



A Websense® White Paper

# Protecting Essential Information

Securing the Foundation of the Internet Business Platform

**websense**®  
ESSENTIAL INFORMATION PROTECTION™

The Internet may be today's most crucial enterprise productivity tool. However, unfettered use of this business platform can endanger an even more critical business asset—an organization's essential information. Information at immediate risk ranges from sensitive intellectual property to financial statements to customer and employee data.

Security managers must shift their protection emphasis from guarding against inbound attacks at the infrastructure level—a model suited to perimeter boundaries and the Internet as a simple content resource—to guarding essential information against blended threats and accidental or malicious loss, in tune with Web 2.0 and the Internet as a business platform.

The requirements for Web security, email security, and data loss prevention have changed. Read on to learn:

- [Where and why traditional approaches fail](#)
- [How accuracy and context drive effective information-focused security](#)
- [What to do to protect essential information and say Yes to, rather than block, business processes that take advantage of Web 2.0 and the Internet business platform](#)

## Introduction

Today, the Internet touches every facet and asset of business. Efficient organizations rely heavily on the Internet as a business platform—through software-as-a-service and Web-based applications, remote workplaces, and extended partner ecosystems. This Web 2.0 platform enables competitive advantages and Employee 2.0, the anywhere, anytime, always-connected worker.

Yesterday's enterprises locked precious source code, proprietary research, financial statements, and personally identifiable information inside secure servers or behind isolated network segments. Progressive enterprises now let this essential information flow freely within and beyond their boundaries.

For security managers, the Internet platform is both friend and foe. Web 2.0 allows for unprecedented collaboration and exchange of information, and companies that close the door on the opportunities offered by Web 2.0 risk losing their competitive edge. But Web 2.0 also introduces an entirely new type of risk, with Internet-enabled threats that take full advantage of new technologies and vulnerabilities. Threats that no longer focus on either the core or the extended edge of the network, but instead, use Web 2.0 and converged communications to integrate invisibly with day-to-day operations.

The risks are not all from the bad guys or from the outside, either. The openness of the Internet platform has also increased the risk from the inside. Whether opening up liability issues with inappropriate content, reducing productivity, or allowing accidental and malicious loss of essential business information, Internet-enabled risks are forcing security managers to deal with more than just black or white security issues.

To keep up with these changes, data and network protections must evolve as well. Defenses that take at-the-network or on-the-endpoint, signature or behavior-based, good or bad approaches simply will not guard against these threats. Worse, these approaches use a simplistic "on or off" model of access and blocking that can cripple the Internet business platform. No enterprise can just turn the Internet "off." The Internet is a business tool that must be managed and appropriately protected, like every other significant asset in the business. Security managers must find a way to say Yes to these advances with the confidence that the company's essential information is safely guarded.

**\$400 MILLION:** The value of trade secrets stolen by a DuPont scientist for a Chinese rival<sup>1</sup>

## Appropriate Protection for Essential Information

Application of appropriate protection is both critical and subjective. Each business must protect its sensitive information and workflows in ways that match its environment, risks, and risk posture. Let's consider today's challenges and remedies.

### Can sensitive and regulated data be identified and its loss prevented?

**The situation:** Data is the currency of organizations today. It is stored in, and accessed from, databases, document repositories, file shares, end-user file systems, and portable storage. It is exchanged inside the organization and shared outside with vendors, partners, end-users, consumers, the government, and many other constituents.

<sup>1</sup> <http://www.scmagazineus.com/Former-DuPont-scientist-gets-18-months-in-jail-to-close-out-400-million-corporate-espionage-case/article/96290/>

**The problem:** Data is often stored, used, and exchanged inappropriately. It is also increasingly the target of attack and theft. Failure to protect data results in risks of non-compliance, fines, lawsuits, loss of competitive advantage, brand damage, and even violations of national security. Proliferation of Web-based applications and information exchange compound these risks.

**Today's response:** Traditional data loss prevention tools rely on simplistic “on or off” controls based on primitive data identification. For instance, basic “guessing” around keyword matching can result in false positives or multiple matches that do not constitute actual violations. Yet these results trigger blocks on transmission or collection of files. Blocking data in motion or removing data at rest with this false-positive laden approach literally brings the flow of information, and, by extension, the business, to a halt. In addition, these “on or off” solutions typically have no concept of business workflow or policies that can adapt controls to match changing business needs.

Japanese officers, who should never have had the data in question on their systems, downloaded classified data about the United States Aegis missile defense system in an exchange of porn.<sup>2</sup>

An AMA survey said 18 percent of companies block employee visits to external blogs.<sup>3</sup> Why do enterprises care? Cisco was sued based on an employee's external blog.<sup>4</sup>

#### Can IT managers say Yes to blogs?

**The situation:** Blogs are a great Web 2.0 example of information exchange and user-generated content. Blogs can help a financial organization discover companies to invest in, a media company to gather storyline ideas, or a technology company to search for market opportunities and drive brand awareness.

**The problem:** Exchanging innocent information is fine, but no entity wants its users to be compromised by vulnerabilities on a blog, bring inappropriate content into the organization, waste time, or worse, post sensitive client information, new storylines, or intellectual property. These issues mean liability for the organization.

**Today's response:** Traditional content and network security can only respond by turning off blog communication wholesale or leaving it on with the uncomfortable knowledge of unmitigated risk. This heavy-handed response does not match business needs for information exchange and modern tools.

“Even for enterprises that aren't concerned about productivity erosion, the Web threat environment is too virulent to ignore.” – Burton Group.<sup>5</sup>

#### Can tools accurately differentiate good Web 2.0 from bad?

**The situation:** Web 2.0 is very different from the world of informational sites in simple content categories. Web 2.0 uses dynamic programming to build unique Web pages that present different content to suit the moment, history, and attributes of the user. This Web is not just about the coffee break visit to MySpace, but about commercial sites—Wikipedia, LinkedIn, YouTube, and Google—that support legitimate research and business operations.

<sup>2</sup> <http://www.infosecnews.org/hypermail/0704/13040.html>

<sup>3</sup> <http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/>

<sup>4</sup> <http://www.forbes.com/technology/forbes/2008/0407/044a.html>

<sup>5</sup> “Burton Group Security and Risk Management Strategies report, “Web Filtering: Completing the Evolution from Acceptable-Use to Serious Malware Defense.” Jan. 1 08 <http://www.burtongroup.com/Research/PublicDocument.aspx?cid=1185>

**The problem:** Changes in Internet technologies make it possible for criminals to target essential information and invite accidental disclosure. Along with acceptable and “safe” content, Web 2.0 sites can also readily host transitory malware and spiked user-contributed content that’s unmonitored and unregulated. There is no “click to accept” button to alert users. Corrupt links, malicious widgets, and embedded scripts introduce malware within content and within pages. Users visiting benign sites can be redirected to sites that scan the user’s computer for sensitive data, passwords, and vulnerabilities.

**Today’s response:** Today’s responses rely on traditional concepts of blocking based on good or bad sites. This fails to keep up with the pace of change vulnerability at the content level. Adding reputation is not enough to address the content-based threats. For example, the reputation of MySpace varies depending on the content being served on each page and when good sites like MSNBC are compromised at the content level, reputation is irrelevant. Without such content becoming part of granular understanding of the overall site and its respective classification, traditional solutions over- or under-block and cannot facilitate safe business use of the Web.

Among 26,000 sites compromised by a search engine exploit, MSNBC was hacked just before broadcasting the March 2008 NCAA college basketball tournament.<sup>6</sup>

The increasingly common occurrence of threats involving multiple channels is shaping the content security market, and a silo-based approach to e-mail and Web filtering will respond poorly to such threats. – Forrester Research<sup>7</sup>

#### Can solutions protect users and data from blended email and Web 2.0 attacks?

**The situation:** Email and Web applications have become tightly entwined in webmail and email with HTTP content. These communication channels also serve other enterprise applications like ERP and CRM, especially in hosted services. Converged communications streamline workflows, reduce error, and enable non-stop operations.

**The problem:** Today’s commercial crime rings combine spam, email, and application channels in cross-channel techniques. For example, one type of inbound blended threat uses email to lure viewers to counterfeit URLs, or even to known good URLs that have been compromised with rogue code to capture email passwords and plant key logging software or Trojans. What is most dangerous is that this malware can be tailored to steal specific data of high value to the individual and the enterprise. These targeted compromises often go unnoticed, especially on niche industry sites.

**Today’s response:** Most enterprises still protect each communication channel and direction with independent outbound email and data content filters, inbound filtering of spam and viruses, and blocking of inappropriate and malicious URLs. These separate silos look at the URLs or the email headers, but not both, and they rarely pay attention to the data itself or proactively block its outbound transmission. They react based on a historical view of threats built on outdated inspections, signatures, reputation, and behavior. Blended threats easily bypass these inspections by morphing and moving around the Web while stealing data.

March 2008: The large Hannaford Brothers supermarket chain was sued after network intrusions may have compromised 4.2 million credit card records.<sup>8</sup>

6 <http://www.itbusiness.ca/it/client/en/Home/News.asp?id=47631>

7 “Content Security Is Becoming A Competition Among Suites: Websense Rounds Out Its Security Portfolio With Its Acquisition Of SurfControl” by Chenxi Wang, Ph.D., December 2007, Forrester Research, Inc.

8 [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9070281&taxonomyId=14&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9070281&taxonomyId=14&intsrc=kc_top)

These examples illustrate the complexity and difficulty of protecting the Internet platform. Traditional solutions have proven inadequate, judging by a 2008 IDC survey on top network security threats. With inadvertent data loss at the top of the list for the first time, security managers now worry most about:

1. Employees inadvertently exposing sensitive data
2. Trojans, viruses, worms and other malicious code
3. Spam
4. Data stolen by employees or business partners
5. Hackers<sup>9</sup>

## New Requirements

Security defenses must shift the protection emphasis from guarding infrastructure from inbound attacks—a model suited to perimeter boundaries and the Internet as a content resource—to guarding essential information from outbound data loss, in tune with Web 2.0 and the Internet as a business platform. Instead of working in silos, protections must collaborate across application channels, inspection techniques, and usage perspectives. Through collaboration, tools can examine both content and context in real-time to accurately identify and block sophisticated threats.

For long-term success, two constituencies must be satisfied: risk managers and end-users. Risk managers want visibility and reliable control over data loss. End-users want to stay productive and effective. End-user needs cannot be trivialized. Frustrated (or malicious) users will find ways to circumvent tools or insist blocking rules be tamed to the point of irrelevance. With these demanding audiences, solutions must adapt efficiently to both threats and business requirements.

## A New Information Protection Formula = Accuracy + Context

Accuracy and context are central to success. Accurate identification requires deep analysis of content and data, both externally, on the Internet, and internally, traversing the network and on corporate systems and servers. Accuracy must be maintained as the data and content is used and edited, on Web sites, and in enterprise applications. Given the pace of content change (constant and instant), accurate identification requires significant computing and research resources, as well as sharing of threat information to detect threats that cross communication channels: “There’s malware in your spam,” “There’s a spammer on that Web site,” or “That data cannot be posted to that blog or emailed to that address.”

Acknowledging context requires solutions to consider multiple aspects of usage before acting. Instead of thinking about technology channels—Is this email? Is this a Web site?—tools must move to assessing the content and the data, as well as the context of its use: Who is the user? What is the data type? What are the communication channels and applications being used in the workflow? This broader perspective creates a more nuanced and accurate protection system than the sledgehammer, all-or-nothing approach of the past. Incorporation of context makes assessments relevant and controls meaningful.

A key aspect of context is the Internet itself. Is the Internet destination valid for the business, or does it compromise regulatory compliance, security, or proprietary business information? This contextual knowledge combines knowledge of the Web with knowledge of threats to flag risky destinations, clarify spam addresses, and detect inappropriate transmissions. Organizations can make better decisions about the risk of access or the risk of information exchange.

Applying these requirements for accurate identification and context-aware responses, the table below summarizes characteristics that mark the shift from a security framework that is infrastructure-based to one that is information-based.

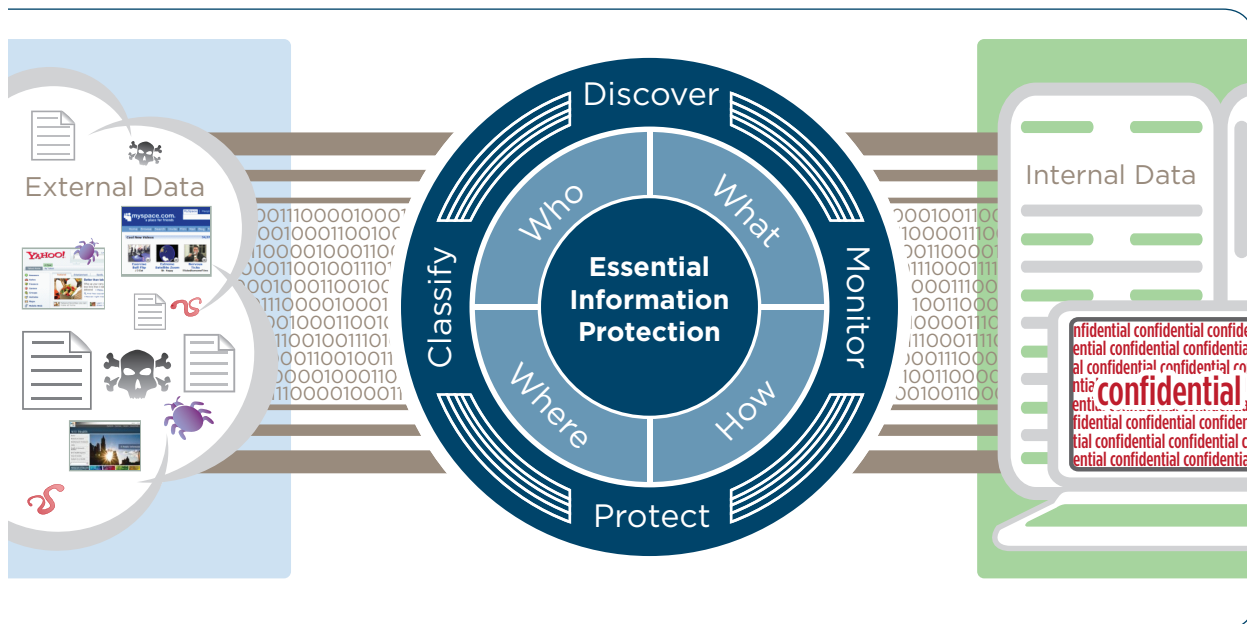
Solution Requirements to Protect and Enable the Internet Business Platform

<p>Characteristics</p>	<ul style="list-style-type: none"> <li>• Incorporates Web, email, and data loss controls for full coverage</li> <li>• Inspects inbound and outbound data flows of multiple channels</li> <li>• Combines multiple detection, identification, and classification techniques</li> <li>• Incorporates two-way knowledge of users, data, channels, and Internet destinations</li> <li>• Provides simple mechanisms for quickly deploying accurate policies and gaining visibility, with flexibility to adjust and layer additional controls and processes as risk is understood</li> <li>• Despite the dynamic nature of content and data, establishes lasting association of policies with users, data, destinations, and communication channels</li> </ul>
<p>Examples</p>	<ul style="list-style-type: none"> <li>• <b>Data Loss Prevention:</b> The solution should be able to accurately identify information across data at rest in repositories and file systems; data in motion within and outbound from the organization; and data in use in applications at the endpoint. The solution should also be able to understand what that data means in terms of regulations, proprietary data, and internal policies and allow tuning of policies to business processes. At the same time, it should be able to apply consistent policies and enable workflows that range from incident management, automated incident response and notification, summary and detailed reporting.</li> <li>• <b>Content, Information, and User-Aware Blogging:</b> The solution should understand the category of the blog, be able to identify the user, and identify the data in real-time, with enough accuracy to be able to block posting of any information that is too private. By correctly classifying the host site, reputation, and actual content of a blog, the solution should prevent the compromise of users and systems or inappropriate access to the blog.</li> <li>• <b>Web 2.0 Threats:</b> The solution should be able to understand Web sites, Web content, applications, and malware beyond reputation alone, considering usage and Internet context for a real-time risk assessment. Only with this level of understanding can threats be blocked accurately and in real-time. Even if a well-known and trusted site with a good reputation were compromised, the threat would be prevented.</li> <li>• <b>Blended Web and Email Threats:</b> A solution should be able to identify links in an email and trace them back to malicious sites or content. Based on this accurate identification, solutions should be able to act in real-time to block the email and any other attempts to access that Web site, view content, or transmit data to that destination.</li> </ul>

## Say Yes with Essential Information Protection™

Websense® integrates Web security, messaging security, and data security to protect essential information and enable productive, safe use of the Internet platform. Websense Essential Information Protection defends cross-channel communications, safeguards Web 2.0 usage, and prevents data loss. Essential Information Protection uses the ThreatSeeker™ Network, an advanced infrastructure for early threat discovery across email and Web channels, real-time identification and blocking of high-risk Web sites, and data identification techniques and technologies. Websense Web, messaging, and data security solutions use security intelligence from the ThreatSeeker Network to provide the most up-to-date protection from data loss, unwanted content, and malicious threats.

The ThreatSeeker Network combines heuristics, binary analysis, reputation, image analysis, lexical analysis, pattern detection, statistical analysis, natural language processing, data fingerprinting, and actual research experts across disciplines. These tightly coupled techniques and capabilities identify and classify data and content within the enterprise and across the Internet to drive understanding of new threats as they develop.



Websense Essential Information Protection classifies external threats and monitors internal data use to prevent the loss of regulated and confidential information.

Websense solutions harness this precise classification and Internet context to address Web security and appropriate use, email security and compliance, and data loss prevention. These solutions combine to go beyond traditional security to prevent blended threats that cross inbound and outbound risk vectors and jeopardize essential information. Through direct product integration and in combination with the research of the ThreatSeeker Network, this suite of products considers the full range of relevant components: the user, the data, the communication channels, and the Internet destination.

With this approach, Websense is unique in accurately, seamlessly, and instantly identifying and managing:

- **Who** is authorized to access specific Web sites, sensitive content or applications in real-time
- **What** data is critically important to the organization and must be protected from accidental or intentional leaks
- **How** users are allowed to communicate sensitive data, and how online resources can be used more safely and productively by the organization
- **Where** users are allowed to go online, and where sensitive data can be sent safely

Integrated Web, messaging, and data security solutions from Websense make organizations more safe and efficient. Websense provides the safety net in which employees can stay productive on any network, anytime, anywhere. Risk managers reduce legal liability, enforce compliance policy, prevent data loss, and gain visibility into their businesses in light of changing risks. By combining advanced research techniques with efficient, integrated controls, Websense Essential Information Protection provides a unique combination of Web, content, and user intelligence to stop threats at their source, thereby helping businesses realize the full potential of the Internet business platform and allowing security managers to say Yes to new technologies and capabilities.

## Summary

Although today's Internet is business-critical, its use endangers essential business information, from proprietary formulas and source code to business plans and customer lists. Converged email and Web threats fueled by Web 2.0 technologies now employ surreptitious maneuvers to circumvent traditional protections.

To ensure risk mitigation keeps in step with the threat climate, enterprises must rethink their approaches to Web, messaging, and data security. Instead of thinking about technologies, organizations must think about data. It's all about the data. How is it used? Who is using it? Where and when is it safe to use? Who can receive it? Which channels can safely send it?

This data-driven view means that, rather than investing in protection silos with limited coverage, enterprises will merge defenses across the technologies, the communication channels, and the applications through which data is transported and utilized. This integration increases the accuracy of detection and the quality of response. More than just proactive enforcement, this integration provides appropriate protection, because it allows the use of context to understand legitimate business uses and adapt responses. By protecting sensitive data, the essential information of each business, organizations can both embrace and defend the Internet business platform.

## About Websense, Inc

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, messaging and data protection technologies, provides Essential Information Protection for more than 42 million employees at more than 50,000 organizations worldwide. Distributed through its 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. For more information, visit [www.websense.com](http://www.websense.com) and

- **Sign up for security alerts and threat reports:**  
<http://www.websense.com/securitylabs/>
- **View solution information and supporting educational materials**  
<http://www.websense.com/global/en/ProductsServices/>
- **Download white papers or case studies and join webcasts**  
<http://www.websense.com/global/en/ResourceCenter/>
- **Evaluate solutions**  
<http://www.websense.com/global/en/Downloads/>
- **Locate and contact a Channel Partner**  
<http://www.websense.com/global/en/Partners/Channel/FindPartner/>