

# DeviceLock White Paper

## Inhalt:

- [Warum DeviceLock?](#)
- [Was ist so besonders an DeviceLock?](#)
- [Wer braucht DeviceLock?](#)
- [Wie funktioniert DeviceLock?](#)
- [Wer hat DeviceLock entwickelt?](#)
- [Wo können Sie DeviceLock Software erhalten?](#)
- [Technischer Support für DeviceLock](#)
- [Preise für DeviceLock](#)
- [Bestellung und Registrierung](#)
- [Kontaktinformation](#)



## Warum DeviceLock?

Die Kontrolle darüber zu haben, was in ein Computernetzwerk eines Unternehmens heraufgeladen oder aus ihm heruntergeladen wird, ist zentral für die IT-Sicherheit. Aber eben diese Kontrolle zu behalten, wird von Tag zu Tag schwieriger. Die schnell wachsende Popularität von tragbaren USB-Speichergeräten stellt eine offensichtliche Bedrohung dar. Dieser Markt wächst exponentiell\*, wobei die Geräte immer schneller, immer kleiner und immer leistungsfähiger werden. Und denken Sie an Bluetooth-Geräte, die so bedienerfreundlich konzipiert sind, dass sie standardmäßig mit jedem erreichbaren Bluetooth-Client kommunizieren – und der erreichbare Bereich kann ziemlich weit sein. Außerdem verlangt der Markt nach immer besserem Netzwerkzugang für drahtlose Geräte, und diese Nachfrage lässt sich wahrscheinlich nicht von Sicherheitsbedenken eindämmen.

Auf kurze Sicht stellen die Marktkräfte überwältigende Sicherheitsprobleme dar. Es ist nicht etwa so, dass die Unternehmen über die wachsende Verwundbarkeit nicht Bescheid wüssten. Die Medien berichten oft über Fälle, in denen Übeltäter von innerhalb oder außerhalb eines Unternehmens sensible Informationen herunterladen und abziehen, wobei die Ziele von Wirtschaftsspionage über Erpressung bis hin zu Terrorismus reichen. Es ist auch nicht so, dass Unternehmen nichts in Sachen Sicherheit täten. Investitionen in Firewalls, Verschlüsselung und andere Technologien und Kontrollen, die konzipiert sind, um Netzwerkdaten vor Diebstahl über das Internet zu schützen, nehmen sicherlich zu. Allerdings bieten diese Maßnahmen wenig Schutz für lokal ungesicherte Geräte und Ports. Sie können nichts gegen den angestellten Spion ausrichten, der einen 2 GB-Memorystick am Schlüsselanhänger mitbringt, ihn in den USB-Port einsteckt und beginnt, sensible Daten herunterzuladen. Ebenso wenig werden sie den frustrierten Angestellten daran hindern, mit einem ähnlichen Gerät einen Trojaner oder ein anderes schädliches Programm in das Netzwerk zu laden. Um diesen Problemen zu begegnen, ist es notwendig, dass Administratoren kontrollieren können, wer wann Zugriff auf externe Medienlaufwerke hat.

DeviceLock von DeviceLock, Inc. bietet dieses Kontrollniveau für Microsoft Windows-basierte Netzwerke. Es ist eine reine Software-Lösung, die es Netzwerkadministratoren erlaubt, Berechtigungen zuzuweisen für USB- und FireWire-Ports, für WiFi- und Bluetooth-Adapter wie auch für Disketten- und CD-ROM-Laufwerke, für Bandgeräte und andere entnehmbare Medien. Es löst also physische Sicherheitsprobleme ohne physische Sperren.

---

\* Die Zahl der USB Flash Drives wird von etwa 10 Millionen ausgelieferten Geräten im Jahre 2002 auf voraussichtlich nahezu 50 Millionen im Jahre 2006 steigen, gemäß einer Studie von Semco Research Corp, „Will USB Flash Drives Change Our Lives?“

## Was ist so besonders an DeviceLock?

Indem DeviceLock Netzwerkkontrolle darüber bietet, welche Benutzer auf Ports und Geräte auf einem lokalen Computer zugreifen können, schließt es ein potenziell riesiges Sicherheitsloch auf einfache und kostengünstige Weise. Es bedeutet also eine große Verbesserung gegenüber dem Nichtstun. Verglichen mit physischen Lösungen, welche die Lagerung und Verwaltung von Hardware-Sperren und Schlüsseln erfordern, ist es viel billiger und lässt sich viel einfacher im gesamten Unternehmen implementieren. Verglichen mit anderen rein softwarebasierten Methoden zur Kontrolle lokaler Hardware durch den Administrator (wie etwa die Änderung des BIOS) ist DeviceLock eine elegantere, einfacher zu skalierende Lösung.

DeviceLock bietet eine klare und bedienerfreundliche Oberfläche mit einfachen Setup-Assistenten und vielfältigen grafischen Ansichten der Information. Netzwerkadministratoren können DeviceLock sogar von Ferne auf Workstations installieren und warten. Konzipiert, um unter Windows NT/2000/XP/Vista/7 und Windows Server 2003/2008 zu laufen, bietet es auch automatisierten Support für die Installation und Deinstallation.

DeviceLock kann auch per Gruppenrichtlinie in einer Active-Directory-Domäne verwaltet und bereitgestellt werden. Gruppenrichtlinien bieten Flexibilität und unterstützen ausführliche Konfigurationsinformation mit Hilfe von Verzeichnisdiensten und Mitgliedschaft in Sicherheitsgruppen. Richtlinien-Einstellungen werden mit Hilfe des Snap-Ins Microsoft Management Console (MMC) für Gruppenrichtlinien erstellt. Eine engere Integration in das Active Directory erleichtert Systemadministratoren die Verwaltung und den Einsatz von Berechtigungen per DeviceLock für große Netzwerke. Durch Integration in das Active Directory müssen keine weiteren Anwendungen anderer Hersteller für zentralisierte Verwaltung und Verteilung mehr installiert werden. DeviceLock benötigt keine eigene serverbasierte Version, um das gesamte Netzwerk zu steuern, stattdessen verwendet es Standardfunktionen, die das Active Directory bereitstellt.

Für Unternehmen, die standardmäßig Software- und Hardware-basierte Verschlüsselungslösungen wie PGP Whole Disk Encryption, TrueCrypt, DriveCrypt und Lexar SAFE PSD S1100 und SAFE PSD S1100 USB-Laufwerke einsetzen, erlaubt DeviceLock den Administratoren, die Richtlinien zur Verschlüsselung, die ihre Mitarbeiter befolgen müssen, wenn sie entnehmbare Geräte für Speicherung und Abruf von Unternehmensdaten verwenden, zentral zu definieren und aus der Ferne zu steuern. So kann beispielsweise bestimmten Mitarbeitern oder ihren Gruppen erlaubt werden, nur auf solche USB-Flash-Laufwerke zu schreiben oder von ihnen zu lesen, die auf bestimmte Weise verschlüsselt wurden, während anderen Benutzern des Unternehmensnetzwerks erlaubt werden kann, von nicht-verschlüsselten entnehmbaren Speichergeräten nur zu lesen, aber nicht auf sie zu schreiben.

DeviceLock schützt nicht nur Ihr Netzwerk und Ihre lokalen Computer vor Datendiebstahl und Netzwerkbeschädigung durch entnehmbare Datenträger, sondern erlaubt Ihnen auch, die Port- und Geräteaktivität vollständig zu protokollieren.

Der IT-Auditor des Unternehmens kann mit Hilfe der optionalen Daten-Shadowing-Funktion von DeviceLock signifikant zuverlässiger sicherstellen, dass keine sensiblen Informationen auf entnehmbaren Medien nach außen gelangen. Diese Funktion erfasst vollständige Kopien der Dateien, die auf autorisierte entnehmbare Geräte und Windows Mobile PDAs/Smartphones kopiert, auf CD/DVD gebrannt oder sogar von autorisierten Benutzern ausgedruckt werden. Shadowing-Kopien werden auf einer zentralen Komponente eines bestehenden Servers und auf einer beliebigen bestehenden ODBC-kompatiblen SQL-Infrastruktur gespeichert.

DeviceLock Search Server ermöglicht Volltextsuche in auf DeviceLock Enterprise Server gespeicherten Protokolldaten. Die Volltextsuchfunktion ist besonders nützlich in Situationen, in denen der IT-Auditor des Unternehmens nach Shadow-Kopien von Dokumenten aufgrund ihres Inhalts suchen muss. DeviceLock Search Server kann Dokumente automatisch erkennen,

indizieren, durchsuchen und anzeigen, und zwar in den folgenden Formaten: Adobe Acrobat (PDF), Ami Pro, Archive (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (Dokumente, Spreadsheets und Präsentationen), Quattro Pro, WordPerfect, WordStar und viele andere.

## **Wer braucht DeviceLock?**

Zu dem schnell wachsenden Kundenstamm von DeviceLock zählen Unternehmen, die auf die sichere Handhabung von Kunden- und Unternehmensdaten geprüft werden, Regierungsbehörden, die sensible Informationen verwalten, und professionelle Dienstleistungsfirmen und andere kleine und mittlere Unternehmen, die den Zugriff auf Geräte steuern müssen.

Hier sind ein paar Beispiele für die Verwendung von DeviceLock:

- Kontrollieren Sie, welche Benutzer oder Gruppen Zugriff haben auf USB-, FireWire-, Infrarot-, COM- und LPT-Ports; WiFi- und Bluetooth-Adapter; jeden Druckertyp, einschließlich lokale, virtuelle und Netzwerkdrucker; Windows Mobile, BlackBerry, iPhone und Palm OS-basierte PDAs und Smartphones; ebenso wie DVD/CD-ROMs, Diskettenlaufwerke und andere entnehmbare und Plug-and-Play-Geräte.
- Erlauben oder verweigern Sie selektiv den Zugriff auf gewisse Dateitypen für entnehmbare Medien.
- Kontrollieren Sie den Zugriff auf Laufwerke abhängig von Tageszeit und Wochentag.
- Definieren Sie, welche Arten von Daten (Dateien, Kalender, E-Mails, Aufgaben, Notizen usw.) zwischen Unternehmens-PCs und persönlichen mobilen Geräten synchronisiert werden dürfen.
- Definieren Sie verschiedene Online- vs. Offline-Sicherheitseinstellungen für den gleichen Benutzer oder die gleiche Benutzergruppe.
- Erkennen Sie verschlüsselte PGP-, DriveCrypt- und TrueCrypt-Festplatten (USB Flash Drives und andere entnehmbare Medien) ebenso wie Lexar SAFE PSD und Lexar JumpDrive SAFE S3000 verschlüsselte Flash Drives und wenden Sie spezielle „verschlüsselte“ Berechtigungen darauf an.
- Autorisieren Sie nur spezifische USB-Geräte, die ungeachtet anderer Einstellungen nicht gesperrt werden.
- Gewähren Sie Benutzern temporären Zugriff auf USB-Geräte, wenn keine Netzwerkverbindung besteht (Sie liefern den Benutzern telefonisch spezielle Zugriffscodes, die temporär den Zugriff auf die gewünschten Geräte freigeben).
- Identifizieren Sie eine spezifische DVD/CD-ROM über die Datensignatur eindeutig und autorisieren Sie den Zugriff darauf, auch wenn DeviceLock das DVD/CD-ROM-Laufwerk ansonsten blockiert hat.
- Schützen Sie sich gegen Benutzer mit lokalen Administratorrechten, so dass sie DeviceLock Service nicht deaktivieren oder von ihren Rechnern entfernen können, wenn sie nicht in der Liste der DeviceLock-Administratoren stehen.
- Suchen Sie nach Text in allen Shadowing-Dateien und Prüfprotokollen, die in der zentralen Datenbank gespeichert sind.

- Setzen Sie Geräte in den Schreibgeschützt-Modus.
- Schützen Sie Datenträger vor zufälligem oder absichtlichem Formatieren.
- Erkennen und blockieren Sie Hardware-Keylogger (USB und PS/2).
- Verteilen Sie Berechtigungen und Einstellungen per Gruppenrichtlinien in einer Active Directory-Domäne.
- Verwenden Sie das Standard-Windows-RSoP-Snap-In, um die gegenwärtig angewandte DeviceLock-Richtlinie anzuzeigen, und auch um vorherzusagen, welche Richtlinie in einer bestimmten Situation angewendet wird.
- Steuern Sie alles aus der Ferne mit Hilfe der zentralen Managementkonsole.
- Nutzen Sie ein vollständiges Protokoll der Port- und Geräteaktivitäten, wie etwa Uploads und Downloads durch Benutzer und Dateinamen im Standard-Windows-Ereignisprotokoll.
- Spiegeln Sie alle Daten (Shadowing), die auf externe Speichergeräte kopiert werden (entnehmbare, Disketten, DVD/CD-ROM), Windows Mobile, iPhone oder Palm OS PDAs und Smartphones, die über COM- und LPT-Ports übertragen werden, selbst diejenigen, die ausgedruckt werden.
- Speichern Sie die Shadowing-Daten auf einer zentralen Komponente eines bestehenden Servers und jeder beliebigen ODBC-kompatiblen SQL-Infrastruktur.
- Überwachen Sie entfernte Rechner in Echtzeit, überprüfen Sie den Status von DeviceLock Service (ob er läuft oder nicht), die Übereinstimmung mit Richtlinien und die Integrität.
- Generieren Sie einen Bericht bezüglich der eingerichteten Berechtigungen und Einstellungen.
- Erstellen Sie anhand der auf dem Server gespeicherten Prüf- und Shadow-Protokolle grafische Berichte.
- Generieren Sie einen Bericht, in dem die USB-, FireWire- und PCMCIA-Geräte angezeigt werden, die aktuell an Computer angeschlossen sind und diejenigen, die angeschlossen waren.
- Erstellen Sie ein benutzerdefiniertes MSI-Paket für DeviceLock Service mit vordefinierten Richtlinien.

### **Wie funktioniert DeviceLock?**

DeviceLock funktioniert auf jedem Computer, auf dem Windows NT 4.0/2000/XP/Vista/7 oder Windows Server 2003/2008 läuft. Es unterstützt 32-Bit- und 64-Bit-Plattformen.

DeviceLock besteht aus drei Teilen: dem Agenten, dem Server und der Managementkonsole:

1. DeviceLock Service (der Agent) ist das Herzstück von DeviceLock. DeviceLock Service wird auf jedem Clientsystem installiert, läuft automatisch und bietet Laufwerkschutz auf dem Clientrechner, wobei es für die lokalen Benutzer dieses Computers unsichtbar bleibt.
2. DeviceLock Enterprise Server ist die optionale Komponente für zentralisierte Sammlung und Speicherung der Shadow-Daten und Prüfprotokolle. DeviceLock Enterprise Server verwendet MS SQL Server für die Speicherung seiner Daten.

DeviceLock Content Security Server ist auch eine optionale Komponente, die DeviceLock Search Server enthält, mit dem sofort über alle Shadowing-Dateien und anderen auf DeviceLock Enterprise Server gespeicherten Protokollen nach Text gesucht werden kann.

3. Die Managementkonsole ist die Steuerungsschnittstelle, die Systemadministratoren verwenden, um jedes System, auf dem DeviceLock Service läuft, aus der Ferne zu verwalten. DeviceLock wird mit drei verschiedenen Managementkonsolen ausgeliefert: DeviceLock Management Console (das MMC Snap-In), DeviceLock Enterprise Manager und DeviceLock Group Policy Manager (integriert im Windows Group Policy Editor).

### **Wer hat DeviceLock entwickelt?**

**DeviceLock wurde von DeviceLock Inc. entwickelt.** Seit seiner Gründung im Jahre 1996 bietet DeviceLock Inc. (ehemals SmartLine Inc.) Lösungen für Informationssicherheit und Netzwerkmanagement für Organisationen, die sich auf Microsoft Windows-Technologien stützen. Mit Hilfe der bewährten Expertise von DeviceLock bei Technologien zur Zugriffssteuerung können Kunden die Sicherheit, Produktivität und Verfügbarkeit ihrer Systeme verbessern. IT-Fachleute entscheiden sich für Lösungen von DeviceLock Inc., um diese geschäftskritischen Systeme zu administrieren, zu prüfen und zu schützen. Zu den Kunden des Unternehmens zählen BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank und verschiedene Regierungsbehörden und Ministerien. DeviceLock Inc. ist eine internationale Organisation mit Niederlassungen in San Ramon (Kalifornien, USA), London, Ratingen und Mailand.

### **Wo können Sie DeviceLock Software erhalten?**

Eine kostenlose, voll funktionsfähige Demoversion kann hier heruntergeladen werden:  
<http://www.devicelock.com/de/dl/download.html>

### **Technischer Support für DeviceLock**

Technischer Support ist verfügbar für Kunden von DeviceLock über E-Mail an [support@devicelock.com](mailto:support@devicelock.com). Es gibt eine Website, die auch eine Fülle an Support-Informationen bietet, einschließlich bekannter Probleme und häufig gestellter Fragen (FAQ):  
<http://www.devicelock.com/de/support.html>

Sie erreichen unseren technischen Support auch unter: +1-925-231-0042. Der telefonische Support ist erreichbar von Montag bis Freitag von 8 – 17 Uhr.

### **Preise für DeviceLock**

DeviceLock kostet EUR 31.20 für eine Einzellizenz. Preisnachlässe sind erhältlich für Mehrbenutzer-Lizenzen und für Bildungseinrichtungen. Für Preise für mehrere Benutzer siehe:  
<http://www.devicelock.com/de/dl/register.html>

### **Bestellung und Registrierung**

Es sind mehrere Methoden zur Bestellung / Registrierung von DeviceLock möglich:

Über eine sichere Website im World Wide Web (mit Kreditkarte)  
Per Telefon (mit Kreditkarte)  
Per Fax (mit Kreditkarte)

Per Post (mit Scheck)  
Per Bestellung

Weitere Informationen über Bestellmodalitäten finden Sie unter:  
<http://www.deviceclock.com/de/dl/register.html>

## **Kontaktinformation**

### **DeviceLock Deutschland:**

Halskestr. 21, 40880 Ratingen  
TEL: +49 (2102) 89211-0  
FAX: +49 (2102) 89211-29

### **DeviceLock Italien:**

Via Falcone 7, 20123 Mailand, Italien  
TEL: +39-02-86391432  
FAX: +39-02-86391407

### **DeviceLock Großbritannien:**

The 401 Centre, 302 Regent Street, London, W1B 3HH, GB  
TEL (gebührenfrei): +44-(0)-800-047-0969  
FAX: +44-(0)-207-691-7978

### **DeviceLock USA:**

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA  
TEL (gebührenfrei): +1-866-668-5625  
FAX: +1-646-349-2996

[sales@deviceclock.com](mailto:sales@deviceclock.com)  
[support@deviceclock.com](mailto:support@deviceclock.com)

<http://www.deviceclock.com/de>