

# Lumension Device Control

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



Lumension Device Control (LDC, ehemals Sanctuary Device Control) ermöglicht eine policybasierte Kontrolle der Nutzung externer Geräte im Hinblick auf die Steuerung des ein- und abgehenden Datenflusses an den Endpunkten. Durch den Rückgriff auf ein Whitelist-Konzept sorgt LDC 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, dann prüft der Device Control-Kernel-Treiber die Zugriffsrechte des Benutzers in der Zugriffskontrollliste (ACL). Wenn der Benutzer über eine entsprechende Zugriffsberechtigung für das Gerät verfügt, wird ihm ein Lese- oder Lese-/Schreibzugriff eingeräumt. Ist der Benutzer dahingegen nicht berechtigt, auf das Gerät zuzugreifen, dann erhält er eine kontextgerechte Benachrichtigung mit entsprechendem Warnhinweis (Zugriffsverweigerung).

## Einfachheit, Schnelligkeit und Flexibilität bei Administration und Management

Lumension 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 Oberfläche in „Baumstruktur“-Format.

Die Gerätepolicies sind mit den in Active Directory™ oder eDirectory™ gespeicherten Benutzer- und Benutzergruppendaten verknüpft und tragen dadurch zu einer wesentlichen Vereinfachung der Verwaltung der Geräteresourcen an den Endpunkten bei.

## Detaillierte Audit-Funktionen

Durch den Rückgriff auf die zum Patent angemeldete bidirektionale I/O-Shadowing-Technologie werden die Namen bzw. 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 können verschlüsselt werden, sodass ein sicherer Betrieb und Transport möglich wird, d. h. die Gefahr des Zugriffs durch nicht autorisierte Benutzer auf vertrauliche Daten wird ausgegrenzt. Die Benutzer können auf ihre verschlüsselten Daten auch von Rechnern aus zugreifen, auf denen die Lumension-Software nicht installiert wurde.

Anhand zentraler wie auch dezentraler Verschlüsselungsschemata erhalten die Lumension-Administratoren die erforderliche Flexibilität, um mobile Medien von einem zentralen Standpunkt aus zu verschlüsseln oder ganz im Gegenteil Benutzern die selbstständige Verschlüsselung ihrer mobilen Medien zu ermöglichen. Damit und das ist von ganz entscheidender Bedeutung lässt sich die Nutzung der verschlüsselten Medien umfassend kontrollieren.

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

## Reduzierung des Risikos von Datenverlust

Unternehmen sehen sich heute kontinuierlich mit dem Risiko eines Verlusts ihrer Daten aufgrund der Verwendung mobiler Medien 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<sup>1</sup>. 75 Prozent der Fortune 1000-Unternehmen wurden Opfer eines versehentlichen und/oder beabsichtigten Datenverlustes<sup>2</sup>, wobei für die Wiederherstellung verlorener bzw. gestohlener Unternehmensdaten durchschnittlich Kosten in Höhe von 5 Millionen US-Dollar anfallen das sind 30 % mehr als 2005<sup>3</sup>.

Nicht verwaltete mobile Medien können schnell alle Schleusen öffnen und es ermöglichen, dass Daten in die falschen Hände gelangen, ob nun beabsichtigt oder versehentlich. Darüber hinaus machen Datenschutzregelungen und Bestimmungen hinsichtlich interner Kontrollen 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.

## Unterstützte Gerätetypen

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

## Unterstützte Ports

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

Quellen:

<sup>1</sup> Yankee Group 2005, ESG 2005, Forrester 2005

<sup>2</sup> 2006, CSI/FBI-Studie zu Computerverbrechen und -sicherheit

<sup>3</sup> 2006, Studie des Ponemon Institute zu den Kosten für Einbrüche in die Datensicherheit

Eigenschaften	Funktionen	Vorteile
Whitelist	Benutzern oder Benutzergruppen werden Zugriffsberechtigungen für autorisierte Geräte zugewiesen. Standardmäßig gilt: Keine Autorisierung, kein Zugriff	Eliminiert unbekannte oder unerwünschte Geräte in Ihrem Netzwerk und reduziert das Risiko von Datenverlust
Flexible Verschlüsselungsoptionen für mobile Medien	Administratoren können mobile Medien und CDs/DVDs von einem zentralen Standort aus verschlüsseln oder Benutzer zur Verschlüsselung der Medien und CDs/DVDs bei deren Nutzung verpflichten	Stellt sicher, dass sensible Daten nicht versehentlich über einen nicht autorisierten Zugriff verfügbar werden
Eindeutige Identifizierung und Autorisierung spezifischer Medien	Autorisierung von DVD/CD-ROM-Kollektionen, Gewährung von Zugriff für Benutzer bzw. Benutzergruppen und Verschlüsselung mobiler Medien anhand eindeutiger Ids	Beschränkt den DVD/CD-ROM-Zugriff auf Discs, die dem Unternehmensstandard entsprechen, sodass die Verwendung nicht autorisierten Inhalts verhindert werden kann, und/oder verschlüsselt mobile Medien, um die
Detaillierte Einstellung der Berechtigungen im Rahmen der Gerätekontrolle	Mögliche Berechtigungseinstellungen: Lese-/Schreibzugriff, zeitlich begrenzter Zugriff, Online/Offline-Nutzung, Berechtigung auf Basis des Bustyps sowie des Gerätetyps wie z.B. HDD/Nicht-HDD-Geräte	Eliminiert das Risiko eines Zugriffs auf das Netzwerk durch nichtautorisierte Geräte und stattdieg gleichzeitig die Benutzer mit der erforderlichen Flexibilität aus
Plug&Play Geräte	Identifizierung von Plug&Play-Geräten bei laufender Tätigkeit	Gewährleistet eine Benutzerproduktivität ohne Unterbrechung, indem die Zugriffsberechtigung für Plug&Play-Geräte parallel zu deren Identifizierung erteilt wird
Option für patentiertes bidirektionales Shadowing	Die Shadowing-Technologie ermöglicht die Speicherung aller Daten, die aus mobilen Geräten ausgelesen und/oder darauf geschrieben werden	Erfasst den Datenfluss von Informationen in das und aus dem Netzwerk, wodurch sich das gegebene Risiko begrenzen und ein möglicher Datenverlust weitgehend verhindern lässt
Berechtigungen auf Grundlage einer Zugriffskontrollliste	Begrenzung des Umfangs der Daten, die von einem Benutzer pro Tag von einem Endpunkt auf ein Gerät kopiert werden können	Eliminiert das Risiko des Verlusts grosser Mengen vertraulicher Daten, indem diese das Netzwerk verlassen.
Rollenbasierte Zugriffskontrolle	Zuweisung von Berechtigungen für Benutzer/Benutzergruppen auf der Grundlage ihrer Identität in Active Directory oder eDirectory	Ermöglicht eine detaillierte Zuweisung von Benutzerberechtigungen in Verbindung mit den Anmeldedaten des Benutzers, ungeachtet des jeweiligen Rechners
PGP Whole Disk Encryption	Administratoren haben die Möglichkeit, ihre FIPS-konforme Standard-Verschlüsselungstechnologie durch ein zentralisiertes Verschlüsselungsmanagement und die Unterstützung für sekundäre Festplatten mit hoher Kapazität zu ergänzen. Diese Funktionen stehen mit dem Produkt PGP Whole Disk Encryption zur Verfügung.	Gewährleistet den Schutz von Daten auf externen Geräten über eine FIPS-validierte Verschlüsselung
Dateityp-Filterung	Kontrolle des Typs der auf mobile Geräte geschriebenen bzw. von dort ausgelesenen Dateien auf Basis des File-Headers	Reduziert das Risiko des Eindringens unerwünschter Dateien in das Netzwerk sowie des Verlusts sensibler Dateien durch Verlassen des Netzwerks
Kennwortbasierte Sperre	Sperren Sie den Zugriff für Benutzer nach drei fehlgeschlagenen Anmeldeversuchen	Begrenzt das Risiko eines Eindringens durch Hacker in verlorene oder gestohlene Geräte
Kennwortwiederherstellung	Stellen Sie den Zugriff auf Geräte nach dem Verlust von Kennwörtern oder dem Ausscheiden von Benutzern aus der Firma wieder her	Ermöglicht die Wiederherstellung verschlüsselter Daten auf mobilen Geräten
Unterstützung für zahlreiche Sprachen	Auf den Sanctuary Clientrechnern werden 13 Sprachen unterstützt	Verbessert die Arbeit der Benutzer in internationalen Unternehmen
Unterstützung für 64-Bit-Plattformen	Nutzen Sie Ihre leistungsstarke 64-Bit-Unternehmensinfrastruktur und bieten Sie ihr ausreichenden Schutz mithilfe von Sanctuary - dazu gehört Agent-Support für 64 Bit Windows Server 2003, Windows und Windows Vista sowie 64-Bit-Support für SQL Server 2005	Stellt zahlreiche Funktionen zur Gerätekontrolle sowohl für 32- als auch für 64-Bit-Plattformen bereit

## Ihr Partner für IT Automation und IT Security

Deutschland / Österreich:  
 IBV Informatik GmbH  
 Marie-Curie-Str. 4  
 D - 79539 Lörrach

Tel. 0049 7621 / 40 92 0  
 Fax 0049 7621 / 40 92 22

Internet: [www.ibvinfo.com](http://www.ibvinfo.com) +++ Email: [info@ibvinfo.com](mailto:info@ibvinfo.com)

Schweiz:  
 IBV Informatik AG  
 Schönenwerdstrasse 7  
 CH - 8902 Urdorf

Tel. 0041 44 / 745 92 92  
 Fax 0041 44 / 745 92 93

