How to Deal with Today’s Multi-Platform, Multi-Vendor Patch Management Mess

Organizations need a comprehensive patch management solution which provides endpoint protection beyond the typical operating system in order to effectively and efficiently minimize risks caused by the vulnerabilities that are inevitable in modern computing systems.

By David Strom
These days aren’t easy for enterprise patch management

Numerous studies show that patching is still an issue

Achieving Success in Patch Management

Do You Know What Needs Patching?

How Many Patch Solutions Do You Need?

Do You Test Before Roll-Out?

How Do You Measure Performance?

Conclusion: Comprehensive Patching For The Win

About the Author

About Lumension Security, Inc.
THESE DAYS AREN’T EASY FOR ENTERPRISE PATCH MANAGEMENT

The practice of keeping the variety of servers, desktops, laptops, smartphones, tablets and other end user devices up-to-date with the latest operating system software, drivers, and security updates has gotten more complex. Apart from the fact that we all use a variety of endpoint computing devices for our work and home lives, the rise of “there’s an app for that” mentality makes it commonplace to download anything from the Internet. This means that just about everything we use nowadays is constantly in a state of flux. Even our cars have software-downloadable patches to keep their firmware and controls up to date!

My iPhone had 72 applications that were outdated, according to iTunes. My Wordpress blog has 13 plug-ins that have more recent versions, not counting the update to the basic blogging software that I haven’t yet installed. Adobe Flash—one of the more common vulnerable applications in use today—is updated almost daily, or so it seems. And I haven’t even gotten my own standard Windows desktops and servers running a host of operating systems—let alone the bevy of other business, productivity and other applications which I use regularly. That is a lot of different systems to maintain. Some days it seems as if that is all I do: bring one thing or another up to its latest version utilizing numerous free, built-in update tools.

But, beyond the effort required, why should we care?

NUMEROUS STUDIES SHOW THAT PATCHING IS STILL AN ISSUE

There are an abundance of studies and reports featuring patching as core to an organization’s IT defenses. And each month we see news articles highlighting organizations whose networks were brought to their knees due to botnet-driven attacks like DDoS, targeted malware, spam, etc.

The analyst firm Forrester “sees continued interest and a sustained level of investment in vulnerability management” for several reasons, including:

- Regulations which dictate formal vulnerability management.
- A threat landscape in which exploits are released with increasing rapidity.
- A view of vulnerability management as an essential element of IT risk management in mature organizations.¹

A recent patch management study by Aberdeen² that shows smaller organizations lag behind the bigger ones when it comes to patch management, and that patching everything running inside an organization is still not commonplace.

Part of the problem is that patching is a multi-dimensional and complex issue. While organizations can utilize native update tools and free updates from Microsoft, the most commonly attacked software today is via 3rd party applications. In fact, Secunia says “An 80% reduction in risk can be achieved by either patching the 12 most critical or the 37 most prevalent programs in a sample portfolio.”³

They go on to point out that, in order to you would need at least 12 different update mechanisms to keep these endpoints up-to-date.

Patching the Typical Endpoint *
(comprising the top-50 software portfolio)

<table>
<thead>
<tr>
<th>Type</th>
<th>Vulnerabilities</th>
<th>Patching</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>count</td>
<td>pct</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>100</td>
<td>11.5%</td>
<td>1</td>
</tr>
<tr>
<td>(28 programs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apps</td>
<td>84</td>
<td>9.7%</td>
<td></td>
</tr>
<tr>
<td>Third Party</td>
<td>685</td>
<td>78.9%</td>
<td>11</td>
</tr>
<tr>
<td>(22 programs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>total</td>
<td>869</td>
<td>100%</td>
<td>12</td>
</tr>
</tbody>
</table>

This becomes necessary because, according to The SANS Institute, the “… primary initial infection vector used to compromise computers that have Internet access. Those same client-side vulnerabilities are exploited by attackers when users visit infected web sites.” SANS cites the main culprits with older and unpatched versions of commonly used programs such as Adobe PDF Reader and Flash, among other apps.⁴

And these vulnerabilities are exploited for a very specific reason these days: to make money, by either stealing your valuable organizational IP (such as new product development plans, trade or manufacturing secrets, customer lists and more) or so-called “toxic data” such as customer or employee Personally Identifiable Information (PII). These data breaches can cost the organization in

---

²Aberdeen, To Patch, or Not to Patch? (Not If, But How), October 2011; see http://www.aberdeen.com/ Aberdeen-Library/7404/ A-patch-vulnerability-management.aspx
³Secunia, Yearly Report 2011, February 2012; see also http://secunia.com/blog/299/;
⁴The SANS Institute, Top Cyber Security Risks, September 2009; see http://www.sans.org/top-cyber-security-risks/summary.php
many ways, reaching beyond the bottom line to customer churn, organizational reputation and possibly even their entire future. After all, while the latest survey from the Ponemon Institute puts the average cost of a data breaches at $214 per record, in some cases this can lead to bankruptcy.

Bottom line, just about everything these days is updated frequently, and you can’t just use a Windows-only worldview any longer. And as the number of individual apps proliferates, it is getting harder to keep track, harder to prevent gaps in coverage, and harder to do all this cost-effectively.

So, what should we do?

**ACHIEVING SUCCESS IN PATCH MANAGEMENT**

Gartner tries to get a handle on this by segregating the entire universe of patch management tool providers into four sectors:

- The PC configuration life cycle management space that are used to manage an entire fleet of desktop PCs for the most part and handle their configuration, loading of applications and patching;
- Server provisioning and configuration management, which includes inventory and software distribution and auditing and remote control;
- Virtual server patching tools, that are specific to that space and can handle VM images that aren’t currently mounted or running in any hypervisors but still need updating; and
- Specific patching-focused vendors.

This range of different providers is needed because there are so many different kinds of systems to patch. As they say, “Patching has predominantly been focused on Windows platforms, but as IT organizations realize the potential risks involved, the need to patch multi-platforms and applications (including middleware and databases) has become a significant focus as well.”

So with the known threats to an organization’s network environment, why are so many trying to patch using ‘free’ tools? With Microsoft WSUS, an organization would need an additional 11 auto-update mechanisms to protect against the top 50 software portfolio (Microsoft OS, MS apps and 3rd party apps). Therefore, finding a vendor platform that can identify and patch vulnerabilities across heterogeneous OS’s, configurations and 3rd party applications in an IT environment, is the Holy Grail.

Let’s look at four questions you should be asking yourself about your patch management processes and tools.

**DO YOU KNOW WHAT NEEDS PATCHING?**

An important piece of the patch management puzzle is being able to do an accurate inventory and assessment of your desktop and server assets. Are there non-standard browser versions that are running and installed by your end users? Do you have devices with access to your WiFi network that were purchased / installed outside of the IT department’s knowledge? What about PCs that are powered off when you are scanning them, can you come back and wake them up remotely to see what is contained on each desktop?

Integrated asset discovery will provide full network visibility and continuous control across both physical and virtual environments in your organization. This functionality is critical to portraying an accurate picture of ‘how’ vulnerable your network is, allowing you to prioritize the identified vulnerabilities. After all, you can only address known issues.

**HOW MANY PATCH SOLUTIONS DO YOU NEED?**

A common security management framework is essential to maintain the integrity of your entire endpoint population. Gartner recommends that organizations, regardless of their size, establish standards and consistent policies before attempting any kind of automated patch management. They say: “Enterprises should strive for a consolidated strategy for configuration and patching wherever possible, but recognize that only a few configuration management vendors offer best-of-breed patching.”

It isn’t just about installing updates in some automated fashion.

---

6Ponemon Institute, 2011 Cost of a Data Breach, April 2011; see also http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

6Take, for instance, the case of DigiNotar, which was forced into bankruptcy after a data breach in mid-2011; see http://www.scmagazine.com/after-breach-diginotar-folds-into-voluntary-bankruptcy/article/212424/.

but the ability to manage updates alongside other security tools such as anti-virus protection, host-based firewalls, blocking particular ports or devices, and whitelisting and blacklisting specific applications. You need the appropriate integration across these activities to maintain and secure your endpoints from attack or compromise.

DO YOU TEST BEFORE ROLL-OUT?
Sometimes Microsoft and other vendors release a patch too soon, creating complications for other apps or for particular situations. Or one vendor’s patch may break another vendor’s product. This is particularly the case with Internet-based apps that have a complex series of dependencies on particular Java machines or scripting tools that require a narrow set of Web browser versions to operate. You need to be able to test deployments in a sandbox setting and ensure that they are appropriate for your particular user base with your complete collection of standard enterprise apps.

HOW DO YOU MEASURE PERFORMANCE?
While it is difficult to say that a particular solution prevented a series of attacks or exploits, you can make a case for reduced support costs and increases in productivity and compliance. You should also look at how many systems were exploited as a result of a lag time in applying the current patches. Another measurement could be the amount of IT man-hours required to run the entire patching solution, and how often you need to redo any failed patches. Finally, you can look at how much time (including IT effort and end-user downtime) is spent eradicating malware designed to exploit known vulnerabilities.

CONCLUSION: COMPREHENSIVE PATCHING FOR THE WIN
Free tools aren’t a complete solution for today’s wide-flung organizations with a heterogeneous infrastructure using an extensive array of applications. If you are looking for an organization-wide patching solution that can handle a wide variety of situations, then you need to look beyond the free tools that are available from Microsoft (such as WSUS) and others. These free tools often provide a false sense of security, leaving your organization open to the exploitation of known vulnerabilities.

The most comprehensive patching solution for today’s organizations will include heterogeneous OS support for easy patch and remediation across multiple platforms and third-party vulnerability content. These crucial elements reduce an organization’s risk of exploitation by known vulnerabilities that can lead to costly data breaches.

ABOUT THE AUTHOR
David Strom is an expert on networking and Internet applications who has been writing about these topics for more than 25 years for a number of IT and general-interest publications. He is currently the Business Channels Editor of ReadWriteWeb and was the founding editor-in-chief for Network Computing magazine. His Web site is at http://strom.com/.

ABOUT LUMENSION SECURITY, INC.
Lumension Security, Inc., a global leader in endpoint management and 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, Antivirus 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 Texas, Florida, Washington D.C., Ireland, Luxembourg, Singapore, the United Kingdom, and Australia. Lumension: IT Secured. Success Optimized.™

More information can be found at www.lumension.com.