THE ULTIMATE GUIDE TO BUILDING A PATCH STRATEGY

How To Identify, Prioritize and Install Patches Accurately and Efficiently

BACKGROUND

In 2003, Microsoft introduced what is commonly known as Patch Tuesday, the second Tuesday of each month (sometimes the fourth) when the company releases the newest updates or malware database refreshes for its Windows operating system and software applications.

These patches update individual files specific to enabling Windows and other Microsoft software to work properly. They are determined by Microsoft to have security issues or “bugs” that could carry the potential of a malicious and undetectable attack to a computer or an entire system.

To reduce costs associated with patch deployment, Microsoft chose the day after Monday because the first day of the workweek presents enough challenges that demand attention. By waiting a day, IT managers still have enough time to make any fixes before the weekend while allowing them to focus on high-priority issues that await Monday morning. Though patches are only sent out on Tuesday, if a critical fix arises, it is sent out regardless of the day of the week.

While patches usually fix the issues for which they are intended, they can also become the cause of a new problem, particularly if the patches are administered by the uninitiated. Someone with little or no experience can often do more harm than good. Wiith new vulnerabilities being discovered every day, it’s critical for a company to ensure that software and business applications are safe and running smoothly.

With a sound, cloud-based strategy for patching and update management, your organization can minimize risks and reduce costs.

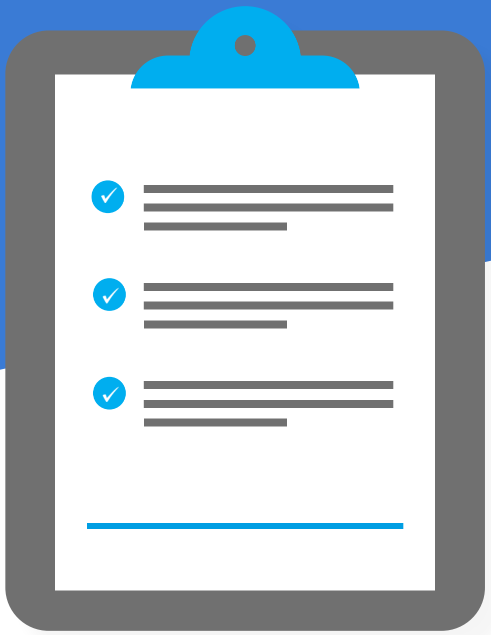
GETTING STARTED: PATCH I.D.

Getting safely started in the patch management environment can be daunting, particularly for companies that have an IT department of one. Challenges inherently arise and when they do, it is important to understand how to patch accurately and efficiently.

In order to build a patching strategy, it is important to consider the three general categories of updates when prioritizing issues: critical, important, and optional. Critical updates typically involve security, privacy and reliability, while important updates address non-critical problems to help enhance the computing experience. Optional updates can include updates to drivers, for example, or new software, and they often enhance computing as well.

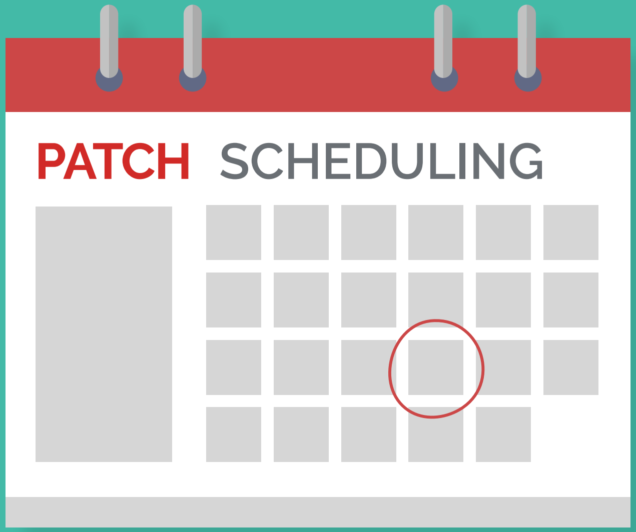
REQUIREMENTS FOR A **SUCCESSFUL PATCHING STRATEGY**

An efficient and cost-effective patch management strategy is crucial to the success of any business, considering the risks from a mobile workforce and the increasing number of employees working remotely in today's expanding global market. However, it's one thing to deploy patches as they are released and another to confidently update all of your company devices - at any time from any location to ensure a safe environment every day.



Along with developing or customizing a patch management policy for your entire organization, which can be structured by filters or groups in order to identify devices with specific criteria, a natural first step is to identify compliance and security issues with a system-wide audit and assessment.

Equally important is allowing for sufficient time to analyze current security and plan remediation activity, as well as the ability to address issues such as major outages and virus outbreaks. It is therefore crucial to have a toolset that can scan and identify missing updates on all endpoints. deploying them safely whether your end-users are based out of home or in other remote locations.



CREATING AND SCHEDULING
A SUCCESSFUL BASELINE

Creating a baseline sets a standard within your organization and allows for introducing control measures that ensure a successful updates and patch deployment. A successful baseline is a group of fully tested updates deployed each month in a phased and controlled manner. Initially, the baseline could contain as few as five updates, but each month the baseline should be appended with the next list of qualified updates.

Deciding which updates qualify for the baseline depends on the toolset, but the priority is often derived from the Common Vulnerability Scoring System (CVSS), which is a free and open industry standard for assessing the severity of computer system security vulnerabilities. The system identifies severity by vulnerability, threat or risk on a scale from 0 to 10, with vulnerabilities in the 7.0-10.0 range, threats in the 4.0-6.9 range and risks between 0-3.9.

Once you've created a successful baseline, it's best to organize your IT environment into logical groups, either by department, region, location or device type. Each month, use your toolset to deploy the baseline to your estate on an agreed upon schedule. Keep in mind that any new or rebuilt devices that appear on the network will collect all the missing updates from previous baselines.

It's also important to download or update your calendar, then populate the calendar and include it on all change requests. Use it day to day when scheduling or reviewing changes as the most common errors occur when the wrong devices are upgraded on the wrong day.

EMPLOYING EFFECTIVE TESTING STRATEGIES

Never use your own machine when testing. Instead, build a “test rig” of virtual machines (VMware, Microsoft Virtual PC, Oracle Virtual Box) and clone several endpoints that are the most representative of your environment. If a patch breaks your own device, you’ll not only be frustrated, but your device will also take a day to fix. So never start with your own and always check to see if the patch has an uninstaller.

This is one of the most crucial factors to consider in any testing strategy. If the patch has no method to uninstall, extra tests are needed. Test systems should be representative of your estate and conducted through specific criteria, with evidence reviewed and approved by someone other than the tester.

Always test with an open mind. If you deploy a patch, record what you see. If there’s a failure at any point of the process, test again rather than ignoring it. If failure occurs after deploying the patch, simply go back, uninstall the patch and reinstall it. If the result is still the same, pinpoint the problem by identifying the source, whether it’s the hardware, the machine or the software.

PHASE 1

RESEARCH

Before you start applying patches, become familiar with what the updates will fix and what operating system the update effects. The following series of questions will reveal the information you need: Does the update require a reboot? Is it silent? Does it require any user interaction? How large is the update?

PHASE 2

IDENTIFICATION & TESTING

Use your toolset to identify at least five devices for the number of missing updates. Remember: the more updates you install at any given time, the greater the risk for user interruption. This results in frustration for your end users and more calls to the helpdesk. Pay particular attention to any reboot requirements. As a rule, reboot at least twice to ensure the update has been applied.

PHASE 3

SUCCESS CRITERIA

Success can be measured in many different ways including the number of incidents raised on the helpdesk following deployments. Success can also be measured by the ease of which the process can be followed and regularly repeated. The positive reports you can produce from your toolset are better still. When a software update installs correctly without interruptions and does not conflict with other software, report your success!

PREVENTION IS THE BEST MEDICINE

With an automated update and patch management system in place, your organization not only increases its likelihood that security is maintained, but also increases business processes that can include remote power management. It's surprising how simple functions that enable an automatic shutdown and wake up of systems can save a company a significant amount of money over time.

As machines get faster and applications become more available, new vulnerabilities are bound to be discovered daily. It's prevention that will set your organization on the path for success and there's no better time than the present to get started with an update and patch management system that becomes part of your everyday routine. A safe and effective IT environment will give your organization a competitive edge not only by increasing productivity but also by providing your workforce with the tools they need to reach their highest potential.

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