

PatchLink Security Configuration Management™



Sixty five percent of threats exploit improperly configured endpoints¹, which drift out of compliance over time primarily because of changes made by employees within the firewall². According to the SANS Institute's best practices for preventing top 20 risks³, organizations should:

- ☑ Configure systems, from the first day, with the most secure configuration that your business functionality will allow, and use automation to keep users from installing/uninstalling software.
- ☑ Use automation to make sure systems maintain their secure configuration, remain fully patched with the latest version of the software (including keeping anti-virus software up to date)

To put an end to threats associated with mis-configured endpoints, Lumension Security™ - PatchLink Security Configuration Management™ provides out-of-the-box regulatory, standards-based assessment and industry best practices templates to ensure endpoints and applications are properly configured.

Advanced Secure Configuration and Policy Management

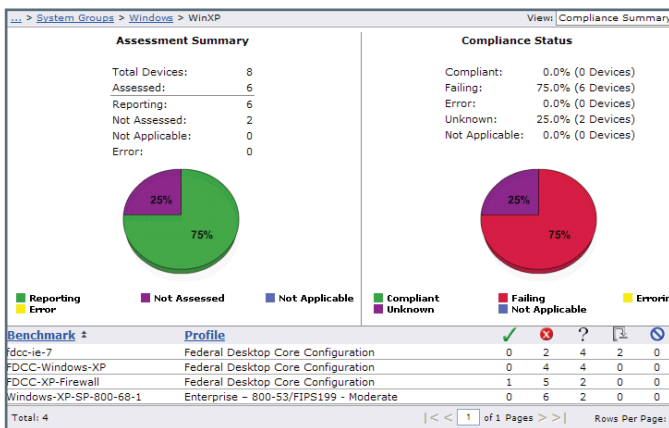
PatchLink Security Configuration Management™ seamlessly integrates with its proven, market leading solutions, PatchLink Scan and PatchLink Update, to deliver a comprehensive network and agent-based risk assessment of software flaws and configuration vulnerabilities, rapid remediation, continuous validation and policy compliance reporting.

Eliminate Endpoint Risk

Through proactive and automated configuration issue identification and correction, PatchLink Security Configuration Management™ ensures that corporate endpoints do not drift out of compliance over time. Continuous assessment, monitoring and reporting of security configuration policies eliminates the largest source of risk at the endpoint.

Simplify Regulatory or Policy Compliance

PatchLink Security Configuration Management™ leverages best practices templates from leading security think tanks such as the National Institute of Standards and Technology (NIST), which developed the Security Content Automation Protocol (SCAP), a repository of security content to help automate and standardize technical control compliance activities, vulnerability checks of both application mis-configurations and software flaws, and security measurement. SCAP security checklists are available in a standard eXtensible Markup Language format that PatchLink Security Configuration Management™ is able to import to help build, operate, measure and maintain secure systems according to official government security recommendations or specific industry security standards such as FDCC or PCI DSS.



PatchLink Security Configuration Management Compliance Dashboard

Features & Benefits

- ☑ **Open, Standards-Based Approach:** Leverages security best practices to ensure secure configurations
- ☑ **Actionable Information:** Consolidates content from variety of sources and delivers information with context to properly remediate
- ☑ **Policy Management:** Define, edit and import/export security configuration policies
- ☑ **Policy Assessment:** Flexible mechanism to assess and apply appropriate policies to applicable systems
- ☑ **Policy Compliance:** Reports configuration compliance against policy
- ☑ **Policy Enforcement:** Rapid remediation of configuration issues
- ☑ **Centralized User Interface:** Technical controls and asset entities are consolidated into a single UI
- ☑ **Consolidated Architecture:** Comprehensive approach within one architecture and framework for securing the endpoint

Reduce IT Operations and Support Costs

By managing all vulnerability activities from one single solution, PatchLink Security Configuration Management™ enables organizations to improve their endpoint security and network performance, while lowering operational and support costs. Leveraging SCAP content as well as both agent and network-based scanning technology to automate the management of security configurations, PatchLink Security Configuration Management™ eliminates the need to manage and interpret a wide range of results from non-integrated scanners and agents.

1. John Pescatore, Vice President, Gartner Inc.
2. Khalid Kark, senior analyst, Forrester Research Inc. as reported by Robert Westervelt, News Editor, SearchSecurity.com "Compliance drives security configuration management", 25 Apr 2007
3. <http://www.sans.org/top20/>

Secure Endpoint Configurations from Internal Threats

Enterprise endpoints are targeted by threats from within the corporate walls, whether users' configuration changes are inadvertent or on purpose. PatchLink Security Configuration Management™ mitigates risk from a variety of internal threats including:

- ▣ **Boot Process** - An unauthorized individual boots a computer from third-party media (e.g., removable drives, USB token storage devices), which could permit an attacker to circumvent operating system security measures and gain unauthorized access to information. PatchLink Security Configuration Management™ controls include hard drive encryption, device control and a physical security interview.
- ▣ **Unauthorized Local Access** - An individual who is not permitted to access a system gains local access. PatchLink Security Configuration Management™ controls include logon banners, auto logoff, screen saver password, strong passwords and device control.
- ▣ **Privilege Escalation** - An authorized user with normal user-level rights escalates the account's privileges to gain administrator-level access. PatchLink Security Configuration Management™ controls include the ability to restrict access to all administrator-level accounts and administrative tools, configuration files, and settings, disable unnecessary services and install critical patches.

Secure Endpoint Configurations from External Threats

External threats target vulnerable endpoints that are not configured properly. PatchLink Security Configuration Management™ mitigates external threats that target vulnerabilities such as:

- ▣ **Network Services** - Remote attackers exploit vulnerable network services on a system, including gaining unauthorized access to services and data, and causing a denial of service (DoS) condition. PatchLink Security Configuration Management™ controls include disabling unused services, installing patches, using strong authentication, enforcing password policies, and configuring firewalls.
- ▣ **Data Disclosure** - A third party intercepts confidential data sent over a network. PatchLink Security Configuration Management™ controls include using switched networks, deploying CMF/DLP technologies, using a secure user identification and authentication system (NLTmV2, Kerberos) and encrypting network communications.

How It Works and What It Can Monitor

Policy Import

Import of policy standards according to SCAP checklists (e.g. FDCC).

Automated Assessment

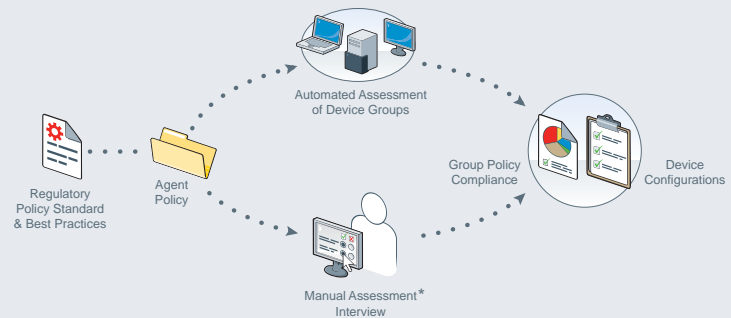
Used with PatchLink Update™ or PatchLink Scan™, automated assessment against the checklist is performed.

Manual Assessment*

In order to be exhaustive, manual assessment interview allows the mapping of non-IT automated security checks such as physical security checks.

Policy Compliance Management & Reporting

Both automated assessment and manual assessment interview checks are consolidated to provide a comprehensive compliance monitoring and reporting tools



- ▣ Event Log Policy Settings
- ▣ File Permission Settings
- ▣ Local policies Group
- ▣ System Services Group
- ▣ Network Settings
- ▣ System Settings

- ▣ Windows Components
- ▣ Local User Policy Settings
- ▣ Security Patches
- ▣ Firewall Settings
- ▣ IE Settings
- ▣ Application Settings

Assess Your Endpoint Configurations Today

With PatchLink Security Configuration Management™, you can proactively assess endpoint configurations using a best practices approach. For more information on a free 30-day evaluation of PatchLink Security Configuration Management™ visit us on the web at www.lumension.com/scm.

*: available in next PatchLink Security Configuration Management™ release



Lumension Security
15880 North Greenway Hayden Loop
Suite 100
Scottsdale, AZ 85260
United States of America
+1 480 970 10250 / www.lumension.com



©2008 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.