

TECH TRACKER

For IT By IT

If The Patch Fits, Use It

We put five patch management systems to the test. See which is the best fit for you.

IN NOVEMBER, WE WENT IN search of a way to automatically shield our systems from the thousands of application vulnerabilities that will hit this year. Five vendors took part in our Patch Management Rolling Review, sending products to our Windward Consulting Real-World Labs: BigFix, Kaseya, LANDesk, Lumension, and Shavlik. See our Analyst Assessment, right, for evaluation criteria and ratings.

Two main decision points for companies choosing a patch management suite are breadth of operating system support and dependence on agents, and we saw a lot of variation here. Though we found some great agent management utilities, sometimes the requirement to install one more piece of software is a deal breaker. For these companies, Shavlik's NetChk Protect can run without agents.

For multiplatform patching, consider Lumension's PatchLink Update, LANDesk's Patch Manager, and BigFix's Patch Management Enterprise Suite. Each supports varied Windows, Linux, and Unix platforms; provides robust patch deployment features; and regularly updates the patch content available. BigFix and LANDesk are multifunctional endpoint manage-



ment suites that include patching, while Lumension's PatchLink is purely a patch manager.

BigFix's Enterprise Suite excels at bandwidth management, allowing both static and dynamic throttling while enabling settings to control bandwidth at endpoint, server, and all distribution points. We also liked its distributed architecture and support for a broad base of operating systems and apps. On the downside, all this functionality comes with a learning curve, as BigFix's terminology and structure are different from what's standard in the rest of the patch management field. And, while BigFix shows when vendors

recommend reboots with a patch, all deployments default to a no-reboot setting.

LANDesk's Patch Manager is, like BigFix, part of a comprehensive endpoint management package. We found its user interface a tad cumbersome, but of all the products tested, Patch Manager was the only one with an automated process to facilitate ITIL change management practices—a huge plus. Its Parallel Patch Process defines testing and rollout processes that can be clearly documented and transparent to a change management board, as well as enabling highly efficient deployment of patches. These plus an automated process for copying patches to an entire subnet through one client and an option to auto-fix vulnerabilities helped LANDesk capture our Editor's Choice.

However, environments looking to automate patching of AIX, Solaris, and HP-UX should be aware that LANDesk only scans those operating systems—it doesn't deploy patches to them.

Lumension's PatchLink is a multiplatform patch manager without the extras of endpoint management. We found PatchLink easy to use, and it's the only multiplatform entry with a browser-accessible administrative interface.

For desktop patching, Kaseya's Managed Services Edition provides extensive administrative functionality and flexibility on Windows or Mac OS X systems, though we were disappointed that the selection of natively supported patches is limited to Microsoft applications that fall under Windows Update. Beyond that, you'll need custom scripts.

Shavlik also specializes in Windows-focused patching, with optional agents. Shavlik NetChk Protect's bandwidth throttling isn't as precise as we'd have liked, but it is available during agentless patching. NetChk Protect automatically checks for new patches and updates before every scan and can make use of a distributed patch repository architecture.

Note that we chose not to review Novell's ZENworks Patch Management in the course of this Rolling Review because it licenses PatchLink's product. However, those looking into full endpoint management, or to add patching to an existing ZENworks environment, should feel confident in the patch management that Novell provides.
—MICHAEL BIDDICK (mbiddick@nwc.com)

Real-World Analyst Assessment Patch Management

UNACCEPTABLE ← ● — ● — ● — ● — ● → IDEAL	BigFix	Kaseya	LAN-Desk	Lumension	Shavlik
Short List ✓, Editor's Choice ☆	✓		✓☆	✓	
Integration with external patch knowledge base or subscription services	●	●	●	●	●
Strength of change control mechanisms	●	●	●	●	●
Efficiency in dealing with corrupt patches	●	●	●	●	●
Ability to determine which applications need patching	●	●	●	●	●
Rollback capabilities	●	●	●	●	●
Flexibility of patch scheduling	●	●	●	●	●
Breadth of operating system support	●	●	●	●	●
Price versus features	●	●	●	●	●

BigFix Enterprise Suite is a complete endpoint management system that can be used to patch and control all aspects of your heterogeneous environment. Like most rivals, it does require agents, but we were pleased with its cross-platform support. Total list price for our test environment was \$20,250.

Kaseya Managed Services Edition is very easy to use, but operating system support is limited and agent configuration is kludgy. Still, the price is right: A one-time licensing fee with no annual subscriptions for the software or patches. In our scenario, Kaseya charged \$12 per device for 600 Windows machines, for a total of \$7,200.

LANDesk Patch Manager supports a wide range of apps and operating systems and is a good choice if you need comprehensive endpoint and change management. The product provided thorough vulnerability discovery and remediation and a robust array of tools, though features are relatively limited for non-Windows devices. Pricing for our 600-node test site was \$17,400.

Lumension PatchLink manages critical security and application patches across most operating systems from a single, easy-to-use Web-based console, and patches are updated daily. But be prepared for higher ongoing costs: PatchLink doesn't use a perpetual license model, so for our environment, we would spend about \$27,000 for the first year, then pay \$25,000 in following years.

Shavlik NetChk Protect simplifies management of critical security patches and watches for spyware, malware, and unwanted applications in Windows environments, all from a single, simple-to-use console, without requiring agents. We liked its virtualization support and a mechanism to throttle network bandwidth. Price is \$19,200 for 300 Windows machines plus 300 virtual machines running Windows, including the first year's maintenance.