



## PatchLink<sup>®</sup> Update<sup>™</sup> 6.0 Technical White Paper

---

Cross-platform Security Patch Management  
and vulnerability detection and correction.



© PatchLink Corporation 1997-2004. ALL RIGHTS RESERVED

PatchLink Corporation  
3370 N. Hayden Road #123-175  
Scottsdale, AZ 85251  
T: 480.970.1025  
F: 480.970.6323

PLU6WP-V01-04-12-2004

<b>Abstract</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>The PATCHLINK UPDATE Solution</b>	<b>5</b>
Client-side Features	5
Server-side Features	8
<b>Scenarios</b>	<b>17</b>
Managed Desktop and Servers	17
Managed Data Center	17
Automatic Client Updates	17
Recurring Schedule	17
Proactive Notification	18
Building Custom Packages	18
Automatic Replication	18
<b>Client-Side: Agent Installation</b>	<b>19</b>
Installing Client Software	19
<b>PatchLink Customer Case Study</b>	<b>20</b>
<b>About PatchLink Corporation</b>	<b>22</b>

## Abstract

This white paper describes the features of PatchLink® Update™, a solution platform 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, 2K3), UNIX (Linux, Solaris, AIX, HP-UX, etc.), Apple MAC and Novell NetWare. PATCHLINK UPDATE 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 was founded in 1991 and 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 or vulnerability 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. User Control Over Reboot and Deployment**

PATCHLINK UPDATE allows administrators to give flexibility and control to the users by allowing users to interact with the PatchLink agent. Users can decide when to install a package or when to reboot. Some of the features of the User Control are:

- Reboot now or Snooze till later
- Install the Package now or later
- Snooze for a period of time

**c. Multiple Patch Deployment to multiple OS for rapid Deployment**

PATCHLINK UPDATE allows administrators to deploy a series of patches to series of Client computers with different OSs in one simple interface. This feature provides a list of applicable patches for the given list of computers and allows Administrators to quickly select all the patches that they need and deploy them. The PATCHLINK UPDATE Server automatically orders the patches in a proper sequence so they can be installed correctly.

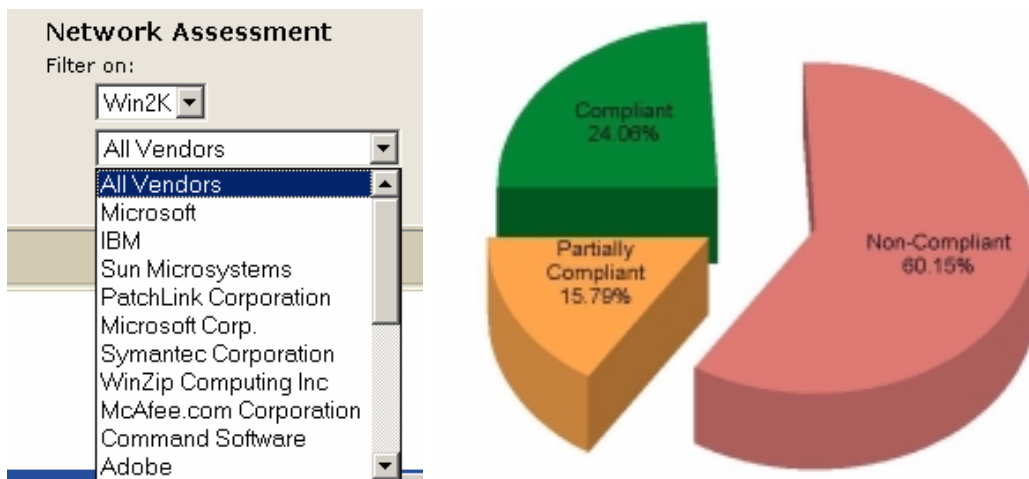
**d. Active Directory and LDAP integration**

PATCHLINK UPDATE easily integrates into existing Active directory or LDAP for Group Management and Client systems.

- Synchronize between directory groups and PATCHLINK UPDATE
- Synchronize computers between OU and PATCHLINK UPDATE

**e. Network Vulnerabilities Assessment**

Using the Network Vulnerabilities Assessment PATCHLINK UPDATE can quickly tell administrator how secure and compliant their network is against current patch related vulnerabilities. These reports can also provide Organization Management a level of understanding regarding current risks.



**f. 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 client patch delivery using HTTP or HTTPS. This server can also automatically cache critical patches from the PATCHLINK UPDATE Master Archive. Administrators can utilize the built-in software distribution feature to distribute any software package to any desktop.

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

After viewing the enterprise report matrix, the administrator can control which updates or packages from the PATCHLINK UPDATE Server are pushed to client computers. PatchLink recommends each patch be tested internally before deploying them to the 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 is 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	✓	✗	⚙	⚙	⚙	
MS02-016-0314147: Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run	Critical	1	6	0	0	7	
MS02-013 - Java Applet Can Redirect Browser Traffic	Critical	1	5	0	0	6	
MS02-014-0313829 - Unchecked Buffer in Windows Shell Could Lead to Code Execution	Critical	0	3	0	0	3	
MS02-018-0314733: Cumulative Patch for Internet Information Service	Critical	1	4	0	0	5	
MS02-022-0321661: Unchecked Buffer in MSN Chat Control (MSN Messenger)	Critical	4	1	0	0	5	

**h. 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. Rules set by the Administrator control the behavior of the patch installation during the patch deployment.

**i. Comprehensive patch testing**

PatchLink continuously researches, tests and approves patches before they are released by to customers. 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 variations 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 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.
- **Digital 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 digital fingerprints make up a detection report, which is viewable in the report matrix. The PatchLink Master Archive currently hosts one of the largest automated digital 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 bandwidth should be utilized during large deployments.
- **Chained installation:** The administrator can minimize repetitive rebooting by taking advantage of 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 and increases the uptime for mission critical computers. Qchain rearranges the DLL files 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>
		GenuineIntel x86 Family 6 Model 5 Stepping 2 at ~350MHz
		<b>Computer Name</b>
		\\EDDYA
+		GenuineIntel x86 Family 6 Model 7 Stepping 3 at ~498MHz
+		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 in an enterprise-wide solution. Agents accelerate the performance of large-scale deployments 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. This approach can be extremely slow and is 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, thus providing bandwidth-throttling capabilities.
- Agent-less Patch tools that require a domain connection and 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 have direct access to 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 identifies the reason why patch tools without an agent cannot operate on these platforms. PATCHLINK UPDATE securely covers the entire Windows family.

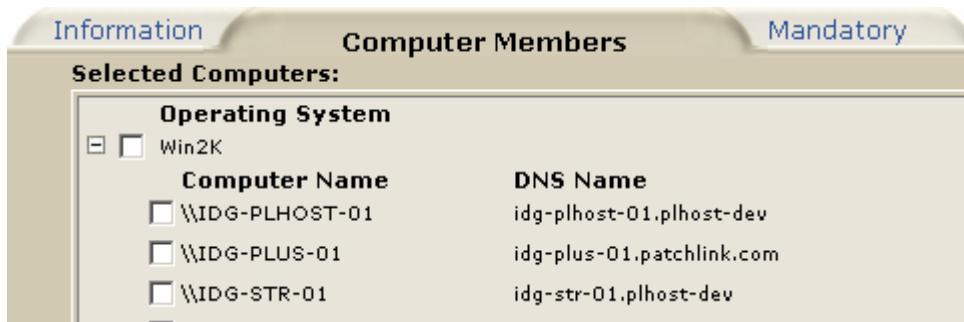
### Server-side Features

PATCHLINK UPDATE is based on PatchLink's proven technology for automated patch detection and deployment, enabling the management and distribution of critical patches and software packages that resolve known security vulnerabilities and other stability issues with. 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, including Windows 2003 Server. Internet Information Services (IIS) must be enabled on the server.

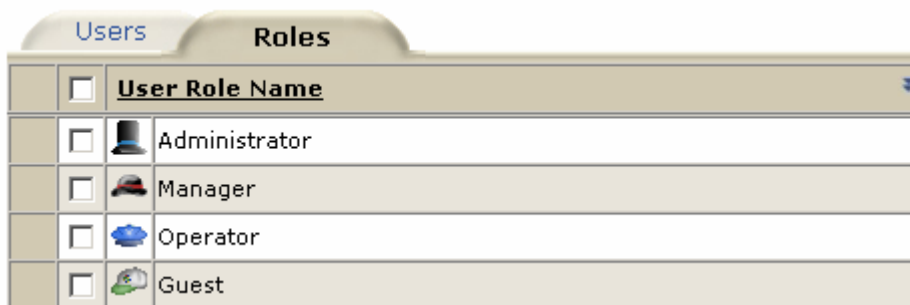
The server features include:

- **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.



- Role-based Administration Control:** The Administrator can create arbitrary Roles for Server users to only have access to a certain section of the application. Users can be assigned to manage only certain computers. This feature allows for administrators to create groups of computers that are managed by Operators or Managers who are responsible for that group. This feature also narrows the view and control of the product only to the computers that have been assigned to Operators while using a single PatchLink Server. The Administrator can manage and view all computers while Operators and other users with restricted access can only manage computers that were assigned to them by the Administrator.



- Built-in security:** The administrative pages are restricted to administrators on the PATCHLINK UPDATE Server. 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.

+	<input type="checkbox"/>		MS00-077 - NetMeeting Desktop Sharing Vulnerability
-	<input type="checkbox"/>		MS00-078 - Web Server Folder Traversal security vulnerability 2K

The entire package has successfully been downloaded from the host site. It is ready for deployment to computers.

Status: *Enabled*

Version: *4*

Request Status: *Successfully Requested*

Replication Status: *Package has been replicated.*

Created By: *PatchLink Corp.*

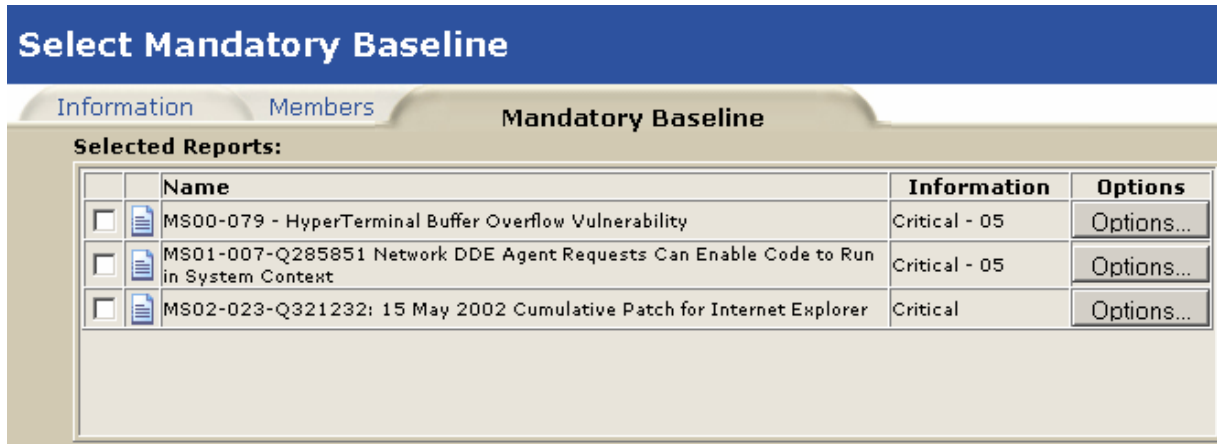
Created On: *9/23/2001 10:09:14 PM*

- 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, Oracle, Corel, Symantec, McAfee, Sophos, Command, Real Audio, MP3, Compaq, WinZip, Citrix, Novell and many others. This critical feature provides clients with a more secure network.



- Mandatory patch policy with automatic deployment and automatic ordering for single reboot:** 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, MS03-041, MS03-042, MS03-043, Adobe Acrobat Reader 5.0 and Service Pack 4, then all computers that join this group will automatically have, MS03-041, MS03-04, MS03-043, Adobe Acrobat Reader 5.0 and Service Pack 4 installed on them automatically. These patches are ordered

and qchained together to minimize reboots. Patches that are over-written by tape backup restorations 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 are replaced, PATCHLINK UPDATE will send an email alert to the administrator(s). The computer(s) in question and the reason(s) for non-compliance can be identified quickly and easily. The compliance locking system can be used with mandatory patch deployment to automatically patch the system that is non-compliant. In this case, as soon as a locked patch or application is removed, it is 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 manage it automatically at preset times.
- Software distribution:** Administrators have the flexibility to create software distribution packages. They can then deploy these packages in the same manner as other PatchLink packages. For example, a package could contain the Office 2000 installer and be deployed to every desktop in a department.

- **Content import/export:** For updating computers on networks that are not connected to the Internet, the server allows patches 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 that require complete isolation.
- **Building custom patches:** Administrators who have custom applications can use the package creation option to build and rollout custom applications and patches. This feature allows any corporate application to be rolled out to any applicable operating system.
- **Recurring distributions:** PATCHLINK UPDATE Server has the ability to distribute corporate data such as white pages or Anti-Virus definition files to any operating system. Using recurring schedules, any 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” capability 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 to meet mandatory baselines.
- **Multiple operating system support:** PATCHLINK UPDATE Server is designed on open standards and protocols to support operating systems such 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: Deleted

Info	Detection Reports	Inventory	Membership	Mandatory	Deployments	Total
<input type="checkbox"/>		<b>Report Name</b>		<b>Impact</b>		
<input type="checkbox"/>		MS02-013 - Java Applet Can Redirect Browser Traffic		Critical	0 2 0 0 0 2	2
<input type="checkbox"/>		MS02-014-0313829 - Unchecked Buffer in Windows Shell Could Lead to Code Execution		Critical	0 2 0 0 0 2	2
<input type="checkbox"/>		MS02-018-0319733: Cumulative Patch for Internet Information Service		Critical	0 3 0 0 0 3	3
<input type="checkbox"/>		MS02-022-0321661: Unchecked Buffer in MSN Chat Control (MSN Messenger)		Critical	1 0 0 0 0 1	1
<input type="checkbox"/>		MS02-023-0321232: 15 May 2002 Cumulative Patch for Internet Explorer		Critical	0 2 0 0 0 2	2
<input type="checkbox"/>		MS02-024-0320205: Authentication Flaw in Windows Debugger can Lead to Elevated Privileges		Critical	0 3 0 0 0 3	3
<input type="checkbox"/>		Norton AntiVirus Def files (Jun 10, 2002)		Critical	0 3 0 0 0 3	3
<input type="checkbox"/>		PatchLink Update Server Release 3.01.10		Critical	0 3 0 0 0 3	3
<input type="checkbox"/>		Win2K - Security Rollup Package, January, 2002		Critical	0 2 0 0 0 2	2
<input type="checkbox"/>		Win2K Service Pack 2		Critical	2 1 0 0 0 3	3
<input type="checkbox"/>		MS01-039-CODE RED-0300972 Unchecked Buffer in Index Server ISAPI Extension		Critical - 01	0 3 0 0 0 3	3
<input type="checkbox"/>		MS02-004-0307298-Unchecked Buffer in Telnet Server Could Lead to Arbitrary Code Execution		Critical - 01	0 3 0 0 0 3	3
<input type="checkbox"/>		MS02-008 - XMLHTTP Control Can Allow Access to Local Files for MSXML 2.6		Critical - 01	0 1 0 0 0 1	1

- Intelligent Multiple Patch Deployment (IMPD™):** IMPD technology ensures that proper patches are deployed to 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 is installed on the proper operating system — the patch for the 9x platform will install on the 9x OS, the patch for NT will 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 because administrators do not have to determine which patch is for which platform.
- Applicable patch detection and patch interdependency:** This very important feature helps administrators select only the applicable patches specific client computers, eliminating the task of sorting through hundreds of unrelated patches. PATCHLINK UPDATE presents the administrator 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 through 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 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 deployment:** 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. In the report view, 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 greatly simplifies the effort to ensure 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 a patch's specific uninstall capabilities and provide full rollback functionality to undo or "roll back" an entire deployment. This function is typically used to uninstall a patch that has generated problems. (Only available if the patch was built by the software manufacturer to support rollback functionality).
- 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.

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 an individual computer or a group and then 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 large numbers of servers 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 servers. The use of agent policies will help the administrator to setup the hours of operation for each group of servers.

### **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. This can then be rolled out to selected computers eliminating the need for additional software distribution products.

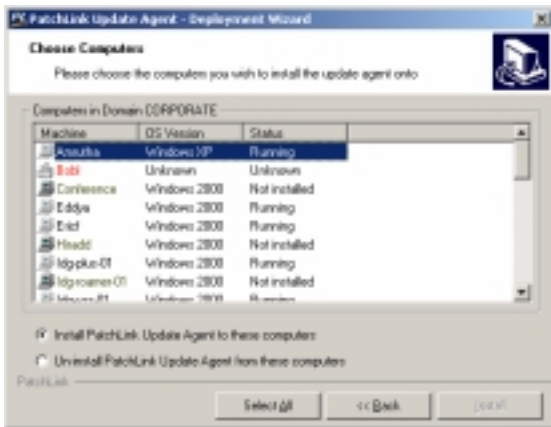
### **Secured Automatic Replication**

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. The initial investment was only \$995 for the server software and \$12 for each single-user license (per year). 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® 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.