Patch Management Buyer's Guide

A Guide to Purchasing Patch Management

ninjaOne

Patch Management Buyer's Guide

Technology offers boundless opportunities to make workflows more efficient and accomplish things never thought possible.

60%

The percentage of breaches that could have been avoided with an available patch that wasn't applied. — Ponemon Institute

15 mins

How long organizations have before a CVE is announced before attackers begin scanning for vulnerabilities.
— Palo Alto Networks Unit 42

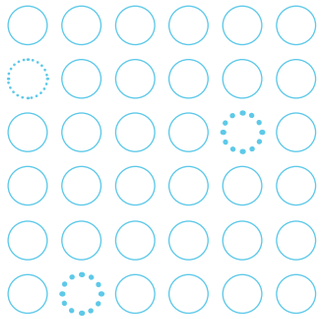
Unfortunately, as organizations add more technology and expand their digital footprint, they leave themselves open to attack. Within the National Vulnerability Database (NVD), there were 26,448 CVEs published last year, an increase of 20% over 2021. Without swift action, unpatched vulnerabilities can become easily exploited, leading to a loss of valuable data, money, and time.

As the vulnerability count shows no signs of slowing, proper patch management has become an absolute necessity. Without one, there are far too many patches to wrangle. And with limited time to act on announced vulnerabilities, managing the process manually is nearly impossible. Organizations that prioritize automating patch management can remediate urgent security flaws and address unexpected performance issues, giving organizations peace of mind. A proper patch management tool can also provide a structured, automated process that will help to remove human error and save time.

If you're reading this guide, you probably already understand the importance of a comprehensive patch management solution, but you may be stuck on where to go next. "Is my current patching method sufficient? What features should I prioritize? What questions should I be asking potential vendors?" In this guide, we'll be answering these questions (and more) with helpful tips and resources you can use along your journey.

Top Reasons IT Looks for New Patching Solutions

Most organizations understand the importance of patch management, they may even have an existing patching process, but how do they know if a new patching solution should be on their list? Here are a few signs that it could be time:



1. They don't have a reliable patching process in place

Without a cohesive patch management process, IT teams often find themselves without visibility or control over patching. Without centralized management, IT teams will rely on end users to patch and reboot their devices when needed, leading to missed patches and unresolved vulnerabilities that IT cannot see.

2. Their current solution no longer fits their business needs

The way businesses operate has changed fundamentally in the past few years, so their current patch management solution may no longer fit their needs. They may need to support the patching needs of remote and hybrid employees, meaning their on-prem solution is no longer sufficient. Or maybe they still have legacy tools in place that need to be replaced. Whatever the case may be, it could be the right time to reevaluate.

continued →

Top Reasons IT Looks for New Patching Solutions

3. Their current solution no longer fits their business needs

The way businesses operate has changed fundamentally in the past few years, so their current patch management solution may no longer fit their needs. They may need to support the patching needs of remote and hybrid employees, meaning their on-prem solution is no longer sufficient. Or maybe they still have legacy tools in place that need to be replaced. Whatever the case may be, it could be the right time to reevaluate.

4. Their organization has new security requirements

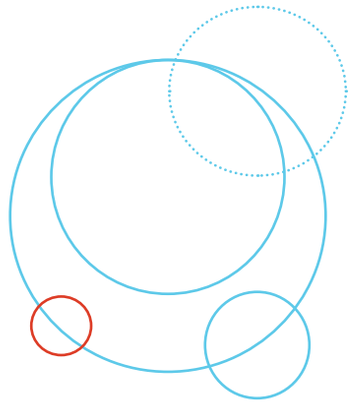
Similar to changing business needs, organizations might have new security requirements as they expand. Often times, certain industries have specific security regulations, so it's important to consider how the current solution is supporting those regulations.

5. Their current solution is no longer performing well

From time to time, it's important for orgs to take a look at their existing tech and determine if it's still performing adequately, or if they need to examine different options. Before diving into new options, they should track performance metrics on the current patch management platform. Some potential metrics to track: patch compliance rate (percent of devices that are fully patched), first pass patch success rate (percent of patches that are applied successfully without intervention), patch coverage (percent of endpoints under management covered by patch solution), and average time to patch.


“Automated patching has transformed our IT estate providing consistency and heightening our security stance to our users.”
- Sam P., IT Infrastructure Manager

How to Evaluate a Patching Solution



If you've determined that a new patching solution may be in your future, here are some key features to consider as you make your decision:

- Operating systems supported
- Third party-applications supported
- Level of patch automation (combine schedules, automation tools)
- Level of patch control
- Patch remediation tools
- Patching data and visibility
- Implementation and management complexity
- Support for hybrid and remote devices
- User interface
- Pricing and subscription options

Operating system requirements

Which operating systems are in your environment that need to be patched? Potential OS requirement could include Windows, Linux, macOS, Windows Server, etc.

Third-party application support

During your research, make a list of the third-party applications you'd like to support and compare it to the list provided by the new vendor.

Level of patch automation

By implementing automation processes into your patching plan, you can quickly patch critical issues and minimize your security risk. A great patch management tool will have a number of automation tools available to identify, analyze, approve, deploying, and validating patches.

Level of patch control

Not all patches are safe to deploy, so your patch management platform should be able to support manual patch approvals and rejections based on your discretion as well as ad-hoc patch deployments to resolve zero-days. Robust alerting on patch failures is also critical to remediated failed patches quickly.

Patch remediation tools

The patching process is always full of challenges, and a new solution should come with a set of patch remediation tools to make your patching journey more efficient. Tools like a remote terminal, patch blocking functionality, a patch uninstall workflow, and registry editor will help you quickly resolve patching issues.

Patching data and visibility

Visibility is critical to effective patch management. Patching dashboards and performance reports are essential to discovering potential vulnerabilities, understanding the criticality of a vulnerability, ensuring your devices are up-to-date, and proving patch status for governance purposes.

Implementation and management complexity

Many patch management tools have a high barrier to entry, leading to greater burdens on IT. These tools are often super complex, hard to implement, and require ongoing maintenance. All of these downsides will end up incurring high costs and decreases in productivity. Investing in a cloud solution is one way to avoid on-prem maintenance costs and extensive training.

Support for hybrid and remote devices

If your organization's tools don't work well for remote employees, require a VPN to work, or add complexity for the end-user you'll achieve lower patch compliance and have more vulnerable devices in the field. In these instances, achieving an acceptable level of patch compliance on takes more time out from IT and reduces productivity for end-users.

User interface

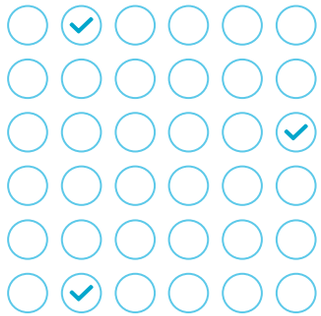
An effective patching solution means little with an interface that's a pain to use. When evaluating new solutions, make sure the interface is intuitive and works for you.

Pricing and subscription options

Pricing will depend on a number of different factors, including payment frequency, feature availability, package types, and more. Keep track of all pricing during your search and figure out how it may fit within your monthly, quarterly, or yearly IT budget.

How NinjaOne's Patch Management Excels

Patch management is a key component of our unified IT management solution, enabling you to consolidate patching into your full IT operations workflow. Here are few reasons why you should add Ninja to your patch management evaluation list:



Fully cloud-based

With the NinjaOne platform, you get a fully cloud-based platform, which means there is little to no overhead and maintenance, infinite scalability, implementation is fast and simple, and you can support distributed offices as well as field, hybrid, and remote employees. You also save money with no hardware, maintenance, or labor costs associated with the infrastructure. On-prem solutions can often be plagued with legacy issues, which can be remedied by using an up-to-date cloud platform.

Windows, Mac, Linux, and 3rd party application support

NinjaOne makes it easy to patch all your endpoints by supporting Windows, Mac, and Linux patch management. You'll likely need to be able to patch more than just operating systems, which means that you can take advantage of the hundreds of third-party applications that are supported by NinjaOne. You can patch any of these apps across all your managed endpoints automatically to remove known vulnerabilities.

How NinjaOne's Patch Management Excels

Comprehensive automation workflow

NinjaOne offers fully automated patching, supporting the patching process from pre-patch to post-patch. You can deploy scripts, automate your patch approval and denial process, automatically generate tickets and notifications, force updates, reboot devices, and more. NinjaOne enables you to automate your entire patching process.

Patch approval profiles

Included in the automation workflow are patch approval profiles, which allow you to customize patching rules based on severity ratings and patch categories. You can choose to automatically approve, automatically reject, or manually approve / reject patches based on their patch category, making most patches zero touch.

Ad-hoc patching actions

In addition to full patch automation, Ninja enables ad-hoc patching actions across individual or groups of devices for fast response to critical issues. Scan, deploy, or uninstall patches at the push of a button to immediately remediate zero-days or rollback bad patches.

Full visibility into patching data

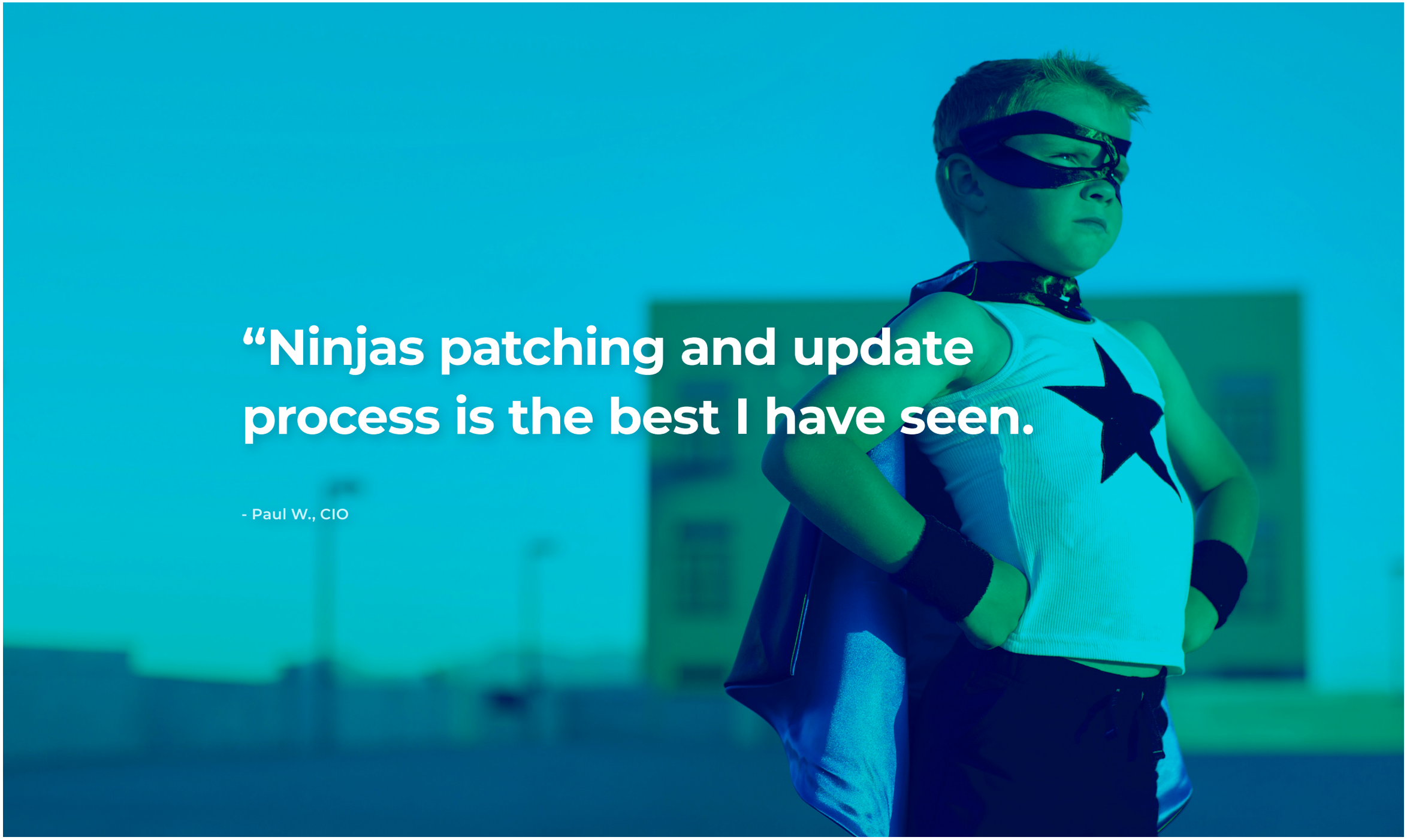
NinjaOne gives you complete visibility into your patching process, so you know the state of all your endpoints at a glance. Ninja provides wide visibility with per-patch and per-endpoint data on known vulnerabilities, including CVE (Common Vulnerability and Exposure) bulletins, CVSS (Common Vulnerability Scoring System) scores, and KB articles. You can easily report on patch compliance status and get proactive alerts on failed or problem patches for faster remediation.

Patch remediation tools

As a unified IT management solution, Ninja includes a suite of tools that help you deliver better patch success rates, including a remote terminal, registry editor, task manager, script deployment tool, and patch rollback utility. When a patch fails, these remote tools help you remediate the issue quickly so you can redeploy the patch and remove the vulnerability.

Real-time device health and performance monitoring

NinjaOne gives you real-time device telemetry data so you can see when the devices were last patched, see if devices are compliant with specific security standards, get proactive alerts and notifications about patching behavior, and understand device states.


“Ninjas patching and update process is the best I have seen.
- Paul W., CIO

ninjaOne

For more information on the NinjaOne patch management solution, check out NinjaOne.com/patch-management.