WHY PATCH MANAGEMENT MATTERS

Understanding the return on investment of managed patching — for both MSPs and their customers

solarwinds n-able

COMMUNICATING THE VALUE OF MANAGED PATCHING

As long as there are hackers willing to exploit software vulnerabilities and security breaches, patching will continue to be a critical element of the package offered by managed service providers (MSPs) to small- and medium-sized businesses (SMBs).

While patching is important for companies of any size, SMBs are particularly challenged to address the sheer volume of security vulnerabilities that can be exploited within their operating systems, web servers, databases and applications — and the overwhelming number of fixes being released to address them.

In the past five years, 459 vulnerabilities have been reported across the various Windows® operating systems.[1] And in 2010–2011 alone, Adobe® issued 399 security bulletins and nearly 200 patches to protect its users from application-based vulnerabilities.[2] Factoring in the multitude of third-party software and applications used across all business environments — and with 'bring your own device' policies making every new smartphone and tablet a possible new point of network infection — it's no longer reasonable for SMBs to rely on their own employees to manually download and apply the required patches.

The costs and consequences of poor patch management

The high-level impacts of spyware, ransomware, rootkits, spambots, hijackers and other online attacks that can enter a company's network through unpatched vulnerabilities are clear: decreased productivity, lost revenue and damaged reputation. What happens if sensitive personal or financial information is stolen — and what happens if that loss results in legal action? And if an SMB's systems are knocked offline, what is the cost of that downtime in terms of both human resources and lost opportunities?

SMBs are generally aware of the consequences of not patching. Unfortunately, the way they go about patching is outdated, with many still doing the task on their own or having a technician install patches manually across their workstations and devices on an irregular, ad hoc basis. Needless to say, neither approach is cost-effective, efficient or secure. For SMBs, the cost of patching systems in this way can be expressed as follows:

(Hours x Billing Rate x Number of Systems) + (Patch Failure % x [Hours x Billing Rate x Number of Systems])

If it takes a combined two hours each month to manually update a single system and the SMB has 100 computers across its organization, that's 200 hours of work each month. With the technician charging a billable rate of $18 per hour, manual patching will cost that business $3,600 each month — and that's assuming a patch failure rate of zero and no unintended consequences from the applied patches, both of which are very unlikely.

Overcoming customer objections to managed patching

Given the costs and consequences involved, why aren't more SMBs adopting a fully managed, outsourced approach to patching? Some of the common objections MSPs hear include:

"Windows updates itself. I don't need a patch management strategy."

Automated services like Windows Update® depend on the end user manually accepting and downloading patches. Given the volume of patches required, this leaves far too much room for error: users can repeatedly ignore patch prompts, leaving their systems vulnerable long after a patch has been released. In addition, Windows is no longer the only software that needs to be patched: third-party applications are now the most common point of entry for malicious attacks.

"We'll patch the system if we hear about a problem."

Patching takes time and exploits move quickly, capable of spreading through a company's network in a matter of minutes. If the SMB is updating each system manually, how can they be sure they will be able to react before an infection takes hold?

[1] Secunia. (2014). Secunia Vulnerability Review 2014: Key figures and facts from a global IT security perspective. Available from: https://secunia.com/?action=fetch&filename=secunia_vulnerability_review_2014.pdf.

[2] Adobe. (n.d.). Security bulletins and advisories. Available from: http://helpx.adobe.com/security.html.

"If we're compromised, we can deal with it using antivirus."

Even the best antivirus software in the world can't protect against all malware. Some types of vulnerabilities, like rootkits, can't be caught by antivirus programs — they might be disguised as legitimate system API calls, for example — and require difficult, time-consuming, manual effort to locate and remove.

THE RETURN ON INVESTMENT OF MANAGED PATCHING

In light of these common challenges and misconceptions, an outsourced patch management strategy delivered by a reliable, trusted MSP can give SMBs the protection they need at a cost they can afford. And from the MSP's perspective — many of whom still rely on basic, labor-intensive patching tools that eat into their profitability — incorporating an automated patching solution into their managed service offering gives them an easier way of delivering patches that is both low effort and high return.

The benefits for SMBs are self-evident: a fully managed approach to patching gives them the assurance that their networks are protected and devices secured, reducing system downtime while also saving them the hassle of worrying about patch installation.

For MSPs, the decision to offer any kind of service ultimately boils down to return on investment. The centralized, streamlined management of patching reduces support ticket volume and improves support response times — and can even help build recurring revenue from purely reactive customers who would typically purchase very little in the way of managed services.

Building recurring revenue

Approximately 80 percent of the SMB market takes a very reactive approach to IT. They don't want to pay an MSP to actively manage and monitor each and every server, laptop and workstation throughout their organization — instead, they follow the 'break–fix' model, calling on MSPs only when a system goes down. While these reactive customers are typically reluctant to purchase the complete package of managed services (including antivirus, backup, automation, reporting, remote control and more), it may be possible to sell them on a single recurring service, with patching being a particularly low-cost, low-barrier-to-entry service.

The challenge for most MSPs is that while patching is a relatively low-cost service to deliver (which appeals to the customer), on its own it does not offer high enough margins to sell as a standalone managed service. As a result, patching is usually available only as part of a more comprehensive service offering that is too expensive for most SMBs. Fortunately, there is a middle ground where MSPs can meet the patching and security needs of their cost-averse, reactive customers and build their own business at the same time.

Some remote monitoring and management solutions, such as SolarWinds N-able's N-central® platform, allow MSPs to offer 'freemium' licenses for select services to help them get a foot in the door. Free monitoring probes can be deployed throughout a customer's network, gathering the data necessary to paint a clear picture of the company's current patching status and where vulnerabilities need to be addressed. By providing this kind of free consultation, MSPs can win their customers' trust and eventually sell them on a solitary recurring service to fix their current vulnerabilities and keep them secure moving forward — an approach that is likely to be much more appealing to them than a costly, full-blown managed service package.

Streamlining the process with centralized, remote management

More service does not have to equal more labor. A centralized approach to patching makes it possible to quickly patch all customer devices across multiple sites with the press of a single button, greatly reducing the amount of time it takes to roll out new patches. In addition, managed patching allows for the easy scaling of services. Once an MSP has started to provide managed patching, they can seamlessly add hundreds of customers and thousands of additional devices and remotely patch all of them without any additional time or effort — making it a low-labor, high-margin offering when used in conjunction with other managed services.

Improving support response times and reducing support ticket volume

Managed patching allows MSPs to standardize patch versioning across a customer's organization. By updating all of the customer's systems and applications to the same patch version, MSPs can create a consistent baseline for all of the software across the entire company. And by restricting or allowing software patches at the organizational level, they can know exactly what application version their customers are using when they call for support — reducing their support workload and, in turn, improving support response times.

Plus, with that baseline in hand, if the MSP is notified that a specific patch is causing problems, they can prevent unstable patches from rolling out or quickly roll back all customer devices to a previous version of that patch — before they get flooded with support calls — to reduce their support ticket volume.

THE SOLARWINDS N-ABLE APPROACH TO MANAGED PATCHING

Just as manually patching their own devices is not a cost-effective proposition for SMBs, it's also insufficient for MSPs looking to protect their customers against the latest security threats. MSPs require an automated solution that makes their life easier — like the one provided through SolarWinds N-able's Patch Manager.

How Patch Manager works

The way Patch Manager works with the N-central remote monitoring and management platform is illustrated in Figure 1 on the next page.

First, every device in a customer's network communicates with Windows Update (or the appropriate third-party patch service), which responds back with a list of applicable patches for that device — meaning MSPs don't have to capture that information manually and can deal only with the patches that are needed in each customer's particular environment. Once the MSP has approved a patch for deployment, N-central pushes the approval to the user device so that it knows it needs to install a patch. The device then reaches out to a locally installed probe, which downloads the patch payload from Microsoft's servers and pushes it back to the device to be installed.

Core features of Patch Manager

Giving MSPs full control over patching

Patch Manager allows MSPs to approve patches by device (to test on a single machine before applying it throughout the entire network, for example) or by patch (to ensure a given patch is installed across every system). Auto-approval rules can also be established for patches from certain vendors or for certain mission-critical applications so they are instantly applied as soon as they become available.

Once Patch Manager has notified the MSP that a new patch is available, with just a few clicks it can be rolled out to a specific customer's devices or to the MSP's entire customer base. With the ability to schedule when patches are downloaded and installed, MSPs can delay rebooting user devices until a more convenient time so as to not disrupt the customer's workflow or productivity. And because Patch Manager can update systems remotely, it can be used in organizations that are widely dispersed or have users who do not come into the office on a regular basis — ensuring employees who take their laptops home are never at risk of missing a pre-scheduled patching window.

Patching third-party applications

Patch Manager can install Windows updates and patch more than 20 of the most commonly used third-party applications, including those from vendors such as Adobe, Oracle®, Skype®, Apple®, Google® and Mozilla®— making it easy for MSPs to address the full range of security vulnerabilities across all of their customer devices and applications.

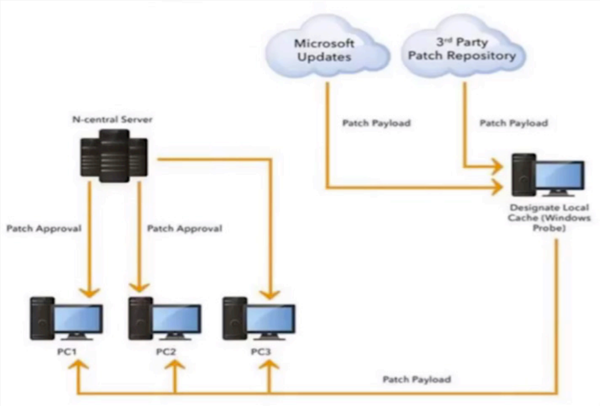

FIGURE 1:

How N-able Patch Manager works

Reporting on patch status

Patch Manager generates user-friendly graphical reports summarizing each device's Windows and third-party application patching status. By sending their customers a weekly or monthly report on their work, MSPs can clearly demonstrate the value they provide and the impact they are having on their customers' IT environments—and the ongoing progress being made to address their system vulnerabilities.

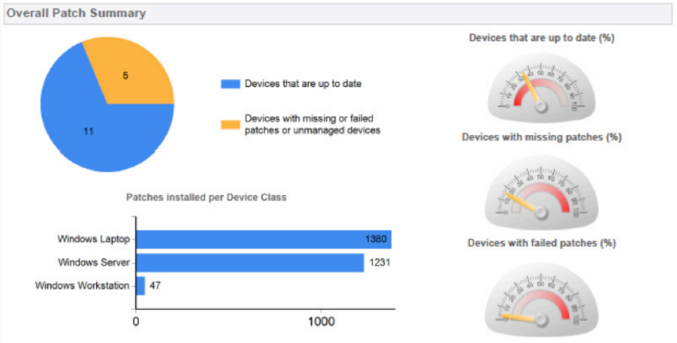
Overall Patch Summary
5
11
Devices that are up to date
Devices with missing or failed patches or unmanaged devices
Patches installed per Device Class
Windows Laptop
Windows Server
Windows Workstation
1380
1231
47
0
1000
Devices that are up to date (%)
Devices with missing patches (%)
Devices with failed patches (%)

FIGURE 2:

Easy-to-understand patch status reports

CONCLUSION

For MSPs to consider patch management a worthwhile service to offer to their customers, it has to bring a solid return on investment. Accelerating and streamlining the scheduling and installation of patches across all customers and devices is essential for reducing an MSP's workload to maximize productivity and reduce costs — but customer satisfaction also plays a big role in realizing an effective return on investment. Being able to view the status of deployed patches across customer environments to see patch adoption and success rates — and then being able to relay that information through easy-to-understand summary reports — will help MSPs clearly explain to their customers where more work is needed to keep particular devices or systems up to date.

When customers see these results and the ongoing progress being made to address the vulnerabilities in their systems, they will be more inclined to not only continue using the managed patching service but may also look to add other managed services to their package — and for any MSP, that's the key to building and growing their business.

ABOUT SOLARWINDS N-ABLE

SolarWinds N-able is the global leading provider of complete IT management, Automation, and MSP business transformation solutions. N-able's award-winning N-central® is the industry's #1 RMM and MSP Service Automation Platform. N-able has a proven track record of helping MSPs standardize and automate the setup and delivery of IT services in order to achieve true scalability. N-central is backed by the most comprehensive business enablement support services available today and the industry's only Freemium licensing model. Thousands of MSPs use N-able solutions to deliver scalable, flexible, profitable managed services to over 100,000 SMBs worldwide. With offices in North America, the Netherlands and Australia, N-able is 100% channel-friendly and maintains strategic partnerships with Microsoft®, Intel®, IBM®, CA®, and Cisco® among others.

Corporate Headquarters
SolarWinds N-able
450 March Road, 4th Floor
Ottawa, Ontario
K2K 3K2 Canada
Tel: +1 (613) 592-6676
Toll Free: 1-877-655-4689
Fax: +1 (613) 592-224

The Netherlands
Koningin Wilhelminalaan 3
527 LA, Utrecht
Tel: +31 (0) 30 298 5285

Australia
Level 9
15 Blue Street
North Sydney
Sydney, New South Wales
2060 Australia
Tel: +61 (0) 2 8412 4905