

Sophos for Marshal

Spyware, viruses, worms, Trojans, adware and other unwanted or unauthorized applications are not just an email problem. They also infiltrate networks via web browsing. That explains why today's organizations are looking for integrated antivirus, anti-spyware, anti-spam and URL filtering solutions to protect against internet threats. It has become clear that combined detection techniques are essential today.

KEY BENEFITS

- Administrators can be notified instantly by email when a virus has been detected and put into quarantine or blocked
- The system allows administrators to monitor email and web traffic in realtime and check for known and unknown threats, including viruses, Trojans, worms, spyware, adware and potentially unwanted applications (PUAs)* that may have been detected and put into quarantine
- Incoming and outgoing emails and files from the Internet are checked for viruses, Trojans, worms, spyware, adware and potentially unwanted applications (PUAs)* in one scan reducing the impact on end-user productivity
- Malware is detected in compressed email attachments including recursive archives in the M86 MailMarshal product
- Latest protection is provided with automatic rapid updates from the global network of SophosLabs through M86's secured infrastructure on a 24x7x365 basis

THE BUSINESS ISSUE

The 21st century has seen a rapid acceleration in the evolution of new threats to organizations, both in the velocity of change and the increased malice of intent. Five years ago most threats were viruses and worms designed primarily to disrupt networks and crash computers. In the last two years, there has been a significant change in motivation, and therefore method, towards deliberate, focused attacks, designed specifically to make money for the perpetrators.

Productivity is being increasingly compromised by unmanaged web browsing. According to internet management software firm Burstek, approximately 8 percent of the websites visited are assessed as posing potential legal liability to employers, such as sites that offer pornography or gambling. Gartner has stated that 'over 70% of cyber attacks occur at the web (or website) application layer", and WhiteHat security has found that 8 out of 10 websites currently have serious vulnerabilities.

Likewise, emails has become a major liability and with inboxes being overrun with more and more unwanted email that threatens business productivity, regulatory compliance, and network security, organizations are having to look at what is being mailed in, out and around the network at the gateway and at the mail server.

Organizations are facing a growing number of leaks of confidential data, proprietary information, or intellectual property by their employees. Data stolen by an employee or a business partner ranks as the seventh greatest threat to enterprise security and, according to IDC, the most costly incidents are those that are deliberate, malicious action.

THE SOLUTION

Sophos for Marshal is now fully integrated into M86 MailMarshal SMTP, M86 MailMarshal Exchange, and M86 WebMarshal. This combined solution addresses the security challenges by protecting organizations against infection and legal risk, while also meeting end users' demands for performance and accessibility.

M86 MailMarshal SMTP uses the Sophos for Marshal module to protect the email gateway against email borne threats. It detects, disinfects, deletes or quarantines viruses, spyware, Trojans and worms. The management system enables administrators to monitor realtime malware activity as well as create configurable management reports, highlighting trends and any areas of concern (number of detected viruses, number of viruses that were not deleted, for example). Virus reports can be easily exported for further analysis or inclusion into wider management reports.

Sophos for Marshal also integrates with M86 WebMarshal at the Internet Gateway level. The Sophos for Marshal module inspects and secures web traffic against viruses, spyware, Trojans, worms and other potentially unwanted applications (PUAs)*. Through M86 WebMarshal's solution, it prevents access to malicious websites, hidden malicious code and undesirable content.

INNOVATIVE TECHNOLOGIES

M86 MailMarshal and M86 WebMarshal now benefit through Sophos for Marshal from the latest Sophos engine update. This includes:

- A range of technologies, including Dynamic Code Analysis™, pattern matching, emulation and heuristics, that automatically check for malicious code
- Genotype virus-detection technology which proactively blocks families of viruses and Behaviour Genotype protection that protects against zero-day malware
- A built-in mechanism ensuring that emails or web files get properly scanned even during an update by using the "hot updating" technology

SOPHOS FOR MARSHAL SYSTEM REQUIREMENTS:

M86 MailMarshal SMTP	6.1.4.x or later
M86 MailMarshal Exchange	5.2.0.X or later
M86 WebMarshal	3.7.5.x or later

* (PUAs): The Sophos engine includes protection from a wide range of common adware and potentially unwanted applications (PUAs). PUA is a term used to describe applications that, while not malicious, are generally considered unsuitable for business networks. The major PUA classifications are non-malicious spyware, adware, dialers, hacking tools and remote administration tools.

Sources

1. Burstek release 2005 internet usage study
2. Marketscope for URL filtering 2006. Lawrence Orans and Arabella Hallawell. Gartner, Inc. March 2006
3. WhiteHat Security Risk report. April 2007.
<http://www.whitehatsec.com/home/resources/wp/whitepapers.html>
4. Worldwide information protection and control (IPC) 2007 - 2011 forecast and analysis: securing the world's new currency. Doc #206750.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Eilerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 03/28/10