

DATA LEAKAGE CHALLENGES

With increasing frequency and severity, more and more organisations are becoming victims of high-profile leaks that started with a simple click of the SEND button or an innocuous Instant Messaging conversation.

80-90% of leaks are accidental or unintentional. GARTNER

The threat of data leakage is considered by many to be the biggest security threat today, with breaches leading to the potential for diminished customer confidence, loss of competitive advantage and failure to meet compliance regulations.

Biggest threat to your organisation's security? - 52% answered leakage of proprietary / confidential information. MERRILL LYNCH STUDY OF 50 CISOs, 2006

Data leaks are very costly. They can invoke regulatory penalties, costs of making amends to damaged parties and the cost of restoring confidence in a compromised company.

Data leaks cost companies \$182 per record. PONEMON INSTITUTE

Most organisations lack visibility into where their confidential data is stored, who is using it and how, whether they're emailing it, posting it to websites, copying to USB, or saving it locally. Without visibility, you can't effectively implement controls.

WHAT IF YOU COULD...

Determine where confidential data is located on your network?

Organisations employ many data storage systems from which critical data is accessed and exported into other forms. This data is stored on laptops, USB drives and discs and is routinely accessed, transferred and left forgotten on open, often vulnerable, file shares.

Monitor where sensitive data travels in and out of your network?

Organisations often lack visibility into who is using their data and how. By monitoring communications you can get visibility into business processes, manage compliance and risk policies and effectively report on corporate governance.

Set policies to enforce where and how data should move?

Information leaks are not an IT problem; they are a business problem. Thus, organisations require controls that are aligned to business processes...for example: forcing encryption for communications to business partners but blocking those to other destinations, or blocking data transfers to removable media. Ultimately, with intelligent enforcement you can enable business but secure the data.

Leverage your existing investment in Websense?

For intelligent information security, Websense's DLP solutions integrate with its web filtering/web security deployment to provide both advanced policy controls to manage who and what go where and how. You can leverage your existing investment to set policies for where data can go, just as you do for where your users can go.

WEBSense DATA SECURITY SUITE

Data Discovery and Classification

- Agent-less network and/or local data discovery to efficiently discover and classify confidential information
- Third-generation fingerprinting to accurately identify all forms of data
- Visibility into where data is stored throughout the organisation to support data security policies

Data Monitoring and Reporting

- Monitor internal and external communications, including email, web, print and instant messaging with over 600 out-of-the-box templates
- Audit business processes to identify who is sending what information where, refine policies and workflows and reduce risk on the network and at the endpoint
- Accurately monitor proprietary data, including source code, CAD drawings and other proprietary content

Data Protection and Control

- Built-in policy enforcement based on users, data, destinations, channels and regulations, on and off the network
- Automated policy controls with advanced workflow and management
- Scalable, enterprise-ready solution that integrates with existing infrastructure, including encryption (file and mail), proxy, security information management (SIM), etc.

QUESTIONS TO ASK

- What data is confidential?
 - Where is your confidential data?
 - Should it be there?
 - Is it safe?
 - Who is using your confidential data and how?
 - What are the risky business processes?
 - What are the bad employee habits?
 - How do you currently secure your data?
 - How effective is this?
 - What is your risk level?
 - How do you know?
- Situation:**
- What kind of data must you secure?
 - What regulations apply to you and your confidential data?
- Problem:**
- Are you concerned about loss of data via: email, the web, FTP, USB?
 - How do you currently report on data security compliance?
- Implication:**
- What would losing data mean to your organisation? Brand? Competitive advantage?
- Need:**
- What would it mean if you could automate policy and compliance controls for data security to users, data, destinations and channels?

OVERCOMING OBJECTIONS

Q. How is Websense better than the competition?

A. Websense Data Security Suite is the only solution that includes content and context awareness to secure who and what go where and how. No other solution can provide the level of control to secure business processes, prevent data loss and achieve regulatory compliance. Websense provides this through its security research teams and patented technologies (PreciseID™ and ThreatSeeker™ technologies).

Q. How do you secure data at the endpoint?

A. Websense has an integrated network and endpoint DLP solution that extends coverage for data discovery, monitoring, and protection to the endpoint, whether the user is on or off the network. Websense is unique among DLP vendors because of our open endpoint architecture (ability to integrate with device control solutions), local discovery and our application awareness and control.

Q. Websense is a filtering vendor... how do you now offer DLP?

A. In January 2007, Websense acquired PortAuthority Technologies - the leader in DLP - who, through 10 years of R&D, developed twenty-seven patent-pending technologies. We have hundreds of DLP deployments worldwide and can provide reference customers to demonstrate the maturity and effectiveness of our solution; we are the only vendor to have integrated our portfolio. We have 100% customer retention on our DLP product line.

SOLUTION: WEBSense DATA SECURITY SUITE

Websense Data Security Suite, the leading data loss prevention solution, accurately prevents data leakage, secures business processes and manages compliance and risk by discovering where data is located, monitoring its use and protecting it on the network and at the endpoint.

The solution includes four modules:

Websense Data Discover – Discovers and classifies data distributed throughout the enterprise.

Websense Data Monitor – Monitors who is using what data, and how.

Websense Data Protect – Protects data with policy-based controls that map to business processes.

Websense Data Endpoint – Extends data security to the endpoint with integrated management and reporting.

COMPETITION

	OVERVIEW	WEAKNESSES
EMC/RSA	Enterprise focused Strong Discovery Capabilities Gartner MQ Leader	<ul style="list-style-type: none"> Lacks native connectors to most database and legacy systems requiring data to be manually exported – inefficient and poses a security risk Cannot prevent leaks internal to the organisation (e.g. local email / print) Requires endpoint for some protocol enforcement Less accurate in discovery / monitoring / protection
Symantec	Enterprise focused Early Leadership Gartner MQ Leader	<ul style="list-style-type: none"> Cannot monitor or protect internal leaks, or enforce off the network Cannot protect external leaks with context (WHO and WHERE) Can lead to false positives / negatives and does not integrate with most database systems for automated fingerprint updating Requires more administrators: 1 for 10,000 users monitored
Vericept	Enterprise focused Early Leadership Focused on PCI Gartner MQ Leader	<ul style="list-style-type: none"> Includes the same weaknesses as Symantec Only protects WHAT sent HOW for email (SMTP) Many customer reports of problems with stability, scalability and support No destination awareness; only weak acceptable use policies

TARGET MARKETS

RENEWALS:

- Renewing web filtering and web security accounts with over 500 seats, especially in regulated verticals

VERTICALS:

- Finance, Retail, Manufacturing, Technology, Healthcare, Higher Education, Federal/State Government

COMPANY SIZE:

- 500+ employees; however, medium-sized companies with regulatory restrictions may be inclined to purchase

PROOF POINTS

Detection Accuracy:

- Accurately identify confidential data on the network and endpoint
- 3rd generation fingerprinting on the network and at the endpoint. It is the most accurate form of data identification for structured and unstructured data.
- Natural Language Processing enables customised policies for identification and protection of unique and / or complex forms of data.

Solution Coverage:

- Discover, monitor and protect over 400 file formats on or off the network
- Coverage for both structured and unstructured data
- Over 600 pre-defined templates for regulatory compliance, customer information and intellectual property, applicable worldwide

Policy Framework:

Intelligently map data policies to business processes for protection on the network and at the endpoint

- Who: granular monitoring and enforcement of user-based policies
- What: accurate identification of what data is being used or transmitted
- Where: destination awareness and control for monitoring and enforcement based on destination
- How: advanced protocol management, native enforcement and an open architecture for a broad array of communication channels, including: email, web, IM, USB, print, copy / paste etc.

TARGET BUYER

Primary Buyers: CSO (Decision Maker)

- Responsible for ensuring inbound and outbound policy compliance.
- Wants a solution that proactively identifies threats (internal and external).
- Responsible for developing and managing security processes.
- Wants to reduce risk amidst conflicting business priorities.
- Requires metrics to demonstrate effectiveness.

CIO (Executive Sponsor)

- Wants to enable access to information and services while maintaining an acceptable risk.
- Responsible for reducing security & compliance costs.
- Wants to reduce IT costs.
- Responsible for long-term strategy and system planning.
- Ensures that systems are future-proof.
- Improve quality of service to internal customers

PRICING

Data Security Suite is sold under a subscription model, with one, two, and three year pricing terms. Customers may purchase Data Discover, Data Monitor, Data Protect, Data Endpoint or Websense Data Security Suite. Pricing is provided by authorised resellers. Websense does not sell or distribute HP, IBM or Dell platforms.