

The Cost of “Free” Versus Best of Breed:

Cost and Security Efficacy- Shavlik vs. Microsoft Patch Solutions

Introduction:

An effective patch management program is fundamental to a sound security program. Gartner and CERT both state that more than 90% of all security exploits could be avoided if organizations would simply completely patch their systems. A recent *InfoWorld* [article](#) suggests that more than 98% of 20,000 randomly surveyed systems across many companies contained at least 1 unpatched application, 46% contained 11 or more unsecure applications. Many of these were non-Microsoft applications. Not surprisingly, the hacking community has learned that many organizations are patching Microsoft OS and Office applications, but the vast majority of organizations do nothing to protect themselves from patchable vulnerabilities from highly pervasive non-Microsoft applications like Java, Adobe, Firefox and dozens more. The consequence- you guessed it, an explosion in exploits for non-Microsoft applications. Beginning in 2008, Shavlik routinely issued more security updates for non-Microsoft applications than Microsoft OS & Applications. The analyst community agrees. In another recent [article](#), Gartner suggests that organizations using “free” Microsoft patch solutions as “good enough” are incurring significant additional costs and that if organizations are looking for the most effective patch solutions, they need to look to purpose-built, best of breed solutions. Of course a patch management program requires not only technology but strong process, including patch selection, testing and more. Process matters are beyond the scope for this paper, which is focused on giving you *high level requirements* for a patch management technology and relevant cost considerations.

What are the properties of an effective patch management program?

A complete list of requirements depends to a degree on an organizations risk tolerance. If your organization is looking to maximize security while minimizing administration costs associated with your patch program, look for:

- **Machine Coverage**: An effective solution covers your entire infrastructure and does not leave out important parts of your environment such as non-domain joined machines, off-line virtual machines and frequently disconnected laptops. Preference may be given to a solution that can discover machines on your network.
- **Application Coverage**: A solution should cover all of the applications you deem appropriately in-scope for patch management. The days of not covering non-Microsoft applications may soon be past. Many organizations also have in-house applications. It makes sense to have a program that incorporates or can incorporate ANY security or bug-fix update. In the past, many organizations did not patch non-Microsoft applications proactively because the labor costs to do so would be prohibitive. Often these organizations scrambled to push out patches in response to zero-day or other “in the wild” exploits. This method leaves organizations vulnerable, reactive and incompletely patched. Organizations should seek to proactively patch, as part of their security operations program, all applications that are present on a certain percentage of their network. We suggest patching applications that are present on at least 5% to 10% of servers or workstations.
- **Off-line Laptop Coverage**: An effective patch management program enables organizations to apply real or near real-time security updates to highly vulnerable laptops that are often off the network. Exploits like Conficker often found their way on to networks via laptops that went unpatched month after month simply because they are not present on the network at patch time.
- **Scanning Accuracy**: An effective patch management program is based on scan results that can be trusted. Scans should never rely on simple registry scans. Deeper, file level scans are required to ensure a patch cycle

was not disrupted, for one of many possible reasons, resulting in a positive registry entry but an effectively unpatched system. False positives like this are very dangerous. Again, it would be helpful if a solution could also discover systems so machines are not missed because of broken or missing agents. Scanning accuracy and scanning coverage are highly related.

- **Appropriate Basic Reporting and other Functionality:** Effective patch solutions have at their disposal technologies that enable them to do important things like patch roll-back should it be determined that a patch is causing instability on their network. Further, organizations should evaluate the reports offered by automation tools to ensure they provide the information needed to evaluate risk and meet compliance and audit needs. Such reporting should extend beyond a list of what machines have which patches and extend to provide a detailed evaluation of risk exposure, including a rank ordering of vulnerable machines, a listing of the criticality of patches that are not applied, who applied patches and when and perhaps more. Organizations will often have different reporting needs; check to ensure the available reports meet your needs both today and in the future.
- **Low Cost of Administration:** An effective patch solution is highly automated and does not require, for all but the largest organizations, more than one or two hours of dedicated personnel time per month to scan and deploy patches to all machines and to all in-scope applications. Further, facilities should be in place to ensure obstacles to a fully automated patch program can be readily overcome. This includes, for example, the ability to stop a service before a machine is rebooted if there is concern that such an application may hang at reboot. Another example would be the ability to pull a machine from a cluster, patch it, and then return it to a cluster without manual intervention. If it is time intensive or not fully automated, it is not an effective patch process for cost-conscious organizations.

How do I quantify the cost advantage of Shavlik over a Microsoft patch solution (MPS)?

First, Shavlik has a [ROI calculator](#) for addressing WSUS. WSUS underpins all MPS solutions. This cost model only takes into account the cost of time spent on your patch process. It does not consider return on risk-mitigation savings associated with unplanned down time, possible damage to brand, or the loss or misuse of customer or other critical data. This should be considered if you believe Shavlik improves IT Security. Let's reexamine some of the requirements listed above in light of how they can affect the total cost of ownership (TCO) of a solution.

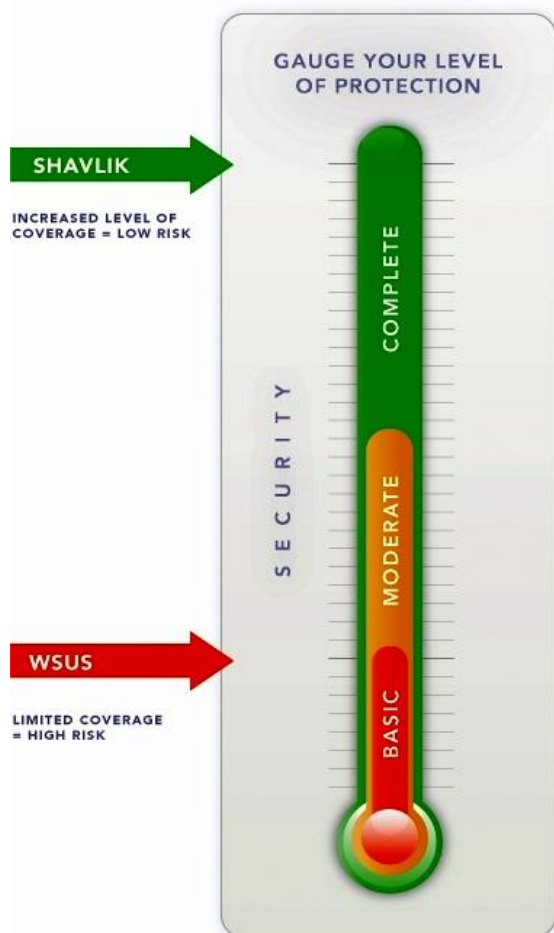
- **Machine & Off-line Laptop & Virtual Machine Coverage:** In most cases, organizations that want to reach all of their servers and workstations must purchase, roll-out and administer another solution to address these machines. There are significant labor costs and some software acquisition costs involved here. If organizations chose to patch only a percentage of their machines, risk-related costs should be considered. Many exploits, like the recent Conficker worm, found their way onto networks via machines that were either not addressed by their patch solution, or through laptops that did not receive timely updates because they were off the network during patch cycles. Shavlik enables agents on laptops to check-in over the internet with a repository placed in your DMZ. As long as your users access the internet, they will be patched. Additionally, there are no comprehensive patch management solutions other than Shavlik that provide the ability to locate and patch **off-line VM sessions**. Like off-line laptops, these VM sessions can greatly increase your threat surface. Once a machine has been off-line for a period of time, it is sure to be missing security updates. These vulnerabilities can be freely exploited once the machine is brought on-line. Only with Shavlik can you do a search of your drives to find off-line VM sessions, mount and patch these sessions (without physically starting the VM) and return it to its previous state- ready to apply the patches the moment the VM is brought on-line. Lastly, Shavlik can be implemented via agentless technology, allowing organizations to run IP range scans to find machines on their network. We will find

ANY machine on your network, whether it has an agent installed on it or not. This increases your patch coverage, identifies rogue machines, and reduces change and configuration management costs associated with maintaining unneeded agents. . Non-domain joined machines are easily patched by Shavlik, however these are not addressable via Microsoft solutions. Free is not free if it does not patch your machines.

- **Application Coverage**: MPS has out of the box coverage for only a [small percentage](#) of the applications that should be patched (see illustration at the bottom of this paper). There is no way to patch these applications with WSUS. Efforts could be made to patch these applications using SMS/SCCM, but very significant administrative costs apply to building the data to patch these applications. Shavlik, for example, spends over 600 hours MONTHLY to build and test the data for the applications we cover. This is with a highly trained data team. Organizations can expect to spend a similar amount of time, monthly, to build a patch management program on par with Shavlik's application coverage across a highly heterogeneous network. Organizations could elect to patch only a small subset of these applications or patch on a reactive basis to "in the wild" exploits, but there are still hard costs associated with these efforts and of course significant risk that you may pick the wrong applications to patch.
- **Scanning Accuracy**: False positives plague many patch solutions, not just WSUS, SMS & SCCM. Shavlik is an acknowledged leader in this space and has been chosen as an OEM partner to provide scanning capabilities for solution providers like BladeLogic, VMware, BMC Marimba and many more. During a recent customer audit on just 95 machines (a mix of servers and workstations managed by overlapping WSUS and Altiris scans) we found more than 600 missing patches. Many of these related to applications they could not or were not patching, but more than 150 were Microsoft related patches, many years old, OS related and critical. Organizations could purchase a tool like Shavlik NetChk Protect Audit Edition, but there are software acquisition costs and duplicated efforts. Of course having a trusted source for a true "second opinion" is a best practice. Shavlik is more than willing to prove to organizations that they are not as well patched as they think. Ask and we will prove it.
- **Reporting and other Features**: Shavlik provides 25+ reports- many times that of any MPS. Furthermore, Shavlik provides much more detailed information on your patch efforts, telling you who patched the machine, when the patch was applied, and of the missing patches, which are critical, important and so on. Graphical data are presented for at-a-glance information, detailed root cause data is provided any time a machine is not scanned or patched. We even provide a list of your most vulnerable machines and much more. To assemble information like this with a MPS would be untenable. More likely you will go without. Going without means more time spent on IT security audits (with accompanying costs) and less visibility into your security. Furthermore, Shavlik allows numerous automated email reports not available on any Microsoft patch solution. For many organizations, this significantly reduces administration time because they don't have to log into the console often to find reports or results. Scan and deployment reports can be sent to administrators so they can effectively manage Shavlik from their inbox. Application or system owners can receive reports in advance of a reboot that show what was found and the date and time a reboot is scheduled. This increases communication and reduces the chance for unplanned down-time. Shavlik offers right click and click patch roll-back. WSUS does not offer any similar functionality. While this is seldom used, should you need it, the ability to rapidly uninstall patches can greatly diminish application down-time. Also, because you can instantly push patches with Shavlik's agentless (or agent-based) patch solution, you will never be left flat-footed should you need to get patches out in a hurry. Agentless also means you know PRECISELY when a machine will be rebooted and therefore will not face costs or adverse exposure associated with unplanned downtime. Granular machine targeting ensures you do not have to rely on your Active Directory OU structure to define how you will differently target machines with different patch policies. This is just a start; there are MANY additional differences.

- **Low Cost of Administration:** There are many ways Shavlik reduces costs associated with ongoing administration- some have been discussed previously. Our application was designed at the onset for ease of use, and Shavlik has built-in tools to script around most anything that prevents full automation- the emailed reports further extends our ability to allow you to set and forget your patch process. Everything needed to patch **all** your machines, **all** in-scope applications is included. None of this is available with Microsoft patch solutions without very extensive & costly customization efforts.
- **Other Cost Saving Current Functionality:** Shavlik offers additional features and integrated applications that are not available on any Microsoft patch solution. As of June, 2009, Shavlik makes available free, integrated, high performance AV, Malware and Root-kit detection and removal with our patch solution. This alone can off-set much of the cost of our solution. Shavlik believes you should patch all of the applications you need, and remove the ones you don't want. Included with our patch management application (NetChk Protect) is full application blacklisting or whitelisting so you can block the use of unauthorized applications on your network. These threat management tools offer significant additional value.

Shavlik offers simplification, visibility, safety, & cost reduction through automation



Shavlik Any-Patch, Anywhere Solutions Cover All These Products

3RD PARTY APPLICATIONS

- | | | |
|-----------------|-------------------|--------------------|
| Adobe Acrobat | Apple Safari | Sun JAVA |
| Adobe Flash | Blackberry Server | Thunderbird |
| Adobe Reader | Citrix | VMware Server |
| Apache | Firefox | VMware Workstation |
| Apple iTunes | RealPlayer | WinZip |
| Apple Quicktime | Skype | |

MICROSOFT OPERATING SYSTEMS AND APPLICATIONS

- | | | | |
|------------------------------|---------------------------------|-----------------------------------|-----------------------------------|
| Access 2000 | Internet Explorer 5.5 | Project 2000 | Visual Studio .NET |
| BizTalk Server | Internet Information Server 4.0 | Publisher 2000 | Windows 2000 SP3 |
| Client Security | ISA Server 2000 | Services for Unix | Windows Forefront Client Security |
| Commerce Server | Java Virtual Machine | SNA Server | Windows Live |
| Content Management Server | MSDE 2000 SP3 | SQL Server 2000 SP3 | Windows Journal Viewer |
| Excel 2000 | MSN Messenger | SQL Server 5.5 | Windows NT 4.0 |
| Exchange Server 5.5/2000 | Office 2000 XP Gold | SQL Server 7.0 | Word 2000 |
| Front Page Server Extensions | Office XP Gold | Step by Step Interactive Training | World Viewer 2000 |
| Host Integration Server | Office XP SP1 | Visual Basic for Applications | |
| IE 6.0 Gold 2000 | PowerPoint 2000 | Visual Foxpro | |
| IIS 5 SP3 | Producer for PowerPoint | | |

WSUS ONLY COVERS CURRENT MICROSOFT OPERATING SYSTEMS AND APPLICATIONS

- | | | | |
|-------------------------------|---------------------|----------------------|---------------------|
| DirectX | Internet Explorer 7 | SharePoint | Windows 2000 SP4 |
| Exchange Server 2003, 2007 | MDAC | SQL Server 2000 SP4 | Windows Server 2008 |
| ISA Server 2004 | .NET Framework | SQL Server 2005 | Windows XP |
| IE 5.01 SP4 | Office 2003 | Windows Defender | Windows Vista |
| Internet Services 5, 5.1, 6.0 | Office 2007 | Windows Media Player | X64 |
| Internet Explorer 6 | Office XP SP2+ | Windows Server 2003 | |

FOR A COMPLETE LIST OF SUPPORTED PRODUCTS, PLEASE SEE <http://xml.shavlik.com/data/supportedproducts6x.htm>

Shavlik also provides, at no charge, a wizard-driven custom XML editor so you can literally patch anything on the windows platform. The illustrated coverage is also what is covered, out of the box, for SMS & SCCM. Shavlik replaces WSUS, or augments SMS/SCCM so they can do what they were primarily designed for. Shavlik is purpose-built for patch management.