

White Paper

PatchLink Vulnerability Management for Managed Services

Delivering the most advanced vulnerability management solution available today in a managed services model.

May 2006



"Over 90% of security exploits are carried out through vulnerabilities for which there are known patches."

Source: Gartner Group

"Companies may avoid the capital expenses of effective security by letting outside providers own some of the equipment."

Steve Hunt, Giga Information Group

"Managed security services will maintain its current trajectory to attract customer adoption"

Allan Carey, IDC

Introduction

Today's IT organizations face an almost insurmountable task – securing large numbers of computers from the never-ending barrage of malicious attacks, while at the same time facing an ever-increasing number and complexity of vulnerabilities. According to the Carnegie Mellon University CERT Coordination Center, a major reporting center for Internet security attacks; there have been more than 300,000 security exploits in the past 5 years alone. Shockingly, over 90% of these attacks are leveled against know vulnerabilities for which there is a publicly available patch.

The consistent and systematic application of security patches would all but eliminate the impact from external security attacks. Unfortunately, many companies - especially small and medium-sized businesses (SMBs) – lack the expertise or resources to effectively implement and manage an automated security patch and vulnerability management solution.

Managed Services for Vulnerability Management – a Growth Market

A recent study by Secure Enterprise shows that over 64% of IT groups are understaffed. The technical staff designated to prevent malicious activities and comply with federal regulations is simply stretched too thin. A separate study found that 60 percent of businesses were "unprepared" and lacked the necessary resources to handle their IT security. Unfortunately, this is not uncommon. Many businesses today are wholly unprepared to deal with IT security in any meaningful way. Even if they could identify the appropriate human resources, the cost of obtaining those resources would be prohibitive. "Companies may avoid the capital expenses of effective security by letting outside providers own some of the equipment. Good security staffs are difficult to find, and most companies have not elected to train, develop and retain security expertise in-house. For those reasons, leveraging the skills and personnel of an outsourcing vendor is very appealing."

There are simply not enough budget and man hours available to most IT organizations to protect their computers against the myriad of security threats using traditional methods.

In response to the dual challenge of increasing security threats and fewer resources, IDC projects that the managed security services market will surpass \$21.7 billion by 2007, and Gartner Research predicts an annual growth rate of 60 percent for the next several years. While the adoption of managed services for areas such as network firewalls and intrusion detection has been widespread, the market for managed vulnerability assessment and remediation services has yet to be exploited. The inability to internally manage the enormous challenge of identifying and remediating network vulnerabilities is fueling dramatic growth in this market segment. The MSSP market is anticipated to grow incrementally as organizations take a more proactive approach to network security," said Allan Carey, program manager of IDC.

"More organizations will look to managed security services providers that offer integrated security solutions and services, including security patch and vulnerability management that are designed to simplify and automate

“PatchLink offers value by enabling MSSPs to deliver automated scanning, assessment and remediation capabilities at customer sites”

Allan Carey, IDC

processes. To this end, PatchLink offers value by enabling MSSPs to deliver automated scanning, assessment and remediation capabilities at customer sites combined with custom content delivery, asset tracking and inventory and remote machine management capabilities.” Because of the economies of scale, outsourcing is often cheaper and of a higher quality than an end user can provide with in-house resources. Managed services allow a company to operate with a reduced staff while realizing increased value from more efficient use of the managed service provider’s infrastructure investment.

The Solution – PatchLink Update for Managed Services

So how do organizations ensure that their IT resources are secure when their budget won’t support an initial investment in vulnerability management hardware and software? The answer is the PatchLink Update for managed services platform. The PatchLink Update for managed services platform allows our managed services partners to address this opportunity – by remotely assessing customers’ network resources and distributing necessary security patches, as well as ongoing monitoring and detailed status reports.

PatchLink’s Managed Security platform enables you to offer your customers the power of PatchLink Update; the world’s most advanced automated patch management solution, in a proven hosted model. “As the main data center for 137 community banks and credit unions throughout the Northeastern United States, COCC is really on the front lines for these institutions when it comes to protecting

them from a wide range of technical and security risks,” said Brent Biernat, AVP – Network Management at Avon, a Connecticut-based COCC. “PatchLink helps our clients through their annual banking examinations, which are critical to business continuity, by automating and documenting their software update process. Our clients couldn’t get the job done without PatchLink.”

The PatchLink Managed Security Services solutions provides our managed services partners with hosted patch management capabilities that relieve the security burden from your customers’ overly stressed IT departments.

PatchLink Update for Managed Services Benefits

The primary benefit managed service providers will gain by adding the PatchLink Update managed services platform to their services portfolio is the increase in high margin revenue. As margins on traditional hardware and software sales continue to decrease, managed services provide a means to increase revenue and maintain profitability. Secondary benefits include the penetration of new accounts, improved response to customer demands, a renewable and consistent revenue stream, and operational efficiencies. The services model also makes it easier to form

"stickier" relationships with clients by adding new services as they become available.

- ☑ **Revenue Growth** - new sales opportunities to customers that lack the resources to bring an automated patch management solution on site, and hire/train appropriate personnel
- ☑ **Increased Profitability** - higher-margin revenue to offset shrinking margins in commoditized hardware and software
- ☑ **Revenue Predictability** - renewable revenue stream through ongoing monthly patch subscription
- ☑ **Expanded Service Offering** - ability to offer customers accurate and cost-effective solution to complex security challenges
- ☑ **Cost Reduction** - streamlined business processes and efficient use of staff - managing multiple customers from a single security assessment and remediation interface
- ☑ **Consistent Customer Service Levels** - respond to customer demands for greater flexibility in the management of their technical security

In addition to providing numerous benefits to the managed services provider, the solution will dramatically impact end-users. It is sometimes all an IT department can do to keep their organization's network protected, much less have time to focus on the core competencies necessary to propel the interests of the organization forward. Delivering vulnerability assessment and remediation as a service will allow your customers to focus on high-value activities. Additionally, the system will eliminate some of the pressures of regulatory compliance and of maintaining a

24/7 watch over their IT assets. PatchLink Update managed services platform allows your customers to:

- Focus on the core IT competencies necessary to propel their organization forward
- Leverage the power of PatchLink Update without the initial capital investment
- Receive automated audit & reporting support for regulatory compliance
- Ensure consistent, effective asset inventory and security monitoring of your IT resources

PatchLink Update for Managed Services – How it Works

PatchLink Update is a leading enterprise-level, security patch and vulnerability management solution that gives managed services providers an automated, cross-platform, and vendor-neutral security system for detecting vulnerabilities and deploying system and application patches throughout their customers' networks. PatchLink Update is the only fully Internet-based security patch management software for all Microsoft, AIX, HP-UX, Solaris, Linux, Novell NetWare, and Mac OS-X operating systems. PatchLink Update is

“PatchLink helps our clients... by automating and documenting their software update process”

Brent Biernat, COCC

extremely scalable and can support redundant and high-availability topologies including clustering, auto failover and load-balancing.

“With the emergence of new generation threats, security concerns continue to top our customers’ priority lists and we are seeing a strong demand for patch management,” said Matthew Sutton, CEO of HyBlue, a leading IT security MSSP.

“To meet customer demand and complete our security portfolio, we needed to find the best vulnerability management solution. PatchLink rose to the top after a thorough evaluation of patch management solutions based on its cross-platform support, fingerprinting technology and extensive patch repository. PatchLink Update allows us to efficiently manage customer client machines to reduce downtime, increase network security and reduce costs associated with patch management. PatchLink Update, combined with HyBlue’s unique system monitoring provides a unique value to our customers”

PatchLink Update utilizes an agent-based system to maximize security accuracy and system scalability. The local agents provide an array of functions, including patented Patch Fingerprinting™ (to determine what patches are absent on a host), software inventorying, service monitoring, hardware profiling, customizable polling, and certain aspects of network attachment control and system quarantine for noncompliant systems. With our advanced Agent Management Center (AMC) dashboard, managed services professionals can quickly and efficiently roll out agents to all of the servers and desktops within their customers’ networks.

Once installed, the agents consistently run a detailed file and registry scan to identify the vulnerabilities that exist on each registered computer. The managed services partner uses this information to develop a comprehensive analysis of the necessary patches, hot fixes, service packs and software updates. Once patch levels are assessed and inventoried and appropriate patches are securely downloaded from the PatchLink Global Patch Repository to your local managed services PatchLink Update Master Server through your patch subscription. PatchLink Update’s remediation capabilities give our MSPs partners the ability to automatically distribute these patches to servers and/or desktops throughout your customer sites, depending on policy-based rules and patch management best practice standards.

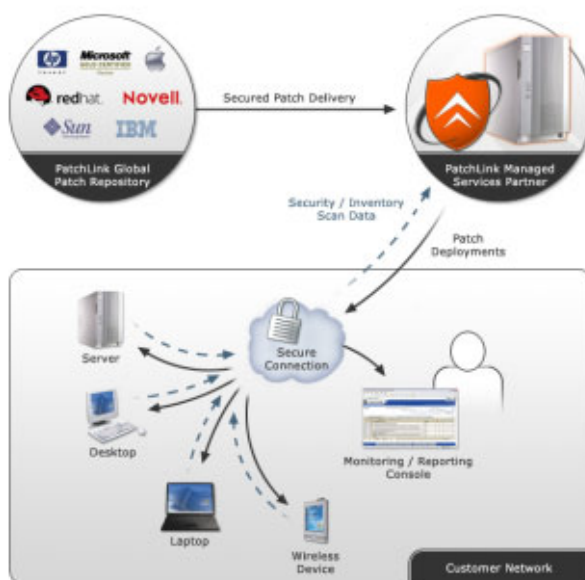


Note: As recommended with all patches, you should first deploy the patch within your test environment before rolling it out into production.

In order to expedite patch distribution for managed services providers that work with large, geographically dispersed customers, PatchLink Update uses a hierarchical model via its PatchLink Distribution Point™ (PDP) technology. PatchLink PDP provides multi-tiered distribution capabilities that optimizes the propagation of patches and provides synchronization among multiple distribution servers for high availability and resiliency to service outages. If desired, PatchLink’s FastPatch™ technology can allow target hosts to automatically determine the nearest managed services distribution server, in order to minimize the impact on bandwidth and to improve the speed of

deployment. This feature is particularly useful for wide area network, branch office, and other low-bandwidth sites. PatchLink Update also allows our MSSP partners to create delegated administrator accounts, in order to support a disparate install base using a distributed management model.

PatchLink Update has also been designed for administrative flexibility and ease-of-use, with customer grouping according to multiple criteria and an easy easy-to-use web based graphical user interface. All customer administration, audit and reporting can be done using a Web browser. Because of the high level of automation and ease of use, PatchLink Update can greatly reduce the time it takes to mitigate your customers' server and workstation services vulnerabilities. And the web-based design enables you provide your managed services customers' with visibility into the patch analysis and remediation process.



Unique Capabilities of the PatchLink MSSP Solution

PatchLink has been delivering our award-winning PatchLink Update solution in a hosted managed services model for several years. As a 100% web based solution that relies on remote agents for patch analysis and remediation with a highly secure subscription model, our platform is uniquely suited for delivery via managed services (for a complete feature list, please refer to Appendix A):

Multi-platform Support - one of the greatest challenges managed security providers face is supporting heterogeneous IT environments. PatchLink Update's combination of a continuous multi-vendor patch subscription with a cross-platform agent-based assessment and remediation process is ideally suited for a heterogonous managed services model.

Rapid Deployment - with PatchLink Update, you can be up and providing services to your customers within hours. Server software installation is quick

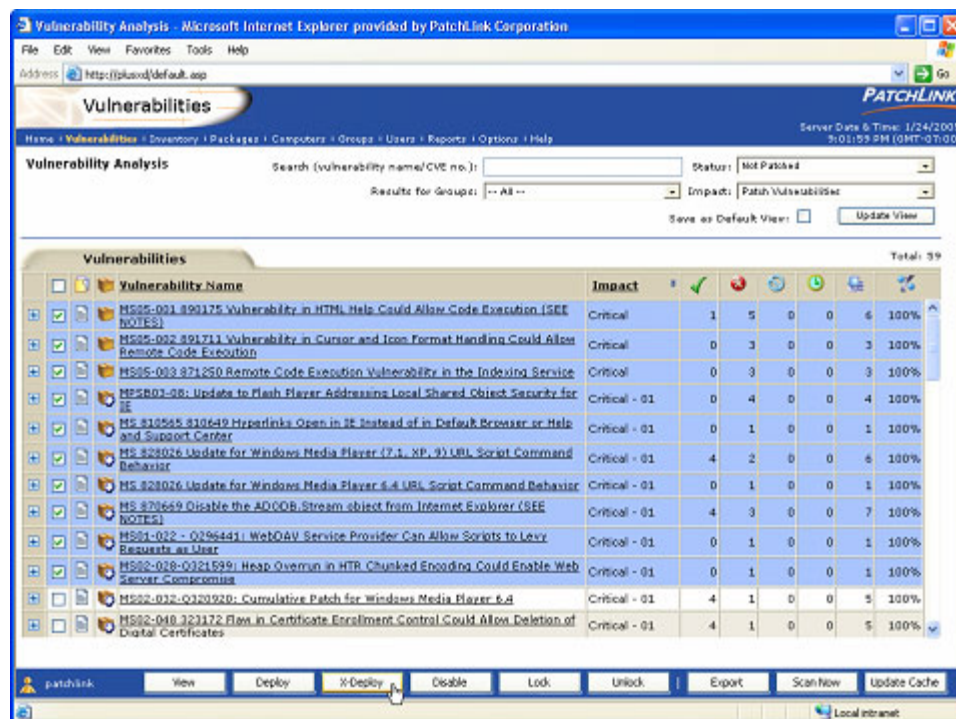


and easy. Agent deployment is fast and flexible through numerous wizard-assisted agent distribution mechanisms that simplify installation, and maintenance of agents across your diverse customer base. The administrative console is a simple yet powerful web-based interface with built-in role based security, alerts, and wizards.

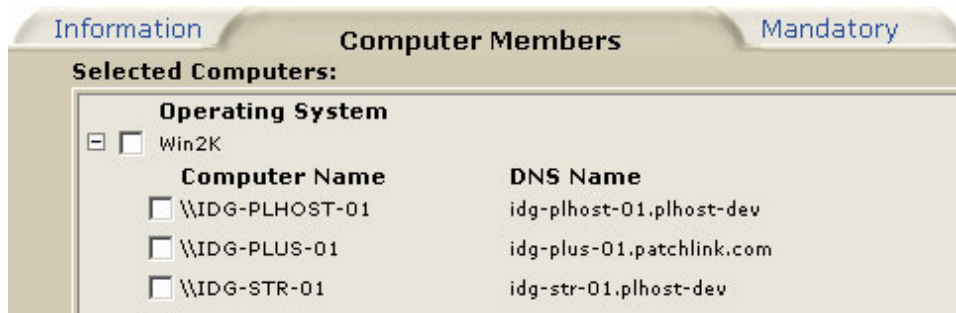
Comprehensive Patch Testing - PatchLink tests each patch it collects against over 250 standard images to provide an extra level of protection against inadvertent negative impact in your environment. During the testing process, our quality assurance professionals note any anomalous behavior encountered during patch installation, as well as any side effects experienced during the use of common applications, following that patch's installation. Patches that are found to be defective or to consistently interfere with normal computer operations are rejected by these engineers and are not added to the repository. In the event of a rejected patch, we work with the vendor that created the patch to correct the problem. Patches that are accepted are "packaged" – to include patented fingerprint assessment technology and installation information.

Ongoing Customer Vulnerability Assessment and Remediation Status -

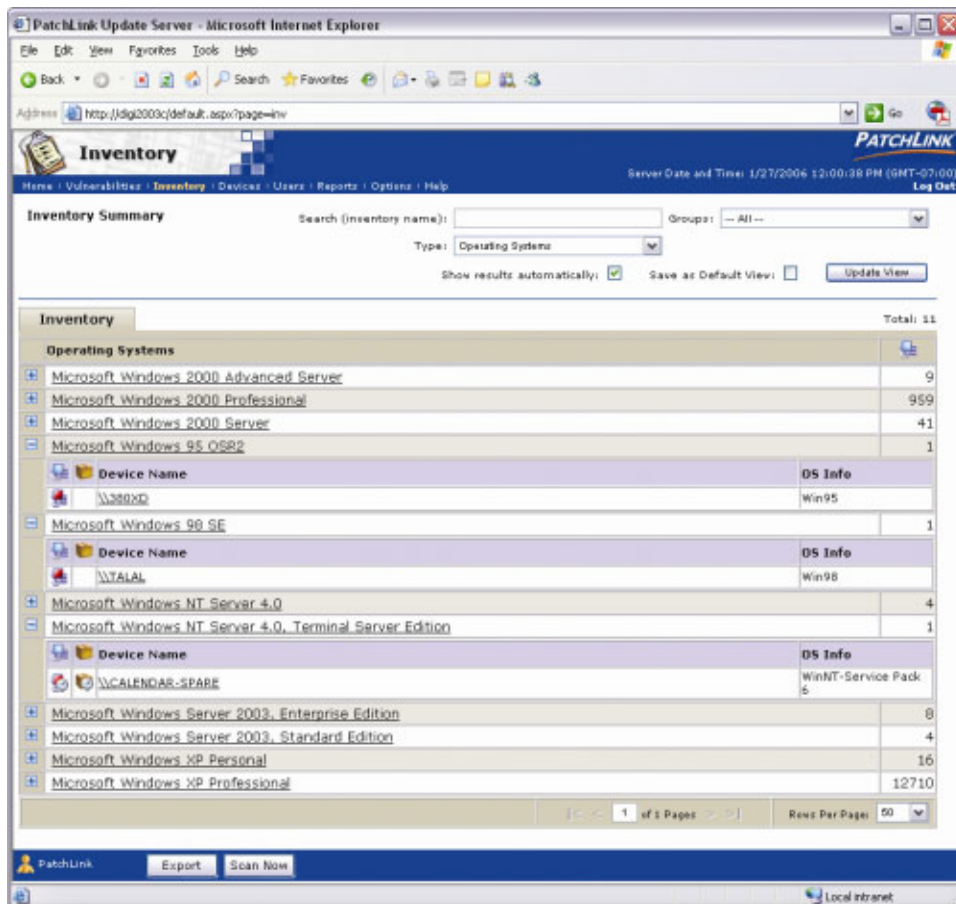
All client-side agents scan the local machines on a regular basis to determine the specific patch updates that are required to meet pre-defined security policies. These remote agents communicate these requirements to your managed services PatchLink Update Server, which aggregates the information to generate a security matrix for all of the customers' machines (see sample screen shot below). You can then provide this information to your customers on a regular basis.



Flexible Customer Setup - setup and track clients with extraordinary ease and detail. Multi-level grouping enables you to create the level of detail for tracking on a client by client basis. Work with single or multiple servers and workstations or cross client and cross domain quickly and easily.



Accurate Asset Discovery – the PatchLink Update agent will perform a comprehensive internal scan of the hardware, software, and services on each of the machines on your customers’ networks – including servers, desktops and mobile machines. This solution will allow you to quickly and accurately identify the technical resources throughout these networks, the way those assets are being used (or misused), and whether or not the asset is currently in compliance with stated configuration and licensing policies.



Patented Threat Assessment and Remediation – leverage a patented fingerprint technology to accurately assess the security threats in your customers’ networks. Once threats are identified, they can be automatically remediated according to your customers’ security policies using our unique mandatory baseline function.

Secure, Flexible Management and Reporting – a key component of successful managed services is client communication. PatchLink Update provides detailed reports that let you inform your customers of their vulnerability management and regulatory compliance progress along with asset inventorying - and simplifies your system administration.

Reports Patch Status for Win2K



Extensive Sales and Marketing Support - PatchLink supports our managed services providers with a wide variety of tools, resources and demand generation activities that will help you bring the PatchLink Update for managed services platform to your regional area, including:

- Co-operative market development funds (MDF based on sales volume and training expenses)
- A quick-start pack of marketing material (Brochures, Data Sheets, White Papers, Presentations)
- Case Studies, Press Releases, 3rd Party Review, etc)
- A streamlined start-up process – offer managed security services within a few days
- Use of PatchLink Authorized Partner logo
- Online and regional classroom training resources
- Direct access to PatchLink through an assigned Territory Account Manager
- Listing on PatchLink partner Web site as a Services Partner
- Joint PR and co-branded marketing activities
- Lead referrals
- Flexible licensing options
- Access to the secure partner web portal
- Comprehensive technical support plan based on the requirements of the solution

Potential Pitfalls of Managed Security Services

Like any new technical implementation, there are a few potential roadblocks to the successful entry into the managed services market for vulnerability management. The single biggest mistake that solution providers make when entering this market is attempting to attract customers using the same sales approach that was used for the more traditional model. When selling security services, you must gain an in-depth understanding of your customers' security objectives, current policies and technical environment. The second major mistake has to do with hiring security generalists to implement the managed services platform. Generally,

customers will pay a negotiated set rate for services, no matter how long it takes a MSP to deliver. Having qualified personnel that understand the vulnerability management process will ensure your implementations remain highly profitable. Other challenges to hosted vulnerability management success include pricing on a cost-basis instead of the value delivered, failing to provide your technical sales and support staff with in-depth training, or attempting to add a vulnerability management technology that was not designed to be delivered in a hosted model. Experts also highly recommend that MSPs focus on recurring revenue models and standardize on extensible technology platforms to develop reusable expertise.

Conclusion

Managed security services solutions are transforming the channel. Solution providers are adopting managed services to expand offset shrinking margins in commoditized hardware and software, penetrate new business opportunities and relieve the burden of regulatory compliance requirements that now demand an enormous amount of their customer's time and effort. According to the 2006 VARBusiness State of the Market (SOM) survey, most solution providers are offering a service in some form or are planning to in the coming year. Solution providers expanding beyond product sales earn, on average, nearly a quarter of their revenue from managed services. The key is ensuring that managed services run with the same level of transparency that they would on-site. Properly implemented, vulnerability management in managed services model with PatchLink Update has the potential to create more consistent, higher-margin revenue streams while streamlining business processes. For information on becoming a PatchLink Managed Services Partner, please contact PatchLink MSP Development at 480-444-1681, e-mail businessdevelopment@patchlink.com, or visit us at patchlink.com/partners/.



PatchLink Corporation
Scottsdale, AZ 85255
480.970.1025

www.patchlink.com

Appendix A: PatchLink Update Features

Requirement	PatchLink Product/Capability
Agent-Based	Enables protection of laptop and mobile devices that are often disconnected from the network and reduces network bandwidth usage
Asset Management	PatchLink agent identifies and reports all software, hardware and services inventory and supports software distribution
Audit & Recovery	Ensures ongoing compliance with security policies and ability to recover from crashes
Automated Agent Distribution	Allows you to locate unmanaged network endpoints and deploy the patching agent, ensuring maximum coverage and protection
Automatic Notifications	Distribution of e-mail alerts directly to administrator(s) allows for proactive security and administrative management
Comprehensive Patch Testing	Reduces the risk that a patch may inadvertently cause a negative impact on the network
Digital Fingerprint™ Accuracy	PatchLink's unique assessment approach ensures the highest level of accuracy in the detection of security vulnerabilities
Market-Leading Patch Repository	Support for all major OS and applications used in the enterprise to ensure that all software is accurately patched
Flexible Application Reporting	Simple yet powerful status and audit tools allow quick and easy management reports on the status of the organization's security
Flexible Scanning and Deployments	Allows the Administrator to control the scanning and patch distribution schedule to minimize business disruptions
Fully Internet-Based	Communications based upon standard protocols (TCP-IP/ HTTP & HTTPS) ensuring maximum accessibility and ease of use
Group Management	Ability to create customer computer groups increases IT efficiency
Highly Scalable	High-availability topologies and PatchLink Distribution Point architecture ensures complete coverage for the largest worldwide networks
Web Interface	Enables wide access to an easy-to-use administrative interface
Multi-Patch Deployments	Ability to deliver multiple patches to multiple computers in one distribution increases IT productivity
Multi-Platform Support	Enables you to secure all operating systems in heterogeneous networks, including Windows, UNIX, Linux, Apple, and Novell.
Patch Compliance Alerts	If a patch is removed or dropped due to restoring a backup or installing a new application, an e-mail alert can be sent to notify of the missing patch
Policy-Based Administration	Ensures that all systems meet a mandatory baseline policy – a key aspect of regulatory compliance

Role-Based Administration	Enables System Administrator to delegate activities to improve productivity while maintaining security
Subscription Service	Secure download of pre-tested and pre-packaged patches from a dedicated PatchLink host ensures no unauthorized packages enter your network