

Lumension Patch and Remediation™ (FORMERLY PATCHLINK)

Identify and Patch Software Security Vulnerabilities and Prevent Configuration Drift

IT administrators can't possibly stay updated on and implement the flood of software vulnerability patches consistently released by all the vendors used in their heterogeneous environments. With software companies shortening software and OS lifecycles and releasing software prematurely, the number of bugs and design flaws is growing exponentially – on average, 19 new vulnerabilities are released per day.¹

Rapid, Accurate and Secure Patch Management

Today's IT departments are busy, spending the majority of their time fixing virus-infected user desktops and reactively fighting malware attacks, rather than proactively securing the organization's network and preventing security vulnerabilities from being exploited.

One recent virus attack was followed up with 6,000 different variations in just one night, but a patch for the underlying vulnerability had been available for a month. Add to that the proliferation of Web 2.0, social networking, and virtual environments creating new avenues to introduce malware into the workplace.

Lumension Patch and Remediation streamlines and automates the patch management process in even the most complex, heterogeneous environments. Through proactive alerting on issues, you can address them immediately.

Lumension Patch and Remediation provides:

- » Rapid, accurate and secure patch management
- » Automated collection, analysis and delivery of patches
- » Security for your organization from worms, Trojans, viruses and other malicious threats
- » Single consolidated solution for heterogeneous environments provides effective management at a significantly reduced TCO

Key Features

- » Comprehensive Assessment of IT Assets
- » Open Architecture to Support Complex Environment
- » Supports Heterogeneous Environments
- » Rapid, Automated Patch Deployment
- » NAC Support
- » Automatic Notifications
- » Highly Scalable
- » Multi-Patch Deployments
- » Flexible Reporting
- » Role and Policy-based Administration

Datasheet

Key Benefits

- » Enables You to Stay Ahead of Remote Threats
- » Streamlines Patch Management Across Heterogeneous Environments
- » Provides Visibility into Real-Time Patch Status and Overall Security Posture
- » Reduces TCO by Saving IT Operations Time and Effort

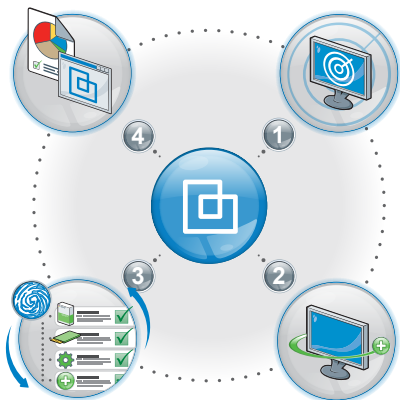
"We can now quickly determine which machines are patched and have achieved a manageable level of automation in the application of necessary patches. We have not been subject to any major virus attacks since deploying Lumension and using its centralized management capability. Critical patches can be quickly applied to all machines across our distributed network".

**Mike Walder, Support Consultant,
East Sussex Council**



1) National Vulnerability database, March 2009

How Lumension Patch and Remediation Works



1. **Discover** - application, operating system and configuration vulnerabilities on managed endpoints through comprehensive agent-based scan.
2. **Remediate** - vulnerabilities and rapidly deploy patches based on defined policies.
3. **Profile** - for every patch is created including software, hardware, drivers and existing and missing patches for each machine.
4. **Report** - on operational, management and compliance initiatives.

Key Features

Comprehensive Assessment of IT Assets: Provides comprehensive understanding of security posture for inventory and management of both physical and virtual environments via in-depth assessment of vulnerabilities, patch status, security configurations, installed software, and hardware inventory.

Open Architecture: Supporting open standards and multiple sources of content, Lumension Patch and Remediation delivers a customizable and diverse platform for operational security management.

Supports Heterogeneous Environments: Vulnerability audits and remediation with wide support across major OS platforms (Windows, Linux, MacOS, Sun Solaris, HP, etc.), POSIX and infrastructure devices - all from one single console.

Multi-Patch Deployments: Delivers multiple patches to multiple computers in one distribution.

Automatic Notifications: E-mail alerts can be sent to administrators to notify them of a variety of issues, including subscription or remediation failures and upcoming license expiration.

Comprehensive Remediation Actions: Vulnerability audits include security configurations, OS and application vulnerabilities, null passwords, patch-level related vulnerabilities, known hacking tools, malware, common worms, and P2P software checks.

Flexible Reporting: More than 20 reports that provide detailed information the patch and remediation management process, including agent policy status, vulnerability deployments, asset inventory and more.

Highly Scalable: Complete coverage for the largest worldwide networks with high-availability topologies and distribution point architecture. Packages are cached locally, minimizing network traffic and optimizing bandwidth utilization.

Role- and Policy-based Administration: Ensures that all your systems meet a mandatory baseline policy – a key aspect of corporate security and regulatory compliance.

NAC Support: Automatically assess endpoints as they attempt to gain access to the network and remediate to a compliant state before access is allowed.

System Requirements

- » **Server:** Windows Server 2003 with Microsoft SQL Server 2005 and .NET Framework, 2008
- » **Agent Coverage:** Apple Mac OS X, Hewlett Packard HP-UX, IBM AIX, Novell SUSE Linux, RHEL, Sun Solaris, Windows: 98, NT, 2000, XP, Vista, Windows Server: 2003, 2008

Other Lumension Products

- » Lumension Device Control
- » Lumension Application Control
- » Lumension Patch & Remediation
- » Lumension Scan
- » Lumension Vulnerability Management
- » Lumension Enterprise Reporting
- » Lumension NAC Integrator



www.lumension.com

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

