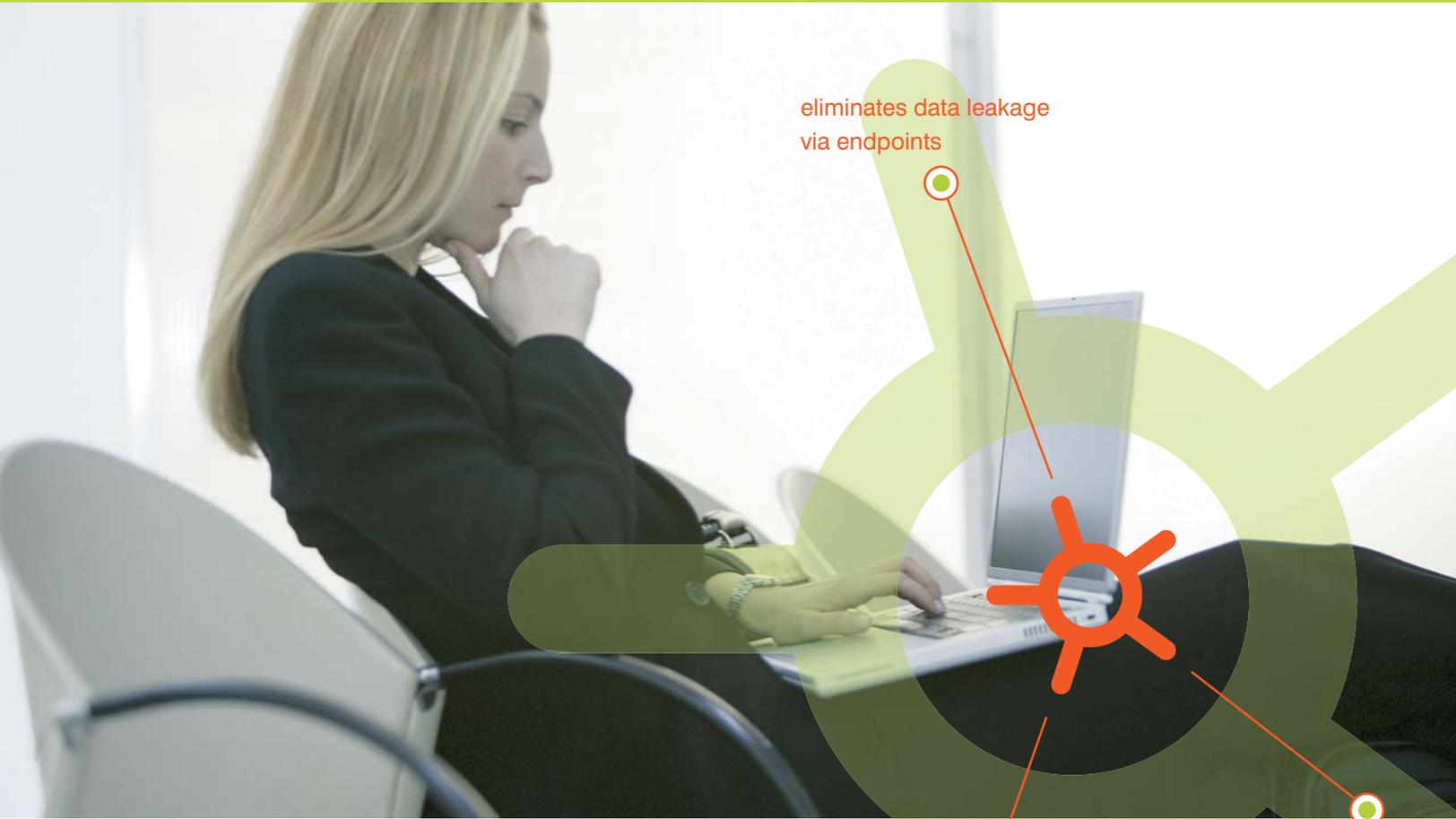# safend protector v3.0

Robust Endpoint Security

eliminates data leakage
via endpoints

delivers granular visibility
and control over physical
and wireless ports

enables connectivity and
productivity with security

safend
Securing Your Endpoints

regain control of your endpoints

endpoint security – challenges and risks

The Financial Times calls removable media a "clear and present danger." Security analysts issue urgent advisories to their clients regarding the dangers of popular MP3 players. Corporate legal teams prepare for the inevitable worst case legal or regulatory scenario.

Nowhere is the internal threat more tangible than at the endpoint, where over 60% of confidential data resides according to IDC. When a trusted user has easy access to sensitive information – no gateway solution or written security policy can mitigate the risk.

It's simply too easy for employees, partners, and even executives to connect an MP3 player, digital camera, or memory stick – and walk away with sensitive or confidential material. Beyond malicious intent, removable media with mission-critical information is easily lost, misplaced, or accidentally exposed via connectivity to unsecured public wireless networks.

Recent research has found that internal IP theft via USB ports alone is a problem faced by almost 40% of enterprises (Yankee Group) – and cost US companies alone $50 billion last year (The Economist).

The only solution: comprehensive and granular control over access to physical and wireless ports.

> "Protector provides strong data protection for any size organization, with robust central management and the flexibility to enforce your corporate policies for removable storage devices…"
>
> *Information Security Magazine, February 2006*

stop data leakage through endpoints and removable media

Safend Protector v3.0 is the industry's most comprehensive, secure and easy-to-use endpoint security solution - controlling every endpoint and every device, over every network or interface.

Safend Protector monitors real-time traffic and applies customized, highly-granular security policies over all physical, wireless and removable storage interfaces, including:

PHYSICAL INTERFACES	WIRELESS INTERFACES	REMOVABLE STORAGE
USB	WiFi	CD / DVDs
FireWire	Bluetooth	Flash Drives
PCMCIA	Infra Red (IrDA)	Zip Drives
Serial		Floppy Drives
SD		Tape Drives
Parallel		

Safend Protector detects and allows restriction of devices by 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 access, or even block devices above a certain storage capacity. 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 flexible management console, Safend Protector lets administrators create comprehensive and granular endpoint security policies. Policies are exported directly to Active Directory as Group Policy Objects (GPOs), ready to be assigned to relevant Organizational Units (OUs) and silently installed on clients.

With built-in alerting capability, administrators can get immediate notifications of any activity that requires an immediate response. Alerts are available via email, SNMP, Syslog, Windows Event Viewer, popup messages and even custom scripts.
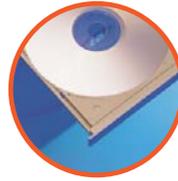
uncompromised control with tamper-proof agent

Safend Protector's lightweight and tamper-proof client-side agents are easily deployed, installed silently at the endpoint with no reboot required. The Protector agent operates at the kernel level, and includes redundant, multi-tiered anti-tampering features to guarantee permanent control over endpoints. Even local administrators can't circumvent security policy. In addition, agents are invisible to end-users until a non-approved device is connected, at which time a custom-defined notification appears.

part of the safend security suite

Part of the Safend Security Suite, Safend Protector interfaces seamlessly with Safend Auditor and Safend Secured USB Drive to offer the first end-to-end enterprise endpoint security solution.

SAFEND AUDITOR V3.0

Lightweight, clientless software utility that provides organizations with the visibility needed to identify and manage endpoint vulnerabilities. Safend Auditor transparently and rapidly queries all organizational PCs - locating and documenting all devices that are or have ever been locally connected.

SAFEND SECURE USB DRIVE

Ultra secure flash drive that features strong full-drive hardware-based encryption, reinforced with complex passwords. Deployed together with Safend Protector, Safend's USB drives are easily white-listed for secure access to endpoints, creating a secure network of authorized devices, and allowing employees to safely enjoy the benefits of USB storage.

WHAT'S NEW IN SAFEND PROTECTOR V3.O

The newest version of Safend Protector introduces additional strong security features and enhanced usability:

- **granular WiFi control**

  By MAC address, SSID, or the security level of the network

- **file name logging**

  Creates forensic logs of all files moving in and out of the organization via removable storage

- **Cisco NAC integration**

  Creates rules that mandate the presence of Safend Protector Client before the endpoint is allowed on your network

- **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

- **anti hardware keylogger**

  Detects and blocks keyloggers connected to USB keyboards, preventing attempts to record your keystrokes

- **usability, management and other functional enhancements**

  Tighter Active Directory integration, OTP for suspending agents securely, defining roles within the management console, server architecture, enhanced logging, alerting and reporting, and integral interfaces to third party management tools

safend protector management console
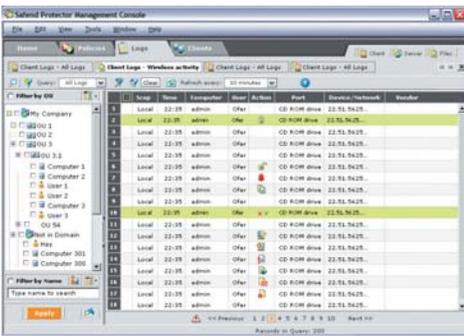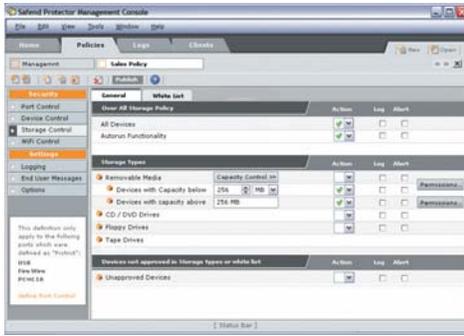
The intuitive Safend Protector Management Console allows easy definition and enforcement of port-specific security policy definition. In addition, it enables detailed log reporting for comprehensive analysis or immediate notifications.

SAFEND PROTECTOR ADVANTAGES

granular control

Detects and restricts devices by device type, device model or unique serial number

policy flexibility

Separate policies can be defined for any domain, group, computer, or user; policies are easily associated with Active Directory Organizational Units (OUs) for GPO update

advanced policy enforcement

Via independent, kernel-level, real-time analysis of low-level port traffic

secure agent

Silent deployment, redundant multi-tiered anti-tampering prevents security policy circumvention

intuitive management

Seamlessly integrates into Active Directory or other network management software

easy auditing and visibility

Encrypted logs and alerts can be viewed in the management console or integrated with third-party software for comprehensive analysis or immediate notifications

multilingual

Safend Protector speaks your language, allowing easier local administration

digital membrane technology

Safend Protector is based on a protocol-level, semi-permeable barrier that can be "wrapped around" any device. At the heart of this barrier - the "Digital Membrane" - is a unique kernel-level protocol inspection engine that analyses all inbound and outbound communications interfaces for a given device in real time. The engine monitors and controls all incoming and outgoing traffic for each device, blocking or allowing access or data based on highly-granular security policies. The result - total policy-based monitoring and control at all protocol layers, enabling previously unheard-of visibility and control over devices, applications, and actual data transferred.

about safend

Safend is a leading provider of innovative endpoint security solutions that protect against corporate data leakage and penetration via physical and wireless ports. Safend's products, available exclusively through resellers worldwide, are deployed by security-aware government agencies and multinational enterprises in sectors such as healthcare, finance and technology across the globe. The privately held company, founded in 2003, is headquartered in Tel Aviv with offices in Philadelphia.

w w w . s a f e n d . c o m