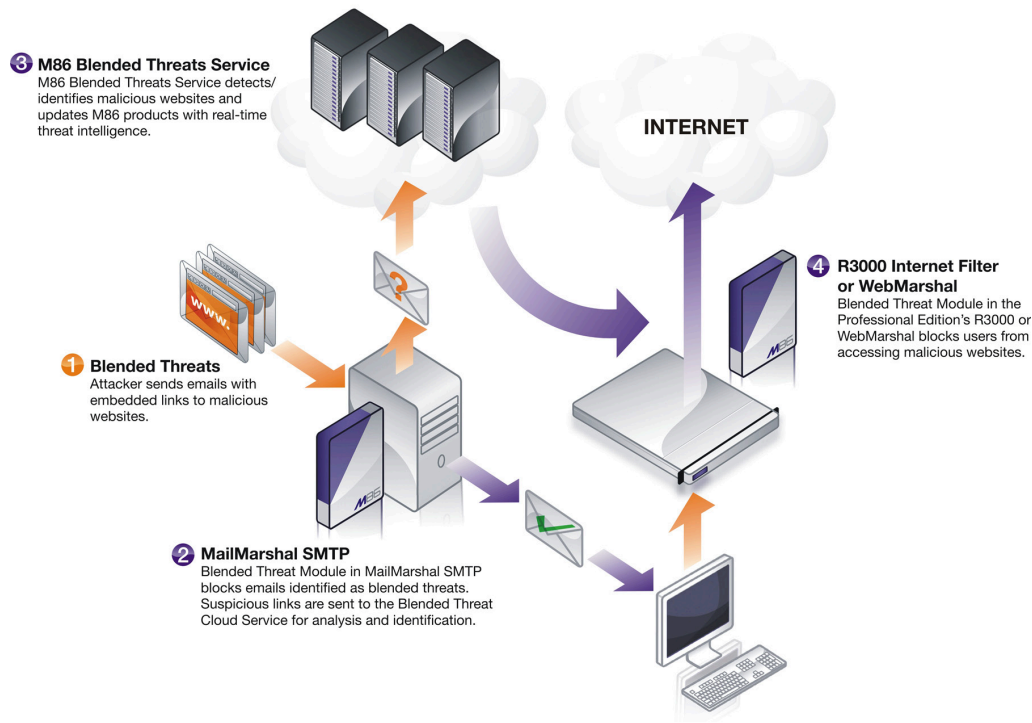


# Blended Threats Module™

## Blended Threat Protection for MailMarshal SMTP

The Blended Threats Module™ is a unique solution that addresses the growing issue of blended threats that originate in email and infect through the Web. Blended threats are successful because they by-pass email malware scanning as there is no attachment by downloading its malicious payload through the Web when a user clicks on the embedded URL link. The malware often changes frequently to avoid detection by traditional anti-virus solutions. The Blended Threats Module goes beyond the protection offered by leading signature based malware scanners by using innovative cloud-based behavioral analysis to determine the malicious nature of any suspect URL links found within email and then feeds this intelligence into MailMarshal SMTP to pro-actively block blended threats at the email gateway.



### KEY FEATURES

- Blended Threats Module for MailMarshal SMTP blocks emails with known malicious URL links in them at the email gateway.
- The cloud-based Blended Threats Service utilizes innovative cloud-based behavioral analysis to determine the malicious nature of any suspect URL links.
- The behavioral analysis technology goes beyond the protection offered by signature-based malware scanners by observing what the destination website tries to do to determine its nature as good or malicious.

### OVERVIEW

Organizations of all sizes continue to be challenged by increasingly sophisticated security threats. Attackers, motivated by financial gain, are constantly inventing new ways to penetrate corporate defences and access valuable data. Their tools include new zero-day attacks, targeted threats, use of mass variant attacks and now, blended threats initiated via email. These threats are designed to evade traditional signature-based security products and comprise an ever-growing percentage of malware.

Email blended threats, in particular, have become a key means of distributing malware. They exploit the “blind spot” many organizations have in their email malware protection and evade typical signature-based anti-virus products by eliminating the need for the malware to be attached to the message. Instead the blended email threats provides a malicious link designed to lure the recipient to a website where new variants of malware are downloaded, often without any interaction from the user. All organizations—small and large—need a strategy to deal with these ever changing and increasingly more sophisticated email threats.

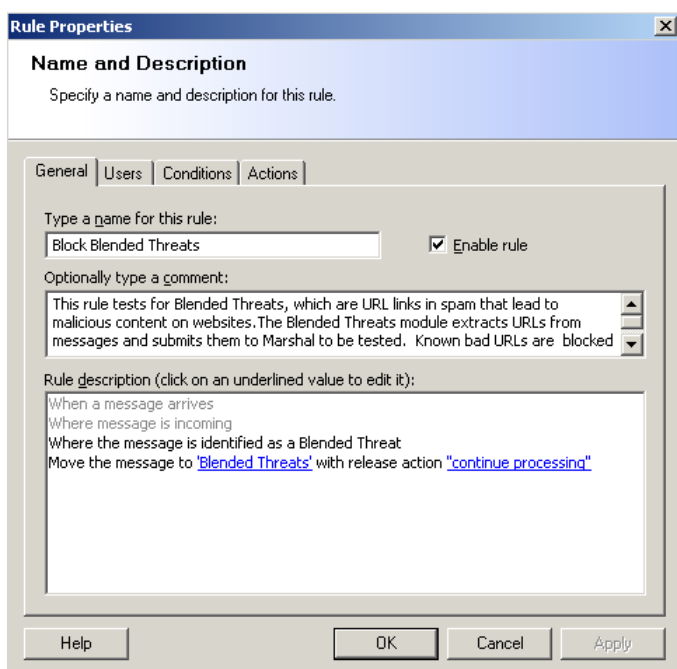
These new emerging email threats are specifically designed to evade the existing security technology available to organizations across email and Web. Blended threats have enjoyed great success in penetrating these existing security defenses and enabling Bot and malware infections. Microsoft research has reported that up to 4% of corporate computers and 30% of home computers are currently infected with malicious Bot code. A new, more innovative approach is required that is not dependent on up-to-date malware signatures or chance associations with spam and botnets.

## INTRODUCING BLENDED THREATS MODULE

The Blended Threats Module uses new and unique detection methods and technology to this new threat. It is a subscription service available for MailMarshal SMTP.

The service uses the combination of a local querying agent in MailMarshal SMTP with innovative cloud-based behavioral analysis to populate the Blended Threats Service, which in turn feeds into updated blended threats to the MailMarshal SMTP. The Blended Threats Module provides comprehensive protection from emerging blended threats, enhancing and augmenting anti-virus and anti-spam protection in MailMarshal. In addition, updated blended threats are also integrated into the M86 Filter List available for the R3000 Internet Filtering Appliance and WebMarshal Secure Web Gateway products.

The Blended Threats Module is a natural extension to malware scanning on your email gateway; the blended threats initiated through email have no attachment or embedded active code to scan. Relying on the reputation of the sender or the sending IP address is also limited in its ability to catch these email messages, they might look to be from people you know, or come from popular sites like Hotmail or Gmail.



## KEY BENEFITS

The Blended Threats Module provides multiple benefits:

- **Block threats in email** – with the advent of blended threats in email a lot of trust has gone from using URL links in legitimate email messages. The Blended Threats Module blocks the email before it reaches the user stopping the threat before it reaches the inbox and giving users higher peace of mind.
- **Rapid response to new attacks** – Blended threat attacks often utilize legitimate Web sites and last for only a few hours. The Blended Threats Module utilizes cloud-based real-time detection, stopping the threat as it happens.
- **Accurate malware detection** – Blended threats most often use new malware variants in order to bypass signature-based malware scanning solutions. The Blended Threats Module uses behavioral analysis technology to detect new variants to protect from internet borne malware and malicious links.
- **Around the clock protection** – the Blended Threats Service operates 24x7 consuming information and suspect links from M86's extensive customer base email and Web security solutions and other feeds monitored by M86 Security Labs and the specialist threat analysts.
- **At-a-glance console integration** – The Blended Threat Module integrates seamlessly into MailMarshal SMTP interface, allowing administrators to track blended threat attacks in the MailMarshal console.
- **Zero administration** – Once configured, the Blended threats module is completely autonomous and self-contained, requiring no ongoing administration.
- **High value threat protection for little additional cost** – The Blended Threats Module can be purchased as a low-cost addition to yearly product maintenance or your yearly malware subscriptions.

## HOW THE BLENDED THREAT MODULE WORKS

The Blended Threat Module in MailMarshal SMTP examines the email and extracts suspect URLs. It then compares any suspicious links against the locally cached copy of the Blended Threats Knowledge Service, if still unknown it forwards the suspicious link to the cloud-based Blended Threat Knowledge Service for analysis and identification. The cloud service also includes URL databases updated by M86 Security Lab analysts and other proprietary messaging sources, providing an additional means to identify potential threats on the Web. These threats are automatically and proactively analyzed to observe the actual behavior of the message or content in a secure and protected environment.

Confirmed threats are submitted to the Blended Threat Knowledge Service. This service is then fed back into the M86 Filter List and integrated into M86's Web products—such as the R3000 Internet filter and WebMarshal—to provide accurate, reliable protection against blended threats across email and Web.

The analysis engine behind the Blended Threats Knowledge Service observes the behavior of potential blended threats, reviewing the active content and even activating links to the embedded URLs. The Blended Threats Knowledge Service handle large traffic volumes and administrator settings provide options to blacklist and whitelist URLs, as well as, block, warn, or neutralize the blended threats. Because the Blended Threat Module doesn't rely on signatures, it provides a critical layer for catching and neutralizing new exploits.

## ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit [www.m86security.com](http://www.m86security.com).

---

### 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 848080  
Fax: +44 (0) 1256 848060

**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 11.05.09