

SELECTING PATCH SOFTWARE

Author Rod Trent provides a comprehensive list of criteria for selecting patch management software (*The Administrator Shortcut Guide to Patch Management*, New Boundaries Technologies, Realtimedpublishers.com, 2004, pp. 39–46). Obvious considerations need no explanation, such as ease of use and cost. When purchasing a third-party patch management software program, which is highly recommended, make sure it comes from a reputable software company, especially one that specializes in system security. These vendors are more likely to test patches for a variety of systems and provide technical-support alerts for patches that can cause problems. Other considerations are as follows:

Agent Versus Agentless Patch Management Software

When considering the purchase of patch management software, one of the first steps is to determine whether an agent or agentless patch management system is needed. In an agent system, each computer within the organization must have the patch management software installed. These systems scan the host computer and report the various versions of software programs installed to a central location (i.e., network server), with the necessary patches being sent back to the host computer for installation by the user or upon reboot. Agentless patch management systems are installed at a central location (i.e., central server) and periodically scan all computers on the network. Once a computer in need of a patch is identified, the patch is sent to the appropriate computer. If a critical patch needs to be distributed immediately, an agentless system can send patches only to those computers connected to the central server. If an organization has a large number of laptop computers that travel and are not always connected to the central server, an agent system may be the better choice. Generally, agent patch software is more expensive because licensed copies of the software reside on each host computer.

Platform Support

One challenge for large organizations is the variety of operating systems and versions thereof used to run the applications. The more operating systems used, the more complex the operating environment, and thus the patch environment. In such cases, it is important that the patch software can operate under

different operating systems, such as Windows Vista, Windows NT, Windows XP, Windows 98, Linux, and Mac OS. Even smaller organizations may be using various versions of the same operating system. Attacks will target the weakest part of an information system, so it is important that all components are working with the patch software to strengthen information system security.

System Targeting

System targeting allows for targeted patches; that is, deployment of patches to specific computers. This targeted approach will enable the patch management team to deploy patches based on the risk hierarchy. It also enables patches to be sent only to those computers that need them, reducing the bandwidth needed. System targeting can also help during the testing of patches in the event that the patch testing was incomplete prior to the deployment, which may occur when a zero-day vulnerability is discovered, by tracking those computers that received a specific patch.

Customized Deployment

Customized deployment allows the software to spell out when and to whom patches will be sent. For routine operations, patch software should allow for patches to be sent throughout the system during nonpeak hours to reduce the possibility of an impact on system functionality. Some patch management products allow users to adjust the bandwidth to reduce the impact. Once a patch resides on an individual computer, how the patch is installed must be decided upon by the patch management team. In many cases, patches require a system reboot. End users should be sufficiently trained to understand the critical importance of their involvement in patch management, as well as the consequences of failing to fulfill the organization's expectations. Some patch software applications automatically reboot systems and do not allow end users to override a system-initiated reboot.

Regardless of the application that is used, an organization should have patch software that is flexible enough to accommodate any desired deployment needs. The right software features can significantly increase the responsiveness of the patch management system to security threats.