Websense® DataEndpoint

DATASHEET

Secure data outside the dissolving perimeter.

The traditional security perimeter has dissolved as the modern workforce has become increasingly mobile. Studies show that Drive Media/USB is the second highest ranked breach vector for data theft. Enterprises must meet the security challenge that accompanies the productivity needs of the mobile worker. The ability to identify and secure confidential data as it migrates from protected environments onto endpoint devices is key.

Why is Websense the best choice?

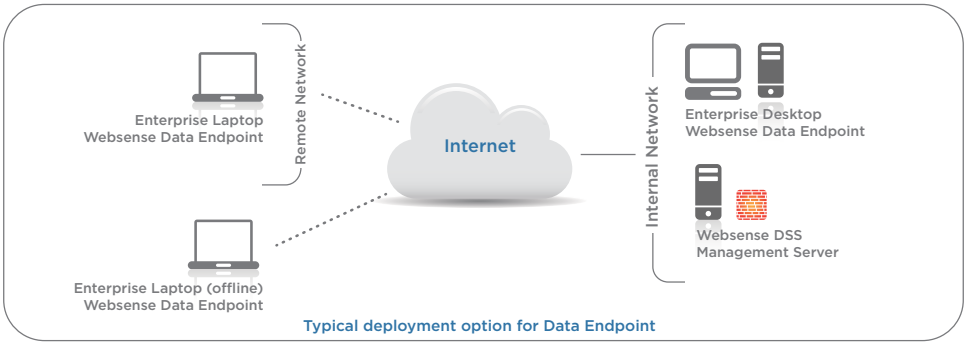
Websense® Data Endpoint is a comprehensive, secure and easy-to-use endpoint data loss prevention (DLP) solution. Data Endpoint monitors real-time traffic and extends visibility and control over where confidential data is allowed to migrate; who is using it; how it is being used; where it is being transferred; and what real-time action is taken to prevent data loss at the endpoint. Data Endpoint allows security administrators to either block or monitor and log files that present a policy breach. Forensic monitoring enables the creation of policies that allow full visibility of content traffic and contain data loss at the endpoint without restricting device usage.

Advanced Defenses

- Data Endpoint is the industry's first and only endpoint solution to support MAC OS X and Windows.
- Fingerprints are compressed onto the endpoint to enable true off-network endpoint protection.
- Data Endpoint is built on an open architecture, and includes an integrated policy framework with Websense Data Security Suite for centralized management and reporting of both network and endpoint data policies in a single, comprehensive DLP solution.

Granular Policy and Endpoint Control

- Automated policy enforcement allows enterprises to log/audit, block, ask confirmation from user, and notify administrators when confidential information is copied to removable devices.
- Unrivaled visibility and control over cut and paste, file access, screen capture, and print for client software applications, endpoints and peripheral devices.



Typical deployment option for Data Endpoint

PROTECTIONS
WEB ☐ EMAIL ☐ DATA ☑

PLATFORMS
SOFTWARE ☑ APPLIANCE ☐ CLOUD ☐ HYBRID ☐

Advanced Defenses

- Off-network protection.
- Supports MAC OS X and Windows.
- Portable decryption for USBs and portable media.
- Automated policy enforcement.
- Monitors data transferred onto Android smartphones

Improved Protection

- Block confidential data from being moved onto unapproved devices.
- Monitor or block Print Screen operations of confidential data.
- Encrypt sensitive information copied to removable devices.
- Protect fingerprinted data even when the endpoint is off network.

Improve Process Flow

- Enable end user self-remediation with administrator auditing.
- Enable incident work flow through email notifications.
- Enable both Data Endpoint and Cloud Web Security Gateway agents for complete advanced threat and data theft protection.

"Websense Data Security Suite alerts told us when sensitive data was moved or sent out of the organization."

-Amir Shahar
Information Security Manager
Cellcom Israel

websense® TRITON™

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.

Websense Data Endpoint uses DICE to classify data in a contextually aware manner.

Your Needs	Websense Solutions
Protect your data while employees work off network	Websense advanced machine learning allows for the fingerprinting of large amounts of data with ease. Fingerprints are compressed and stored on the endpoint for true off-network endpoint protection.
Automated enforcement options including device control	Keep your employees productive and your data secure with flexible enforcement options such as block/move/copy/print device to application, block screen print, user notification, user confirmation and audit/logging. Allow legitimate use of device if data is not confidential with data-centric device control.
Visibility into device, application, and storage of confidential data on end-user systems	Device monitoring and control of removable storage, external hard drives, printing, burning to CDs/DVDs, copy/paste/screen print to clipboard and file access. Discovery by file type, size, age; ad-hoc or scheduled; full or differential scan. Classification by regulated data type such as credit card numbers.
Ease of deployment and administration	Websense offers one unified console for gateway, endpoint and discovery for ease of management. Plus self-release remediation and update processes with admin auditing, and work flow through mail notifications.
Allow employees to use USBs and portable media while securing your data	Portable decryption for USBs and portable media requires the user to supply a password before copying sensitive files to removable devices.
Extend your endpoint coverage to Mac OS X	Websense is the first and only in the industry to extend data endpoint protection to Mac OS X.
Simplified and unified architecture for ease of use and lower TCO	DICE is universal in all DLP capabilities and unified across all TRITON architecture.

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.

websense® TRITON™