DeviceLock, Inc.

DeviceLock DLP 8

■

Reviewer's Guide

Table of Contents

Insider Data Breaches Endanger Corporate IT Security

In the past ten years, advances in computing technologies, electronics and telecommunications, combined with the "viral" consumerization of "personal" devices that are being used and approved by corporate IT, have dramatically changed the ways and methods of how "business" data is accessed, communicated, protected and stored. .

The groundbreaking transformation started a decade ago from the explosive growth in capacity of portable USB storage devices complemented by their ease of use, pocket-friendly dimensions and reduced prices. With USB and other flash-based removable storage, it became much easier to exchange data with colleagues, business partners and clients and – a few years later – even carry the entire image of your desktop environment literally hanging on a USB keychain dongle.

With the proliferation of Web 2.0 technologies, social media for many organizations have evolved into a vital tool to support and speed up business processes. Nowadays, social media are used both internally and externally to build the corporate brand, improve the company's reputation and customer loyalty, hire talented staff, mobilize the collective knowledge of employees, shorten the development cycle and improve the responsiveness of technical support processes. HR managers look for job candidates on LinkedIn and XING, research & development teams publish their development guides on corporate Wikis, while technical support personnel use instant messengers to troubleshoot critical issues in real-time with customers.

Instant messaging (IM) has become another undeniably useful IT "utility" for organizations of any kind. The most illustrative example is Skype. Its simplicity and automatic self-configuration, ability to punch through network perimeters, high quality multimedia calls in combination with large savings from its use have made Skype a truly indispensable communications platform across the globe. Statistics from 2011 show that 35% of all Skype users were small businesses, which used it as their primary communications tool.

In 2007-2009, a new incarnation of ultra-portable storage "devices" emerged – "virtual drives" living in the "cloud". They could be accessible or "plugged in" to any computer via the Internet and used as easily as physical hard drives or, alternatively, accessed from a web browser. Besides, they were free for personal use. Google Drive, Dropbox, SkyDrive, Amazon S3 and many other cloud-based file sharing services have instantly "intoxicated" users of corporate networks by making file storage and exchanges extremely easy, fast and reliable – both for personal use and business purposes. Today, most organizations, regardless of size, allow their employees to use file sharing services in order to simplify and ease internal and external information exchange.

More recently, the "bring your own device" (BYOD) model has become the "mobile steroid" of corporate IT consumerization. In certain industries BYOD devices have already mobilized almost the entire workforce. Via remote VPN or terminal sessions, employees can access corporate email and business applications, as well as data stored centrally on the organization's servers. Not only it is virtually impossible to stop the BYOD "invasion" into the enterprise, but this would be counterproductive since the use of private devices for business has been shown to increase employee productivity and job satisfaction.

However, alongside the benefits brought to organizations by the advanced technologies and IT consumerization, they have also become a fertile "nutrient medium" for a whole new range of information security threats and risks of a scale and severity never seen before.

These threats stem from the convergence of the following factors:

- Firewalls, VPN, anti-virus and other security technologies that were successfully used to protect corporate networks and computers from Internet-borne threats offered virtually no protection from locally unsecured devices and ports. Their security mechanisms were simply not designed to stop a disgruntled employee from plugging a flash drive or smartphone in the USB port of their corporate desktop to download confidential data and walk it out the door undetected.
- Along with the many marketing benefits brought to businesses, social media have triggered several IT security problems. In addition to extra network bandwidth consumption, deteriorated employee productivity and exposure to inappropriate content, the use of social media in the enterprise has increased the risks of malware infections and leakage of confidential information. The infections occur when employees download

files and data to their business computers. Data leaks happen when employees accidentally or deliberately publish or upload sensitive corporate data to social websites or other destinations outside of the protected organization's network perimeter.

- On the one hand, Skype provides the highest level of communications security in the industry – all user calls, chats and file transfers are strongly encrypted with a government-grade algorithm and a proprietary key management protocol that is not vulnerable to man-in-the-middle attacks. On the other hand, the user-centric design intrinsic to the Skype architecture is focused on providing data security exclusively for end users. Skype protects them against any threat and control from the outside environment – be it a network, an application on the same computer or its operating system. Skype's end-to-end traffic encryption cannot be proxied by security gateways or host-resident software as is practiced for standard SSL tunnels. As a result, conventional IT security solutions cannot detect and block data leaks via Skype. Neither can such incidents be traced back to individuals committing the violation. In the network, it is only possible to fully block the Skype's traffic from a particular computer – but this "all-or-nothing" measure would totally prevent using Skype as the valuable business communications tool it has proven to be.
- Unrestricted employee access to cloud-based file storage and sharing services is considered to be more dangerous than uncontrolled use of removable storage devices by today's IT security departments. Once a document with confidential corporate information has been uploaded by an employee to their private account in a cloud-based storage, the organization completely looses its control over whom the employee could allow access to this document in future.
- The BYOD models implemented today have created an enormous vector of new threats to corporate IT security resulting from the private ownership of BYOD devices. IT departments do not completely control them, but must try to secure their use to the best of their abilities with available tools. For most BYOD devices in use today, if an employee uses or stores corporate data in the private environment on the BYOD device, it means that the employee could grant access or send this corporate data to anyone without any control from the IT security department. Even most Mobile Device Management (MDM) security solutions can only rely upon remote-kill and/or remote-wipe features should the device emerge again on the network, but those are truly last resort options for devices reported as lost or stolen. None of these features stop otherwise unintentional data egress, nor certainly intentional data leakage.
- Finally, a fundamental factor for corporate IT security is that the cybercrime industry has commercialized stolen data: rather than just disrupt, delete, or hassle the user, cybercrime's ultimate goal now and going forward is the financial profit gained from selling valuable information stolen from individuals, businesses and government organizations – everything from personal credit cards and passwords to intellectual property and national secrets. As the cybercrime ecosystem has become information-centric, the technologies and tools used by cyber thieves are purely targeting data. This is why modern malware attacks incorporate sophisticated exfiltration provisioning components whose mission is to covertly transfer captured data from compromised corporate computers and other devices to collection points in the "Dark Web" of the Internet.

To a large extent, it is this "hunt for data" that has led to the growth of cybercrime damage to the global economy to total more than €240 billion a year[1].

And it is *the cumulative outcome of the above threat vectors that has rendered conventional IT security solutions designed to protect IT infrastructure components practically helpless against this* ***new breed of attacks****.*

As a result, data breaches are on the rise. According to the database of worldwide security breaches maintained by Risk Based Security, during the first nine months of 2014 the number of records exposed in registered incidents has reached 904 million[2] and already exceeded by more than 10% the total annual number of records compromised in 2013.

---

[1] Grant Thornton Ireland, *Cybercrime* Report, April 2014 www.grantthornton.ie/db/Attachments/Cybercrime-020414.pdf

[2] http://www.riskbasedsecurity.com/reports/2014-Q3DataBreachQuickView.pdf

In the "2014 Cost of Data Breach Study: Global Analysis" annual report[3], the Ponemon Institute estimates the average total cost of a data breach for organizations in the United States as $5.85 million which implies a $201 loss incurred for every compromised user record.

It is important to note that a significant percentage of all data breach incidents involves insiders – employees and other legitimate users of corporate IT systems. In the same report on the cost of data breaches, the Ponemon Institute has noted that 30% of all data breaches in 2013 were caused by human data handling factors.

The scale and severity of insider data leaks stem from human nature – mistakes, negligence, misconduct, or if users become victims of social engineering attacks. The unpredictable behavior of human beings, which is the root cause of many data leakage scenarios, will never change despite strict corporate regulations, special trainings, administrative sanctions and penalties.

According to the Privacy Rights Clearinghouse[4], among all records compromised in the United States last year, 78% were related to insider incidents.

In the "Data Protection Compliance – 2014 Research Report"[5] based on the analysis of Data Protection Act contraventions in the U.K. from January 2013 to October 2014, IT Governance Ltd has revealed that "employee errors and negligence were the biggest reason for data breaches". 32% of all incidents were due to personal or sensitive data being inappropriately disclosed or sent to the wrong recipient, and 24% of all incidents were due to data or a mobile device being lost.

At the same time, it is trusted employees who create, transform and utilize most information in every organization. As endpoint computers are their main data interaction workspace, Windows PCs complemented recently by the increases in Apple OS Macs, popular "tablets" and other BYOD devices have become critical nodes of IT infrastructure where the largest portion of confidential and sensitive corporate data is created, used and stored. If user access to data and their transfer from endpoint computers are not controlled by the organization, this imminently leads to costly data leaks that are directly *caused* or *triggered* by insiders.

Why DeviceLock?

The growing threat of insider data leaks cannot be neutralized by traditional *network*- and *infrastructure-centric* security solutions because they are not designed to detect and control data flows, data operations and data objects. Neither can they detect the meaningful content of data and enforce protective actions based on its content, value and sensitivity.

In order to prevent data leakage from corporate endpoints, an IT security solution should leverage *data-centric* security mechanisms:

- Primarily, it should move the security focus from the corporate network perimeter down to every computer individually in every possible operating mode – in the office/network, at home or on the road.
- Secondly, it is not enough to control generic user access to the computer, network and applications. The solution should also control data access and transfer operations, as well as leak-prone internal and outgoing data flows on the computer. Implementation of these *contextual* controls over actions with data based on *who, how, where from, where to, when* and similar criteria are as necessary as any other security criteria.
- Finally, to enforce the principle of least privilege in data use permissions, the solution should also inspect and filter the *content* of data transferred, accessed and stored on the computer in order to ultimately decide to allow, block, mitigate, audit, shadow, or alert the particular data transaction at hand.

These exact requirements have become the fundamentals of the endpoint DLP solution developed by DeviceLock.

DeviceLock DLP implements and effectively coordinates a **full-featured set of *contextual* and *content-aware* controls over *data in use*, *data in motion* and *data at rest* that is designed**

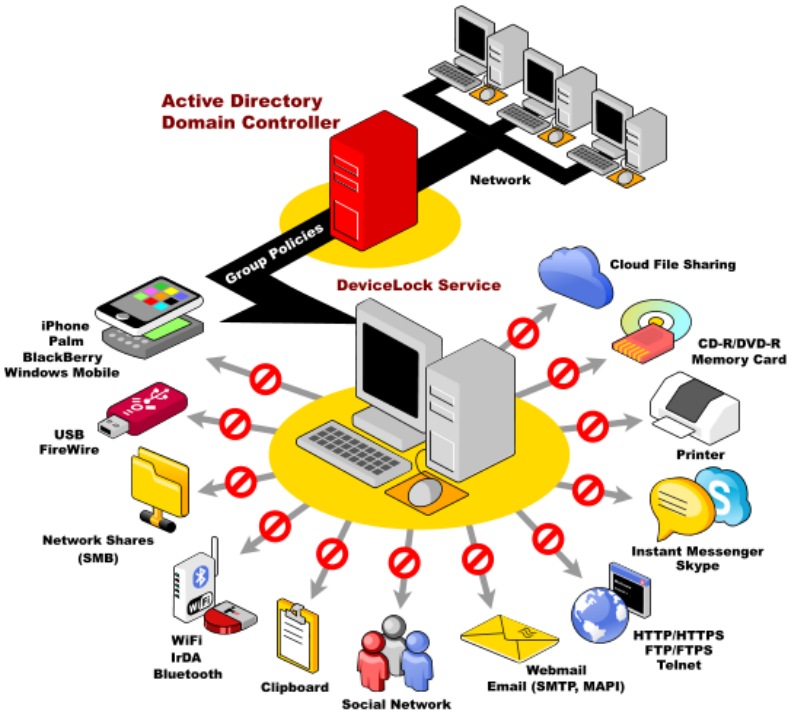
[3] http://public.dhe.ibm.com/common/ssi/ecm/en/sel03027usen/SEL03027USEN.PDF

[4] https://www.privacyrights.org/data-breach

[5] http://www.itgovernance.co.uk/data-protection-compliance-report.aspx

specifically for preventing information leaks from corporate computers *without interrupting normal and approved business processes*.

DeviceLock DLP includes a lightweight enforcement DLP agent that runs on the protected computer or within virtualized OS sessions. DeviceLock is managed via Active Directory Group Policy or more traditional central management consoles for LDAP networks, workgroups, or standalone systems.. Running transparently for end users and applications, the DeviceLock Agent protects endpoint computers against uncontrolled data access and transfer via *local ports, peripherals and channels, as well as via network communications*.



To prevent leakage of "data-at-rest" stored on corporate endpoints and in the network, the DeviceLock Discovery Server and its Discovery Agents scan content of files residing on network shares, storage systems and Windows computers inside and outside of the corporate network to locate documents with exposed sensitive content and process them with automated remediation actions.

The solution is simple, yet scalable and easy to operate due to the deployment, policy management and administration of DeviceLock Agents can be performed from the corporate Microsoft Active Directory via its native configuration feature – Group Policies.

By preventing data leaks from corporate endpoints, DeviceLock DLP helps IT organizations *reduce information security risks and comply with corporate data use policies, state regulations and IT security standards*.

The proven value of DLP solutions in terms of return on investment (ROI) has been independently verified by the Ponemon Institute in their recent "2014 Cost of Cyber Crime Study"[6] based on feedback from 59 large multinational and US companies, who in the past year became victims of cybercrime attacks.

What's So Special about DeviceLock?

DeviceLock DLP benefits are based on its technical differentiators – the capabilities that other DLP products either do not support at all, do not go far enough in depth, or that implement with substantial deficiencies.

[6] http://www8.hp.com/us/en/hp-news/press-release.html?id=1815969

The DeviceLock Agent has the widest set of endpoint contextual controls over local ports, peripheral, virtual and redirected devices, the Windows clipboard -- as well as many popular network applications and protocols -- in the industry.

DeviceLock DLP can be deployed and fully managed from an Active Directory installation without any separate DLP management server or Microsoft application server requiring additional "CALs". In fact, DeviceLock uses Active Directory as its DLP management platform, and without ever changing the schema, scripting, or using clunky workarounds like ADMx profiles.

Going beyond DLP for Windows computers, the DeviceLock provides an endpoint agent for Apple OS "Mac" computers, which supports essential port and device control capabilities that can also be conveniently managed via Group Policies from Microsoft Active Directory. In addition, the DeviceLock Agent for Mac integrates with Apple's FileVault encryption feature in order to only allow users copying data to a removable storage if it is encrypted by FileVault.

DeviceLock offers the most comprehensive and scalable logging subsystem with automatic log collection to a central MSSQL or SQL Express database, content-aware data shadowing and built-in full-text searching.

With DeviceLock, data leaks via the printing channel are prevented by a printer- and application-independent content filtering technology that also enables for all shadow copies of printed documents to be stored as searchable PDF files – regardless of their original formats. It is important to note that DeviceLock enforces controls over the printing of documents *regardless of whether they have already been saved as files* in the file system, which is an ability not supported in competitive DLP products.

For Instant Messaging applications controlled by DeviceLock, not only the content of live chat sessions but also outgoing files are content-inspected and filtered before allowing for their transfer if they follow the data rules.

Control over Skype communications in DeviceLock includes content filtering, logging and shadowing of outgoing chat messages and files, as well as identity-based control of Skype media "phone" calls.

The unique advantages of DeviceLock's endpoint-resident Optical Character Recognition (OCR) features within content rules in comparison with server or gateway-based OCR solutions include its ability to prevent leakage of sensitive data in images via local data channels on the endpoint, as well as from mobile computers when used outside of the corporate network.

Unrestricted employee access to cloud-based file storage/sharing services is considered even more dangerous than uncontrolled use of removable storage devices. With DeviceLock, organizations can inspect and restrict the content of data their employees upload from corporate computers to such popular services as Dropbox, OneDrive (SkyDrive), Google Drive, Amazon S3 and others.

In addition to all above, the DeviceLock Virtual DLP feature delivers content-aware endpoint DLP for BYOD solutions based on remote virtualization platforms, such as Microsoft RDS, Citrix XenDesktop and VMware View. Citrix and VMware have certified DeviceLock DLP as Citrix® Ready and VMware® Ready respectively.

Combined together, DeviceLock DLP technical differentiators, incremental licensing and attractive pricing create its unique value to customers and provide several advantages over the competition:

- With more endpoint data channels and communications protected at contextual and content levels, more leakage scenarios are secured. Simply stated, the DeviceLock Agent has *better preventive DLP controls* than its rivals.
- With DeviceLock, there is *no need to use a separate DLP management platform* – because DeviceLock agents can be centrally deployed and fully managed *natively* via Group Policies from the Microsoft GPMC – a tool familiar to every Microsoft systems and security administrator. As a result, DeviceLock is easier to learn, deploy and maintain than any other DLP solution.
- Thanks to its *native* management integration with Active Directory GPOs, DeviceLock DLP seamlessly *scales from SMB-size deployments up to large enterprises*. Essentially, DeviceLock DLP is as scalable as Microsoft Active Directory.

- Customer investments in DeviceLock products are fully protected, because DeviceLock DLP that supports *incremental functional upgrades from the basic port-device control option up to its full content-aware endpoint DLP Suite*. It is important to note that the additional of modules require neither DeviceLock agent re-installation to endpoints nor any infrastructure modifications in the customer's network.
- And, finally, with its more than 18-year growth history on the international market and customers from sensitive industries, defense and government in 100+ countries, DeviceLock DLP is a *time-proven, award winning and trusted infosecurity product*.

All these benefits make DeviceLock DLP the *best price-performance endpoint DLP solution* that enables organizations of any size and industry to protect corporate computers against insider data leakage while achieving compliance with corporate data protection policies, governmental regulations and industry standards.

Who Needs DeviceLock?

DeviceLock's fast growing customer base includes enterprises that are audited for secure handling of sensitive customer and corporate data, governmental agencies that manage classified information, and professional service firms and other small and medium-size businesses who need to control access to devices and other data egress points.

The following are a few examples of DeviceLock uses:

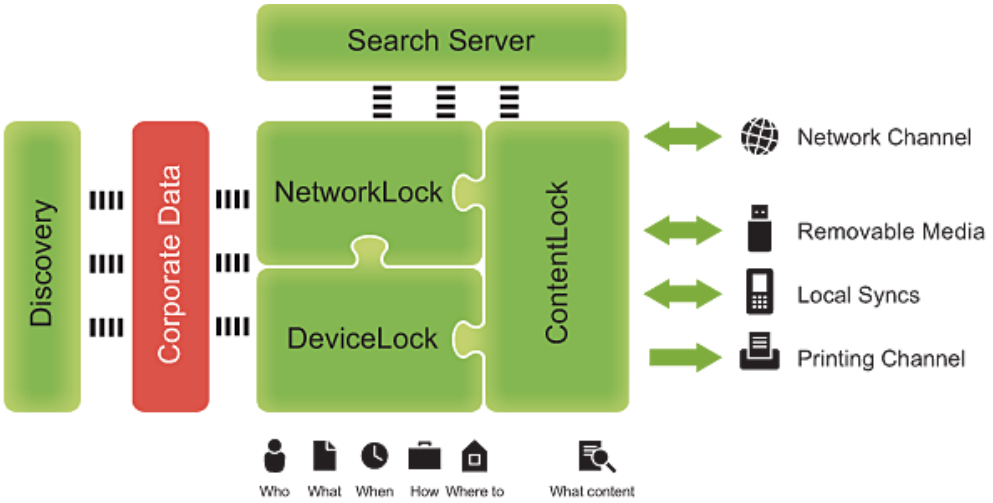
- Control which users or groups can access USB, FireWire, Infrared, COM and LPT ports; Wi-Fi and Bluetooth adapters; the Windows Clipboard; any type of printer, including local, network and virtual printers; Windows Mobile, BlackBerry, iPhone, iPod Touch, iPad and Palm OS-based PDAs and smartphones; DVD/CD-ROMs; floppy drives; and other removable, MTP, Plug-and-Play, and virtually mapped devices.
- Control which users or groups can access network protocols and applications (FTP, HTTP, SMTP, MAPI (Outlook), Telnet, SMB, Instant Messengers, Webmail services and Social Networks).
- Selectively grant or deny access by user and group to use or send information based on verified file types, as well as textual content of data in files or sessions detected by using keywords, document properties, Oracle IRM tags and regular expressions patterns. These and other filter rule types can be combined with Boolean logical operators and numerical thresholds to specify triggering conditions for more precise filter and remediation results. To ease the task of specifying content patterns, the product is shipped with hundreds of pre-built industry- and country-specific keyword dictionaries, as well as RegExp templates for common sensitive information types, such as Social Security Numbers, credit cards, bank accounts, addresses, driver licenses, etc. It is also possible to define custom keyword dictionaries and Regular Expression templates – either from scratch or by modifying those pre-built in the product. The accuracy of content detection is increased by morphological analysis of keywords in eight popular languages.
- Detect and protect confidential data presented in graphical form with a built-in optical character recognition (OCR) engine that extracts and inspects pieces of text in 25+ languages from images in graphical files of more than 30 formats, as well as from pictures embedded in documents, files, archives, emails, instant messages, posts to social networks, screenshots, etc.
- Protect corporate "data at rest" with DeviceLock Discovery that:
    - automatically scans data residing on network shares, storage systems and Windows endpoint computers;
    - locates documents with exposed sensitive content and provides options to protect them with remediation actions;
    - initiates incident management procedures with real-time alerts to Security Information and Event Management (SIEM) systems and/or data security personnel in the organization.
- Control access to devices and protocols depending on the hour of day and day of the week.
- Define which types of data (files, calendars, emails, tasks, notes, etc.) are allowed to synchronize between corporate PCs and personal iOS, Window Mobile, and Palm mobile devices.

- Define different online vs. offline security policies for the same user or group of users.
- Detect removable drives encrypted with Windows BitLocker To Go™, Apple® OS X FileVault, Sophos® SafeGuard Easy®, SecurStar® DriveCrypt® (DCPPE), TrueCrypt®, PGP® Whole Disk Encryption, Infotecs SafeDisk®, Lexar® Media S1100/S3000 and apply special "encrypted" access permissions to them.
- Authorize only specific USB devices that will not be locked regardless of any other settings, and yet still audit and shadow file activities using them.
- Securely grant users temporary access to specific USB devices otherwise blocked by policy when there is no network connection by providing users with two-step access codes over the phone that temporarily unlock access to requested devices for terms of one-time use on up to one month).
- Uniquely identify a specific DVD/BD/CD-ROM disk by its data signature and authorize read-only access to it, even when DeviceLock has otherwise blocked the DVD/BD/CD-ROM optical disk drive.
- Protect against users with local administrator privileges so they can't disable the DeviceLock Service or remove it from their computers, if they are not in the access control list of DeviceLock Administrators.
- Search of text within shadowed files and across audit logs stored in the centralized repository.
- Set devices in read-only mode.
- Protect disks from accidental or intentional formatting.
- Detect and block hardware keyloggers (USB and PS/2).
- Control user access to local ports and peripherals on Mac computers running Apple OS X operating systems including Snow Leopard, Lion, Mountain Lion, Mavericks and Yosemite.
- Flexibly control user communications via popular network applications and protocols with a module that uses a deep packet inspection (DPI) technology locally on the endpoint to detect and filter network traffic regardless of the network ports they use by reconstructing messages and sessions and extracting parameters for to-be-transferred data objects and file attachments. These can trigger specified controls based on verifiable file types, managed IM or Telnet application, protocol and network parameters, as well as whitelisted activities by user-group/sender-recipient identifiers and web resource URLs. In addition, the content of extracted data objects (e.g. files, emails, etc.) can be further inspected by content-aware policy rules.
- Deploy agents, permissions and settings via Group Policy in an Active Directory domain.
- Unify DLP policy management for both Windows and Mac computers in the most simple and scalable way – via Group Policies from the corporate Active Directory by using the DeviceLock snap-in to Microsoft Group Policy Management Console (GPMC).
- Use the standard Windows RSoP snap-in to view the DeviceLock policy currently being applied, as well as to predict what policy would be applied in a given situation.
- Control everything remotely using the admin's choice of centralized DeviceLock management consoles that includes – among others – a web-based console option.
- Get a complete log of peripheral port, device and managed network protocol activity, such as uploads and downloads by users and filenames in the standard Windows Event Log.
- Mirror all data (shadowing) copied to external storage devices (removable, floppy, optical DVD/BD/CD-ROM), Windows Mobile, iPhone, iPod Touch, iPad or Palm OS PDAs and smartphones, transferred via COM and LPT ports, transmitted over managed network protocols and even printed.
- Store shadow data on a centralized component of an existing server and any existing ODBC-compliant MSSQL infrastructure.
- Monitor remote computers in real-time by checking DeviceLock Agent Service status (running or not, version), policy consistency and integrity.
- Generate a report concerning the permissions and settings for selected endpoints.
- Make graphical reports based on the logs (audit and shadow) stored in the central repository.

- Generate a report and/or view displaying the USB, FireWire and PCMCIA Plug-and-Play devices currently connected to computers and those that were historically connected.
- Create a custom MSI package for deploying DeviceLock Agents with predefined policies.

How Does DeviceLock Work?

Functionally, DeviceLock DLP consists of two complementary yet independent software products: DeviceLock Endpoint DLP Suite and DeviceLock Discovery. The products and their modules can be licensed in various bundles to allow customers incremental upgrades from the basic device control solution up to the all-inclusive content-aware endpoint DLP solution.



The fundamental functional component of DeviceLock Endpoint DLP Suite – ***DeviceLock® Core*** – enforces contextual controls over local data channels that include peripheral devices and ports, document printing, synchronizations with locally connected mobile devices (such as smartphones and tablets), screenprints and copy operations via the Windows Clipboard, as well as detects and blocks key loggers on protected computers. This component also includes all necessary central management and administration tools.

A deep packet inspection (DPI) technology is used by another Endpoint Suite's component – ***NetworkLock™*** – to control plain and encrypted user communications via popular network applications and protocols involved with web browsing, email and webmail, instant massaging, social media networking, cloud-based file sharing, FTP file transfers, SMB file shares and even Telnet sessions.

Another functional component – ***ContentLock™*** – performs on-the-fly content inspection and filtering of files and other data objects accessed or attempting to be transferred from the protected computer.

In addition to these preventive components, an optional administrative reporting component – ***DeviceLock Search Server*** (DLSS) – can be used to perform full-text searches in the central audit and shadow log repository. DLSS is aimed at making the otherwise labor-intensive processes of information security auditing, incident investigations and forensic analysis more accurate, convenient and time-efficient.

Bundled in different combinations with each other, DeviceLock Core, NetworkLock, ContentLock and DLSS together implement various functional subsets of the DeviceLock Endpoint DLP Suite.

To prevent leakage of "data-at-rest" stored on corporate endpoints and in the network, a separate content discovery component called ***DeviceLock Discovery*** scans files residing on network shares, storage systems and Windows computers to locate documents with exposed sensitive content and processes them with configurable automatic remediation actions.

The modular architecture and incremental functional licensing make DeviceLock DLP a practical and affordable solution for organizations of any size and budget – from small businesses to large enterprises.

Structurally, DeviceLock DLP consists of the following components:

- *DeviceLock Agent* – an endpoint DLP agent that performs all types of data leak prevention functions on its host computer. These include content inspection, filtering and discovery,; device control; event logging and alerting; as well as data shadowing.
- *DeviceLock Discovery Agent* – a dedicated content discovery software client for scanning local file systems and accessible network shares on Windows computers (desktops, laptops or servers) that are not otherwise protected by full-function DeviceLock Agents.
- *DeviceLock Discovery Server* – a content discovery server that remotely scans and remediates files on network shares and storage systems via the SMB/CIFS protocol, as well as deploys and manages DeviceLock Discovery Agents.
- *DeviceLock management consoles* – Administrative console options include DeviceLock Group Policy Manager snap-in to the Microsoft GPMC, DeviceLock Enterprise Manager, DeviceLock Management Console and the DeviceLock WebConsole. The management consoles are used for access, audit, shadow and alert policy management and administration of DeviceLock DLP components. Customers can choose different consoles depending on the size and type of their corporate network.
- *DeviceLock Enterprise Server* (DLES) – an optional server component for centralized collection and storage of audit and shadow logs aggregated from managed DeviceLock Agents on endpoints. DLES uses Microsoft SQL Server or SQL Express and secure folder structures to store its aggregated audit and shadow data.
- *DeviceLock Search Server* (DLSS) – an optional and separately licensed server component that performs full-text searches in the central audit and shadow log database managed by DLES.

What Types of Computers DeviceLock DLP Protects?

DeviceLock Agents and DeviceLock Discovery Agents protect desktops, laptops and servers that run 32- and 64-bit versions of Windows NT/2000/XP/Vista/7/8/8.1 and Windows Server 2003-2012 R2.

DeviceLock Agent for Mac protects computers running Apple OS X Snow Leopard, Lion, Mountain Lion, Mavericks and Yosemite.

In addition, DeviceLock DLP seamlessly supports various virtualization environments:

- In the mode when DeviceLock Agents run on Windows servers used as hosts for remote Windows sessions or desktop virtualization in Microsoft RDS, Citrix XenDesktop/XenApp and VMware Horizon View platforms, the contextual and content-aware DLP controls of DeviceLock Agents are "remoted" to any kind of connected BYOD devices for preventing data leakage in sessions based on these virtualization platforms. Citrix and VMware have certified DeviceLock DLP as Citrix® Ready and VMware® Ready.
- Any Windows platforms protected by DeviceLock Agents can run as guest OS in local hypervisor-based solutions including VMware Workstation, VMware Player, Oracle VM VirtualBox and Windows Virtual PC.

Who Developed DeviceLock?

DeviceLock's developer is DeviceLock, Inc.

Since its inception in 1996, DeviceLock provides device control and endpoint data leak prevention software solutions to businesses of all sizes and industries. Protecting more than 5 million computers in more than 70,000 organizations worldwide, DeviceLock has a vast range of customers including financial institutions; local, state and federal government agencies; defense contractors; classified military networks; healthcare providers; telecommunications companies and educational institutions. Based in San Ramon, California, DeviceLock, Inc. is an international organization with offices in London (UK), Ratingen (Germany), Milan (Italy), Vancouver (Canada) and Moscow (Russia).

Where Can You Get DeviceLock Software?

A free, fully functional trial demo version is available for download from: www.devicelock.com/dl/download.html.

DeviceLock Technical Support

Technical support is available for DeviceLock customers by sending e-mail to support@devicelock.com. There is a web site that also offers a wealth of support information that includes a Knowledge Base and Frequently Asked Questions: www.devicelock.com/support.html.

You can also contact our technical support team at: +1-925-231-0042. Phone support hours are Monday to Friday, 8am - 5pm PT.

DeviceLock Ordering and Pricing

Customers wishing to purchase fewer than fifty endpoint licenses may purchase online with a credit card.

Customers who require fifty or more endpoint licenses should contact us so that we may provide volume pricing options and/or refer them to an authorized DeviceLock reseller that can provide pricing for both software and services.

Contact Information

DeviceLock Americas

3130 Crow Canyon Place, Suite 215

San Ramon, CA 94583, **USA**

1066 West Hastings Street Ste 2300

Vancouver, BC, V6E 3X2 **Canada**

Email: us.sales@devicelock.com

Toll Free: +1 866 668 5625

Phone: +1 925 231 4400

Fax: +1 925 886 2629

DeviceLock Europe

Halskestr. 21

40880 Ratingen, **Germany**

Phone: +49 2102 131840

Fax: +49 2102 1318429

DeviceLock Italy

Via Falcone 7

20123 Milan, **Italy**

Phone: +39 02 86391432

Fax: +39 02 86391407

DeviceLock Russia

M. Semenovskaya d. 9 st. 9 Office

140, 107023 Moscow, **Russia**

Phone: +7 495 647 9937

DeviceLock U.K.

The 401 Centre, 302 Regent Street

London, W1B 3HH, **UK**

Phone: +44 (0) 800 047 0969

Fax: +44 (0) 207 691 7978

Website

www.devicelock.com