SOPHOS

CLOUD READY

Sophos Central Server Protection for Linux

Linux systems are used for critical roles like web servers and internal file servers, and are increasingly targeted by attackers. In addition to being susceptible to Linux-based and cross-platform threats, unprotected Linux machines can also become distribution points for Windows, Mac, and Android malware. Sophos Central Server Protection protects a wide range of distributions running on-premises and in the cloud.

Highlights

- Effective malware detection
- Excellent performance with low impact
- Container aware
- Malicious traffic detection
- Cloud Workload Discovery
- AWS Auto Scaling support
- Synchronized Security
- Easy to manage

Effective and secure

Detects malware using advanced heuristics and uses Live Protection to look up suspicious files in real time via SophosLabs. To prevent servers from becoming distribution points, Sophos also detects Windows, Mac, and Android malware on Linux machines.

Excellent performance, low impact

Tuned for performance, the threat protection agent keeps your Linux servers secure without slowing them down. To further optimize performance, exclusions can be configured using directories, file names, and wildcards.

Malicious traffic detection (MTD)

When outbound communication to a malicious command and control server is detected, potentially resulting from the Linux server having been compromised, Sophos Central Server Protection will alert you in the console.

Cloud Workload Discovery

Gain visibility of server workloads running on Amazon Web Services (AWS) and enforce a consistent security policy across both on-premises and cloud environments. Use of AWS APIs enables automated discovery of Linux server workloads across global regions and multiple cloud accounts, presented via an intuitive drilldown visualization.

AWS Auto Scaling support

Server Protection policies can be applied to AWS Auto Scaling Groups in Sophos Central, ensuring that newly-created instances have the correct policy applied automatically. Terminated instances are removed automatically from the console and useful AWS information is displayed (for example lifecycle state, AMI ID, region) for ease of management.

Synchronized Security Heartbeat™

Synchronized Security is a best-of-breed security system that enables your defences to be as coordinated as the attacks they protect against. Sophos Central Server Protection and Sophos XG Firewall work together to detect and prevent advanced attacks, enable automated incident response, and provide real-time insight and control, for simpler, better IT security management.

Easy to manage with Sophos Central

Managing your security from Sophos Central means you no longer need to deploy console servers just to get started. Sophos Central provides out-of-the-box policies for servers to ensure you get the most effective protection from day one.

Using a synchronized security management platform, you'll benefit from the management of Sophos Endpoint Protection, Intercept X, Encryption, Mobile, Wireless, Email, and Phish Threat, all from a single pane of glass.

Supported distributions	System requirements
Amazon Linux	x86_64
CentOS	Disk space: 1GB
Debian	Free Memory: 1GB
Oracle Enterprise Linux	English and Japanese
Red Hat Enterprise Linux	
SUSE Linux Enterprise	
Ubuntu	

For full details about supported distributions and system requirements, see https://community.sophos.com/kb/en-us/16819

Licensing

Sophos Central Server Protection is licensed per server/virtual machine. Entitlement is included within the following subscriptions:

- Central Server Protection (SVRC)
- Central Intercept X Advanced for Server (SVRCIXA)

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

2020-04-03 DS (PS)

SOPHOS