

Server Workload Protection



Linux Protection

Intercept X Advanced for Server, Intercept X Advanced for Server with XDR and Intercept X Advanced for Server with MTR

Cloud or datacenter, host and container. Protect your infrastructure now and as it evolves with Sophos high-impact workload protection that's low impact on performance.

Minimize Time to Detect and Respond

Get comprehensive visibility of your hosts and container workloads, identifying malware, exploits, and anomalous behavior before they can get a foothold. Extended detection and response [XDR] provides detailed insight into hosts, containers, endpoints, network traffic, and cloud provider native security services.

Cloud-native behavioral and exploit runtime detections identify threats including container escapes, kernel exploits, and privilege escalation attempts. Streamlined threat investigation workflows prioritize high-risk incident detections and consolidate connected events to increase efficiency and save time.

Improve Security Operations

Combat threats with actionable host and container runtime visibility and threat detections delivered through our central management console, or integrated into your existing automation, orchestration, log management, and incident response tooling.

Choose from two deployment options to best fit your requirements. Sophos Central management gives security teams critical information to investigate and respond to behavioral, exploit, and malware threats in one place. API integration via the Linux sensor* is fine-tuned for maximum performance, funneling rich information into your data management platform of choice.

Get Performance Without Friction

Intercept X for Server protection is optimized for DevSecOps workflows, identifying sophisticated attacks as they happen without requiring a kernel module, orchestration, baselining, or system scans. Optimized resource limits, including CPU, memory, and data collection limits, further avoid costly downtime from overloaded hosts and stability issues. Ensuring you optimize application performance and uptime.

Highlights

- Secures cloud, on-premises, and virtual Linux workloads and containers
- Minimizes time to detect and respond to threats
- Optimized for mission critical workloads where performance is crucial
- Leverage endpoint, network, email, cloud, M365, and mobile data with extended detection and response [XDR]
- Understand and secure your wider cloud environment with included cloud security posture management
- Provides 24/7/365 security delivered as a fully managed service

* Coming soon

Automate Your Cloud Security Checklist

Design your cloud environment to meet best-practice standards with the visibility and tools to maintain them with integrated cloud security posture management covering your wider public cloud environment:

- ▶ Proactively identify unsanctioned activity, host and container image vulnerabilities, and misconfigurations across Amazon AWS, Microsoft Azure, and Google Cloud Platform (GCP)
- ▶ Continuously discover cloud resources with detailed inventory and visibility of Sophos host protection and Sophos Firewall deployments
- ▶ Automatically overlay security best practice standards to detect gaps in posture, identify quick wins and critical issues
- ▶ Detect high-risk anomalies in user IAM role behavior, pinpointing unusual access patterns, locations, and malicious behaviors quickly to prevent a breach

Partnership That Augments Your Team

Sophos Managed Threat Response expert SOC analysts work in partnership with your team, monitoring your environment 24/7/365, and proactively hunting for and remediating threats on your behalf with the Linux expertise needed to increase efficiency. Sophos analysts respond to potential threats, look for indicators of compromise and provide detailed analysis on events including what happened, where, when, how and why.

Technical Specifications

For the latest information please read the [Linux system requirements](#). For details on Windows functionality see the [Windows datasheet](#).

Features	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Advanced
Protection (Including deep learning malware detection, file scanning and more)	✓	✓	✓
CSPM (Cloud security posture management – see and secure your wider cloud environment)	✓	✓	✓
XDR (Extended detection and response)		✓	✓
MTR (Managed threat response – 24/7/365 threat hunting and response service)			✓

Try it now for free
 Register for a free 30-day evaluation at sophos.com/server

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

North American Sales
 Toll Free: 1-866-866-2802
 Email: nasales@sophos.com

Australia and New Zealand Sales
 Tel: +61 2 9409 9100
 Email: sales@sophos.com.au

Asia Sales
 Tel: +65 62244168
 Email: salesasia@sophos.com