



## Seven Design Requirements for Web 2.0 Threat Prevention

## Table of Contents

Executive Summary	3
Introduction	3
Web 2.0 Defined	4
Web 2.0 Delivers Business Value	5
Web 2.0 Security Concerns	5
Inbound threats	5
“But we are spending billions worldwide on security!!!”	6
Outbound Threats	8
Solving the Web 2.0 Security Dilemma	8
Recommendations	8
The Solution: Seven Design Requirements for Web 2.0 Threat Prevention	9
Requirement #1: Deploy real-time reputation-based URL and message filtering for all domains—even those not yet categorized	9
Requirement #2: Deploy anti-malware protection utilizing real-time, local “intent-based” analysis of code to protect against unknown threats, as well as signature-based, anti-malware protection for known threats	10
Requirement #3: implement bi-directional filtering and application control at the gateway for all web traffic, including web protocols from HTTP to IM and encrypted traffic	10
Requirement #4: Data leakage protection on all key and web messaging protocols	10
Requirement #5: Ensure that all caches and proxies are “security-aware” for safety and efficiency gains	11
Requirement #6: Design security infrastructure for layering of defenses with minimal number of secure devices	11
Requirement #7: Use comprehensive access, management, and reporting tools	12
McAfee Products and Technologies for Web 2.0 Protection	12
Integrated Gateway Appliances	13
McAfee Web Gateway	13
McAfee Email Gateway	14
Data loss prevention	15
Data loss prevention products and services	15
McAfee Security Technologies	15
TrustedSource	15
Anti-malware module	16
Conclusion	17
Next Steps	17
About McAfee	18

### Executive Summary

Today's web is helping change how and where we work. Is Web 2.0 technology used in your business? Do you know if your web gateway, applications and confidential data are at risk?

The aging web and messaging security solutions that most enterprises currently have in place are simply not providing the protection that's needed in today's dynamic environment. To both enable Web 2.0 use and address Web 2.0 threats effectively, companies need to build on traditional security protocols with a new generation of multi-layered security that includes both inbound and outbound protection, reputation-based filtering, and multi-function security appliances at the network gateway. A new Forrester Consulting study titled *Next-Generation Secure Web Gateway Trends and Requirements* finds that while use of Web 2.0 is enabling business and growing, a majority of organizations continue to lose the battle against the non-relenting Web 2.0 threats—losing in terms of infections, data loss, and costs to the business.<sup>1</sup> Compared to a similar study conducted in 2007<sup>2</sup>, the new research shows rapid adoption of Web 2.0 technologies, associated malware threats and an increasingly mobile and distributed workforce are driving requirements for next generation web security gateways.<sup>1</sup>

Drawing on customer experience; data gathered from McAfee's global web and messaging reputation system, TrustedSource™ technology; and the findings of Forrester Consulting and other third-party sources, we'll outline in this paper the new Web 2.0 threats and explain why most security solutions in place today can't adequately protect against these threats. We'll then propose a set of Seven Design Requirements for Web 2.0 Threat Prevention, and give an overview of McAfee product and technology offerings that address these requirements.

### Introduction

The Internet today is a different place than it once was. Widely referred to as "Web 2.0," today's more interconnected and interactive Internet will continue to evolve as innovators use new web technologies to implement new applications. Too often, however, Web 2.0 innovations are designed with security as an afterthought, while end-user adoption of Web 2.0 far outpaces the implementation of adequate security solutions.

Applications are now Internet-enabled, and corporate intranets and extranets are supporting critical business processes. Entire businesses are being built on web infrastructures, with many mainstream organizations already using sophisticated Web 2.0 technologies both internally and externally. Today's business model relies on the web to provide inbound access for remote employees, partners, and customers from any location, anywhere in the world. Internal employees also reach beyond the edge of the corporate network to communicate and gather information across the Internet. These innovations have brought businesses great efficiencies, and have enabled companies to affordably expand their sphere around the globe.

However, the addition of rich, browser-based, bidirectional Web 2.0 applications to this web-dependant business model introduces major new risks to the enterprise. When web-based communications are both inbound and outbound, so too are the related threats. And as Web 2.0 has become an integral part of legitimate business operations, so too has it become integral to Internet-based criminal operations.

Security officers and IT professionals have a tough job: protecting the enterprise from malware, ensuring regulatory compliance, and preventing data leakage—all while ensuring that employees can stay productive. These security issues exist for all IP-based traffic, whether email, VoIP, instant messaging, web access, file transfers, or other enterprise applications communicating over IP.

In short, Web 2.0 and related applications expose organizations to both inbound and outbound security threats that overmatch the legacy security measures originally designed for a simpler, less interactive web

1 "Next-Generation Secure Web Gateway Trends and Requirements," Forrester Consulting, December 2008.

2 "Internet Risk Management in the Web 2.0 World," Forrester Consulting, September 2007.

environment. A new generation of security threats is bringing malicious attacks led by highly organized cyber-criminals with sophisticated tools, targeting specific organizations to disrupt business, steal sensitive information, and profit financially.

Read on as we take a closer look at these new threats and why legacy web security solutions offer limited protection. We'll then outline a new, proactive security paradigm to help you secure Web 2.0 applications and protect your enterprise and the employees that use these applications on a daily basis.

**Web 2.0 Defined**

The original definition of Web 2.0 has been credited to Tim O'Reilly and O'Reilly Media, and was said to be the result of a brainstorming session that resulted in the first Web 2.0 Conference. A true, definitive definition of Web 2.0 is hard to pin down. In fact, a static definition would be impossible because Web. 2.0 is in its essence dynamic. In the initial brainstorming session, Tom O'Reilly and O'Reilly Media formulated a sense of Web 2.0 by example:

McAfee Web Gateway (Webwasher), detected 99.7 percent out of the 1,164,662 samples.<sup>3</sup>

Web 1.0		Web 2.0
DoubleClick	⇒	Googe AdSense
Ofoto	⇒	Flickr
Akamai	⇒	BitTorrent
mp3.com	⇒	Napster
Britannica Online	⇒	Wikipedia
personal Websites	⇒	Blogging
evite	⇒	upcoming.org and EVDB
domain name speculation	⇒	search engine optimization
page view	⇒	cost per click
screen scraping	⇒	Web services
publishing	⇒	participation
content management systems	⇒	tagging ("folksonomy")
stickiness	⇒	syndication

This definition-by example-was originally published in Tim O'Reilly's 2005 article, "What is Web 2.0."<sup>4</sup> Analyzing O'Reilly's examples, we can see that the movement from Web 1.0 to Web 2.0 involves an improvement in the user experience, adding features that respond to user input and that often allow the user to create or influence the content provided by web-based applications. Compared to the first generation of websites—which were largely read-only—Web 2.0 offers interactive technologies and personalized usage models such as blogging, social bookmarking, wikis, podcasts, RSS feeds, online communities, and online web services such as eBay and Gmail.

The phrase "Web 2.0" characterizes these "upgrades" to the web experience, in the same way that version numbering is commonly used to designate software upgrades. However, as actor, comedian, author, and broadcaster Stephen Fry has pointed out in a widely seen interview, Web 2.0 differs from the traditional model of software upgrades. It's not the web platform itself that has changed, Fry explains. Instead, Web 2.0 is "...an idea in people's heads rather than a reality. It's actually an idea that the reciprocity between the user and the provider is what's emphasized. In other words, genuine interactivity, if you like, simply because people can upload as well as download."<sup>5</sup>

3 "AV-Test release latest results," Virus Bulletin, September 2008. [http://www.virusbtn.com/news/2008/09\\_02](http://www.virusbtn.com/news/2008/09_02)

4 <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-Web-20.html>

5 <http://www.videojug.com/interview/stephen-fry-web-20>

Beyond delivering two-way interactivity, Web 2.0 also signals a transition from websites as isolated information silos to interlinked computing platforms that behave more like software, as well as to an interlinked social environment where users have the freedom to generate, distribute, share, and re-use content. Taken together, all these characteristics allow the web to provide more value to individual users, as well as to companies that are incorporating Web 2.0 capabilities into their business processes.

**Web 2.0 Delivers Business Value**

Some of the most popular Web 2.0 applications are consumer-focused, and include music- and video-sharing, social networking, and other interactive web experiences that some employees may be tempted to use on their company-provided equipment. On the other hand, use of Web 2.0 applications is changing and many sites previously thought to be consumer-focused now have the potential to deliver significant business value. The studies by Forrester Consulting confirm this fact, showing that numerous Web 2.0 applications are useful for business purposes.<sup>6</sup> The studies show that while webmail and content sharing applications use may have declined slightly they continue to find high business value year-over-year. The real growth in Web 2.0 use for business purposes appears to be for the streaming media and social network sites.

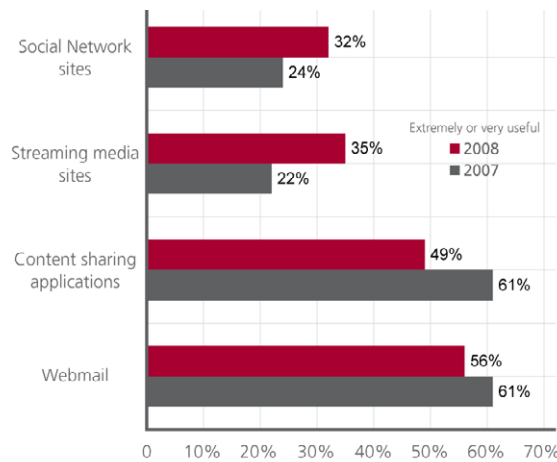


Figure 1: Please rate the usefulness of each category of Web 2.0 application for your organization

Because individual users and entire enterprises find Web 2.0 to be incredibly useful, it's here to stay. Given that fact, how do you secure the enterprise against the threats created by the broad adoption of Web 2.0 applications?

**Web 2.0 Security Concerns**

**Inbound threats**

The press is full of examples of Web 2.0 security threats, such as the Monster.com data breach<sup>7</sup> and the Heartland data breach that enabled malware to steal compromised credit card data.<sup>8</sup> Hacking tools continue to be developed to help cyber-criminals create sophisticated malware. Many of these malicious tools are widely available on the Internet at low cost, and are developed with simple "point and click" interfaces, lowering the skill level required to break into corporate computers in order to disrupt operations or steal information.

<sup>6</sup> "Internet Risk Management in the Web 2.0 World," Forrester Consulting, September 2007.

<sup>7</sup> <http://www.msnbc.com/id/20534586/>

<sup>8</sup> <http://www.networkworld.com/news/2009/012009-heartland-security-breach.html>

Many of these threats are greatly refined, using not only Web (HTTP) but also encrypted (HTTPS) and email (SMTP) protocols to pull off their attacks. One example reported in PCWorld demonstrates that no site is immune from malware attacks, including a community action site for President Obama, “The scam starts when the victim sees what appears to be a video posted to the my.barackobama.com website. It reads simply “click here to see movie.” By clicking on the fake video, the user is taken to another website that looks like a YouTube page filled with pornography. Clicking on the fake YouTube link prompts the victim to download what appears to be a piece of video decompression software called a codec. The fake codec is actually the Trojan program.”<sup>9</sup>

And since Web 2.0 enables users’ to post links and information on other sites, the malware easily propagates. The PCWorld article explains, “To make matters worse, hackers are also putting links to the malicious Barackobama.com pages in comment forms all over the web, making them likely to come up as Google searches results. Because of the way search engines work, pages hosted on a popular site like Barackobama.com are typically given a higher search result ranking than other web pages.”

The publicity around such attacks has not gone unnoticed. Enterprise security management is aware of the security risks inherent in the adoption of Web 2.0 technologies and applications. The Forrester studies found that data leakage and viruses were the top two concerns in both the 2007 and 2008 studies, with concerns about data leakage over the web inching slightly ahead of viruses in 2008. This risk appears to concern large organizations more than those with 1,000 or less employees.<sup>10</sup>

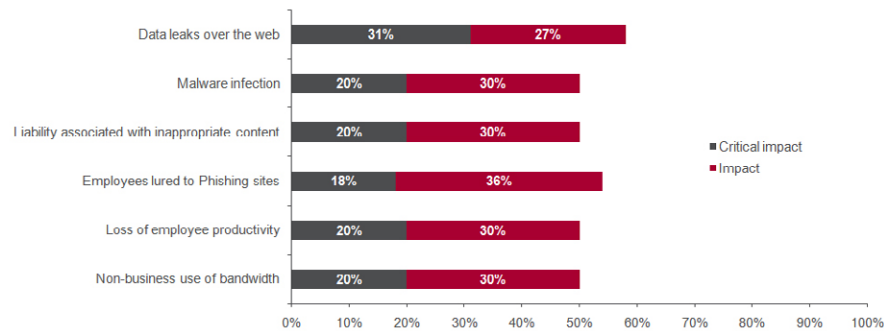


Figure 2: Data leaks have significant business impact

**“But we are spending billions worldwide on security!!!”**

Over time, the majority of security issues have been addressed with the underlying protocols for Web 1.0. And organizations have deployed solutions like signature-based anti-virus and category-based web filtering to bolster security, providing very effective in protection against early Web 1.0 threats. Yet the attacks continue and security managers are rightfully concerned.

Today’s layering of new next-generation programming languages on top of the underlying protocols in Web 2.0 has given those with malicious intent a whole new set of technologies to exploit. Signature-based solutions and other Web 1.0 security practices continue to be a necessary part of the security infrastructure, but they’re no longer enough by themselves. A great example of the security gap is AJAX, the popular Web 2.0 programming language. The asynchronous nature of AJAX clearly improves the users’ experience on a website by taking interactivity to an entirely new level. However, it also dramatically increases the chances that things can go terribly wrong from a security perspective.

One tactic used by cyber-criminals is to leverage their sophisticated knowledge to plant worms on host machines. These compromised machines, known as zombies, are rented out to carry out phishing, spam or other attacks.<sup>10</sup>

In addition to for-hire zombie networks (“botnets”) cyber-criminals also use sophisticated tools to deploy seemingly innocent content which actually contains Trojan horses with malicious functions. These targeted Trojan horses present a threat to the organization in that, on the surface, they appear harmless and may even take the form of a useful application or an entertaining game. Often these attacks utilize common productivity tools like MS Office files transmitted via work email or via personal email that employees access via encrypted web mail. Once opened by the recipient, the Trojan is released, opening the door for corporate data espionage, data theft, and the release of additional malware. Traditional anti-virus solutions are ineffective in stopping the attack because there is no known signature.

Targeted attacks are increasingly brief in duration and small in the number of samples sent out. Often they consist of malware that is designed to bypass the targeted company’s signature-based anti-virus protection. Since the attack can end in just a few hours, data may have already been stolen before anyone knows it has happened.<sup>11, 12</sup>

And it is not just files coming into an organization with hidden Trojans that can introduce malware. Seemingly innocent web pages that employees may access for legitimate purposes can introduce malware or spyware into a network. This is potentially much more dangerous. Users can be educated not to click on suspicious email attachments, but malicious websites may contain active code that launches automatically as soon as the web page is viewed. Can we teach an end end-user what sites are trustworthy and which are not? Unfortunately we can’t.

One example of how signature-based anti-virus protection and category-based URL filtering have become obsolete due to the dynamic nature of Web 2.0 threats is a program now available called “eVade o’Matic Module,” or VOMM for short, which automates the creation and modification of code so that it constantly changes its signature to avoid anti-virus detection while taking advantage of the same browser vulnerability. VOMM enables malicious code to literally have an infinite number of possible signatures, so that the malware can always stay a step ahead of the anti-virus software. In short, its purpose is to make an intrusion attempt undetectable by signature-based anti-virus protection.<sup>13</sup>

Malicious attacks are also now utilizing the very technologies that were created to provide security. For example, to secure financial transactions, encrypted HTTP was created (HTTPS) to ensure that financial data was not “in the clear” on the Internet. However, attackers can also use this secure connection to transmit malware, and carry out a malicious attack that is undetectable by legacy security solutions like anti-virus.<sup>14</sup> Because most legacy security solutions cannot be applied to encrypted traffic, we refer to this portion of network traffic as the “SSL blind spot.”

Is it any wonder then, that worldwide, organizations collectively spend billions each year on security software—especially signature-based anti-virus solutions—yet organizations are not adequately protected?

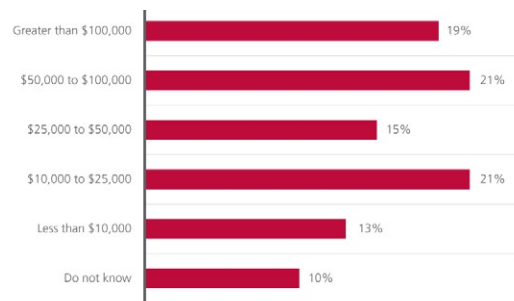


Figure 3: In the past fiscal year, how much did your organization spend on malware cleanup?

11 [http://news.com.com/2102-7349\\_3-6125453.html?tag=st.util.print](http://news.com.com/2102-7349_3-6125453.html?tag=st.util.print)  
12 <http://www.itpro.co.uk/security/news/99467/2006-the-year-of-targeted-malware.html>  
13 <http://www.itsecurity.com/features/news-feature-metasploit-vomm-102906/>  
14 [http://www.windowsecurity.com/whitepapers/Hackers\\_Tricks\\_to\\_Avoid\\_Detection\\_.html](http://www.windowsecurity.com/whitepapers/Hackers_Tricks_to_Avoid_Detection_.html)

The 2008 Forrester study notes:

- Year after year, despite the proliferation of anti-virus software, these cost figures do not let up. The reality is that web-based malware is a whole new class of threats, different from traditional computer viruses. It requires different analysis and detection methods, which are still nascent for many web filtering solutions.
- The cost figures are clearly dependent on the size of the organization—large companies tend to spend more on malware cleanup. In our study, we found that companies with 3,000 or more employees are more likely to spend more than \$100,000 per year on malware cleanup, while none on the sub-1,000 organizations spent more than \$100,000.

### Outbound Threats

In addition to inbound threats, there are also outbound data leakage threats that jeopardize critical and sensitive information vital to an organization's success. Attackers aren't always outsiders in faraway countries. Data thieves, industrial spies, and cyber-vandals can, and often do, operate within a company's own boundaries. Moreover, outbound threats aren't always the result of an intentional attack by an insider; sometimes they occur when an employee unintentionally opens or allows a "back door" to be opened by downloading a rogue application that has not been approved by IT.

Outbound data leakage is a concern for two reasons: the risk of intellectual property loss and the need to comply with regulatory mandates and industry requirements, including SOX, HIPAA, GLBA, PCI, and more. Many organizations imagine that simply filtering their email provides sufficient protection. While doing so is a key factor in a leakage prevention strategy, a multi-protocol approach to data leakage security—where network security administrators also pay attention to web protocols—is best. Rapid adoption of blogs, wikis, and employee access to personal email (which is sometimes encrypted) via the web are all potential data leakage points for the enterprise. As a result web (HTTP), encrypted web (HTTPS), instant messaging (IM), and file transfers (FTP) are all potential data leakage methodologies because all of these protocols can be used to convey proprietary information out of the enterprise.

The 2008 Forrester study found that organizations are beginning to look to web filtering solutions to perform data leak prevention.

### Solving the Web 2.0 Security Dilemma

As we have seen, existing deployments of legacy category-only web filtering and signature-based anti-virus solutions are inadequate to protect against Web 2.0 threats. The Forrester studies show that organizations widely recognize this fact. Given the security gap, what should organizations do to provide strong security in our rapidly evolving Web 2.0 world?

### Recommendations

The 2008 Forrester study suggests organizations considering security enhancements, including next-generation web filtering technologies, should look to vendors with these capabilities:

- Malware detection that specifically addresses web-borne threats
- A solid in-the-cloud infrastructure
- Strong integration and consolidation strategy
- Fine-grained Web 2.0 application control

### The Solution: Seven Design Requirements for Web 2.0 Threat Prevention

Forrester's recommendations include product and technology investments in next-generation proactive protection. To achieve this, McAfee recommends implementing these *Seven Design Requirements for Web 2.0 Threat Prevention*:

1. Deploy proactive, real-time, reputation-based URL and message filtering for all domains—even those not yet categorized
2. Deploy anti-malware protection utilizing real-time, local “intent-based” analysis of code to protect against unknown threats, as well as signature-based, anti-malware protection for known threats
3. Implement bi-directional filtering and application control at the gateway for all web traffic, including web protocols from HTTP to IM and encrypted traffic
4. Monitor for, and protect against, data leakage on all key web and messaging protocols
5. Ensure that, when deployed, all proxies and caches are fully security-aware
6. Design layered defenses with a minimal number of proven and secured devices
7. Use robust management and audit reporting tools for all web and messaging protocols, services, and solutions including filtering, malware, and caching.

#### **Requirement #1: Deploy real-time reputation-based URL and message filtering for all domains—even those not yet categorized**

Just as legacy anti-virus solutions that utilize signatures are inadequate to stop malware, legacy URL filtering solutions are also insufficient. These solutions rely on categorized databases of URL entries that are updated only a few times per day. What is needed is a “reputation system” that assigns global reputations to URLs and IP addresses, working alongside categorized databases to provide an additional layer of protection far stronger than URL filtering alone.

A sophisticated, third-generation reputation system provides a mechanism for determining the risk associated with receiving data from a particular website. This reputation can be used in conjunction with categories in an organization's security policy, providing the ability to make appropriate decisions based on both category and security reputation information. This reputation-based URL filtering solution needs to be global in scope and internationalized to handle websites in any language.

It is critical that the reputation system provide both web and messaging reputation. Since malicious attacks are often based on multiple protocols, the reputation system must be aware of both email and web threats. For example, a new domain without content cannot be categorized, but if it is associated with IP addresses that have a history of sending spam, phishing attacks, or other malicious emails, then the web reputation for this uncategorized domain can be determined and security protection can be provided to users who try to access the domain.

Organizations should deploy email gateways that utilize sender reputation to stop malicious attacks, often launched via spam and social engineering. Email reputation is also critical as spam, phishing and other malicious emails will include an URL or IP address that needs to be immediately fed back into the Web gateway security infrastructure.

**Requirement #2: Deploy anti-malware protection utilizing real-time, local “intent-based” analysis of code to protect against unknown threats, as well as signature-based, anti-malware protection for known threats**

Enterprises should deploy intent-based anti-malware at both the web and email gateway. These solutions include a signature-based anti-virus engine to stop known threats but, more importantly, address the problem illustrated in the 2007 Forrester study:

Realigning your security policies with risk initiatives would call for shifting malware protection to be the No. 1 priority. This should result in the subsequent deployment of Web-filtering capabilities beyond URL filtering and signature scanning. More specifically, protection against Web-borne malware should include website reputations, real-time behavioral analysis, and heuristics-based detection that allows for more thorough content inspection and detection of zero-day threats.<sup>15</sup>

These malware solutions utilize “intent-based” analysis to examine code at the gateway entering via an email attachment or mobile code that will execute in the browser. Malware protection should:

- Perform a “magicbyte” analysis of each file to determine the actual file type
- Safeguard against files that are disguised to be something they are not
- Disallow media types that are potentially hazardous (like unknown ActiveX)
- Check active code for valid digital signatures
- Execute behavioral analysis to determine if it will behave in a known manner
- Analyze scripts to determine if they are trying to exploit vulnerabilities on the client
- Neutralize attacks as needed

Most important is notifying a global reputation system whenever any web or email gateway finds malware for which no signature exists. This is critical to participation in the reputation ecosystem. Whenever malware is found on a web page or in an email, the reputation system is notified so that the reputation for that domain or IP can be immediately updated to protect all organizations participating in the reputation ecosystem.

For more information on how to stop malware please see our Stopping the Targeted Attack white paper.<sup>16</sup>

**Requirement #3: implement bi-directional filtering and application control at the gateway for all web traffic, including web protocols from HTTP to IM and encrypted traffic**

Applications that communicate over encrypted and unencrypted protocols need to be controlled in both directions. This includes controlling access to websites, blogs, wikis, IM, P2P, and other applications, as well as monitoring the connections for malware coming in and data leakage going out. With the high percentages of corporate web traffic now being encrypted (HTTPS), it is imperative to be able to selectively decrypt this content at the gateway to provide security while respecting privacy for access to sensitive sites such as personal finance sites.

**Requirement #4: Data leakage protection on all key and web messaging protocols**

Providing data leakage protection on all outbound content via either the web or email requires a four-step process. From defining corporate and regulatory policies to detecting and enforcing them, to proving compliance to auditors, this process is the surest way to ensure that no inappropriate information ever leaves your gateway.

The four steps to achieve compliance are:

- *Policy definition*—Knowing what should be done and by whom
- *Violation detection*—Determining the actual content in a message and whether or not it constitutes sensitive information that needs to be protected
- *Automatic enforcement*—Applying the appropriate security measures based on content and senders
- *Reporting and auditing*—Proving what happened

Data leakage protection should be provided over encrypted and unencrypted protocols for both messaging and web traffic. As with application control, this includes controlling access to websites, blogs, wikis, IM, P2P, and other applications, as well as monitoring connections for data leakage. And as with application control, it is imperative to be able to selectively decrypt encrypted traffic at the gateway to provide security while respecting privacy for access to sensitive sites.

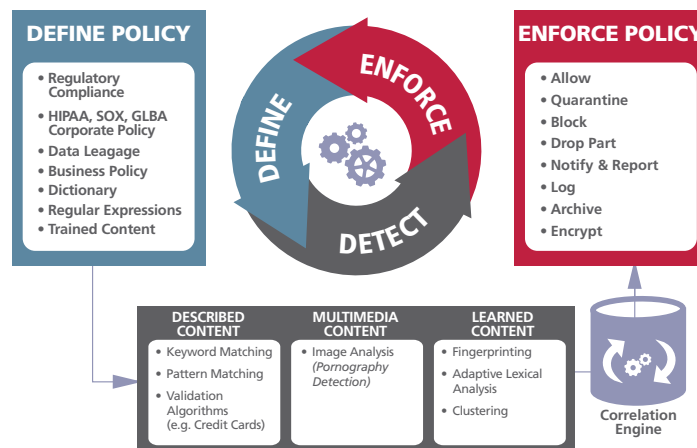


Figure 4: Data leakage requirements

**Requirement #5: Ensure that all caches and proxies are “security-aware” for safety and efficiency gains**

Objects that are cacheable must be filtered for malware, security reputation, and URL filtering policy prior to delivery to the requestor’s browser. Cached objects must have these filters applied each time the object is delivered to the end user because the reputation may have changed since the object was originally cached. Or, the security policy of this requestor may be different from previous requestors in terms of security reputation, URL filter policy, or malware. Deploying caches and proxies that are not security aware runs the risk of delivering malicious code to the user.

**Requirement #6: Design security infrastructure for layering of defenses with minimal number of secure devices**

Gateway security today provides for a robust point of policy definition, enforcement, and monitoring. Given the use of gateways as security enforcement points, it is important to ensure that the devices are secure, and to provide layering of defenses within the device as well as in concert with other devices and endpoint security. As we have seen, today’s most effective defense combines signature bases as well as reputation-based and intent-based defenses—all working together. In addition, devices must not create “blind spots” such as SSL traffic, or introduce new vulnerabilities themselves.

To cost-effectively manage risk, today's web gateway requirement is for a single-solution approach that houses the security and caching engines in the same application, tightly integrated, sharing the same memory, and—above all—residing on the same appliance. In addition to having fewer vendors to deal with, you get added protection by replacing point solutions with integrated, multifunction appliances that provide best-of-breed functionality, since the cache can be security-aware, malware detection can be integrated with reputation-based filtering, and so on. In addition, effective outbound protection can now be as important as inbound protection for protocols such as Web and SMTP. Solutions that manage both inbound and outbound risk reduce costs and increase security by providing for additional opportunities for consolidation and efficiency.

**Requirement #7: Use comprehensive access, management, and reporting tools**

Enterprises should deploy solutions that provide “at-a-glance” reporting on the status and health of their email and web gateways. They also need both real-time and forensic reporting that allows them to drill down into problems for remediation and post-event analysis. Robust and extensible reporting is critical to your ability to understand risk, refine policy, and measure compliance.

**McAfee Products and Technologies for Web 2.0 Protection**

Building on these principles, McAfee is actively investing in its web gateway security solution, McAfee® Web Gateway (Webwasher), its email gateway security solution, McAfee® Email Gateway (IronMail), and its data loss prevention products and services to provide the industry's most complete protection against threats from Web 2.0 and beyond. McAfee is positioned in the Leader's Quadrant of Gartner's Web Gateway Magic Quadrant<sup>17</sup> as well as the Email Security Boundaries Magic Quadrant.<sup>18</sup> The Web Gateway and Email Gateway solutions are also positioned as Top Players in Radicati Group's 2008 Market Quadrant's for web and email.<sup>19, 20</sup> In addition, we continue to invest in our core technologies to manage Web 2.0 risk, TrustedSource, our global reputation system that provides security to all customers on the TrustedSource network, as well as our award-winning and market-leading anti-malware and outbound compliance engines.

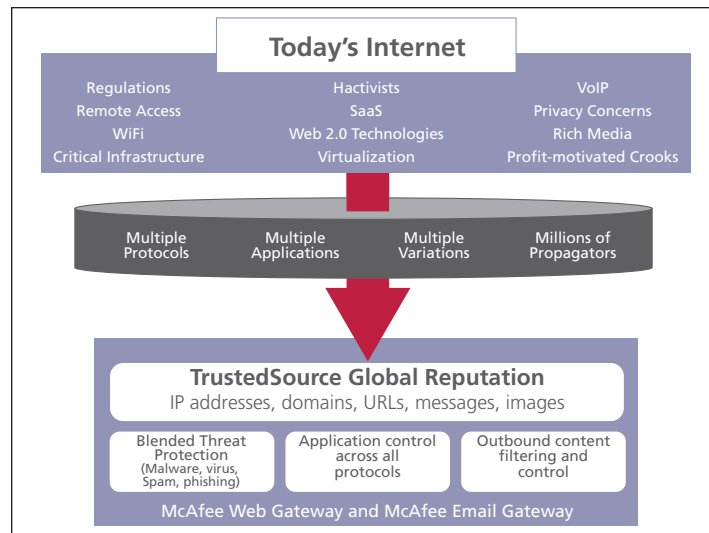


Figure 5: McAfee products and technologies for Web 2.0 Protection

17 Peter Firstbrook, Lawrence Orans, and Arabella Hallawell, “Magic Quadrant for Secure Web Gateway,” Gartner, Inc., 2008.

18 Peter Firstbrook and Arabella Hallawell, “Magic Quadrant for Email Security Boundaries,” Gartner, Inc., September 2008.

19 “Corporate Web Security—2008 Market Quadrant,” Radicati Group, Inc., June 2008.

20 Matt Anderson and Sara Radicati, “Email Security Appliances—2008 Market Quadrant,” Radicati Group, Inc., November 2008.

### Integrated Gateway Appliances

#### McAfee Web Gateway

McAfee Web Gateway delivers comprehensive protection against Internet-borne threats, including every aspect of Web 2.0 traffic. It filters all inbound and outbound web traffic for spyware, malware, viruses, data leakage, and Internet misuse. On the inbound side, the anti-malware engine not only scans for known virus signatures, it also analyzes the intent of all content and active code entering the network via web pages. The solution's deep content inspection can even detect and block harmful code that's SSL encrypted. All outbound traffic is inspected to enforce an organization's Internet use policy and protect it from losing confidential information through various web protocols. Finally, McAfee Web Gateway is the only Internet gateway product to employ TrustedSource global reputation protection.

McAfee Web Gateway is a truly integrated solution that replaces legacy point solutions. Its unified interface combines all the content protection applications enterprises need in one solution—including reputation-based web filtering, anti-malware (with anti-virus signatures), SSL scanning, a next-generation security cache, anti-spyware, and enterprise-level reporting on all web traffic. And McAfee Web Gateway integrates with McAfee Email Gateway intelligence. This is a critical feature since many of today's attacks utilize multiple modes—for example, an attack may begin with a seemingly innocent email with an embedded URL that, when accessed by the recipient, launches a web-based attack.

Traditional URL filtering solutions stop users from visiting certain sites that cause liability risks, loss of productivity, or sap bandwidth, but do very little to protect against legitimate websites that have been compromised. McAfee has defined a new standard in URL filtering with its integration of TrustedSource reputation technology, including reputations for millions of URLs in our award-winning McAfee web database. Instead of relying solely on a static list of categorized URLs, our web database enhances protection by adding "Internet reputation" to what is known about the URL and enables a "block or allow" decision based on real-time information. The ability to implement security policy based on both URL category and web reputation dramatically improves filtering accuracy and protection. Whenever a McAfee Web Gateway finds malware in a web page, the threat is not only stopped at the gateway but also reported back to McAfee via TrustedSource in real time, providing intelligence and protection to all our customers.

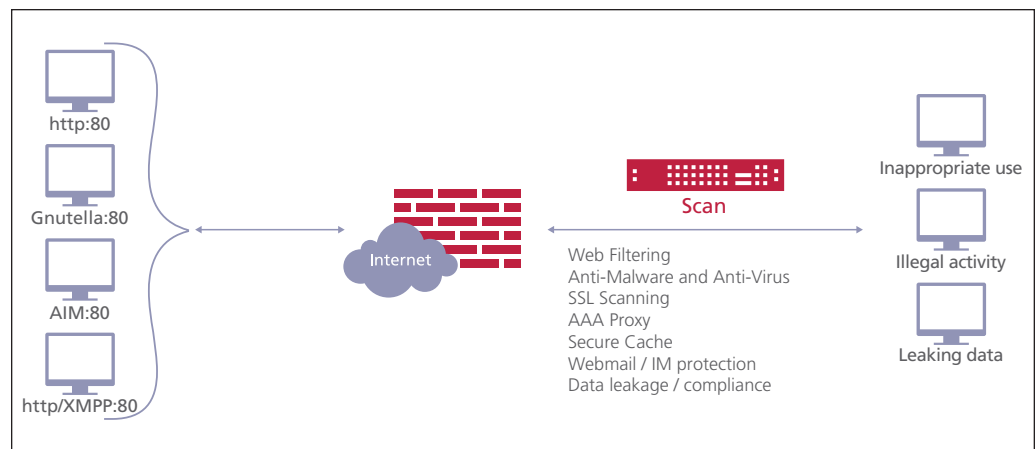


Figure 6: McAfee Web Gateway Solution: Protection from Web 2.0 Threats

### McAfee Email Gateway

Trusted by the world's largest and most respected organizations, including more than 52 percent of the Fortune 500, McAfee Email Gateway (Ironmail) is the most trusted solution in enterprise messaging security. It defends enterprises from inbound email-borne threats such as spam, viruses, phishing, directory harvest (DHA), denial-of-service attacks, and intrusions. With the industry's only 99 percent spam detection accuracy guarantee, McAfee Email Gateway combines local information from the network with TrustedSource global intelligence to provide the most complete protection against inbound threats. The solution also provides outbound protection against data leakage and policy violations to meet regulatory compliance such as HIPAA, PCI DSS, SOX, and GLBA. Administrators are empowered to deliver the best possible email protection and prove it with enterprise-class reporting, exportable report logs, real-time dashboards, and alerts. Included in this product line is the McAfee Email Gateway Encryption appliance.

McAfee Email Gateway blocks the bad and guards the good. It's a unique combination of:

- DGlobal and local protection to provide maximum effectiveness
- Multiple-protocol protection to provide maximum coverage
- Custom-built appliance protection to provide maximum ROI
- Best-of-breed inbound plus outbound protection to provide maximum enforcement

McAfee Email Gateway solutions are unique in that they:

- Deliver constant and ongoing optimal security, rather than a temporary window of protection
- Prevent direct attacks as well as attacks on the email infrastructure
- Provide proven protections, tested every day in the most demanding environments in the world, including:
  - » Enterprises of every size and industry
  - » Government agencies worldwide
  - » Educational institutions
- Apply consistent policy enforcements against multiple messaging protocols
- Protect outbound content as securely as inbound messages

This complete family of application-specific, bi-directional messaging security and compliance appliances fully leverages the global intelligence of TrustedSource. They are designed to perform at enterprise-speeds, scale to meet global requirements, and can be deployed and managed with minimal overhead.

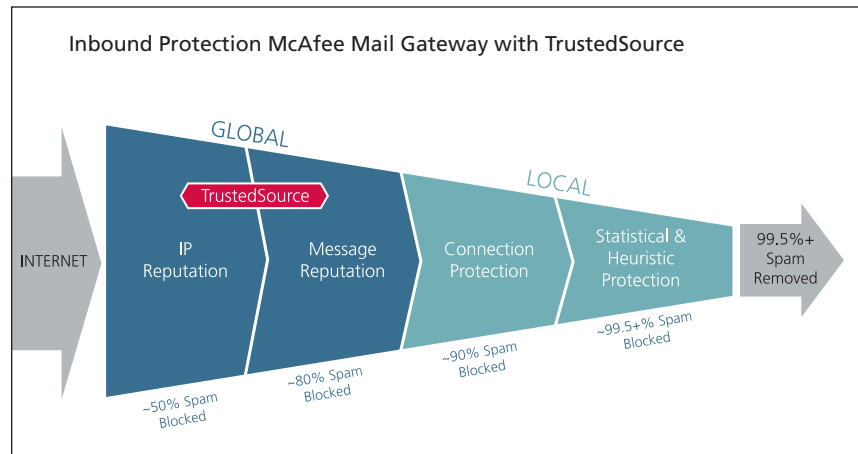


Figure 7: McAfee Email Gateway Security

### Data loss prevention

McAfee provides end-to-end protection enabling you to implement best practices to prevent information loss regardless of how that information is used, stored, or transferred. Centralized management, auditing, reporting, incident and case management, and detailed forensics combined with our innovative learning capabilities greatly reduce the time and effort required to get protection, significantly lower the total cost of ownership, and enable you to quickly adapt to changing business requirements.

Comprehensive information protection requires protection in three key areas:

- *Data-in-Motion*—Deployed at the network perimeter, McAfee can inspect incoming and outgoing traffic to accurately identify information security violations.
- *Data-at-Rest*—Deployed in the campus network, McAfee can connect to and inspect the contents of laptops, desktops, servers, and information repositories to identify sensitive material, and arm data-in-motion and data-in-use systems to protect it accordingly.
- *Data-in-Use*—Deployed as an agent on the user desktop or laptop, McAfee can provide information protection whether the user is on the network or off the network through virtually any I/O channel that presents an information security risk.

### Data loss prevention products and services

- *McAfee Network DLP Discover*—Automates the process of understanding your information, how it is used, how it is accessed, and the relationships between information elements; swarms across your network and data center interrogating all of your information sources to help you uncover, understand, and classify your information according to your security policies.
- *McAfee Network DLP Monitor*—Passively monitors all network traffic interpreting content and context of the traffic to uncover and report on issues that could lead to information loss, even if you don't know anything about your information.
- *McAfee Network DLP Prevent*—Intelligently monitors all network traffic blocking activities that would lead to information loss.
- *McAfee Network DLP Manager*—Provides detailed case management, incident management, policy management and configuration, and other administrative functions for McAfee Network DLP Discover, McAfee Network DLP Monitor, and McAfee Network DLP Prevent.
- *McAfee Network Security Platform Forensics*—Leverages Network DLP learning and capture technologies to generate detailed forensics of attempts at a data breach from nodes on your network detected by McAfee Network Intrusion Detection and Prevention systems.
- *McAfee Foundstone Professional Services*—Our professional services can help companies define their security policies, do an internal risk assessment and calculate and define their risk due to potential data leakage or loss.

### McAfee Security Technologies

To support these security products, McAfee has invested extensive time and resources in the underlying technologies that can create this strong security model. The first, and most important, is McAfee TrustedSource, our global reputation service.

#### TrustedSource

McAfee TrustedSource is a global threat correlation engine and intelligence base of global messaging and communication behavior, including reputation, volume, and trends for email, web traffic and malware. It works by analyzing and characterizing Internet traffic to make it understandable and actionable. By accumulating data from thousands of sensors located across the world, TrustedSource creates a profile of all sender activity on the Internet and watches these patterns for deviations from expected behavior. It then generates a reputation score based on multiple protocols, which is then incorporated into our products to enable them to quickly and accurately identify and reject unwanted traffic.

From its early days of simply assigning reputations to IP senders, TrustedSource now provides more reputations, with more granularity, than any other reputation service available. TrustedSource assigns reputations to:

- IP Senders
- Messages
- Attachments and images
- URLs
- Domains

TrustedSource was originally developed to keep enterprises ahead of the spammers in the ongoing battle for the inbox. Because it sees over 110 billion messages a month—more than any other messaging security technology—TrustedSource can provide superior accuracy when creating a reputation score. Relying on this score, TrustedSource can block up to 80 percent of connections based purely on reputation data (over 6.2 terabytes of spam every day), increasing security levels while maintaining a false positive rate of less than one in one million.

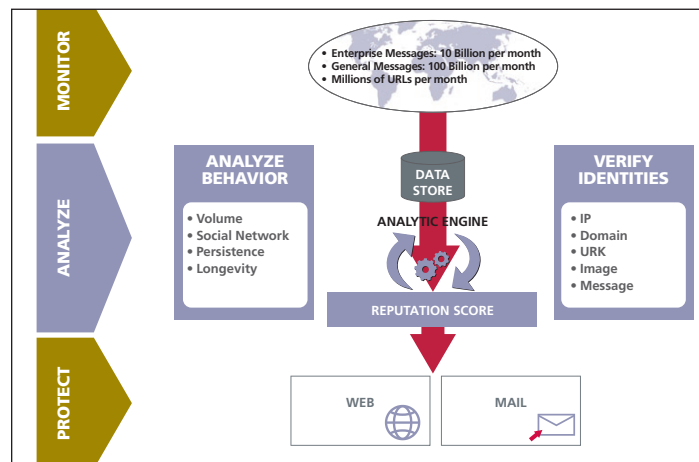


Figure 8: McAfee TrustedSource Global Reputation Service

But spam is only one threat in today’s world. Since its inception, TrustedSource has been expanded to protect against all forms of attacks, both known and unknown, via either the Web or email.

As part of McAfee’s vision to provide comprehensive enterprise security, McAfee Web Gateway incorporates global intelligence from TrustedSource. TrustedSource provides real-time reputation scores for URLs, domains, and IPs based on web page content, images, and behavior. TrustedSource also considers historical information such as knowledge that a site has been repeatedly compromised in the recent past. Using this real-time scoring, McAfee Web Gateway allows organizations to detect and prevent security threats such as spyware, phishing, or other malware.

**Anti-malware module**

The McAfee Web Anti-Malware is a next-generation approach to protecting the network from malware. Rated #1 by AV-test.org, an independent research center,<sup>21</sup> the Anti-Malware add-on contains a signature-based anti-virus engine to protect against known threats, as well as a proactive behavioral analysis engine that analyzes mobile code at the gateway to determine its intent and whether should it be allowed to reach the desktop. Through the effectiveness of this intent analysis, the Anti-Malware add-on has consistently delivered number-one ratings in independent tests.

21 Anti-Malware test performed by AV-Test.org and published on <http://www.eweek.com/article2/0,1895,2023127,00.asp>

For a detailed discussion of how the Anti-Malware Module protects the web gateway, please see our white paper, "The Secure Anti-Malware Engine."<sup>22</sup>

### Conclusion

With more than 90 percent of organizations already reporting business value from Web 2.0 adoption, these technologies and applications are here to stay, and are destined to become as much a part of our Internet use as email and web browsing. Web 2.0 adoption is creating new security risks for organizations. The previous generation of web and messaging solutions, which depend on signatures and categorization, have proven both theoretically and in practice to be insufficient for managing the new risks of the Web 2.0 world and beyond.

Clearly, organizations must deploy new solutions to counter these threats. These new solutions must use reputation- and intent-based techniques to thwart the short-lived, targeted attacks which are becoming the new standard. The principle design requirements for these solutions are well understood and implemented today in commercial products.

McAfee Web Gateway and Email Gateway provide proactive, reputation- and intent-based solutions that meet the needs of today's evolving threat landscape, are recognized by third parties and independent test labs as highly effective, and are affordable, secure and reliable.

### Next Steps

Check out your domain's reputation with our Domain Health Check service. This free report provides you with information on the publicly observed messaging and web traffic on your domain and any associated net blocks that you provide. The information in this report comes from the McAfee TrustedSource Service, a global reputation service that tracks messaging and web activity for every domain on the Internet.

You can also attend a weekly Webinar hosted by McAfee to learn more about Web Gateway, Email Gateway, and other McAfee products. Video demonstrations are also available for McAfee Web Gateway and Email Gateway, as well as an extensive library of data sheets and white papers. All of these can be found at [www.mcafee.com](http://www.mcafee.com).

When you've learned what you need to know, and are ready to secure your enterprise with McAfee, contact our one of our channel partners for more information on evaluating and purchasing McAfee Web Gateway, Email Gateway, and other McAfee solutions. To find the partner nearest you, go to <http://www.mcafee.com/us/partners/default.asp>.

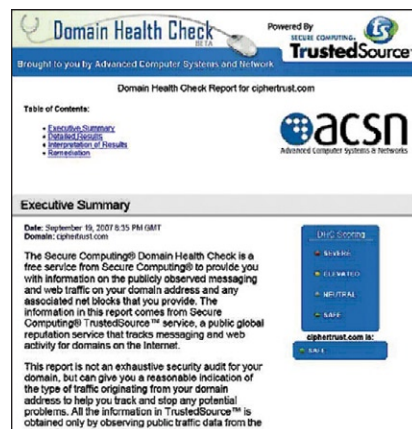


Figure 9: McAfee Domain Health Check

### About McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. <http://www.mcafee.com>.

