Lumension® Endpoint Management and Security Suite

Application Control

Lumension
IT Secured. Success Optimized.™

Secure Endpoints from the Rising Volume and Sophistication of Malware

Over 11.9 million new malware signatures are now identified each month. More sophisticated and zero-day attacks are also on the rise. But traditional, single line-of-defense security tools such as anti-virus are not able to keep up.

This scenario impacts organizations' bottom line significantly - 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 productivity.[1]

Lumension® Application Control provides effective malware protection and increases IT and end-user productivity by preventing any unknown, un-trusted or malicious applications from executing, as well as preventing memory-based attacks. 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 *Lumension*® Device Control, and *Lumension*® AntiVirus to deliver a powerful and practical defense-in-depth approach to securing your endpoints.

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.
- Quickly define application whitelist policies by taking snapshot of endpoint environment to establish baseline and then optimizing policies before deployment by running in monitor or log-only mode.
- 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.
- Continuous protection for online and offline endpoints by preventing the installation and use of unauthorized software and the introduction and execution of malicious code, including memory-based attacks.
- 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 reimages.
- Enforcement policies that reduce local admin account risk and ensure standardized system configurations to enable only trusted and authorized applications to run – without completely removing local admin rights.

Key Benefits

- Provides Continuous Application Visibility and Control
- Prevents Targeted Malware and Zero-Day Attacks
- Protects Against Memory Injection Attacks
- Enforces Trusted Application Environment
- Improves System Performance and Availability
- Reduces Endpoint Security TCO
- Integrates with Antivirus, Device/Port Control and Patch Management Tools for Defense-in-Depth

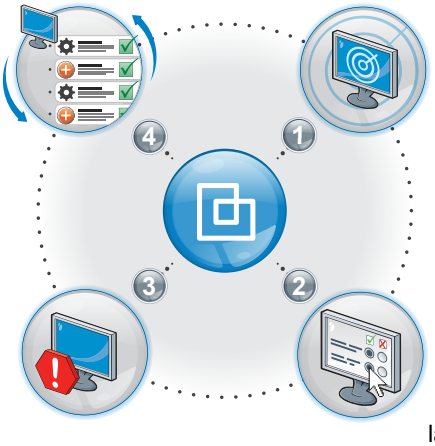
Key Features

- Application Whitelisting
- Advanced Memory Protection
- Application Reputation Scoring
- Easy Auditor / Lockdown
- Automated Trust Engine
- Local Authorization
- Centralized Application Management
- Application Event Log
- Denied Application Policy
- Flexible User- and Machine-based Policy Enforcement
- Offline Computer Protection
- Integration with *Lumension*® Endpoint Management and Security Suite

"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

1. Ponemon Institute, 2011 State of Endpoint Risk

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 via the *Lumension*® Endpoint Integrity Service.
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.

System Requirements

Visit lumension.com for the latest product details and information.

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

Key Features

Application Whitelisting:

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

Advanced Memory Protection:

Provides integrated protection against memory injection attacks by validating all new processes, even those initiated by approved running applications.

Application Reputation Scoring:

Cloud-based Verification Rating via the *Lumension*® Endpoint Integrity Service (EIS) provides IT admins and end users alike with background information on new or unknown applications when making trust decisions.

Easy Auditor / Lockdown:

Allows IT to automatically create, assess, implement and maintain individualized whitelist of trusted applications without disrupting end user productivity.

Automated 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.

Local Authorization:

Lets end users make ad hoc changes with accountability and control, by tracking end user change and enabling administrators to reverse the change if necessary.

Centralized Application Management:

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.