu erkennen und zu bereinigen



### Intelligenter DevSecOps

Schnelle Infrastructure-as-Code-Änderungen aufgrund von Continuous Deployment und DevOps-Praktiken ermöglichen, dass mehrmals am Tag neue Software veröffentlicht wird. IT-Abteilungen stehen dadurch enorm unter Druck, für zuverlässige Sicherheit zu sorgen. Dank der API-basierten Architektur von Sophos Cloud Optix lässt sich IT-Sicherheit nahtlos in Ihre DevOps-Prozesse integrieren. So sind Ihre Veröffentlichungen zuverlässig geschützt.

### Erkennen von Abweichungen und Schutzmaßnahmen

Überwachen Sie Konfigurationsstandards kontinuierlich und erkennen Sie Abweichungen; verhindern Sie Änderungen an kritischen Einstellungen, die zu Sicherheitslücken in Ihrem Unternehmen führen könnten.

### Proaktives Prüfen von Infrastruktur-Vorlagen

Prüfen Sie kontinuierlich Infrastructure-as-Code-Vorlagen, die von Lösungen wie Terraform, Github oder Bitbucket bereitgestellt werden, um Fehlkonfigurationen zu erkennen, die zur Bereitstellung einer Infrastruktur mit Schwachstellen führen könnten.

### Integration von SIEM und DevOps-Tools

Integrieren Sie Sicherheitstools von Fremdanbietern wie SIEM und DevOps-Tools für CI/CD zur Vereinfachung von Sicherheitsprozessen.

### Einfache Lizenzierung und Bereitstellung

Der agentenlose SaaS-basierte Service von Sophos Cloud Optix arbeitet perfekt mit Ihren vorhandenen Business-Tools zusammen.

Die Verbindung zu Cloudkonten in AWS-, Azure- oder GCP-Umgebungen ist ganz einfach, dank der bereitgestellten Anleitungen und Skripte, die über die nativen Cloud-APIs nur einen Lesezugriff erstellen. Verbindungen lassen sich in wenigen Minuten aufbauen. Nach Abschluss der Bereitstellung kann Cloud Optix sofort Ihre Cloud-Umgebung überprüfen und Ihnen wichtige Informationen liefern.

### Cloud Security ist eine gemeinsame Verantwortung

Public Cloud-Anbieter bieten ein hohes Maß an Plattform-Flexibilität. Die Anbieter sorgen zwar für den physischen Schutz im Rechenzentrum, doch die virtuelle Trennung von Daten und Umgebungen, unabhängig vom Inhalt der Cloud, liegt in Ihrer eigenen Verantwortung.

Cloud Optix bietet eine kontinuierliche Transparenz, Compliance und Reaktion auf Bedrohungen. Informationen zu unserem kompletten Angebot an Lösungen für den Schutz Ihrer Workloads in der Public Cloud erhalten Sie unter [sophos.de/public-cloud](https://sophos.de/public-cloud).

#### Sophos Cloud Optix: Funktionen

Zentrale Übersicht für mehrere Clouds	✓
Visualisierung der Netzwerktopologie	✓
Network Traffic Visualization Overlay	✓
Security Group Visualization Overlay	✓
Erkennung von Anomalien – Netzwerkdatenverkehr	✓
Erkennung von Anomalien – Verhalten Benutzeranmeldung	✓
Inventory – Hosts, Netzwerke, Speicher, IAM	✓
Inventory – AWS CloudTrail	✓
Inventory – serverlos	✓
Kontinuierliche Überprüfung der Compliance	✓
Compliance-Richtlinien (CIS, FEDRAMP, FFIEC, DSGVO, HIPAA, ISO 27001, PCI DSS 3.2, SOC2, EBU R 143)	✓
CIS-Bewertungsrichtlinien	✓
Anpassbare Richtlinien	✓
Compliance/Best Practice-Warnmeldungen und -Berichte	✓
Bereinigung und Schutzmaßnahmen	✓
DevSecOps-Skriptüberprüfung	✓

## Kostenlose Demo oder Testversion

Alle Cloud Optix Funktionen 30 Tage lang kostenlos testen unter [www.sophos.de/cloud-optix](https://www.sophos.de/cloud-optix)

Sales DACH [Deutschland, Österreich, Schweiz]  
Tel.: +49 611 5858 0 | +49 721 255 16 0  
E-Mail: [sales@sophos.de](mailto:sales@sophos.de)