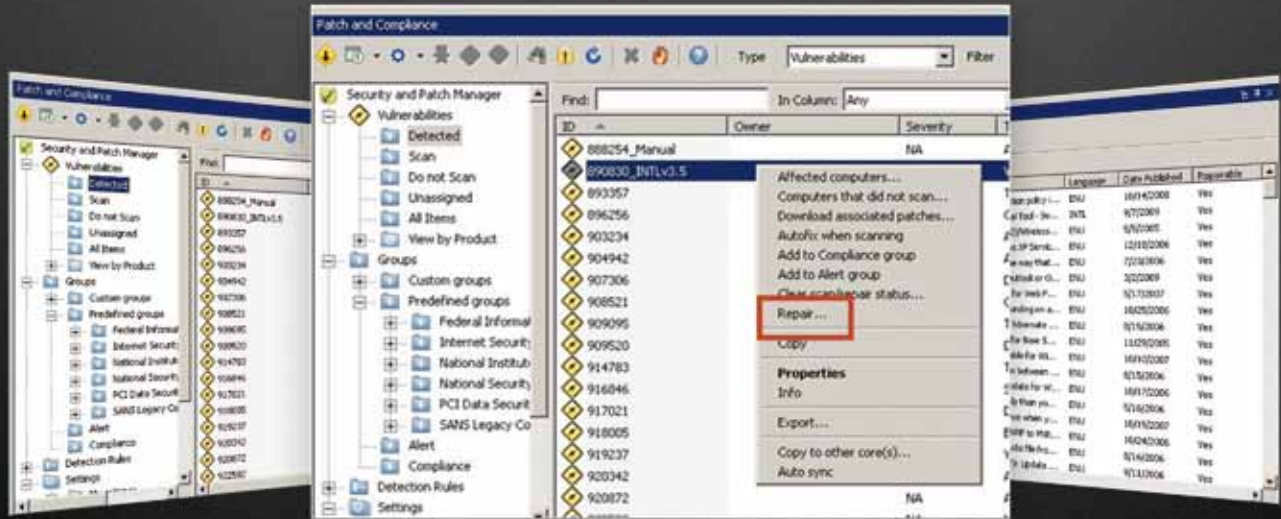


# LANDesk® Patch Manager



Automate Vulnerability Assessment and Patch Management  
across Your Heterogeneous IT Environment



*“LANDesk® Patch Manager gives you a complete detailed list of which machines have been updated and which machines have not. [And] LANDesk tests the patches before we get them, giving us more reliable patches.”*

—Adel Kamali  
Head of User Support  
Abu Dhabi Water and Electricity  
Authority (ADWEA)

*“Now we can secure and patch our entire environment in one hour with a single engineer. LANDesk saves us at least 280 man-hours per patch.”*

—Edward Skaff  
Manager  
Exempla Healthcare

*“The console lets us deploy patches remotely so we don’t have to send anyone out to a site. We can manage the entire patch process from our operations here in Sydney, pushing out updates, rebooting computers and then knowing with a certainty that they’ll function properly the next day.”*

—Luke Doherty  
IT Manager  
InterContinental Hotels  
Group PLC

## Easily Keep Up with Security Threats and Patches

Whether from hackers, viruses, or ordinary bugs, your software and operating systems are vulnerable to security and performance threats. Keeping up with the constant stream of patches is an ongoing drain on your IT staff as they struggle to research, evaluate, test, and apply patches across the enterprise. And if the task of keeping up proves too strenuous, it will put your whole network at risk.

### LANDesk® Patch Manager: Complete Patch Management

Companies have long recognized the necessity of patching operating systems. However, today the majority of malware attacks exploit application vulnerabilities. That’s why we created LANDesk® Patch Manager. This invaluable subscription service automates vulnerability assessment and patch management for both operating systems and applications—even in wildly heterogeneous environments—and then remediates them within minutes so your IT department guarantees baseline security, stability, and performance.

LANDesk Patch Manager gives you the power to:

- Boost productivity and reduce headaches by quickly evaluating systems with active vulnerability scanning
- Maximize peace of mind by using industry-standard information sources to identify vulnerabilities
- Gain control with a single tool to research, review, and download available patches
- Increase system uptime and user satisfaction by efficiently remediating known vulnerabilities through automated targeting and patch distribution
- Automate patch deployment using the Parallel Patch Process in LANDesk® Process Manager
- Automatically maintain patch currency and save time by establishing active patch management policies

### Efficiency Boosts Productivity

LANDesk Patch Manager lets you actively scan managed computers to identify application and operating system vulnerabilities. Define your own custom vulnerabilities to support individual application, policy, or security needs, then view assessment results directly in the console.

### Efficiency Increases Control

LANDesk Patch Manager delivers automatic, efficient patch remediation. It lets you quickly schedule distribution tasks to apply patches to individual computers, computers’ roles, or groups of computers by integrating with your existing directory, such as Active Directory. You can also establish policies that automatically install patches for specified operating systems. And you can download and install new patches as they become available with autofix remediation.

Further, LANDesk Patch Manager also facilitates easy reporting on remediation efforts, including which computers required a specific patch, which ones are already patched, and which require manual remediation. You can also quickly identify computers that couldn’t be updated in order to address special needs or requirements, as well as report both success and ongoing remediation needs.

In addition, you can easily track compliance with standards such as Payment Card Industry Data Security Standards (PCI DSS), SANS, National Institute of Standards and Technology (NIST), National Security Agency (NSA), Federal Information Security Management Act (FISMA), and more. And if you're in the process of implementing those standards, LANDesk Patch Manager lets you track progress and helps you determine how best to complete the process of achieving compliance.

## Save Time

LANDesk Patch Manager includes exclusive LANDesk® software distribution technologies. LANDesk® Targeted Multicast™ minimizes bandwidth used when distributing large packages to multiple users—without requiring dedicated hardware or router reconfigurations. LANDesk® Peer Download™ leverages local bandwidth efficiency to access packages that were already delivered to a subnet. LANDesk Patch Manager lets you use these technologies to easily pre-stage patches to each local system cache and then quickly roll them out once approved by your change control board. What's more, you can automate patch deployment with Parallel Patch Process, improving your ability to automatically patch vulnerable systems and maintain patch policies across your network.

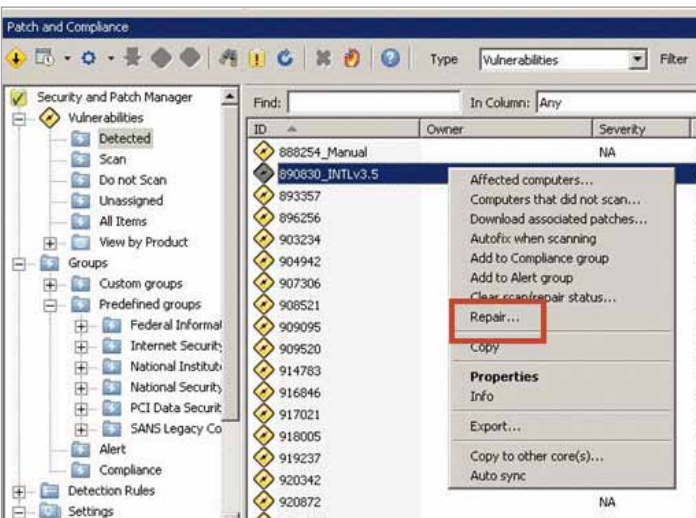
## Never Miss a Beat

One of the great features of LANDesk Patch Manager is that it lets you set up e-mail or pager alerts when a specific vulnerability or severity level is detected. It also monitors the status of each installation and displays it on-screen so you can quickly and easily track remediation and ensure that each patch reaches its target. When remediation is complete, you can audit target machines to ensure correct configuration. The net result is that you're free to focus on machines that really need your time.

LANDesk Patch Manager lets you view vulnerabilities directly from the console, and you can even sort by vulnerability, patch, application, or machine to quickly identify needs. To remediate vulnerabilities directly from there, simply right-click on the appropriate item.

## Access and Patch Devices Anywhere in the World

Combining LANDesk Patch Manager with the LANDesk® Management Gateway appliance increases your capabilities exponentially by enabling you to assess vulnerability and remediate systems anywhere in the world. Use this potent combination to enforce policies on systems used by remote users or traveling employees.



LANDesk® Patch Manager lets you view vulnerabilities directly in the console and sort by vulnerability, patch, application, or machine. You can then remediate vulnerabilities with a simple right-click.



## Patch, Manage, Configure, and Secure from a Single Console

LANDesk Patch Manager is a stand-alone patch subscription service that integrates with the patch and update management technology in LANDesk® Management Suite to let you proactively see, manage, update, and protect your IT systems via a single console. LANDesk Management Suite is the integrated, intelligent path to painless Microsoft® Windows® 7 migration, comprehensive software asset management, and robust endpoint security. You can start with LANDesk Patch Manager and upgrade to the full LANDesk Management Suite whenever you're ready.

LANDesk Patch Manager can also be easily upgraded to LANDesk® Security Suite for a comprehensive security management solution that lets you automatically detect and deploy security patches with active endpoint security management, a personal firewall, quarantine capabilities, active threat analysis, spyware detection and removal, antivirus enforcement, access control, data leakage protection, application blacklisting, configuration security tools, and more—all from a single console.

# Key Features

## Scanning

- Enables you to set behaviors at agent deployment that determine when the vulnerability scanner runs, how required reboots are handled, and whether autofix is enabled
- Performs vulnerability assessment using industry-standard information sources
- Lets you prioritize patch severity for added control
- Includes custom vulnerability definitions that let you support your own application, policy, or security needs
- Checks multiple data sources for vulnerability information to help ensure that you get accurate patches for your enterprise systems
- Lets you decide when necessary tasks are performed with assessment and distribution scheduling
- Notifies you by email or pager when a vulnerability is detected and/or a new definition is downloaded
- Includes a CPU utilization control for 'vulscan' in scan and repair settings

## Remediation

- Shows you which patches depend on each other so you know what new vulnerabilities a patch might introduce
- Lets you filter out older, obsolete patches, speeding the time to a fully patched state; obsolete patches remain available if needed
- Automates patch deployment using the Parallel Patch Process functionality in LANDesk® Process Manager
- Offers multiple delivery options—including scheduled tasks, policy, and autofix—to give you control over remediation; use options alone or in combination to fix current vulnerabilities and ensure future patch security
- Uses endpoint reboot logic to let you choose what works best for your environment—snooze, custom messages, or unattended; display messages to give users control of when patches are installed and whether to reboot or snooze
- Pre-stages patches to end-system caches using LANDesk Targeted Multicast and LANDesk Peer Download for efficient distribution and reduced impact on network traffic. When your control board approves the patch, instantaneously install it off the local cache
- Gives you ultimate control over each endpoint with policy-based management
- Allows you to choose when necessary tasks are performed via assessment and distribution scheduling

## Comprehensive Control

- Delivers scalable architecture that leverages your existing hardware to improve ROI
- Lets users create and edit settings to gain control over client feedback, repair options, bandwidth usage, and more
- Displays all patches installed on a client—whether they're installed by LANDesk or another product
- Enables easy rollback for any patch available from the LANDesk patch management database, regardless of whether they were distributed using LANDesk Patch Manager or another tool
- Enables you to configure the tool so it doesn't patch when an application is in full-screen mode

## Analysis, Reporting, Compliance, and Alerting

- Includes reports on custom vulnerabilities, LANDesk® updates, custom patch installations, and scanned and repaired patch histories, patch levels, and more; trending analysis also lets you evaluate progress toward corporate or industry security policies
- Provides real-time alerts for security breaches and provides control over which vulnerabilities you receive alerts for; lets you choose to receive alerts on newly available definitions based on type and severity, and if new definitions are downloaded
- Makes vulnerability reports available from the Web console for added convenience
- Enables you to assess and enforce alignment with compliance standards such as Payment Card Industry Data Security Standards (PCI DSS), SANS, National Institute of Standards and Technology (NIST), National Security Agency (NSA), Federal Information Security Management Act (FISMA) and more
- Includes a *View as Report* option in the Security and Patch Information dialog

## Heterogeneous Platform Support

- Offers full vulnerability detection and remediation for computers running Windows, Red Hat Linux, SUSE Linux, and Mac OS X
- Includes vulnerability detection and reporting for computers running HP-UX, IBM AIX, and Solaris

Visit [www.landesk.com](http://www.landesk.com) for more information.

This information is provided in connection with LANDesk products. No license, express or implied, by estoppel or otherwise, or warranty is granted by this document. LANDesk does not warrant that this material is error free, and LANDesk reserves the right to update, correct or modify this material, including any specifications and product descriptions, at any time, without notice. For the most current product information, visit [www.landesk.com](http://www.landesk.com).

Copyright © 2009, Avocent Corporation. All rights reserved. Avocent, LANDesk and Touchpaper and their respective logos are among the registered trademarks or trademarks of Avocent Corporation, its subsidiaries or its affiliated companies in the United States and/or other countries.

\*Other brands and names are the property of their respective owners. LSI-0867 1209/BB/NH

