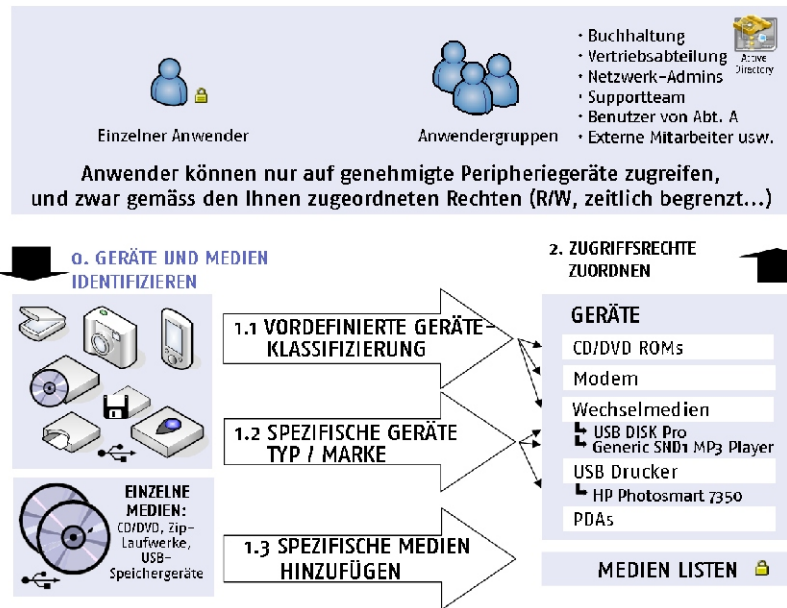


Sanctuary® Device Control erweitert die Kontrolle der Sicherheitsrichtlinien von I/O-Geräten sowohl auf Windows als auch auf Novell Umgebungen. Nach dem Grundsatz des möglichst restriktiven Zugriffs ist für alle Benutzer der Zugriff standardmäßig nicht erlaubt. Um diesen zu gewähren, braucht der Administrator nur die Objekte (OUs, Benutzer und Benutzergruppen) den Geräten oder Geräteklassen zuzuordnen.

Administration wird schnell, einfach und flexibel



Nach der Installation von Sanctuary® Device Control erfasst der Administrator (Schritt 0) alle verschiedenen Geräte (Standard und unternehmensspezifische Geräte) und Medien (CDs, DVDs, usw.). Anschließend werden die Geräte gemäß den Windows-Geräteklassen automatisch vordefinierten Geräteklassen zugeordnet (Schritt 1.1). Der Administrator kann ebenfalls spezifische Geräte je nach Art oder Typ festlegen (Schritt 1.2). Die spezifischen Medien (CDs, DVDs, usw.) werden in die Media List eingefügt (Schritt 1.3). Der Administrator braucht nur die Zugriffsrechte und Attribute den Benutzern, Benutzergruppen oder einem bestimmten Computer zuzuweisen (Schritt 2).

Die Administration von Änderungen und Erweiterungen geschieht zentral mit einem einfachen "Outlook style"-Interface.

Verwaltete Gerätezugangssteuerung

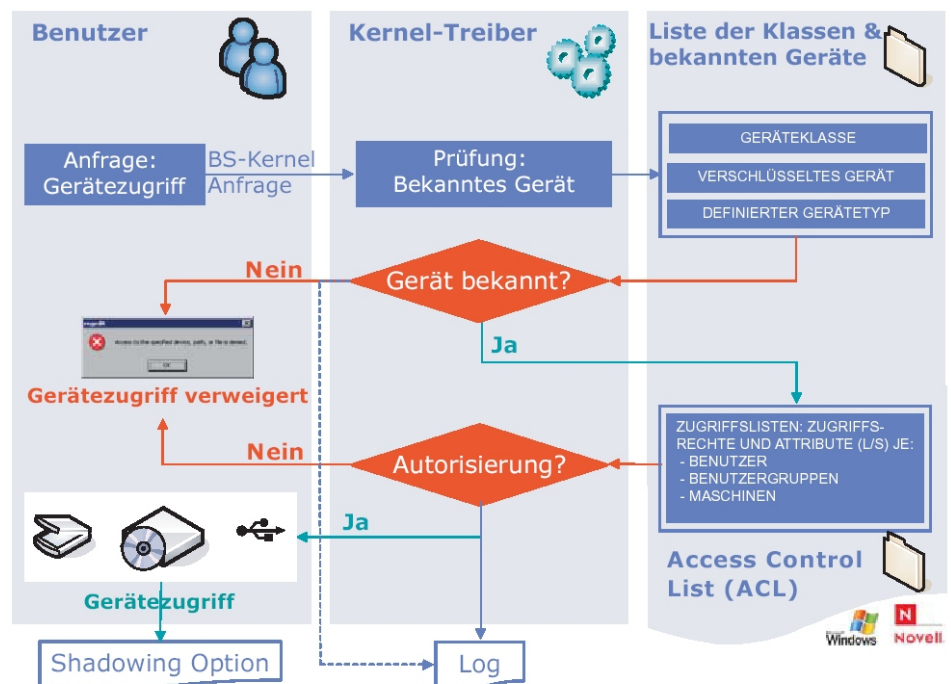
Jedes Mal, wenn ein Nutzer auf ein Gerät zugreifen will, wird die Anforderung auf Kernel-Ebene durch den Treiber von Sanctuary® Device Control abgefangen.

Wenn das Gerät nicht in der Liste der autorisierten Klassen aufgeführt ist, verweigert Sanctuary® Device Control seine Nutzung.

Wenn das Gerät (in der Geräteklassenliste) vorhanden ist, überprüft der Treiber die Benutzerrechte in der Zugriffskontrollliste (Access Control List, ACL). In diesem Fall hat der Benutzer die Zugriffsrechte auf das Gerät, z. B. einen CD-Brenner. Die Rechte werden mit Lese- oder Schreibzugriff erteilt.

Wenn der Benutzer keine Rechte zum Gerät hat, erscheint eine Meldung, die ihm die Zugriffsverweigerung mitteilt.

Sanctuary® Device Control kann die Übertragung von Daten zu autorisierten Geräten überwachen. Die Shadowing-Option kann entweder nur den Namen der kopierten Datei oder eine komplette Kopie derselben liefern. Die kopierten Daten werden zur späteren Inspektion durch den Administrator zum Anwendungs-Server hochgeladen. Sanctuary® Device Control bietet auch vollständige Überwachung aller Administratormassnahmen einschließlich aller Änderungen von Zugriffsrechten auf Geräte.



Hauptfunktionen und -merkmale

Zugriffsrechte unterliegen einer Zugriffskontrollliste (Access Control List, ACL)

- Auf Benutzer oder Benutzergruppe abgestimmte Zugriffsrechte
- Rechnerspezifische Zugriffsrechte möglich

Einzelgeräte-"White List"

- Verhinderung der Nutzung unbekannter Geräte
- Zulassung spezifischer Gerätetypen in einer Klasse
- Eindeutige Kennzeichnung eines bestimmten Gerätes*

Zeitlich eingeplanter und befristeter Zugriff

- Lese- und/oder Schreibzugriff
- Zeitlich eingeplanter Zugriff für eine vordefinierte Dauer
- Befristeter Zugriff

Eindeutige Kennzeichnung und Zulassung bestimmter Wechselmedien

- Erstellung von DVD-/CD-ROM-Sammlungen und Zugriffsgewährung für Benutzer oder Benutzergruppen
- Erstellung von Listen bestimmter Wechselmedien mit eindeutigen IDs und Zugriffsrechte für Benutzer*
- Möglichkeit der Autorisierung beliebiger Wechselmedien für beliebige Benutzer und anschließende Verschlüsselung der Daten auf dem Wechselmedium

Plug-and-Play-Geräte: Hot-Plug-Unterstützung

- Erkennung von Plug-and-Play-Geräten im laufenden Betrieb
- Anwendung der ACL in Echtzeit

Mächtige Audit-Fähigkeiten und Shadowing

- Fähigkeit, sämtliche auf externe Geräte oder bestimmte Ports gesendete Daten aufzuzeichnen
- Eine vollständige Kopie der auf einem E/A-Gerät gespeicherten Daten kann erfasst und zentral hinterlegt werden (in Echtzeit oder verzögert)
- Fortgeschrittene Reporting-Möglichkeiten (Benutzer bzw. Gerätebezogen)
- Unterstützt alle CD/DVD Brennertypen
- Shadow-Regeln können auf Geräte und Gerätegruppen und pro Benutzer vergeben werden

Beschränkung der kopierten Datenmenge

- Möglichkeit, die Datenmenge zu beschränken, die vom PC (oder Netzwerk) auf ein externes Gerät (Wechselmedien oder Diskette) kopiert wird

Ereignisanzeige

- Benachrichtigung der Benutzer mit angepassten Mitteilungen bei Zugriffsverletzungen

Offline Updates

- Fähigkeit, Updates an Computer zu senden, die nicht mit dem Netzwerk verbunden sind

Getrennte Rechner geschützt

- Auf dem getrennten PC oder Laptop wird eine lokale Kopie der letzten Zugriffsrechteliste gespeichert. Selbst wenn dieser vom Netzwerk getrennt ist, bleibt umfassender Schutz gegeben. Aktualisierungen werden gegebenenfalls bei der nächsten Anmeldung wirksam

Kontextbezogene Rechtevergabe

- Erlaubt die Festlegung von eindeutigen Richtlinien für sämtliche Geräte sowohl innerhalb (online) als auch außerhalb (offline) des Unternehmensnetzwerkes

Skalierbarkeit

- Die Nutzung einer dreistufigen Architektur (Anwendungsserver, Datenbank, Client) bietet dem Unternehmen flexible Einsatzmöglichkeiten und Skalierbarkeit

Option "Easy Exchange"

- Autorisierte Benutzer können auf verschlüsselte Wechselmedien zugreifen ohne vorherige Installation irgendwelcher Software und auch ohne administrative Berechtigungen

Active Directory und eDirectory Unterstützung

- Einrichten der Zugriffsrechte auf I/O-Geräte für existierende Windows Active Directory und Novell eDirectory Objekte
- Die Delegation von Administrationsrechten der Active Directory Organizational Units wird automatisch in die Verwaltung von Sanctuary® Device Control übernommen

Abwehr von PS/2 und USB Hardware Keyloggern

- Fähigkeit, den PS/2 Port zu blockieren und so die Benutzung von USB-Tastaturen zu erzwingen, um die Bedrohung durch PS/2 Hardware Keyloggern zu verhindern
- Möglichkeit zum Sperren gängiger USB Keylogger

Aktualisierung der Zugriffsrechte

- Aktualisierungen der Zugriffsrechte werden bei jeder Anmeldung wirksam
- Zuweisung der Zugriffsrechte im laufenden Betrieb möglich (ohne erneute Anmeldung)

Verteilung der Sanctuary Client-Software

- Die Client-Software kann installiert werden, ohne dass der Applikationsserver erreichbar ist – optional mit bereits konfigurierten Berechtigungen

Unbeaufsichtigte Installation (Silent Installation)

- Verwendung aller Installationstools, die das MSI Setup benutzen (z.B. Microsoft Systems Management, Group Policies, WinInstall, usw.)
- Das Deploy-Tool besitzt die Fähigkeit zur Installation und Deinstallation, zum Upgrade und zur Abfrage des Client-Status'

*Nicht unterstützt mit Novell