

Lumension® Vulnerability Management



Integrated, Proactive Software Vulnerability Assessment and Patch Management

As more IT organizations are supporting heterogeneous environments with increasingly diverse operating systems and applications, they need an automated and streamlined vulnerability management solution to simplify and expedite the process. Lumension Vulnerability Management enables enterprises to effectively manage the entire vulnerability lifecycle utilizing automated vulnerability assessment, patch management and remediation.

Vulnerability Management Business Drivers and Challenges

Considering that over 90% of cyber attacks exploit known security flaws for which remediation is available¹, effective vulnerability and patch management should be on every company's to-do list. However, in today's economy, enterprises are forced to do more with less and maintain a secure IT environment while keeping operating costs low.

This creates an enormous challenge for enterprises in light of more virtualized environments, as well as an increasing number of remote employees who reduce the organization's visibility into the network and control over the devices that are brought in and out of the environment.

Additionally, IT security is under tremendous pressure to show compliance with regulatory or corporate policies as well as industry best-practices to prevent system configuration drift.

When faced with all these challenges, it is important that organizations find the right balance between effectively addressing network security and compliance concerns while keeping a low total cost of ownership (TCO).



“We can now quickly determine which machines are patched and have achieved a manageable level of automation in the application of necessary patches. We have not been subject to any major virus attacks since deploying Lumension and using its centralized management capability.

Critical patches can be quickly applied to all machines across our distributed network.”

Mike Walder, Support Consultant, East Sussex Council

Complete Vulnerability Management from Assessment to Remediation with a Single, Proven Solution

Lumension Vulnerability Management delivers automated vulnerability assessment and patch management through an integrated solution that enables you to automatically detect risks, deploy patches and defend your business information across a complex, highly-distributed physical and virtual environment with greater efficiency and minimal impact to productivity. All of these activities are seamlessly integrated into a single management console for complete visibility into your network.

Obtaining visibility into your environment and providing comprehensive reporting capabilities are of utmost importance so you can automatically identify and remediate issues and provide validation of security policies against industry standards and compliance with IT security aspects of government regulations.

The Lumension Vulnerability Management solution combines award-winning products, such as Lumension[®] Scan, Lumension[®] Patch and Remediation, Lumension[®] Security Configuration Management, and Lumension[®] Content Wizard.

1. Gartner Inc.

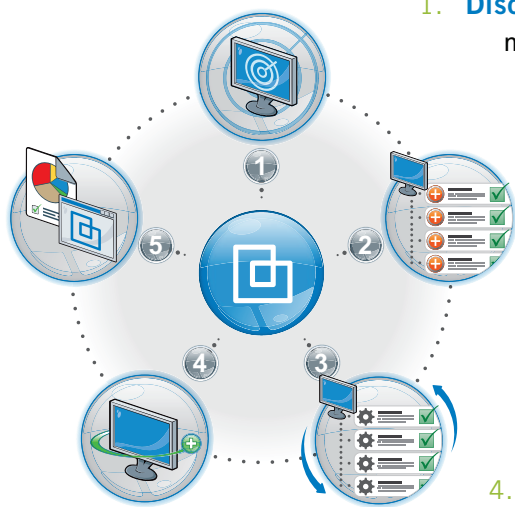
“Lumension is easy to install, use and manage, allowing us to roll out patches quickly and efficiently. It has also reduced our risk profile and enabled us to meet internal audit requirements around network security.”

Duncan Kelly, Manager Information Services,
Kingston City Council



By consolidating vulnerability data with centralized policy enforcement and compliance reporting, the Lumension Vulnerability Management solution enables you to effectively manage the entire vulnerability lifecycle and transition from a reactive security model to a proactive risk management approach:

- » Gain complete visibility of your heterogeneous network environment.
- » Proactively identify known issues before they can be exploited.
- » Focus on your most critical security risks first.
- » Automatically deploy patches to an entire network.
- » Gain a holistic view your environmental risk.



- 1. Discover:** Uncover all of your IT assets, both managed and unmanaged, through in-depth scans and flexible grouping and classification options.
- 2. Assess:** Identify all of your endpoints for OS, application and security configuration vulnerabilities via network and agent-based scanners.
- 3. Prioritize:** Rank vulnerabilities by severity or organizational impact.
- 4. Remediate:** Continuously monitor, detect and enforce patch management and remediation policies across all major platforms and applications.
- 5. Report:** Leverage a full range of operational and management reports that consolidate discovery, assessment and remediation information in a single management console.

How Lumension Vulnerability Management Works

Key Benefits

- » Delivers Full Network Visibility
- » Reduces Endpoint Risk
- » Reduces Operational Expenses and TCO
- » Provides Holistic View of Environmental Risk

“Patching is a huge part of our security strategy. We need to control the patching for our environment, rather than turn on Windows Update for all of our computers, because we have a lot of applications that have dependencies on each other. Before deploying patches, we need to run a test to make sure they won’t affect our core systems. Lumension allows us to do this very effectively.”

Tony Hildesheim, Vice President of IT, WESCU

Take Control of Your Vulnerability Management

Ensure a streamlined vulnerability management process that mitigates your critical risks. Contact your local Lumension sales representative or reseller today or visit us at www.lumension.com.



“Managing a diverse network environment across 20 different locations is no longer a full-time job for our IT staff as Lumension has been instrumental in mitigating risks and relieving IT security pain. It is a robust solution that delivers high performance, thorough assessment, remediation and continuous monitoring to ensure it works around the clock to secure our network without disrupting our computing environment.”

Jim Czyzewski - Sr. Info. Systems Specialist, MidMichigan Medical Center

Key Features

- » Provides visibility into the entire network environment, including virtual machines.
- » Thorough and accurate discovery of network assets via both network and agent-based scans.
- » Proactively identifies known software and security configuration vulnerabilities before they can be exploited.
- » Automatically deploys patches to an entire network and enables custom patch development and deployment.
- » Provides regulatory and industry-best practices reporting templates to demonstrate compliance against established regulatory standards with both out-of-the-box and customizable queries.
- » Offers a single, scalable solution to patch and remediate a heterogeneous network; i.e. Windows, Linux, Unix, and Mac.
- » Provides composite reports aggregating discovery, assessment and remediation results to provide a more complete view of the environment.
- » Delivers Security Content Automation Protocol (SCAP) validated configuration assessments.
- » Identifies high-risk vulnerabilities that are not patch-related.

www.lumension.com

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

Online Resources

- » [FREE TRIAL](#)
- » [Patch Tuesday Blog](#)
- » [Vulnerability Management Blog](#)
- » [Vulnerability Scanner](#)
- » [Automating the Vulnerability Management Lifecycle](#)
- » [Webcast - Staying Ahead of Threats](#)
- » [Podcast: How Shiseido Enforces an Always-on Security Posture](#)
- » [Ogren Group Security Business Analysis - Lumension: a Case Study in Proactively Managing Endpoint Risk](#)
- » [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
- » 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

 **Lumension**
IT Secured. Success Optimized.™

LVM-SB-EN-04-26-10