Server Workload Protection

Linux Protection

Intercept X Advanced for Server, Intercept X Advanced for Server with XDR und Intercept X Advanced for Server with MDR

Cloud oder Rechenzentrum, Host und Container: Schützen Sie Ihre Infrastruktur jetzt und in Zukunft mit leistungsstarkem Workload-Schutz, der praktisch keinen Einfluss auf die Performance hat.

Blitzschnelle Erkennungs- und Reaktionszeiten

Erhalten Sie vollständige Transparenz über Ihre Hosts und Container-Workloads und identifizieren Sie Malware, Exploits sowie ungewöhnliche Verhaltensweisen, bevor sie im Netzwerk Fuß fassen können. XDR (Extended Detection and Response) bietet detaillierte Einsicht in Hosts, Container, Endpoints, Netzwerkverkehr und native Security-Services von Cloud-Anbietern.

Cloud-native Verhaltens- und Exploit-Laufzeiterkennungen (Runtime Detections) identifizieren Bedrohungen wie Container Escapes, Kernel-Exploits und Versuche, die Berechtigungsstufe zu erhöhen. Optimierte Bedrohungsanalyse-Workflows priorisieren die Erkennung hochriskanter Vorfälle und konsolidieren verbundene Ereignisse, um die Effizienz zu steigern und Zeit zu sparen.

Optimierung von Security Operations

Bekämpfen Sie Bedrohungen durch aussagekräftige Einblicke in Host- und Container-Laufzeit sowie Bedrohungserkennungen. Diese werden entweder über unsere zentrale Management-Konsole bereitgestellt oder lassen sich mit verschiedenen Bereitstellungsoptionen in Ihre vorhandenen Threat-Response-Tools integrieren.

Verwaltung über Sophos Central – Durch den leichtgewichtigen Linux-Agenten erhalten Sicherheits-Teams die Informationen, die sie benötigen, damit sie Verhaltens-, Exploit- und Malware-Bedrohungen an einem zentralen Ort analysieren und bekämpfen können. Bei diesem Bereitstellungsmodell wird der Linux-Host überwacht. Dabei können Security-Experten alle 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. Er integriert umfangreiche laufzeitbasierte Bedrohungserkennungen per API in Host- oder Container-Umgebungen – mit Ihren vorhandenen Threat-Response-Tools. So erhalten Sie umfangreichere Erkennungen, mehr Kontrolle über die Erstellung benutzerdefinierter Regelsätze und Konfigurations-Optionen zur Optimierung der Auslastung von Host-Ressourcen.

Reibungslose Performance

Der Schutz von Intercept X for Server ist für DevSecOps-Workflows optimiert und erkennt hochentwickelte Angriffe bei ihrer Ausführung – ohne Kernel-Modul, Orchestrierung, Baselining oder Systemscans. Mit optimierten Ressourcenlimits wie CPU-, Arbeitsspeicher- und Datenerfassungs-Grenzen vermeiden Sie kostspielige Ausfallzeiten durch überlastete Hosts und Stabilitätsprobleme. So sorgen Sie für eine Optimierung der Anwendungs-Performance und -Verfügbarkeit.

Highlights

- Schützt Linux-Workloads und -Container – lokal, virtuell und in der Cloud
- Verkürzt Erkennungs- und Reaktionszeiten
- Ist für geschäftskritische Workloads optimiert, bei denen die Performance entscheidend ist
- Kann dank Extended Detection and Response (XDR) auf Endpoint-, Netzwerk-, E-Mail-, Cloud-, M365- und mobile Daten zurückgreifen
- Sorgt dank integriertem Cloud Security Posture Management für Transparenz und Schutz in Ihrer gesamten Cloud-Umgebung
- Bietet 24/7/365-Sicherheit als Fully-Managed-Service

SOPHOS

Automatisierung Ihrer Cloud-Security-Checkliste

Entwerfen Sie Cloud-Umgebungen, die bewährten Security Best Practices entsprechen, und nutzen Sie zu deren Verwaltung die Transparenz und Tools des integrierten Cloud Security Posture Managements, das Ihre gesamte Public-Cloud-Umgebung abdeckt.

- Erkennen Sie proaktiv unzulässige Aktivitäten, Host- und Container-Image-Schwachstellen sowie Fehlkonfigurationen in Amazon Web Services (AWS), Microsoft Azure und der Google Cloud Platform (GCP)
- Ermitteln Sie kontinuierlich Cloud-Ressourcen – mit detailliertem Inventory und Transparenz über den Sophos-Host-Schutz und Sophos Firewall-Bereitstellungen
- Überlagern Sie automatisch Security-Best-Practice-Standards, um Sicherheitslücken, schnelle Erfolge („Quick Wins") und kritische Probleme zu erkennen
- Decken Sie risikoreiche Anomalien im Verhalten von Benutzer-IAM-Rollen auf und verhindern Sie Verstöße, indem Sie ungewöhnliche Zugriffsmuster, Standorte und schädliche Verhaltensweisen schnell erkennen

Partnerschaft zur Verstärkung Ihres Teams

Die SOC-Experten von Sophos Managed Detection and Response arbeiten eng mit Ihrem Team zusammen, überwachen Ihre Umgebung 24/7/365 und suchen proaktiv nach Bedrohungen. Erkannte Bedrohungen werden für Sie unter Anwendung Linux-spezifischer Experten-Standards effizient beseitigt. Sophos-Analysten reagieren auf potenzielle Bedrohungen, suchen nach „Indicators of Compromise" und liefern detaillierte Analysen der Ereignisse – was ist wo, wann, wie und warum passiert?

Technische Spezifikationen

Aktuelle Informationen entnehmen Sie bitte den Linux-Systemvoraussetzungen. Einzelheiten zur Windows-Funktionalität finden Sie im Windows-Datenblatt.

Funktionen	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MDR Complete
Linux Protection Agent (u. a. Malware-Scans, Exploit Prevention und Dateiscans)	✓	✓	✓
Linux Sensor (Integration von laufzeitbasierten Linux- und Container-Erkennungen in Ihre vorhandenen Threat-Response-Tools per API)		✓	✓
Sichere Cloud-Infrastruktur (Überwachung der Cloud Security Posture zum Verhindern von Sicherheits- und Compliance-Risiken)	✓	✓	✓
XDR (Extended Detection and Response)		✓	✓
MDR (Managed Detection and Response – 24/7/365 Threat Hunting and Response Service)			✓

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter sophos.de/server

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

22-10-21 DS-DE (PC)

SOPHOS