

Sophos Protection for Linux



Erhältlich mit den Lizenzen „Intercept X Advanced for Server“ und „Intercept X Advanced for Server with EDR“

Schützen Sie Ihre lokalen, virtuellen und Cloud-Linux-Server vor den neuesten Cybersecurity-Bedrohungen.

Stoppt unbekannte Bedrohungen

Die Deep-Learning-KI erkennt und blockiert neue und unbekannte Malware besonders zuverlässig. Um Bedrohungen ohne Signaturen zu erkennen, werden Dateiattribute aus Millionen von Samples untersucht.

Linux-, Windows-, Mac- und Android-Malware wird vollständig beseitigt, sodass Ihre Linux-Server vor den neuesten Cybersecurity-Bedrohungen geschützt bleiben.

Maximale Transparenz

Sophos EDR (Endpoint Detection and Response) wurde speziell entwickelt, um IT-Administratoren und Sicherheitsanalysten bei Anwendungsfällen in IT Operations und beim Threat Hunting zu unterstützen. Suchen Sie beispielsweise nach Servern mit RDP-Aktivierung oder nicht gepatchten Software-Schwachstellen.

Sophos XDR (Extended Detection and Response) geht über Server und Endpoints hinaus und erfasst auch Firewall-, E-Mail- und weitere Datenquellen*. So erhalten Sie einen ganzheitlichen Überblick über die Cybersicherheit Ihres Unternehmens und haben die Möglichkeit, bei Bedarf jederzeit Detailinformationen abzurufen. Gehen Sie beispielsweise Problemen mit dem Büronetzwerk auf den Grund und ermitteln Sie, welche Anwendung diese verursacht.

Die gesamte Cloud-Umgebung im Blick

Sehen und schützen Sie Ihr gesamtes Multi-Cloud-Inventory. Sie können Ihre Cloud Workloads sowie kritische Cloud Services wie S3 Buckets, Datenbanken und serverlose Funktionen erfassen, verdächtige Aktivitäten oder unsichere Bereitstellungen erkennen und Sicherheitslücken schließen.

Einfache Verwaltung und Bereitstellung

Dank Sophos Central lassen sich Ihre Server leicht verwalten. Richtlinienverwaltung, Warnmeldungen und Reports werden Ihnen alle in derselben Konsole angezeigt. Schützen Sie Server in der Cloud, vor Ort, in virtuellen und gemischten Umgebungen (Linux und Windows).

Highlights

- Schützt lokale, virtuelle und Cloud-Server-Bereitstellungen
- Stoppt neue und unbekannte Bedrohungen mit Deep-Learning-KI
- Beantwortet wichtige IT-Operations- und Threat-Hunting-Fragen mit EDR
- Zeigt und nutzt Firewall-, E-Mail- und andere Datenquellen mit XDR*
- Transparenz und Sicherheit für Ihre gesamte Cloud-Umgebung, inklusive S3-Buckets und Datenbanken
- Bietet 24/7/365-Sicherheit als Fully-Managed-Service

* Integration von Sophos Cloud Optix und Sophos Mobile XDR erfolgt in Kürze

Managed Threat Response (MTR)

Kunden können auf Wunsch 24/7 Managed Detection and Response mit Threat Hunting durch ein Sophos-Expertenteam als Fully-Managed-Service hinzufügen.

Lizenzstruktur

Sophos Protection for Linux ist in den folgenden Lizenzen enthalten: „Intercept X Advanced for Server“ und „Intercept X Advanced for Server with EDR“

Funktionen	Sophos Protection for Linux
Deep-Learning-Malware-Erkennung	✓
Anti-Malware-Dateiscans	✓
Live Protection	✓
Verwaltung Ihres Sicherheitsstatus in der Cloud (Cloud Hosts überwachen und schützen, serverlose Funktionen, S3-Buckets etc.)	✓
Live Discover (SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben – EDR)	✓ [EDR-Lizenz erforderlich]
Live Response (Remote-Terminal-Zugriff für weitere Analysen und Reaktionsmaßnahmen – EDR)	✓ [EDR-Lizenz erforderlich]
Produktübergreifende Datenquellen und Abfragen – z. B. Firewall, E-Mail (XDR)	✓ [XDR-Lizenz erforderlich]

Detaillierte Informationen zur Lizenzierung finden Sie im [Lizenz-Guide](#).

Es ist ein alternativer Bereitstellungs-Agent verfügbar, der Anti-Malware, Live Protection, Malicious Traffic Detection und Synchronized Security umfasst. Beachten Sie, dass dieser Agent nicht in Verbindung mit Sophos Protection for Linux verwendet werden kann.

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