



Taking a Proactive Approach to Patch Management

BEST PRACTICES GUIDE

It's a fact of business today: because of the economy, most organizations are asking everyone, including the IT staff, to do more with less. But tight budgets and the need for the IT department to be a "jack of all trades" (and specialists at nothing) could leave organizations vulnerable to attack.

Setting up secure borders at the datacenter is no longer enough. Security must extend to virtual machines and the endpoints that connect to the network. But managing patch updates for these resources can be a complicated process. The sheer numbers of endpoints make it almost impossible for the IT staff to update each one individually, and the limited visibility the department has into the endpoints' configurations can make it even more of a challenge. Also impacting security is the fact that the IT staff may not be able to keep up with the latest threats, research issues of concern to the fullest extent and understand the magnitude of the threats since they are unable to direct all their attention to security matters.

To ensure that your organization is protected, your IT departments must take a proactive approach to patch management. This white paper will show the importance of patch management in protecting your organization. In addition, it will outline best practices that can be implemented to ensure your organization can address security proactively, rather than having to react and inefficiently utilize valuable resources when viruses, malware or worms attack.

Threats from Every Direction

There are three primary types of threats that may impact an organization that does not have a good patch management strategy in place:

- **Malware and viruses** – Individual endpoints, or an entire network, can be infected with malware and viruses through a variety of methods. Malware and viruses can come through websites, instant messaging and email attachments. The most common types of malware and viruses include worms, which are self-replicating malware that can spread to other computers without user interaction, such as conficker or stuxnet; trojans, which provide a backdoor into an infected system; and botnets, which run silently in the background while waiting for operators commands to deliver denial of service attacks or mass email spam relays.
- **Data leakage** – This security breach can happen when critical company information gets into the hands of a rogue employee or is accessed by hackers.
- **Denial-of-service attacks** – In this scenario, multiple systems can attack a single vulnerable point in an attempt to cause disruptions in service.

What is Patch Management?

Simply put, patch management involves acquiring, testing and installing multiple code changes ("patches") to a computer system or application. For effective patch management, an organization or individual must stay current on which patches are available and when, then decide what patches are appropriate for particular systems. Once patches have been deployed to an organization, systems must be tested to ensure they were installed properly and the IT staff must document all associated procedures, such as the specific configurations required.

Every organization handles patch management in its own unique way—from the person or group that is responsible for installing patches and when they do it, to how it is done. Some use an agent for making patches, or they rely on agentless solutions. Some do it manually, while others rely on automated solutions. Some use only Windows Server Update Services (WSUS) to patch their Microsoft Windows operating systems and other Microsoft software, ignoring patches to other third-party applications which can be more problematic.

When undertaking patch management, there are a number of challenges your organization must address. For instance, it is important to know the difference between a security patch and a non-security patch. A security patch is one that fixes a vulnerability that could be exploited, while a non-security patch repairs a problem with a software program and does not impact security. When addressing either type of these patches, it is imperative that they are applied to every machine (physical or virtual) and that they are applied correctly. By not taking this second step and ensuring proper installation, you can be lulled into a false sense of security and still be at risk to having your network exploited.

You can no longer count on antivirus and antispyware alone to defend against today's and tomorrow's threats. With so many new tools to create malware, the number of new threats is growing each day at explosive levels. These threats cannot be managed solely in a reactive manner with antivirus and antispyware solutions. To truly control risks, security must be managed proactively using patching to inoculate machines from threats. To ensure optimal security, patching is required on three levels. These levels include operating system, application and virtual machine.

Most organizations rely on Microsoft's monthly patch update, commonly referred to as "Patch Tuesday." On the second Tuesday of each month, Microsoft issues its latest security and software patches. However, this is not the only time you'll see patches from Microsoft or other vendors. If Microsoft decides that the threat of vulnerability is too high to wait for the next Patch Tuesday, it will release a patch immediately. The same holds true for other software vendors, which release patches whenever they become available. This constant stream of updates from a variety of sources can make it difficult for your organization to ensure that it has all of the most current patches your network and systems require.

Also complicating patch management is the growing number of physical and virtual machines in use, which provide even more new entry points for security threats each day. The physical machines that require patching include the obvious endpoints, such as servers, desktop computers and laptops. But there are other security threats that you may not initially think of such as removable storage devices and software applications, including third-party applications from Adobe, Apple and Sun. Laptops and removable storage devices present additional challenges because they're often disconnected from the network and not readily visible, making it difficult to track and manage patching effectively. The virtual machines that can expose an organization's vulnerabilities include software environments or operating systems designed to emulate a real machine. These can sometimes be offline when scans or updates are being performed, resulting in the chance that critical patches are not installed.

Other patch management problems faced by IT departments include complicated or inefficient solutions for patches and limited visibility or operational processes to properly manage and maintain the security of endpoints. For instance, some solutions require use of multiple agents or require users to patch each machine individually without the assistance of automation. And because of the limited visibility into the endpoints, the IT department cannot control patches and confirm that they've been installed properly to ensure optimal security.

Best Practices for Patch Management

To simplify processes for your organization's IT staff and to ensure maximum effectiveness of patch management efforts, there are several best practices that you can apply.

- **Time for a critical assessment** – From the start you should inventory what you have, so you know what you need to protect. This inventory should include all the physical and virtual machines in use, as well as the software installed on each machine. For instance, your organization may provide Microsoft Internet Explorer as the standard browser, but individual employees may install other browsers, like Firefox, because of their own preferences. During this process you should migrate away from end-of-life software, such as Windows NT, Windows 2000 and Office 2000, which are no longer supported by patches. If you find this software on individual computers, you should upgrade to more current versions. And finally, you should remove software that is not being used by individual employees in the course of their daily work. By doing this, you eliminate the risk of the system being attacked by a threat that relies on that particular software.
- **To Microsoft and beyond** – While organizations can get free updates from Microsoft WSUS, it's important to realize that the most commonly attacked software is not from Microsoft. According to The SANS Institute, the majority of the top 10 most exploited applications were third party applications from Sun/Oracle (Java) and Adobe (Acrobat, Flash and Reader). As a result, a patch management program would not be considered complete or effective if it didn't include patching these prominent vulnerabilities.
- **Set a schedule for patching** – Patching should not be an afterthought. At a minimum, patches should be applied at least monthly, and if possible shortly after Patch Tuesday. However to ensure maximum security, a more frequent schedule is preferred. Once determined, this maintenance schedule should be shared with the entire organization. As part of the regular updates, the IT staff should test patches against a group of test machines to ensure that the patch does not adversely impact functionality of the applications or network.

- **Partner with an expert** – If your IT staff does not have the time to live and breathe patch management, it is imperative you find a partner who does. You should seek solutions by experts who focus specifically on security threats and patch management, rather than those who simply provide vulnerability management. By working with a true patch management vendor, you will be able to not only identify the vulnerable programs, but you also can patch them properly. In addition to finding the right partner, your IT team should continue to follow the latest developments in the patch management world – from reputable blogs and websites such as patchmanagement.org – in order to help prioritize patch installation and understand recent security advisories and zero-day exploits.
- **Automate whenever possible** – Finding an automated patch management solution can save your IT department time and money and increase compliance with internal and government regulations. Automated systems often will provide patches shortly after they are released and can update systems—including virtual servers, laptops and devices—without requiring too much time and effort. In addition, these automated solutions provide control over deployments, and greater visibility into the success of patch installations.

By utilizing these best practices, your organization can set up an effective and efficient patch management process that will enable the IT staff to spend more time focusing on their key responsibilities rather than fighting viruses or other security breaches that can occur if patches are not implemented correctly.

VMware Go Pro: Secure Your Entire IT Infrastructure

VMware Go™ Pro was developed in partnership with Shavlik Technologies and uses the same proven patching engine as Shavlik's flagship product NetChk Protect. VMware Go Pro leverages Shavlik's expertise in patch management to simplify patch management, so the IT team can focus on strategic business initiatives. VMware Go Pro secures both physical and virtual IT infrastructure by patching operating systems and applications on virtual machines, as well as all the endpoints that connect to the network. That means from the guest OS on a virtual machine to the application on an end user laptop you're protected. In addition to patching Operating Systems and applications from Microsoft, VMware Go Pro also patches the most frequently targeted applications from Adobe, Apple, Google, and Mozilla. It also identifies patch severity levels so you can easily prioritize based on severity level and address the most serious vulnerabilities first. And since VMware Go Pro is a web-based service, the IT team can access these capabilities from anywhere.

VMware Go Pro provides a comprehensive and easy to use patch management solution that will streamline patch management for your organization ultimately saving it time and money. Instead of multiple point solutions for assessment and patching of different pieces of the IT infrastructure, VMware Go Pro is a single solution managed from a simple web console that can protect your entire IT infrastructure from vulnerabilities. All this comes in an affordable package designed to make enterprise class security achievable by businesses of any size.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-TECH-WP-PATCH-BEST-PRACTICES-USLET-101