SAVI - Flexible virus protection wherever it's needed

Richard Jacobs, Sophos Inc, USA

Part # tr00011j/971209

What is SAVI?

The **S**ophos **A**nti-**V**irus **I**nterface (SAVI) programme brings Sophos' world renowned virus protection to environments beyond the conventional desktop and file-server. The programme allows 3rd party software developers to integrate their applications with *Sophos Anti-Virus*. Typical applications include:

- Email monitoring
- WWW download monitoring
- FTP download monitoring
- Firewalls
- Backup applications

SAVI integrates with *Sophos Anti-Virus* running under Windows NT.

Calling into this sophisticated network oriented package, **SAVI** brings Sophos' 10 years of experience in the anti-virus field to developers working in other fields, maximizing performance and minimizing development costs.

Why SAVI?

Until now 3rd party applications requiring automated virus protection have had to call command line versions of virus scanners. *Sophos Anti-Virus* has always included, and continues to include, a command line interface for this, and other, purposes. However there are a number of limitations to command line of operation:

Virus database initialization

Command line virus scanners must re-initialize every time a file needs to be swept. This can take several seconds. This delay is not noticeable when checking a whole disk, but becomes a major overhead when checking a single file, which typically takes a fraction of a second. There is an additional overhead introduced every time that Windows NT has to start a new command prompt session, in order to call the scanner.

With **SAVI**, the virus database is initialized once at startup and subsequent communication is routed directly into the **SAVI** Dynamic Link Library (DLL), **no** command prompts are needed. *Sophos Anti-Virus* is then able to react instantly to individual requests to sweep files, without further initialization. Performance improvements typically exceed 10 fold when compared to command line virus scanners. (30 fold improvements are possible, depending on the 3rd party application)

Memory requirements

Each time a command line scanner is initialized, it reserves memory for itself. With over 12,000 viruses currently identified, virus engines typically require more than 1Mbyte of memory. Email monitors, and more significantly WWW monitors, which operate at a company's Internet gateway, may process hundreds of requests simultaneously. This will not only deny memory to other applications, but may dramatically affect Internet access speed as Windows NT is overloaded.

SAVI eliminates memory constraints by using a single multi-threading copy of the virus database to process all requests.

SAVI is an integral part of Sophos' main Windows NT, service based, GUI application. This ensures that the functionality provided through **SAVI** exactly matches that available to other *Sophos Anti-Virus* users.

SAVI Compliance

Integralis MIMEsweeper

MIMEsweeper is a centralized Internet/Intranet content monitoring system. Specifically designed to monitor email and WWW access, MIMEsweeper provides company wide protection against a range of threats, including:

- Virus protection **- through Sophos'** SAVI **interface**

- Junk email
- Unauthorized transmission of confidential information
- Transmission of inappropriate information

MIMEsweeper consists of 2 modules:

MAILsweeper: Available for SMTP (Internet mail), Lotus cc:Mail, Novell GroupWise and Lotus Notes. In all cases traffic is routed through MIMEsweeper to ensure that it monitors both email content and attachments.

WEBsweeper: Monitors WWW downloads for a complete organization, acting as a caching Web proxy server

MIMEsweeper analyzes data and attachments in email and WWW downloads. Once it has identified attachments, MIMEsweeper uses a system of "Validators" to check the various components identified. The VALSWEEP validator, developed jointly by Sophos and Integralis, uses the **SAVI** interface to communicate with *Sophos Anti-Virus* and provide high speed virus detection. Infected items can then be quarantined and logged by MIMEsweeper, preventing any further infection.

An OPSEC compliant version of MIMEsweeper, allowing integration with Check Point's FireWall-1 product is also available. Through the **SAVI** interface MIMEsweeper for FireWall-1 allows *Sophos Anti-Virus* to virus check all traffic through the firewall, including HTTP, SMTP and FTP protocols, with minimal performance impact.