GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

# Selecting Patch Management Software

Michael Foster
GIAC Security Essentials Certification (GSEC)
Version 1.4b Option 1
27 Jan 2004

**Abstract**
Network administrators and information security personnel are faced with the constant challenge to keep the network protected against current threats as well as stay on top of upgrades to applications and operating systems. While there are several ways to accomplish this, some of the most efficient methods employ patch management applications. With all the choices out there, choosing the best application for the network can be a daunting task. This paper will illustrate a software selection process and review some of the major patch management software applications and features to look for in making your decision.

## What is Patch Management Software?

Patch management software applications seek to consolidate, automate and simplify the tasks of keeping your network protected with the latest security patches. There are standalone products and those that offer patch management plug-ins as part of a larger network management suite. Patch management tools perform the following tasks:

- Inventory the network: Gather information on target machines.
- Query the network: Search for specific patches or applications.
- Identify missing patches: Compare the target machine's patch and application configurations to established baselines and identify discrepancies.
- Apply patches to machines: Load and install required patches.
- Validate patch installation: Verify the patch was installed and the machine was rebooted if necessary.
- Reporting: Compile data and create reports for tracking purposes.

Patch management software employs two major types of architecture; non-agent-based products and agent-based products. These products use different methods to gather information and administer patches. Each product has advantages and disadvantages.

## Non-agent-based products

Non-Agent-based products scan target machines to determine their configuration and compare it to a baseline. The server then compiles a report of the hosts that are missing patches or applications. An administrator then prepares a package that is deployed to the appropriate hosts.

- Advantages: Non-agent based products are easy to deploy can be installed quickly and are usually less expensive. This type of product is considered best for enclosed, static networks.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Disadvantages: Requires services such as Remote Registry, Remote Procedure Call and SMB network access to be enabled. Scanning all hosts on the network can consume large amounts of bandwidth and degrade performance. Perimeter control devices such as firewalls may interfere with scan traffic. When a scan is conducted it takes a snap-shot of the network. Any hosts which are not currently on the network are missed.

**Agent-based products**

Agent-based products require an agent to be installed and running on the host machine. The agent periodically queries the server and compares the host's configuration to the baseline stored on the server. When a new patch or application is available the product can be configured to pull and install the patch or create a notification that the host is out of compliance.

- Advantages: Less network traffic. Processing is done on the host machine. Avoids network scanning restrictions. Machines that are powered down or roam off the network can poll the server as soon as they return. If a host is missing a required application or patch it can be configured to pull it from the server and load it automatically.
- Disadvantages: More costly and time consuming to deploy. Administrators must manage all the applications required by the hosts. Usually more expensive to purchase and maintain.

**Software Selection Process**

The selection process consists of the following steps: establishing requirements, compiling a checklist of questions, interview the manufacturer and demo the products, then make a final decision.

**Establish Requirements**

- Consult Management. The first step in preparing the selection process is to determine the command climate. What is the attitude of management concerning patch management? Is there an established threat response timeframe in the network security policy? What are the budgetary limits? There are a number of free applications available. These applications typically lack the reporting functions and ease of use that the fee based applications provide. What are the resource limits and timeframe for implementation? Non-agent-based applications are faster to deploy and require less manpower for initial implementation.

- Assess the Network. Network size and configuration is a major consideration. Classified networks may require hard drives to be removed and stored overnight or when the user is away, this would prevent maintenance and patch distribution after hours. An agent-based patch management system would ensure that all hosts were patched once they log onto the network. The number of clients to manage and whether these clients are distributed across multiple sites and LANs

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

will determine which type of patch management software architecture is required. If there are bandwidth restrictions then an agent-based product may be more desirable since the software does not have to generate the traffic required to scan the network.

- Determine the level of functionality required. Will a stand-alone patch management product suffice or is an integrated network management solution required? Many vendors offer patch management software as a plug-in or portion of a larger network management application. Reporting requirements should be determined. The type of systems and applications to be managed must be identified as well. Many of the free applications provide patch management only.

**Question Checklist**

Once the requirements have been established a checklist of questions for the vendor should be prepared. These questions should be centered toward the network and how the product can fill the needs of the company. The following list contains suggested questions to add to the checklist.

- What platforms can the product manage? If the network uses several different operating systems and hardware platforms will the product support all of them?
- What types of applications can the product manage and distribute? If non-Microsoft applications such as Anti-virus software must be managed can the product support that requirement?
- How does the product distribute software? Does the product push out the package on demand; pull to the hosts automatically or at a scheduled time, or both options? Can an administrator create custom packages to distribute other software or Qchain multiple patches to distribute as one package? Does the product only distribute pre-configured packages from the product's home repository?
- If the product distributes patches from the company instead of Microsoft, what changes and testing are done to these patches? Despite any testing by the parent company, all patches should be tested in-house before distribution.
- How much flexibility does the administrator have in distribution? Can an administrator copy the software to a host machine then schedule installation at another time? Can the administrator control the level of user visibility and interaction?
- How are patches validated? Can the product report which hosts have the software loaded but have not been rebooted and are therefore still vulnerable? Does it verify file versions as well as registry keys?
- How is scanning accomplished? Does the product take a one-time snapshot of the network or is there continuous scanning? How much bandwidth is consumed and how intrusive are the scans? How does the product handle the problem of roaming computers or computers that are powered off on a regular basis?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Can an administrator control the bandwidth consumption? Some products provide the option to throttle bandwidth usage during scanning and distribution.
- Can the product group machines by custom specifications?

**Interviews, Demos and Trial Usage**
Once requirements have been established and a checklist of questions is compiled then the actual process of selecting the software can commence. There are many vendors distributing patch management software in some form or another. Use the criteria established in the requirements step to narrow the search down to a manageable number of prospects. Contact the companies in order to gain detailed information on their products and to schedule demonstrations and sales proposals. Downloading trial versions of the software can provide more insight on the product.

**Final Decision**
Compile analysis reports on the best products and submit the analysis reports along with IT recommendations to management for review and approval. Listed below are some of the well known patch management applications.

**Types of Patch Management Software**

**-Free Software-**

**Windows Update Service**
http://v4.windowsupdate.microsoft.com/en/default.asp
This service is an online extension of Windows. Computers can be configured to automatically contact the Microsoft Windows Update site and scan for any missing patches or driver updates. This requires access to the internet, user or administrator interaction if automatic installation is not selected and the administrator will have no control over the installation of critical updates. This option may be desirable for workgroups or very small networks but this provides no reporting capability so some other form of verification is required. Secured networks may not have the appropriate access required to support this service.

- Advantages: Allows users to keep their computers updated automatically or administrators to establish policies to keep them updated
- Disadvantages: Limited control over which patches are loaded. Requires Internet access. No reporting features for multiple hosts.

**Microsoft Software Update Services**
http://www.microsoft.com/windowsserversystem/sus/default.mspx
Software Update Services (SUS) is very much like an internal version of Windows Update Service. An SUS server is configured and the host machine's Automatic Update Service is pointed to the internal server instead of the Microsoft site. The SUS server is synchronized with Microsoft's site and any new

© SANS Institute 2004, Author retains full rights.

patches or updates are listed on the SUS server. An administrator then reviews the list and selects which updates are to be downloaded and made available to the host machines. SUS requires Windows XP or 2000, a server with IIS available and configuration on host machines.

- Advantages: Allows administrators to control which patches are loaded. All hosts are loaded from a central, trusted source.
- Disadvantages: No scanning capability, no report capability.

**HFNetCheck**
http://www.shavlik.com/pHFNetChkEXE.aspx
Shavlik Technologies' tool for scanning the network for missing patches. HFNetCheck works with Windows NT 4.0, Windows 2000, and Windows XP. It can scan these operating systems as well as IIS, Exchange Server, SQL server, Front Page Server Extensions and others. HFNetCheck is a scanning tool, it cannot distribute software. Shavlik Technologies sells HFNetCheckPro which is a more complete patch management application that will distribute software.

- Advantages: Industry-recognized scanning tool incorporated by other products.
- Disadvantages: Scanning only, will not distribute software.

**Microsoft Baseline Security Analyzer**
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp
Microsoft Baseline Security Analyzer (MBSA) is a scanning tool based off of and incorporating HFNetCheck. MBSA scans for missing patches and also reports on poor security configurations. There have been reports of MBSA scans returning false positives and conflicting with Windows Update scans. Microsoft released a new version of MBSA in January 2004 to correct these shortcomings. MBSA runs on Windows 2000, XP and Windows Server 2003 and scans these products as well as Windows NT4.0, IIS, SQL Server, Exchange Server, IE, Windows Media Player and several Microsoft products. While MBSA scans for more vulnerabilities than HFNetCheck does, it is still a scanning tool and incapable of software distribution.

- Advantages: Scans for missing patches and poor security configurations.
- Disadvantages: Scanning only, will not distribute software.

**-Fee-based Software-**

**Microsoft Systems Management Server 2003**
http://www.microsoft.com/smserver/evaluation/default.asp
Agent-based
Cost: Server license with 25 agents - $1,909. Additional packs of 20 agents - $1,089

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft Systems Management Server (SMS) is Microsoft's answer to patch management. Its features include Application Deployment, Asset Management and Inventory, Patch Management, Mobility features and Windows Management Services Integration. SMS allows for application deployment by creating packages for distribution across specified collections. SMS allows for customized grouping based on specified prerequisites. SMS 2003 runs on Microsoft Server 2000 and Server 2003. The agents can run on Microsoft Operating Systems from Windows 98 up through Server 2003. Prior versions of SMS have received mixed reviews and have had problems with distribution and validation. The SMS 2003 version has numerous improvements designed to overcome these problems.

- Advantages: Custom package creation for software distribution. Recently upgraded to improve performance.
- Disadvantages: Plagued by reliability problems in the past.

**Altiris Patch Management Solution**

http://www.altiris.com/products/

Agent-based Enterprise Management

Cost: Based on the suites selected, Client and Mobile suite is $80 per seat initial cost includes support and maintenance for one year. Annual maintenance (optional) cost is $12 per seat per year.

The Altiris Patch Management Solution is a component of a larger application designed for enterprise management. The company's product is grouped into three major suites which are composed of modules called "solutions". The three major suites are Asset, Client and Mobile, and Server Provisioning. The Asset suite inventories the network assets and records configuration, applications and usage information. The Client and Mobile suite offers comprehensive management and control of desktops, notebooks and handhelds. The Server Provisioning suite offers management and control of servers to include monitoring, backup and recovery software distribution and patch management. Altiris' product has connectors for Active Directory, HP Openview, Remedy and Wise Package Studio. The Active Directory connector allows administrators to import groups from Active Directory, Windows NT and Windows 2000. The Openview connector links reporting and tracking from asset management back to HP Openview. The Remedy connector links inventory to Remedy. The Altiris product is designed for overall enterprise management and includes features beyond basic patch management. System requirements and support: The Altiris Notification Server runs on Windows NT 4 Server, Windows 2000 Server and Windows XP. The management interfaces and remote control features are web-based and require IIS running on the Notification Server. Altiris supports Windows 9x through XP with plans to support Macintosh in the future. Handheld support includes Windows CE, Pocket PC, and Palm for handhelds. Server support includes Windows NT through 2003, UNIX including Solaris, HP-UX, SunOS, Linux, SuSE, Red Hat, and Windows .Net.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Advantages: Extended functionality available to include shadow copy, profile cloning, image distribution and remote control. Web-based interface. Manages more than Windows products.
- Disadvantages: Higher cost than stand-alone products. Additional features add to the overall cost. Some features require multiple agents to be deployed on host machines.

**UpdateEXPERT v6.1**
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp
Agent-Based or Non-Agent-Based
Cost: From $14 per seat for 100 seats to $4.83 per seat for 10,000 seats, annually.
UpdateEXPERT (UE) from St. Bernard is a stand-alone patch management product. It has the distinction of using both agent-based and non-agent-based management depending on the need. The major focus is on non-agent-based deployment using Remote Procedure Call. The product supports loading "leaf-agents" on machines that are secured against remote management or in protected areas such as a DMZ. This feature gives an administrator the flexibility to use either approach. Patch deployment occurs on non-agent hosts when an administrator pushes a patch to the target machines. The patch is installed on the machine according to a schedule set by the administrator. Agent-based hosts pull the patch as needed. UE maintains a metadatabase of patches with information on deploying and validating patches as well as ensuring that all dependencies are met prior to patching. Another feature of the metadatabase is that patches are grouped by Operating System and severity. UE receives favorable reviews and has received praise for its reporting functions. UE has plug in support for HP Openview and disconnected networks support for government organizations. One limitation of UE is that it provides management for Windows products only.

- Advantages: Flexible architecture, strong report functions, patch metadatabase.
- Disadvantages: Manages Windows products only.

**Patchlink Update**
http://www.patchlink.com/products/emanagement_services/patchlink_update.html
Agent-based
Cost: One-time fee of $1498.80 per distribution server. Annual fee for Windows agents: $18 0-1000 nodes, $16.56 for 1000, $9.90 for 10,000 nodes. UNIX and Novell agents start at $60 ea.
Patchlink Update is another standalone patch management tool that receives high praise. The parent company maintains a repository database that contains patches from Microsoft, IBM, Adobe, Corel, Symantec, McAfee, Compaq, WinZip, Citrix, Novell and others. The patches on this repository are pre-tested and modified to increase stability and performance with the patch management software. Patches are supplied with severity rating and background information

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and research by the company. A key advantage of Patchlink Update is that it is compatible with Windows, UNIX and Novell products. Patch deployment and verification has shown to be reliable. Patchlink Update supports custom package deployment, grouping, recurring distribution, disaster recovery, Anti-virus support and software inventory change control. All communication, to include patch distribution occurs over port 80 or 443. If an administrator wishes to increase security then all traffic can travel over SSL. Patchlink Update does not require RPC.

- Patchlink Update Advantages: Multi-platform support, improved patch database, reliable distribution and validation, increased security provisions.
- Disadvantages: Agent installation can be troublesome, especially with UNIX and Novell agents. If machines are moved around the network then agents may need to be reinstalled.

**Ecora Patch Manager**

http://www.ecora.com/ecora/products/patchmanager/

Non-agent-based

Cost: Annual rate ranging from $50.70 per client to $11.05 per client for 1000 clients. Cost is dependent on number of clients. The company also offers Perpetual licenses with annual maintenance costs.

Ecora's Patch Manager (EPM) is a standalone product that also integrates with a larger configuration management suite. EPM has a powerful change management log that allows administrators to track changes in software loads. EPM runs on Microsoft Windows servers from NT 4.0 up through Server 2003. The product supports Microsoft operating systems and Solaris, with plans to expand to other platforms in the future. Due to its non-agent-based architecture installation and patch distribution is easy. Unfortunately, custom package distribution is not supported so EPM can only distribute Microsoft and Solaris products.

- Advantages: Fast and easy to install and distribute software. Powerful change management log.
- Disadvantages: Limited platform support. Does not support custom package distribution.

**Conclusion**

The products listed in this paper are a sample of the many products offered for patch management. Each product has advantages and disadvantages; there is no one product that is perfect for every environment. The key to success is to develop a selection process and adhere to it. This process begins with establishing requirements, then compiling a checklist of questions, interviewing the manufacturer and testing demo versions of the products and ultimately make a final decision. A strong selection process can tackle the intimidating task of selecting an appropriate patch management solution and produce a solution that supports the company's mission.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## Resources

### Articles

Fontana, John "How to Handle Patch Management." Network World. 3 Dec 2003. URL: http://www.nwfusion.com/research/2003/1201howtopatch.html. (23 Jan 2004).

Andress, Mandy. "Windows Patch Management Tools." Network World. 3 Mar 2003. URL: http://www.nwfusion.com/reviews/2003/0303patchrev.html. (20 Jan 2004).

Mueller, Patrick. "Patchlink helps keep windows closed." Network and Systems Management Review. 2 Sep 2002. URL: http://www.nwc.com/1318/1318f3.html. (20 Jan 2004).

Fontana, John. "Microsoft upgrades security tool that verifies system configuration." 20 Jan 2004.
URL: http://www.nwfusion.com/news/2004/0120microbase.html. (23 Jan 2004).

Sturdevant, Cameron. "Review: Ecora Patch Manager 2.0." 30 May 2003.
URL: http://www.eweek.com/article2/0,4149,1112991,00.asp. (15 Dec 2003).

Bradley, Tony. "The Price is Right!." Full Review: Microsoft Baseline Security Analyzer. URL: http://netsecurity.about.com/cs/productreviews/fr/aafr100803.htm (20 Jan 2004).

### Manufacturers

Microsoft Corporation. "About Windows Update." Windows Update.
URL: http://v4.windowsupdate.microsoft.com/en/default.asp. (12 Dec 2003).

Microsoft Corporation. "Software Update Services. " Microsoft Windows Server System. URL: http://www.microsoft.com/windowsserversystem/sus/default.mspx. (12 Dec 2003).

Shavlik Technologies. "HFNetCheck.exe" Product Description.
URL: http://www.shavlik.com/pHFNetChkEXE.aspx. (12 Dec 2003).

Microsoft Corporation. "Microsoft Baseline Security Analyzer V1.2." 2004. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp. (20 Jan 2004).

Microsoft Corporation. "SMS 2003 Product Information: Overview." Microsoft Systems Management Server. 2004.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

URL: http://www.microsoft.com/smserver/evaluation/default.asp. (20 Jan 2004).

Altiris. “Client Management.” Product Description. 2003.
URL: http://www.altiris.com/products/clientmgmt/. (20 Jan 2004).

Altiris. “Client Management Suite System Requirements.” 2003.
URL: http://www.altiris.com/products/sysreq.asp?id=22209. (20 Jan 2004).

Altiris. “Altiris Sales” URL: http://www.altiris.com/sales/find.asp?oc=rm.
(24 Jan 2004).

St. Bernard Software. “UpdateEXPERT.” Product Description. 2004 URL:
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp
(20 Jan 2004).

St. Bernard Software. “UpdateEXPERT 6.X Knowledgebase.” 12 Jan 2004.
URL:
http://www.stbernard.com/products/support/updateexpert/uetechfaqs/updateexpert.htm. (24 Jan 2004).

PatchLink Corporation. “PatchLink Update 5.0 The Standard in Patch Management.” Product Description. URL:
http://www.patchlink.com/products/emanagement_services/patchlink_update.html. (21 Jan 2004).

PatchLink Corporation. “Purchase/Subscription Information.”
URL: http://www.patchlink.com/products/buy_now.html. (23 Jan 2004)

Ecora. “Ecora Patch Manager.” Product Description.
URL: http://www.ecora.com/ecora/products/patchmanager/. (23 Jan 2004).

Ecora. “Contact Us.” Contact Information.
URL: http://www.ecora.com/ecora/company/contact_us.asp. (25 Jan 2004).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.