

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.

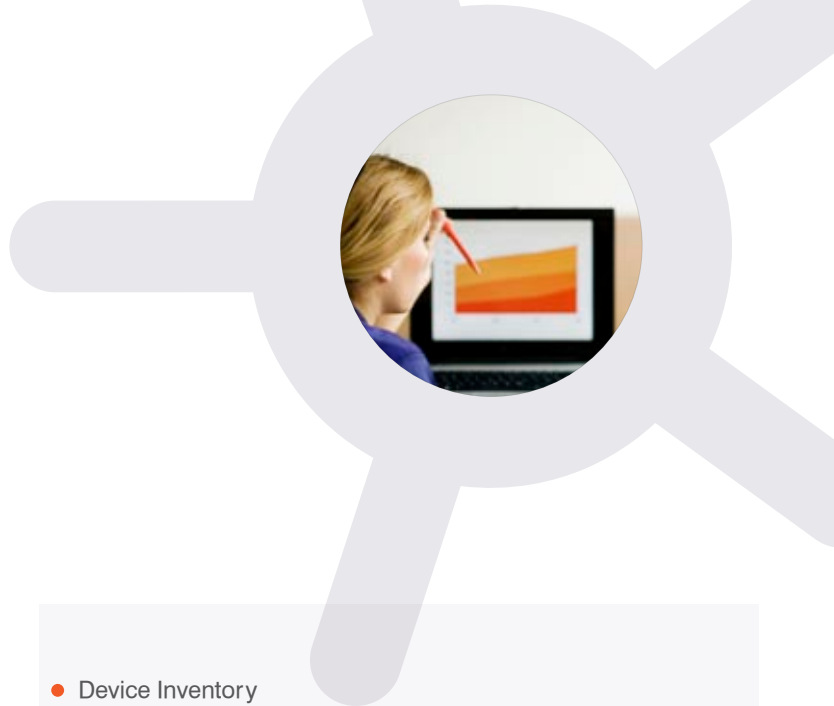
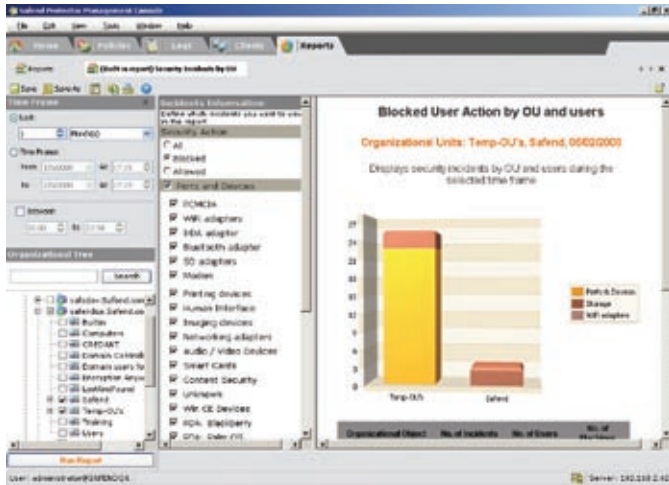
organization. The reports can be scheduled and sent periodically by email to predefined recipients in order to ensure continuous tracking of the organization's data security status and compliance to internal security policies. Coupled with Safend Protector's built-in compliance policy settings for HIPAA, 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.

safend auditor

Comprehensive Endpoint Visibility



- Comprehensive visibility of who's connecting what to corporate endpoints
- Visibility over all USB, PCMCIA, FireWire and WiFi ports
- Granular record of all current and past device connections
- Quick ramp-up, zero overhead, short learning curve
- Simple and powerful reporting

Endpoints | What You Can't See Can Hurt You

In the world of security, the unknown is always the greatest threat. In the realm of endpoint data leakage prevention, this threat is multiplied by thousands – and often tens of thousands - of individual ports, interfaces, and devices that connect to networks every day.

With an estimated 60% of sensitive corporate data residing on these endpoints (IDC), and data loss via removable media harming more than 50% of companies (Forrester research)- today's network administrators and security officers are getting up close and personal with endpoints.

They're looking for detailed, high-resolution visibility of actual individual endpoint activity - ongoing and historical. Because only through an in-depth understanding of what's happening at the endpoint can security professionals define and enforce endpoint security policies that are in-line with real-world usage.

Safend Auditor | Knowledge is Power

Safend Auditor gives administrators the power to discover who's connecting what devices to each and every corporate PC.

A lightweight, intuitive, clientless software utility, Safend Auditor illuminates enterprise endpoint blind spots – providing organizations with the visibility necessary to identify and effectively manage endpoint vulnerabilities.

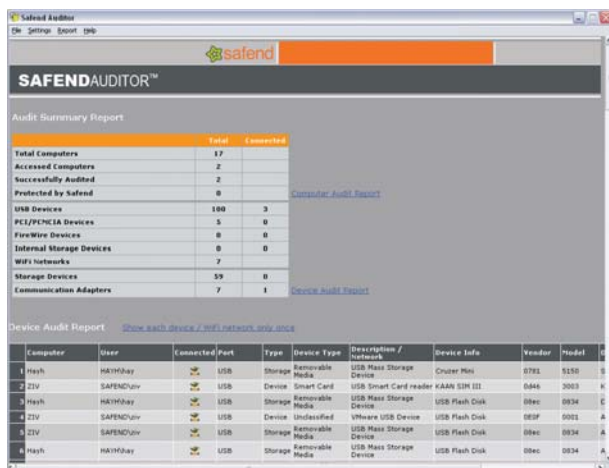
With Safend Auditor, administrators can differentiate between secure productivity enhancers, such as authentication tokens, and potential security threats, such as mass-storage MP3 players. Safend Auditor also tracks which WiFi networks employees are connecting to - secure encrypted networks or exposed public networks. Using data gathered by Safend Auditor, administrators can map out granular security policies that exactly meet their business needs.



FREE trial at
www.safend.com

Rapid Scanning of All Network Endpoints

With no endpoint client installation required, Safend Auditor transparently and rapidly queries all organizational network endpoints, locating and documenting all devices that are or have been locally connected. Safend Auditor checks all USB, PCMCIA, FireWire, and WiFi ports – granularly identifying endpoint devices connected for each user, both currently and historically.



The screenshot shows the Safend Auditor interface. The top section is the 'Audit Summary Report' with a table showing counts for various device categories. The bottom section is the 'Device Audit Report' table, which lists individual devices with columns for Computer, User, Connected, Port, Type, Device Type, Description / Network, Device Info, Vendor, and Model.

	Total	Connected
Total Computers	17	
Accessed Computers	2	
Successfully Audited	2	
Protected by Safend	0	
USB Devices	180	3
PC/PCMCIA Devices	5	0
FireWire Devices	0	0
Internal Storage Devices	0	0
WiFi Networks	7	
Storage Devices	59	0
Communication Adapters	7	1

Computer	User	Connected	Port	Type	Device Type	Description / Network	Device Info	Vendor	Model
1	Hash	HA1Mh4y	USB	Storage	Removable Media	USB Mass Storage Device	Cruzer Mini	0781	5150
2	23V	SAFENDuliv	USB	Device	Smart Card	USB Smart Card reader	KAAH S3H 031	0846	2003
3	Hash	HA1Mh4y	USB	Storage	Removable Media	USB Mass Storage Device	USB Flash Disk	080c	0834
4	23V	SAFENDuliv	USB	Storage	Unclassified	Virtual USB Device	USB Flash Disk	080F	0001
5	23V	SAFENDuliv	USB	Storage	Removable Media	USB Mass Storage Device	USB Flash Disk	080c	0834
6	Hash	HA1Mh4y	USB	Storage	Removable Media	USB Mass Storage Device	USB Flash Disk	080c	0834

Easy to Understand Reports

The results of the Safend Auditor audit are viewable in HTML format, or as an XML table that is easily exported to Excel or other applications for additional analysis and review. The report identifies devices by type, manufacturer, model and serial number, and users according to their Active Directory definitions.

Safend Auditor Advantages

- **Simple and easy to use**
Administrators simply choose the group of computers to audit, and view the results immediately
- **Comprehensive coverage**
Identifies all USB, FireWire, and PCMCIA devices, and WiFi network connections
- **Current and historical audits**
Reports all devices currently or previously connected to any endpoint
- **Precise device identification**
Gathers detailed device information, allowing tailoring of security policies to exact vulnerabilities
- **Clientless**
Runs without endpoint client
- **Low resource consumption**
Audits take minutes and do not affect network performance
- **Intuitive output**
Audit results presented in easy-to-read HTML or XML report, easily exportable to MS Excel
- **Seamless compatibility**
Fully compatible with existing network management or administrative tools such as Active Directory
- **Endpoint specific audits**
Easy auditing of selected endpoints, Active Directory groups, IP address ranges, or the entire enterprise

Endpoint Control | Integration With Safend Protector

Safend Protector is the industry's most comprehensive, secure and easy-to-use endpoint data leakage prevention solution - controlling every endpoint and every device, over every network or interface. Seamlessly integrated with Safend Protector, Safend Auditor allows easy transfer of devices discovered in audits to Safend Protector's "whitelist" of approved devices.

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.



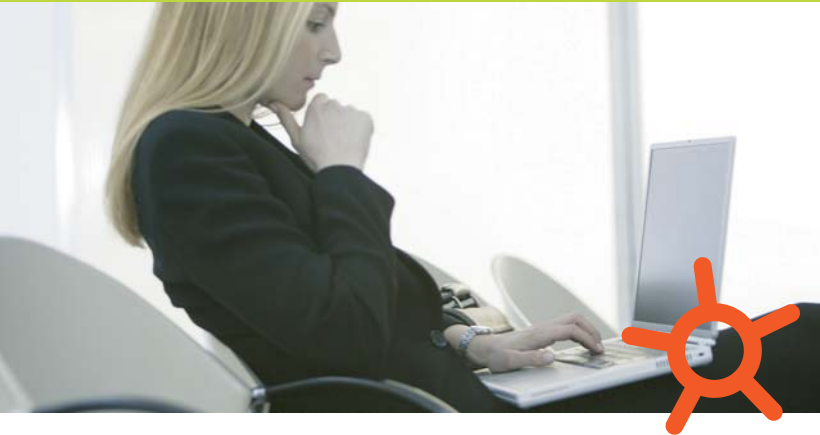
Safend Ltd. 32 Habarzel Street, Tel-Aviv 69710, Israel Tel: +972.3.6442662, Fax: +972.3.6486146

Safend Inc. 2 Penn Center, Suite 301, Philadelphia, PA 19102, USA Tel: +1.215.496.9646, Fax: +1.215.496.0251

Toll free from the US (to US and Israel): 1.888.225.9193 info@safend.com

safend protector

Robust Endpoint Data Leakage Prevention



- Protect your enterprise from data leakage and theft
- Eliminate targeted attacks via physical and wireless interfaces
- Enable connectivity and productivity without compromising security
- Enable compliance with regulatory data security and privacy standards

Endpoint Data Leakage | Challenges and Risks

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.

Growing numbers of removable storage devices, physical and wireless interfaces and users with access to sensitive information have made data leakage via endpoints – both accidental and malicious - a very real threat. It's simply too easy for someone to connect a MP3 player, digital camera, or memory stick to an enterprise endpoint and walk away with sensitive material. It's just as easy to use WiFi or a 3G modem to bridge classified internal networks to open external networks.

Stop Data Leakage through Endpoints and Removable Media

Safend Protector is the industry's most comprehensive, secure and easy-to-use endpoint data leakage prevention solution - controlling every endpoint and every device, over every interface.

Safend Protector monitors real-time traffic and applies customized, highly-granular security policies over all physical/wireless interfaces and external storage devices:

PHYSICAL INTERFACES	WIRELESS INTERFACES	STORAGE
<ul style="list-style-type: none">● USB● FireWire● PCMCIA● Secure Digital (SD)● Parallel● Serial● Modem● Internal Ports	<ul style="list-style-type: none">● WiFi● Bluetooth● Infra Red (IrDA)	<ul style="list-style-type: none">● Removable Storage Devices● External Hard Drives● CD / DVD Drives● Floppy Drives● Tape Drives

Safend Protector detects and allows the restriction of devices by device type, model or even specific device serial number. For storage devices, Safend Protector allows security administrators to either block all storage devices completely, permit read-only and encrypt all data. It also monitors, blocks and logs files that are downloaded to or read from these devices. WiFi controls are based on MAC address, SSID, or network security level.

Security Policy | Flexible Strategy, Simple Implementation

Safend understands that different organizations have different needs and different corporate cultures. That's why Safend Protector allows administrators to first choose their endpoint security strategy, and then implement it in line with their unique organizational needs.

Safend Protector creates forensic logs of all data moving in and out of the organization, allowing administrators to create policies that don't necessarily restrict device usage, but allow full visibility of device activity and content traffic. Through a built-in and flexible management console, Safend Protector allows administrators to create comprehensive and granular endpoint security policies.

Safend Protector Features and Benefits

- **Granular control** - detects and restricts data transfers by device type, device model or unique serial number.
- **Data awareness** - inspects files by their type and allows, blocks or restricts the transfer of unauthorized file types to and from external storage devices.
- **Flexible and intuitive policy management** - separate policies can be defined for any domain, group, computer, or user; policies are seamlessly integrated with Active Directory or Novell eDirectory organizational objects.
- **Built-in compliance policies** - includes detailed configurations for achieving security policies that are mapped to specific regulatory compliance standards.
- **Data encryption** - encrypts corporate data in motion on removable storage devices and CD/DVDs.
- **Granular WiFi control** - by MAC address, SSID, or the security level of the network.
- **Anti bridging** - prevents hybrid network bridging by blocking WiFi, Bluetooth, Modems or IrDA while the PC is connected to the wired corporate LAN.
- **Anti hardware keylogger** - blocks both USB and PS/2 hardware keyloggers.
- **U3 and autorun control** - turns U3 USB drives into regular USB drives while attached to organization endpoints, protecting against auto-launch programs by blocking autorun.
- **Track offline usage of removable storage** - tracks file transfers to/from Safend encrypted devices on non-corporate computers (offline) and logs the user's actions once the device is reconnected to the network.
- **Interface for content inspection add-on** - examines file "content", before it is allowed to be downloaded to an external storage device.

What's New in Safend Protector

- Compliance Reporting
- File Shadowing
- Enforced CD/DVD disk encryption
- Server Clustering
- Domain Partitioning

Safend Reporter Add-on for greater visibility

The Safend Reporter add-on feature provides security incidents reports by incident type, users and organizational units. Extensive reports on policy distribution, deployment status, and device inventory are also included.

System Requirements | Client

- Windows 2000 Professional
- Windows XP Professional (All Service Packs)
- Windows XP Tablet PC Edition
- Windows 2003 (All Service Packs)
- Windows Vista

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.



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

Toll free from the US (to US and Israel): 1.888.225.9193 info@safend.com