

Lumension Endpoint Protection™



Proactive Endpoint Protection to Ensure a Trusted Application Environment

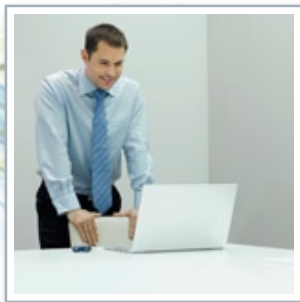
With the emergence of consumer technology in the workplace, social networking, Web 2.0 technologies and increasingly sophisticated cyber criminals, securing your endpoints is an uphill battle. Lumension Endpoint Protection stops endpoints from becoming a doorway for security threats to enter and sensitive data to escape and provides an effective method for creating a trusted and productive environment.

Endpoint Protection Business Drivers and Challenges

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

And, malware is on the rise. In fact analysts estimate that 75% of enterprises were infected with financially motivated, targeted malware that evaded traditional perimeter and host defenses.¹ According to a recent study, malware has grown over 500% with more than 5.49 million unique samples of malicious software in 2007.² Additionally, 2008 saw the rise of targeted attacks, which are now being designed to specifically bypass antivirus solutions.

Solid endpoint protection requires a proactive approach that is flexible enough to balance user productivity 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 malware and unknown threats while enforcing the use of authorized software. With Lumension Application Control™, which is the primary component of Lumension Endpoint Protection solution, you can centrally manage, monitor, and control applications. By employing an application whitelisting approach, you can ensure that only authorized applications can run on laptops, PCs, servers, terminal services servers, and thin clients, preventing the execution of unknown or malicious code.

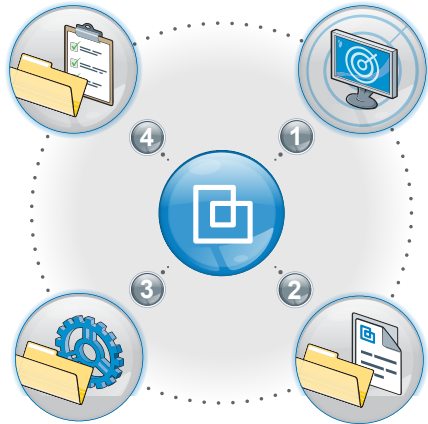
Malware only needs seconds to infect systems, far quicker than antivirus companies can release signatures. You need your mission-critical servers available 24/7. With application whitelisting in place only authorized applications can run on your servers, locking them down from threats.

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'll 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, 2008

“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:** Identify all executable files, collect profiles and organize into pre-defined file 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 legal applications can run on a computer.
- 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.
- 4. Report:** Demonstrate policy compliance and ensure software license compliance by drilling down on suspicious behavior for security or legal follow-up.

How Lumension Endpoint Protection Works

Key Benefits

- » Automates Security Enforcement
- » Saves Time and Improves Desktop and Server Management
- » Enforces Compliance in Your Organization
- » Adapts to Your Growing Business

“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.



“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.
- » Fully supports both Windows Active Directory and Novell eDirectory / NDS structure.

www.lumension.com

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

