safend

Endpoint Information Leakage Prevention Solutions

Adhere to regulatory data security and privacy standards

Maintain optimal balance between productivity and information security

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

safend

Securing Your Endpoints

Effective Information Protection Starts at the Endpoint

Solutions from Safend safeguard against endpoint information leakage. By delivering granular visibility and control over enduser devices and ports, Safend enables the protection of sensitive data-at-rest and data-in-motion, without sacrificing productivity.

Endpoint Information Leakage | The Threat

In the decade since VPN and firewall technologies became mainstream, large investments in gateway solutions have proven ineffective when faced with one rogue or negligent employee with a portable storage device.

Business survival and success is built on information security. Organizations depend on the security of their data - from intellectual property such as business plans and trade secrets, to customer confidential information 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 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, interfaces (physical and wireless), and users with access to sensitive information have made information 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. According to Forrester, data loss through endpoints is now a leading endpoint security concern - ahead of Malware, Spyware and other threats.

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

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 information leakage prevention (ILP) 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, 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 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, including a full audit trail. Without an effective solution in place to both secure and monitor endpoints, compliance is difficult to achieve.

The Cost of Data Leakage

- Average cost per data breach incident was $5 million dollars in 2006, and growing 30% annually - *Ponemon Institute*
- Information breaches trigger an average 5% drop in company share prices

  Recovery to pre-incident levels takes nearly a year - *EMA Research*

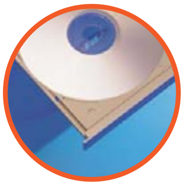
The Challenge | Effective Endpoint Information Leakage Prevention

Despite the clear and present danger of information leakage, implementing effective endpoint ILP remains an uphill climb for most organizations.

Today's external devices - flash drives, communication adapters, smart phones and more - are tremendous productivity enhancers. These devices keep employees in touch and connected, and help to create competitive advantage. Securing endpoints without impacting productivity demands a highly-flexible solution that takes into account the dynamics of real-world work environments.

Since many end users view external devices as personal and private - often balking at and circumventing imposed security solutions - today's ILP solutions need to be transparent. At the same time, there's no room for compromise. All possible endpoint information 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 and Control

Safend creates solutions that are designed for complete endpoint ILP 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's solutions enable organizations to enjoy the productivity benefits of mobile computing, without sacrificing security.

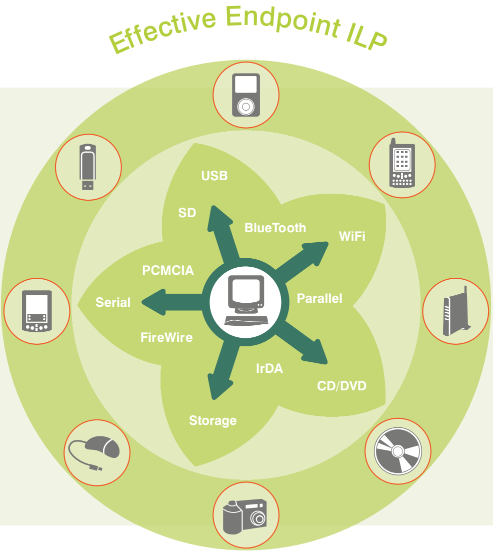
Safend eliminates information leakage from thousands of endpoints, delivering comprehensive visibility and total control over all available avenues to sensitive information.

VISABILITY

Only with detailed visibility of endpoint activity - ongoing and historical - can security administrators hope to monitor and enforce a security policy that is in-line with real-world usage. Safend 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 monitors real-time traffic and applies customized security policies over all physical, wireless and removable storage interfaces. Safend 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 network and firewall, Safend 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 Delivers

- Content-aware visibility over every single endpoint
- Granular control over all physical/ wireless interfaces and storage devices
- On-board protection of sensitive data stored on any enterprise computer

Why Safend?

- Intelligently secure and monitor every single endpoint
- Protect valuable corporate intellectual property and company confidential data
- Protect sensitive customer and employee information
- Maintain regulatory data security compliance
- Prevent reputation and revenue damage resulting from security breaches
- Balance the demand for mobility with the need for security

Customer Testimonies

"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 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. Founded in 2003, Safend is a privately held company headquartered in Tel Aviv with US headquarters in Philadelphia. For more information, visit www.safend.com.

safend
Securing Your Endpoints
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