

Six Steps for Implementing an Effective Web Security Solution

Real-time Malware Protection and Business Enablement in a Web 2.0 Environment

INTRODUCTION

Businesses operate in a competitive, fast-paced global economy. It's critical that they connect with customers and partners quickly to address opportunities in real time, otherwise they fall behind. To excel, businesses adopt new technologies and applications that enable efficient information exchange, collaboration and ultimately, result in increased revenue.

Web 2.0 applications, among the most quickly-adopted technologies today, are now critical tools for many organizations. Once perceived as a means to connect socially, this relatively new medium has been embraced for business use, including marketing, recruiting and technical support. Most businesses maintain a corporate presence on social networking sites such as Facebook, Twitter and YouTube, and many use Web 2.0 applications to implement company blogs or customer feedback on their own websites. An organization's participation on social networking sites is generally expected—the same way individual company websites became standard years ago. Plus, today's employees expect a certain level of access to social networking sites while at work.

With this in mind, there's a debate between allowing and denying Web 2.0 and social media use in the workplace due to the related security implications. These sites provide valuable capabilities and opportunities, but how do businesses enable access to them without impacting productivity, risking data loss or increasing vulnerability to malware threats? Without access, businesses lose the competitive advantage and mindshare gained from strategic social media engagement.

This white paper addresses the risks that concern IT security professionals, many of which they feel powerless to control. These include malware infections through legitimate, trusted websites; new and dynamic malware that eludes traditional detection methods; and vulnerabilities inherent in Web 2.0 applications. And because demand for Web 2.0 access is only going to increase, organizations need to support safe, controlled access to Web 2.0 sites, taking a more proactive, positive approach to Web security.

CONTENTS

Web 2.0 Applications: From Static to Dynamic Content	3
Who Can You Trust? Legitimate Websites as Preferred Targets	3
How Cybercriminals Evade Web Security	4
Common Malware Infection Techniques	5
Best Practices for Implementing a Web Security Solution	7
Step 1: Establish Who and What You Need to Protect	7
Step 2: Understand Your Organization’s Web Security and Productivity Requirements	7
Step 3: Understand Web Security Methods	8
Step 4: Evaluate Web Security and Productivity Solutions	8
Step 5: Implement an Effective Internet Acceptable Use Policy	9
5a: Create the Policy	9
5b: Communicate the Policy	10
5c: Enforce the Policy	10
Step 6: Monitor, Report and Adjust Regularly	10
Choosing the Right Solution for Your Organization.....	11
How the M86 Secure Web Gateway Analyzes a Web Page.....	11
Benefits of the M86 Secure Web Gateway	12
Web Security.....	12
Productivity Enablement.....	12
Coverage for Remote and Mobile Users.....	13
Visibility into Web Activities through Reporting.....	13
Conclusion	14

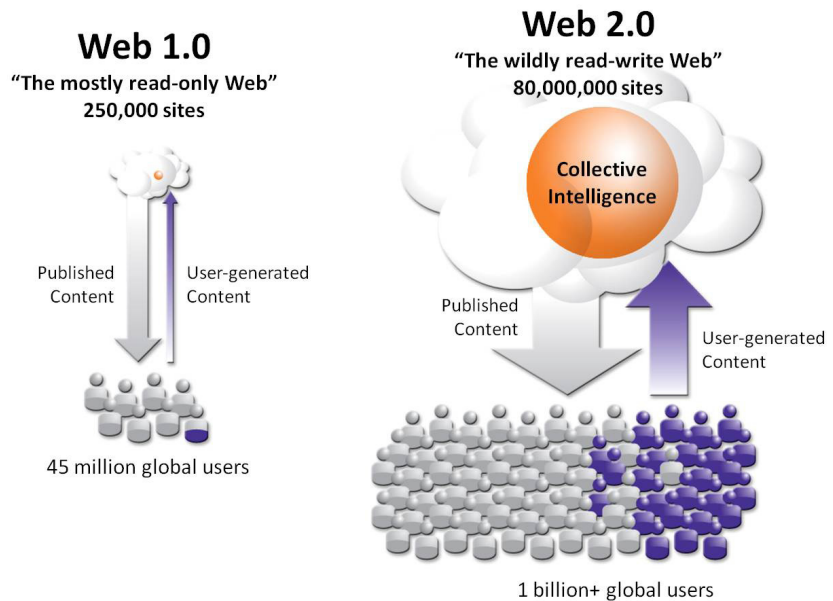
WEB 2.0 APPLICATIONS: FROM STATIC TO DYNAMIC CONTENT

More than 92 percent of new threats occur through the Web, predominantly through vulnerabilities in Web 2.0-enabled sites and applications and third-party content, such as ads and banners, that appear on primary websites. What makes these sites especially vulnerable to attacks?

More than 92 percent of new threats occur through the Web, predominantly through vulnerabilities in Web 2.0-enabled sites and applications and third-party content, such as ads and banners...

Before Web 2.0 applications entered the mainstream, web pages consisted of static HTML, and companies simply pushed read-only content to users. In other words, users didn't really interact with the content. Web 2.0 entered the scene and provided a platform for dynamic Web pages, enabling third parties to submit content to a site for a collaborative online experience.

In essence, Web 2.0 applications were created to provide a venue for publishing user-generated content from multiple sources. These technologies allow users to share and exchange information online easily through company-sponsored and social media sites.



Development technologies such as I-Flex®, AJAX, Adobe Flash® and Java® drive dynamic content from multiple sources and allow users to freely post and share information in real time. A single Web 2.0 page may be built with multiple development languages and incorporate many different technologies.

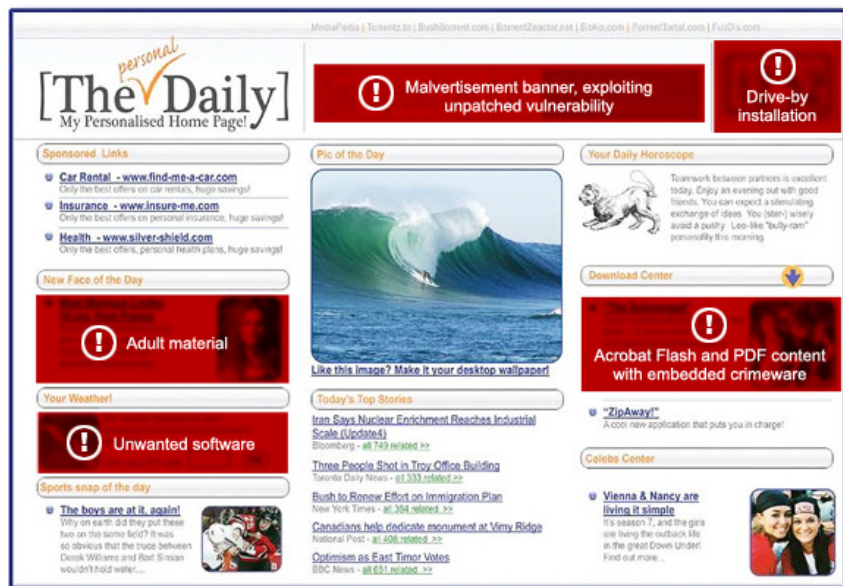
In addition, features such as iFrames allow a single Web page to present content from multiple sources, though it's all perceived to be part of a single HTML document. iFrames are used frequently for third-party advertisements. The ability to track cookies and user preferences enables websites to present rich personalized content to users. However, it also increases vulnerabilities by opening new opportunities for Cybercriminals to compromise websites.

Who Can You Trust? Legitimate Websites as Preferred Targets

As Web 2.0 tools become more popular, associated technologies have expanded beyond social networking and news sites. More traditional, trusted companies are adding RSS feeds, blogs, user forums, third-party ads and Web applications to enhance their visitors' online experiences and increase sales. Because legitimate sites are trusted by most users, Cybercriminals prefer to infect them with malware and increase the potential number of victims. Some of the websites recently affected include Walmart, The New York Times and The Wall Street Journal. It's not just about Twitter, Facebook or YouTube—this is a universal Web problem.

Approximately 85 percent of Web-based malware infections occur on legitimate websites.

Simply blocking social media sites will not protect an organization from Web threats. Approximately 85 percent of Web-based malware infections occur on legitimate websites. That means organizations can no longer rely on blacklists or reputation to protect their networks from “drive-by” infections.



How Cybercriminals Evade Web Security

How do Cybercriminals compromise Web 2.0 applications and other legitimate websites? They exploit known and newly-discovered application vulnerabilities and use those deficiencies to inject malicious code. The most well-known and common methods include:

- **SQL Injection**
SQL injection vulnerabilities allow Cybercriminals to access and manipulate the database behind the site, system or application. They can modify the content on a legitimate website to extract data or inject malware. This code injection technique exploits a security vulnerability that occurs in the database layer of the application server. SQL code is entered into Web forms such as login fields or browser address fields—anywhere a user inputs text into a field that interacts with the website's back end database.

For example, in June 2008, visitors to the Walmart website were exposed to malware when Cybercriminals exploited a vulnerability in a Flash player plug-in and used it to modify the server's database through SQL injection.

- **Cross-site Scripting (XSS)**
This application vulnerability enables Cybercriminals to inject malicious script into web pages. Injected content often contains mobile code elements, including JavaScript®, ActiveX®, VBScript®, Adobe Flash® or even HTML. Once inserted into a dynamic website, the embedded elements gather private data, issue requests to the Web application, read private user information (including cookies), or install a virus on the user's computer. This type of script can also redistribute malicious content across the Internet with the full authority of the user and the hosting site. Dynamic websites are most vulnerable to XSS attacks on secure data.

For example, on Sept. 22, 2010, Twitter was infected with an XSS worm that directed users to a pornographic site through a seemingly innocent pop-up box. Moving the mouse over the link—without even clicking on it—redirected users to the site. This “onMouseOver” event could have been more serious if it had directed users to a site that downloaded malware onto their systems.

A single piece of malware can have a nearly unlimited number of signature permutations, making it impossible to detect through traditional detection methods.

- **Malvertisements**

These malicious Web ads contain active scripts that download malware or force unwanted content onto a user's computer. Even respected news sites like [The New York Times](#) can and have unknowingly served malware to their readers.

- **Stolen File Transfer Protocol (FTP) Credentials**

In a [finding by M86 Security](#), 8,700 stolen FTP credentials, including user names, passwords and server addresses were discovered and available for purchase. Stolen FTP credentials allow hackers to break into servers and upload malware with only a couple of clicks.

Many corporations use "secure" FTP (secure communication does not validate content and is unable to protect when credentials are stolen) to upload and maintain the content of their websites as well as to disseminate files between senders and recipients. Through this simple transfer mechanism, otherwise legitimate websites and other back end information exchanges can be modified easily to include and serve malicious code.

In May 2009, the [Gumblar worm](#) compromised thousands of legitimate websites using stolen FTP credentials to distribute malware that was hosted on an attacker-controlled server.

- **Cross-site Request Forgery (CSRF)**

Unlike cross-site scripting, which exploits a user's trust in a particular site, CSRF exploits the browser. This malicious exploit transmits unauthorized commands from a trusted user website. Malicious code on the infected servers can issue "authenticated" requests on behalf of the website. In April 2010, PayPal discovered and patched a [CSRF vulnerability](#).

Common Malware Infection Techniques

Often, malware only infects a legitimate website for hours at a time and is redistributed to evade detection. Cybercriminals use the following techniques to prevent and/or delay malware discovery and optimize their results.

- **Dynamic Code Obfuscation**

Obfuscation is a technique developed and used for legitimate business reasons such as deterring reverse engineering or code tampering and protecting against the loss of intellectual property. Potential loss of investment became a considerable issue with the advent of widely-used, just-in-time compilation languages such as Java, which are simpler to reverse engineer than their real machine counterparts.

Through code obfuscation, the look of code can be altered without modifying the operation or intent of the program. In other words, code obfuscation is the perfect mechanism for disguising malware without the need to find new application vulnerabilities, and this renders anti-virus and signature-based detection technologies powerless. Through obfuscation, viruses, Trojans and other malware (even those already identified) can be modified to change their appearance, evading detection.

As dynamic obfuscation techniques evolved, malware could automatically change as often as every server request. A single piece of malware can have a nearly unlimited number of signature permutations, making it impossible to detect through traditional detection methods.

The widespread proliferation of dynamic code obfuscation was illustrated in an analysis conducted by M86 Security Labs in 2007. In this analysis of live end-user traffic in the UK (including more than 10 million unique URLs), M86 found that more than 80% of the detected malicious code was obfuscated in an effective attempt to evade signature-based products like anti-virus, IDS/IPS and URL filtering.

Though convenient for social networking posts, shortened URLs make it easy for Cybercriminals to obscure malicious links and difficult for users to determine what content they'll actually receive. Not surprisingly, the majority of malicious links detected by M86 Security Labs on social networking sites in 2009 were shortened URLs.

- **Hiding Malicious Links in shortened URLs**
Shortened URLs, another form of obfuscation, have been popularized by Twitter, which restricts the number of characters allowed in a posted URL. This process masks the original source URL, replacing it with a shorter address. Though convenient for social networking posts, shortened URLs make it easy for Cybercriminals to obscure malicious links and difficult for users to determine what content they'll actually receive. Not surprisingly, the majority of malicious links detected by M86 Security Labs on social networking sites in 2009 were shortened URLs.
- **Social Engineering**
Using social engineering, Cybercriminals trick unsuspecting users into downloading malware by clicking on a link or pop-up box. These attacks usually originate in blended threats emails, which coax users to click what appears to be a legitimate link, or on websites that urge users to update their security software, join a new online game or re-connect with an old friend. All that's required is a single mouse click or mouse-over to trigger the malicious download.
- **Drive-by Downloads**
Drive-by downloads use a browser's ability to execute background code to connect computers to servers that are rigged with malicious exploits. The malicious program downloads onto the user's system automatically, and no action is required by the user. Simply viewing the malicious content is enough for malware infection.

Propagating Malware Infections

Malware can be automated to infect thousands of websites. As reported by M86 Security Labs, Web threats like [Asprox](#) locate vulnerable sites automatically, using common vehicles such as a Google search to launch a SQL attack that infects thousands of websites.

How can you stay one step ahead of methods such as dynamically obfuscated code? How can you enable your business to function in a Web 2.0 environment and safeguard your network from malware hidden on legitimate websites? Users need to access content to perform their jobs, and companies need to secure their online environments from Web threats. Simply blocking content is antiquated, and it severely limits the ability to leverage legitimate applications that can improve business. It's no longer an acceptable solution in today's business environment. Instead, an understanding of the intent of content is required. The following best practices guide will outline the steps organizations need to take to implement a secure, productive Web environment.

BEST PRACTICES FOR IMPLEMENTING A WEB SECURITY SOLUTION

An effective Web security solution should support a company's Web policy. Organizations need to decide who and what they need to secure, determine their risk comfort levels and understand what kinds of malware attacks are possible. Any website that provides access to its users and customers, including social networking, large grocery chains, banking, education, government, news or gaming sites, can be compromised with malware.

In a recent [Zeus attack](#) discovered by M86 Security Labs, more than 3,000 customer accounts for a large UK financial institution were compromised and over \$889,000 was transferred illegally. Even static websites are not immune to threats through back-door mechanisms, improper code review, faulty migration practices and lost credentials—all of which are outside the control of the end-user community.

To protect your organization and users from Web-based threats, follow these steps:

Step 1: Establish Who and What You Need to Protect

It's important to determine who you need to protect and what is of value.

Who do you need to protect?

- Corporate employees
- Visitors, customers and contractors (onsite access)
- Branch and remote offices and mobile workers

What is of value?

- Customer records
- Employee records
- Intellectual property
- Financial information
- Competitive information
- IT systems, access information
- Corporate or agency brand reputation

Step 2: Understand Your Organization's Web Security and Productivity Requirements

What are your organization's security and productivity requirements? Determining an optimal balance will help you implement the appropriate solution for your network environment.

Productivity

To ensure user productivity, implement policy control that manages what users can view and when. For example, URL filtering is a solution for in-depth policy control management. This allows granular control over users' Web activity. And quota management determines how much time and bandwidth can be used.

Security

An organization's users and networks require protection from Web exploits such as adware, Trojans, system monitors, keyloggers, malicious/tracking cookies, browser hijackers, browser helper objects and phishing attacks delivered through cross-site scripting, cross-site request forgery, SQL injections or invisible iFrames. Protection from these threats requires security methods that go beyond standard, reactive techniques. How do you know whether your existing security solution uses reactive or proactive techniques? This will be explored further in steps 3 and 4.

It's important to safeguard your organization from Web threats and maintain a productive work environment. Once you understand your organization's Web security and productivity requirements, you can better evaluate the available Web solutions.

Step 3: Understand Web Security Methods

When reviewing Web security solutions, think about future needs and expectations, as well as what's currently in place. Does your solution contain proactive or reactive methods? And how do they differ?

Reactive Methods

Though they are useful in detecting known threats and enforcing policies, traditional security solutions such as anti-virus scanning, URL filtering and reputation scores are reactive, and therefore less effective in protecting against new malware. These solutions block known viruses and worms by comparing content against signature databases, URL categories or reputation scores, all of which need to be updated each time a new attack is discovered. These reactive solutions simply cannot combat unknown and targeted attacks such as spyware, phishing, worms, Trojans, viruses or blended threats.

Proactive Methods

Today's sophisticated attacks require a solution that analyzes content behavior in real time and determines whether that content is malicious. Scanning and inspecting all active content as users access it and blocking malicious content **at the gateway** is extremely important. The solution should de-obfuscate the malicious code—as it's being downloaded by the user, recognize any hidden exploits contained in the code, and block it in real time at the gateway.

Proactive control like Real-time Code Analysis detects malicious intent of new, emerging malware. Look for a solution that helps neutralize threats on trusted, legitimate websites by removing malicious code and repairing web pages, allowing users to continue their work without interruption.

Step 4: Evaluate Web Security and Productivity Solutions

In reality, no organization is immune to security threats. Individual technologies and tools will vary according to your business requirements and risk assessment. When evaluating web security solutions, it is important to understand the technologies used and how effective they are at preventing malware attacks. Below is a list of security methods most vendors use in their solutions.

URL Filtering

URL filtering controls employee browsing habits and improves productivity and network performance. Although millions of URLs are scanned each day, URL categorization has become ineffective in detecting modern malware because the majority of infections occur through legitimate websites. In a test conducted by M86 Security Labs, out of 15,000 malicious URLs, only 3 percent were listed as known malware or spyware sites; 34 percent were listed as legitimate sites; and 63 percent were uncategorized.

URL filtering was designed to be a productivity tool—not a security tool. As such, it doesn't detect and block malicious code stored in legitimate caching servers, search engines or Web 2.0 sites. It can only detect and block websites that are stored in a URL database.

IP Reputation Lists

Reputation scores are assigned to domains using parameters such as the IP of the hosted site, the site owner, how long the domain is registered and whether the URL appears in mass spam emails. Reputation scores only apply for the name of the domain registrar—not for individual web pages, so malware-infected pages can exist on legitimate websites that have high reputation scores.

Most new infected web pages are found on legitimate sites and will go undetected by URL- and reputation-based solutions. Cybercriminals evade reputation services by inserting malicious code into legitimate websites or on Web 2.0 sites.

Scanning and inspecting active content as users access it and blocking the malicious content at the gateway is extremely important.

Look for a solution that removes malicious code from the page and still delivers legitimate content—in contrast to blocking the URL completely—to enable optimal productivity in a Web 2.0 work environment.

In an M86 Security Labs study, at least six in 10 malicious URLs pass undetected in the absence of real-time code analysis technology.

Anti-virus

Useful for blocking known attacks in the first line of defense, gateway anti-virus solutions look for signatures of known attacks, require days or longer to release a new signature, and often miss attacks that use SSL, code obfuscation and other anti-forensic methods.

A recent study by M86 Security Labs used three scanners on 15,000 active malicious URLs. The outcome? Anti-virus blocked 39 percent of the 15,000 active malicious URLs, leaving 61 percent of malicious URLs undetected. Considering that three scanners were used for this test, the individual results of any single anti-virus application would have been worse.

With dynamic cyber-attacks, malicious content is morphed during distribution, so no matching signature is available. In fact, one-shot signatures will never be captured in an anti-virus database. JavaScript® and other mobile code can be written in different ways and modified to target the same vulnerability. To block this code, a signature is required for each possible code structure. Even with the use of statistical or heuristic models, only limited success can be achieved. Moreover, Polymorphic viruses continuously morph so future signature updates will not detect them.

Real-time Proactive Technology

It is important to scan all content as users access it and to identify potential threats without the need for a historical signature database lookup. With Real-time Code Analysis, all inbound and outbound Web content is scanned and analyzed at the time of the request—before it is delivered to the user. By determining code intent, known and undiscovered Crimeware, malware, Trojans, targeted attacks and other malicious web content are detected and blocked before they can penetrate corporate networks.

In an M86 Security Labs study, at least six in 10 malicious URLs pass undetected in the absence of real-time code analysis technology. http://www.m86security.com/documents/pdfs/security_labs/security_labs_report.pdf

Step 5: Implement an Effective Internet Acceptable Use Policy (AUP)

Establish thorough policies that address all Web, social networking and Web 2.0 tools currently in use or that might be used in the future. To be successful, an Acceptable Use Policy must be enforceable. This usually requires the installation of security software or hardware that monitors, blocks and reports inappropriate use of an organization's IT infrastructure.

5a: Create the Policy

Though communicating and enforcing your AUP is imperative, employees should be able to focus on their jobs without worrying about Web security. As part of a basic AUP, your organization should address the following factors:

Policy requirements for AUPs

- Outline what is and isn't acceptable, while preserving company culture.
- Involve human resources, executive management and an employee committee, if possible, when creating corporate and departmental Internet AUPs.
- Include policies for onsite and mobile users.
- Select a solution that can differentiate between internal and external users and allows policies to be established based on location or time of day.
- Inform staff about what is acceptable inside and outside business hours, if there is any difference. This needs to be stated clearly in the policy.
- Reserve the right to monitor all Web access on the company network, and inform employees about your monitoring and reporting policy.
- Enforce policies and set precedents consistently.
- Identify specific acceptable uses for different individuals or groups because blanket policies do not work.

Choose solutions that enable flexible policy enforcement options for employees who rely on Web-based tools. Look for technologies such as M86's Granular Social Media Control, administrators to flexibly manage access to social media sites by user groups...

Policy requirements for content

- Determine which employee, partner, customer and business data should be protected and include rules that address data distribution both within and outside of your organization.
- Include social media policies that protect brand identity and image.

Policy requirements for governance

- Determine which industry, regional or federal compliance regulations apply to your organization and address these requirements in the AUP.

5b: Communicate the Policy

Once you've created the appropriate policy for your organization, educate your users about what constitutes acceptable Web use and explain how the policy will be enforced. Policy communication should:

- Customize the block or coach page and explain why action was taken to block or warn the user.
- Include a link on the block or coach page for information about your corporate Internet AUP to reinforce and re-educate users about the policy.

5c: Enforce the Policy

Though policy communication is an important first step, technical enforcement of the policy removes the security burden from users and ensures adherence to your organization's Internet AUP. When implementing policy enforcement methods, you should:

- Select a centrally-managed solution that provides consistent security policy for onsite, remote and mobile users.
- Select a solution that offers flexible allowing, blocking and coaching modes for different users/groups.
- Choose solutions that enable flexible policy enforcement options for employees who rely on Web-based tools. Look for technologies such as M86's Granular Social Media Control. This allows administrators to manage access to social media sites by user groups flexibly—allowing everything from full access to read-only access (ability to post status, comments and updates disabled) to no access.

Step 6: Monitor, Report and Adjust Regularly

An important part of any Web security solution is reporting. The ability to quickly generate reports and store data helps enforce your Internet AUP and enables long-term proof of compliance. When choosing a reporting solution, you should:

- Decide whether you need high-level or detailed forensic reports.
- Determine who will require reports and how long you need to keep data. If increased data storage is required for regulatory compliance or if user data must be stored on-premises, consider a standalone reporting solution that can be kept onsite.
- Determine what you want to monitor regularly. If a complete view of your onsite, remote and mobile use is required, look for a reporting solution that receives all Web traffic.
- Save time by scheduling the reports and automate report delivery on a weekly, monthly or yearly basis. Or determine what activity or behavior will trigger an audit or report, such as multiple violations occurring within a short period of time.
- Establish a regular yearly audit of your organization's Web security controls. Identify holes in security systems, including unprotected ports, unmonitored application protocols, outdated or inadequate policies, etc.
- Involve key stakeholders from different departments when evaluating corporate and departmental Internet AUPs.

Once you've evaluated the best practices steps above, you can more easily identify the most appropriate and effective Web security solution for your organization.

CHOOSING THE RIGHT SOLUTION FOR YOUR ORGANIZATION

A Web gateway solution that offers proactive, real-time security protection against Web threats as well as policy management and reporting is ideal.

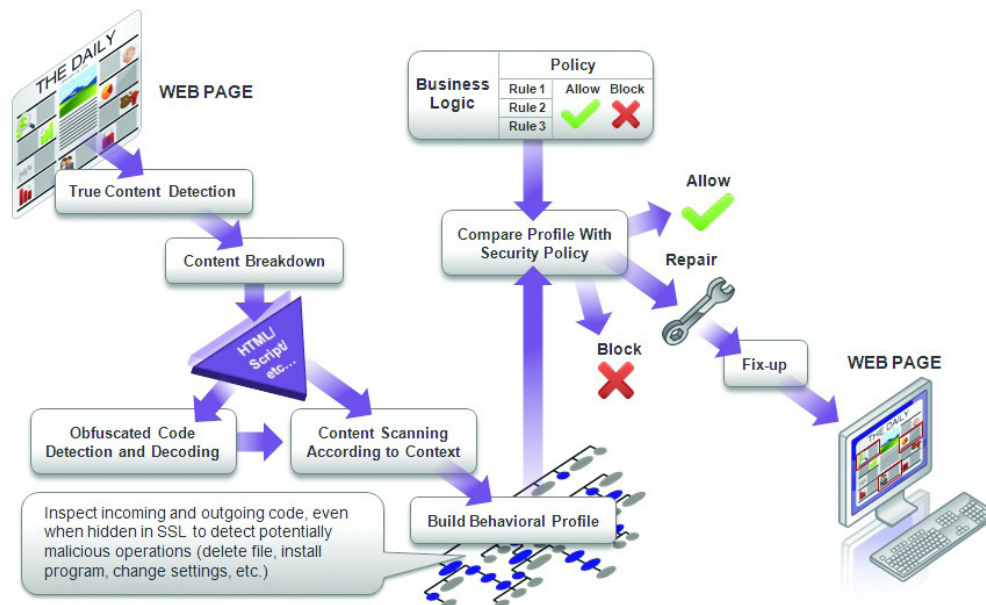
M86 Security addresses the challenges described in this paper with the M86 Secure Web Gateway (M86 SWG), a proactive solution that:

- Secures onsite, mobile and remote office employees.
- Prevents data leakage and reputation loss that can result from inappropriate employee posts to Web 2.0 sites.
- Offers proactive protection from Web threats at the gateway with patented Real-time Code Analysis and Dynamic Web Repair™ technologies.
- Includes the M86 Web Filter List, multiple anti-virus options and real-time proactive technology for a total solution. By layering reactive and proactive controls, it provides optimum performance for speed and detection rates.
- Provides policy enforcement and granular social media controls.
- Enables easy access to high-level and detailed forensic reporting for regular security and policy audits.

The M86 SWG protects organizations from new and dynamic malware using real-time code analysis technology. Through policy enforcement and granular Web controls, it enables organizations to manage productivity, reduce data breach risks and access Web 2.0 applications safely. When combined with the scalable M86 Security Reporter, it offers fast, detailed reporting for visibility into Web activity and long-term proof of compliance. Its hybrid cloud option extends full, consistent protection to mobile and remote users through a single management interface. Easy to manage and integrate, the M86 SWG requires minimal support and resources, making it a cost-effective solution.

How the M86 Secure Web Gateway Analyzes a Web Page

1. All content is analyzed for its true content type.
2. The content is then broken down into its separate parts.
3. These parts are processed by the specialist processing engines in the Real-time Code Analysis technology, such as the PDF scanner, JavaScript scanner, behavioral engine, etc.
4. This results in an overall behavioral profile for the Web page which is then compared with the user's security policy.
5. The security policy defines what is blocked, allowed or removed from the page.
6. Before the Web page is delivered, the Dynamic Web Repair™ engine ensures that the page is safe for the user to view.



M86 achieves the highest rate of malicious code prevention by analyzing every piece of web content in real time, regardless of its original source.

BENEFITS OF THE M86 SECURE WEB GATEWAY

The M86 SWG protects organizations at the Web gateway, using complementary technologies that prevent malware in real time, ensure uninterrupted productivity and assist with policy enforcement.

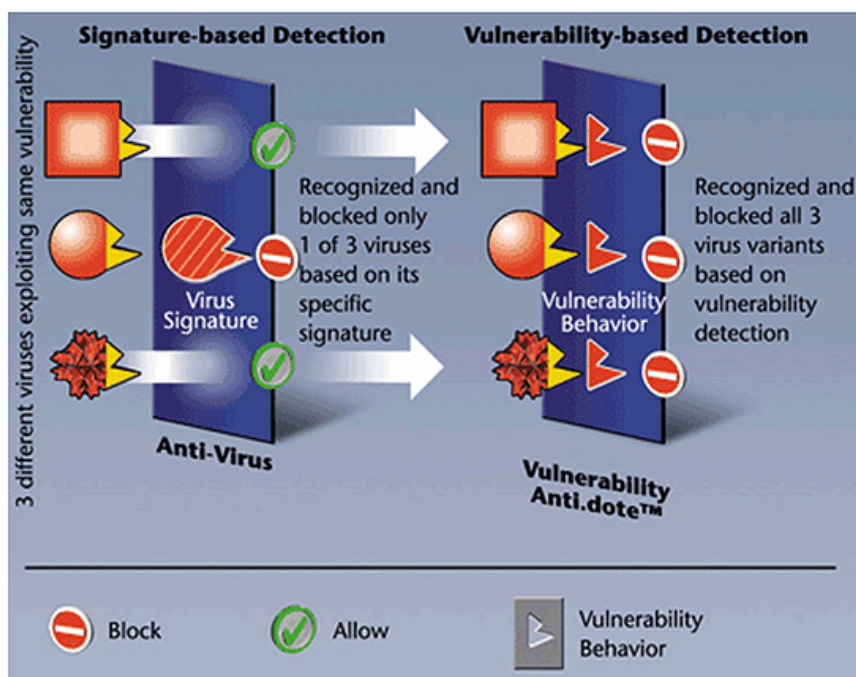
Web Security

Real-time Malware Protection

With M86's **Real-time Code Analysis** technology, it's easy to protect your organization from new and unknown web threats such as spyware, phishing, Trojans, obfuscated code, Web 2.0/AJAX exploits and other malicious code. This technology enables organizations to block malicious attacks on-the-fly, without requiring signatures or patches. M86 achieves the highest rate of malicious code prevention by analyzing every piece of web content in real time, regardless of its original source. This is the only security solution capable of understanding the true intent of the code in real time and then blocking/allowing the content based on that intent. M86 prevents any malicious web content from entering the corporate network, allowing companies to maximize productivity without security concerns.

Elimination of Vulnerabilities

Vulnerability Anti.dote™ technology provides an optimal balance between powerful, proactive web security and minimal patch management overhead. Based on M86's knowledge of new software vulnerabilities, behavioral rules are created that enable Vulnerability Anti.dote scanning engines to identify and block content that tries to exploit one or more vulnerabilities.



Productivity Enablement

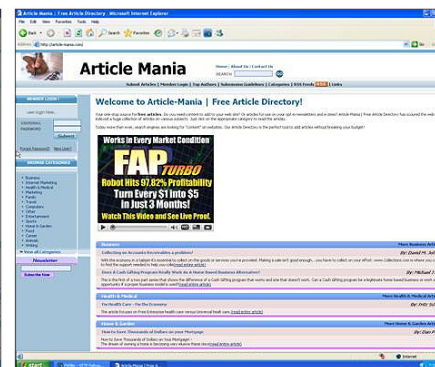
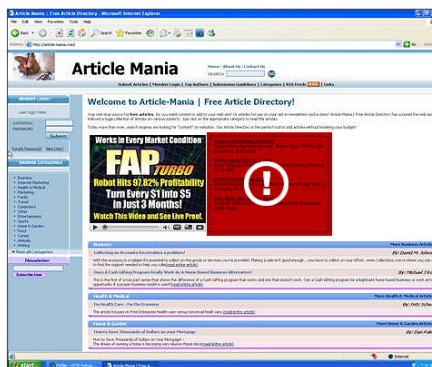
Most security solutions simply block infected web pages on legitimate websites, prohibiting users from accessing the information they need. **M86 Dynamic Web Repair™** technology neutralizes malicious code—without blocking the web page. It then repairs the content and delivers it to the user, maintaining productivity. This helps reduce the threats that can be found on legitimate websites, and it significantly reduces help desk calls from users blocked from job-related sites.

In a recent M86 test of almost one million URLs (from the Alexa list of top sites), Dynamic Web Repair™ fixed 99 percent of malicious URLs (from the Alexa list of top sites), Dynamic Web Repair™ fixed 99 percent of malicious URLs.

In a recent M86 test of almost one million URLs (from the Alexa list of top sites), Dynamic Web Repair™ fixed 99 percent of malicious URLs. This technology removes specific, malicious code script without impacting the page structure or functionality. Many other solutions remove all Flash elements, ad banners, etc., because they are unable to analyze the code in real time and are forced to remove the good and the bad. This means a safe Flash product video could be removed along with a third-party ad that could contain malware, preventing the user from accessing necessary content.

Without Dynamic Web Repair: The website hosts a virus (Trojan Downloader.JS.iFrame.aqf)

Using Dynamic Web Repair: The same page with malicious content removed and repaired



Social Media and Productivity Control

Often, organizations are forced to choose between allowing uncontrolled Web 2.0 access and blocking these sites completely. M86's **Granular Social Media Control** enables organizations to run websites for selected users in read-only mode to block posts, comments or uploads to Web 2.0 sites, while allowing users to access other site functions. This prevents posts or uploads that could leak critical data or lead to reputation damage.

With the **M86 Web Filter List**, M86 SWG customers have access to the industry's leading URL list with more than 100 categories for granular policy enforcement.

Coverage for Mobile, Remote and Branch Office Users

The **M86 Secure Web Service Hybrid** is the first Web security solution to integrate Real-time Code Analysis, on-premises appliance technology and cloud-based services within a single management interface. Web security policies are managed using a single management console, providing consistent coverage to mobile and remote users—the same robust security provided to onsite workers.

Visibility into Web Activities through Reporting

The M86 Security Reporter is a scalable solution that provides a complete view of an organization's Web activities. Deep, forensic security reporting provides a wide range of reporting views and dashboards, and reports can be scheduled and customized to fit the needs of individual stakeholders.

Many reporting solutions impose limits on data, but the M86 Security Reporter includes up to 12 TB of storage, allowing organizations to prove compliance and meet legal discovery requirements for years of Web activity data.

The M86 Secure Web Service Hybrid is the first Web security solution to integrate Real-time Code Analysis, on-premises appliance technology and cloud-based services within a single management interface.

CONCLUSION

What is an acceptable level of risk? Each organization has a different answer, and it's important to evaluate individual security requirements and productivity tools before selecting the most appropriate solution. Today's sophisticated security challenges have lowered risk tolerance among all businesses. Malware infiltrates legitimate websites and social media applications, leaving users, data and networks vulnerable, and no organization is immune to cyber-attacks.

The M86 Secure Web Gateway provides proactive malware prevention as well as productivity-enabling technologies that safeguard users while allowing them to do their jobs efficiently. And it significantly reduces risks—to compliance, reputation, data and cyber theft.

To learn more about the most effective ways to protect your organization from the latest Web-based threats, visit www.m86security.com.

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 25,000 customers and 26 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.

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
Suite 3, Level 7, 100 Walker St.
North Sydney NSW 2060
Australia
Phone: +61 (0)2 9466 5800
Fax: +61 (0)2 9466 5899

Version 10/14/10