

OEM Live Protection

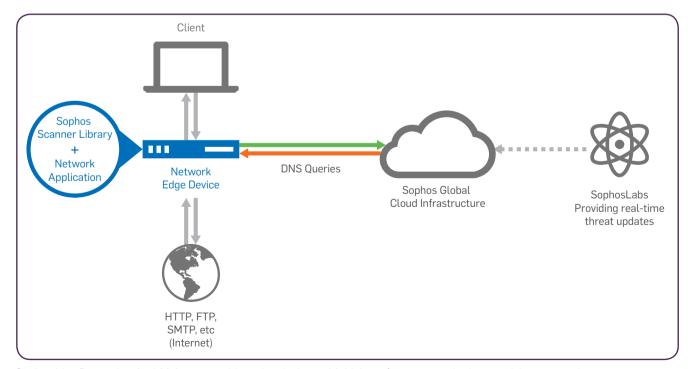
High-performance anti-malware for Network Edge Devices

Our Sophos Live Protection Anti-Malware is a high-performance anti-malware solution for UTMs, web appliances, routers and other network devices. It uses real-time information from SophosLabs, a global network of threat analysis centers. Using the power of cloud look-ups, SophosLabs delivers effective protection against threats for multiple types of traffic with minimal impact on system resources.

How does it work?

Sophos Live Protection Anti-Malware prevents users from visiting compromised websites and downloading or receiving malware.

- For HTTP, URI lookups are blocked when accessing known bad and compromised websites. Checksums are used to detect static malware downloads that are not caught by URL blocking
- For other supported protocols (FTP, SMTP, POP3, IMAP, IM), checksums detect static malware
- Furthermore, automatic and transparent look-up analysis provides even more protection. Most importantly, this is conducted behind the scenes, so users are not disrupted



Sophos Live Protection Anti-Malware provides edge devices with high performance and robust antivirus protection.

The core components of Sophos Live Protection Anti-Malware

URI lookups	Stops vast majority of threats
Checksum detection	Stops malware distributed through email attachments, IM and other protocols
Cloud lookup	Better protection with real time access to the SophosLabs malware database
Easily updateable scanning logic	Reduces the need for code changes and firmware updates

High performance

- Uses cloud look-ups for URIs and checksums
- Compact and efficient scanner library
- Features a data-trickling function allowing the main application to push file chunks as they become available. The scanner then returns control to the main application as soon as possible
- Increases performance using hardware SHA-1 acceleration if available on the system
- Intelligent checksumming implemented in several stages, minimizing CPU overhead
- Dynamically chooses the fastest server manual setup not required
- Several configuration options available for tweaking Live Protection library performance (e.g., caching and retry queries)

Low system resource and maintenance requirements

- Flexible memory requirements for data (i.e. amount of memory required dependent) on number of concurrent scans
- Lightweight scanner library minimizes memory requirements
- Scanner logic updateable with data updates reduces need for firmware refreshes refine policies fast without impacting user productivity

Industry-leading 24/7/365 support

- In-house expertise
- Dedicated technical account managers to help you integrate our technology and ensure customer satisfaction
- Specialized OEM support delivered by engineers that speak your language and are available 24/7/365 by email or telephone
- Around-the-clock analysis of the global threat landscape through the SophosLabs

Easy to implement

- Detailed integration documentation and evaluation toolkit provided
- A worldwide network of servers maintained by Sophos respond to URI and file queries
- The main application conducts actual network transmission using Sophos Live Protection
- Simple C-based programming interface
- Easy malware description integration by providing links to the descriptions of blocked threats

Platforms Supported

Operation Systems

- FreeBSD 7.0+ (32-bit)
- Linux
- Other OSs can be supported on agreement

Memory

- Flash or Disk usage: 120KB (dynamically linked, 32-bit Intel x86) and 720KB (statically linked, 32-bit Intel x86)
- RAM: variable depending on number of simultaneous searches (8MB for 2,000 searches)

Evaluation application (harness)

- OS: FreeBSD 7.0+ (32-bit); other OSs can be supported on agreement
- Memory: 2-MB RAM, 1-MB hard disk or flash space

To request an OEM product evaluation

visit sophos.com/oem

OEM Worldwide Sales Toll Free: 1-866-866-2802 Email: oem.sales@sophos.com

