



A Websense® White Paper

Extending Your Web Security Solution to Address Data Loss

Web Security Must Evolve

Web 2.0 technologies are transforming the Web. What was once little more than a resource for obtaining relatively static information has now become a highly dynamic communications medium that is well suited as a platform for modern business applications. Traditional means for achieving Web security must transform accordingly as businesses now require control over not just where their users go on the Web, but where their data is going as well. An appropriate solution will:

- Enable legitimate business activities while securing users *and* data;
- Minimize corporate and compliance oriented risks due to data loss;
- Expose broken business practices and facilitate their remediation;
- Score a quick win for the Web security team as it helps solve what is rapidly becoming a major challenge for businesses.

Web 2.0 is Transforming Business



The Web is the New Application Platform

Web 2.0 technologies have forever changed the nature of the Web and, along with it, the nature of Web security. Web content is now highly dynamic, precipitating the need for security solutions that are capable of real-time assessment, categorization, and threat control. But that's not all. Web 2.0 has also turned things around, quite literally, by enabling the use of the Web as a channel for outbound communications. Because of its ability to enhance collaboration and further facilitate business processes, this particular aspect of Web 2.0 is generally viewed as a positive. Nonetheless, it has a significant downside as well: it dramatically increases the potential of the Web channel as an avenue for the unwanted exposure of confidential data.

Fortunately, Websense provides its customers with a straightforward yet feature-rich and highly robust solution to this problem. Specifically, users of our Web security products can substantially increase the value of these solutions simply by implementing a fully integrated set of market-leading data loss prevention (DLP) capabilities that is also available from Websense.

Evolution of the Web Security Challenge

Establishing adequate Web security originally required little more than implementing URL filtering, ideally supplemented with antivirus and Web reputation capabilities. These technologies were all an IT department needed to effectively keep users from accessing unproductive and harmful sites while also providing protection for their relatively rare encounters with Web-borne malware.

Web 2.0, however, has changed everything. Although they provide many attractive features to enhance both personal and business-oriented communication, Web 2.0 technologies complicate matters considerably from a security perspective.

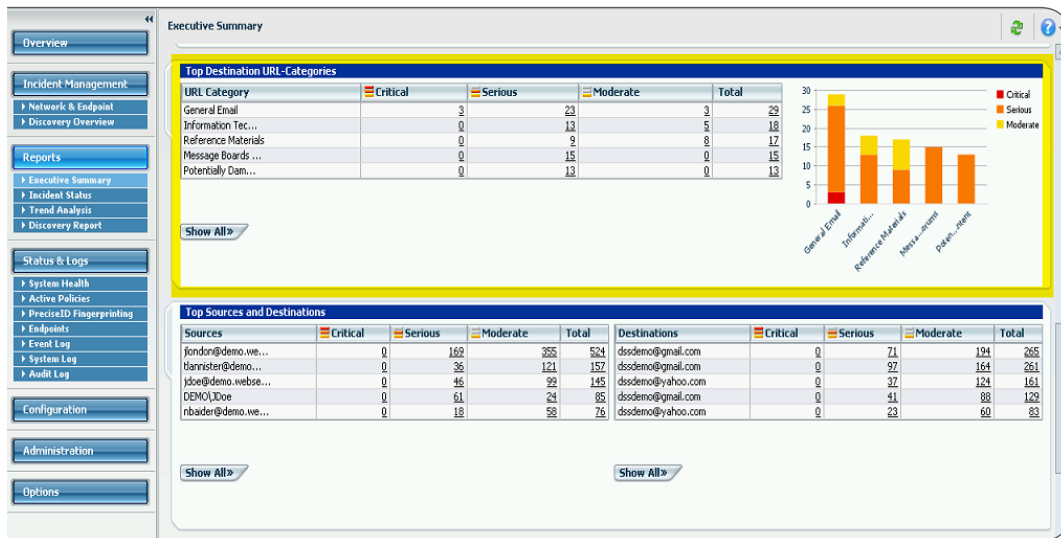
- Web 2.0 sites are far more complex and expansive, often involving millions of pages of highly diverse material;
- Web 2.0 content is highly dynamic, often involving real-time execution of code and/or the compilation of material sourced from any number of other sites; and,
- The widespread use of scripts and other forms of active code makes it exceedingly easy for even legitimate sites to become compromised.

As a result, adequately addressing Web security now requires traditional technologies that rely on prior identification and classification of sites, content, and associated threats be supplemented with real-time content analysis, categorization, and security scanning capabilities.

Organizations should not stop there though. Ideally, CIOs should also consider the need for their Web security solutions to incorporate essential data security capabilities. Indeed, the importance of Web traffic as a vehicle for either the inadvertent or malicious loss of confidential data should not be underestimated. Just consider these points:

- Another significant characteristic of Web 2.0 technologies is that they facilitate the distribution of user-generated content. This includes the ability to readily post not just personnel data but business-oriented information as well.
- Although email has been the weaker link when it comes to data security – at least in terms of the quantity of data loss incidents historically attributed to it – there have been no substantial changes to how this communications channel is being used. In contrast, Web 2.0 has profoundly changed both the way and extent we use the Web, in turn precipitating a major, step-function increase in the potential for data loss via the Web channel.
- Somewhat ironically, this potential may even be magnified by the consumerization of IT and the steady adoption of Web 2.0 and closely related software-as-a-service (SaaS) offerings to support legitimate business needs. These use cases effectively validate the outbound flow of data over the Web and, in the absence of compensating guidance or controls, can easily lead to users believing it's acceptable to employ other data export/sharing services, particularly if they help them get their jobs done (e.g., Google Docs, Twitter, and LinkedIn).
- Finally, it's not just a matter of user-generated content and a growing population of Web-borne malware designed to steal sensitive data. With the introduction of innovative sites and tools like Dropbox (www.getdropbox.com), data loss over the Web channel is also rising based on the fact that Web protocols and services are steadily displacing other methods historically used for data transfer, such as FTP and to some extent even email (e.g., when the size of an attachment exceeds enforced limits).

The impact of these changes, simply put, is that the need to protect confidential data has effectively become another integral element of the Web security challenge confronting today's businesses.



Get Context for Data Loss with URL Destination Awareness

An Integrated Problem Deserves an Integrated Solution

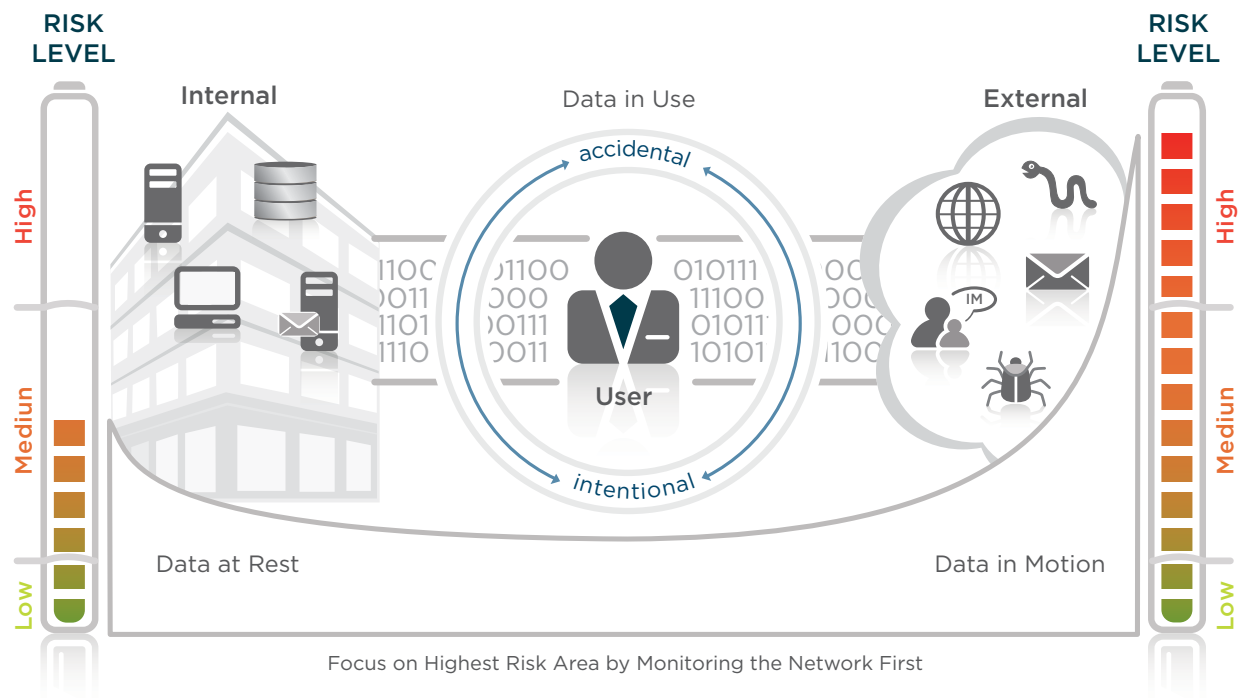
In addition to offering an extensive collection of Web security products capable of accounting for the dynamic nature of Web 2.0 content, Websense also provides a market-leading DLP solution, the Websense Data Security Suite. Associated capabilities can be implemented in a standalone manner, or, more appropriately for Websense customers, as an integrated extension of your existing Web security infrastructure. Indeed, whether it's Websense Web Filter, Websense Web Security, or Websense Web Security Gateway, your organization can leverage the same solution already being used to control who goes where on the Web to also manage what goes where. This way:

- Protection can be achieved for both users and data with an integrated solution;
- Comprehensive acceptable use policies (AUPs) that govern the exchange of data via the Web can be set up and enforced with simple yet powerful policy controls; and,
- The productivity, liability, and security risks due to inbound content associated with visiting Web sites can efficiently and effectively be mitigated at the same time as those due to the unauthorized exposure of confidential data (e.g., loss of competitive advantage and noncompliance with applicable regulations).

The capacity to integrate with the complete portfolio of Websense Web security products is just one strength of this solution. Other advantages include enabling organizations to take a practical approach to data security, a comprehensive and unrivaled set of functional capabilities, and the extensive value it delivers.

Enabling a Practical Approach to Addressing Data Loss

Many IT organizations are intimidated by the prospect of purchasing and implementing a DLP solution. This stems from a widely held belief that a DLP initiative is a complicated undertaking, one that can only get off the ground by first defining exactly what constitutes confidential data and then conducting an exhaustive search to discover every location where it resides. This is a misconception however, and, at least for the Websense solution, need not be the case. It makes just as much sense - if not more - to instead begin by monitoring the organization's network to gain visibility into the actual flow of sensitive information and then take corrective action.



Indeed, the benefits of such an approach include the following:

- Organizations are able to focus on the greatest risk first. Both stored data and data in use on end-user machines represent the potential for a loss incident. In contrast, when confidential data is actually detected exiting the network - for example, in an email message, web-application transaction, or blog entry - risk has become reality.
- Effort and expenses can be reduced. Organizations need not waste time having lengthy debates on what might be happening and which bits and pieces of information should be protected. By first monitoring their networks, hard evidence of what's actually happening can be obtained, in turn facilitating and streamlining data identification, classification, and policy development processes.
- A quick win can be scored. Instead of taking months to achieve a meaningful result, reports that demonstrate the real extent of an organization's data loss problem can be generated in hours or days. Moreover, losses can even begin to be curtailed in the same timeframe. Targeted administrative measures alone, such as clarifying acceptable use policies and issuing

notifications or warnings, will typically reduce data loss occurrences by 50% or more. The credibility thus gained should, at a minimum, pave the way for IT to pursue the remainder of its DLP agenda.

These benefits are why the data security integration with Web Filter and our other Web security products is focused first and foremost on enabling our customers to monitor for and optionally protect against confidential data exiting their networks. This way it only takes a small investment to realize a rather substantial return.



Efficiently Measure the Extent of Your Data Loss Problem

Another strength of the solution, though, is that these core capabilities are themselves just a subset of the complete Websense Data Security Suite. What this means is that if and when your organization decides to, it can easily extend its DLP implementation to also address “data at rest” (i.e., wherever it is stored) and “data in use” (whenever it is being processed on an end-user’s machine).

The Websense Data Security Suite

The Websense Data Security Suite is comprised of four, fully integrated modules that can be deployed based on customer need:

Websense Data Monitor	Monitors the network for who is using what data, and how
Websense Data Protect	Protects data in network transmissions with policy-based controls that map to business processes.
Websense Data Endpoint	Extends monitoring and enforcement to the endpoint to secure user activity
Websense Data Discover	Discovers and classifies data distributed throughout the enterprise

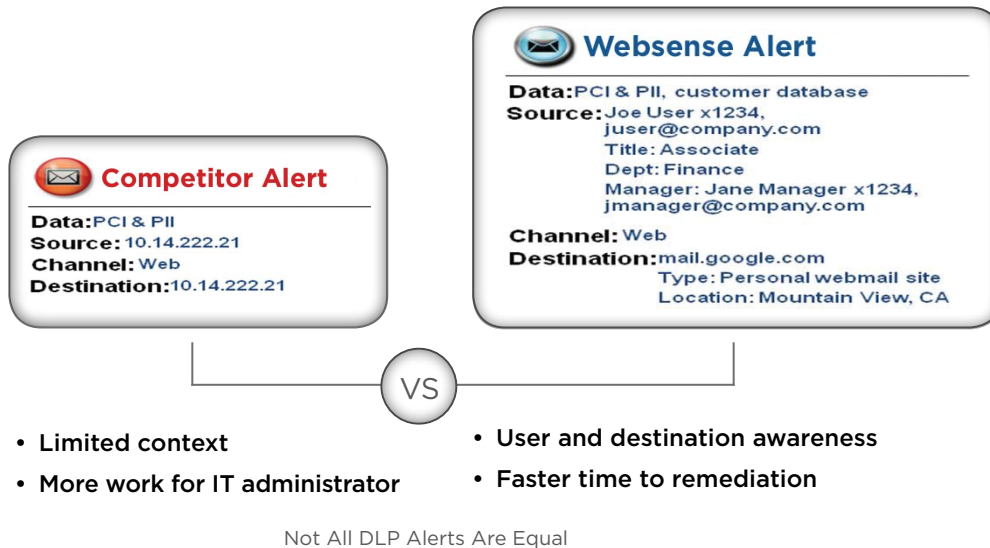
Providing Unmatched Capabilities

Drilling down a level brings us to the specific features and functions associated with the integrated data security capabilities. Market-leading across the board, these are the elements that enable Websense customers to efficiently and effectively gain insight into and have complete control over the confidential data flowing across their networks.

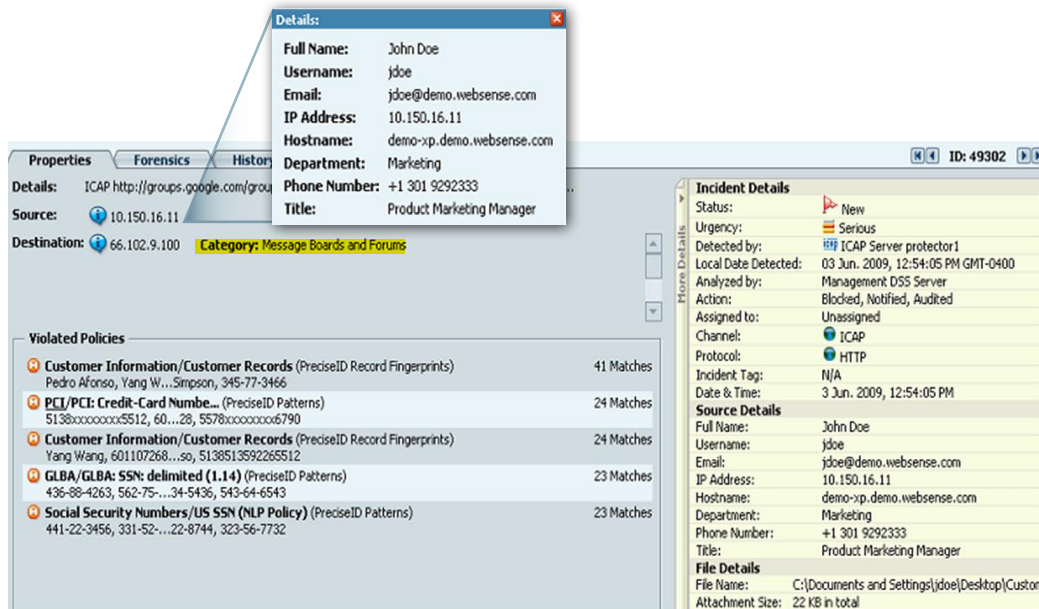
Comprehensive Visibility

Competing solutions shed light only on what pieces of data are being lost and how the loss is occurring – that is, via which specific protocol or communication mechanism. This minimal amount of context is problematic because it often leads to false positives and inhibits policy decisions and accurate reporting. In contrast, the Websense solution also provides details about who specifically is sending the data, and, via its real-time destination awareness feature, where specifically that data is being sent. Furthermore, these insights can be obtained for web (HTTP), secure web (HTTPS), and dynamic Web 2.0 sessions.

Consider a typical data loss alert where only IP addresses and application channel are presented, leaving the burden on the system operator to determine whom to notify and which specific destinations are receiving the subject data.



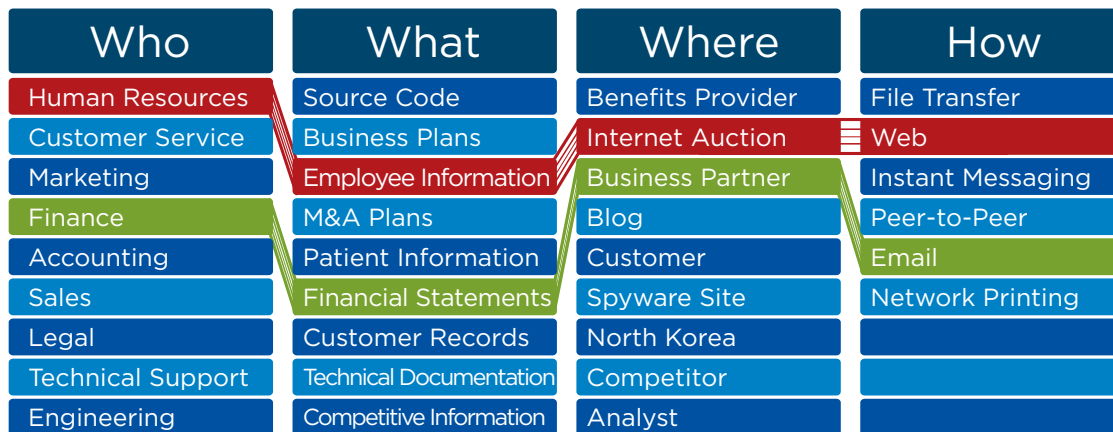
In comparison, the Websense DLP capabilities provide greater visibility and considerably reduce the burden placed on your operations staff not only by making it clear that PCI and PII data have been lost via a Web channel, but also by revealing the identity information of the person responsible for the offending traffic and where specifically it is heading.



Actionable Incident Management with URL and Destination Awareness

Powerful Policy Framework

The same elements used to gain visibility into the flow of confidential data – who, what, where, and how – are also the basis for an advanced policy framework used to gain control over it. With this framework, organizations can create data policies that intelligently and accurately map to their specific business processes. In this way, legitimate business transactions can smoothly and granularly be enabled at the same time that unsanctioned activities are subjected to a range of potential enforcement actions such as blocking, quarantining, forced encryption, and notification.



Customers gain granular visibility and control over *who* can send *what* data *where* and *how*.

High Detection Accuracy

The need for accuracy is critical in a DLP solution. Even a small percentage of false positives can mean hundreds of spurious events, each with the potential to disrupt essential business functions and cost a company substantial sums of money, and each requiring the attention of IT operations and/or helpdesk staff. This is why Websense supplements the usual collection of keyword, dictionary, regular expression, file matching, statistical analysis and correlation techniques with its patented PreciseID™ technology, a ground-breaking detection mechanism that also offers natural language processing. The solution also benefits from the Websense ThreatSeeker™ Network, a collection of over 50 million systems that continuously monitors Internet content for emerging threats and automatically provides corresponding updates to all Websense email, Web, and data security products.

Flexible Architecture

As discussed, Websense DLP capabilities can be operated in an integrated manner with any of the Websense Web security products, using either a passby (span port) or inline (proxy, tap) arrangement. Alternately they can also be configured to work with a standard Web proxy or Websense Email Security. Customers benefit as well from the investment protection afforded by the ability to integrate other modules of the Websense Data Security Suite into their DLP implementation as needed, for example, to enable discovery and endpoint monitoring and control.

Robust Management

Centralized management is provided for all lifecycle functions. Policy configuration is facilitated by built-in wizards and an extensive collection of Websense-maintained templates covering the full array of industry regulations (e.g., PCI, GLBA, HIPAA, and SOX) and types of sensitive information, such as PII (personally identifiable information), PHI (personal healthcare information), and PFI (personal financial information). Administrators can easily analyze, track, and remediate policy violations while also generating and distributing executive-level and detailed reports to accurately show the state of their DLP initiative and related compliance efforts.

Delivering Extensive Value

Web 2.0 has forever changed the scope of what constitutes Web security: providing protection for confidential data riding within your Web traffic is now part of the challenge as well. For customers of our Web security products, however, meeting this challenge doesn't have to be a complicated and costly endeavor. All you need to do is implement the integrated data security capabilities that Websense also has to offer.

Among its many benefits, taking this approach will allow you to:

- Enable legitimate business activities involving Web 2.0 technologies while securing users and data by detecting and protecting against broken business processes, inadvertent errors, and data-stealing malware.
- Achieve greater operational efficiency, particularly compared to alternative solutions which fail to provide visibility into the who and where dimensions of a potential data loss event.

- Manage and report not just on where users are going on the Web – which corresponds to the half of the solution you already have – but on where your data is going as well, including for compliance purposes.
- Trust the quality and effectiveness of the solution given that it's from Websense, a company with an unmatched heritage and track record of excellence in the content security market.

Not only that, but helping to solve what is rapidly becoming a major problem for most organizations – providing comprehensive visibility and reliable control over where data is going – will solidly reinforce the relevancy and credibility of the Web security team by clearly demonstrating its value “to the business.”

So what are you waiting for?