

safend

Securing Your Endpoints



endpoints – the achilles heel of corporate security

It's a fact. Gateway solutions and written security policies alone cannot secure enterprise data from those closest to it – employees, partners, and even senior executives.

It's simply too easy to connect a smartphone, MP3 player, digital camera, or memory stick – and walk away with sensitive or confidential material. The damage: almost \$50 billion to US companies last year alone (The Economist).

Existing endpoint security solutions either leave endpoint ports completely inaccessible – lowering productivity – or rely wholly on trust that policy will be obeyed. As a result, organizations must today choose between endpoint accessibility or endpoint security.

endpoint security – a regulatory imperative

Regulatory security initiatives such as Sarbanes Oxley (SOX), HIPAA, FISMA, and BASEL II require organizations to maintain ongoing and highly-granular visibility into endpoint user activity. They also demand immediate remedy of security breaches at the endpoint, including full audit trail. Without an effective solution in place to both secure and monitor, compliance achieved is easily lost.

the need - visibility and control

In order to secure vulnerable endpoints and maintain data integrity and regulatory compliance, organizations need to achieve both visibility and control over endpoints:

visibility

Only with detailed, high resolution visibility of endpoint activity - ongoing and historical – can security administrators hope to define and enforce a security policy that is in-line with real-world usage.

control

Without absolute enforceability, the best endpoint security policy can't work. Highly-granular control of endpoint activity – down to the level of individual user, port, device and usage scenarios – is key to achieving security with productivity.

ENDPOINT SECURITY FACTS

-  60% of confidential data resides on the endpoint (IDC)
-  Internal IP theft via USB ports has harmed almost 40% of enterprises (Yankee Group)
-  Over 70% of security breaches originate from within (Vista Research)

safend - the end of productivity-security tradeoffs

Safend develops, markets, and supports comprehensive endpoint security solutions that enable organizations to enjoy the productivity benefits of mobile computing - without sacrificing security.

Safend's advanced solutions deliver granular visibility and control over network endpoints, exposing and remediating existing and potential threats to ensure comprehensive internal data security.



SAFEND AUDITOR™ Comprehensive Endpoint Visibility

Safend Auditor is a 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 been locally connected.



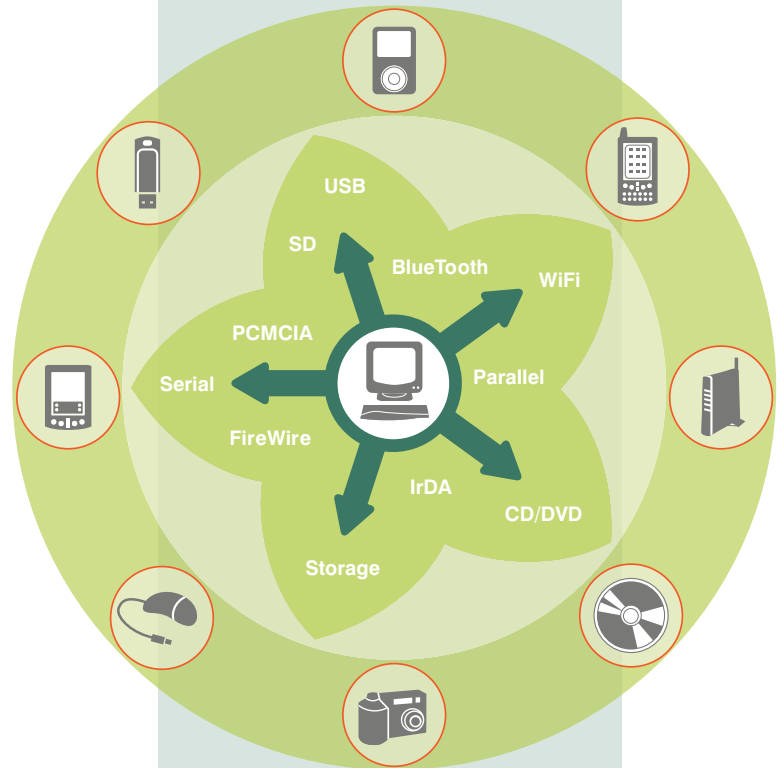
SAFEND PROTECTOR™ Robust Endpoint Security

Enabling IT and security administrators to regain complete control over all network endpoints, Safend Protector monitors real-time traffic and applies customized, highly-granular security policies over all physical, wireless and removable storage interfaces. Safend Protector's uniquely tamper-proof local agents detect and restrict devices by device type, model or individual device serial number.

digital membrane technology

Safend solutions are 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.

ironclad endpoint security



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.



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

Copyright© 2006 Safend Ltd. The information contained herein is accurate at the time of publishing and subject to change without notice.