Lumension® Endpoint Management and Security Suite

Patch and Remediation

Datasheet

Effectively Manage the Changing IT Environment

As IT environments have become increasingly complex, supporting virtual and distributed platforms, companies must ensure that they maintain control of their information and systems management. IT organizations often manage multiple point-based technologies, which add complexity and cost. A new approach is required to simplify the IT environment and ensure enhanced security and IT risk management with the lowest total cost of ownership possible.

Lumension® Endpoint Management and Security Suite delivers an end-to-end suite of solution capabilities across endpoint operations, security, compliance and IT risk management to reduce complexity, optimize TCO, improve visibility and deliver control back to IT.

Rapid, Accurate and Secure Patch and Remediation Management

To effectively reduce your threat exposure from the flood of software vulnerabilities and mis-configurations, rapid, accurate and secure patch management is critical. 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]

Today's IT departments are often expending resources reacting to poorly managed systems and security incidents, rather than effectively securing and maintaining endpoints to prevent security vulnerabilities from being exploited.

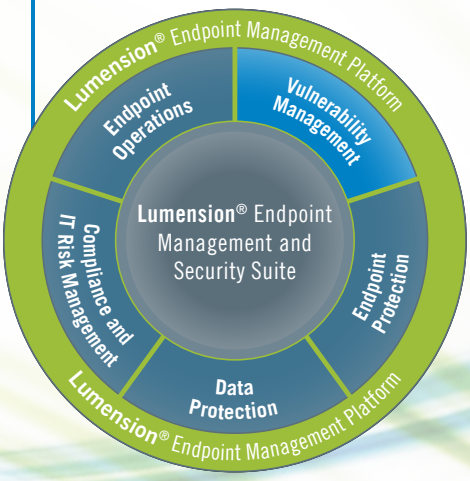
Lumension® Patch and Remediation provides:

- A single, intuitive management console for easy patch and remediation administration across multiple platforms, including Windows, Unix, Linux and Mac OS, as well as many applications
- Enhanced asset discovery for full network visibility and continuous control across both physical and virtual environments
- Automated policy baselines to ensure that patches, configurations, remediations, and other tasks are continuously enforced
- Extensibility and customization via *Lumension*® Content Wizard including power policy management, software deployment and removal, desktop configuration templates and custom task scripting
- Enhanced Wake-on-LAN to provide complete visibility and control over powered down systems and ensure that critical patches and software updates are successfully deployed
- Integration with Network Access Control (NAC) solutions to remediate 'non-compliant' machines to a compliant state before gaining access to the network

Key Benefits

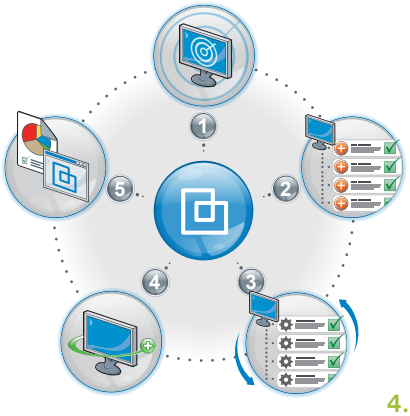
- Elevate Security Posture and Proactively Reduce Risk
- Save Time and Cost Through Automation
- Visibility and Control of All Endpoints Whether Online or Offline
- Comprehensive Support for OS and Third Party Applications
- Streamline and Centralize Management of Heterogeneous Environments
- Improve Operational Efficiency While Reducing Energy Consumption
- Extensible and Customized Scripting

"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 :** Gain complete visibility of your heterogeneous network environment. Proactively discover all of your IT assets, both managed and unmanaged, through in-depth scans and flexible grouping and classification options.
2. **Assess:** Proactively identify known issues before they can be exploited. Perform a deep analysis and thorough OS, application, and security configuration vulnerability assessments.
3. **Prioritize:** Focus on your most critical security risks first.
4. **Remediate:** Automatically deploy patches to an entire network. Simplify the process of maintaining a secure environment by continuously monitoring, detecting and remediating policy-driven environments across all major platforms and applications.
5. **Report:** Gain a holistic view your environmental risk. Access a full range of operational and management reports that consolidate discovery, assessment, and remediation information on a single management console.

Key Features

Integrated Endpoint Management Console: Features web-, role- and workflow-based navigation and seamlessly integrates with other LEMSS product modules to simplify and optimize endpoint operations.

Automated Discovery and Assessment of IT Assets: Provides inventory and management of both physical and virtual environments via in-depth assessment of vulnerabilities, patch status, security configurations, installed software and managed and unmanaged hardware inventory.

Enhanced Wake-on-LAN: Eliminates blind spots in ongoing network maintenance and ensures that offline machines receive critical patches and software updates. Increased energy efficiency is achieved when combined with power policy distribution via Lumension Content Wizard.

Highly Scalable for Distributed Environments: Delivers complete coverage for the largest worldwide networks with high-availability topologies.

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

Single Solution for Heterogeneous Environments: Vulnerability audits and remediation with wide support across major OS platforms (Windows – including Windows 7 and Server 2008 R2, Linux, MacOS, Sun Solaris, HP, etc.), POSIX and infrastructure devices — all from one console.

Diverse, Flexible Reporting: Provides detailed information across the patch and remediation management process, including agent policy status, vulnerability deployments, asset inventory and more.

Comprehensive Patch, Remediation, and Configuration Capabilities: Assessments include security configurations, OS, application and patch-level related vulnerabilities, null passwords, known hacking tools, malware, common worms, and P2P software checks.

Continuous Policy Enforcement: Automatically enforces patches, configurations, remediations and other custom and repetitive tasks. Baseline policies can be easily exported and applied across multiple groups and servers for consistency.

Single Infrastructure: Delivers a customizable and diverse platform for operational security management, supporting open standards and multiple sources of content.

System Requirements

- **Server**: Windows Server 2003, 2008 or 2008 R2 with Microsoft SQL Server 2005 or 2008 and .NET Framework
- **Agent Coverage**: Apple Mac OS X, CentOS, Hewlett Packard HP-UX, IBM AIX, Novell SUSE Linux, Oracle Enterprise Linux, RHEL, Sun Solaris, Windows: 2000, XP, Vista, 7, Windows Server: 2003, 2008, 2008 R2

Complete Requirements

Online Resources

- FREE TRIAL
- Patch Tuesday Blog
- Vulnerability Mgmt. Blog
- Vulnerability Scanner
- Automating the Vulnerability Management Lifecycle

OTIKA

OTIKA
Phone: 01 71 11 31 45
lumension@otika.fr
www.otika.fr

Lumension
IT Secured. Success Optimized.™