

Why “Free” Patch Management Tools Could Cost You More

Today’s current economic situation underscores the importance of scrutinizing all business expenses, particularly within IT. Although point patching products may look more attractive on the surface, closer inspection often reveals hidden costs and missing capabilities.

The result: fragmented patch management and weaker security posture while also being a more costly and cumbersome option for organizations to maintain.

Selecting the Right Solution Can Save Your Company Time and Money

Today’s current economic situation underscores the importance of scrutinizing all business expenses, particularly within IT. As organizations look to keep operating expenses down, “free” technology solutions start to look more attractive. However, when choosing a solution for patching your systems and servers, it is important to consider the total cost of ownership (TCO) and the difference in key capabilities between point patching products and comprehensive patch management solutions. Although point patching products may look more attractive on the surface, closer inspection often reveals hidden costs and missing capabilities. These solutions ultimately could end up costing organizations more money in the end to fully protect their IT environments due to lack of scalability, coverage and flexibility. The result: fragmented patch management and weaker security posture while also being a more costly and cumbersome option for organizations to maintain.

Point Patching versus Complete Patch Management

Point patching products solve very specific problems, but a major drawback to free utilities is that they do not support heterogeneous environments with numerous platforms and third party applications. Furthermore, these tools do not consolidate nor centralize the management of mixed systems and applications, patch deployments and mainte-

nance tools nor do they have the ability to discover blind spots that are not being managed. The result is a point product with a fragmented approach to vulnerability management and lack of visibility of the overall patching and risk posture. The unanswered needs for the organization to manage third party applications and OS’s often force the use of multiple disparate tools as well as consume large quantities of staff resources.

“Patching is a huge part of our security strategy. We need to control the patching for our environment, rather than turn on Windows Update for all of our computers, because we have a lot of applications that have dependencies on each other. Before deploying patches, we need to run a test to make sure they won’t affect our core systems. Lumension allows us to do this very effectively.”

Tony Hildesheim, Vice President of IT, WSECU

A better choice is a complete patch management solution which is comprised of more than simply sending patches to Windows devices. Comprehensive patch management and remediation solutions address the entire vulnerability management lifecycle:

- » Automated discovery of all unmanaged and rogue devices on the network
- » Full network scanning to determine vulnerabilities and exposures
- » Rapid patching and remediation of all IT assets from a centralized management

console

- » Ongoing validation and maintenance of correct patch and configuration levels on systems
- » Robust management and reporting

A complete patch management solution provides a single platform and a robust content repository that can address patch management in a holistic manner without the requirement to procure multiple point products or the increase in staffing to author scripts on an ad hoc basis for third party applications. The advantage to these solutions is an overall lower operating cost due to consolidated management as well as a stronger overall security posture and flexibility to proactively address issues with less staffing burden.

“Managing a diverse network environment across 20 different locations is no longer a full-time job for our IT staff as Lumension has been instrumental in mitigating risks and relieving IT security pain. It is a robust solution that delivers high performance, thorough assessment, remediation and continuous monitoring to ensure it works around the clock to secure our network without disrupting our computing environment.”

**Jim Czyzewski – Sr. Info. Systems Specialist,
MidMichigan Medical Center**

The Hidden Costs and Missing Capabilities of Point Patching Products

When it comes to “free” solutions, the traditional consumer adage wisely urges us to: “Remember, if it looks too good to be true, it probably is.”

Microsoft OS and Applications Only

Most free tools provide organizations with the basic capability to patch only Microsoft Operating Systems and Microsoft applications. But that’s all. There is no support for non-Microsoft applications or operating systems. Even the most homogeneous Microsoft environments have a myriad of third party applications running that require regular assessment and patch management to ensure critical vulnerabilities are mitigated and regulatory compliance standards are met. The modern IT environment is simply too diverse and heterogeneous not to include the use of applications such as Acrobat Reader, Apple’s QuickTime or Sun’s Java Runtime Engine, an enabler of OS-independent applications. Additionally, unless an organization implements an application control policy, users may also have introduced personal productivity or entertainment applications, such as Apple’s iTunes, which may further diversify the variety of well-known applications subject to patching. This means organizations are not only faced with patching Windows and non-Windows OS’s and applications, but also custom applications.

Requires Additional Point Products Even for Windows-only Environments

As critical vulnerabilities are inevitably introduced through these non-Microsoft applications, organizations that focus solely on Microsoft patches are left with a gaping unanswered need and will have to reactively invest in additional technology and possibly staff to address this shortfall. The decision to go with the “free” tool in this case results in the ultimate need for multiple point products to solve the patch management challenge, rather than using a consolidated solution that effectively manages the needs of the organization while also reducing operational TCO.

Even Microsoft has noted that more than 9 out of 10 recent software exposures are the result of user productivity software ¹.

A business should consider mitigating risk across a variety of attack vectors. The table below illustrates the breadth of potential exposure across technologies.

Vulnerability Surface	Percentage
Windows OS & Microsoft Applications	38%
Apple & Apple Applications	24%
Other Applications for Windows ²	29%
Network, Network OS & Network Technologies	7%
Unix and Linux Only Platforms & Applications	3%

US CERT Technical Cyber Security Alerts 2006-2008³

To focus only on Microsoft applications leaves a large exposure that can be targeted.

Cannot Consolidate Operations

Though many businesses may be “Windows-only” shops in their choice of Operating System utilization, numerous organizations implement a variety of OS's (such as MAC OS X, Sun Solaris, HP-UX, Red Hat Enterprise and SUSE Linux). Having a well-rounded patch management solution allows organizations to effectively address the OS patching needs across diverse IT environment, simplifies operation burden, and reduces operating expense.

Does Not Satisfy Regulatory Compliance Requirements

This breadth of application and OS support may be particularly important in light of compliance considerations. For example, if a company's financial compliance internal control system utilizes IT/application security, then there are a set of high level criteria that may be assessed by audit under Section 404 of SOX. In an audit checklist for SOX 404 compliance, there may be a requirement that patching extend to every product utilized in the IT control system. If your tool cannot address non-Microsoft applications, then it cannot earn a check mark for the audit list item. Some other method of patching the non-supported applications must be specified to meet compliance requirements.

Poor Discovery of Unmanaged Assets

Since free tools are typically designed to only manage Windows systems, they rely heavily on Active Directory to understand what assets are deployed in the IT environment. Un-managed or rogue de-

1. Microsoft Security Intelligence Report: January through June 2008, Vinny Gullotto, et al.
2. Includes Windows only as well multiple OS Applications
3. Source US-CERT (www.us-cert.gov) Technical Cyber Alerts as of October 31, 2008

vices will not be identified for further inspection. This lack of visibility or intelligence results in dangerous blind spots that can leave poorly managed assets completely vulnerable to attack, undermining even the best attempts to ensure standard adherence to security policies.

Requires Domain Membership

These free tools require that all managed Windows systems be members of the domain. Many IT environments simply cannot guarantee that all of their critical Windows systems are being effectively managed through Active Directory. Assets not being managed through the domain will not be eligible for the free tools. This in effect means that any organization running isolated workgroups will not be able to deploy these tools in their environment.

Poor System Software and Hardware Inventory

Since the free patch tools are focused on Windows patches, they do not capture inventory information about installed non-Windows software and local hardware. This lack of context limits the usefulness of the tools, and an additional solution will be needed to collect this information.

Cannot Manage System Configurations

Patch management is just one part of a comprehensive vulnerability management process. According to Gartner, 65 percent of all network exploits are attributed to system misconfigurations, by far the largest cause of network security problems⁴. Security configuration setting issues can be attributed

to just as many of the known vulnerabilities that need to be managed in order to have secure and running operations. The drawback to a free patch management tool is that it does not provide security best practices or native capabilities to assess and remediate misconfiguration issues.

Overall Higher Labor and Product Costs

The need for multiple point products and the staffing burden required to manage free patch management tools is a concern that even Gartner has weighed in on. According to a recent report by Gartner⁵, some organizations continue to use free patch management tools which are more manually-intensive, but ultimately face significantly higher labor costs for content analysis, testing and deployment.

Complete Patch Management Solution is the Right Solution

Lumension delivers a complete patch management solution that provides broad third party application coverage as well as support for all major Operating Systems. This universal coverage eliminates the hidden costs associated with point patching products by consolidating vulnerability assessment and patch deployment from a centralized management console and empowering organizations to accomplish more with less staffing burden.

Lumension's complete patch management solution provides the foundation for a more successful and cost-effective implementation over free patch man-

4. John Pescatore, Gartner Fellow

5. Gartner: The Patch Management Market: Collision or Coexistence? Ronni Colville, March 2008

agement tools in several ways, including:

- » Comprehensive support for heterogeneous environments, including multiple OS's and broad coverage of common third party applications
- » Consolidation of operations with a single solution
- » Meeting compliance requirements for patch and vulnerability management
- » Automated discovery of all assets in the IT environment, including unmanaged and rogue devices
- » GUI-based authoring tool for custom content needs
- » Assessment of security configurations as well as patches
- » Reducing the TCO of patch management

“Lumension gives us a more security-centric view of the network, allowing us to gain greater insight into the network and a better overall view into the system. We are able to more rapidly adjust to changes in the business, making our IT operation much more proactive and flexible, and therefore more productive.”

Anthony Sica, Executive Director of IT, Shiseido

In addition to providing a more complete solution for patch management, Lumension delivers capabilities for policy compliance. Lumension Security Configuration Management™ provides open standards-based configuration management and moni-

toring and assessment of computing systems to ensure adherence with regulatory requirements or specific company-defined policies. Lumension also enables customers to leverage the National Institute for Security and Technology's (NIST) security content database. Administrators may review these best practices from NIST and quickly assess their compliance posture.

In the event that organizations require custom content that is tailored specifically to their environment, Lumension Developers Kit™ provides a GUI that makes authoring simple and does not require extensive training or labor cycles. This, combined with Lumension's flexible approach to discovering and managing even non-domain assets, dramatically reduces the complexity and overhead of a successful patch management process.

The consolidated management and flexibility of Lumension's offering provides greater operational efficiency and lowered TCO due to less resources and time needed to manage the patch management process. In addition to the expanded capabilities of Lumension's complete patch management solution, the award-winning solution delivers granular capabilities that deliver more versatility over free software available in the market today, including:

- » The ability to perform wizard-based, multi-patch deployments
- » The support for phased rollouts
- » The ability to easily specify narrow installation windows

Why “Free” Patch Management Tools Could Cost You More

- » The automatic initiation of prerequisite activities including, for example, patch precedence and data backup
- » A flexible and minimally disruptive end user experience where patch deployments may be snoozed, or installed with or without delayed reboot
- » Sophistication of administrative management (that is role-based access control beyond simple read and full permission divisions)
- » The rapidness of vulnerability assessments without dependence on the propagation of group policy objects (GPO's)
- » Machine grouping methods beyond OS, including grouping by IP address range and Active Directory attributes
- » Active Directory integration that facilitates patch management mechanisms similar to the management of GPO's

Continued »

Conclusion

While “free” tools appear to be an enticing solution for patch management, looking deeper into the needs of the organization leads to selection of a more complete patch management solution which results in reduced long-term risk and optimized operating expense.

Function	Lumension Vulnerability Management	Free Point Patching Products
Patch Microsoft OS	✓	✓
Support for 3rd party applications and OS's	✓	✗
Consolidate patch management operations	✓	✗
Discover unmanaged assets	✓	✗
Support for non-Active Directory environments	✓	✗
Security Configuration Management	✓	✗
Full system inventory collection	✓	✗
GUI-based custom authoring tool	✓	✗
Reduces staff burden	✓	✗
Lowers patch management TCO	✓	✗
Granular patching control	✓	✗
Complete solution does not require additional point products	✓	✗

Lumension vs. Free Patch Software Functional Comparison

“We can now quickly determine which machines are patched and have achieved a manageable level of automation in the application of necessary patches. We have not been subject to any major virus attacks since deploying Lumension and using its centralized management capability. Critical patches can be quickly applied to all machines across our distributed network”.

Mike Walder, Support Consultant, East Sussex Council

About Lumension

Lumension™, Inc., a global leader in operational endpoint 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 Reporting and Compliance 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, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.lumension.com.



Global Headquarters

15580 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260 USA
phone: +1.888.725.7828
fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance