

# Safend Protector



Sicherheit für Schnittstellen und Wechseldatenträger:

## 66 % der Diebe sitzen innerhalb der Firewall

*FireWire-Festplatten, USB-Sticks mit X Gigabite und selbst Bluetooth-Handys dienen als Einbruchswerkzeug und um die Beute „wegzuschleppen“. Der Safend Protector schützt das IT-System wirksam vor diesen „internen“ Bedrohungen. Er liefert alle Möglichkeiten um Sicherheitslücken, die durch die unkontrollierte und nicht erlaubte Benutzung von Schnittstellen und Endgeräten entstehen, effektiv zu schließen.*

Die Bedrohung:

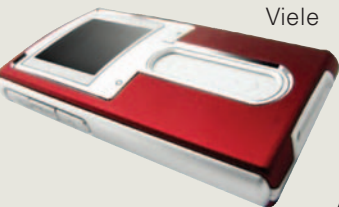
- USB-Stick
- FireWire-Harddisk
- Bluetooth-Handy
- SD-Karten
- usw.



Der **Safend Protector** ist das Tool, mit dem offene Schnittstellen zuverlässig erkannt, für den erlaubten Gebrauch geöffnet und ansonsten konsequent verschlossen werden. Von Bluetooth bis WiFi!

### Außen hui, innen ...?

Viele IT-Sicherheits-Spezialisten haben sich auf den Schutz vor externen Angriffen konzentriert. Ihr Netzwerk ist durch eine Firewall gut gesichert. Ihre Anti-Viren-Lösung ist stets aktuell und die Patches immer up-to-date.



Aber: Die größte Gefahr droht Unternehmen inzwischen von Mitarbeitern, Kollegen und anderen Personen innerhalb der Firewall: An ungeschützten Schnittstellen klaffen interne Sicherheitslücken.

### Neue Gefahren im Taschenformat

Auf einen iPod mit 60 GB Speicher passen gut 15000 Songs – aber auch die gesamten Personaldaten eines Industriekonzerns. Mit Handys können Viren eingeschleust werden. Auf USB-Sticks haben ganze Datenbanken Platz. Und mit einer einzigen selbst gebrannten DVD oder CD stehlen professionelle Industriespione oder verärgerte Praktikanten die Konstruktionspläne ganzer Flugzeuge. In der Hosentasche!

### Geschlossene Schnittstellen sind sicher

Nur wenn die Schnittstellen vor Ort sicher sind, ist es auch das System! Es gilt also, jedes Device strikt zu überwachen und nicht benötigte Schnittstellen konsequent zu verschließen. Diese Aufgabe löst der **Safend Protector** mit Hilfe einer zentralen Steuereinheit, die jede Schnittstelle im Netz erkennt und für den benötigten Gebrauch öffnet. Und ansonsten versperrt. Damit Diebe keine Chance haben.

### DAS SIND DIE FEATURES:

#### ■ Einfaches Management

Der Safend Protector arbeitet mit Hilfe von netzwerkweit geltenden Regeln und Voreinstellungen zur Benutzung von Schnittstellen und kritischen Endgeräten. Das Erstellen und Ändern dieser Regeln erfolgt mit Hilfe der Konsole von Safend Protector in nur 3 Schritten. Zusätzlich werden hier Parameter für das Logging und Alerting definiert. Die Konsole integriert sich nahtlos in das Active Directory oder in andere Managementlösungen.

#### ■ Flexibilität

Die Protector Richtlinien werden für das Unternehmen, Domänen, Abteilungen, PCs oder Anwender definiert.

#### Diese Ports werden wirkungsvoll vom Safend Protector geschützt:

- FireWire
- PCMCIA
- Seriell
- Parallel
- Bluetooth
- WiFi
- IrDA

#### Endgeräte wie

- CD-/DVD-Brenner
- SD-Karten
- ZIP -und Bandlaufwerke
- Massenspeichergeräte

#### ■ Übersichtliche Ergebnisse

Soweit möglich klassifiziert Safend Protector die Endgeräte nach Gerätetyp, Modell und Seriennummer. Damit kann z. B. ein bestimmtes Druckermodell oder ein über die Seriennummer identifizierter Drucker beim Abteilungsleiter explizit freigegeben werden.

#### ■ Daten- und Geräteanalyse in Echtzeit

Alle über Schnittstellen ein- bzw. ausgehenden Daten werden über die „Multi-Protokoll-Analyse“ in Echtzeit verifiziert und unabhängig vom installierten Betriebssystem überprüft, womit auch vorsätzlich irreführende bzw. falsche Installationen erkannt werden.

### ... UND DAS SIND DIE FAKTEN:

- In den Unternehmen liegen ca. 60 % der Datenbestände ungeschützt offen.
- Allein im Jahr 2004 verursachte interner Datendiebstahl in den USA einen Schaden von 50 Milliarden US \$.
- Jedes 2. Virus wird von innen, z. B. von Mitarbeitern absichtlich oder versehentlich eingeschleust.
- 70 % der Schäden mit einer Schadenshöhe über 100.000 Euro werden von internen Sicherheitsmängeln verursacht.

80 GB Konstruktionspläne in der „Westentasche“

### China produziert billigen „AIBUS A 381“

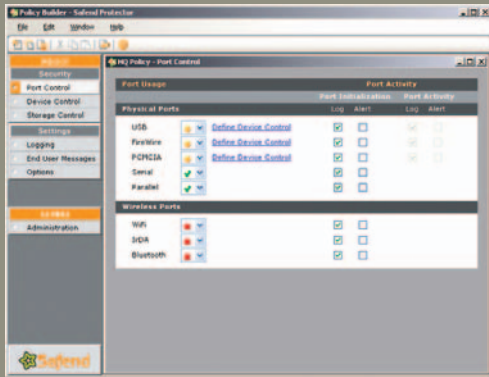
Toulouse (sparks) – Schock für die europäische Flugzeugindustrie: Nachdem ein Kantinenarbeiter die gesamten Pläne des neuen Projektes auf seine USB-Flashcard kopieren konnte, sind die vertraulichen Daten jetzt offensichtlich in China gelandet. Gestern wandte sich ein Wok-Hersteller aus Peking an die internationale Presse. Der auf Raubkopien spezialisierte Betrieb kündigte die Produktion eines gleichwertigen, aber um 75 % günstigeren Passagierflugzeugs Typ „AIBUS A 381“ an. Die ersten Vorbestellungen seien bereits eingegangen. Der gesamten europäischen Flugzeugindustrie droht jetzt der Absturz.



## Sicherheit für Schnittstellen und Wechseldatenträger

### ■ Doppelte Sicherheit

Der Safend Protector Client verwaltet gleichzeitig zwei verschiedene Richtlinien für PC und User. Die User-Richtlinie hat hierbei eine höhere Priorität.



**Den Überblick behalten und effizient Sicherheitslücken schließen mit dem Safend Protector.**

### ■ Whitelist

Über Safend Auditor gefundene Endgeräte können sofort in die Liste der autorisierten Endgeräte (Whitelist) aufgenommen werden.

### ■ Storage Devices

Safend Protector kann Storage Devices sperren, nur spezielle, z. B. verschlüsselte Endgeräte erlauben, die Ports auf read-only setzen oder die Kapazität limitieren.

### ■ Anti-Tampering-Funktionen

verhindern eine De-Installation des Clients auf PCs.

### ■ Safend Auditor

Safend Protector beinhaltet Safend Auditor und damit ein Monitoring-Tool, das Ihnen alle Endgeräte anzeigt, die während der letzten 6 Monate an den PCs angeschlossen waren.



**SAFEND  
AUDITOR**

*Safend Auditor erkennt unternehmensweit alle relevanten Schnittstellen (USB, WiFi, FireWire, PCMCIA, Bluetooth, Infrarot (IrDA), seriell und parallel) und Storage Devices (CD/DVD-, Flash-, Zip-, Disketten- und Bandlaufwerke, Massenspeichergeräte).*

■ **Safend Auditor** ist als reines Analysetool auch einzeln erhältlich.

■ **Safend Protector** kann nur in Verbindung mit Safend Auditor lizenziert und eingesetzt werden. Dieses Bundle erlaubt die Kontrolle und das Durchsetzen Ihrer Sicherheitsrichtlinien.



### Systemvoraussetzungen:

- **Betriebssystem der Domäne:**  
Windows 2000 Server (Service Pack 3-4)  
Windows 2003 Server (Service Pack 0-1)
- **Betriebssystem am Endgerät:**  
Windows 2000 Professional (Service Pack 3-4)  
Windows XP (Service Pack 0-2)  
Windows 2000 Server (Service Pack 3-4)  
Windows 2003 Server (Service Pack 0-1)  
Windows XP Tablet PC Edition
- **Betriebssystem für die Konsole:s,**  
Windows XP (Service Pack 1 oder 2)  
Windows 2003 Server und .NET-Framework

### Kostenlose Demoverision!

**Finden Sie alle  
Sicherheitslücken in  
Ihrem Unternehmen.**

**Kostenlos!  
Jetzt downloaden:**

[www.prosoft.de/safend](http://www.prosoft.de/safend)

## Wir wollen ein gutes Betriebssystem noch besser machen!

Mit erstklassigen Third-Party-Softwarelösungen für anspruchsvolle Administratoren, komplexe Problemstellungen und sensible Anwendungen! Tools, die umfassend getestet wurden und auch in kritischen Umgebungen jederzeit bestehen. Darüber hinaus stehen wir unseren Kunden stets beratend und unterstützend zur Seite: vom Roll-out-Konzept über die Installation – auch von (oft kostenlosen) Testversionen – bis zur Mitarbeiterschulung. Direkt bei Ihnen vor Ort! Sprechen Sie mit uns.



ProSoft Software Vertriebs GmbH  
Bürgermeister-Graf-Ring 10 - 82538 Geretsried  
Tel: +49 (0)8171/405-0 - Fax: +49 (0)8171/405-400  
info@prosoft.de

