Das ist neu: Sophos Cloud Native Security

Umfassender Multi-Cloud-Schutz über Umgebungen, Workloads und Identitäten hinweg

SOPHOS
Cybersecurity delivered.

Eine einzige, integrierte Cloud-Security-Lösung

Die Umstellung auf Cloud-Technologien wie Hosts, Container, Speicher-Services und Infrastructure as Code bedeutet, dass Unternehmen ihre Transparenz erhöhen müssen, um sich vor Fehlkonfigurationen, Malware, Ransomware, Sicherheitsverletzungen und weiteren Risiken zu schützen.

Sophos Cloud Native Security umfasst Tools, die Ihnen die erforderliche Transparenz bieten. Zudem sorgt unsere Lösung für robuste, schwer zu kompromittierende und schnell wiederherstellbare Cloud-Umgebungen. Eine einzige, integrierte Lösung für Amazon Web Services, Microsoft Azure und Google Cloud Platform kombiniert Sophos Cloud Optix und Sophos Intercept X Advanced for Server with XDR.

In Sophos Central, der zentralen Management-Konsole von Sophos, suchen Sie nach Bedrohungen, erhalten priorisierte Erkennungen und profitieren von automatisch verbundenen Sicherheitsereignissen, mit denen Sie die Analyse- und Reaktionszeiten verkürzen – an einem zentralen Ort.

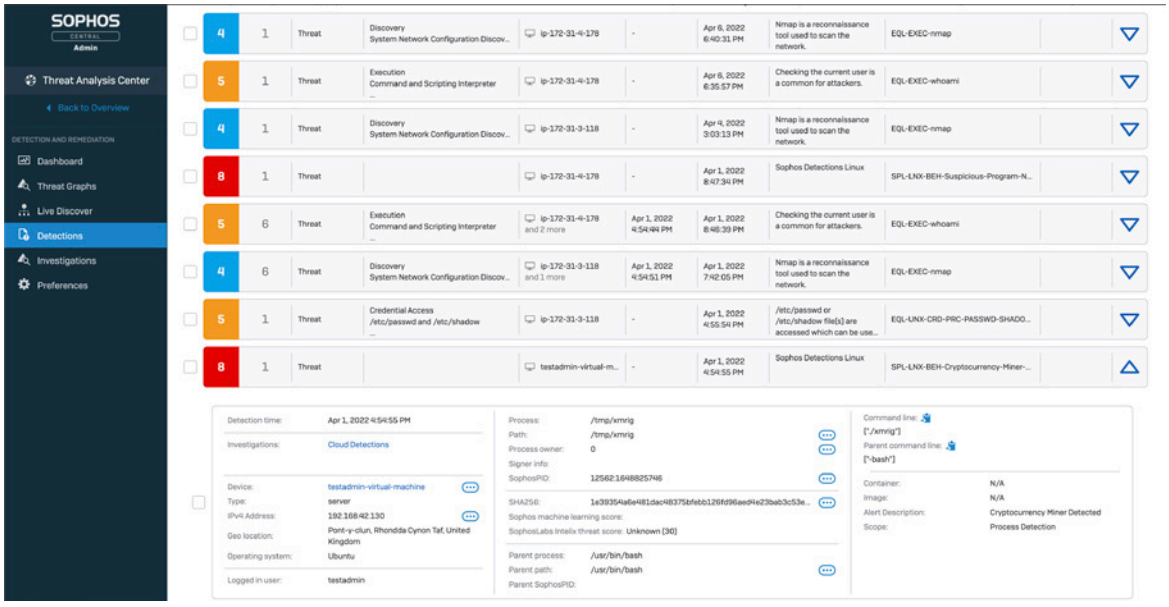
Die nächste Generation von Sophos Server Protection

Zur Sicherung Ihrer Server-Workloads in der Public Cloud hat Sophos seinen bewährten Windows-Schutz jetzt auch auf Bereitstellungen in Linux ausgeweitet – einem der gängigsten Betriebssysteme in der Cloud.

Seit Anfang dieses Jahres umfasst die Server Protection für Cloud-Workloads verhaltensbasierte und Exploit-laufzeitbasierte Container-Erkennungen und erfasst komplexe Linux-Sicherheitsvorfälle so bereits bei deren Auftreten.

Sophos Cloud Native Security liefert Ihnen die Workload-Schutzfunktionen, die Sie benötigen, um Ihre Infrastruktur und Daten jetzt und in Zukunft in der Cloud zu schützen.

- Schützen Sie alles: Cloud, Rechenzentrum, Host, Container, Windows oder Linux.
- Profitieren Sie von maximaler Performance und Betriebszeit mit leichtgewichtigem Linux- und Windows-Host-Schutz über einen Agent oder eine API für Linux.
- Ermitteln Sie komplexe Linux- und Container-Sicherheitsvorfälle zur Laufzeit und ohne Bereitstellung eines Kernel-Moduls.
- Schützen Sie Windows-Hosts und mobile Mitarbeiter vor Ransomware, 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 Extended Detection and Response (XDR), um Ereignisse zu priorisieren und miteinander zu verbinden.



Beispiel für laufzeitbasierte Linux-Bedrohungserkennungen in der Konsole von Sophos Central.

Bereitstellungsoptionen für den Cloud-Workload-Schutz

Verwaltung über Sophos Central – Dank der Verwaltung über Sophos Central liefert der leichtgewichtige Linux-Agent Security-Teams entscheidende Informationen, mit denen sie Verhaltens-, Exploit- und Malware-Bedrohungen in Windows und Linux an einem zentralen Ort analysieren und bekämpfen können. Bei diesem Bereitstellungsmodell wird der Host überwacht. Dabei können Security-Experten Sophos-Lösungen über eine einzige Konsole verwalten und nahtlos zwischen Threat Hunting, Bereinigung und Verwaltung wechseln.

API-Integration – Der Sophos Linux Sensor lässt sich sehr flexibel bereitstellen und ist auf bestmögliche Performance ausgerichtet. Unser Sensor integriert umfangreiche laufzeitbasierte Bedrohungserkennungen per API in Host- oder Container-Umgebungen – mit Ihren vorhandenen Threat-Response-Tools. So erhalten Sie mehr Kontrolle zur Erstellung benutzerdefinierter Regelsätze, die nur Laufzeit-Verhaltenserkennungen enthalten, die für bestimmte Security-Anwendungsfälle erforderlich sind.

Zusätzlich zum Sophos Linux Agent bietet der Sophos Linux Sensor:

- Weitere Erkennungen: Zugriff auf zusätzliche Erkennungen zur Ausnutzung von Anwendungen und Systemen
- Konfiguration und Optimierung: Optionen zum Ändern von „Erlauben/Blockieren"-Listen für Standard-Erkennungen
- Ressourcen-Optimierung: Konfigurationsoptionen zum Optimieren der Auslastung von Host-Ressourcen

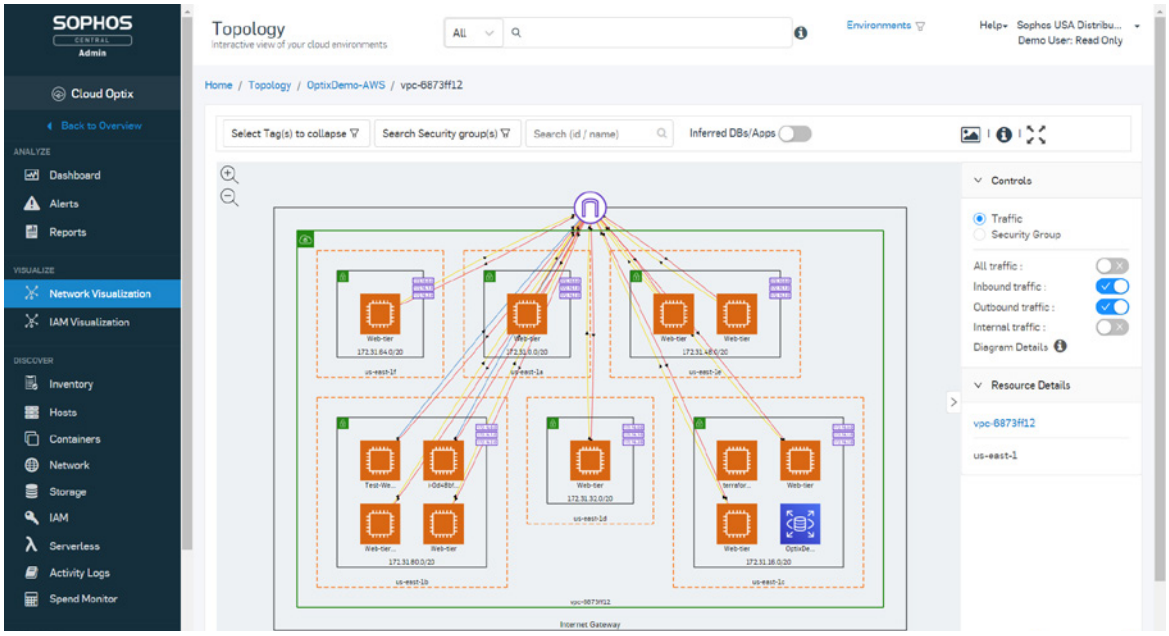
Mehr Transparenz

Die Verringerung Ihrer gesamten Angriffsfläche in AWS-, Azure- und GCP-Umgebungen geht über den Schutz und die Erkennung von Cloud-Workload-Bedrohungen hinaus. Aus diesem Grund konsolidiert Sophos Cloud Native Security Ihren Security-Toolkit in einer Kombi-Lösung. Das Paket umfasst Cloud Security Posture Management, Kubernetes Security Posture Management, Infrastructure-as-Code-Security, Berechtigungsmanagement für Cloud-Infrastrukturen sowie die Überwachung von Cloud-Ausgaben.

Transparenz, Governance und Compliance in Multi-Cloud-Umgebungen

Steigern Sie die Effizienz mit agentenlosen Transparenz- und Remediation-Tools für AWS-, Azure-, GCP-, Kubernetes-, Infrastructure-as-Code- und Docker-Hub-Umgebungen in einer zentralen Konsole.

- Verschaffen Sie sich einen Gesamtüberblick mit On-Demand-Inventories und exportierbaren Netzwerk-Topologie-Visualisierungen.
- Integrieren Sie Security-Services von Cloud-Anbietern in einer zentralen Ansicht, einschließlich Azure Advisor, Azure Sentinel, AWS Security Hub, Amazon GuardDuty, AWS CloudTrail, AWS IAM Access Analyzer, Amazon Detective, Amazon Inspector, AWS Systems Manager und AWS Trusted Advisor.
- Stoppen Sie die Schatten-IT dank automatischer Erkennung Ihrer Assets und Visualisierung von Sophos-Workload-Protection-Agents und Firewall-Bereitstellungen.
- Verhindern und beheben Sie Konfigurationsrisiken in Hosts, Containern, Kubernetes, serverlosen Funktionen, Speicher- und Datenbankdiensten sowie Netzwerk-Sicherheitsgruppen.
- Überwachen und gewährleisten Sie Sicherheits- und Compliance-Standards dauerhaft mit Hilfe von Richtlinien, die automatisch Ihren Umgebungen zugeordnet werden. So ersparen Sie sich wochenlange Arbeit mit sofort Audit-fähigen Reports. Die Richtlinien umfassen unter anderem CIS-Bewertungsrichtlinien, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2 und Sophos Best Practices.
- Verfolgen Sie Cloud-Ausgaben für mehrere AWS- und Azure-Services nebeneinander auf einem Bildschirm für mehr Transparenz. Erhalten Sie Empfehlungen von Sophos zum Optimieren Ihrer Cloud-Anbieter-Ausgaben oder integrieren Sie die Services AWS Trusted Advisor und Azure Advisor.
- Vermeiden Sie eine Flut irrelevanter Warnmeldungen und erkennen Sie schnelle Erfolge („Quick Wins") und kritische Probleme mit risikobewerteten, farbcodierten Warnmeldungen und detaillierten Schritten zur Bereinigung.

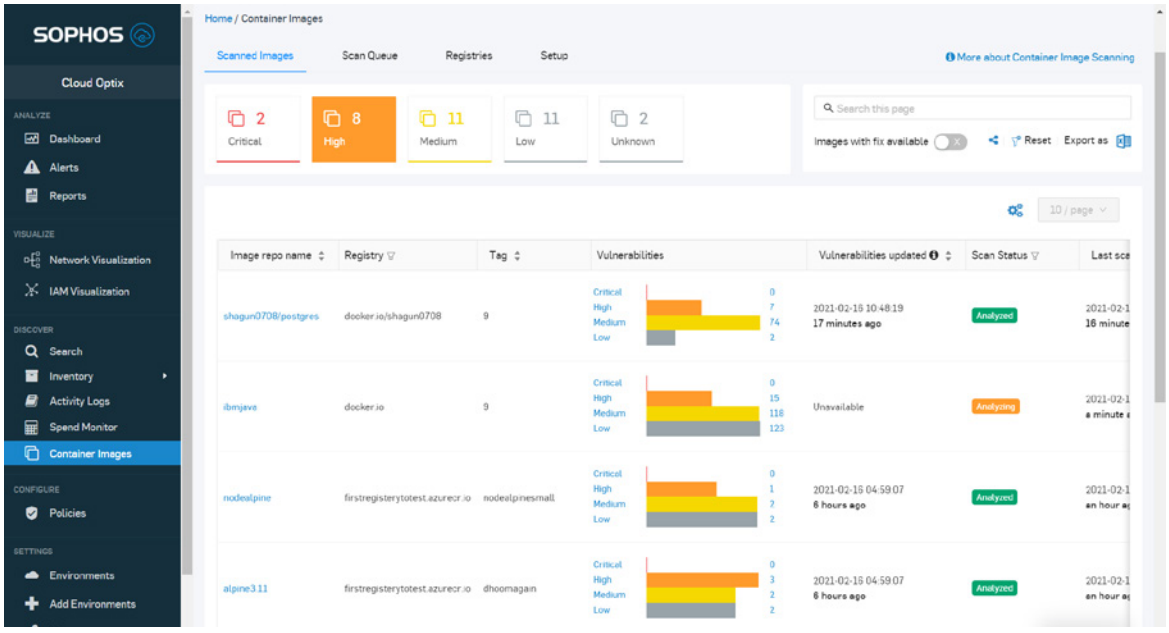


Beispiel für die Visualisierung der Netzwerktopologie für AWS von Sophos mit Sicherheitsgruppen-Analyse.

Risiken reduzieren – ohne Einbußen bei der DevOps-Geschwindigkeit

Ermöglichen Sie schnelle und sichere Entwicklung mit integrierten Sicherheits- und Compliance-Prüfungen in jeder Phase der Entwicklungs-Pipeline.

- Erkennen Sie automatisch Fehlkonfigurationen, eingebettete Passwörter und Schlüssel in Terraform-, AWS-CloudFormation-, Ansible-, Kubernetes- und Azure Resource Manager-Vorlagendateien.
- Verhindern Sie die Bereitstellung von Containern mit Betriebssystem-Schwachstellen und identifizieren Sie verfügbare Fehlerbehebungen. Dabei werden Amazon ECR, ACR und Docker Hub Registries, Infrastructure-as-Code-Umgebungen sowie Images in Build-Pipelines unterstützt.
- Nutzen Sie die nahtlose Integration in GitHub und Bitbucket und erhalten Sie On-Demand-Scan-Ergebnisse in Sophos Central oder scannen Sie mit der REST API Infrastructure-as-Code-Vorlagen und Container Images in jeder Entwicklungsphase.

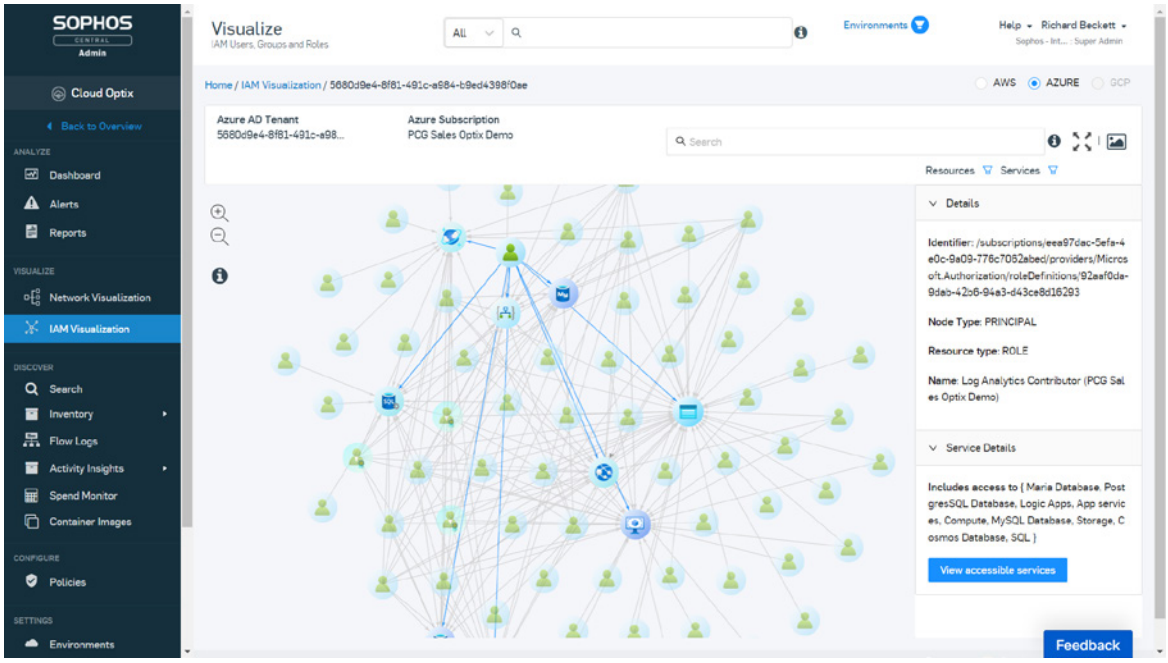


Beispiel für die Ergebnisübersicht der Schwachstellen-Analyse von Sophos-Container-Image-Scans.

„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.
- Decken Sie anhand von ungewöhnlichen Zugriffsmustern und Standorten Identitätsdiebstahl und missbräuchliche Nutzungen von Zugangsdaten auf.
- Ermitteln Sie verwaiste, nicht verwaltete und veraltete Microsoft-IAM-Rollen, über die sich Unbefugte Zugriff zu Umgebungen verschaffen könnten.
- Visualisieren Sie komplexe, untereinander verflochtene AWS-IAM-Rollen, um Zugriffe mit überprivilegierten Berechtigungen schnell zu ermitteln und zu unterbinden.
- Stellen Sie mit SophosAI Verbindungen zwischen verschiedenen risikoreichen Anomalien im Benutzerverhalten in AWS-Umgebungen her, um Verstöße zu verhindern.

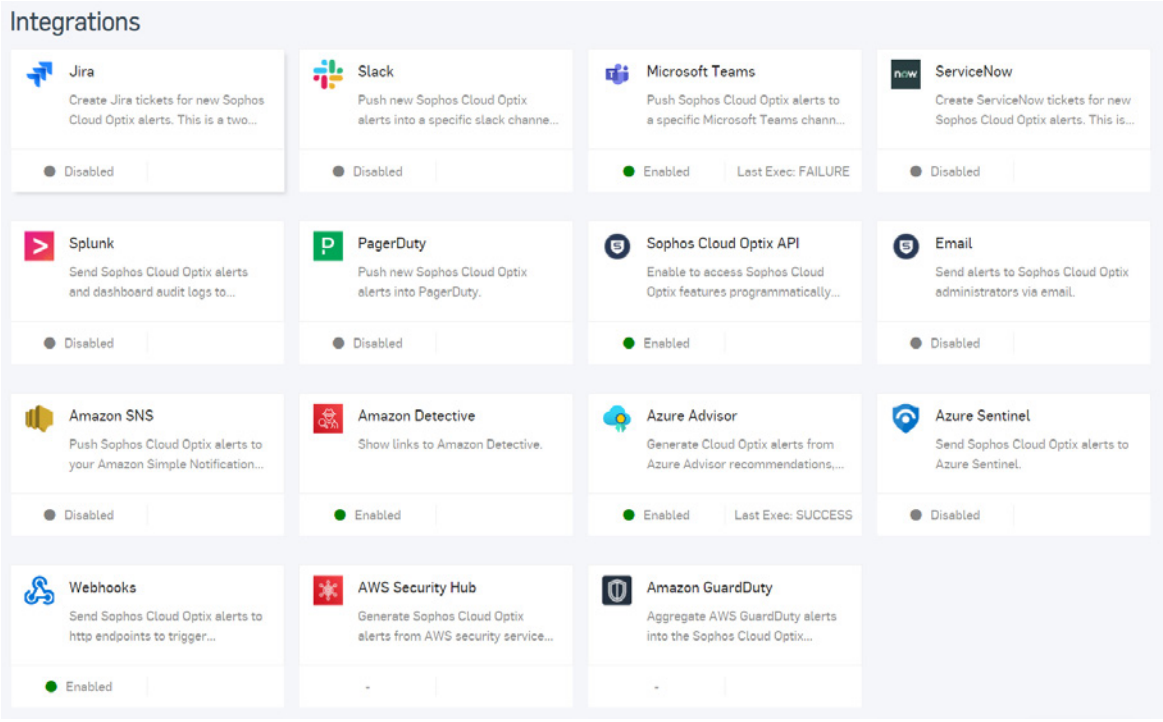


Beispiel für die IAM-Visualisierung von Sophos für Microsoft Azure.

Optimierte Sicherheitsabläufe und effektivere Zusammenarbeit

Erhöhen Sie die Agilität im gesamten Unternehmen und integrieren Sie Warnmeldungen zum Sicherheitsstatus von Cloud-Umgebungen in wenigen Klicks in Ihre vorhandenen SIEM-, Collaboration-, Workflow- und DevOps-Tools.

- Security Operations: Erhalten Sie sofortige Benachrichtigungen zu Sicherheits- und Compliance-Events durch die Integration mit Splunk, Azure Sentinel und PagerDuty.
- Collaboration-Tools: Senden Sie sofortige Warnmeldungen an Slack, Microsoft Teams oder Amazon Simple Notification Service (SNS), um Vorfälle unternehmensübergreifend zu beheben.
- Workflow-Management: Erstellen Sie JIRA- und ServiceNow-Tickets direkt in Sophos Central, um die Reaktion auf Vorfälle nahtlos in Ihre Standard-Workflows einzubinden. Durch die wechselseitige Integration werden doppelte Tickets vermieden.



Beispiel für beliebte Sophos-Integrationen zur Verwaltung von Warnmeldungen der Cloud-Security-Posture-Management-Lösung.

Partnerschaften zur Verstärkung Ihres Teams

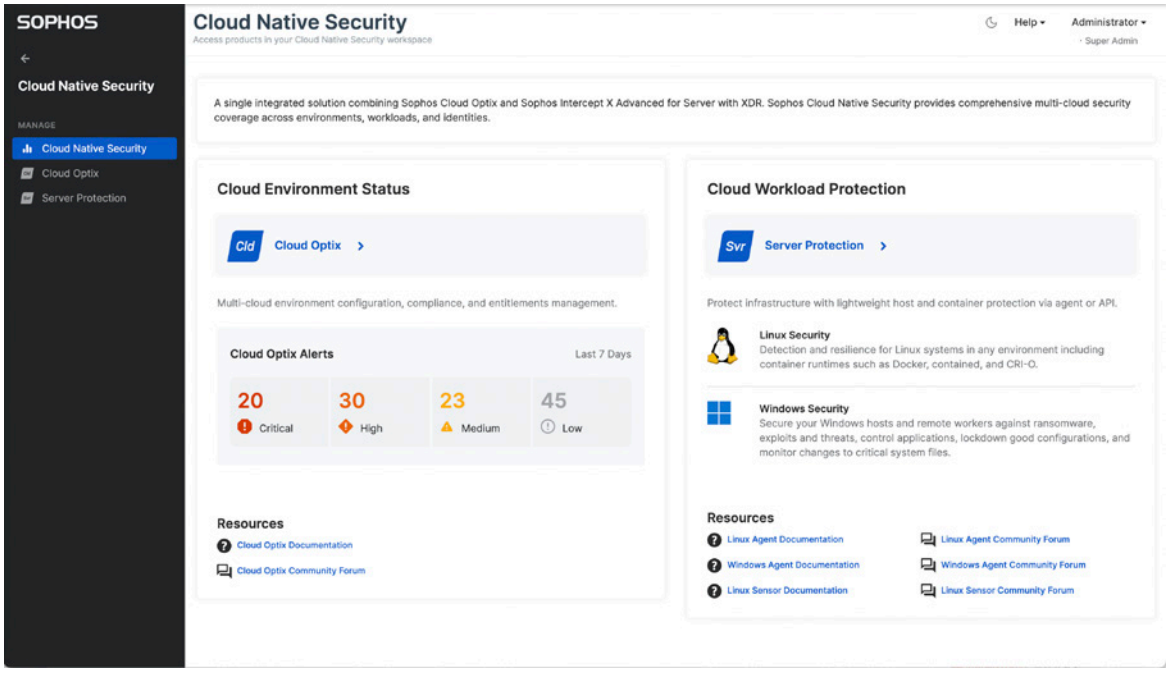
Sie bestimmen, wie Ihr Schutz verwaltet wird: von Ihren eigenen Sicherheitsteams, über einen Sophos-Partner oder über den Sophos Managed Threat Response (MTR) Service. Unser MTR-Team unterstützt Kunden rund um die Uhr beim Bedrohungsmonitoring und bei der Reaktion auf Bedrohungen.

Sophos MTR ist die perfekte Ergänzung zu Sophos Cloud Native Security. Dieser Managed Threat 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 kompromittieren.

Verfügbarkeit von Sophos Cloud Native Security

Das neue kombinierte Paket ist für alle Kunden als Upgrade der folgenden Produkte verfügbar: Intercept X Essentials for Server, Intercept X Advanced for Server und Intercept X Advanced for Server with XDR.

Nach der Aktivierung sehen Kunden und Partner einen neuen Eintrag „CNS" in der Navigation auf der linken Seite in Sophos Central. Der Eintrag ist mit einem neuen Übersichts-Dashboard zu Cloud Native Security verlinkt, das Zugriff auf Sophos Cloud Optix und Intercept X Advanced for Server with XDR bietet.



Screenshot des Dashboards von Sophos Cloud Native Security in der Management-Konsole von Sophos Central.

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion
unter www.sophos.de/cloud

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

22-07-06 DE (DD)

SOPHOS