



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.

Device Control leverages role based access control to enforce user accessibility. If the device is known and the user has access rights to the 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

Sanctuary's patented bi-directional Shadowing 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, CDs and DVDs 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 devices, CDs and DVDs or enable users to encrypt on their own and enforce the use of that encrypted media.

In addition, administrators may enforce standard FIPS-compliant encryption technology with centralized encryption key management and support for large secondary hard drives provided by PGP Whole Disk Encryption.

Sources:

1. 2007 CSI/FBI Computer Crime and Security Survey
2. IT Policy Compliance, Taking Action to Protect Sensitive Data, Benchmark Research Report, February 2007
3. Privacy Rights Clearinghouse - www.privacyrights.org/ar/ChronDataBreaches.htm

Reduce Risk of Data Leakage

☐ Data breaches remain the leading cause of financial losses for enterprises today with the average loss per incident equal to \$350,424¹. And data is being lost or stolen at an alarming rate – 68% experiencing six losses of sensitive data annually². All in all, more than 200 million records were exposed in 2007³ – and those are just the ones we know about.

☐ 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 |
| ☐ PDAs | ☐ CD/DVD Burners/Players |
| ☐ Tape Drives | ☐ Scanners |
| ☐ Hard Drives | ☐ Smart Card Readers |
| ☐ Floppy Drives | ☐ Biotech Drives |
| ☐ Modems | ☐ USB Printers |

Supported Connectivity

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

Feature	Function	Benefit
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
Flexible Encryption Options for Removable Media and CD/DVD	Administrators may centrally encrypt removable media and CD/DVDs or force users to encrypt media and CD/DVDs at time of use	Ensures that sensitive data is not inadvertently exposed to those without authorized access
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
Granular Policy Control	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
Plug and Play Devices	Detect Plug and Play Devices "on the fly"	Ensures user productivity is not disrupted by applying permissions for plug and play devices when detected
Patented Bi-Directional Shadowing Option	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 data leakage
Data Copy Restriction	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
Role Based Access Control	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
PGP Whole Disk Encryption	Administrators may optionally enforce standard FIPS-compliant encryption technology with centralized encryption key management and support for large secondary hard drives provided by PGP Whole Disk Encryption	Ensures that data on external devices can be protected with FIPS-validated encryption
File Type Filtering	Control the type of files that are moved to and from removable devices	Reduces risk of unwanted files (or malware) from entering and sensitive files from leaving the network
Password Lockout	Lockout users after three failed password attempts	Reduces risk of hackers breaking into lost or stolen devices
Password Recovery	Recover access to devices when passwords are forgotten or user leaves company	Enables recovery of encrypted data on removable devices
Multi-Language Support	Supports 12 languages on Sanctuary client machines	Improves user experience in international organizations
64-bit Platform Support	Utilize and protect powerful 64-bit business infrastructure with Sanctuary including agent support for 64-bit Windows Server 2003, Windows and Windows Vista as well as 64-bit Support for SQL Server 2005	Delivers device control capabilities for both 32 and 64 bit platforms.

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.

Enforce Your Device 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 - United Kingdom

Unit C1, Windsor Place
Faraday Road, Crawley
West Sussex RH10 9TF

+44 (0) 1908 357 897 / 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.