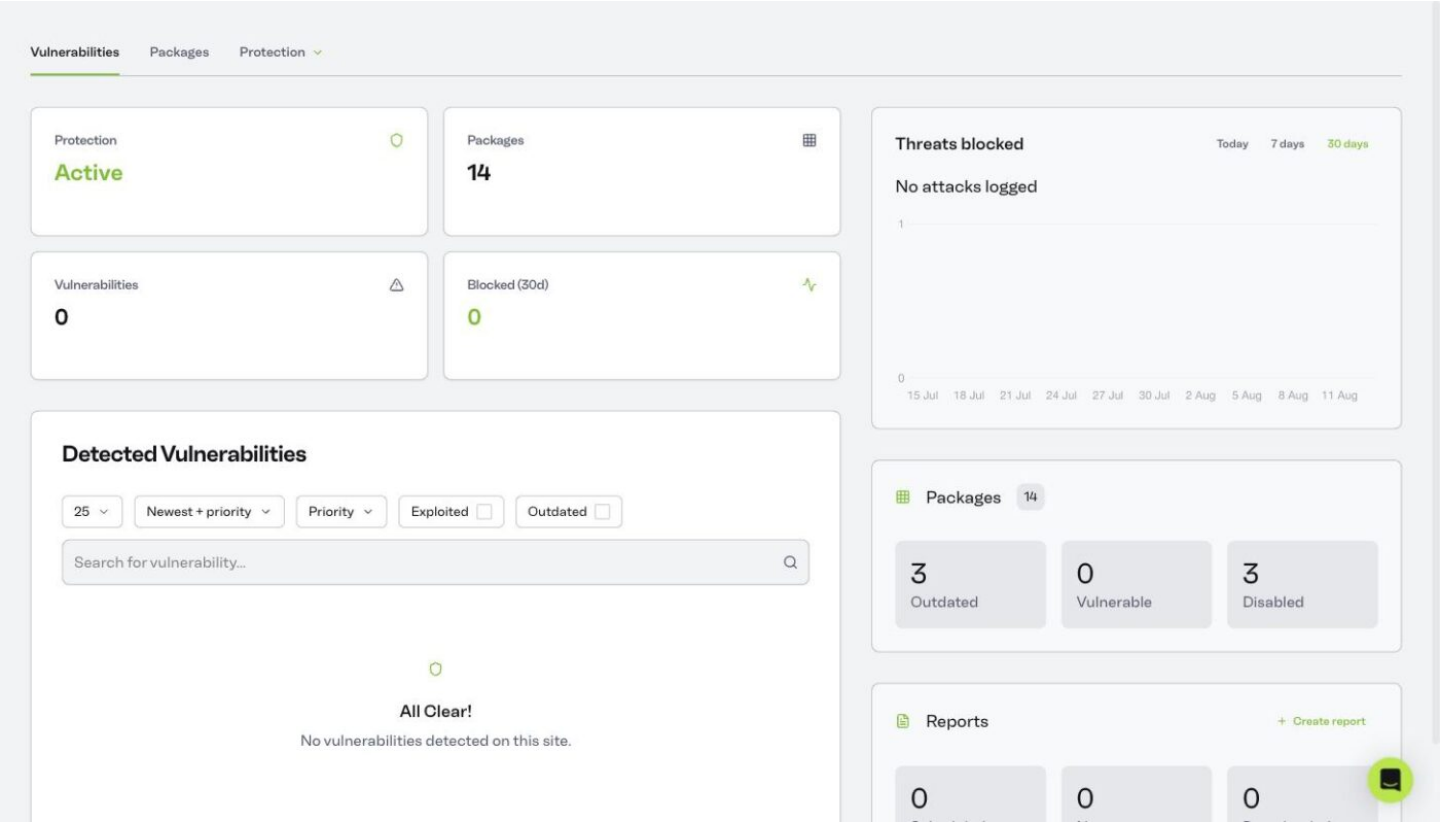
Patchstack dashboard, alerts, and reports

Patchstack · https://www.aeserver.com/support/patchstack-dashboard-alerts-reports/

Your Patchstack dashboard gives you an up-to-date view of your site's protection. You can see it as the Security overview on your service page in the AEserver client area, or open the full portal with **Login to Patchstack**. This guide explains what each part means, how to read a vulnerability entry, and how reports work.

The dashboard at a glance

Area	What it shows
Protection	Confirms protection is active on your site.
Vulnerabilities	How many known vulnerabilities currently affect your site.
Blocked (30d)	Threats blocked in the last 30 days, with a Threats blocked chart for today, 7 days or 30 days.
Packages	The plugins and themes on your site, including how many are outdated, vulnerable or disabled.
Detected Vulnerabilities	The vulnerabilities found, which you can filter by priority, exploited or outdated.
Protection tab	The modules protecting your site and any banned IP addresses.



The Patchstack dashboard for a protected site.

Reading a vulnerability entry

When a vulnerability is found on your site, it is listed under Detected Vulnerabilities. Entries are prioritized by real-world risk, so you can focus on what matters instead of being flooded with noise. A typical entry tells you:

- which plugin or theme is affected, and the vulnerable version
- its priority, and whether it is known to be exploited
- whether a mitigation rule is already protecting you (in most cases, it is)
- the recommended action, usually to update when convenient

NoteA listed vulnerability does **not** mean your site has been hacked. In most cases it means a vulnerability was found and **already mitigated**. It is there so you can apply the official update on your own schedule.

Hardening and the IP blocklist

Alongside mitigation rules, two more modules protect your site automatically. An advanced hardening module blocks common WordPress attack patterns, such as attempts to upload PHP files or give a user administrator rights, and a community IP blocklist blocks requests from IP addresses known for attacks. There is nothing to switch on.

NoteUnder **Protection** you will find the modules protecting your site and any banned IP addresses. If you have a question about a setting, contact our support team.

Reports

Use **Create report** in the Reports panel to produce a summary of what was found, mitigated and blocked over a period. Reports can also be scheduled to run weekly or monthly. They are useful for your own records, for compliance evidence, and for agencies showing clients the value of the protection in place.

TipManaging client sites? Forward the periodic report, or export it as part of your maintenance reporting. Each site has its own dashboard and report.
Get Patchstack Protection Not protected yet? See pricing and get started.