

## Data Loss Prevention am Endpoint

In Statistiken wird immer wieder deutlich, dass die größten Sicherheitsrisiken innerhalb der Unternehmen selbst lauern. Da sich über 70 % der Unternehmensdaten auf Endpoints befinden, kann durch schriftliche Sicherheitsrichtlinien und reine Gateway-Sicherheitslösungen die Gefahr von Informationslecks im Unternehmen nicht entschärft werden. Durch die zunehmende Anzahl an Wechselmedien, physikalischen und drahtlosen Schnittstellen sowie Usern mit Zugang zu sensiblen Daten werden Informationslecks an Endpoints, egal ob unbeabsichtigt oder bösartig, zu einer echten Bedrohung für Unternehmen. Es ist eben ganz einfach, an einem Endpoint (z.B. PC) einen USB-Stick, iPod oder eine Digitalkamera anzuschließen und sensible Daten herunterzuladen. Genauso einfach können über WiFi, Bluetooth oder 3G-Modems geschützte interne Netzwerke mit offenen externen Netzwerken verbunden werden.

SafeGuard PortProtector wurde speziell zur Bewältigung dieser Sicherheitsrisiken entworfen. Das Programm kontrolliert jeden Endpoint und jedes Gerät an allen Schnittstellen und gewährleistet so einen einfachen und flexiblen Schutz vor ungewollten Informationsverlusten. SafeGuard PortProtector überwacht den Datenverkehr in Echtzeit und wendet darauf abgestimmte, detailliert einstellbare Sicherheitsrichtlinien für alle Arten von Schnittstellen und externen Speichergeräten an:

- » Physikalische Schnittstellen: USB, FireWire, PCMCIA, parallel, seriell usw.
- » Drahtlose Schnittstellen: WiFi, Bluetooth, Infrarot (IrDA)
- » Externe Speicher: Wechselmedien, CD/DVD, mobile Festplatten usw.

SafeGuard PortProtector erkennt Gerätetypen, Modelle und sogar bestimmte Seriennummern und ermöglicht so eine Begrenzung des Datenverkehrs. Mit SafeGuard PortProtector können Administratoren Speichermedien vollständig blockieren, reinen Lesezugriff zu diesen erteilen oder alle auf diesen Medien enthaltenen Daten verschlüsseln. Zudem können auf diese Geräte geschriebene oder von ihnen gelesene Dateien überwacht, blockiert und protokolliert werden.

Zusätzlich steht Administratoren mit SafeGuard PortAuditor ein umfangreiches Werkzeug zur Verfügung, mit dem sie einen Überblick über die Verbindungen an Unternehmens-Endpoints gewinnen. Mit SafeGuard PortAuditor kann zwischen sicheren und produktivitätssteigernden Verbindungen wie z.B. Authentifizierungstoken und potenziellen Sicherheitsbedrohungen wie Massenspeichergeräten (MP3-Playern) unterschieden werden. Mit diesen Informationen können granulare Sicherheitsrichtlinien aufgesetzt und durchgesetzt werden, die exakt auf die geschäftlichen Anforderungen des Unternehmens zugeschnitten sind.

Durch die umfassenden Schutzmechanismen sowie die einfache Verwaltung und problemlose Benutzung ist SafeGuard PortProtector die ideale Lösung, um Datenverluste zu vermeiden.

## Vorteile

### Erhöhte Sicherheit

- » Schutz vor Datenlecks und -diebstahl sowie Eindringen und Verbreitung von Malware
- » Umfassendes Reporting über Sicherheitsrisiken mit SafeGuard PortAuditor
- » Erkennen und Einschränken des Datentransfers nach Gerätetyp, -modell und Seriennummer
- » Überprüfen nach Dateityp, Beschränkung des unbefugten Datentransfers von externen bzw. an externe Speichermedien
- » Optionale Speicherung von Dateien, die von Usern auf Datenträger exportiert werden, als gespiegelte Datei („Schattenkopie“) am Server
- » Schutz der Unternehmensdaten beim Übermitteln an externe Speicher und Nachverfolgen der Offline-Verwendung
- » Blockieren von USB- und PS/2-Hardware-Keyloggern

### Einfache Verwaltung

- » Separate Sicherheitsrichtlinien für Domains, Gruppen, Computer oder User
- » Komfortable Verwaltung durch Integration von Microsoft Active Directory und Novell eDirectory
- » Rollenbasierte Administration
- » Verschlüsselte Protokoll-Dateien und Warnmeldungen können zur einfachen Berichterstellung oder Überprüfung in der Management-Konsole angezeigt oder für umfangreiche Analysen mit Drittsoftware integriert werden.

### Einfache Handhabung

- » SafeGuard PortProtector läuft transparent im Hintergrund
- » Veränderungen der Arbeitsgewohnheiten oder Training der Enduser überflüssig

## Die wichtigsten Funktionen

### Sicherheit

- Detaillierte Kontrolle: Erkennen und Begrenzen des Datentransfers nach Gerätetyp, Modell, Seriennummer und Datentyp, aber auch nach tatsächlichem Inhalt
- Datensicherheit: Schutz der Unternehmensdaten beim Übermitteln an externe Speicher und Nachverfolgen der Offline-Verwendung
- Dateispiegelung: Kopiert ein User Daten auf einen externen Datenträger, kann dieser Vorgang protokolliert oder zusätzlich eine „Schattenkopie“ dieser Daten am Server hinterlegt werden, so dass im Falle eines Verlustes des Datenträgers sein Inhalt genau rekonstruiert werden kann
- Secure Agent: Diskreter Einsatz im Hintergrund, redundantes Anti-Tampering verhindert eine Umgehung der Sicherheitsregeln
- Dateitypbasierte Kontrolle des Datentransfers sowohl von als auch auf externe Speichermedien
- Einfache Prüfung und Einsichtnahme: Verschlüsselte Protokoll-Dateien und Warnmeldungen können in der Management-Konsole angezeigt oder für umfangreiche Analysen und unverzügliche Benachrichtigungen mit Drittsoftware integriert werden
- Verbessertes Richtlinien-Enforcement über unabhängige auf Kernel-Ebene erfolgende Echtzeit-Analysen des systemnahen Port-Traffics
- Automatische Lastverteilung über mehrere Management-Server in einem Cluster möglich
- Integrierte Compliance-Richtlinien: Speziell konfigurierte Richtlinien, die eine direkte Verknüpfung von Sicherheitsrichtlinien mit Compliance-Standards (z.B. PCI, HIPAA, SOX, FISMA) ermöglichen

### Einfach handhabbar

- Enduser müssen ihre gewohnten Arbeitsabläufe nicht ändern
- Hohe Akzeptanz auf Userseite, da keine zusätzliches Training erforderlich ist

### Prüfung des Sicherheitsstatus am Endpoint

- Umfassender Überblick darüber, welcher User was mit welchem Endpoint verbindet
- Überblick über alle USB-, PCMCIA-, FireWire- und WiFi-Schnittstellen
- Detaillierte Aufzeichnung aller aktuellen und beendeten Geräteverbindungen
- Einfaches und aussagekräftiges Reporting

### System-Administration

- Flexible Richtlinien: Für alle Domains, Gruppen, Computer oder User können gesonderte Richtlinien festgelegt werden; Richtlinien können einfach Active Directory oder Novell-Organisationsobjekten zugeordnet werden
- Hierarchische Verwaltung über rollenbasierte Administration
- Intuitives Management: Nahtlose Integration mit Microsoft Active Directory, Novell eDirectory oder anderer Netzwerkmanagement-Software

### Sicherheitsfunktionen

- Kontrolle über Ports
- Kontrolle über Geräte
- Kontrolle über Speichervorgänge
- Verschlüsselung von Wechselmedien
- Dateityp-Kontrolle
- Inhaltsüberprüfung
- Protokollieren der Dateinamen
- Nachverfolgung der Offlineverwendung von verschlüsselten Geräten
- Granulare WiFi-Kontrolle
- Verzeichnis zugelassener CDs/DVDs
- Blockieren von Netzwerkbrücken
- Interne Port-Kontrolle
- Granulare Wi-Fi-Kontrolle
- Kontrolle der U3- und Autorun-Kontrolle
- Blockieren von USB- und PS/2-Hardware-Keyloggern
- Integration von Cisco NAC

## Systemanforderungen

### Hardware

- » PC mit Intel Pentium oder ähnlichem Prozessor
- » Mind. 25MB freier Festplattenspeicher

### Betriebssysteme

- » Microsoft Windows 2000
- » Microsoft Windows XP Professional (alle Service-Packs)
- » Microsoft Windows XP Tablet PC Edition
- » Microsoft Windows 2003 (alle Service-Packs)
- » Microsoft Windows Vista Business/Enterprise/Ultimate (SP1-2) 32-Bit
- » Microsoft Windows 7 Business/Enterprise/Ultimate 32-Bit

### Sprachen

- » Deutsch, Englisch, Japanisch\*
- » Administratorseitige Anpassung von Enduser-Nachrichten in allen Sprachen möglich

## Port-Kontrolle

### Physikalische Schnittstellen

- » USB
- » FireWire
- » PCMCIA
- » Secure Digital (SD)
- » Parallel
- » Seriell
- » Modem
- » Interne Ports

### Drahtlose Schnittstellen

- » Wi-Fi
- » Bluetooth
- » Infrarot (IrDA)

## Speicher-Kontrolle

- » Wechselmedien
- » Externe Festplatten
- » CD/DVD-Laufwerke
- » Diskettenlaufwerke
- » Bandlaufwerke

\*in Planung