

# Lumension® Endpoint Protection



## Proactive & Complete Protection to Ensure a Trusted Endpoint Environment

With the emergence of consumer technology in the workplace, social networking, Web 2.0 technologies and increasingly sophisticated cyber criminals, securing your endpoints is an uphill battle. Lumension Endpoint Protection combines proven antivirus technologies and innovative application whitelisting to establish a trusted endpoint environment to stop unwanted change, neutralize security threats, and prevent sensitive data from escaping.

## Endpoint Protection Business Drivers and Challenges

In today's economy balancing the ease of doing business with endpoint security is a challenge. Endpoints are no longer bound to an office desk in a controlled environment. Employees are increasingly installing unauthorized and illegal applications on laptops and PCs which can cause increased support calls, performance issues and downtime.

And, malware and targeted attacks are on the rise. In fact analysts estimate that 75 percent of enterprises were infected with financially motivated, targeted malware that evaded traditional perimeter and host defenses.<sup>1</sup> According to a recent study, more than 21 million unique samples of malicious software were reported.<sup>2</sup>

Solid endpoint protection requires a proactive and complete approach that provides true defense-in-depth and is flexible enough to balance user productivity and convenience together with enterprise security needs.



“Lumension provides a single, seamless view of everything accessing or attempting to access the network through corporate endpoints from a device and application perspective, providing a new level of visibility into the network then was previously possible.”

Rob Israel, CIO, John C. Lincoln Health Network

## Secure Enterprise Endpoints from Malware and Unauthorized Software that Impacts Productivity and Security

The Lumension Endpoint Protection solution fully protects endpoints from known malware and unknown threats (such as zero-day exploits) while enforcing the use of only authorized software. With *Lumension*® Application Control and *Lumension*® AntiVirus, you can prevent known and unknown malware and centrally manage, monitor, and control application installation and use in your environment.

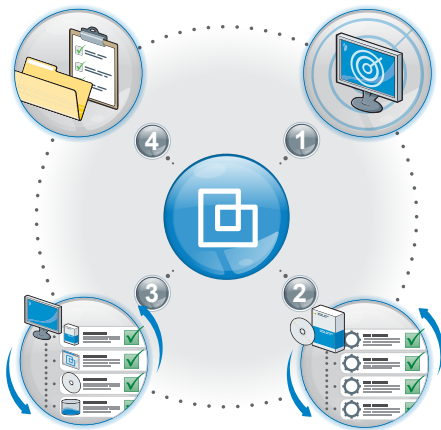
With the combination of antivirus and application whitelisting capabilities, known malware can be quickly removed from endpoints and only trusted applications will be authorized to run on your servers, locking them down from threats. This defense-in-depth approach protects endpoints by establishing a trusted environment.

In addition, you can improve operational desktop and server management by eliminating the unnecessary support calls and performance issues that come with managing unauthorized and illegal software. You can easily demonstrate compliance by discovering all applications in your environment, by enforcing software license policies and by providing a detailed audit trail of all application execution attempts.

1. Gartner Research, [Gartner's Top Predictions for IT Organizations and Users, 2007 and Beyond](#), Daryl C. Plummer, December 1, 2006  
2. [www.AVtest.org](#), 2009, cumulative unique malware samples reported through 24-July-2009

“It is a huge relief to know that when we give an employee a PC that we’ve configured and know how it works that it is going to stay that way because Lumension ensures that the user can’t install or run anything you don’t want them to. No other product I know has the same level of quality and security as Lumension.”

Ben Crewe, Systems Engineer, Australian Aerospace



**1. Discover:** Scan for and remove all known malware to establish a clean environment. Identify and organize all endpoint applications and executables into predefined management groups.

**2. Implement:** Assign permissions for applications to run based on executable, user, or user group attributes; use an application whitelist approach to ensure that only authorized and trusted applications can run on endpoints. Continue blocking known malware and use behavioral analysis tools to assess new unknown code which may or may not be legitimate.

**3. Monitor:** Monitor the effectiveness of endpoint security policies in real time and identify potential threats by logging all application execution attempts and recording all policy changes and administrator activities. Maintain ongoing antivirus scanning to identify and remove any “dead malware” that, although prevented by application control, is still present on endpoints.

**4. Report:** Demonstrate policy compliance and ensure software license compliance by drilling down on suspicious behavior for security or legal follow-up. Report on malware prevention and remediation on behavior of unknown or suspicious code and on current threat levels.

## How Lumension Endpoint Protection Works

### Key Benefits

- » Prevents Known and Unknown Malware (e.g., zero-day exploits)
- » Removes Malware from Endpoints
- » Allows only Trusted Applications to Run
- » Saves Time and Improves Desktop and Server Management
- » Reduces IT Support Burden
- » Enforces Compliance in Your Organization
- » Improves Endpoint Performance and End-User Productivity

“At EC Suite, security has always been a top priority. Our philosophy is that security efforts should proactively stay ahead of emerging threats, not simply react to them. Lumension’s Endpoint Protection and Vulnerability Management solutions have been integral components to this positive approach, keeping our sensitive information and digital assets safe from both external and internal threats.”

William Bell, Director of Information Security, EC Suite

# Take Control of Your Endpoint Protection

Protect your organization from threats starting today. Contact your local Lumension sales representative, reseller or visit us at [www.lumension.com](http://www.lumension.com).



“Since we’ve installed Lumension we’ve never had a call out to a PC due to the settings being changed or software downloaded to a machine. The People’s Network has been problematic to run from many perspectives but

Lumension’s solution has never let us down. It’s the best software we have on the People’s Network.”

Matthew Waite, IT Consultant, Hampshire County Libraries

## Key Features

- » Automatically determines what applications are in use throughout your organization.
- » Defines security policy with global and user- and/or machine-specific rules based on organizational needs using a “whitelist” approach.
- » Enforces application usage policies across your entire network.
- » Automatically logs network events related to your endpoint security policy.
- » Provides organization-wide control and enforcement using scalable client-server architecture with a central database which facilitates load balancing and distributed control.
- » Installs tamper-proof agents on every endpoint on the network that are protected against unauthorized removal.
- » Lumension Application Control fully supports both Windows Active Directory and Novell eDirectory / NDS structure.
- » Recognizes, blocks, and removes viruses, worms, Trojans and other types of malware such as keyloggers, hijackers and rootkits.
- » Protects against new and unknown malware (e.g., zero-day threats) via: **DNA Matching** which provides partial signature matching, **SandBox** which delivers behavioral analysis and safe emulation in a virtual environment, and **Exploit Detection** which detects malware exploiting vulnerabilities used in document types such as OLE2, MDB, WMF, JPEG, RIFF and SWF.
- » Ensures that any malware that manages to evade detection is not allowed to remain on network assets (servers, endpoints, etc.) indefinitely.

[www.lumension.com](http://www.lumension.com)

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Mgmt.

## Online Resources

- » [FREE TRIAL](#)
- » [Endpoint Protection Blog](#)
- » [Application Scanner](#)
- » [Whitelisting Technology Improves Security, Reliability and Performance Via Trusted Change](#)
- » [Ogren Group Security Business Analysis - Lumension: A Case Study in Proactively Managing Endpoint Risk](#)
- » [Application Security Whitelisting: Keep the Bad Guys Out - Let the Good Guys In](#)
- » [Minimizing Security-Related Total Cost of Ownership](#)

## Contact Lumension

- » Global Headquarters  
15880 N. Greenway Hayden  
Suite 100  
Scottsdale, AZ 85260  
+1.480.970.1025  
[sales@lumension.com](mailto:sales@lumension.com)
- » United Kingdom  
+44.0.1908.357.897  
[sales.uk@lumension.com](mailto:sales.uk@lumension.com)
- » Europe  
+352.265.364.11  
[sales-emea@lumension.com](mailto:sales-emea@lumension.com)
- » Asia & Pacific  
+65.6725.6415  
[sales-apac@lumension.com](mailto:sales-apac@lumension.com)

