From ENTmag.com:

News

print article

More News
- Yukon's Broad Beta Slated for Second Half of 2002
- Microsoft Tool to Tighten .NET-SQL Server Bond
- Exchange SP2 Enhances Outlook Web Access
- Compaq Offers Windows Systems Based on Oracle Clustering
- Goner Mass-Mailing Worm Makes the Rounds

Hotfix Management Tools Maturing

by Stephen Swoyer

11/15/2001 — If service pack and hotfix management have traditionally been tricky propositions in the Windows NT/Windows 2000 spaces, they've recently become downright onerous. Consider the situation of John Hunter, a senior network systems programmer at Indiana University, who says that it takes him almost two hours to completely patch a Windows NT 4.0 Server after he's finished installing the operating system software.

"The sheer number of patches that need to be applied is incredible, and some of them have to be applied in a specific order. I find it hard to know for sure which order stuff has to go in, and then you've always got certain ones that you're not sure you need. Of course, you're also supposed to reboot after you apply most of the patches," he says.

The rigors of hotfix management, in particular, have carved a very important market niche for vendors such as St. Bernard Software, Shavlik Technologies, Configuresoft Inc., Gravity Storm Software and Patchlink Corp., among others, which provide hotfix query and reporting tools. Even Microsoft has jumped into the fray, and offers a freely downloadable hotfix query tool, HFNETCHK.EXE, which is based on a more versatile tool from Shavlik Technologies. IT managers now have more options than ever when it comes to managing hotfix compliance in their environments.

Indiana University's Hunter, for example, uses a tool called UpdateExpert from St. Bernard Software to keep on top of hotfix- and service pack-compliance in his IT department.

"With a few clicks, I can apply one or many patches to one or many servers, and I can easily see which of those servers need the patch, or already have it," he says. "And if a new patch comes out for a security concern, we can easily see if some of those servers already have that patch or not. Because sometimes they roll different patches together, so you may already have the patch from some other subset of patches."

It wasn't always this way, however.

Background

In 1997, NTBugtraq editor Russ Cooper introduced what's believed to be the first hotfix compliance testing tool: A Web-based facility –- hosted on his NTBugtraq Web site –- that searched for new hotfixes on Microsoft's FTP site and automatically scripted hyperlinks to them once they were discovered. The service was important then because the Microsoft Security Response Center hadn't yet been created, so Microsoft didn't have a procedure for alerting customers to new hotfixes or potential vulnerabilities. More often than not, then, NT 4.0 users were forced to proactively monitor Microsoft's unwieldy FTP site in search of new, and sometimes cryptically documented, fixes.

Cooper's Hotfix Checker provided an alternative method and gave birth to a veritable cottage industry of compliance-checking tools. In late 1997, for example, MTE Software Inc. front-man Mark T. Edmead began work on

SPQuery, a client-based utility that combined the discovery capabilities of Cooper's Web-based Hotfix Checker with a querying facility that could determine whether or not specific hotfixes were installed on a client system. Edmead released SPQuery in early 1998. Shortly thereafter, Gregg Branham and Rick Osborne of consultancy and integration firm Altus Network Solutions introduced SPCheck, a tool that was similar to SPQuery, but which was available as a free download.

Skipping forward, St. Bernard Software acquired SPQuery from MTE Software in early 2000 and subsequently rebranded it Update Expert. Meanwhile, Microsoft abandoned its practice of posting hotfix updates to its FTP site, breaking Cooper's Hotfix Checker facility once and for all.

The Market Today

Most of the vendors with a stake in the hotfix management space say that the damage wrought by a spate of high-profile worm attacks (Code Red versions 1, 2 and possibly 3; Code Blue; Nimda) has helped to further ratchet up demand for their products. But that's not all.

According to Ron Kaplan, product manager with St. Bernard Software, the worm attacks have forced IT organizations to rethink the ways in which they approach hotfix management in the first place.

"I believe a year ago or more, [hotfix management] was kind of an if-it-ain't-broke-don't-fix-it attitude. Today, because more and more revenue is directly tied to whether or not your systems are secure, it's now become standard practice to deploy hotfixes and to treat [hotfix management] more seriously," Kaplan argues.

Alex Goldstein, president and CEO of Configuresoft, agrees. "We have seen a couple of our customers that now have direct budgets for figuring out how they're going to deal with patches," Goldstein says. "And most of the time it's because their CIO has said that he wants to be able to sleep at night without having to worry about whether or not all of his systems are patched."

By and large, vendors in the hotfix management space offer products that compete functionally with one another. St. Bernard Software, Configuresoft, Gravity Storm and PatchLink, for example, provide tools that monitor, report and take action on distributed Windows NT 4.0 and Windows 2000 systems.

Shavlik Technologies' HFNetChk Pro, on the other hand, facilitates hotfix monitoring and reporting, but doesn't include an actionable management component. But Shavlik scored a coup in August when Microsoft released a command-line tool, HFNETCHK.EXE, based on Shavlik's considerably more robust HFNetChk Pro. HFNETCHK.EXE, for its part, had as its antecedent an IIS 5.0 hotfix checking tool, also based on a Shavlik design, called HFCHECK.WSF.

Dean Gutzke, executive director of business development with Shavlik, says that the availability of HFNETCHK.EXE has encouraged a lot of IT organizations to ask about his company's GUI-based HFNetChk Pro tool. "As a direct result of that, we've been getting responses from all over the world," he says.

Although HFNetChk Pro doesn't provide a facility to remotely deploy hotfixes on distributed Windows NT 4.0 or Windows 2000 systems, Shavlik's Gutzke says that IT organizations can use Microsoft's own Systems Management Server platform or any of several other remote software installation tools to accomplish this. "We concentrate on the reporting and monitoring, so we give you a robust graphic user interface with detailed reporting, and we tie directly into Microsoft's XML database for up-to-date hotfix information," he says.

Configuresoft, for its part, markets Enterprise Configuration Manager (ECM), a systems management tool for Windows NT 4.0 and Windows 2000 systems. In addition to its hotfix management facility, which marries an automatic discovery feature with reporting capabilities and an actionable administrative component, ECM also collects other systems management data, as well.

“We capture pretty much everything we can get our hands on, so that means not only hotfix information, but also device drivers and file system information, event log data, the security elements of the local SAM, all of the information that’s in the registry. So we grab it and put it all into one big repository,” says Randy Streu, vice president of product management with Configuresoft.

For IT organizations that want to be able to remotely deploy hotfixes, but which don’t necessarily want the systems management capabilities of a tool like ECM, St. Bernard Software, PatchLink and Gravity Storm are eager to fill the bill. At the same time, however, St. Bernard Software’s Kaplan cautions that IT organizations shouldn’t select a hotfix management tool simply because of its remote deployment capabilities.

“Deployment is really wonderful and terrific, but at the end of the day, there are a lot of deployment tools out there. Most of our development work goes into understanding the interdependences from one hotfix to another, understanding how to validate hotfixes, how can they be combined to eliminate reboots, things like that,” he says.

Conclusion

For users like George Kasica, president of systems integration firm and consultancy Netwrx Consulting Inc. in Jackson, Wis., a hotfix management tool like St. Bernard Software’s UpdateExpert has made all of the difference.

“We were killing ourselves here trying to keep everything up to date. It’s not just NT, it’s SQL, it’s IE,” he says. “But now I’m able to download the update once and apply it to all of our systems at one time, rather than having to go to each physical box and run the update. I can also figure out what’s vulnerable and what actually needs to be updated, rather than just randomly installing hotfixes on every system.”

And other tools, like Microsoft’s own HFNETCHK.EXE utility are helping, as well, IT managers say. “We’ve … found that running HFNETCHK in a batch file as a scheduled process helps us keep on top of patches,” says Simon Jones, an IT administrator with a large UK-based telecommunications firm.

Stephen Swoyer is a contributing editor at ENT and a freelance IT reporter. You can contact Stephen about "Hotfix Management Tools Maturing" at stephen.swoyer@shakespeareandcompany.net.

back to previous page