



A Websense® White Paper

SECURING THE SOCIAL ENTERPRISE

websense®
ESSENTIAL INFORMATION PROTECTION™

Table of Contents

Executive Summary3

A Consumer Fad, A Commercial Fact4

The Social Enterprise5

Attacks Ramp Up.....6

Proper Protection is the Key.....7

Acceptable Use Policy.....7

Malware Detection.....8

Data Loss Prevention.....9

Bottom Line9

Reporting on Crime: The Websense® 2010 Threat Report10

Websense Solutions: Web Security Done Right.....11

About Websense11

Business embraces the social Web with steely focus on thwarting the enterprise-size risks that come with it.

Executive Summary

Social networking and Web 2.0 are all the rage. With Facebook, Twitter, Bebo, YouTube, Google, Yahoo, Flickr, LinkedIn, WordPress, and more, there are over a billion socially active people today — a number that continues to grow at an astounding rate. And it's not just a teen or consumer fad anymore. The social Web has emerged as a valuable business tool for the modern enterprise touting rich applications with real-time interaction and user-generated content.

There is no denying that the social Web *is* the new Web. Nearly every enterprise is using it in one way or another. But along with its enormous popularity come enterprise-size risks. So in the race to maximize its potential, enterprises must take due care to completely protect the business. Unfortunately, most aren't yet prepared to do that, lacking the proper controls to effectively enforce acceptable use policy, prevent new forms of malware, and protect sensitive data.

This paper delves into the social networking security landscape — the good, the bad and the ugly — and offers practical guidance toward harnessing the power of the social Web to help businesses benefit from it.

A Consumer Fad, A Commercial Fact

The Web has come a long way in a very short time. At its inception, interactions were primarily passive with big business presenting information to viewers in a very one-directional manner. Of late, though, it's taken a decidedly different turn — it's gone social. The days of passive viewing have vanished and a highly interactive form of the Web has emerged.

The social Web and Web 2.0 encourage interaction and user-generated content. Websites solicit response, collaboration, comments, and opinions. Users can see and share whatever they want, whenever they want. Whether a social networking site, video sharing application, blogging platform, or news forum, 65 percent of the top 100 most commonly visited sites today are based on this notion of collaboration and content generation (Source: Websense® 2010 Threat Report).

Of course, the social Web's roots are in the consumer space with some obvious fan favorites. Friends and families are using Facebook to keep in touch and manage their personal lives. Colleagues are networking through LinkedIn. Millions are making life announcements via Twitter and posting their talent on YouTube. Young and old are soaking up the applications, searching world events through iGoogle and posting opinions to MSNBC.com. Blogging has become an outlet for the consumer voice.

But as quickly as social networking has stormed personal lives, it has infiltrated the workplace, too. Enterprises have discovered that the consumer phenomenon is also a valuable tool for business and they're already using it to modernize business processes, corporate communications, and employee collaboration. Perhaps more important, it's proving instrumental to customer service, sales, and marketing programs and even partner communications.

Whereas traditional tools — like promotional material, advertisements and even email — are far removed from target audiences and static in nature, social networking sites are personal and engaging. The social Web provides a real-time, bidirectional channel that allows enterprises to capture and relate with their markets. They can access the emotion of the customer base that ultimately frames and reframes brand perception. They can lobby interest and build the relationships that drive buyer behavior. The Web is where customers are. It's where the money is.

Indeed, the social Web has become a viral sensation. Facebook touts over 500 million active users, each month sharing more than 30 billion pieces of content — from Web links, news stories, and blog posts to notes and photo albums. LinkedIn claims 60 million users. Twitter estimates 175 million registered users, accounting for 95 million tweets per day. YouTube facilitates more than 2 billion views a day, and Google processes over one billion search requests and twenty-four perabytes of user-generated data every day.

The Business of Being Social

As the social Web gains momentum, commercial successes are plenty:

- One of the world's largest technology providers recently used Facebook to post announcements, create dialog, and solicit feedback from customers in lieu of an in-person trade event.
- A fast-food conglomerate leveraged FourSquare to increase foot traffic.
- A large financial institution forgoes traditional reference checks during the hiring process, instead consulting LinkedIn and even Facebook to evaluate candidates with an uncensored look into their background and character.
- Kim Kardashian and her promoters use Twitter to generate buzz for her television shows and keep her name in the limelight.



The Social Enterprise

With that kind of track record, it's no surprise that, according to a recent Websense @Work Study, 95 percent of organizations allow access to Web 2.0 sites. They certainly can't avoid the most popular sites and still expect to compete effectively in today's digital economy. So the social Web has become their new reality. And that's changing the face of business and creating enterprise-size risks.

In this new social enterprise, users are empowered and emboldened, eagerly tapping into all things Web. Although well-intentioned, they are pushing the limits, stretching enterprise perimeters, and opening otherwise closed doors. And as users swing those doors open, enterprises are dealing with a new age of Web code. The industry has moved beyond traditional HTML to script-based code, like JavaScript, XML, and Flash. All of this is testing the stamina of legacy security protections like URL filtering and antivirus solutions.

Composite	HTML	Composite	DHTML, Flash, Java
Size	71.2 KB	Size	1.26 MB
Scripts	None	Scripts	8 Java Scripts (924KB)
Files	4	Files	22
Sources	1 - Google	Sources	More than 1,000

Google vs. iGoogle

At the same time, social networking has become the primary target of hackers and those wishing to commit fraud. Results showcased in the Websense 2010 Threat Report demonstrate how the majority of high-ranking sites are perilously close to danger. In fact, an astounding 55.9 percent of social networking sites are now only two clicks away from something bad.

Obviously, the stakes are high for enterprises. Just consider a sampling of recent high-profile security breaches. The Heartland Payment Systems scandal rocked the financial sector when customer credit/debit card accounts were exposed. The case eventually settled for \$140 million, in addition to direct remediation costs. A glitch in an AT&T-designed Web application exposed 100,000 email addresses employed by iPad users to access their iTunes accounts. And then the Stuxnet attack brought focus on a whole new set of concerns by targeting critical infrastructure.

And when it comes to the social enterprise, criminals are seeing pay dirt. On one hand, enterprise social networking access is hard to control and lock down — there are just so many opportunities, so many users, and so many vulnerability points. On the other hand, those enterprises are rich in data. They're a veritable gold mine in today's universal currency, housing customer account information, patents, sales and marketing plans, and much more. With greater vulnerabilities and greater payoffs, the criminal element is mesmerized by opportunity.

Attacks Ramp Up

All the while, online threats are evolving at record speed. The industry is experiencing a deluge of attacks — each more strategic than the last. The masterminds, in many cases, are criminal organizations motivated by data and money, rather than fame and mischief as in years past. This was proven by an advanced persistent threat, known as Aurora, which leveraged Google and a previously unknown Internet Explorer vulnerability to pilfer data. The attack was specifically designed to evade traditional antivirus and Web reputation defenses to gain access to enterprise assets and sensitive information.

The social Web is a perfect breeding ground for such onslaughts. According to the Websense 2010 Threat Report, the Web is typically where threats are being delivered. In fact, the research reveals that 52 percent of data-stealing attacks occurred over the Web. The security team also points to a 111.4 percent increase in the number of malicious websites from 2009 to 2010. Even more disturbing, 79.9 percent of websites with malicious code were legitimate sites that had been compromised — meaning the sites that everyone visits everyday are potentially bad news.

Today's threats are a mix of approaches. Old methods are being modernized for the new social Web. Phishing, for example, has moved to Facebook which is increasingly being used to display malicious campaigns. In one situation, an email seemingly from Facebook Security asks users to confirm their account like traditional phishing attacks, and it's loaded from within Facebook to appear more legitimate. Equally dangerous, common malware, for example Koobface, has been spread via Facebook, Friendster, Bebo, and other social networking sites, often spamming "friends" with a link to a malicious website. Another Facebook worm, called Boonana, has lured users into installing a Java applet with its own brand of nasty code.

People looking to commit fraud are mining sites like LinkedIn and Plaxo for private data and trade secrets, while "scam of the day" attacks are effectively replacing traditional social engineering stings. In evidence, tricksters on Facebook, Twitter, and other sites entice unwitting users with offers for free iPhone or access to illicit photos. Those users are giving up sensitive account information and permitting access to their social profiles.

Meanwhile, new threats are being engineered to take advantage of social networking vulnerabilities. Search engine optimization (SEO) poisoning attacks, for instance, are gaining momentum. When users innocently initiate searches on the latest buzz — from the Haiti earthquake or Bloombox Fuel Cell research to something as innocuous as Lindsay Lohan's famed arrest — they could get in trouble. Some 22.4 percent of simple trending and news searches lead to something bad, reports Websense Security Labs™. In fact, searching for breaking trends and current news could be more risky than searching for objectionable content.

Another example of a new form of threat zeroes in on the ever-popular blogging craze. Blogs are obviously not designed with security in mind. That said, WordPress, the most widely used platform was recently the focus of an injection attack. In just over two weeks, 250,000 injections occurred with over 37,000 URLs in the wild continuing to be injected, according to Websense Security Labs. That's a lot of potentially tainted blogs exposed to a lot of unwitting visitors.

Searching for Trouble

A particularly nasty SEO poisoning attack targeted terms related to the recent earthquake in Haiti, leading users to rogue malware. Caring people searched the Internet for the latest updates on the disaster, discovered the extent of the earthquake through photos or videos, and found ways to make charitable donations. Instead, they found their own disaster by way of malware — which had less than a 20 percent detection rate by traditional antivirus solutions, according to the Websense 2010 Threat Report.

[2010 Haiti earthquake - Wikipedia, the free encyclopedia](#)
 The 2010 Haiti earthquake was a catastrophic magnitude 7.0 Mw earthquake, epicentre near the town of Léogâne, approximately 25 km (15 miles) west of Port-au-Prince. Casualties of the 2010 Haiti earthquake - Damage to infrastructure in the en.wikipedia.org/wiki/2010_Haiti_earthquake - Cached - Similar

[Haiti Earthquake - Special Coverage on CNN.com](#)
 Full coverage includes news, aid efforts, interviews, background, iReport and more. With photo gallery, video and interactive map. US. www.cnn.com/SPECIALS/2010/haiti.quake/ - Cached - Similar

[Haiti Earthquake of 2010 - The New York Times](#)
 Feb 17, 2011 ... A massive earthquake struck Haiti on Jan. 12, 2010, leveling Port-au-Prince. www.nytimes.com/info/haiti-earthquake-2010/ - Cached - Similar - Add to

And as these threat models continue to evolve, attackers are perfecting their game. Overall, attacks tend to be more effective, more pervasive. They increasingly target the most broadly popular brands, celebrities, and news items for maximum exposure. Criminals are also putting extra effort into making content look more believable — more likely to dupe unsuspecting users. They go to great lengths to avoid the traditional trappings, such as misspellings, unrealistic claims, and imperfect brand representation. Just look at today's version of a phishing page that can be loaded from within Facebook using an iFrame to appear more legitimate.

The motivation behind all of these advances is for criminals to get deeper and deeper into the enterprise — and walk away with more of the spoils.

Proper Protection is the Key

In the end, it's the enterprise's job to protect its content. But even knowing that the vast majority of today's most popular sites are categorized as social in nature, many businesses are not equipped with the right security and control technologies to handle the risks that accompany the social Web.

Blocking all access to these sites is simply not feasible. The social Web is a critical, new business tool with too much potential to pass by. It is the new Web. And at the same time, going into it blind is far too risky — especially when Facebook alone accounts for 18 percent of internet traffic today. Relying on old controls, like URL filtering, is insufficient because it only validates the integrity of a site, not the actual content being accessed on that site. And antivirus solutions just look at files via signatures, when the social Web and its underlying applications are script-based. So those technologies are essentially blind to the potential risks of social networking sites.

So how does one lock down the social Web? Is real-time protection against this ever-evolving onslaught of threats even achievable? How does one understand and analyze the risks? Can one effectively enforce use policy in a way that adequately protects business?

Arming the enterprise with acceptable answers to these poignant questions necessitates more granular visibility into and control over what comes into and goes out of the company — particularly at the content level. That's a whole new way of looking at Web security and must be applied across three different vectors of protection: Acceptable use policy, malware defense, and data protection.

Acceptable Use Policy

First and foremost, enterprises need to extend acceptable use policy (AUP) to their social networking security. Most have spent a lot of time and money creating use policies for the Internet, policies that control what users do and see. Now, they need to apply that same due care to the social Web.

As it stands, when the URL category for social networking allows access, users can do and see anything on the site. But objectionable content may be readily available which violates AUP. Consider, for example, the iGoogle home page. Arguably, iGoogle is just as social as Facebook since users can access applications and share content indiscriminately. From one perspective, it's a legitimate page and can be considered

The Negative Side of Fame

Celebrities are popular targets of malicious exploits, aiding unwittingly in the speedy spread of malware. Justin Timberlake's 3.7 million fans were recently subjected to a malicious link on his and 250,000 other Facebook walls. With close to 19 million followers, Lady Gaga got caught hosting 1,717 instances of profanity, 372 spammy links, and 93 directly malicious links on her Facebook wall in a single week.

The Facebook logo, consisting of the word "facebook" in a bold, blue, lowercase sans-serif font.

instrumental to any number of job functions within the enterprise. But that site is also a mashup of applications for everything from news feeds to games — which could spell trouble.

Many enterprises may be tempted to “just say no.” In reality, though, unilaterally locking access is out of the question. Instead, they should create use policies that say “yes” to the right kind of access, allowing the good traffic that facilitates productivity and blocking the bad traffic that could be a security threat. So with iGoogle, users can be permitted to catch up on news and perform work-related searches, but be denied access to things like gambling applications and illicit material.

The only way to apply proper AUP is by analyzing and classifying discrete bits of content in real time. That means enterprises should be thinking about the social Web not in terms of sites, but in terms of the content on them as the user accesses it. They must be able to allow access to that URL level and then granularly control what users see and do with content on that site — even from behind a login or SSL. Some legacy technologies will send the URL of a page back for analysis, but if it's under SSL or behind a login, that security engine will be unable to access the same content. Enterprises must be in control, determining what content is inappropriate and to what extent access is curtailed in a calculated and meaningful fashion.

Malware Detection

Enterprises also must be able to perform real-time security scanning for malware on the social Web. Attackers are getting more creative in finding new avenues to infect systems and steal data. The majority of websites with malicious code are legitimate, luring unsuspecting users into their well-laid traps.

As attacks increasingly move to social networking sites, old-style attacks are being reborn to new social applications while modern threats like advanced persistent threats (APT) and Web exploits target vulnerabilities in the browser and gaps in antivirus solutions. Still, enterprises are responsible for the integrity of their social networking relationships and an infection could have devastating impact on brand, customer loyalty, and even revenue — not to mention the internal harm and cost of remediation.

So enterprises must protect against these new and old threats by having complete visibility into the traffic entering and leaving the network. Unfortunately, traditional security solutions are not enough. Network firewalls are built on standard HTTP and HTTPS protocols and require URL-level filtering. And old-school antivirus solutions analyze file-level transfers, while Web reputation services fail to cover where 79 percent of threats are — on legitimate websites. All of this is ineffective against today's threats as many social networking sites, like Bing and Google, are all about script-based code.

And with malware amuck, it's simply too risky to rely on legacy security technology. For example, iGoogle content can stream for any number of legitimate business reasons, most notably news searches. But when an employee clicks on a bad search result, corrupt code can make its way into the enterprise. Similarly, an uninformed employee could access a posting on his Facebook page during work hours and open a bad link only to wreck havoc on his production machine.

With this new form of malware lurking around every social corner, enterprises must be able to analyze content streams to detect anything malicious — from embedded code to executables and links — before it does damage. Or pay the consequences of having to fix the damage after the fact.

Mashing It Up With iGoogle

iGoogle Web portals are a hugely popular way for users to create a personalized Web portal or home page. The sites are a mashup of different applications, news feeds and valuable business tools. But they also allow for gadgets like GoogleGram, YouTube Channel, Meteosi, and eBay Gadget, along with access to games like Farmville and Mafia Wars. All of which put enterprises at risk for malware, inappropriate content, and unproductive time.



Data Loss Prevention

Malware is also a contributor to data loss. Websense® Security Labs™ reports that 39 percent of malicious Web attacks include data-stealing code. That's a fairly sobering statistic considering the number of applications delivered via the Web today — including those from human resources, payroll, engineering, customer service, sales, and more. All of which involve sensitive interactions that are core to enterprise operations. So enterprises must take appropriate steps to block exposure to that data-stealing code.

But it's also important to control data loss resulting from outbound interactions. One of the prime benefits of social networking is that users can share content. That sharing tends to be agnostic to the type of content — public or private, sensitive or not. The risk of exposure is high, both from intentional acts or unfortunate mistakes. A disgruntled employee can use his webmail account to transfer customer files to a competitor. Corporate bloggers can inadvertently pre-release new product information. A mistake on Twitter could expose a confidential marketing plan to the masses. A personal opinion posted to a news article on MSNBC.com could subject a company to legal woes.

Enterprises need to be able to scan for outbound data loss, analyzing content with user and destination awareness. And that gets tricky with Web communications — that is, HTTP, HTTPS, and FTP traffic in lieu of traditional channels, like email and print, because most technologies are not able to detect the source and destination of a Web transfer. Some vendors advocate a “block-all posts to Facebook” strategy, simply because their solutions can't readily distinguish between the posting of a grocery list or a customer list. But that closed approach breaks the social Web which is built to be interactive. Without that two-way collaboration, its utility erodes.

What's more, not just any data loss prevention will do in today's social Web. In order for a solution to be effective, it actually needs to work. That means “DLP Lite” solutions that rely only on basic keywords, dictionaries, and regular expressions simply won't cut it. They'll lead to false positives, negatives, and aren't expandable to address things like removable media or data discovery, leading to higher solution costs and complexity.

What enterprises need are multiple detection mechanisms and content classifiers with high accuracy and granular control. They need to eliminate false positive and false negatives, responding immediately to legitimate loss events with the tight tactics — whether that's blocking, quarantining, or encrypting traffic. There's just too much at stake not to take data loss seriously, especially in a socially oriented Web.

Bottom Line

When it comes to the social Web, enterprises really have no choice in the matter. It is the new reality, especially when so many of the most popular sites today are of a social nature. But more importantly, the new social Web represents opportunity and innovation. And frankly, that's a must in today's competitive economy. Enterprises must utilize all the tools at their disposal to reign successfully — and that includes the social Web.

Embracing social networking halfway is not the way to go. To fully harness its power, enterprises must be able to move forward with near abandon. And that only happens when they have the peace of mind of knowing that their business is fully protected — that they are controlling access to individual pieces of content in a way that enables enforcement of AUP, prevents malware, and protects data. Without that, business faces extreme and unnecessary risk.

It's important to cover all the bases with all the right protections, while focusing on simplicity in implementation. Enterprises need maximum visibility and control to respond quickly and efficiently to security threats. And that means steering away from strategies with multiple solutions, multiple consoles, redundant infrastructures, and vendors.

With such protection in place, enterprises can leverage social networking to its fullest. Many are doing just that. Armed forces for a large government agency are using Facebook to maintain all important family bonds while troops are deployed. A major U.S. airline has improved customer service by posting travel delays, weather alerts, and airfare specials via social networking sites like Facebook, Twitter, YouTube, and Flickr. And a \$1,000 FourSquare campaign by a large fast-food chain resulted in a 33 percent increase in foot traffic in one day.

One need only imagine those kinds of results to appreciate the opportunity at hand. So get social, but be smart about it.

Reporting on Crime: The Websense® 2010 Threat Report

Want a glimpse into the wicked world behind the social Web? The Websense 2010 Threat Report provides that look with stunning revelations into the many risks and remedies.

Based on the Websense ThreatSeeker® Network, Websense Security Labs™ scours the Web, identifying, classifying, and monitoring global Internet threats and trends for enterprises around the world. Utilizing hundreds of technologies — including honeyclients, honeypots, reputation systems, machine learning, and advanced grid computing systems — the system analyzes more than one billion pieces of content daily. In fact, every hour the ThreatSeeker Network scans more than 40 million websites for malicious code and nearly 10 million emails for unwanted content and malicious code.

And that translates into unparalleled visibility into the state of Web security. The Websense 2010 Threat Report summarizes that research with real-world insight into the security challenges that come with the social Web in 2010.

According to the report, the most visited websites of 2010 offered superior content and functionality with the majority having a more socially dynamic presence. Meanwhile, hackers upped their ante, adjusting their strategies with social networking in mind. Attacks became more blended, sophisticated, and targeted — introducing new tricks and methods of delivery, including script-based attacks and search engine optimization (SEO) poisoning. Some threats and botnets were reinvented with vigor and most attacks rallied around stealing data.

A sample of key statistical findings include:

- **111.4%** increase in the number of malicious websites from 2009 to 2010.
- **79.9%** of websites with malicious code were legitimate sites.
- **22.4%** of searches for breaking trends and current news led to malware.
- **52%** of data-stealing attacks occurred over the Web.
- **65%** of the top 100 most popular sites are categorized as social networking or search.

In the end, enterprises are reported to be putting up defenses against the parade of social networking security threats.

For a copy of the full report, please visit:

http://www.websense.com/content/threat-report-2010-introduction.aspx?intcmp=HomePageCampaign_MainFlash-Banner-ThreatReport-110910

Websense Solutions: Web Security Done Right

Developed within Websense Security Labs, the Websense ThreatSeeker® Network is the technology foundation for its Web security, email security, and data security solutions. The system provides the intelligence that underlies essential information protection by delivering real-time reputation analysis, expanded behavioral analysis, and actual data identification.

Putting that foundation to work for better control over social networking threats, Websense Web Security Gateway solutions are the industry's leading secure Web gateway solutions. It is part of the Websense TRITON solution, which provides the best protection against modern Web threats at the lowest total cost of ownership. Web Security Gateway solutions offer:

- **Dynamic and Scripted Web Malware Protection** – Real-time security scanning provided by the Websense Advanced Classification Engine (ACE) helps protect against legacy file-based attacks as well as Web scripts and dynamic threats that evade traditional antivirus.
- **Web 2.0 Employee Productivity** – Real-time content classification from ACE removes inappropriate content from complex, dynamic, and password-protected Web 2.0 sites that cannot be accurately classified by traditional URL filtering.
- **Data Loss Prevention and Compliance Controls** – The Websense TruWeb DLP™ capability offers enterprise-class Web data loss prevention. It establishes the controls needed to enable outbound communications to destinations like webmail and social networks while helping enterprises meet compliance mandates to control disclosure of sensitive data.
- **Lowest Total Cost of Ownership (TCO)** – The Websense TRITON Console and Websense TruHybrid™ deployment reduce the number of appliances, management systems, and vendors that must be supported across the enterprise.

These are the only solutions to provide enterprise-class data loss prevention and unified management of hybrid on-premise/Security-as-a-Service (SaaS) deployments. Secure Web gateway solutions enable organizations to leverage the power of social networking and Web 2.0 without worrying about malware, inappropriate content, employee productivity, or disclosure of sensitive information.

For more information, please visit: <http://www.websense.com/content/WebSecurityOverview.aspx>

About Websense

Websense, Inc. (NASDAQ: WBSN), a global leader in unified Web, data, and email content security, delivers the best security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market, and small organizations around the world. Distributed through a global network of channel partners and delivered as software, appliances, and Security-as-a-Service (SaaS), Websense unified content security helps organizations take advantage of powerful new communication, collaboration, and Web 2.0 business tools while protecting from advanced persistent threats, preventing the loss of confidential information, and enforcing Internet use and security policies. Websense is headquartered in San Diego, Calif. with offices around the world.

For more information, please visit: <http://www.websense.com/content/Home.aspx>