IDC
Analyze the Future

WHITE PAPER

Best Practices for Securing Web 2.0

Sponsored by: Websense

Brian E. Burke

June 2009

IDC OPINION

Like it or not, Web 2.0 is quickly becoming "enterprise 2.0" as a growing number of Web applications make their way into the corporate environment, bringing with them even more security concerns and attack vectors. It is IDC's opinion that organizations should embrace the value of Web 2.0 tools as a way to help lower costs and increase collaboration with little to no administrative burden on IT staff. Failed attempts to ban or discourage use of consumer instant messaging networks in the past taught organizations that it is not good for business (e.g., employee productivity and morale) to say no to workers who wish to use tools such as Twitter or Facebook to collaborate and stay connected with clients, prospects, and partners. Furthermore, to ignore the pervasive use of Web 2.0 technologies belies the reality of most business environments today, where everything from SaaS applications and Webmail to desktop replacement technologies plays a crucial role in day-to-day operations while presenting many unaddressed risks.

The challenge for organizations is that many Web 2.0 applications were designed for consumers, not for business users whose online activities can have dire consequences for their organizations if the tools are used irresponsibly. This challenge is compounded by the fact that the Web 2.0 applications that were designed for business use were not designed for existing security frameworks, architectures, and deployments. Moreover, virtually all of the top 100 Web sites, from Google and Yahoo! to Wikipedia and MSNBC, rely on or host some type of user-generated content, and the risk profile and challenge for organizations only increase. Fortunately, a growing amount of help is available for organizations looking to allow their workers to use Web 2.0 tools responsibly without sacrificing security and regulatory compliance requirements. In this tough economic climate, increasing collaboration and reducing costs are more important than ever. Web 2.0 technologies, if used securely, can help organizations increase collaboration and productivity and drive revenue. In response to these challenges, IDC has partnered with Websense to further understand the current pain points organizations face in dealing with the adoption of Web 2.0 technologies. Our research found that:

- 95% of organizations allow access to Web 2.0 sites, and 62% of IT managers think Web 2.0 is necessary to their business (source: Websense's 2009 Web2.0@Work survey).
- 64% of IT managers permit access to social network sites primarily used for business, but a significant 1 in 2 organizations (49%) allow access to social network sites primarily used for personal use (source: Websense's 2009 Web2.0@Work survey).

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

- 27% of global IT managers in large organizations are not sure about the access status of some Web 2.0 sites (source: Websense's 2009 Web2.0@Work survey).

- 70% of organizations view Web 2.0 as a serious concern for data loss prevention (source: IDC's 2008 *Security Survey*).

METHODOLOGY

This white paper was designed with the aim of revealing, understanding, analyzing, and presenting the predominant issues relating to the adoption of Web 2.0 technologies in the corporate environment. The paper draws on data from Websense's 2009 Web2.0@Work survey of 1,300 IT managers at large organizations across 10 countries and existing IDC research. Using this body of knowledge, we describe the overall business and technical challenges that organizations face in dealing with Web 2.0 issues and provide guidance on the types of solutions that play a key role in addressing today's complex threat environment. This paper discusses the limitations of traditional Web security technologies and the need for more advanced security techniques in dealing with Web 2.0.

SITUATION OVERVIEW

Web 2.0: Embrace or Extinguish?

Web 2.0 is not really a new technology offering; rather, it is about using existing technologies to enhance usability, collaboration, and information sharing and gathering over the Internet. To get a clearer picture, one must look at the different technologies existing under the umbrella phrase of Web 2.0 as a taxonomy, as shown in Figure 1.

The taxonomy illustrates the unique challenges associated with Web 2.0, including:

- Web 2.0 sites that rely on user-generated content to compile and present content in new ways

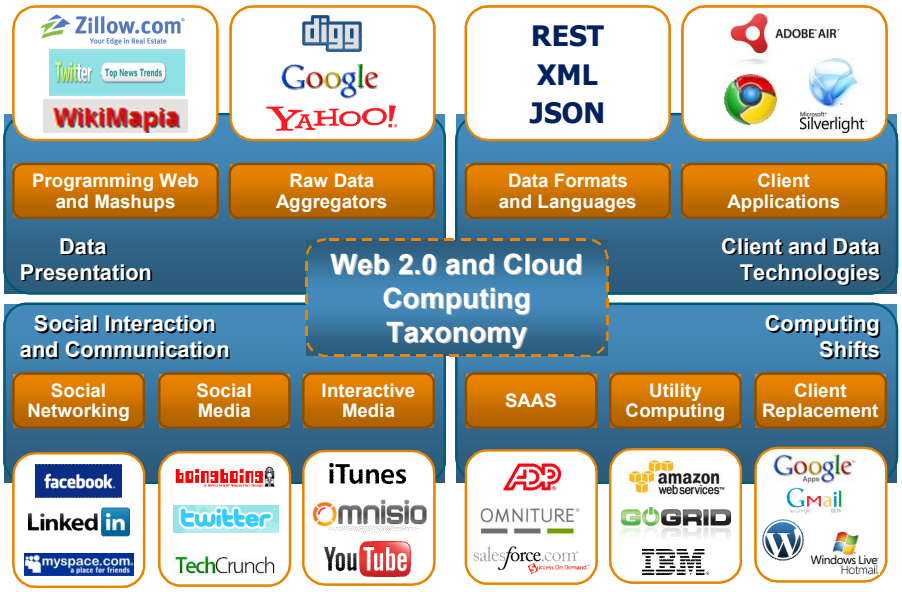
- New client and data technologies that move beyond the HTML Web of the past and into newer, richer mechanisms to share content

- New mechanisms to share and store data and use noninternal architectures from Salesforce to Google Apps

- Social interaction and communication that are supplanting many of the traditional modes of collaborating, communicating, and sharing information

FIGURE 1

Web 2.0 Taxonomy



Source: Websense, 2009

Many organizations are embracing these Web 2.0 technologies to enhance relationships with clients and provide differentiating service and personalization or to streamline their infrastructures and replace traditional infrastructure and reduce communication costs. IDC believes the combination of a global recession, the need for both IT and information workers to do even more with even less, and the growing availability of Web 2.0 tools will cause the adoption and usage of enterprise social networking, blogs, microblogs, SaaS applications, wikis, and other tools to skyrocket.

IDC strongly urges organizations to create a security strategy that empowers and encourages workers to innovate with Web 2.0 rather than hinders such efforts. During this recession, organizations need to strengthen relationships with customers and prospects; tap the collective wisdom of partners, customers, and others to augment the knowledge of shrinking workforces; and gain a competitive advantage over firms that continue to make the mistake of saying "No we can't" to Web 2.0.

IDC strongly urges organizations to create a security strategy that empowers and encourages workers to innovate with Web 2.0.

However, many organizations are struggling with balancing the business value of Web 2.0 technologies with the risks and security implications of many nonsecure and uncontrolled Web 2.0 environments. IT is feeling pressure from users and executives alike to allow greater access to Web 2.0 technologies and at the same time protect against malware and information leaks over this pervasive environment for new content usage, information sharing, and communication. The Web2.0@Work survey found that 86% of IT managers feel pressure to allow access to Web 2.0 sites and applications from within their organization and that 30% of this pressure is coming from C-level and director-level staff. It's clear that IT cannot say no to C-level executives. Organizations need the tools to embrace Web 2.0 technologies while ensuring security and compliance.

Web 2.0: The Consumerization of IT

The Web 2.0 world is no longer black and white. An interesting phenomenon is taking shape that IDC is calling the "consumerization of IT." Social networking sites, such as Facebook, which were once considered to be only consumer applications, are quickly moving into the enterprise environment. IDC has spoken to many organizations that tell us that the current generation of new employees, fresh out of college, is expecting access to Web 2.0 networks such as Facebook and Twitter. These new employees do not communicate with traditional email and are bringing their social networking tendencies with them into the workplace. Although this may seem anathema or in some ways trivial to traditional IT and security staff, it is a very real trend that will increasingly impact organizations. In fact, high-level management staff told IDC that they have lost potential employees because the employer would not allow access to Web 2.0 applications at work.

IDC believes a growing number of consumer-oriented Web 2.0 technologies will continue to saturate the corporate environment. The boundaries between consumer and corporate Web 2.0 environments are blurring. Even the use of the top 100 Web properties transitions from static content to dynamic and interactive user-generated Web 2.0 content. Many employees now use interactive content portals and social networking applications such as Facebook to communicate with a mix of friends, coworkers, and customers. This is creating a complex security challenge for organizations of all sizes. These environments create both a risk of data leaks and new channels for malware.

The boundaries between consumer and corporate Web 2.0 environments are blurring.

Lines are clearly blurring between professional life and personal life, and in such "consumerization," security policies must be flexible, extensive, and pervasive. Trade-offs must be found between the user's comfort and global security. Forbidding personal use of the computer was the best practice some years ago, but it is not possible anymore due to users' skills and needs.

Web 2.0 Threat Environment

Web 2.0 environments are increasingly being used as the threat vector of choice by hackers and cybercriminals to distribute malware and perpetrate identity theft, financial fraud, and corporate espionage. Hackers are leveraging the popularity of Web 2.0 to reach the greatest number of users and are targeting nonsecure Web 2.0 sites that are extremely vulnerable to compromises.

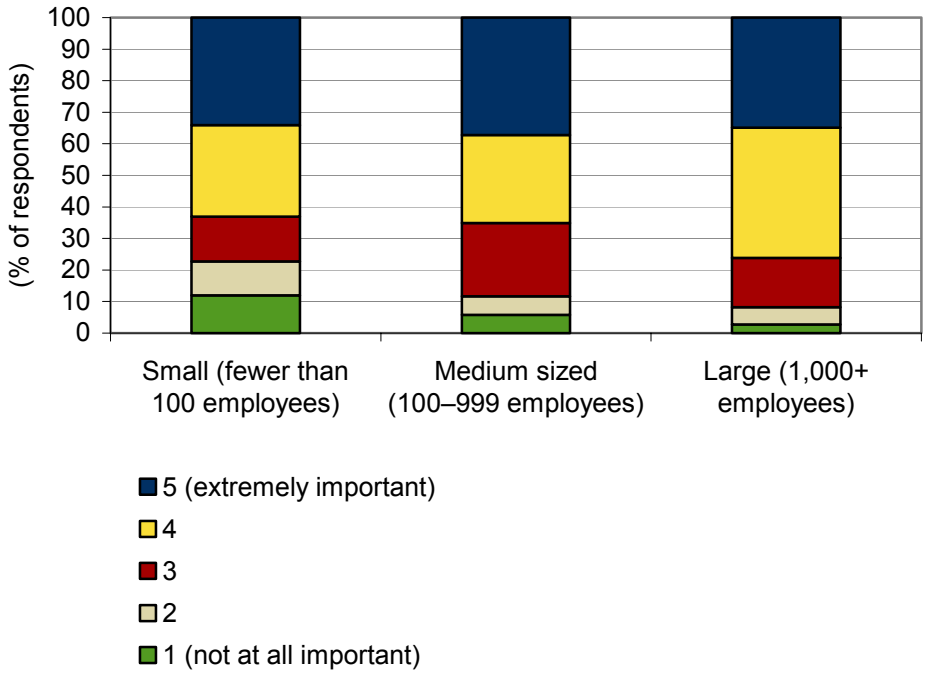
Web 2.0 also presents a significant data loss prevention (DLP) challenge for many enterprises. Message boards, blogs, tweets, and other types of social networking sites are becoming pipelines for information leakage and compliance violations. In fact, a recent IDC survey showed that 37% of confidential information leaks occurred via the Web. The same survey also showed that almost 70% of organizations believe that monitoring employee use of the Web to prevent data leaks and compliance violations is a major concern (see Figure 2). Given that Web 2.0 exposes organizations to both inbound and outbound security threats, IDC believes that future Web security solutions must analyze traffic bidirectionally.

Given that Web 2.0 exposes organizations to both inbound and outbound security threats, IDC believes that future Web security solutions must analyze traffic bidirectionally.

FIGURE 2

Importance of Monitoring Employee Web 2.0 Use by Company Size

Q. Using a 5-point scale where 5 is extremely important and 1 is not at all important, please rate the importance of monitoring employee use of Web 2.0 to prevent data leaks and compliance violations.



n = 433

Source: IDC's *Security Survey*, 2008

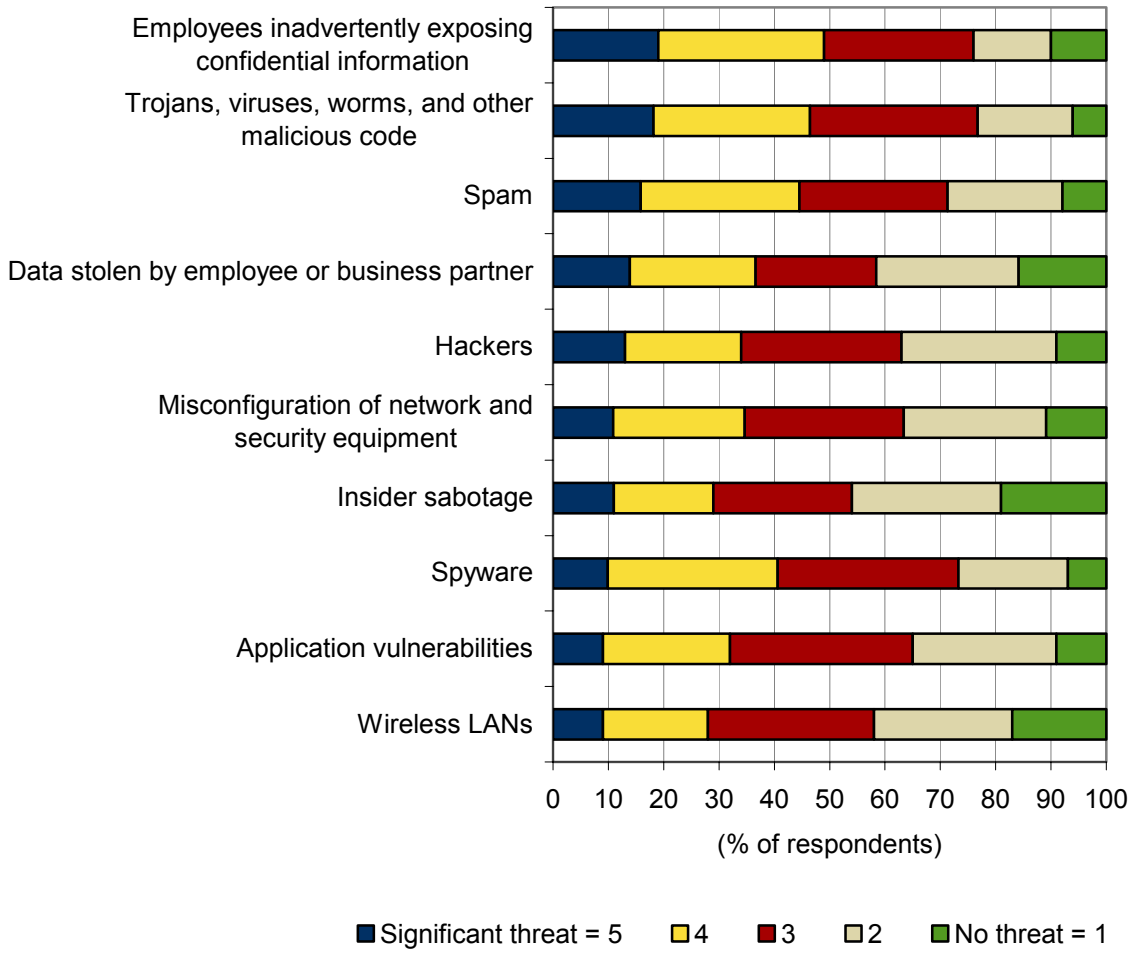
In IDC's annual security survey of IT and security professionals, participants were asked to rate the top threats to their company's network security. Figure 3 displays the top 10 threats in 2007. IDC believes many of these threats are directly related to the growing popularity of Web 2.0, including the following:

- The exposure of confidential information is now the single greatest threat to enterprise security. A recent IDC survey on information protection and control (IPC) showed that Web email or Web posting (e.g., message boards, blogs) accounted for 37% of information leaks. We also found that almost 70% of all organizations view Web 2.0 as a serious concern for DLP. Government and industry regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and various SEC regulations are forcing corporations to secure the use of all electronic forms of communications, including the Web.

- Trojans, viruses, worms, and other types of malicious code ranked as the second greatest threat to enterprise security. Virus writers and hackers are increasingly leveraging the popularity and complexity of Web 2.0 sites to target the greatest number of users. The practice of hackers planting malicious code on legitimate Web sites is quickly becoming the norm. Hackers and malware developers are aggressively innovating ways to compromise popular Web 2.0 sites and others to install malicious code designed to steal personal and/or business confidential information and to be difficult to detect.
- Spam has risen back up the list and is number three among the top threats to enterprise security. The pure volume of spam continues to rise at a rapid pace, and malicious attacks are becoming more sophisticated (e.g., blended threats that combine spam, spyware, viruses, and other malware in their attacks). Spammers are increasingly using spam to lure users to malicious Web sites.
- Spyware continues to be both a security and a system management nightmare. Theft of confidential information, loss of productivity, consumption of large amounts of bandwidth, corruption of desktops, and a spike in the number of help desk calls related to spyware are overwhelming many IT departments. More recently, spyware has evolved from a mischievous hobby to a money-making criminal venture that has attracted a new breed of sophisticated hackers and organized crime. The Web is without a doubt the single greatest source of spyware infections.

FIGURE 3

Top 10 Threats to Enterprise Security



n = 433

Source: IDC's *Security Survey*, 2008

WEB 2.0 BEST PRACTICES

Securing Web 2.0

The advances in Web 2.0 technologies in recent years require a new generation of Web security tools that go well beyond traditional URL filtering.

IDC has identified 10 best practices that organizations should consider when choosing a Web security solution to address the risks of Web 2.0:

1. **Dynamic Web 2.0 defenses.** Threats in today's Web 2.0 world incorporate the worst of Web 1.0 threats with some new variations mixed in for good measure. Traditional known threats such as file-based antivirus attacks still exist along with a new generation of script-based attacks that are designed to compromise the Web

browser and other applications. Mixed in with these threats are blended or polymorphic attacks that change every time a user visits a Web site or accesses a file. What is clear is that static defenses such as traditional antivirus inspection, site reputation, or stripping of attachment types are doomed to failure. Effective defenses must be dynamic in nature to match the dynamic threats they face. The real-time nature of Web 2.0 demands a new generation of protection technologies that work in real time to inspect all of the aspects of the Web page and to correlate these different objects into a single view of the environment into which the end user is entering. Only when the complete content and context of the Web page have been analyzed can an accurate judgment be made on the potential threats contained.

Effective defenses must be dynamic in nature.

2. **Real-time content classification.** The high volume of user-generated content in the Web 2.0 environment requires that effective Web security solutions have real-time deep content analysis and classification. Many Web 2.0 sites today incorporate some form of a Web site mashup that may be customized to an individual's interests. iGoogle, one of the most common and seemingly innocuous mashups, can potentially be the weakest link in a company's security policy because of the complexity that even simple mashups introduce to the security and control equation. Dynamic classification comes into play for Web 2.0 when looking at social sites that use mashups or multiple frames. It is necessary to have a system capable of analyzing multiple flows in real time to let in the good information while keeping out the bad and inappropriate information. Besides the ability to individually block frames on the mashup, the Web security solution should be able to identify access to restricted Web sites through channels such as "Proxy Avoidance" or "Anonymizer" Web sites and Google Translate.

It is necessary to have a system capable of analyzing multiple flows in real time to let in the good information while keeping out the bad and inappropriate information.

3. **Employee access.** Employee education is the cornerstone for effective Web 2.0 risk management. IDC believes employees must understand both the benefits of Web 2.0 technologies and the threats and risks. Web 2.0 technologies are used in a wide variety of sites, ranging from mission critical to harmless. A mature Web 2.0 security solution must allow access to mission-critical SaaS Web sites (e.g., Salesforce.com) while enabling safe and controlled access to nonbusiness sites such as social networking or interactive media. In the past, simply blocking all nonbusiness sites might have been an option, but today most employees expect some limited and controlled access to personal Web sites. A mature Web 2.0 solution can provide safe but time-limited access to sites for personal use. An organization, for example, may want to allow up to 60 minutes per day of access to personal Web sites (Web-based email, social networking, etc.). A Web 2.0 security solution must allow this kind of rationed access.

4. **Data loss prevention.** Web 2.0 presents a significant DLP challenge for many enterprises. Message boards, blogs, and social networking sites are becoming pipelines for information leakage and corporate compliance violations. As we open the doors to Web 2.0 applications that we might have simply blocked in the past, we have to ensure that sensitive information is not leaked over Web-based email, posted to Internet message boards, or shared over social networking Web sites. A Web 2.0 user may inadvertently post confidential information on blogs or post other data that is business critical. An integrated DLP-Web solution adds the identity and location context to the access, making sure that confidential data is not leaked out of the organization.

5. **Application control.** Many Web 2.0 applications and newer instant messaging tools leverage evasive techniques to communicate and share information. The challenge of identifying these applications and applying appropriate policy is a burden facing many organizations today. Many Web 2.0 properties include Web-based applications within the site. An organization may wish to allow Facebook and even Gmail access, for example, but may want to block Google Chat for instant messaging, Facebook-delivered games, and proxy avoidance applications. A mature solution must provide control over these applications whether they run over HTTP, HTTPS, or some other protocol. The right solution should provide the right level of granularity of control that ensures that the users have secure access.

6. **Remote access.** The growing number of mobile and remote users is creating a complex distributed workplace. Many corporate applications are being moved to the Web 2.0 environment to allow remote employees to work more efficiently. Users don't simply sit in their office and work anymore — today's mobile employees are almost as likely to be connected from home or from a public WiFi hotspot as they are to be sitting in the corporate office. An effective Web 2.0 solution should provide the customer with choices on how to support the remote user while ensuring the application of a consistent policy throughout the organization.

7. **Unified policy management.** Policy management is the point at which all of the different technologies used to enforce a policy should come together. The focus of a policy should be the user or group of users to which the policy applies and the threats and behaviors that the business wishes to address. Web 2.0 requires a policy to address multiple technology stacks, everything from malware protection to objectionable content and application control. This complexity can lead to errors in translating a corporate policy into reality unless the policy management engine is designed to pull all of these items together into a single policy that can be applied on a global basis.

8. **Comprehensive reporting and logging.** Because employees may use wikis, blogs, and other Web 2.0 technologies located outside the corporate network for collaboration on sensitive, internal projects, reporting and logging for audit and forensics are considered critical. Often, corporations enable access without any restrictions. However, they log and report on all activities as the basis for potentially implementing future policies. The solution must enable multiple levels of reporting, including easy-to-interpret summary reports and the ability to drill down and quickly investigate violations against specific policy categories or by specific users and groups.

9. **Performance and scalability.** To be successful, any solution must provide high performance and deliver security and control without impacting the ability of end users to perform their duties. Scalability, or the ability of the solution to expand and adapt to current or future needs, is a large issue with Web 2.0 because Web 2.0 is still rapidly evolving and it is impossible to define what future requirements may be. A solution that is modular in design and distributed in nature, while being completely integrated in its analysis, management, and reporting capabilities, offers the best approach to keeping up with the uncertain demands that are sure to arise as the Web 2.0 world continues to mature and change.

10. **The server side of Web 2.0.** To get the most from the marketing and customer service aspects of Web 2.0, companies are increasingly allowing their customers to post comments on public support forums, ask-the-editor sites, Facebook blogs, etc. If organizations are going to set up their own such communities, they need to ensure that malware and inappropriate content are not posted on the sites associated with their brand. To limit liability and protect their brand, organizations need to think about how they can scan blog posts before those posts hit their Web 2.0 sites. In essence, companies need to think about both sides of the Web 2.0 coin — the client side *and* the server side. The client is more important at the moment, but moving ahead, companies will need to have their own properties to reap the biggest marketing benefit.

SUMMARY RECOMMENDATIONS: FIVE KEY SECURITY CONFIGURATIONS TO USE

- **Protect your organization:** Enable both real-time content and security scanning on all categories of Web sites that leverage user-generated content from search engines and Webmail to social networking.

- **Enable Web 2.0 benefits:** Use drill-down reports to gain visibility into which users and groups most consistently try to access Web 2.0 technology and create a policy to enable the safe and appropriate use of these tools.

- **Increase productivity:** Control specific applications like instant messaging over the Web by users with measures like time allotment, bandwidth-based controls, or content restrictions.

- **Get full visibility:** Decrypt and examine the content, including data for all HTTPS traffic to Web 2.0 sites and for applications like Webmail for inbound threats and outbound risks.

- **Protect your data:** Monitor and report on sensitive and regulated data sent over or posted via the Web by users, intended destinations, and the category of site or Web application. Then, create the appropriate enforcement policy that protects and enables the organization.

WEBSENSE OVERVIEW

Securing Web 2.0

Company Overview

Websense Inc. (NASDAQ: WBSN) is a global leader in integrated Web, data, and email security, providing Essential Information Protection for more than 42 million employees at more than 50,000 organizations worldwide. Headquartered in San Diego, California, Websense distributes its solutions through a global network of channel partners. Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information, and enforce Internet use and security policies. Websense has its roots in Web filtering

and continues to develop its core strength in discovering and classifying content across all its product offerings. Websense provides visibility into the internal and external movement of information in the Web 2.0 world, with extensive management of who is authorized to access Web sites, content, or applications, as well as what data must be protected from leaks, where users and data can go online, and how data and online resources can be communicated and used.

Web 2.0 Security Overview

- Websense Web Security Gateway allows organizations to secure Web traffic effectively while still enabling the latest Web-based tools and applications. Through a multivector traffic-scanning engine, the Websense Web Security Gateway analyzes Web traffic in real time, instantly categorizing new sites and dynamic content and proactively discovering security risks and blocking dangerous malware.

- Using the Websense ThreatSeeker Network, the Websense Web Security Gateway provides advanced analytics, including rules, signatures, heuristics, and application behaviors, to detect and block proxy avoidance, hacking sites, adult content, botnets, keyloggers, phishing attacks, spyware, and many other types of unsafe content. Websense Web Security Gateway also closes a common security gap: decrypting and analyzing SSL-encrypted content before it enters the network.

CHALLENGES/OPPORTUNITIES

With Web 2.0 applications the challenge is to imagine threats where no perceived threats exist today. As conditions change and companies use Web 2.0 for large enterprise projects that involve sensitive data, security will need to be applied to this environment. The tolerance for simply applying security after a problem will be seen as increasingly poor, legally deficient, and ignorant of emerging threat environments.

Still, changing behaviors and perceptions requires an incremental approach. The first step is monitoring so that IT understands the issues and can prepare solutions. The next step is reporting on the findings in such a way that senior executives and business unit managers can understand the benefits of controlled collaboration where customer information and intellectual property (IP) are protected from mistaken, mischievous, and malicious exposure. This phased approach is slow and cumbersome to implement, but necessary. In concert, technologies must support gradual migration while also offering the flexibility to deal with monitoring, reporting, and enforcement. The policy enforcement aspect must be flexible enough to handle both draconian and laissez-faire attitudes toward these environments.

CONCLUSION: THE INFINITE POSSIBILITIES BETWEEN ABJECT FEAR AND LAISSEZ-FAIRE

Instead of rolling up into a ball like an armadillo as an instinctive survival tactic or just adopting a laissez-faire process in which "anything goes," successful organizations should embrace and implement Web 2.0 technologies.

To minimize the risks associated with Web 2.0, organizations will need to deploy a new generation of content-based security gateways that enable the safe and productive use of Web 2.0.