

**Demystifying
Web 2.0**

Opportunities • Threats • Defenses

Demystifying Web 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 services, Web 2.0 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.

“**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

■ **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

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
- 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 take full advantage of email and web technologies, while protecting themselves against the threats. As Web 2.0 began to take shape, we worked hard to ensure that our solutions were ready to allow our customers to embrace collaboration..

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.

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, such as Twitter, 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.

Wikis

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

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 usercreated 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



Ajax

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?'

The challenges of Web 2.0

In this “point and click”, collaborative world, valuable business communication happens fast. So fast, in fact, it’s easy to forget how likely it is to invite new risks or accidentally share confidential or sensitive data in ways that create real compliance concerns for your enterprise.

And, as more Web 2.0 and social networking collaboration tools jump over firewalls, they bring new risks into your enterprise. The opportunity to introduce new types of data-stealing malware into your protected environment becomes your security team’s daily reality. Would you like to unleash the power of collaboration without:

- Losing control of your intellectual property or customer sensitive data?
- Reducing employee productivity?
- Introducing a new security threats or dangerous malware into your enterprise?
- Creating compliance concerns when Web 2.0 communications can’t be audited?
- Spending more money on hardware and acquiring new licensing and support costs?

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.



Clearswift enables collaboration through Web 2.0

With Clearswift, you can expect your people to collaborate confidently without jeopardizing your enterprise's reputation, brand, intellectual property or ability to comply with global regulations. Our content-aware solutions for collaborative enterprises, protects your sensitive data with policies you design for the way your people really work. Using Clearswift, you can create just about any policy to protect or enable any type of sensitive content in the ways that best fit your compliance, risk posture or collaboration needs. Communication are tracked, audited and logged for your compliance program.

Collaborate confidently

MIMESweeper, is a content-aware engine we've perfected over the last two decades to understand content from the inside out. By allowing you to see the content employees are sharing with collaboration tools, MIMESweeper enables you to define business communications confidently.

Understanding what is being communicated in today's collaborative culture is important because seemingly innocent files from social networking sites are easily cloaked to steal your data. Legacy security systems like DLP, URL and anti-spam blockers can't recognize this malware because it is undetectable to their content processing engines.

Only with Clearswift can you truly be aware of what content is, from the inside out, to enable confident and safe collaboration that won't disrupt your business.

Adaptable policy management

If you can define a policy on paper, you can define it with our solutions. Many of our 17,000 customers find that for the first time, they can easily define acceptable business communications customized to their unique risk posture. And if a market condition or compliance regulation changes, you can easily change policies without business interruptions.

Auditable collaboration

Everything that happens in the Clearswift solution is auditable and reportable. Reports can be created and shared with your executive management, compliance and audit team or scheduled for daily, weekly, monthly delivery - you decide. We make it easy to demonstrate you are creating one standard of care across all communications.

Virtualize your DMZ and reduce hardware and operating costs

We're one of the few content security companies to deliver our solution as VMware or as a virtual appliance that can run on your own hardware. This dramatically reduces hardware, management and infrastructure costs. And because nobody understands content like Clearswift, you can consolidate and virtualize all those anti-spam, malware, spyware and virus products you have sitting in the DMZ on our platform, dramatically reducing your hardware, licensing and support costs immediately.



A solution that allows you to get on with the way you work

For content that needs to be protected, you can apply specific policy actions to take place at gateway instead of relying on employees to remember when they must take action to protect sensitive information. For example, you re-route emails back to the sender or apply encryption to protect content at the gateway, without requiring employees to know, or do anything. This is just one of the many actions you can take to protect your organization without necessarily blocking the important communication that could be mission-critical to your business.

Peace of mind while collaborating In a point-and-click world, mistakes can happen to the best of us. Often, the risks we divert are human errors: non-compliant email exchanges, misdirected emails containing sensitive data, or the accidental downloading of malware from a social networking site. Unfortunately, URL filters and anti-spam products won't save you from these threats.

That's why at Clearswift we provide true bi-directional content protection with unmatched policy management. With our solutions which have been trusted over the decades, you can have peace of mind, knowing only the right content will be delivered to the right people in the right ways.

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:

- Enable business growth through collaboration.
- Define policies according to the way your people work.
- Auditable collaboration - everything that happens is auditable.
- Virtualize your DMZ and reduce costs.
- Reduce costs by consolidating multiple security vendors.

Contact Clearswift

United States

Clearswift Corporation
161 Gaither Drive
Centerpointe Suite
101Mt. Laurel,
NJ 08054

Tel: +1 800 982 6109
Fax: +1 888-888-6884

Spain

Cerro de los Gamos 1,
Edif. 1
28224 Pozuelo de Alarcón,
Madrid

Tel: +34 91 7901219 / +34 91 7901220
Fax: +34 91 7901112

United Kingdom

1310 Waterside,
Arlington Business Park,
Theale,
Reading,
Berkshire, RG7 4SA

Tel: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Germany

Amsinckstrasse 67,
20097 Hamburg

Tel: +49 40 23 999 0
Fax: +49 40 23 999 100

Australia

Level 5, Suite 504,
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