Automatic patch management applications

In 2006, the CERT program at the Carnegie Mellon Software Technology Institute released a statistic of up to 8,000 vulnerable applications that needed to be patched.

In the future, vendors will only offer secure software, patching will only be a matter of the past. Of course this will be effective remedy for our lives. In 2006, the CERT program at the Carnegie Mellon Software Technology Institute released a statistic of up to 8,000 vulnerable applications that needed to be patched. 30% increase compared to 2005. Not all dangers are successfully patched. Today we are facing more attacks than ever before and with many companies specializing in IT patching is still a lot of worries, because they mostly lack tools, methods and resources. necessary for effective patching.

But that is not the reason for us to stop. No less than 14 patch management agents are continuing to research and offer new products. Each product has its own strengths and weaknesses. Firms are hoping to bring most of these products into the lab in the future, which will highlight resources like PatchManagement.org Listserv, and make a decision to discuss patch management topics. wide-ranging security in operating systems, applications and network devices.

In large companies patch management will be a component of distributed management systems and comprehensive software configuration. Smaller companies can also engage with standalone tools, but many companies need different products for different types of applications and devices. When you manage, automation also has problems such as document changes, checks to make sure that the patch does not destroy other applications and implements methods to avoid network interruptions.

What happens in Redmond .

In response to the need to patch familiar applications such as computer use, Windows upgrades and Microsoft's market dominance focused on this issue. Since the release of Windows 98, Microsoft has included automatic patching on Windows servers and desktops. The current version is Windows Server Update Services or WSUS provides an internal management software that continuously updates to Microsoft Update system. Using WSUS can automatically distribute patches and update them to another machine from a central server.

WSUS was started as a software update service and focused only on operating system patches and bug fixes. The current version extends beyond the scope of the software that can be updated and is a major improvement when using the Windows Microsoft Update website. You will save bandwidth, time and disk space. Although individual computers do not connect to an external server, it concentrates patches through an internal central server. With Windows 2008, this feature will work with the application. WSUS is a free download program on the Microsoft website.

But most companies have many other machines that are not just desktops and Windows servers. Therefore, the free tool of Microsoft does not meet the requirements of big companies.

Provide timely

Patch management tools are often found at software distribution sites. The more popular the reserve and configuration management in the beginning, the more it will be expanded. Are these tools worthwhile? It depends on the type of patch you need to deploy. If you are responsible for network devices as well as servers and desktops, a tool that can handle all these problems like Opsware of HP will be very valuable. If you only have problems on desktops, you can use CA's patching program. If you need to patch the server, do you only use Windows, or Unix, Linux, and virtual systems?

Maximum automation is very important. You should not patch it manually. Record a detailed list of every step in the patching process, from collecting information to determining the severity of every detail when detecting patches affecting other systems. or decide which end points will be updated. Requesting all the above steps can be automated in the software you are using.

Controlling changes is as important as patch management. How often and how often does your patch apply? Who can deploy or allow updates? How are the patches checked before being released? What problems motivate them to come back? All these questions define the whole process. We often see firms spending more than a month on patching applications, targeting viruses and security breaches.

Understand how many devices you have already managed, and future caveats are also important when considering software. Within the scope of management from 50 to 100 devices, can reach hundreds of thousands. Large companies consider using configuration products related to each other such as software distribution or CMDB, including ensuring flexible patch management capabilities. If you have a property and inventory system, check the patch management function.

Applying patches against negative impacts whether you want to be without users and the network, consider those products to solve the abuse and devices that cannot be connected at the same time. Can it use network bandwidth effectively, such as multi-function distribution channel leasing, high compression, restart test capability? If a communication link is cut off, the end device is an out-of-network laptop or for some reason the application failure fails, what will happen? There will have to be a direction for the software to stop having to patch it up again and follow a series of notifications, warning from this repeat failure.

The report is also very important. Ensure that the product can support verification as well as notifications to provide clearer information about what patch management applications are doing. In many Sarbanes-Oxley-protected public organizations, this is a strict requirement that, if not paid attention, can have serious consequences.

Software firms "save"

In general, there are four categories of patch management products based on functions and user agents: Desktops and Window servers with optional agents; Windows desktops and servers with required agents; Multi-platform systems with required agents and a virtual data / support center. Here are some products we have put into testing.

Windows desktops and servers with optional kernels : Many organizations are willing to devote dedicated resources to patching hundreds or even thousands of Windows desktops and servers before a virus or malicious code spreads. spread throughout the network. Products such as Shavlik's NetChk Protect combine patching and spyware management with the option of using agent-based architecture; It can patch nearly 700 applications and Window operating systems. Many vendors, including BMC, Symantec and Microsoft use Shavlik to manage patches.

Similar to Shavlik, Ecora's Patch Manager gives administrators the option to use agents or run without them. By gathering research, appraising and installing patches on both Windows clients and servers, Ecora uses bandwidth to limit network resources to patching. Important functions such as reverse patching and the ability to specify test patch environments prior to production deployment have been promised by Ecora, and many accompanying reports support testing.

Desktops and Window servers with required agents : Agents commonly used in environments that are not allowed to access device management, such as disconnected laptops on the community network.

Kaseya's Patch Management software automatically detects error updates and can automatically deploy the installation on a specific chart. When the program scans it can summarize the results for each machine and decide whether and what errors and updates will be applied. Administrators can also monitor and verify patches. Novell's ZENworks configuration management program will issue a notification when there is a new security update and ensure that the update has been delivered. Novell provides a group of security experts to support many organizations updated websites.

IBM Configuration Manager provides automatic patching capabilities for Microsoft clients and servers in distributed environments. Configuration Manager can also scan clients, identify errors, build a patch plan and distribute the requested copies to the client. Like IBM, Patch Management of CA Unicenter also focuses on Window typically desktops. CA monitors and evaluates the latest patches.

Multi-platform, agents are required

If you have a machine environment including Unix, Linux and or Mac OS, the provider will support multi-system applications and operating systems. In addition to offering larger management products, BigFix provides patch management and security updates for major operating systems as well as general applications and can

handle more than 50,000 devices. You need to run the BigFix server on Windows and deploy an agent on each management node.

LANDesk's Patch Manager includes a donation service that will gather and analyze patches for heterogeneous environments. Like other programs, it scans management devices to identify vulnerable applications and operating systems; When an error is detected, you can download the combined patch and research requirements, depending on the impact. LANDesk monitors the status of each installation and provides detailed bandwidth and notification to a wide range of operating systems.

The BMC Patch Manager, formerly Marimba, provides testing capabilities that allow administrators to minimize risk by analyzing the impact a patch will have on an endpoint and identify conflicts or problems. Other threads before patching. BMC Patch Manager Policy Engine facilitates initial patch installation and subsequent control patches to ensure installation of endpoint management.

PatchLink Patch Management of Lumension automatically collects, analyzes and distributes the patch software on multiple operating systems. It also focuses on reporting.

Other vendors approach the CMDB deployment to manage and control the patch. ConfigureSoft's Enterprise Configuration Manager (ECM) automatically detects new systems and monitors security configuration changes for the latest patch information available. The ECM team operates by function or role and supports testing on other configurations. The software continuously updates patch status on all machines and maintains the patch verification process. Similarly, Altiris Patch Management by Symantec is centralized, easy to expand storage to operating systems, hardware and software.

Multi-platform, required agents, centralized support / virtual data centers : When companies aim to consolidate data centers and virtual machines to reduce costs and increase efficiency and security Can maintain the server uniformly. Patch management is important, noting compatibility with vendors that support complex operating systems including Windows, Linux and Unix servers on VMware, Opsware / SAS of HP or BladeLogic.

BladeLogic is more focused on the central server data environment than the desktop and supports operating systems and server components such as central components, utilities, system software and multi-tier applications. virtual environment. BladeLogic uses a policy-based approach where all changes are applied to a policy, which is then synchronized with the destination server. The company believes that this method has low cost combined with management servers. Configuration management also highlights a single multi-line command line interface for using authentication protocol ranges. All communications are encrypted, and all user activity can be allowed based on rules, key to highly secure environments and things that are not available in the market.

Opsware SAS will automatically search for hardware, configuration and software. With large configuration redundancy, SAS can identify and patch a large number of servers as well as create and monitor patch execution. SAS also uses the best control methods to respond quickly to security security or patch vulnerability.

7 shortcomings when patching

1. Do not check the patch in advance. Some patches will not be compatible or even corrupt other applications.

2. There is no reverse version. If the patch fails, you need to re-create it.

3. Dead network. Deploying multiple patches at the same time through the network will affect other applications that are annoying to users.

4. "Reboot" Many patches require users to reboot the system, please restart when appropriate.

5. Loss of patch. Often users rush into searching for missing patches. Using the latest version optimizes downtime.

6. Do not patch up the audit. If the patch is regular, you need tracking that hinders the application to provide auditing and reporting.

7. Do not formalize the patching process. One way to identify users can approve patches and implement them to successfully manage the patch.