# DeviceLock®

GROUP POLICY-INTEGRATED ENDPOINT DATA LEAK PREVENTION (DLP) SUITE FOR PROTECTING 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 who copy proprietary or sensitive information from their computers to flash memory sticks, smartphones, cameras, PDA's, DVD/CDROMs, or other convenient forms of portable storage. Data leaks may also spring from user emails, instant messages, web forms, social network exchanges, file sharing cloud services or telnet sessions. Wireless endpoint interfaces like Wi-Fi, Bluetooth, and Infrared as well connected mobile devices provide additional avenues for data loss. Likewise, endpoint PCs can be infected with vicious malware or keyloggers that harvest user keystrokes and send the stolen data over SMTP or FTP channels into criminal hands. While these threat vectors can evade conventional network security solutions and native Windows/Mac controls, the DeviceLock Endpoint Data Leak Prevention (DLP) Suite addresses them. It enforces data protection and auditing policies with awareness of both the context and content of data flows across endpoint channels where leaks can otherwise occur. DeviceLock also delivers Virtual DLP to VM and BYOD devices. Virtual DLP extends DeviceLock DLP to a variety of session-based, streamed and local virtual machines and to BYOD devices using desktop and application virtualization architectures.

# Endpoint DLP With Context & Content Awareness

The most efficient approach to data leakage prevention is to start with contextual control — that is, blocking or allowing data flows by recognizing the authenticated user, security group memberships, data types, device types or network protocol, flow direction, state of media or SSL encryption, the date and time, etc.

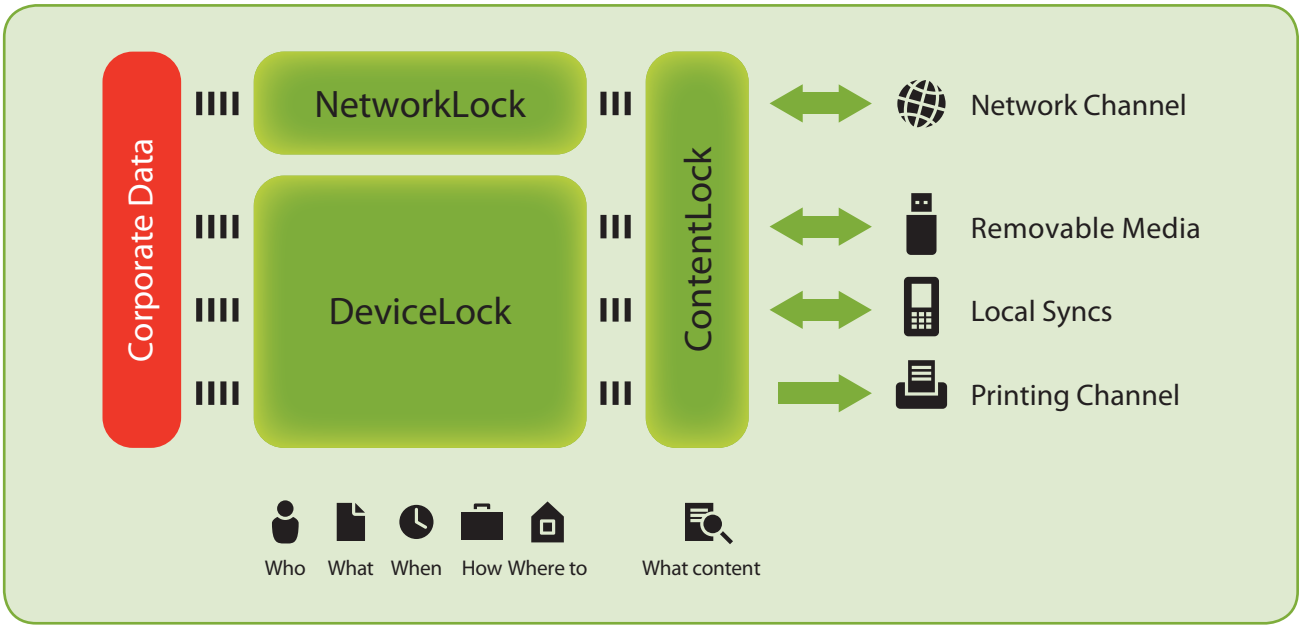
There are also many scenarios that require a deeper level of awareness than contextual parameters alone can provide. For example, even trusted employees handle data that contains personally identifiable information (PII), financials, health data, "Confidential", or other intellectual property content. Security administrators gain greater peace of mind and data security compliance by passing all data flows that might contain any of these data elements through content analysis and filtering rules before allowing the data transfer to complete.

DeviceLock Endpoint DLP Suite provides both contextual AND content-based controls for maximum leakage prevention at minimum cost. Its multi-layered inspection and interception engine provides granular control over a full range of data leakage pathways and will further ensure that no sensitive data is escaping through content analysis and filtering that can be applied to endpoint data exchanges with removable media, Plug-n-Play devices, printers, email, web and other network communications.

With DeviceLock, security administrators can precisely match access rights to job function with regard to transferring, receiving and storing data on media attached to corporate computers or through network protocols. 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 provides a straightforward approach to DLP management that allows security administrators to use familiar Microsoft Windows Active Directory® Group Policy Objects (GPOs) and snap-in DeviceLock consoles to centrally define DLP policies and automatically push them to distributed agents for continual enforcement on both physical and virtual Windows endpoints.

With DeviceLock, administrators can centrally control, log, shadow-copy, alert, and analyze end-user data transfers to all types of peripheral devices and ports, as well as network communications on managed endpoint 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. DeviceLock consumes a minimum of disk space and memory, is transparent as desired to end users, and can operate in tamper-proof mode in case users are also local administrators.

With its fine-grained endpoint contextual controls complemented by content filtering for the most vulnerable endpoint data channels, DeviceLock Endpoint DLP Suite significantly reduces the risk of sensitive information leaking from employees' computers due to simple negligence or malicious intent. DeviceLock DLP is a security platform that includes data protection policy templates and promotes compliance with corporate information handling rules, as well as legal mandates like HIPAA, Sarbanes-Oxley, and PCI DSS.



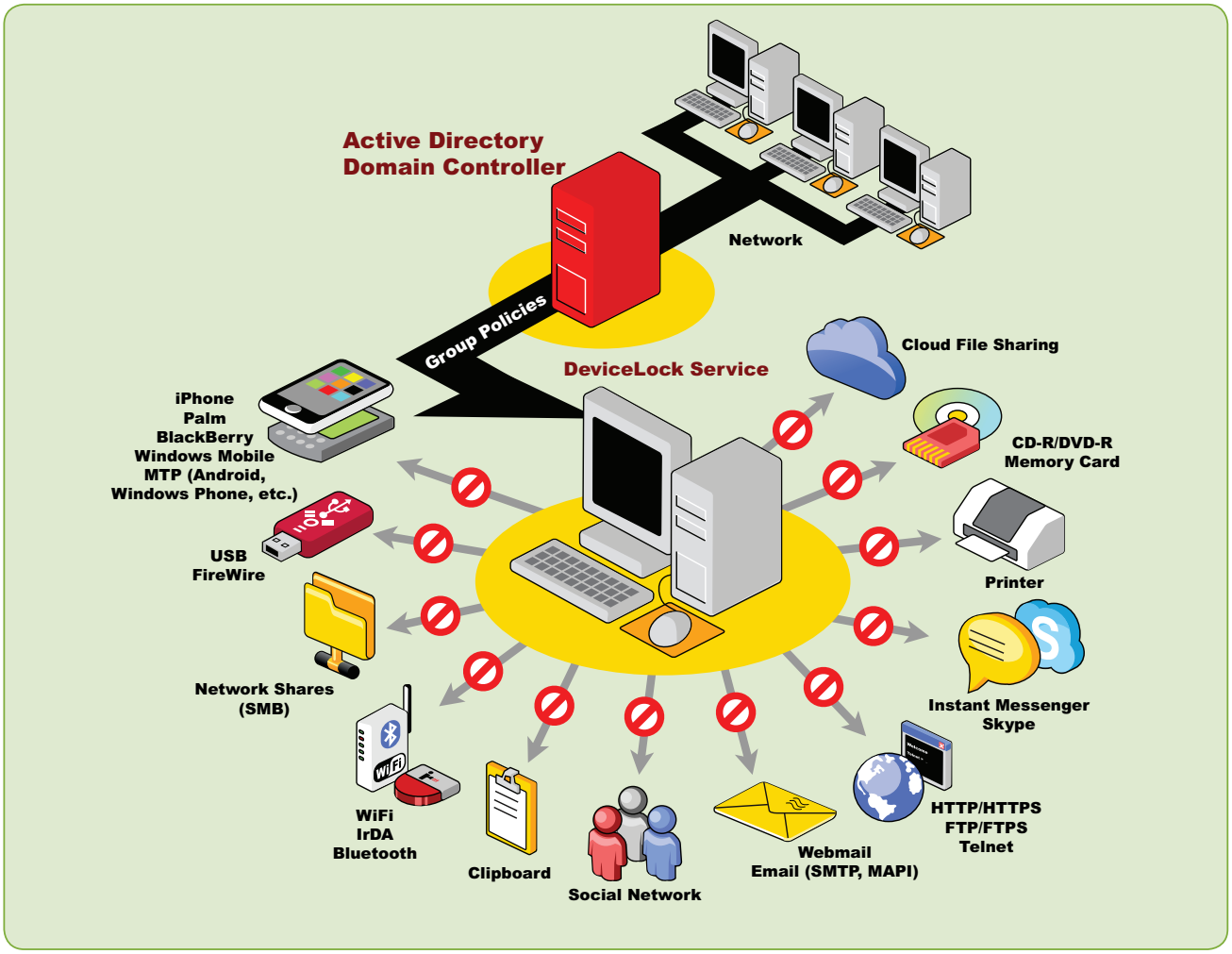

**Core DeviceLock functionality enforces device access policy by port (interface), device class, device type, device model, unique device ID, hour-of-day, day-of-the-week, as well as by discrete access parameters such as write, read-only, and format. Device types can be configured to only allow access to verified file types and to adhere to enforced use-of-encryption rules. NetworkLock extends the ability to control the context of data communications to network protocols and applications. ContentLock provides advanced content filtering rules across the data channels that DeviceLock and NetworkLock manage.**

# Modular Structure and Licensing

DeviceLock Endpoint DLP Suite is comprised of a modular set of complementary function-specific components that can be licensed separately or in any combination that meets current security requirements. Existing customers have a secure upgrade path for DeviceLock functionality and the option to expand endpoint security with their choice of 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® Core** module component includes an entire set of contextual controls together with event logging, data shadowing and alerting for all local data channels on protected computers. These include peripheral devices and ports, tethered smartphones/PDA's, MTP-enabled devices (such as Android and Windows Phone smartphones, etc.), clipboard, mapped virtual devices, printscreens, and document printing. DeviceLock Core provides the mandatory platform, central management and all administrative components for the other functional modules of the product suite.
- The pre-integrated **NetworkLock™** component provides contextual control functions over network communications like web, email and more. NetworkLock's port-independent protocol detection and selective control, message and session reconstruction with file, data, and parameter extraction all provide deep packet inspection, as well as event logging, alerting and data shadowing.
- The pre-integrated **ContentLock™** component implements content filtering of files transferred to and from removable media and Plug-n-Play devices, as well as of various data objects from network communications that are reconstructed and passed to it by NetworkLock. These include emails, instant messages, web forms, attachments, social media exchanges, and file transfers.
- **DeviceLock® Search Server (DLSS)** is another separately licensed component that indexes and performs full text searches on data in the central shadowing and event log database. DLSS is designed to make the labor-intensive processes of information security compliance auditing, incident investigations, and forensic analysis more precise, convenient and time-efficient.

The DeviceLock core module component is mandatory for every product installation. All other modules, including NetworkLock, ContentLock, and DeviceLock Search Server, are separately licensed add-ons. This modular product structure and flexible licensing scheme enable DeviceLock customers the option to cost-effectively deploy endpoint DLP features in stages. They can start with the essential set of port and device control functions incorporated in the core component and then incrementally add function-specific module licenses to "activate" pre-integrated capabilities as security and compliance requirements grow.




- **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, refer to the Product Specifications section.**

# DeviceLock Features and Benefits

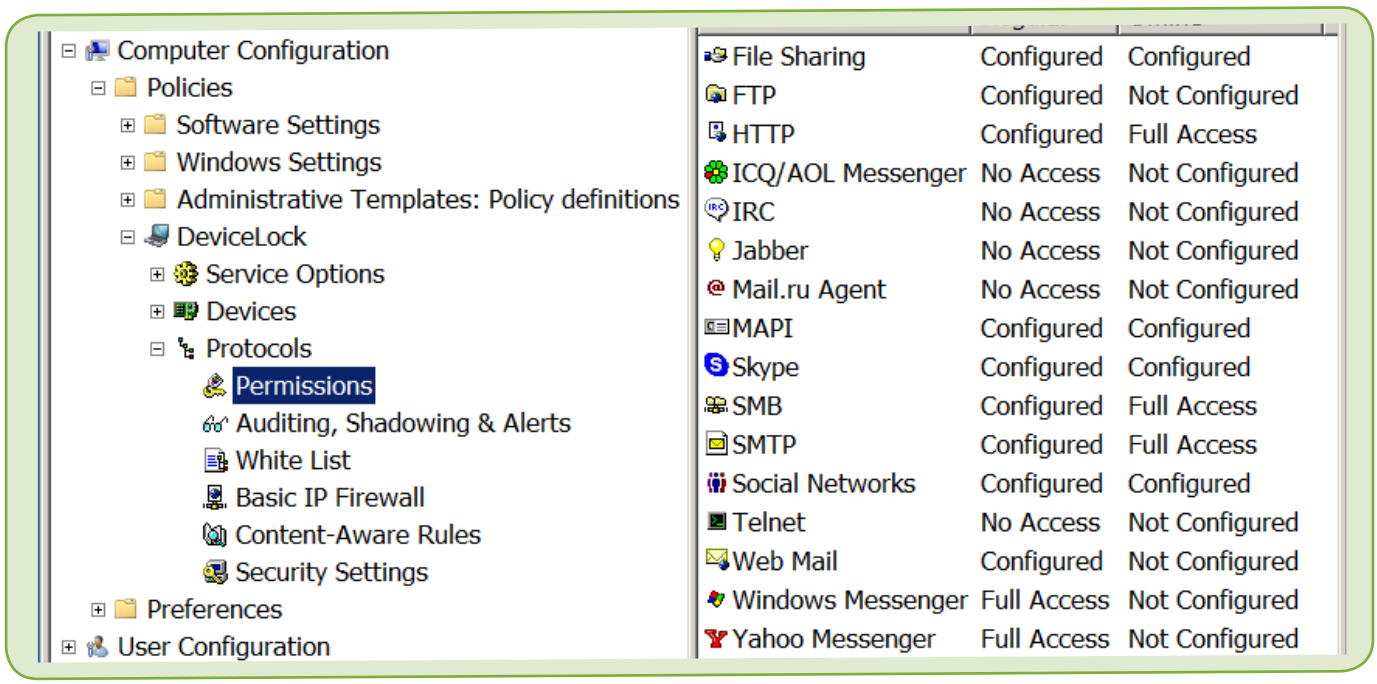
DeviceLock Endpoint DLP Suite delivers essential content filtering capabilities and reliable control over network communications on top of DeviceLock's best-in-industry context-based controls, whereby access to local ports and peripheral devices on corporate endpoint computers is under a DeviceLock administrator's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

**Active Directory Group Policy Integration.** DeviceLock's primary console integrates directly with the Microsoft Management Console (MMC) Active Directory (AD) Group Policy interface. As Group Policy and MMC-style interfaces are completely familiar to AD administrators, there is no proprietary interface to learn or training classes needed to effectively manage endpoint DLP policies centrally. The mere 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 without any scripts, ADM templates, or schema changes whatsoever. Administrators can dynamically manage endpoint settings right along with their other Group Policy–automated tasks. Absent a Group Policy environment, DeviceLock also has classic Windows consoles and a web browser console that can centrally manage agents on any AD, Novell, LDAP, or 'workgroup' IP network of Windows computers. XML-based policy templates can be shared across all DeviceLock consoles.

**Device Whitelisting.** Of the many layers of device security supported by DeviceLock, the USB device model and device ID layers are handled using a whitelist approach. Administrators can scan for and whitelist a specific corporate-issued model of USB drive and DeviceLock will allow only designated users or group members to have access to these at the endpoint. All other unlisted devices and unlisted users are blocked by default. Administrators can even whitelist a single, unique device ID, while locking all other devices of the same brand and model, as long as the device manufacturer has implemented a standard unique identifier.

**Secure Policy Exceptions.** DeviceLock provides a certificate controlled Temporary USB Whitelist Control Panel applet that users can run to securely request short-term use of a USB-mounted device that is otherwise blocked by the local DeviceLock policy...even while the laptop is off the internal network. The specific USB device is mounted and then selected within the applet to generate a unique code that is tied to elements of the device, computer, and user account. The code must be provided to a DeviceLock administrator for evaluation and approval. If approved, a device code is generated for the user that includes the allowed duration of use for up to one month. The rest of the original security policy remains intact and enforced during this authorized "exception device" usage period.

**Network Communications Control.** The NetworkLock module adds comprehensive contextual control over endpoint network communications like network protocols, web applications, and listed Instant Messenger applications like Skype. Regular and SSL-tunneled email communications (SMTP, Exchange-MAPI, and listed web mail services) are controlled with messages and file attachments handled and filtered separately. NetworkLock also controls web access and other HTTP-based applications with the ability to extract the content from encrypted HTTPS sessions. Web applications social networks, cloud-based file sharing web services, and web mail services are secured separately from the HTTP control for easier configuration, while supported sites can be whitelisted for approved users within NetworkLock. See the Product Specifications section for a list of supported web mail services, social networks, cloud-based file sharing services, and instant messengers controlled by NetworkLock.




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

**Content Filtering.** Extending DeviceLock and NetworkLock capabilities beyond contextual security parameters, the ContentLock module can analyze and filter the content of data copied to removable media drives, to other Plug-n-Play storage devices, to the clipboard, or even attempts to print. ContentLock also filters data objects and sessions from within network communications. These include email, web access and popular HTTP-based applications like web mail services, social networks, cloud-based file sharing services, instant messengers, file attachments, web forms/posts, and FTP file transfers.

The content analysis engine can extract textual data from more than 160 file formats and data types and then apply effective and reliable content filtering methods based on pre-built templates of Regular Expression (RegExp) patterns, industry-specific keyword filters (HIPAA, PCI, etc.), document meta properties, verified file types and more. ContentLock templates can be modified with numerical threshold conditions and/or combined with Boolean logic operators (and/or/not/...) for unmatched flexibility of control and to help eliminate 'false positives'.

| Description | Type | Action(s) | Applies To | Device Type(s) | Send Alert | Log Event | Profile |
|---|---|---|---|---|---|---|---|
| Executable | File Type Detection | Deny: Write, Write Encrypted, Read, Read Encrypted | Permissions | Removable | Enabled | Enabled | Regular |
| HIPAA ICD9 | Keywords | Deny: Read | Permissions | Optical Drive | Enabled | Enabled | Regular |
| Password Protected | Document Properties | Allow: Write, Write Encrypted | Shadowing | Removable | Disabled | Disabled | Regular |
| Phone Numbers and Emails | Complex | Deny: Clipboard Outgoing Text, Clipboard Incoming T... | Permissions | TS Devices | Disabled | Enabled | Regular |
| US Social Security Number | Pattern | Deny: Write, Write Encrypted, Read, Read Encrypted | Permissions | Removable | Disabled | Enabled | Offline |
| US Social Security Number | Pattern | Deny: Print | Permissions, Shadowing | Printer | Enabled | Disabled | Regular |

| Description | Type | Action(s) | Applies To | Protocol(s) | Send Alert | Log Event | Profile |
|---|---|---|---|---|---|---|---|
| Bank ABA | Keywords | Allow: Outgoing Messages, Outgoing Files | Shadowing | Social Networks | Disabled | Disabled | Regular |
| Credit Card Number | Pattern | Deny: POST Requests, Outgoing Files, Encrypted PO... | Permissions | HTTP | Enabled | Disabled | Regular |
| Images, CAD & Drawing | File Type Detection | Deny: Outgoing Files, Encrypted Outgoing Files | Permissions | FTP | Enabled | Disabled | Regular |
| Password Protected | Document Properties | Allow: Outgoing Messages, Outgoing Files | Permissions, Shadowing | MAPI | Enabled | Enabled | Regular |
| PCI GLBA | Keywords | Deny: Outgoing Messages, Outgoing Files | Permissions | Skype | Disabled | Enabled | Offline |
| Phone Numbers and Emails | Complex | Deny: POST Requests, Outgoing Files, Encrypted PO... | Permissions | File Sharing | Enabled | Enabled | Regular |
| US Phone Number | Pattern | Deny: Outgoing Messages, Outgoing Files | Permissions | Yahoo Messenger | Enabled | Enabled | Regular |

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

**Virtual DLP for BYOD Devices.** DeviceLock's Virtual DLP features provide the ability to protect any BYOD device against insider data leaks when using leading desktop and application virtualization solutions like Citrix XenApp/ XenDesktop, Microsoft RDS and VMWare View. Running on a VDI Host or Terminal Server, DeviceLock "remotes" content-aware endpoint DLP policies to the securely connected BYOD device to create a virtual endpoint DLP agent that prevents uncontrolled data exchanges to local media, hosted applications and network connections of the device while "in session". This approach unifies DeviceLock DLP across physical and virtual Windows and BYOD environments.

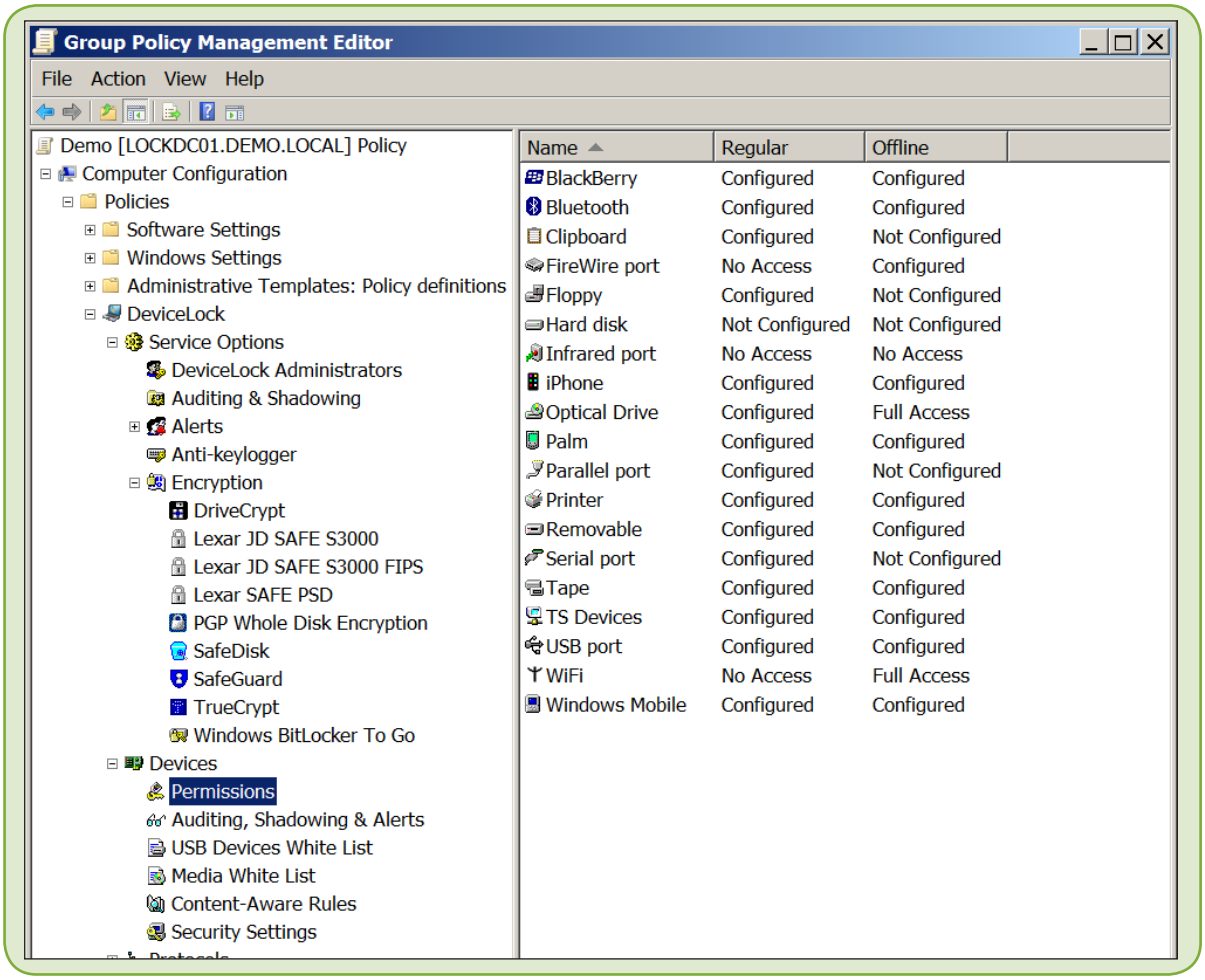
**Clipboard Control.** DeviceLock enables administrators to effectively block data leaks at their earliest stage—when users deliberately or accidentally transfer unauthorized data between different applications and documents on their local computer through the Windows clipboard and print-screen mechanisms. DeviceLock can selectively control user/group access to objects of different data types that are copied into the clipboard. These types include files, textual data, images, audio fragments (i.e. captured with Windows Sound Recorder), and even data of "unidentified" types. In addition, content of textual data copied via the clipboard can be monitored and filtered. DeviceLock DLP separately, independently and uniquely protects and filters clipboard operations when redirected to a remote BYOD device in a terminal session to provide Virtual DLP. Screenshot operations, including the Windows PrintScreen keyboard function and the capture features of third-party applications, can be blocked or mitigated for specific users/ groups to prevent one of the oldest methods of data theft.

**Mobile Device Local Sync Control.** Administrators can use DeviceLock's patented Local Sync technology to set granular access control, auditing, and shadowing rules for mobile devices that use Microsoft Windows Mobile®, Apple iPhone®/iPad®/iPod touch® or Palm® operating systems' local data synchronization. Permissions are uniquely granular and define which "types" of mobile device data (files, pictures, emails, contacts, calendars, etc.) that specified users/groups are allowed to synchronize between managed endpoints and personal mobile devices regardless of the connection interface. Android® devices are controlled by their port connection and "removable media" rules while BlackBerry® smartphones are specifically supported with device presence detection, access control and event logging.

**Printing Security.** DeviceLock puts local and network printing under the strict control of administrators. By intercepting Print Spooler operations, DeviceLock enables administrators to centrally control user access and content of print requests sent to local, network, and even virtual printers from DeviceLock-managed endpoints. In addition, for USB-connected printers, specified printer vendor models and/or unique printer device IDs can be allowed for designated users and groups. Printing events can be logged and the actual print job data can be shadow-copied, collected, and stored centrally for audit and post-analysis.

**Removable Media Encryption Integration.** DeviceLock takes an open integration approach to enforced use of encryption for removable media. It recognizes vendor-specific encryption on removable media when encountered, and it blocks, allows or mitigates access to the device according to predefined use-of-encryption policies. DeviceLock customers have the option of using the encryption solution that best fits their security scenarios among best-of-breed technologies that include: Windows BitLocker To Go™, PGP® Whole Disk Encryption, TrueCrypt®, SafeDisk®, Sophos® Safeguard Easy®, SecurStar® DriveCrypt Plus Pack Enterprise (DCPPE) and Lexar Media's S1100/ S3000 series USB flash drives. DeviceLock allows for discrete access rules for both encrypted and unencrypted or 'Generic' partitions on removable media that use any of the integrated encryption solutions mentioned above. Verified encrypted partitions can be granted write access while any 'Generic' partitions might be blocked or only allowed to be read. Also, any pre-encrypted USB media can be selectively whitelisted with its usage strictly enforced with DeviceLock.

**Offline Endpoint Security.** Administrators can define different online vs. offline security policies for the same user account based on a laptop's network status. For example, one could disable Wi-Fi when docked to the wired corporate network to avoid network "bridging" data leaks and then to enable Wi-Fi when undocked. Or, NetworkLock can be implemented when offline to mimic perimeter network based DLP settings or other security conditions when the laptop is "in the wild."




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

**Anti-Keylogger.** DeviceLock detects USB keyloggers to alert the user, alert admins, or even block 'keyboards' or 'USB hubs' posing as these devices. This allows administrators to securely allow all single-function USB mice and keyboards by their generic HID device class. DeviceLock also obfuscates PS/2 keyboard input and forces PS/2 keyloggers to record unintelligible text instead of real keystrokes.

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

# DeviceLock Observation Mode

DeviceLock is often used at first to collect an audit 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-repudiable audit trail for compliance officials. When a leak is discovered, attempted, or even suspected, DeviceLock provides tools to capture and forensically view objects and associated logs for use as evidence or for corrective policy action.

**Audit Logging.** DeviceLock's auditing capability tracks user and file activity for specified device types, ports and protocols on a managed computer. It can pre-filter auditable events by user/group, by day/hour, by true file type, by port/device type/protocol, 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 or Mac with GMT timestamps. Within DeviceLock's column-based viewers, logs can be sorted by column data and filtered on any string-based criteria with wildcard operators to achieve a desired view of the captured audit data. Logs can also 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/BD burners into the original separated files upon auto-collection by the DeviceLock Enterprise Server (DLES) service collection agents. A full copy of the files can be saved to a secure share populated for forensic review. Shadow data can be pre-filtered by user/group, day/hour, file type, and content to narrow down what is captured and then 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), local quota settings, and optimal DLES server auto-selection.

**Agent Monitoring.** DeviceLock Enterprise Server service agents can monitor remote computers in real time by checking the DeviceLock endpoint agent status (running or not), version, policy consistency and integrity. The detailed information is written to the Monitoring log.

**Alerting.** DeviceLock provides both SNMP and SMTP based alerting capabilities driven by DeviceLock DLP endpoint events for real time notification of sensitive user activities on protected endpoints on the network.

**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 when generated.

**Data Search.** The separately licensed DeviceLock Search Server (DLSS) module 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. The DLSS supports indexing and searching in more than 160 file formats. Language independent 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" (AND) logic with special character wildcards to refine or expand searches. Default results are sorted by 'hit count', though 'term weighting' or 'field weighting' are options. The DLSS also supports full-text indexing and searching of printouts to audit virtually all document printing.

**"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."**

**Data Security Specialist, University of Alabama Health System**

# Product Specifications

## Infrastructure (Installable) Components

- DeviceLock Agent
- DeviceLock Enterprise Server
  DeviceLock Content Security Server
- Consoles: DeviceLock Group Policy Manager
  DeviceLock Management Console
  DeviceLock Enterprise Manager
  DeviceLock WebConsole w/ Apache

## Ports Secured

- USB, FireWire, Infrared, Serial, Parallel

## Device Types Controlled (Partial List)

- Floppies, CD-ROMs/DVDs/BDs, any removable storage (flash drives, memory cards, PC cards, etc.), Hard drives, Tape/Optical devices, WiFi & Bluetooth adapters, Windows Mobile, Palm OS, Apple iPhone/iPod touch/iPad & BlackBerry Devices, MTP-enabled devices (such as Android and Windows Phone smartphones), Printers (local, network and virtual), Modems, Scanners, Cameras, Terminal Services devices

## Clipboard Control

- Inter-application clipboard copy/paste operations
- Data types independently controlled: files, textual data, images, audio, unidentified data with text content filtering
- Screenshot operations (PrintScreen and 3rd-party applications)

## Data Types Controlled & File Formats Parsed

- More than 4,100 verifiable file types
- Data synchronization protocol objects: Microsoft ActiveSync®, Palm® HotSync, Apple iTunes®
- 160+ file formats including nested archives

## Network Communications Controlled

- **Email/Web Mail**: MAPI (Microsoft Exchange), SMTP/SMTPS, Gmail, Yahoo! Mail, Hotmail (Outlook.com), AOL Mail, GMX.de, Web.de, Mail.ru, Rambler Mail, Yandex Mail
- **Social Networking**: Facebook (+API), Twitter, Google+, LinkedIn, Tumblr, MySpace, Vkontakte (+API), XING.com, LiveJournal, MeinVZ.de, StudiVZ.de, Disqus, LiveInternet.ru, Odnoklassniki.ru
- **Instant Messengers**: Skype, ICQ/AOL, Windows Live Messenger, Yahoo! Messenger, IRC, Jabber, Mail.ru Agent
- **Cloud File Sharing Web Services**: Google Drive, Dropbox, SkyDrive, RapidShare, Amazon S3, Yandex Disk, iFolder.ru (Rusfolder.com), Narod.ru
- **Internet Protocols**: HTTP/HTTPS, FTP/FTPS, Telnet
- **Other**: SMB disk shares, Skype Incoming/Outgoing Calls

## Content Filtering Technologies

- Industry-specific (HIPAA, etc) keyword matching template with 'whole word', 'case' options and morphological analysis for words in English, French, Italian, German, Spanish/Catalan, Russian, Portuguese, and Polish
- Pre-built Regular Expression (RegExp) pattern templates with numerical threshold conditions & Boolean (and/or/not/...) rule connectors (Ex. SSN, passport, other government issued numbers, credit cards, banking industry numbers, etc.)
- File and extended document properties (name, size, if password protected, if contains text, last modified date/time, title, subject, tags, categories, comments, authors, Oracle IRM, etc.)
- Content contingent shadowing of removable media, Plug-n-Play storage devices, printing, network protocols, PDA local synchronizations and clipboard operations for all parsed file formats and data types

## Full-Text Audit & Shadow Repository Searching

- All parsed file formats and data types
- PCL, Postscript, and other printout formats
- 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, Japanese, Russian, and Spanish

## Encryption Integration

- Windows 7 BitLocker To Go™
- TrueCrypt®
- Infotecs SafeDisk®
- Lexar® Media S1100/S3000
- PGP® Whole Disk Encryption
- SecurStar® DriveCrypt® (DCPPE)
- Sophos® Safeguard Easy®
- Apple® OS X FileVault

## Virtualized Environment Control

- DeviceLock DLP controls redirected removable drives, network shares, USB devices, printers, clipboard, and serial ports via desktop and session remoting protocols (RDP, ICA, PCoIP, HTML5/WebSockets) as well as network communications of Virtual Desktop & Terminal Session clients. Provides Virtual DLP for BYOD devices restricted to only accessing corporate applications/data in this way

## System Requirements

- **Agent**: Windows NT 4.0/2000/XP/Vista/7/8/8.1, Server 2003-2012 R2 or Apple OS X 10.6.8/10.7/10.8/10.9 (32-bit/64-bit versions); CPU Pentium 4, 64MB RAM, HDD 100MB
- **Consoles**: Windows 2000/XP/Vista/7/8/8.1 or Server 2003-2012 R2; CPU Pentium 4, 2GB RAM, HDD 600MB
- **DeviceLock Enterprise Server**: Windows Server 2003-2012 R2; 2xCPU Intel Xeon Quad-Core 2.33GHz, RAM 8GB, HDD 800GB if hosting SQL DB; MSEE/MSDE/SQLExpress or MS SQL Server


**AMERICAS**
DeviceLock, Inc.
3130 Crow Canyon Place, Suite 215
San Ramon, CA 94583, USA

4720 Kingsway, Suite 2600
Burnaby, BC V5H 4N2, Canada

email: us.sales@devicelock.com
Toll Free: +1 866 668 5625
Phone: +1 925 231 4400
Fax: +1 925 886 2629

**UNITED KINGDOM**
DeviceLock, Inc.
The 401 Centre, 302 Regent Street
London, W1B 3HH, UK
Toll Free: +44 (0) 800 047 0969
Fax: +44 (0) 207 691 7978

**ITALY**
DeviceLock, Srl
Via Falcone 7
20123 Milan, Italy
Phone: +39 02 86391432
Fax: +39 02 86391407

**GERMANY**
DeviceLock Europe, GmbH
Halskestr. 21
40880 Ratingen, Germany
Phone: +49 2102 89211-0
Fax: +49 2102 89211-29

**RUSSIA**
DeviceLock, Russia
M. Semenovskaya d. 9 st. 9 Office 140, 107023 Moscow, Russia
Phone: +7 495 647-9937


[ For more information: www.devicelock.com ]