Patchstack Protection: Overview and how it works

Patchstack · https://www.aeserver.com/support/patchstack-protection-overview/

Patchstack Protection checks every plugin, theme and WordPress core version on your website and mitigates vulnerabilities automatically, sometimes up to 48 hours before they are publicly disclosed. This guide explains why WordPress sites get hacked, how Patchstack Protection stops it, and where to find everything.

Why WordPress sites get hacked

Most hacked websites were never targeted personally. Attackers run automated bots that scan the whole internet for sites running a plugin or theme with a known security flaw. When they find one, the exploit is automatic.

In 2025, 99% of new WordPress vulnerabilities were found in plugins and themes rather than WordPress itself, and Patchstack counted 11,334 new vulnerabilities across the ecosystem, up 42% on the year before. Keeping software updated helps, but there is always a gap between a flaw being discovered and a fix being released and applied. Some flaws never receive an official fix at all.

NoteYou cannot close this gap by hand. Even a well-maintained site is exposed for the days or weeks between a vulnerability being discovered and you applying the update. Closing that gap is the job Patchstack Protection does for you.

What Patchstack Protection monitors

Patchstack Protection is licensed **per website**. On each protected site it checks:

- every installed **plugin** and its version
- every installed **theme** and its version
- the **WordPress core** version

Each is matched against Patchstack's vulnerability database, and checked again whenever your software changes. Patchstack describes itself as the world's #1 WordPress vulnerability intelligence provider. Because the check runs inside your site, it knows exactly which vulnerabilities affect you and which do not.

How it works

1. You activate it once

Order Patchstack Protection from your AEserver client area. If your site is hosted with us the lightweight plugin is installed automatically via your hosting control panel, so there is nothing to configure. Sites hosted elsewhere use the Download Plugin action instead. See Activate Patchstack Protection for the step-by-step guide.

2. Your software is checked automatically

Your plugins, themes and core are matched against Patchstack's vulnerability database, backed by more than 12,000 mitigation rules. New rules are added as vulnerabilities are found, sometimes up to 48 hours before a vulnerability is publicly disclosed.

3. Vulnerabilities are mitigated automatically

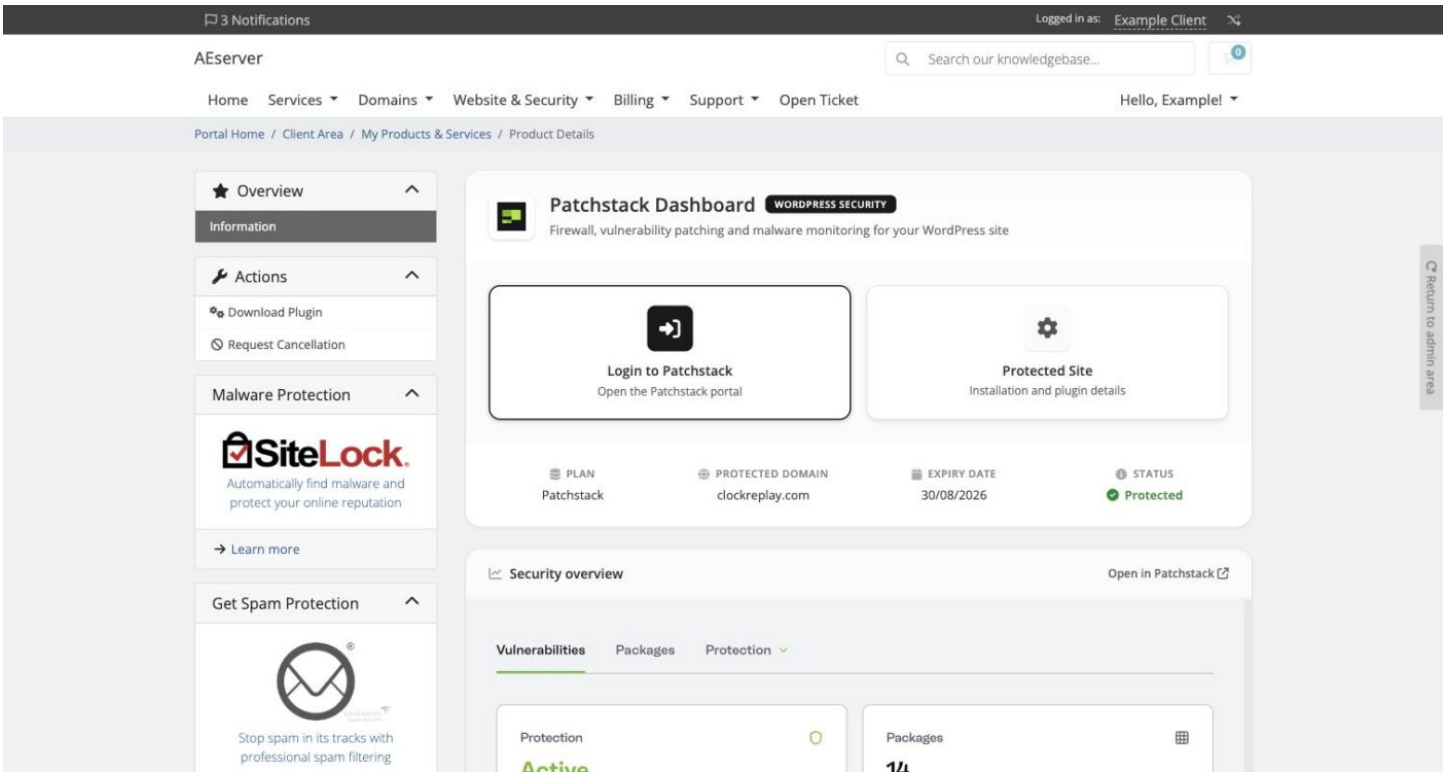
When a high or medium priority vulnerability affects your site, a precise mitigation rule (a vPatch) deploys automatically and blocks exploit attempts. Your plugin and theme code is never modified, so the rule itself cannot break your site. You then apply the official update on your own schedule, protected in the meantime.

Where to find it

Sign in to your AEserver client area, open **My Products and Services**, and select your Patchstack Protection service. From there you can reach:

Shortcut	What it does

Login to Patchstack	Opens the full Patchstack portal for your site.
Protected Site	Shows which WordPress installation is protected, the plugin version and when it last synced.
Security overview	Shows protection status, detected vulnerabilities, threats blocked and reports, right on the service page.
Download Plugin	For sites hosted elsewhere: downloads the plugin to install on your WordPress site.
Request Cancellation	Cancels the service for that website.



Your Patchstack Protection service in the AEserver client area.

Why the intelligence behind it matters

Protection is only as good as the vulnerability data behind it, and this is where Patchstack differs from a general-purpose firewall.

- Patchstack is a registered **CVE Numbering Authority** and describes itself as the largest processor of open-source vulnerability intelligence, so it is frequently the first organisation to know a vulnerability exists.
- Patchstack can mitigate vulnerabilities **up to 48 hours** before they are publicly disclosed, so protected sites can be covered before the details are public.
- Mitigation rules are triggered **only on demand**, for software you actually run, rather than loading a generic rule set on every request.

That last point is why the performance cost is negligible. Patchstack publishes these figures for the overhead per request on its RapidMitigate page:

PHP version	Rules deployed	Mean time	Memory
PHP 7.x	1	0.08 ms	0.7 KB
PHP 7.x	10	0.35 ms	0.7 KB
PHP 8.x	1	0.04 ms	0.33 KB
PHP 8.x	10	0.06 ms	0.33 KB

For context, that is a fraction of a millisecond on a page that typically takes several hundred. Patchstack reports this approach as up to 10x less resource-intensive than generic pattern-matching solutions, with a near-zero false positive rate.

What it does not do

ImportantAn alert does **not** mean your site was hacked. In most cases it means a vulnerability was found and **already mitigated**. The alert simply lets you know so you can apply the official update when convenient.
Patchstack Protection prevents hacks; it does not remove malware from a site that is already compromised. If you believe your site is already infected, contact AEserver support first and we will guide you through clean-up options before enabling protection. It also does not replace backups: backups protect you against data loss from any cause, and we recommend keeping them active alongside protection.

Glossary

Vulnerability

: A security flaw in a plugin, theme or WordPress core that attackers can exploit to take over or damage a site.

Exploit

: The specific technique attackers use to take advantage of a vulnerability.

Mitigation rule (vPatch)

: A precise rule that blocks the way a vulnerability is exploited, applied at runtime without changing your plugin or theme code.

Zero-day

: A vulnerability being exploited before an official fix exists. Mitigation rules can cover these.

Public disclosure

: The moment a vulnerability is announced publicly. Protection can land up to 48 hours earlier.

Hardening

: Extra safeguards that block common WordPress attack patterns, such as attempts to upload PHP files or give a user administrator rights.

IP blocklist

: A list of IP addresses known for attacks, built from activity across the Patchstack network. Requests from these addresses are blocked.

License

: Your per-website subscription. Each protected site has its own license key and dashboard.

Get Patchstack Protection Set up takes minutes and protection runs continuously in the background. See pricing and get started.