Tips for Effective Patch Management

A Wanstor Guide

wanstor

Contents

Introduction

As intrusion points continue to evolve and expand, malicious attacks have become more pervasive and harder to prevent. This means an effective patch management strategy should be the first line of defence in building endpoint security. However, many IT teams simply ignore patch management as it can be seen as a time consuming and boring task to undertake on a regular basis.

Wanstor's desktop management team have spoken to several IT Managers in recent months. They have stated that, 'off the record', patch management is an endless burden which consumes huge amounts of process time, people resource and budget. Because of this attitude informal, ad hoc patching without a central strategy often takes place and fails to deliver what patching is supposed to deliver; a safe, secure and available IT environment.

At Wanstor, we believe patch management is a crucial task which should be at the top of the IT team's task list each week. Without an effective patch management programme in place, businesses are leaving themselves open to security attacks and breaches.

We find that with just a few practices and capabilities, patch management can actually become an easily executed task. In this article, Wanstor's patch management experts have pooled together their knowledge to develop a set of simple tips that can make patch management simpler, more effective and less expensive.

Understand your network

At Wanstor, we believe the first tip is probably the most important: *Understand your network*. It's important to understand that a network is only as strong as its weakest link, whether the business is considering IT security, stability or functionality. It only takes one unpatched computer to make the entire network vulnerable.

Patch management is about bringing the entire network (every computer and device), up to an acceptable level. To do so, the IT team needs to start by knowing exactly what's on their business and guest networks.

From Wanstor's network management experience we often find a lack of visibility or lack of awareness around dangerous blind spots by IT teams can leave poorly managed assets vulnerable to attack. This undermines even the best attempts to make sure of standard adherence to security policies.

The first action an IT team should take is to conduct an asset inventory to find out exactly what is on the company network. By undertaking this task the IT team can then quickly gather information about what is or isn't patched and where any vulnerabilities may appear.

We suggest all businesses invest in a network monitoring tool, this will give them real time insights into what devices are using the network and any potential non patched machines. So your first tip for simplifying patch management is to automate device discovery and asset assessment.

Discovery often starts with automated scans of your network, using a variety of techniques to find active devices and identify them. Once devices have been found, they can be assessed and inventoried. Inventory might involve scanning each machine to see what kind of hardware it uses, as well as to see what software applications are installed.

A subsequent patch assessment can tell you which applications are up to date and which ones need patches. In one automated process, you can quickly determine the state of the network and how vulnerable it is to security threats through non patched machines.

By having a true picture of the network, the IT team can understand more about the patch management work needed now and in the future, so patch management tasks can be allocated at relevant times.

Assess the patch status

Scanning computers and assessing their patch status isn't a one-off activity that the IT team does on an ad-hoc basis. We believe it should be an ongoing regular activity that forms an essential part of simplified patch management. The reason behind this approach is once you have an effective patch management process in place, you can automate a lot of the manual tasks and activities.

Periodic scans and patch assessments can help the IT team to identify computers where automated patch management isn't working, so they can manually address those computers and correct the problem. The purpose of a regular process of scanning and assessment is to focus the IT team's attention where it's needed, and thus reducing wasted effort.

Scanning and assessing can also help the IT Manager to manage a large patch management workload, particularly when they are just beginning to implement patch management procedures. It is important that IT Managers understand not every patch is equal in severity or criticality. An effective patch assessment report can let them focus on the computers that need immediate attention for severe issues, helping the IT Manager to prevent the worst possible problems as quickly as possible. They can then work through less-critical patch problems using a phased approach.

Use a single source for patches

Often IT Managers complicate patch management by relying on multiple point solutions for deployment - one solution for Microsoft updates, another for Adobe, a third for Mac OS patches, and so on. Many Microsoft-centric businesses rely on their free WSUS product to deploy official patches to their software and operating systems.

But how do IT Managers handle patches for other critical software?

The reality is that businesses are faced with patching not only Windows operating systems and applications, but also vendor and custom applications that Microsoft's WSUS cannot address. Solutions like WSUS do not consolidate management of mixed systems and applications. Nor do they have the ability to expose unmanaged content.

Every time IT Managers introduce a new solution or process into the IT environment, they face new procedures and challenges to maintenance.

We believe it better to have a single patch management solution covering Microsoft, third-party software, PC and Apple hardware and devices, client systems, servers and so on. For many of our customers, a ManageEngine patch management solution is in place to address this challenge.

A single source for patches offers a number of advantages. It helps reduce the complexity of IT infrastructure by consolidating multiple patching solutions. This results in simplified team training and end-user communications and reduces overall operating costs due to consolidated management and effective use of staff.

A single source for patches encourages a more robust security posture overall, with flexibility in proactively addressing issues. It also prepares the business for a varied environment whether this already exists or not.

From experience, Wanstor understands the need for differentiation within IT estates - that one Apple machine, for example, in a multi-user business run on Windows. With the right patch management solution, it doesn't matter - everything is managed from one location.

> A single source for patches encourages a more robust overall security posture

In summary, having the right single source patch management solution in place can make the business more flexible by enabling IT to adopt the technologies it needs without having to worry that it won't be able to keep them patched properly.

Make sure you can roll back

One of the most crucial capabilities IT Managers can add to their patching strategy is the ability to roll back or *undo* patches. The ability to undo updates or changes made by any patch provides the entire IT team with greater peace of mind.

Whether rolled out unintentionally, recalled or instructed not to deploy by parent vendors, a roll-back strategy allowing patch removal simplifies the role of IT.

Additionally, the ability to roll back patches helps simplify the actual rollout process in the first place. With the knowledge that patches can easily be removed, the IT team may feel more comfortable deploying patches that have not been subjected to rigorous testing beforehand.

This results in a reduction of overheads involved in testing patches and the faster deployment of critical patches to end users, while allowing teams to keep the IT estate both reliable and secure.

Using a phased approach

Another way to simplify patch management is to create phased releases. There are a number of reasons to adopt this approach.

Firstly, larger businesses might not have the infrastructure needed to push out a given set of patches to a large population at the same time. A phased release helps avoid bottlenecks and keeps everything moving smoothly.

IT Managers can schedule patch deployments by geographic location, by department or by any other criteria. Orderly, phased approaches can be more easily and effectively communicated to users, who will be less likely to suffer negative impact when they have an expectation of what's coming, and when.

Secondly, not every patch needs to be treated the same. Critical patches may need to be pushed out immediately to computers that are more sensitive to whatever problem the patch addresses. Less critical patches might be able to wait for a regular maintenance period.

Some critical patches might apply only to certain servers, or to certain departments; others might need to be pushed out to the entire business.

Thirdly, phased approaches can help mitigate the need for patch testing. Roll out patches first to trusted users, like members of the IT team or users who've volunteered.

By approaching it this way, users who understand technology can act as part of the patch testing phase, since they're better equipped to deal with patch-related problems and to communicate those problems to IT for resolution.

At Wanstor, we have found the best way to conduct phased patch releases is by means of a policy-driven targeting system. Centrally controlled, top-level policies define target populations, enabling the IT team to be in control at all times. This makes it easier to plan schedules, user communications and other aspects of the overall patch management process.

Improve the administrator experience

One of the more difficult aspects of patch management has always been the IT administrator's experience.

With a proper patching solution, IT administrators should be able to coordinate patch updates across complex and distributed user bases, and have visibility into the patching phases on a machine by machine basis.

Additionally IT administrators need to focus on what has failed, meaning they need reports and alerts that help them concentrate their attention on the systems that require attention.

Reports that identify non-compliant computers, alerts that trigger IT administrator responses to failures and other tools can all help simplify patch management.

Don’t forget the user experience

One reason why patch management can become tedious is its impact on the businesses users. Many users will not understand or know that a patch is coming and why it is important for their PC, laptop or mobile device.

This can often lead to user frustration as they may have to restart their device in the middle of the day for example. When developing a patch management strategy the IT team should take user disruption into account and have a plan in place to placate and educate users.

We believe part of a good user experience is giving users some control over the patching process. Set deadlines that define when a patch must be installed, but give users the ability to postpone the install up to that deadline, or to opt to conduct the installation right away.

For example, end users, particularly those who are remote and mobile with limited time on the actual network, can prioritize their work using system scheduling options for patches requiring reboots.

Communication is also part of a good user experience. Helping users understand that patches are available, when they must be installed, and when they may be installed, all helps reduce negative impact and user downtime, as well as user frustration.

A good patch management process, backed up by appropriate tools, can help make those communications automatic, thereby ensuring a better overall user experience.

Develop solutions of the right size

One reason many IT teams fail to develop a mature patch management policy is the sheer volume of free tools, solutions and approaches that exist in the marketplace.

For example, a massive multinational business with tens of thousands of users and a huge IT department can probably afford the overheads of a large-scale patch management system.

They can afford to assign individual experts to run the system, dedicate infrastructural resources in hosting the system, and invest the time required to plan and deploy a solution. But that does not accurately describe each and every business.

For small or medium sized businesses, quite often they cannot afford dedicated IT staff managing a patch management tool, or devote dozens of computers and massive amounts of network bandwidth to the same. They do not have the time for a long planning and deployment process.

If these businesses deploy the wrong patch management tool or approach, they will find themselves frustrated, overwhelmed, unsuccessful and, more importantly, at risk of security breaches.

It is therefore important to choose a patch management approach and associated tools that fit your business size.

Consider the overhead you're willing to deal with in terms of cost and staff resource, the size of your environment, and the amount of time you have to plan and deploy a solution.

For many businesses, it makes greater financial and IT sense to outsource patch management to a managed service provider who has experience in different patch management tools, techniques and processes, ensuring that the right solution can easily be developed, deployed and managed.

Be organised for success

Proper organisation is critical to effective patch management. Every day, the IT team will receive dozens or even hundreds of software updates. Simply reviewing them, categorising them, and selecting approved ones for deployment can become a full-time job, but how many businesses can afford an IT Manager whose only role it is to look after updates and patches?

In Wanstor's experience not many - if any at all.

The first way to stay organised is to use a single patch management tool that can accommodate the entire IT environment. Seeing all of the patches in one place will enable far better organisation than having to review patch lists across different tools.

Having only one patch management solution also enables IT Managers more control over scheduling patches, and will allow them to set up patch windows with specific guidelines and forced updates to make sure users experience minimal disruption during working hours.

Another way to stay organised is to use tools and processes that embed their own inventory information and intelligence about incoming patches.

If the IT team has a tool that can auto-categorise patches into different levels of severity, or which allows them to choose to download only the operating system and application patches relevant to their network, the need to manage patches that are not applicable can be eliminated, promoting focus on critical and relevant updates.

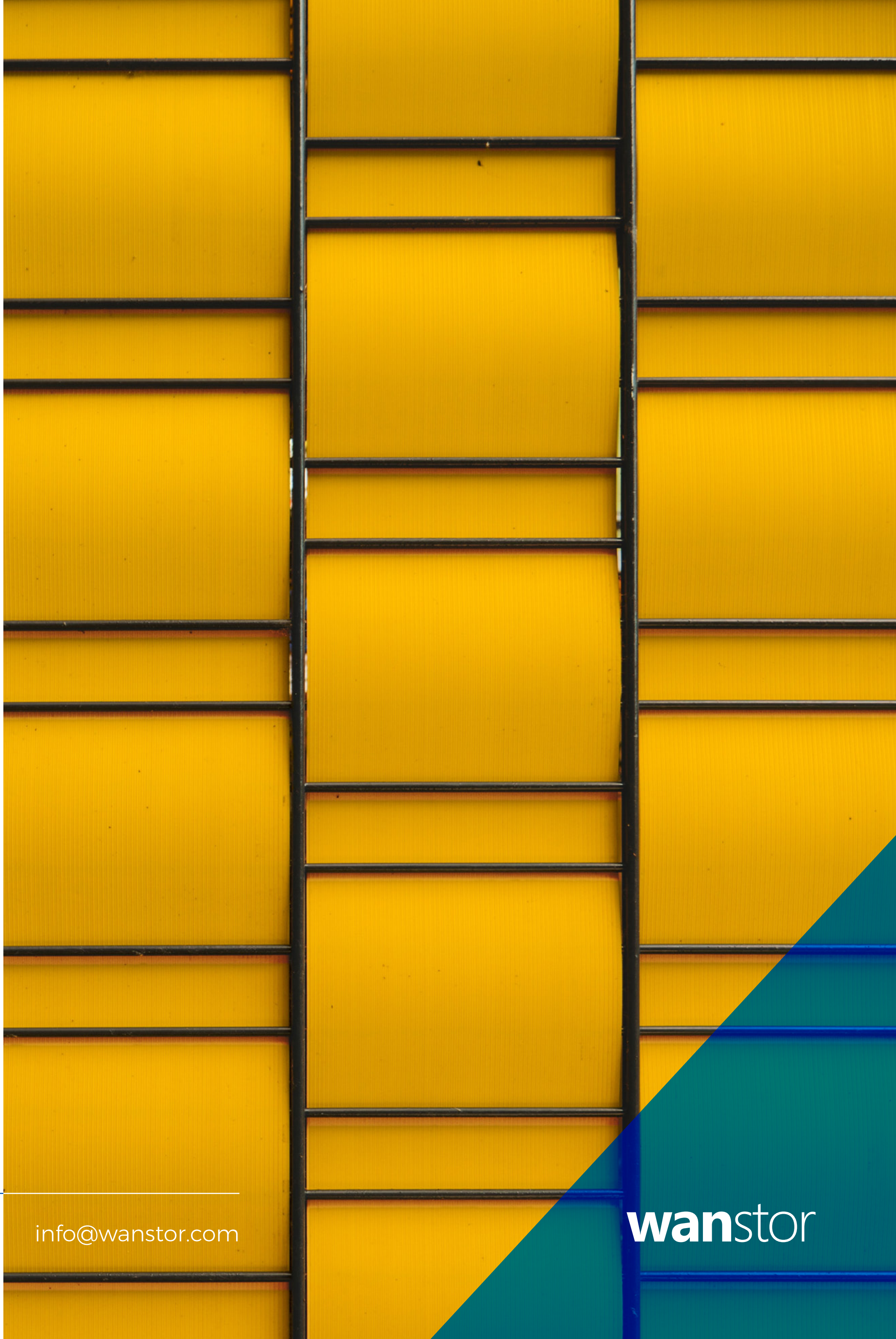
Organising patches by vendor, affected user population and other criteria will also help the business make better decisions about patch deployment, as those decisions will be made faster with less cost and employee overheads.

Final thoughts

At Wanstor, we believe that patch management is crucial to IT security success. Replacing old, ad hoc approaches to patching with a comprehensive, systematic strategy will improve security and reduce the patch management workload.

By following the tips detailed in this article, Wanstor's patch management experts believe that many businesses can eliminate network vulnerabilities, deploy patches in an orderly and controlled fashion, streamline and simplify the involvement required of end users, and improve regulatory compliance, whilst saving the IT team time, money and effort.

For more information on Wanstor's patch management solutions, please call us on **0333 123 0360**, email us at **info@wanstor.com**, or visit us online at **www.wanstor.com**.



wanstor