

# Sophos Protection for Linux



Svr

Available with Intercept X Advanced for Server and Intercept X Advanced for Server with EDR licenses

Secure your Linux cloud, on-premises and virtual servers from the latest cybersecurity threats.

## Unparalleled Visibility

Sophos EDR (Endpoint Detection and Response) is designed for both IT administrators and security analysts to solve IT operations and threat hunting use cases. For example, find servers that have RDP enabled or unpatched software vulnerabilities.

Sophos XDR (Extended Detection and Response) goes beyond servers and endpoints, integrating firewall, email and other data sources\*. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail. For example, understand office network issues and what is causing them.

## See Your Wider Cloud Environment

See and secure your entire multi-cloud inventory. You can detect your cloud workloads as well as critical cloud services including S3 buckets, databases and serverless functions, identify suspicious activity, spot insecure deployments and close security gaps.

## Simplify Management and Deployment

Sophos Central makes managing your servers easy. Policy management, alerts and reporting are all accessed from the same console. Secure servers that are in the cloud, on-premises, or virtual even in mixed (Linux and Windows) estates.

## Highlights

- Secures cloud, on-premises and virtual Linux server deployments
- Answers critical IT operations and threat hunting questions with EDR
- See and leverage firewall, email and other data sources with XDR\*
- Understand and secure your wider cloud environment such as S3 buckets and databases
- Provides 24/7/365 security delivered as a fully managed service

\*Sophos Cloud Optix and Sophos Mobile XDR integration coming soon

### Managed Threat Response (MTR)

Customers can choose to add 24/7 threat hunting, detection and response delivered by a team of Sophos experts as a fully managed service.

### Licensing

Sophos Protection for Linux is included with the following licenses: Intercept X Advanced for Server and Intercept X Advanced for Server with EDR licenses.

Features	Sophos Protection for Linux
Cloud Security Posture Management (monitor and secure cloud hosts, serverless functions, S3 buckets and more)	✓
Live Discover (SQL querying for threat hunting & IT security operations hygiene - EDR)	✓ <i>[Requires EDR license]</i>
Live Response (remote terminal access for further investigation and response - EDR)	✓ <i>[Requires EDR license]</i>
Cross-product Data Sources & Querying e.g. Firewall, Email (XDR)	✓ <i>[Requires XDR license]</i>

For more detailed licensing, please see the [license guide](#).

An alternative deployment agent is available that includes Anti-malware, Live Protection, Malicious Traffic Detection and Synchronized Security. Note that this agent cannot be used in conjunction with Sophos Protection for Linux.

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: [sales@sophos.com](mailto:sales@sophos.com)

North American Sales  
Toll Free: 1-866-866-2802  
Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales  
Tel: +65 62244168  
Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)