

WEBSense
CONTENT PROTECTION
SUITE



Protecting customer and other confidential information from malicious and accidental leaks is a top business and IT security challenge facing organizations today. Compounding this problem, CIOs and CSOs must protect their information amid pressure from regulatory and corporate compliance requirements, customer and competitive pressures, and the rising cost and publicity of information leaks.

“85% of respondents report that they had a data breach involving the loss or theft of customer, consumer, or employee data in the past 24 months.”

Ponemon Institute, 2007

WebSense® Content Protection Suite is the leading solution to prevent information leaks—external and internal, accidental and malicious. WebSense Content Protection Suite discovers where information is located in a network, monitors who is using the information and how they are using it, and protects the information, securing business processes, managing risk, and assisting with compliance.

WebSense Content Protection Suite is the only information leak prevention (ILP) solution that provides content, context, and destination awareness, allowing administrators to manage who can send what information, where, and how. Using agentless discovery tools and patented PreciseID™ fingerprinting technology, WebSense Content Protection Suite automatically discovers hosts and shares inside the network—including servers and endpoints—and the data stored on them and allows administrators to create and implement content enforcement policies. WebSense Content Protection Suite goes beyond simple keyword and pattern matching solutions; it provides Deep Content Control™ to discover, monitor, and protect confidential information, including personally identifiable information (PII), regulatory data, and intellectual property (IP), regardless of the file type or format.

Discover, monitor, and protect who can send what information where and how with Content Protection Suite.			
	Discover	Monitor	Protect
Who	Automatically integrate with existing directory services to enable lookups for granular user activity detail	Create customized reports for regular activity by location, group, and/or user, and analyze usage trends	Create policies, automate workflows, and manage incidents forensically in real-time
What	Automatically discover structured and unstructured data with agentless classification tools	Report on data usage and accurately monitor business processes to examine what data is in use and by whom	Secure confidential information by creating granular policies to restrict the use of sensitive data to its intended group of users
Where	Identify where data is stored in the network and combine with web intelligence to uncover the type of website to which it is being sent	Evaluate business processes to determine if data is in breach of compliance requirements and refine data security policies accordingly	Enforce policies based on decision-ready destination intelligence, e.g., prevent any information from being sent to compromised websites
How	Determine contextual content awareness by understanding how data is used by whom, its format, and location	Examine a broad range of communication channels (e.g., web, email, IM, print, etc.) and protocols, regardless of the port used	Protect data with automated controls on who sends what information where, and how, encompassing both internal and external communication

WEBSense CONTENT PROTECTION SUITE



Discover

Websense Content Protection Suite discovers information, applications, and protocols throughout the network—in data repositories, file shares, whether on servers or endpoints. Armed with the knowledge of where data is, organizations can identify broken business processes, create efficient workflows, and establish policies to protect confidential information.

PreciseID, included with Websense Content Protection Suite, is a third generation data fingerprinting technology that goes far beyond simple keyword, pattern matching, and regular expression engines. PreciseID accurately fingerprints both structured and unstructured data regardless of file type or format. Websense Content Protection Suite creates multiple fingerprints per file via a one-way mathematical representation, analyzing the content within the document so that it can monitor and protect the data no matter how it has been manipulated. PreciseID provides the industry's lowest rate of false positives and false negatives by using multiple detection methods for in-depth data analysis, correlating relational data points as well as metadata. This gives organizations decision-ready information they can act on.

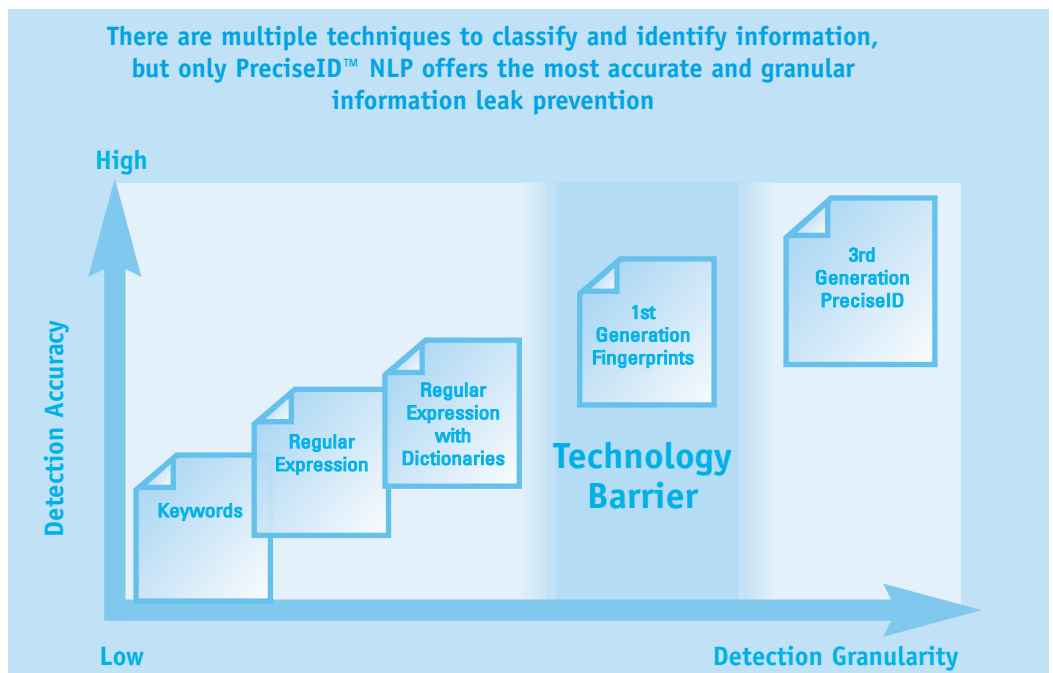
Websense Content Protection Suite fingerprints information from most databases and analyzes hundreds of megabytes each minute. Its sophisticated algorithms can distinguish if a Social Security number belongs to a customer or an employee, allowing organizations to implement data protection policies that are relevant to specific business processes. Websense Content Protection Suite also covers a broad range of unstructured data, including financial data, software source code, business plans, and product designs. It categorizes the content by its type, risk, and/or applicable state/federal regulation. These capabilities enable IT departments to establish enforceable security policies, in line with business requirements.

"Websense should be on the shortlist of any enterprise that requires comprehensive CMF/DLP functionality."

Gartner Magic Quadrant for CMF/DLP, 2Q07

"[Websense] focus on enforcement really makes a difference."

Network Computing



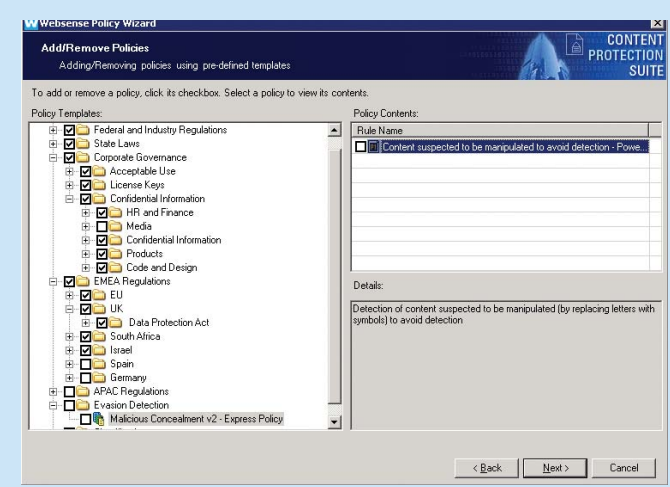


Monitor

Websense Content Protection Suite provides real-time monitoring of your information controls whether information resides on a server or an endpoint, is transferred to a USB or optical drive, or is sent by email, FTP, HTTP, or printed.

Websense Content Protection Suite passively monitors most business communications—both external and internal—including a wide range of protocols such as email, network printing, FTP, HTTP and HTTPS, and instant messaging (IM). Administrators can identify what information is being used, where it is being transmitted, and by whom from a centralized management and reporting console.

Websense has the only information leak prevention solution that includes a robust data analysis engine that integrates with directory services and Web intelligence solutions to provide in-depth reporting of users, groups, and destinations. It includes intelligent protocol discovery to detect protocol communications regardless of port, and automatically categorizes incidents by type, regulation, and severity to provide valuable insight into regulatory compliance and corporate governance incidents. Powerful forensics and distributed analysis technology allows sharing of remediation tasks across large, decentralized organizations for better efficiency, while core policy decisions are administered centrally.



The screenshot shows the 'Websense Policy Wizard' window. The title bar reads 'Websense Policy Wizard' and 'CONTENT PROTECTION SUITE'. The main window is titled 'Add/Remove Policies' and contains a tree view of 'Policy Templates' on the left and a 'Policy Contents' pane on the right. The tree view includes categories like 'Federal and Industry Regulations', 'State Laws', 'Corporate Governance', 'Acceptable Use', 'License Keys', 'Confidential Information', 'HR and Finance', 'Media', 'Confidential Information', 'Products', 'Code and Design', 'EMEA Regulations', 'EU', 'UK', 'Data Protection Act', 'South Africa', 'Israel', 'Spain', 'Germany', 'APAC Regulations', 'Evasion Detection', and 'Malicious Concealment v2 - Express Policy'. The 'Policy Contents' pane shows a table with one row: 'Content suspected to be manipulated to avoid detection - Powe...'. Below this is a 'Details' section with the text: 'Detection of content suspected to be manipulated (by replacing letters with symbols) to avoid detection'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

"The average data breach costs companies \$5 million."

Network World, 2006

Websense Content Protection Suite includes over 150 pre-defined policies for out-of-the-box auditing enforcement.

