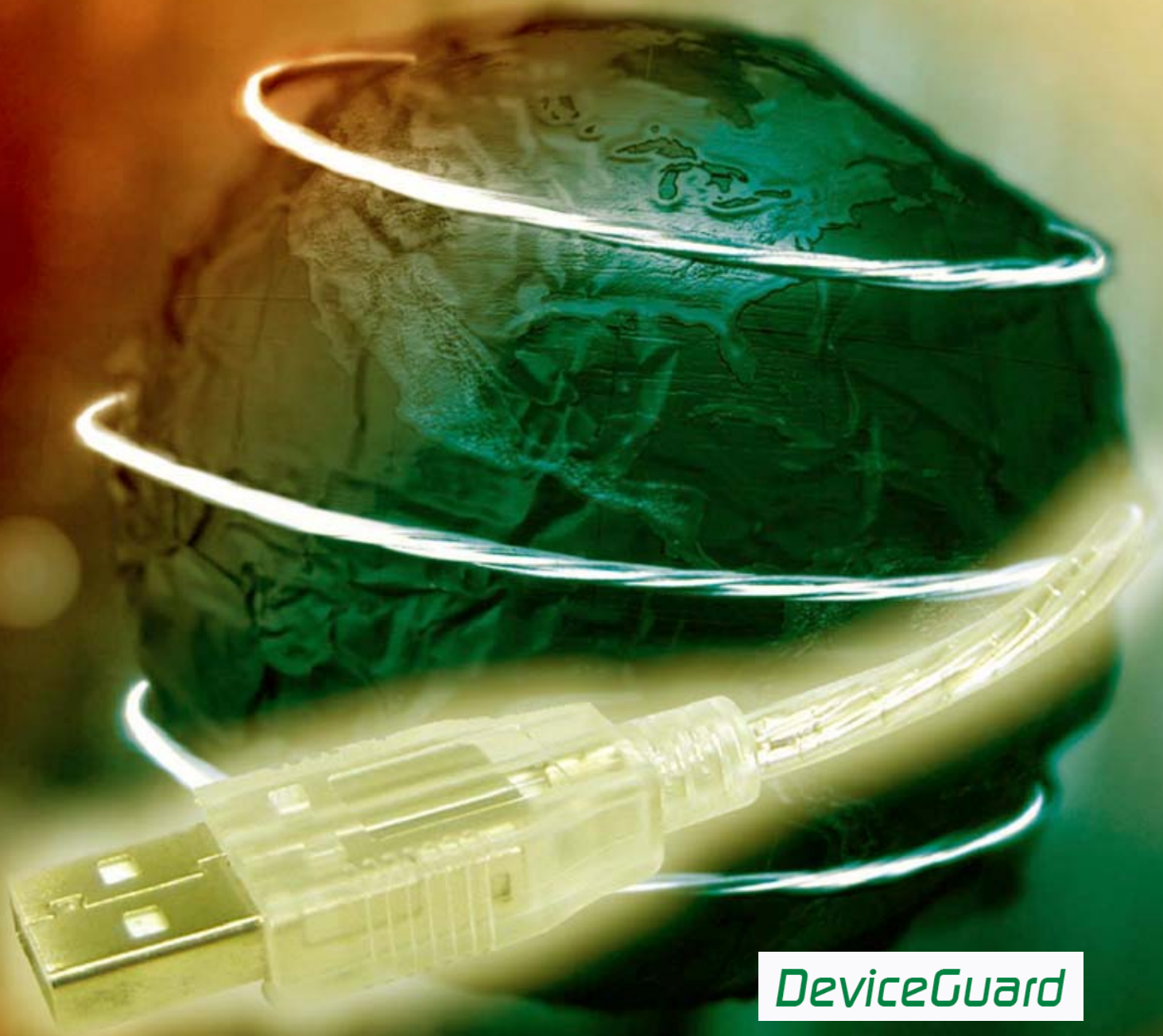


DeviceGuard

Die Software für sichere Schnittstellen.



DeviceGuard

DeviceGuard – Die Software für sichere Schnittstellen.

Das Problem mit den unsicheren Schnittstellen

Das Problem kennt jeder. Über USB, FireWire, PCMCIA oder Parallelport werden Datenträger am PC angebunden und der ungehemmte Datenaustausch kann beginnen. Unter Windows NT 4.0 war dies weniger ein Problem, da z. B. USB nicht unterstützt wurde. Nun haben wir USB, alle freuen sich über die Flexibilität, aber die Datensicherheit bleibt auf der Strecke. Im Zeitalter von Memory-Sticks, USB-Festplatten, FireWire-Festplatten und Digitalkameras wird der Umgang mit Datenträgern deutlich flexibler.

Der praktische Ansatz

Logische Laufwerke

Die meisten Medien, über die Daten ausgetauscht werden, stehen als logische Laufwerke auf dem Windows Desktop zur Verfügung. Hier interessiert es uns zunächst nicht, welches physikalische Medium dahinter steckt, sondern wie es sich dem Anwender präsentiert. Und das sind fast immer Wechseldatenträger (Memory-Sticks, PCMCIA-Festplatten, USB-Festplatten, Digitalkameras).

USB-Schnittstellen

Die meisten mobilen Geräte, die heutzutage an PCs / Notebooks ansteckbar sind, werden über USB angeschlossen. Dies sind Tastaturen, Mäuse, Joysticks, Drucker, Scanner, Festplatten, Flash-Card-Reader, Soundadapter, Digitalkameras und Netzwerkadapter.

Das Besondere an DeviceGuard

- Extrem klein, effizient und robust
- Einfache Implementierung und beinahe wartungsfrei
- Kein separates Administrationstool erforderlich
- Kein Overhead
- Sehr flexibel in den Einsatz- und Konfigurationsmöglichkeiten
- Besonders preiswert

Was bietet DeviceGuard?

DeviceGuard überwacht die logischen Laufwerke, die dem Anwender auf dem Desktop präsentiert werden und steuert den Zugriff auf diese Laufwerke auf Computer- und / oder Benutzer-Ebene. DeviceGuard überwacht alle an den USB-Ports angeschlossenen Geräte und steuert den Zugriff auf Computer- und / oder Benutzer-Ebene.

Administration von DeviceGuard

Sämtliche Konfigurationsparameter für DeviceGuard stehen in der Registry (HKLM / HKCU) und werden bevorzugt über Gruppenrichtlinien des Microsoft Active Directory administriert. Dies muss aber nicht sein – DeviceGuard kann auch über alle anderen Registry-Administrations-Möglichkeiten, die dem Administrator zur Verfügung stehen, konfiguriert werden. Durch die transparente Dokumentation aller Konfigurationsmöglichkeiten kann der Administrator leicht selbst Hand anlegen.

Die Registry-basierte Konfiguration hat den positiven Nebeneffekt, dass DeviceGuard nach der Erstkonfiguration auch ohne Netzwerk korrekt arbeitet.





Protokollierung

Optional kann DeviceGuard alle wichtigen Aktionen auf unterschiedliche Weise protokollieren (LOG-Datei und / oder SMTP Nachrichten). Die Protokollierung umfasst hauptsächlich die durch DeviceGuard initiierten Sperrungen. Optional kann auch eine Unterdrückung von Benutzerinformationen erfolgen. Somit ist nicht nachvollziehbar, welcher Benutzer versucht hat, ein nicht erwünschtes Gerät an einem PC in Betrieb zu nehmen. Dieser Punkt wird häufig von Betriebsräten / Personalräten gefordert.

Sicherheit von DeviceGuard

DeviceGuard läuft als Dienst mit lokalen System-Rechten und kann nicht als Benutzer oder Hauptbenutzer beendet werden. Den gleichen Schutz erfahren der Task (deviceguard) und das Hauptprogramm (deviceguard.exe).

Die Konfigurationsparameter in der Registry können ebenfalls durch den Anwender nicht verändert werden.

Installation

Zur Installation von DeviceGuard auf PCs und Notebooks ist ein Softwarepaket für die meisten Softwareverteilungs-Produkte vorbereitet. Die Installation muss mit administrativen Rechten erfolgen.

Systemvoraussetzungen

DeviceGuard läuft auf allen Systemen mit

- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista (beta).

Kontakt

e-mail: info.kilonca.de
Website: www.kilonca.de

