

Real-time Security

for the Borderless Network

Vision. Experience. Leadership.



M86TM
SECURITY

M86 Security

Real-time Security for the Borderless Network

This is a time of unprecedented progress in Web 2.0 applications, social media and other Web and messaging technologies. Integral to organizations, these useful tools enhance productivity by enabling more people to work remotely, facilitating the expedient exchange of information, and connecting us in ways never before possible. But there are side effects. While information moves fast, cybercriminals act faster. And organizations face complex new challenges in Web and email security. It's with these and future challenges in mind that M86 Security describes our mission: to provide real-time security for the borderless network.

As the only company that provides real-time malware protection for Web and email, we offer technologies that secure organizations within and beyond network boundaries, extending protection for Web-based applications that reside in the cloud and for mobile workers who require anywhere access to Web and email tools.

For more than 15 years, M86 Security has provided indispensable Web and email security solutions that protect our customers from emerging threats, secure their confidential information and ensure regulatory compliance. We've led the development of many technologies used today, including one of the industry's first Web filters, early content security software, and the first hybrid cloud Web security service. Additionally, we were the first to deliver real-time code analysis technology in our award-winning Secure Web Gateway.

Through a series of strategic acquisitions, M86 Security recently procured several new technologies, including real-time and behavior-based malware detection, to complement our existing product portfolio.

"It's the strength of our proactive malware protection, such as our patented real-time code analysis technology, and the flexibility of our appliance, software, and cloud-based deployments that make us a technology and solution leader."

John Vigouroux
President and CEO, M86 Security



Now, with more than 24,000 customers and 17 million users in 96 countries, M86 Security is the global expert in real-time threat protection and the largest provider of secure Web gateway appliances.

From small businesses to Fortune 500 enterprises, M86 Security serves organizations in a variety of industries, including healthcare, financial services, government, education, and manufacturing—each with different security needs. That's why we offer flexible, scalable solutions and deployment options tailored to the size and individual requirements of any organization.

According to John Vigouroux, M86's president and CEO, "It's the strength of our proactive malware protection, such as our patented real-time code analysis technology, and the flexibility of our appliance, software, and cloud-based deployments that make us a technology and solution leader."

How M86 Leads in Technology Innovation

- Largest provider of secure Web gateway appliances
- Largest independent provider of Web and email security
- Only company with real-time malware protection for both Web and email
- First to deliver a blended threats solution
- First to deliver a hybrid cloud Web security service
- First to deliver real-time code analysis in our secure Web gateway

M86 Security Executive Management Team



Bruce Green
Chief Operating Officer



William Kilmer
Chief Marketing Officer



Rodney S. Miller
Chief Financial Officer

Tomorrow's Technologies, Today

Cybercriminals are tenacious—and they're organized. Motivated by lucrative payoffs, networks of criminals continuously develop new, sophisticated ways to infiltrate organizations via the Web and email. Our security experts understand that successful solutions need to cost-effectively preempt these threats without impeding legitimate user access and productivity.

Our patented Real-time Code Analysis, behavior-based malware detection, deep content inspection and Dynamic Web Repair™ technologies outclass others on the market, evidenced by the devout loyalty of our customers, their ongoing recommendations, and the awards and ratings we've received throughout the years.

For example, our forward-thinking approach to security earned M86 Visionary designations in two 2010 Gartner Magic Quadrant reports: one for Secure Email Gateways¹ and one for Secure Web Gateways².

"We take time to know our customers and understand their security challenges. It's with this knowledge that M86 Security develops the technologies and solutions that differentiate us in the market," states William Kilmer, chief marketing officer, M86 Security. "To us, being named a Visionary in both Gartner reports reaffirms our position and commitment to protecting customers from today's threats such as targeted attacks, blended threats and Web-based malware."

For years, M86 products have earned awards and winning reviews from SC Magazine, a leading publication for IT security professionals. Most recently, the M86 Secure Web Gateway received the magazine's 5-star rating for features, performance, support and documentation. According to SC's Peter Stephenson, "We find it to be a good value for the money due to its highly powerful features. This appliance goes above and beyond a standard anti-malware gateway."

And Virus Bulletin, a respected security publication, noted what our customers have known for years: that our M86 MailMarshal SMTP email security solution is superior to similar products on the market. Receiving the highest spam detection rate of all products tested (99.62%), M86 MailMarshal SMTP took Virus Bulletin's Gold spam award.

1. "Magic Quadrant for Secure Web Gateways", Peter Firstbrook, Lawrence Orans, January 8, 2010
2. "Magic Quadrant for Secure Email Gateways", Peter Firstbrook, Eric Ouellet, April 27, 2010

Recent Awards and Recognition

M86 Secure Web Gateway

- SC Magazine's Highly Commended Award for the Product of the Year Category at AusCERT 2010
- SC Magazine's 5-star Rating
- Visionary Designation in Gartner's Magic Quadrant Survey Report¹

M86 Secure Web Service Hybrid

- CRN's 100 Coolest Cloud Computing Products: Top 20 Coolest Cloud Security Products

M86 MailMarshal SMT

- Virus Bulletin Gold Spam Award
- Visionary Designation in Gartner's Magic Quadrant Survey Report²

M86 Security Timeline

November / 2008

8e6 Technologies and Marshal Software merged to form Marshal8e6, the largest independent provider of content security and a leader in secure Web gateways.

March / 2009

Marshal8e6 acquired Avinti, procuring its advanced behavior-based malware technology to address blended threats.

September / 2009

Marshal8e6 rebranded, changing the company name to M86 Security.

November / 2009

M86 Security acquired Finjan Software along with its powerful secure Web gateway solution and patented Real-time Code Analysis technology for advanced Web malware detection.

January / 2010

M86 Security emerged as a single-source provider of Web and email gateway security, encryption and DLP solutions and the world's largest provider of secure Web gateway appliances.

M86 Secure Web Gateway recognized as Visionary in the 2010 Gartner Magic Quadrant Report for Secure Web Gateways¹.

March / 2010

The company launched the Secure Web Service Hybrid.

April / 2010

M86 MailMarshal SMT recognized as Visionary in the 2010 Gartner Magic Quadrant Report for Secure Email Gateways².



Crucial Solutions for Critical Security Challenges

Preventing Malware at the Internet Gateway

Today, cybercriminals use the Web as their medium of choice for most malware attacks. According to Bradley Anstis, M86 Security's vice president of technical strategy, more than 90 percent of all malware is delivered through the Web. Why? Because most organizations lack strong controls on their Web gateways, and Web-based applications are inherently susceptible to malware. Cybercriminals successfully use obfuscation techniques, exploit zero-hour vulnerabilities, and hijack legitimate websites to infiltrate networks and steal critical data.

M86's secure Web gateway solution addresses the growing malware problem, enabling companies to access the Web safely and productively. At the core of this solution is our **Vital Web Security Suite™**, a group of complementary technologies that include **Real-time Code Analysis**, **Vulnerability Anti.dote™**, and **Dynamic Web Repair™**. Together, they provide the most accurate and comprehensive real-time Web security protection available.

Our award-winning, patented Real-time Code Analysis technology detects and blocks new and dynamic malware at the gateway, analyzing incoming and outgoing Web content, regardless of origin and without signature matching. As a result, malware is detected and blocked before entering the network—even when hiding in encrypted SSL traffic.

Combatting Zero-day Threats

Using zero-day or even zero-hour threats, cybercriminals target their attacks during

the Window of Vulnerability that exists from the time a vulnerability is detected to the moment a patch is applied. Using behavioral analysis, **Vulnerability Anti.dote™** identifies and blocks malicious content that exploits known and newly-discovered Web vulnerabilities. Its scanners detect these weaknesses at the point of discovery, eliminating exposure to the threat. And it's the only technology that provides true zero-hour defense, even against unpublished vulnerabilities.

Eliminating Web 2.0 Vulnerabilities

M86's secure Web gateway solution prevents malicious content from entering corporate networks via Web 2.0 applications, which are common conduits for malware infection. **Real-time Code Analysis** detects malicious code embedded in Web 2.0 pages and disables the malware, allowing access to legitimate content on the same page.

Customer : Munich Airport

Challenge: To prevent Web-based attacks, differentiate between legitimate and malicious Active Content and create granular security policies for different user groups—all while ensuring airport systems remain online at all times.

Solution: M86 Secure Web Gateway

"M86 Real-time Code Analysis technology has been invaluable to us in blocking malicious code embedded in Active Content, keeping our critical information systems free from Web threats."

—Marc Lindike, Vice President, Operations and Services, Munich Airport

Blocking Blended Threats

Many organizations grapple with threats that originate in emails and then infect networks through Web use. To combat these attacks, our behavior-based detection technology goes beyond signature-based scanning. It also uses cloud-based behavioral analysis to determine the malicious intent of URLs within email. The data is then fed into M86's Web security solutions to ensure comprehensive Web and email malware protection.

Customer: Vulcan Steel

Challenge: To safeguard sensitive data, minimize liability risks and secure the network from malware and spam.

Solutions: M86 MailMarshal Exchange/SMTP

"The amount of spam we receive now is almost zero thanks to the filtering from M86 MailMarshal SMTP. That has had great benefits in terms of malware protection, increased network performance and reduced management time."

—Tony Salmon, Chief Information Officer, Vulcan Steel

Safeguarding Sensitive Information

By the time an organization requires damage control, its reputation has already been compromised. Loss of sensitive corporate and customer data triggers a series of compliance issues and liability risks that cost in time and revenue. M86 Security's Web, email and endpoint security solutions mitigate these risks

by preventing loss of confidential data such as customer information, financial records, credit card numbers, patient data and employee information.

These solutions enable our customers to configure policies that address compliance regulations, including PCI, HIPAA, GLBA, SOX, CISP, FISMA and CIPA, as well as California SB1386, which requires companies to disclose data breaches. Inspection of outbound communications and deep analysis of various content types prevent confidential data from ever leaving the network.

In addition, our Web security solutions help enforce specific policies. For example, organizations can allow employees to access Facebook but prevent posts, eliminating data leakage risks. Policies for each worker remain the same, regardless of location.

Customer: St. Jude Children's Research Hospital

Challenge: To comply with HIPAA regulations by preventing patient information leaks and to protect the hospital while allowing scientists to use the Internet freely.

Solution: M86 Web Filter and Reporter

"It's a very cost-effective solution—its accuracy and reliability has saved us by not wasting our resources. M86 has a great product for any organization facing policy enforcement and/or compliance challenges. The system keeps running, monitoring, recording, and blocking, which is exactly what a customer would expect."

—Monroe Wesley, Manager of Information Security, St. Jude Children's Research Hospital

Inspecting Email Content and Attachments

With a constant influx of spam and malware, plus compliance and data loss concerns, messaging administrators juggle a myriad of email security challenges. M86 Security's deep content inspection technology does more than simply identify and block attachment types—it actually scans content within attachments. This prevents a user from renaming a document to bypass security, and as a result, it reduces the burden for messaging administrators and prevents data leakage.

Ensuring Productivity

Social networking. Web surfing. Online gaming. Instant messaging. The list of potential employee distractions goes on and on—and it's growing. Allowing access to the Web and its associated tools while minimizing the impacts on productivity is a balancing act.

Most organizations institute an Acceptable Use Policy (AUP) as a first step in controlling Web use. Educating employees about the AUP is important, but enforcement is key. This is where M86 Security's productivity solutions can help.

Curbing Distractions and Enforcing Acceptable Use Policies

In addition to preventing access to inappropriate content, **URL filtering** empowers organizations to monitor employee Web use and enforce AUPs.

M86 URL filtering solutions enable our customers to set policies for dozens

of Web categories, including Web 2.0, business-related sites, Webmail, streaming media, personal websites, and more. This helps ensure that employees remain on task, spending their time on work-related websites.

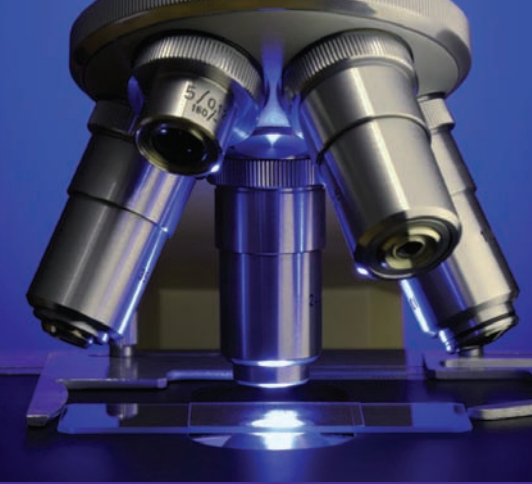
Removing Malware from Web Pages without Blocking Valid Content

Often, employees require access to legitimate websites in their daily tasks. But what happens when one of these websites is infected with malware? Most technologies simply block the Web page, consequently prohibiting users from completing their jobs. But our solution is different. M86's **Dynamic Web Repair™** technology neutralizes the malicious code without blocking the website. After eliminating the malware, Dynamic Web Repair™ delivers the safe Web content to the user—maintaining productivity.

Controlling the Use of Web 2.0 Applications

Though Web 2.0 applications, including social networking sites like Facebook, give organizations exciting new ways to engage their customers and gather information, excessive personal use in the workplace can reduce productivity significantly. Our customers want a way to benefit from Web 2.0 tools while ensuring a secure, productive environment—and that's what we've provided.

Our secure Web gateway solution enables organizations to assign policies by user, controlling the way employees use Web 2.0 applications without blocking them completely. Collaborative applications such as instant messaging, Skype and P2P can be restricted to beneficial uses.



Advanced Threat Intelligence: M86 Security Labs

Central to our Web and email technologies is M86 Security Labs, a specialized global team of security experts and researchers. Their mission? To detect current and emerging threats and mitigate them quickly. By using data feeds from the Internet security community and internal intelligence gathered from our customers and products, our team analyzes massive amounts of threat information and provides comprehensive, always-adapting defense against email and Web threats.

Our experts disseminate this intelligence to our installed base of security products, ensuring the latest threats are prevented. In addition, M86 Security Labs provides zero-day protection to our customers, securing them from new exploits the day they're discovered.

Built from the ground up, the M86 Web Filter Database, one of the tools developed by our labs, is widely regarded as the most complete and accurate filtering database ever compiled.

"M86 Security Labs is at the core of the company—protecting customers, driving innovation and ensuring that we inform the wider community on the latest Internet threats," says Bradley Anstis. "We produce a highly active blog and publish papers about new and emerging threats. M86 Security Labs leads the industry in specific areas of research such as spam, spambots, attack toolkits and the methods for infecting legitimate websites."

Securing the Mobile Workforce

Extending Web and email protection to mobile workers is imperative to the overall security of any organization. Increasingly, as employees work from home, airports, coffee shops and branch locations, administrators require the same high level of threat protection and productivity enforcement they receive from on-premises solutions.

That's why M86 developed the first Web solution to integrate a Web security appliance with cloud-based services. This hybrid cloud service enables administrators to centrally manage security across the corporate network to remote workers and branch offices.

Providing Visibility into Web and Email Traffic

Organizations need a complete picture of their Web and email traffic to effectively monitor security threats and ensure productivity. M86 Security's powerful logging and reporting capabilities enable management to implement policies that improve security, efficiency and productivity throughout an organization.

As the most comprehensive, detailed real-time reporting solution on the market, we offer the only dedicated appliance that processes and displays Internet filtering use logs without impacting network performance or functions.

Our reporting solution includes high-level executive reports that identify anomalous Internet activity through easy-to-read graphical reports. Detailed, drill-down forensic reporting gauges user intent by documenting URLs visited and search strings used within a search engine text box.

M86 Security's Real-time Threat Dashboard offers a customizable gauge view of online activity. It displays an organizational snapshot of multiple threat categories and top offenders based on predefined thresholds and policies.

Customer: HMSHost

Challenge: To manage and protect mobile users from Web-based threats.
Solutions: M86 Secure Web Gateway and M86 Secure Web Service Hybrid

"The combination of the M86 Secure Web Gateway appliance and M86 Secure Web Service Hybrid solution will allow us to address the security concerns of our remote workers who utilize laptops outside the office as well as computers that are used for our critical business operations at airports. It also helps us address PCI compliance through logging and reports from a single source. The fact that we can manage both the on-site appliance and the cloud service from one central point is great and helps us with providing consistent information to all key stakeholders, including our senior management."

—Erik Wouterson, Senior Systems Engineer, HMSHost

Choosing the Right Deployment Option

Whether our customers choose appliance, software, virtualization, cloud or hybrid cloud deployment, M86 Security offers the platform most suitable for their networks. With our scalable, flexible deployment options, our customers know they'll receive exceptional performance in a platform that will grow with their company.

Q & A



The following Q&A session with Bradley Anstis, vice president of technical strategy, M86 Security, discusses prevailing and anticipated Web and email threats as well as key considerations for selecting effective security solutions. He also explains how M86 Security addresses today's security challenges, enabling organizations to improve productivity and restore their trust in Internet use.



What are the prevalent security threats faced by organizations today?



How can businesses protect themselves from these threats?



Attacks have become more targeted and complex in recent years. We know that traditional controls are no



A combination of technologies is needed. While reactive security controls like URL filtering and anti-virus

longer as effective in protecting an organization's network because threats have shifted dramatically from email to the Web, which is now the number one way malware is distributed. In addition, the majority of email threats now come from links to malicious websites rather than through attachments.

scanning protect users from known threats, proactive-based solutions are vital for addressing new and unknown threats. It's the right combination of reactive and proactive technologies that yields complete coverage with optimum performance.

Cybercrime (and its malware) remains a major threat to businesses and has become a booming multi-billion dollar business, surpassing the illegal drug economy.

Most importantly, organizations need to detect and eliminate these threats and attacks as early as possible. That's why technologies that work at the network perimeter or up in the cloud are always part of the recommended solution.

Q

“Deploying a secure Web gateway is a must because it brings together the two main requirements of Web security: security controls and productivity controls.”



A

“It’s the right combination of reactive and proactive technologies that yields complete coverage with optimum performance.”

Also consider the vectors used in these attacks. The Web is a popular vector now, but many of these attacks are initiated in email. Therefore it’s best practice to deploy effective security solutions across email and the Web—even better if the two solutions correlate threat data between them. M86’s solutions do this. Other important steps to take include:

1. Ensuring applications are updated since most vulnerabilities occur in dated versions of browsers and applications.
2. Removing administrative rights for most users to reduce vulnerabilities.
3. Conducting sensitive tasks on separate systems or networks to decrease attack risk.
4. Educating network users about social engineering, phishing, man-in-the-middle malware, etc.

Q There’s a lot of buzz around hybrid and cloud computing. What should an organization consider when evaluating which deployment option would best fit its security environment?

A It’s important to look internally and determine exactly what a security solution can achieve, and what policies it needs to support. Considerations must be balanced with the desire to block threats as early as possible in the cloud or at the network perimeter.

A hybrid solution with a single-administration and management/reporting interface across both the on-premises and cloud-based components is ideal. However, there isn’t one right answer for all organizations.

Q What should an organization look for when considering a Web security tool?

A More than 90 percent of all malware is delivered through the Web. Deploying a secure Web gateway is a must because it brings together the two main requirements of Web security: security controls and productivity controls. These efforts can be extended further by data leakage prevention controls which support policy enforcement with effective reporting and management.

A proactive approach is important due to the increasing popularity of dynamically-created malware and polymorphic viruses that are designed to evade reactive security controls. For example, the

Real-time Code Analysis technology within our secure Web gateway provides an effective proactive capability in addition to the reactive capabilities of anti-virus scanning and URL filtering lists.

A staggering 80-85 percent of all infected websites are legitimate. The ability to perform Dynamic Web Repair™ also plays an important role in neutralizing the threat posed by compromised legitimate websites that users need to access to be productive.

Policy management along with reporting and management tools provide a great value for an organization seeking to improve its security posture.

Q Are there areas where organizations should focus their email security efforts?

A Email security solutions should take a similar approach to secure Web gateways. Proactive security controls and coverage for blended threats must be considered. In addition, a tool which has a depth of policy conditions and actions can meet the needs of organizations today while helping them prepare for the future.

A clear and concise view into the email environment for growth predictions, policy adherence, and security attacks is equally vital in staying ahead of an organization’s requirements. Additionally, a centralized management console with appropriate interfaces can positively impact the ability to manage email.

Q How does M86 envision the next level of security threats?

A We continue to see an increase in malware. Furthermore, sophisticated iframe injections have emerged as the latest problem with legitimate websites. We also believe threats to users of smartphones and other mobile devices, including the iPad and other mobile platforms, will grow. Security threats are no longer static, but dynamic in nature, and must be addressed accordingly.



What are some of the methods M86 uses to successfully protect organizations?



With patented Real-time Code Analysis technology, M86 offers organizations an unprecedented level of Web protection. Through a dedicated analysis engine, we conduct assessments to understand active content. Results from analysis engines are then compared to the user's active policy, and the page is either allowed, blocked or malicious content is neutralized on the page with Dynamic Web Repair™. At that point, the content can be delivered safely to the user. This Web stripping effort may seem unusual, but simply blocking content could severely disrupt a user who may have a legitimate need to visit a website.

With its proactive approach, our tool can detect dynamically-created malware and malicious code that has not been seen previously, only adding milliseconds of latency to a user's browsing experience.



Do M86 solutions differ from other products on the market?



The biggest difference between M86 solutions and other offerings is that we use real-time, proactive security technology in addition to reactive solutions such as URL filtering. Others continue to rely only on reactive controls which aren't designed to thwart today's sophisticated threats.



Are there unique methods M86 uses to thwart email threats?



The proactive behavioral analysis technology used for our email security solution takes a similar approach to our Real-time Code Analysis for assessing Web content. Behavioral analysis extracts email attachments and

any embedded links, running them through a virtualized machine. An observation engine then examines how attachments or links impact the virtualized environment to determine if there is any malicious intent.

Blended threats continue to pose a major concern. Attackers who use blended threats capitalize on the fact that most organizations have weak security controls on their Web gateways. Behavioral analysis lies at the heart of our innovative blended threats service, allowing us to fully protect M86 customers by stopping those attacks at the email gateway before they reach users.

“We take time to know our customers and understand their security challenges. It's with this knowledge that M86 Security develops the technologies and solutions that differentiate us in the market. To us, being named a Visionary in both Gartner reports reaffirms our position and commitment to protecting customers from today's threats such as targeted attacks, blended threats and Web-based malware.”

William Kilmer
Chief Marketing Officer, M86 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 advanced 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.



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

www.m86security.com