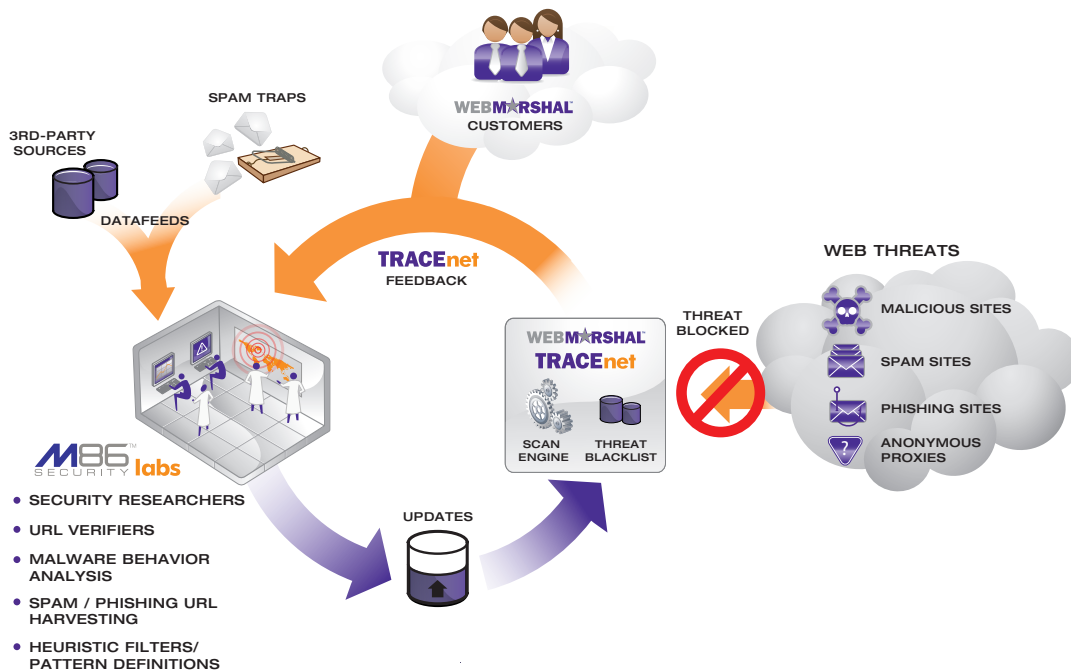


# M86 TRACEnet

## Web Threat Security Network for M86 WebMarshal

M86 TRACEnet is a unique Web security solution for M86 WebMarshal that provides protection against blended threats, malicious websites, spam and phishing websites, and anonymous proxy servers. It is a multi-faceted solution, integrating threat intelligence from a range of sources to provide unmatched versatility and comprehensive protection against new and emerging Web threats.



## OVERVIEW

Internet users today are faced with a multitude of security threats — viruses, Trojans, spyware, scareware, botnets, browser vulnerability exploits, social engineering scams, malicious Search Engine Optimization, cross-site scripting attacks, blended threats — the list can seem endless.

The Web 2.0 environment has created new opportunities for hackers and criminals to steal private information, infect computers with malware and ultimately derive a profit any way they can. These criminals are professional and employ an increasingly sophisticated range of tactics and blended attacks, which are nearly indistinguishable from legitimate Web content, to circumvent security solutions and scam even the most experienced Internet users.

In the past, websites were granted an inherent level of trust which was retained indefinitely. This approach to web security worked when the status of those trusted sites didn't change and hackers hosted malicious content on their own websites.

## KEY FEATURES

- Prevents access to malicious websites and blended threat sites linked to spam, botnets, phishing, and private proxy servers.
- Incorporates multiple technologies such as URL blacklists, real-time content scanning, heuristic filters and malware behavior analysis to identify and block threats on-the-fly.
- Employs constant threat updates from the M86 Security Labs, including URLs harvested from millions of spam and phishing emails captured every day.
- Utilizes real-world feedback and threat intelligence gathered from thousands of M86 WebMarshal servers, ensuring timely and relevant identification of new and emerging threats.
- Provides a live dashboard to view detected threats, enabling you to measure the effectiveness of M86 TRACEnet security and demonstrate return on investment to your stakeholders.

Today, the significant majority of malware is distributed via 'legitimate' websites which have been compromised by hackers, rendering a website's reputation and trusted status obsolete.

Traditional anti-virus solutions are no longer effective on their own in today's threat landscape as the methods of infection and the malicious payloads have changed dramatically. Web security solutions must adapt to become multi-faceted — able to cope with a range of threats utilizing a variety of attack vectors and complex exploits.

## INTRODUCING M86 TRACeNet

M86 TRACeNet is our answer to this requirement for more agile, up to the minute and broad-reaching threat protection. It is a new subscription service for Web threat security in M86 WebMarshal.

M86 TRACeNet is a combination of technologies and service updates integrated into M86 WebMarshal to provide in-depth protection against critical and emerging web threats. M86 TRACeNet augments and extends M86 WebMarshal's other Web threat security features including anti-virus and spyware scanners, lexical filters, file scanning and file mime-type identification.

M86 TRACeNet incorporates threat-related URL blacklists, real-time content scanning, malware behavior analysis, dynamic updates and live threat reporting into a single cohesive solution. It is automatically maintained and updated by our M86 Security Labs and requires no ongoing administration.

## THREATS

M86 TRACeNet protects against four key classes of web-based threats:

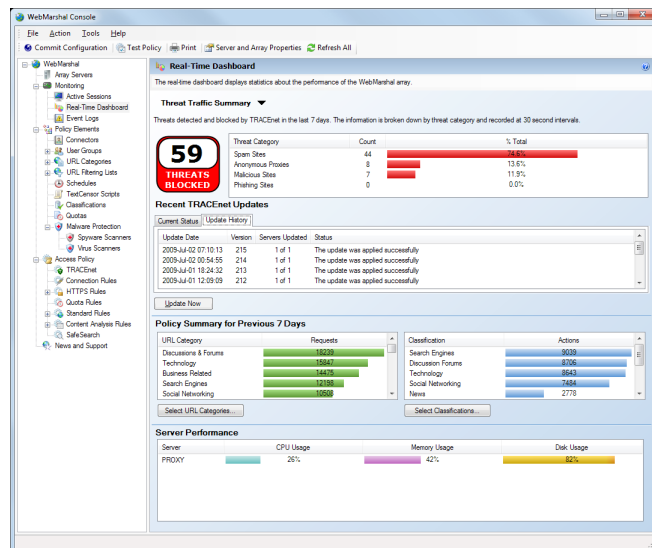
- **Malicious Sites** – sites which contain malware, browser vulnerability exploits, Cross Site Scripting (XSS) or are part of a blended attack.
- **Phishing Sites** – fraudulent sites established by scammers to lure Internet users into revealing private information. Typically, these sites impersonate legitimate businesses, such as banks, and are designed to harvest authentication credentials.
- **Spam Sites** – sites associated with spam; either being promoted through spam, supporting spam campaigns or botnet-related social engineering sites designed to infect a computer and convert it into a spambot.
- **Anonymous Proxies** – security bypass sites which can potentially allow users to circumvent web security precautions and acceptable use policies, thus creating an insider threat to your organization.

M86 TRACeNet blocks these threats using a combination of URL blacklists and real-time website content analysis. Dangerous websites encountered in the wild that are not already in the M86 TRACeNet blacklist are detected using real-time scanning. These sites are reported back to our M86 Security Labs where they are analyzed further using proprietary behavioral analysis technology and validated by our engineers.

## KEY BENEFITS

M86 TRACeNet provides multiple benefits:

- **Safer and More Secure Web Browsing**  
Your users and your network are protected against the full spectrum of Internet threats; not just viruses and spyware but dubious spam sites, phishing attempts, current social engineering scams, browser vulnerability exploits and emerging blended threats.
- **Reduced Infection Clean-up Costs and Effort**  
Your IT department will be able to spend more time on productive, business critical tasks rather than cleaning up botnet infections/spyware infestations and attempting to recover corrupted or maliciously encrypted data.
- **Versatile and Flexible Threat Protection**  
M86 TRACeNet can be dynamically upgraded. This enables our M86 Security Labs to add new functionality and threat detection capabilities to M86 TRACeNet without the need for local administrator intervention, server restarts or disruption to Web browsing services.
- **Constant Peace of Mind**  
M86 TRACeNet is continually updated with the latest Threat intelligence sourced from live spam and phishing email campaigns, reputable independent security researchers and real-time threat feedback from thousands of globally distributed M86 WebMarshal servers.
- **Zero Administration**  
Once configured, M86 TRACeNet is completely autonomous and self-contained, requiring no ongoing administration.
- **High Value Threat Protection—No Additional Cost**  
M86 TRACeNet subscription entitlements are inclusive with annual M86 WebMarshal product maintenance. There are no separate or hidden charges.



THE M86 TRACeNet DASHBOARD DISPLAYS INFORMATION ON RECENTLY BLOCKED THREATS, THE TYPES OF THREATS DETECTED AND AN UPDATE HISTORY TO HELP YOU UNDERSTAND THE RANGE OF THREATS YOUR ORGANIZATION ENCOUNTERS AND THE PROTECTION M86 WebMarshal PROVIDES.

## HOW M86 TRACEnet WORKS

M86 TRACEnet is very different from more traditional signature-based anti-virus products and even more recent reputation-based filters.

The key to how M86 TRACEnet works is the data and threat intelligence sourced by our M86 Security Labs. Our Labs receive millions of spam and phishing emails every day. Over 90% of these unsolicited messages contain a URL link. The URLs are harvested and combined with additional data feeds from reputable third-party sources.

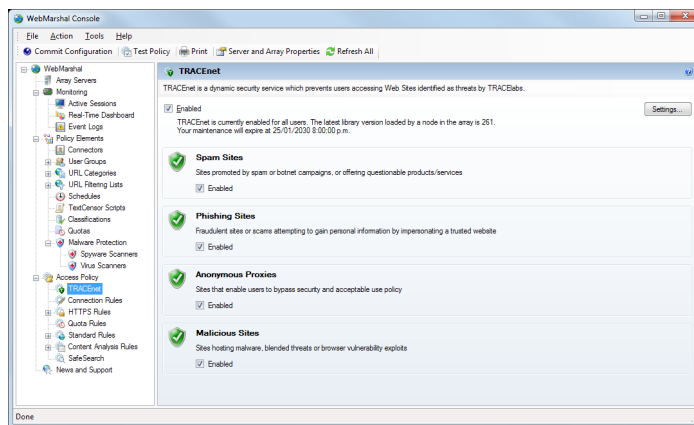
These URLs are analyzed by our Labs researchers and processed through proprietary technologies such as our malware behavior analysis servers to confirm the presence of malware or unwanted applications.

Our M86 Security Labs researchers also examine many of these URLs in 'sandbox' environments to classify revealing characteristics or traits inherent to the different classes of threats that M86 TRACEnet addresses. From these traits, our M86 Security Labs develop real-time filters which allow M86 TRACEnet to identify new threat sites in real-time.

Threats detected in real-time on live M86 WebMarshal servers are automatically reported to M86 Security Labs for validation and inclusion in the next update for the benefit of all M86 WebMarshal users. This cycle of continuous feedback and live threat identification creates the M86 TRACEnet network, providing greater coverage and relevance for M86 WebMarshal threat security.

## 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.



M86 TRACEnet ADMINISTRATION IS SET AND FORGET. A SIMPLE CHECK BOX ENABLES ALL CATEGORIES OF PROTECTION OR CHOOSE THE CATEGORIES YOU DESIRE. M86 TRACEnet IS SELF MAINTAINING WITH DYNAMICALLY ENABLED UPDATES. YOU CAN EVEN ENABLE YOUR USERS TO SEND FEEDBACK DIRECTLY TO OUR M86 SECURITY LABS IF A SITE HAS BEEN INCORRECTLY CLASSIFIED.

## 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  
Eilerslie, Auckland, 1051  
New Zealand  
Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720

Version 03/28/10