# Server Workload Protection


## Linux Protection

### Intercept X Advanced for Server, Intercept X Advanced for Server with XDR and Intercept X Advanced for Server with MDR

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 threat response tools with a choice of deployment options.

**Sophos Central Management** – This lightweight Linux agent gives security teams the critical information they need to investigate and respond to behavioral, exploit, and malware threats in one place. Monitoring the Linux host, this deployment option allows teams to manage all their Sophos solutions from a single pane of glass, seamlessly moving between threat hunting, remediation and management.

**API Integration** - Sophos Linux Sensor is a highly flexible deployment option that is fine-tuned for performance. The Linux sensor uses APIs to integrate rich runtime threat detections, in host or container environments, with your existing threat response tools. Providing a wider range of detections, control to create custom rule sets, and configuration options to tune host resource utilization.

## 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

SOPHOS

## 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 Detection and 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 th 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 MDR Complete |
|---|---|---|---|
| **Linux Protection Agent** (Including malware scanning, exploit prevention, file scanning, and more) | ✔ | ✔ | ✔ |
| **Linux Sensor** (Integrate Linux and container runtime threat detections with your existing threat response tools via API) | | ✔ | ✔ |
| **Cloud Infrastructure Security** (Monitor cloud security posture to prevent security and compliance risks) | ✔ | ✔ | ✔ |
| **XDR** (Extended detection and response) | | ✔ | ✔ |
| **MDR** (Managed Detection and 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



22-10-21 DS-EN (PC)

SOPHOS