# Handbuch für autonomes Patching

ninjaOne

## NAP-Ausgabe



Autonomes Patching für
einen gesunden Schlaf

Jedes IT-Team kennt das: Endlose manuelle Updates, nächtliche Patching-Marathons und die ständige Sorge „Was, wenn dieser Patch Probleme verursacht?“

Selbst mit Skripten kann die IT-Abteilung in einer Schleife stecken bleiben: Beobachten, Genehmigen, Neustarten, Zurücksetzen, Wiederholen. Eine autonome Lösung sieht anders aus.

Autonomes Patching ist der Wendepunkt. Anstatt jeden Prozessschritt manuell abarbeiten zu müssen, können Sie die Regeln definieren und den Prozess der Patch-Intelligence und Automatisierung überlassen.

# NAP - Niemals ahnungslos patchen

Der Kern des autonomen Patchings ist einfach: Definieren Sie Ihre Richtlinien, und lassen Sie das System diese ausführen, während Sie sich auf andere Aufgaben konzentrieren.

## Behalten Sie den Überblick

Wenn autonomes Patching richtig in die Praxis umgesetzt wird, werden kritische Schwachstellen automatisch Endpunkten zugeordnet, nach Schweregrad eingestuft und übersichtlich angezeigt. Kein Tabellen-Chaos mehr. CVSS-Schwellenwerte helfen der IT-Abteilung, Prioritäten zu setzen und die kritischsten Schwachstellen zuerst zu patchen, während Updates mit niedrigerem Schweregrad in einem sicheren Rhythmus verarbeitet werden.

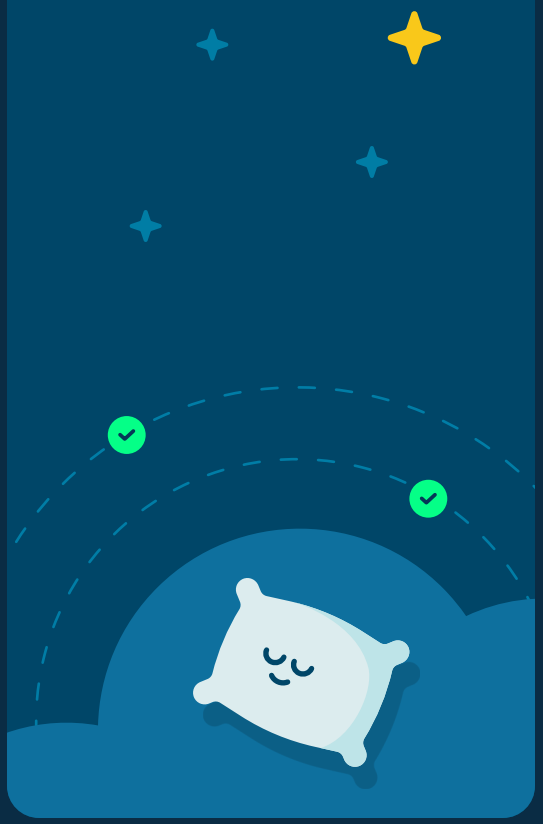
## Intelligence-basierte Automatisierung

KI-gestützte Patch-Intelligence verwendet Erkenntnisse von Anbietern, Foren und Telemetrie, um die Patch-Stabilität vorherzusagen. Folglich werden riskante Updates abgebrochen, bevor sie Probleme verursachen. Genehmigungs-Workflows folgen Ihren Richtlinien, sodass kritische Patches unmittelbar angewendet werden, bekannte problematische Windows-KBs sofort blockiert werden und der Rest nach Plan läuft.

## Sicher auch im Schlaf

Stabile Patches werden gemäß den Vorgaben der Richtlinienautomatisierung bereitgestellt, und Compliance-Protokolle sowie Dashboards laufen im Hintergrund, sodass die IT-Abteilung nicht in Panik gerät und für das nächste Audit bereit ist, ohne dass zusätzliche manuelle Arbeit anfällt.

**Zu den Nebenwirkungen kann Freizeit gehören, von der Sie nichts geahnt haben.**



# Traumhaftes Patching oder Patching-Alptraum

Mit manuellem Patching bleibt die IT-Abteilung im Überlebensmodus. Die Automatisierung hilft, erfordert aber dennoch Überwachung. Das autonome Patching ändert den Rhythmus völlig.

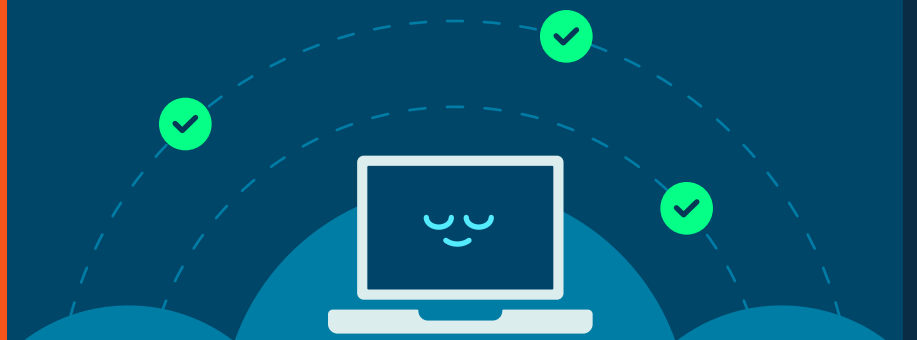
## Das Leben vor der Autonomie kann ein Patching-Albtraum sein

Jedes Update ist mit Risiken verbunden, jeder Zyklus kostet Stunden, und an die Compliance denkt man oft erst im Nachgang. Sie jagen CVEs in verschiedenen Tools hinterher, überprüfen Patch-Hinweise bis spät in die Nacht und sind gestresst, wenn fehlerhafte Updates bei Endbenutzer:innen ankommen.



## Das Leben nach der Autonomie ähnelt einem Patching-Traum

Patching wird zu einem kontrollierten, wiederholbaren Prozess. Updates werden in sicheren Phasen über gruppenbasierte Bereitstellungen ausgerollt, instabile Patches werden durch KI gestoppt, bevor sie viele Endbenutzer:innen erreichen, und die Compliance-Berichterstellung ist immer aktiv. Die IT-Abteilung behält die Kontrolle und gewinnt wertvolle Zeit zurück. Es ist immer noch Ihr Prozess, nur leichter, sicherer und intelligenter.



# Was Sie zurückgewinnen

Mit autonomem Patching sparen Sie nicht nur Zeit ein. Vielmehr schaffen Sie echte Ruhe und können sich auf Ihre IT-Strategie konzentrieren, anstatt sich um Patches zu kümmern.

### Vorteile für IT-Teams:

- Sie sparen jede Woche Stunden, indem sie sich nicht mehr um das Patching kümmern müssen.
- Wegen der schnellen Behebung von CVEs mit hohem Schweregrad entstehen weniger Risiken.
- Dank intelligenter Reboot-Richtlinien werden weniger Benutzerbeschwerden eingereicht.
- Audit-Bereitschaft wird im Prozess berücksichtigt.

# Nur der Anfang

Wenn sich Ihre Patch-Zyklen immer noch wie nächtliche Marathons anfühlen, sollten Sie diese nicht weiter durchführen. Autonomes Patching verdeutlicht, welches Potenzial entsteht, wenn intelligente Automatisierung die Hauptarbeit übernimmt.

Mit NinjaOne Autonomous Patch Management werden Schwachstellen sofort erkannt, fehlerhafte Updates werden vor dem Ausrollen blockiert, und die Compliance-Berichterstellung ist immer aktiv.

Sind Sie neugierig, wie Sie den nächsten Schritt machen können? Erfahren Sie mehr darüber, wie autonomes Patching Ihr Team entlasten und Ihnen mehr Zeit in Ihrem Arbeitsalltag verschaffen kann.

Mehr erfahren

