

How we keep your membership site secure

What we do on every site we look after, what we add when a breach would really hurt, and what happens if something does go wrong. Written to hand to your board, your IT lead or your insurer.

STANDARD

ON EVERY SITE WE LOOK AFTER

A firewall that blocks known attacks before the fix ships

Patchstack by default. When a flaw is disclosed in a plugin you run, its virtual patches block known attacks on that flaw while the vendor is still writing the fix. Wordfence where Patchstack doesn't fit.

Daily vulnerability checks

Each managed site is checked every day for plugins and themes with known flaws. The results land in our team's Slack, not in an inbox nobody reads.

Updates tested before they reach you

We update a staging copy first, then test the parts that earn you money: login, checkout, renewals and members-only content.

Admin access you can account for

When we take a site on, we review everyone with admin rights and remove the accounts nobody can explain.

When a plugin flaw makes the news, we check your site

When a serious flaw hits a plugin our clients use, we check every affected site and tell you what we found. We did this across our client sites when BuddyBoss disclosed a critical flaw in March 2026.

ON REQUEST

WHEN A BREACH WOULD REALLY HURT

Admin behind a private network

Only people connected with a key we issue can reach the WordPress login and admin screens. Members sign in as normal. A stolen admin password is no longer enough to get into your dashboard.

A locked file system

The server can read your site's code but can't change it, so an attacker can't quietly install a plugin or rewrite your theme. Code changes go through us.

Git-based deployment

Every code change is versioned, with a record of who changed what and a clean way to roll back.

Two-factor login and scoped vendor accounts

Two-factor login for every admin. Your agency or contractors get named accounts with only the access their job needs.

A banned-plugin list

No database browsers, file managers or run-any-code plugins. Each one hands direct access to your data or files to whoever controls an admin login.

IF YOUR SITE IS COMPROMISED

Lock everyone out first

We reset every password and sign everyone out by rotating the site's security keys.

Find out what changed

We trace the intrusion through the logs the site has, remove what the attacker added, and close the way they got in.

A written debrief

What happened, how it happened, what we fixed, and what we recommend so it doesn't happen again, written so you can hand it to your board.

IF WE HOST YOU ON MEMBERHOST

Your own isolated environment

Your site runs in its own environment, walled off from every other client's.

Traffic filtered before it reaches your site

Cloudflare sits in front of your site, with a firewall at the server as a second layer.

Hosting is optional. If you host elsewhere, we check which of these your host supports.