



## **Patch Management 2.0: Evolving Your Patch Management Technology to Proactively Combat Security Challenges**

[www.lumension.com](http://www.lumension.com)



## Overview

The realities of security and compliance have changed considerably since patch management faced its first big paradigm shift some years ago. At that time many organizations wrestled with the transition from manual patching and remediation to an automated process. Of course, nothing in security is ever static, so it is no surprise that patch management has continued to evolve since then. Though still automated, today's best patch management tools and techniques are significantly different from their predecessors. In this whitepaper, Lumension Security's Matt Mosher, Senior Vice President of the Americas, gives an historical perspective on how this evolution unfolded and why it is important for organizations to evolve their patch management technology in order to remain on top of increasing security attacks.

## Changing Patch Landscape

When standalone patch management was first introduced, most organizations were primarily concerned with patching the operating system layer—and the majority of those concerns were directed toward the Microsoft Windows environment. This focus was simply a byproduct of IT security's status at the time. Attackers buffeted machines with assaults that targeted the Windows vulnerabilities that cropped up each day. These bad guys were aware that even those vulnerabilities with readily-available fixes were consistently left un-patched. Organizations couldn't keep up with the volume of vulnerabilities hitting the Windows platform with a manual patching process. It was even tougher for heterogeneous IT environments that were distributed across multiple disparate locations.

Then patch automation came along and helped organizations close the time gap between patch availability and patch deployment. In addition, Microsoft made a commitment to improve the quality of its patches for the Windows operating system. While both of these factors could be considered successes, in some ways the risk was merely shifted elsewhere.

Once the wily hackers found resistance at the operating system, they began looking for lower-hanging fruit. Today, the path of least resistance for malicious intrusion is found by attacking alternate Linux and UNIX operating systems, taking advantage of system mis-configurations and targeting numerous vulnerabilities found at the application layer. Particularly popular among hackers these days are the vulnerability-ridden Web 2.0 applications that many organizations churn out with more regard for functionality and deployment speed than security.

All of these factors pose serious elements of risk that the original standalone patch management or the vendor's native patch solutions just can't handle. The un-evolved patch management tool doesn't help organizations get a handle on application patching, particularly in the case of the dynamic Web 2.0 infrastructure and of legacy systems. Additionally, the basic patch management solution has limited capabilities for automatically updating cross-platform IT environments – especially the Linux and UNIX platforms. Even today, many organizations still patch UNIX machines manually because of these limitations.

These factors can contribute to a lot of strain on businesses coping with increased compliance pressures. Trying to manage disparate methodologies for patching different elements of a heterogeneous environment is not only cumbersome and impractical, but it often doesn't meet the reporting requirements set out by regulatory guidelines. Businesses need simplified processes that can easily be documented and reported for regulatory auditors. The less streamlined the



patching process is, the more inconsistent the reporting will be. Without an easy way for data to be pulled together, it won't be done often enough or consistently enough to avoid issues.

Clearly, today's IT environment is much more dynamic, complex and highly distributed than when patch management first sprang into existence. Add to that the mounting reporting requirements necessary for compliance and it becomes evident that there is a call for a new breed of patch management technology.

### **Evolving the Patch Management Technology**

The key word in the evolution of patch management technology is centralization. At this point, most IT departments have bought into patch management and understand that they need to bring in some level of automation to help them secure their machines. Whereas in the past they were told they just needed to expedite patching machines in the Windows environment, now they need to patch throughout the entire infrastructure; from the OS level to the application layer. Plus, IT personnel need to prove the integrity of those patches and they must report on all of this in a timely fashion. The only way to accomplish this objective is through continuously monitoring patch status with on-demand centralized reporting.

The evolved suite of patch management tools automates the patch management process throughout the entire infrastructure. It provides streamlined patching of applications that range from unsupported legacy applications to unique Web 2.0 programs. It gives organizations the ability to bring together automated remediation of both security patches and operational patches—a key feature for managing UNIX, which does not differentiate between 'types' of patches. It also consolidates activities that once were under the sole domain of vulnerability assessment tools in order to help patch management accomplish its ultimate goal of mitigating vulnerability risks.

Standalone patch management tools once depended on separate vulnerability assessment products to discover, assess and prioritize the criticality of vulnerabilities. Without this validation, organizations using un-evolved patch management tools had to depend on the word of their software vendor that a given patch actually took care of the vulnerabilities it claimed to fix.

Similarly, businesses needed these separate vulnerability scanners to identify the mis-configurations of operating systems and applications that left machines open to attack. This created a difficulty in that standalone patch management tools were not equipped to properly handle configuration vulnerabilities, but vulnerability scanners could only report on the errors. They usually didn't offer any actionable information about these errors or provide any recourse for mitigation.

Patch management tools have now progressed to the point where they can centralize these two tasks into the overall patch management infrastructure. Advanced patch management includes reliable third-party assessment of patch effectiveness and a reliable method of both identifying and remediating mis-configurations. Doing so eliminates the cost of redundant assessment systems such as employing separate patch management and vulnerability assessment solutions, but still provides the redundant assessment base on different source data.

All of this centralization and consolidation is not only critical to streamline IT security and operations practices, it also greatly aids organizations' compliance efforts. Bringing everything



under one patch management umbrella gives an organization the power to report on all of its patching activities in one fell swoop. No longer are there separate reports on Windows patching, UNIX patching, configuration management and application fixes. Everything can be included in one easy-to-produce and easy-to-read report that also verifies the effectiveness based on third-party vulnerability 'fingerprints.'

### **Lumension Security's Proactive Approach to Patch Management**

Lumension Security not only pioneered the first and industry leading patch management product, but continues to drive the patch management evolution. The Lumension Security suite of patch management and vulnerability remediation technologies extend patch automation to every element of the IT infrastructure, instead of focusing just on Microsoft Windows patches. Lumension Security extends its automated discovery, vulnerability assessment, remediation, validation, security configuration management and compliance reporting across today's heterogeneous, highly complex and distributed IT environments.

The Lumension Security solution provides an easier way to automatically patch alternate platforms, even UNIX. Unlike other tools on the market, Lumension Security's patch management solutions expedite collection, analysis and deployment of both operational and security patches within the UNIX environment. They also give organizations the ability to patch a greater range of applications. Lumension Security's PatchLink Developers Kit (PDK) offers businesses a way to rapidly deploy custom content such as updates to legacy applications or Web 2.0 application fixes.

Additionally, Lumension Security's patch management framework offers comprehensive third-party assessment of deployed patches from reliable sources such as Mitre Common Vulnerabilities and Exposures (CVE). It also offers a method for seeking out vulnerable mis-configurations and remediating them once they are found.

All of this is accomplished through a powerful combination of network and agent-based discovery, scanning and remediation. By harnessing the best attributes of both network scans and system agents, Lumension Security is able to ensure constant discovery and remediation of all devices on or off the network.

Most importantly, Lumension Security understands that in today's regulatory environment, sound reporting of remediation is as important as deploying the patches themselves. Because Lumension Security combined all the necessary patch and vulnerability management tools into a single framework, it is able to offer centralized reporting that gives a comprehensive view of the risk environment.



**Lumension Security**

15880 N. Greenway-Hayden Loop, Suite 100

Scottsdale, AZ 85260

[www.lumension.com](http://www.lumension.com)