Sophos Anti-Malware SDK

Malware threats are constantly increasing in both volume and sophistication. These threats are designed to bypass traditional defenses, making it difficult for security vendors to detect and classify them effectively. The proliferation of cloud networks, SD-WAN, and remote work models have also given malware authors a larger attack surface to target. To effectively protect against these threats, Sophos offers a leading SDK, merging multiple technologies and processes that allow cybersecurity vendors the ability to enhance their solutions.

Malware protection leveraged by leading cybersecurity providers

Sophos' security technology defends against malware, zero-day attacks, and advanced persistent threats (APTs). It is used by security vendors in their appliances, endpoints, and cloud infrastructure and is integrated throughout the Sophos product line as a core defense system. The technology is easy to integrate into both on-premises and cloud solutions.

Layered security technologies in a single engine

Sophos' anti-malware technology provides comprehensive multi-layered protection by combining Deep Learning models with signature-based detection and Behavioral Genotype. It utilizes telemetry and data from all of Sophos' products, including endpoint, network, and cloud security solutions, to deliver the broadest possible threat analysis. Additionally, the Sophos Anti-Malware SDK can be configured for web and email traffic and can be customized for specific use cases to enhance detection.

Modular and extensible through cloud enhancements

The Sophos SDK resides on-prem and can be enhanced by adding Sophos' cloud services. Unidentified or potentially harmful files can be sent to Global Reputation in the form of hashes, or for further analysis using Deep Learning models and dynamic analysis. The modular design of the Anti-Malware SDK enables OEM partners to extend its capabilities from cloud lookups to static and dynamic analysis.

Combining global telemetry, industry-leading threat hunting and rigorous AI

Enhanced by Sophos X-Ops, bringing together three teams of cybersecurity experts at Sophos: SophosLabs, Sophos SecOps, and SophosAI. It helps organizations better defend against constantly evolving and increasingly complex cyberattacks by leveraging each team's real-time, predictive, and thoroughly researched threat intelligence. The teams work together to provide stronger, more innovative protection, detection, and response capabilities.

Key Highlights

- Deployed to over 100 million devices worldwide
- Supports a wide range of OEM use cases
- Protects against known and unknown threats using SophosLabs threat intelligence and AI-driven detection technologies
- Efficient memory usage with multi-threading options
- Leverages cloud-assisted protection to improve threat response and reduce false positives

Power of Sophos X-Ops

- Unifies SophosLabs, SecOps (Managed Threat Response, Rapid Response, and Security Operations group), and SophosAI under one umbrella
- The joint task force model draws unique expertise from each team to deliver more innovative and faster protection
- Sophos X-Ops intelligence helps OEM partners contain modern threats like ransomware and zero-day malware early and neutralize the adversaries

SOPHOS

Key Features and Benefits to Security Vendors

Multi-layered
Combining multiple detection technologies offers unique benefits, allowing organizations to maximize their strengths. Machine learning-based detection is proactive in detecting zero-day threats, while Virus Detection Library (VDL) offers the fastest detection of known malware. Additionally, Global Reputation is used as a compensating control, further improving the true positive rate.

Machine Learning
Trained on an extensive dataset of malicious and benign Portable Executable (PE) files, Sophos' machine learning provides high-quality detections for known malware and early protection against zero-day threats.

Virus Definition Files
Signatures, created by Threat Researchers, offer the fastest, most reliable way of detecting security threats. They can also be used as a control to further improve true positive rates of machine learning technology.

Targeted Detection
Sophos Anti-Malware SDK enables OEM partners to fine-tune detection for specific traffic, enabling enhanced detection for web & email traffic and files.

Context Web (CXWeb) - Based on a combination of content analysis (file properties) and source context (URL characteristics), CXWeb provides an effective defense against zero-day web-based attacks.

Context Mail (CXMail) - Designed to be highly effective against zero-day malware attacks that spread via emails. Applies stricter rules aimed at dynamic content delivered in email attachments and proactively identifies polymorphic malicious documents and executables.

True File Type (TFT) - TFT allows a client application to accurately detect the file type of a file passed to Sophos Anti-Malware SDK.

Extensible Modules

The following cloud lookups can supplement Sophos Anti-Malware SDK with additional threat intelligence:

Global Reputation – Enables access to the latest SophosLabs reputation intelligence to detect threats with greater accuracy

Static Analysis – Enables quicker verdicts for malicious files using multiple machine learning models. This is particularly useful in convicting never-before-seen suspicious files

Dynamic Analysis (Sandboxing) –Helps further analyze suspicious files and zero-day malware with advanced behavior-based detection

Technical Specifications	**Sophos Antivirus SDK** A C/C++ COM-based interface is supplied as a Dynamic Link Library (DLL) on Windows and a shared library on UNIX & Linux. **Sophos Antivirus Dynamic Interface (SAV-DI)** Runs as a service or as a daemon; supports multiple high-level programming languages, including Perl, Python, Java, C#, .NET, and VBScript.
Engine Size	~100 MB
Supported Platforms and Architecture	x86, x64, and ARM64 coverage for Windows, Linux, and macOS

OEM Contact
Email: oem@sophos.com

For more information

Please visit Sophos.com/oem

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

© Copyright 2023. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2023-04-13 DS-EN (PS)

SOPHOS