



**CLEARSWIFT™**  
Simplifying content security



# Demystifying Web 2.0

Opportunities • Threats • Defenses



## Demystifying Web 2.0

Anyone who spends any time online cannot have failed to notice. People are using the Web in new ways; ways that make the ‘brochureware’ of the early Web experience look and feel decidedly flat.

It’s a new world, characterized by a wave of new jargon, brands and web based experiences. MySpace. FaceBook. Wikipedia. Flickr. Twitter. YouTube. Mashups. Blogs. Newsfeeds.

Clearly something is going on here.

Back in 2004, Tim O’Reilly of O’Reilly Media gave a name to this new wave of Web experiences. He called it Web 2.0.

Unfortunately, O’Reilly never really stopped to nail down a definition of Web 2.0. Today, the term means many different things to many different people and therefore, some would say, means nothing at all.

But just because it’s difficult to define doesn’t mean that Web 2.0 isn’t real. In fact, while pundits argue about its precise definition, Web 2.0 applications have been quietly (and not so quietly) taking the Web by storm and transforming the way even the most staid corporations approach collaboration and knowledge sharing.

“**Web 2.0** refers to a perceived second generation of web-based communities and hosted services — such as social networking sites, wikis and folksonomies — which facilitate collaboration and sharing between users.”

Wikipedia





## Web 2.0 and Enterprise 2.0

Nearly all Web 2.0 applications started life as consumer-focused services, only later finding their way into the enterprise.

But unlike many consumer 'toys', Web 2.0 actually delivers impressive benefits to the enterprise, including:

- **Streamlining collaboration** within and beyond the enterprise
- **Accelerating search** and information retrieval
- **Capturing knowledge assets** and facilitating knowledge transfer
- **Speeding application development** and deployment
- **Communicating with stakeholders** in new ways

Some of these benefits are 'soft'. Others are quantifiable. But all have combined to earn the attention of line-of-business managers and IT strategists alike. Web 2.0 is here to stay.

In fact, it's now evolving into Enterprise 2.0 – the application of Web 2.0 technologies to workers using network software within an organization.

- *87% of US employees access Web 2.0 sites each week*
- *46% of employees discuss work-related issues on social media websites*
- *59% of UK employees aged 18-29 believe they should be entitled to access Web 2.0 content for personal use, from work*

*Clearswift Survey – The Impact of Web 2.0 on Corporate Security, 2007*

*“The collaborative nature of Web 2.0 is a phenomenon business must address.”*

*Computer Weekly, 5 June 2007*

## Threat 2.0™

THREAT 2.0

Every new technology introduced into the enterprise brings with it new threats. Web 2.0 is no different, with threats including:

- Infection and downtime – caused by viruses, worms, Trojans and spyware specifically carried by Web 2.0 applications
- Data leaks – as staff members get lulled into a false sense of security, or intentionally share things they shouldn't share
- Legal prosecution – for illegal activities or regulatory breaches
- Productivity loss – as users spend more time on blogs and social networking sites than on work
- Resource waste – as servers and networks become congested with frivolous multimedia content
- Reputation damage – as any of the above abuses hit the headlines

These threats may look similar to the threat landscape associated with Web and email use in general. But the unique nature of Web 2.0 technologies demand a new understanding and new defenses.

“The tension between control and freedom plays out every time a consumer-focused technology makes into the enterprise, but it's particularly pronounced for Web 2.0.”

Computer Weekly, June 2007





## Clearswift can help

At Clearswift, we've been helping enterprises protect themselves against Internet-base threats for nearly twenty years. As Web 2.0 began to take shape, we worked hard to ensure that our Web security solutions were ready.

As a result, the MIMESweeper for Web software and the MIMESweeper Web Appliance solutions are already protecting hundreds of major organizations from the threats posed by Web 2.0 services.

This guide is a quick introduction to the main Web 2.0 applications, their uses and their risks. Given the dynamic nature of Web 2.0, it can never be the last word on the subject. Instead, think of it as the first word in a dialogue that we hope will improve the security of every enterprise, whether or not they choose to use our technology.

We're always updating our own understanding of Web 2.0 in real enterprise deployments, so please keep in touch.

### The Web 2.0 pillars

Blogs • Wikis • Folksonomies •  
Social Networking • RSS or  
Newsfeeds • Social Tagging or  
Bookmarking • User-generated  
Media • Mashups • Podcasts

**60%** of companies are  
already using Web 2.0  
technologies.

Internet World survey, May 2007





## Blogging

### What it is

Contraction of a 'Web log' – the published text of an author's thoughts, with entries displayed in reverse chronological order. Readers can subscribe to a blog, link to it, share links and post comments.

Blogs have exploded over the last few years as users discover how easy it is to publish thoughts to a potentially global audience. Technorati tracks over 75,000 new blogs created every day.

### A few examples

Engadget, Boing Boing, Lifehacker, Seth's Blog, IBM Developerworks Blog.

### Enterprise benefits

Blogs offer a powerful new way to communicate with the world. Enterprises have adopted them for their ability to provide:

- A more personal complement to traditional communications
- Informal forums for discussing issues with staff, customers and partners
- Fast, efficient collaboration tools for teams
- Accelerated information access
- An ability to influence perceptions of organizations and/or brands

### Threats

Blogs are notorious for lulling people into a false sense of security. Their informal nature belies their power to disseminate often highly sensitive information extremely quickly to an unknown audience. The hazards include:

- Confidential data leaks
- Legal liability
- Damage to reputation and brands
- Undermining of customer, partner or stakeholder trust
- Virus and malware attacks
- Loss of productivity

Examples of blogs getting authors and their employers in trouble are legion. Clearly, blog use cannot go un-monitored.

### Blogging blunder costs fashion editor her job.

An assistant beauty editor at Ladies Home Journal lost her job because she shared details about her job, her boss and her colleagues in her 'Jolie in NYC' blog.

Her advice to bloggers? "Think before you write and definitely don't write about your industry."

MSNBC July 2005

"News.com reports that 59% of CEOs believe blogs are a useful internal communication tool while 47% believe that they are useful for external communication."

Prologger.net

### Like Blogging only... smaller

In Micro-blogging, users write brief text updates (usually a few hundred characters) about their life on the go, then post them via text messaging, instant messaging, email or the Web.





**What they are**

Wiki is a Hawaiian word meaning "quick". A wiki is a website that allows visitors to add, remove or edit content.

**A few examples**

Wikipedia, Wiktionary, Memory Alpha (a Star Trek wiki), Wikitravel.org, world66.com.

**Enterprise benefits**

Wikis are a powerful collaborative technology that can create a valuable knowledge base with very little centralized resource. Benefits include:

- Fast, low-cost knowledge capture and classification
- Support for collaborative projects
- Simplified search and information access

**Threats**

The open philosophy behind most wikis means that anyone is allowed to generate and edit content. Unfortunately, this assumes that all contributors are well-meaning – a dangerous assumption – that can lead to:

- Vandalism
- Intentional disruption or misinformation ('trolling')
- Confidential data leaks
- Virus and malware attacks
- Poor authentication of users and editors

Wikis are good hiding places for confidential information that would never be allowed to escape through email. Anything from customer data, financial information, confidential designs and plans and staff records can be including (unwittingly or otherwise) in a wiki.

**Wiki Smear**

In 2005, John Seigenthaler, former editor of the Nashville Tennessean, was shocked to read on Wikipedia that he "was thought to have been directly involved in the Kennedy assassinations."

The false information had been on the site for several months and an unknown number of people had read it, and possibly posted it on or linked it to other sites.



## Folksonomies

Folksonomies

### What they are

A folksonomy is a user-generated taxonomy used to categorize Web content (Web pages, images, links, videos, etc.) so that it can be easily searched, discovered and retrieved.

### A few examples

Flickr, del.icio.us, Digg, Backflip.com.

### Enterprise benefits

Because they're user-generated, well-developed folksonomies make sense of large bodies of information from the user's perspective by providing:

- Fast, easy classification of unstructured information
- Simplified search, discovery and access
- Support for projects
- Accumulation of enterprise knowledge

### Threats

Folksonomies (and wikis) lack expert control, which could compromise their accuracy. But generally, as folksonomies classify information stored elsewhere, the threats relate to the classified information itself:

- Linking to illegal or inappropriate content
- Linking to confidential data
- Linking to malware-infected sites or files

These threats can be hard to detect as the actual policy breach is contained in the target information rather than in the folksonomy itself.

### Tag, you're it

Folksonomies are built using Social Tagging, also known as Social Bookmarking. The idea is popping up everywhere: let users drive the way information is stored, classified, shared and searched.

"Social tagging helps to naturally elevate certain topics above others by making them more popular."

Computer Weekly 5 June 2007

"Although folksonomies can be useful for specific applications, they do not provide a standardized means of classifying and managing content that can be consistently applied across the enterprise."

IBM, Taxonomy Management



## Social Networking

### What it is

A Social Network is a virtual community. Members create their own pages, link to other members and communicate by voice, chat, instant message, videoconference and blog.

### A few examples

Friendster, MySpace, Bebo, Facebook, LinkedIn.

### Enterprise benefits

Enterprises have turned to social networking to facilitate community building and collaboration. Rather than impose a structure on a community, social networking allows users to build their own structure, maintain their own content and build relationships with each other by:

- Building community among staff and stakeholders
- Fostering collaboration and communication
- Enabling projects with many participants

### Threats

Like many Web 2.0 applications, Social Networking tends to accept each user's identity and credentials on trust. It's easy to mask one's true identity and pretend to be someone else. Some of the risks:

- Sharing confidential information with an unauthorized person
- Accepting information from non-trusted sources
- Infection from social network-specific malware
- Phishing attacks

### MySpace Phishing

Beginning in March 2007, the Google security team detected a five-fold increase in overall phishing page views, with 95% of the new phishing traffic targeting MySpace pages.

Google Online Security Blog

“Social networking sites and blogs carry an even greater risk for data leakage and brand damage than email, because anyone can potentially access them”

Katie Gotzen, Frost & Sullivan



## RSS or Newsfeeds

### What they are

Really Simple Syndication (RSS) is a Web feed format used to publish frequently updated content such as blog entries, news headlines or podcasts. It lets users subscribe to their favorite “feeds”, receiving automatic updates.

### A few examples

Topix.net, New York Times Week In Review, CNET Blogs.

### Enterprise benefits

RSS has already gained a foothold in the enterprise, with an increasing number of organizations using it to:

- Create content and knowledge management systems
- Disseminate information to customers and partners
- Update stakeholders on issues of interest
- Within IT, to syndicate application, database and object data

### Threats

RSS is difficult to consume safely. The design features that make it easy for a feed to be ‘thrown together’ also make it difficult to secure. Risks include:

- Untrusted sources can subscribe or hijack feeds
- Confidential information can be ‘pushed’ to unknown subscribers
- Open to a wide range of scripting exploits
- Vulnerable to phishing attacks

“RSS is the ideal way to present valuable, recently created information to the right people without overwhelming their email inbox.”

Enterprise RSS, June 5, 2007

### The Podcasting Boom

A podcast is simply an audio or video newsfeed, distributed using RSS. Unfortunately, multimedia files are notorious hiding places for malicious code...

“RSS is getting popular, as a result of which it is being linked to important financial databases. It poses a threat in two dimensions. On the server side customized feed routines can be exploited by an attacker. On the client side session hijacking and malicious code execution is possible.”

Help Net Security, 12 March 2007

“In an RSS attack scenario, users click on links that appear to be from trusted sites (sites to which they have subscribed). At the offending sites, victims turn over their personal information to phishers, rather than to legitimate organizations.”

Search Security.com, September 2005





## User-generated Media

### What is it

User Generated Media or Content is anything produced by end-users as opposed to traditional media companies.

### A few examples

YouTube, Flickr, Outloud.tv, Halfbakery.com.

### Enterprise benefits

Forums, media-sharing sites, wikis and folksonomies are all examples of User-Generated Media. Enterprises have been using them all to:

- Quickly generate content valued by community members
- Share content with minimal infrastructure and administration
- Involve customers and staff in dialog

### Threats

The dangers of User Generated Media come down to 'who is the user?' and 'who is the consumer?' Risks include:

- Posting of illegal or inappropriate content
- Leaking confidential information
- Hijacking by attackers
- Reputation damage from untrusted users


### MySpace Worm

"Security experts are increasingly warning about the dangers of sites that host user-created content. In particular, features of movie files that allow certain types of scripting have become a popular way to launch malicious software attacks. Web worms that use cross-site scripting flaws on sites such as MySpace are increasingly a worry."

Securityfocus.com, December 2006

"Though the value and reach that user-generated content can project is tremendous, huge obstacles exist to harnessing its influence."

DM News August 2006





## Mash-ups

### What are they

A mash-up is a website or application that combines content from more than one source into an integrated experience.

The term comes from the music world, where it refers to a song made up entirely of parts of other songs.

### A few examples

iGoogle, HousingMaps.com, Chicagocrime.org, Amazon Light.

### Enterprise benefits

These are early days for enterprise mash-ups. Some Web brands such as Google and Amazon have embraced them, welcoming third party developers with open application interfaces. The benefits:

- Fast, 'bottom up' application development
- Fuelling creativity
- Streamlining internal processes
- Creating an ecosystem around key applications

### Threats

Mash-ups lack any kind of integrated and federated identity management or authentication, so managing user credentials is a major loophole. Also, mash-ups often use enterprise data without asking first and then present it in unintended ways. This presents a range of threats, including:

- Misuse of corporate data or application code
- Unwitting participation in illegal or improper activity
- Confidential leaks
- Malware infection

"With all the innovation on the Web with mash-ups, real work needs to be done on standards, identity, process and security to bring them into the enterprise."

WebProNews, May 8, 2007

"Mashups and other **Web 2.0** technologies are being implemented by 'shadow IT' groups, tech savvy managers who want to implement without waiting for IT approval."

Rod Smith, IBM VP of Emerging Technologies





### **What is it**

Asynchronous JavaScript and Extensible Markup Language (XML) is a grouping of technologies that allow seemingly more immediate, uninterrupted interactions through the browser. Many Web 2.0 applications use Ajax to improve the user experience.

### **A few examples**

There are already millions of Ajax-enabled sites and its popularity is growing fast.

### **Enterprise benefits**

Enterprises use Ajax for the same reasons Web 2.0 applications do: to improve the user experience and streamline integration with third party services.

### **Threats**

Unlike traditional Web applications, Ajax applications extend across both client and server. This necessitates a trust relationship between client and server that can be exploited by an attacker. This creates significant new vulnerabilities including:

- Cross-Site Scripting – injecting code that exposes the user to cookie theft, keystroke logging, screen scraping and denial of service attack
- Phishing – increasingly common on social networking sites
- Ajax-specific malware – including Super-worms and Ajax bridges

For a more complete discussion of Ajax-related security threats for developers, please refer to our 'Web 2.0 Security White Paper: Is the Web Broken?'



## Defending against Web 2.0 threats

The Web 2.0 threats we've just summarized can be organized into three clusters:

Malware and Malicious Content – exposure to inbound viruses and worms as well as pornography, hate speech, harassment, etc

Confidential Data Leaks – loss of confidential information such as customer data, product designs, plans and financial disclosures

Productivity Loss – Employees wasting time on no-work-related Web 2.0 services

All three of these can be actively addressed using the 'Three E's' approach that Clearswift advocates:

### 1. Establish a clear security policy

Effective risk management starts with users and users need guidance. Your existing Internet security policy should be updated to take Web 2.0 activities and threats into account.

For help and advice on developing an effective Internet Security Policy, including a sample based on our own in-house policy, please refer to the 'Clearswift Policy Toolkit'.

### 2. Educate users

A policy can't change user behavior if nobody knows about it or understands it.

It's essential to distribute the policy to all employees and ask for explicit agreement, with a signature. The policy should be available on the intranet for all to refer to and updated regularly.

Clearswift's user guides such as 'The 7 Deadly Sins of Blogging' and 'IM Etiquette' can help.

### 3. Enforce the policy

A policy without teeth is no defense at all. Enforce your policies on Web 2.0 usage by filtering all Web traffic, blocking policy breaches and acting on illicit activity.

**Content filtering is an indispensable part of policy enforcement. It pays to get the best solution you can and to let all employees know that you are filtering Web traffic.**

### Unwanted headlines

A car-maker hit the headlines recently when sixteen staff were disciplined for circulating pornographic images over internal email. The email found its way to the parent company's network and a full investigation was ordered.





## The power of content filtering

*The power of content filtering*

Content filtering scans all Web traffic – including traffic to and from Web 2.0 sites – for malware, illegal or inappropriate use, data leaks and other policy breaches.

The best content filtering technologies are policy-driven, allowing Administrators to configure specific, granular policies for different departments, user groups, individual users, time of day, destination website, 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, etc.

Content filtering is often combined with URL filtering, allowing Administrators to block or allow specific websites or classes of website.

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



## Clearswift and Web 2.0

Clearswift was one of the first security vendors to identify the new risks posed by Web 2.0 activity and to build Web 2.0 defenses into our products.

The MIMESweeper for Web product line offers robust, policy-driven Web 2.0 security, delivered as an appliance, as software or in combination.

MIMESweeper for Web Software uses the most sophisticated content security engine available to offer unrivalled protection against both incoming and outgoing Web and Web 2.0 threats.

MIMESweeper for Web is the only Web security solution to include full content analysis, full HTTP-compliant proxy with 4GB cache, integrated policy management plus comprehensive graphical reporting tools. It is also the only solution to integrate flawlessly with third-party anti-virus solutions. And for those without a URL filter, the MIMESweeper for Web URL Filter is available as a plug-in.

**The MIMESweeper Web Appliance** is the first enterprise-class Web and Web 2.0 security solution, covering all Web threats in a single box that's easy to deploy, manage and support.

For the first time, all the essential, best-of-breed Web security software is integrated with pre-installed policies on a hardened Linux appliance and future-proofed with auto-updating of all software components.


The MIMESweeper Web Appliance combines Clearswift's award-winning content security with best-of-breed URL filtering, anti-virus and anti-spyware technology into an integrated, easy-to-manage Web security solution.





## The Benefits

*THE BENEFITS*



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

### Relevant Resources

The Clearswift Policy Toolkit

15 Mistakes in Web Security

MIMESweeper for Web 5.2 Factsheet

MIMESweeper for Web Appliance Factsheet

Clearswift Survey – The Impact of Web 2.0 on Corporate Security

### User Guides

The 7 Deadly Sins of Blogging

The Guide to IM Etiquette



## Clearswift simplifies content security.

*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.

---

## Contact Clearswift

### United States

100 Marine Parkway, Suite 550  
Redwood City, CA 94065  
Tel: +1 800 982 6109 | Fax: +1 888-888-6884

### United Kingdom

1310 Waterside, Arlington Business Park, Theale,  
Reading, Berkshire, RG7 4SA  
Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

### Spain

Cerro de los Gamos 1, Edif. 1  
28224 Pozuelo de Alarcón, Madrid  
Tel: +34 91 7901219 / +34 91 7901220 | Fax: +34 91 7901112

### Germany

Amsinckstrasse 67, 20097 Hamburg  
Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

### Australia

Ground Floor, 165 Walker Street, North Sydney,  
New South Wales, 2060  
Tel: +61 2 9424 1200 | Fax: +61 2 9424 1201

### Japan

Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku  
Tokyo 105-0011  
Tel: +81 (3) 5777 2248 | Fax: +81 (3) 5777 2249

