



“Data loss via the Web is four times more likely than email.”

Data Loss Open Security Foundation

Websense

Data Security Solutions

From tarnished brand reputation to regulatory fines, the adverse impacts of data breaches are clear. Just a single incident of data loss can erode a business’s competitive advantage, weaken consumer confidence, and result in fines or penalties from regulators. The problem is further exacerbated with rapid proliferation of mobile computing devices, widespread use of peripheral devices, and easy access to file-sharing software — all increasing the opportunity for data loss. Websense offers comprehensive data security solutions that can help secure your essential information by providing visibility into what data is confidential, where it’s stored, how it is transmitted, and who is using it.

How It Works

Websense® data security solutions secure organizations against a wide range of data loss scenarios with a single policy framework for network and endpoint data loss prevention (DLP) and confidential data discovery using both local and network scans. These solutions are available as individual modules, or an integrated suite, enabling the highest level of deployment flexibility.

The individual modules available in Websense data security solutions offer specific DLP capabilities to suit organizations’ unique needs. Websense Data Security Suite includes all the modules offering a comprehensive solution. Additionally, we’ve embedded

our enterprise-class DLP technology into our Web and email security solutions to enable organizations to easily adopt an expandable, fully capable solution to prevent inbound threats as well as manage outbound risks associated with data loss and regulatory compliance. Whether starting from the data loss prevention solutions embedded in Websense Web or email solutions or from deployment of individual data security modules, customers can quickly expand their deployment to Websense Data Security Suite to secure other channels as well as leverage the full data loss prevention capabilities.

Websense Data Security Suite

Websense Data Security Suite includes four integrated modules, managed under a single policy framework, which together provide visibility and control over network and endpoint data loss as well as comprehensive data discovery across enterprise storage systems.

- **Websense Data Monitor:** Monitors for data loss on network (Web, email, FTP, other)
- **Websense Data Protect: (includes Websense Data Monitor)** Enforces automated, policy-based controls to block, quarantine, route to encryption gateway, audit and log, or notify users of violations
- **Websense Data Endpoint:** Monitors and enforces automated, policy-based controls for data in use via applications and peripheral devices on endpoints; local discovery and classification of confidential data
- **Websense Data Discover:** Discovers and classifies confidential data stored in enterprise repositories, with customizable remediation action including file removal

Websense Data Security Suite is the only solution with native enforcement of Web (HTTP), secure Web (HTTPS), and email (SMTP) traffic, eliminating the need for additional expensive third-party proxy solutions. It integrates with any Websense Web security solution, which routes outbound Web traffic to Websense Data Monitor for analysis.



“We had zero visibility into our data security until we received the initial report from the Websense solution.”

Roger McIlmoyle

Director of technology services
TLC Vision

Websense Data Monitor

Websense Data Monitor is the leading network data loss prevention solution to monitor and report on data losses. Unlike competitive solutions that focus merely on what confidential data is being lost, Websense Data Monitor automatically provides context to identify what customer data is being lost and real-time information on who is using the confidential data and where the data is going.

Websense Data Monitor offers:

- **Unrivaled visibility** into Web 2.0 applications, including real-time destination awareness of what data is sent where and by whom.
- **Accurate identification of confidential data** with a comprehensive set of technologies, including policy templates for regulated data and fingerprinting of known confidential data.
- **Flexible architecture** to reduce deployment costs, including integration with Websense Web security.

Websense Data Protect

Building on the capabilities of Websense Data Monitor, Websense Data Protect is the leading network data loss prevention solution to monitor and automatically protect against data loss. With granular and automated levels of control, Websense Data Protect can help prevent loss of sensitive data with less effort and manual intervention.

Websense Data Protect offers:

- **Automated, policy-based enforcement** options including block, quarantine, file removal, encrypt, audit/log, and user notification in real time.
- **Extensible and powerful policy framework** providing visibility and control over confidential data on your network.
- **Websense Data Monitor** features and capabilities.

Websense Data Endpoint

Websense Data Endpoint extends the visibility and control to endpoints over what confidential data is and should be stored; who is using it; how it is being used; where it is being transferred; and what real-time action is taken to prevent data loss at the endpoint. Providing unrivaled visibility and control over copy-paste, screen capture, print, and transfer to removable media, Websense Data Endpoint can enforce policies in the endpoint environment with minimal overhead.

Websense Data Endpoint offers:

- **Automated enforcement** including block, application control/removal, audit/log, confirm, notify user.
- **Unrivaled visibility and control** over copy-paste, file access, screen capture, and print for client software applications (including applications with evasive, encrypted network behavior, such as Skype), endpoints (regardless of location), and peripheral devices.
- **Operational efficiency** with minimal impact on endpoint, including options to disable discovery when using battery.
- **Accurate identification of confidential data** with a comprehensive set of technologies.
- **Discovery and classification** of all confidential data on endpoint.

Websense Data Discover

Websense Data Discover is an agent-less solution that remotely scans specified network files shares, databases, email servers, data repositories, and desktops to discover and classify confidential data. It automatically enforces data protection policies on these systems by applying actions including encryption, file removal, file replacement, notification, auditing, and logging of policy violations.

Websense Data Discover offers:

- **Discovery and classification of confidential data** stored on the network in known locations by scanning specified IP address ranges where confidential data is known to reside.
- **Automated remediation** of unsecured confidential data on data repositories.
- **Operational efficiency with minimal impact on server performance**, using off-peak scheduling of scans.
- **Accurate identification of confidential data** with a comprehensive set of technologies, using policy templates for regulated data and fingerprinting of known confidential data.
- **Extensible and powerful policy framework** providing visibility and control over all confidential data.

Reduced Cost and Complexity

Comprehensive DLP security coverage can include multiple software and hardware deployments, which can add to the overall solution cost and increase complexity. The increase in cost and complexity is the biggest challenge facing most DLP deployments. With Websense data security solutions, organizations can start with a small but effective DLP solution, such as Websense Web Security Gateway and upgrade to the Data Security Suite as their organizations and requirements grow. Additionally, the full Data Security Suite is easy to deploy and manage, and can be operational in under an hour. The high integration capabilities of Websense data security solutions also minimize the amount of hardware needed to deploy a comprehensive solution.

Unified Content Security Management and Reporting

Management and reporting capabilities are critical in any security solution deployment. Not only must they provide simple intuitive interfaces but they must also consolidate many tasks, sometimes spanning multiple security solutions. Websense data loss prevention solutions are managed by the Websense TRITON™ Console. It combines the management and reporting capabilities for Web, email, and data loss prevention technologies into a single Web-based interface resulting in greater visibility and control. It includes over 55 built-in reports, extensive customization capabilities, policy wizards, configuration templates, and other innovative capabilities to reduce cost and greatly simplify management tasks.

Whether deploying Websense Data Security Suite, one of the data security modules, or Web security or email security solutions, the Websense TRITON Console offers a single management solution for all your security needs today and into the future.



“[For internal breaches], two-thirds were the result of deliberate action and the rest were unintentional.”

Verizon Business
2009 Data Breach

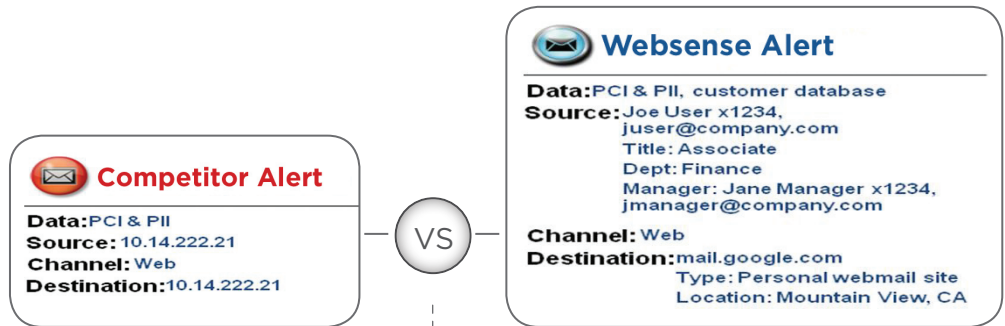


“31 percent of reported data loss incidents are attributed to a stolen laptop, stolen desktop, or lost media.”

DatalossDB

Open Security Foundation

Visibility and Control with Destination Awareness



- Limited context
- More work for IT administrator

Consider a typical data loss alert, where only the IP address and application channel is presented, leaving the burden on the IT manager to determine who to notify and what specific destinations may be receiving confidential data.

- User and destination awareness
- Faster time to remediation

With Websense data security solutions it's easy to see that PCI and PII data have been lost via a Web channel (**how**), through a specific webmail URL (**where**), by Joe User in Finance (**who**)—providing visibility, *efficiently*. This alert is also relevant and actionable given that it is generated in real time, providing contact details, title, and anything else provided by integration with Websense Web Security.

Application Awareness and Device Control on Endpoints

Employees create risk by copying data to peripheral storage devices from local applications. If an employee copies data from a business application to local email software, Websense reports on this event with details on the user, the endpoint, the confidential data, the application, and the destination for this data. Other endpoint DLP solutions provide insufficient visibility into applications and data, blocking actions which may actually include legitimate business activities.

Comprehensive Discovery for Efficient Remediation

Once a data breach has occurred, a current inventory of this data helps determine the possible sources of the loss. Websense Data Discover uses network scanning of data repositories to find confidential data in known locations, classify this data, and initiate remediation action including encryption or file removal. The incident management view includes a link to the specific file, the category in which this data falls (fingerprinted or regulated data), the file owner (to assign the incident for remediation), and any remediation action that has already been enforced to address the violation. When used with Websense Data Endpoint, which discovers data locally using a software agent, the solution provides comprehensive, scalable discovery for both online and offline systems

Features	Benefits
Automated real-time enforcement options across network, endpoint and discovered data repositories	<ul style="list-style-type: none"> • Flexible enforcement options including user notification, audit/log, and more • Network traffic: Quarantine, block, route to third-party encryption gateway, remove content • Endpoint activity: Block move/copy/print of confidential data from applications to external devices, block screen print, user notification, user confirmation/audit/logging • Discovery: Removal or replacement (using credentials and automated scripts), encryption (third-party integration with Voltage file encryption) of stored data

Features	Benefits
DLP for Security-as-a-Service (SaaS) applications	<ul style="list-style-type: none"> • Ensure sensitive data are only uploaded to identified and approved SaaS application • Enforce type of information that can be downloaded locally from SaaS application
Smart Detection capability to detect data loss covering multiple communications	<ul style="list-style-type: none"> • Detect small amounts of confidential data sent over multiple communications • Detect large volume of data loss from the sum of confidential data sent over specific time period
Visibility into numerous network channels through passive traffic monitoring	<ul style="list-style-type: none"> • Network monitoring Web (HTTP), secure Web (HTTPS), email (SMTP), IM (AOL, Yahoo, MSN), FTP, printing (optional OCR agent), dynamic Web 2.0 content • Reduce violations by 50 percent with user notification of violations
Visibility into device, application, and storage of confidential data content on end user-systems	<ul style="list-style-type: none"> • Manage data loss risk due to user mobility and misuse of data • Location awareness: Apply policies on/off network, offline • Portability: Local fingerprint storage with minimal storage footprint • Device monitoring and control of removable storage, external hard drives, printing, burning to CDs/DVDs, copy/paste/screen print to clipboard, file access • Application monitoring triggered by user, user group, predefined application or application groups • Classification by regulated data type such as credit card numbers
Discovery of confidential data in local and network data repositories	<ul style="list-style-type: none"> • Comprehensive discovery: Network scans, local scans (via endpoint software agent); ad-hoc or scheduled scans • Coverage: Network-based scan of databases, file shares, Exchange, SharePoint; local scan based on file type, size, age • Identification: Over 400 file types, including Microsoft Exchange PSTs; file fingerprints, compliance templates
Built-in data identification using patented Websense Precise ID™ technologies	<ul style="list-style-type: none"> • Automated, accurate identification of confidential data: Keywords, dictionaries, fingerprinting, regular expressions, thresholds, context, proximity, and correlation for unstructured, structured data (e.g. database) • Effective detection: Reduce false positives and business disruption by disregarding data if not mapped to customer data (by using fingerprints) or if below specified threshold
Flexible deployment options including built-in Web proxy and integration with third-party Web proxies	<ul style="list-style-type: none"> • Websense Web Security integration: Route HTTP, HTTPS, FTP traffic for analysis by Websense Data Security via ICAP protocol • No need for additional solutions: HTTP, SMTP, IM, FTP and HTTPS (with Websense Web Security, for Web proxy) • Flexible and cost effective: (1) Monitor or protect mode, (2) passby/span port or inline/tap, (3) with Websense Web Security or any standard Web proxy, (4) with Websense Email Security or any SMTP-compliant MTA • Efficiency: Schedule discovery scans when system, not running off battery (endpoint); during off-peak hours; network-based (coverage) vs. agent-based (performance); exception lists in IP range for network discovery • Endpoint agent deployment: Microsoft SMS or other methods; Avoid conflict with antivirus, personal firewalls; Phased deployment with user profiles; enable/disable agent • Investment protection: Deploy modules in phases, as needed



“[Websense solutions] provide industry-leading accuracy, automatically searching the content located throughout our organization and identifying where our sensitive data resides.”

Addison Avenue Federal Credit Union

Websense Data

Discover customer

Technical Specifications:

WebSense Data Security Suite Technical Specs

See Users Guide for more details

DSS Protector (monitoring component)

System Resources

See Certified Hardware document for more details

Certified Vendors: IBM, HP, Dell,
Network Engines

Dual or quad core Intel Xeon processors
1, 2, 4 GB RAM (fully buffered DIM)
Minimum 74 GB, hot pluggable hard drives
NIC 1000/100/10 Mbps

Software Resources (included)

Hardened Linux Operating System with
WebSense Data Monitor or Data Protect
software

DSS Server (management component)

System Resources

Two 2.4 GHz Intel or AMD Processors or better
4 GB RAM

Four 74 GB, 15K RPM, SCSI U320 hard drives
(minimum) in RAID 1+0
NIC 1000/100/10

Software Resources

Windows 2003 Server standard R2 edition
latest Service Pack

DSS Endpoint (end point software agent)

System Resources

Pentium 4 @ 1.8ghz or above
• Minimal 512MB RAM on Windows XP,
1GB RAM on Windows Vista or Windows
Server 2003

• Minimal 100MB free hard drive space

Software Resources

Supported Operating Systems
• Windows XP (32 bit)
• Windows Vista (32 bit)
• Windows Server 2003 (32 bit)

Part Numbers and Description

SKU: WDSS-X-XXXX-X

Descriptions: WebSense Data Security Suite
Options: # seats, support, printer agent,
content gateway, subscription duration,
new/renew/additional seats.

WebSense, Inc.
San Diego, CA USA
tel 800.723.1166
tel 858.320.8000
www.websense.com

WebSense UK, Ltd.
Reading, Berkshire UK
tel 0118.938.8600
fax 0118.938.8697
www.websense.co.uk

Australia
websense.com.au

Brazil
websense.com/brasil

Colombia
websense.com/latam

France
websense.fr

Germany
websense.de

Hong Kong
websense.cn

India
websense.com

Ireland
websense.co.uk

Israel
websense.com

Italy
websense.it

Japan
websense.jp

Malaysia
websense.com

Mexico
websense.com/latam

PRC
prc.websense.com

Singapore
websense.com

Spain
websense.com.es

Taiwan
websense.cn

UAE
websense.com

Features	Benefits
Comprehensive and current policy templates, centralized policy and incident management and reporting	<ul style="list-style-type: none"> • Built-in wizards to make it easy: Industry, regional regulations (e.g., PCI, UK DPA, GLBA, HIPAA, SOX); pre-defined checks: PII (personally identifiable data), PHI (personal health care information), PCI (payment card industry), PFI (personal financial information). • Apply consistent policies: Network, endpoint, data repositories • We keep track of regulations, so you don't have to: Dedicated team researches and updates templates regularly • Built-in reports for auditors and executives: Distribute tamperproof (PDF) compliance reports with information on total number of incidents based on: Network: User group, policy, regulation, enforcement action, etc. • Endpoint: Device/application channel, user group, policy, regulation, enforcement action taken, etc. • Discovery: IP address, repository type/name, confidential data (type, specific file/record), data owner, remediation action

