

A stitch in time

Windows is a complex beast, in constant need of updating. So let Patch Manager take the strain and handle the patching process for you

BY THOMAS LEE

If you run a Windows system – or for that matter, just about any computer system – keeping it updated is a near-constant task. I've written about this many times in *ESM*, most recently in September 2003.

Patching is hard and requires considerable attention to detail, especially if you've got a diverse inventory of computers. However, there is help out there, and in this article I'll be looking at a package aimed at making patching much easier to manage and control.

The real problem

Windows, whether it be the client (for example, Windows XP) or the server version (Windows Server 2003), is a large and complex computer system. And like all large and complex systems, it has bugs, some of which have created significant problems for end users.

Of course, all complex systems have bugs. Some of these are of no real consequence, and can be lived with, while others are far more serious.

Most Windows users need to patch not only the operating system, but also key applications, such as Office, or application components, including those which Microsoft insists on bundling with the operating system, such as Internet Explorer and Media Player.

Microsoft is aware of the problem. The company is working hard to make the patch management experience easier. New versions of its Software Update Service, MSI

application installer and Windows Update site are all planned for 2004 to simplify things.

Into the breach

While Microsoft has great plans for the future of patching, it's some way from delivering an integrated patch management solution, and most organisations are not able to wait. Fortunately, a number of third-party tools are available that can go a long way to solving your problems. One such problem solver is Ecora Patch Manager, a comprehensive patch management application that manages patches for Windows and UNIX (Solaris) systems.

Ecora is a small (68 employees) US company, based in Portsmouth, New Hampshire, and was founded in 1999. Its product range encompasses recovery, auditing and reporting, change monitoring, patch management, and security. Here in the UK, Ecora is represented by Pillar Solutions. You can visit Pillar's web site at <http://www.pillar-solutions.com>.

Getting started

Installation is simple and straightforward, although it does take time. You should have the necessary systems up and available. Also, if you are using separate machines for the patch repository and so on, you'll need the credentials (username and password) to access those separate machines.

The first step is to get a product licence. For the trial version, you get this over the Internet. You can register for a trial version at <http://www.ecora.com/ecora/partners/pillar-solutions.asp>.

The installation next asks you for a database connection to a SQL or MSDE database holding details about patches, scans and so on. The installation program does a good job of setting this up for you. If you are in a larger organisation, you might wish to create your own, larger, SQL databases, and provide the connection information. This is especially important in large enterprises where SQL databases are carefully managed (backed up, tuned, etc) by a central IT team.

The installation program then loads the patch management knowledge database (PMKDB), which takes some time. The PMKDB holds information about what patches are needed, what patches have been pushed, etc.

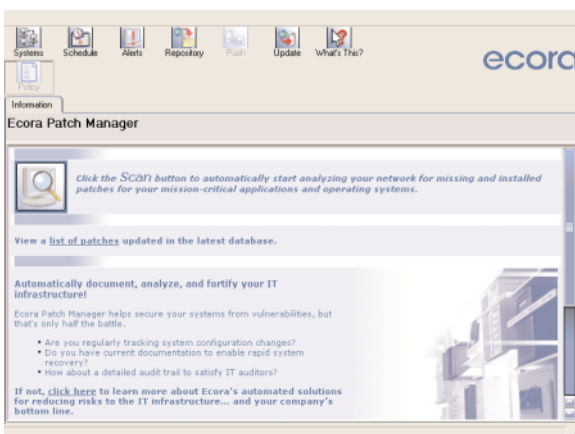


Figure 1: Patch Manager provides numerous options on start-up

System requirements

Microsoft Windows NT 4 SP6a, 2000, XP Professional, NT 4, Terminal Server Edition, SP6; 500MHz CPU or higher; 256Mb RAM or greater; 35Mb free disk space; Internet Explorer 5.01 or higher.

Contact Pillar Solutions for exact requirements.

UK supplier

Pillar Solutions
Tel 01732 363670
E-mail sales@pillar-solutions.com
Web www.pillar-solutions.com

Cost

Patch Manager is priced per node. Contact Pillar Solutions for further details.

Bottom line

Pros Comprehensive, no-nonsense patch management tool covering both the OS and Microsoft Office. First-class support.
Cons Could be more prescriptive.

The scanning process uses this knowledge base to determine which patches a particular system should have and which patches are applied (or not).

You are then asked to create the repository, which is where the individual patches will be loaded. You need to supply the server and share to use, plus the userid and password to use for accessing the share. As should be obvious, the repository needs to sit on a machine and share large enough to hold the patches and with enough muscle to supply the patches to Patch Manager as needed. Finally, you are offered the opportunity to install the Reporting Center. This requires an IIS server. Once this has been done you can begin to use Patch Manager.

Using Patch Manager

When you first start Patch Manager, you are presented with an array of options (**Figure 1**) including scanning systems for required patches, pushing patches as and when required, and reporting. You can configure Patch Manager to send alerts when any problems are discovered during a scan. Additionally, you can define policies to be applied to certain systems. During scanning, these policies can be compared with actual system contents and deviations are highlighted.

Scanning The first step in scanning is to determine which systems to scan. Patch Manager enables you to search for systems in several ways: based on Active Directory, from NetBios, or manually, where you specify host names or host IP address ranges. Patch Manager then goes away and presents you with a list of discovered systems, which you can then select to be scanned.

Scanning can be either immediate or scheduled. The more systems you scan at any given time, the longer the scan takes. Scan time is also affected by the software that is loaded on a given machine.

When Patch Manager scans a system, it determines what operating system is running, then scans the system for patches that, according to the patch database, should be present, and reports those that are not. When scanning has completed, Patch Manager displays the results. These results let you drill down to see each system and the patches that are missing for each system or for each product. As well as presenting the results in the Patch Manager window, the software saves the reports for later review via the Reporting Services feature.

In my scanning tests I found that on some systems Patch Manager was unable to identify whether a patch was installed. Patch Manager's results suggest that this is because a system registry entry is missing – but offers no clues as to what to do (and pushing the patch again does not seem to help). Also, Patch Manager does not recognise, at present, the beta version of Windows 2003 SP1 that I am running on a few of my systems.

Pushing patches Once you have scanned systems, you can download any required patches, then push them out to the systems that need them. The push process requires you to configure Patch Manager with a userid and password that has administrative rights to each computer to which the patch is being pushed.

You can group computers, for example all web servers, and supply common credentials for the group. Once the patches are pushed out to a system, they install and, as needed, the system is rebooted. You can also get Patch Manager to re-scan the patched systems after the patches are installed. This is a nice touch.

Reporting Patch Manager's Reporting Center provides a rich set of reports for end users (such as auditors, etc) that relate to the operation of Patch Manager. The Reporting Center allows you to see a variety of information, including missing patches, pushed patches, computer and application inventory, patch analysis and patch history.

Let's get serious

Make no mistake, Patch Manager is a heavy-duty, no-nonsense product for serious patch management. Most organisations will need to do some work to define the various system groups and patch policies, as well as to populate the initial database. You will almost certainly have to do some investigation after you start to run it, to work out why some patches do not seem to have been applied. You might also wish to consider taking some installation assistance from Pillar to ensure the package is implemented efficiently.

One of the major benefits of Patch Manager is its comprehensive scope, covering both the operating system and Microsoft Office. It also scans non-Windows systems, although the version used for this review only supported Solaris.

Patch Manager did have some glitches. For example, after each scan, it opened the first (not the most recent) scan. I also found that some of the error messages – for example those about 'unsupported versions' – were not as clear as they could be. In general, I'd have liked the product to be more prescriptive – telling the administrator what to do, rather than just what was wrong. But I suspect that the people this tool is aimed at will not find these issues particularly difficult to work around. And it's worth saying that the support is first rate – the folks at Pillar called back quickly to help me resolve some initial issues getting the licence. Support was very slick and professional. <

Thomas Lee is chief technologist at training company QA, and ESM's Windows editor. He is a Microsoft MVP and a frequent speaker at trade events around the world. You can reach him at thomas.lee@esmag.co.uk