Patch Management Solutions Test

A test commissioned by Kaspersky Lab and performed by AV-TEST GmbH

Date of the initial report: 5th June 2013. Last update: 11th November 2013

Executive Summary

From May to July 2013, AV-TEST performed a review of four patch management solutions for enterprise environments. Kaspersky commissioned AV-TEST to run an independent test of these products. The initial testing methodology was provided by Kaspersky and it was reviewed and adopted by AV-TEST to determine the usability and quality of the tested solutions.

The test results clearly show that Kaspersky is outperforming all competitors regarding patching quality and features. VMware achieved the second-best score and was chosen by the testers to have the most intuitive user interface. Lumension was placed third and close behind Symantec was ranked fourth.

Overview

Today software vulnerabilities belong to the main gateways for malware infections and cyber threats. While cyber criminals often use unknown zero-day exploits to infect their victims, they can also revert to a large set of well-known and proven exploits, because of outdated software used within enterprise networks. Such exploits are sold in so-called exploit-packs in the underground. It is a special system for malefactors, which is especially designed to penetrate a user's system. When a user comes to a website with an exploit-pack installed, his system will be attacked by several exploits. It is significant that these exploits are intellectually chosen by the exploit-pack. Updated software greatly augments resistance to all exploits (apparently, excluding 0-day).

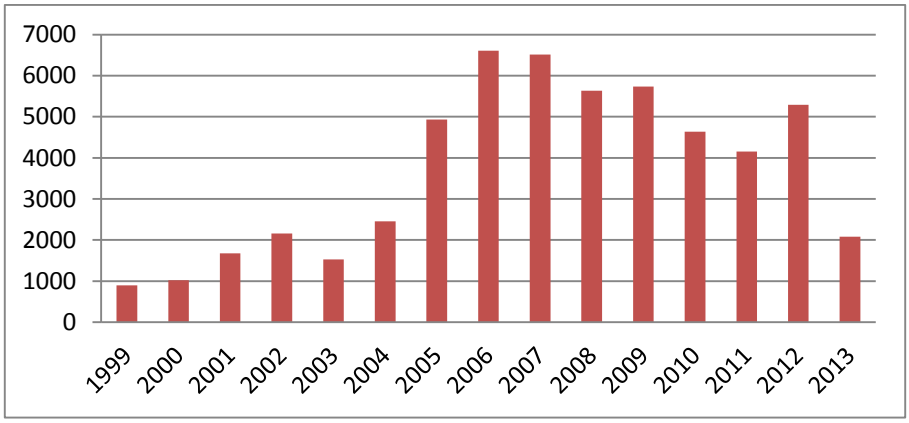

Figure 1: Number of Software Vulnerabilities according to the National Vulnerability Database[1]

[1] http://web.nvd.nist.gov/view/vuln/statistics

While Microsoft provides a central source for updates of all of its applications and operating systems, most 3rd party applications have to supply their own update mechanisms. This may lead to performance issues as well as security holes due to decentralized management.

Patch management solutions were introduced to help system administrators to monitor and centrally manage the deployment of updates for all kinds of software within the enterprise network.

A patch management solution consists of network agents on the client machines, which report the installed applications to the central management console. From the management console the system administrator sees all outdated systems and can schedule the installation of updates.

Products Tested

The following products were tested:

Vendor	Product	Version
Kaspersky	Security Center	10.1.94
Lumension	Endpoint Management and Security Suite	7.3.0.10
Symantec	Altiris Patch Management Solution	7.1 SP2 MP1
VMware	vCenter Protect	8.0.4027.2

Summary

The goal of testing was to measure the potential effectiveness of patch management solutions in closing vulnerabilities to malware and their ease of use.

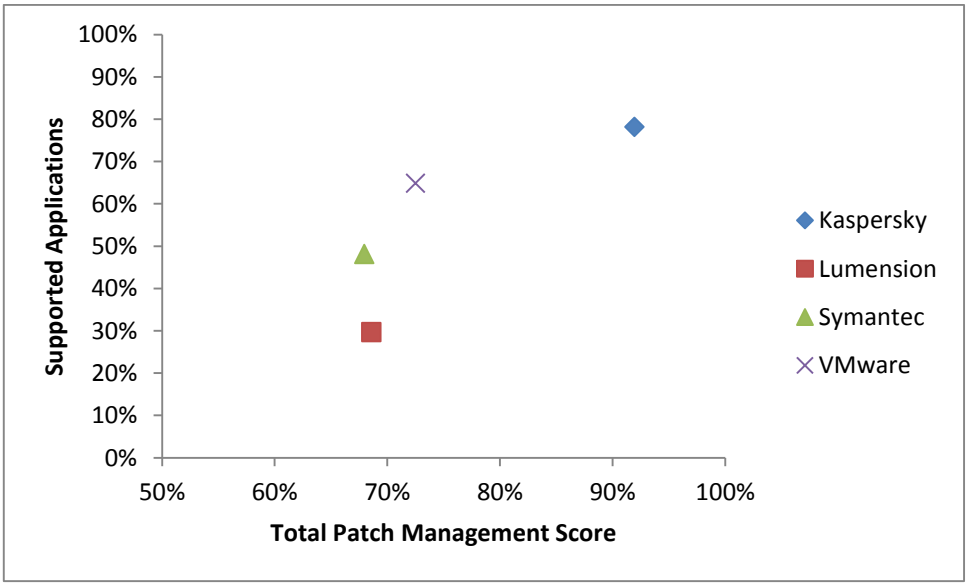

Figure 2: Kasperksy achieved the best total score and supports the most applications

The results of the test indicate that Kaspersky has done a good job with the integration of its patch management solution in Kaspersky Security Center. It supports the most applications and provides the best patching quality in the field. VMware has a good second place and could convince the testers with its intuitive user interface. Lumension lacks in the support of applications, but its

patching quality was good. The score was reduced due to the slow reaction rate to new patches. Symantec has achieved a tight fourth place. Due to its support of Mac OS X and Linux it should still be considered in heterogeneous environments.

Notes to tested products

Kaspersky

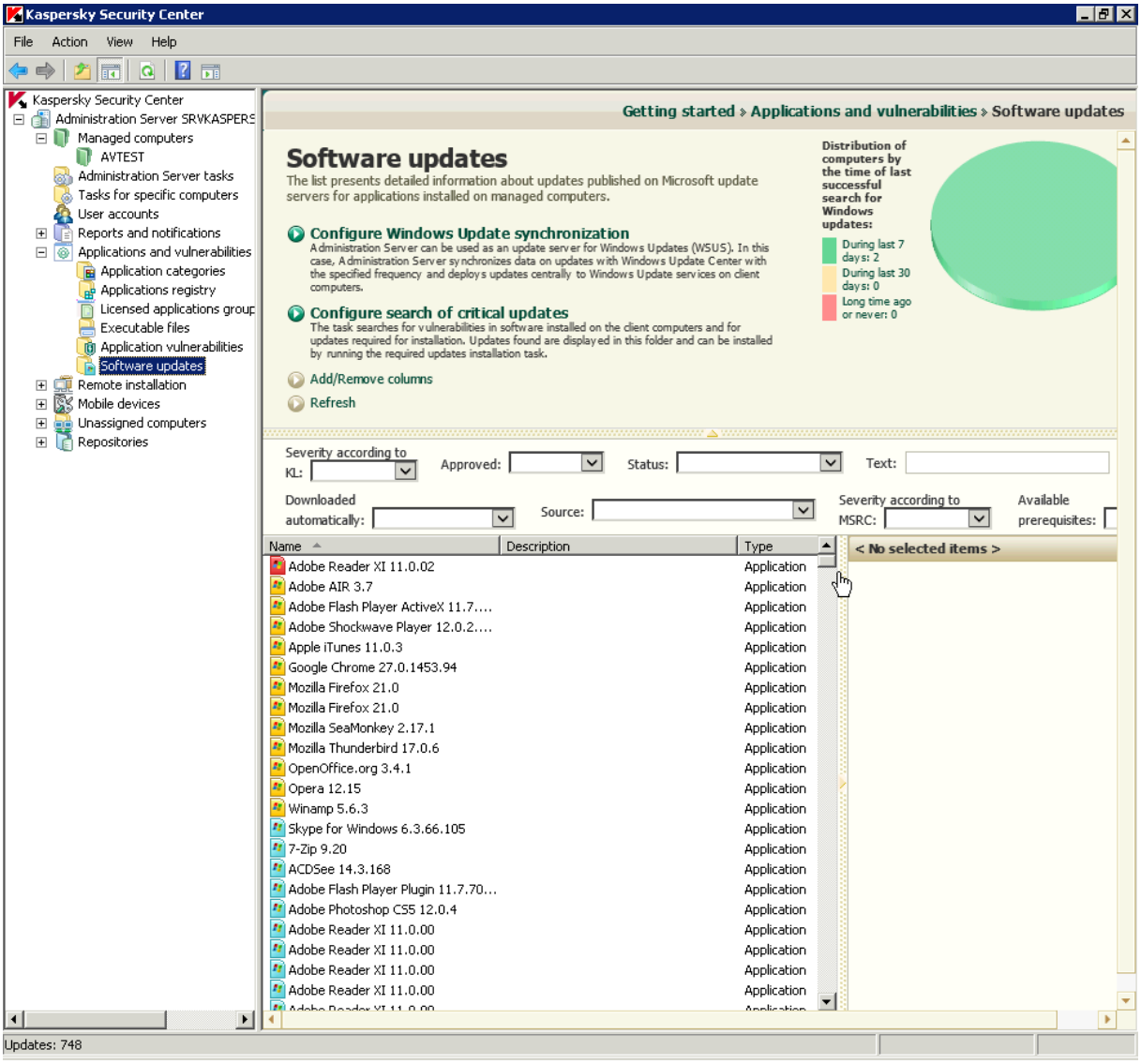

Figure 3: The "Software Updates" module in Kaspersky Security Center shows all available patches

Kaspersky's patch management solution is an additional module for its Security Center. It's an ideal extension for existing Kaspersky installations.

The good integration in Kaspersky Security Center is the main advantage of Kaspersky, especially when enterprises already use Kaspersky Security Center. The usability is similar to other modules like endpoint security. Every task has to be defined first, so the administrator has to create at least a "Find vulnerabilities and critical updates" and a "Install critical updates and fix vulnerabilities" task.

The creation wizards help a lot, but it needs some practice. A scan result of missing patches is not intentionally shown to the administrator, but it is visible when he navigates to “Software Updates”.

Lumension

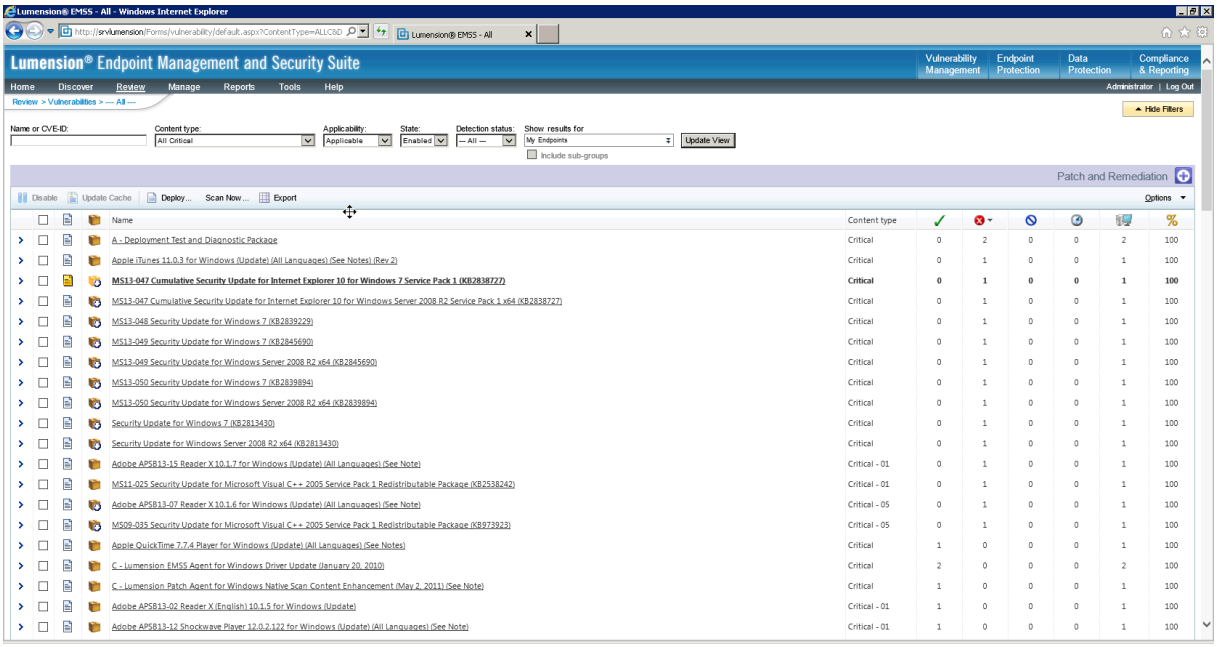

Figure 4: Lumension provides a web-interface

The solution offered by Lumension supports the fewest applications. Therefore it’s not suitable for large enterprises with many different software environments. It has a clear web-based management interface with a customizable dashboard.

The administrator always has a good overview of ongoing tasks and vulnerable machines.

In the deployment wizard a “404 – Server Error” appeared in an IFRAME on the EULA page. But it had no impact on the usability.

The average reaction rate to new patches was more than twice longer than for all other products, which should be considered in critical infrastructures.

Symantec

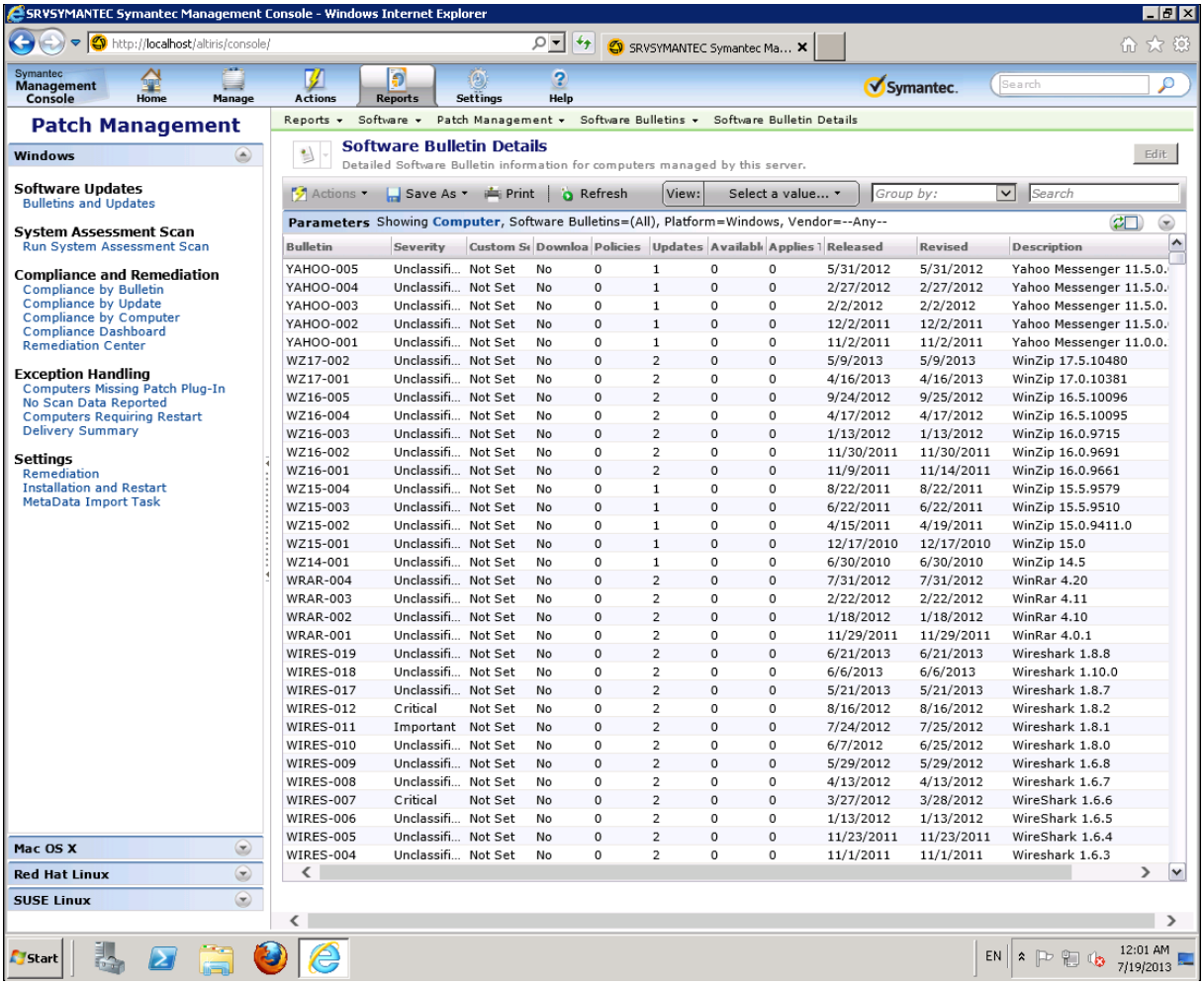

Figure 5: Symantec's web-interface doesn't clearly show the deployment progress of agents and patches

Symantec was placed fourth with less than 1% difference to Lumension.

Beside Windows systems Symantec also provides patch management for Mac OS X, Red Hat and SUSE Linux. The platform has many features targeted on large enterprises, but it makes the patch management more complex than the other solutions. It requires an experienced administrator.

The deployment progress of agents and patches was not clearly visible from the management console.

VMware

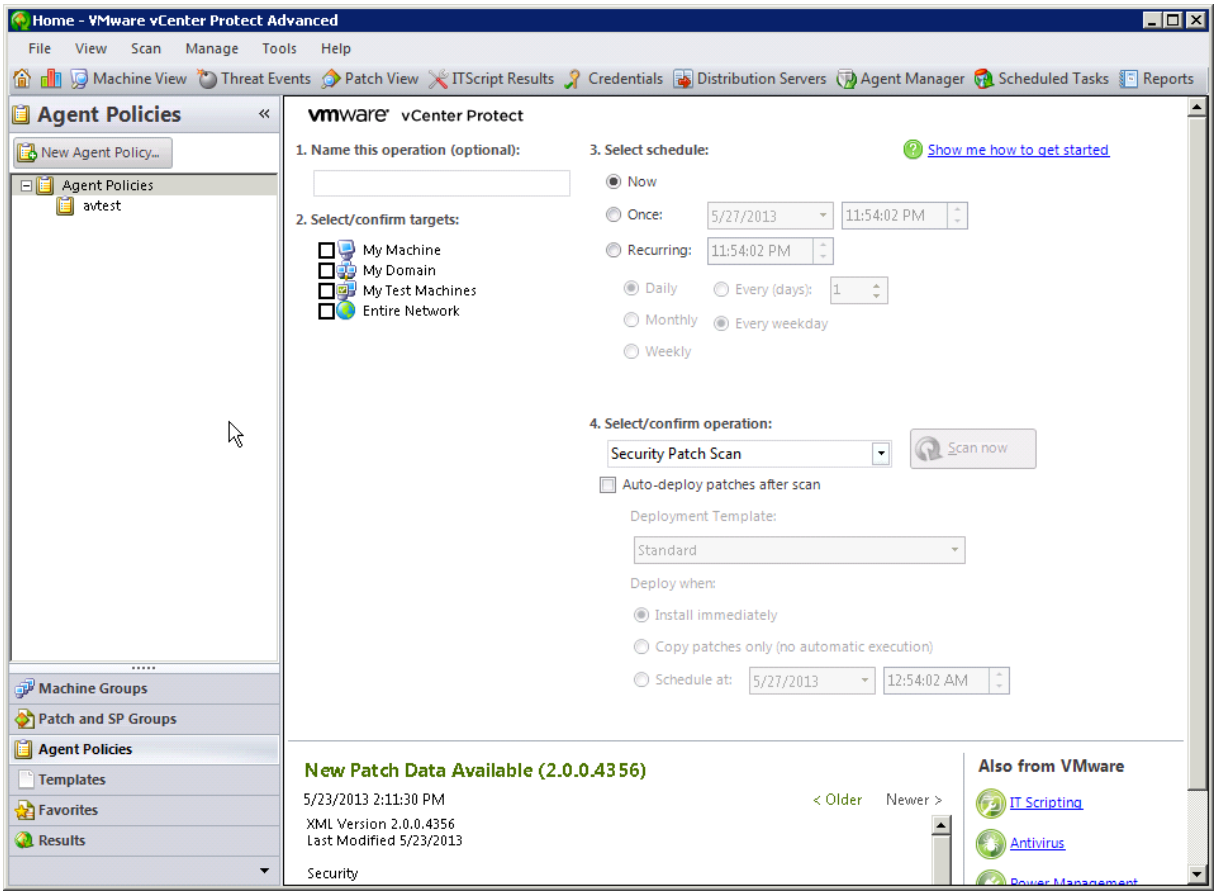

Figure 6: From VMware's start page the administrator can easily run a new Security Patch Scan

When the vCenter Protect management console is set up properly, it's easy to use. The administrator chooses a group of computers to scan for patches. He can monitor the scan process and receives a list of installed and missing patches on the scanned systems. Then he can deploy all or only selected patches to the machines. These tasks can also be scheduled to run automatically.

While the handling was rather easy, the testers also noticed some problems. VMware was unable to patch LibreOffice due to an out-dated download URL. The administrator couldn't specify an alternative source; he has to create a user-defined patch. The solution also couldn't handle installation blocking barriers on the client machine. E.g. if a process needs to be closed to install a patch, the user wasn't prompted to close the process. As workaround the administrator can schedule a pre-deploy reboot.

Test Results

Number of Supported Applications

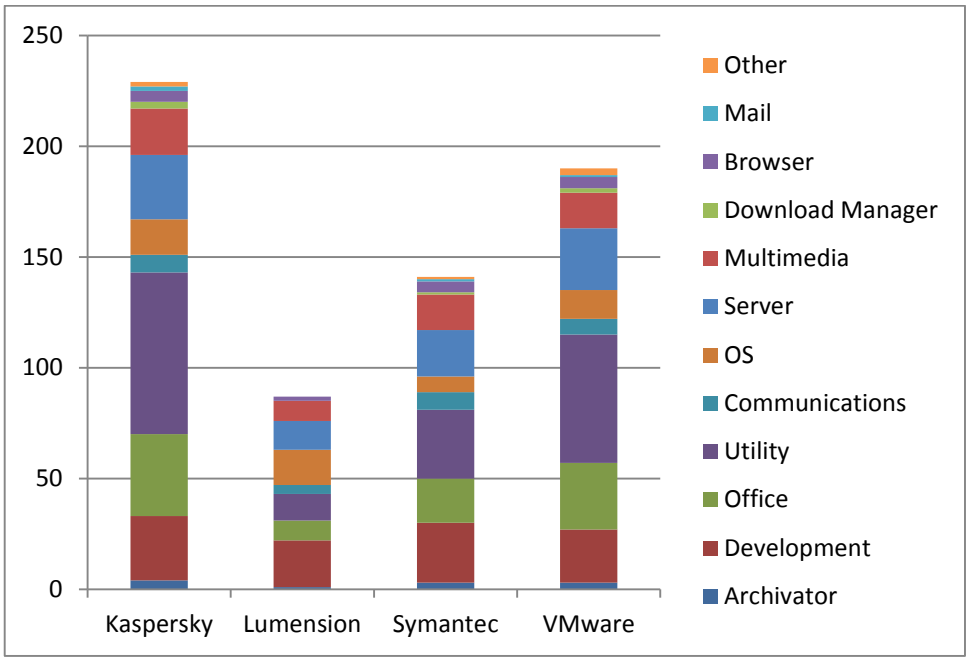

Figure 7: The chart shows the number of supported applications by category

Depending on the business and environment the number of supported applications is more or less important. An administrative department has other requirements than development and engineering.

Kaspersky has the most comprehensive application support, supporting applications of all kinds. Lumension supports the fewest applications and lacks in support of download managers, mail and other applications.

Detection Quality

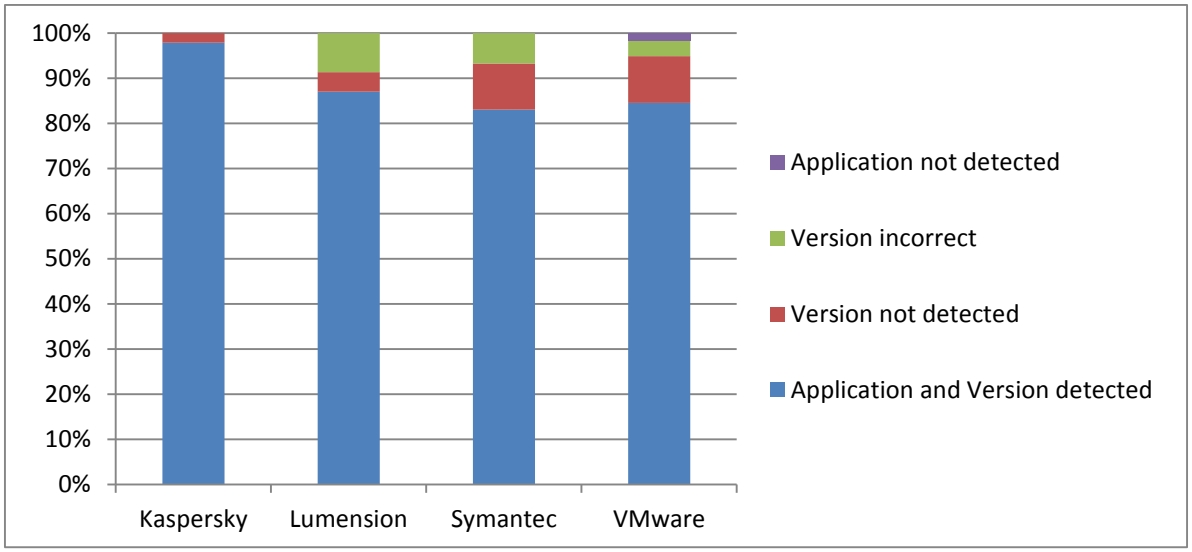

Figure 8: The chart shows the detection quality

The goal of the detection quality test was to determine the quality of the scan results, which are displayed on the central management console. Kaspersky showed the best detection quality, most supported applications are detected very well on the client machines. VMware had some trouble detecting supported applications. Lumension and Symantec could detect all of its supported applications, but for some of them they were unable to determine the correct installed version.

New Patches Reaction Rate

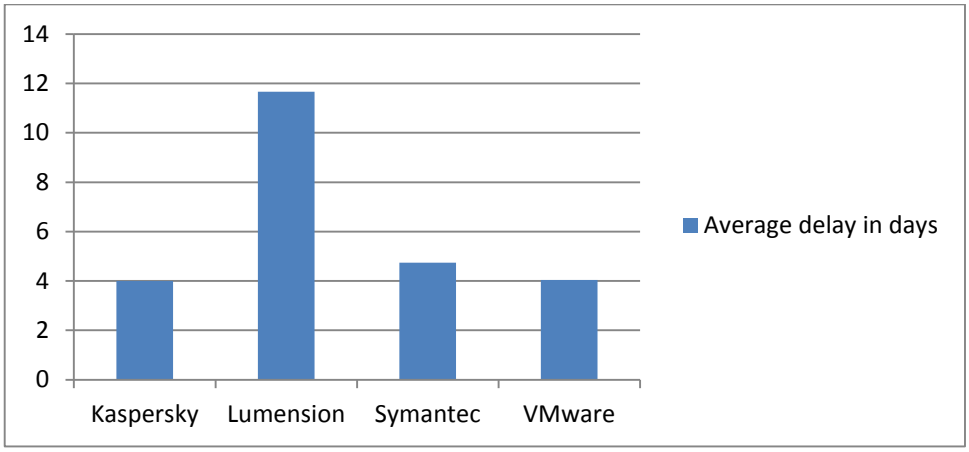

Figure 9: The chart shows the average delay for new patches

When the vulnerability information is published, it's only a matter of time before it's used in attacks. Therefore the reaction rate for new security patches is very important. The testers checked daily, whether new patches were available for the patch management solution.

Kaspersky and VMware had the best reaction rate with an average delay of 4 days. Symantec is close behind with 5 days. The reaction rate of Lumension wasn't satisfying.

Language Support

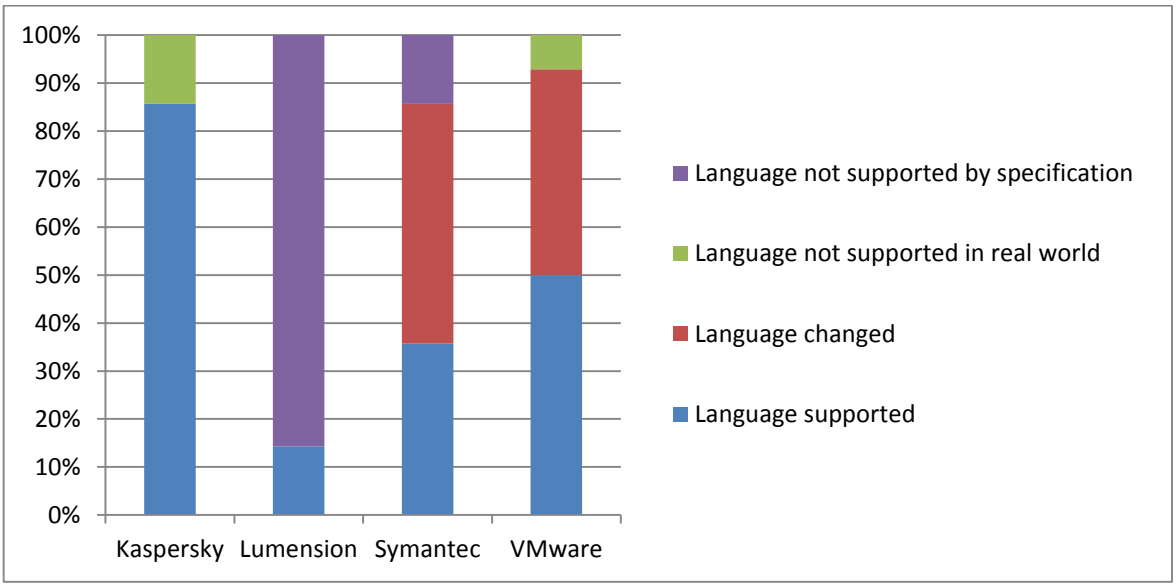

Figure 10: The chart shows the language support capabilities

In large corporate environments the employees may use applications in different languages according to their preferences. Kaspersky has shown the best support of patching applications with

different languages. Symantec and VMware sometimes changed the originally installed language of an application. Lumension supports only a few languages.

Installation Quality

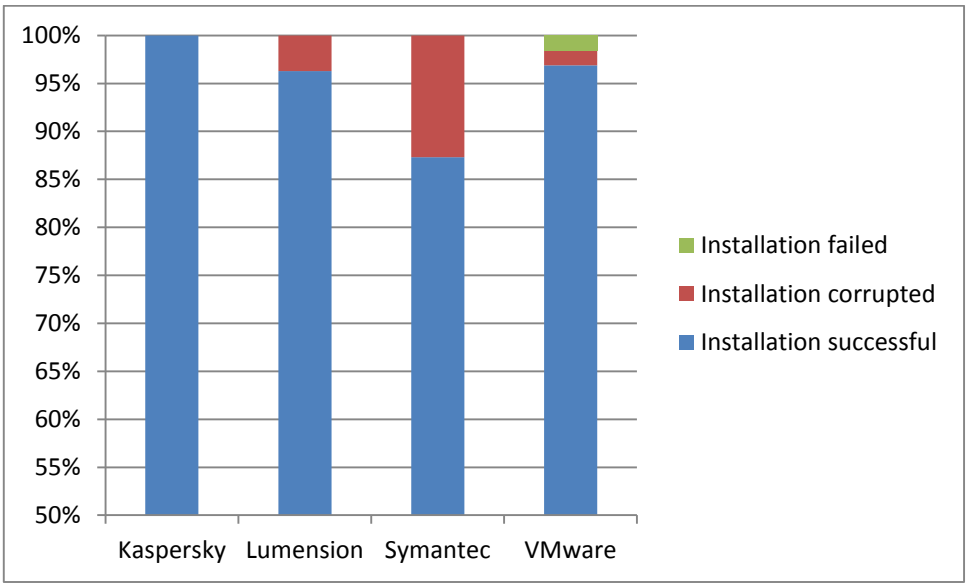

Figure 11: The chart shows the patch installation quality

The installation quality is very important for a patch management solution. A bad installation quality may lead to nonproductive time, because the installations have to be fixed manually before the employees can continue using their applications. Kaspersky was able to patch all applications without effort. Lumension and VMware achieved a good result, but failed in a few cases. Symantec had some problems with the installation of patches. It could only patch about 86% without any problems.

Installation Barriers

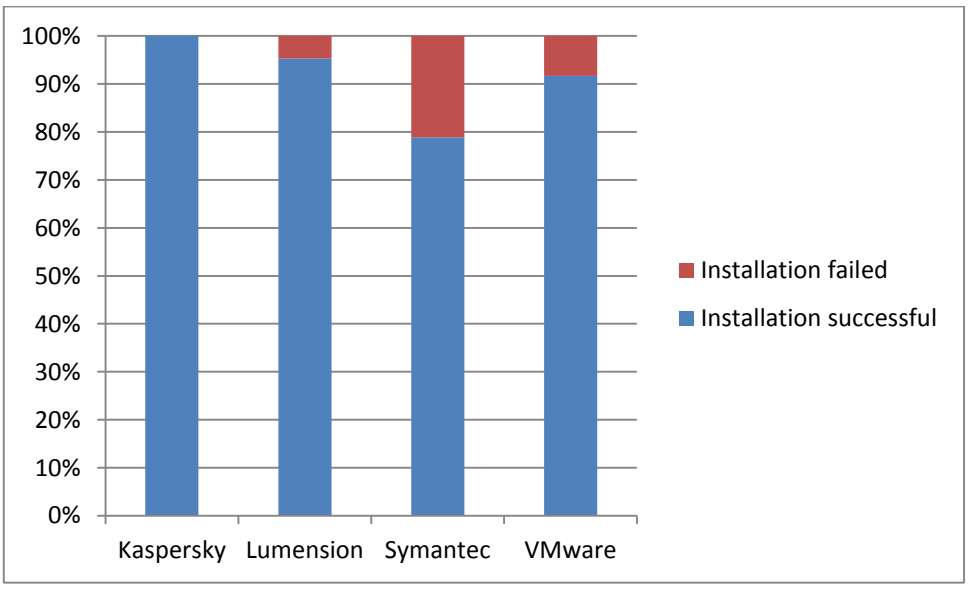

Figure 12: How good could the solution handle installation barriers?

If critical updates are deployed during working time, it's likely that the user does something, which could impede the update process. The test covered the following four barriers: the unpatched

application was running, a browser was opened, the internet connection was unavailable and another setup was running.

Kaspersky could handle all these barriers very well and had no problems. Lumension and VMware are on a similar level, most problems were seen when the unpatched application was running. Symantec had the most problems.

To prevent such barriers all solutions provide the option to schedule a reboot before the update process starts. After a reboot no application is running, except for autostart applications.

Add-on Handling

The patch management solutions usually use the default setup applications to install updated program versions. Such setup applications often include add-ons such as toolbars and performance optimization tools or they modify user specific settings like the browsers start page.

Such add-ons shouldn't be installed during the patching process without knowledge of the administrator as they might implicate a security risk.

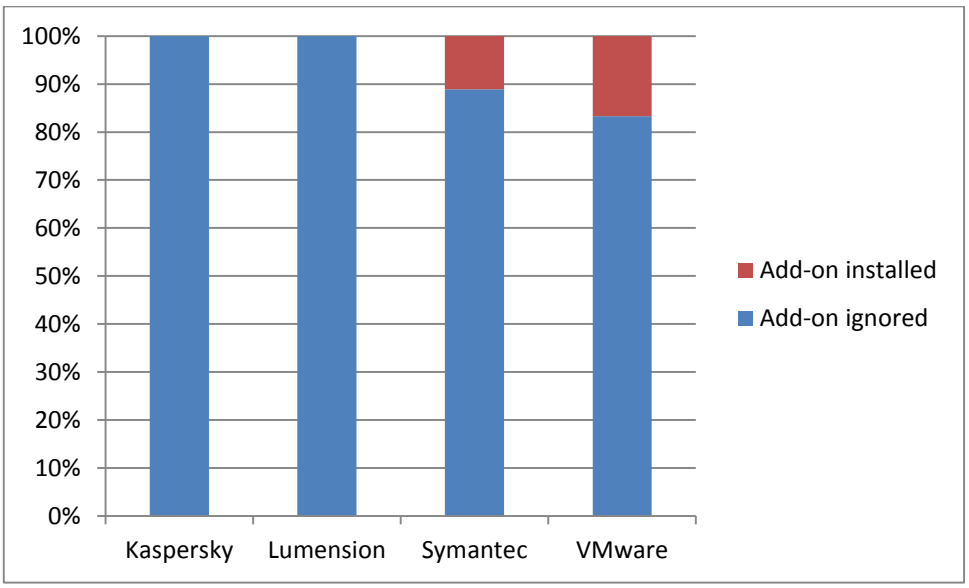

Figure 13: The chart shows how the solutions handled included add-ons

Kaspersky and Lumension ignored all included add-ons and did not allow changing specific settings. Symantec and VMware sometimes installed a browser extension with the application updates.

Auto-Update Configuration

Because of the centrally managed update processes, there is no need for automatically updating applications anymore. Therefore it would be very helpful, if the patch management solution can disable auto-updaters for specific applications.

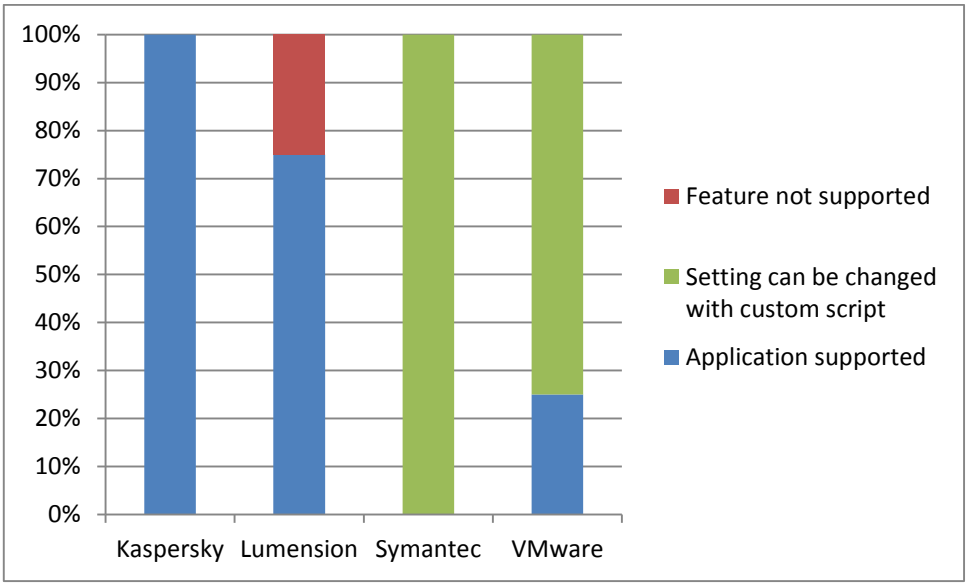

Figure 14: How many applications are supported to disable auto-updates?

Kaspersky has the most comprehensive out-of-the-box support to disable auto-updates. Lumension is on the second place when it comes to out-of-the-box support, but Symantec and VMware can be extended with scripts to perform custom configurations on the clients.

Microsoft Update Support

The Windows Server Update Services (WSUS) provide Microsoft related patches and software updates for the corporate network. A central patch management solution can either control or replace the WSUS, but it must not interfere with the WSUS.

Product	Microsoft Update Support
Kaspersky	Controls WSUS
Lumension	Patches Microsoft applications without WSUS
Symantec	Patches Microsoft applications without WSUS
VMware	Patches Microsoft applications without WSUS

Kaspersky has the only solution which can control the Windows Server Update Services. The other solutions could interfere with the WSUS. Therefore they require special attention of the administrator. As the impact on a running WSUS was not tested, all solutions received the full score.

Reboot Control

To ensure a clean installation of all patches the administrator needs the option to schedule reboots before and after the patching process.

Reboot Feature	Kaspersky	Lumension	Symantec	VMware
Warn User	+	+	+	+
Schedule Reboot	+	+	+	+
Postpone	+	+	+	+
Reboot after full Update Cycle	+	+	+	+

All products have extensive options to handle reboots during the installation of updates.

Accepting EULAs

In corporate environments it is very important to comply with the EULAs of the used applications. As the central point for patch deployment, the patch management solution should be able to display the EULAs to the administrator, so that he can accept or deny them.

Product	Accepting EULAs
Kaspersky	EULA is shown to administrator
Lumension	EULA is shown to administrator
Symantec	Feature not supported
VMware	Feature not supported

Kaspersky and Lumension let the administrator accept or deny each EULA. Symantec and VMware can neither display the EULAs nor accept or deny them.

Testing Methodology

Basic Concept

For each patch management solution a VMware ESXi host was set up to host a server VM and a client VM. The central management console of the solution was installed on the server and the patch management agent was deployed to the client. On the client the vulnerable applications were installed. From the management console the testers scanned for these on the client and then they tried to deploy the appropriate patches.

Detection Quality Test (100 points)

Result	Weight
a supported application was not detected during the scan	0%
the detected application version was incorrect	50%
the application was detected, but the version couldn't be determined	50%
the application and version were detected correctly	100%

New Patches Reaction Rate Test (100 points)

Result	Weight
Delay was between 0 and 3 days	100%
Delay was between 4 and 6 days	75%
Delay was between 7 and 9 days	-100%
Delay was between 10 and 13 days	-175%
Delay was more than 14 days	-200%

Language Support Test (50 points)

Result	Weight
The language was supported	100%
The language was not supported in real world	100%
The language was changed during patching process	50%

Installation Quality Test (50 points)

Result	Weight
The installation went fine	100%
The installation was aborted	0%
The application didn't work after patching	0%

Installation Barriers Test (50 points)

Installation Barrier	Weight
The application to patch was running	100%
A Browser was running	100%
The internet connection was unavailable on the client	100%
Another installation was running	100%

Add-on Handling Test (50 points)

Result	Weight
The add-on was ignored	100%
The add-on was proposed	50%
The add-on was installed	0%

Auto-Update Configuration Test (50 points)

Result	Weight
Auto-updater can be disabled	100%
Auto-updater can't be disabled	0%
Auto-update settings can be changed with custom scripts	50%

Microsoft Update Support Test (50 points)

Result	Weight
PM solution controls WSUS	100%
PM solution patches Microsoft applications without WSUS	100%

Reboot Control Test (50 points)

Result	Weight
The user receives a warning before a reboot	100%
The reboot can be scheduled	100%
The reboot can be postponed	100%
The reboot is performed after a full update cycle	100%

Accepting EULAs Test (50 points)

Result	Weight
The EULA is shown to the administrator	100%
Feature is not supported	0%

Appendix

a. List of vulnerable applications

Application	Version
7-Zip	4.20
7-Zip	9.12
Adobe AIR	2.6.0.19140
Adobe AIR	3.3
Adobe Flash Player	10.3.181.23
Adobe Flash Player	11.1.102.63
Adobe Reader	10.0.0
Adobe Reader	10.0.1

Adobe Reader	10.1.0
Adobe Reader	9.0.0
Adobe Shockwave Player	11.6.0.626
Adobe Shockwave Player	11.6.5.635
Adobe Shockwave Player	11.6.7.637
Adobe Shockwave Player	11.6.8.638
AOL Inc AIM 7	7.582
Apache TomCat	7.0.14
Apple iTunes	10.2.2.12
Apple iTunes	10.7.0.21
Apple iTunes	4.6
Apple QuickTime	7.4.0.91
Apple QuickTime	7.70.80.34
Apple Safari	5.34.50.0
Audacity	1.3.14
FileZilla	3.0.0
FileZilla	3.1.6
FileZilla	3.5.1
Foxit Reader	5.01.0523
Gimp	2.8.0
Google Chrome	14.0.835.124
Google Chrome	22.0.1229.94
Google Chrome	23.0.1271.95
Google Desktop	4
Google Earth	6.1.0.4857
Google Picasa	3.8.117.43
Google Talk	1.0.92
ICQ	6.5.102
ImgBurn	2.5.6.0
LibreOffice	3.4.3
Microsoft Office	2010
Microsoft Project	2010
Microsoft Silverlight	3
Microsoft Visio	2010
Microsoft Visual C++ 2005 Redistributable	8.0.61001
Mozilla FireFox	15.0
Mozilla Firefox	16.0.1
Mozilla Firefox	5.0
Mozilla Firefox	9.0
Mozilla Seamonkey	2.10
Mozilla Seamonkey	2.13.2
Mozilla Seamonkey	2.5
Mozilla Thunderbird	10.0.1
Mozilla Thunderbird	12.00
Mozilla Thunderbird	16.0.1
MSN Messenger	14.0.8117.416
MSN Messenger	6.0.0602

Notepad ++	6.0
Nullsoft WinAmp	5.0
Nullsoft WinAmp	5.56
Nullsoft WinAmp	5.62
OpenOffice	3.1
Opera	12.00
Opera	12.02
Opera	5.0
Opera	6.0
Opera	11.11.2109
Oracle Java Runtime Environment	6.0.250
Oracle OpenOffice.org	3.1.9399
Oracle OpenOffice.org	3.4
paint.NET	3.0.7
Pidgin	2.10.0
Rarlab WinRAR	4
Rarlab WinRAR	4.01.1
RealPlayer	15.0.1.13
Skype	3.0.0.198
Skype	5.3.0.113
TortoiseSVN	1.7.9.23248
VLC Media Player	1.1.11
WinRAR	4.11
WinZIP	15.0
WinZip	15.0.9302
Wireshark	1.6.2
Yahoo Messenger	11.50.0152