Original Source: The Importance and Benefits of Effective Patch Management

Written by:Adam Shepherd

Why patch management?

Technology is a crucial part of business, but corporate IT systems rely on so many different pieces of software that keeping everything fully up-to-date can seem like an impossible task.

Do you prioritise servers or employee workstations? Do you focus on security fixes or compatibility updates? And how do you keep track of which patches have been applied? These are difficult questions and they're even harder to tackle if you're a smaller business.

That's why patch management tools should be a crucial part of any IT manager's arsenal. Not only do they allow you to take all of the hassles out of patch deployment by automating the process, they also provide an overview of your network's health, letting you know what your liabilities might be and how urgently a fix is needed.

What is patch management?

Perhaps it's important to go back to basics for a moment. Patch management is the process of making sure that every piece of software used within a company is up-to-date

with the most current versions (you might think the version you've bought is the latest but bugs are routinely found after GA and rather than just ignoring, vendors have to add a sticking plaster until the next update) released by the manufacturer. This includes enterprise-level products like server operating systems and database products, as well as more basic tools like Internet Explorer and Adobe Flash.

For all but the very smallest of SMBs, manually checking for and applying software patches would be a Sisyphean task, which is where patch management software comes in. Rather than forcing IT staff – or staff generally if you don't have a tech team - to manually update critical systems, patch management will automatically handle the update process for every node on the corporate network.

This includes endpoints in physically inaccessible locations, such as employees' company smartphones, or laptops being used by remote workers. The ability to schedule patch and update deployments means that no matter what time-zone the endpoint is in, fixes can be applied at a time that isn't going to disrupt your business.

Why is patch management so important?

Unpatched systems are one of the easiest attack vectors for criminals looking to gain access to corporate networks. Hackers and security researchers are constantly discovering new vulnerabilities, and companies are constantly issuing patches to deal with them. If those patches are not applied, however, cyber criminals have an easy entry point into your networks.

Patch management also ensures that all your enterprise equipment keeps working as it should. Technology is notoriously fickle beast, and even minor software bugs can lead to major headaches and plummetting employee productivity. Automatic application of

patches ensures that any potential problems can be resolved as soon as possible before your business grinds to a halt.

What are the benefits of patch management?

The most obvious benefit of using patch management is that it ensures nothing slips through the cracks. It's frighteningly easy for a seldom-used piece of software to get forgotten about, and if it doesn't get patched it can introduce major security holes.

Patch managers also free up huge amounts of time, allowing IT staff to focus on other, more productive areas of the business. Rather than laboriously combing through update lists, they can be working on ways to get the most business benefit out of existing systems, or modernising IT deployments through digital transformation.

Patch management is also incredibly important in this new age of increased mobility and remote working. While manually updating on-site systems may be time-consuming, it is at least possible - but what do you do if some of your staff work from home, or if a critical patch is released for an employee's mobile device? Patch management can make sure that all your corporate devices stay updated, regardless of where they are.

What does effective patch management look like?

The most effective way to manage patches is going to vary between organisations, but a few factors remain constant. The main key consideration is prioritisation of patches. Critical security fixes should be applied as soon as possible, but beyond that there are other factors to take into account. IT managers should consider how often a piece of software is used, as well as how business-critical it is before deciding how urgently to apply a patch.

Another hallmark of effective patch management is choosing the best time to schedule them in. Making sure that updates are only installed out of working hours will minimise the disruption to business workflows, ensuring that employees aren't left twiddling their thumbs while important applications are updating.

Finally, patch managers can also be used to inform intelligent purchasing decisions for future investment. Many patch managers will give IT managers in-depth information about not only which nodes need patching, but the patches themselves. If a particular vendor is issuing frequent patches, it may indicate that its products pose a security risk and that you might want to look at alternative options.

Want to know more about effective patch management? Click here to download the whitepaper.

This is an independent article written by IT Pro, sponsored by SolarWinds MSP to celebrate thought leadership in IT. Learn more about SolarWinds MSP's Remote management and enjoy a free 30-day trial by clicking here.