DeviceLock®

Proactive Endpoint Security

Why Consider an Endpoint DLP Solution?

GROUP POLICY-INTEGRATED DATA LEAK PREVENTION FOR PROTECTING SENSITIVE INFORMATION

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 and Macs to flash memory sticks, smartphones, cameras, PDAs, 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 as 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 or Apple macOS controls, the DeviceLock data leak prevention (DLP) solution addresses them. DeviceLock DLP 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's separate content discovery capabilities help prevent leakage of data stored on corporate computers, network shares and storage systems. DeviceLock also delivers Virtual DLP that extends data leak prevention to a variety of session-based, streamed and local virtual machines as well as to BYOD devices using desktop and application virtualization architectures.

DeviceLock® 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, trusted employees can handle data that contains personally identifiable information (PII), financials, health data, "Confidential", or intellectual property (IP) 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 proceed.

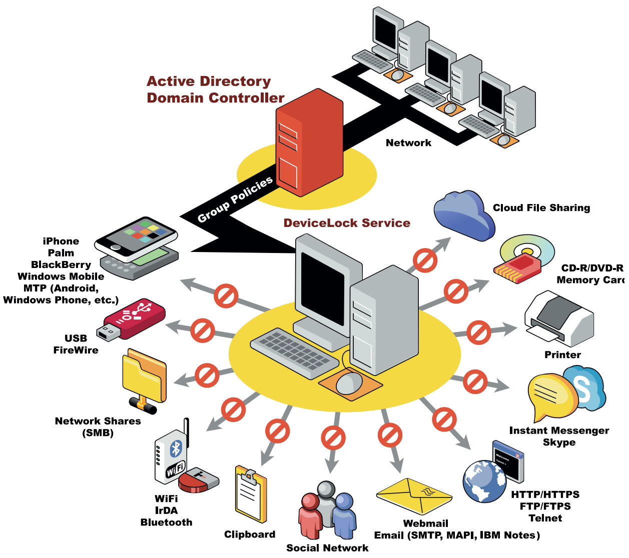
DeviceLock DLP provides both contextual *and* content-based controls on protected endpoint computers for maximum leakage prevention at minimum cost. Its multi-layered inspection and interception engine provides granular control over a full range of data leakage pathways in both "data-in-use" and "data-in-motion" scenarios to further ensure that data each customer defines as sensitive is not escaping. DeviceLock's content analysis and filtering can be applied to endpoint data exchanges with removable media, Plug-n-Play devices, printers, SMB file shares, email, web, Skype and IM sessions, as well as other network communications. In addition, content awareness is fundamental for preventing leakages of "data-at-rest" – a critical DLP function that DeviceLock provides with its Discovery module for inspecting data residing on network shares, storage systems and Windows endpoint computers.

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 MMC snap-in DeviceLock consoles. These centrally defined DLP policies in Active Directory are automatically pushed to distributed agents for continual enforcement on physical and virtual Windows endpoints as well as Apple macOS computers.

DeviceLock enables administrators to centrally control, log, shadow-copy, alert and analyze end-user data transfers to most leak-prone types of peripheral devices and ports, as well as network communications on protected 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. The DeviceLock endpoint agent 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.

Extending its data protection beyond "data-in-use" and "data-in-motion" from endpoints, DeviceLock Discovery can automatically scan and inspect the file content on Windows servers, other network-accessible data stores and Windows endpoint peripherals in the corporate IT environment in order to detect and remediate "data-at-rest" storage policy violations.

With its fine-grained contextual controls complemented by content filtering for the most vulnerable endpoint data channels, DeviceLock DLP 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.



Enterprises can protect endpoints against data leakage with DeviceLock DLP Suite

DeviceLock® Modular Structure and Licensing

DeviceLock DLP 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** component includes an entire set of contextual controls together with event logging, data shadowing and alerting for local data channels on protected computers. These include peripheral devices and ports, clipboard, tethered smartphones/PDA's, MTP-enabled devices (Android, Windows Phone, etc.), mapped drives redirected to desktop and application sessions from remote BYOD devices, printscreens and document printing. DeviceLock Core provides the mandatory platform, as well as all central management and administrative components for other functional modules of the DeviceLock Endpoint DLP Suite.

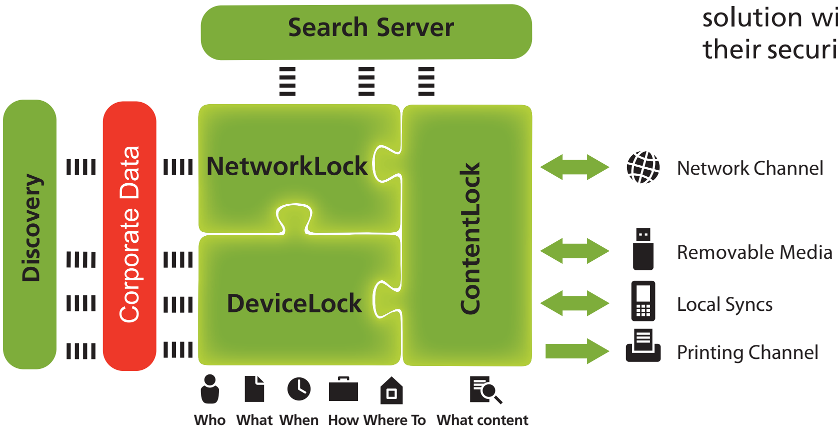
- The pre-integrated **NetworkLock™** component provides contextual control functions over network communications like web, email and more. NetworkLock's port-independent protocol detection along with complete session data reconstruction and extraction allow for deep packet inspection, event logging, 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, webmails, file attachments, instant messages, web forms, social media exchanges and file transfers.

- **DeviceLock® Discovery** is a separate functional component that enables organizations to gain visibility and control over confidential "data-at-rest" stored across their IT environment in order to proactively prevent data breaches and achieve compliance with regulatory and corporate data security requirements. The detailed information for DeviceLock Discovery can be found in a separate brochure.

- **DeviceLock® Search Server (DLSS)** is an optional add-on 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.

- **Licensing.** The DeviceLock Core component is mandatory for every installation of the DeviceLock Endpoint DLP that optionally includes NetworkLock, ContentLock and DeviceLock Search Server licensed separately. DeviceLock Discovery, which can be licensed and used independently of any other DeviceLock component, includes the Discovery Server and Discovery Agents. DeviceLock Discovery seamlessly integrates with any combination of DeviceLock Endpoint DLP components version 8 or higher by leveraging the built-in content discovery capabilities of DeviceLock Agents. This modular product structure and flexible licensing enable DeviceLock customers the option to cost-effectively deploy 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. Customers can then extend the solution with "data-at-rest" content discovery as their security and compliance requirements grow.



Control of DLP data flow

[www.devicelock.de]

DeviceLock® Features and Benefits

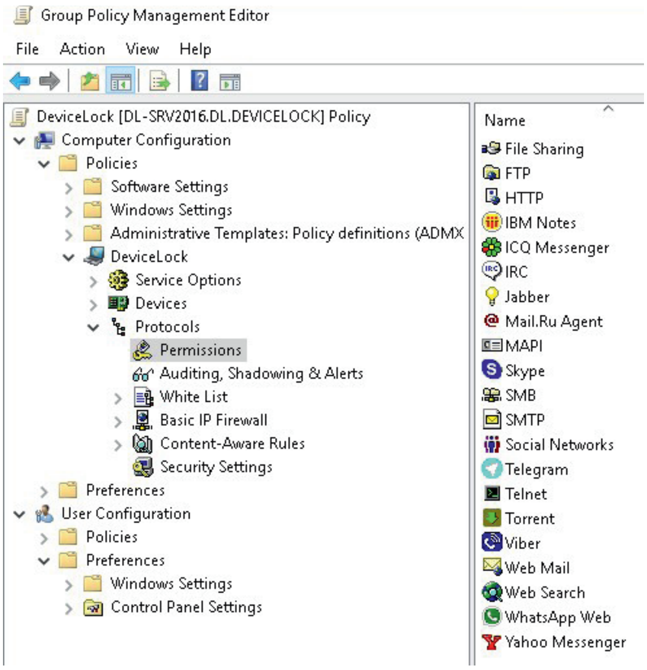
DeviceLock DLP delivers essential content filtering and discovery capabilities, as well as reliable control over network communications on top of DeviceLock's best-in-industry context-based controls, whereby access to local ports and peripheral devices on corporate endpoint computers is under a DeviceLock 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 both Windows and Apple macOS 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 Novell, LDAP, or 'workgroup' IP network of Windows and Apple macOS computers. XML-based policy templates can be shared across all DeviceLock consoles.

Device Whitelisting. Of the many layers of Windows and Apple macOS 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 can be 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 Windows 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 access 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 Windows endpoint network communications including SMB file shares, network protocols, web applications and listed Instant Messenger applications like Skype. Regular and SSL-tunneled email communications (SMTP, Exchange-MAPI, IBM Notes and listed webmail 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, web searches, social networks, cloud-based file sharing web access and webmail services are secured separately from the HTTP control for easier configuration, while supported sites, URLs, email addresses and sender/recipient IDs can be whitelisted for approved users within NetworkLock. In addition, peer-to-peer file sharing connections by torrent clients on corporate computers can be contextually allowed or blocked while their details are logged and real-time alerts are sent out. Refer to the Product Specifications section for a list of supported webmail services, social networks, cloud-based file sharing services, web search engines and instant messengers controlled by NetworkLock.



DeviceLock [DL-SRV2016.DL.DEVICELOCK] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX
    - DeviceLock
      - Service Options
      - Devices
      - Protocols
        - Permissions
        - Auditing, Shadowing & Alerts
        - White List
        - Basic IP Firewall
        - Content-Aware Rules
        - Security Settings
  - Preferences
- User Configuration
  - Policies
  - Preferences
    - Windows Settings
    - Control Panel Settings

Name
- File Sharing
- FTP
- HTTP
- IBM Notes
- ICQ Messenger
- IRC
- Jabber
- Mail.Ru Agent
- MAPI
- Skype
- SMB
- SMTP
- Social Networks
- Telegram
- Telnet
- Torrent
- Viber
- Web Mail
- Web Search
- WhatsApp Web
- Yahoo Messenger

NetworkLock controls permissions for network communications in GPO

DeviceLock® Features and Benefits

Content Filtering. Extending DeviceLock and NetworkLock capabilities beyond contextual security, ContentLock can analyze and filter the textual and binary content of data copied to removable drives, to other Plug-n-Play storage devices, to the clipboard, data sent for printing and even data hidden in screenshots, graphical files or images in documents. ContentLock also filters the content of data objects and sessions within controlled network communications. These include SMB network shares, email, web access, and HTTP-based applications like webmails, social networks, cloud-based file sharing services, instant messengers, file attachments, web forms/posts/searches, and FTP file transfers. The content analysis engine can extract textual data from 150+ file formats and data types and then apply effective and reliable content filtering methods. Content detection of structured data is based on pre-built templates of Regular Expression (RegExp) patterns and industry-specific keyword dictionaries (HIPAA, PCI, etc.), while data fingerprinting is used to detect unstructured textual and binary content. Data fingerprints are categorized to their respective Data Classifications with certain levels of importance or secrecy (e.g. "Restricted", "Confidential", "Secret", "Top Secret", etc.). In addition, ContentLock can recognize and use for content filtering classification labels assigned to documents and files by Boldon James Classifier products. Document meta properties and verified file types can be content analysis factors. Content detection rules can be configured with numerical threshold conditions and/or combined with Boolean logic operators (AND/OR/NOT) for unmatched flexibility of control.

Host-Resident OCR. Complementing content filtering of textual-based data objects, a built-in optical character recognition (OCR) engine allows DeviceLock DLP to quickly, efficiently and accurately extract and inspect textual data from pictures in documents and graphical files of many image formats. With 30+ languages recognized, this highly efficient OCR engine uses DeviceLock's regular expressions, keyword dictionaries and other advanced methods to improve recognition and deliver the ability to discover and protect exposed confidential data presented in graphical form. Unique to DeviceLock DLP is that the OCR module runs in each of its enforcement oriented components: DeviceLock Agent, DeviceLock Discovery Server and DeviceLock Discovery Agent. This distributed OCR architecture tremendously improves the overall functional scope and performance of the solution. Since the graphical objects stored on endpoints can be inspected by local host-resident OCR modules, this decreases the load to the Discovery Server, as well as reduces the „scan" traffic on the corporate network.

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 remote desktop and application virtualization solutions like Citrix XenApp/XenDesktop, Microsoft RDS and VMware Horizon View. Running on a VDI Host or Terminal Server, DeviceLock "remotes" contextual and content-aware endpoint DLP controls to the connected remote BYOD device as a virtual endpoint DLP agent that prevents uncontrolled data exchanges to local peripherals, hosted applications and network connections of the BYOD 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, and even data of "unidentified" types. In addition, content of textual data, files, images, screenshots and unidentified binaries copied via the clipboard can be monitored and filtered. DeviceLock DLP separately, independently and uniquely protects and filters data operations of the clipboard redirected from a remote BYOD device to a terminal session to provide Virtual DLP. Screenshot operations can be blocked for specific users/groups, including screen capturing by Windows and third party applications. If screenshots are allowed contextually by policy, ContentLock's advanced OCR content inspection can filter the textual content of captured screen images according to DLP policies on-the-fly.

Mobile Device Local Sync Control. Administrators can use DeviceLock's patented Local Sync control technology to set granular access control, auditing, and shadowing rules for data that Microsoft Windows Mobile®, Apple iPhone®/iPad®/iPod touch® or Palm® mobile devices exchange through local synchronizations with Windows endpoints. Permissions are uniquely granular and define which "types" of mobile device data that specified users/groups are allowed to synchronize between managed endpoints and personal mobile devices regardless of the connection interface. Presence detection, access control and event logging for Android®, Windows Phone and other MTP devices, as well as BlackBerry® smartphones are specifically supported at the device type level.

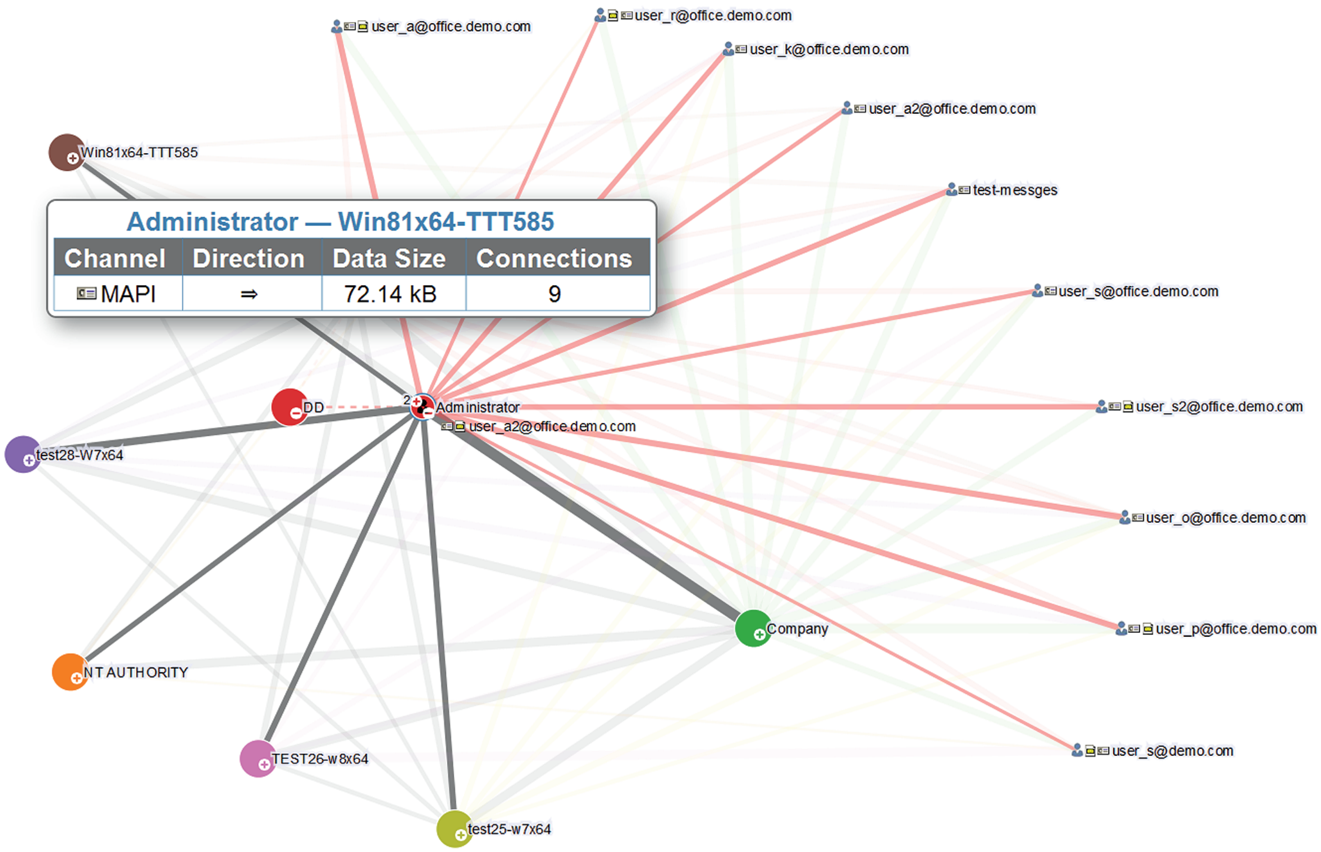
DeviceLock® Features and Benefits

Printing Security. DeviceLock puts printing from Windows endpoints under the strict control of security administrators. By intercepting Print Spooler operations, DeviceLock allows to centrally control user access and content of printed documents sent to local, network and even virtual printers from protected computers. In addition to character-based content inspection, DeviceLock uses its OCR capabilities to analyze the textual content of pictures contained in printed documents. Besides, 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 in searchable PDF format, collected and stored centrally for audit and post-analysis.

Offline Endpoint Security. Administrators can define different online vs. offline security policies for the same user account based on a Windows or Mac 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. On Windows computers, NetworkLock can be used when offline to enforce network perimeter-like DLP settings or other security conditions when the laptop is "in the wild."

Tamper Protection. The configurable 'DeviceLock Administrators' feature prevents tampering with DeviceLock policy settings locally on Windows and Apple macOS, even by users with 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 and upgrade the agent or modify DeviceLock policies in any way.

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. With the interactive Relations Chart report generated from the log data about user communications, DeviceLock administrators can view and easily analyze relationships between users within the organization and with their external contacts. This HTML-based report, which can be viewed in a web browser or in the DeviceLock Management Console, shows user connections for the following applications and protocols: ICQ Messenger, Jabber, Skype, Skype for Web, Yahoo Messenger, IBM Notes, SMTP, Webmail, and Social Networks.



Administrator — Win81x64-TTT585

Channel	Direction	Data Size	Connections
MAPI	⇒	72.14 kB	9

Graphical Relations Chart Example: The flow of blocked communication attempts due to policy violations are shown above from collected log data

[www.devicelock.de]

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 access control or content policy action.

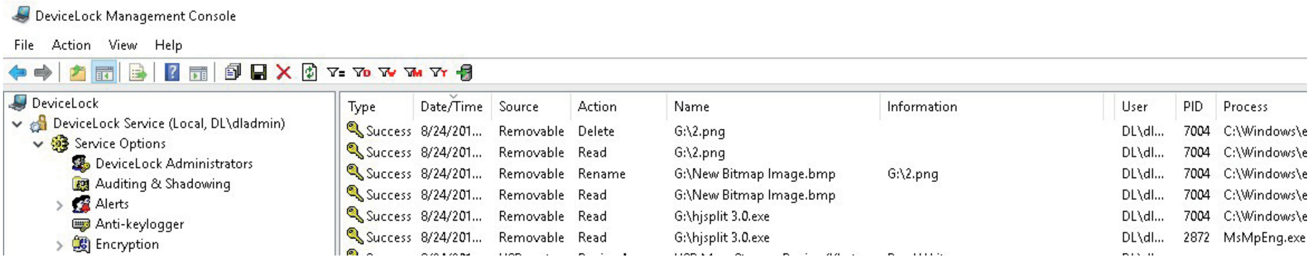
Audit Logging. DeviceLock's auditing capability tracks user and file activity for specified device types, ports and protocols on a managed computer. It can pre-filter auditable events by user/group, by day/hour, by true file type, by port/device type/protocol, by reads/writes and by success/failure events. DeviceLock employs the standard event logging subsystem on Windows and Apple macOS. 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 Windows 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 SNMP, SYSLOG and SMTP based alerting capabilities driven by DeviceLock DLP endpoint events for real time notification of sensitive user activities on protected Windows endpoints on the network.

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 convenient. The DLSS supports indexing and searching in more than 100+ file formats. In addition, the built-in OCR technology allows the extraction of text in 30+ languages from images (such as scanned documents, screen shots, etc.) of more than 30 formats for further indexing by DLSS. 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', although 'term weighting' or 'field weighting' are also options. DLSS also supports full-text indexing and searching of printouts to audit virtually all document printing.



DeviceLock
- DeviceLock Service (Local, DL\dladmin)
  - Service Options
    - DeviceLock Administrators
    - Auditing & Shadowing
    - Alerts
    - Anti-keylogger
    - Encryption

Type	Date/Time	Source	Action	Name	Information	User	PID	Process
Success	8/24/201...	Removable	Delete	G:\2.png		DL\dl...	7004	C:\Windows\e
Success	8/24/201...	Removable	Read	G:\2.png		DL\dl...	7004	C:\Windows\e
Success	8/24/201...	Removable	Rename	G:\New Bitmap Image.bmp	G:\2.png	DL\dl...	7004	C:\Windows\e
Success	8/24/201...	Removable	Read	G:\New Bitmap Image.bmp		DL\dl...	7004	C:\Windows\e
Success	8/24/201...	Removable	Read	G:\hjsplit 3.0.exe		DL\dl...	7004	C:\Windows\e
Success	8/24/201...	Removable	Read	G:\hjsplit 3.0.exe		DL\dl...	2872	MsMpEng.exe

The tamper-proof Audit Log displays detailed information about individual user activity

DeviceLock® Product Specifications

Infrastructure (Installable) Components

- Agents and Servers: DeviceLock Agent (Windows and Apple macOS), DeviceLock Discovery Agent (Windows), DeviceLock Enterprise Server, DeviceLock Content Security Server (Discovery Server, Search Server)
- Management Consoles: DeviceLock Group Policy Manager (MMC snap-in to Microsoft GPMC), DeviceLock Management Console (MMC snap-in), DeviceLock Enterprise Manager, DeviceLock WebConsole w/Apache

Ports Secured

- **Windows:** USB, FireWire, Infrared, Serial, Parallel
- **Mac:** USB, FireWire, Serial
- **Session terminal/BYOD:** USB, Serial

Device Types Controlled (Partial List)

- **Windows:** removable storage (flash drives, memory cards, PC Cards, eSATA, etc.), CD-ROM/DVD/BD, floppies, hard drives, tapes, Wi-Fi and Bluetooth adapters, Apple iPhone/iPod touch/iPad, Windows Mobile, Palm OS, BlackBerry, MTP-enabled devices (such as Android and Windows Phone), printers (local, network and virtual), modems, scanners, cameras
- **Mac:** removable storage, hard drives, CD-ROM/DVD/BD, Wi-Fi and Bluetooth adapters
- **Session terminal/BYOD:** mapped drives (removable, optical, hard), USB devices

Clipboard Control (Windows)

- Inter/intra-application copy-paste operations via Windows clipboard
- Copy operations between host and guest OS clipboards
- Data transfers between Windows and desktop/application session clipboards
- Screenshot operations (Print Screen and 3rd party applications)

Network Communications Controlled

- **Email:** SMTP/SMTPS, Microsoft Outlook (MAPI), IBM Notes
- **Webmail:** AOL Mail, freenet.de, Gmail, GMX.de, Hotmail/Outlook.com, NAVER, Outlook Web App/Access (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail
- **Social Networking:** Disqus, Facebook (+API), Google+, Instagram, LinkedIn, LiveJournal, MeinVZ.de, MySpace, Pinterest, StudiVZ.de, Tumblr, Twitter, Vkontakte (+API), XING.com
- **Instant Messengers:** ICQ Messenger, IRC, Jabber, Yahoo! Messenger, Skype/Skype for Web/Skype for Business Web App, Telegram, Viber, WhatsApp
- **Cloud File Sharing Web Services:** Amazon S3, Box, Dropbox, freenet.de, GitHub, GMX.de, Google Docs/Google Drive, iCloud, Magenta-CLOUD, MediaFire, MEGA, OneDrive, Sendspace, Web.de, WeTransfer, Yandex.Disk, 4shared
- **Web Searches:** Google, Yandex, Bing, Baidu, Yahoo, Ask.com, AOL Search, Rambler, Wolfram Alpha, DuckDuckGo, WebCrawler, Search.com, Wayback Machine, Dogpile, StartPage, Excite, NAVER, Web.de
- **Internet Protocols:** HTTP/HTTPS, FTP/FTPS, Telnet
- **Other:** SMB disk shares, Skype Private Conversations, Skype media calls, Torrent, Tor Browser traffic

Content-Aware Controls

- **Controlled Channels:** storage devices (removable, floppy, optical CD/DVD/BD drives), printers (local, network, virtual), clipboard (Windows, desktop/application session), mapped drives (desktop/application session), network communications (email, webmail, IM, social networks, cloud file sharing services, HTTP/HTTPS, FTP/FTPS, SMB file shares)
- **Content Types Controlled:** textual content, binary data, data types
- **Textual Content Objects:** parsable file formats (100+) & archives (40+), textual data (in emails, messages, web forms, etc.), images (OCR processing), Oracle IRM-sealed documents, unidentified binary data, data objects classified by Boldon James Classifier.
- **Textual Content Detection Methods:** keywords and keyword dictionaries (160+ prebuilt, user-configurable) with morphological analysis (English, French, German, Italian, Russian, Spanish, Catalan Spanish, Portuguese, Polish), RegExp templates (90+ prebuilt, user-configurable), data fingerprints for partial/exact document matching within Data Classifications (pre-built, user-configurable)
- **Binary Data Detection Methods:** data fingerprints
- **Controlled Data Types:** verified file types (5,300+), file/document properties, embedded image properties, clipboard data types (files, textual data, images, audio, unidentified), sync protocol objects (Microsoft ActiveSync®, WMDC, Apple iTunes®, Palm® HotSync), Oracle IRM-sealed documents (security contexts)
- **Content-Aware Data Shadowing:** for controlled channels and content types
- **OCR Features:** endpoint-resident OCR processing, 30+ graphical formats, 30+ languages, integrated DeviceLock keyword dictionaries and regular expressions, rotated/mirrored/inverted images

Encryption Integration

- **Windows:** Windows BitLocker To Go™, Sophos® SafeGuard Easy®, SecurStar® DriveCrypt® (DCPPE), TrueCrypt®, Symantec Disk Encryption, Infotecs SafeDisk®, SafeToGo
- **Mac:** Apple® macOS FileVault

Central Log Collection

- Proprietary secure protocol with traffic shaping/priority
- SYSLOG

Alert Delivery Methods

- SMTP, SNMP, SYSLOG

Content Discovery

- **Scan Targets:** Windows endpoint computers (file systems, email repositories, mounted peripherals), Windows Servers, network shares, storage systems, synchronization folders of cloud-based file hosting applications
- **Scan modes:** agentless, agent-based, mixed
- **Scan operations:** manual and scheduled automatic task execution
- **Remediation actions:** Delete, Safe Delete, Delete Container, Set Permissions (for NTFS files), Log, Alert, Notify User, Encrypt (using EFS for NTFS files)
- **Other features:** static & dynamic target list configuration, discovery reports, automatic on-demand Discovery Agent installation/removal

System Requirements

- **Agents:** Windows NT/2000/XP/Vista/7/8/8.1/10/Server 2003-2016 (32/64-bit); OS X 10.6 up to macOS 10.13 (32/64-bit); Microsoft RDS, Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View; VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC; CPU Pentium 4, 512MB RAM, HDD 400MB
- **Consoles:** Windows 2000/XP/Vista/7/8/8.1/10/Server 2003-2016 (32/64-bit); CPU Pentium 4, 512MB RAM, HDD 1GB
- **DeviceLock Enterprise Server, DeviceLock Discovery Server, DeviceLock Search Server:** Windows Server 2003-2016 (32/64-bit), Microsoft RDS, Citrix XenServer, VMware vSphere Desktop; 2xCPU Intel Xeon Quad-Core 2.33GHz, RAM 8GB, HDD 800GB (if hosting SQL DB); SQL Express/MS SQL Server 2005-2017

[www.devicelock.de]

DeviceLock Europe GmbH
Halskestr. 21
40880 Ratingen
Germany

Phone +49.2102.131840
Fax +49.2102.1318429
info@devicelock.de
www.devicelock.de

For DeviceLock offices in
AMERICA, CANADA,
UNITED KINGDOM and ITALY
please refer to:

www.devicelock.com