SOPHOS
Security made simple.

Sophos Antivirus SDK

Integrate the award-winning Sophos anti-malware engine into your solution

Sophos Antivirus SDK enables software vendors, hardware vendors and service providers to easily integrate the Sophos anti-malware engine into their own applications and solutions. Used by many of the world's leading IT companies, the comprehensive C/C++ API and alternative interfaces allow for seamless integration and detection of malware and potentially unwanted applications (PUAs).

Key Benefits

- Deployed to over 100 million devices worldwide
- Native C/C++ COMbased interface
- Complete SDK to support OEM and third party use cases
- Provides protection against known and unknown threats
- Efficient memory usage with multi-threading options available
- Support for 32 and 64 bit platforms
- Proactive technologies included to guard against zero-day threats
- Uses the cloud to improve threat response, reduce false positives and provide up to the minute protection

Proactive malware detection

Sophos Behavioral Genotype Protection provides immediate zero-day protection from more than 80% of emerging threats. Our behavioral rule sets are constantly validated against an extensive library of malware samples and legitimate applications, ensuring accurate detection and reducing false positives.

Optimized product performance

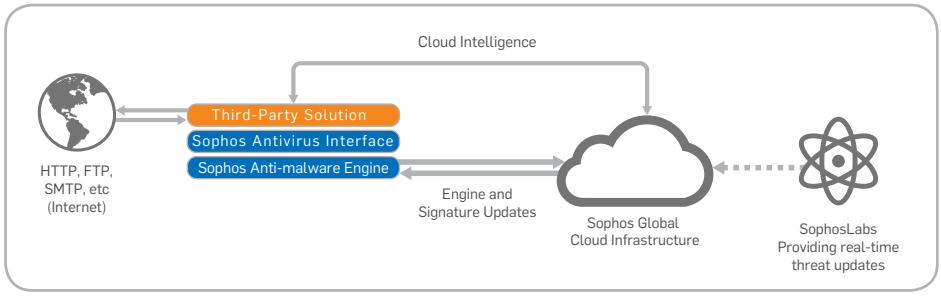
It improves your resource usage by requiring only one copy of the malware information database to service all requests. It doesn't require frequent loading and re-initialization. Also you'll get continuity of service using our "hot updating" mechanism. This allows for loading of new data in parallel with the previous data.

Industry-leading 24/7/365 support

Our in-house expertise helps you integrate our technology while ensuring your customers satisfaction. You'll get specialized OEM support delivered by engineers that speak your language and are available 24/7/365 by email or telephone.

Easy integration and backwards compatibility

It allows integration with Windows and Unix/Linux platforms, including the most commonly used open source solutions. Our native C/C++ COM-based interface is available across all versions for cross-platform consistency. Once you integrate using Sophos Antivirus SDK, your solution is compatible with all future releases of the Sophos anti-malware engine. We'll get you started with SDK Integration resources, including documentation and sample applications. The SDK is also available with additional detection capabilities for PUAs and suspicious files.



Sophos Antivirus SDK provides complete malware protection for third-party solutions.

Sophos Live Protection

A feature that enables real-time lookups to detect malicious attacks faster and with added accuracy.

- **Faster threat response with 'in-the-cloud' checking** Uses real-time information on the latest threats from SophosLabs; enabling products to provide up-to-the-minute detection.
- **Increased accuracy with early stage detection** Helps thwart malicious code and evolved malware early; more accurate protection with an increased amount of detection data.
- **Effective mitigation of false-positives** Remediates false positive entries with cloud information; whitelisting in the cloud prevents erroneous detection of system files as malicious.
- **Telemetry data helps SophosLabs improve detections** Data from Live Protection allows SophosLabs to improve existing detections, find new malware patterns, and target emerging threat vectors.

Context Web (CXWeb)

CXWeb provides effective defense against zero-day web-based attacks. The detection strategy is based on a combination of content analysis (file properties) and source context (URL characteristics).

The technology is particularly effective against exploit kits and is recommended for all 'web proxy' solutions.

Context Mail (CXMail)

CXMail is designed to be highly effective against zero-day malware attacks that are spread via emails.

The technology applies stricter rules aimed at active content that is delivered in email attachments and proactively identifies polymorphic malicious documents and executables.

The higher detection rate of CXMail is achieved by identifying strongly suspicious content that is not regularly associated with email communication.

True File Type (TFT)

TFT allows a client application to accurately detect the file type of a file passed to Sophos Antivirus SDK.

- File detection based on SophosLabs malware detection technology
- Maintained and supported by SophosLabs
- File types sorted into Group, Type, and Subtype allowing granular control over files
- File types mapped to specific threat levels based on potential risk

Technical Specifications

Interface options

Third-party applications can benefit from the full functionality of the Sophos anti-malware engine. Choose between:

- **Sophos Antivirus SDK**
  A C/C++ COM-based interface supplied as a Dynamic Link Library (DLL) on Windows and a shared library on UNIX & Linux.
- **Sophos Antivirus Dynamic Interface (SAV-DI)**
  A socket-based wrapper for the SDK that runs outof process as a service on Windows and a daemon on Unix/Linux. You can call SAV-DI from multiple high-level programming languages including Perl, Python, Java, C#, .NET and VBScript.

Supported platforms

- Windows
- Linux
- Unix
- Mac

For more information

Please visit Sophos.com/oem

OEM Contact
Email: oem.sales@sophos.com

2016-09-19 DS-NA (PC)

SOPHOS