

Managing Risk While Maintaining Performance – The Real Challenge

Budgets are tight. Staffing is down. Expectations are high. And threats to your network are relentless. The reality of proactively keeping pace with security challenges means you have to quickly and efficiently implement the necessary pieces to reduce risk and support continuity in complex environments.

PatchLink provides the industry leading security solution which stands as a cornerstone for managing critical patches, providing detailed compliance reporting, integration to 3rd party scanning, quarantine solutions, and remediating known security vulnerabilities. PATCHLINK UPDATE increases and maintains your network's security posture by quickly and accurately deploying multiple security patches in single deployment effort. Our proven technology helps you easily manage the complexities involved in multiple security patch deployments to significantly reduce the time, effort, and cost necessary to deploy the increasing number of newly released security patches. PATCHLINK UPDATE helps solve common and uncommon security problems faced by IT organizations worldwide.

Risk Mitigation Through Vulnerability Elimination

Reduce risks associated with liability, non-compliance, lost revenue, and damaged customer confidence. Automatically detect and eliminate vulnerabilities.

Security Policy Adherence

Define policies that are automatically and universally deployed. Audit and report for completeness, accuracy, and continuance.

Availability and Scalability

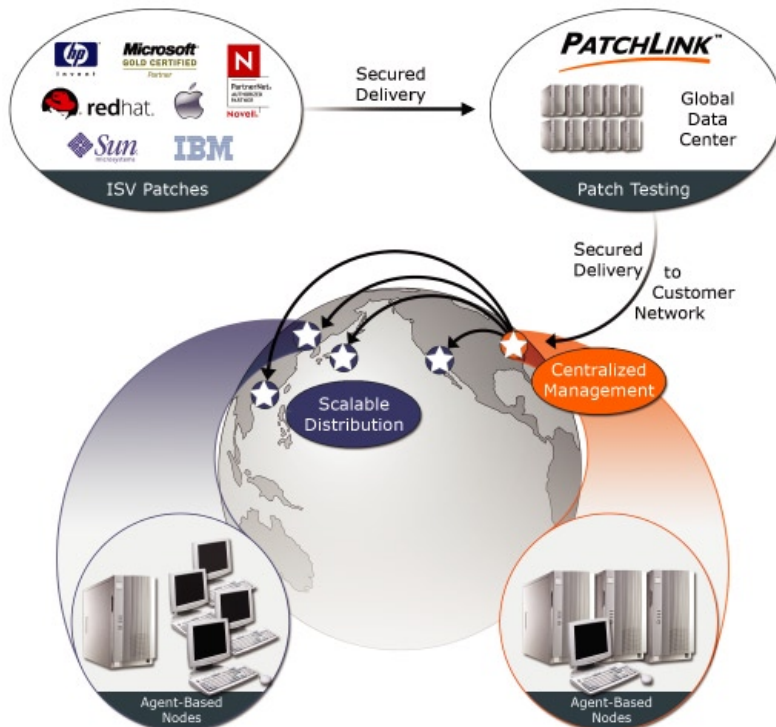
Meet service-level requirements for critical systems, while scaling to meet the needs of organizations both small, medium, and enterprise.

Reduced Costs

Automate patch-related monitoring, analysis, reporting, testing, deployment, and maintenance to significantly decrease administrative costs.



PATCHLINK UPDATE Architecture



PatchLink's architecture provides you with proven security, accuracy, and scalability.

We start by acquiring OS and application patches as well as AV definition updates from key Independent Software Vendors (ISV). These patches are then combined with a patent pending fingerprint technology, that includes granular file version information to provide the industry's most accurate matching, deployment, and tracking of the update. Packages are thoroughly tested in our labs and stored in PatchLink's highly secure data centers.

Patches are then securely distributed to the PATCHLINK UPDATE server(s) located inside your environment. These packages can then in turn be cached at key locations throughout your organization, providing fast and efficient package distribution to multiple locations. Agents installed on each node communicate with the PATCHLINK UPDATE server to determine, based on policy, what patches they are required to download and install from the nearest distribution point.

Industry Leading Functionality

• Automated Vulnerability & Patch Management

Automated Vulnerability & Patch Management

Continuous, Automated Deployment – Schedules off-hour, or recurring deployments to maintain a complete and continuous security profile without increased administrative costs.

Advanced Multi-Patch Deployments – Wizard-driven approach to multi-patch deployment simplifies and speeds complex deployments. Includes a visual pre-deployment summary to show the effects of each patch in the deployment.

Digital Patch Fingerprinting™ – Scans each system to accurately determine applicable updates and verifies patch status to fix “patch collisions” caused by installation overwrites, re-imaging, etc. PatchLink has the largest automated digital patch fingerprinting repository in the world.

Reporting and Assessment – Top-level graphical assessments supported by deployment detail provide real-time patch security status. Allows you to easily confirm and report on policy compliance requirements such as SARBOX, HIPAA, and FISMA.

• Policy-based Deployment & Remediation

Policy-Based – Mandatory patch baselines and policies include settings, scheduling, and minimum requirements to ensure corporate network security policies are automatically applied throughout the organization.

Role Management – Administrator-created roles define operator scope and capability to keep administrative security consistent with policies. The administrator has full control over the deployment of the patch or software installation including reboot options allowing for increased and predictable availability of key servers within the organization.

Inventory Change Control – By locking down information about hardware and software installed at client workstations, administrator can be automatically informed when hardware or software is installed or removed allowing them to assess modifications and determine appropriate action.

• Solution Flexibility for Diverse Environments

Multi-Platform Support – The only patch detection and deployment software available for managing heterogeneous networks including all MS operating systems, UNIX, Linux, Sun HP, IBM and Macintosh. Includes remote monitoring from any platform.

Multiple Agent Deployment Options – Provides various options for managing agent deployment to meet the needs of your organization. Includes ability to deploy on computers as they are imaged so they are quickly and automatically brought into compliance with default system baselines.

• Scalable to Meet the Needs of Global Enterprises

Centralized Management with Distributed Deployment – Centralized security policies supported by FastPatch™ (is this still valid?) intelligent distribution allows you to maintain centralized control while increasing deployment speeds. Minimizes WAN and user productivity impact.

Enterprise Support – Provides scalability and availability via clustered and automatic fail-over configurations so you are able to scale your network security while meeting stringent service-level requirements.

Web Standards – HTTP/HTTPS transport for maximum compatibility with existing infrastructure provides support for intranet/extranet/Internet topologies and ensures compatibility with other security products.



Network Security from a Proven Leader

PatchLink Corporation is the established leader for enterprise-wide security patch, vulnerability, and compliancy management. Recognized by Inc. magazine as one of the fastest-growing companies in the US, PatchLink's market-leading PATCHLINK UPDATE is used by top-ranked enterprises in federal and state government, industry, education and non-profit markets. Clients of PatchLink include the armed forces, EPA, USDA and NASA; global companies, like Thomson Financial, Virgin Airlines and Boeing; and major regional companies, including many BlueCross BlueShield plans across the country; and top educational institutions. The Company is headquartered in Scottsdale, Arizona with major offices in metropolitan Washington D.C; London; and Singapore.

PATCHLINK UPDATE Server - Minimum Requirements
Windows 2000 / 2003 Server (latest service packs); IIS
Pentium 1Ghz, 512 Mb RAM, 5 Gb available disk space.

PLU62DS-091305