



PATCHING FATIGUE

THE TOP 7 IT MANAGER COMPLAINTS

(and what to do about them)

WHAT IS PATCHING FATIGUE?

A term that's cropped up recently among IT managers is "patching fatigue."

The overwhelming number of patches makes keeping an environment up-to-date arguably the most difficult item on any IT manager's to-do list.

According to the 2016 IBM Security Report, which covers 18 years of patches, there are over 100,000 known vulnerabilities. That works out to around 5,000 a year per device. Only a few hundred would affect each device in a network at any time, but these security risks pile up quickly.

Even with a small environment, that's a monumental task for any IT manager. It's no wonder patch fatigue has caught the attention of many IT departments. If there are multiple operating systems, departments with different software needs, or roaming users then network security challenges are compounded.

Tripwire recently conducted a survey of nearly 500 US-based IT professionals, and an overwhelming majority (76 percent) admit to confusion regarding patching and are struggling to keep up. It's why patch management services and MSPs are growing in adoption and customer base.

Patching shouldn't be something that's managed when issues appear, by then it's usually too late – often resulting in a compromised network. A detailed plan of attack can mitigate most pain points IT managers suffer.

Here are the seven top complaints contributing to patching fatigue – and what to do about them.



Problem #1

PATCH MANAGEMENT IS TOO TIME CONSUMING

No matter the size of the organization, whether it's a few hundred or over 1,000 endpoints, patching can take hundreds of hours every month. There's also added concern if a patch requires a system restart, more so for servers, as significant downtime and lost business is a likely result.



WHAT TO DO ABOUT IT

Deploy a patch management tool that automates the patching process during maintenance windows when the business is least affected, usually during weekends or after hours. It also helps to focus first on mission critical patches and identify areas that are most vulnerable.



Problem #2

IT'S MORE THAN MICROSOFT AND OPERATING SYSTEMS

The patching process isn't limited to Windows or other operating systems. Third-party applications also have patches and not all the patches are created equal. Vendors like WordPress are relatively simple to update, but Java and Flash are often painpoints for IT managers.

WHAT TO DO ABOUT IT

Ideally the patch management tool also operates with major third-party vendors. It's imperative to identify what software is on which devices. If a department or collection of devices share similar software then grouping the patches together will save time and resources.



Problem #3

JAVA AND FLASH

THE PROBLEM CHILDREN

Two of the largest contributors to patch fatigue are Java and Flash because they are typically bundled with other products. Bundling creates version control issues as it's difficult to know which patches for Java and Flash were deployed to which devices.



WHAT TO DO ABOUT IT

Having an inventory tool is the best way to manage the issue. Properly scanning each device for the software and software version enables proper patch deployment and removes any guesswork.

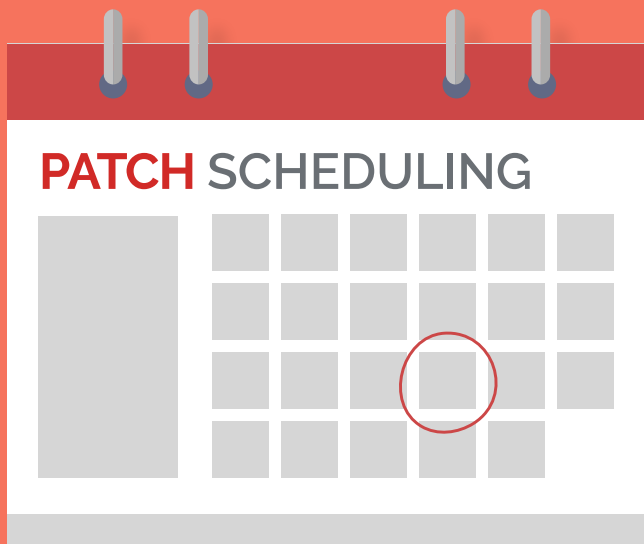


Problem #4

STRUCTURED SCHEDULING AND CRITICAL FIXES

Patch Tuesday is Microsoft's monthly release cycle – always the second Tuesday of the month – providing updates for its catalogue of products. While many IT managers would rather have critical fixes released on an as created basis, the schedule has eased the burden for many IT managers. Companies like Apple, however, release on an intermittent basis so if the environment has various operating systems, there's a greater challenge.





WHAT TO DO ABOUT IT

Get on a schedule. The schedule doesn't have to match Microsoft's, though many IT departments implement a Patch Saturday. It's recommended to take one period during the month to patch devices. Rotating through groups of devices for less critical patches helps spread the workload. Patching needs to take place quarterly at a minimum, otherwise it's too dangerous for network security.

Problem #5

WHAT VERSION IS THIS? WINDOWS 10 BRANCHING

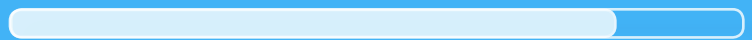
Microsoft's new strategy for Windows 10 involves updating the OS in two different fashions. Long-term servicing branch (LTSB) is the familiar Windows update with security updates and bug fixes, but alternatively customers can use the current branch (CB) which includes new features. New features help end-users, but testing and possible system downtimes are the most immediate drawbacks.



WHAT TO DO ABOUT IT

Test before updating to the CB. If the business has legacy applications tied to older OS versions then updating to the current branch is probably unwise. Staying up to date is important, but not at the cost of doing business.

TESTING ...



Problem #6

DON'T DEPLOY EVERY PATCH

The Common Vulnerability Scoring System (CVSS) is an industry standard methodology to classify how critical a patch is to a device. But what matters most is how critical a patch is to a device in the business network. Many patches can be ignored due to vendor issued severity, and conversely patches not rated highly among most devices could be critical to the environment.




WHAT TO DO ABOUT IT

Controlling the selection of missing updates, especially those with serious consequences if not deployed, lessens the potential impact. A patch management tool that also identifies patches and gives greater clarity limits the strain.

Problem #7

PATCHING & VULNERABILITY MANAGEMENT

Patching and vulnerabilities are frequently intermingled terms, but are not interchangeable. Even after patching there are still vulnerabilities that may exist in the network and it's important to identify where these potential pitfalls exist. Legacy applications and older OS versions are prime targets as patches are in place, but don't completely insulate the network.

A solid blue shape that starts as a thin wedge at the bottom left and expands diagonally upwards to the right, filling the bottom right corner of the page.

WHAT TO DO ABOUT IT

Patching is the first step for securing an IT network, but the job hardly stops there. Gaining a thorough understanding of the IT network through accurate reporting identifies areas of concern. It's also important to remove discontinued products, this alone mitigates many problems. Until devices begin self-upgrading or self-patching it falls to the IT manager to discover the best way to manage each challenge. However, a dedicated patching tool helps relieve many headaches associated with patching fatigue.





CLOUD MANAGEMENT SUITE



Patch Management



Software Distribution



Remote Control



Discovery & Inventory



Inventory History



IT Reporting

SO EASY.

Manage all your devices inside or outside your network from the cloud without the need to deploy agents.

[Start a free trial →](#)



ABOUT US

Cloud Management Suite allows you to get the complete picture of your entire IT environment from the cloud. Automatically discover network devices, remotely deploy software applications and automate patch management. A single web based console allows access to any device from anywhere, all without the need to install agents on your endpoints.

Headquartered in Aliso Viejo, Calif., Cloud Management Suite is a growing and dynamic organization with offices in four countries and 12 partners in nine countries. For more information about Cloud Management Suite and how we've revolutionized IT systems management, visit www.cloudmanagementsuite.com.



CALL

US: +1 (949) 270-1903
UK: +44 (0) 1256-806567

CONNECT

www.cloudmanagementsuite.com
info@cloudmanagementsuite.com