

Marshal EndPoint Security

Protect Data and Networks from Internal Security Threats

You've spent millions keeping your data safe from hackers outside the organization. But thanks to the popularity of small data storage devices such as USB flash drives, MP3 players and PDAs, it's now easier to steal data from the inside than it is to break in to your IT systems across the internet.

Marshal EndPoint Security helps protect your data, both on and off the network, by:

- Preventing the transfer of files to or from unauthorized portable devices
- Automatically encrypting data copied to approved devices
- Providing complete visibility of device and file accesses

MAINTAINING THE INTEGRITY OF THE NETWORK

Whether it's an opportunist taking documents to a competitor or a well-meaning employee copying an infected file to the network, leaving portable device use unchecked is an invitation to disaster.

Marshal EndPoint Security prevents the unwanted transfer of data to or from portable devices by automatically enforcing security policies based on a user's legitimate need to access specific device types. User access can be blocked, limited to read-only or left unrestricted according to the individual's security privileges and device type in use.

SECURING DATA IN TRANSIT

Nearly two-thirds of all USB drives are lost by their owners. Without the right protection, what's to stop that data ending up in the wrong hands?

Marshal EndPoint Security can automatically encrypt all data copied to authorized storage devices such as USB flash drives. Using the latest Blowfish and AES 256-bit ciphers, Marshal EndPoint Security ensures that even if data is lost in transit, it won't create a costly and embarrassing security breach.

TOTAL VISIBILITY

You can't manage security if you can't see what's being connected to the network, what files are being accessed and how the security policy is being applied.

Marshal EndPoint Security provides complete visibility of all user and administrator actions, recording everything from individual device connections to the most popular files read from or copied to portable devices. A full audit trail of administrator actions completes the range of forensics available.

Regardless of whether the device is connected locally or wirelessly, if the PC is on the corporate network or offline, Marshal EndPoint Security constantly manages device connections to ensure the integrity of your network is not compromised.

Through its combination of strong security and flexible management capabilities, Marshal EndPoint Security prevents both malicious and accidental security breaches, keeping data safe, both on and off the network.

Marshal EndPoint prevents the unwanted connection of all common device types



ADVANTAGES

Single-Screen Admin

All administration, including creating, modifying and deploying either corporatewide or personalized security policies can be done in Marshal EndPoint Security's singlescreen Policy Control Center. There is no need to repeatedly switch back and forth between multiple windows.

One-Click Deployment

Client agents can be deployed and updated across Active Directory and NT domains from within the Marshal EndPoint Security Control Center, without third-party software distribution tools.

Advanced Device Granularity

Marshal EndPoint Security can manage both entire device 'classes' as well as specific devices. Using the Policy Customizer, it is easy to create white lists of corporate approved devices.

Total Visibility

Marshal EndPoint Security automatically records device connections, file accesses and policy changes.

These forensics can be viewed directly from the main Control Center in tabular or in graphical form, or can be exported into CSV format.

Intuitive Processes and Wizards

Designed to work the way you want to, Marshal EndPoint Security features wizards which will help you create and deploy security policies faster than ever. Intuitive processes make changing permissions or updating policies an easy task for any authorized user without the need for specialist training.

Super-Strength Encryption

256-bit AES and Blowfish ciphers are the strongest available, ensuring that any data carried offsite is protected against misuse by unauthorized third parties. The choice of global or personal keys give maximum flexibility for security management.

User Notification

Marshal EndPoint Security's configurable dialogs help organizations ensure that employees are informed about security policies, reducing help desk calls and improving user acceptance.

Marshal EndPoint Security is shipped with a default installation of MDSE which is the recommended database. SQL is supported for customers who prefer this format.

SYSTEM REQUIREMENTS

Supported Clients	Microsoft Windows NT/2000/2003/XP
Policy Control Center	Microsoft Windows 2000/2003/XP Apache Web Server* or IIS Marshal EndPoint Security requires a domain-based Windows network.
Database (optional)	Marshal EndPoint Security is shipped with a default installation of MDSE which is the recommended database. SQL is supported for customers who prefer this format. * Shipped with product

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