

Lumension® Vulnerability Management vs. Microsoft® Windows Server Update Services Total Cost of Ownership (TCO) Comparison

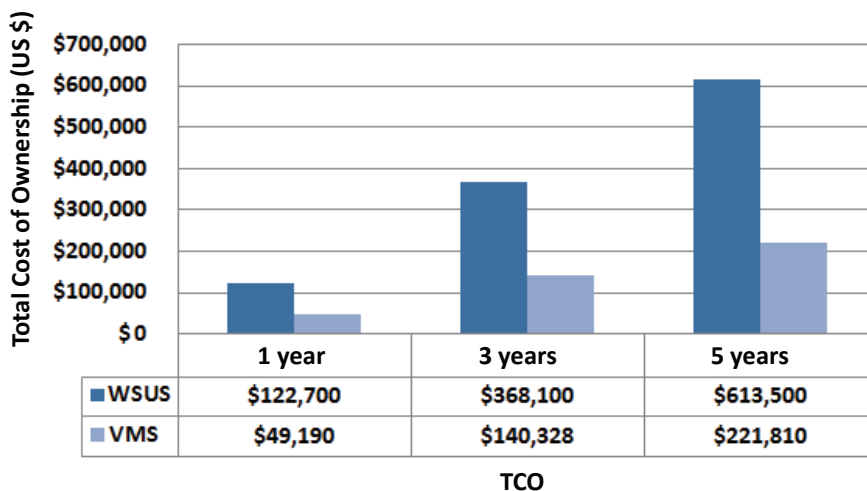
EXECUTIVE SUMMARY

The Lumension Vulnerability Management Solution provides much lower Total Cost of Ownership than Microsoft's free Windows Server Update Services and provides a full range of services including patching Microsoft, non-Microsoft, and custom applications; built-in reporting, software removal, flexibility of management control, granular patch control, Common Vulnerabilities and Exposures (CVE)-based patching, discovering new/unauthorized client system, up-to-date asset assessment and network visibility.

THE BOTTOM LINE

- 1 Lumension VMS can provide 60%, 62%, and 64% savings over the Microsoft WSUS for 1, 3 and 5 years, respectively
- 2 Lumension VMS can save an enterprise with 500 workstations \$73,510 over 1 year, \$227,772 over 3 years, and \$391,690 over 5 years respectively
- 3 Lumension's TCO advantage over WSUS arises from its diverse application support, powerful operational tools including custom content creation, software removal, and extensive reporting capabilities
- 4 Lumension's support for multiple Operating Systems will have an even greater TCO savings for more heterogeneous OS deployments

Estimated TCO for Microsoft WSUS and Lumension VMS for an Enterprise Network with 500 Workstations



Source: Tolly, July 2009

Figure 1



Overview

The current economic situation is causing a growing number of organizations to trim their IT expenses. However, security is a necessity for most, if not all, organizations.

Tolly engineers tested the *Lumension*® Vulnerability Management solution (referenced as VMS hereafter) and the free Microsoft® Windows Server Update Services 3.0 SP1 (referenced as WSUS hereafter) and designed a model to compare the long-term Total Cost of Ownership (TCO) for both products.

Tolly engineers designed the TCO model following a generic patch management framework for Microsoft applications, non-Microsoft applications (such as Adobe Acrobat, Mozilla Firefox, etc.) and custom applications (like corporate applications created by the users). The TCO analysis assumed an enterprise network with 500 workstations. Annual labor costs and the software subscription price were also considered in the model. All labor time estimates are based on hands-on testing by Tolly engineers.

Vulnerabilities in non-Microsoft applications represent an ever increasing portion of software security risks. Only 38% of vulnerabilities are from Windows Operating System and Microsoft Applications according to the US CERT Technical Cyber Security Alerts 2006 - 2008 as of October 31, 2008.

Tests showed that the Lumension VMS supported patching Microsoft applications, non-Microsoft applications,

and custom applications while Microsoft WSUS only supported patching Microsoft applications.

Tests also found that the Lumension VMS took about 1/10th the time to deploy a non-Microsoft or a custom application patch compared to using alternative methods for WSUS - a savings in time estimated to be worth around \$4,000 per patch.

Up-to-date asset assessment is essential for system administrators. Tolly engineers observed that the hardware and software inventory for the entire network could be viewed using VMS with administrator credentials. This feature could save administrators a significant amount of time during preparation, deployment confirmation, and documentation steps of the software patching process.

Reporting capability of a software update service is of great interest and value to system administrators. Tolly engineers verified that the VMS's built-in reporting functionality generated information-rich reports while WSUS only provided basic reports with limited information.


Consider the retail industry, where Payment Card Industry Data Security Standard (PCI DSS) compliance is required. Patching is specified in requirement 6.1:

"Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release."

Lumension

Vulnerability Management Solution

Total Cost of Ownership (TCO) Analysis



Tested July 2009

Lumension® Enterprise Reporting (part of VMS, referenced as ERS hereafter) provides multiple reports (e.g. Critical Patch Status report, Patch Assessment Report, Patch Release Report) which provide direct evidence for proving compliance. With WSUS, this level of reporting would require considerable additional time and effort.

Test Methodology and Results

Non-Microsoft Application Patching

Tolly engineers configured one baseline to mandate the JRE 1.6 package and another baseline to mandate the Adobe Reader 9.0 package and deployed them to all workstations using *Lumension*® Patch and Remediation. It took 10 to 20 minutes to create each baseline and successfully deploy it.

After the deployment, Tolly engineers logged into the test workstations and verified that the JRE has been patched to version 1.6 and the Adobe Reader has been patched to 9.0. The



Lumension Patch and Remediation console also showed that both patches had been successfully deployed to all clients.

WSUS console does not support patching non-Microsoft applications. Thus, the test case could not be executed. To deploy this update, a WSUS administrator could acquire the binary patches from vendors, use third party software to create Microsoft Installer (MSI) files, and then deploy patches via the Group Policy.

Microsoft documents show that the WSUS 3.0 API supports the publishing of local updates and applications. This approach is complicated and not likely in widespread use. This API method will be as labor intensive, if not more so, than the non-Microsoft application patching method represented in the TCO model.

CVE-based Patching

Monitoring vulnerability announcement feeds -- such as those provided by Bugtraq or National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) -- and being able to remediate identified vulnerabilities quickly and efficiently is important in reducing an organization's risk and optimizing operational expense.

One Microsoft vulnerability -- CVE-2009-1137 for Microsoft Office Powerpoint 2003 SP3, and one non-Microsoft vulnerability -- CVE-2009-0950 for Apple iTunes before 8.2 were tested.

Tolly engineers searched the package with the CVE number and deployed the patch to all workstations as

needed in the Lumension Patch and Remediate console.

Using WSUS, vulnerabilities can be searched by Title, Description, and Microsoft Knowledge Base (KB) article number. If the vulnerability is only known to the administrator by CVE, the cross mapping must be done manually in the patching software.

New/Unauthorized Client System Discovery

When a new or unauthorized workstation was introduced into the network, *Lumension*[®] Scan was able to discover the new workstation's information like operating system version when the workstation's firewall was disabled. When the new workstation's firewall was enabled, the Lumension Scan was still able to discover the new system, albeit with basic information on its configuration.

When using either the appropriate domain or local credentials of the new workstation, Lumension Scan rapidly deployed the Lumension VMS agent to the workstation, scanned all vulnerabilities on it, and patched it into compliance with the established mandatory baseline. It took approximately 20 minutes to discover all new workstations and mandate one patch to them.

Tolly engineers used the free Microsoft Baseline Security Analyzer (MBSA) to detect the new workstation because WSUS does not have functionality equivalent to Lumension Scan. MBSA's discovery speed was much slower than Lumension Scan and can only be used to scan for Microsoft applications.

Also, to enable WSUS to manage new or non-domain workstations which cannot be configured through the Group Policy, Tolly engineers had to configure local Group Policy entries on those workstations. This is sometimes impossible for system administrators if the workstation is in a remote branch.

Software Removal

Tolly engineers used the *Lumension*[®] Content Wizard on the server to identify the unwanted software - Apple iTunes in this test - on the network, and create the uninstall package. The package was then deployed to workstations as appropriate. The iTunes application was successfully uninstalled from all tested workstations within 10 minutes.

WSUS does not have software removal functionality. Thus, this test case failed for WSUS. WSUS administrators could use Group Policy to uninstall unwanted applications via MSI files, or log into the client to remove the applications manually.

Up-to-Date Asset Assessment and Network Visibility

Tolly engineers verified that the 'Hardware Asset Management Report by Device', the 'Software Asset Management Report by Device' and the 'Device Software and Service Report' generated via the Lumension Patch and Remediation console exactly reflected the asset inventory of all workstations, accurate to within one hour.



The Lumension Enterprise Reporting server's more detailed reports reflected the asset inventory of all workstations managed by Lumension Patch and Remediation with a reporting interval of one day.

WSUS does not provide full hardware and software inventory visibility.

Built-in Reporting Capabilities

Tolly engineers utilized the Lumension Enterprise Reporting to generate various reports like the 'Hardware Inventory Metrics Report', the 'Software Asset Management Report', the 'Operating System Patch Trending Report', the 'Device Check-in Status Report', the 'Deployment Summary Report', and the 'Vulnerability, Hardware and OS Report'.

All reports reflected the inventory for all workstations accurate 'within one day'. Lumension's built-in reporting functionality was simple to manage in the GUI-based console. It took less than 10 minutes to generate a report and to save it in different formats.

WSUS provides limited native reporting capability including Update, Computer and Synchronization Status reports. For a WSUS administrator to create reports comparable to Lumension's reports, they must either utilize WSUS APIs or tools such as the SQL Server 2005 Report builder to query on the WSUS database

or other tools developed by third parties.

Custom Application Patching

Tolly engineers used Lumension Content Wizard to create the custom patch package to apply Logitech Driver KhallInstallWrapper 4.00.121 utilizing an MSI file. The package was then deployed to all workstations via the Lumension Patch and Remediation console.

Tolly engineers also tested deploying Winzip 12.1.8519 to all workstations utilizing an MSI file. It took around 10 minutes to deploy a custom patch with Lumension VMS.

WSUS console does not support custom patching.

Granularity of Patch Control

Granularity of control over vulnerability and patch management affords administrators better flexibility in accommodating enterprise requirements and end-user experience with minimal disruption.

Tolly engineers tested the reboot notification functionality which allowed users to cancel or delay the reboot, and the deployment notification functionality which also allowed users to cancel or delay a patch deployment. Engineers

tested this feature using the Adobe Reader 9.1.2 patch.

This functionality could be enabled or disabled in each patch deployment activity. Also, the Lumension Patch and Remediate console allowed Tolly engineers to set the agent operation hours to narrow the patch deployment window.

WSUS allowed users to delay the restart or decline the Microsoft update. However, all these settings for WSUS had to be made through Group Policy and as a result they are not easily customized for each patch.

Flexibility of Management Control

Tolly engineers examined the flexibility of management control using the Lumension VMS by logging in using different user roles such as Guest, Operator, Manager and Administrator. A Guest user could only view the information in the console and could not operate the system. An Operator could deploy packages, export information, and scan the clients. A Manager could do most of the functions except rebooting clients and configuring user's settings. An Administrator had full control of the VMS.

WSUS provided only full access or read-only access to the WSUS management console.



IT Administration Time Analysis for a Generic Patch Management Framework

High Level Patch Process Step	Tolly Process / Included Steps	Microsoft Patch		Non-Microsoft Patch & Custom Patch	
Perform Risk and Compliance based Asset Management and Prioritization (referenced as Asset Assessment in figure 3)	<ul style="list-style-type: none"> Discover Assets Introduce New and Unauthorized System Confirm Network Status and System Maintenance Classify Asset Value and Risk Establish Workflow and Groups 	15 hr/mo for Lumension VMS			
		40 hr/mo for Microsoft WSUS			
		VMS	WSUS	VMS	WSUS
Monitor Advisories Evaluate	Watch for Pre-Announcements Study Vendor Information CClassify Patch Risk and Value	1 hr/mo	1 hr/mo	1 hr/patch	8 hr/patch
	Determine Pre-Requisites				
Prioritize and Schedule	Prioritize Potential Patches	1 hr/mo	1 hr/mo	1 hr/patch	1 hr/patch
	Change Control				
	Identify Test Groups				
Acquire	Acquire 3rd Party Vendor Supplied Patch Distribution and Necessary Prerequisites	0	0	0	10 hr/patch for Non-Microsoft Patches and 3 for Custom Patches
Create and Test Deployment Package	Create Installation Package				
Testing	Staged Testing	2 hr/mo	3 hr/mo	2 hr/patch	5 hr/patch
Deployment	Installation of the Patches (Staged)	3 hr/mo	6 hr/mo	3 hr/patch	40 hr/patch
	Check to Ensure Systems are Patched				
Clean Up	Determine Failure Causes / Adjust Distribution Parameters	0.5 hr/mo	2 hr/mo	0.5 hr/patch	5 hr/patch
	Remediate	0.5 hr/mo	1 hr/mo	0.5 hr/patch	2 hr/patch
Document and Update Configuration Standards	Deployment History and Standards / Baseline Document	1 hr/mo	2 hr/mo	1 hr/patch	5 hr/patch
	Compliance and Corporate Reporting	1 hr/mo	5 hr/mo	1 hr/patch	10 hr/patch
Sub Total		10 hr/mo	21 hr/mo	10 hr/patch	86 hr/non-Microsoft patch 79 hr/custom patch

Note:

- * hr/mo means hour(s)/month; hr/patch means hour(s)/patch.
- * The labor time analysis is based on a 500 workstations enterprise scenario.
- * Microsoft patching cycle is once per month; non-Microsoft and custom patching cycle is once per quarter.
- * As WSUS does not easily facilitate non-Microsoft patches, a labor minimizing GPO model has been used for WSUS and non-Microsoft patches.
- * Labor time may vary for different enterprises according to network infrastructures, administrators' skills, and enterprise required security level.

Source: Tolly, July 2009

Figure 2



Total Annual IT Administration Cost Estimate

	Asset Assessment	Microsoft Applications	Non-Microsoft Applications	Custom Applications	Software Removal	Total Labor Time	Total Labor Cost
Microsoft WSUS	480 hrs/year	252 hrs/year	1,376 hrs/year	316 hrs/year	30 hrs/year	2,454 hrs/year	\$122,700
Lumension VMS	180 hrs/year	120 hrs/year	160 hrs/year	40 hrs/year	1 hr/year	501 hrs/year	\$25,050

Note:

* Labor time per year is calculated based on an enterprise with 4 non-Microsoft applications and one custom application scenario.

* The IT labor rate is assumed at \$50/hour. According to salary.com, the average annual compensation for one System Administrator is \$99,542.

Source: Tolly, July 2009

Figure 3

IT Administration Time Analysis

Risk and Compliance-based Asset Management and Prioritization

The IT administration time estimate in figure 2 for this step is based on the observations from the New/Unauthorized System Client Detection test, the up-to-date Asset Assessment and Network Visibility test, the Management of Non-Active Directory

Machines test, and the Built-in Reporting Capabilities test.

Tests showed that the Lumension VMS will save administrators plenty of time compared to WSUS because of its up-to-date asset assessment for hardware, Microsoft applications, and non-Microsoft applications.

Detailed reports generated by VMS also help administrators to track the patching history.

New/unauthorized clients introduction and non-domain management functionalities avoid administrators

manually get the inventory of those clients onsite. Lumension Scan can schedule daily discovery and scan job to mandate all new/unauthorized workstations in time.

Deploy and Confirm Deployment

The IT administration time estimate for this step is based on the Non-Microsoft Application Patching test, the New/Unauthorized Client System Detection test, the up-to-date Asset Assessment and Network Visibility test, the Granularity of Patch Control

Heterogeneous Operating System Environment Analysis (Based on document research without testing)

Organizations often must support a heterogeneous environment that includes Microsoft Windows operating systems and other systems like the Red Hat Enterprise Linux, SUSE Enterprise Linux, Sun Solaris, etc.

The Lumension VMS supports various platforms in the same way as it supports Windows. Enterprises may choose to use free tools like Yum, MREPO, Red Hat Spacewalk (only supports Fedora and CentOS), etc. to manage Linux workstations. However, one solution providing multi-platform support, like Lumension, has benefits in technical support, assets assessment, and reporting capability. By utilizing Lumension VMS, additional hardware and software costs for OS specific tools may be avoided and significant TCO benefit be realized by the organization in managing their heterogeneous network.



test, and the Management of Non-Active Directory machines test.

Deploying Microsoft and non-Microsoft patches follows the same procedure in Lumension VMS. After approving the deployment of a package, administrators are able to monitor the whole progress for each workstation, whether the station is on or off the domain.

WSUS supports Microsoft application patching similar to Lumension VMS. The main difference is that WSUS's procedure is more complex through Group Policy. For non-domain clients, administrators have to change the local Group Policy manually. Also, administrators need to take further steps to confirm the patch deployment success on non-domain clients.

For non-Microsoft application, the patch deployment method using Group Policy has limitations including a lack of scheduling, centralized reporting, inventory, checkpoint restart, and bandwidth throttling. Administrators cannot monitor the patching progress and confirm the deployment. Further steps are required.

Document and Update Configuration Standards

The IT administration time estimate for this step is based on the up-to-date Asset Assessment and Network Visibility test and the Built-in Reporting Capabilities test.

As described in the test results section, Lumension VMS's reporting capability provided administrators with rich reporting tools without need for additional development work.

TCO Analysis

Annual IT labor cost estimate in figure 3 was calculated from the IT administration time analysis shown in figure 2.

The price for the Lumension VMS was provided by Lumension. The TCO for the Lumension VMS include the annual IT administration cost shown in figure 3 and the 1-, 3- and 5-year subscription prices for Lumension VMS products (one Lumension Patch and Remediate Server, 500 Lumension Patch and Remediate Agents, 500 Lumension Content Wizards, 500 Lumension Scan, one Lumension Enterprise Reporting Server, and 500 Enterprise Reporting Client Licenses).

As the Microsoft WSUS and MBSA are both free products, only the cost of IT administration time was counted towards the calculation of the TCO for WSUS.

Cost of hardware and other software components is similar for both products and has not been included in the TCO model.

Labor costs were drawn from the "system administrator compensation"

Salary.com website in August 2009.

Test Bed Setup

Two HP ProLiant ML310 G5 servers were used. Windows Server® 2003 R2 operating systems were installed on both of them. Active Directory server, DNS server, DHCP server, IIS server roles were enable on the first server. Also, SQL Server 2005 SP3 with reporting service, WSUS 3.0 SP1 and Microsoft MSBA server were installed.

On the second server, Tolly engineers installed the VMware workstation 6.5 to support two virtual machines. Both virtual machines are with Windows Server 2003 R2 as well. The Lumension Patch and Remediation server, Lumension Content Wizard, and Lumension Scan were installed on the first virtual machine. The Lumension Enterprise Reporting server was installed on the second virtual machine.

Eight PCs were divided into two groups. Each group had one PC with Windows® XP SP2, one PC with Windows XP SP3, one PC with Windows Vista® SP1 and one PC with Windows Vista SP2. All PCs and the Domain Controller server were in one domain. Tolly engineers also used another two PCs with Windows XP SP3 and Windows Vista SP2 as new/unauthorized/non-domain workstations. (See figure 4 on the next page.)

The applications pre-installed on all workstations were: Adobe Reader 8.1.2,



Java Runtime Environment (JRE) 1.5, iTunes 8.0.1, Microsoft Office 2003 SP3, WinZip 11.1, Logitech Driver KhallInstallWrapper 4.00.121, Firefox 1.0.6.

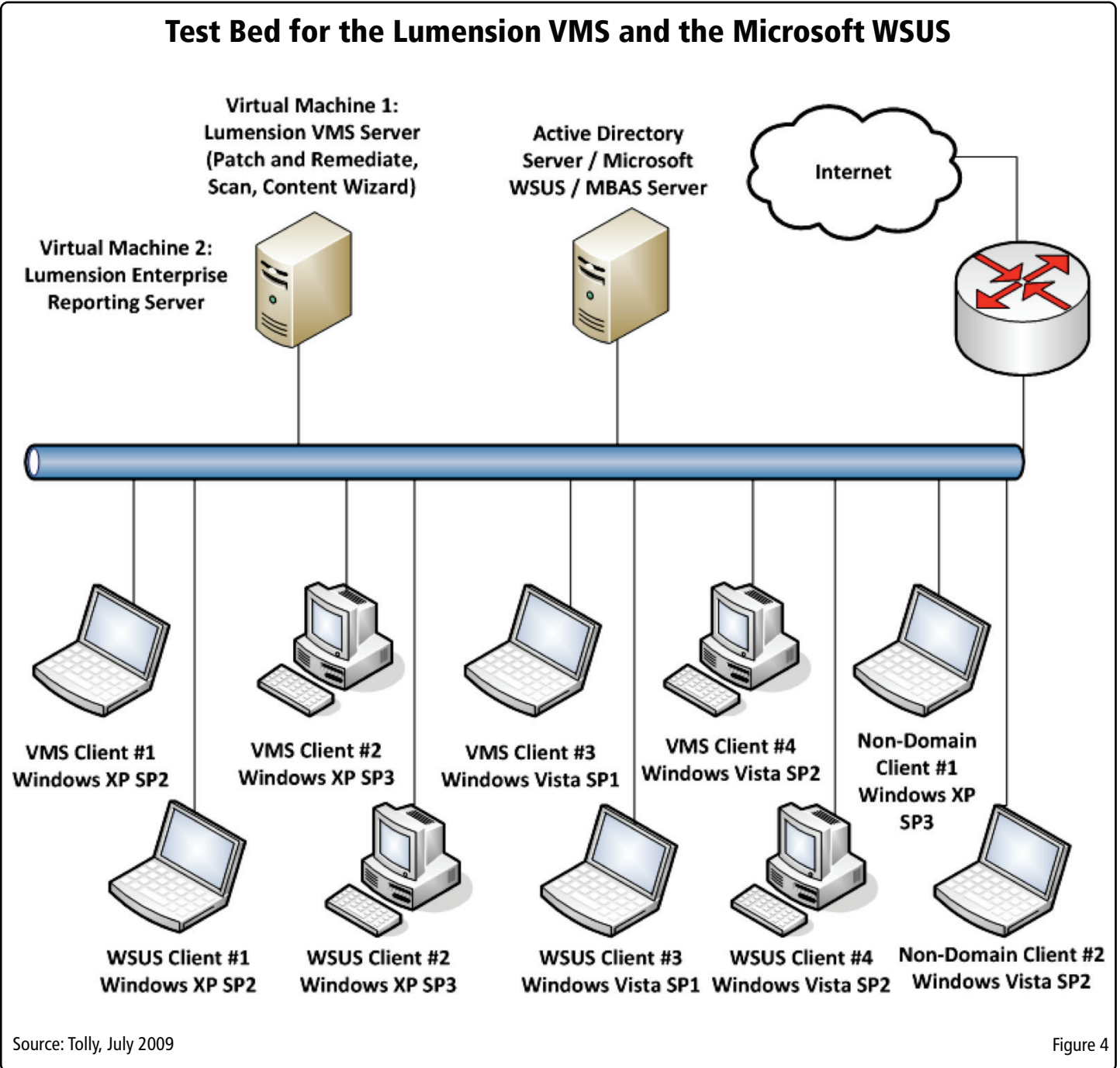
Lumension Patch and Remediate server version 6.4.0.1550, Lumension Scan

version (PatchLink Security Management Console) version 6.4.7.73 with Vulnerability

Update version 184 and CVE version 20040901, Lumension Content Wizard version 6.4.220.100 Premium Edition, Lumension Enterprise Reporting Services

version 6.4.3191.15157, Microsoft Windows Server Update Services 3.0 SP1 version 3.1.6001.65, Microsoft Baseline Security Analyzer Version 2.1 (2.1.2104.0) were used for testing.

Test Bed for the Lumension VMS and the Microsoft WSUS



Source: Tolly, July 2009

Figure 4



About Lumension®

Lumension®, a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and IT Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Utah, Florida, Luxembourg, the United Kingdom, Ireland, Spain, Australia, and Singapore.

Lumension: IT Secured. Success Optimized.™

More information can be found at www.lumension.com

About Tolly...

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services. You can reach the company via E-mail at sales@tolly.com, or via telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
<http://www.tolly.com>

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.