

# PatchLink® Update™ 4.0 White Paper Cross-platform Security Patch Management

By PatchLink Corporation

<b>Abstract</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>The PatchLink Update Solution</b>	<b>4</b>
Client-side Features	4
Server-side Features	6
<b>Scenarios</b>	<b>14</b>
Managed Desktop and Servers	14
Managed Data Center	14
Automatic Client Updates	14
Recurring Schedule	14
Proactive Notification	15
Building Custom Packages	15
Automatic Replication	15
<b>Client-Side: Agent Installation</b>	<b>16</b>
Installing Client Software	16
<b>PatchLink Customer Case Study</b>	<b>17</b>
<b>About PatchLink Corporation</b>	<b>18</b>

## Abstract

This white paper describes the features of PatchLink® Update™ 4.0, a new solution for managing and distributing critical patches that resolve known security vulnerabilities and other stability issues in all Microsoft operating systems (95, 98, ME, NT, W2K, XP, .NET), UNIX (Linux, Solaris, AIX, HP-UX, etc.), and Novell Netware. PatchLink Update 4.0 is the only patch detection and deployment software available for managing these heterogeneous network environments. This paper also includes solutions for customer scenarios which incorporate PatchLink Update.

PatchLink Corporation is the pioneer in automated patch management technology and has been developing, researching and shipping products for patch management since 1996. PatchLink's patent-pending technology is capable of accurately fingerprinting and locating patches and their interdependencies on a variety of platforms using open Internet protocols.

This paper is written for information technology managers and system administrators who want to automatically and securely keep all the computers in their network up-to-date with security patches and other updates.

## Introduction

PatchLink Update is built on proven technology for automated patch detection and deployment for managing and distributing critical patches that resolve known security vulnerabilities and other stability issues with operating systems.

Today, corporations are required to frequently check vendor Web sites to find out about new patches. Upon learning that a vendor has a new software, hardware or driver patch, they have to manually download the relevant patches that have been made available since their last visit to the vendor's site, test the patch (es), and then distribute the patch (es) manually or by using their traditional software-distribution tools.

PatchLink Update solves these challenges by providing proactive notification of critical updates to computers whether or not they have Internet access. Additionally, this technology provides a simple and automatic solution for distributing software updates, software packages and any other data to the networked desktops and servers.

PatchLink Update addresses the need for critical patch-management within any size organization by providing the following features:

**a. Automatic content replication service via the Internet using 128-bit SSL**

The content replication service is a server-side component that retrieves the latest critical updates and software from the private site known as the PatchLink Update Master Archive using a 128-bit SSL connection. As new updates are added to the PatchLink Update Master Archive, their meta data are downloaded automatically. If patches are marked as critical, then they are downloaded and cached for rapid deployment. Each patch has an installer, prerequisite signature and fingerprint identification. Information is sent in one direction only: from the PatchLink Update Master Archive to the user's PatchLink Update Server. All information is encrypted, CRC checked, compressed, digitally signed, and downloaded over a 128-bit SSL connection. The SSL connection validates and confirms the authenticity of the patch source.

**Subscription Service**      Licenses      Agents

**Subscription Service Information**

**Last Subscription Poll:** 6/7/2002 11:43:31 AM  
**Subscription Agent Status:** Sleeping  
**Account ID:** CA1C2FAF-5702-4EE7-942C-AF2136E9C

**Subscription Service History**

Type	Status	Start Date
Packages	Completed	6/7/2002 11:43:31 AM
Reports	Completed	6/7/2002 11:40:03 AM
Licenses	Completed	6/7/2002 11:30:06 AM
Packages	Completed	6/7/2002 5:36:24 AM

**b. PatchLink Update Server (PLUS)**

This easy-to-use server application acts as the patch source for client computers. It contains the replication service and administrative tools for managing updates and software packages. It can scan and schedule patch delivery to the clients using the HTTP or HTTPS protocol. This server can also automatically cache the critical patches from the PatchLink Update Master Archive. Users can utilize the built-in software distribution feature and distribute any software packages to any desktop.

**c. Administrator control over updates and packages**

After viewing the enterprise report matrix, the administrator controls which updates or packages from the PatchLink Update Server are to be pushed to client computers. PatchLink recommends that you test each patch internally before deploying them to your enterprise. Each enterprise is different and an update may act differently in each environment. The administrator has full control over the deployment of the patch or software that gets installed onto the client computer including reboot options. The administrator can set or change client agent policies as well.

**Detection Reports** Total

Report Name	Impact	✓	✗	⚙	⚙	⚙	Total
MS02-006-0314147: Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run	Critical	1	6	0	0	0	7
MS02-013 - Java Applet Can Redirect Browser Traffic	Critical	1	5	0	0	0	6
MS02-014-0313829 - Unchecked Buffer in Windows Shell Could Lead to Code Execution	Critical	0	3	0	0	0	3
MS02-018-0319730: Cumulative Patch for Internet Information Service	Critical	1	4	0	0	0	5
MS02-022-0321661: Unchecked Buffer in MSN Chat Control (MSN Messenger)	Critical	4	1	0	0	0	5

**d. An intelligent client-side agent on computers (desktops or servers)**

The client-side agent checks the intranet-hosted PatchLink Update Server to automatically determine which updates are needed. It will then report the information back to the PatchLink Update Server that will create the report matrix for the administrator. The administrator approves the deployment of

patches by using the deployment wizard. Administrator-approved updates or packages are downloaded in the background and auto-installed according to the schedule set by the administrator. The rules control the behavior of the patch installation set by the administrator during the patch deployment.

e. **Comprehensive patch testing**

PatchLink continuously researches, tests and approves patches before they are released by PatchLink. For example, when a hot fix for W2K is released, it is installed on over 250 different configurations of W2K including standard W2K, W2K with SQL server, W2K with Office, W2K with Exchange, and so on with a variation of other service packs and hot fixes.

## The PatchLink Update Solution

PatchLink Update consists of both client-side and server-side components for critical patch management and basic software distribution.












### Client-side Features

PatchLink Corporation has a patent pending on its technology and is the leading company in automated patch detection and deployment.

PatchLink Update is a proactive service that enables administrators to automatically download and install software packages and updates such as critical operating-system fixes and security patches. The features include:

- **Built-in security:** Uses digital security identification to register against the PatchLink Update Server. Before installing a downloaded update, it verifies the digital certificate, CRC check, compression and encryption on each file.
- **Patch signature:** A technology that can scan the system and determine if the prerequisite for each patch has been met. This is done by checking the proper software version and proper hardware drivers.
- **Patch Fingerprinting™:** PatchLink Update detection service will scan the system and determine which updates are applicable to a particular computer. Both the patch signature and fingerprints make a detection report, which is viewable in the report matrix. The PatchLink Master Archives currently host one of the largest automated patch fingerprinting repositories in the world.

- **Background downloads:** PatchLink Update uses a Secure Background Transfer Service (SBTS), which has built-in bandwidth throttling. The network administrator can decide how the bandwidth should be utilized during large deployments.
- **Chained installation:** The administrator can minimize repetitive rebooting by taking advantage of the Qchain.exe. If multiple updates are installed which require multiple reboots, the administrator, using Qchain, can deploy them with only one reboot. This minimizes the reboot process to increase the uptime for mission critical computers. Qchain rearranges the DLL in the proper order so the latest update will take effect. Administrators can chose this option during the deployment.
- **Workstation inventory (discovery agent):** PatchLink Update has an inventory discovery agent so it can pinpoint the needed software and hardware drivers for your client computers. The discovery agent also scans the client computer for the necessary signatures and fingerprints.

+		Monitors
+		Network adapters
+		Non-Plug and Play Drivers
+		NT Apm/Legacy Support
+		Ports (COM & LPT)
-		Processors
		<b>Device</b>
		<ul style="list-style-type: none"> <li>-  GenuineIntel x86 Family 6 Model 5 Stepping 2 at ~350MHz <ul style="list-style-type: none"> <li> <b>Computer Name</b></li> <li> \\EDDYA</li> </ul> </li> <li>+  GenuineIntel x86 Family 6 Model 7 Stepping 3 at ~498MHz</li> </ul>
+		RAM

- **Resume downloads:** PatchLink Update is capable of detecting interruption and service outage. If the user has a mobile workstation, they can simply disconnect the computer and reconnect at a different location. As long as the PatchLink Update Server can be accessed via TCP/IP, the service will resume its download from the point at which it got interrupted.
- **Mobile-user enabled:** PatchLink Update allows administrators to deploy patches and software updates to computers which are not connected to the network at the time of deployment. Once a mobile user connects to the corporate network, PatchLink Update will automatically scan their system and perform the necessary functions to keep their system up-to-date.
- **Advanced client agent technology for secure downloads (PatchLink Agent):** PatchLink Update uses advanced client-side agent technology to communicate with the PatchLink Update

Server. The main reason for using agents is to increase performance and scalability of an enterprise-wide solution. Agents accelerate the performance of a large-scale deployment and a single enhanced Update Server can service literally tens of thousands of Web-based client agents. PatchLink Update agents can work across firewalls and operate on literally any computer that has a TCP/IP connection to the enterprise network.

- Most major enterprise software management tools use agents, such as Microsoft SMS, Active Directory, IBM's Tivoli products, Symantec Anti-Virus, McAfee Anti-Virus and Novell Zen. In large networks, agents can "wake up" and report to the server when they have information to report in parallel. In comparison, tools that do not use agents must rely on remote API calls, which must be polled continuously from the server and can be extremely slow and not scalable in large environments.
- Agents can receive compressed files to conserve bandwidth and, for increased security, also identify if the patch has been tampered with. An agent can resume a download when it is disconnected from a network and reconnect at different locations — a necessity for mobile users. Patch tools that lack an agent must download the entire service pack or file every time they are interrupted and rely on a permanent LAN connection to function. They also tend to generate spikes in bandwidth utilization as patches are deployed. PatchLink Update Server can be tuned to only allocate a given amount of bandwidth per agent connection to take advantage of bandwidth-throttling.
- Patch tools that rely on a domain connection and do not have an agent rely on "Remote Registry" Service. This service provides registry information to a remote computer and may be a security risk in many organizations where client computers are on the Internet. It allows a remote computer to read the registry information of a client computer. PatchLink Update does not use this service due to security reasons. Also this service is not available on Windows 95, Windows 98, and Windows ME — which describes why patch tools without an agent cannot operate on these platforms. PatchLink Update covers the entire Windows family securely.

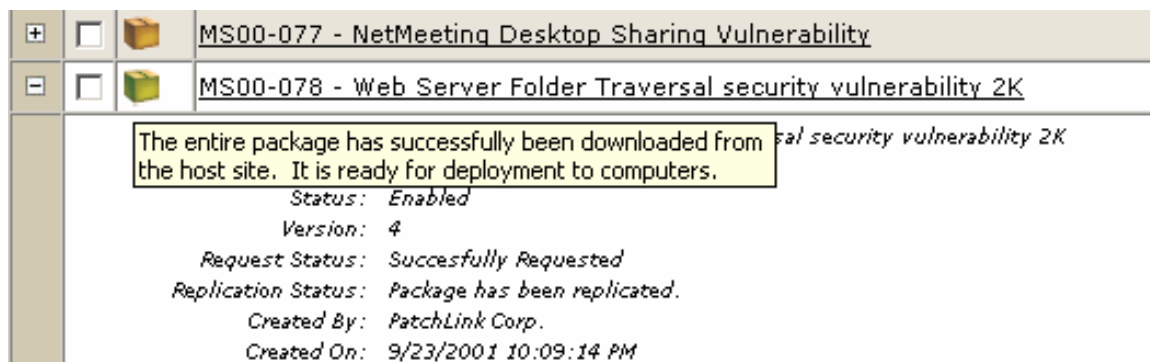
## **Server-side Features**

PatchLink Update is based on PatchLink's proven technology for automated patch detection and deployment for managing and distributing critical patches and software packages that resolve known security vulnerabilities and other stability issues with operating systems. The company has successfully

fulfilled customer patch requirements since mid-1996. PatchLink Update Server runs on Windows 2000 Server with Service Pack 2 or later. Internet Information Services (IIS) must be enabled on the server.

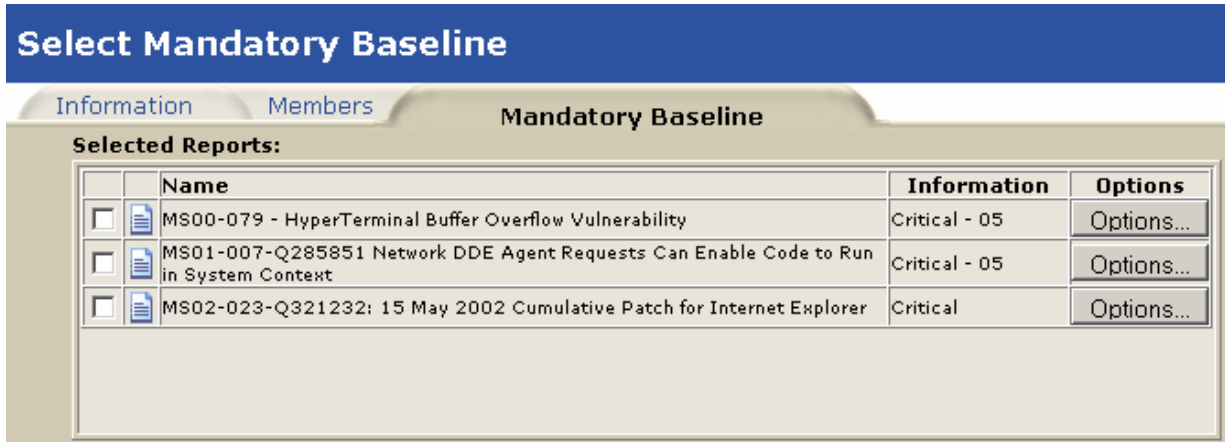
The server features include:

- **Built-in security:** The administrative pages are restricted to administrators on the PatchLink Update Server. The replication uses SSL and validates the digital certificates on any downloads to the update server. If the certificates are not from PatchLink Update, the server fails and sends an email alert to the administrator. All information is encrypted, CRC checked, compressed, digitally signed, and downloaded over a 128-bit SSL connection.



- **Support for multi-vendor patches (comprehensive patch scanning):** PatchLink has been building its patch repository since late 1996 and has one of the world's largest repositories of automated patch fingerprints. This extremely important feature of PatchLink Update allows the server to scan client computers for patch-related security vulnerabilities from Microsoft, as well as IBM, Adobe, Corel, Symantec, McAfee, Compaq, WinZip, Citrix, Novell and many others. This critical feature provides clients with a more secure network.
- **Grouping:** PatchLink Update can group arbitrary sets of computers of any OS into a container, which can then be managed by administrators. The product operates in the scope of the selected group and allows for easier management of deployments, fingerprint reporting, inventory reporting, mandatory patch baseline policy and client agent policy. Each computer group has properties that include Members, Client Agent Policy and Mandatory Patch Baseline Policy. Administrators can select any groups including user-definable groups for deployment.
- **Mandatory patch policy with automatic deployment:** PatchLink Update has a mandatory patch baseline policy for each group of computers. This feature can be used to automatically patch shrink-wrapped operating systems and applications to a particular organization's standards. Once the mandatory patch policies are set, as new computers become members of a group, all mandatory patches and packages are automatically installed. For example, if mandatory patch baseline policy for

a W2K group includes Office 2000, Adobe Acrobat Reader 5.0 and Service Pack 2, then all computers that join this group will have Office 2000, Adobe Acrobat Reader 5.0 and Service Pack 2 installed on them automatically. Patches that are dropped by restoring software from tape backup or reinstalling software are automatically reinstalled. The baseline integrity is maintained by the PatchLink Update Server.



- Patch Compliance Assurance Mechanism (PCAM™):** PatchLink Update has the ability to lock down the information about a set of patches and update the configuration against a group of computers. If the compliance lock is broken, an email alert will be sent to the selected administrators. For example, a group of W2K computers may be created and called "IIS Servers." A compliance locking system is used to lock down all OS security patches and IIS related patches. If at any point the related patches or DLLs get replaced, PatchLink Update will send an email alert to the administrator(s). The computer(s) in question and the reason(s) for noncompliance can be identified quickly and easily. The compliance locking system can be used with mandatory patch deployment to automatically patch the system that is noncompliant. In this case, as soon as a patch or software is removed, they are reinstalled automatically and the administrator is notified by email.
- Content replication:** The server replicates the content from the PatchLink Update Master Archive over a highly secure link. This is done manually or automatically. The administrator can set a schedule or have the replication component of the server do it automatically at preset times.
- Software distribution:** Administrators have the flexibility of creating software packages. They can then deploy these packages in the same manner as other PatchLink packages to the client computers. For example, a package could contain Office 2000 and be deployed to every desktop.
- Content import/export:** For updating computers on networks that are not connected to the Internet, the server allows the hosted content to be exported and then imported into another

PatchLink Update Server. This is useful for highly secure networks such as within the military and government.

- **Building custom patches:** Administrators who have custom applications can use the “package create” option to create and rollout custom applications and patches. This feature allows any corporate application to be rolled out to any applicable operating system.
- **Recurring distribution task:** PatchLink Update Server has the ability to distribute corporate data such as white pages or Anti-Virus definition files to any operating system. Using the recurring schedules, a database or document can be continually distributed to all computers inside and outside of the enterprise, including to mobile users. This feature is useful when users have data files that need to be continually updated such as Anti-Virus definition files.
- **Fully automatic disaster recovery:** The “advanced disaster recovery” option allows the administrator to automatically recover from system failure such as hard disk crashes and server hardware failure. In the event of such failure, administrators simply create another server with the same DNS name and reinstall the PatchLink Update software with the same serial number. All agents will connect automatically and repopulate the system.
- **Multiple operating system support:** PatchLink Update Server is designed on open architecture and protocols to support such operating systems as the Windows family, UNIX family and NetWare. This product makes use of HTTP, HTTPS, XML, SSL and other Internet-standard protocols.
- **Automatic Caching System (ACS):** PatchLink Update Server will automatically cache packages that are marked as critical. This feature allows administrators to have the critical and security-related patches available for rapid deployment. During the Code Red and Nimda attacks, the Microsoft Web site was overwhelmed by users. Some users tried for hours to connect and download the related patches. PatchLink’s technology will automatically download the critical and security-related patches in the background and store them on the PatchLink Update Server. Then it will automatically scan for the computers that need the related patch. As administrators are notified about the critical patch

vulnerabilities, the package is also cached. Administrators can tell which packages are cached and which are not by simply looking at the related icons or selecting the detailed information on the packages. Other non-critical patches are automatically cached when they are first deployed.

Detection Reports by Group: Win2K Filter By: Detected

Info		Detection Reports	Inventory	Membership	Mandatory	Deployments	Total
	Report Name	Impact					
	MS02-013 - Java Applet Can Redirect Browser Traffic	Critical	0	2	0	0	2
	MS02-014-0313829 - Unchecked Buffer in Windows Shell Could Lead to Code Execution	Critical	0	2	0	0	2
	MS02-018-0319733: Cumulative Patch for Internet Information Service	Critical	0	3	0	0	3
	MS02-022-0321661: Unchecked Buffer in MSN Chat Control (MSN Messenger)	Critical	1	0	0	0	1
	MS02-023-0321232: 15 May 2002 Cumulative Patch for Internet Explorer	Critical	0	2	0	0	2
	MS02-024-0320206: Authentication Flaw in Windows Debugger can Lead to Elevated Privileges	Critical	0	3	0	0	3
	Norton Antivirus Def files (Jun 10, 2002)	Critical	0	3	0	0	3
	PatchLink Update Server Release 3.01.10	Critical	0	3	0	0	3
	Win2K - Security Rollup Package, January, 2002	Critical	0	2	0	0	2
	Win2K Service Pack 2	Critical	2	1	0	0	3
	MS01-033-CODE RED-0300972 Unchecked Buffer in Index Server ISAPI Extension	Critical - 01	0	3	0	0	3
	MS02-004-0307298-Unchecked Buffer in Telnet Server Could Lead to Arbitrary Code Execution	Critical - 01	0	3	0	0	3
	MS02-008 - XMLHTTP Control Can Allow Access to Local Files for MSXML 2.6	Critical - 01	0	1	0	0	1

- Intelligent Multiple Patch Deployment (IMPD™):** IMPD technology allows the proper patches to be deployed on the correct operating system. For example, Microsoft may have a bulletin for MSxx-xxx that has several different patches for various platforms. In this situation, administrators can simply select MSxx-xxx for deployment and then select all required computers regardless of the OS. The IMPD ensures that the patch gets installed on the proper operating system — the patch for the 9x platform would install on the 9x OS, the patch for NT would install on the NT OS, the patch for W2K would install on the W2K OS, and so on. This unique feature is used to speed up the patch deployment process so administrators do not have to determine which patch is for which platform.
- Applicable patch detection and patch interdependency:** This very important feature will help administrators select only the applicable patches for the client computers, eliminating the task of sorting through hundreds of unrelated patches. PatchLink Update will present the user with only the applicable patches for their specified environment. For example, PatchLink Update will show administrators the IIS related patches only if they have IIS installed on a client computer. For each patch, the application is first detected by using signatures and then the proper fingerprints are run against the application. This patent-pending process guarantees that when a patch is deployed, the client has the application and can install the patch. PatchLink Update will automatically calculate the interdependencies of patches against client computers. For example, on a W2K platform, PatchLink

Update will recommend Service Pack 2 and once Service Pack 2 is installed it will then recommend Security Rollup for that client since "Security Rollup" has a dependency on Service Pack 2. PatchLink Update reads both the registry and the file information for the correct fingerprinting to validate the patch identification.

- **Directory Neutral:** PatchLink Update is platform neutral and does not require a directory such as NDS, Domain or Active Directory to operate. However, the product is extremely flexible and can easily integrate with any network architecture.
- **Selective patch or software:** Patches are not automatically installed unless they are part of the mandatory patch baseline policy for a given group. Once administrators have tested and gained a level of confidence in a patch, they can add it to the mandatory baseline for a group. This will enable the patch to automatically deploy when a computer — a member of that group — indicates that it needs the patch. The master report view will show the matrix of all selected patches against all known computers. Computers are automatically grouped by that patches that they require.
- **Anti-Virus compatible:** PatchLink Update fully supports and is capable of patching and updating the definition and data files for Anti-Virus applications. This feature is used to make sure all corporate users including an organization's mobile workforce are updated with the latest Anti-Virus definition and data files.
- **Software inventory change control:** PatchLink Update has the ability to lock down the information about all of the installed software at client workstations within a group of computers. This feature is used to inform administrators about users who install new software or remove existing software on their computers. As new software is installed or existing software removed, an email

alert is sent to the selected administrators to inform them of the changes. The email includes the client computer name and the modifications done to that client computer.

+		<u>Microsoft .NET Framework (English) v1.0.3705</u>
+		<u>Microsoft FrontPage Server Extensions 2002</u>
+		<u>Microsoft Internet Explorer 6</u>
+		<u>Microsoft MapPoint 2002 North America</u>
-		<u>Microsoft Office 2000 SR-1 Premium</u>
<b>Computer Name</b>		
		\\ADMIN-PC
+		<u>Microsoft Project Server 2002</u>
+		<u>Microsoft SharePoint</u>
+		<u>Microsoft SQL Server 2000</u>

- Service change control:** Administrators can lock down the information about all of the services at client workstations within a group of computers. This feature is used to inform the administrator about users who stop or start certain services without their knowledge. As users change the status of their services, an email alert is sent to the selected administrator(s). The email includes the client computer names and the modifications done to the client computers.
- Hardware inventory change control:** PatchLink Update has the ability to lock down the information about all of the installed hardware at a client workstation within a group of computers. This feature is used to inform the administrator about users who add or remove hardware on their computers. If this feature is used, then as hardware is added or removed from the workstation, an email alert is sent to the selected administrator(s). The email includes the client computer name and the modifications done to that client computer.

+		<b>Hardware Device Classes</b>
+		BIOS
+		Computer
+		Disk drives
-		Display adapters
		<b>Device</b>
	+	ATI Technologies Inc. 3D RAGE IIC PC]
	+	Diamond Multimedia Fire GL1000 Pro
	-	Intel Corporation 810 Graphics Controller Hub
		<b>Computer Name</b>
		\\WIN2000PRO
	+	S3 VIRGE DX/GX
+		DVD/CD-ROM drives

- Uninstall and rollback an entire patch deployment:** PatchLink Update can take advantage of the patch uninstall capabilities and provide full rollback functionality to undo or “roll back” an entire deployment of a patch to the network. This function is used to uninstall a patch that has generated problems.
- Configurable agent policy with hours of operation for mission critical servers:** The configurable agent policy allows administrators to define the agent communication interval and operating hours. Agents are capable of communicating with the PatchLink Update Server even if they are behind a firewall. This is done with no modification to the firewall by taking advantage of HTTP and HTTPS protocols. Each client agent can have one or more policies active at a given time. This feature allows administrators to set up mission critical computers to only receive patches within a given time frame. For example, administrators may want policies set to only roll out patches to production servers between the hours of 12:00 AM and 2:00AM.

\*Polling Interval: 15 Minutes

Logging Level: None

Agent Timer: Disable

Agent Start: 12:00 AM

Stop Time: 2:00 AM

- Status by email notification:** The PatchLink Update Server has email notification that provides for each alert in the system to be sent to one or more administrators. These alerts include status of the deployment, new patches, low disk space and other errors that may happen during normal operation.

E-Mail Notification									
Current E-Mail Notifications									
	New Reports	New Agent Registrations	Subscription Failure	Deployment Failure	Low System Disk Space	Low Storage Disk Space	Low Available License Count	Up-Coming License Expiration	License Expiration
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- New Patch arrivals:** As new patches arrive into the system, the fingerprints are sent to the proper client agents to be scanned. An email is then sent to the administrator, which includes the patch impact and description of the patch.

## Scenarios

---

### **Managed Desktop and Servers**

As new patches are released, the PatchLink Update Server downloads the proper fingerprint from the PatchLink Update Master Archive and then checks to see if there are any computers that meet the profile by sending the fingerprints to the workstations to be scanned. The administrator is then notified of the new patch and its impact to the work environment. The report matrix quickly informs the administrator which computers or groups need the patch and which do not. The administrator simply selects a group or individual computers and deploys. The administrator can set the time of the deployment and decide whether or not to reboot after the patch installation.

### **Managed Data Center**

In a managed data center, the administrator creates a group for each cluster of servers. This will help the administrator manage thousands of computers easily. Administrators can test all critical updates published from the PatchLink Update Master Archive service before they are deployed to client computers on the network. After the testing has been successful, the administrator can then deploy the patch to all or just a group of computers. The use of agent policies will help the administrator to setup the hours of operation for each group of computers.

### **Automatic Client Updates**

From time to time, PatchLink Corporation creates a patch for its own software. Administrators can select the PatchLink client HotFix (just like any other patch) and update all client software.

### **Recurring Schedule**

PatchLink Update allows for recurring schedules to be created using the deployment wizard. Using recurring schedules, a database or document can be continuously distributed to all computers inside and outside the corporation including mobile users. Recurring schedules can also be used to reboot servers. For example, the administrator can create a recurring task that would reboot specific servers every Sunday at midnight.

## **Proactive Notification**

The administrator is automatically notified whenever anything changes in their patch, hardware, software and installed services configuration.

## **Building Custom Packages**

An administrator using a custom application may choose to update that application from time to time. Using PatchLink Update, the administrator can build a custom software package, patch or policy-specific script and then rollout to selected computers eliminating the need for additional software distribution products.

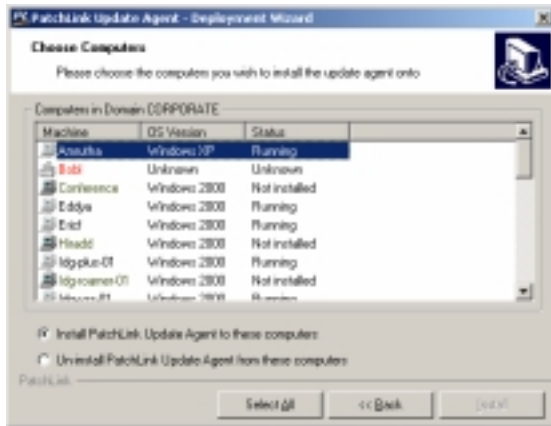
## **Automatic Replication**

The replication service is a server-side component that retrieves the latest critical updates from the private PatchLink Update Master Archive. As new updates are added to the PatchLink Update Master Archive, their meta data is downloaded automatically. If patches are marked as critical, they are downloaded and cached for rapid deployment. Each patch has an installer, prerequisite signature and fingerprint identification. Information is sent in one direction only; from the Master Archive to the user's PatchLink Update Server. All information is encrypted, CRC checked, compressed, digitally signed, and downloaded over a 128-bit SSL connection. The SSL connection validates and confirms the authenticity of the patch source.

## Client-Side: Agent Installation

### Installing Client Software

Client agent software can be installed by running a wizard that allows it to be pushed to all computers in the domain. Administrators can select all or individual computers to install the client agent software. The Client Agent has a control panel, which can be used to see the status of the agent software.



# Time Too Valuable to Waste Searching for Latest Security Updates

*Interliant Inc. Selects PatchLink Update for Automated Patch Detection and Distribution*

## Interliant Battens Down the “Security” Hatches

Interliant, Inc. is a leading provider of managed infrastructure solutions that encompass messaging, security and hosting plus an integrated set of professional services products. While these offerings make it easier and more cost-effective for Interliant customers to acquire, maintain and manage their IT infrastructures, these outsourced offerings are only as good as the security software the provider chooses to operate and maintain.

Fully understanding the critical nature of a secure environment, Interliant’s Manager of Windows Engineering George Velasquez decided to investigate new and better ways to solve a common patch detection and distribution dilemma — system administrators who quite simply don’t have the time to patch. Up until recently, Velasquez, caught in the same predicament as many other systems managers, was at the mercy of the manual patching nightmare — hours of upon hours of hot fixes and patch detection and distribution via the manual support of multiple systems administrators.

This tedious and costly approach to detecting and fixing security holes in the company’s enterprise Windows environment and its commitment to quality 24x7x365 uptime, ultimately led Velasquez to PatchLink Corporation and its premier automated patch detection and deployment solution — PatchLink Update.

## PatchLink Update Cost-Effectively Secures Interliant’s Enterprise Systems

Due to the mass hosting of its customers’ messaging and server infrastructures, Interliant depends on the reliability and scalability of the products the company incorporates into its network environment. “When Code Red hit, we couldn’t apply the patches fast enough and a stable and optimized environment is critical to our business and to our customers’ business as well,” said Velasquez. “We found PatchLink Update’s centralized patch distribution and hardware inventory capabilities to be very appealing. Another deciding factor was the attractive pricing model PatchLink uses for their update server and agents, making the product very affordable.”

PatchLink Update is patch vulnerability assessment and deployment software that has been the focus of PatchLink Corporation’s research and attention for the past five years. For large and small businesses alike, PatchLink Update automates the discovery, deployment and protection of corporate systems against patch-related security vulnerabilities like Code Red and NIMDA.

Interliant looked at a number of products before deciding to test PatchLink Update. The quality, reliability, and scalability of the product together with its affordability convinced Interliant to purchase and implement the vulnerability assessment and deployment software. By integrating this automated patch solution, Interliant has greatly improved its ability to protect its customers’ systems as well as its own from the onslaught of cyber-terrorism.

## PatchLink Update Eases the Pain

At the heart of Velasquez’s patching needs was a software solution that he could easily implement across several different server domains, operate, and train others to use that centralized the distribution of patches. Velasquez continues, “The old way [of patching] requires too many system administrators to complete the rollout of new patches and hot fixes. Coordination of the upgrades was sometimes a hassle and the overtime that was required for testing and completing patch and hot-fix installations was also a huge factor in our selection of PatchLink Update.”

As the industry’s first solution to automatically detect patch-related security vulnerabilities on all machines within a network, PatchLink Update provides a fast and efficient method for immediately patching security

holes across enterprise boundaries using a patent-pending Patch Fingerprinting technology. This technology works in conjunction with PatchLink's subscription-based Patch Archive, the largest patch repository of security and vendor patches available today. By utilizing the Patch Archive, customers can ensure that their corporate network inventory is always current with the latest patches.

### **Interliant Realizes Immediate ROI**

As easy as it is to install and rollout, one of the quantitative benefits that Interliant has already realized is improved productivity. "One system administrator is now able to perform the job of 10, and the time to implement a new patch has been reduced by 70 percent," cites Velasquez. While the hard numbers are still rolling in, it is safe to say that this type of increase in productivity is saving the Windows engineering group at Interliant thousands of dollars each month.

"Your company hit the nail on the head with this product offering," notes Velasquez. "Hands down, PatchLink Update is one of the best products I have tested for patching and hardware inventory. And, it doesn't hurt that the pricing for this security product is also very affordable."

### **About PatchLink Corporation**

Established in 1991, PatchLink Corporation has built a strong reputation in providing top quality software products at substantial savings to system and networking professionals. PatchLink is a leading provider of enterprise patch detection and deployment software and is one of the first companies to offer this capability over the Internet. The Company's software sets a new standard for the assessment and prevention of patch-related security breaches, in addition to monitoring and incident reporting. PatchLink's patch detection and deployment software is available via CD-ROM. Additionally, the Company maintains and markets WebConsole<sup>®</sup> IT Management Suite. PatchLink products are installed on more than 2 million network servers worldwide. For additional information on PatchLink, visit [www.patchlink.com](http://www.patchlink.com) or call 480.970.1025, Opt. 1.

# # #

Copyright (C) 2002 PatchLink Corporation. All rights reserved. PatchLink(tm), the PatchLink logo, Patch Fingerprinting and the PatchLink product names and logos are either registered trademarks or trademarks of PatchLink Corporation. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.