

Sophos Anti-Virus Dynamic Interface (SAV-DI)

Providing your customers with malware protection locally or over the network

Sophos Antivirus Dynamic Interface (SAV-DI) is a general-purpose interface to the Sophos anti-malware engine. SAV-DI enables applications written in any language, on any system to scan files and data locally or over the network for viruses, Trojans, worms, spyware and adware.

Key Benefits

- ▶ Provides a general purpose interface to the Sophos anti-malware engine
- ▶ Allows file and data scanning for viruses, Trojans, worms, spyware and adware locally and over the network
- ▶ Provides multi-platform coverage (32 and 64 bits)
- ▶ Supports ICAP
- ▶ Proactive technologies guard against zero-day threats
- ▶ Includes 24/7/365 dedicated in-house OEM support for the duration of the license

Seamless integration

SAV-DI allows you to access to the Sophos anti-malware engine via a multitude of high-level programming languages, including Perl, Python, Java, C#, .NET and VBScript. Our dynamic interface integrates with the most commonly used open-source solutions. It supports multiple transport mechanisms (TCP ports, named pipes, UNIX domain sockets) and protocols (ICAP, SSSP and Sophie) in heterogeneous environments.

We also provide you with all of the necessary integration resources (documentation and sample applications) to get you started, at no extra charge.

Ease of administration

SAV-DI offers a single unified engine available on Linux, UNIX and recent versions of Windows. And since all of the virus signatures are cross-platform compatible, it reduces your administration overhead.

Through automatic virus signatures and engine library updates, we're able to deliver you and your customers effective, around-the-clock protection against viruses, Trojans, worms, spyware and adware with no interruption of service.

Superior malware detection technologies

The Sophos anti-malware engine increases detection rates by combining a number of detection technologies such as Dynamic Code Analysis, pattern matching, emulation and heuristics. Sophos Behavioral Genotype Protection—our most innovative technology—provides immediate zero-day protection from more than 80% of emerging threats. Our behavioral rule sets ensure accurate detection and reduce false positives by validating against an extensive library of malware samples and legitimate applications.

High Performance

SAV-DI improves your resource usage by using a single copy of the malware information database for all requests. You can run SAV-DI as a daemon, efficiently scanning for malware as needed, scanning twenty times faster compared with traditional command line scanners. Sophos Behavioral Genotype Protection allows us to significantly improve the scanning speed since the code doesn't need to be executed to determine whether a file is malicious or not.

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.

Platforms supported

- Windows
- FreeBSD 32/64 bit
- Linux 32/64 bit
- Solaris Sparc 32 bit

System requirements (including Scanning Engine)

- 150 MB disk space and 150 MB of free memory

To request an OEM product evaluation
visit sophos.com/oem

OEM Worldwide Sales
Email: oem.sales@sophos.com