



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

Data Loss Open Security Foundation

Websense

Data Security Suite

From tarnished brand reputation to regulatory fines, the adverse impacts of a data breach are clear. The problem is exacerbated with mobile devices and easy access to file sharing software, all creating opportunities for data loss. Websense® Data Security Suite is a data loss prevention solution which can help secure your essential information by providing visibility into what data is confidential, where and how it is transmitted or stored, and who is using it.

How It Works

Websense Data Security Suite covers multiple 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. The approach is modular, which

means you decide how to deploy, based on your business needs. The suite is tightly integrated with Websense Web and email security products for enforcement that is built in or supported via third-party integration.

The Websense Data Security Suite provides:

- **A complete DLP suite** to identify, monitor, and protect confidential data across the network, on user desktops and laptops, and in network data repositories
- **The option to start with one or more modules** for cost-effective DLP
- **Unrivalled visibility and control** with automated, real-time enforcement over Web 2.0 applications, where dynamic user-generated content is an increasing risk
- **Accurate and easy identification of confidential data**, with policy templates for industry regulations and file fingerprinting
- **Powerful policy framework** providing visibility and control over who (user details), how (applications), where (destination awareness), and what (confidential data) moves on your network
- **Flexible architecture** to reduce deployment costs, including integration with Websense Web Security and other Web proxy solutions

The 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 customisable 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, returning a disposition based on which the Web security solution enforces policy.



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

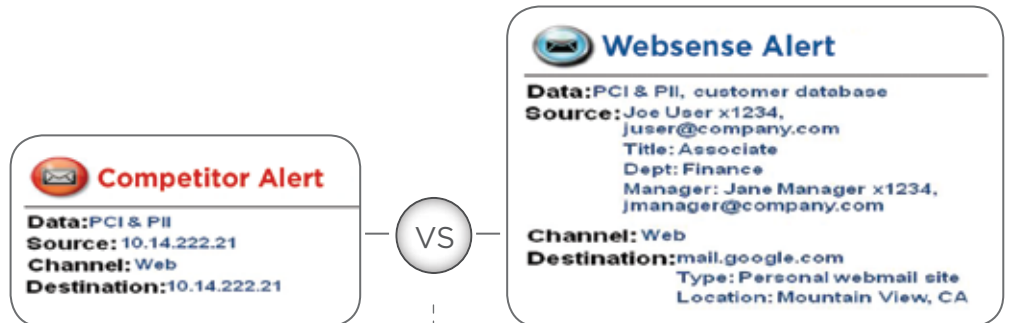
Roger McIlmoyle

Director of technology services
TLC Vision

The solution offers visibility and control in three areas:

DLP Area	Websense Coverage	Websense Products
Data in Motion	Visibility: Web, secure web (HTTPS), email, FTP, IM, P2P and more with user and destination awareness for Web Control: automated, policy-based enforcement with blocking, encryption, quarantine, logging, user notification, file removal	Data Monitor Data Protect
Data in Use	Visibility: client applications (pre-defined, custom), removable devices, actions (copy, paste, screen print, print); local discovery Control: automated, policy-based enforcement with blocking (with helpdesk bypass option), logging, user notification, file removal	Data Endpoint
Data at Rest	Visibility: into databases, file shares, Exchange, Share Point through network discovery Control: automated, policy-based enforcement with logging, user notification, file removal, encryption, change file permissions	Data Discover

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 Monitor 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
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 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 organisation 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

Italy
websense.it

Brazil
websense.com/brasil

Japan
websense.jp

Colombia
websense.com/latam

Malaysia
websense.com

France
websense.fr

Mexico
websense.com/latam

Germany
websense.de

PRC
prc.websense.com

Hong Kong
websense.cn

Singapore
websense.com

India
websense.com

Spain
websense.com.es

Ireland
websense.co.uk

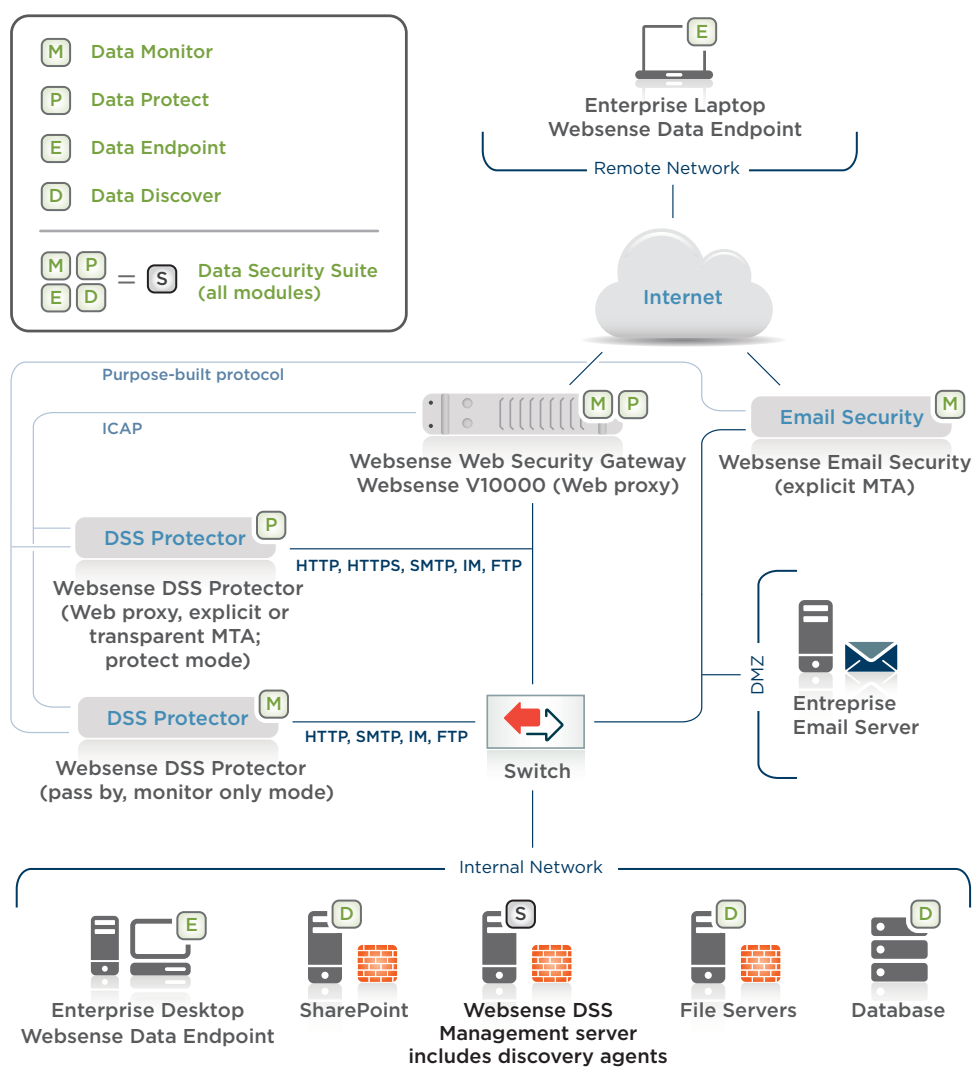
Taiwan
websense.cn

Israel
websense.com

UAE
websense.com

Comprehensive and current policy templates, centralised policy and incident management and reporting

- **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 healthcare information), PCI (credit card data), 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 by...
 - **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



Optimal deployment of the WebSense Data Security Suite

For more information, to start a free trial of WebSense Web solutions, or to view an online demo, visit www.websense.com/evaluations.