



Patch Management



Increase the safety, security and efficiency of critical IT 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

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.

With increasing regulation that requires companies to demonstrate control over financial records and other data, these threats represent more than just an IT problem. Data security and integrity is a business issue.

Information-gathering: The Great Time Sink

In 2004 the Computer Emergency Response Center (CERT) at Carnegie Mellon University reported 3,780 different vulnerabilities (see www.cert.org for more information).

If your security team spends only 20 minutes to evaluate each vulnerability description, that would require more than 157 full work days just to evaluate threats. Even if you skip 3/4 of those as being irrelevant, that still amounts to more than 39 work days—and nothing has been downloaded, tested or installed yet.

Turn information into action

Developing patch security requires an enormous amount of information. Your security team needs to track hardware, software and operating systems running on each computer—and which versions of drivers, applications and patches are currently installed. Then understand the nature and extent of known vulnerabilities for each platform. Then know which patches are already installed, which still need to be installed and which are irrelevant.

It's not the most difficult task your security team 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.

OVERVIEW

Business Need—Keep up with the latest patches to ensure security and performance 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 deployment with patch and security management from LANDesk

- Seamless integration with LANDesk® Management Suite 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
- User-defined vulnerabilities identify unique configuration or security issues and support custom patches
- 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 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 your security team establishes.

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

That solution exists.

The LANDesk® Solution

Automated patch management is available from LANDesk as a standalone solution in LANDesk® Patch Manager, or as a component of both LANDesk® Security Suite and LANDesk® Management Suite.

The LANDesk patch management solution efficiently automates vulnerability assessment, remediation and ongoing patch management. Features include:

- Seamless integration with other LANDesk solutions unifies key management tasks in a single, comprehensive management environment
- Automated assessment of systems against industry-standard information sources helps ensure complete 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

LANDesk patch management helps increase the security and efficiency of critical systems so IT can spend less time maintaining the computing environment and more time improving it.

Leverage existing management power

LANDesk® patch management leverages proven LANDesk targeting, software distribution and policy management technologies 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

LANDesk® patch management uses industry-standard sources to determine both machine vulnerability and patch availability. This helps ensure rapid access to current validated data. LANDesk patch management 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. LANDesk patch management searches out the latest data and automatically evaluates systems against known vulnerabilities.

User-defined vulnerabilities

LANDesk® patch management 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, 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 accepted best 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. LANDesk® patch management 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.

LANDesk® patch management can take advantage of exclusive LANDesk® Targeted Multicast™ and Peer Download™ technologies to minimize network impact, increase patch

“Manually building and deploying patches is a very labor-intensive process. LANDesk saves us at least 280 man-hours per patch.”

EDWARD SKAFF

EXEMPLA HEALTH CARE

MANAGER

availability and speed deployment to all affected machines at once.

The LANDesk patch management solution 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 powerful policy-based configuration management tools to automate patch maintenance.

LANDesk® patch management can leverage application policies 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 policy-based management 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

LANDesk® patch management 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.

Rapid results

LANDesk® patch management 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

LANDesk® patch management seamlessly integrates with LANDesk® Management Suite 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 management enables a level of efficiency and control that's virtually impossible with standalone products or bolt-on tools.

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/>

LANDesk—Leading Patch Management Solutions

LANDesk is an industry leading provider of easy to use, integrated solutions for desktop, server and mobile device management. LANDesk® solutions are proven, with millions of managed nodes deployed 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 product trial so you can see for yourself how LANDesk solutions can ease your systems management pain from the very first day.



Corporate Headquarters

698 West 10000 South

Suite 500

South Jordan, Utah 84095

www.landesk.com

FOR PRODUCT INFORMATION

Brazil + (55 11) 3048-4080
Canada+ 1-800-982-2130
China+ 8610-8518-3138
Europe + 44 (0) 118-902-6200
France0810 000 212
Ireland + 353 (0)1 809-4268
Italy+ 39 (02) 72 54 64 64
Japan + 81 (3) 3435-8261
Mexico+ 52-55-5448-4933
U.S.+ 1-800-982-2130

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.