Lumension® Endpoint Management and Security Suite

Security Configuration Management

Lumension
IT Secured. Success Optimized.™

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.

Assess and Manage Endpoint Security Configurations

Proactively managing configurations is as critical to endpoint security as staying on top of your critical patches because, as data from Verizon DBIRs over the years has strongly suggested, poor configuration management and poor control over default settings, upgrades and general system hardening factor in most data breaches.

Introducing *Lumension*® Security Configuration Management

Lumension® Security Configuration Management, available as a modular offering on *Lumension*® Endpoint Management and Security Suite, 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 the United States Government Configuration Baseline (USGCB).

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 supporting all tier IV checklists for Windows endpoints

Key Benefits

- Increases Visibility into Security Posture
- Reduces Configuration Drift
- Ensures Continuous Compliance via Automatic Policy Enforcement
- Improves Audit Readiness
- Integrates with Endpoint Operational and Security Modules for Defense-in-Depth

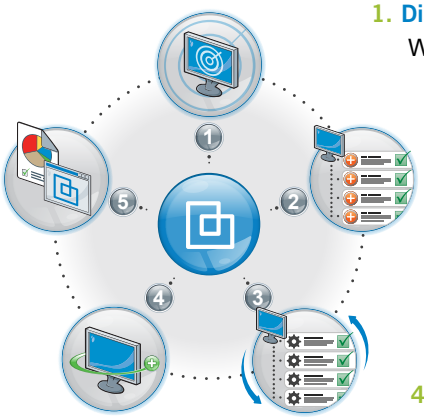
Key Features

- Security Configuration Management
- Out-of-the-Box Checklist Templates
- NIST Validated Solution
- Continuous Policy Assessment and Enforcement
- Based on Open Standards for Easy Customization
- Security Configuration and Posture Reporting

"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 configurations in your Windows 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 all tier IV checklists for Windows endpoints.
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.

System Requirements

Visit lumension.com for the latest product details and information.

Online Resources

- FREE TRIAL
- Vulnerability Mgmt. Blog
- *Lumension*® Application Scanner Tool
- Automating the Vulnerability Management Lifecycle Whitepaper

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 the United States Government Configuration Baseline (USGCB).

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 iimplementation 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.

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.

Integration with *Lumension*® Endpoint Management and Security Suite:

Integrates with other Lumension product modules to streamline and improve IT operations and security, reduce agent bloat and improve endpoint visibility.