

Automated Patch Management: Impressive Return on Investment

The Benefits of Automated Patch Management

An automated solution can reduce the annual cost of patching from US\$222 to US\$40 per computer, resulting in an expected savings of more than US\$180,000 per year for an organization with 1000 computers.

It's a simple truth: applying patches is the only definitive way to keep vulnerable systems from being exploited. Accordingly, most organizations acknowledge the need for a formal patch management strategy and solution. They clearly recognize the potential risk in the proliferation of new vulnerabilities and associated threats. The realities of today's IT environment require that organizations not only deploy more patches than ever before, but also that they do so with a greater degree of urgency.

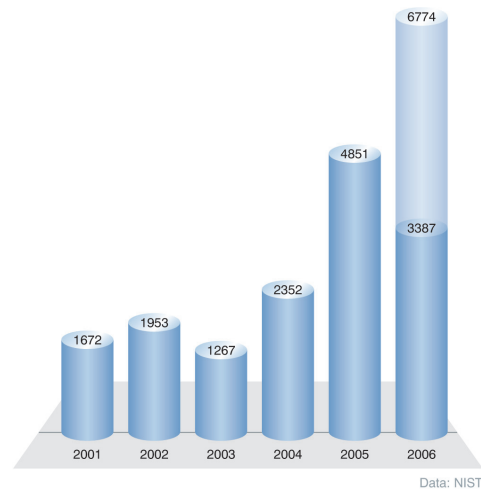
Given these demands, it makes sense to implement an automated patch management solution. However, IT and security personnel inevitably need to justify such an investment. They need solid data that quantifies the cost savings and other benefits of automated

patch management. This paper shows that, relative to a manual approach, an automated solution can reduce the annual cost of patching from US\$222 to US\$40 per computer, resulting in an expected savings of more than US\$180,000 per year for an organization with 1000 computers.

Cost-benefits Analysis

An analysis of the benefits of automated patch management includes many factors, not all of which are straightforward. The assumptions, choices and rationale provided in the following sections are based on the experience of the authors, the expertise of the developers and engineers at Novell, and continuous feedback collected from the extensive Novell® customer base.

Increasing Number of Vulnerabilities
(vulnerabilities per year)



Increasing Speed of Exploitation
(days to exploit)

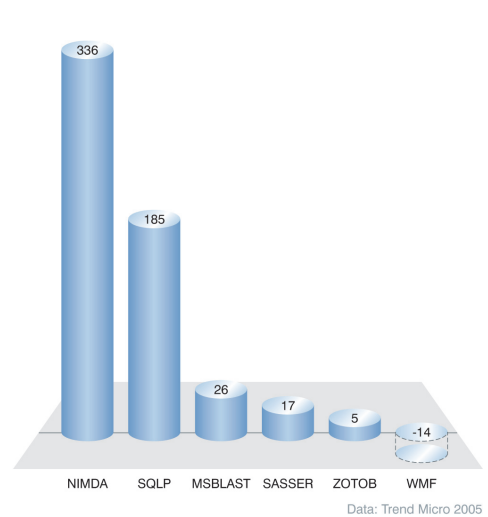


Figure 1. A Perfect Storm for Information Security

Overview of Benefits

Reduced administrator effort is the most significant quantifiable benefit of automated patch management. Organizations see this benefit after automating many steps of an intensive manual patching process. An automated solution offers greater efficiency of operations by taking over many of the labor-intensive functions at each step in the process.

Other benefits are more difficult to quantify, such as the ability to remediate vulnerabilities sooner through frequent cycles of the automated patch management solution. Doing so often saves organizations from successful attacks, but the actual number of such occurrences is irregular and unpredictable. Instead, the real value of such preventive measures is the risk reduction that yields a range of benefits: data and revenue security, protection of brand credibility and decreased risk of legal liability.

The potential magnitude of these benefits is so great that objections to running more frequent patch management cycles (such as concerns about lost productivity) become relatively meaningless. Indeed, even a single successful attack could lead to the loss of millions of dollars, particularly if the incident receives any degree of public attention.

So, even though the benefits of automated patch management are sometimes difficult to measure, decision makers at every level can agree that such a solution saves time and money, increases enterprise security, protects the brand and frees valuable resources to pursue mission-critical business goals. As helpful as large-magnitude qualitative benefits can be, they simply do not have the same persuasive power as hard data, especially if it demonstrates exceptional savings.

Description of Scenario

With this truth in mind, Table 1 provides hard data. It compares manual and automated approaches to the patch management process in a hypothetical enterprise. Although this model is adaptable to virtually any organization, it was built on the following scenario:

- *There are 1,000 end-user computing stations split between two sufficiently different builds (combinations of hardware, operating system and applications), and certain tasks must be performed independently for each group.*
- *There is a moderate level of heterogeneity, with operating systems and applications from multiple vendors requiring a total number of patches approximately twice the annual average of patches encountered by a Microsoft-only shop ($2 \times 160 = 320$). However, risk analysis and shrewd planning result in the need to deploy only three-quarters of this number (240).*
- *The organization prefers to aggregate its patches and deploy them at regularly scheduled monthly intervals. However, they will conduct additional, off-cycle rollouts in critical situations (two per year).*

When needed to supplement real-world data, estimates favored the manual approach. As a result, the actual cost advantage that any given organization derives from automated patch management is likely to be somewhat greater than what the model predicts.

The Findings

The model predicts that, due to a per-computer reduction in patch management costs from US\$222 to US\$40 per year, an automated patch management solution will yield an annual savings of approximately US\$182,000. In other words, without even accounting for any of the additional benefits, automated patch management will provide a return on investment (ROI) of approximately 450 percent, essentially paying for itself in less than three months.

Even though the benefits of automated patch management are sometimes difficult to measure, decision makers at every level can agree that such a solution saves time and money, increases enterprise security, protects the brand and frees valuable resources to pursue mission-critical business goals.

In today's environment of risk proliferation and fast-following threats, automated patch management is an intuitively appealing solution.

Novell ZENworks Patch Management features flexible system inventory capabilities, a streamlined patch deployment wizard, and assessment and validation services that are based on patented Patch Fingerprinting Technology. Not all solutions share these capabilities.

† "The Top 10 Requirements for Enterprise Patch and Vulnerability Management" is accessible at: www.novell.com/patchmanagement

The largest contributions to these projected cost savings come from gains in the deployment step of the patch management process. Most of these gains are due to the ability of client-side agents to minimize distribution/installation errors and to facilitate any required troubleshooting.

While deployment-related tasks are responsible for the greatest degree of savings, they are not the only ones that have an impact. Gains are made in other steps of the patch management process as well. Even these smaller gains reduce annual labor by 940 hours, resulting in savings (US\$47,000) that are more than twice the cost of the patch management solution (US\$20,300). Again, a significant portion of the benefit can be attributed to the client agents. They automate both the pre-deployment task of patch selection as well as the post-deployment task of periodically validating that each patch remains properly installed. In addition to patch management, they can also facilitate inventory management by identifying the software and hardware components residing on all managed systems.

Results Will Vary

The cost analysis model and savings projections of Table 1 are based on a wealth of experimental data. Nonetheless, a number of factors can affect the real-world outcome for any given organization. Some of the more significant factors include:

- *Size of organization*
- *Degree of centralization and decentralization*
- *Level of administrator expertise*
- *Diversity of operating systems*
- *Diversity of application portfolio*
- *Complexity of system configurations*
- *Enterprise policies and procedures*

In addition, the patch management product that is selected can be another potentially significant factor. By no means are they all created equal. For example, Novell ZENworks® Patch Management features flexible system inventory capabilities, a streamlined patch deployment wizard, and assessment and validation services that are based on patented Patch Fingerprinting Technology. Not all solutions share these capabilities. Nor will they all exhibit the advantages attributed to an agent-based architecture. For assistance selecting a high quality automated patch management solution, see the separately published whitepaper, "The Top 10 Requirements for Enterprise Patch and Vulnerability Management."[†]

Table 1: Cost Comparison of Manual and Automated Patch Management

Notes		
Variables and Assumptions		
Number of computers	1,000	
Classes of computers	2	
Applicable patches per year	320	Annual average for Microsoftx2 to account for other applications and systems
Install rate	75 percent	One per month, plus 2 out-of-phase cycles to account for emergencies
Install cycles (rollouts)/year	14	
Hourly rate (US\$)	50	
Workdays/year	250	
Install failure rate, manual	15 percent	Scripts don't work properly, glitches due to custom images and so forth
Install failure rate, automated	1 percent	
Local install rate, manual	15 percent	Pre-emptively decide to patch locally
Local install rate, automated	0 percent	

Task	Task Units (i.e. frequency)	Hours per Task Unit		Annual Labor (Hours)	
		Manual	Automated	Manual	Automated
Patch Management Process					
Research					
Identify available patches	per workday	.5	.17	125	43
Analysis					
Establish scope of applicability	per patch	.5	.17	160	54
Determine whether to install	per patch	.5	.5	160	160
Testing					
Install in test environment	per class/rollout	.5	.17	140	5
Establish impact	per class/rollout	2	2	56	56
Preparation					
Determine distribution plan	per class/rollout	1	1	28	28
Compile patches	per class/rollout	3	0	84	0
Script/configure plan detail	per class/rollout	9	.25	252	7
Deployment					
Local installs in production	per computer/rollout	.5	.5	1,050	0
Troubleshoot failures	per computer/rollout	1	.25	2,100	35
Monitoring					
Reporting	per rollout	8	.17	112	2
Validate installation	per month	15	.17	180	2
		Total		4,447	392

	Manual	Automated	Notes
Summary of Costs			
Patch process	US\$222,350	US\$19,604	
Patch management software	US\$0	US\$18,000	
Patch management hardware	US\$0	US\$800	annual cost = one time cost divided by three years
Patch management training	US\$0	US\$250	annual cost = one time cost divided by three years
Patch management installation	US\$0	US\$400	annual cost = one time cost divided by three years
Annual maintenance	US\$0	US\$480	20 percent of one-time hardware costs
Total annual costs	US\$223,350	US\$39,534	
Total annual cost savings		US\$183,816	

Summary

In today's environment of risk proliferation and fast-following threats, automated patch management is an intuitively appealing solution. The qualitative benefits alone can often be quite compelling, with more accurate and potentially quicker patching leading to an overall reduction in risk and fewer successful attacks. Quantifiable cost savings are substantial; an enterprise patch-management solution featuring a high degree of automation will reduce the annual cost to patch a single computer from US\$222 to US\$40. This represents an annual savings of more than US\$180,000 for an organization with 1,000 workstations.

About the Author

Mark Bouchard, CISSP, is the founder of Missing Link Security Services, LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security topics for nearly 10 years. He is passionate about helping enterprises address their information security challenges. During his career, he has assisted hundreds of organizations worldwide with everything from strategic initiatives (e.g., creating five-year security plans and overarching security architectures) to tactical decisions involving the justification, selection, acquisition, implementation and operation of their security and privacy solutions.

www.novell.com



Contact your local Novell
Solutions Provider, or call
Novell at:

1 888 321 4272 U.S./Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA