

SOPHOS

Sophos Technology Licensing

Solutions Guide



OEM PARTNERING WITH SOPHOS

Welcome to the Sophos technology licensing solutions guide, which explains how you can profit from incorporating our industry-leading technologies into your own security products and services to provide round-the-clock protection from malware, unwanted applications, and spam.

We offer unique benefits to our partners, including:

- **Award-winning performance** – Our rapid response to emerging threats means we achieve the highest levels of customer satisfaction in the industry. Our ability to detect malware, defend against spam, and enforce email policy consistently places us higher than other vendors in independent rankings. We receive regular certification from testing bodies, such as ICSA Labs, West Coast Labs, and Virus Bulletin.
- **Simple, low-risk integration** – specially designed resources make it simple and straightforward to add our technology across a wide range of operating systems and network environments.
- **Dedicated support** – our technical support centers operate 24-hours a day, and our dedicated OEM support team will give you the consultancy and tools you need for successful integration.
- **Proven reliability** – No other security vendor offers the length and depth of experience, cross-threat knowledge, integrated solutions, performance, and support that Sophos does.

Sophos technology is already used in 30% of the security appliances in the market today and is integrated into a number of gateway and desktop software security solutions. It is licensed by more than seventy-five OEM, managed service provider, technology, and strategic alliance partners, including well-known brands such as Microsoft, Ironport (Cisco), Internet Security Systems (IBM), Mirapoint, Ciphertrust (Secure Computing), Network Appliance, EMC, and WebRoot.

We look forward to sharing our expertise with you and helping you discover the benefits of working with us.

To find out more about our current OEM partners and how to become one, please visit www.sophos.com/partners/oem.

CONTENTS

ABOUT SOPHOS	5
Cross-threat visibility and expertise	6
PROTECTING THE WEB, EMAIL, AND ENDPOINT	7
Combating blended threats	7
Industry-leading technologies	8
Genotype technology: zero-day threat protection	8
Behavioral Genotype Protection: pre-execution detection	8
INTEGRATION PRODUCTS AND SERVICES	10
SAV Interface (SAVI)	10
Integrating with SAV Interface	11
SAV Interface Software Developers Kit	11
SAV Dynamic Interface	11
Sophos IP Reputation Service	12
Integrating with Sophos IP Reputation Service	12
Sophos Anti-Spam Interface (SASI)	13
Integrating with SASI	13
Sophos PureMessage for UNIX	14
Integrating with Sophos PureMessage for UNIX	14
SOPHOS ALERT SERVICES	15
Sophos ZombieAlert	15
Sophos PhishAlert	15
24/7 SUPPORT	16
Integration support	16
Dedicated technical support	16

ABOUT SOPHOS

Sophos is a global company and world leader in IT security and control with headquarters in Boston, Massachusetts and Oxford, UK. With more than 20 years' experience, we offer complete protection and control to over 100 million users in 150 countries. SophosLabs™ – our global network of threat analysis centers – defends business, education and government organizations against known and unknown malware, spyware, intrusions, adware and unwanted applications, spam, and policy abuse, and provides comprehensive network access control (NAC).

Our products are engineered specifically for the IT professional and we focus exclusively on the needs of the enterprise market. We provide our solutions direct to customers, via resellers channels, and through OEM and technology partnerships. Through these collaborations and shared resources, through our rapid response to emerging threats, and through our award-winning technology, we ensure that we continue to bring new, comprehensive, security solutions to the marketplace.

SOPHOSLABS

In licensing Sophos technology, OEM and technology partners have access to the industry-leading threat detection capabilities delivered by SophosLabs.

Cross-threat visibility and expertise

SophosLabs™ is the industry's only research group with a truly integrated understanding of today's rapidly evolving threat landscape, in which spammers, phishers, and spyware and virus writers are collaborating to create complex, blended threats.

Through its rare combination of cross-threat expertise, powerful integrated technologies, and access to data, SophosLabs is uniquely placed to provide consolidated protection to combat the increasing sophistication of today's financially motivated threats.

With labs strategically placed around the globe (Boston, Vancouver, Sydney, and Oxford), we have unprecedented insight into new malware, adware and exploits, and the 24-hour in-house analysis to provide unrivaled speed of response to new and emerging viruses, spam and web-based threats.

Every month, our experts and systems analyze tens of thousands of files. Every day they analyze millions of emails and billions of webpages. Our broad base of data sources includes spam traps in over 50 countries, third-party resources and search engines, global email traffic from customer deployments, and daily feeds of known malicious URLs.

This cross-threat visibility and expertise allows us to update, create, and deploy protection to you and your customers 24 hours a day, 365 days a year.

PROTECTING THE WEB, EMAIL AND ENDPOINT

Because of the unique way in which our labs operate, Sophos is able to provide complete protection – at the web and email gateways and at the endpoint. Competing vendors who have only anti-malware facilities rather than fully integrated research labs, have to rely on their partners for the web and spam threat data, which adds risk and delay to providing protection. Since spam campaigns now exist for only a couple of hours or even minutes before mutating, it is possible that the campaign will have come and gone by the time the security vendor finds out about it.

Our knowledge and experience enable you to offer your customers the unique benefits of:

- Integrated expertise for fast response and rapid detection, regardless of the methods being used by the threat to spread.
- Leading technologies providing proactive protection against zero-day threats and suspicious behavior.

Combating blended threats

The integrated research and analysis in SophosLabs ensure that our products and those of our OEM partners will block even the most complex of today's threats – no matter how complicated their spreading methods. A typical scenario for a new threat is:

- 1 A malicious spam email arrives at a Sophos spam trap, linking to a malicious webpage, such as a fake ecard greeting.
- 2 SophosLabs analyzes the email, following the URL link to a drive-by downloadable Trojan.
- 3 SophosLabs extracts the spam identities and URL, and:
 - adds the information to our anti-spam detection data.
 - adds the URL to our web-threat database.
 - adds the Trojan to our virus database.
- 4 The characteristics of the malware are extracted and used to create proactive protection.
- 5 Updated protection is automatically deployed to all Sophos customers at each of the stages.
- 6 SophosLabs continues to monitor the webpage for new variations of the threat and automatically adds protection for any that are found.

Industry-leading technologies

SophosLabs combines a range of highly tuned techniques and technology to combat malware and spam. Traditional signature-based detection is significantly enhanced by Sophos Genotype® technology and Sophos Behavioral Genotype Protection to deliver zero-day, pre-execution protection from malware. Sophos Genotype® technology combines with content scanning, obfuscation detection, sender reputation filtering, URI analysis and other techniques to block spam and malicious websites.

Genotype technology: zero-day threat protection

Genotype technology protects businesses by delivering preemptive generic protection against threats before they emerge. Delivering protection at the desktop, laptop, server and gateway, Genotype technology is incorporated in the Sophos virus detection engine and anti-spam engine and works by detecting new variants of existing families of viruses and spam campaigns. Our Genotype database contains terabytes of malicious and suspicious behavior data.

Genotype malware detection

Writers of viruses and other malware regularly reuse the majority of original virus code. Even if new malicious functionality has been added, the new virus remains similar to the original threat and is part of the same family. The similarities can be considered “genes” and detecting the presence of these genes in other files is evidence that those files are also malicious. Non-malicious files will not share the same combination of genes and so false positives are avoided.

Genotype spam detection

A single spam campaign can often use a variety of sending IP addresses, URLs, randomized content, and other attributes in order to attempt to avoid detection. SophosLabs analysts use Genotype technology to identify specific genes that remain consistent throughout the campaign to accurately and proactively detect the campaign with a very low risk of false positives. Extracted genes are matched with genotypes of all known threats from a particular campaign using a finely tuned scoring system.

Behavioral Genotype Protection: pre-execution detection

Behavioral Genotype Protection builds on the proactive protection of Genotype technology to deliver the broader zero-day benefits of a Host Intrusion Prevention System (HIPS). Incorporated in the Sophos malware detection engine, it compares genes not just with those of known families of malware, but with those of known bad content and behavior more generally.

By identifying genes from all the malware it has ever collected, SophosLabs can identify the characteristics and combinations of genes that appear in malware. It compares this information with information about the genes that are seen in known good files, and in this way it minimizes the risk of incorrectly identifying a file as malicious when it is not.

There are several hundred behavioral characteristics common across malware.

Examples of these characteristics are:

- Using a packer (a compression tool that reduces the size of the executable)*
- Searching for publisher information
- Using a particular programming language
- Attempting to access the internet
- Containing certain strings
- Adding registry entries.

So a simple example of a gene might be as follows: if an application is packed, written in Visual Basic, accesses the internet, and contains references to banking websites, there is a very strong likelihood of it being a banking Trojan.

The advantages of Behavioral Genotype Protection over runtime HIPS are:

- Malicious code is prevented from executing at all, whereas runtime HIPS can only interrupt code that has already partly executed.
- Because the analysis is performed before any code executes, it can be carried out at the email and web gateway as well as at the desktop.
- SophosLabs rapidly validates the rule sets against terabytes of legitimate code, eliminating false positives. By comparison, identifying false positives with runtime HIPS is a huge and practically impossible task.
- Scanning is performed within the Sophos malware detection engine, without requiring any additional software to be purchased, installed, run or managed.

*21 percent of all malware in SophosLabs' collection is packed, but only 1 in 100,000 clean files is.

INTEGRATION PRODUCTS AND SERVICES

Sophos offers a range of technologies that can be easily integrated into an OEM partner's and service provider's solutions:

- SAV Interface (SAVI)
- Sophos IP Reputation Service
- Sophos Anti-Spam Interface (SASI)
- PureMessage for UNIX

The following section provides a high-level overview of these technologies and the resources we provide to help you integrate them into your products and services.

SAV Interface

SAV Interface (Sophos Anti-Virus Interface) is the most widely licensed of Sophos's technology offerings. It lets you integrate high-speed detection of malware and unwanted applications into your own industry-standard firewalls, email and web filtering products, anti-spyware products, and other security solutions. It is also used to scan files being stored on network storage servers, and to scan Instant Messaging.

SAV Interface enables you to provide your customers with complete protection via one solution and supports Windows 2000+, various Linux and UNIX distributions, and more. For full details of platforms supported, please visit www.sophos.com/savi/sysreqs.html.

Easy integration

- A single scan protects against viruses, spyware, worms, Trojans, adware and other potentially unwanted applications (PUAs).
- SAV Interface is backwards compatible, so once integrated, your product will be compatible with all future releases of the scanning engine.

Great protection

- Sophos receives regular recognition for its spyware and virus detection from West Coast Labs, Virus Bulletin, and ICSA Labs.
- Sophos Genotype[®] virus detection technology proactively blocks families of viruses, and Behavioral Genotype Protection automatically guards against zero-day threats by analyzing the behavior of the code before it executes.

High performance

- SAV Interface ensures minimum impact on system performance with fast scanning speeds and the smallest (5KB) updates in the industry.
- Single-engine scanning eliminates excessive memory usage by using a single, multi-threaded copy of the virus detection engine to process all requests.

Integrating with SAV Interface

SAV Interface integration resources give you all the information you will need to build an application with integrated virus protection. Integration resources include:

- SAV Interface Software Developers Kit (SDK)
- SAV Dynamic Interface (SAVDI).

Both SAV Interface SDK and SAVDI are provided free of charge to OEM partners. They are available from www.sophos.com/partners/oem (credentials required). Note that the virus detection engine itself is downloaded separately.

SAV Interface SDK

Most OEM partners use the SAV Interface SDK to assist with their integration. It is designed for partners who want to use SAV Interface as a low-level application programming interface in order to have the fullest functionality and most efficient performance.

- SAV Interface SDK uses COM-based interfaces that can be used with C++ syntax or C syntax and benefit from native Windows support.
- User manuals provide information about initialization, use and configuration of SAV Interface and detail all the functions of the SAV Interface interfaces together with the syntax for calling them, parameters and return values.
- SAV Interface headers and demo applications are provided in C and C++.

SAVDI

SAV Dynamic Interface (SAVDI) provides an easy-to-integrate, general-purpose interface to the Sophos detection engine. It enables programs written in any language to scan files and data for malware and is particularly popular with ISPs/ASPs running in a .NET environment.

- SAVDI runs as a daemon (or service in Windows terminology) therefore running as a background process to efficiently scan for malware as required.
- A network mode allows the malware scanner to run on a separate system so threats can be scanned using either a remote or local SAVDI.
- Many languages or programming environments are supported, including Perl, Python, Java, C#, .NET, and VBScript.
- Updates to virus data, SAV Interface, and engine libraries can be carried out without a break in service.
- Communication is via configurable TCP ports, Named Pipes on Windows and UNIX domain sockets.
- Supporting documentation details available configuration options and sample programs which can be compiled and run on any supported platform.

Sophos IP Reputation Service

Sophos's IP Reputation Service allows security/UTM solutions to accurately and efficiently drop connections from known bad IP addresses, greatly increasing overall throughput and capacity.

Easy integration

- Sophos IP Reputation Service uses a simple, industry-standard DNSBL (Domain Name System Block Lists) integration
- It can be easily deployed in most MTA (Mail Transfer Agent) and platform environments

Great protection

- Sophos IP Reputation Service eliminates up to 80% of spam at the connection level with virtually no false positives.

High performance

- Sophos IP Reputation Service uses a very efficient, DNS-based query to compare a connection's sending IP with Sophos's IP Block List to determine whether that connection should be rejected or accepted.
- It can be used alone to get rid of the bulk of spam, or it can be used in conjunction with SASI's content-level anti-spam checks to catch more than 98% of spam.

Integrating with Sophos IP Reputation Service

IP reputation capabilities are included with PureMessage for UNIX and SASI (see the following two pages). However, IP Reputation can also be purchased as a separate service (credentials required).

- Sophos provides instructions and details on how to point to the relevant DNSBL queries on our servers.

Sophos Anti-Spam Interface (SASI)

Sophos Anti-Spam Interface (SASI) lets you integrate award-winning anti-spam protection into your own industry-standard software, appliances, or services, blocking spam and protecting your customers from phishing attacks. It integrates easily with email security and management solutions as well as those offering broader gateway capabilities, such as web/IM filtering or firewall functionality.

Easy integration

- Straightforward integration enables partners to pass email messages to SASI and obtain a spam/not-spam verdict.

Great protection

- Sophos anti-spam protection has achieved the West Coast Labs Anti-Spam Premium Checkmark Certification and was independently tested by Veritest* where it achieved a 98.59% capture rate.
- SASI uses a variety of anti-spam techniques including proactive Genotype technology, sender reputation checks (including identification of bots/zombies), call-to-action checks (e.g., URLs within messages), spam “identities” or checksums, image fingerprints, and header and content analysis.
- SophosLabs provides 24/7, real-time updates to spam rules ensuring consistent, accurate protection against spam and phishing attacks.

High performance

- SASI provides complete spam protection on its own, but for best performance we recommend deploying our IP Reputation Service at the connection level and SASI at the content inspection level.

Integrating with SASI

SASI integration resources give you all the information you will need to build an application with integrated spam protection (credentials required).

Integration resources include:

- SASI SDK, which includes the anti-spam engine

Both are downloaded together from an FTP site, and the SASI SDK is provided free of charge as part of the SASI license.

- SASI provides a C language API that developers can use to access the anti-spam engine.
- The SASI user manual, which is part of the SDK, provides information about engine initialization, passing a message to the engine for scanning, and accessing the result of the scan.

* Veritest Report, December 2005

Sophos PureMessage for UNIX

Sophos PureMessage for UNIX is ideal for environments where extensive email management capability is required, for example for managed service providers. It interfaces with all leading messaging solutions and enables complete email management across a variety of platforms and operating systems. PureMessage for UNIX is a complete email content security solution, providing anti-virus and other malware protection, anti-spam protection, and inbound and outbound email policy enforcement.

Easy integration

- PureMessage for UNIX works in conjunction with several mail transfer agents (MTAs), including sendmail, Postfix, and JSMS. For full details of MTAs and versions supported, visit www.sophos.com/unix/sysreqs.html.
- A powerful set of web-based configuration and reporting tools, automated updates, centralized administration, and scheduled jobs minimize the amount of administration required to manage gateway security for your customers.
- Access to configuration settings, quarantine management, and reporting can be delegated to your customers using a highly usable web-based interface. This can be fully segregated and customized for each customer even in a mutualized/multi-tenant deployment.

Great protection

- PureMessage effectively identifies more than 98% of spam and protects against email scams, including phishing attacks.
- Award-winning technology detects, disinfects or quarantines viruses, spyware, Trojans and worms in incoming and outgoing email.
- PureMessage incorporates a highly flexible policy environment to support complex security or regulatory compliance requirements.
- Real-time updates to spam rules and updated malware data as frequently as every five minutes enable 24/7 protection.

High performance

- The Sophos IP Block List effectively eliminates up to 80% of spam at the connection level, reducing scanning requirements and accelerating delivery of clean mail.

Integrating with Sophos PureMessage for UNIX

Sophos PureMessage for UNIX's flexible APIs and deployment options allow it to be integrated across a variety of platforms and into a wide variety of environments, including virtualized environments. Everything you need to integrate it into your solution is included in the download (credentials required).

- PureMessage can fit into various types of messaging infrastructure, directory services, and reporting systems.
- It includes multi-server management tools and flexible delegated administration configuration tools to help integration with provisioning systems.

SOPHOS ALERT SERVICES

In addition to the technologies described above, Sophos offers two alert services that are of particular value to the ISP/ASP/MSP market.

Sophos ZombieAlert

Sophos ZombieAlert™ Service provides you with an immediate warning if spammers have hijacked computers on your own or a customer's network to send spam or launch denial-of-service attacks.

ZombieAlert immediately emails you with detailed message samples and IP address information as soon as the threat is identified. You can then quickly identify, disinfect and protect compromised computers or alert your customer to do so.

Sophos PhishAlert

Sophos PhishAlert™ Service protects primary targets of phishing attacks, such as banks. It provides fast, near real-time alerts of phishing campaigns so you can take steps to shut down the imitation website and protect your customers' customers.

This service also protects against identity theft by providing information on hosts of phishing sites.

You or your customers receive two types of email from Sophos:

- Ongoing alerts that provide rapid notification of new attacks.
- Periodic reports that summarize overall phishing activity.

24/7 SUPPORT

Integration support

Our dedicated OEM support team provides you with the consultancy and tools you need to integrate our technology successfully and ensure customer satisfaction. We also provide transition assistance and skills transfer to ensure you achieve rapid, optimal integration of Sophos solutions. Our experts have successfully engaged with some of the most recognized organizations in the world to meet their specific requirements and develop complete endpoint and gateway security, maximizing their return on investment.

Dedicated technical support

The excellence of Sophos in-house support services sets us apart from our competitors. As a Sophos partner, you benefit from 24-hour support provided by a globally managed team every day of the year. You can contact our engineers for one-to-one support by email or telephone, or use our web-based support knowledgebase.

Our technical support organization operates from support centers across the world, providing the highest level of expertise, professionalism and customer service, around the clock.

To find out more about our OEM partners and how to become one, please visit www.sophos.com/partners/oem.

