

Sanctuary® Device Control



Complete Control of all Removable Media, Endpoint Devices and Port Access

Sanctuary® Device Control, a component of Sanctuary, provides policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints. By employing a whitelist approach, Sanctuary Device Control enables only authorized devices to connect to a network, laptop, thin client or desktop. Unauthorized device access is prohibited by default.

If the device is known, the Device Control driver checks the user rights in the Access Control List (ACL). If a user has access rights to a device, either Read or Read/Write access is granted. If a user does not have access rights to the device, a customizable "Access Denied" notification alerts the user.

Simple, Fast, Flexible Administration and Management

Sanctuary Device Control enables the administrator to rapidly identify devices and then assign permissions by device class, specific device or specific media to user(s) / user group(s) or to a specific computer. Administration of device control access rights is accomplished centrally through a simple "tree-style" interface.

Device policies are linked to user and user-group information stored in Active Directory™ or eDirectory™, dramatically simplifying the management of endpoint device resources.

Detailed Audit Capabilities

Lumension Security patented shadowing I/O bi-directional technology records filename or file content as it is read from or written to floppy, CD/DVD and removable devices. All device access attempts can be logged, as well as any administrator actions, including changes of any devices' access rights.

Enforced Encryption

Portable devices can be encrypted for safe use and transported without the fear of exposing your confidential data to unauthorized users. Users can access their encrypted data even on computers that do not have Sanctuary installed.

Centralized and decentralized encryption schemas provide the flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and enforce the use of that encrypted media.

Also available, Sanctuary Application Control with integrated Sanctuary management console. Sanctuary Application Control provides policy-based enforcement of application use to secure endpoints from malware, spyware, zero-day threats and unwanted or unlicensed software.

Sources:

1. Yankee Group 2005, ESG 2005, Forrester 2005
2. 2006 CSI/FBI Computer Crime and Security Survey
3. Ponemon Institute's 2006 Cost of Data Breach Study

Reduce Risk of Data Leakage

Enterprises today are constantly challenged with data leakage caused by removable media and the resulting regulatory compliance issues which dominate enterprise IT's 'Top Ten Concerns' lists¹. Seventy-five percent of Fortune 1000 companies fell victim to accidental and/or malicious data leakage², with the average cost of recovering lost/stolen corporate data at \$5 million, a 30% increase since 2005³.

Unmanaged removable media can easily open the floodgates for data to escape into the wrong hands, whether intentionally or accidentally. Furthermore, regulations governing privacy and internal controls require the control of inbound and outbound data flow. Sanctuary provides the necessary controls to manage the data flowing to and from network endpoints and audits the use of devices to prove compliance with internal policies or government regulations.

Supported Device Types

- | | |
|-------------------|------------------------|
| USB Memory Sticks | Wireless LAN Adapters |
| ZIP Drives | Digital Cameras |
| PDA's | CD/DVD Burners/Players |
| Tape Drives | Scanners |
| Hard Drives | Smart Card Readers |
| Floppy Drives | USB Printers |
| Biotech Drives | |
| Modems | |

Supported Connectivity

- | | |
|-----------|-------|
| USB | LPT |
| FireWire | IrDA |
| BlueTooth | IDE |
| WiFi | COM |
| PCMCIA | S-ATA |
| PS/2 | SCSI |

Feature	Function	Benefits
Whitelist	Assign permissions for authorized devices to user or user group, and by default, those not authorized are not allowed	Eliminates unknown or unwanted devices in your network, reducing the risk of data leakage
Access Control List Based Permissions	Assign permissions to a user/user group based on their Active Directory or eDirectory identity	Provides granular user permissions that remain with 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 more	Eliminates risk of unauthorized devices connecting to the network while providing the flexibility users demand
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 unauthorized viewing
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
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 filename or complete file 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 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 USB keyboard usage 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
Disconnected/ Remote Computer Protected	Enables constant protection by keeping a local copy of the last list of permissions on the disconnected machine	Secures computer regardless of network connection, ensuring that remote or disconnected users are also protected
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
Powerful Log Analysis and Reporting	Detailed log analysis with flexible filter, sort and display options and stored query templates as well as central reporting	Demonstrates policy compliance and drills down on suspicious behavior for legal or management follow up
Active Directory and eDirectory Support	Leverages user and user group definitions in existing Active Directory and eDirectory	Reduces setup and maintenance of users and user groups
Multi-Language Support	Supports 12 languages on Sanctuary client machines	Improves user experience in international organizations
Custom Reports	Custom query templates can be scheduled to automatically generate reports in HTML, XML or CSV formats and delivered via email or network file share	Produces data required for compliance audit purposes and management reporting in a report format or data format for easy integration into a 3rd party system
Password Lockout and Recovery	Lockout users after three failed attempts; recover access to devices when passwords are forgotten	Reduces risk of hackers breaking into devices; enables recovery of encrypted data on devices
Offline Temporary Permissions	Challenge/response system generates new permissions on disconnected machines, allowing for temporary permissions to users on demand, even when a user is not connected to the network	Enables provision of temporary permissions to users on demand, even when not connected

Enforce Your Application Usage Policy Today

For more information, and to receive a free 30 day evaluation; visit us on the web at www.lumension.com.



Lumension Security - Luxembourg

Atrium Business Park
Z.A. Bourmicht
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364 11 / www.lumension.com



Sanctuary® - A Lumension Brand.

©2007 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.