



## Complete Prevention of Malware and Unwanted Applications

Sanctuary® Application Control, a component of Sanctuary, provides policy-based enforcement of application use to secure endpoints from malware, spyware, zero-day threats and unwanted or unlicensed software. By employing a whitelist approach, Sanctuary Application Control enables only authorized applications to execute on a network server, terminal services server, thin client, laptop or desktop. Unauthorized applications are prohibited from executing.

Malware is virtually eliminated and control is given to administrators over unwanted and unauthorized applications, including bandwidth stealing P2P applications.

## Simple, Fast, Flexible Administration and Management

Sanctuary Application Control enables administrators to rapidly identify applications and to assign permissions for applications to users, user groups or a particular computer

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

## Automated Discovery

Sanctuary is pre-configured in a non-blocking mode to simplify the discovery phase so that administrators can uncover all of the applications that are executing on the endpoints.

## Detailed Audit Capabilities

All application execution attempts can be logged, as well as any administrator actions, including changes of any application policy authorizations.

## Flexible Authorization Rules

Administrators can allow trusted users to authorize their own applications, providing ultimate flexibility. Administrators stay informed and in control with the ability to override local authorization.

## Application Control Server Edition:

Provides server security software that enforces application use policies to secure mission critical servers from unauthorized, illegal or unwanted applications by default and preventing any interruption to the flow of your business.

## Application Control Terminal Services Edition:

Enforces application use policies to secure Windows or Citrix terminal services environments from unauthorized, illegal or unwanted applications by default.

Also available, Sanctuary Device Control with integrated Sanctuary management console. Sanctuary Device Control provides policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints, reducing the risk of data leakage.

### Overview

- ☑ Protects against 100% of known and unknown threats
- ☑ Safeguards against zero-day threats and targeted attacks
- ☑ Controls proliferation of unwanted applications from burdening network bandwidth
- ☑ Maximizes benefits of new technologies and minimizes risk of network disruption

### Protect Against Malware, Spyware and Zero-Day Threats

- ☑ The security landscape is shifting from large, widespread malware outbreaks to targeted, focused threats. Traditional solutions cannot possibly defend against these types of attacks as evidenced by the fact that of the 99 percent of enterprises which have anti-virus solutions, 62 percent suffered an infection in 2005<sup>1</sup>. Endpoints are the likeliest entry point for malware. And the threat is proliferating - a leading antivirus vendor expects to double its recorded threats to 400,000 by 2008.
- ☑ With more end users installing non-business related programs and an increased number of threats, 85 percent of corporate machines need to be rebuilt every year<sup>1</sup>. The average enterprise downtime for each virus attack is 23 person days, with 31 person days required to achieve full recovery<sup>2</sup>.

Sources:

1. 2005 Yankee Group Security Leaders and Laggards Survey
2. 2005 National Survey on Data Security Breach Notification, Ponemon Institute

Feature	Function	Benefit
Whitelist	Assign permissions for authorized applications to users or user groups, and by default those not authorized are not allowed	Eliminates unknown or unwanted applications in your network, reducing the risk of malware and spyware and ultimately improving network stability
Standard File Definitions	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
Script / Macro Protection	Controls the execution of specific VBScript, Microsoft Office VBA and JavaScript with central authorization or a prompt to local users	Extends application policy enforcement to include specific scripts/macros, enabling business without compromising 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 and subdirectory scans to discover new applications and packages while online or offline	Provides flexible and fast option to identify new and updated 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, while maintaining a log for administrator review	Delivers 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
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
Offline Computer Protection	Local copy of updated hashes and permissions is kept on each machine	Ensures that remote/ disconnected users are constantly protected
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
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.

## 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](http://www.lumension.com).



**Lumension Security**  
 15880 N Greenway-Hayden, Suite 100  
 Scottsdale, AZ 85260  
 480.970.1025 \ [www.lumension.com](http://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.