

safend

Securing Your Endpoints



Strengthening the Bench *Building Platforms for Information Leakage Prevention*

CIOs, CSOs, and anyone else with a C in his or her title is acutely aware of the daily dose of data leaks, virus infections, and laptop thefts that land on the front page or are broadcast over the airwaves. The business community's response has been an urgent demand for a remedy for data threats. Industry research firm, Datamonitor, recently estimated that enterprises world-wide will have invested \$15.8 billion into securing their networks and systems by the end of this year.

In response to this demand, information security vendors have been more than happy to glut the market with products, competing to develop the all-inclusive, end-to-end, magic formula for securing all data on all fronts from all threats. But the unfortunate reality is that there is no silver bullet. As daily headlines indicate, companies continue to be victimized by data thieves, hackers, and disgruntled employees, yet the miracle cure-all has not materialized. Instead, IT departments are deploying multi-faceted products that include firewalls, internet security, email monitoring, content control, and disk encryption but continue to ignore the vulnerabilities presented by employee misuse of data.

A better strategy for securing corporate information is the development of wider security platforms or "benches" that are based on solid information leakage prevention (ILP) capabilities such as those offered by endpoint ILP solution provider, Safend. Safend's products, Safend Protector and Safend Auditor were developed to integrate well with the majority of network, internet, and systems security products and allow companies to customize their security strategy by monitoring and controlling who has access to sensitive data and how it is transported.

Safend Solutions

Safend Endpoint Leakage Prevention solutions protect enterprises against corporate data loss while ensuring compliance with regulatory data security and privacy standards. The Solutions monitor real-time traffic and applies customized security policies over physical, wireless and removable storage interfaces (USB, FireWire, WiFi, CD/DVDs) and portable media players.

Safend Auditor is a clientless software tool provides organizations with the visibility needed to pinpoint and manage vulnerabilities in an enterprise's PCs and laptop environment. Safend Auditor transparently and rapidly monitors enterprise PCs - locating and documenting all devices that are or have been locally connected. Safend Auditor features include:

- **Non-intrusive**, clientless and very easy to use
- **Reliable**, precise and simple device discovery
- **Comprehensive reports** of devices currently or previously connected to any endpoint
- **Real-time report** on-screen or report exported to MS Excel or XML
- **Fully compatible with Microsoft Active Directory** and other domain management software
- **Audits** selected PCs, groups or the entire enterprise

Safend Protector is a comprehensive security solution that prevents data loss and targeted attacks by controlling access points to corporate PCs and laptops. Safend Protector monitors real-time traffic and applies customized security policies over all physical, wireless, and removable storage devices including USB, FireWire, WiFi, Bluetooth, Infrared (IrDA) and CD/DVDs. Safend Protector detects, logs, and restricts unapproved data transfer from any computer in the enterprise. Each computer is protected 100% of the time, even when it is not connected to the network. Adding protection from unwanted access to data outside the firewall, Safend Protector can further ensure that mobile users and data are secure by encrypting any data written to removable storage devices or by enforcing the use of hardware encrypted flash drives only.

Safend Protector 3.2 Product Features

- **Granular control** - detects and restricts data transfers by device type, device model or unique serial number.
- **Data Awareness**- inspects files for their type and controls the transfer of unauthorized file types to and from external storage devices.
- **Policy Flexibility** - defines policies for any domain, group, computer, or user; policies are easily associated with Active Directory or Novell organizational objects.
- **Data Protection** – protects corporate data in motion by encrypting data on external storage devices and tracking offline use.
- **Intuitive Management** - integrates seamlessly into Active Directory or other network mgmt software.
- **Tamper-proof** - advanced policy enforcement via kernel-level, real-time analysis of low-level port traffic. Client side agents are silently deployed; redundant multi-tiered anti-tampering prevents security policy circumvention.
- **Granular WiFi Control** – controls by MAC address, SSID, or the security level of the network. Prevents hybrid network bridging by blocking wireless devices while the PC is connected to wired corporate LAN.
- **Anti Hardware Keylogger** – blocks both USB and PS/2 hardware keyloggers, which can record every keystroke entered through an endpoint.
- **File Type Control** - analyzes files as they are transferred to/from external storage devices and blocks or authorizes them based on their "type".
- **CD/DVD Media White Lists** - identifies the data on each medium and approves removable media based on digital signatures; controls and restricts use of CD/DVD drives.
- **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 device is reconnected to the network.
- **Removable Device Encryption** - restrict the usage of encrypted storage devices to company computers by use of AES with a 256-bit key encryption.
- **CD/DVD Disk Encryption** - encrypts data on CD/DVD media and external hard drives using FIPS approved AES with a 256-bit key.
- **Interface for Content Inspection** - examines file "content" before it is allowed to be downloaded to an external storage device. (Websense partnership).

Of course, technology cannot take the place of strict, clearly communicated, corporate policies. However, once these policies are established and mandated, information leakage prevention tools can sharply decrease the likelihood of a data leak, data theft, or loss of sensitive information.

Deploying a wide security bench that monitors and enforces corporate data access policies at the endpoint, then "seating" integrated, risk-specific products on the bench, enables an organization to craft an environment-specific approach based on their individual needs rather than using only a portion of an expensive, and oftentimes complex, end-to-end solution. The bench approach has the added benefit of scaling well to the growth of an organization. Any IT manager will agree that today's information security threats are a drop in the bucket when compared to the ones about to emerge. Similarly, the security risks and compliance mandates encountered by a small to medium business may drastically change as the company grows, their capital accumulates and their information assets increase.

Safend Solutions

- Scalable from one machine to thousands, in both domain and domain-less environments.
- Easily integrates with Microsoft Active Directory and other network management software, allowing utilization of existing user group definitions.
- Seamless integration with Safend Auditor empowers rapid device discovery to white list creation: One click adds audited device to approved list.
- Streamlined policy creation process through intuitive user interface makes set-up quick and easy.

Vendors that make the choice to ensure the interoperability of their solutions will reap the benefits of a changing market landscape. According to the industry research firm Enterprise Strategy Group, of the organizations they recently surveyed that had deployed a data loss prevention solution, approximately one-fourth had implemented an integrated network and host based solution. ESG predicts this number will grow as additional threats to corporate data emerge. Building a defense system from the inside out, starting at the place where users interact with data-the corporate endpoint-appears to be the most efficient and cost-effective way to provide a solid foundation for expanding a protective net as enterprise needs change and technology evolves.

ABOUT SAFEND

Safend is a leading provider of endpoint information 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. Safend's solutions, available through resellers worldwide, are deployed by multinational enterprises, government agencies 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: +1.215.496.6251
Toll free from the US (to US and Israel): 1.888.225.9193 info@safend.com

Copyright © 2007 Safend Ltd. The information contained herein is accurate at the time of publishing and subject to change without notice.