

safend inspector

Content Inspection and Filtering

Preliminary



- Prevent sensitive data leakage through Email, Web, removable storage, and additional data transfer channels
- Avoid user errors and enhance security awareness
- Enable compliance with regulatory, data security, and privacy standards
- Deploy and manage a single agent for all data protection needs

Safend Data Protection Suite

Control all your data protection measures with a **single** management server, a **single** management console and a **single** lightweight agent.

Instantly Assess your current security status with **Safend Auditor**

Precisely Control physical ports and devices with **Safend Protector** and sensitive outbound data with **Safend Inspector**

Transparently Protect your laptops, desktops and removable media with **Safend Encryptor** and Safend Protector Removable Media Encryption

Easily Monitor your security and operational status with **Safend Reporter**

Centrally Manage all security features with Safend's enterprise grade management infrastructure



The Need for Endpoint Content Control

Industry statistics consistently show that the most significant security threat to the organization comes from within. With over 60% of corporate data residing on endpoints, gateway solutions and written security policies alone can not mitigate the risk.

Sensitive data can exit organizational boundaries through multiple channels; it can be carried away on a USB flash drive, burned to a CD, sent via email or posted on the web. While some data transfer channels can be partially disabled to minimize the risk, few organizations can completely disable outbound data traffic without dramatically affecting productivity. To properly balance security and compliance demands with business objectives, enforcement measures must be carefully adjusted to control only the specific data restricted by company policy, without interrupting legitimate user actions.

“The Transportation Security Administration is warning 1,195 of its former employees that a contractor may have mailed their Social Security numbers and birth dates to the wrong addresses and left them open to identity fraud.”
USA Today

“Average cost per data breach incident was \$6.6M and the cost per record was \$202 in 2008.”
Ponemon Institute

“Information breaches trigger an average 5% drop in company share prices. Recovery to pre-incident levels takes nearly a year.”
EMA Research

Safend Inspector - Eliminate Sensitive Data Leakage

Safend Inspector enforces a data-centric security policy across multiple channels, including email, web (HTTP, HTTPS), FTP, external storage devices, CD/DVD burners, PDA devices, file repositories, print screen, local printers, and network printers, without disrupting legitimate business processes or harming end user productivity.

User actions can be stopped, generate an “are you sure?” message, monitored, or generate an alert for the security administrator, based on the actual content of the transferred data as well as the action context and meta data. This protection is fully active regardless if the machine is connected to the organization's network, a home network or used offline.

Security policies are highly granular, and can apply different protection measures according to channel specific context information. For example, a security policy can prevent users from downloading confidential data to external storage devices other than company issued hardware-encrypted devices.

Safend Inspector - Features and Benefits

Comprehensive Protection

Enforces a data-centric security policy across multiple channels, regardless if the machine is connected to the organization's network, a home network or used offline. Additional channels can be added upon demand using Application Data Access Control.

Accurate Data Classification

Multiple data identification techniques can be combined for highly accurate data classification.

Built-in Compliance Policies

Includes preconfigured security policies designed to address specific regulatory compliance standards, such as PCI, HIPAA, and Basel-II.

Rich End User Interaction

Security policies can mandate users to provide justifications for problematic actions. Such a policy can quickly and accurately close the enforcement loop and help users avoid potentially harmful actions without disrupting business processes.

Full Visibility and Audit Trail

Receive detailed logs and reports on security incidents and administrative actions.

Highly scalable

A single management server can manage more than 75,000 agents. Additional servers can be seamlessly added to create a server cluster.

Tamper Resistant

The agent includes multi-tiered anti-tampering capabilities to guarantee permanent control over enterprise endpoints.

Flexible and intuitive management

Automatically synchronizes with Microsoft Active Directory and Novell eDirectory.

Technical Specifications

Controlled Network Channels

- ✓ Email
- ✓ Web (HTTP / HTTPS)
- ✓ Network Printers
- ✓ File Shares
- ✓ FTP

Controlled Endpoint Channels

- ✓ Removable Storage Devices
- ✓ External Hard Drives
- ✓ CD / DVD
- ✓ Local Printers
- ✓ Screen Capture
- ✓ Application Channels (custom)

Certification

- ✓ Common Criteria EAL2 certified
- ✓ FIPS 140-2, "Coordination" phase

System Requirements - Agent

- ✓ Windows XP Professional
(All Service Packs)
- ✓ Windows Vista Enterprise, Business
and Ultimate Editions (SP1)

System Requirements - Server

- ✓ Windows 2003 (All Service Packs)
- ✓ Windows XP Professional (SP2, SP3)
for evaluation only

This preliminary document highlights the functional content of a future Safend product release. All details in this document are provisional and may change without notice. None of the information in this document should be interpreted as a commitment on the part of Safend.

About Safend

Safend is a leading provider of endpoint data protection software. Our products protect against corporate data loss by offering comprehensive data encryption, port control, device control and content inspection, ensuring compliance with regulatory data security and privacy standards. Safend's products encrypt internal and external hard drives, removable storage devices and CD/DVDs; provide granular port and device control over all physical, wireless and removable media devices; and controls sensitive data transferred over endpoint and network channels. With more than 1,200 customers worldwide and 1.7 million licenses sold, Safend's software is deployed by multinational enterprises, government agencies, healthcare organizations, and small to mid-size companies across the globe.



Safend Ltd. 32 Habarzel Street, Tel-Aviv 69710, Israel Tel: +972.3.6442662, Fax: +972.3.6486146
Safend Inc. 2 Penn Center, Suite 301, Philadelphia, PA 19102, USA Tel: +1.215.496.9646, Fax: +1.215.496.0251
Safend S.A. 5, Avenue Gaston Diderich L-1420, Luxembourg Tel: +352 26 87 08 67, Fax: +352 26 87 08 68
Toll free from the US (to US and Israel): 1.888.225.9193 info@safend.com

www.safend.com

Copyright © 2009 Safend Ltd. The information contained herein is accurate at the time of publishing and subject to change without notice. 04/09