Unified data loss prevention for gateways, endpoints and discovery.

From tarnished brand reputation to regulatory fines, the adverse impacts of data breaches are clear. Just a single incident of data loss can erode a business’s competitive advantage, weaken consumer confidence and result in fines or penalties from regulators. The problem is exacerbated by the rapid proliferation of mobile devices, widespread use of peripheral devices, and easy access to file-sharing software — all increase the risk of data loss and data theft.

Why is Websense the best choice?

Websense® Data Security Suite secures against a wide range of data loss scenarios. It provides a single policy framework for network and endpoint data loss prevention (DLP) and confidential data discovery.

- Easily adopt an expandable solution to prevent inbound threats and manage outbound risks associated with data loss and regulatory compliance.
- Over 1,700 predefined policies and templates, categorized by region and industry, simplify policy creation.
- Websense Data Identification and Classification Engine (DICE) is also embedded within web and email security gateways solutions under the unified Websense TRITON™ architecture.

Data Security Suite is comprised of the following modules – which are also available individually to provide the highest level of deployment flexibility:

- **Websense Data Security Gateway**: Monitors common network communication channels such as web and email, FTP, ActiveSync for mobile email and more. When sensitive data is found, Data Security Gateway can block its transmission, log the incident or automatically run a remediation action.

- **Websense Data Endpoint**: Monitors real-time traffic and extends visibility and control over where confidential data is allowed to migrate; who is using it; how it is being used; where it is being transferred; and what real-time action is taken to prevent data loss at the endpoint.

- **Websense Data Discover**: Accurately identifies confidential data, using DICE’s rich set of three data classifiers (described, registered, learned) to give you the most insight into your data.

Reduced Cost and Complexity

- Easy integration with existing network infrastructure.
- One console to centrally manage web, email and DLP security policies.
- 1700+ predefined policies and templates categorized by region and industry.
- Protect IP with advanced data classifiers and natural language processing.
- Manage incidents via email notification.

“Websense Data Security Suite gives us deep visibility into how information is used within our organization, so we can apply the right protection policies to our sensitive and regulated data.”

Matt Tucker, Vice President of IT
Omniamerican Bank
The Websense difference: DICE
(Data Identification and Classification Engine)

Websense DICE combines rich classifiers with real-time contextual awareness of user, data and destination to provide high accuracy and consistent data loss prevention throughout the TRITON architecture. DICE supports three data categories: described, registered and learned. Described data includes regular expressions, dictionaries and natural language classifiers including over 1700 policies and templates. Registered data includes fingerprinting, which can be compressed and stored on the endpoint for off-network protection. Learned data is advanced machine learning technology that employs algorithms to analyze small samples of data to fill the gap between described and registered data for higher accuracy and efficiency. Data theft protection capabilities includes OCR of text within images, detection of custom encrypted files and password file theft, slow data leaks and geo-location awareness. DICE is ubiquitous for discovery, gateways and endpoints with policy management from a single console.

<table>
<thead>
<tr>
<th>Your Needs</th>
<th>Websense Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistent policy creation</td>
<td>1700+ pre-defined policies and templates, categorized by region and industry, enable you to write one policy and apply it across endpoint, network and data repositories. Templates are regularly updated and reviewed by dedicated Websense researchers.</td>
</tr>
<tr>
<td>Protect data stored in images</td>
<td>Only Websense offers OCR of text within images for discovery, monitoring and prevention.</td>
</tr>
<tr>
<td>Simplified and unified architecture for ease of use and lower TCO</td>
<td>Data Security Suite is fully integrated with the TRITON architecture. DICE is universal in all DLP capabilities and unified across all TRITON solutions. Data Endpoint, Data Security Gateway and Data Discover share a single administrative interface.</td>
</tr>
<tr>
<td>Simplified workflow</td>
<td>Websense simplifies workflow by allowing administrators to manage incidents by replying to email notifications.</td>
</tr>
<tr>
<td>Centralized incident management and reporting</td>
<td>Distribute executive or detailed reports showing total number of incidents by device/application channel, user group, policy, regulation, enforcement action taken and more. Show status of compliance efforts.</td>
</tr>
<tr>
<td>In-depth understanding of the data leaving your network</td>
<td>Source and destination awareness, combined with Websense classifiers, enable you to understand who is accessing what kind of data, how it is being used and where it is being transferred -- so your organization can make the most informed policy decisions in real time, and craft effective policies for the future.</td>
</tr>
<tr>
<td>Protect data from sophisticated, slow data leaks</td>
<td>Websense offers another industry first with Drip DLP, which monitors slow data loss over cumulative events to protect your data from slow leaks.</td>
</tr>
<tr>
<td>Ease of deployment and administration</td>
<td>Websense offers one unified console for gateway, endpoint and discovery for ease of management of DLP policies, incidents and reporting.</td>
</tr>
</tbody>
</table>

Mobile, social, and cloud technologies drive productivity. But they also open the door to data theft and advanced attacks that can slip right by anti-virus, URL filtering and firewall defenses. Websense® TRITON™ solutions keep you a step ahead with web, email, data, cloud and mobile security solutions (available together or separately) that share a common architecture. The real-time defenses of Websense ACE (Advanced Classification Engine), plus flexible deployment options and a unified management console, make TRITON solutions vital in today's dynamic environments.

Learn more at www.websense.com  |  +1 800-723-1166  |  info@websense.com

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

© 2013 Websense, Inc. All rights reserved. Websense and Threatseeker® Intelligence Cloud are registered trademarks of Websense, Inc. in the United States and certain international markets. TRITON, X-Series, X10G, and Websense Security Labs are trademarks of Websense, Inc. in the United States and other countries. Websense has numerous other registered and unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owner. Specifications are subject to change. 05-13-2013 EN