

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.

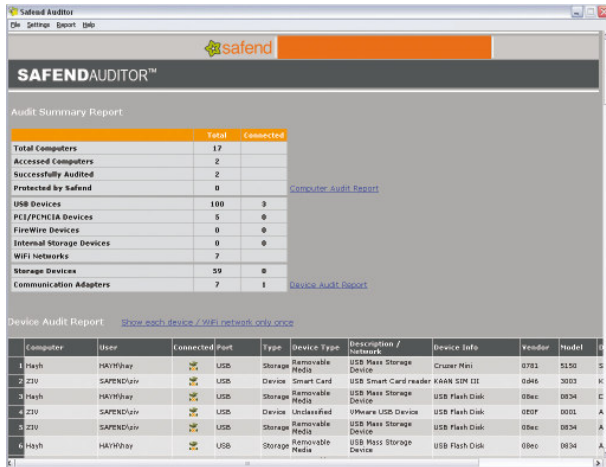
With Safend Auditor, administrators can differentiate between secure productivity enhancers, such as authentication tokens, and potential security threats, such as mass-storage MP3 players. Safend Auditor also tracks which WiFi networks employees are connecting to - secure encrypted networks or exposed 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. At the top, there's a menu bar with 'File', 'Settings', 'Report', and 'Help'. Below that is the 'SAFENDAUDITOR™' logo. The main area is titled 'Audit Summary Report' and contains a table with columns 'Total' and 'Connected'. Below this is a 'Device Audit Report' section with a table listing various devices connected to computers.

	Total	Connected
Total Computers	17	
Accessed Computers	2	
Successfully Audited	2	
Protected by Safend	0	
USB Devices	100	3
PCI/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 / Interface	Device Info	Vendor	Model
1 Hash	HAYHDay	USB	Storage	Removable Media	USB Mass Storage Device	Cruzer Mini	0781	5150 S
2 ZJU	SAFENDUay	USB	Device	Smart Card	USB Smart Card reader KAAN SDN III	0446	3003	K
3 Hash	HAYHDay	USB	Storage	Removable Media	USB Mass Storage Device	USB Flash Disk	0B4c	0834 C
4 ZJU	SAFENDUay	USB	Device	Unclassified	YHware USB Device	USB Flash Disk	080F	0801 A
5 ZJU	SAFENDUay	USB	Storage	Removable Media	USB Mass Storage Device	USB Flash Disk	0B4c	0834 A
6 Hash	HAYHDay	USB	Storage	Removable Media	USB Mass Storage Device	USB Flash Disk	0B4c	0834 A

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.

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 (DLP) solutions that protect against corporate data loss by offering comprehensive solutions for data encryption and port and device control. The Safend DLP Suite encrypts internal and external hard drives, removable storage and CD/DVDs and provides granular port and device control over all physical, wireless and removable media devices, ensuring compliance with regulatory data security and privacy standards. With more than 1,200 customers worldwide and 1.7 million licenses sold, Safend's solutions are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe.



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
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

Copyright © 2009 Safend Ltd. The information contained herein is accurate at the time of publishing and subject to change without notice. 01/09

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