



“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

The effects of a data breach on a business can be enormous; a single incident of data loss can erode a business's competitive advantage, weaken consumer confidence, and tarnish brand reputation. Whether the breach is due to broken business processes or malicious activity, organizations simply can't afford to find out if they've got problems until it's too late. Industry regulations and corporate governance mandate data security policies to monitor and prevent loss of confidential data, leading organizations to look at data loss prevention (DLP) technology.

Threats to confidential data can be introduced in many ways, both intentional and accidental. Employees upload confidential data to social networking sites, email unencrypted, confidential data to partners or simply surf Web sites hosting data-stealing malware. How does a business secure its processes and guard against malicious activity that may lead to data loss?

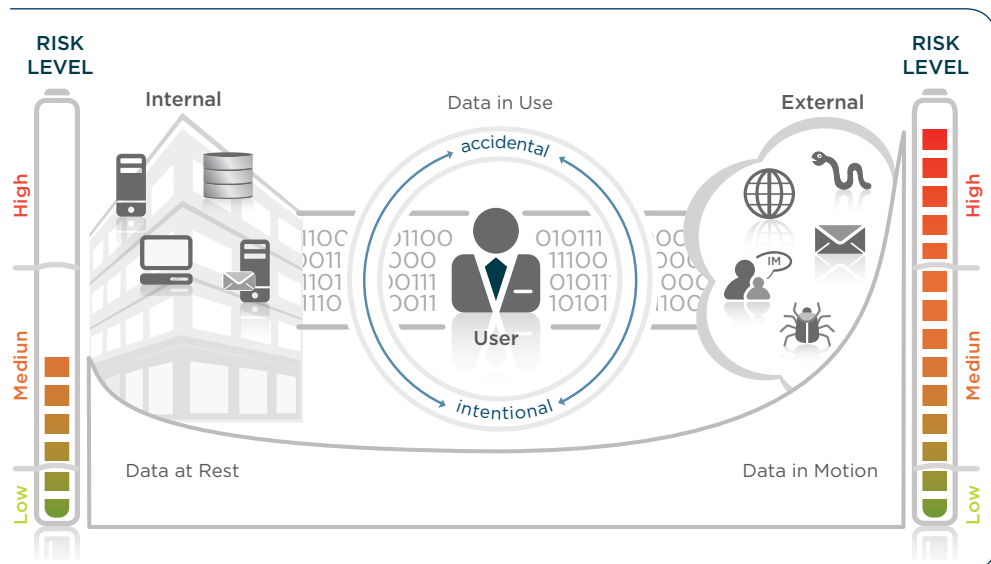
How It Works

Websense® Data Monitor is the leading network data loss prevention solution to monitor and report on data loss. Unlike competitive solutions that focus only on what confidential data is being lost and how (over Web or email), Websense Data Monitor is the only solution to

automatically provide context to identify **what** customer data is being lost and real-time information on **who** is using the confidential data and **where** this data is going over the Web. This means more actionable alerts and less effort for administrators to address violations.

The 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



Data in motion presents the greatest risk for data loss



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

**Data Loss
Open Security Foundation**

Why Start DLP with Network Monitoring?

The primary risk of data loss is the misuse or unauthorized disclosure of confidential data. If a DLP solution sees confidential data leaking over email and blogs, one must assume that risk has become reality and that they **have** been compromised. In contrast, stored data could be at risk due to insufficient access controls but has not yet been compromised. Similarly, copying data to removable storage devices presents the potential for that device to be stolen, but that risk is still moderate if the device is in the possession of an authorized user. In short, if confidential data is in motion on your network, any number of unauthorized users may see this data, thereby presenting the greatest risk. The attack on your data is in progress and stakeholders must be notified or the attack must be blocked.

Different aspects of the data life cycle present different relative risks:

DLP Area	Data in Motion	Data in Use	Data at Rest
Risk Example	One to Many—one authorized user could leak confidential data to MANY unauthorized users, by posting to a social networking site	One to One—user copies confidential data from business application to USB drive, which could be stolen	One to Unknown—Data resides on server and is presumably only accessed by authorized users, who may then lose data by sending it (Data in Motion) or copying it (Data in Use)
Relative Risk Level	High	Medium	Low

More Visibility, More Efficiency:

Competitor Alert

Data: PCI & PII
Source: 10.14.222.21
Channel: Web
Destination: 10.14.222.21

Websense Alert

Data: PCI & PII, customer database
Source: Joe User x1234,
 juser@company.com
 Title: Associate
 Dept: Finance
 Manager: Jane Manager x1234,
 jmanager@company.com

Channel: Web
Destination: mail.google.com
 Type: Personal webmail site
 Location: Mountain View, CA

VS

- 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 efficient visibility. 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.



“Percentage of malicious Web attacks that include data stealing code: 39. Percentage of data stealing attacks that are conducted over the Web: 57 (a 24 percent increase in the second half of 2008).”

Websense Security Labs

Features	Benefits
<p>Unrivaled visibility into numerous network channels through passive traffic monitoring</p>	<ul style="list-style-type: none"> • Network monitoring of HTTP, HTTPS, SMTP, IM, FTP, P2P, printing, dynamic Web 2.0 content • Reduce violations by 50 percent with user notification of policy violations • Real-time destination awareness and user details for Web traffic reduces manual efforts to resolve IP addresses to user machines, user identities, and destination URL categories • Monitoring of internal email communications for when confidential data is sent from one employee to another • Option to monitor specific application ports: Administrator can monitor for business processes on known application ports
<p>Built-in data identification using patented Precise ID™ technologies</p>	<ul style="list-style-type: none"> • Automated, accurate identification of confidential data: keywords, dictionaries, fingerprinting, regular expressions, thresholds, context, proximity, and correlation for both unstructured and structured data, regular expressions, thresholds, context, proximity, correlation and combinations between database fields, etc. • Effective detection: Reduce false positives by disregarding data if not mapped to customer data (by using fingerprints) or if below specified threshold
<p>Flexible deployment options including built-in Web proxy and integration with third-party Web proxies</p>	<ul style="list-style-type: none"> • Simple deployment with Websense Web Security integration: Route traffic for analysis from Web security via ICAP protocol • No need for additional solutions: Built-in monitoring for HTTP, SMTP, IM, FTP, P2P and HTTPS • Flexible and cost effective: Multiple deployment options – in monitoring mode (1) passby/span port, inline/tap, LAN (2) with Websense Web Security or with standard Web proxy (3) with Websense Email Security using purpose-built protocol • Investment protection: Add DLP modules for network protection, endpoint and discovery as needed
<p>Comprehensive and current policy templates, centralized policy and incident management and reporting</p>	<ul style="list-style-type: none"> • Built-in wizards to make it easy: Websense-maintained templates for industry, regional regulations; Pre-defined checks for PII, PHI, PCI, and PFI • Apply consistent policies across network channels including Web, secure Web, email, FTP, IM, P2P and more • We keep track of regulations, so you don't have to: Dedicated research team reviews industry and regional regulations and updates templates regularly • Built-in reports for auditors and executives: summary and detailed reports showing number of incidents by channel, by user group, by policy, by regulation, and more. Show state of compliance efforts.

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 86981
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.co.uk

Italy
websense.it

Japan
websense.jp

Malaysia
websense.com

Mexico
websense.com/latam

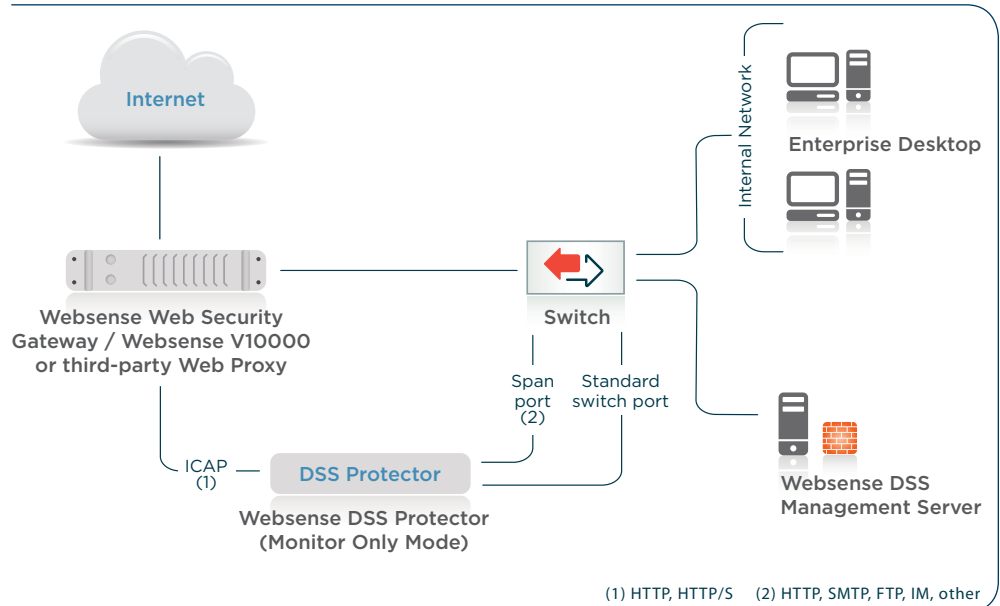
PRC
prc.websense.com

Singapore
websense.com

Spain
websense.com.es

Taiwan
websense.cn

UAE
websense.com



Typical deployment option for Data Monitor

Technical Specifications:

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

Part Numbers and Description

SKU: WDM-X-XXXX-X

Descriptions: Websense Data Monitor

Options: # seats, support, printer agent, content gateway, subscription duration, new/renew/additional seats.