

# safend reporter

## Comprehensive Reporting and Analysis



- Enable compliance with comprehensive security and operational reporting
- Identify common security breaches by user or groups
- Analyze reports at a high level or detailed view

### Endpoint Data Leakage | 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's endpoint Data Leakage Prevention solutions (DLP) provide granular control over every potential endpoint leakage channel and Safend Reporter provides the visibility and analysis tools organizations need to stay ahead of data security and compliance reporting requirements.

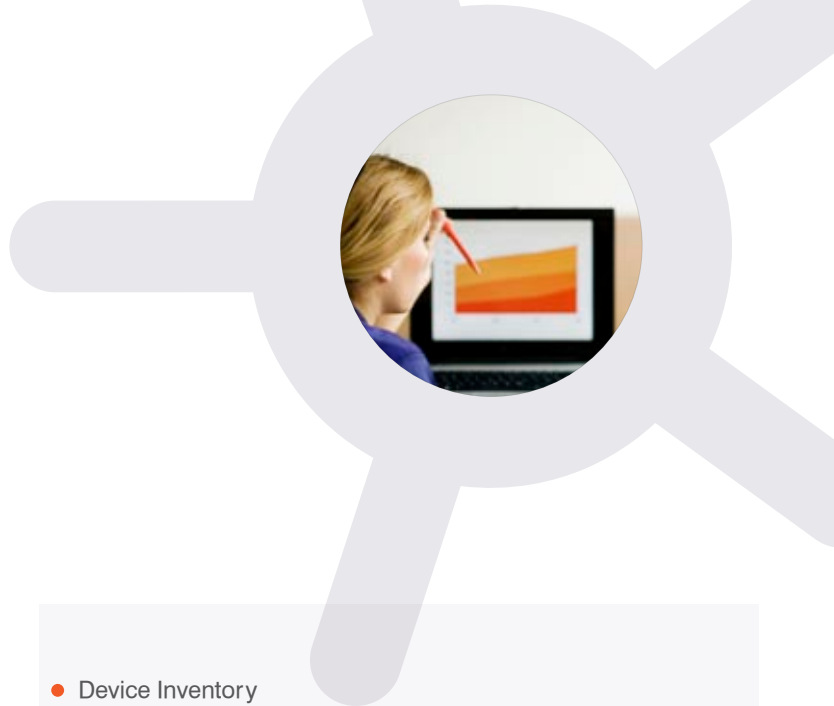
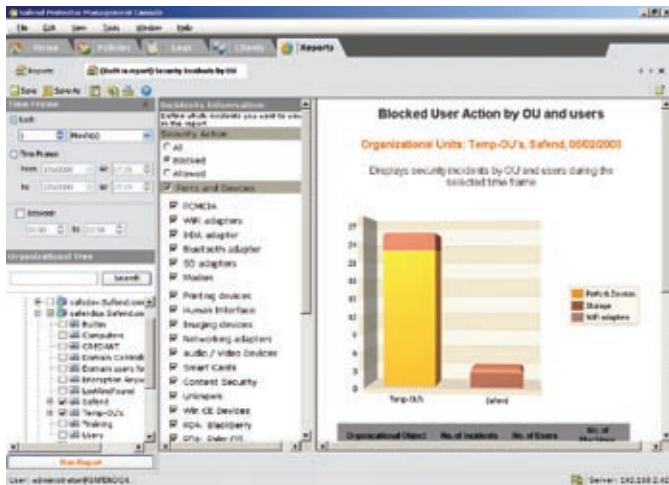
organization. The reports can be scheduled and sent periodically by email to predefined recipients in order to ensure continuous tracking of the organization's data security status and compliance to internal security policies. Coupled with Safend Protector's built-in compliance policy settings for HIPAA, PCI and SOX, Safend Reporter provides unparalleled regulatory compliance reporting that helps meet the data accountability tenets of these and other compliance standards.

### Safend Reporter | A Heightened Level of Visibility

Safend Reporter is an add-on module to Safend Protector that provides a new level of visibility to the Safend protected organization, addressing the security and operational reporting needs of an organization's IT and Security personnel. The reporting tool 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 delivers detailed reports to data security personnel within the organization.

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





## 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 the Safend Protector Client deployment across the enterprise. The report shows the percentage of the organization's machines protected by the Safend Client and provides a detailed list of the machines not yet protected.

- 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 feature facilitates the continuous tracking of the organization's security status.

**Safend Reporter is an add-module to Safend Protector and requires the purchase of an additional license.**

## About Safend

Safend is a leading provider of endpoint data leakage prevention solutions that protect against corporate data loss via physical, wireless and removable media ports while ensuring compliance with regulatory data security and privacy standards. With more than 700 customers worldwide and 1.5 million licenses sold, Safend's solutions are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe. Founded in 2003, Safend is a privately held company funded by Elron Electronics (NASDAQ and TASE: ELRN), Intel Capital and Walden Israel. Safend is headquartered in Tel Aviv with U.S. headquarters in Philadelphia. For more information, visit [www.safend.com](http://www.safend.com).