

safend

Endpoint Data Protection

Adhere to regulatory data security and privacy standards



Maintain optimal balance between productivity and data security

Protect corporate IP, trade secrets, sensitive customer and employee data

Effective Data Protection Starts at the Endpoint

Safend's products protect organizations from data leakage and theft. Safend's granular port and device control combined with its comprehensive encryption enables complete protection of sensitive data-in-use, data-at-rest and data-in-motion, without sacrificing productivity.

Endpoint Data Leakage - The Threat

Firewall and VPN technologies are no longer enough: An entire hard drive can be now be downloaded to a smart phone or thumb drive in a matter of minutes and laptops are all too easily lost or stolen.

Business survival and success is built on data security. Organizations depend on the security of their data - from intellectual property such as business plans and trade secrets, to sensitive customer data like health records, financial information and social security numbers. And, regulators demand assurances that confidential data remains accessible only to authorized users.

Industry statistics consistently show that the most significant security threat to the enterprise 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 laptops, removable storage devices, interfaces (physical and wireless), and users with access to sensitive data have made data leakage via endpoints - both accidental and malicious - a very real threat. It's simply too easy for a laptop to be lost or stolen, or for sensitive data to walk away on a MP3 player, digital camera, or memory stick. According to Forrester, data loss through endpoints is now a leading endpoint security concern - ahead of Malware, Spyware and other threats.

Endpoint Security - A Financial Imperative

As more and more highly-publicized data security breaches occur, enterprises are faced with immeasurable damage to their reputations and staggering monetary losses. In response, corporate IT and security executives must adopt improved endpoint data protection and data leakage prevention strategies.

In fact, Aberdeen estimates that without a sound endpoint data protection solution, organizations may lose millions of dollars from misplaced IP and unapproved use of valuable data.

Endpoint Security - A Regulatory Imperative

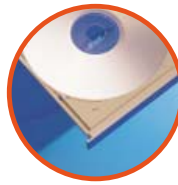
Regulatory security initiatives such as Sarbanes Oxley (SOX), HIPAA, PCI, FISMA, BASEL II, and the UK Data Protection Act (DPA) require organizations to maintain ongoing visibility into endpoint activity. In today's sensitive regulatory climate, organizations are expected to demonstrate a comprehensive data protection strategy and understanding of all data transfer activities. They need to identify and limit leakage in every form and from every possible avenue while providing immediate remedy for security breaches detected, and a full audit trail. Without an effective solution in place to both secure and monitor endpoints, compliance is difficult to achieve.

The Endpoint Threat in Numbers

- 52% of companies surveyed have suffered data loss via USB drives and other removable media – Forrester Report 2007
- Over 70% of security breaches and data thefts originate from within - Vista Research

The Cost of Data Leakage

- Average cost per data breach incident was \$6.6M and the cost per record was \$202 in 2008 - Ponemon Institute
- Information breaches trigger an average 5% drop in company share prices. Recovery to pre-incident levels takes nearly a year - EMA Research



The Challenge - Effective Endpoint Data Protection

Despite the clear and present danger of data leakage, implementing effective endpoint data protection remains an uphill battle for most organizations.

Laptops, external devices, PDAs, smart phones and more are tremendous productivity enhancers. They keep employees in touch and connected and help to create competitive advantage. Securing endpoints - without impacting employee productivity and system performance - demands a highly-flexible solution that takes into account the dynamics of real-world work environments.

Many end users view external devices as personal, and view encryption of any kind as a headache - often balking at and circumventing imposed security measures. As a result, today's data protection solutions need to be transparent without compromising the data security of an organization. All possible endpoint data leakage avenues must be managed with powerful, enforceable, tamper-proof security.

It is clear that identifying sensitive data or suspicious activity is paramount to data protection. Organizations require deep visibility of ongoing and historical endpoint activity, and are implementing endpoint security solutions that track data transfers based on company data security policies.

The Ultimate Combination of Visibility, Control and Protection

Safend Data Protection Suite provides complete endpoint data protection from the ground up - offering security administrators the power of granular visibility over every potential endpoint leakage channel, sophisticated security policy creation, and enforcement.

Featuring easy deployment, seamless maintenance for administrators, and maximum transparency for end users, Safend Data Protection Suite enables organizations to enjoy the productivity benefits of mobile computing without sacrificing security.

Safend Data Protection Suite eliminates data leakage from endpoints, delivering comprehensive visibility, complete data protection and total control over all available avenues to sensitive data.

VISIBILITY

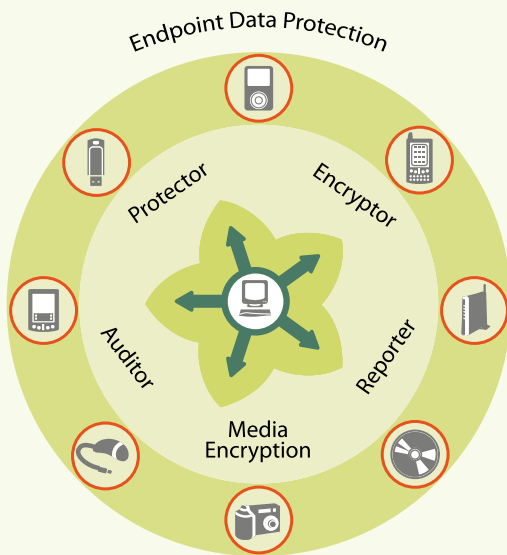
Only with detailed visibility of endpoint activity - ongoing and historical - can security administrators effectively monitor and enforce a security policy that is in-line with real-world usage. Safend Data Protection Suite provides organizations with the power to transparently and rapidly query all organizational endpoints while locating and documenting all devices that are or have ever been locally connected.

CONTROL

Without absolute enforceability, the best endpoint security policies won't work. Granular control of endpoint activity and content is crucial to achieving security. Safend Data Protection Suite monitors real-time traffic and applies customized security policies over all physical, wireless and removable storage interfaces. Safend Data Protection Suite 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.

PROTECTION

Safend Data Protection Suite guards the data stored on hard drives with its innovative, easy to manage hard disk encryption. Safend Data Protection Suite also ensures that mobile users and data are secure by encrypting any data written to removable media such as USB flash drives, external hard drives and CD/DVD.



Instantly Assess your current security status with **Safend Auditor**

Precisely Control physical ports and devices with **Safend Protector**

Transparently Protect your laptops, desktops, and removable media with **Safend Encryptor** and Safend Protector Removable Media Encryption

Easily Monitor your security and operational status with **Safend Reporter**

Centrally Manage all security features with Safend's enterprise grade management infrastructure

Why Safend?

- Control all your data protection measures with a single management server, single management console and a single lightweight agent.
- Operational friendly deployment and management
- Best of breed port and device control
- Hard disk encryption is completely transparent and does not change end user experience and common IT procedures
- Comprehensive and enforceable Media Encryption
- Track file transfers from encrypted devices even on non-corporate computers

Customer Testimonials

"Simply telling more than 500 people not to use their USB ports was just not a realistic solution...Safend gives us what we need to maintain the privacy and integrity of our client information."

- Bill Liston, IT Solutions Technician, ConnectiCare

"Safend's products are well thought out and actually accomplish more than we expected. The product is robust, helping us in our proactive quest to identify potential problems."

- Alan Pomerantz, Chief Security Officer, Philadelphia Stock Exchange

"Since installing Safend, we have been able to easily monitor and control all device activity in our organization...the deployment went very smoothly - no errors, no hassles...saving us time and needless effort."

- Michael Apt, IT and Security Manager, SCD

About Safend

Safend is a leading provider of endpoint data protection software. Our products protect against corporate data loss by offering comprehensive data encryption and port and device control. Safend's products encrypt internal and external hard drives, removable storage devices and CD/DVDs and provide 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 software is deployed by multinational enterprises, government agencies, healthcare organizations, 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. 03/09