

Application Control

Secure Endpoints from the Rising Volume and Sophistication of Malware

More than 2 million new malware signatures are now identified each month. More sophisticated and zero-day attacks are also on the rise. But traditional security defenses, such as anti-virus, are not able to keep up. And the impact to organizations' bottom line is significant - malware driven costs can be as much as 50 percent of an organization's endpoint TCO due to increased help desk calls, reimaging costs, network downtime and lost employee productivity¹.

[Lumension® Application Control](#) provides complete malware protection and increases IT and end-user productivity by preventing any unknown, un-trusted or malicious applications from executing. With [Lumension® Application Control](#), IT administrators can quickly identify all applications running in their environment and enforce a comprehensive whitelist policy that prevents unauthorized applications, malware and un-trusted change.

[Lumension® Application Control](#) overcomes the traditional challenges associated with stand-alone, point application control products through innovative features that add both whitelist management flexibility and ease-of-use - all enabled within the [Lumension® Endpoint Management and Security Suite](#), which integrates [Lumension® Application Control](#) with [Lumension® Patch and Remediation](#) and [Lumension® AntiVirus](#) to deliver a powerful and innovative application whitelisting solution, [Lumension® Intelligent Whitelisting™](#).

[Lumension® Application Control](#) provides:

- » Comprehensive application visibility across your entire endpoint environment to identify and eliminate IT risk, as well as software conflicts that impact productivity and TCO.
- » Quick definition of application whitelist policies by taking a snapshot of the endpoint environment to establish baseline application whitelist policies and then optimizing policies before deployment by running in a monitor-log only mode.
- » Effective enforcement of application whitelist policies, rather than relying on self-policing.
- » Automatic security from zero-day attacks, without waiting for an anti-virus definition to be developed and provided and without waiting for the latest vulnerability patches.
- » Complete protection at all times by effectively preventing the installation and use of unauthorized software and the introduction and execution of malicious code - whether or not the endpoint is online or offline.
- » Increased productivity and reduced endpoint TCO by improving the stability and performance of the network environment and minimizing operational support costs, such as IT help desk calls and endpoint reimaging.
- » Enforcement policies that reduce local admin account risk and ensure standardized system configurations to enable only trusted and authorized applications to run – without taking away local admin rights.

Key Features

- » Application Whitelisting
- » Easy Lockdown
- » Easy Auditor
- » Trust Engine
- » Application Library
- » Application Event Log
- » Denied Application Policy
- » Flexible User- and Machine-based Policy Enforcement
- » Offline Computer Protection
- » Integration with [Lumension® Endpoint Management and Security Suite](#)

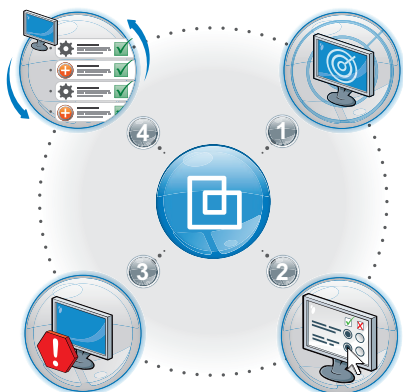
Key Benefits

- » Prevents Known and Unknown Threats
- » Blocks Targeted Malware and Zero-Day Attacks
- » Enforces Trusted Application Environment
- » Improves PC and Server Availability
- » Reduces Endpoint Security TCO
- » Integrates with Antivirus and Patch Management Tools for Defense-in-Depth

"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. **Discover** - Snapshot individual endpoints to identify and catalog all executables currently running on them and quickly determine potential application risk.

2. **Define** - Create policies that automate how new applications are introduced and executed on endpoints using Lumension's flexible, rules-based Trust Engine, ensuring that the whitelist is constantly updated to permit authorized applications to run.

3. **Enforce** - Block unknown and unauthorized applications from executing by default and prevent zero-day attacks automatically, before the latest anti-virus definitions or vulnerability patches are deployed. Reduce IT risk even further by extending whitelist policies to end users with Local Admin privileges.

4. **Manage** - Update whitelists using the Trust Engine to deploy software (and software updates). Generate reports to demonstrate compliance with security policies, and to conduct forensics as necessary.

Key Features

Application Whitelisting: Eliminates unknown or unwanted applications in your network, reducing the risk and cost of malware, and ultimately improving network stability.

Easy Lockdown: Provides immediate security without disrupting productivity by automating the creation of your whitelist.

Easy Auditor: Enables IT to assess the impact of an application whitelist policy and reduces IT burden in creating and maintaining a whitelist of trusted applications.

Trust Engine: Allows flexible, trust-based policies to be managed across multiple variables without imposing a laborious manual process as changes are approved automatically and do not require administrator involvement.

Application Library: Aggregates all data collected by local snapshot scans and provides grouping and filtering options for application policy management for complete visibility.

Application Event Log: Provides powerful log analysis and reporting while delivering necessary visibility into endpoint events.

Denied Application Policy: Prevents users from installing or running applications that have been deemed as unwanted for security, productivity or licensing reasons.

Flexible User- and Machine-based Policy Enforcement: Provides granular and flexible policy control to accommodate any use-case scenario.

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

Integration with Lumension® Endpoint Management and Security Suite: Integrates with other Lumension product modules to streamline and improve IT operations and security, reduce agent bloat and improve endpoint visibility.

www.lumension.com

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

System Requirements

- » **Server:** Windows Server 2003, 2003 R2, 2008, and 2008 R2
- » **Client:** Windows XP Pro, Windows Vista, Windows 7, and Windows Server 2003, 2003 R2, 2008, and 2008 R2

[Complete Requirements](#)

Online Resources

- » [FREE TRIAL](#)
- » [Endpoint Protection Blog](#)
- » [Lumension® Application Scanner Tool](#)
- » [Intelligent Whitelisting: An Introduction to More Effective and Efficient Endpoint Security](#)
- » [Key Strategies to Address Rising Application Risk in Your Enterprise](#)

Contact Lumension

- » Global Headquarters
8660 E. Hartford Dr.
Suite 300
Scottsdale, AZ 85255
+1.480.970.1025
sales@lumension.com
- » United Kingdom
+44.0.1908.357.897
sales.uk@lumension.com
- » Europe
+352.265.364.11
sales-emea@lumension.com
- » Asia & Pacific
+65.6725.6415
sales-apac@lumension.com

 **Lumension®**
IT Secured. Success Optimized.™

LAC-DS-EN-04-11-11