



Dear Readers:

The Web continues to evolve.

The excitement of the Web as a business platform has spurred tremendous growth in Web products and services that fall under the Web 2.0 umbrella. Today, Internet users are much more involved in the content creation that makes up the online world, and Web 2.0 sites and services are being widely used within companies by employees who have learned how to use them outside the business arena.

Web sites that did not exist five years ago are now at the top of the most visited and used sites on the Web. Yesterday's teenagers and college students, who have grown up using MySpace, YouTube and other Web 2.0 sites are bringing their social habits into the workplace, and creating a number of challenges for employers.

As Clearswift has uncovered through a series of surveys and whitepapers, Web 2.0 technology is having a major impact on everything from employee productivity to enterprise security. Through-out this paper you will learn about the benefits, as well as the concerns, of Web 2.0 technology.

While some of the benefits of Web 2.0 applications are clear, such as enhancing collaboration among dispersed team members; accelerating search and information retrieval; and building knowledge centers, the challenges of hastily adopting Web 2.0 solutions are also clear.

Many of the problems arise as Web 2.0 applications are used without any measure of their impact on the enterprise. Often businesses have little knowledge of how they are being used, how much time employees use them, and exactly what information is being shared. As a result, organizations face compliance and security risks and potentially, lose the benefits of Web 2.0 through a drain on employee productivity.

According to Gartner, "The dynamic and distributed nature of Web 2.0 applications means that some new approaches will be required to maintain the necessary level of business strength security" *Web 2.0 Needs Security101, John Pescatore, 2 November 2006.*

As the popularity of Web 2.0 applications has grown, Clearswift, like Gartner, has recognized the potential compliance and security threats. And as Web 2.0 has continued to take shape, we have worked hard to ensure that our web security solutions are ready to meet the demands of the enterprise.

In this paper, Gartner will discuss the importance of extending Web application security processes and controls to Web 2.0 solutions prior to the deployment of application. We will support Gartner's research and recommendation with Clearswift's experience and examples to provide you a strong overview of Web 2.0, its role in the enterprise and how to safely capitalize on new technology.

Sincerely,

Jon Lee
CEO, Clearswift

In this issue

• <i>From the Gartner Files:</i> Web 2.0 Needs Security 101	2
• Web 2.0 Makes Inroads in Business	4
• Content Security 2.0 The Impact of Web 2.0 on Corporate Security	6
• M&C Saatchi Embrace Web 2.0 Technologies; Implement Clearswift's MIMESweeper Web Appliance for Content Security	7
• MIMESweeper Web Content Security	8
• 10 Essential Steps to Web Security	9
• About Clearswift	10

Web 2.0 Needs Security 101

Ignoring security during the Web 1.0 deployment led to Web site defacement, identity theft and business losses. Building security into Web 2.0 applications should be done before applications are deployed to avoid a negative business impact.

WHAT YOU NEED TO KNOW

Deploying Web 2.0 applications without building security into them will lead to putting customer data and business reputation at risk. Extending Web application security processes and controls to Web 2.0 applications should be done before applications are deployed to avoid negative business impact.

ANALYSIS

In “Web 2.0: Get Ready for the Next Old Thing,” Gartner defined the key characteristics of Web 2.0:

- User-generated data and metadata
- Open application programming interfaces (APIs) and open-source software
- Lightweight technology, such as Ajax, representational state transfer (REST) and Really Simple Syndication (RSS)
- “Mashups” of content coming from multiple public APIs

From a security perspective, this sounds like *deja vu* all over again – in the early 1990s, the use of HTML and HTTP and JavaScript as part of Web 1.0 was the next new thing. Basic security tenets were ignored in that rush to new technologies, leading to years of Web defacements, mass worms, cross-site scripting, “phishing” and identity theft. If enterprises don’t demand basic security capabilities in Web 2.0 applications and don’t adapt existing security processes and controls to the new concepts, waves of security incidents and business interruption will wipe out any increase in productivity or customer value.

Building security into Web 2.0 applications is not all that difficult: Many of the same simple security principles that are routinely in place for application development apply. We discuss what is new and different about Web 2.0 from a security perspective and provide recommendations for how to build security in from the start.

Being User-Centric and Secure

The Wikipedia is the poster child for the Web 2.0 user centrism and participatory focus. Con-

tent comes from users who volunteer to create or update sections, rather than from a limited, centrally selected and audited set of experts. While the wiki approach can lead to broader and more rapidly evolving coverage of topics, it has also been vulnerable to misinformation and denial-of-service attacks, as random authors make malicious or specious changes to sections. The Wikipedia has already had to evolve editorial controls to restrict updates on particular topics and require levels of authentication to combat such vandalism.

Another user-centric aspect is the incorporation of user-generated metadata in Web 2.0. Even sites that are merely using user-centric approaches to aggregate opinions, such as movie, restaurant or hotel rating sites, must provide these services, or they face manipulation through automated approaches, such as click fraud that is already rampant in online advertising. Essentially, being able to tell the difference between actual human being users and automated bots will be the first requirement, and then having the ability to treat input differently depending on the identity of the real user will be the next requirement.

Sites that aggregate and present information that users will assume is factual must incorporate authentication, integrity, access control and nonrepudiation services. Authentication services allow any user to determine who created what and allow users over time to make their own decisions about what contributors to rely on, and which to filter out or ignore. Integrity services allow users to be sure that content has not been changed by any other party. Access control services allow only authorized users to modify certain types of information. Nonrepudiation services provide the evidence that would be required to support or deny any claims of malfeasance or illegal conduct on the part of the enterprise publishing the information.

Another user-centric concept of Web 2.0 is greater personalization of content, often using insight gathered from observing user actions

in searching and accessing data. Data such as clickstream or search stream data can be valuable targets for attackers. The integrity of this data needs to be assured, both during collection and when stored.

Security Through Openness

Software and APIs that are designed and built with security in mind, knowing that they will be exposed to open-source scrutiny, generally lead to increased security. Similarly, the use of proven security protocols and open industry standards in Web 2.0 instead of proprietary approaches will be a net improvement in Web security. However, badly designed and written software and APIs that are rushed to market can be a disaster – just making APIs open or providing source code does not guarantee any higher level of security. Using unproven open-source comments may lead to increased security vulnerabilities and raise licensing issues. Enterprises have to apply license management tools to open-source software to make sure there are no legal issues, and all software (proprietary or open source) needs to be developed with security in mind and needs to be tested for vulnerabilities. For more information, see “Open-Source and Closed-Source AD Security: Combining the Benefits of Both Paradigms.”

Another aspect of openness in a Web 2.0 world is open business communications, such as the use of CEO blogs to communicate corporate vision and create community around products and services. For most corporations (certainly all publicly traded ones), communications by the CEO must be carefully thought out and vetted, whether they occur in a blog, during a TV interview or in formal business correspondence. Blog entries (both personal and corporate) by employees may present conflicting information to customers and may allow sensitive corporate and customer information to leak. Content monitoring and filtering tools need to be extended to inspect information being posted to blogs, and blog sites need to be made secure from attempts by attackers to modify content.

Lightweight Protocols Still Need Heavy-weight Security

Web 2.0 concepts emphasize the use of loose coupling, using lightweight protocols and languages. Complexity is almost invariably an enemy of security, but lightweight does not always mean simple. In the early days of the Web, CGI scripts were a lightweight way of making the original static Web sites more interactive, and they were also the source of the vast majority of vulnerabilities that enabled waves of Web site defacements attacks. Other lightweight techniques, such as the use of hidden HTML tags and URL parameter “stuffing,” also left huge holes for attackers to exploit.

Ajax and RSS are two primary examples of lightweight components that are key to most Web 2.0 applications. Ajax is essentially used to provide client-side executables to support dynamic display of information and local user interaction, as well as allow dynamic data feeds that do not require user action to refresh local data. Essentially, at the start of a session, the browser downloads an Ajax “engine,” which then executes locally to both interact with the user and make asynchronous requests from the originating server. While JavaScript has been used prior to Web 2.0 to animate Web pages, the Ajax approach involves much more communications, interfaces and code – they all increase the attack surface area and overall complexity, which thus increases risk.

While the Ajax engine can only communicate back to the server it was downloaded from, Web 2.0 has introduced the concept of Ajax “bridges” – basically, server-side proxies that can communicate to external Web sites on behalf of the client-side Ajax engines. In the early days of the Web, server side includes providing a similar function and was yet another source of easily exploited vulnerabilities. By allowing dynamic inclusion of content and executables on the server side, these approaches provide openings for external attack and make vulnerability discovery much more difficult. Ajax bridges will introduce similar risks into Web 2.0.

RSS is an XML-based standard for allowing RSS-aware programs to subscribe to RSS information feeds. Most people are already familiar

with viewing blogs and news articles through RSS feeds on their Web browsers, but RSS has extension capabilities (specifically, the enclosure tag) that allow any file to be pushed out, including executables. Web 2.0 applications that use RSS to subscribe to stock price feeds, for example, will happily download executables added to that data feed, and many RSS readers will happily load those executables. The lack of input validation on Web forms led to buffer overflow and command injection attacks; the use of unfiltered RSS feeds will do the same.

Two other lightweight technologies often used as part of Web 2.0 applications are REST and plain old XML (POX). REST essentially models every document and Web application as a resource with a Uniform Resource Identifier. REST uses HTTP and the standard HTTP functions (DELETE, GET, POST, PUT) to provide interaction. The use of POX really doesn't raise any additional security issues beyond those in any Web services application, except that many developers using POX avoid the use of XML schema, which negates the use of schema validation approaches to detect the most-common forms of attack.

You Say Mashup, I Say Cross-Site Scripting

The third key concept in Web 2.0 is the idea of mashups, which mix content from the host server with feeds from public APIs. A real estate site that puts multiple listing service icons on top of the map from another site is a common example. The term “mashup” comes from the recording industry, in which one artist can create a new song by “mashing up” samples from other works and adding effects and new content. This obviously raises copyright and legal issues, as well as some major business issues. For example, content from a controversial or illegal Web site could be placed on top of corporate-sponsored information (think of someone placing hate symbols over some houses for sale that are shown in an online neighborhood map). There are major security problems to be resolved, as well – hostile mashups that mix in password capture screens with legitimate content, for example.

Once again, good old Web 1.0 provides a cautionary tale. Early security problems with

Note 1 Basic Security Services

Authentication – Verifying the claimed identity of a user or computer process. This can be simply the act of verifying an online identity (such as a previously registered user name), or it can extend to verifying the real world identity of a user.

Integrity – Assuring that any change of content can be detected

Nonrepudiation – The collection and preservation of evidence to support a defense against any claims made against the enterprise

JavaScript led to the incorporation of “same origin” controls – basically only allowing client-side JavaScript to communicate back to the site from whence it came. However, a number of basic vulnerabilities in these mechanisms were discovered, allowing attackers to create their own content (such as a bogus login screen) to appear in the midst of valid content from the legitimate server. Essentially, cross-site scripting is the bad guys doing evil mashups. Web 2.0 mashups that are not done securely will lead to huge openings for new forms of phishing and other attacks.

Recommendations

The major recommendations to ensure that the use of lightweight protocols and languages in Web 2.0 applications are very similar to the basic HTTP security guidelines:

- A threat model should be developed at the start of application development and should be used to drive security requirements into all application requirements. Security standards should be specified for all security services required to address the threats (see Note 1 on basic security services).
- All Web 2.0 code should be subject to vulnerability testing, at a minimum, before the applications are allowed into production use, and ideally during build

and integration. When Web 2.0 dynamics dictate that source code is not available, binaries and runtime executables will need to be analyzed.

- All Web 2.0 interactions should be subject to filtering and validation to minimize the potential for attack insertion.
- In particular, all query strings should be examined to detect command injection and other typical attacks.

- Any Web 2.0 unique security constructs should be reviewed against known threats and coding best practices prior to development.

The dynamic and distributed nature of Web 2.0 applications means that some new approaches will be required to maintain the necessary level of business strength security. Vulnerability assessment techniques will need to be extended to deal with client-side executables

and service-oriented architectures. Intrusion prevention (both host- and network-based) will have to be extended to deal with more scripting code and new protocols. However, extending well-known application security approaches to all new Web 2.0 applications should be done first and should be done prior to allowing any Web 2.0 applications to go into production use.

Gartner RAS Core Research Note G00144174,
John Pescatore, 2 November 2006

Web 2.0 Makes Inroads in Business

Businesses utilize the web every day as a critical business tool. As the web has evolved from a collection of Web sites to a platform for the next generation of applications and business services, it is being used in new ways that are making it easier to do everything from shop-

ping and sharing to collaborating with friends and completing education courses.

This comfort level with the next generation of the Web, or Web 2.0 as it has been coined, is also demonstrated by a wave of jargon,

brands and experiences that have worked their way into virtually every aspect of daily life. Television shows about the origins of online videos. Popular news broadcasters and newspapers quoting and interviewing bloggers. Students citing Wikipedia as a reference in their research papers. And one-time Webizens of MySpace now transcending all media with music or art.

Web 2.0 is also finding its way into the business world, as former high school and college students who were avid users of IM, FaceBook, Yahoo! Mail and Flickr, are bringing their habits and Web applications into the workplace. Nearly all Web 2.0 applications started life as consumer-focused services and are beginning to penetrate the enterprise and transform the way even the most staid corporations approach collaboration and knowledge sharing.

This evolution of Web 2.0 into the enterprise has had its challenges, but it is easy to understand why some businesses looking seriously at these applications. Web 2.0 applications are easy to use and deliver impressive benefits to the enterprise.



For example:

- New search technology makes it easier and faster to find information in all corners of the Web;
- Blogs, wikis and other applications are making it easier to capture knowledge assets, exchange information and create knowledge centers for the benefit of future business initiatives;
- Web-based software development languages are making it easier to create and deploy Web 2.0 applications and services that can help businesses;
- Social networking, social media and wikis provide the potential to streamline collaboration within and beyond the enterprise; and
- Web 2.0 applications and services provide new ways to communicate faster and easier with stakeholders.

While familiarity with the Web has opened worlds of opportunity for everyday users and businesses alike, it has also introduced a new breed of security challenges for business owners and operators. Web 2.0 applications are almost too prevalent and too easy to use. A recent Clearswift survey found that 87 percent of U.S. workers access Web 2.0 sites each week and 46 percent of them discuss work related issues on social media sites.

The problem is that Web 2.0 applications are being used across businesses without measurement of their impact in terms of risk, and with little filtering or monitoring of activity. According to the Clearswift survey, more than 35 percent of companies do not monitor their employees Internet usage, and another 48 percent didn't know if they had lost confidential information via Web 2.0 applications or the Internet.

Like their employees, companies have grown comfortable with the Internet, and the familiarity, or casualness, has created an environment that places the company and its bottom line at risk. The benefits of Web 2.0 are being overshadowed by two core challenges;

a drain on employee productivity and higher security risks including inbound malware and outbound data loss.

As a result of the rapid evolution of Web 2.0, we are witnessing the convergence of social networking on a massive scale and the adoption of new combinations of technologies that significantly increase the possibilities for attacks. Over the past couple of years, we have learned that Web 2.0 technologies are vulnerable to security threats, particularly infection and downtime caused by viruses, worms, Trojans and spyware. The combination of scale and an increase in vulnerabilities offers irresistible opportunities to organized crime.

About two years ago, organized criminals discovered that around 70% of web applications harbored security flaws and began to switch from targeting operating system weaknesses to those in the applications. The Web is now the preferred vector for malware, and Web applications are facing a massive escalation in attacks.

Beyond the employee productivity issue and the increased security risks are the challenges associated with content and data leaks. Social networking, blogging, wikis, IM, etc., are all about sharing information, and often these activities are done casually without regard for the sensitivity of information being shared, as demonstrated by our research. Controlling what, how and where corporate information is shared has become increasingly difficult with Web 2.0 technologies. Unless monitored, content leaks through Web 2.0 solutions position the company for legal prosecution for illegal activities or regulatory breaches for illegal activities, and can harm the reputation of the company as internal issues hit the headlines.

While many of the threats associated with Web 2.0 are similar to the those associated with Web and email use in general, the unique nature of Web 2.0 technologies requires a new understanding and new defenses.

For the past 20 years, Clearswift has been helping enterprises protect themselves against Internet-based threats. As Web 2.0 has emerged, we have worked to ensure that our Web security solutions are ready.

The first line of defense for any organization is the Internet policy, which must be tailored to the needs of your business and adaptable to meet the requirements of different users. Effective risk management starts with users and users need guidance. Once a policy is in place, it is essential to distribute the policy to all employees and ask for explicit agreement, with a signature. The policy should be updated regularly and available on the intranet for all to reference.

A policy without teeth is no defense at all. Companies must be prepared to enforce their policies on Web 2.0 usage by filtering Web mail, all Web traffic, blocking policy breaches, blocking web activity that bypasses the approved HTTP proxy or any other ports used by evasive applications and acting on illicit activity. Content filtering is at the heart of a solution to combat Web 2.0 threats, and is an indispensable part of policy enforcement.

Content filtering scans all web traffic, including traffic to and from Web 2.0 sites. Content filtering is policy driven, allowing administrators to configure specific, granular policies for different departments, users groups, individuals, time of day, destination, etc.

Powerful content filtering must also be able to identify every known payload type. Payload analysis can then block content that breaches policy, including profanity, and content containing words such as 'confidential,' project names, credit card numbers, social security or national insurance numbers, DRM tags and watermarks.

Content filtering should be combined with URL filtering, allowing administrators to block or allow specific websites or classes of website, and with malware and spyware protection at the web gateway.

Finally, an effective content filtering tool must be easy to deploy, configure, maintain and update, with rich reporting to improve policy and strategy.

MIMESweeper, by Clearswift, monitors all user active Internet channels including web browsing; web mail; instant messaging; file sharing; proxy anonymizers; P2P applications and of course Web 2.0 data exchanges.

MIMESweeper protects from all **content integrity** threats through:

- **Data Leak Prevention** – preventing the leakage of confidential information, PCI and PII data as well as loss via Wiki's, blogs and other Web 2.0 applications
- **Compliance to laws and regulations** - Enforcing data content compliance for HIPAA, SOX, SEC, etc.

- **Legal and HR protection** – including defamation, hate speech, the downloading or exposure to inappropriate material
- **Employee productivity** – the prevention of inappropriate or excessive web browsing

MIMESweeper mitigates **network security threats** by providing hygiene solutions for:

- **The prevention of virus infections** - covering anti-virus, anti-malware, anti-spyware, evasive application blocking (P2P, Anonymizers), the prevention of VB script and other injection files. MIMESweeper does this by determining true file types for accurate identification and scanning
- **The prevention of network degradation** – covering loss of bandwidth by limiting or stopping downloads of large media files and preventing access to known bad sites with URL filtering

Web 2.0 technologies are not going away and organizations are finding Web-based applications and services have a positive impact their business. However, as Gartner recently stated, "Adopting Web 2.0 to increase collaboration within organizations opens the door to significant security risks which need to be addressed, and "the use of the technology means companies relinquish a 'level of control that they historically would not tolerate,' meaning a rethink of security is essential." To incorporate Web 2.0 the right way, organizations must begin with a strong policy and use a proven technology to enforce the policy, going beyond simple URL filtering to address fundamental network security and business integrity threats. By doing so, they will ensure that company resources and proprietary information are protected, employees stay on task and they maintain their ethical and legal integrity.

Source: Clearswift

Content Security 2.0 The Impact of Web 2.0 on Corporate Security

Recently, Clearswift commissioned research to establish how popular new Web 2.0 technologies and sites really are among office workers to determine the scale of the potential threat to corporate security.

In the United States and the United Kingdom it is clear that Web 2.0 social media sites are becoming widely used, particularly among younger employees. A sampling of the data shows that:

- **83%** of US office workers have accessed social media of some description from work
- **71%** of 18-29 year old office workers in the UK accessed social media sites from work at least a few times a week with 39% having accessed them several times a day
- **63%** of US office workers accessed social media at least once a day and 82% at least a few times a week
- **27%** of 18-29 year old office workers in the UK spent three or more hours a week accessing social media sites from work

Also, employees are putting sensitive corporate information at risk by discussing work-related issues via social media from the office:

- Almost one third (**30%**) of office workers in the US have discussed work-related issues via social media
- **42%** of 18-29 year old UK office workers discussed work-related issues via social media sites

However, some businesses are failing to protect themselves against these threats:

- **19.1%** of IT and business decision-makers didn't have a policy governing appropriate use of the Internet including social media sites and 2.8% didn't know whether they did or not
- Almost half (**48.3%**) of those polled didn't know whether they had lost confidential information via social media outlets

Nor are they embracing these emerging technologies in order to benefit their companies:

- **40.8%** of IT and business decision-makers considered social media to be relevant to today's corporate environment, yet only **11.1%** were already making use of it from a business perspective

Organizations can benefit from the explosion of Web 2.0 by using its tools to disseminate corporate messages and share content. However, they can also be exposed by employee use of such tools. The majority of data leaked from enterprises happens as a result of accidental or malicious employee behavior, not outside threats such as hackers. There are now numerous ways that sensitive information can escape from a company, thanks to the explosion of Web 2.0 content sharing sites – the outbound web threat is no longer just webmail. Also, confidential data leaks and damage to reputation can be just as serious, or arguably more serious, than external threats such as viruses,



spyware and spam and our research shows that businesses know this to be the case.

Never before has it been more important for companies to consider controlling use of the web as well as email and protecting against outbound threats as well as inbound.

However, striking the balance between security and access to Web 2.0 collaboration technologies for business benefit is key. Blocking access is simply not an option. It will prevent the businesses enjoying the benefits of Web 2.0 sites themselves. The Web 2.0 world brings with it significant data leakage risks and the research clearly shows that the scope of the mass usage of Web 2.0 tools by employees. While it is cause for concern, it is not cause for alarm. By taking a smart approach to web security, businesses will be able to unlock the power of these new Internet services for competitive advantage.



Source: Clearswift

M&C Saatchi Embrace Web 2.0 Technologies; Implement Clearswift's MIMESweeper Web Appliance for Content Security

Introduction

M&C Saatchi is a global advertising agency renowned for its work with companies such as British Airways and KFC. It was founded in 1995 following the Saatchi brothers' departure from Saatchi & Saatchi and now has 18 offices in 13 countries. In 2004, 49 per cent of the company was floated on the London Stock Exchange's AIM.

Gavin Singh is IT Support Manager at the company's headquarters and manages the IT needs of all the staff based there. Singh has been at M&C Saatchi for a year and a half and leads a team of six.

The Challenge

- Allowing employees appropriate levels of web access based on their job roles

- Allowing staff safe access to specific Web 2.0 technologies
- Maintaining a secure, virus-free business environment
- Reducing management, maintenance and administration time
- Enabling staff to securely view streaming video media

As a creative business, having access to the Internet is vital to M&C Saatchi employees. In the advertising industry it is important to keep on top of current affairs and trends and to be completely familiar with what is happening on the web. However, the IT team needs to ensure Internet use does not pose a threat to either the business or its staff, as well as maintaining a reliable system with minimum downtime, meaning no virus or malware attacks.

It is also important for M&C Saatchi to control exactly what staff have access to, in order to maximise client-related working time.

“At M&C Saatchi we need to be flexible with our Internet use policy. Different staff have different requirements for their Internet access and it is the IT team that has the duty of meeting these requirements,” says Singh. “Within the creative industries, much emphasis is being placed on new Web 2.0 concepts such as Second Life and Facebook and employees are naturally wanting to experiment. We have to be able to ensure they can do this both safely and within company policy. For us, content security is the key – we need security that guards against harmful or restricted content, without denying access to anything relevant.”



The Results: Flexible Policy Management

A key requirement for M&C Saatchi is the ability to put policies in place to restrict or allow web access as necessary – it is not just a case of blocking access to anything potentially harmful.

“My team and I do block access to certain URLs universally, such as those hosting webmail services,” says Singh. “However, there are other websites which cannot be treated so uniformly. For instance, our designers and creatives need access to a far wider range of content than other staff, so it is simply not possible for us to just block some sites. We need to allow access to certain things so we needed a solution that we could trust to protect the business from any threats associated with these sites.”

Clearswift’s Web Appliance allows the IT team to set up policies allowing individuals or groups to view specific websites, while blocking others from having access to them. The Web Appliance offers the most granular policy management in the industry, with policy templates and wizards to make it easy to design, deploy and update. For example, the creative team may be working on a campaign based on Second Life so they would need to access the virtual world for business purposes. For other staff however, spending hours in Second Life would be an inappropriate use of company time.

An area where policy management is very applicable is with Web 2.0 sites. Many of the staff at M&C Saatchi need access to sites which host videos. Clearswift’s Web Appliance is able to analyse all data travelling through the web gateway, including video files, to determine if it contains harmful or inappropriate content, and then send or block according to an organisation’s policy. This means M&C Saatchi’s IT Team can allow certain employees access to these sites, safe in the knowledge that they are secure.

Source: Clearswift

The Solution: MIMESweeper Web Appliance CSW500

- Provides a complete web content security package in one box
- Protects against confidential information leaking via webmail or Web 2.0 sites such as social network sites, blogs etc.
- Allows companies to implement granular policy management, powerful reporting functions and policy wizards
- Provides protection against inbound threats such as spyware and virus attacks; allows URL blocking
- Quick and easy 30 minute installation and simple to manage once up and running via web-based user interface

MIMESweeper Web Content Security

MIMESweeper™ Web Appliance

MIMESweeper™ Web Appliance offers essential web protection in one fast to deploy, easy to use and manage, high performance appliance. It's been specifically designed to simplify the tasks of creating, enforcing and managing user based content policies at the Internet gateway, by combining a unique selection of the world's leading web security technologies.

The MIMESweeper content and policy engine is complimented by Kaspersky's high detection rate Anti-Virus, Aluria's comprehensive Spyware detection engine, and the world's leading URL Filter, all delivered in a simple to install, rapid deployment, hardened Linux Appliance.

MIMESweeper™ for Web

MIMESweeper™ for Web is an effective web security solution, enabling the creation, enforcement and management of highly complex and granular user based web content policies for HTTP traffic. It offers optional plug-in add-ons, including the world's leading URL Filter and Kaspersky's Anti-Virus.

The unique strengths of the MIMESweeper™ for Web solution are its ability to find and analyze the real content of the files flowing to and from an organization via the Internet.

MIMESweeper™ IM Enterprise Edition

MIMESweeper™ IM Enterprise Edition secures, controls and manages Internet applications including Instant Messaging, Peer to Peer, File sharing and web anonymizers.

The MIMESweeper for IM server software securely manages all types of legitimate IM communications providing enhanced IM content, policy, and security checks, plus advanced auditing, compliance and archiving features. It also records all IM conversations in order, adds disclaimers, scans for viruses, and creates tamperproof versions for storage.



The Benefits of MIMESweeper

The Web 2.0 security window has been left open for too long. Clearswift's web and Web 2.0 solutions close the window, so you can:

- Stop virus and malware infections from web downloads including web-based email and Web 2.0 services
- Block surfing of illegal, inappropriate or dangerous websites
- Prevent confidential data leaks through

web mail, web file transfers and Web 2.0 services

- Block illegal and unauthorized downloads
- Reduce productivity loss due to non-work-related web browsing
- Protect your brands and corporate reputation
- Prevent regulatory breaches and litigation

Source: Clearswift

10 Essential Steps to Web Security

The new Web 2.0 applications – from social networking to tagging, blogging and presence-aware services like IM – reflect the new web-enabled relationships forming between individuals and enterprises.

Unfortunately, each new development of the web brings with it a new species of parasite. Spyware, adware, keyloggers, blogspam and IM viruses seem to sprout up within days of any new trend. Clearly, it's never been more important to protect your enterprise from the hazards of uninhibited browsing.

Below is a list of ten essential steps to Web security:

1. All web security must start with policy. Policy focuses attention on the things you need to stop, drives up compliance, enforces fairness by making rules clear to everyone and facilitates prosecution of the guilty and defense against regulations.
2. When it comes to policy, one size does not fit all. It must reflect the way you do business and dictate your technology.
3. Attack spyware from multiple angles. Stop it at the gateway, at the desktop, and stop it from 'calling home.'
4. Use a comprehensive URL filter to block whatever kinds of sites your policy demands, and supplement the filter with a blacklist and whitelist of your own
5. Your Web security must be able to decompose all container file types, including spreadsheets, Word documents, zip files, etc., to scan for deeply embedded malware.
6. Implement bi-directional Web security. It is important to protect against both Web download threats, as well as information that is uploaded to the Web. Uploaded material can lead to prosecution and embarrassment.
7. Protect against IM traffic coming in and going out.



8. Monitor all web activity. Web security should include comprehensive monitoring, reporting and analysis.
9. Deploying, updating, managing and monitoring processes need to be designed with the real world in mind. Simplify, automate and streamline your policy enforcement and web security.
10. Keep an eye on emerging Web activities. As new web services emerge, make sure to reflect your view of them in your policy. Rule of thumb: if it moves, it can be scanned, filtered and protected.

The above steps are important, and it's even more important to focus on the principles behind the steps, including policy, vigilance, simplification, automation and transparency. While putting these principles into action starts with these steps, the parasites never stand still and never stop coming, and it is important

that organizations are always looking forward and have a technology that is constantly ready for what's next.

Start with your own policy. Does it reflect all of the issues identified above? Is everyone in your organization familiar with the policy? Is it continually updated to reflect new threats and activities? Do you have the right technologies in place to enforce your policy at all gateways and in both directions?

Clearswift is one of the pioneers in web security, beginning when 56kpbs seemed fast. Clearswift has seen every type of attack in every kind of environment from small businesses to global enterprises. All of Clearswift's solutions reflect experience in real deployments and the company invests massive resources into staying on top of every emerging Internet-borne threat.

Source: Clearswift



About Clearswift

Clearswift simplifies content security.

Our products help organizations enforce best-practice email and web use, ensuring all traffic complies with internal policy and external regulations.

Our range of content filtering solutions makes it easy to deploy, manage and maintain no-compromise email and web security for both inbound and outbound traffic.

Clearswift is the only vendor to offer comprehensive, policy-based content security in all three deployment methods: as software, as an appliance and as a managed service.

All three platforms are designed to take the hassle out of securing internet traffic, with a clear, intuitive management interface; automatic, 'zero-touch' updates; powerful reporting and common-sense policy management.

Twenty years of experience across 17,000 organizations has helped us raise security standards while simplifying security management at the same time.

We've helped many of the world's most successful organizations use the internet with confidence and are committed to staying ahead of the market and helping our customers defend against all emerging threats.

www.clearswift.com

Enterprise Security and Web 2.0 – The Impact is published by Clearswift. Editorial supplied by Clearswift is independent of Gartner analysis. All Gartner research is © 2007 by Gartner, Inc. and/or its Affiliates. All rights reserved. All Gartner materials are used with Gartner's permission and in no way does the use or publication of Gartner research indicate Gartner's endorsement of Clearswift's products and/or strategies. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.