DeviceLock White Paper

Contents:

Why DeviceLock?

Controlling what's being uploaded and downloaded from a company's computer network is basic to IT security. Yet, the job is getting harder every day. The fast-growing popularity of portable USB storage devices is one obvious threat. This market is growing exponentially*, with the devices getting faster, increasing in capacity and shrinking in size by the day. Then consider Bluetooth devices that, to promote ease-of-use, are set to communicate by default with any Bluetooth client within range — and ranges can be surprisingly vast. Likewise, there is a market clamoring for better network access for wireless devices, and this demand is likely to overrule any objections related to security.

In the short-term, the market forces in play are overwhelming security concerns. It's not that corporations don't know about the growing vulnerability. Instances of mal-doers from inside or outside a corporation downloading and extracting sensitive information for purposes that range from competitive business intelligence to extortion to terrorism receive frequent media attention. Also, it's not that corporations aren't doing anything about security. Investment in firewalls, encryption, and other technologies and controls designed to protect network data from theft across the Internet is certainly on the rise. However, these measures offer little protection from locally unsecured devices and ports. They won't stop the employee spy who brings a 2GB keychain drive to work, plugs it into the USB port, and begins to download sensitive data. Nor will they impede the disgruntled employee who uses a similar device to upload a Trojan or other malicious program into the network. To stem these problems, it's necessary for administrators to have control over who has access to external media drives and when they have access.

DeviceLock from DeviceLock, Inc. provides this level of control over Microsoft Windows-based networks. It is a software-only solution that allows network administrators to assign permission for USB and FireWire ports, for WiFi and Bluetooth adapters, as well as for floppy drives, CD-ROM drives, tape devices and other removable media. It solves such physical security problems without physical locks.

NetworkLock, an extension to DeviceLock, provides control over network communications. Administrators can designate user access to the FTP, HTTP, SMTP, Telnet protocols, instant messengers (ICQ/AOL Instant Messenger, Windows Live Messenger and Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), webmail and social networking applications

* From about 10 million units shipped in 2002, the number of USB Flash Drive units expected to be shipped in 2006 will have climbed to nearly 50 million units, per a Semico Research Corp study, "Will USB Flash Drives Change Our Lives?"

(Gmail, Yahoo! Mail, Hotmail; Facebook, Myspace, LinkedIn, LiveJournal, Odnoklassniki, Vkontakte, Twitter).

ContentLock, another extension to DeviceLock, extracts and filters the content of data copied to removable drives and plug-n-play storage devices, as well as that transmitted over the network. Administrators can create rules that specify which content can be copied and transmitted.

What's so special about DeviceLock?

By providing network control over which users can access ports and devices on a local computer, DeviceLock closes a potentially huge security hole in a simple, cost-effective manner. So, it's a big improvement over doing nothing. Compared to physical solutions requiring the storage and management of hardware locks and keys, it's much cheaper and easier to implement across an enterprise. Compared to other administrator-enforced, software-only ways to control local hardware (such as changing the BIOS) DeviceLock is a more elegant, easier to scale solution.

DeviceLock features a clean and simple-to-use user interface with easy setup wizards and multiple graphical views of the information. Network administrator can even set up and maintain DeviceLock on workstations remotely. Designed to run under Windows NT/2000/XP/Vista/7 and Windows Server 2003/2008, it also provides automated support for Install and Uninstall.

DeviceLock also can be managed and deployed via Group Policy in an Active Directory domain. Group Policy uses directory services and security group membership to provide flexibility and support extensive configuration information. Policy settings are created using the Microsoft Management Console (MMC) snap-in for Group Policy. Tighter integration into the Active Directory makes DeviceLock's permissions management and deployment easier for large networks and more convenient for system administrators. Integration into the Active Directory eliminates the need to install more third-party applications for centralized management and deployment. DeviceLock does not need to have its own server-based version to control the entire network, instead it uses standard functions provided by the Active Directory.

For enterprises standardized on software and hardware-based encryption solutions like PGP Whole Disk Encryption, TrueCrypt, Windows BitLocker To Go, DriveCrypt and Lexar JumpDrive SAFE S3000 and SAFE PSD S1100 USB drives, DeviceLock allows administrators to centrally define and remotely control the encryption policies their employees must follow when using removable devices for storing and retrieving corporate data. For example, certain employees or their groups can be allowed to write to and read from only specifically encrypted USB flash drives, while other users of the corporate network can be permitted to "read only" from non-encrypted removable storage devices but not write to them.

In addition to protecting network and local computers against data theft and network corruption, DeviceLock allows you to get a complete log of port, device and network activity.

The DeviceLock's optional data shadowing capability significantly enhances the corporate IT auditor's ability to ensure that sensitive information has not left the premises. It captures full copies of files that are copied to authorized removable devices and Windows Mobile PDAs/smartphones, burned to CD/DVD, transmitted over the network or printed by authorized end users. Shadow copies are stored on a centralized component of an existing server and any existing ODBC-compliant SQL infrastructure of the customer's choosing.

DeviceLock Search Server provides full-text searching of logged data stored on DeviceLock Enterprise Server. The full-text search functionality is especially useful in situations when the corporate IT auditor needs to search for shadow copies of documents based on their contents. DeviceLock Search Server can automatically recognize, index, search and display documents in many formats, such as: Adobe Acrobat (PDF), Ami Pro, Archives (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works,

OpenOffice (documents, spreadsheets and presentations), Quattro Pro, WordPerfect, WordStar and many others.

Who needs DeviceLock?

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

The following are a few examples of DeviceLock uses:

- Control which users or groups can access USB, FireWire, Infrared, COM and LPT ports; WiFi 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; as well as DVD/CD-ROMs, floppy drives, and other removable and Plug-and-Play devices.

- Control which users or groups can access network protocols and applications (FTP, HTTP, SMTP, Telnet, Instant Messengers, Webmail services and Social Networks).

- Selectively grant or deny access to information based on real file types, regular expressions patterns with numerical conditions and Boolean combinations of matching criteria and keywords.

- Separately control access to images that contain text (for example, scanned documents, screen shots of documents) and images that do not contain text.

- Control access to devices and protocols depending on the time 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 mobile devices.

- Define different online vs. offline security policies for the same user or set of users.

- Detect encrypted PGP, DriveCrypt and TrueCrypt disks (USB Flash Drives and other removable media), Lexar SAFE PSD- and Lexar JumpDrive SAFE S3000-encrypted flash drives as well as BitLocker To Go-encrypted drives and apply special "encrypted" permissions to them.

- Authorize only specific USB devices that will not be locked regardless of any other settings.

- Grant users temporary access to USB devices when there is no network connection (you provide users with the special access codes over the phone that temporarily unlock access to requested devices).

- Uniquely identify a specific DVD/CD-ROM disk by the data signature and authorize access to it, even when DeviceLock has otherwise blocked the DVD/CD-ROM drive.

- Protect against users with local administrator privileges so they can't disable DeviceLock Service or remove it from their computers, if they are not in the list of DeviceLock administrators.

- Search of text across shadowed files and audit logs stored in the centralized database.

- Set devices in read-only mode.

- Protect disks from accidental or intentional formatting.
- Detect and block hardware keyloggers (USB and PS/2).
- Deploy permissions and settings via Group Policy in an Active Directory domain.
- 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 centralized management console.
- Get a complete log of port, device and network 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, DVD/CD-ROM), Windows Mobile, iPhone, iPod Touch, iPad or Palm OS PDAs and smartphones, transferred via COM and LPT ports, transmitted over the network and even printed.
- Store shadow data on a centralized component of an existing server and any existing ODBC-compliant SQL infrastructure.
- Monitor remote computers in real-time, checking DeviceLock Service status (running or not), policy consistency and integrity.
- Generate a report concerning the permissions and settings that have been set.
- Make graphical reports based on the logs (audit and shadow) stored on the server.
- Generate a report displaying the USB, FireWire and PCMCIA devices currently connected to computers and those that were connected.
- Create a custom MSI package for DeviceLock Service with predefined policies.

How does DeviceLock work?

DeviceLock works on any computer using Windows NT 4.0/2000/XP/Vista/7 or Windows Server 2003/2008. It supports 32-bit and 64-bit platforms.

DeviceLock consists of three parts: the agent, the server and the management console:

1. DeviceLock Service (the agent) is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device and network protection on the client machine while remaining invisible to that computer's local users.

2. DeviceLock Enterprise Server is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data.

   DeviceLock Content Security Server is also the optional component which includes DeviceLock Search Server for instant search of text across shadowed files and other logs stored on DeviceLock Enterprise Server.

3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock

Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor).

Who developed DeviceLock?

DeviceLock's developer is DeviceLock, Inc. Since its inception in 1996, DeviceLock, Inc. (formerly SmartLine Inc) has been providing information security and network management solutions to organizations that rely on Microsoft Windows technologies. DeviceLock's proven expertise with access control technologies helps customers improve security, productivity and system availability. IT professionals choose DeviceLock, Inc. solutions to administer, audit and protect these critical systems. The company's customers include BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, and various state and federal government agencies and departments. DeviceLock, Inc. is an international organization with offices in San Ramon (California), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).

Where can you get DeviceLock software?

A free, fully functional demo 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 including known issues 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 pricing

DeviceLock costs € 40 (Euro) for a basic single-user license. Discounts are available for multi-user licenses and for Educational Institutions. For multi-user pricing see:
http://www.devicelock.com/dl/register.html.

If you want to use the capabilities of NetworkLock and ContentLock, you must purchase NetworkLock and ContentLock licenses in addition to basic DeviceLock licenses.

Ordering and registration methods

There are several ordering / registration methods available for DeviceLock:

On the World Wide Web using secured web site (by credit card)
By Phone (by credit card)
By Fax (by credit card)
By Mail (by check)
By Purchase Orders

For more information on how to order see: http://www.devicelock.com/dl/register.html.

Contact information

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germany
TEL: +49 (2102) 89211-0
FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milan, Italy
TEL: +39-02-86391432
FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, UK
TEL (toll-free): +44-(0)-800-047-0969
FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA
TEL (toll-free): +1-866-668-5625
FAX: +1-646-349-2996

sales@devicelock.com
support@devicelock.com

www.devicelock.com