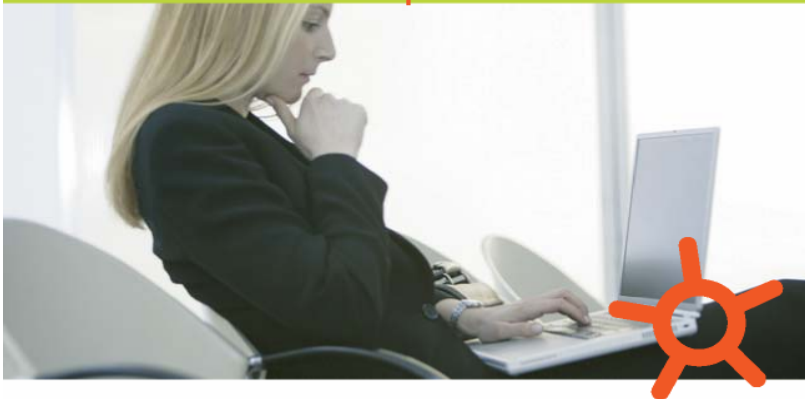


safend protector

Robust Endpoint Information 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 Information 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 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. 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 information 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 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, encrypt all data on devices as well as monitoring, blocking and logging 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 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 for their type and controls the transfer of unauthorized file types to and from external storage devices.
- Policy flexibility - separate policies can be defined 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 - seamlessly integrates into Active Directory or other network management software.
- Tamper-proof - advanced policy enforcement via independent, 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 — by MAC address, SSID, or the security level of the network. 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, which can record every keystroke entered through an endpoint.
- U3 and Autorun Control — turns U3 USB drives into regular USB drives while attached to organization endpoints, and protects against dangerous auto-launch programs by blocking autorun.
- Easy auditing - encrypted logs and alerts can be viewed in the management console or integrated with third-party software for comprehensive analysis or immediate notifications.

What's New in Safend Protector

- File Type Control
- Track Offline Usage of Removable Storage
- Internal Ports Protection (IDE, SCSI, SATA, PCI etc.)
- Novell eDirectory Synchronization Internal/External DB
- Support for Windows Vista

The Most Comprehensive Information Leakage Prevention Available

Safend Protector can now be integrated with a leading gateway information leakage prevention solution to provide the industry's first content-aware, policy based gateway and endpoint ILP solution.

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 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.

