



PatchLink Update and Microsoft Systems Management Server 2003

A Complementary Combination for Effective Patch
and Systems Management

Introduction

A relatively common issue facing IT organizations today is the question of whether to invest in both a change and configuration management solution, such as Microsoft Systems Management Server 2003 (SMS), and an enterprise patch and vulnerability management solution, such as PatchLink Update. More specifically, in many cases it is actually about whether to add a product like PatchLink Update to their portfolio when SMS has already been deployed for several years.

Accordingly, this paper will examine the capabilities of each of these solutions relative to the typical challenges facing organizations today in order to demonstrate that it is not really a matter of one versus the other. Indeed, for most organizations both products are appropriate, if not necessary, to achieve an effective patch and systems management solution. In particular, Microsoft SMS provides foundational systems management capabilities, such as software distribution, while PatchLink Update adds advanced patch management capabilities that are essential to keeping up with today's steadily emerging vulnerabilities and rapidly spreading threats.

Enterprise Challenges

It is an undeniable fact that IT and security personnel are under constant pressure to address a wide range of challenges facing their organizations. For example, a handful of the most relevant issues include: accounting for the rapid pace and diversity of business “opportunities” (i.e., needs), maintaining a high degree of efficiency and affordability, achieving compliance with a plethora of regulatory requirements, defending against a mounting array of threats, and accounting for the increasing mobility of users and their computing systems.

The Speed and Diversity of Business

The pace and very nature of business and its associated opportunities imply, if not actually demand, that users be armed in a timely manner with the ever-changing portfolio of resources they need to get their jobs done. Among other things, this means being able to quickly provision them with new applications (or even just upgrades) on an as-needed basis. Often, it will also mean supporting a diverse set of computing devices.

The Economics of Efficiency

Budgets are always constrained. But this does not relieve the need for organizations to steadily move forward technologically – investing in new “solutions” in order to keep pace with change and competition alike. Balancing this equation means saving money where you can, and always spending it wisely. Two good means to these ends include achieving greater efficiency through automation of routine management tasks and proper planning of new application and technology acquisitions based on accurate accounting of currently available resources and their usage.

Compliance is Mandatory

Government and industry enforced requirements, primarily pertaining to information privacy and the security of associated systems, are an unavoidable reality. Fundamental necessities in terms of achieving compliance with them include: being able to identify all of the resources (i.e., applications and systems) in play, understanding how specifically they are being used, and tightly controlling their configurations to ensure they remain consistent with desired policies.

Patching for Protection

Automatic patch management capabilities have become a critical component of an organization’s information security strategy. They are necessary to proactively address the growing number of new vulnerabilities that are being disclosed and the dramatically shrinking window of opportunity to react before corresponding threats appear in the wild. Indeed, recent data obtained from multiple sources indicates that we have reached a point where over 100 new vulnerabilities are being discovered each and every week. Furthermore, for the most common (or significant) of these, exploit code is typically being released within 1 to 3 days of initial disclosure. Under these conditions it is

simply impractical to rely on manual methods to achieve remediation of exploitable systems.¹

Mobility Matters

Improvements in productivity, responsiveness, and quality of life are causing organizations to increasingly embrace mobile and remote computing solutions. A significant result of this trend is that organizations must now also address each of the previous challenges for a growing diversity and population of applications, platforms, and devices that are not LAN-based and essentially not always connected .

Combining Complementary Products to Create an Ideal Solution

Given the scope of the aforementioned challenges it is unrealistic to expect that a single product can be used to achieve an optimal solution. That said, it is certainly true that Microsoft's SMS represents a decent stab at accomplishing just that feat.

Systems Management Server 2003 – A Solid Foundation

Systems Management Server 2003 is Microsoft's flag-ship offering for change and configuration management of Window's based systems. In this regard, its core functional areas include the following:

- Granularly target-able software distribution and installation based on system attributes and covering OS images as well as applications;
- High-performance inventory scans that yield a comprehensive asset management database covering both system hardware and software components;
- On and offline metering of application usage to reconcile software licensing and plan future purchases;
- Mobile system management, including enhanced support of core capabilities for mobile users and extension of coverage to devices running Pocket PC, Windows CE, and XP Embedded; and
- Security patch management, including vulnerability assessment and patch deployment.

The first thing to realize is how well this set of services aligns with the previously provided list of representative challenges confronting organizations today. Each enterprise need is met, at least to some extent, thereby yielding a solid foundation of essential functionality.

The second thing to realize, however, is that SMS was originally designed and intended to address only the first three of these services (i.e., software distribution, inventory, and metering). Consequently, these are the areas where its capabilities are the most mature and, therefore, where it provides the greatest degree of benefit.

In contrast, for patch management SMS 2003 pretty much relies on the same underlying components and technology that are present in Microsoft's Windows Server Update Services (WSUS). The primary implication is that despite having better management functionality than WSUS (e.g., in terms of targeting and deploying patches, more informative reporting), SMS 2003 still exhibits a number of potentially significant shortcomings. Chief among these are relatively limited coverage (i.e., only Windows operating systems and only a subset of Microsoft applications), as well as inconsistent and slow performance when it comes to accurately detecting the presence and proper installation of available patches.

What About WSUS?

Windows Server Update Services, or WSUS, was released mid-2005 as an upgrade/replacement to Microsoft's original Software Update Services (SUS). Comprised of three primary components (i.e., a management server, a web site where updates are published, and a client agent), it provides patch management capabilities for a subset of Microsoft's operating systems (i.e., Windows 2000+) and applications (i.e., Exchange 2000+, SQL Server 2000+, and Office 2003+). However, this narrow scope of coverage, in addition to rather basic controls for targeting, distributing, installing, and monitoring patches, significantly limits its applicability (see Table 1 for additional details). Indeed, Microsoft's own documentation indicates that WSUS is just a "first step", delivering core infrastructure that is intended to support future development of more advanced update management applications. The result is that despite the fact that its software components are free, WSUS is really only a good fit for smaller organizations that operate Microsoft-centric computing environments. For organizations that are larger and/or that have more diverse portfolios of operating systems and applications, WSUS will inevitably be redundant with the more broadly applicable, enterprise-class patch and vulnerability management system that will be needed to supplement its basic capabilities.

Fortunately, it is these and a handful of other potentially important areas where PatchLink Update excels. The result, particularly for organizations with needs in any of these areas, is that PatchLink Update is an ideal complement to SMS 2003 – providing a much-needed extension of its capabilities relative to the efficiency, compliance, and patch management challenges, while helping meet each of the remaining objectives as well.

PatchLink Update – Adding Advanced Patch and Vulnerability Management Capabilities

PatchLink Update is the central product in PatchLink's enterprise patch and vulnerability management solution, which also includes a number of integrated add-on products (identified below). The primary components of PatchLink Update are a hosted repository of thoroughly tested patches, customer-based Update Servers, client agents that account for a vast array of platforms, and intermediate distribution points (i.e., servers) that can be used to achieve highly scalable implementations.

As already alluded to, PatchLink Update is highly complementary to SMS 2003. In particular, it is an appropriate addition for organizations with any of the following needs – all of which represent areas in which it excels:

- The need to support heterogeneous environments;
- The need for comprehensive, independent testing;
- The need for fast and flexible patch deployment;
- The need for efficient, accurate monitoring and enforcement of patch status; and,
- The need for extensibility and integration of related security tools.

“Our situation was that we had 50,000+ workstations and servers. With differences between regions (e.g., some using Group Policy Objects, others using login scripts, and yet others having nothing of the sort), SMS was only able to run on about 60% of the workstations, and almost none of the servers.”

“With PatchLink Update, we are able to test and deploy patches four times faster than with SMS.”

“Getting the system to patch our critical servers in narrow, non-recurring time slots proved to be a challenge with SMS. Doing it with PatchLink was straightforward.”

“PatchLink’s patch detection accuracy is outstanding. Along with the baselining capabilities, it allows us to pretty much let the system run on its own. We only interact with it once or twice a month to process any new patches that become available.”

Heterogeneous Environments.

One aspect of this issue is the need to provide automated patch management services for more than just the operating systems and applications that come from Microsoft. To accomplish this, the PatchLink Agent is available in two different versions. A native Win32 option supports all versions of Windows shipped in the last 10 years, while a Java based option extends support to include most versions of: Mac OS, Novell Netware, HP-UX, IBM-AIX, Sun Solaris, and Red Hat Enterprise Linux. Furthermore, PatchLink Update provides patches for a broad array of both Microsoft applications and the most common third-party applications and utilities in use at enterprises today (e.g., Internet Explorer, MSN Messenger, SharePoint, Citrix ICA, Adobe Acrobat, RealPlayer). Without this degree of in-depth coverage, most large organizations would continuously find themselves still having to fend off attacks against a potentially large set of un-remediated vulnerabilities.

Yet another important aspect of this issue is the need to provide coverage for “out-of-scope” Microsoft hosts. For example, the coverage and/or scope of functions with SMS are often dependent on host membership in a Active Directory domain. In contrast, PatchLink Update provides consistent functionality regardless of the network/directory architecture and type.

Comprehensive Testing

With the volume and speed of vulnerabilities and threats confronting them today, many organizations inevitably struggle with the task of testing new patches prior to deploying them. Fortunately, all patch packages that are distributed to customers are first subjected by PatchLink to a rigorous quality assurance process. This includes testing them in more than 250 different operating system configurations, thereby providing greater assurance of patch quality and potentially reducing the degree of testing that the organization needs to complete on its own.

Fast and Flexible Deployment

The nature of today’s threat landscape also dictates being able to deploy patches rapidly. This is supported in part by the aforementioned testing, as well as by accurate monitoring capabilities (covered in the next section). However, it is also achieved via overall ease of use and flexibility of the management application for PatchLink Update. A wizard to architect multi-patch deployments, extensive host grouping capabilities, support for phased rollouts, the ability to easily specify narrow installation windows, automatic initiation of prerequisite activities (e.g., patch precedence, data backup), and rapid verification of successful installs are just a handful of the features that help to accelerate the overall patch management process.

Accurate Monitoring and Enforcement

In terms of detection capabilities, PatchLink’s patented Patch Fingerprinting Technology provides unmatched accuracy when it comes to establishing the presence and proper installation of patch and update packages. Among other benefits, this directly supports another tremendously helpful feature. Specifically, PatchLink Update is capable of managing to baselines. In other words, the system can be set to routinely monitor managed hosts (i.e., endpoints), checking that they conform to minimum patch levels, and initiating

“The flexibility provided by the PDK is great. It keeps us from having to purchase or separately implement a bunch of other applications and utilities to get additional client security and configuration tasks completed.”

patch installation/re-installation to remediate them as needed. Again, without this type of accuracy and continuous monitoring, especially in terms of identifying partially installed or otherwise corrupted patches, organizations can be left with a false sense of security – believing their systems to be effectively patched when that is not actually the case.

Integration and Extensibility

Add-on products in the PatchLink portfolio greatly extend the capabilities of the core product, enabling its transformation into a broader and more complete patch and vulnerability management solution. For example:

- PatchLink Developers Kit (PDK) enables extensive customization, including custom application deployment and patching and system configuration.
- PatchLink Enterprise Reporting provides advanced reporting and trend analysis to measure and demonstrate network security and compliance across the enterprise.
- PatchLink Scanner Integration Module supports 3rd-party vulnerability scanning tools to supplement native scanning capabilities. Imported results become part of the overall remediation workflow, and can then be addressed by patches from the PatchLink repository, patches that are custom built and distributed via the PatchLink infrastructure, or by other remediation actions (e.g., configuration changes) implemented by taking advantage of the PDK.
- PatchLink Quarantine enables Update’s client assessment, policy evaluation, and remediation capabilities to be coupled with the access control capabilities of available networking and security gateways to achieve a full-featured network admission control (NAC) implementation.

Summary

The reality of the challenges facing organizations today often necessitates that they implement an enterprise solution for software distribution and other related systems management capabilities. However, the nature of the combined threat and vulnerability landscape also dictates that they put in place an automated solution for efficient patch management of the broadest possible set of their applications and systems. Consequently, for most organizations it will be appropriate to invest in both a change and configuration management tool such as SMS 2003, and an enterprise-class patch and vulnerability management product such as PatchLink Update. Indeed, in terms of meeting enterprise requirements, the capabilities of these two products are highly complementary.

For further information, please visit www.patchlink.com, or contact a PatchLink representative at 480.970.1025 opt 2.

Table 1: Summary of Patch and Vulnerability Management Capabilities

Capabilities	Microsoft WSUS	Microsoft SMS	PatchLink Update
Security Patch and Vulnerability Management	Basic	Intermediate	Advanced
Coverage for Microsoft Systems & Applications	Partial	Yes	Yes
Coverage for Heterogeneous Environments	No	No	Yes
Comprehensive Patch Testing	No	No	Yes
Fast and Flexible Patch Deployment	No	No	Yes
Accurate Patch Monitoring & Continuous Enforcement	No	No	Yes
Integration of Vulnerability Scanner Data & Extensibility	No	No	Yes

Footnotes

1. For further justification on the necessity and value of automated update and patch management tools, readers are referred to National Institute of Standards and Technology (NIST) Special Publication 800-40, "Creating a Patch and Vulnerability Management Program", which is accessible at: <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>



PatchLink Corporation
Scottsdale, AZ 85255
480.970.1025

www.patchlink.com