

## Lumension Application Control™ (FORMERLY SANCTUARY)

### Prevent Unauthorized Software and Reduce Endpoint Security TCO with Application Whitelisting

The battle to protect the IT assets from malware and unauthorized software is a costly, ongoing struggle taking up valuable resources and time.

Each time a new malware threat appears or unsupported software causes a compatibility conflict, IT has to stop what they're doing to resolve the issue. Whether that's updating antivirus signatures to ensure that systems and information are protected or re-imaging laptops due to software conflict blue-screens, the end result is an increased support burden and lower operational efficiency.

#### Secure Endpoints, Servers, Kiosks and POS Systems from Malware

The threats aren't going to stop and antivirus software alone cannot control the problem as malware threats are being developed faster than the necessary fixes. Malware has grown over 500% with more than 5.49 million unique samples of malicious software in 2007<sup>1</sup> and 2008 has seen the rise of targeted attacks, which are now being designed to specifically bypass antivirus solutions.

Lumension Application Control enables you to prevent the execution of malicious code utilizing application whitelisting. This approach allows only authorized applications to run on laptops, PCs, servers, terminal services servers and thin clients without relying on antivirus signature-updates, freeing up network bandwidth and IT resources.

With no viral attacks to thwart, malware to hunt down, or incompatible applications to invoke the blue screen of death, you can spend more time on more strategic activities instead of constantly fixing computers.

#### Lumension Application Control provides:

- » Endpoint protection from malware without relying on signature updates
- » Optimized IT support with decreased helpdesk calls to support unauthorized software
- » Improved system availability and service levels by preventing known and unknown threats
- » Audit-readiness with detailed tracking of all application execution attempts and policy changes

#### Key Features

- » Application Whitelisting
- » Automated Application Discovery
- » Standard File Definitions
- » Automatic Authorization of Software Updates
- » Script / Macro Protection
- » Flexible File Authorization
- » Local Authorization
- » Spread Check
- » Offline Computer Protection
- » Active Directory and eDirectory Support

#### Datasheet

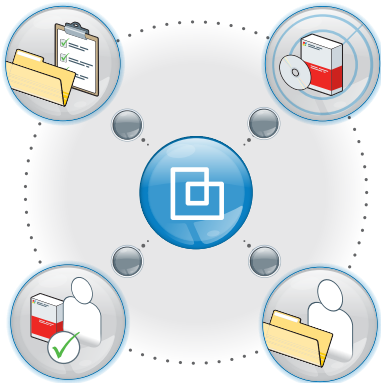
#### Key Benefits

- » Prevents Known and Unknown Threats
- » Blocks Targeted Malware and Zero-Day Attacks
- » Enforces Trusted Application Environment
- » Improves Server Availability
- » Reduces Endpoint Security TCO

*"Lumension enables me to explicitly list the applications that are allowed to run on our banks' machines. All other executables - including any malicious code - simply will not run. With Lumension, I can stay ahead of potential challenges, providing peace of mind for the banks' executives and auditors, and ultimately, our customers."*

**Brent Rickels, VP Technology,**  
First National Bank of Bosque County

## How Lumension Application Control Works



1. **Identify** - all executable files, collect profiles and organize into pre-defined file groups.
2. **Assign** - rights to execute based on executable and user/group attributes.
3. **Authorize or Deny** - a user who wants to execute an application. If the user or the application does not have rights, access is denied.
4. **Audit** - a detailed trail of attempts and actions, along with proof that your software licenses are in compliance.

### Key Features

**Application Whitelisting:** Eliminates unknown or unwanted applications on your network and automates application discovery for creating or updating whitelists.

**Automated Application Discovery:** Provides flexible and fast options to create or update whitelists.

**Spread Check:** Contains risk of malicious code spreading through the network due to local authorization by disabling suspicious executables that are locally authorized on too many computers.

**Active Directory and eDirectory Support:** Reduces setup and maintenance of users and user groups by leveraging definitions in existing Active Directory and eDirectory.

**Automatic Authorization of Software Updates:** Eliminates risk of accidentally restricting user access to frequently updated Microsoft applications.

**Script / Macro Protection:** Extends application policy enforcement to include specific scripts/macros, enabling business without compromising protection.

**Flexible File Authorization:** Provides flexible and fast option to identify new and updated applications for review and ultimately to generate whitelists.

**Local Authorization:** Delivers flexibility to the user, without giving up administrative control by allowing trusted users to authorize applications locally, while maintaining a log for your review.

**Offline Computer Protection:** Ensures that remote/ disconnected users are constantly protected by keeping a local copy of updated hashes and permissions on each machine.

**Standard File Definitions:** Speeds and simplifies whitelist definition with classified, pre-loaded whitelist of all supported OS files.

### » System Requirements

- » **Server:** Windows 2000, Windows 2003
- Client:** Windows XP, Windows 2000, Windows 2003, Windows Vista, Windows XPe



Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance

