

# Dependabot vs Renovate

A vendor-neutral technical comparison for security teams | August 2026



[konvu.com/compare/dependabot-vs-renovate](https://konvu.com/compare/dependabot-vs-renovate)

**TL;DR** Dependabot is a GitHub-hosted service you configure with a short YAML file. Renovate is an open-source job you can run anywhere, with 200+ documented options and native support for GitLab, Bitbucket, Azure DevOps and Gitea. Both are free for the primary use case. Renovate's free hosted tier allows one concurrent job on a four-hour cycle.

## Head-to-head overview

| Category         | Dependabot                                                                                                                                         | Renovate                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Deployment       | GitHub-hosted service, GitHub only. The dependabot-core engine is MIT and supports GitLab, Bitbucket, Azure DevOps and CodeCommit at library level | Mend-hosted app (GitHub and Bitbucket Cloud only) or self-hosted anywhere. Source is AGPL-3.0-only      |
| Configuration    | One dependabot.yml per repo. No preset inheritance. 6 match dimensions for groups                                                                  | 200+ options, four-layer config hierarchy, shared presets via extends. 19 packageRules match dimensions |
| Automerge        | No config key exists. Repo-level auto-merge plus a dependabot/fetch-metadata Actions workflow you maintain                                         | Native automerge, conditions live in the same config as everything else                                 |
| Release cooldown | cooldown, default-on at 3 days since 2026-07-14. Security updates exempt                                                                           | minimumReleaseAge, opt-in (defaults to null) but configurable per packageRule                           |
| Ecosystems       | 38 named managers across 33 package-ecosystem values                                                                                               | Over 100 manager modules                                                                                |
| Arbitrary files  | Hard-coded updaters only (pre-commit, rust-toolchain, flake.lock, vcpkg). No user-defined regex                                                    | customManagers with customType: point a regex at any file and extract a version                         |
| PR limits        | 5 open version PRs per ecosystem. Security PRs have a separate limit of 10. Defers rather than drops                                               | prConcurrentLimit 10, prHourlyLimit 2 by default                                                        |

## Where one side is materially deeper

| Capability           | Dependabot                                                | Renovate                                                                                                                         |
|----------------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Platform reach       | GitHub only as a product, including GHES                  | GitHub, GitLab, Bitbucket, Azure DevOps, Gitea, Forgejo, Gerrit. Dependency Dashboard unsupported on Azure, Bitbucket and Gerrit |
| Org-wide policy      | Per-repo YAML. Still no org-level dependabot.yml          | One preset repo inherited by every other repo. Changing the preset changes the org                                               |
| GitHub Actions       | GitHub repo syntax only. No docker:// or GHCR action refs | Also Gitea/Forgejo, SHA256, ratchet: comments, and with: version inputs                                                          |
| Vendoring            | Supported for Yarn v2+, Go modules and Bundler            | Not supported                                                                                                                    |
| Malware alerts       | GA across 8 ecosystems (2026-07-28)                       | Experimental and off by default                                                                                                  |
| Post-update commands | No equivalent                                             | postUpgradeTasks, self-hosted only, gated by an allowedCommands allowlist                                                        |

## Cost: list price is zero for both, so the difference is elsewhere

| Item              | Dependabot                                                                                                      | Renovate                                                                                      |
|-------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| The tool          | Free on every plan and repo type. GitHub does not bill Dependabot's own update jobs                             | Free. Self-hosted under AGPL, or the Mend hosted free tier                                    |
| Free tier ceiling | Runs on GitHub infrastructure, no published per-org limit                                                       | 1 concurrent job, 4-hour cycle, 30-minute timeout, 1 vCPU / 3GB                               |
| What costs money  | Dependency review, security overview and custom auto-triage rules need GitHub Code Security at \$30/commiter/mo | Enterprise Cloud adds 16 concurrent jobs, hourly runs, Merge Confidence Workflows and support |

## When to pick which

### Pick Dependabot when:

- You are on GitHub and want updates running today
- Zero-config security updates and a 3-day default cooldown are enough
- Native security tab and dependency graph context matter
- Nobody on the team owns dependency tooling as a job

### Pick Renovate when:

- Repo count is high enough that preset inheritance pays for itself
- You are not on GitHub (budget for self-hosting off Bitbucket Cloud)
- Version strings live outside manifest files (customManagers)
- You want automerge policy in config, not in an Actions workflow