



Vermeidung von Datenverlusten über Endpunkte und Wechselmedien

In Statistiken wird immer wieder deutlich, dass die größten Sicherheitsrisiken innerhalb der Unternehmen selbst lauern. Da sich über 70 % der Unternehmensdaten auf Endgeräten befinden, kann durch schriftliche Sicherheitsrichtlinien und reine Gateway-Sicherheitslösungen die Gefahr von Informationslecks im Unternehmen nicht entschärft werden.

Durch die zunehmende Anzahl an Wechselmedien, drahtlosen Schnittstellen sowie Benutzern mit Zugang zu sensiblen Daten wurden Informationslecks an Endpunkten, egal ob unbeabsichtigt oder bösartig, zu einer echten Bedrohung für Unternehmen. Es ist eben ganz einfach, an einem Endgerät – wie einem 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 Endpunkt 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 diesen gelesene Dateien überwacht, blockiert und protokolliert werden.

Zusätzlich steht mit **SafeGuard PortAuditor** Administratoren ein umfangreiches Werkzeug zur Verfügung, mit dem sie einen Überblick über die Verbindungen an Unternehmens-Endpunkten 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.

Die Vorteile

Verbesserte Sicherheit

- SafeGuard PortProtector schützt vor Datenlecks und -diebstahl sowie Eindringen und Verbreitung von Malware
- Umfassendes Reporting über Sicherheitsrisiken mit SafeGuard PortAuditor
- Erkennen und Einschränkung des Datentransfers nach Gerätetyp, -modell und Seriennummer
- Überprüfen nach Dateityp, Beschränkung des unbefugten Datentransfers von externen bzw. an externe Speichermedien
- Speichert vom Benutzer auf Datenträger exportierte Dateien optional 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

- Für alle Domänen, Gruppen, Computer oder Benutzer können gesonderte Sicherheitsregeln festgelegt werden
- Komfortable Verwaltung durch die Integration von Microsoft Active Directory® und Novell® eDirectory™
- Rollenbasierte Administration
- Verschlüsselte Log-Dateien und Warnmeldungen können zur einfachen Berichterstellung oder Überprüfung in der Managementkonsole angezeigt oder für umfangreiche Analysen mit Drittsoftware integriert werden

Einfache Handhabung

- SafeGuard PortProtector läuft transparent im Hintergrund – keine Veränderung der Arbeitsgewohnheiten oder Schulung der Endbenutzer notwendig

Über Utimaco – The Data Security Company.

Utimaco ist der führende Anbieter von Datensicherheitslösungen. Die Data Security Company ermöglicht mittleren bis großen Unternehmen den Schutz ihrer wertvollen Daten vor Angriffen und sorgt für die Einhaltung von Datenschutzbestimmungen, indem sie Vertraulichkeit und Integrität der Daten schützt. Die fortschrittlichen SafeGuard-Lösungen helfen, die Daten unter allen Umständen zu verwalten und zu schützen: beim Speichern (Data at Rest), während der Übertragung (Data in Motion) und während der Verarbeitung (Data in Use). Utimaco bietet seinen Kunden über ein weltweites Netzwerk von Partnern und Tochterunternehmen in Europa, den USA und Asien einen umfassenden Support vor Ort. Weitere Informationen finden Sie unter www.utimaco.de

Systemanforderungen

Hardware

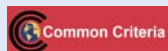
- Intel Pentium® oder vergleichbar
- Mindestens 25 MB freier Festplattenspeicher

Betriebssystem

- 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™

Zertifizierungen

- Common Criteria EAL 2



Sicherheitsfunktionen

- Kontrolle über Ports
- Kontrolle über Geräte
- Kontrolle über Speichervorgänge
- Verschlüsselung von Wechselmedien
- Kontrolle der Dateitypen
- Inhaltsüberwachung
- Protokollieren der Dateinamen
- Offlineverwendung von verschlüsselten Geräten nachverfolgen
- Granulare WiFi-Kontrolle
- Verzeichnis zugelassener CDs/DVDs
- Blockieren von Netzwerkbrücken
- Kontrolle über interne Ports
- Granulare WiFi-Kontrolle
- Kontrolle der U3- und Autorun-Funktionen
- Blockieren von USB- und PS/2-Hardware-Keyloggern
- Integration mit Cisco® NAC

Kontrolle über die Ports

Physikalische Schnittstellen

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

Drahtlose Schnittstellen

- WiFi
- Bluetooth
- WiFi, Bluetooth, Infrarot (IrDA)

Speichermedien

- Wechselspeichermedien
- Externe Festplatten
- CD/DVD-Laufwerke
- Diskettenlaufwerke
- Bandlaufwerke

Sprachversionen

- Englisch, Deutsch*, Japanisch*
- Hinweismeldungen für die Anwender können vom Administrator in beliebigen Sprachen definiert werden

*geplant

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 Benutzer 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

Prüfung des Sicherheitsstatus am Endpunkt

- Umfassender Überblick darüber, welcher Benutzer was mit welchem Endpunkt verbindet
- Überblick über alle USB-, PCMCIA-, FireWire- und WiFi-Schnittstellen
- Detaillierte Aufzeichnung aller aktuellen und beendeten Geräteverbindungen
- Einfache und aussagekräftige Berichte

System Administration

- Flexible Regeln: Für alle Domänen, Gruppen, Computer oder Benutzer können gesonderte Regeln festgelegt werden; Regeln 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
- Einfache Prüfung und Einsichtnahme: Verschlüsselte Log-Dateien und Warnmeldungen können in der Managementkonsole angezeigt oder für umfangreiche Analysen und unverzügliche Benachrichtigungen mit Drittsoftware integriert werden
- Automatische Lastverteilung über mehrere Management Server in einem Cluster möglich

Problemlose Nutzung

- Endbenutzer müssen ihre gewohnten Arbeitsabläufe nicht ändern
- Hohe Benutzerakzeptanz, da keine zusätzlichen Schulungen erforderlich

Weitere Informationen

- Auf unserer Website www.utimaco.de/portprotector finden Sie weitere Informationen.

Utimaco Safeware Partner:

Copyright Information

© 2007-2008 – Utimaco Safeware AG
SafeGuard® PortProtector Version 3.30

Alle SafeGuard Produkte sind eingetragene Marken der Utimaco Safeware AG. Alle anderen Marken sind Marken der jeweiligen Inhaber. Einzelne Funktionen können plattformbedingt, aufgrund der unterschiedlichen Fähigkeiten der Betriebssysteme, unterschiedliche Ausprägungen haben.

