

ENDPOINT SECURITY

## Business challenge

The increasingly complex nature of today's fast-moving threats radically changes the criteria for defence across the network, placing demands on the system administrator for an integrated, multi-tier approach. Organisations face the daunting task of securing all operating systems, including Linux®, from viruses, spyware, Trojans and worms. Solutions need to be fast, reliable and able to adapt to the ever-changing Linux environment.

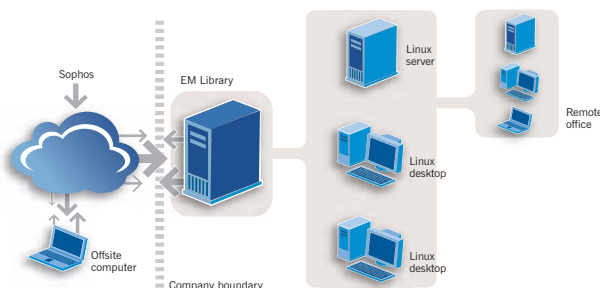
## The Sophos solution

Sophos Anti-Virus® is purpose-built for business and provides complex, multi-platform networks with reliable protection. Sophos Anti-Virus for Linux protects computers through on-access, scheduled and on-demand scanning using minimal network or system overhead. Decision Caching™ technology provides performance-enhanced on-access scans by scanning only files that have changed since last accessed. Award-winning technology in the Sophos virus detection engine ensures endpoint servers, desktops and laptops remain free from viruses, spyware, Trojans and worms.

A choice of a secure web GUI or comprehensive command line interface enables administrators to optimise anti-virus protection for their specific environments, while comprehensive messaging enables Sophos Anti-Virus to alert them to any virus incidents.

Designed to adapt to the ever-changing Linux environment, Sophos Anti-Virus integrates with the Linux kernel for improved performance, stability and support of multiple file system interfaces. Support for many Linux kernels, allows administrators to change, upgrade and compile kernels when required<sup>1</sup>.

The latest virus detection updates from SophosLabs™ are automatically downloaded from Sophos by EM Library in Windows environments or through cascading servers and web-based CIDs (central installation directories) in pure Linux environments, ensuring total protection at every potential entry point. Genotype™ virus detection technology enables Sophos Anti-Virus to protect against families of viruses even before specific detection is available.



*Sophos Anti-Virus: protecting Linux and other endpoint computers*

## Key benefits

- » Detects and disinfects viruses, spyware, Trojans and worms on access, on demand or at scheduled times.
- » Ensures superior scanning performance and reliability using a uniquely designed kernel interface module.
- » Cleans Windows viruses in a non-Windows environment.
- » Provides pre-compiled support for the widest range of Linux versions and kernels.
- » Supports customised Linux versions and kernels through automatic recompilations<sup>1</sup>.
- » Ensures total protection using "hot updating" technology.
- » Scans all file systems, not just Samba shares, through "scan everywhere" functionality.
- » Enables configuration and detailed logging via a command line interface or web GUI.
- » Alerts administrators of virus incidents.
- » Enables selective scanning through extensive file exclusions.
- » Supports Linux servers and desktops.
- » Updates automatically with the latest protection from SophosLabs™, a global network of threat analysis centres.
- » Includes unlimited 24-hour telephone, email and online support, 365 days a year.

## ENDPOINT SECURITY

### Technical details

#### Function

Protects Linux servers and desktops by detecting, reporting and disinfecting viruses, spyware, Trojans and worms.

#### Scanning

- Provides on-access, on-demand and scheduled scanning – using “at” or “cron” – of volumes, directories and individual files via a secure web GUI or command line interface.
- Decision Caching technology improves on-access scanning performance by intercepting and scanning only files that have changed since last accessed.

#### Management and configuration

A secure web GUI or command line interface provides administrators with central configuration and management of Sophos Anti-Virus on Linux computers.

#### Updating

Sophos Anti-Virus is kept up to date automatically:

- Using EM Library to distribute updates efficiently across a multi-platform network.
- Using cascading servers and web-based updating direct from Sophos in pure Linux environments.
- Direct from Sophos or the company website for offsite computers.

#### Anti-virus technologies

- A range of technologies, including Dynamic Code Analysis™, pattern matching, emulation and heuristics, automatically check for malicious code.
- Genotype detection technology proactively blocks families of viruses even before specific virus signatures are available.

#### Virus alerts

- Administrators are kept up to date with virus incidents via SMTP email.
- Alerts for remote computers are queued until they connect to the network.

#### Languages available

English and Japanese.

Sophos Anti-Virus is also available for a wide range of non-Linux platforms, from gateway to endpoint, including Windows, Macintosh, UNIX, NetWare, OpenVMS and OS/2. These solutions are described on separate datasheets.

To evaluate Sophos Anti-Virus for Linux, visit [www.sophos.com/products](http://www.sophos.com/products)

### System requirements

#### Distributions supported

##### On-access and on-demand scanning

- » Red Hat Linux 7.2/8.0/9.0
- » Red Hat Enterprise Linux ES/AS 2.1/3
- » Red Hat Enterprise Workstation 2.1/3
- » SUSE Linux 7.2/8.0
- » SUSE Linux Enterprise Server 8.0/9.0
- » SUSE Linux Professional 9.0/9.1/9.2/9.3
- » TurboLinux 8 Server, Enterprise Server 8, 10 Server

##### On-demand scanning only

- » TurboLinux 6 AS/7 on Intel
- » Red Hat Linux 5.1/5.2/6.0/6.1 on Intel
- » SUSE Linux 6/8 on Intel
- » Red Hat Linux 5.1/5.2 on Alpha

#### Hardware

Intel 32-bit hardware. This includes:

- » Single-processor systems
- » Multi-processor systems
- » Hyper-threaded processor systems

<sup>1</sup>Note: If you recompile Sophos Anti-Virus for Linux to support a Linux distribution unsupported by Sophos, or a customised Linux kernel, Sophos reserves the right not to provide support where any such recompilation (or customisation) has taken place. Sophos will use reasonable endeavours to provide first-line support. Should issues arise that require second-line support, or any other escalation process, Sophos cannot guarantee that such issues will be resolved.

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centres, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.