Exposé Your Threats with Unparalleled Vulnerability Assessment

With more than 30,000 known software vulnerabilities and countless configuration and access point threats, identifying all of the risks to your network can seem overwhelming.

Fortunately, there is a way. The Vulnerability Assessment Solution from PatchLink is an essential Common Criteria EAL2 certified network security tool that will identify and display all potential threats, on all of your network devices, quickly and with absolute precision.

Vulnerability Assessment Solution:

The PatchLink Vulnerability Assessment Solution is comprised of two leading security products; PatchLink Scan™ and the PatchLink Security Management Console™ (Enterprise or Standard edition). These two products work together seamlessly to:

- Rapidly identify and inventory all devices on your network
- Scan (network-based) all devices for software and configuration-based vulnerabilities
- Prioritize identified threats against a robust vulnerability database
- Deliver comprehensive reports of scan results

Rapid and Complete Asset Discovery

You can only secure the devices you know about. The PatchLink Vulnerability Assessment Solution thoroughly identifies and inventories all of the assets running on your network, including servers, desktops, laptops, routers, switches, printers, wireless access points, and more. This discovery can be performed using IP ranges, Active Directory, and/or Network Neighborhood enumerations. And discovery methods can be used separately or in conjunction, as the management console transparently merges all results into a single, cohesive asset list.

* Carnegie Mellon University's Computer Emergency Response Team (CERT) reports 30,780 known vulnerabilities between 1995 and 2006
Accurate Threat Assessment and Prioritization

The PatchLink Vulnerability Assessment Solution was designed to deliver a solid balance of scan speed and accuracy via its adaptive scan techniques and false response correlation technology. Through deep inspection of target systems that includes redundant file attribute and registry value correlation, as well as SSH tunneling and authenticated OS fingerprinting refinement, the scanner identifies all software threats, including missing patches, out-of-date antivirus signatures, worms, Trojans, and more. The scan also runs detailed configuration checks on ports, users, shares, groups, agents and services. To guarantee thorough analysis, the solution is able to adapt its scanning technique based on its level of access, with the ability to run anonymous scans against target systems upon which it cannot authenticate.

The powerful yet easy to use role-based PatchLink Security Management Console displays all relevant information for each device and vulnerability discovered during a particular scan. The solution prioritizes vulnerabilities based on critical asset and vulnerability score-carding to aid in the remediation process. The solution also provides remediation information and recommendations for implementing corrective action. This resource database is based on the knowledge of a team of expert security engineers who continually research security advisories, knowledge base papers and professional security group articles.

Advanced Vulnerability and Compliance Reporting

To provide insightful and concise views of the security posture of your network, the PatchLink Vulnerability Assessment Solution includes a wide range of executive summary and detailed administrative reports. The reports can include aggregated or detailed information on scan configurations, vulnerabilities, policy compliance and more, enabling quick analysis of potential threats and severity levels to help you determine the best action plan. The reporting capability provides simple point and click capability to quickly ascertain the enterprise security posture relative to common industry tracking mechanisms, including SANs, bugtraq, CVE, IAW, CERT and many more.

The Common Criteria EAL2 certified PatchLink Vulnerability Assessment Solution will help you proactively identify all potential threats to your network. For more information, contact us today at 480 970-1025 (option1) or sales@patchlink.com, or visit our website at www.patchlink.com/solutions/pvas.aspx.

Features & Benefits

Complete Asset Discovery
Identifies all network devices and performs configuration and informational checks on ports, services, users, shares and groups

Comprehensive Scan Coverage
Performs checks of antivirus, sharing tools, worms, Trojans, configuration issues and more on Windows NT®, Windows® 95/98/2000/Me/XP, Windows® Server 2003, Sun® Solaris™, HP-UX, RedHat™/Mandrake Linux®, HP Printers and Cisco® Routers

Adaptive Scanning
Provides broad based scanning via anonymous or user-supplied credentialed scans

Consolidated Views
Multiple scans can be merged together to form a more comprehensive security posture

Role-Based Administration
Enables distributed management of scan activity by user roles

Auto Scheduling
Automate recurring scan tasks to scan specific machines, groups, vulnerabilities or other criteria on a daily, weekly or monthly basis

Risk-Based Prioritization
Ability to score vulnerabilities to direct remediation efforts to critical systems

Remediation Recommendations
Extensive vulnerability database with informational resources and remediation recommendations

Highly Scalable
Distributed architecture supports even the largest networks (millions of nodes)

Comprehensive Reporting
Ability to create and export (RTF, PDF, HTML, etc) high-level or detailed reports of all scan data to confirm policy compliance

Extensive Security Certifications & Standards
Common Criteria EAL2, Section 508, MITRE CVE, Bugtraq, SANS Top 20 and many other certifications and identifiers.
PatchLink Products:
As the market leader in patch and vulnerability management, PatchLink offers comprehensive solutions for IT organizations facing the challenges of today’s increasing threat landscape.

PatchLink Security Management Console™
Effectively manage the entire vulnerability management lifecycle including network discovery, agent deployment, threat assessment and remediation, and reporting - all from a single, unified view. The PatchLink Security Management Console is a role-based administrative interface that provides centralized control of multiple PatchLink assessment and/or remediation engines and a central source for report generation.

PatchLink Update™
Protect heterogeneous environments from threats and intrusions with the market leading patch management solution. PatchLink Update enables you to automate the collection, analysis, and delivery of patches throughout your heterogeneous network. PatchLink has the world’s largest repository of pre-tested patches, with more than 14,000 patches for major current and legacy operating systems and applications.

PatchLink Scan™
Complete stand-alone network-based scanning solution that allows you to assess and analyze network threats through a comprehensive external scan of all of the devices on your network, including servers, desktop computers, laptops, routers, printers, switches and more.

PatchLink Developers Kit™
Create custom vulnerability remediation content to address security threats that are not software related, or for which there is no publicly available patch. Using the PDK, you can quickly eliminate hardware configuration issues, update application settings, remove unauthorized files and applications, enforce security policies, patch custom software, respond to zero day vulnerabilities, distribute commercial or proprietary software, and much more.

PatchLink Enterprise Reporting™
Create policy-based, enterprise wide compliance reports in support of government regulations such as Sarbanes-Oxley, HIPAA, FISMA and the European Directive. An extension of PatchLink Update, Enterprise Reporting is a robust data warehouse that allows you to easily create and share reports on all aspects of your vulnerability management process.

PatchLink Quarantine™
Seamlessly incorporate PatchLink’s patented threat assessment and remediation into your access control solution. Through established integrations with leading network access control (NAC) vendors (ForeScout, Juniper, Lockdown and Vernier) and support for all major industry standards (Cisco NAC, Trusted Computer Group’s Trusted Network Connect (TNC) and Microsoft Network Access Protection (NAP) (in development)), PatchLink Quarantine ensures that devices blocked by your access control solution are quickly and automatically reformed back into policy compliance, allowing restricted users to safely access the resources they need to remain productive.

Copyright © 2007 PatchLink Corporation. All Rights reserved.
PatchLink, the PatchLink logo, PatchLink Security Management Console, PatchLink Update, PatchLink-Scan, PatchLink Developers Kit, PatchLink Enterprise Reporting and PatchLink Quarantine are trademarks or registered trademarks of PatchLink Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
U.S. Patent No. 6,990,660 and other patents pending.