Pocket Guide to Autonomous Patching

ninjaOne®

NAP Edition

Set it, forget it...nap
optional, but recommended.

Every IT team has lived it: endless manual updates, late-night patch marathons, and the constant anxiety of “what if this patch breaks something?”

Even with scripts, IT can still get stuck in a loop – watching, approving, rebooting, rolling back. That’s not autonomy.

Autonomous patching is the turning point. Instead of being glued to every step, you define the rules and let intelligence + automation run the process.

Let’s NAP – Never Aimlessly Patch (again)

The heart of autonomous patching is simple: define your policies, then let the system carry them out while you focus elsewhere.

Navigate the noise

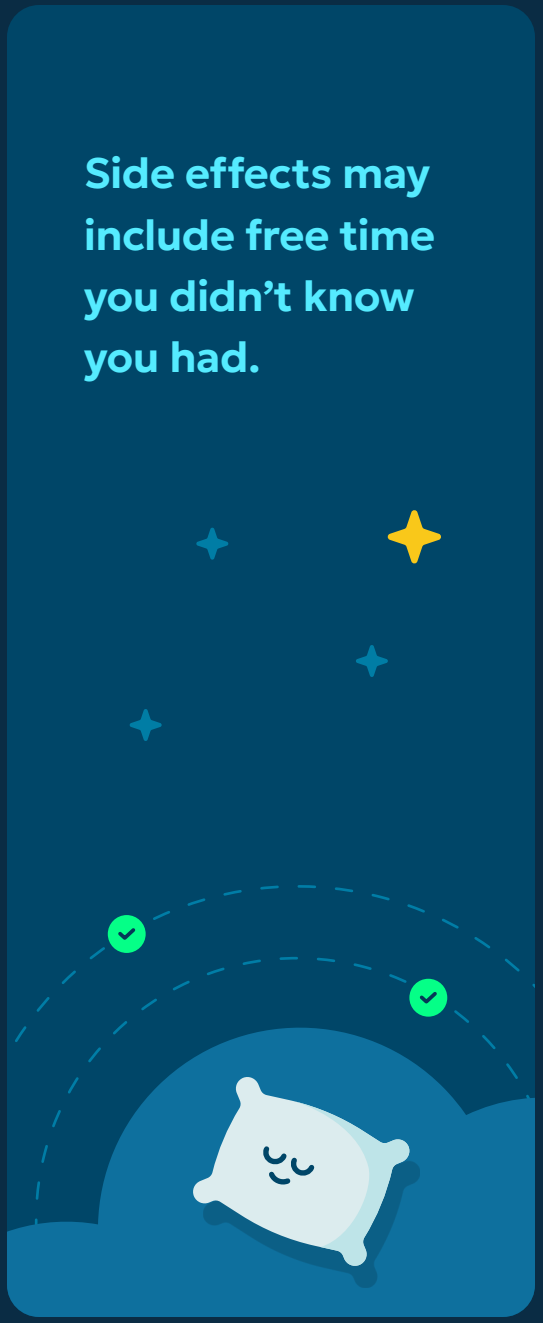
When autonomous patching is done right, critical vulnerabilities are mapped to endpoints automatically, ranked by severity, and surfaced where you can see them directly. No more scavenger hunts across spreadsheets. CVSS scoring thresholds help IT prioritize and patch the “9s and 10s” first, while lower-severity updates fall into a safer cadence.

Automate with intelligence

AI-powered patch intelligence pulls insights from vendors, forums, and telemetry to predict patch stability. Risky updates are paused before they cause trouble. Approval workflows follow your policies, so critical patches move immediately, known-bad KBs are blocked outright, and the rest flow on schedule.

Protect in your sleep

Stable patches move forward as defined by policy automation, and compliance logs and dashboards hum in the background, keeping IT out of panic mode and ready for the next audit without adding manual work.



Patch nightmares vs. Patch dreams

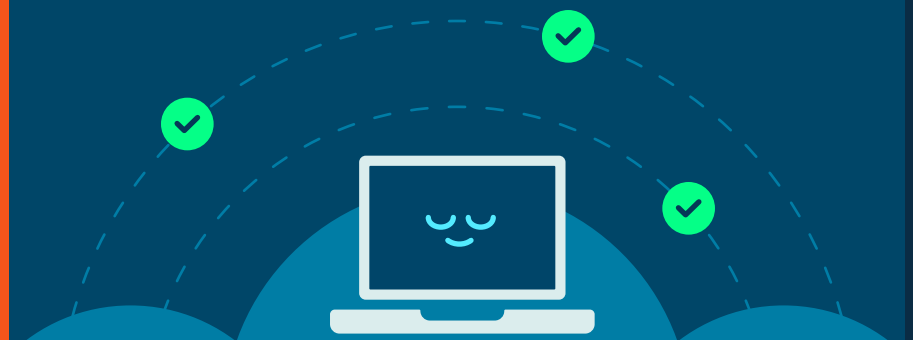
Manual patching keeps IT in survival mode. Automation helps but still demands supervision. Autonomous patching changes the rhythm completely.

Life before autonomy can be a patching nightmare

Every update is a gamble, every cycle eats hours, and compliance is something you scramble for after the fact. You're chasing down CVEs across multiple tools, double-checking patch notes late at night, and stressing out when bad updates hit end users.

Life after autonomy can be a patching dream

Patching becomes a controlled, repeatable process. Updates roll out in safe phases with ring-based deployments, unstable patches are paused by AI before they spread, and compliance reporting is always on. IT stays ahead and gets valuable time back. It's still your process, just lighter, safer, and smarter.



What you gain back

With autonomous patching, you gain more than hours back on the clock. You also get true peace of mind and room to focus on IT strategy instead of babysitting patches.

IT teams gain:

- Hours back every week by cutting out patch babysitting
- Lower risk with faster closure of high-severity CVEs
- Fewer user complaints thanks to intelligent reboot policies
- Audit readiness baked into the process

Just the beginning

If your patch cycles still feel like late night marathons, you don't have to keep running them. Autonomous patching shows what's possible when intelligence and automation do the heavy lifting.

With NinjaOne Autonomous Patch Management, vulnerabilities are mapped instantly, bad updates are blocked before rolling out, and compliance reporting is always on.

Curious how to take the next step? Keep exploring how autonomous patching can free up your team and give you back hours in your workday.

Keep exploring