
PROTECT YOUR NETWORK PERIMETER FROM THE WIDEST VARIETY OF VIRUS THREATS.

# Sophos Anti-Virus

## A FULLY INTEGRATED LAYER OF VIRUS PROTECTION ON IRONPORT EMAIL SECURITY APPLIANCES

### OVERVIEW

The scale and complexity of recent virus attacks have highlighted the importance of a robust, secure messaging platform to protect your network perimeter. The traditional approach of being able to identify and block known viruses is no longer enough.

In an era of greater virus attacks which are more complex, morph more quickly, and spread faster, anti-virus engines strain to protect customer networks appropriately. With the increased damage complex viruses cause, the cleanup costs for infected PCs continues to rise.

To combat this evolving threat, IronPort® offers the most comprehensive multi-scan, multi-vendor anti-virus solution:

- *IronPort Virus Outbreak Filters*™ – a critical first layer of preventive defense against new outbreaks, detecting and stopping viruses before any other technology.
- Integrated Sophos anti-virus engine – enabling traditional virus detection methods to ensure protection against even the most complex virus attacks.

The combination of proprietary IronPort technology and virus filtering from Sophos provides maximum virus security, without compromising scalability.

### FEATURES

With the highest performance virus scanning technology in the industry, Sophos anti-virus technology is a fully integrated layer of virus protection on the *IronPort C-Series*™ and *IronPort X-Series*™ email security appliances.

#### MULTIPLE DETECTION METHODS: PROTECTION AGAINST THE WIDEST VARIETY OF VIRUSES

During the scanning process, the Sophos anti-virus engine analyzes each incoming message and file, identifies the type and then applies the relevant technique to ensure highest throughput and efficacy. The Sophos anti-virus engine employs multiple detection methods, such as:

**Pattern Matching** can identify a virus by a specific code sequence or for code sequences known to be present within a virus. In doing so, the patterns are created to ensure that the engine catches not only the original virus but derivatives within the same virus family.

**Emulation technology** is included to detect polymorphic viruses and an online decompressor to scan multi-layer attachments. The robust engine supports multiple scanning modes to optimize performance.

**Advanced heuristic techniques,** based on behavioral genotype protection, are utilized by the engine to ensure that variants of viruses are caught with minimal information available about virus code patterns.

## FEATURES (CONTINUED)

### MULTIPLE OPTIONS FOR VIRUS HANDLING

**Administrators have multiple options** to handle virus infected messages. As viruses evolve, new strains of attacks try to bypass anti-virus protection by concealing viruses within password protected files or mal-formed messages. The IronPort solution detects potentially dangerous messages, giving the administrator full control over how these messages are handled by the system.

**The fully integrated Virus Quarantine** provides additional options to customers to determine what actions to take on viral messages along with end-user notification options.

**The unparalleled performance** of IronPort's email security appliances protects your email infrastructure from being overwhelmed by large-scale virus outbreaks and ensures that your mission critical email will continue to be accepted.

### ONLY SIGNATURE-BASED GATEWAY ANTI-VIRUS SOLUTION INTEGRATED WITH A PREVENTIVE ANTI-VIRUS SOLUTION

**Prevention and protection** are provided by *IronPort Virus Outbreak Filters*. During any virus outbreak, there is invariably a period of time between virus detection and when the actual anti-virus identity file is deployed. During this period, administrators can utilize *IronPort Virus Outbreak Filters* technology to identify and quarantine viruses based on known patterns and delete or archive the messages until new identity files can be updated. This innovative, preventive anti-virus solution is fully integrated with the Sophos anti-virus engine and has the ability to rescan messages automatically when there are new signature updates during an outbreak.

## BENEFITS

**IronPort and Sophos – Better Together** IronPort combines Sophos' anti-virus technology with *IronPort Virus Outbreak Filters* – resulting in even better virus prevention and protection, while maintaining near zero false positive rates.

**Highest Efficacy** Sophos is widely regarded within the industry as having the fastest performing and most accurate virus scanner available. Sophos was awarded the VB 100% award in the April 2007 edition of Virus Bulletin. This is the 37th time Sophos Anti-Virus has won a VB 100% award, confirming its position as one of the most powerful and accurate virus protection products available.

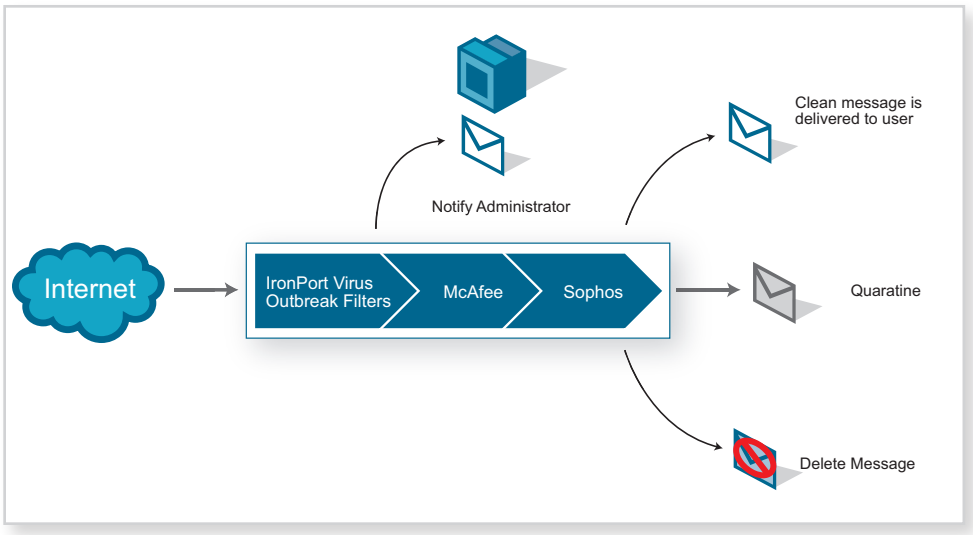
Virus Bulletin tested 16 different anti-virus products for their detection rates, lack of false alarms, and speed of scanning. Sophos successfully detected all of the in the wild, macro and polymorphic viruses (100 percent detection rate) with no false alarms.

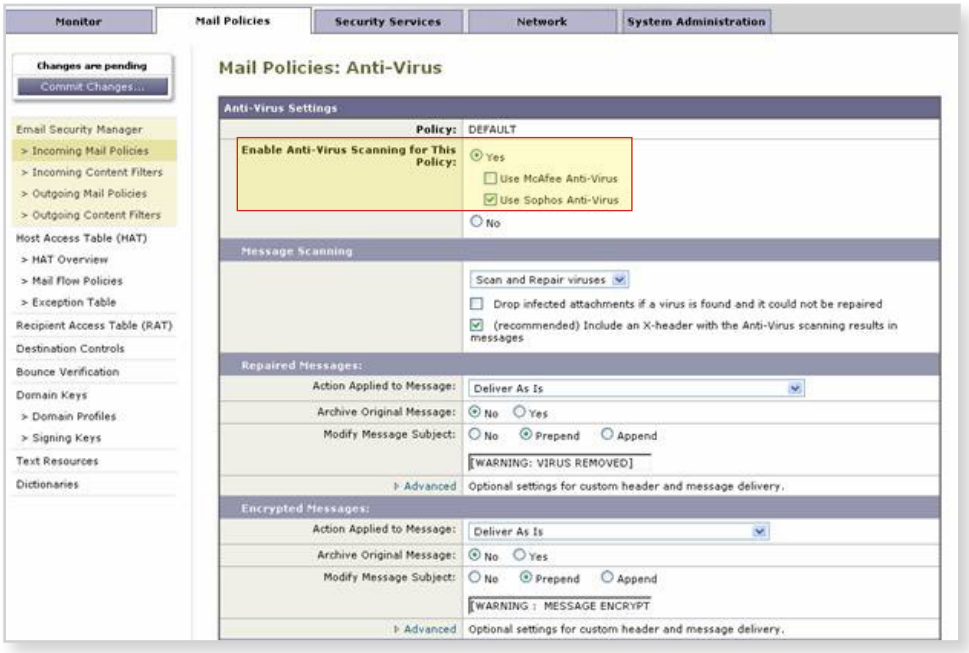
**Lower TCO with an Integrated Gateway Solution** With integrated management and deployment within the appliances, the solution offers ease of management with automatic updates and "set and forget" policies to address any customer specific requirements. Additionally, performing virus filtering at the gateway significantly reduces the resources needed at the groupware servers and the bandwidth requirements within the network.

FIGURE 1.

## FLEXIBLE AND INTUITIVE INTERFACE FOR EASE OF MANAGEMENT

IronPort email security appliances with Sophos anti-virus provide multiple layers of defense against potential viruses.



## SUMMARY

### MULTI-LAYERED SECURITY WITH IRONPORT AND SOPHOS

With the growth in number and complexity of viruses, it is critical that customers protect their networks with solutions that provide coverage against the widest variety of virus threats.

IronPort's anti-virus offerings (*IronPort Virus Outbreak Filters* and Sophos Anti-Virus) provide a multi-layered, multi-vendor approach to virus filtering – by offering a high performance virus scanning solution, integrated at the gateway.

With IronPort's proprietary *AsyncOS*™ operating system, the *IronPort C-Series* and *IronPort X-Series* email security appliances can process hundreds of messages per second. Whereas, traditional MTAs can only handle 10 to 20 messages per second. The unparalleled performance of IronPort's email security appliances protects your email infrastructure from being overwhelmed by large-scale virus outbreaks and ensures that your mission critical email will continue to be accepted.

## CONTACT US

### HOW TO GET STARTED WITH IRONPORT

IronPort sales representatives, channel partners, and support engineers are ready to help you evaluate how IronPort products can make your email infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from IronPort's industry leading products, please call 650-989-6530 or visit us on the Web at www.ironport.com/leader

**IronPort Systems, Inc.**
950 Elm Avenue, San Bruno, CA 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use — providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

SOPHOS
05/07
DOC RELEASE