



Websense[®] Essential Information Protection[™] Technical White Paper

How Technology Unification
Delivers the Best Security with the
Lowest Total Cost of Ownership

Contents

- Executive Summary4
- Balancing Business Opportunity With Security Risks5
- The Websense Approach: Essential Information Protection™6
- Websense Integrated Solutions: ESSENTIAL INFORMATION PROTECTION in Action.....8
- Integrated Web and Data Security10
 - Business Issue 11
 - Integration Overview..... 11
 - Use Cases..... 12
 - Differentiation 13
 - User and destination awareness 13
 - Native visibility into encrypted traffic 13
 - Simple yet powerful management..... 13
 - Simplified incident reporting 14
 - Lower total cost of ownership (TCO). 14
 - Integration as part of Essential Information Protection 14
 - Benefits..... 14
- Integrated Email and Data Security..... 15
 - Business Issue 15
 - Integration Overview..... 15
 - Use Cases..... 16
 - Differentiation 17
 - Email security with built-in data security dictionaries 17
 - Email security integration with full data security solution..... 17
 - Purpose-built integration between email and data security solutions..... 18
 - Data security policy-based encryption through email Security-as-a-Service 18
 - Simplified yet powerful policy management 18
 - Simplified email confidentiality enforcement..... 19
 - Benefits..... 19
- Integrated Data Security with Endpoint Application Controls 20
 - Business Issue 20
 - Integration Overview..... 20
 - Use Cases..... 20
 - Differentiation 21

- End-user policy profiles 21
- Content-aware endpoint device visibility 21
- Endpoint operation visibility 22
- Endpoint application visibility 22
- Application selection through predefined groups 22
- Integrated reporting with network DLP..... 22
- Integrated reporting with network discovery scans 23
- Simplified yet powerful policy management 23
- Lower total cost of ownership..... 23
- Integration as part of Essential Information Protection 24
- Benefits 24
- Integrated Web and Email Security 25
 - Business Issue 25
 - Integration Overview 25
 - Use Cases..... 25
 - Differentiation 26
 - Built-in Web security intelligence 26
 - Simple yet powerful management..... 26
 - Single view for hosted security customers..... 26
 - Benefits 27
- Integrated Threat Analysis Across Web, Email, and Data Security 28
 - Business Issue 28
 - Integration Overview 28
 - Use Cases..... 29
 - Differentiation 30
 - Prompt, highly efficient threat-discovery methods..... 30
 - Practical, effective threat identification methodology 30
 - Accurate classification of data 30
 - Adaptive visibility and realignment for effective threat management..... 30
 - Benefits 31
- Conclusion 32
 - Integrated Solutions Address Today’s Security Threats 32
 - Convergence demands integration 32
 - Diversity demands integration 32
 - Compliance demands integration 32
 - The Business Case for Essential Information Protection..... 32

Executive Summary

Today, successful organizations depend upon their ability to collaborate, communicate, and share information online. Established tools, such as email and the Web, are now more important than ever before, while emerging Web 2.0 applications, blogs, and social networking sites allow organizations to work in new, more efficient, and innovative ways.

Yet these technologies also expose businesses and other organizations to a variety of new and emerging information security risks. Malware and malicious Web sites pose external threats to confidential data, and the inappropriate use or distribution of such data creates equally pressing internal threats. Existing point security solutions, such as anti-malware or antispam tools, address some of these threats, yet they fail to detect many others. While a growing number of integrated content security suites attempt to fill the need for more advanced security solutions, these offerings often create more problems than they solve — increasing complexity, costs, and even creating redundancy in some areas yet leaving gaps in coverage in others.

In order to succeed in this new, more connected threat environment, business and risk managers require a unified solution architecture that allows them to offer their users the ability to access applications and information where and when it is required, without exposing the organization to security threats, data loss, and compliance risks.

Websense® achieves this goal with its adaptable solution architecture of Web security, email security, and data loss prevention — delivering a unified content security platform called Essential Information Protection™. Essential Information Protection empowers users, enabling communication and collaboration across new and legacy applications. It protects users and sensitive data against internal and external threats, and it allows users to work productively online without exposing an organization to security, legal, or other liability risks.

Essential Information Protection is designed to help organizations make the most of their IT security investments. Websense accomplishes this by adapting to process workflows, eliminating the gaps that traditional point solutions often leave, and leveraging a unified content analysis across its unified Web, email, and data security portfolio. As a result, Websense solutions work effectively as modular components, yet they also act as a unified and powerful content security solution that enables organizations to increase security effectiveness while decreasing total cost of ownership (TCO). Finally, Websense offers a unified set of policy management and reporting tools that allow businesses and other organizations to work more efficiently and productively, and more easily and accurately report on information security.

Many companies claim to offer content security suites that accomplish the same objectives. Yet this is a market where point products still play a very large role and where many “integrated” solutions still take a narrow, silo-oriented approach to information security. A recent Forrester Research study, for example, concluded that the content security market remains a work in progress where “only a small number of vendors reported adequate suite functionality.” According to Forrester, among a handful of top-tier content security offerings, “Websense is the only vendor that is clearly in the Leader category for content security suites.”ⁱ

This white paper will explain why Websense Essential Information Protection offers the most compelling information security solution available on the market today. We will illustrate how Websense, through unified content analysis, solution architecture, and platform, uniquely addresses five, real-world security scenarios.

Balancing Business Opportunity With Security Risks

In today's business environment the ability to share information represents a vital competitive advantage. Email, instant messaging, and a host of other Internet-enabled tools facilitate the free flow of information between co-workers, customers, and business partners. At the same time, a new generation of Web 2.0 applications, including blogs, wikis, and social networking sites, employ user-generated content and dynamic updates to distribute information more efficiently than ever before.

Yet these new technologies also introduce a new class of security threats. Many of these emerging threats can be difficult to distinguish from legitimate business opportunities, especially when they move so quickly and migrate along channels that evade traditional security safeguards. Threats emerge, evolve, and multiply on a daily basis, combining traditional attack vectors with completely new – and often extremely dangerous – Web 2.0 threats.

Web 2.0: Same Risks, with a Twist

- **Data loss:** Increased risk due to dynamic, user-generated content posted to legitimate Web sites.
- **Blended security threats:** Attackers use legacy business applications, such as email, to trick users into clicking URLs that lead to malicious Web 2.0 applications, thus evading point security solutions.

Point security solutions often fail to recognize these new risks, much less to manage them effectively, given the multiple policy, detection engine, and reporting frameworks. They assume that threats only manifest themselves in a single channel; as a result, they are unable to correlate threats across multiple applications.

A unified content security solution, by comparison, does a better job of managing blended Web, email, and data security risks. These solutions offer the ability to call upon a robust, far-reaching set of threat-assessment and intelligence tools, leaving businesses exposed to fast-moving, rapidly evolving security threats. A unified content security solution allows companies to manage risk without hindering legitimate business operations. It understands the role that context plays in the security decision-making process; it reaches across multiple communication channels, content categories, and usage scenarios to recognize potential security threats. It addresses both external and internal security threats, preventing the loss or misuse of proprietary business data just as effectively as it stops traditional malware or perimeter-security attacks.

Just as important, such a solution provides the management, policy definition, and reporting tools that businesses rely upon to maintain control and to maximize the returns on their IT security investments. Successful businesses always attempt to select solutions that maximize return on investment (ROI) while minimizing their TCO. In the current economic climate, these considerations are more important than ever before.

The Websense Approach: Essential Information Protection

Websense defines its unified content security as Essential Information Protection. It is possible to summarize Essential Information Protection in terms of several key principles, which drive the technical capabilities built into the company's Web, email, and data security products, as well as its underlying threat-assessment and intelligence infrastructure:

1. **Empower users** — Enable communication, collaboration, and information exchange over the Web, including Web 2.0, email, and other business applications and communications platforms.
2. **Keep users safe** — Provide real-time access to Web and email content combined with real-time, dynamic blocking of malware and malicious content sources.
3. **Enforce acceptable use policies** — Ensure that employees can go where they need to go online, while keeping them productive and limiting company liability.
4. **Enforce data security policies** — Protect confidential business data and guarantee regulatory compliance across common business applications and communication channels.
5. **Deliver accuracy and context through integration** — Provide comprehensive security that combines Web, email, and data loss prevention in unified policy architecture.

Above all, Essential Information Protection is designed to **empower** users while keeping them safe, using real-time protection combined with highly accurate threat-detection and data identification techniques. The key difference between Websense and other content security providers is unification on three fronts:

1. **Unified Content Analysis** — Websense ThreatSeeker® Network integrates threat feeds and classification intelligence for Web security, email security, and data loss prevention, delivering the best protection for blended and emerging threats.
2. **Unified Solution** — Combined architecture for Web security, email security, and data loss prevention enable greater control and unified management to reduce complexity, and providing increased coverage.
3. **Unified Platform** — On premise and cloud-based delivery platforms are integrated to support hybrid deployments, consolidation, and reduced TCO.

Websense Web, email, and data security solutions employ a fundamentally unique approach to information security. Its solutions are designed to offer superior functionality on a stand-alone basis, while also providing important advantages for companies that integrate various solution combinations. In either case, Websense solutions are designed to achieve three strategic objectives:

- 1. Adapt to existing business workflows** — thus eliminating the opportunity costs characteristic of traditional point-security products while still delivering superior blended-threat management capabilities.
- 2. Increase security effectiveness** — by eliminating gaps in point security solutions with a seamless, integrated offering that leverages a common threat-intelligence infrastructure across Web, email, and data channels.
- 3. Provide flexibility and lower TCO** — that combines a modular-solution architecture with powerful integration capabilities, a unified policy architecture, and multiple deployment options, including Security-as-a-Service (SaaS), appliance, and software-based implementations.

Websense Integrated Solutions: Essential Information Protection in Action

Let's take to a closer look at precisely how Essential Information Protection delivers information security in a number of real-world situations. In the next section, we will examine these five key areas where Websense Web, email, and data security solutions combine to offer important integration advantages:

1. Web and data security
2. Email and data security
3. Endpoint application control and data security
4. Web and email security
5. Threat analysis and protection across Web and email security

Integration Areas	Specific Integration Areas	Benefits
Data and Web	<ul style="list-style-type: none"> • Data security policy definition with built-in URL categories • Data security incident management with user and destination awareness 	<ul style="list-style-type: none"> • Allow data upload to certain types of Web sites while restricting confidential data transfer to risky Web sites • Efficiently respond to data security incidents using knowledge of high-risk Web sites and accurate user identification
Data and Email	<ul style="list-style-type: none"> • Email security policy definition with offload to data security solution for full analysis • Email security policy definition with basic, built-in data security policies • Email security enforcement using hosted encryption service 	<ul style="list-style-type: none"> • Facilitate communication by allowing confidential emails to authorized users while preventing data loss. • Protect users by blocking user access via emails, to Web sites, which may have been compromised, or otherwise hosting malicious content from URLs received in emails.
Data and Application	<ul style="list-style-type: none"> • Visibility and control over copy, paste, and print across endpoint applications and peripheral devices, with content awareness 	<ul style="list-style-type: none"> • Allow data copy to some external devices as long as data isn't from business-confidential applications

Integration Areas	Specific Integration Areas	Benefits
Web and Email	<ul style="list-style-type: none"> • Email security policy definition with built-in Web link reputation • Hosted security solutions with integrated management and reporting 	<ul style="list-style-type: none"> • Protect users by blocking user access to suspicious Web sites from URLs received in emails • Lower TCO through simplified management of two key business security areas :Web and email
Threat Intelligence with Web , Email, Data Security	<ul style="list-style-type: none"> • Threat Intelligence from proven process of Discover → Identify→ Classify → Adapt – all applied to Web, email, and data security solutions 	<ul style="list-style-type: none"> • Prepare for common and emerging threats against business systems. • Protect security investments by using current solutions for years to come, since threat intelligence will continue to evolve.

Integrated Web and Data Security

Business Issue

Your company probably knows where its **employees** are going on the Web. But does your company know where its **data** is going?

Many companies today use Web security solutions to enforce acceptable use policies and to track employee Web site usage. In spite of growing business confidentiality and compliance risks, however, organizations often lack meaningful control over the use and misuse of confidential data. As new Web 2.0 applications such as wikis, blogs, and social networking sites drive the “consumerization” of enterprise information technology, security risks involving confidential or regulated business data will only increase.



Figure 1: The Web is the New Application Platform

As the Internet continues its exponential growth as a universal platform for business communication, collaboration, and information exchange, the risk of losing confidential data over Web and other business communication channels like email and FTP will also grow dramatically. Although many rogue Web sites are known to host malware, legitimate Web sites are also a source of concern: According to one study, 79 percent of data breaches are attributed to attacks involving Web applications.ⁱⁱ

How can organizations protect confidential data against such attacks without inhibiting legitimate business activities? First, they must **identify** key business data sources to comply with external regulations and with internal data security policies. Then they must **monitor** the business processes that pose the greatest risk to data security and **protect** this data against unauthorized access or use. Websense integrated Web and data security solutions are designed to achieve all three of these objectives.

Integration Overview

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. — IDCⁱⁱⁱ

Websense Web and data security solutions are part of the Websense Essential Information Protection platform. Websense Web security solutions^{iv} protect end-users against accessing inappropriate Web sites or downloading malicious content via the Web and other network protocols. Websense data security solutions^v also protect end-users against losing data via the Web or other network protocols. These two product groups are integrated through the use of:

- A data security policy framework that leverages real-time Web intelligence.
- Real-time Web destination information lookup capabilities to classify and prioritize data loss violations.
- Real-time user information lookup capabilities to accurately report the source of data loss violations.

In addition, data security policy definitions offer highly granular information about where data is going. Administrators can define, monitor, and control access to specific categories of Web sites (e.g., “Message Boards and Forums”). This granular control enables management of the Web as a business tool rather than as an IT security concern. The underlying Web intelligence is delivered via a hosted service that incorporates feeds from the Threat Seeker Network, the threat research and intelligence component of the Essential Information Protection platform.

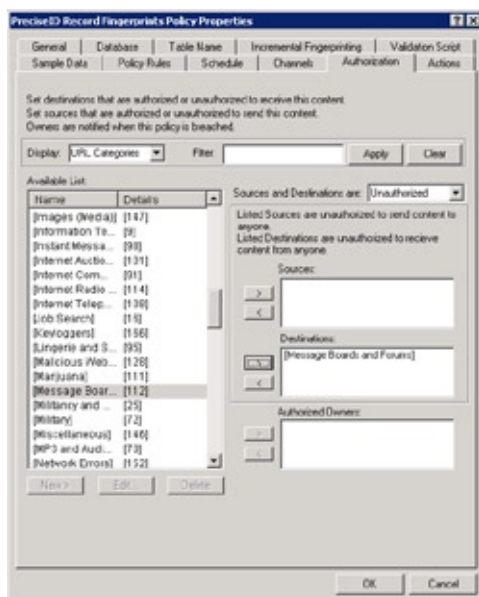


Figure 2: Data Security Policy Definition Leverages Hosted Web Intelligence

For organizations that deploy combined Websense Web security and data security solutions, the Websense Linking Service provides real-time insights into who is sending business data and where the data is going. This includes the ability to map, in real time, source IP addresses to user names and other contact details, including the user's role, manager, and more. In addition, real-time destination IP address lookups reveal the destination Web URL and site category through the use of Websense ThreatSeeker Network intelligence capabilities.

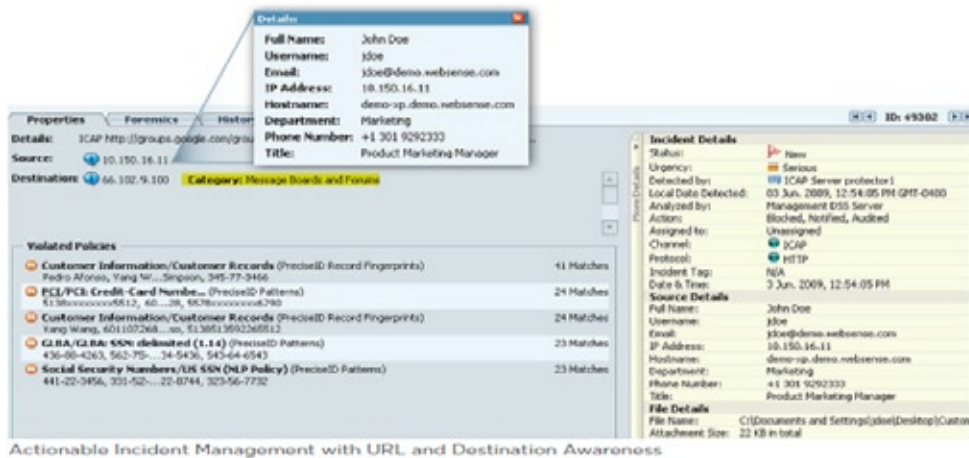


Figure 3: Actionable Incident Management with User and Destination Awareness

Use Cases

Malicious code and malicious end-user intent are not the only root causes of data loss. In many cases, a legitimate desire to improve efficiency and cost-effectiveness drive activities that lead inadvertently to the loss of confidential data. Consider three scenarios in which well-meaning employees place business data at risk:

1. The use of Web 2.0 applications to meet a business need that a company's existing IT services cannot meet
2. Efforts to reduce PR and marketing costs by launching promotions and marketing campaigns using free Web 2.0 services
3. Attempts to bypass current IT infrastructure limitations by using Web 2.0 services

An actual case illustrates the first example: A hospital where doctors and nurses required the ability to share patient data easily, using any computer. The hospital's IT department had not yet implemented a solution capable of performing this task; as a result, the staff turned to Google Docs to share patient evaluations, histories, and diagnosis information. This activity created obvious regulatory compliance risks, since both government regulations (HIPAA) and third-party industry standards (The Joint Commission) restrict the uncontrolled distribution of patient data over open networks. Even if this data had been shared using the "secure" version of Google Docs (<https://docs.google.com>), the practice would have created serious legal and business risks.

The second example is also increasingly common, as companies adapt Web 2.0 services such as YouTube and Facebook as low-cost ways to reach large numbers of potential customers. Many public relations firms, for example, now use Web 2.0 services to ensure that the press picks up their news releases. The media outlets, in turn, use Web 2.0 services, such as blogs and Twitter feeds to deliver news to their readers. While fast and cost-effective, these distribution channels increase the risk that confidential data, such as product roadmaps or company acquisition news, could leak out prematurely.

The third set of Web 2.0 data loss risks involves cases where existing IT resources are not capable of meeting employee needs. As more users work with video, graphics, presentations, and other very large files, they may encounter problems with storage quotas on a company's file servers, FTP servers, or email systems. Out of frustration and necessity, users turn to online storage sites (e.g., www.getdropbox.com) or email services for large file attachments (e.g., www.yousendit.com). While these services meet legitimate user needs, companies that lack visibility into these services or control over the data being stored face serious data security risks.

Differentiation

Not all Web and data security solutions are alike, yet most of them are blind to significant data loss risks involving Web applications. Websense sheds light on these areas with a number of capabilities — some built into the individual solutions, others unique to the integration between the two.

User and destination awareness. Most vendors limit user-level reporting data to a source IP address. Others provide more detailed user contact information after the fact, mapping IP addresses with LDAP database lookups. When companies use DHCP to provision IP addresses dynamically or when multiple users share access to the same systems, these after-the-fact lookups simply don't work.

Websense Web and data security solutions employ real-time IP address lookups from Windows domain controllers and leverage a proprietary user service — an approach that provides timely, accurate, and detailed user information. Both solutions also provide real-time lookups of Web site categories — a core competency for Websense, which employs both automated tools and manual research techniques to track millions of unique Web sites. Organizations that deploy combined Websense Web and data security solutions reap major benefits from these integrated capabilities.

Native visibility into encrypted traffic. Many Web 2.0 services use SSL and HTTPS to provide point-to-point data encryption. While these protocols address the risk of hackers sniffing traffic on public networks, they do not prevent users from transporting confidential data to remote locations beyond a company's control. Websense Web security solutions include a built-in SSL proxy which can pass decrypted traffic to the data security solution for additional inspection. This allows the business to monitor usage of secure document storage services such as Google Docs and GetDropBox. With Websense, the business can enable access to these resources for personal files while preventing confidential business data from being uploaded.

Simple yet powerful management. Websense data security solutions offer a policy wizard that allows administrators to select relevant regions and industries, automatically generating a set of rules that specify what types of data to identify and monitor. This solution also allows administrators to specify where to apply these solutions based on Web destination categories, while still allowing predefined exceptions to the rules (such as the Google Docs example cited above).

Simplified incident reporting. Websense Web and data security solutions support the ability to generate reports on Web and data security events and to distribute these reports automatically to key decision makers. When both solutions are deployed together, data security violation reports also display

detailed user contact and Web destination information, reducing the time required to identify individual violators and take remedial action. Without these capabilities, administrators must manually review domain controller logs to look up IP addresses, map them to timestamps, and retrieve accurate user information — a huge burden for organizations that may have to investigate hundreds of violations at any given time.

Lower total cost of ownership (TCO). Streamlined security policy definition and incident management processes save time and reduce demand on a company's IT staff resources. In addition, the ability to track Web destinations, to detect the transfer of regulated and business-confidential data, and to retrieve detailed user information allow companies to implement more business-aware security policies, reduce false positives, and cut the number of potential violations for administrators to investigate. Finally, the use of a Web security solution with a built-in SSL proxy eliminates the cost and complexity of deploying and managing a third-party solution to gain visibility into encrypted Web traffic.

Integration as part of Essential Information Protection. Web and data security integration is just one example of a strategy that Websense implements across all of its products and research disciplines. These integrated capabilities give companies improved visibility and greater control over business information as the information traverses various applications.

Benefits

An integrated Websense Web and data security solution provides the accuracy and the context awareness required to achieve higher, faster ROI. The Websense solutions combine industry-leading DLP technology with a practical, business-oriented policy framework that simplifies deployment, management, and reporting, while also delivering lower TCO. This information-centered security framework empowers organizations to leverage Internet communications channels and Web 2.0 applications without increasing their exposure to data security risks. And it extends these capabilities to every part of an enterprise IT infrastructure, including core networks, branch offices, remote or mobile workers, and cloud-based computing environments.

Integration Area: Web and data security. Blended Threat: Data loss via Web 2.0 channels.

Integration Benefits:

- Access accurate risk and compliance reporting data combined with granular policy controls, including rules based on predefined Web site categories.
- Work with simple yet powerful incident management tools that deliver real-time user and Web destination information.

Integrated Email and Data Security

Business Issue

Email remains a mission-critical business tool. As a result, companies now rely heavily upon point security solutions, such as antispam and antivirus protection, to preserve the integrity and availability of their email service. Yet inbound threats are not the only problems: Email now accounts for a significant number of data-breach incidents.^{vi} As a result, the ability to monitor email for confidential business data is now an essential part of any reasonable data security strategy.

Integration Overview

Websense Email Security and Websense Hosted Email Security solutions use built-in dictionaries to detect keywords and other data types based on industry regulations (such as PCI, state privacy laws, etc.), business-confidential information (e.g., finance or legal terminology), and appropriate-use guidelines (e.g., prohibitions on adult content or drug references). Both solutions' detection capabilities include true file-type identification, content extraction from attachments, multilanguage dictionary support, regulatory compliance templates, and a regular expression engine — intelligence ported from Websense market-leading data loss prevention solutions.



Figure 4: Email Security With Built-In DLP Policies

In addition to native DLP built into Websense Email Security, these solutions are also designed to route email to Websense data security via a purpose-built interface, allowing an integrated solution to inspect selected email and file attachments in even greater detail. The data security solution automatically returns a suggested disposition for the inspected content, and the email security solution then enforces the appropriate policy. The email routing process is optimized for performance and security; by inspecting content “out of band,” the combination of Websense data and email security solutions simplifies the network architecture.

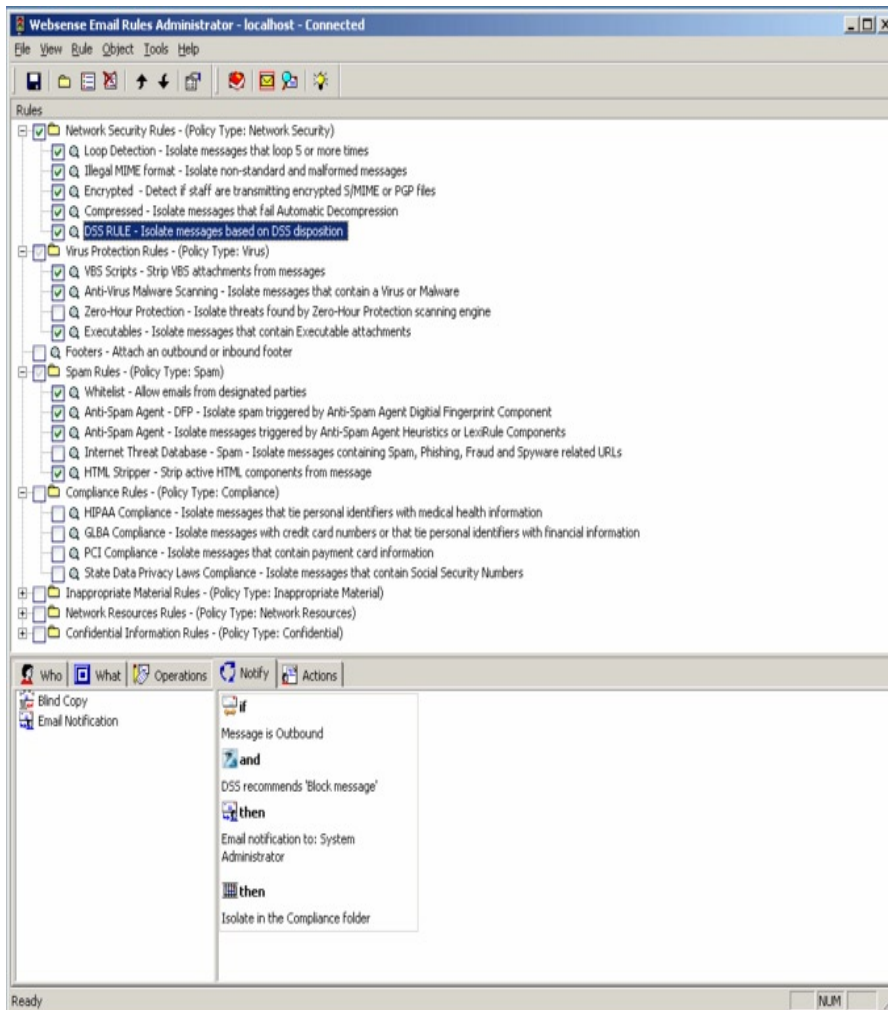


Figure 5: Email Security Purpose-Built Integration With Data Security

Use Cases

Companies often are not aware of data loss risks involving email. They are simply too preoccupied with the day-to-day challenges of maintaining mission-critical service levels and fighting spam. It may be difficult to convince senior managers that there even is a problem without proof — and such proof, in turn, may require a company to invest in a full-blown DLP solution or to pay additional licensing fees for email security software.

Yet when these challenges reduce a company's data loss visibility, they leave it vulnerable to a number of serious risks:

1. Employees may break the law or violate industry guidelines by emailing sensitive data in clear-text format to outside recipients
2. Privileged users could email business-confidential information to unauthorized recipients
3. Privileged users may email business-confidential information in clear-text format to authorized business partners

To illustrate the first example, consider a case where an individual emails his or her own credit card information to an outside recipient in order to make a purchase — a risky and very unwise thing to do. Now consider the business consequences if the same individual emails **several** credit card numbers to an outside recipient, indicating a malicious leak of possible customer credit card data. Such an action would (at the very least) violate PCI Data Security Standards, which prohibit the transmission of credit card data over open, public networks.^{vii}

The second example could involve an employee who emails business-confidential data, such as product roadmaps or technical diagrams, to an unauthorized recipient outside the company. The employee's action violates the company's data security policies, risks exposing sensitive data to competitors, and could ultimately damage the company's vital business interests.

The third type of violation involves a legitimate business activity where it is necessary to share confidential data, such as legal documents, with partners or outside vendors. By sending this information in clear-text format, however, the user exposes it to hackers or malicious insiders who can intercept it and use it in an inappropriate or illegal manner.

Differentiation

Websense offers the ability to protect business data against email-related risks, using a range of capabilities built into its integrated data security and Websense email security solutions.

Email security with built-in data security dictionaries. Organizations gain access to built-in data security capabilities without the additional licensing costs or IT personnel requirements associated with a full enterprise-class DLP solution. This approach eliminates two of the most common objections to data security initiatives, while providing the tools companies require to gain visibility into email-based data security risks.

Email security integration with full data security solution. These built-in data security capabilities offer a tremendous advantage over typical email security solutions. Over time, however, a company may conclude that they are viewing just part of a much larger security issue. When keyword detection techniques uncover a certain number of data loss violations, for example, it is likely that more sophisticated tools, such as email document attachments, may also pose a data loss risk.

Rather than deploying a stand-alone email traffic-monitoring infrastructure, a company can augment its existing Websense Email Security deployment with an additional Websense data security module to perform a deep analysis of its email traffic, based on a set of predefined conditions. The data security solution performs a policy-based content analysis and then sends a disposition (or recommended action) back to the email security solution, which then uses its own infrastructure to perform necessary enforcement such as blocking, quarantining, or routing to a third-party encryption gateway.

Purpose-built integration between email and data security solutions. Very few email security solutions are capable of integrating with a full DLP solution. Even when this level of integration is available, the email security solution almost always uses MTA chaining method to offload data from email to the data security solution over SMTP. This creates a potential point of failure, since the email security solution must serve as a queue for **all** outbound email, whether or not a message requires closer inspection. When the outbound email queue is long or when there are a large number of emails being processed, the data inspection process will also slow down.

Websense email security solutions, by comparison, use a data security agent API to route specific email attachments or content to the data security solution. The result is a more efficient and more fault-tolerant method for inspecting outbound email.

Data security policy-based encryption through email Security-as-a-Service. Encryption by its nature complicates a data security workflow. In addition to adding an extra step to the process, encryption key management and processing tasks require imposing some processing overhead. Integrated Websense data and email security solutions address this problem by taking a policy-based approach to encryption, rather than requiring encryption for every outbound email. The email security solution has visibility into sender and recipient information, along with categories defined either by the system administrator or by the email reputation service. If a user emails content to a partner, for example, this could trigger an offload to data security for further inspection, as described in the previous section. If this data is found to be confidential in nature but necessary for business, a disposition to “encrypt” is returned to email security, which then routes the email to the Websense hosted email security service to perform the encryption.



Figure 6: Data Security Routes to Hosted Email Encryption

Simplified yet powerful policy management. Email security administrators can easily enhance their outbound security policies by selecting predefined templates for confidential data, all within the same familiar management framework. For cases where a full data security policy is in place, these administrators can simply write a rule to offload certain types of email (e.g., based on sender, recipient, or outbound destination) to the data security solution, which is managed by another administrative group, responsible for more detailed data security policies.

Simplified email confidentiality enforcement. It is not necessary to provision additional infrastructure to enforce encryption on confidential emails. An organization's existing email security infrastructure can be leveraged to block, send notification, quarantine, or audit these emails. For encryption, Websense offers a hosted email encryption solution (service) which can be provisioned with a simple check box.

Benefits

Integration enhances both stand-alone email and data security solutions. Email security customers benefit from built-in content inspection capabilities that other vendors offer only for an additional licensing fee — when they offer such capabilities at all. Using this built-in capability to provide visibility into data loss violations, organizations can justify an investment in full DLP capabilities, over email and other network channels, using the Websense® Data Monitor module. In both cases, Websense customers benefit from the ability to leverage an existing email security infrastructure to enforce DLP policies by blocking, quarantining, or encrypting messages. Finally, Websense data security customers benefit from seamless integration with an email Security-as-a-Service encryption solution, eliminating the need to provision a separate, on-premise email encryption gateway.

Integration Area: Email and data security.

Blended Threat: Confidential data in email or email attachments.

Integration Benefits:

- Employ a simple, cost-effective method to gain basic visibility into email-related security threats.
- Implement an intuitive policy framework that employs simple, one-line references to full data security policies.
- Use a quick, low-impact method to provision email as a service.

Integrated Data Security with Endpoint Application Controls

Business Issue

While many data-loss incidents involve the Web or email, these certainly are not the only problems. Factors such as a growing number of mobile or remote workers, the easy availability of high-capacity, highly portable storage peripherals, and easy access to confidential data through client software also represent growing security risks. As a result, it is essential for companies to employ tools that allow them to monitor and control endpoint data use more effectively.

Integration Overview

Websense Data Endpoint solution extends visibility and control over confidential data from Web and email to endpoints. It can determine where confidential data is stored on a given endpoint (through local discovery); who is using it; how it is being used (with what applications); where it is being transferred (USB storage, printer); and what real-time action (e.g., blocking) is required to prevent a data loss violation. This solution also provides unrivaled visibility and control over copy-and-paste operations between client applications. The endpoint agent can enforce data security policies anywhere (e.g., offline, online, or remote connectivity), and is compatible with other endpoint agents. A small-footprint endpoint agent supplies all of these capabilities with minimal overhead.

Use Cases

Most DLP solutions naturally focus on areas such as Web and email in order to identify common sources of data loss risk on enterprise networks. Network-based DLP solutions, however, cannot fully address other scenarios in which emerging IT trends, including increased user mobility and unrestricted access to client software, set the stage for new types of data loss risks. Consider a few examples that illustrate the need for improved visibility into endpoint security:

1. A user copies confidential data from an endpoint business application to an instant messenger client in order to send this data to an outside contact
2. A user in a company's finance department copies data from a spreadsheet into a text file and then copies the text file to a USB storage device
3. An executive who is privy to sensitive customer data and financial information travels frequently. Unfortunately, the executive's laptop is stolen during a business trip

The first example involves a business application used to access intellectual property. An engineer could copy recently created software code from the business application to an instant messaging (IM) application, sending it in real time to an unauthorized recipient. That IM communication may not be seen by a network DLP solution, either because of encryption of the IM protocol or the client may be connected to a public network (working from home or using a public hot spot).

In the second example, an employee has the ability to access and update spreadsheets containing corporate finance information. The employee wants to work on the spreadsheets at home and copies the files to a USB key — an acceptable activity, as long as the employee uses an approved storage key that employs encryption to protect the files. A typical DLP solution handles this situation in one of two ways: either it does not apply endpoint protection (in which case the employee could use a non-standard,

non-encrypted USB key in violation of company policy) or it applies a simplistic security policy that blocks copying to **any** USB device (in which case it prevents a legitimate business activity).

In the third scenario, routine network discovery scans usually miss the traveling executive's laptop, so a detailed and current inventory of the confidential data on this system is rarely available. As a result, when the laptop turns up missing, the corporate risk management team cannot determine the scope of the data breach. The company must spend the time and money required to notify every customer and business partner that their information may have been compromised, in order to comply with GLBA (the Gramm-Leach-Bliley Act) as well as various state privacy or data-breach disclosure laws.

Differentiation

End-user policy profiles. One size does not fit all when it comes to endpoint DLP policies. Finance and legal professionals who work with highly privileged data, for example, need different sets of controls than hourly employees who perform routine data entry tasks. Just as clearly, a globe-trotting executive carrying a laptop full of sensitive business documents requires more scrutiny with respect to data discovery and device control than a marketing professional who works in the office but makes heavy use of instant messaging and collaboration software. In each case, an effective solution requires the ability to customize security policies based on a user's organizational role, job duties, and other factors.

Content-aware endpoint device visibility. Surprisingly, many endpoint DLP solutions still employ a crude, simplistic approach that blocks the ability to copy **any** data to **any** external storage device. This approach is a major obstacle to companies that want to enable the legitimate and productive use of endpoint resources.

Websense extends its deep content-inspection capabilities from the network DLP solution to the endpoint, including capabilities such as file fingerprinting to monitor business-confidential data. End-user profiles combined with content-aware device control policies enable a much wider range of legitimate use cases: If an authorized user wants to copy spreadsheets to a USB key in order to work at

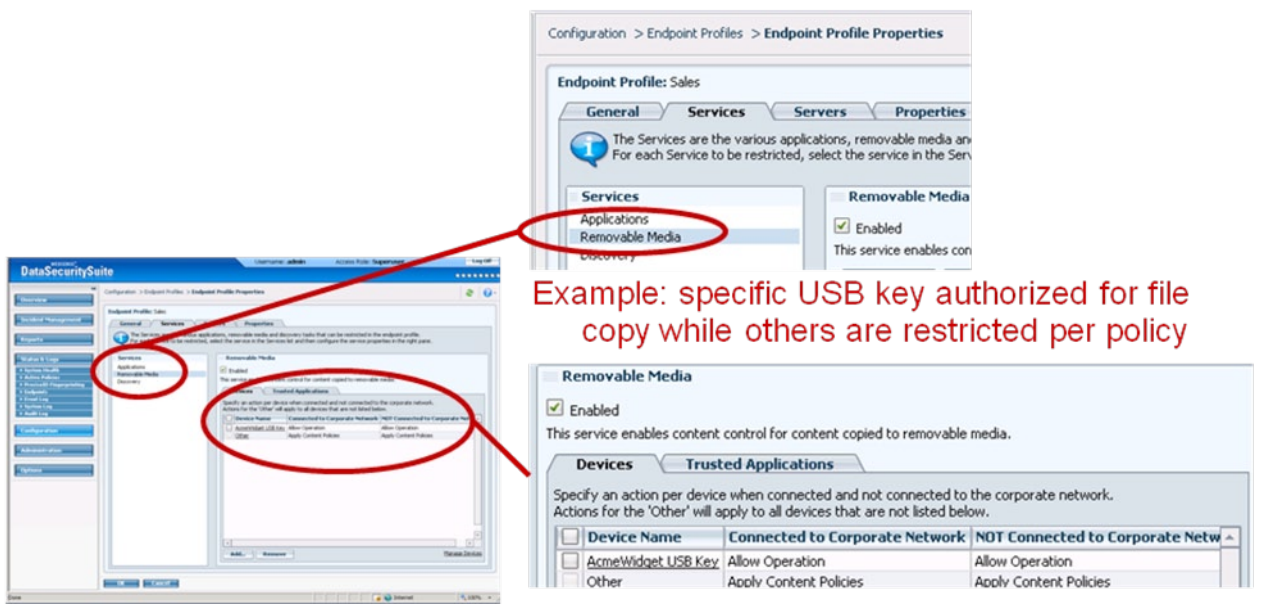


Figure 7: Enable Legitimate Use of USB Devices

home, the DLP policy will recognize this as an acceptable activity — but only if the employee copies the files to a specific company-issued, encrypted USB key, or copies files that do not contain sensitive data.

Endpoint operation visibility. While most endpoint DLP solutions limit their visibility into confidential data being copied to external storage devices, Websense Data Endpoint extends visibility and control to other endpoint operations, including printing, cut-and-paste, file access, and screen captures.

Endpoint application visibility. The endpoint operations, however, are only meaningful when it is possible to define policies based on specific source and destination applications. It should, for example, be possible to recognize an attempt to copy confidential data from an Excel spreadsheet to an IM client as a policy violation.

Websense Data Endpoint provides this level of visibility into endpoint applications, thus giving administrators far more effective control over endpoint operations. Competing solutions tend to rely exclusively upon detection methods, such as regular expressions or fingerprinting . If a local application is known to create or access confidential data (such as new customer records or application source code), then the endpoint security solution can assume that **any** data coming out of the application is confidential.

Application selection through predefined groups. While endpoint application monitoring can be powerful, it can also be cumbersome given the sheer number of applications that may be present on any given endpoint. To simplify this process, Websense supports the ability to define endpoint security policies based on application categories (e.g., file sharing, word processing, or spreadsheets), all through the use of a simple dropdown box.

Integrated reporting with network DLP. The Websense endpoint DLP solution presents incident reports in the same interface as network DLP violations. This allows for simplified incident management, since administrators can sort violations by policy category (e.g., GLBA, HIPAA, business-confidential) or channel (e.g., Web, email, endpoint).

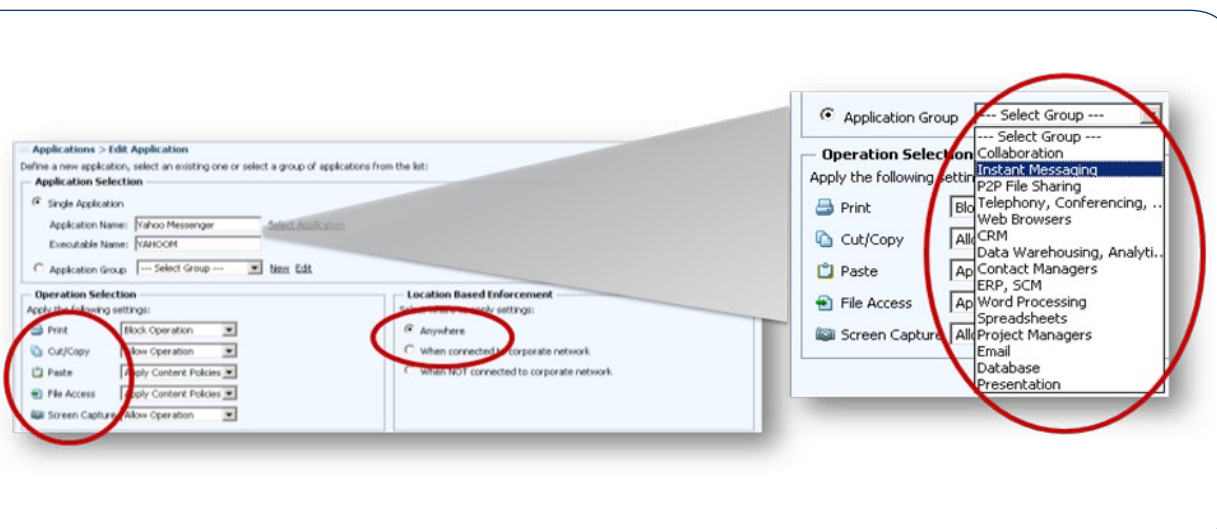


Figure 8: Visibility Into Endpoint Applications and Actions

Integrated reporting with network discovery scans. Most DLP solution suites offer a network discovery component. Those with endpoint DLP capabilities, however, rarely offer integrated discovery reporting tools that combine results from both network and endpoint scans.

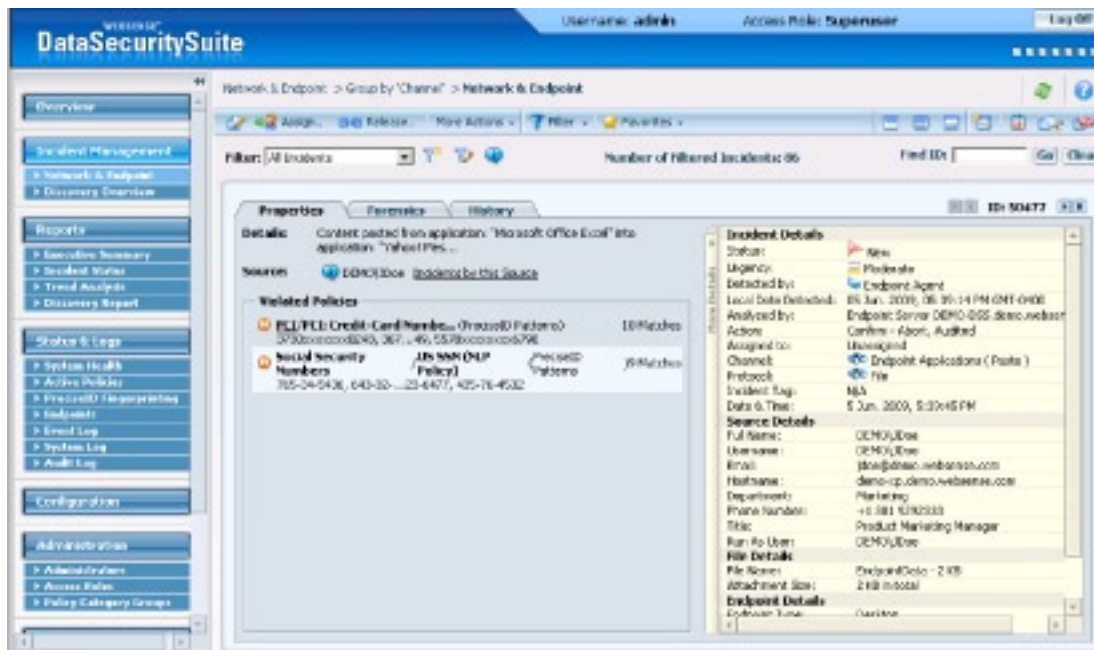


Figure 9: Unified Incident Reporting With Network DLP and Discovery

Websense data security solutions provide dashboards and reports for confidential data discovery scans that combine and correlate network and endpoint discovery results. Websense makes these discovery results available through the same user interface used to monitor network DLP incidents. In cases where mobile users work frequently away from the office or on the road (as illustrated in the prior example), data combined and correlated using both network and endpoint discovery scans offers the best way to mitigate the data loss risks associated with a lost or stolen laptop.

Simplified yet powerful policy management. Websense Data Endpoint DLP policies support customization based on the type of user (e.g., executive versus engineering) and the user’s work location (e.g., offline, online, or remote connectivity). These policy-customization capabilities, combined with application visibility and control over specific endpoint operations, enable a powerful yet easy to use approach to endpoint DLP policy management.

Lower total cost of ownership. Administrators will spend less time dealing with incident-management tasks through the use of a unified interface that displays both network DLP/discovery events as well as endpoint DLP/discovery events. Customized incident reporting and filtering capabilities also simplify and streamline the incident-management process. Superior endpoint application and operation visibility capabilities provide more accurate, highly granular information, allowing investigators to move quickly to determine the precise source and cause of a data leak violation. Finally, Websense Data Endpoint solutions deliver the same integration benefits as the Web and email solutions discussed above, reducing false positives and cutting the number of incidents that require individual attention.

Integration as part of essential information protection. Web and data security integration is but one example of a strategy Websense employs across all of its products and research disciplines. All of these integration capabilities deliver greater visibility into and control over business information as it traverses other business applications.

Benefits

Essential Information Protection protects and enables the legitimate use of business applications. This is true even in an extended enterprise environment where mobile end-users and client software applications may disrupt the ability to control confidential business data. Websense Data Endpoint solution addresses these challenges, adding the content-aware device control, visibility into client applications and peripheral storage devices, and control over cut-and-paste or screen-capture operations that other endpoint DLP solutions fail to provide. The Websense Data Endpoint solution also adds value with its integrated approach to network discovery, allowing organizations to keep accurate, up-to-date inventories of confidential data on end-user systems — essential information when risk managers respond to a data-breach incident.

Integration Area: Data security with application controls.
Blended Threat: Confidential data lost due to the inappropriate use of client software.

Integration Benefits:

- Gain more granular control over data, with visibility into potential data loss risks involving client applications — individually or by application category.
- Address cases where confidential data is contained in an endpoint application but has not yet been fingerprinted.
- Limit risks associated with asset theft by using a combination of network and endpoint discovery scanning to identify and inventory confidential business data.

Integrated Web and Email Security

Business Issue

A new threat associated with email traffic has arisen. In the past, email typically carried malware in the form of attachments. Today, however, over 85 percent of all unsolicited email now contains a URL link, and many of these links serve as delivery mechanisms for Trojans, spyware, and other malware variants. Malware-laden attachments are a well-known issue and most email security solutions deal effectively with this threat. Yet when an attack combines email and Web-based malware, the problem gets much more complicated. As a result, most organizations suffer from email-security blind spots when they deal with these blended-channel threats. Point email security solutions are especially likely to overlook blended security threats that combine multiple channels (such as Web-based applications, email, and IM tools) with sophisticated, fast-moving, and often highly customized malware variants.

Integration Overview

Websense integrates its email security and email Security-as-a-Service solutions with an underlying URL database. The Websense URL database provides enhanced antispam and malware detection capabilities by mapping all known malicious URLs to a set of specific threat categories (e.g. spyware, phishing, key loggers) This ability to perform backend URL analysis and to correlate known threats improves the ability to detect spam while reducing the risk of false positives. An integrated policy interface allows administrators to address security risks faster and more effectively; Websense Email Security, for example, makes it easy to define rules to isolate messages containing URLs based on destination Web site categories, rather than listing specific URLs by name. When an organization is able to block access to malicious URLs in email, it can substantially reduce its potential exposure to data-stealing malware variants.

Use Cases

Web reputation services can prevent some types of Web-borne malware attacks. In many other cases, however, point solutions that focus solely on URL filtering are inadequate. These point solutions usually will not, for example, detect legitimate Web sites that fall prey to hackers and serve as unwitting malware distribution sources. In such cases, businesses are at risk unless they can also monitor and assess the security of **any** content downloaded from **any** Web site, whether or not the site is a legitimate business destination.

Another common case involves the use of spam to direct users to malicious Web sites. Point antispam solutions may identify known senders of malicious email, but they rarely correlate the spam email content to Web sites known to host malware, phishing attacks, or other malicious content. For example, an email containing image spam that looks exactly like a user's banking site may redirect them to a phishing site, or one mimicking a legitimate e-commerce Web site could actually point them to a malware hosting site. When an email security solution relies on sender reputation, it may fail to catch these attacks in cases where the solution has not yet rated the sender or when a legitimate sender falls prey to spoofing or to a compromised mail server.

Differentiation

Built-in web security intelligence. Websense Email Security solutions scan inbound email for typical spam content, but they also scan for URLs which may redirect users to a malicious or compromised Web site. Real-time Web category lookups — a core competency for Websense solutions — ensure that even in cases where malware morphs or malicious Web sites adopt different IP addresses and domain names, inbound email is always identified and neutralized when it poses a security threat.

Simple yet powerful management. The Websense Email Security policy interface enables data security rules (as described in the previous section) and also leverages the Websense Web security database to enforce enhanced antispam rules.

Single view for hosted security customers. Customers using hosted versions of the Websense Web and email security solutions can view incidents involving both channels from a single administrative interface. This feature reduces the number of consoles required to manage both areas and makes the management process more efficient.

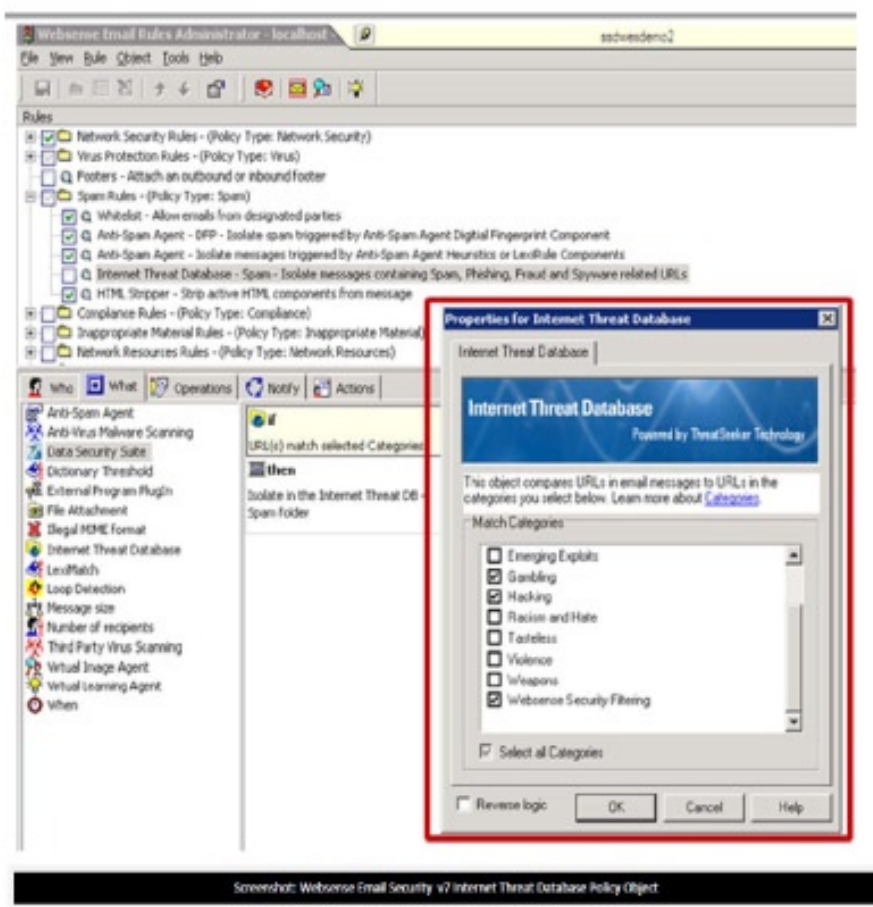


Figure 10: Email Security Integration With Web Threat Database



Figure 11: Integrated Email and Web Security Reporting

Benefits

Email continues to be a critical business application, and its security plays a vital role in Essential Information Protection. The dynamic nature of the Web and the ability to embed URLs in emails creates an environment ripe for spammers and other security threats. Websense email security solutions inspect inbound email for links to known malicious or compromised Web sites; they offer superior antispam capabilities, stop blended security threats, and quickly shut down emerging attack variants. Using Websense Web intelligence and destination-awareness features, administrators need to activate just a single rule to block access to URLs that pose a business risk. And when businesses leverage combined Websense hosted Web and email security functions, they are able to reduce total cost of ownership by employing streamlined, single-console management and reporting tools.

Integration Area: Web and email security.

Blended Threat: Web links embedded in email messages that point to malicious sites or content.

Integration Benefits:

- Improve spam detection rates and block emerging spam threats.
- Reduce email volume by blocking spam “in the cloud,” using Web reputation services and content inspection.
- Leverage the existing email security policy interface to integrate Web security.
- Simplify reporting for hosted Web and email security customers through a single management console.

Integrated Threat Analysis Across Web, Email, and Data Security

Business Issue

When companies weigh the best security solutions for a particular business technology area, factors such as coverage (e.g., Web, email, and data), performance, and price all play an important role. Ultimately, however, all of these factors are irrelevant when a solution lacks robust intelligence capabilities. Without support from an accurate, effective security-research practice, Web, email, and data security solutions may actually inhibit legitimate business processes and increase business data security risks.

Integration Overview

The ThreatSeeker Network provides the underlying intelligence for all Websense security solutions. Real-time Web site security threat assessment and content classification tools produce a rich URL database; the Websense Web, email, and data security solutions, in turn, leverage this database to perform a variety of threat-assessment and security tasks. The Threat Seeker Network can, for example, identify security threats by placing new Web content into virtual machines and testing them for malicious activity. It can also provide zero-day protection for Websense Web security solutions by updating an organization's Websense Web Security Gateway automatically, providing them with up-to-date information about newly analyzed malware variants.

The ThreatSeeker Network integrates Websense Email Security with this URL database, allowing the email security solution to deliver enhanced antispam capabilities. As discussed previously in the Web and email security use cases, administrators can implement a single rule to block malicious URLs from all incoming email.

Websense Security Labs™ follows a proven methodology to address malware threats and data loss risks. This methodology works to: (1) Discover (collect malware samples); (2) Identify (apply reputation analysis); (3) Classify (analyze malware binaries and apply content detection techniques); and (4) Adapt (develop signatures and identify malicious behaviors).

(The "Websense Content Research Cortex" white paper discusses these capabilities and related topics in greater detail.)



Figure 12: Websense Content Research Cortex

Use Cases

Consider some of the key information security capabilities that a comprehensive threat intelligence framework provides:

- Current reputation data on Web sites
- Up-to-date reputation data on spammers and other malicious email sources
- The ability to detect legitimate Web sites that have been compromised
- The ability to block malicious content from legitimate email senders
- Detection of malware variants as they morph between a point of origin and destination
- Tracking of industry regulations dealing with data discovery and protection
- The ability to detect business-confidential data quickly and accurately
- Comprehensive attack anatomy characteristics, including how malware is created and how it ultimately reaches end-users or application servers

In each of these cases, the absence of a real-time intelligence infrastructure can compromise the efficiency and accuracy of a security solution. In the first case, for example, an inaccurate or overly aggressive threat/data loss detection scheme could block legitimate business activities. And in the second case, a lack of timely intelligence could overlook potential data losses or allow malicious code to infect business systems.

Differentiation

Prompt, highly efficient threat-discovery methods. While any vendor with an in-house security research practice will claim expertise in this area, only Websense offers both its Threat Seeker Network, which is designed to perform massively scalable malware data collection tasks, and the Internet HoneyGrid™, a related intelligence infrastructure that probes the Internet to seek out new malware variants. (“The Websense ThreatSeeker Network: Leveraging Websense HoneyGrid Computing” white paper provides a detailed account of this adaptive network-discovery infrastructure and its underlying technical capabilities.)

Practical, effective threat identification methodology. Research for the sake of research has its place in the security technology industry, but this approach does not offer the best solution for securing a company’s business information assets. Websense employs proven threat-assessment capabilities that extend across protocols, content types, and data transformation methods; its protocol coverage, for example, includes HTTP (Web), HTTPS (secure Web), SMTP (email), instant messaging, FTP, remote access, peer-to-peer and streaming media, among many others. These capabilities drive the underlying intelligence infrastructure for Websense Web, email, and data security solutions, each of which monitors various combinations of these protocols.

Since both malware and confidential data may reside within a number of different formats, it is also essential to detect and analyze content in standard documents, executables, Web source files (e.g., XML, HTML) and a wide range of multimedia formats. Websense solutions are fully capable of performing these content-parsing and analysis tasks. And since relevant data is subject to a variety of transformation methods — many of which allow attackers to evade more simplistic security solutions — Websense solutions are also capable of detecting natural language, encryption, compression, and data-obfuscation transformations.

Accurate classification of data. Confidential content is as unique as your business. Websense invests heavily in the computational expertise required to create new fingerprinting methods — a key technology required to classify and track business-confidential data. Reputation-based classification methods (such as those involving Web sites or email addresses) are another area where Websense applies its research expertise. Websense Web security solutions rely upon Real-Time Content Categorization (RTCC) and Real-Time Security Scanning (RTSS) to scan Web sites continuously, using an advanced machine learning model, to identify and assess possible security threats. For email security, a combination of email attribute inspection techniques (including both headers and content), reputation services, fingerprinting, and Bayesian machine learning plays a similar role.

Adaptive visibility and realignment for effective threat management. Researchers must adapt quickly to keep up with emerging security threats and new threat vectors. Websense provides in-depth visibility into emerging threats using its ThreatSeeker Network and “Tracker” database, correlating and cross-referencing threat information from a wide variety of sources. As new threats emerge and existing ones evolve, the ThreatSeeker Network analyzes statistics gathered from its data mining capabilities to realign its intelligence-gathering and threat-assessment tasks. Websense combines these automated tools with a team of experienced, highly trained human researchers to maintain an unrivaled threat intelligence practice.

Benefits

Essential Information Protection is not about locking down business information under any circumstances, at any cost. Essential Information Protection is about monitoring business processes and gathering relevant context; it allows companies to manage genuine security risks without hindering legitimate business activities. Websense Security Labs employs a range of technical and human research tools to generate comprehensive, real-time information about Web, email, and data security risks; this information, in turn, is fed automatically into the company's respective security solutions. Businesses can rest assured that Websense carries the burden of maintaining and managing this infrastructure, while passing along the benefits to its customers.

Integration Area: Threat analysis across Web, email, and data security. Blended Threat: New and evolving threats to Web, email, and data security.

Integration Benefit:

- Implement highly accurate threat-detection capabilities across Web, email, and data security solutions, combined with a comprehensive methodology for discovering, identifying, and adapting to emerging security threats.

Conclusion

Integrated Solutions Address Today's Security Threats

Businesses must continue to adopt new technology and new communication methods to stay relevant. The same is true of business security solutions; as the growing prevalence of botnets, hacker attacks, and data breaches demonstrates, point security solutions that fail to keep up with new security threats are quickly becoming irrelevant. As a result, only integrated security solutions provide the necessary **accuracy** and **context** required to stay ahead of emerging threats.

Convergence demands integration. In many cases, security threats are now hosted using one application but delivered using another one; spammers, for example, send email designed to trick users into clicking URLs, sending them to Web sites that then deploy malware on the victim's system. This converged threat environment demands solutions that seamlessly combine integrated products and an underlying threat intelligence infrastructure — a challenge that Websense Web and email security solutions are designed specifically to meet. And for companies forced to work with reduced infrastructure budgets and smaller IT staffs, Security-as-a-Service versions of the Websense Web and email security solutions offer a very cost-effective alternative.

Diversity demands integration. Attackers may use multiple communications channels, including the Web, email, IM, and FTP, to deliver malware payloads or malicious URLs to end-users. The same channels, along with a host of end-user applications and data storage options (such as peripheral devices and online Web storage) also provide opportunities to create, store, and transmit confidential data. As a result, threat protection and data security solutions require the ability to see into and control all of these channels. Websense Web and email security solutions are designed to cover inbound malware threats across these channels, while Websense data security solutions, integrated with Web, email, and endpoint security components, address a correspondingly wide range of internal data loss threats.

Compliance demands integration. Industry standards, government regulations, and business data security policies all require the ability to monitor and control confidential data no matter where it is located or how it is used. Since integrated Websense solutions reach across networks, communications channels, and content types, they are also uniquely suited to address these compliance concerns. Websense solutions also meet the granular policy definition and reporting requirements associated with many regulatory compliance regimes.

The Business Case for Essential Information Protection

As we have demonstrated, Websense integrated Web, email, and data solutions, combined with the power of a unified content intelligence network, offer a unique value proposition. Compared to point solutions and competing content security suites, Websense Essential Information Protection delivers far more powerful and comprehensive security capabilities. Yet Essential Information Protection also adds business value by adapting to a company's existing business workflows and organizational requirements, allowing these security capabilities to work without disrupting legitimate communication, collaboration, and information-sharing.

As Forrester Research and other third-party research organizations point out, Web-based communication and collaboration tools now provide an essential competitive edge. Websense makes it possible for companies to take full advantage of these capabilities without sacrificing security or exposing sensitive data to unnecessary risks. In addition, companies that adopt Websense Essential

Information Protection solutions are able to achieve this combination of security and flexibility while also achieving a measurably lower total cost of ownership.

Websense technology integration delivers on the promise of Essential Information Protection with both built-in and stand-alone integration points across its Web, data, and email security solutions. The following summary provides an overview of these integration points:

Websense Essential Information Protection meets the demands of today's businesses with modular yet integrated solutions designed to address the challenges associated with technological diversity, convergence, and compliance. Visit <http://www.websense.com/content/Products.aspx> for more details on how Essential Information Protection can enable your business to work more safely and productively.



©2010 Websense, Inc. All rights reserved.

Websense, the Websense logo and ThreatSeeker are registered trademarks and Essential Information Protection is a trademark of Websense, Inc. in the U.S. and various countries. All other trademarks are the property of their respective owners.

ⁱ"The Forrester Wave: Content Security Suites Q2 2009," pg. 6, Forrester Research, Inc.

ⁱⁱ"2009 Data Breach Investigations Report", p. 18, VerizonBusiness, 2009.

ⁱⁱⁱBest Practices for Securing Web 2.0", White Paper by IDC, Brian E. Burke, June 2009, Sponsored by Websense

^{iv}Includes Websense® Web Filter, Websense® Web Security, Websense® Web Security Gateway and the Websense® V10000™ appliance

^vIncludes Websense®Data Security Suite, whose components also standalone modules: Websense® Data Monitor, Websense®Data Protect, Websense®Data Discover, and Websense®Data Endpoint

^{vi}Open Security Foundation: <http://datalosssdb.org/statistics>

^{vii}Refer to official site for PCI Data Security Standard: <https://pcisecuritystandards.org/>