



# Patch Management



Increase the safety, security and efficiency of critical systems so IT can spend less time maintaining the computing environment and more time improving it.

# Develop and maintain patch level security—automatically

## The Challenge:

Your business computing environment is under siege, both from malicious attack and from ordinary maintenance issues and bugs. New hardware and software is released every day, along with the patches to repair inevitable vulnerabilities. Just keeping up with the change can be a full-time job that leaves little time for other IT tasks.

## Massive threat

In 2003 Computer Emergency Response Center (CERT) at Carnegie Mellon University reported more than 137,000 distinct security incidents resulting from nearly 3,800 different vulnerabilities—an increase of more than 50,000 incidents over 2002 (see [www.cert.org](http://www.cert.org) for more information).

Some threats come from buggy software, some from hackers dedicated to exploiting holes in application or OS security. The massive impact of worms and viruses such as Slammer, Blaster, MyDoom and Sasser demonstrates the power of these threats, and the potential costs to business. Wherever threats come from, they pose a hazard to corporate data and productivity that IT departments must deal with.

## The Great Time Sink

In 2002 CERT reported more than 4,100 different vulnerabilities. If IT spends only 20 minutes to evaluate each vulnerability description, that would require more than 170 full work days just to evaluate threats. Even if IT skips 3/4 of those as being obviously irrelevant, that still amounts to nearly 43 work days—and nothing has been downloaded, tested or installed yet.

## Turn information into action

Developing patch security requires an enormous amount of information. IT needs to track what hardware, software and operating systems are running on each computer—and which versions of drivers, applications and patches are currently installed. They need to understand the

known vulnerabilities for each platform they support. Then IT needs to know which patches are already installed, which need to be installed and which are irrelevant.

It's not the most difficult task IT faces, but it is among the most time consuming.

## Establish patch security

IT needs an effective patch distribution system that can quickly identify targets, efficiently distribute patches across the network, and report successful patch installation. When remediation is complete IT needs to verify that all machines are current and secure.

Then the process starts over again the very next day as new vulnerabilities are discovered and new patches are released. It never ends.

## Automate the process

IT needs to break out of the manual assess-and-remediate loop and find a way to automate the process.

The best solution scans each computer's hardware and software configuration, then it downloads the right patches and automatically installs them on the right computers according to specific policies that IT establishes.

The best solution is fast, efficient and secure, and integrates directly with your existing systems management solution.

That solution exists.

## OVERVIEW

**Business Need**—Keep up with the latest patches to ensure security throughout the computing environment.

- Determine current hardware and software configurations across the enterprise
- Assess current vulnerability against the most current industry knowledge
- Review and select the right patches for each computing platform
- Remediate vulnerabilities quickly and efficiently to establish patch level security
- Proactively maintain patch currency with automated assessment and install

**Solution**—Active vulnerability assessment, remediation and patch management with Patch Manager 8 from LANDesk Software

- Seamless integration with LANDesk® Management Suite 8 for unified systems management
- Extensive vulnerability scanning to identify current state of patch security for desktops, server and mobiles
- Automatic evaluation of current state against industry standard databases of known vulnerabilities
- Easy identification and distribution of the right patches for each vulnerable computer
- Status monitoring to help ensure that patches are successfully installed
- Policy-based configuration management to keep patches up to date—automatically

# The LANDesk® Solution

LANDesk® Patch Manager 8 efficiently automates vulnerability assessment, remediation and ongoing patch management. Features include:

- Seamless integration with LANDesk Management Suite 8 unifies key management tasks in a single, comprehensive management environment
- Automated assessment of systems against industry-standard information sources ensures the most current and accurate vulnerability assessment
- User-defined vulnerability detection helps identify unique threats and quickly determine compliance with security standards, then optionally deliver custom patches
- Custom patches can be secured using an MD5 hash algorithm to help protect against tampering
- Console display of detected vulnerabilities eases planning, targeting and decision-making
- Automatic patch download and distribution package creation speeds time to resolution
- Pre-tested patches are verified to install and function as intended; research notes and test notes for each patch are accessible with one click
- Task completion, status monitoring and inventory auditing help IT ensure that patches are successfully installed
- Policy-based management can automatically identify, download, target, and install patches based on IT-defined rules to enable active patch management and computing security

## Leverage management power

LANDesk Patch Manager 8 extends the power of LANDesk Management Suite 8, leveraging its targeting, software distribution and policy management features to create unmatched efficiency. Vulnerability scan results are stored in the unified database to keep data consistent and enable easy analysis and reporting on all data.

That maximizes your existing investments in systems management, reduces both training and infrastructure costs, and helps keep IT working efficiently in a single, integrated console.

## Active assessment

Patch Manager uses industry-standard sources to determine both machine vulnerability and patch availability. This helps ensure rapid access to current validated data. Patch Manager

automatically checks dependencies and requirements to give you the information you need to select the right patches.

Patches are pre-tested and verified to install and function as intended. Test notes and additional research is available with a click of the mouse. There's no need for IT staff to search news boards or rely on vendors to send out their own patch announcements. Patch Manager searches out the latest data and automatically evaluates systems against known vulnerabilities.

## User-defined vulnerabilities

Patch Manager gives you the ability to define custom vulnerability rules that quickly detect and identify security issues, configuration problems, missing files and more. Define rules for specific operating systems so you can quickly identify variances to corporate,

“LANDesk Patch Manager gives me the confidence that our company is protected. It identifies any vulnerabilities that we might have and enables us to quickly and efficiently push out the security updates and releases to fix them. That level of automation is worth its weight in gold.”

STEVEN O'SULLIVAN  
PC SYSTEMS MANAGER  
HUGHES SUPPLY

industry or regulatory standards and quickly remedy any problems.

You can also define custom patches to install files or applications and remediate user-defined vulnerabilities. Assign any distributable package file as a patch, along with any commands or directives needed to complete your remediation efforts. Custom patches can be secured using an MD5 hash algorithm to help protect against tampering and ensure that the patch you created is the one that's delivered.

### Controlled automation

You can choose full automation for hands-off patch management, or you can step through the assessment and remediation process only after you've made explicit decisions.

It's good practice, for example, to test patches for critical servers before deployment to ensure that the patch itself doesn't interfere with other processes or services. Similarly, some patches may address issues that are irrelevant in your environment and can be safely skipped. Patch Manager gives you the choice to do it your way.

### Efficient remediation

Once vulnerabilities are identified, you can choose how to remediate them. View by platform, application, computer or detected vulnerability to quickly and easily select targets.

Begin remediation with a mouse click. Choose to distribute packages to specific computers using the task scheduler, define configuration policies automatically install needed patches throughout the network, or choose autofix for fully automated hands-off remediation for all vulnerable computers.

Patch Manager can take advantage of LANDesk Targeted Multicast™

and Peer Download™ technologies to minimize network impact, increase patch availability and speed deployment to all affected machines at once.

Patch Manager monitors the status of each install and displays that status on-screen so you can quickly and easily track remediation and ensure that each patch reaches its target.

When remediation is complete, IT can audit each target machine to ensure correct configuration and report successful remediation. The result is that most patches can be installed quickly, easily and automatically while IT works on other tasks. IT can spend time only on those machines that require it.

### Policy-based maintenance

Once current vulnerabilities are assessed and remediated, IT can use LANDesk Management Suite's powerful Application Policy Management (APM) features to automate patch maintenance.

Patch Manager can leverage APM to assess and remediate a machine's vulnerabilities based on OS, configuration, organizational role or any LDAP attribute tracked by your directory service system. Because APM can implement policies based on both machine inventory and directory service attributes, IT can refine policies as needed to ensure patch security and currency.

### Heterogeneous platform support

Patch Manager supports both client and server platforms for a wide variety of operating systems. Broad platform support helps ensure that the entire enterprise is kept up to date, not just machines running a particular OS. Extended language support means you can protect your IT assets wherever they might be.

Download a fully functioning 100-node, time-limited product trial so you can see for yourself how LANDesk solutions can help ease your systems management pain from the first day of deployment.

<http://www.landesk.com/>

## Rapid results

Patch Manager can begin vulnerability assessment and remediation from the moment it's installed, and can begin remediation on the very first day. The result is that IT can quickly implement and maintain patch-level security across the enterprise in only a few days.

## Integrated Solution

Patch Manager seamlessly integrates with LANDesk Management Suite 8

to provide not only quick vulnerability assessment, but rapid remediation and hands-off maintenance—automatically.

By leveraging existing software deployment and automated policy management, LANDesk Patch Manager 8 enables a level of efficiency and control that's virtually impossible with standalone products or bolt-on tools.

## LANDesk Software, a Patch Management solutions leader

LANDesk Software is an industry leading provider of easy to use, integrated solutions for desktop, server and mobile device management. LANDesk solutions are proven, with more than 250 million managed nodes worldwide.

Find out for yourself. Call or visit our Web site to learn more about LANDesk solutions, then download a fully functioning 100-node, time-limited LANDesk Management Suite product trial so you can see for yourself how LANDesk solutions can ease your systems management pain from the very first day.

helps ensure that the entire enterprise is kept up to date, not just machines running a particular OS. Extended language support means you can protect your IT assets wherever they might be.



**Corporate Headquarters**

698 West 10000 South

Suite 500

South Jordan, Utah 84095

[www.landesk.com](http://www.landesk.com)

**FOR PRODUCT INFORMATION**

U.S. and Canada ..... +1-800-982-2130

Europe ..... +44-845-230-5580

Japan ..... +81-3-3435-8261

Brazil ..... +55-11-5503-6502

Mexico ..... +52-55-5093-8211

China ..... +8610-8518-3138

THIS INFORMATION IS PROVIDED IN CONNECTION WITH LANDESK SOFTWARE PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, OR WARRANTY IS GRANTED BY THIS DOCUMENT. LANDESK SOFTWARE DOES NOT WARRANT THAT THIS MATERIAL IS ERROR FREE, AND LANDESK SOFTWARE 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 [HTTP://WWW.LANDESK.COM](http://WWW.LANDESK.COM).

COPYRIGHT © 2004 LANDESK SOFTWARE, LTD. OR ITS AFFILIATES. ALL RIGHTS RESERVED. LANDESK, TARGETED MULTICAST AND PEER DOWNLOAD ARE REGISTERED TRADEMARKS OR TRADEMARKS OF LANDESK SOFTWARE, LTD. OR ITS AFFILIATES IN THE UNITED STATES AND/OR OTHER COUNTRIES.

EACH CUSTOMER'S RESULTS MAY VARY BASED ON ITS UNIQUE SET OF FACTS AND CIRCUMSTANCES.

\*OTHER NAMES OR BRANDS MAY BE CLAIMED AS THE PROPERTY OF OTHERS.