

Security Configuration Management

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

Assess and Manage Endpoint Security Configurations

Proactively monitoring configurations is just as important as the need to rapidly apply critical patches because 60 percent of all exploited vulnerabilities are due to insecure configurations.¹ Lumension® Security Configuration Management ensures that endpoints are securely configured and in compliance with industry best practices and regulatory standards. A NIST validated solution, Lumension Security Configuration Management provides continuous assessment of policy templates including Microsoft Windows Security Guides, NIST Special Publication 800-68, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), National Security Agency (NSA) and Office of Management and Budget (OMB) Federal Desktop Core Configurations (FDCC).

Lumension Security Configuration Management provides:

- » Management of security configuration baselines for workstations, servers, and mobile laptops from a single point of control
- » Continuous and proactive assessment to prevent configuration drift and ensure policy compliance
- » Out-of-the-box regulatory and industry standards-based configuration templates
- » Identification of configuration-based risk through monitoring and reporting on systems that are non-compliant
- » A NIST-validated solution

Key Features

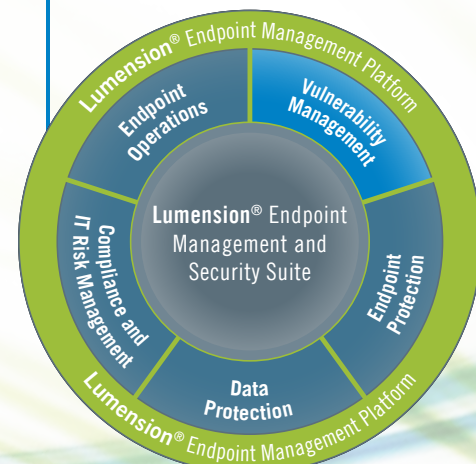
- » Security Configuration Management
- » Out-of-the-box Checklist Templates
- » NIST Validated Solution
- » Continuous Policy Assessment and Enforcement
- » Integrated Lumension Endpoint Management and Security Suite Module
- » Based on Open Standards for Easy Customization
- » Security Configuration and Posture Reporting

Key Benefits

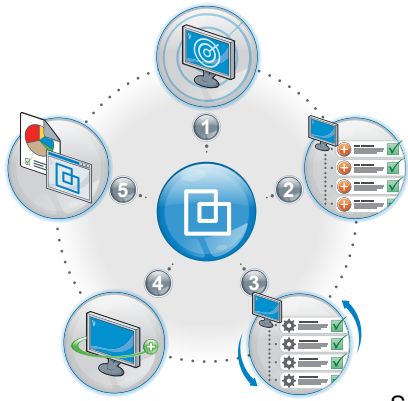
- » Ensures Compliance and Audit-Readiness
- » Increases Visibility of Security Posture
- » Reduces Configuration Drift
- » Demonstrates Continuous Compliance Through Automatic Policy Enforcement

“Lumension gives us a more security-centric view of the network, allowing us to gain greater insight into the network and a better overall view into the system. We are able to more rapidly adjust to changes in the business, making our IT operation much more proactive and flexible, and therefore more productive”.

Anthony Sica, Executive Director of IT, Shiseido



How Lumension Security Configuration Management 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 security configuration issues against best practice and standards based policies including Microsoft Windows Security Guides, NIST Special Publication 800-68, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), National Security Agency (NSA) and Office of Management and Budget (OMB) Federal Desktop Core Configurations (FDCC).

- 3. Prioritize:** Focus on your most critical security risks first.
- 4. Remediate:** Create automated policy baselines that 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 of your security configuration policy violations. Access a full range of operational and management reports that consolidate discovery, assessment, and remediation information on a single management console.

Key Features

Security Configuration Management: Ensures that endpoint operating systems and applications are securely configured and in compliance with industry best practices and regulatory standards.

Out-of-the-box Checklist Templates: Microsoft Windows Security Guides, NIST Special Publication 800-68, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), National Security Agency (NSA) and Office of Management and Budget (OMB) Federal Desktop Core Configurations (FDCC).

NIST-Validated for Accuracy: NIST validation ensures accurate assessments of policy checklists and configurations as defined in the National Vulnerability Database.

Continuous Policy Assessment and Enforcement: Delivers ongoing and flexible mechanism to assess and apply appropriate policies to applicable systems with Lumension® Content Wizard.

Fully Customizable: Open standards implementation ensures policy management via an extendable and customizable architecture providing the ability to add, create, define, edit and import/export security configuration policies and checklists based on industry standards in an easy-to-edit XML format.

Integrated LEMSS Module: Centrally managed through the Lumension Endpoint Management and Security Suite for improved visibility and reduced complexity.

Security Configuration and Posture Reporting: Automates security checks including event log policy settings, file permission settings, local policies group, system services group, network settings, system settings, windows components, local user policy setting, security patches, firewall settings, IE settings application settings.

System Requirements

Lumension® Patch and Remediation

- » **Server:** Windows Server 2003, 2008
- » **Agent Coverage:** Windows 7, Vista, XP, Windows Server: 2008 R2, 2008, 2003

[Complete Requirements](#)

Online Resources

- » [FREE TRIAL](#)
- » [Vulnerability Mgmt. Blog](#)
- » [Vulnerability Scanner](#)
- » [Automating the Vulnerability Management Lifecycle](#)
- » [FDCC – Achieving Compliance with the Lowest Total Cost of Ownership](#)

OTIKA

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

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