DeviceLock®

ENDPOINT DATA LEAK PREVENTION 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 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 threat vectors can evade conventional 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 where leaks can otherwise occur.

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 user, the data types, the interface, the device or network protocol, the flow direction, the state of encryption, the date and time, etc.

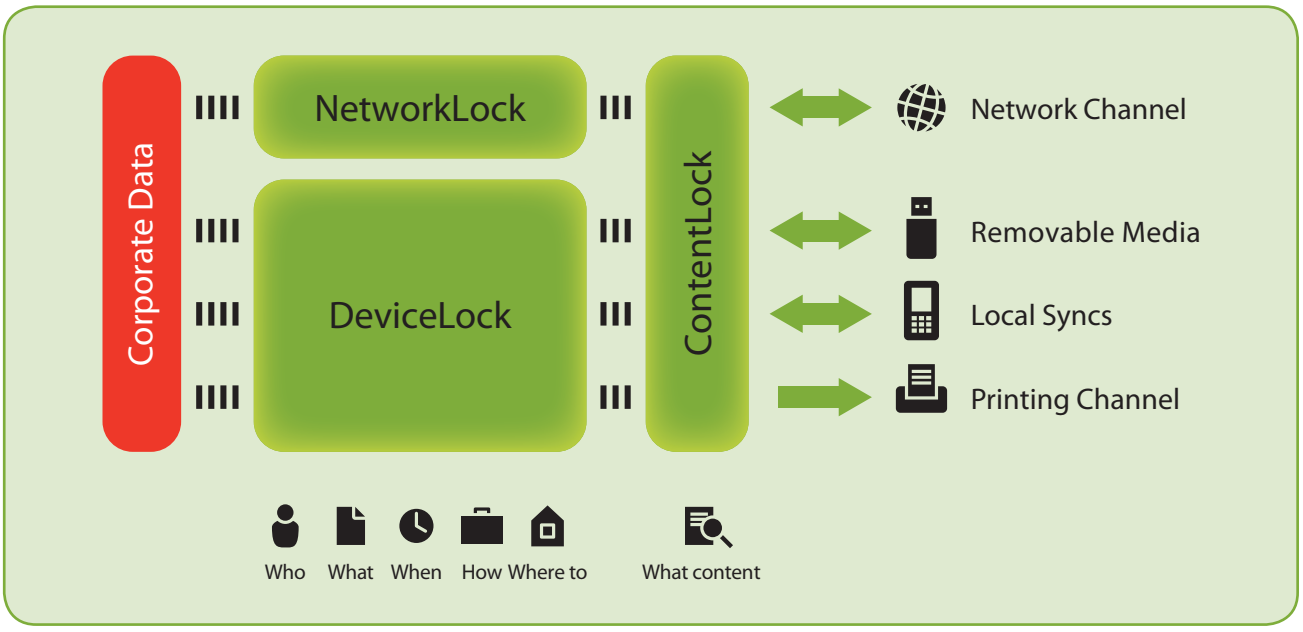
Some scenarios call for a deeper level of awareness than context alone can provide; for example, when the data being handled contains personally identifiable information, when the input/output channel is conventionally open and uncontrolled, and when the users involved have situations or backgrounds 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 Plug-n-Play devices, as well as with network communications.

With DeviceLock, security administrators can precisely match user rights to job function with regard to transferring, receiving and storing data on media attached to 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 locally 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 consuming a minimum of disk space and memory, remaining as transparent as desired to the end users, and while running in tamper-proof mode.

With its fine-grained endpoint contextual controls complemented by content filtering for the most vulnerable 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 platform 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.



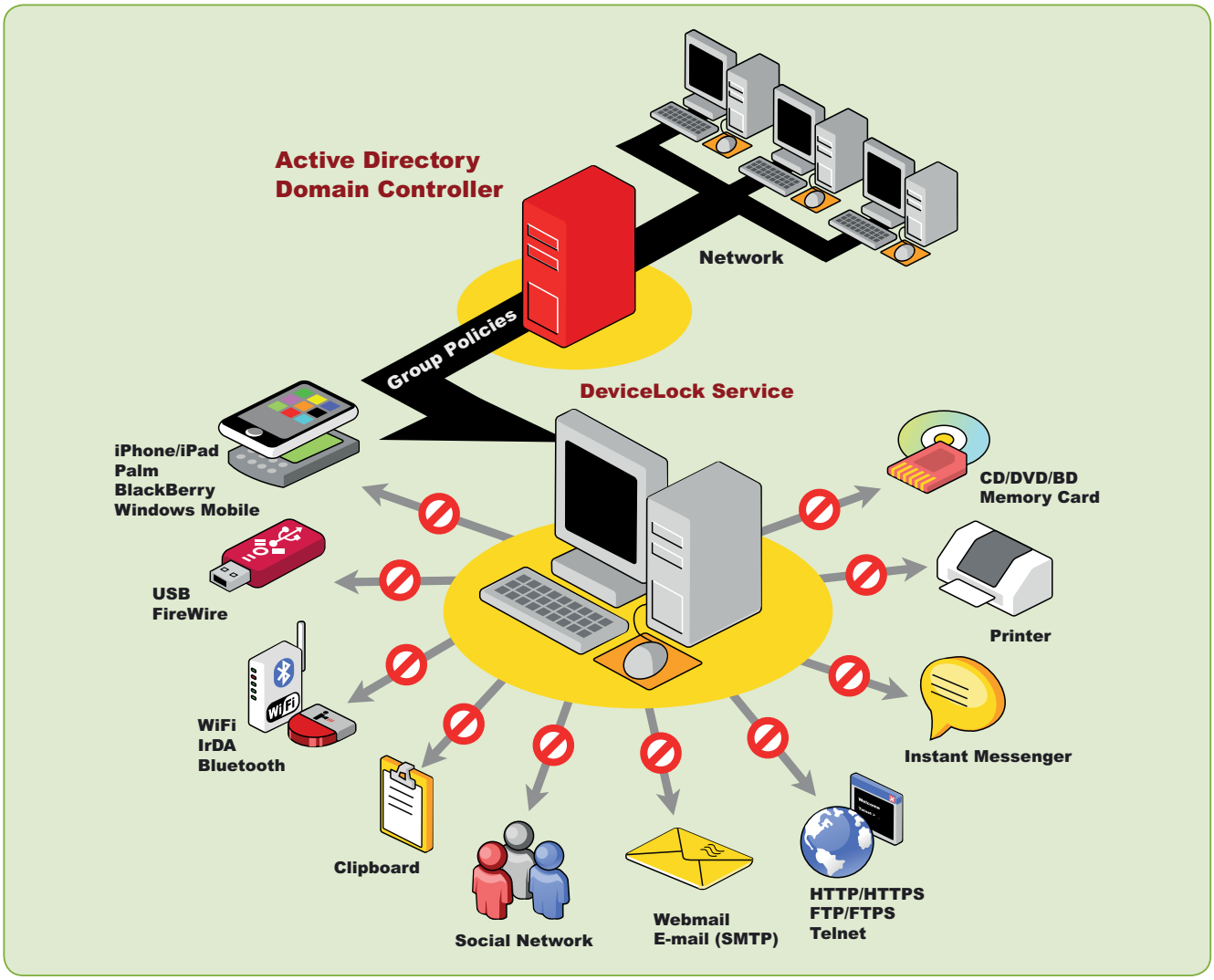
Core DeviceLock functionality enforces device access policy by port (interface), device class, device type, device model, unique device ID, hour-of-day, day-of-the-week, as well as by discrete access parameters such as write, read-only, and format. Device types can be configured to only allow access 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 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. These include peripheral devices and ports, connected smartphones/PDA's, and document printing. DeviceLock provides the core 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 with 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 pre-integrated 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 from network communications that are reconstructed and passed to it by NetworkLock. These include emails, instant messages, web forms, attachments, social media exchanges, file transfers, and telnet sessions.
- DeviceLock® Search Server (DLSS) is another separately licensed component that 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 core DeviceLock component is mandatory for every product installation. All other modules, including NetworkLock, ContentLock, and DeviceLock Search Server, are separately licensed, optional and pre-integrated add-ons. This modular product structure and flexible licensing scheme enable DeviceLock customers 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 new function-specific module licenses to "activate" additional 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

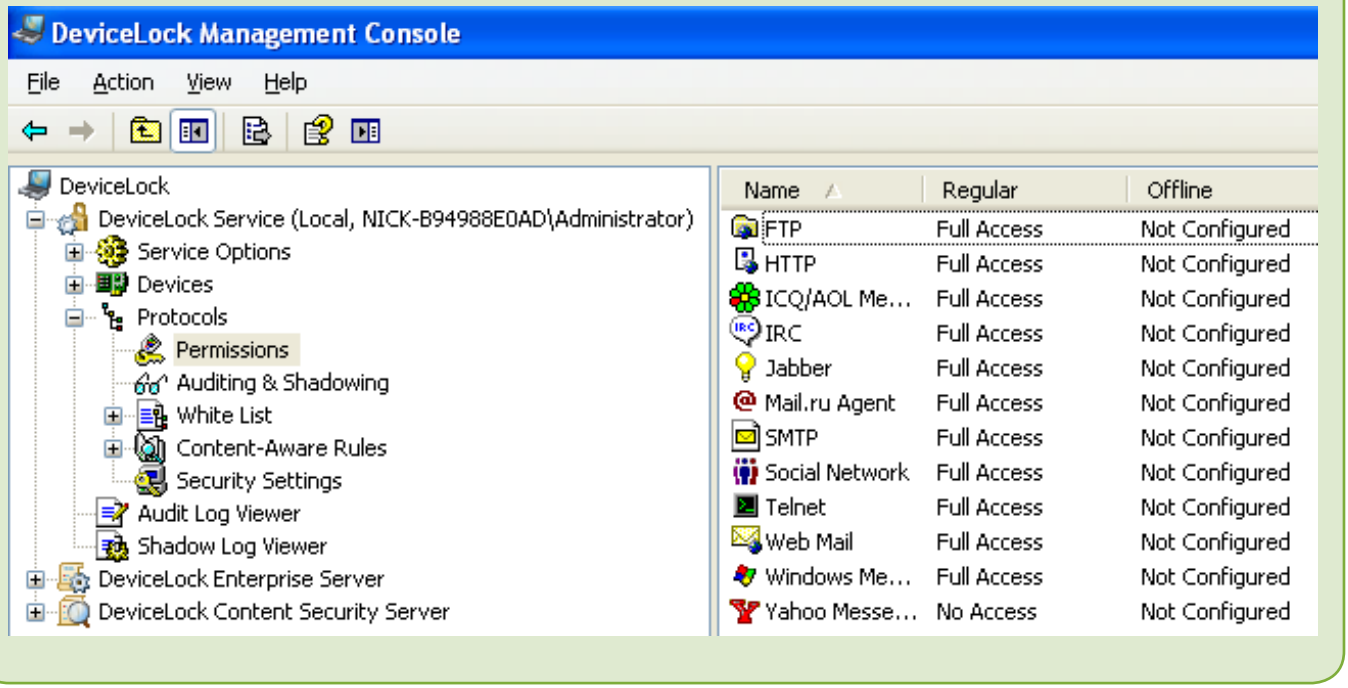
DeviceLock Endpoint DLP Suite delivers essential content filtering capabilities and reliable control over network communications on top of DeviceLock's best-in-industry context-based controls, whereby access to local ports and peripheral devices on corporate endpoint computers is under a DeviceLock administrator's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

Active Directory Group Policy Integration. DeviceLock's 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–automated 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, Novell, 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.

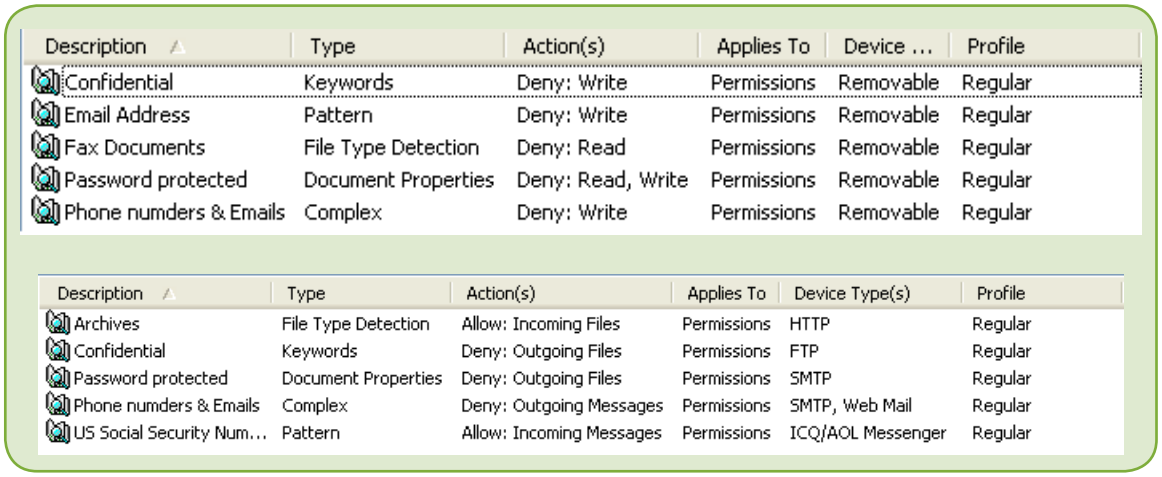
Device Whitelisting. Among the five layers of Windows device control supported by DeviceLock, the USB device model and device ID levels are handled using a whitelist approach, whereby the DeviceLock administrator can explicitly assign users/groups to a USB device. Administrators can whitelist a specific 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 authorized 'exception device' usage period.

Network Communications Control. An optional component of the DeviceLock Endpoint DLP Suite, the NetworkLock module adds comprehensive contextual control over endpoint network communications. NetworkLock supports port-independent network protocol and application detection with selective blocking, message and session reconstruction with file, data, and parameter extraction, as well as event logging and data shadowing. NetworkLock controls heavily trafficked network protocols and applications. These include plain and SSL-tunneled SMTP email communications with messages and attachments handled separately. NetworkLock also controls web access and other HTTP-based applications with the ability to extract the content from encrypted HTTPS sessions. See the Product Specifications section for a list of all webmail and social media applications 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 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 from within network communications. These include email, web access and other HTTP-based applications like webmail and social networking, many popular instant messaging applications, FTP file transfers, and telnet sessions. 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-aware rules, pre-built industry-specific keyword lists can be used as filter criteria, as well as common "RegExp" data pattern templates for sensitive information types like social security numbers, credit cards, addresses, etc.



Description	Type	Action(s)	Applies To	Device ...	Profile
Confidential	Keywords	Deny: Write	Permissions	Removable	Regular
Email Address	Pattern	Deny: Write	Permissions	Removable	Regular
Fax Documents	File Type Detection	Deny: Read	Permissions	Removable	Regular
Password protected	Document Properties	Deny: Read, Write	Permissions	Removable	Regular
Phone numders & Emails	Complex	Deny: Write	Permissions	Removable	Regular

Description	Type	Action(s)	Applies To	Device Type(s)	Profile
Archives	File Type Detection	Allow: Incoming Files	Permissions	HTTP	Regular
Confidential	Keywords	Deny: Outgoing Files	Permissions	FTP	Regular
Password protected	Document Properties	Deny: Outgoing Files	Permissions	SMTP	Regular
Phone numders & Emails	Complex	Deny: Outgoing Messages	Permissions	SMTP, Web Mail	Regular
US Social Security Num...	Pattern	Allow: Incoming Messages	Permissions	ICQ/AOL Messenger	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.

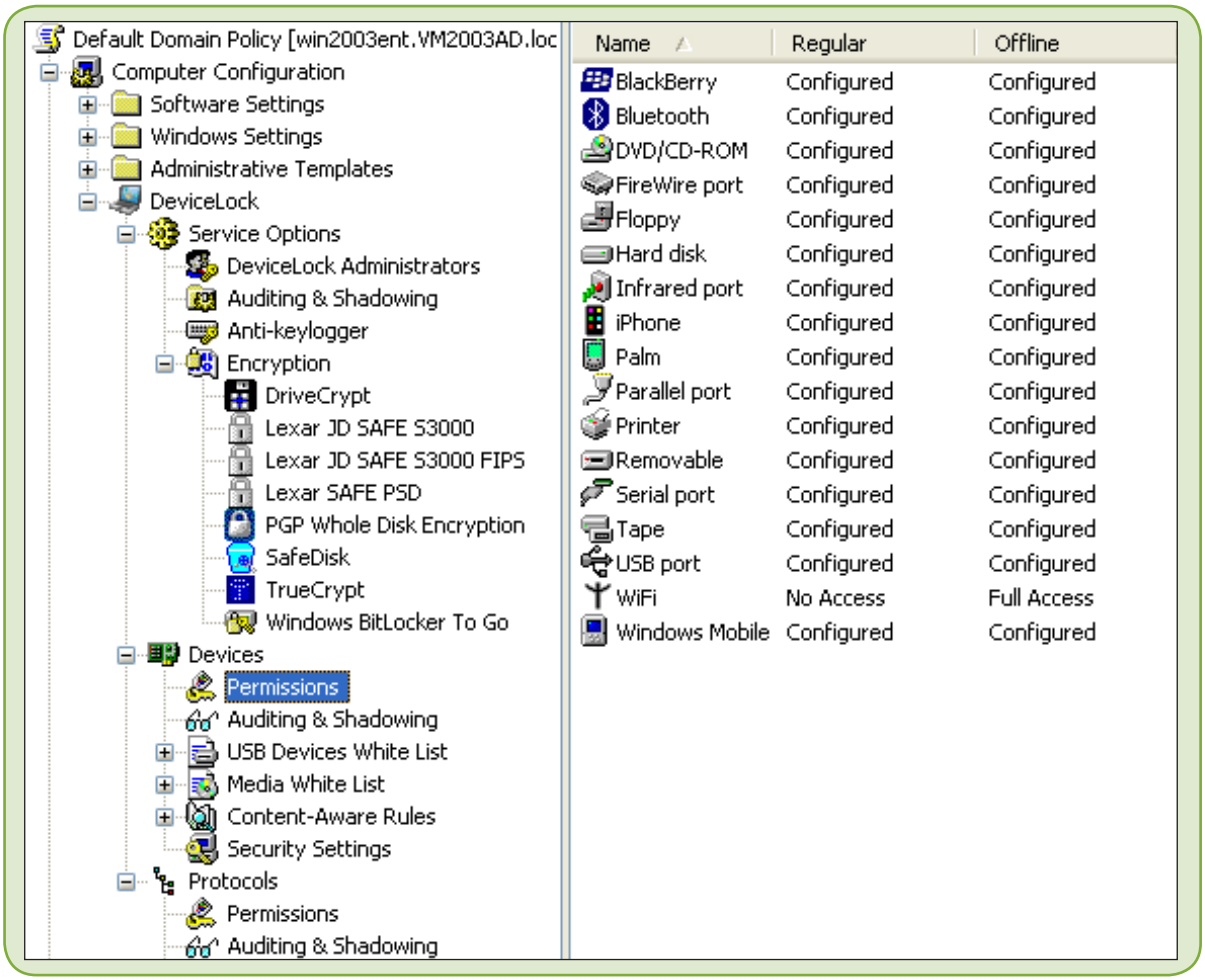
True File Type Control. Administrators can selectively grant or deny access to over 4,000 specific file types for removable media. When a file type policy is configured, DeviceLock will look into a file's binary content to determine its true type (regardless of file name and extension) and enforce control 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, including the Windows PrintScreen function and similar features of third-party applications, can be blocked or mitigated for specific users/groups and at specific computers.

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 the Microsoft Windows Mobile®, Apple iPhone®/iPad®/iPod touch® or Palm® operating systems' local data synchronization. Permissions are presented with fine granularity and define which types of data (files, pictures, emails, contacts, calendars, etc.) specified users and/or groups are allowed to synchronize between managed 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 Print Spooler operations, DeviceLock enables administrators to centrally control user access to local, network, and even virtual printers from DeviceLock-managed PCs. 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 media when encountered, and it blocks, allows or mitigates access to the device according to predefined encryption policies. 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; TrueCrypt®; SafeDisk®, 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 partitions of removable media that use any of the integrated encryption solutions mentioned above. With its partnering approach, DeviceLock is positioned to quickly add support for more encryption vendors as the market demands. In addition, any pre-encrypted USB media can be selectively whitelisted with usage strictly enforced.



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.

Network-Awareness. Administrators 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 network "bridging" data leaks and then 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 single-function USB mice and keyboards by their generic device 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.

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 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 and ports on a local computer. It can prefilter 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. 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 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 prefiltered by user/group, day/hour, file type, and content to narrow down what is copied 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 can monitor remote computers in real-time by checking DeviceLock agent status (running or not), version, policy consistency and integrity. The detailed information is written to the Monitoring log. Should this process uncover that some DeviceLock agents are older versions or are inconsistent with the current security policy template, DeviceLock can then be used to remotely update those agents to the current version and 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 when generated.

Data Search. The optional and 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. 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 are available options. The DLSS also supports full-text indexing and searching of printouts in PCL and PostScript languages 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."

David Gardner, Data Security Specialist, University of Alabama at Birmingham Health System

Product Specifications

Infrastructure (Installable) Components
- DeviceLock agent
- DeviceLock Enterprise Server (DLES)
- Consoles: DeviceLock Group Policy Manager (DLGPM)
  DeviceLock Management Console (DLMC)
  DeviceLock Enterprise Manager (DLEM)

Licensed Modules
- DeviceLock® (core required)
- NetworkLock™
- ContentLock™
- DeviceLock Search Server (DLSS)

Ports Secured
- USB, FireWire, Infrared, Serial, Parallel

Device Types Controlled (Partial List)
- Floppies, CD-ROMs/DVDs, any removable storage (flash drives, memory cards, PC cards, etc.), Hard drives, Tape/Optical devices, WiFi adapters, Bluetooth adapters, Windows Mobile, Palm OS, Apple iPhone/iPod touch/iPad and BlackBerry Devices, Printers (local, network and virtual), Modems, Scanners, Cameras.

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

Data Types Controlled
- More than 4,000 file types
- Data synchronization protocol objects: Microsoft ActiveSync®, Palm® HotSync, iTunes®
- Pictures containing text as image

Network Communications Controlled
- Web Mail (including mobile versions): Gmail, Yahoo!Mail, Windows Live Mail , AOL Mail, Mail.Ru, Yandex.Mail, WEB.DE, GMX.de
- Social Networking (including mobile versions): Google+, Facebook, Twitter, LiveJournal, LinkedIn, MySpace, Odnoklassniki, Vkontakte , XING.com, Studivz.de, Meinvz.de, Schuelervz.net
- Instant Messengers: ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent
- Internet Protocols: HTTP/HTTP over SSL, SMTP/SMTP over SSL, FTP/FTP over SSL, Telnet

Content Filtering Technologies
- Industry-specific and custom keyword filter templates
- Advanced Regular Expression (RegExp) 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.)

Content Filtering Channels
- Removable media and other Plug-n-Play storage devices
- Network communications

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

Content-Aware Data Shadowing
- Removable media and other Plug-n-Play storage devices, network communications, local syncronizations, clipboard operations
- All parsed file formats and data types

Full-Text Searching
- All parsed file formats and data types
- 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, Japanese, Russian & Spanish

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

Approved Encrypted Devices
- IronKey®: D20XXX, S-200 & D200 Series Enterprise, Personal & Basic Models
- Systematic Development Group: LOK-IT
- BlockMaster®: SafeSticks
- Lexar Media: SAFE S1100 & S3000 Series
- SanDisk®: Cruzer® Enterprise Series

Component Dependencies
- ContentLock, NetworkLock and DLSS require 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/64-bit versions); CPU Pentium 4, 64MB RAM, HDD 25MB
- DeviceLock consoles: Windows NT 4.0/2000/XP/Vista/7 or Server 2003/2008 (32-bit /64-bit versions); CPU Pentium 4, 2GB RAM, HDD 800GB
- DeviceLock Enterprise Server: Windows Server 2003 R2; 2xCPU Intel Xeon Quad-Core 2.33GHz, RAM 8GB, HDD 800GB; MSEE/MSDE or MS SQL Server

[For more information: www.devicelock.com]

UNITED STATES
2440 Camino Ramon, Ste. 130
San Ramon, CA 94583, USA
email: us.sales@devicelock.com
Toll Free: +1 866 668 5625
Phone: +1 925 231 4400
Fax: +1 925 886 2629

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

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

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

DeviceLock
Proactive Endpoint Security