



Securing Data at the Endpoint

Four Steps to Protect Your Enterprise from Data Leakage

Thursday, March 20, 2008

www.lumension.com



Introduction

The workplace is changing as we speak as security has virtually disappeared from the traditional enterprise IT landscape. With new technologies such as inexpensive storage devices and removable media disseminating information further and further away from the core, as well as an influx of spyware, phishing programs and keyloggers, enterprises' data security is constantly under attack.

In this seemingly chaotic environment, data security has become one of the primary challenges facing all organizations. From its existence as ones and zeroes on disks to its aggregation as useful knowledge, managers must increasingly consider data throughout its lifecycle. Not to mention the numerous industry and federal mandates calling for increased data confidentiality and protection. Indeed, safeguarding your organization's most valuable assets – its data – is more critical than ever.

IT managers have good reasons to worry. A recent spate of data thefts and security breaches has created the potential for a huge amount of personal and sensitive data to become compromised:

- ▣ A disgruntled Boeing employee used his internal access rights to download 320,000 sensitive files, transfer them to a thumb drive and remove them from company property.
- ▣ A Fidelity National Information Services, Inc. senior database administrator sold the personal information of 8.5 million consumers to a data broker. The Veteran's Affairs Department reported the May 2006 theft of a laptop and external drive containing information for more than 26.5 million veterans and active-duty troops. The VA has also reported two other cases in Minneapolis
- ▣ Thumb drives containing information on US soldiers and secret informants have been sold by Afghan teenagers for \$40 apiece.
- ▣ McDonald's Japan was forced to recall up to 10,000 MP3 players it gave away as a promotion after discovering that the devices carried a nasty spyware Trojan.



- ▣ Wilcox Memorial Hospital warned more than 130,000 former and current patients about the disappearance of a USB thumb data drive containing personal information. The information could be read with Adobe Acrobat Reader and was not encrypted to limit access.
- ▣ 53% of respondents to a study by the Ponemon Institute indicated that they would never be able to determine what information was lost on a USB memory stick.

These instances of thefts and spyware infiltrations have enterprises looking long and hard at any number of potential holes in existing security nets for data leakage. And the unfortunate truth is that they are looking squarely in the mirror at themselves and their own employees. According to a variety of sources, the most significant security breaches come from insiders – both from malicious and seemingly benign activities. And now, with a barrage of new, portable storage technologies, it's never been easier for information to literally walk out the door on an iPod®, storage device, digital camera, CD/DVD, etc. Merely browsing the Internet can potentially expose your computer – and your data – to spyware and keyloggers, which can execute on your machine without your knowledge.

Today's Fluid Workforce

Never before have there been so many mobile workers. In the United States alone, more than 44 million were classified as teleworkers (Dieringer Research Group) and more than 100 million teleworkers are expected by 2010 (WorldatWork's Telework Trendlines 2007).

Since personal networks are less secure than a controlled enterprise network, laptops and other portable devices are potentially exposed to more security holes. As a result, such a significant level of movement within our workforce - contractors, employees, and partners, means making sure that information stays within the confines of the organization is a major concern.

But today's workforce isn't just becoming more mobile – it's becoming more efficient. As technologies evolve with faster processors and huge storage capacities, workers are able to quickly share and disseminate large amounts of data, allowing for increased efficiency – and increased risk of data leakage.



As a result of workers' becoming increasingly mobile, as well as needing to quickly share and disseminate data, laptops and computers are becoming more personal, loaded with non-business applications. Personal entertainment devices are typically purposed to playing music or displaying pictures, utilizing copyright controls to manage the files on them. They pose added issues of not only appropriate use, but also expose your organization to the potential for spyware and keyloggers to infiltrate the network.

Does your company or agency govern the use of personal entertainment devices, including access to network sites to share music or pictures? Sites like iTunes, MySpace, and personal photo sharing sites not only represent a significant amount of overall network traffic, but could be latent gateways to spyware and keyloggers – all threats to your agency's valuable data.



The Technologies Behind Today's Workforce

Technology has supported our need for mobility and has also provided additional means of communication. Removable storage media is at the center of a variety of new ways we can share and use information. There are many new form factors for removable media today: the small cards used in PDAs and cameras; thumb drives used to move files between PCs; and personal entertainment devices, such as iPods, which may have as much as 160 Gigabytes of storage capacity.

Devices as Entry Point for Spyware

1. McDonald's Japan recalled MP3 players it offered as a prize, after discovering that the prizes were loaded with a particularly nasty strain of malware. Up to 10,000 people might have been exposed to the QQpass spyware Trojan after claiming a Flash MP3 player.

2. One company conducted a "Social Engineering" experiment, in which 20 USB devices (preloaded with a Trojan that would collect passwords and then email the data to the program's creator) were planted around office buildings waiting for the unsuspecting pawns. Fifteen of these sticks were plugged into corporate machines, and ultimately compromised the individual and organization's security

Only a few years ago, a thumb drive with 128 Megabytes of storage capacity would have cost over \$100. That same stick costs less than \$20 today. Conservative estimates predict that the cost of removable storage will drop 50% in price year-to-year and recent Gartner studies suggest a greater price drop should be expected. Removable devices can take on forms like pens and wristwatches, making it impossible to attempt to control their use by "search and seizure." You would be hard-pressed to find someone that does not own at least a couple different types of removable media today.

Most personal media devices can be connected to a PC via USB or firewire connections. Today's PCs sport as many USB ports as there are

cupholders in a mini-van, so there's no problem finding an available port. Microsoft Windows® makes it simple to use these devices. Plug and play means that these devices can simply be plugged in - Windows will do the rest by automatically detecting them and installing the right drivers for their use. Today, with transfer rates up to 480 megabits per second, it takes less than



five minutes to move up to 60 Gigabytes of data. An entire PC can be copied to a removable media device and carried away in a matter of minutes.

The new breed of smart U3 USB devices which not only store large amounts of data, but also include self-launching and self-running applications, expose data to threats at both the device and application levels – all in one fell swoop.

However, an enterprise's data is not at risk only because of removable or portable devices. An emerging version of data theft tools are designed specifically to run on U3 devices. These Trojans are designed so that simply inserting the U3 into a USB port will automatically activate Trojans which then copy and remove sensitive information from a network within minutes. These smarter attacks have placed sensitive data at further risk and have made execution control a critical component to any organization's IT security policy.

Wave of New Policies and Penalties for Regulatory Compliance

Say the terms SOX, HIPAA, DPA, BS 7799, ISO 1779, FISMA and M-06-16 Mandate, and nearly everyone in the corporate and government space will recognize them as regulations governing the management of personal information. Many can even articulate what corporate responsibilities are with regard to protecting privacy. At a high level it's simple: provide assurance that an employee's or organization's information is always protected from compromise, used on a need-to-know basis only, and that provenance can be provided to show how and by whom it was used. Unfortunately, few know precisely what they need to do or how to demonstrate compliance with these regulations, while users run unauthorized software, remove data from organizational networks – when they travel or work at home – and download infected or inappropriate files, which can expose vulnerabilities that enable the theft or loss of critical information.

These regulations boil down to the need for acceptable use policies and a means of enforcing and reporting on them. Today's typical IT department has policies in place that govern the use of information: where and how it may be accessed, how it must be handled to protect its confidentiality. This is a major 'first step' - defining acceptable use, including the employees' responsibilities for compliance. Most organizations take this step and the second one: gaining



management's support behind it, and communicating this policy to the employees. Many organizations stop here, resulting in an un-enforced information use policy. Without enforcement, a security policy only has teeth when a blatant violation occurs. It can do little to stem the constant leakage of data that moves silently in and out of the agency.

So why not simply ban the use of portable devices and certain applications altogether? Suppose you prohibit the use of removable media of any sort within your enterprise? Violations can be dealt with on the spot. Some organizations do have that sort of policy in place, but it is like trying to stem the tide of progress. It is also just shy of having no policy at all - unenforceability is the death of many security policies.

To enforce a complete ban, you would have to eventually ban cell phones, eBooks, and the variety of form factors that we can anticipate removable media will take on in the near future. You would have to enforce a complete ban on certain applications as well. What would make more sense is to determine an acceptable use policy for these devices and applications. Determine how they may be used securely, and make them work for you rather than against. While you cannot control the next wave of technology or the next threat, you can control user behavior.

Device and Application Control in the Enterprise

This is the case for device and application control -- determining what devices and applications can be used, by whom, when, and how. Governing their use is far more practical than attempting to prohibit what amounts to a major IT evolution in how we handle data individually. We can make personal devices extensions of the organization which enable users to choose how they work and share data. If information must be encrypted at all times in a steady state, this can be done with nearly all forms of removable media. Some encryption mechanisms can tie individual users directly to the data and/or to the media itself, preventing anyone else from using it. When this type of device management is paired with application control, you're not only securing the device itself, but you're also preventing those devices from launching dangerous executables, which may endanger your data.

Encryption in conjunction with enforcement can also provide proof of provenance. If you can track who had confidential data, how they used it, and were assured that they could not share it outside of the enterprise, then that fulfills the need for a comprehensive audit trail required by some of the regulations mentioned previously.



Steps to Implementing Effective Device and Application Control

Device and Application Control provide ways to develop and enforce a granular use policy for how software applications, removable media, or any device that can be accessed from an end user's PC, can be used. There are a few important steps to take in implementing a strong usage policy. Developing and enforcing a device and application use policy must be done in a non-disruptive fashion, minimizing any adverse impact of going from a non-controlled to a controlled use environment.

Step 1: Discover - Know Your Users

The first step involves identifying all devices and applications in use, or available to, users in your organization. In addition, you will need to determine whether all end users will have the same rights - are there levels of confidentiality or other organizational groupings that will govern who should be able to transport information and how they will be allowed to do so? Many enterprises use identity management to generate and distribute credentials to end users, and to associate access privileges with their credentials. If this information is already in place, then the majority of work required in developing a device or application use policy is complete. If not in place, policy groups may be developed in a number of ways with a variety of different tools.

Step 2: Develop - Determine Acceptable Device and Application Use

The next step entails identifying all the potential devices and applications that will be approved for use. For example, it might make sense to enable all removable media, but for 'read' access only, enabling employees to bring in data, but not remove it from the enterprise. It might make more sense to require some encryption and authentication. It might also make sense to allow only certain groups to install Instant Messaging or Peer-to-Peer software. A sensible approach would be to scan for all devices and applications and monitor their use over a period of time to determine what policies should be developed.

Step 3: Deploy and Enforce - Pull the Trigger

Once acceptable devices and applications and their use rules are identified and associated with user groups, management buy-in is essential to succeed. When that is obtained, it is time to let enterprise end users know what to expect. Communications are extremely important to prevent disruption and rebellion. If end users know what to expect and have time to anticipate the change,



there is far more likelihood for minimal impact on end users and infrastructure alike. Once policies are developed, tuned and communicated, ensure that they are more than just a piece of paper - they must be enforceable.

Step 4: Audit - Prove Policy Compliance

The final step is to demonstrate policy compliance through comprehensive auditing and reporting. The ability to drill down on suspicious user behavior enables the organization to follow up on the matter and take appropriate actions. Being able to audit user behavior also proves effectiveness or lack thereof with the policies in place.



Lumension's Sanctuary[®]

Lumension's Sanctuary provides policy-based application and device control that proactively secures your organization from data threats, including data leakage, malware and spyware. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to be accessible on an endpoint – facilitating security and systems management, while providing necessary flexibility to the organization.


Sanctuary is comprised of two modules to secure your endpoints:

 **Sanctuary Application Control**

Provides policy-based enforcement of application use to secure endpoints from malware, spyware and unwanted or unlicensed software.

 **Sanctuary Device Control**

Provides policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints.

 Sanctuary validates applications and removable devices as they are used within an enterprise. Applications or devices that are not authorized are simply not allowed to execute. Through a central console, application and device control policies are quickly established and enforced through two simple steps: Identification and Assignment. Since Sanctuary works with devices and applications, it enables agencies to develop granular use policies - working with the devices and applications rather than simply enabling or disabling them. Sanctuary policies are managed per user or user group as well as per computer. For devices, policies are enforced by time constraints, encryption, volume of data, data transfer and much more criteria. Linking application and device policies to user and user-group information stored in Microsoft[®] Windows[®] Active Directory[™] or Novell eDirectory[™], Sanctuary enables the immediate association of user groups to devices and applications on the fly - dramatically simplifying the management of endpoint application and device resources.

Sanctuary can also encrypt removable media so that it can be safely used and transported without the fear of exposing your confidential data to unauthorized users. Users can have access to their encrypted data even in computers that do not have Sanctuary client software installed. Centralized and decentralized encryption schemas provide the Sanctuary administrator with the




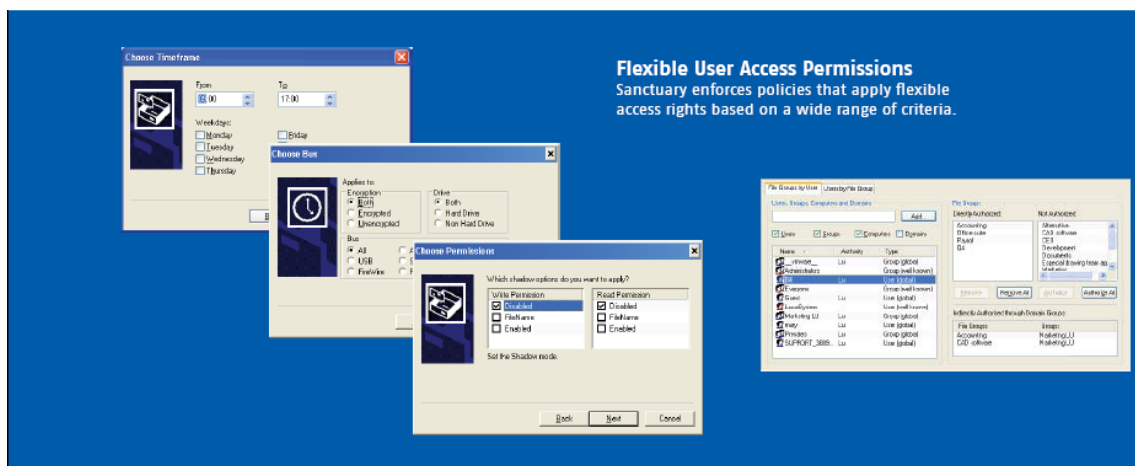
flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and, more importantly, enforce the use of that encrypted media.

Providing the ultimate flexibility, Sanctuary enables administrators to allow trusted users to authorize their own applications. This option provides the best of both worlds - flexibility to users and control for administrators through notifications of activity. Auditing and reporting enable systems administrators to precisely track how devices and applications are used, by whom and how. They can also see when un-authorized device and application usage are attempted and track that as well.

Sanctuary combines the proven capabilities of its application and device control modules, providing organizations with the most comprehensive solution for endpoint security management – all from one console. Sanctuary removes the risk of data leakage, malware and spyware, improves IT security and network bandwidth, reduces the effort and cost associated with supporting endpoint technologies and assures regulatory compliance.

Sanctuary:

-  Prevents data leakage via removable media, malware or spyware
-  Protects against malware, viruses and spyware
-  Safeguards against zero-day threats
-  Controls proliferation of unwanted applications and devices
-  Assures and proves compliance with regulations governing privacy and accountability
-  Maximizes benefits of new technologies and minimizes risk



Flexible User Access Permissions
Sanctuary enforces policies that apply flexible access rights based on a wide range of criteria.

Name	Activity	Type
Admins	Loc	Group (Self Admin)
Administrators	Loc	Group (Self Admin)
Everyone	Loc	Group (Self Admin)
LocalSystem	Loc	Low (Self Admin)
LocalSystem	Loc	Low (Self Admin)
Network	Loc	Group (Self Admin)
Users	Loc	Group (Self Admin)
SUPPORT_385	Loc	Low (Self Admin)



Sanctuary Technical Specifications[®]

Common features

Feature	Function	Benefit
Whitelist	Assign permissions for authorized devices and applications to users or user groups, and by default those not authorized are not allowed	Eliminates unknown or unwanted devices and applications in your network, reducing the risk of data leakage and malware and ultimately improving network stability
Integrated Sanctuary Suite Console	Single management console for centralized configuration and management of application and device usage policies	Simplifies application and device management with extensive logging and reporting of connected devices, files and applications
Custom Access Denied Notifications	Customizable messages displayed to end user signaling access denied	Communicates organization-specific instructions, such as providing Help Desk contact information
Multi-Language Support	Supports 12 languages on Sanctuary client machines	Improves end user experience in international organizations
Offline Permission Updates	Export of permissions to a file for import into offline computers	Enables updating of offline client systems with current Sanctuary permissions
Unified Log Management and Reporting	Sanctuary Device Control and Application Control logs are stored and displayed in a common format	Delivers more powerful forensic analysis by identifying the relationship between device, application usage and shadowed files
Flexible Log Queries	Enables administrator to search logs and sort results; Multiple entries can be	Provides powerful log analysis enabling quick drill down to a specific issue



Feature	Function	Benefit
	stacked together to condense information	
Stored Log Query Templates	Pre-defined templates available; Configuration of any log query can be saved	Provides fast and easy review of logs on a regular basis
Log File Export	Displayed log entries can be saved in a CSV file format	Provides flexibility to review and analyze logs in any CSV compliant application
File Compression	Files are sent in a compressed format from the client to the server, from the server to the client and from the server to the console, and Shadowed files are compressed for storage	Optimizes network bandwidth and increases efficiency, taking less storage space, as well as providing faster file retrieval from remote servers
Disconnected/Remote Computer Protected	Enables constant protection by keeping a local copy of the last list of hashes and permissions on the disconnected machine	Secures computer regardless of network connection, ensuring that remote or disconnected users are also protected
Decentralized Files Storage	Shadow files, scans and log files are stored with each Sanctuary Application Server, maintaining central access from the management console	Reduces the bandwidth required to transmit and store files in large or complex enterprises
Active Directory and eDirectory Support	Leverages user and user group definitions in existing Microsoft Active Directory and Novell eDirectory	Eliminates duplicated effort of defining users /user groups for access control lists, reducing setup and ongoing maintenance
Highly Scalable Architecture	Three tier architecture with Database, one or more Application servers, and Client	Provides flexible and scalable deployment options in large and complex networks



Feature	Function	Benefit
Silent Unattended Installations	Install with any deployment tools which use MSI Setup (e.g. Microsoft Systems Management Server (SMS), Group Policies, WinInstall, etc.)	Enables faster and easier deployment
Audit of Administrator Actions	Full auditing and reporting of all Administrator actions	Demonstrates regulatory compliance ensuring configuration remains intact and identify potential abuse or training needs
Differential Updates	Sanctuary Application Server sends smaller delta file updates to the clients for Sanctuary Application Control file signatures and all Sanctuary permissions	Optimizes performance on a highly decentralized network and/or working with a slower network connection
Automated Permission Updates	New permissions are updated at logon, every hour and upon network connection status change; Application file signatures updated at each logon	Automates policy updates requiring no user intervention, ensuring that users are working with latest policies
Push Changes to Permissions	Permission changes for applications or devices can be pushed to one or many users	Implements new policies regarding applications or devices immediately – no reliance on reboot or restart of network connection

Sanctuary Device Control Name Feature Description

Feature	Function	Benefit
Access Control List Based	Assign permissions to a user/user group based on their	Provides granular user permissions that remain with



Permissions	Active Directory or eDirectory identity	user login regardless of machine
Granular Device Control Permission Settings	Permission settings include read/write, scheduled access, temporary access, online/offline, I/O bus type, HDD/non-HDD devices and much more	Eliminates risk of unauthorized devices connecting to the network while providing the flexibility users need to conduct business
Uniquely Identify and Authorize Specific Media	Authorize DVD/CD-ROM collections, grant access to users or user groups and encrypt removable media with unique ID's	Limits DVD/CD-ROM access to company standard discs, to avoid use of unauthorized content and/or encrypt removable media to prevent the content from being viewed by unauthorized users
Plug and Play Devices: Hot Plug Support	Detect Plug and Play Devices "on the fly"	Ensures user productivity is not disrupted by applying permissions for plug and play devices when detected
Bi-Directional Shadowing Option	Patented Shadowing technology records data that is read from and/or written to a removable device	Captures the flow of information into and out of your network, reducing risk and containing impact of data leakage
Restrict the Amount of Data Copied	Restrict the daily amount of data copied from an endpoint to a device on a per-user basis	Removes risk of large pieces of confidential information leaving the network
Prevention of PS/2 and USB Hardware Keyloggers	Block PS/2 port; Enforce the usage of USB keyboards and detect/block popular models of USB keyloggers	Reduces risk of attackers capturing passwords and other confidential information through keyloggers
Flexible Encryption Options for Removable Media	Administrators may centrally encrypt removable media or force users to encrypt media at time of use	Ensures that sensitive data is not inadvertently exposed to those without authorized access



File Type Filtering	Control the type of files that are moved to and from removable devices	Reduces risk of unwanted files from entering and sensitive files from leaving the network
---------------------	--	---

Sanctuary Application Control

Feature	Function	Benefit
Standard File Definitions	A classified, pre-loaded whitelist of all supported OS files	Speeds and simplifies whitelist definition
Automated Application Discovery	Process of identifying, categorizing and authorizing applications which produces a record of all executables on client computers, file servers and/or local directories	Provides flexible and fast options to create or update whitelists
Automatic Authorization of Software Updates	Automatic authorization of Microsoft software updates through integration with Windows Updates: SUS and WSUS	Eliminates risk of accidentally restricting user access to frequently updated Microsoft applications
Script / Macro Protection	Controls the execution of VBScript, Microsoft Office VBA and JavaScript with central authorization or a prompt to local users	Extends application policy enforcement to include scripts/macros for even greater protection
Path Protection	Optional file authorization based on location or path rules; Create a Trusted Owner, such as administrator, to reinforce security	Provides flexibility to support executable files for which hash definitions are not useful or applicable (i.e. auto-changing .exe files)
Non-Blocking Mode	Execute and log activity for administrator review	Enables Sanctuary to identify current state before defining and enforcing policy
Flexible File Authorization	Versatile File Processor (FileTool.exe) enables directory	Provides flexible and fast option to identify new and updated



Feature	Function	Benefit
	and subdirectory scans to discover new applications and packages while online or offline	applications for review and ultimately to generate whitelists
Nested Executable File Groups	Hierarchical structure of organizing file groups	Provides fast administration of file groups and assignment of user permissions
Relaxed Logon	Executes logon scripts without authorization and automatically switches system into blocking mode after either a set of time or at the end of the script	Eliminates need to administer logon scripts in Sanctuary without compromising the security of the system
Local Authorization	Trusted users can authorize applications locally, maintaining an audit log for administrator review	Delivers the ultimate in flexibility to the user, without giving up administrative control
Spread Check	Disables suspicious executables that are locally authorized on too many computers	Contains risk of malicious code spreading through network due to local authorization



About Lumension Security

Lumension Security, formed by the combination of PatchLink[®] Corporation and SecureWave[®] S.A., is a recognized, global security management company, providing unified protection and control of all enterprise endpoints to more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Positive Security model, Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes automated asset discovery, vulnerability assessment, remediation and validation; application and device control; integration with leading network access control solutions; and extensive policy compliance reporting. Headquartered in Scottsdale, Arizona Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore.

©2008 Lumension Security. All rights reserved. Lumension Security, the Lumension logo, PatchLink[®] and Sanctuary[®] are trademarks or registered trademarks of Lumension Security. All other trademarks are the property of their respective owners.



Lumension Security

15880 N. Greenway-Hayden Loop, Suite 100

Scottsdale, AZ 85260

www.lumension.com