

safend reporter

Comprehensive Reporting and Analysis



- Enable compliance with regulatory, data security, and privacy standards
- Identify common security breaches by user or organizational units
- Analyze reports at a high level or detailed view
- Monitor all your data protection measures with a single software

Safend Data Protection Suite

will protect your organization against endpoint data loss, misuse or theft through its single server, single console, single agent architecture. The award winning suite includes:

Safend Auditor - immediately recognize security risks by identifying WiFi ports or devices currently or historically connected to endpoints.

Safend Discoverer - locate and map sensitive data at rest.

Safend Inspector - inspect, classify and block leakage of sensitive content through email, IM, Web, external storage, printers and more.

Safend Encryptor - transparently encrypt laptops and PC's.

Safend Protector - block or encrypt data transferred to external media and devices (CD/DVD, USB, Firewire, etc.) and block connections to unsecure wireless networks.

Safend Reporter - easily generate graphical regulatory compliance reports and security log summaries through an intuitive tool.

Endpoint Data Protection - The Demand for Comprehensive Reporting

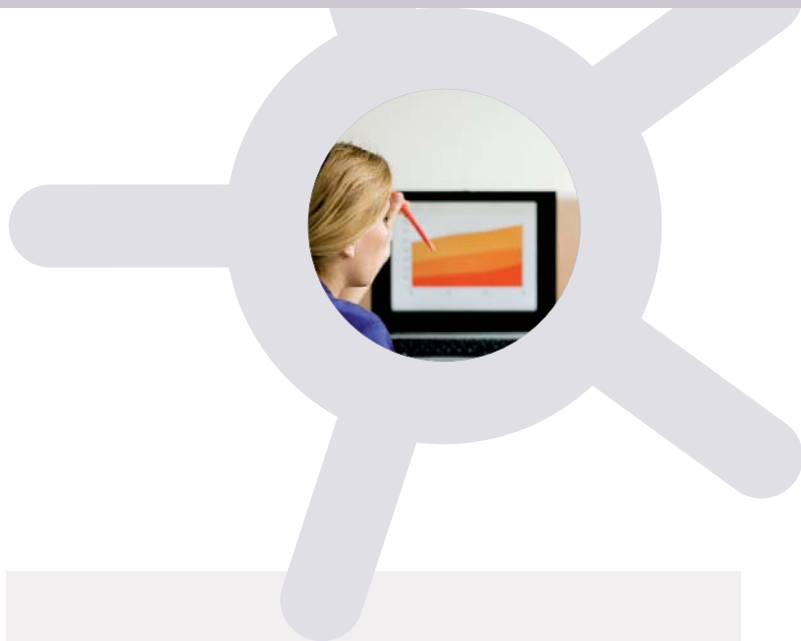
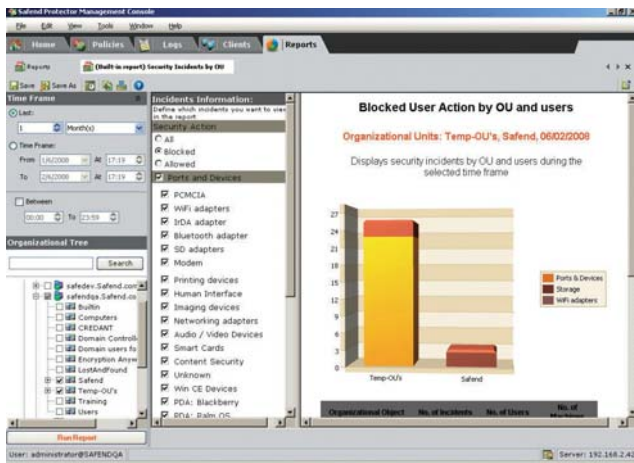
With the regulatory compliance reporting mandates of Sarbanes Oxley, (SOX), HIPAA, PCI, FISMA, BASEL II, UK Data Protection Act (DPA) and others, the effective use of data security intelligence has become increasingly important and the need for comprehensive reporting is more prevalent than ever.

Safend Reporter - A Heightened Level of Visibility

Safend Reporter is a component of the **Safend Data Protection Suite** that addresses the security and operational reporting needs of an organization's IT and security personnel. **Safend Reporter** presents information in a clear, easy to understand dashboard format that can benefit all viewers including non technical and executives, through drill-down capabilities.

Safend Reporter allows easy detection of specific employees and departments that frequently disregard internal security policies, while the administrative reports assist in the deployment, policy distribution and overall visibility of endpoint activity within the organization. The reports can be scheduled and sent periodically by email to predefined recipients in order to ensure continuous tracking of the organization's data security status and compliance to internal security policies. Coupled with Safend Protector's built-in compliance policy settings for HIPAA, PCI and SOX, **Safend Reporter** provides unparalleled regulatory compliance reporting that helps meet the data accountability tenets of these and other compliance standards.





Key Features

- Security incidents by Users and Organizational Units**
 Allows Safend Administrators to view which Organizational Units, specific users and computers are violating the corporate security policies or committing an extraordinary number of “allowed but suspicious” activities. This detailed information highlights unusual events and uncovers malicious or reckless user behavior.
- Security Incident Types**
 Provides the administrator an overview of the most common security incidents within the organization. This report highlights problematic procedures and work practices that should be addressed.
- Policy Distribution**
 Enables administrators to view the entire range of security policies applied on the organization and its overall security policy. It also helps identify endpoints that do not have a valid policy applied to them.
- Deployment Status**
 Allows administrators to view the progress of Safend Agents deployment across the enterprise. The report shows the percentage of the organization’s endpoints protected by the Safend Agent and provides a detailed list of the endpoints not yet protected.

- Encryption Status**
 Provides both a high level overview and detailed information on endpoints encryption status.
- Device Inventory**
 Generates a detailed list of all physical devices that were used within a defined time frame. These devices can be copied to a policy White List in Safend Protector in order to simplify the policy creation process.
- Drill-Down Options**
 Provides drill-down capabilities for a detailed analysis of a report. Administrators can easily investigate suspicious patterns by navigating from a high level view of the organization to specific incident details and the relevant log entries.
- Export Reports**
 Allows reports to be viewed from within the Management Console or exported to one of several popular formats for viewing and analysis outside of the Console.
- Schedule Reports**
 Runs reports periodically and sends results via email to predefined recipients. This facilitates the continuous tracking of the organization’s security status.

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 1,800 customers worldwide and 2.5 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