

Sophos Cloud Native Security



Schutz für Cloud-Umgebungen, -Workloads und -Identitäten

Sophos Cloud Native Security bietet umfassenden Multi-Cloud-Schutz für Amazon-Web-Services-, Microsoft-Azure- und Google-Cloud-Plattform-Umgebungen, -Workloads und -Identitäten – zum schnellen Erkennen und Beseitigen von Sicherheitsrisiken und zum Gewährleisten lückenloser Compliance.

Maximale Unterstützung für Sicherheitsteams

Mit Sophos Cloud Native Security erhalten Sie eine einzige integrierte Cloud-Security-Plattform zur Steigerung der Effizienz und Verkürzung von Reaktionszeiten bei Vorfällen. Sophos Cloud Native Security vereinheitlicht Sicherheitstools für Workloads, Cloud-Umgebungen und die Verwaltung von Berechtigungen, um optimale Transparenz, Sicherheit und Compliance zu gewährleisten. Alle Tools lassen sich für organisationsweite Flexibilität nahtlos in SIEM-, Collaboration-, Workflow- und DevOps-Programme integrieren.

Erkennungs- und Reaktionszeiten minimieren

Erkennen und stoppen Sie Malware, Exploits, Fehlkonfigurationen und anomale Verhaltensweisen mit leistungsstarken Extended Detection and Response (XDR) Tools. Suchen Sie nach Bedrohungen, erhalten Sie priorisierte Erkennungen und profitieren Sie von automatisch verbundenen Sicherheitsereignissen in AWS-, Azure- und GCP-Umgebungen, mit denen Sie die Analyse- und Reaktionszeiten verkürzen.

Cyber-Resilienz auf dem Fast-Track

Cyberkriminelle sind clever und kreativ. Ihr Unternehmen und Ihre Cloud-Umgebungen müssen robust, schwer zu kompromittieren und schnell wiederherstellbar sein. Unsere umfassenden und intuitiven Cloud Security und Remediation Tools können von Ihren eigenen Sicherheitsteams, über einen Sophos-Partner oder über den Sophos Managed Threat Response (MTR) Service verwaltet werden. Mit unserem MTR-Service erhalten Sie erstklassige Cyber-Resilienz im Schnellverfahren und sind sofort optimal auf Sicherheitsvorfälle vorbereitet.

Partnerschaft zur Verstärkung Ihres Teams

Der Sophos MTR Service ist die perfekte Ergänzung zu Sophos Cloud Native Security. Dieser Managed Detection and Response Service kann mit Ihren Teams zusammenarbeiten, Ihre Umgebung 24/7/365 überwachen, auf potenzielle Bedrohungen reagieren, nach „Indicators of Compromise“ suchen und detaillierte Analysen zu Ereignissen liefern – was ist wo, wann, wie und warum passiert? So wird proaktiv verhindert, dass komplexe Bedrohungen Ihre Daten und Systeme ins Visier nehmen.

Integrierte Hybrid Cloud Security

Mit Sophos erhalten Sie nicht nur Cloud native Security, sondern auch eine zentrale Management-Konsole für alle Ihre Sophos Hybrid-Cloud-Cybersecurity-Technologien, einschließlich Endpoint, Mobile, Server, Firewalls, Switches, Secure Wireless, Email Security und Secure Access. Durch den Informationsaustausch zwischen Ihren Produkten in Echtzeit, den zentralen XDR Datalake sowie konsolidierte Dashboards und Warnmeldungen macht Sophos Central Ihre Cybersicherheit einfacher und effektiver.

Highlights

- ▶ Sichere Umgebungen und Workloads in AWS, Azure und GCP
- ▶ Cloud-Workload-Schutz für Linux und Windows
- ▶ Verwaltung Ihres Sicherheitsstatus in der Cloud
- ▶ Kubernetes Security Posture Management
- ▶ Infrastructure as Code Security
- ▶ Verwaltung von Berechtigungen in Cloud-Infrastrukturen
- ▶ Überwachung von Cloud-Ausgaben

Umfassende Multi-Cloud Security Transparenz, Governance und Compliance

Reduzieren Sie Ihre Angriffsfläche durch Transparenz über Multi-Cloud-Umgebungen, um Sicherheitsrisiken zu erkennen und zu beseitigen und die Compliance zu gewährleisten.

- ▶ Steigern Sie die Effizienz mit Cloud Security Posture Management-Tools für AWS-, Azure-, GCP-, Kubernetes-, Infrastructure-as-Code- und Docker-Hub-Umgebungen in einer zentralen Konsole.
- ▶ Sehen Sie alles: Asset Inventories, Netzwerkvisualisierungen, Cloud-Ausgaben und Konfigurationsrisiken.
- ▶ Automatisieren Sie Compliance Assessments und ersparen Sie sich wochenlange Arbeit mit sofort Audit-fähigen Reports.
- ▶ Reduzieren Sie Risiken ohne Einbußen bei der DevOps-Geschwindigkeit – mit Infrastructure as Code und Container-Image Security.
- ▶ Verlassen Sie sich mit risikobewerteten und farbcodierten Warnmeldungen darauf, dass Ressourcen priorisiert werden.

Cloud-Workloads und -Daten schützen

Schützen Sie Ihre Host- und Container-Workloads mit leichtgewichtigen Linux- und Windows-Schutz über einen Agent oder eine API für Linux.

- ▶ Schützen Sie alles: Cloud, Rechenzentrum, Host, Container, Windows oder Linux.
- ▶ Erkennen Sie komplexe Linux-Sicherheitsvorfälle zur Laufzeit und ohne Bereitstellung eines Kernel-Moduls.
- ▶ Schützen Sie Windows-Hosts und mobile Mitarbeiter vor Bedrohungen, Exploits und komplett neuen Bedrohungen.
- ▶ Kontrollieren Sie Anwendungen, sperren Sie Konfigurationen und überwachen Sie Änderungen an wichtigen Windows-Systemdateien.

- ▶ Rationalisieren Sie Bedrohungsanalysen und Reaktionsmaßnahmen mit XDR, um Ereignisse zu priorisieren und miteinander zu verbinden.

„Least Privilege“-Prinzip durchsetzen

Verwalten Sie Identitäten, bevor sie ausgenutzt werden, indem Sie in Multi-Cloud-Umgebungen mittels Verwaltung von Berechtigungen in Cloud-Infrastrukturen jeweils nur die tatsächlich nötigen Rechte zuweisen.

- ▶ Stellen Sie sicher, dass alle Identitäten nur über die Rechte verfügen, die sie zur Erledigung ihrer Aufgaben benötigen.
- ▶ Visualisieren Sie komplexe, untereinander verflochtene IAM-Rollen, um Zugriffe mit überprivilegierten Berechtigungen schnell zu ermitteln und zu unterbinden.
- ▶ Decken Sie anhand von ungewöhnlichen Zugriffsmustern und Standorten Identitätsdiebstahl und missbräuchliche Nutzungen von Zugangsdaten auf.
- ▶ Stellen Sie mit SophosAI Verbindungen zwischen verschiedenen risikoreichen Anomalien im Benutzerverhalten her, um Verstöße zu verhindern.

Sicherheit auf Netzwerk und Anwendungen ausweiten

Schützen Sie Netzwerke und Anwendungen mit der Sophos Firewall. Diese integrierte Lösung kombiniert mehrere führende Sicherheitstechnologien, einschließlich IPS, ATP, URL-Filterung und WAF, in einer einzigen Lösung. Dank Hochverfügbarkeit und flexibler SD-WAN- und VPN-Konnektivität lassen sich beliebige Benutzer an beliebigen Orten schnell und einfach anbinden. Zum Auto-Scaling bietet die Sophos UTM Firewall eine separate Lösung für hochdynamische Umgebungen.

Effizienter Cybersecurity-Kauf

Die Sophos Cybersecurity-Reihe ist direkt bei Sophos, über unser Netzwerk ausgewählter Partner und über den AWS Marketplace erhältlich. So können Kunden ihre Beschaffungsprozesse optimieren. Außerdem wird das Paket auf alle bereits mit Cloud-Anbietern eingegangenen Nutzungsverpflichtungen angerechnet.

Mehr erfahren oder mit
einem Experten sprechen

sophos.de/cloud

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de