

Lumension® Intelligent Whitelisting™



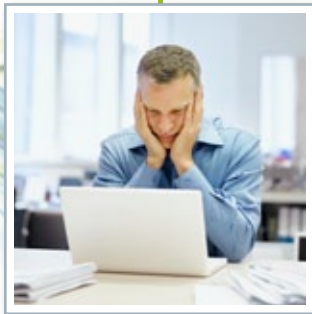
More Effective, Flexible and Easy-to-Manage Endpoint Security Solution that Reduces Malware Risk and Endpoint TCO - Without Impacting Business Productivity

In today's dynamic threat environment, organizations are increasingly vulnerable to sophisticated and targeted malware attacks from financially-motivated cybercriminals. To meet the demands of the new environment, organizations must ensure better centralized control over endpoint configurations to improve their security posture, without impacting end-user productivity.

Endpoint Security Business Drivers and Challenges

In today's decentralized, mobile and always-connected IT environment, endpoints are harder to manage, secure and control than ever before, as end-users regularly enjoy Local Admin control and continually download unauthorized or unwanted third party applications onto endpoints. Organizations are also facing a growing threat from a rising volume of sophisticated and targeted malware designed to bypass traditional security defenses like anti-virus products (AV). The result is that IT professionals are left feeling less secure today than they did even just one year ago.

The continued exponential rise in malware and growing ineffectiveness of traditional anti-virus has led to an increase in IT help desk, remediation and incident response costs as the average organization now reports upwards of 50 malware incidents per month that impact productivity¹. While AV is still a part of the endpoint protection arsenal, it is no longer effective as a stand-alone technology and is adding to the TCO for the endpoint:



- » AV cannot keep up with the almost 1.6 million newly identified instances of malware each month and cannot defend against zero-day or blended threats².
- » AV does not provide the necessary visibility of third party applications installed and running on endpoints and does not help maintain centralized security configurations.
- » AV cannot control actions by users with Local Admin privileges and cannot curb the introduction of unwanted applications.

Application control/whitelisting is a proven endpoint security approach that changes the playing field. Instead of attempting to identify all malware out in the wild – an impossible task in today's threat environment – application whitelisting identifies which software is needed for business operations and enables only those applications approved by IT to run on the endpoint. However, traditional stand-alone application control/whitelisting technologies cannot meet the operational efficiency and flexibility that IT needs when managing endpoints in a dynamic endpoint environment.

Lumension® Intelligent Whitelisting™ combines the iron-clad security effectiveness of application control/whitelisting with the flexibility of automated trust-based change management policies. This makes it easy for IT to implement and manage in both dynamic and locked-down environments alike, while still ensuring business agility and productivity.

Effective and Operational Endpoint Security for Dynamic Environments

Lumension® Intelligent Whitelisting™, which is delivered on the *Lumension*® Endpoint Management and Security Suite, is the industry's first intelligent endpoint security solution that allows organizations to achieve the efficiency of AV with the enhanced security and operational effectiveness of application control/whitelisting and patch management. By combining *Lumension*® AntiVirus, *Lumension*® Application Control and *Lumension*® Patch and Remediation into a fully integrated and unified workflow, Lumension enables IT to deliver much stronger endpoint security without impacting organizational productivity.

1. Ponemon Institute, [State of Endpoint Risk](#) (Nov-10)
2. McAfee Labs, [Threats Report: Third Quarter 2010](#) (Nov-10)

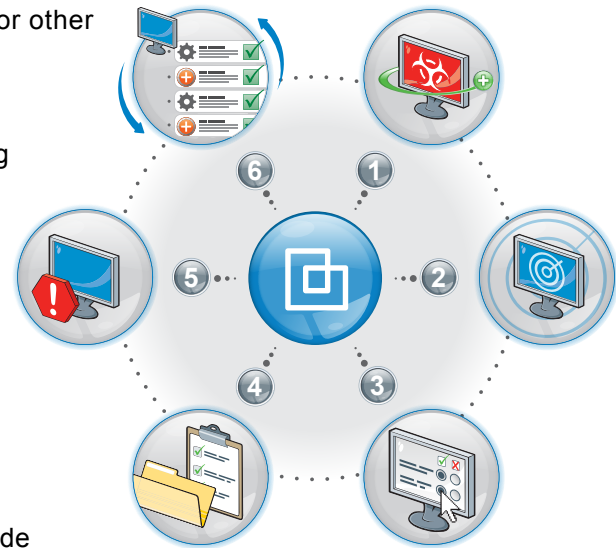
With Lumension® Intelligent Whitelisting™:

- » **Increase Your Endpoint Security** and stop both zero-day and targeted attacks via a defense-in-depth strategy that allows only trusted and known executable to run on endpoints.
- » **Regain Control of Your Endpoints** by reducing Local Admin risk. End-users with Local Admin rights can introduce significant levels of application, vulnerability and configuration risk and leave holes for zero-day and other malware to exploit.
- » **Deliver Flexible, Effective and Easy-to-Use Application Control/Whitelisting**. Unlike traditional, stand-alone application control products, Lumension's integrated Intelligent Whitelisting solution provides increased flexibility by enabling IT to effectively manage trust-based change within a dynamic endpoint environment.
- » **Increase Your Organizational Productivity** by eliminating malware and software conflicts that cause unplanned downtime, freeing IT resources to work on more strategic initiatives, minimizing end user downtime due to malware infection, and applying granular application policy enforcement across roles and users.
- » **Reduce Endpoint TCO** by minimizing the number of IT help desk calls and incident responses due to malware and issues caused by software conflicts, as well as reducing the complexity of maintaining several different and unrelated point products.

How Lumension® Intelligent Whitelisting™ Works

Lumension® Intelligent Whitelisting™ provides flexible control of application usage at the endpoint. By setting up rules around how change can be introduced, rather than focusing solely on what kinds of change should be stopped, a more effective operational model of endpoint security management is achieved. Lumension enables this capability through an easy-to-manage, yet effective unified solution workflow:

1. **Clean** : Scan your endpoint environment using *Lumension®* AntiVirus, or other antimalware products, to automatically identify and remove all known malware.
2. **Discover** : Gain unparalleled visibility into what applications are running across the endpoint environment. Discover known and unknown endpoint applications and quickly determine potential application risk.
3. **Define** : Snapshot the endpoint environment to quickly define baseline application whitelist policies. Automatically approve software updates from trusted software publishers, paths and users and simplify whitelist management with Lumension's flexible, rules-based trust engine. Application whitelist policies are seamlessly updated and deployed to identified endpoints.
4. **Monitor** : Continuously monitor whitelist policies in non-enforcement mode and log all execution attempts. Assess the potential impact of whitelist policies and adjust trust engine rules to achieve an optimal balance between effective endpoint security and end-user productivity.
5. **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.
6. **Manage** : Simplify whitelist management and reduce IT operational headaches by seamlessly integrating with *Lumension®* Patch and Remediation or other third party patching tools. *Lumension®* Intelligent Whitelisting™ automatically updates application whitelist policies when the latest software updates and vulnerability patches are deployed. In-depth reports provide additional insight into your organization's overall security posture and whitelisted environment.



Key Benefits

- » Reduces malware risk by stopping all known malware and helps to prevent zero-day attacks and other malicious applications from entering your IT environment.
 - » Reduces 3rd party application risk by providing enterprise-wide visibility of all running applications and preventing unwanted or unauthorized applications from executing.
 - » Prevents unlicensed, unsupported or unwanted applications from being used on the endpoint, allowing only software that is needed for business reasons and approved by IT to run.
 - » Provides effective endpoint security without sacrificing end user productivity
 - » Reduces endpoint management TCO and malware-related costs (e.g., help desk, re-imaging) while streamlining application whitelist management
 - » Controls end-users with Local Admin privileges that allow them to install and run trusted applications while limiting their actions according to policy.
 - » Supports other third party operational and security products through an open architecture
 - » Reduces IT management burden by automating whitelist policy based on sources of trusted change (e.g., trusted applications, vendors, self-updating programs, location and local authorization)
-

Key Features

Application Control / Whitelisting

Automatically identifies trusted software that is authorized to run on the endpoint and prevents all other applications from executing – whether they are malicious, unwanted or merely not trusted. Supports all executables including typical .EXEs, .DLLs, .COMs, etc. Improves productivity for both IT and end-users.

Trust Engine

Automates whitelist updates based on trust policies to enable whitelist flexibility and business agility without imposing a labor intensive, manual process. The Trust Engine makes whitelist management simple in dynamic environments, and includes:

- » **TRUSTED PUBLISHER:** Enables “on-the-fly” changes to the whitelist when changes are accompanied by a valid and signed certificate by the application provider. Such changes are approved automatically and do not require administrator involvement.
- » **TRUSTED UPDATER:** Permits automated updates to the whitelist when changes are made by specifically authorized programs.
- » **TRUSTED PATH:** Allows the whitelist to be automatically updated as changes are made in the library of known good applications.
- » **LOCAL AUTHORIZATION:** Lets end-users make ad hoc changes with accountability and control, by tracking end-user changes and enabling administrators to reverse those changes if necessary. (available in Q3, 2011)

Easy Lockdown

Simplifies the whitelisting process to immediately enforce policies and prevent any unauthorized changes from occurring. An automated snapshot of each endpoint is used to create a whitelist and begin the enforcement of whitelisting policies. Provides immediate relief from new zero-day and other malware attacks, reducing IT workload.



Take Control of Your Endpoints and Improve Operational Productivity

Streamline management of endpoints and protect your organization from targeted and zero-day threats without impacting business operations. Contact your local Lumension sales representative, reseller or visit us at www.lumension.com.

Key Features Continued

Easy Auditor

Allows administrators to observe and audit whitelisting policies to ensure business needs and security considerations are achieved before enforcement actions are applied. A local snapshot baseline can be built and appropriate action taken, without relying on a global “gold image”. Reduces IT burden in creating and maintaining a whitelist of trusted applications.

Unified Workflow

Ensures a seamless process to scan the IT environment, remove known threats, lock down the IT environment, flexibly manage change coming into the environment, and remove operational friction between IT operations and security. Reduces training and implementation time, with faster time-to-protection.

Integrated Antivirus

Ensure that endpoints are free from known malware before they are locked down and whitelisted by leveraging the fully integrated Lumension AntiVirus product module. Basic malware signature identification along with advanced sandboxing, behavioral analysis, and partial-pattern matching capabilities provide added protection in combination with application whitelisting. Automates malware removal for improved IT and end-user productivity.

Integrated Patch Management

Simultaneously manage application and OS vulnerability risk and security configurations within the fully integrated Lumension Patch and Remediation module. As operational changes are made to mitigate vulnerability risk, such as the deployment of new software and changes to systems configurations, all appropriate whitelist policy updates are made to ensure seamless enforcement without disrupting end-users or burdening administrators. Improves endpoint security without impacting IT and end-user productivity.

Lumension Endpoint Management and Security Suite

Provides the underlying platform architecture for *Lumension*® Intelligent Whitelisting™, with a single agent and single console. Highly scalable architecture reduces overall TCO and enhances IT operations and security visibility.

Online Resources

- » [Learn More about the Evolution of Application Whitelisting](#) intelligentwhitelisting.com
- » [Endpoint Protection Blog](#)
- » [Application Scanner](#)
- » [Whitepaper: Intelligent Whitelisting - An Introduction to More Effective and Efficient Endpoint Security](#)
- » [Podcast: Application Security Whitelisting: Keep the Bad Guys Out - Let the Good Guys In](#)
- » [Product Information: Lumension® Endpoint Management and Security Suite](#)

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