

ContentLock & NetworkLock

The DeviceLock Endpoint DLP Suite includes DeviceLock's best-of-breed device and port access control software, plus the advanced ContentLock™ and NetworkLock™ modules for even more granular security over data objects that attempt to move off of managed endpoints through peripheral devices or network communications. ContentLock and NetworkLock are separately licensed options that take the who-what-when-where-how insight supplied by DeviceLock and amplify its effectiveness in the battle against endpoint data leaks by adding content-awareness and network communication controls.

ContentLock™. The ability to analyze the content of data streams is considered the defining feature of a Data Leak Prevention (DLP) solution by some experts—and it has been the height of complexity and costliness by many early DLP users. Now, with DeviceLock plus ContentLock, IT security administrators can selectively analyze content relevant to its context at the local endpoint with security settings managed from DeviceLock's MMC-based Active Directory Group Policy Objects.

ContentLock supports content filtering for data objects copied to removable drives, other Plug-n-Play storage devices, and through network communications secured by the NetworkLock module on the endpoint. Recognizing more than 80 file data formats and thousands of file types, ContentLock extracts and filters the content of files and other data object types including emails, instant messages, web forms, social network exchanges, telnet sessions, text-in-picture, etc. ContentLock filters data streams based on desired Regular Expression (RegExp) patterns, numerical conditioning and Boolean combinations of

“AND/OR” criteria matching. Over 50 contextual parameters can be used. These include users, computers, groups, ports, interfaces, devices, data channels, types, data flow directions, day/time boundaries, etc.

ContentLock's content filtering technology makes DeviceLock's data shadowing feature even more efficient, scalable and intelligent. Content-based data shadowing is supported for all endpoint data channels including removable and plug-and-play storage devices, network communications, local synchronizations with supported smartphones and document printing. Incoming and/or outgoing transmissions can be conditionally shadowed. By pre-filtering the content of potentially large data objects before shadowing to the log, DeviceLock downsizes the streams to just those objects that contain information meaningful for post-analysis tasks like security compliance auditing, incident investigations, and cyber-forensics. This significantly reduces storage space requirements and network bandwidth consumption for pre-compressed shadow data and log collection back to the central database.

The DeviceLock
Endpoint DLP
Suite enables
control over
data operations
based on
their content
and relevant
contextual
conditions.

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 numbers & Emails	Complex	Deny: Write	Permissions	Removable	Regular

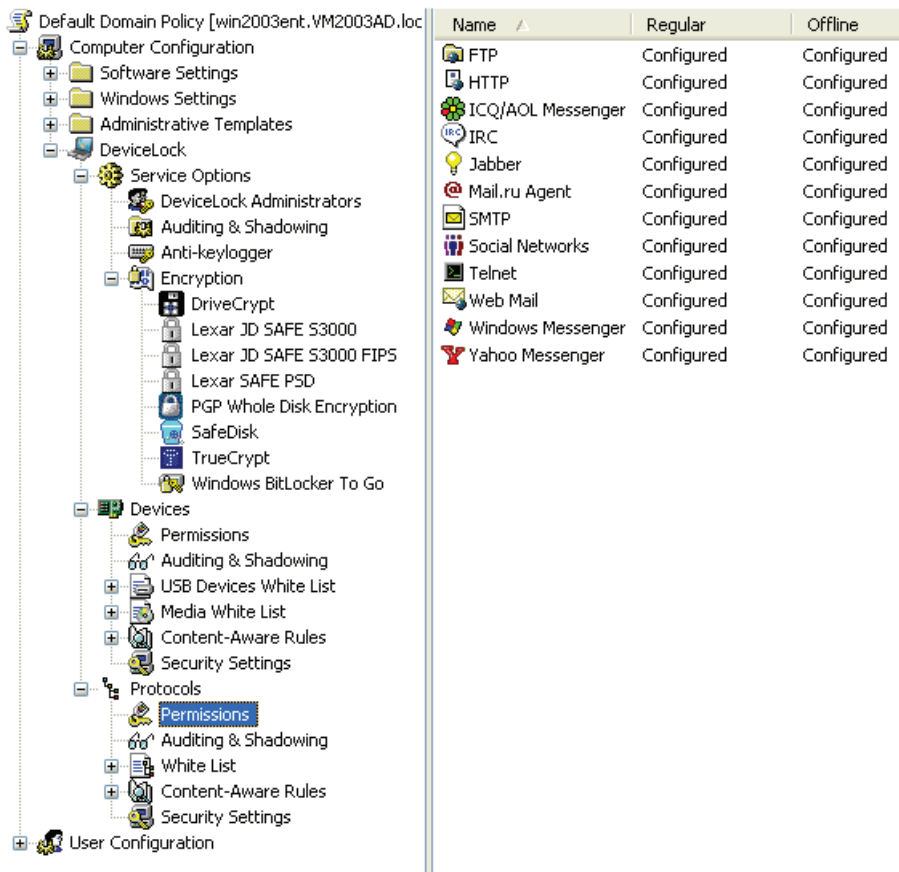
Description	Type	Action(s)	Applies To	Device Type(s)	Profile
Archives	File Type Detection	Allow: Incoming Files	Permissions	HTTP	Regular
Confidential	Keywords	Deny: Outgoing Files	Permissions	FTP	Regular
Password protected	Document Properties	Deny: Outgoing Files	Permissions	SMTP	Regular
Phone numbers & 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 MMC-style interface eases definition of content-aware filtering policies. In the lower-level configuration screens (not shown), detailed rule options using logical operators, pre-built industry-specific keyword dictionaries and Regular Expression templates are presented. These are available for common sensitive information types like Social Security Numbers, credit cards, bank accounts, addresses, driver's license numbers, etc.

NetworkLock™. To address the many under-controlled input/output channels and data leakage scenarios at endpoint computers, the DeviceLock Endpoint DLP Suite also provides contextual control and content filtering of the data objects that commonly comprise inbound and outbound network traffic on the PC.

NetworkLock's detection technology is port-independent and recognizes network applications types and protocols where data leakage can occur (See the chart below for list). NetworkLock can be configured to control web mail, social networking communications, instant messaging, file transfer operations and Telnet sessions. With this module in place, you can specify whitelist-

oriented policies by IP address, address range, subnet masks, network ports and their ranges including those based on “more than/less than” threshold criteria. NetworkLock can intercept, inspect and control plain and SSL-tunneled SMTP email communications with messages and attachments controlled separately, as well as web access and other HTTP-based applications and encrypted HTTPS sessions. Messages and sessions are reconstructed with file, data and parameter information extracted and then passed to the ContentLock module for content filtering. Audit (event) logging and data shadowing trails are maintained as conditionally specified.



NetworkLock's managed network protocols and applications.

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

- Requirements**
- ▶ ContentLock and NetworkLock require installation of the core DeviceLock module.
 - ▶ NetworkLock requires ContentLock for content-aware rule enforcement on network communications.

DLP delivered

as an easy,

precise,

resource-

efficient and

cost-effective

solution.

DeviceLock
Proactive Endpoint Security

2440 Camino Ramon, Ste. 130

San Ramon, CA 94583, USA

email: us.sales@deviceclock.com

Toll Free: +1 866 668 5625

Phone: +1 925 231 4400

Fax: +1 925 886 2629

The 401 Centre, 302 Regent Street

London, W1B 3HH, UK

Toll Free: +44 (0) 800 047 0969

Fax: +44 (0) 207 691 7978

Via Falcone 7

20123 Milan, Italy

Phone: +39 02 86391432

Fax: +39 02 86391407

Halskestr. 21

40880 Ratingen, Germany

Phone: +49 2102 89211-0

Fax: +49 2102 89211-29