

## Norman<sup>®</sup> Virus Control for Marshal

Norman Virus Control (NVC) is a specialty antivirus module that integrates seamlessly with M86 solutions such as M86 MailMarshal and M86 WebMarshal. When combined with M86 solutions, Norman provides real-time antivirus scanning of emails and Web files at the Internet gateway. Norman creates a critical layer of antivirus protection at the gateway and server level, preventing viruses from entering your organization before they can reach users' desktops.

### KEY BENEFITS

- Detects and blocks viruses at the Internet gateway before reaching your internal computer network.
- Protects users from opening virus-infected emails, by blocking the emails before they reach individual mailboxes.
- Prevents users from accidentally accessing virus infected Web sites or files by blocking downloads in realtime.
- Provides high-speed virus scanning via multi-threaded message unpacking design.
- Features Norman's innovative new SandBox technology to identify potentially harmful files based on behavior. Provides greater virus detection, particularly against new viruses never seen before.
- Controls viruses in a total policy-based framework. You can choose what happens when viruses are detected. They can be quarantined for investigation or automatically deleted. You can also send notification messages to the administrator or email sender, informing them of the detected virus. Essentially any policy-related measures that you wish to take regarding viruses are possible with M86 MailMarshal and M86 WebMarshal. (Options for email and Web scanning differ.)
- Creates detailed virus incident reports that clearly demonstrate Return on Investment for your staff and executive management. You know when and where a virus was detected, how many viruses have been blocked, and what types of viruses you are blocking.
- Shows real-time monitoring of viruses quarantined in the M86 MailMarshal Today page.
- Provides 24x7x365, always-on virus protection. Users cannot turn off virus protection.
- Scans both incoming and outgoing email. Scans both downloaded and uploaded files to and from the Web.

### THE BUSINESS ISSUE

Email and the Internet are vital business tools, allowing your organization to communicate and access information efficiently. However, they also present vulnerable entry points for viruses and malicious code into your organization, diminishing the benefits that email and the Internet were intended to provide.

The 2006 CSI/FBI Computer Crime and Security Survey reported that 65% of the 615 companies surveyed suffered significant financial losses as a result of virus infection during the year. The average reported cost of these virus infections was US \$69, 125 per company. Other industry experts have estimated that as many as 80% of the world's computers are infected with some form of malicious code, such as spyware. Managing virus security risk in a corporate environment can be very difficult. Users bring all manner of external devices into the office to connect to their computers.

They download unknown files and applications from the Internet. They connect their laptops to unsecured networks outside the office. They open email attachments sent to them by complete strangers. A layered approach to antivirus security incorporating user education, active desktop antivirus and "always on" gateway virus monitoring is fast becoming best practice.

### THE SOLUTION

With Norman Virus Control, you can apply antivirus from one of the world's leading antivirus providers to email and Internet activity before viruses reach the trusted, internal network.

M86 MailMarshal SMTP integrates Norman scanning at the email content inspection level. As messages are filtered for spam and other non-business content, M86 MailMarshal employs Norman to scan each message for viruses and malicious code. Scanning is essentially instant thanks to M86 MailMarshal's multi-threaded design and tight product integration. Infected emails are identified and quarantined. Notification messages can be automatically sent to IT staff, and detailed reports can be generated -- identifying how many and what viruses M86 MailMarshal has blocked over any given period.

Norman also works with M86 MailMarshal Exchange, providing real-time antivirus protection on inter-office Exchange email. M86 WebMarshal integrates Norman at the Web proxy level. Any files requested by users are virus scanned by Norman before they are passed to the user's browser. Users are informed in realtime of suspected virusinfected files and any offending files are automatically blocked. Reports are available detailing how many and what viruses M86 WebMarshal has blocked and what the offending URLs were.

## NORMAN SANDBOX TECHNOLOGY

Norman Virus Control now features Norman's innovative "SandBox" technology. Conventional antivirus solutions rely on signature files that are created when a new virus is discovered in the wild. This requires that the antivirus solution be regularly updated to be effective against the latest virus threats. If it is not, it will not recognize a new virus.

The Norman SandBox technology is designed to identify new viruses that have not been seen before. When a file is passed to Norman Virus Control for checking by M86 MailMarshal or M86 WebMarshal, it is first tested using the virus signature file to see if it is a known virus. If it's not found in the known virus list, it is passed on to the SandBox where the file is let loose to reveal its intentions. The SandBox is a simulated environment controlled by the Norman virus scanner; so, if it is a virus, it cannot actually do any harm.

The SandBox assesses the behavior of the file as it executes. If the file behaves suspiciously or exhibits virus-like qualities, it is classified as harmful. If the file is harmless, it is delivered to the application that requested the check. If it is harmful, it is placed in quarantine thus preventing the network from being infected. The Norman SandBox feature is not only effective against viruses but also spyware and other malicious content.

### NORMAN® VIRUS CONTROL FOR MARSHAL SYSTEM REQUIREMENTS:

- M86 MailMarshal SMTP** 6.2.x.x or later
- M86 MailMarshal Exchange** 5.0 or later
- M86 WebMarshal** 3.7.x.x or later

## 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](http://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  
Ellerslie, Auckland, 1051  
New Zealand  
Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720

Version 03/30/10