# DeviceLock® DLP

Achieve HIPAA Compliance with
The Industry's Most Trusted Endpoint DLP Solution

DID YOU KNOW that over 50% of electronic Protected Health Information (ePHI) security incidents are the result of inadvertent data breaches from trusted internal staff and NOT from external adversaries? And the main source of these internal security breaches are data leaks via computer endpoints.

Since 1996, DeviceLock has pioneered innovative DLP solutions that set the standard for the endpoint security industry. Our multi-award winning solutions have been deployed in some of the world's most security intensive and regulated environments including healthcare organizations, medical research institutions, military hospitals and pharmaceutical companies.

DeviceLock DLP
The Industry Benchmark
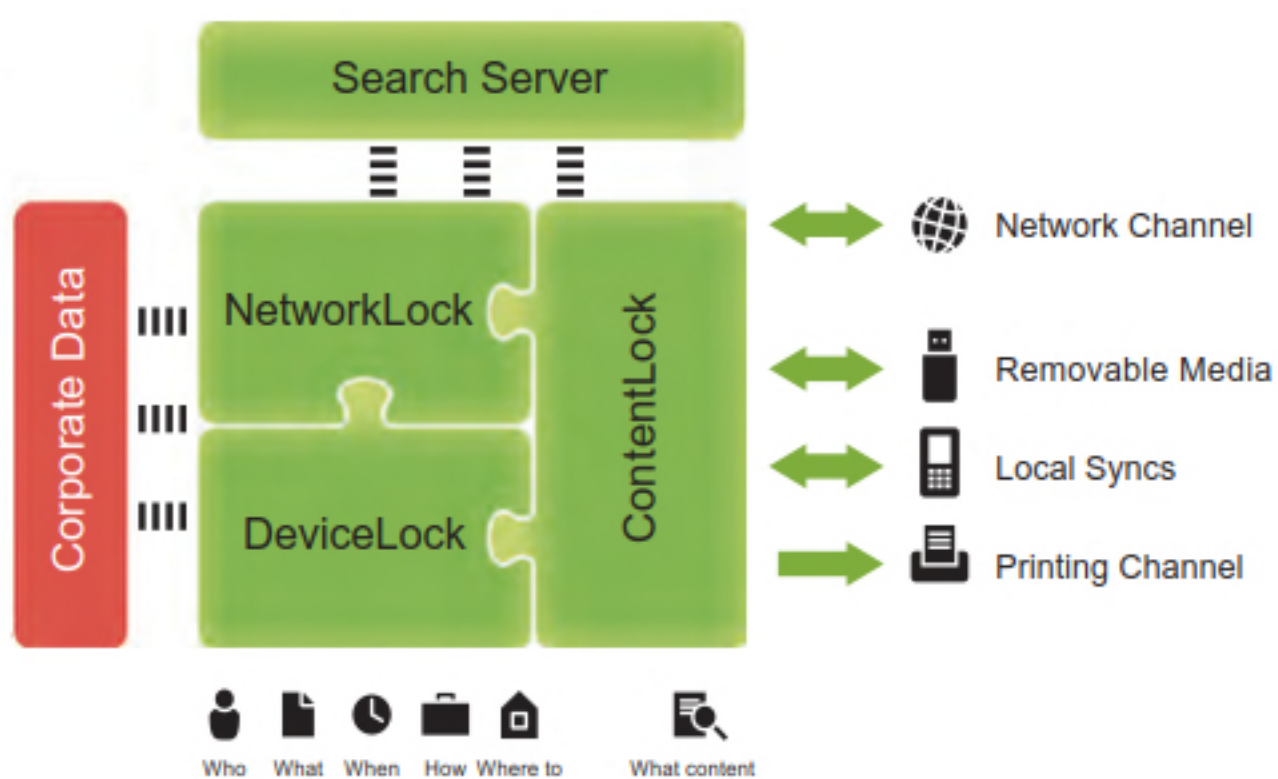
▶ **Context-based Controls** – Block or allow data flows by user, security group membership, file type, device type, network/email protocol, cloud service, hour-of-day, day-of-week, etc.

▶ **Content-based Controls** – Easily configured content rules and filtering of both "data-in-use" and "data-in-motion" ensures ePHI data is not leaking out through endpoints.

▶ **Advanced Monitoring and Reporting** – Centrally log, shadow-copy, alert and forensically analyze end-user data transfers to devices, ports, printers and network communications.

▶ **Content Discovery** – Gain visibility and control over sensitive "data-at-rest" stored across the entire network environment to proactively prevent potential ePHI breaches.

▶ **Extensive Data Handling** – Support for over 5,300 file types, 160 file formats, and on-the-fly OCR in 25+ languages to handle data within files, emails, documents, chat sessions, images, compressed archives and scans.

▶ **Easy Management and Administration** – Native integration via Microsoft Active Directory Group Policy console snap-ins for a highly configurable yet simple to manage endpoint DLP solution for Windows administrators.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

DeviceLock Endpoint DLP Suite 8.0
Peter Stephenson, Technology Editor 9/1/2015

Product Rating

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★★
Overall Rating	★★★★★

SC MAG says:

Strengths Too many to list. **Weaknesses** None that we found. **Verdict** If you want a traditional tool for managing and preventing data leakage at the endpoint, this has got to be your cup of tea. If functionality isn't here you probably don't need it.

Healthcare organizations around the world use DeviceLock to secure their endpoints and ensure compliance with increasingly stringent ePHI legislation. Trusted by over 70,000 organizations of all types, and deployed on over 7 million devices.

Stop Data Leaks at the Source with DeviceLock
Download a free 30-day trial at: www.devicelock.com/download

Product Specifications

Infrastructure (Installable) Components
- DeviceLock Agent (Windows and Apple OS X)
- 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
- **Terminal Services/BYOD/VDI/RDS:** 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
- **Terminal Services/BYOD/VDI/RDS:** mapped drives (removable, optical, hard), USB devices

Clipboard Control
- 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, Gmail, Hotmail/Outlook.com, GMX.de, Web.de, Yahoo! Mail, Mail.ru, Rambler Mail, Yandex Mail, Outlook Web App/Access (OWA)
- **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 Messenger, IRC, Jabber, Windows Messenger, Yahoo! Messenger, Mail.ru Agent, WhatsApp Web
- **Cloud File Sharing Web Services:** Amazon S3, Dropbox, Google Docs/Google Drive, OneDrive, Box, Rusfolder.com, Cloud Mail.ru, Yandex.Disk,
- **Internet Protocols:** HTTP/HTTPS, FTP/FTPS, Telnet
- **Other:** SMB disk shares, Skype media calls, Torrent

Content-Aware Controls
- **Controlled Channels:** storage devices (removable, floppy, optical drives), printers (local, network, virtual), clipboard, network communications (email, webmail, IM, social networks, cloud file sharing services, HTTP/HTTPS, FTP/FTPS)
- **Content Types Controlled:** textual content, data types
- **Textual Content Objects:** parsable file formats (120+) & archives (40+), textual data (in emails, messages, web forms, etc.), images (OCR processing), Oracle IRM-sealed documents, unidentified binary data
- **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)
- **Controlled Data Types:** verified file types (5300+), 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:** on-the-fly endpoint-resident OCR processing, 25+ 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®, PGP® Whole Disk Encryption, Infotecs SafeDisk®, Lexar® Media S1100/S3000
- **Mac:** Apple® OS X FileVault

Content Discovery
- **Targets:** Windows endpoint computers (file systems, email repositories, mounted peripherals), 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
- **Agent:** Windows NT/2000/XP/Vista/7/8/8.1/10/Server 2003-2012 R2 (32/64-bit); Apple OS X 10.6.8/10.7-10.11 (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 2003-2012 R2 (32/64-bit); CPU Pentium 4, 512GB RAM, HDD 1GB
- **DeviceLock Enterprise Server, DeviceLock Discovery Server, DeviceLock Search Server:** Windows Server 2003-2012 (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, less if not); MSEE/MSDE/SQL Express or MS SQL Server