



71 percent of enterprises cite data leak prevention for flash and USB drives as a must-have.

SearchSecurity.com
Priorities 2009 Survey

Websense Data Endpoint

The essential, confidential data owned by a business provides a distinct competitive advantage. But when a business doesn't have a clear notion of what data it has and where it is stored, that business is at risk.

The problem of data loss is exacerbated by the increase in mobile computing, the widespread use of peripheral storage devices, and easy access to client software with file download and file sharing capabilities. Trusted employees often unknowingly take actions that put data at risk, like copying a list of all of customers to a USB device, printing design drawings or other confidential intellectual property without authorization, using print screen, copy and paste or other actions to transfer confidential data out of an application, or losing a laptop that may contain critical and confidential business information.

Enterprises can identify, monitor, protect, and discover confidential data on end user systems with Websense® Data Endpoint.

How It Works

Websense Data Endpoint picks up where network monitoring and discovery leave off, by extending visibility and control to endpoints over **what** confidential data is and should be stored (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** is taken to prevent the data loss. It provides unrivaled visibility and control over copy, paste, and screen print from client applications to removable media, can be enforced anywhere and is compatible with existing endpoint environments with minimal overhead.

Websense Data Endpoint offers:

- **Automated enforcement** including block, application control/removal, audit/log, confirm, notify user
- **Unrivaled visibility and control** over cut and 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



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

DatalossDB
Open Security Foundation

This alert shows that the user copied data from Internet Explorer to their local email software, and shows the source of the data and the destination, including other applications, not just devices.

The screenshot displays an incident detail window with the following sections:

- Properties:** Content pasted from application: "IE" into application: "Microsoft Outlook Express"
- Source:** DEMO\JDoe
- Incident Details:**
 - Status: New
 - Urgency: Serious
 - Detected by: Endpoint Agent
 - Local Date Detected: 10 Apr. 2009, 05:27:17 PM GMT-0400
 - Analyzed by: Endpoint Server DEMO-DSS.demo.websense.
 - Action: Blocked, Audited
 - Assigned to: Unassigned
 - Channel: Endpoint Applications (Paste)
 - Protocol: File
 - Incident Tag: N/A
 - Date & Time: 10 Apr. 2009, 5:28:05 PM
- Source Details:**
 - Full Name: DEMO\JDoe
 - Username: DEMO\JDoe
 - Email: jdoe@demo.websense.com
 - Hostname: demo-xp.demo.websense.com
 - Title: Product Marketing Manager
 - Manager: Madoff, Bernard
 - Phone Number: +1 301 9292333
 - Department: Marketing
- File Details:**
 - File Name: EndpointData - 9 KB
 - Attachment Size: 9 KB in total
- Endpoint Details:**
 - Endpoint Type: Desktop
 - Application Name: Microsoft Outlook Express
 - Device Type: Internal Hard Drive
 - Policy Version: 0

Incident detail with Websense Data Endpoint

Get More from Your Endpoint DLP

Websense Data Endpoint monitors and prevents loss of confidential data on end-user systems for clipboard operations (cut, copy, paste), printing and print screen (block, no content monitoring) with key benefits in the following scenarios:

Scenarios	Benefits
Client applications	<ul style="list-style-type: none"> Address applications which cannot be monitored on the network due to encrypted or evasive behavior (e.g. Skype) Protect content in business applications (e.g. customer data) while allowing use of personal content in other applications (e.g. photo album software)
Shared machines	<ul style="list-style-type: none"> Contractors (e.g. temps helping with month end finance processing) or teams (e.g. training rooms) Enforce DLP on Citrix and other terminal servers Single agent can enforce different policies on same machine, for different users
Company issued USB keys	<ul style="list-style-type: none"> Can allow confidential data copy to company-issued USB devices supporting encryption. Can otherwise block, satisfying many industry regulations for privacy (e.g. PCI DSS) Can control data write capabilities to these company-issued devices, while only allowing read capability from other devices
Both online (connected to company or public network) and offline (no network connection) enforcement, local fingerprints	<ul style="list-style-type: none"> Enforce Anywhere - both regulated and business-confidential data
Local discovery: runs in background with power-saving features	<ul style="list-style-type: none"> Optimal performance and scalability for managed systems—scan terabytes of data in a short time Single report showing all discovered data, regardless of scan method (e.g. from network scans using Websense Data Discover) Scan managed laptops anywhere - both online and offline



Websense is positioned in the leaders quadrant by Gartner in their most recent Magic Quadrant for Content-Aware Data Loss Prevention.

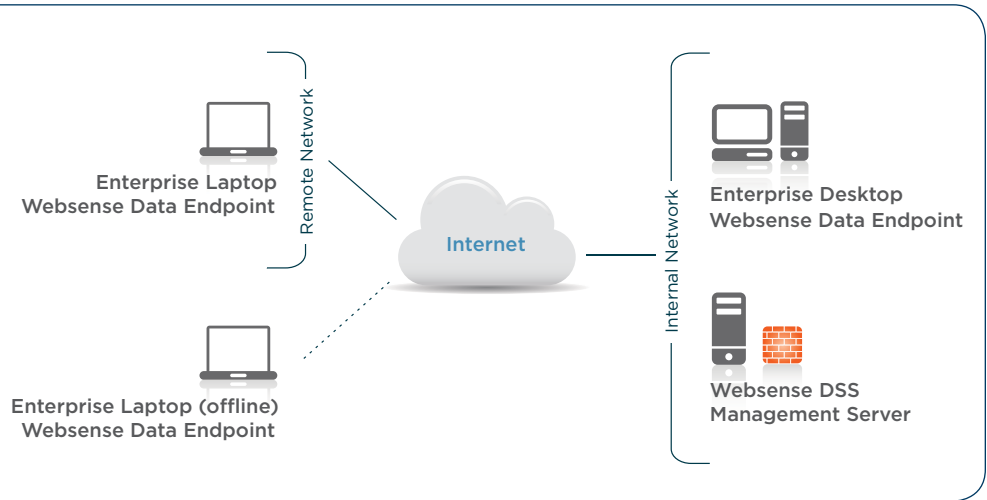
Gartner, Inc. “Magic Quadrant for Content-Aware Data Loss Prevention”* by Eric Ouellet and Paul Proctor, June 22, 2009.

Features	Benefits
<p>Automated enforcement options including device control</p>	<ul style="list-style-type: none"> • Avoid data loss and minimize risk by blocking unauthorized actions to specific peripheral devices • Flexible enforcement options: block move/copy/print from applications to external devices, user notification, user confirmation, audit/logging • Reduce violations with user confirmation and notification of policy violations • Minimize risk of lost or stolen laptops with routine discovery of locally stored data, providing current inventory to make best decision on remediation action • Minimize business disruption with bypass option for use by helpdesk to allow exception • Data-centric device control: Allow legitimate use of devices if data not confidential
<p>Visibility into device, application, and storage of confidential content on end user systems</p>	<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: allow local storage of fingerprints 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 • Discovery by file type, size, age; ad-hoc or scheduled; full or differential scan • Classification by regulated data type such as credit card numbers
<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, 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 (using fingerprints) or if below specified threshold
<p>Flexible deployment options</p>	<ul style="list-style-type: none"> • Efficiency: schedule discovery scans when system idle or when not running off battery • Standard agent deployment methods supported: Deploy agents to end user-systems using automated (e.g. Microsoft SMS) or manual installation methods • Avoid conflict with other endpoint software agents: Configuration options to account for antivirus, firewall, etc. • Phased deployment: user profiles, enable/disable agent—two modes: interactive (visible to user), 'stealth' (hidden from system tray, no user notification)
<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 endpoint, network, network data repositories • 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: Distribute executive and/or detailed reports showing total number of incidents by device/application channel, by user group, by policy, by regulation, enforcement action taken and more. Show status 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	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.co.uk	UAE websense.com



Typical deployment option for Data Endpoint

Technical Specifications:

See *Websense Endpoint Reference Guide* for more details

Data 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)

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: WDE-X-XXXX-X

Descriptions: Websense Data Endpoint

Options: : # seats, support, subscription duration, new/renew/additional seats

*The Magic Quadrant is copyrighted June 22, 2009 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.