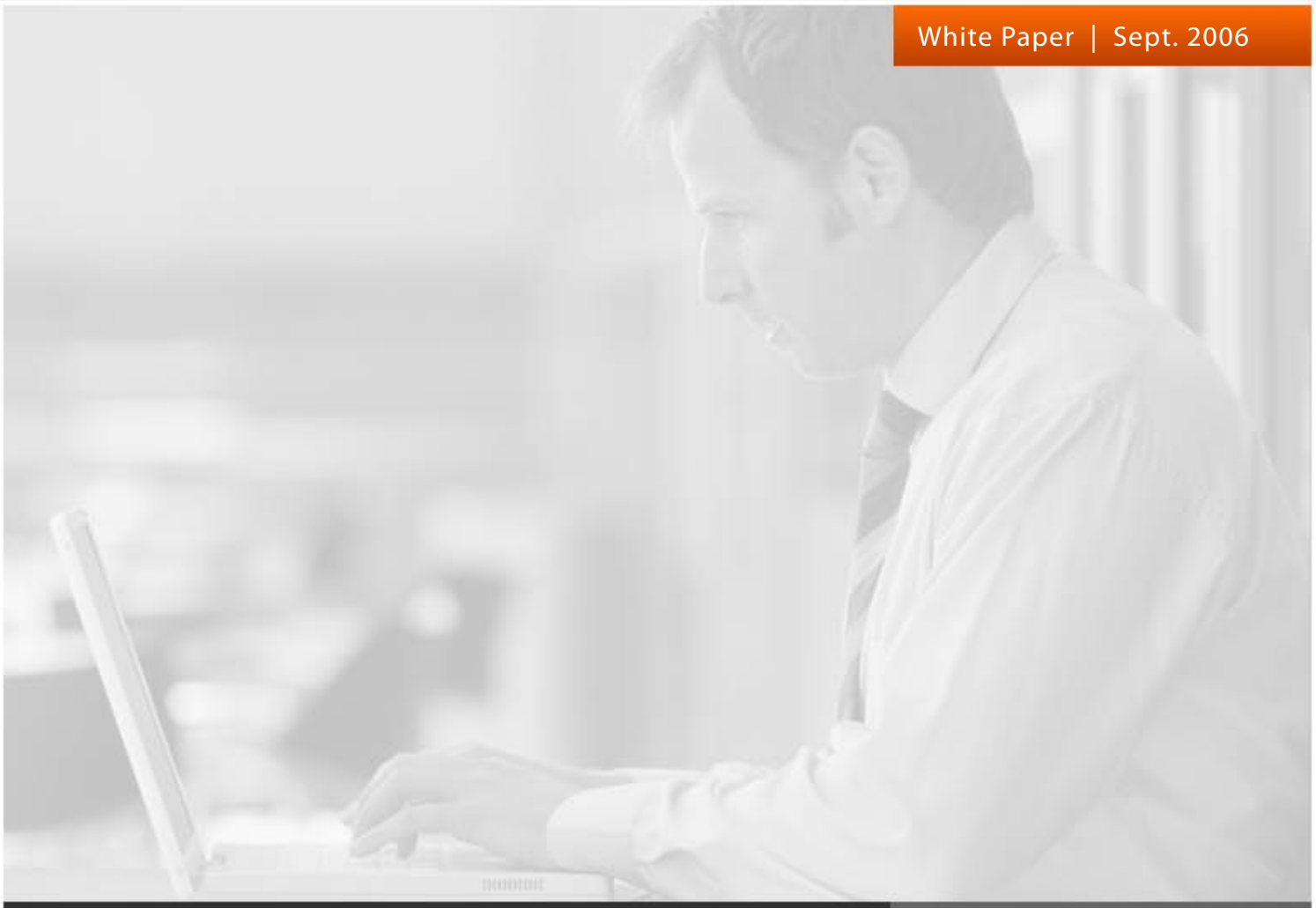
White Paper | Sept. 2006



How PatchLink Meets the Top 10 Requirements for Enterprise Patch and Vulnerability Management

Introduction

It happens, five, ten, twenty times a month: A hardware or software vendor releases a patch (or a pack of patches) for a business-critical system. Getting these patches tested and installed has never been as important as it is today because organizations rely on their information systems and have internal and regulatory pressures to keep those systems secure. Quickly patching vulnerabilities reduces the risk of data being stolen or compromised, of applications being slowed or stopped, and of a security breach harming a company's reputation or bottom line.

But patch management is more complicated than ever. An organization must determine which of its systems from its multiple vendors are eligible for each patch, test the patches to ensure they don't create new problems, find and patch the most critical vulnerabilities first and finally report on the entire process to prove to auditors that the work was done. And, of course, this all must be done as easily and automatically as possible to hold down IT management costs.

PatchLink has described these requirements in an earlier white paper, "The Top Ten Requirements for Effective Enterprise Patch and Vulnerability Management." These requirements were distilled from both SP 800-40 and other resources to provide a comprehensive set of buying criteria.

The purpose of this white paper is to describe how PatchLink Update meets and surpasses these specific requirements, allowing its customers to patch their systems 13 times faster than industry standards and to save more than $180,000 per year (for an organization with 1,000 computers.)

Key enterprise patch and vulnerability requirements are:

1. **Coverage**: Does the solution provide patch management for diverse operating systems and applications, as well as for custom in-house software?

2. **Architecture**: Is the solution based on an open architecture that uses agents to discover and deploy patches to all end points, that is flexible enough for deployment in both centralized and decentralized environments, and that can be customized and integrated with other security products?

3. **Ease of Use and Flexibility**: How intuitive and easily navigable is the management interface? Can the solution be adapted to meet the unique needs of an organization's distributed IT infrastructure, and to its unique policies and processes?

4. **Discovery**: Can the solution establish an inventory of all resources that might be susceptible to vulnerabilities and thus require patching?

5. **Monitoring**: Does the solution continually and accurately monitor patched systems to ensure they remain patched, and issue alerts if they become unpatched due to restorations of older system images or reinstallation of software?

© PatchLink Corporation - September 2006 - www.patchlink.com

6. **Analysis**: Can the solution help prioritize patches by analyzing factors such as the severity of the vulnerability associated with the patch, the existence of any threats which exploit the underlying vulnerability, and the extent to which the patch has been tested?

7. **Testing**: To what extent does the solution vendor provide install/deinstall scripts and other components needed to effectively deploy the patches, and test these packages before distributing them?

8. **Intelligent Deployment**: Does the solution make it easier and less disruptive to deploy upgrades across very large, complex environments with options such as phased rollout, and by giving users control over when to reboot after an upgrade?

9. **Reporting**: Does the solution provide broad and flexible reporting for both operational and executive needs, such as the status of any given patch deployment and the identification of any weaknesses in the organization's patch and vulnerability management program?

10. **Integration**: Can the solution share information with other threat, vulnerability, and risk management tools such as vulnerability scanners to give security managers a better overall view of their environment?

© PatchLink Corporation - September 2006 - www.patchlink.com

Coverage

Most organizations today run a highly diverse mix of applications, operating systems and networking devices, any of which can contain security vulnerabilities and thus become the target of hackers. In fact, the National Vulnerability Database found that 37% of vulnerabilities target popular applications other than Microsoft's and that almost 50% of these are critical vulnerabilities. In addition, many organizations run custom in-house software that must be updated and patched over its lifecycle. Without patch and vulnerability management for all of these platforms, organizations will continually be at the mercy of new exploits, and unable to meet regulatory and internal security requirements.

PatchLink meets this requirement with the industry's largest repository of patches for all major operating systems and applications. This includes more than 10,000 multi-language patches for all major operating systems and over 40 of the most common third-party applications such as Adobe Acrobat, Macromedia Flash, Internet Explorer, MSN Messenger, SharePoint, RealPlayer, and more. PatchLink also supports older operating systems and applications for protection of legacy end-points. And, with the PatchLink Developers Kit™ customers can develop, test, deploy, and monitor custom patch and remediation in their PatchLink Update™ environment.

PatchLink Update Provides :

- Over 10,000 multi-language patches and updates.
- Support for All Major Platforms: including Microsoft Windows OS, Microsoft 64-Bit OS, Mac OS X, Mac on Intel, Novell NetWare, Novell SUSE Linux, HP-UX, IBM AIX, Sun Solaris, Red Hat Linux
- Over 40 Third-Party Application Patches: These include patches for a broad array of Microsoft applications and the most common third-party applications and utilities used in organizations today including Adobe Acrobat, Macromedia Flash, Internet Explorer, MSN Messenger, SharePoint, RealPlayer, and more.
- PatchLink Developers Kit: This security patch creation tool allows customers to develop, test, deploy, and monitor custom patch and remediation in their PatchLink Update environment.
- Support for Legacy OS and Applications: Support for older operating systems includes Windows 98, Windows NT, and older versions of Sun Solaris. Support for older applications includes older versions of Exchange Server and Office.

© PatchLink Corporation - September 2006 - www.patchlink.com

Architecture

Organizations today are more geographically dispersed than ever before, with IT staffs supporting highly mobile workforces as well as both managed and unmanaged end-points that might be spread across multiple time zones and continents. Their IT architectures are often highly complex, including both centralized and distributed architectures as well as existing security products to which a patch and vulnerability management solution must connect.

PatchLink Update is built on a scalable architecture that speeds and automates the patch management process. Automated agent distribution locates and deploys patching agents to unmanaged network endpoints, including laptops. PatchLink Update servers can be implemented in either a centralized or distributed architecture to assure speedy deployment even in widely dispersed and complex environments. By using the optional PatchLink Distribution Point, patches can be also be cached on any computer in the network to enable the distribution of patches over low bandwidth networks or connections between remote offices. Its open architecture also allows for customization and integration with other security products such as third-party access control systems and leading commercial vulnerability scanning products.

PatchLink Update Provides :

- An agent-based architecture which provides protection for all end points including laptops.
- Automated agent distribution which locates unmanaged network endpoints and deploys the patching agent, ensuring maximum coverage and protection.
- Support for standard communication protocols such as TCP-IP/ HTTP & HTTPS.
- Highly scalable product architecture which ensures speedy and complete coverage for even the largest worldwide networks.
- Efficient bandwidth utilization through optimization of network traffic with server and client-side bandwidth throttling options and efficient network bandwidth utilization.
- Secure Content Delivery via 128-bit SSL encrypted and VERISIGN trusted connection along with RSA BSAFE® Encryption for best-of-breed data encryption.

© PatchLink Corporation - September 2006 - www.patchlink.com

Ease of Use and Flexibility

Security patches are of limited use if they can't be deployed quickly, easily and in accordance with a company's unique security policies. Ease of use helps to speed the patch process, and to hold down security management costs. Flexibility in a patch management solution is also crucial so each enterprise can decide which patches are deployed to which systems, and when.

PatchLink Update accelerates patch management with an intuitive Web-based interface and full flexibility in patch deployment, including the ability to group systems according to a wide range of attributes and extensive grouping capabilities. With role-based administration, the system administrator can delegate activities with over 45 individual access rights, which improves the administrator's productivity while maintaining security.

PatchLink Update Provides :

- Intuitive Web-Based Interface: Enables wide access to an easy-to-use administrative interface. Network interruptions have minimal impact on the PatchLink console.
- Extensive Grouping Capabilities: Organizations can define patching policies with grouping based on a wide variety of system or administrator-designated attributes for easy management, with virtually no limit to the number of groups that a resource can be included in.
- Role-Based Administration: Allows system administrators to delegate activities with over 45 individual access rights to improve management productivity while maintaining security.
- Flexible Deployment Options: Wizard-based multi-patch deployments, support for phased rollouts, and deployment within narrow installation windows allows administrators to control deployment based on each organization's unique security policies.
- Policy-Based Administration: Ensures that all systems meet a mandatory baseline policy, automatically remediating end-points that don't meet defined patch levels — a key aspect of regulatory compliance.

© PatchLink Corporation - September 2006 - www.patchlink.com

Discovery

Organizations cannot patch systems they don't know they have, or that they don't know require patching. They need a patch and vulnerability solution that is highly accurate in discovering and remediating un-patched end-points. This discovery process is vital to not only eliminate vulnerabilities, but to comply with regulations such as Sarbanes-Oxley, FISMA, HIPAA and the European Privacy Directive, which The Yankee Group estimates that two-thirds of all enterprises are subject to.

PatchLink's patented Digital Fingerprinting Technology™ provides a highly accurate patch and vulnerability process for automatic assessment, remediation, and continuous monitoring to ensure no systems are left open to attack. Extensive grouping capabilities allow administrators to define patch policies with automatic grouping based on a wide variety of system or administrator-designated attributes including criticality, location, and function.

PatchLink Update Provides :

- Inventory Assessment: Automatic identification and reporting on all software, hardware, and services establishes an accurate inventory of all resources that might be susceptible to vulnerabilities.
- Discover Applicable Updates: Scans the devices on your network to determine exactly which systems need to be patched.
- Extensive Grouping Capabilities: Organizations can define patching policies using a wide variety of system or administrator-designated attributes, with virtually no limit to the number of groups in which a resource can be included.

© PatchLink Corporation - September 2006 - www.patchlink.com

Monitoring

Over the course of a year, approximately 20% of all previously patched systems will become “un-patched” due to the installation of new patches, applications or system rebuilds which replace newer, secure components with older, insecure components. Without continuous monitoring, organizations can be left with a false sense of security — believing their systems to be effectively patched and compliant when that is not actually the case.

PatchLink Update’s patented Digital Fingerprinting Technology ensures that end-points get patched and stay patched by creating a Patch Fingerprint Profile that includes all software, hardware, drivers, existing and missing patches for that machine. Each end-point is then continually monitored to ensure they are patched. Policy-based administration allows administrators to establish a mandatory baseline which automatically remediates end-points that don’t meet defined patch levels — a key aspect of regulatory compliance.

PatchLink Update Provides :

- Patch Fingerprints: PatchLink Update establishes a Patch Fingerprint Profile for each machine that includes all of its software, hardware, drivers, existing, and missing patches. Each end-point is then continually monitored to ensure it is patched and stays patched.
- Policy-Based Administration: Ensures that all systems meet a mandatory baseline policy, automatically remediating end-points that don’t meet defined patch levels — a key aspect of regulatory compliance.
- Patch Compliance Alerts: Automatically alerts administrators via email when a patch is removed or dropped due to changes such as the restoration of a system image or the installation of a new application.

© PatchLink Corporation - September 2006 - www.patchlink.com

Analysis

To maintain security without overrunning their budgets, organizations must be able to quickly determine which patches affect which critical systems, the severity of the threat if the patch is not applied, and whether the patch has been tested for both safety and effectiveness.

For each patch it distributes, PatchLink Update uses information about patch interdependency (which other patches must be present before a new patch can be installed) and patch precedence (the order in which patches must be installed) to present only the patches that need to be applied to each system. By reducing the need for manual analysis of such factors, administrators can more quickly and easily prioritize patch deployments to minimize disruption to users and ensure patches are deployed in accordance with corporate and regulatory security policies.

PatchLink Update Provides :

- Automatic Identification of Patch Prerequisites: PatchLink automatically identifies which existing patches must be present to install new patches, as well as the order in which multiple patches should be installed, and presents only the applicable patches to the system administrator.
- Rapid Verification of Successful (and Failed) Installs: Administrator(s) receive automatic e-mail alerts for failed installations along with successful installation indicators within the PatchLink Administrative Console for proactive troubleshooting and management.

© PatchLink Corporation - September 2006 - www.patchlink.com

Testing

When a vendor releases a patch, it typically includes only the patch itself. But administrators also need a package or wrapper for each patch with information about applicable operating systems and languages, along with install/de-install scripts. Before deployment, they also need to test this package to verify it works correctly.

Because PatchLink provides and tests such patch packages, 78% of PatchLink customers spend less than one day testing patches before deployment. PatchLink's extensive Quality Assurance process ensures that each patch package is tested on all applicable operating systems and languages.

PatchLink Update Provides :

- Patch Package Development: PatchLink develops complete Patch Packages including install/de-install scripts, patch fingerprints, and patch applicability information.
- Patch Quality Assurance Process: PatchLink spends hundreds of hours ensuring that each patch package is pre-tested in all necessary environments, saving customers valuable testing time.
- Patch Pre-Approval: PatchLink makes it easy to deploy patches on a QA server before moving them to production servers for easy deployment management.

© PatchLink Corporation - September 2006 - www.patchlink.com

Intelligent Deployment

Simply rolling out every available patch to every applicable system can cause chaos as users interrupt work to reboot their systems or call help desks about how or whether to install patches. To automatically distribute and install patches across tens, hundreds, or even thousand of systems, a patch management and vulnerability solution must provide phased rollout, settings that allow users to control possibly disruptive actions such as system reboot and automatic verification of proper patch installation. Because of features such as these, PatchLink customers patch 13 times faster than industry standards.

PatchLink Update Provides :

- Wizard-based multi-patch deployments: Administrators can deliver multiple patches to multiple computers in one distribution to increase IT productivity.
- Support for phased rollouts: Allows organizations to define rollout groups from test to final deployment, controlling which patches are rolled out to which systems and when.
- Deployment within narrow installation windows: Administrators can define patch deployment windows and give end-users control over patch activities to minimize disruptions to their work.
- Automatic initiation of prerequisite activities: PatchLink accurately defines patch precedence and interdependencies to ensure only applicable patches are deployed to various systems.
- Rapid verification of successful (and failed) installs: Administrator(s) receive automatic e-mail alerts for failed installations along with successful installation indicators within the PatchLink Administrative Console for proactive troubleshooting and management.

© PatchLink Corporation - September 2006 - www.patchlink.com

Reporting

Organizations not only need to properly patch their systems, but to produce reports proving the patching was done so they can pass IT and regulatory audits. These reports, produced for both operations staff and management, must include the status on any given patch deployment and illuminate failures or exceptions that require troubleshooting. Such reporting is also critical to identify any weaknesses in the organization's ongoing vulnerability and patch management process, and to quantify the effort and results associated with the patch and vulnerability program.

PatchLink Update addresses a full range of both operational and management reporting needs with 21 standard reports that document changes and demonstrate steady progress toward internal and external audit and compliance requirements. More reporting options are available via PatchLink Enterprise Reporting which provides additional trending and operational reporting via an open data warehouse for powerful security reporting.

PatchLink Update Provides :

- Comprehensive Reporting: Twenty-one standard reports document changes and demonstrate steady progress towards internal and external audit and compliance requirements.
- PatchLink Enterprise Reporting (ERS): Powerful security reporting providing trending and operational reporting on all aspects of the patch and vulnerability lifecycle across the enterprise.

© PatchLink Corporation - September 2006 - www.patchlink.com

Integration

As organizations' security initiatives continue to expand, many have adopted a variety of products designed to improve their security posture and to reduce their risk. For example, most organizations are already using vulnerability scanning products and beginning to implement third-party access control systems to scan and block systems based on defined security policies. Rather than use each system as a standalone island of information, organizations want to be able to view as much security-related information as possible within a single console. An open architecture is required to ensure seamless integration of all the security products which are working together to protect the corporate network.

PatchLink Update's open architecture allows for customization and integration with other security products such as third-party access control systems and leading commercial vulnerability scanning products. With PatchLink Update's open architecture, organizations can also integrate their patch management solution with external vulnerability and threat alerting services, intrusion control, and other threat management systems.

PatchLink Update Provides :

- An Open Architecture which makes it easy to customize PatchLink Update and integrate it with other security products.
- PatchLink Developers Kit (PDK) which enables customers to develop, test, deploy, and monitor custom patch and remediation within their PatchLink Update environment.
- PatchLink Quarantine (NAC) combines PatchLink assessment and remediation technologies with leading third-party access control systems to scan and block systems based on defined security policies.
- PatchLink Scanner Integration (SIM) extends the functionality of PatchLink Update to provide seamless integration with leading commercial vulnerability scanning products.
- PatchLink API for integration with third-party products such as Help Desk software.

© PatchLink Corporation - September 2006 - www.patchlink.com

Conclusion

Faced with ever-stricter corporate and regulatory security requirements, IT organizations must do a better job of patching the many different hardware and software platforms on which their businesses rely. Their automated vulnerability and patch management solutions must meet ten key requirements, ranging from support for multivendor environments to ease of use, flexibility, ongoing systems monitoring, an open architecture which can integrate with other security tools along with robust testing and reporting capabilities.

PatchLink Update delivers industry-leading capabilities in each of these critical areas with its patented Digital Fingerprinting Technology which provides accurate discovery and ongoing monitoring of the patch state of vulnerable systems. Its flexible options for policy-based patch deployment give organizations the flexibility to work within their unique needs, while PatchLink's rigorous testing and quality assurance provides customers with not only raw patches, but the patch intelligence needed to quickly and efficiently patch even the largest and most complex environments. Its comprehensive reporting capabilities help assure organizations they can meet both operational and management reporting requirements.

As a result of these industry-leading capabilities, PatchLink customers are able to patch their systems 13 times faster than industry standards, with 78 percent spending less than one day testing patches before deployment. Compared to manual patch processes at an organization with 1,000 computers, PatchLink provides an expected savings of over $180,000 per year, and reduces the amount of administrative time spent on patching by 90 percent, from 4,447 hours to 393 hours. . Given such improvements, it's little surprise that more than 90% of PatchLink customers feel they are more secure now than they were year earlier.

In a world in which software patching is more important, and more complex than ever, organizations need a solution which meets the top ten requirements for enterprise vulnerability and patch management. That solution is PatchLink Update.

About PatchLink Corporation

PatchLink® is the global leader for security patch and vulnerability management solutions, delivering comprehensive, multi-platform assessment and remediation for continuous protection across the enterprise. Offering the most comprehensive platform and application support, PatchLink maintains the largest tested and most up-to-date security patch repository, enabling organizations to accurately assess and remediate vulnerabilities based on established industry best practices. Currently protecting thousands of commercial and government organizations and millions of PCs and servers worldwide, PatchLink effectively eliminates vulnerability risks and enforces security and compliance policies while reducing overall IT costs.

© PatchLink Corporation - September 2006 - www.patchlink.com

PatchLink Corporation
Scottsdale, AZ 85255
480.970.1025

www.patchlink.com

© PatchLink Corporation - September 2006 - www.patchlink.com