

# Device Lock<sup>®</sup>

AN ENDPOINT DATA LEAK PREVENTION SUITE  
TO PROTECT YOUR SENSITIVE INFORMATION

## Why Consider An Endpoint DLP Solution?

The data you are striving to protect behind firewalls and passwords is likely still slipping through your fingers. Data leaks can be initiated by either unwitting employees or users with malicious intent copying proprietary or sensitive information from their PCs to flash memory sticks, smartphones, cameras, PDA's, DVD/CDROMs, or other convenient forms of portable storage. Or, leaks may spring from user emails, instant messages, web forms, social network exchanges or telnet sessions. Wireless endpoint interfaces like Wi-Fi, Bluetooth, and Infrared as well as device synchronization channels provide additional avenues for data loss. Likewise, endpoint PCs can be infected with vicious malware that harvest user keystrokes and send the stolen data over SMTP or FTP channels into criminal hands. While these vulnerabilities can evade both network security solutions and native Windows controls, the DeviceLock Endpoint Data Leak Prevention (DLP) Suite addresses them. It enforces data protection policies with awareness of both the context and content of data flows across endpoint channels.



Data leakage prevention starts with **contextual** control — that is, **blocking** or **allowing** data flows by recognizing the **user**, the **data types**, the **interface**, the device or network **protocol**, the flow **direction**, the state of **encryption**, the **date** and **time**, etc. Some scenarios call for a deeper level of awareness than context alone can provide; for example, when the data being handled contains **personally identifiable information**, when the input/output channel is conventionally **open and uncontrolled**, and when the users involved have situations or backgrounds considered **high risk**. Security administrators can gain greater **peace of mind** by passing data flows that fall into any of these categories through an additional **content analysis** and **filtering** step before allowing the data transfer to complete.

DeviceLock Endpoint DLP Suite provides both **contextual** and **content-based** control for **maximum** leakage prevention at **minimum** upfront and ownership **cost**. Its multi-layered inspection and **interception engine** provides **fine-grained** control over a full range of data leakage pathways at the **context** level. For further confidence that no **sensitive** data is escaping, **content analysis** and **filtering** can be applied to select endpoint data exchanges with **removable media** and PnP devices, as well as with the network. With DeviceLock, security administrators can precisely **match** user rights **to job** function with regard to transferring, receiving and storing data on corporate computers. The resulting **secure** computing environment allows all **legitimate** user actions to proceed unimpeded while **blocking** any **accidental** or deliberate attempts to perform operations outside of preset bounds.

DeviceLock supports a **straightforward** approach to DLP management that allows security administrators to use Microsoft Windows **Active Directory**® Group Policy Objects (GPOs) and DeviceLock consoles for dynamically managing distributed endpoint agents that enforce **centrally defined DLP policies** on their host computers. With DeviceLock in place, you can centrally control, log, **shadow-copy**, and analyze end-user access to and data transfers through all types of peripheral devices and ports, as well as **network communications** on corporate computers. In addition, its agents detect and **block** hardware **keyloggers** to prevent their use in the theft of passwords and other proprietary or personal information. Importantly, DeviceLock does all this while running in a **tamper-proof** mode, remaining **transparent** to end users, and consuming a **minimum** of disk **space** and memory.

With its **fine-grained** endpoint context **controls** complemented by content filtering for the most dangerous data channels, DeviceLock Endpoint DLP Suite **significantly** reduces the risk of sensitive information leaking from employees' computers, whether due to simple **negligence** or **malicious** intent. At the same time, it acts as a security **discipline tool** that enforces stated data protection policies and promotes **compliance** with corporate information handling rules, as well as legal **mandates** like HIPAA, Sarbanes-Oxley, and **PCI DSS**.

DeviceLock®

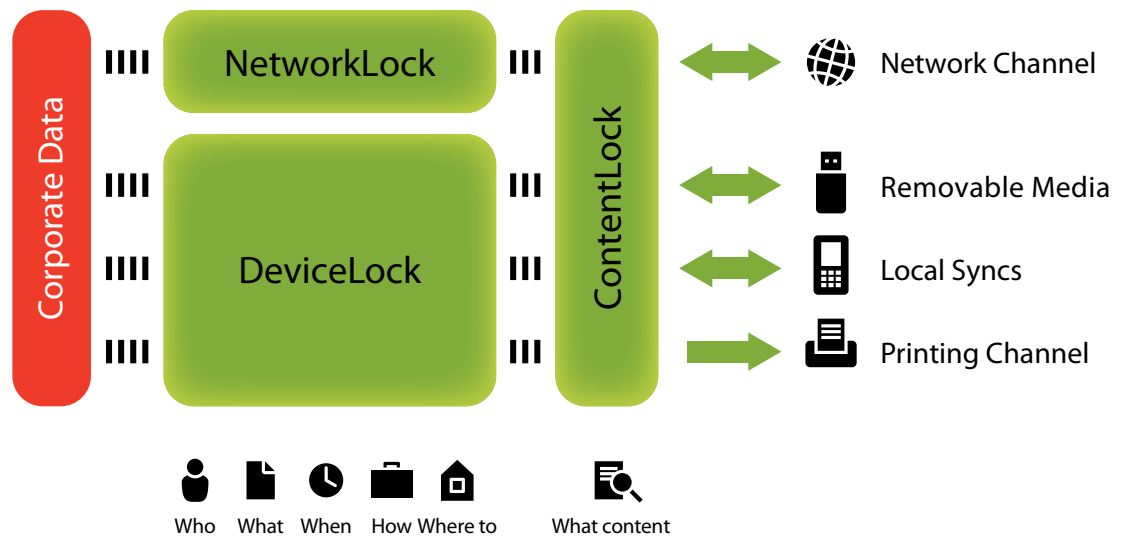
# Modular Structure and Licensing

DeviceLock Endpoint DLP Suite is comprised of a modular set of complementary functional components that can be licensed separately or in any combination that suits current security requirements. Existing customers have a secure upgrade path for their core DeviceLock functionality and the option to expand endpoint security with their choice of new modules. Likewise, new customers can incrementally move up to full-featured endpoint DLP by adding functionality as it is needed and budgets allow.

- ▶ The DeviceLock® component includes an entire set of context controls together with event logging and data shadowing for all local data channels on protected computers including peripheral devices and ports, connected smartphones/PDA's, and document printing. DeviceLock also provides the core platform for all other functional modules of the product suite and includes its central management and administration components.
- ▶ The NetworkLock™ component performs all context control functions over endpoint network communications including port-independent protocol/application detection and selective control, message and session reconstruction with file, data, and parameter extraction, as well as event logging and data shadowing.

- ▶ The ContentLock™ component implements content monitoring and filtering of files transferred to and from removable media and Plug-n-Play devices, as well as of various data objects of network communications reconstructed and passed to it by NetworkLock – like emails, instant messages, web forms, files, social media exchanges, and telnet sessions.
- ▶ DeviceLock® Search Server (DLSS) is another separately licensed component. It performs full-text search in the central shadowing and event log database. DLSS is aimed at making the labor-intensive processes of information security compliance auditing, incident investigations, and forensic analysis more precise, convenient and time-efficient.

The core DeviceLock component is mandatory for every product installation. All other components including NetworkLock, ContentLock and DeviceLock Search Server are separately licensed optional add-ons. This modular product structure and flexible licensing scheme enable DeviceLock customers to cost-effectively deploy endpoint DLP. They can start with the essential set of port and device control functions incorporated in the core component, – and incrementally add new functional licenses to “activate” additional product capabilities as security requirements grow.



- ▶ **Core DeviceLock functionality enforces device access policy by port (interface), device class, device type, device model, unique device ID, hour-of-day, day-of-the-week, as well as by discrete parameters such as write, read-only, and format access. Device types can be configured to only allow access to verified file types and to adhere to enforced encryption rules. NetworkLock extends the ability to control the context of data communications to network protocols and applications. By adding ContentLock, you can ensure that only filtered data objects that do not contain restricted content will be passed to their destinations.**

Data leaks occur when proprietary information is copied to convenient forms of portable storage or when typed, pasted, or otherwise sent via applications using unchecked network protocols.

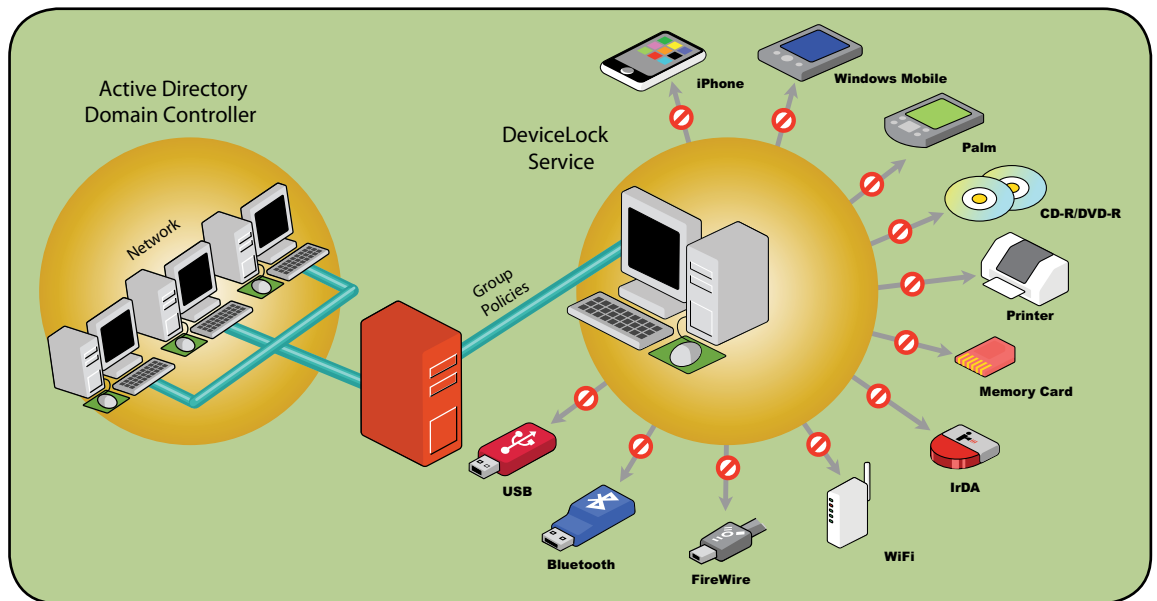
# DeviceLock Features and Benefits

DeviceLock Endpoint DLP Suite delivers essential content filtering capabilities and reliable control over network communications on top of DeviceLock's best-in-industry context-based controls, whereby access to local ports and peripheral devices on corporate endpoint computers is under a DeviceLock administrator's centralized control.

**Active Directory Integration.** DeviceLock's most popular console integrates directly with the Microsoft Management Console (MMC) Active Directory (AD) Group Policy interface. As Group Policy and MMC-style interfaces are common knowledge for AD administrators, there is no proprietary interface to learn or appliance to buy to effectively manage endpoints centrally. The simple presence of the DeviceLock MMC snap-in console on a Group Policy administrator's computer allows for direct integration into the Group Policy Management Console (GPMC) or the Active Directory Users & Computers (ADUC) console with absolutely zero scripts, ADO templates, or schema changes. Security administrators can dynamically manage endpoint

data leakage prevention and audit settings right along with other Group Policy-related tasks. In addition to the MMC snap-in console for Group Policy, DeviceLock also has classic Windows-style administrative consoles that can centrally manage agents on any AD, LDAP, or workgroup network of Windows computers. XML-based policy templates can be shared across all DeviceLock consoles.

**RSOP Support.** The Windows standard Resultant Set of Policy snap-in can be used to identify which DeviceLock group policy is currently being applied and to predict which policy would be applied in a given Organizational Unit (OU) membership scenario.



▶ Enterprises can secure any number of remote endpoints with DeviceLock Endpoint DLP Suite by leveraging its integration with Active Directory and the Windows Group Policy Management Console. NOTE: For a full list of network data channels protected by NetworkLock, see the last page of this brochure.

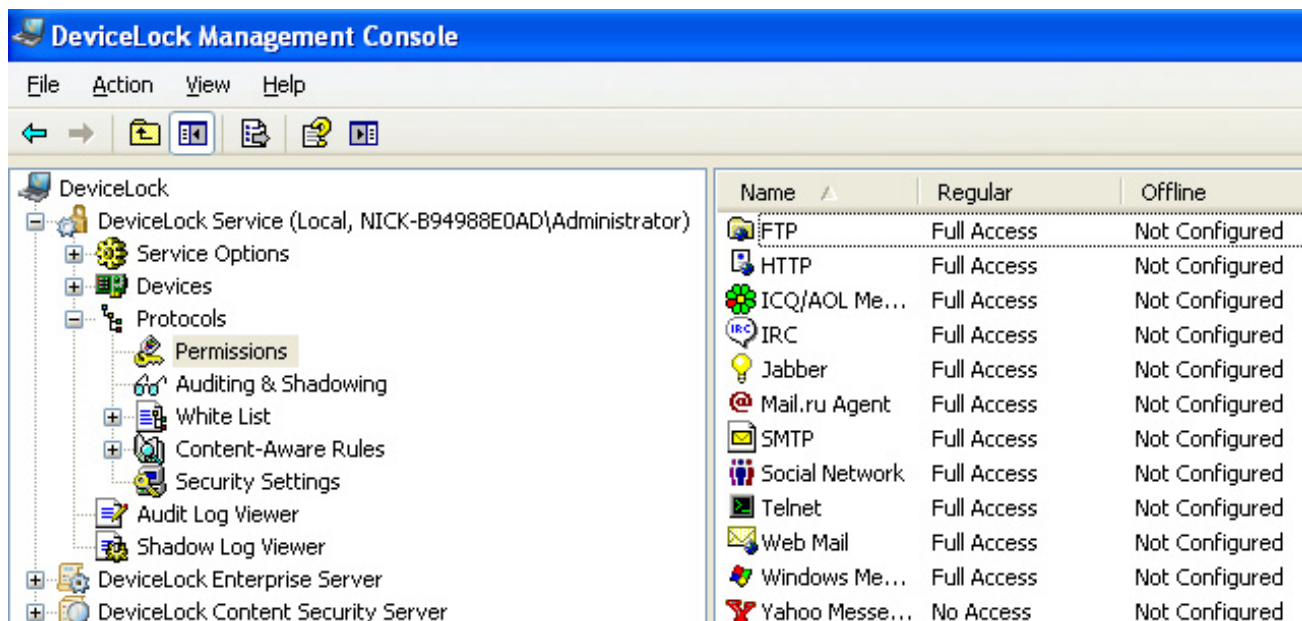
**Device Whitelisting.** Among the five layers of Windows device control supported by DeviceLock, the USB device model and device ID levels are handled using a whitelist approach, whereby the DeviceLock administrator can explicitly assign users/groups to a USB device. Administrators can whitelist a specific corporate-issued model of USB drive, for example, and DeviceLock will allow only designated users to have access with these, while blocking all other unlisted devices and unlisted users by default. Administrators can even whitelist

a single, unique device, while locking out all other devices of the same brand and model, as long as the device manufacturer has implemented a standard unique identifier. There is also a powerful Temporary Whitelist applet that users can run to securely request short-term use of a USB mounted device from a DeviceLock administrator, even while off the network. Meanwhile, the rest of the original security policy remains intact and enforced during this exceptional device-use period.

Studies point to the document printing channel as the most often used for stealing corporate data. Yet, 75% of surveyed IT organizations that use DLP solutions cannot control the content of documents printed from corporate computers.

**Network Communications Control.** Introduced with this version of DeviceLock Endpoint DLP Suite, the NetworkLock component adds comprehensive context control capabilities over endpoint network communications. NetworkLock supports port-independent network protocol and application detection and selective blocking, message and session reconstruction with file, data, and parameter extraction, as well as event logging and data shadowing.

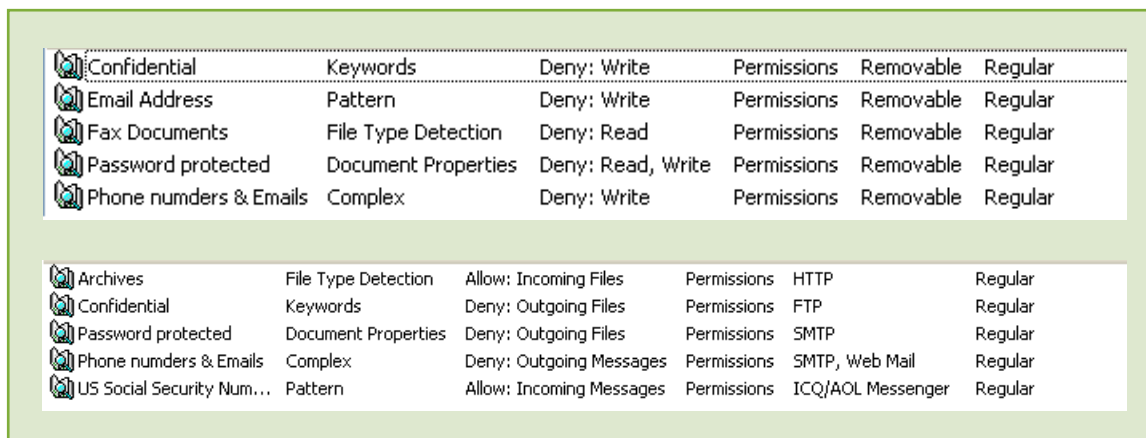
NetworkLock controls most popular network protocols and applications including plain and SSL-tunneled SMTP email communications with messages and attachments handled separately, as well as web access and other HTTP-based applications including content extraction of encrypted HTTPS sessions. See the Product Specifications pages for a list of all webmail and social media applications controlled by NetworkLock.



- ▶ **With NetworkLock you can set user permissions for the network protocols used for web mail, SMTP mail, social networking communications, instant messaging, file transfers and telnet sessions.**

**Content Filtering.** Extending DeviceLock and NetworkLock capabilities beyond context-based security mechanisms, the ContentLock module can filter the content of files copied to removable drives and other Plug-n-Play storage devices, as well as various data objects of network communications. These include email, web access and other HTTP-based applications like webmail and social networking, most popular instant messaging applications, FTP file transfers, and telnet sessions. In addition the content of textual data copied between applications and documents through clipboard operations can be analyzed and filtered according to

DLP policies. The text analysis engine can extract textual data from more than 80 file formats and other data types and then apply effective and reliable content filtering methods based on Regular Expression (RegExp) patterns with numerical conditions and Boolean combinations of matching criteria. To ease the task of specifying content filtering rules, pre-built industry-specific keyword dictionaries can be used, as well as RegExp templates for common sensitive information types including numbers for social security registrations, credit cards, bank accounts, addresses, driver's licenses, etc.



- ▶ **The configuration screens here show high-level samples of content-aware rules per specific device (above) and per specific network protocol (below). ContentLock's MMC-style interface eases definition of content-aware filtering policies.**

"We found

DeviceLock to

be the most

cost-effective

solution for

endpoint device

management

after months

of product

evaluation. It has

proven itself to

be one of the

biggest 'bangs

for the buck'

in our arsenal

of information

security controls."

David Gardner,

Data Security

Specialist,

University of Alabama

at Birmingham

Health System

## DeviceLock Features and Benefits cont.

**True File Type Control.** Administrators can selectively grant or deny access to over 4,000 specific file types for removable media. When a file type policy is configured, DeviceLock will look into a file's binary content to determine its true type (regardless of file name and extension) and enforce control and shadowing actions per the applied policy. For flexibility, Content-Aware Rules for file types can be defined on a per-user or per-group basis at the device type layer. True file type rules can also apply to pre-filtering of shadow copies to reduce the volume of captured data.

**Clipboard Control.** DeviceLock enables security administrators to effectively block data leaks at their very embryonic stage—when users deliberately or accidentally transfer unauthorized data between different applications and documents on their computer through clipboard mechanisms available in Windows operating systems. Copy and Paste operations can be selectively filtered for data exchanges between different applications (e.g. from Word to Excel or OpenOffice). At the context level, DeviceLock supports the ability to selectively control user access to data objects of various types copied into the clipboard including files, textual data, images, audio fragments (like recordings captured by Windows Sound Recorder), and data of unidentified types. Screenshot operations can be blocked for specific users at specific computers including Windows' PrintScreen function, as well as screenshot operations of third-party applications.

**Mobile Device Sync Control.** Administrators can set granular access control, auditing, and shadowing rules for mobile devices that use the Microsoft Windows Mobile®, Apple iPhone®/iPad®/iPod touch® or Palm® operating systems' local data synchronization. Permissions are presented with fine granularity, defining which types of data (files, pictures, emails, contacts, calendars, etc.) specified users and/or groups are allowed to synchronize between corporate PCs and their personal mobile devices regardless of the connection interface. BlackBerry® smartphones are also supported with device presence detection, access control and event logging.

**Printing Security.** DeviceLock puts local and network printing under the strict control of corporate security administration. By intercepting, filtering and tracing Print Spooler operations, DeviceLock enables administrators to centrally specify and locally enforce who is allowed to print, from where, when, and where to. User access to any local, network, and even virtual printers regardless of how they connect to the PC. In addition, for USB connections, printers can be whitelisted on per-vendor, per-model or unique printer basis. Printing events can be logged, and printout copies of any printed documents can be shadow-copied and stored in a central database for audit and post-analysis.

**Removable Media Encryption Integration.** DeviceLock takes an open integration approach to encryption of data uploaded to removable media. Customers have the option of using the encryption solution that best fits their security scenarios among best-of-breed technologies that include: Windows 7 BitLocker To Go™, PGP® Whole Disk Encryption for standard FIPS-certified encryption; TrueCrypt® for free Open Source encryption; SafeDisk®, SecurStar® DriveCrypt Plus Pack Enterprise (DCPPE) software; and Lexar Media's S1100/S3000 series USB flash drives for pre-encrypted removable media. In addition, any pre-encrypted USB media can be selectively whitelisted with usage strictly enforced. DeviceLock allows for discrete access rules for both encrypted and unencrypted partitions of such media. With its partnering approach, DeviceLock is positioned to quickly add support for more encryption vendors as the market demands.

**Network-Awareness.** You can define different online vs. offline security policies for the same user account and computer. A useful setting on a mobile user's laptop, for example, is to disable Wi-Fi when docked to the corporate network to avoid "bridging" data leaks and to enable Wi-Fi when undocked.

**Anti-Keylogger.** DeviceLock detects USB keyloggers to generate alerts or even block keyboards connected to them. This feature allows administrators to securely allow all USB mice and keyboards by class. DeviceLock also obfuscates PS/2 keyboard input and forces PS/2 keyloggers to record unintelligible text instead of real keystrokes.

**Tamper Protection.** Configurable 'DeviceLock Administrators' feature prevents anyone from tampering with settings locally, even users that have local PC system administration privileges. With this feature activated, only designated security administrators working from a DeviceLock console or Group Policy Object (GPO) Editor can install/ uninstall the program or edit DeviceLock policies.

The screenshot shows the Group Policy Management console for 'Default Domain Policy [win2003ent.VM2003AD.loc]'. The left pane shows a tree view with 'DeviceLock' expanded to 'Devices' > 'Permissions'. The right pane displays a table of device access configurations.

Name	Regular	Offline
BlackBerry	Configured	Configured
Bluetooth	Configured	Configured
DVD/CD-ROM	Configured	Configured
FireWire port	Configured	Configured
Floppy	Configured	Configured
Hard disk	Configured	Configured
Infrared port	Configured	Configured
iPhone	Configured	Configured
Palm	Configured	Configured
Parallel port	Configured	Configured
Printer	Configured	Configured
Removable	Configured	Configured
Serial port	Configured	Configured
Tape	Configured	Configured
USB port	Configured	Configured
WiFi	No Access	Full Access
Windows Mobile	Configured	Configured

- ▶ **DeviceLock MMC snap-in to Group Policy Management:** DeviceLock administrators have full central control over access, audit, shadow, and content rules covering potential local data leakage channels across the entire Active Directory domain forest.

# DeviceLock Observation Mode

DeviceLock is often used at first to collect a record of the data objects that end users are moving to removable media, DVD/CD-ROMs, PDAs, through Wi-Fi, and via web email, web forms etc. DeviceLock audit/shadow records are useful in determining the current level of non-compliance exposure and can be used to provide a non-reputable audit trail for compliance officials. When a leak is discovered or even suspected, DeviceLock provides tools to capture and forensically view objects and associated logs for use as evidence.

**Audit Logging.** DeviceLock's auditing capability tracks user and file activity for specified device types and ports on a local computer. It can pre-filter auditable events by user/group, by day/hour, by true file type, by port/device type, by reads/writes, and by success/failure events. DeviceLock employs the standard event logging subsystem and writes audit records to a Windows Event Viewer log with GMT timestamps. Logs can be exported to many standard file formats for import into other reporting and log management solutions.

**Data Shadowing.** DeviceLock's data shadowing function can be set up to mirror all data copied to external storage devices, printed or transferred through serial, parallel, and network ports (with NetworkLock add-on). DeviceLock can also split ISO images produced by CD/DVD burners into the original separated files upon auto-collection by the DeviceLock Enterprise Server (DLES). A full copy of the files can be saved into the SQL database or to a secure share managed by the DLES. Shadow data can be pre-filtered, just like regular audit logging, to narrow down what is collected. DeviceLock's audit and shadowing features are designed for efficient use of transmission and storage resources with stream compression, traffic shaping for quality of service (QoS), performance/quota settings, and automatic optimal DLES server selection.

**Agent Monitoring.** DeviceLock Enterprise Server can monitor remote computers in real-time, checking DeviceLock agent status (running or not), version, policy consistency and integrity. The detailed information is written to the Monitoring log. If this process uncovers DeviceLock agents that are inconsistent with current security policy, DeviceLock can remotely update those agents to settings that will keep the local endpoint policy in compliance.

**Report Plug-n-Play Devices.** The PnP Report allows administrators and auditors to generate a report displaying the USB, FireWire, and PCMCIA devices currently and historically connected to selected computers in the network. This report also allows for efficient population of the USB whitelist as a first step to adding select device models or unique devices to DeviceLock access policies.

**Graphical Reporting.** DeviceLock can generate graphical "canned" reports in HTML, PDF or RTF format based on analysis of DLES-collected audit log and shadow file data. These reports can be auto-emailed to a data security management list or compliance officers if desired.

**Data Search.** The optional, separately licensed DeviceLock Search Server (DLSS) enhances the forensic abilities of DeviceLock by indexing and allowing comprehensive full-text searches of centrally collected DeviceLock audit log and shadow file data. The DLSS aids in the labor-intensive processes of information security compliance auditing, incident investigations, and forensic analysis by making fact-finding faster, more precise, and more convenient. It supports indexing and searching in more than 80 file formats. Language independent word, phrase, and number queries take only seconds to execute once the data has been indexed. Stemming and noise-word filtering are turned on by default for words and phrases in English, French, German, Italian, Japanese, Russian, and Spanish. DLSS uses "all words" logic (AND logic), with some special character wildcards available to refine or expand searches. Results are sorted by "hit count" by default, though term weighting or field weighting for particular words is possible. The DLSS also supports full-text indexing and searching of printouts in PCL and PostScript languages to audit virtually all document printing.

"We have

DeviceLock

for central

management

of local ports

and drives on

employee PCs,

so that they

only use our

corporate-

issue hardware

encrypted flash

drives."

Doug Miller,  
Director of  
IT, Armanino  
McKenna

# Product Specifications

## Structural (Installable) Components

- ▶ DeviceLock Service (agent)
- ▶ DeviceLock Enterprise Server (DLES)
- ▶ Consoles: DeviceLock Group Policy Manager, DeviceLock Management Console, DeviceLock Enterprise Manager

## Functional (Licensable) Components

- ▶ DeviceLock
- ▶ NetworkLock
- ▶ ContentLock
- ▶ DeviceLock Search Server (DLSS)

## Ports Secured

- ▶ USB
- ▶ FireWire
- ▶ Infrared
- ▶ Serial and parallel

## Device Types Controlled

- ▶ Floppies
- ▶ CD-ROMs/DVDs
- ▶ Any removable storage (flash drives, memory cards, etc.)
- ▶ Hard drives
- ▶ Tape devices
- ▶ WiFi adapters
- ▶ Bluetooth adapters
- ▶ Windows Mobile, Palm OS, Apple iPhone/iPod touch/iPad and BlackBerry
- ▶ Printers (local, network and virtual)

## Data Types Controlled

- ▶ More than 4,000 file types
- ▶ Data synchronization protocol objects: Microsoft ActiveSync®, Palm® HotSync, iTunes®
- ▶ Pictures containing text as image (embedded in documents or as separate graphic files)

## Network Communications Controlled

- ▶ Web Mail: Gmail, Yahoo!Mail, Windows Live Mail
- ▶ Social Networking: Facebook, Twitter, LiveJournal, LinkedIn, MySpace, Odnoklassniki, Vkontakte
- ▶ Instant Messengers: ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent.
- ▶ Internet Protocols: FTP, FTP over SSL, HTTP/HTTPS, SMTP and SMTP over SSL
- ▶ Telnet sessions

## Clipboard Control

- ▶ Inter-application clipboard copy/paste operations
- ▶ Data types controlled separately: file types, textual data, images, audio, unidentified
- ▶ Screenshot operations (for PrintScreen and 3rd party applications)

"DeviceLock

was selected

as our solution

because

it got the

highest score

in all key

functional and

management

areas among

the products

we evaluated".

Marcel Dijkstra, ICT  
Manager, Syntrus  
Achmea

# Product Specifications

## Content Filtering Features

### Controlled Data Channels

- ▶ Removable media
- ▶ Other PnP storage devices
- ▶ Network communications (See previous list)

### File Formats Parsed

- ▶ 80+ file formats including Microsoft Office, OpenOffice, Lotus 1-2-3, Email repositories and archives, CSV, DBF, XML, Unicode, GZIP, RAR, ZIP, etc.

### Filtering Technologies

- ▶ Keyword matching
- ▶ Advanced regular expression patterns with numerical conditions and Boolean combination of matching criteria
- ▶ Pre-built RegExp templates (SSN, credit card, bank account, address, passport, driver's license, etc.)
- ▶ Industry-specific keyword dictionaries

### Content-Aware Data Shadowing

- ▶ All endpoint data channels
- ▶ All parsed file formats and data types (See previous list)
- ▶ PCL and Postscript printouts

### Application Control

- ▶ By name of executable for file operations

### Full Text Searching

- ▶ 80+ file formats including Microsoft Office, OpenOffice, Lotus 1-2-3, Email repositories and archives, CSV, DBF, XML, Unicode, GZIP, RAR, ZIP, etc.
- ▶ PCL and Postscript printouts
- ▶ Indexing and search based on: log record parameters, word, phrase, number
- ▶ Search logic: "all words" (AND), default "hit count" weighting, configurable term and field weighting
- ▶ Stemming and noise-word filtering for English, French, German, Italian, Russian, and Spanish

### Encryption Integration

- ▶ Windows 7 BitLocker To Go
- ▶ PGP® Whole Disk Encryption
- ▶ TrueCrypt®
- ▶ Lexar® Media SAFE S1100 & S3000 Series
- ▶ SafeDisk®
- ▶ SecurStar® DriveCrypt® (DCPPE)

### Approved Encrypted Devices

- ▶ IronKey®: D20XXX, S-200 & D200 Series
- ▶ Systematic Development Group LOK-IT
- ▶ Lexar Media SAFE S1100 & S3000 Series
- ▶ SanDisk® Cruzer® Enterprise Series
- ▶ BlockMaster SafeStick

### Component Dependencies

- ▶ ContentLock, NetworkLock and DLSS require installation of the core DeviceLock module
- ▶ ContentLock requires NetworkLock for content filtering of network communications

### System Requirements

- ▶ DeviceLock agent: Windows NT 4.0/2000/XP/Vista/7 or Server 2003/2008 (32-bit and 64-bit versions); CPU Pentium 4, 1GB RAM, HDD 50GB
- ▶ DeviceLock consoles: Windows NT 4.0/2000/XP/Vista/7 or Server 2003/2008 (32-bit and 64-bit versions); CPU Pentium 4, 2GB RAM, HDD 100GB
- ▶ DeviceLock Enterprise Server: Windows Server 2000/2003/2008; CPU Intel Xeon 2.33GHz, RAM 4GB, HDD 500GB; MSDE or MS SQL Server (optionally)



EXPERT DISTRIBUTION

[www.softtek.co.uk](http://www.softtek.co.uk)