SERVER SECURITY, ANY STACK

Your servers under our watch.

Patched before the next alert, with a report every month. We take over the security of the servers your site or service runs on. Any stack, from $290 a month.

FOR

Business owners
Site or service on its own servers

GUARANTEE

The repair on us
if we miss a fix

PLAN

Monthly
any stack · from 3 months

BUDGET

From $290
per month · one site

01 Security Watch – in plain words.

We take over the security of the servers your site or service runs on. Every month we install the updates in an agreed window, watch the security alerts for the versions you run, fix critical holes fast and send a **report in plain words**.

Not only PHP. Whatever runs on your servers, we keep it patched and watched: Linux, nginx or Apache, PHP, Java, Node.js, Python, Docker images, WordPress and custom code.

02 Why it matters – new holes every month, and nobody on your servers.

- **New holes every month.** PHP ships security fixes every four weeks. On 17, 18 and 19 November 2026, OpenJDK, nginx and PHP each fixed serious flaws, and PHP alone fixed 17, seven of them critical.
- **Attackers move faster than updates.** The PHP2Shell flaws were fixed on 21 October 2026. Five days later, CISA added them to its list of vulnerabilities already used in attacks.
- **Nobody owns the servers.** The developer who set them up has moved on. Your hosting does not update what runs on your server. And the version on the screen often stays the same after a fix, so you cannot tell what is closed.
- **What a missed fix costs.** A stranger's page instead of your site, a Google warning in front of your customers, and leads that never reach you.

It happens – on 20 October 2026 we found attackers' pages on the site of a former client that was no longer on our support. By mid November the owner had replaced the whole site with a placeholder. Nobody was watching its server.

03 Our solution – we take over the security of your servers.

Patched and watched, on any stack

EVERY MONTH

- **A starting audit.** Three business days. Access, a full list of what runs on your servers, a backup, missing fixes, unsupported versions and signs of a break-in, then the first patch window and a starting report.
- **A monthly patch window.** On an agreed day we install the updates, restart the services one by one and check your pages, forms and admin.
- **A watch on security alerts.** Between windows we follow the security alerts for the exact versions you run.
- **A fast fix for a critical hole.** A critical fix does not wait for the window. A hole already used in attacks is fixed within one business day after the fix comes out, any other critical hole within three business days. Then we confirm the hole is closed.
- **A monthly report.** What we updated, what we checked and what needs your decision, in plain words.
- **Any stack.** nginx or Apache, PHP, Java, Node.js, Python, Docker images, WordPress and custom code.

04 The result – patched before the next alert, not after a break-in.

One team answers for the security of your servers, so you do not have to think about it.

- ◯ **Your servers patched before the next alert.**
- ◯ **A monthly report** you can forward to a partner or your accountant.
- ◯ **Your site keeps working:** every update with a backup and a check.
- ◯ **One team** that answers for the security of your servers.

05 Proof – we already do this for our clients.

When the PHP2Shell flaws came out, we checked every PHP site we have built: **20 clients, 23 domains**.

When a critical vulnerability comes out, we check the servers, install the fixes and confirm the hole is closed. The full story of the November alerts is in our article at owlab.group/our-blog/post/php-security-release-november-2026.

06 Our guarantee – if we miss a fix, the repair is on us.

OUR GUARANTEE

If your site goes down or gets broken into through a hole we should have closed, **we fix it or restore it from the backup at no cost.**

07 How we start – from your site address to a monthly watch.

From the first look to every month

THREE STEPS

- **1. Send us your site address.** We look at it from the outside for free and tell you what we see.
- **2. The starting audit.** Three business days: a full picture of your servers, the first patch window and a starting report.
- **3. Every month.** Updates in the window, a watch on alerts between windows, and a report at the end of the month.

08 Price – one monthly plan.

For one site and the server it runs on. The contract runs from three months.

$290	**Security Watch, one site** The site and the server it runs on: the patch window, the watch on alerts, critical fixes, the monthly report and the repair on us if we miss a fix.	PER **month**
+$190	**Each next site or server** Added to the same plan.	PER **month**
$350	**Starting audit** Free when you pay the first three months ahead.	ONCE **at start**

BUDGET — From $290 USD · per month

For comparison – one emergency PHP upgrade with us costs $490 per site.

09 Terms – in plain words.

- **Contract.** From three months.
- **Critical fixes.** A hole already used in attacks is fixed within one business day after the fix comes out, any other critical hole within three business days.
- **Guarantee.** If your site goes down or gets broken into through a hole we should have closed, we fix it or restore it from the backup at no cost. The guarantee covers the repair and the restore, not lost sales.
- **Not included.** Moving to a new major version, for example from an old PHP that no longer gets fixes, and cleaning up a server broken into before we took it over. We price them separately after the starting audit.

10 Common questions – we hear.

- **Why every month, and not only when something breaks?** Critical holes now come out every few days. A monthly window keeps the regular updates in order, and the watch catches the critical ones in between.
- **Which stacks do you take?** Any stack on Linux servers: nginx or Apache, PHP, Java, Node.js, Python, Docker images, WordPress and custom code. The starting audit lists everything that runs there.
- **How do you know a fix is really installed?** We check the fixed package from the vendor or your Linux distribution, not only the version number. Distributions often ship a fix without changing that number. The monthly report lists what we checked.
- **Will updates take my site down?** We install updates in the agreed window and restart the services one by one, then check that the site works. If an update needs downtime, we tell you before.
- **Can we start with one urgent fix?** Yes. Send us your site or server address. We look at it from the outside today and tell you what needs fixing.

11 Next step – send us your site address.

We look at it from the outside for free and tell you what needs fixing first. The number is named before you pay.

WRITE TO

vitaliy@owlab.group
FOUNDER AND CEO

OR BOOK A CALL

owlab.group/services/security-watch
ASSISTANT OR A SHORT FORM