

SANS Top 20 Internet Security Risks of 2007 highlights critical vulnerabilities in software on personal computers inside and outside enterprises as a major risk that is frequently targeted by financially motivated hackers. To prevent such risk, SANS suggests using “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).”

Lumension's PatchLink Update, ranked the #1 patch management solution by market share by IDC for the past three years, enables your customers to streamline their security updates (patches and hot fixes) for the software they currently license from your organization. By enabling the automation of the enterprise patch management process, PatchLink Update ensures that your customers are compliant with the latest version of licensed software and that their system configurations are maintained.

With PatchLink Update, organizations have the ability to rapidly respond to security and operational vulnerabilities, across all platforms and applications anywhere in the world – ultimately ensuring the enforcement of their desired security postures and configurations.

“Before PatchLink Update, securing our mobile devices was an organized free-for-all. Without a centralized patching process, we couldn't keep up with vulnerability patching and software upgrades. Now we have comprehensive, automated vulnerability management for our very mobile organization.”

BRIAN OSWALD, BOOZ ALLEN HAMILTON

What is the ISV Security Patch Management Compliance Program?

Lumension Security, the worldwide leader in Unified Protection and Control solutions, including the #1 ranked PatchLink Update, is working with all major software manufacturers to securely and rapidly deliver content updates to licensed customers. Software manufacturers play an integral role in this process, providing the content of these security updates. Lumension Security aims to leverage these content updates to streamline enterprises' overall patch management and remediation process.

Top 5 Benefits to ISV

By utilizing Lumension Security as your enterprise patch distributor, you can:

- 1. Enhance Corporate and Product Brand Reputation**
By empowering your customers to comply with security policies through enterprise-wide vulnerability assessment and remediation capabilities, you will add significant value on top of the software that you develop and further enhance your reputation as a market leader.
- 2. Achieve Higher Level of Customer Satisfaction**
By providing content directly to Lumension's PatchLink Update, you will simplify your customers' enterprise patch management process and ensure that your software remains up-to-date.
- 3. Streamline and Reduce Support Costs**
By ensuring that your software's digital signature is the same as what was installed on your customers' systems, you will ensure secure delivery and ensure that customers are running updated software – and thus receive fewer support calls and issues.
- 4. Ensure License Compliance Validation**
By utilizing Lumension Security as the delivery and enforcement mechanism of your critical patches, you can ensure that your customers are complying with their license agreements.
- 5. Minimize Bandwidth on Patch Deployment Servers**
By giving Lumension Security distribution rights, you will reduce bandwidth on your patch deployment servers – Lumension will pull the patch once and securely and rapidly distribute to all appropriate parties instead of all licensed customers pulling updated content from your servers individually.

Top 5 Benefits to ISV's Customers

- 1. Automatic Software Vulnerability Detection**
PatchLink Update proactively detects and assesses application vulnerabilities on corporate endpoints.
- 2. Additional Vulnerability Testing**
Lumension vulnerability experts add another layer of vulnerability testing before the rapid and secure delivery of content updates.
- 3. Streamlined Patch and Remediation Process**
PatchLink Update provides one-stop shopping for all patch and remediation requirements, with support for all major operating systems, software applications and operational vulnerabilities, and with automated deployments based upon patch criticalities and defined security policies.
- 4. Intelligent, Secure Patch Deployments**
Rapidly deploy any of the 15,000+ patches in the world's largest repository of security content via a 128-bit encrypted VERISIGN trusted connection along with RSA BSAFE® encryption, with advanced capabilities designed to reduce administrative effort and limit end-user disruptions.
- 5. Continuous Validation of Policy Compliance**
Monitor and report the vulnerability and patch status of each managed endpoint, with automatic e-mail alerts for new updates and failed deployments.

Simplifying the Patch Process to Minimize Vulnerability Exposure and Reduce Costs

By consolidating patch and vulnerability information and automating the patch and security configuration process, PatchLink Update enables organizations to:

- ☐ Simplify management of the remediation process
- ☐ Minimize overall endpoint risk through immediate discovery of enterprise assets and security risks and enforcement of security and operational patches
- ☐ Reduce the cost and time required between the detection and remediation of security and operational vulnerabilities
- ☐ Demonstrate compliance with security policies and government regulations through comprehensive auditing and reporting of security and operational patch compliance

How It Works:

Vulnerability Detection and Assessment

PatchLink Update proactively detects and assesses application, operating system and operational vulnerabilities on corporate endpoints.

Remediation Policies Defined

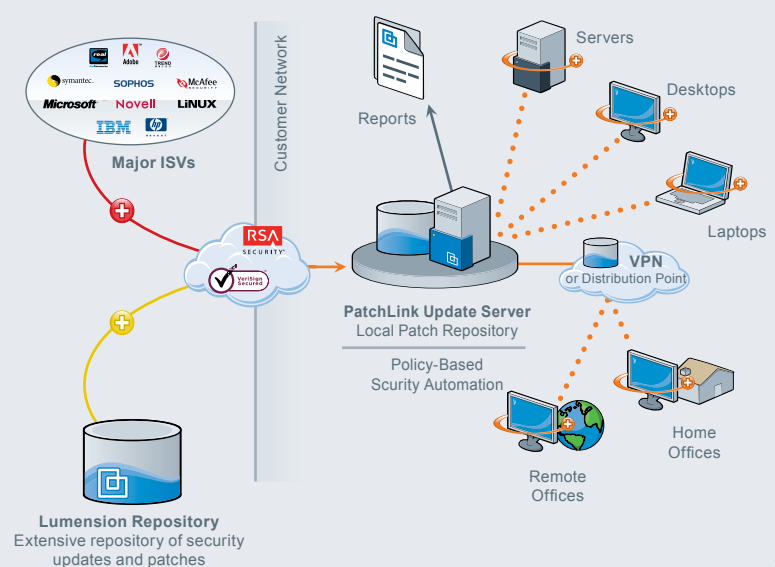
Enterprise-wide change management policies are established around the remediation of security and operational vulnerabilities.

Automated Patch Deployment and Remediation

Automated deployments are scheduled based upon patch criticalities and defined security policies.

Comprehensive Reporting

Each endpoint is continuously monitored and all vulnerabilities are accounted for per machine in terms of what was detected, the criticality of that vulnerability, and when remediation occurred, as well as the current status of the machine.



How to Participate

To participate in Lumension's ISV Security Patch Management Compliance Program and deliver additional value to your organization and your customers, contact the Lumension Security Business Development team at BusinessDevelopment@Lumension.com.



Lumension Security

15880 N Greenway-Hayden Loop, Suite 100 / Scottsdale, AZ 85260 / 480.970.1025 / www.lumension.com

© Copyright, 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.