

Lumension® Endpoint Management and Security Suite Intelligent Whitelisting

Shift Away From Ineffective Endpoint Security

In today's dynamic threat landscape, more sophisticated and targeted threats continue to rapidly increase. Web 2.0 technologies and the social business environment of today's workforce has introduced new IT risks that traditional threat-centric endpoint security approaches (i.e. blacklisting, antimalware) technologies were never designed or intended to protect against.

While more effective, proactive security approaches (i.e. application whitelisting) have been selectively implemented, these solutions have been limited in their ability to adjust to the dynamic needs of today's business environment. As a result they have mostly been relegated to static system environments like point-of-sale (POS) or servers.

To ensure effective endpoint protection in today's increasingly connected and "always on" business arena, organizations must now look beyond traditional threat-centric models where the focus is on identifying the known bad, to a more effective approach centered on identifying the known good, and managing dynamic change through a trust-centric approach.

Introducing Lumension's Intelligent Whitelisting Approach

To address these emerging endpoint security requirements, Lumension shifts the industry debate away from blacklisting vs. whitelisting with Intelligent Whitelisting as part of its *Lumension*® Endpoint Management and Security Suite, the first integrated solution of its kind. This innovative approach enables IT organizations to meet endpoint and application risks head on, without the operational headaches of traditional application whitelisting.

Lumension's Intelligent Whitelisting solution leverages the best of both blacklisting and whitelisting, and manages dynamic change through a rules-based trust manager that can define what types of change are acceptable.

How Lumension's Intelligent Whitelisting Solution Works

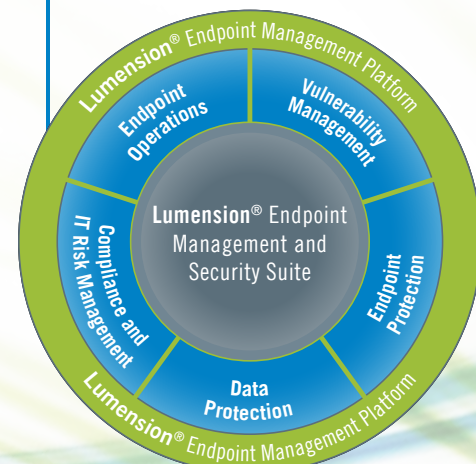
By setting up rules around how change can be introduced, rather than focusing solely on what kinds of change should be stopped, a balanced and more effective operational model of endpoint security management can be achieved. Lumension enables this through a very simple, yet effective unified solution workflow:

- » **Clean IT:** Using Lumension's integrated antivirus technology (*Lumension*® AntiVirus) IT administrators can scan the IT environment for any known malware and automatically remove it.
- » **Lock IT:** With Lumension's Easy Lockdown technology, a "snapshot" of the entire system is taken and a whitelist is automatically created. From this point on nothing new is allowed to execute without first proving it is wanted and trusted.
- » **Trust IT:** Utilizing Lumension's Trusted Change Manager, IT managers can quickly and simply identify the rules by which they want to manage and introduce change into their whitelisted environment.

Datasheet

Key Benefits

- » Stops zero-day attacks, and malicious and unwanted applications from entering your IT environment
- » Works with any existing non-Lumension antivirus and patching capabilities
- » Eliminates operational friction associated with application whitelist management and patching
- » Integrates both blacklisting and whitelisting capabilities for enhanced endpoint security
- » Improves operational performance of endpoints by eliminating software conflicts and reimaging due to malware
- » Prevents unlicensed or unsupported applications from being installed



Eliminate Operational Friction and Endpoint Complexity

Lumension's Intelligent Whitelisting solution eliminates operational friction associated with maintaining application whitelists and ongoing patch management through integration with *Lumension*® Patch and Remediation. This integration now allows for the automatic updating of the whitelist manifest each time a patch is applied. IT managers no longer have to be concerned with maintaining the security level of their whitelisted environment or manually managing the whitelist each time they apply a patch.

As part of the Lumension Endpoint Management and Security Suite, endpoint TCO is reduced and productivity is enhanced as the Intelligent Whitelisting workflow is managed through a single console and deployed on a single server and single agent architecture. Lumension also enables the use of existing non-Lumension antimalware and patching solutions, while still deploying its intelligent whitelisting capabilities, thus offering a non-disruptive solution to the business.

Key Features

Lumension Unified Workflow: Delivers a unified workflow across the integrated capabilities of *Lumension*® Application Control, *Lumension*® AntiVirus and Lumension Patch and Remediation, within a trusted change manager to deliver an easy-to-use, easy-to-implement solution. This unified workflow ensures a seamless process to scan the IT environment, remove known threats, lockdown the IT environment, flexibly manage change coming into the environment, and remove operational friction between IT operations and security.

Easy Lockdown: Takes a “snap shot” of your IT environment and automatically builds the whitelist off that snapshot. Once a system has been locked down new change can't be introduced without passing through Lumension's trusted change manager. Easy Lockdown provides the capability to immediately lock a “gray system” down and prevent any further unauthorized changes from taking place within that environment.

Trusted Change Manager: The trusted change manager is a rules-based policy engine that automates whitelist updates creating a flexible, dynamic whitelisting capability without imposing a laborious manual process. This enables the IT organization to manage trust across multiple variables including trusted vendor (via digital signature and endpoint integrity services), trusted user, trusted software updater, and trusted location.

Lumension Application Control (Whitelisting): Identifies and controls what applications are currently in your IT environment or can be added to your IT environment. Automatically identify trusted software in your enterprise to run while preventing anything else that is not trusted, malicious or just unwanted from executing. All executable content including typical .EXEs, .DLLs, .COMs, etc. are whitelisted along with portable executables for scripting, macros and java applets.

Integrated Lumension Antivirus (Blacklisting) with Lumension Application Control (Whitelisting): Fully integrated Antivirus/malware with application control ensures that IT systems are free from known malware before the IT environment is locked down and whitelisted. Additional sandboxing, and DNA “partial” pattern matching provide added protection along with application whitelisting, and basic malware signature identification.

Integrated Lumension Application Control with Lumension Patch and Remediation: Application whitelist manifests are automatically updated with the latest application hash file information each time a patch is applied. System wide vulnerability risk is reduced as proper patching programs can be maintained within the “whitelisted” environment. This combined integration offers a new level of endpoint protection and reduces overall IT risk.

System Requirements

- » **Server:** Windows Server 2003 or 2008 with Microsoft SQL Server 2005 or 2008 and .NET Framework
- » **Agent Coverage:** Apple Mac OS X, CentOS, Hewlett Packard HP-UX, IBM AIX, Novell SUSE Linux, Oracle Enterprise Linux, RHEL, Sun Solaris, Windows: 2000, XP, Vista, 7, Windows Server: 2003, 2008, 2008 R2

[Complete Requirements](#)

Online Resources

- » [FREE TRIAL](#)
- » [Endpoint Protection Blog](#)
- » [FREE eBook](#)
[Shift Happens: The Evolution in Application Whitelisting](#)

The logo for OTIKA, featuring the word "OTIKA" in a bold, black, sans-serif font. Above the letter "I" is a vertical bar composed of three small squares: the top one is orange, the middle one is yellow, and the bottom one is white.

OTIKA

Phone: 01 71 11 31 45

lumension@otika.fr

www.otika.fr

The Lumension logo, consisting of a blue square icon with a white geometric pattern inside, followed by the word "Lumension" in a bold, blue, sans-serif font. Below "Lumension" is the tagline "IT Secured. Success Optimized." in a smaller, blue, sans-serif font.