

Say Goodbye to **INEFFECTIVE PATCHING**

Reduce Your Risk With Automated Patch
Management and Remediation



Patch Management and Remediation Solution

With major software vendors now reporting more than 8,000 software vulnerabilities¹ each year, eradicating all of the potential threats to your network endpoints is a daunting task. Not to mention the rising amount of threats that attack system configurations.

Fortunately, there is a way. Lumension Security's Patch Management and Remediation Solution allows you to automate the collection, assessment and deployment of software patches and to create and deploy remediation packages that address a wide range of configuration-related issues. This comprehensive solution significantly streamlines the patch management process and adds custom capabilities to address configuration issues, ultimately reducing the incidents of worms, trojans, viruses and targeted malicious attacks.

Lumension's Patch Management and Remediation Solution is comprised of three market-leading security products; PatchLink Update™, PatchLink Developers Kit™ and the PatchLink Security Management Console™. These three products work together seamlessly to:

- ▣ Identify all endpoints (including rogues) and propagate remediation agents
- ▣ Perform detailed agent-based scans for complete vulnerability and patch level status
- ▣ Automate threat remediation with an extensive patch repository covering major operating systems and applications
- ▣ Deliver ongoing patch monitoring and comprehensive reports of patch activity
- ▣ Enforce configuration policies such as closing down vulnerable ports, shutting down dangerous services, identifying and removing unauthorized or expired files and applications, enforcing password policies and registry settings, and much more
- ▣ Respond to zero-day threats even when vendor patches do not exist
- ▣ Develop custom patches for home-grown applications, or legacy software that is no longer supported by the manufacturer

Solution Overview

Protects endpoints from numerous software vulnerabilities and configuration issues through the rapid assessment, testing and deployment of patches and remediation packages.

▣ Thorough discovery and assessment of endpoints providing detailed information on vulnerability and patch level status

▣ Rapid threat remediation through deployment of pre-tested vendor patches and custom configuration packages

▣ Centralized administration of security policies across your network

Mounting Vulnerabilities and Configuration Issues

Protecting against the barrage of security threats, malicious attacks and configuration vulnerabilities threatening the stability of your systems are critical and time-consuming tasks. If left unmanaged, all of these threats can make your systems vulnerable to exploits.

As the window of time between vulnerabilities discovered and exploits launched continues to shrink, the biggest challenge for many organizations is remediating these before an exploit occurs. In fact, 12.5 vulnerabilities are considered serious enough for IT staff to address each day 2. Endpoint configurations also drift out of compliance on a regular basis due to security threats and typical end-user activity, such as loading new drivers onto a machine.

Over 90 percent of cyber attacks exploit known security flaws for which a remediation is available 3. Endpoints must be continuously monitored because even if the software or configuration vulnerability is remediated today, the same one may need to be re-addressed tomorrow.

Automating this time-consuming process can significantly decrease the costs and time involved in securing an organization from threats and meeting internal policy and regulatory compliance requirements. You can protect your enterprise systems and servers with strong patch and remediation enforcement capabilities that enable you to keep your enterprise running effectively.

Proven Remediation of Vulnerabilities

Lumension is the worldwide leading provider of patch management and remediation solutions 4, with patented fingerprinting technology, which ensures the highest level of accuracy in the detection of security vulnerabilities.

Centralized Management and Reporting

With PatchLink Security Management Console™

Intelligent Remediation and Validation

With PatchLink Update™ and PatchLink Developers Kit™

Lumension Patch and Remediation Solution

Centralized Management and Reporting

PatchLink Security Management Console™

Intelligent Remediation and Validation

PatchLink Update™

PatchLink Developers Kit™

How It Works

1. Patch Acquisition

Lumension proactively downloads patches from major software vendors and tests patches on their applicable operating systems and languages

2. PatchLink Secure Patch Delivery

Patches are packaged with our patented Digital Fingerprint technology, added to our repository and securely distributed to your local Patch and Remediation Solution server via a 128-bit encrypted VERISIGN trusted connection along with RSA BSAFE® encryption

3. Vulnerability Assessment and Remediation

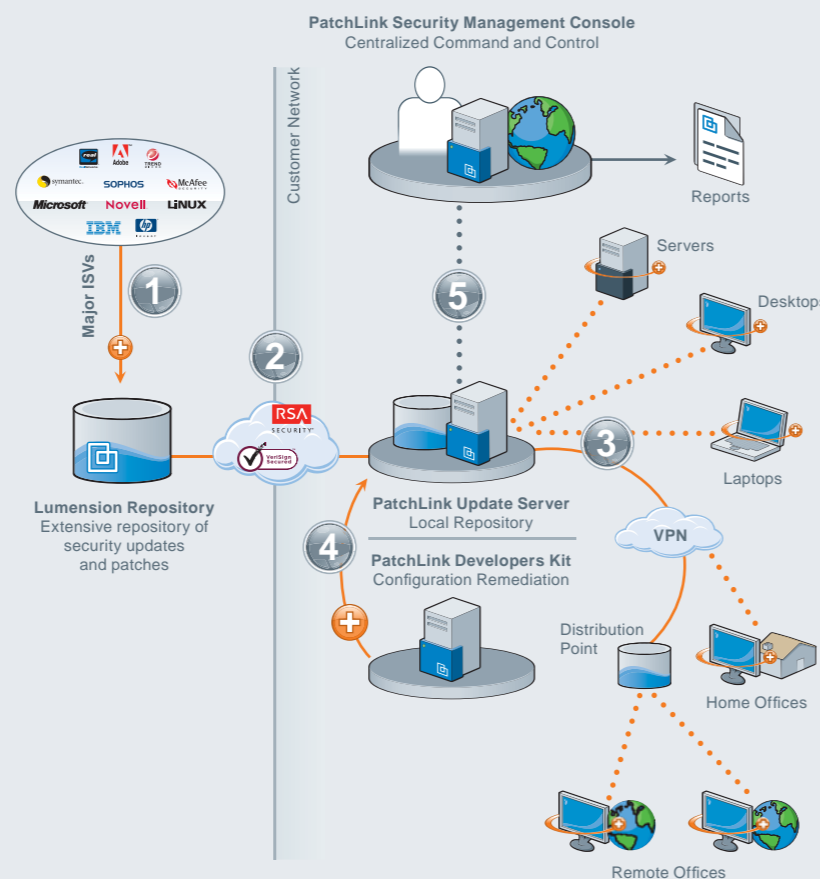
PatchLink Update™ agents detect inventory and vulnerability status for all managed endpoints on scheduled intervals and sends information to the PatchLink Security Management Console™

4. Configuration Remediation

PatchLink Developers Kit™ works in conjunction with PatchLink Update™ to create and deploy remediation packages that address a wide range of configuration issues

5. Centralized Command and Control

Administrator(s) control the entire patch assessment, analysis, remediation and reporting process from a central PatchLink Security Management Console™



Rapid Identification of Unprotected Endpoints

With the dynamic nature of today's business environment, it is imperative that all of your machines are protected, all of the time. Lumension's Patch Management and Remediation Solution rapidly identifies all endpoints that are missing their assessment and remediation agent. Once these unmanaged devices are identified, the solution automatically installs an agent, which immediately scans the machine and returns inventory and vulnerability data.

Thorough, Accurate Vulnerability Identification and Remediation

As part of the Patch Management and Remediation solution, PatchLink Update employs patented agent-based assessment technology to evaluate the applicability and ongoing status of each patch. Threat and inventory information on each endpoint is transferred to the PatchLink Security Management Console for aggregation, analysis and remediation. Agents can run these vulnerability and inventory scans as often as desired, with limited resource utilization and no impact on end users. In addition, the Patch Management and Remediation solution eliminates the time-consuming task of locating, downloading and testing security patches from multiple software vendors. Lumension consolidates security content for all major operating systems and over 40 leading applications into a central repository of more than 15,000 pre-tested patches.

PatchLink Developers Kit™, in combination with PatchLink Update™, allows you to automate the identification, correction and validation of software and hardware configurations on all infrastructure components such as servers, workstations and laptops. Deployed packages can identify systems that have drifted out of compliance with corporate configuration policy and quickly remediate the issue, returning the affected systems to their desired state. Continuous monitoring of configuration policies ensures that policy drift does not recur. As part of the Patch Management and Remediation solution, it enables you to create and deploy remediation packages that address a

wide range of configuration related issues, such as closing down vulnerable ports, shutting down dangerous services, identifying and removing unauthorized or expired files and applications, enforcing password policies and registry settings, and much more.

The powerful, yet easy to use role-based Security Management Console displays all relevant information on vulnerabilities discovered by each local agent. With one click of a mouse, the Administrator(s) can automatically remediate a single rogue endpoint or thousands of machines. To improve IT productivity, the solution includes advanced functionality such as automatic administrative alerts, mandatory baseline policy enforcement, deployment wizards, flexible nested grouping, active directory integration, multi-patch deployment and q-chain support, to name a few.

Continuous Audit and Flexible Compliance Reporting

The Patch Management and Remediation solution provides continuous monitoring of patch and configuration status to ensure ongoing compliance with security policies. This audit of remediated systems, based upon communication intervals defined by the system administrator, ensures the integrity of all previously installed patches and remediation packages.

To demonstrate policy compliance, the solution offers numerous assessment, remediation and aggregated compliance reports. Extensive filtering provides unlimited report flexibility. Information from multiple server installations can be aggregated into consolidated reports that provide a broad view of the security posture of the enterprise relative to common industry tracking mechanisms.

Common Criteria EAL2 Certified

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) Certification Body has asserted that Lumension's Patch and Remediation solution complies with the specified security requirements.

Add-on Products

PatchLink Scan™

Thorough and accurate network-based scanning solution that utilizes safe, adaptive scanning techniques against a comprehensive vulnerability database to identify and scan of all of the devices on your network, including servers, desktop computers, laptops, routers, printers, switches and more.

PatchLink Enterprise Reporting™

Centralized business intelligence solution that enables organizations utilizing PatchLink Update to consolidate security data from across the enterprise, assess business risk through powerful data mining analysis, and demonstrate security policy and regulatory compliance status through flexible, customized reporting.

Also available from Lumension

Lumension's Endpoint Security Solution delivers policy-based application and device control that proactively secures your enterprise endpoints from data threats, including data leakage, malware and spyware.

About Lumension

Lumension Security is a leading global security management company, providing unified protection and control of all enterprise endpoints, applications and devices to more than 5,100 customers and 14 million nodes worldwide. Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions, including vulnerability management, endpoint policy enforcement and extensive policy compliance reporting.

Reduce the Risk of Vulnerability Exploitation

See how you can quickly remediate vulnerabilities before they are exploited and maintain system compliance by contacting your local Lumension sales representative, reseller or by visiting us at www.lumension.com.

What Our Customers Are Saying

"Having a policy-based solution enables our company's systems administrators to enforce the security settings and minimize the patches according to company standards. The savings we experience in terms of reduced labor, together with knowing that our systems are less vulnerable and better protected, makes us more confident and satisfied with our selection of PatchLink Update."

Virgin Atlantic

"Anything we do must be highly automated or it won't scale to the levels we need. Maintaining and protecting our network is a daunting task, which is why having an automated tool like PatchLink Update is so valuable."

Thomson Financial

"Once we saw what PatchLink could do we were knocked out by its flexibility and its ability to remotely provide subcategories for different systems. PatchLink was the only vendor that could do this effectively providing us with the visibility and added security protection we needed."

Australian Defense Force Academy

Sources:

1. Carnegie Mellon University's Computer Emergency Response Team (CERT) (<http://www.cert.org>) reported 8,064 vulnerabilities in 2006
2. National Vulnerability Database - May 9, 2007
3. Gartner Research
4. IDC, Worldwide Security and Vulnerability Management Software 2007-2011 Forecast and Analysis: Governing Security and Risk Management