

- Gewährleistet USB-Sicherheit durch die Verwaltung aller mobilen Medien/ Wechseldatenträgern
- Reduziert das Risiko eines Datendiebstahls/Datenverlustes
- Verhindert die Einführung von Malware über nicht-autorisierte Wechseldatenträger wie z.B. USB-Sticks
- Blockiert USB-Key-Logger
- Verschlüsselt Wechseldatenträger
- Stellt die Konformität mit geltenden Regelungen sicher

Reduzierung des Risikos eines Datenverlustes

Unternehmen sehen sich heute kontinuierlich mit dem Risiko eines Datenverlustes aufgrund der Verwendung mobiler Medien/ Wechseldatenträger und der sich daraus ergebenden Konflikte mit der Regelkonformität konfrontiert. Diese Probleme rangieren ganz oben auf der Top-Ten-Liste der vorrangigen Probleme moderner Unternehmen ¹. 62% der Unternehmen in Großbritannien waren bereits einem Sicherheitseinbruch ausgeliefert, wobei im Durchschnitt 8 Einbrüche pro Jahr verzeichnet werden – dabei verursacht jeder Sicherheitseinbruch Kosten in Höhe von durchschnittlich 90.000 Pfund Sterling ².

Nicht verwaltete mobile Medien/ Wechseldatenträger können schnell alle Schleusen öffnen und den Verlust von Daten in die falschen Hände ermöglichen, ob nun beabsichtigt oder versehentlich. Darüber hinaus machen die für eine private und interne Kontrolle geltenden Regelungen die Überwachung des ein- und abgehenden Datenflusses erforderlich.

Sanctuary bietet die nötige Kontrolle, um den ein- und abgehenden Datenfluss an den Netzwerkendpunkten effizient zu verwalten. Anhand von Audits zur Gerätenutzung lässt sich zudem die Konformität mit den internen Policies und gesetzlichen Regelungen gewährleisten.

Uneingeschränkte Kontrolle über alle mobilen Medien und Endpunktgeräte sowie den gesamten Port-Zugriff



Umfassendes Policy Enforcement für die Gerätenutzung

Sanctuary® Device Control, eine Sanctuary-Komponente, ermöglicht eine Policy-basierte Kontrolle der Nutzung externer Geräte im Hinblick auf die Steuerung des ein- und abgehenden Datenflusses an den Endpunkten. Durch die Verwendung des Whitelist-Konzeptes sorgt Sanctuary Device Control dafür, dass nur autorisierte Geräte auf Netzwerke, Laptops, Thin-Clients oder Desktops zugreifen können. Der Zugriff auf nicht-autorisierte Geräte wird kurzerhand verweigert. Ist ein Gerät bekannt, prüft der Device Control-Treiber die Zugriffsrechte des Benutzers in der Zugriffskontrollliste (ACL). Wenn der Benutzer über eine Zugriffsberechtigung für das Gerät verfügt, wird ihm ein Lese- oder Lese-/Schreibzugriff eingeräumt. Ist der Benutzer hingegen nicht berechtigt, auf das Gerät zuzugreifen, dann erhält er eine kontextgerechte Benachrichtigung mit entsprechendem Warnhinweis (Zugriffsverweigerung).

Administration und Management: einfach, schnell, flexibel

Sanctuary Device Control ermöglicht Administratoren die schnelle Identifizierung von Geräten und im Anschluss daran die Zuweisung von Zugriffsrechten an Benutzer, Benutzergruppen oder bestimmte Computer für eine Geräteklasse, ein bestimmtes Gerät oder ein spezifisches Medium. Die Verwaltung der Gerätezugriffsrechte erfolgt zentral über eine höchst einfache und effiziente Oberfläche.

Die Gerätepolices sind mit den in Active Directory™ oder eDirectory™ gespeicherten

Benutzer- und Benutzergruppendaten verknüpft und tragen dadurch zu einer wesentlichen Vereinfachung der Verwaltung der Gerätere Ressourcen an den Endpunkten bei.

Detaillierte Audit-Funktionen

Unter Verwendung der zum Patent angemeldeten bidirektionalen I/O-Shadowing-Technologie von Sanctuary werden die Namen, auf Wunsch auch der Inhalt aller Dateien aufgezeichnet, die von Disketten, CDs/DVDs und mobilen Geräten eingelesen bzw. darauf geschrieben werden. Jeder versuchte Zugriff auf ein Gerät kann aufgezeichnet werden. Auch die Aufzeichnung der von den Administratoren durchgeführten Aktionen ist möglich, u. a. der an den Zugriffsrechten für Geräte vorgenommenen Änderungen.

Kontrollierte Verschlüsselung

Mobile Geräte/Wechseldatenträger können verschlüsselt werden, sodass ein sicherer Betrieb und Transport möglich wird und die Gefahr des Zugriffs auf vertrauliche Daten durch nicht-autorisierte Benutzer verhindert wird. Die Benutzer können auf ihre verschlüsselten Daten auch von Rechnern aus zugreifen, auf denen die Sanctuary-Software nicht installiert wurde.

Anhand zentraler wie auch dezentraler Verschlüsselungsschemata erhalten die Sanctuary-Administratoren die erforderliche Flexibilität, um mobile Medien von einer zentralen Stelle aus zu verschlüsseln oder Benutzern die selbstständige Verschlüsselung ihrer mobilen Medien/Wechseldatenträger zu ermöglichen. Damit – und das ist von ganz entscheidender Bedeutung – lässt sich die Nutzung der verschlüsselten Medien umfassend kontrollieren.

Eigenschaften	Funktionen	Vorteile
Whitelist	Benutzern oder Benutzergruppen werden Zugriffsberechtigungen für autorisierte Geräte zugewiesen – Standardmäßig gilt: Keine Autorisierung, kein Zugriff	Verhindert die Nutzung unbekannter bzw. unerwünschter Geräte in Ihrem Netzwerk und reduziert das Risiko von Datenverlust und Malware. Hierdurch lässt sich auch die Stabilität des Netzwerks verbessern
Unterstützung mehrerer Sprachen für die Client-Oberfläche	Auf den Sanctuary-Clientrechnern werden 12 Sprachen unterstützt	Vereinfacht die Arbeit für Benutzer in internationalen Unternehmen
Leistungsstarke und flexible Logging-Möglichkeiten und Berichterstattung	Detaillierte Logging-Möglichkeiten mit flexiblen Filter-, Sortier- und Anzeigooptionen und gespeicherten Abfragevorlagen sowie zentraler Berichterstattung	Ermöglicht die Sicherstellung der Policy-Übereinstimmung sowie das Einschreiten bei verdächtigem Verhalten im Hinblick auf die Ergreifung rechtlicher oder verwaltungstechnischer Schritte
Schutz für offline/entfernte Computer	Konstanter Schutz durch die Verwaltung einer lokalen Kopie der letzten Hash- und Berechtigungsliste auf jedem offline Rechner	Ermöglicht den Schutz der Rechner ungeachtet der Netzwerkverbindung, so dass sichergestellt werden kann, dass auch entfernte oder nicht verbundene Benutzer geschützt sind
Unterstützung von Active Directory und eDirectory	Die bereits vorhandenen Benutzer- und Benutzergruppendefinitionen in Microsoft Active Directory und Novell eDirectory werden genutzt	Umgeht den doppelten Arbeitsaufwand bei der Definition von Benutzern/Benutzergruppen für die Zugriffskontrolllisten und reduziert dadurch den Aufwand bei der Konfiguration und laufenden Instandhaltung
Hochskalierbare Architektur	Three-Tier-Architektur mit Datenbank, einem oder mehreren Applikationsservern und Clients	Ermöglicht die flexible und hochskalierbare Gestaltung grosser und komplexer Netzwerke
Silent-Installation ohne Eingriff	Installation mit Hilfe beliebiger Implementierungstools mit MSI-Setup (z. B. Microsoft Systems Management Server (SMS), Group Policies, WinInstall usw.)	Beschleunigt und vereinfacht die Implementierung
Berechtigungen auf der Grundlage einer Zugriffskontrollliste (Access Control List, ACL)	Zugriffsberechtigungen für Geräte, die sich für Benutzer bzw. Benutzergruppen vergeben lassen, basierend auf Active Directory oder eDirectory	Ermöglicht die Erstellung detaillierter Zugriffsrechte für die Benutzer unabhängig vom Arbeitsplatz
Variable Berechtigungsvergabe im Rahmen der Gerätekontrolle	Mögliche Berechtigungseinstellungen: Lese-/Schreibzugriff, zeitlich begrenzter Zugriff, Online/Offline-Nutzung, spezifische Schnittstellen, HDD/Nicht-HDD-Geräte u.v.a	Eliminiert das Risiko eines Zugriffs auf das Netzwerk durch nicht autorisierte Geräte und stattdessen gleichzeitig die Benutzer mit der für ihre Tätigkeit erforderlichen Flexibilität aus
Eindeutige Identifizierung und Autorisierung bestimmter Medien	Bestimmte DVD/CD-ROMs können für den Zugriff von Benutzern oder Benutzergruppen autorisiert und Wechseldatenträger verschlüsselt werden	Verringert den Zugriff auf nur im Unternehmen erlaubte DVDs und CD-ROMs. Verhindert Zugriff auf unerlaubte Daten bzw. den Zugriff auf Daten durch unautorisierte Benutzer
Plug-and-Play-Geräte: Hot Plug Unterstützung	Erkennung von Plug-and-Play-Geräten im laufenden Betrieb	Produktivität bleibt erhalten, die Tätigkeit wird nicht durch die Verwaltung und den Gebrauch von Plug-and-Play-Geräten unterbrochen
Option für bidirektionales Shadowing	Die zum Patent angemeldete Shadowing-Technologie ermöglicht die Speicherung aller Daten, die aus Geräten ausgelesen und/oder darauf geschrieben werden	Erfasst den Fluss von Informationen in das und aus dem Netzwerk, wodurch sich das Risiko und die damit verbundenen Auswirkungen eines Datenverlustes erheblich eingrenzen lassen
Beschränkung der kopierten Datenmenge	Möglichkeit, die Datenmenge zu beschränken, die vom PC (oder Netzwerk) auf ein externes Gerät (Wechselmedien oder Diskette) kopiert wird	Verhindert den Verlust von großen Mengen vertraulicher Informationen
Schutz vor PS/2- und USB-Key-Loggern	Blockierung der PS/2-Anschlüsse, Kontrolle der Nutzung von USB-Tastaturen und Identifizierung/Blockierung aller gängigen Modelle von USB-Key-Loggern	Reduziert das Risiko des Zugriffs auf vertrauliche Informationen über Key-Logger
Dateityp-Filterung	Kontrolle des Dateityps der auf Wechseldatenträger geschriebenen bzw. der von dort ausgelesenen Dateien	Reduziert das Risiko des Eindringens unerwünschter Dateien in das Netzwerk sowie des Verlustes sensibler Dateien aus dem Netzwerk

Zur Verfügung steht ebenfalls Sanctuary Application Control mit integrierter Sanctuary-Managementkonsole. Sanctuary Application Control ermöglicht eine Policy-basierte Kontrolle der Anwendungsnutzung im Hinblick auf den Schutz der Endpunkte vor Malware, Spyware, Zero-Day-Bedrohungen und unerwünschter oder nicht-lizenzierter Software.

Unterstützte Gerätetypen

- USB-Memory-Sticks
- ZIP-Laufwerke
- PDAs
- Bandlaufwerke
- Festplatten
- Diskettenlaufwerke
- Biotech-Laufwerke
- Modems
- Wireless-LAN-Adapter
- Digitalkameras
- CD/ DVD-Brenner/ Player
- Scanner
- Smart Card-Lesegeräte
- USB-Drucker

Unterstützte Schnittstellen

- USB
- FireWire
- BlueTooth
- WiFi
- PCMCIA
- PS/2
- LPT
- IrDA
- IDE
- COM
- S-ATA
- SCSI

Systemanforderungen

Client (nur 32-Bit-Windows)

Windows 2000 (SP 3+) Professional, Windows XP Professional, Windows XPe, Windows Embedded Point of Service, Windows XP Tablet PC Edition

Bei Sanctuary Server/Terminal Services Edition: Windows 2000 Server oder Windows Server 2003

Datenbank

Windows 2000 (SP 3+) Server oder Professional, Windows XP Professional, Windows Server 2003

Microsoft SQL Server (2000/2005), SQL Server 2005 Express Edition oder MSDE 2000

Server

Windows 2000 (SP 4+) Server oder Windows Server 2003

Management-Konsole

Windows 2000 (SP 3+) Server oder Professional, Windows XP Professional, Windows Server 2003

Quellen

- 1 - Yankee Group 2005, ESG 2005, Forrester 2005
- 2 - 2006 CSI/FBI Computer Crime and Security Survey



www.securewave.com
info@securewave.com

Nordamerika

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America
+1 (703) 713 - 3960 Phone
+1 (703) 793 - 7007 Fax

Großbritannien

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom
+44 (0) 1908 357 897 Phone
+44 (0) 1908 357 600 Fax

Kontinental Europa und die restliche Welt

Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364-11 Phone
+352 265 364-12 Fax

© 2007 SecureWave und Sanctuary sind eingetragene Marken der SecureWave SA. Alle Marken von Drittherstellern sind das Eigentum ihrer jeweiligen Inhaber.

