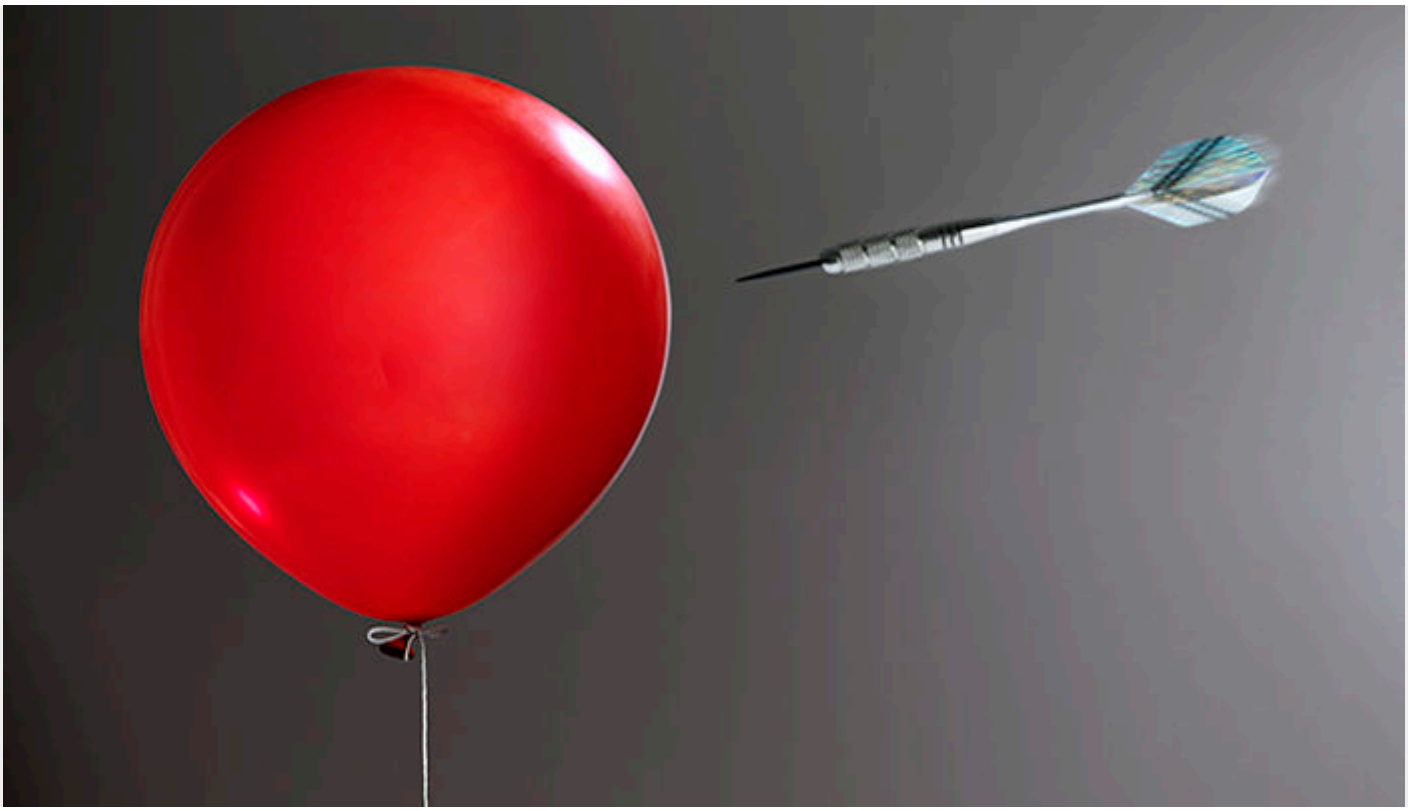
PATCH MANAGEMENT: A BRIEF INTRODUCTION



Anyone who has ever dealt with computer issues knows that maintaining their system is a serious pain in the neck. There's something uniquely frustrating about having your devices work fine one second only to become useless paperweights the next. This issue is a thousand-fold more frustrating and potentially expensive when you start dealing with the complex systems of business devices and computer networks.

There's a reason why IT professions have such good job security—when humans and computers interact, difficulties are bound to arise. Some of the most common issues are a result of neglected maintenance duties and one of the most neglected maintenance tasks is patch management.

What is Patch Management?

Patch management is the process of maintaining computer networks by performing regular patch deployments. Patches are updates to existing software applications and packages. Each patch to a system can vary greatly in severity of importance and difficulty of application.

Some patches are created to repair newly discovered security holes that can leave your entire network vulnerable to outside intrusion while other patches may change the font used for displaying the time on your desktop. Not every patch is groundbreaking, but every patch has the potential to disrupt your operations or cause serious problems down the line if ignored.

Fast, efficient patch management is essential for effective enterprise security. As software vendors discover flaws and vulnerabilities in their products, a timely fix can make all the difference to protect

your business from a damaging compromise. But how can you keep track of all the vulnerable devices in your organization—and ensure that you're deploying the right patches, in the right priority, for optimal risk mitigation? Without a holistic, automated approach to detect, deploy, and manage patches across your organization, it's all too easy to fall behind.

As the speed and complexity of the threat landscape increase, a mature patch management capability can help you ensure that your devices are reliably protected against known software vulnerabilities.

Patch management encompasses four critical elements:

1. Identifying which devices are missing patches
2. Automatically gathering patches from vendors
3. Deploying patches to devices
4. Providing reports to help you make informed business decisions

There are many different kinds of patches created for solving various system issues or just for improving general functionality and software efficiency. The three most common types of patches are security patches, bug fixes, and feature updates.

Security Patches

One of the reasons why patch management is so important is due to how quickly the technology sector can move. This is especially true when considering the dark side of the technology world that is filled with hackers searching day and night for new exploits with which they can leverage to make a quick buck or wreak havoc.

Many patches are created to cover up newly discovered security holes in the system. Oftentimes, these security holes are discovered after they have already been exploited by unsavory types of IT professionals.

Bug-fixing Patches

Other important types of patches are ones that fix application errors and common or uncommon bugs encountered during regular use of the systems. These patches can drastically improve overall operational efficiency by saving time spent dealing with bugs. Some bugs are minor annoyances while others require hours of troubleshooting or workarounds, wasting massive amounts of time over the course of weeks or months of operations.

Patches that repair bugs or system flaws can have a big impact on your bottom line depending on how severe the bugs are and how often they are encountered. This makes efficient patch management a task that can provide immediate value to your organization by ensuring your systems are updated with the most current and bug-free versions of software applications.

Performance and Feature Patches

Modern software companies are in a neverending arms race to provide the best applications on the market. This means they spend a lot of time and money researching and developing improved versions of their currently existing software. Most of today's biggest IT competitors use the Software as a Service (SaaS) business model that allows you to pay a flat rate for access to their most recently

updated products.

These update patches can involve general performance increases like faster computation speeds or lower resource requirements or they can add quality of life features that make using the applications easier and faster. Oftentimes, patches involve a combination of the updates we've mentioned such as patches that improve performance and cover up security holes.

Why is Patch Management Important?

Patch management can become a complex task thanks to the complexity of modern IT systems. Patching a system can require total system reboots, and the patching process can take anywhere from a handful of seconds to several hours for each computer on the network. Furthermore, patches aren't always successfully deployed for various reasons. This has the potential to create a situation where mismanaged patching can result in service outages and massive amounts of downtime.

Leaving the job of patching up to each end user can result in mismanaged systems becoming potential security threats for the entire network. Due to the nature of patches, it's not always possible to predict when a new patch may become available. Different software developers operate on different deployment schedules and an emergency security patch will generally be pushed out quickly to avoid catastrophic incidents. As such, proper patch management plays a key role in maintaining regular business operations without disruption.

Patch management is a multi-faceted process that requires careful planning, risk assessment, and attention to detail. A typical patch management system involves four primary steps: scanning, assessing, deploying, and monitoring.

- **Scanning** - Checking devices or groups of devices for available patches.
- **Assessing** - Analyzing the results of the scan to determine whether any patches need to be applied and assigning them a level of importance.
- **Deploying** - Selecting the patches and applying the changes to the selected devices. This step may involve staggering and scheduling of patches to reduce downtime and prevent users from losing data or experiencing interrupted services.
- **Monitoring** - Keeping tabs on the entire process and ensuring that deployment is completed successfully.

Each step in the patch management process can have multiple processes within it depending on the complexity of the patch and the expected impact applying it will have. Due to the complexity of patch management and its ability to affect operations, many organizations use automation tools to help ensure the process runs as smoothly as possible.

Automation can be used to perform regular scanning operations and generate reports based on the findings. Patch downloading and the necessary resource checking and allocation required to ensure patches are downloaded successfully can also be automated. Many aspects of patch management can be automated, but oversight and planning are still required to ensure networks are minimally impacted during hours of operation.

One of the most important tasks of patch management is prioritizing system patches in order of importance while also balancing out the impact applying those patches will have on operations. This is why patches are often applied automatically during the early hours of the morning; however, patching is often performed with some human oversight to ensure someone is on hand should

anything go awry.

Many patches require downtime as systems may need to reboot to successfully apply the updates and managing resources during this downtime can make the difference between coasting over a speed bump or crashing straight into a brick wall.