DevCorp

MANAGED HOSTING

RECOMMENDED MANAGED PRODUCTION PLATFORM

Managed Hosting: Professional

A stronger operations package for production systems with real users, payments, and daily business workflows.

Professional adds the controls most customer-facing applications need: staging, off-site backups, deeper monitoring, access reviews, clearer maintenance process, and more complete incident handling. It is the recommended baseline when downtime, payment failures, or data loss would create business impact.

Service model

Managed hosting

Package

Professional

Document

Version 1.0 - 2025

Package Overview

Professional adds the controls most customer-facing applications need: staging, off-site backups, deeper monitoring, access reviews, clearer maintenance process, and more complete incident handling. It is the recommended baseline when downtime, payment failures, or data loss would create business impact.

Best fit

- Paid services, subscription products, and customer portals
- Internal teams that rely on the platform every day
- Organisations that need controlled releases and stronger recovery practices

Plain-English value

- The infrastructure is monitored and maintained by DevCorp.
- Operational responsibilities are defined before production use.
- Technical controls can be expanded as risk, traffic, or compliance needs grow.

Production discipline

Staging, runbooks, backups, and alerting reduce release and operations risk.

Better visibility

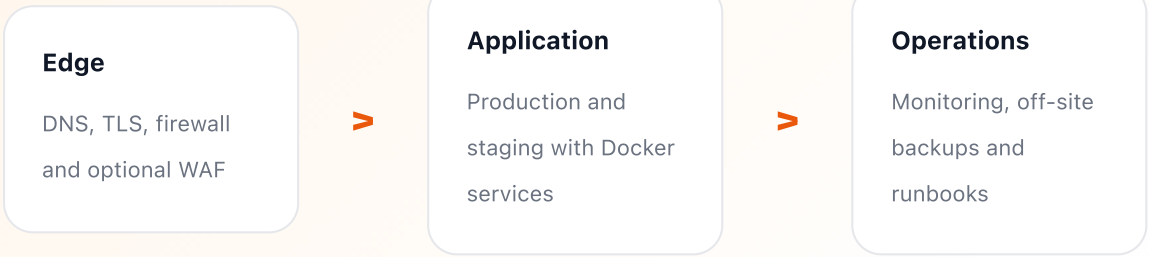
Monitoring includes the application, database, SSL, backups, and public endpoints.

Security maturity

Firewall policy, access review, patch handling, and optional WAF become part of routine service.

Reference Architecture

The architecture is chosen to match the operational risk of the package: simple where simplicity is safer, layered where availability and control matter more.



Technical foundation

- Primary EU production VM sized with database and deployment headroom
- Separate staging environment for release validation
- Host nginx for TLS, static assets, and reverse proxying
- Docker Compose for application, database, and optional queue worker
- Off-site backup target such as Hetzner Storage Box or S3-compatible storage

Compute Platform

We choose the compute platform based on compatibility, stability, and cost/performance. AMD/x86 is usually the safest default; ARM is considered when dependencies and container images are validated.

Platform

AMD/x86 VM is preferred for broad compatibility. ARM can be used for staging or stateless services after dependency checks.

Sizing

Typical starting point: 4 vCPU, 8 GB RAM or larger depending on database size, concurrency, and background jobs.

Scaling

Vertical resize first; split database, workers, or static delivery when monitoring shows pressure.

AMD / x86 strengths

- Best default for PHP, Node.js, MySQL, Docker images, and broad package compatibility.
- Predictable choice for production systems with third-party binaries or legacy dependencies.
- Dedicated or performance-class AMD nodes are preferred for sustained production load.

ARM strengths

- Good cost/performance for compatible stateless services, workers, and staging systems.
- Requires image and dependency validation before production use.
- Usually introduced after the baseline environment is stable and measurable.

Security and Firewall Layers

Security is built in layers: public traffic controls, server firewalls, restricted operator access, secret handling, patching, and optional WAF or VPN controls.

Firewall and access controls

- Cloud firewall with explicit inbound allow-list
- Host firewall with matching least-privilege rules
- Restricted SSH source ranges or VPN/bastion option
- Optional Cloudflare WAF/CDN with rate limiting and bot controls
- Private networking where supported for backup or internal services
- Documented access review for operators and deployment keys

Security baseline

- Least-privilege access for operators and deployment paths
- Secrets stored outside source control
- TLS certificates managed and monitored
- Security updates handled through planned maintenance
- Suspicious login and brute-force activity monitored where applicable

Monitoring, Backup, Operations

A managed service is only useful when it can be observed, recovered, and operated consistently. This package defines what is watched, what is backed up, and how routine operations are handled.

Monitoring

- Everything in Essential
- Database connectivity, slow growth indicators, and disk pressure
- Frontend, admin, API, webhook, and health-check endpoints
- Backup success/failure alerts
- Monthly uptime, capacity, and incident summary

Backup and recovery

- Daily database backups with off-site retention
- Server snapshot or image strategy for faster rebuilds
- Documented restore procedure
- Periodic restore test available as included scope or add-on
- Retention policy agreed during onboarding

Operational support

- Extended business-hours support
- Priority handling for production incidents
- Planned release support
- Maintenance communication before disruptive changes
- Monthly operations review and recommendations

Support terms in brief

- Extended support hours and production incident priorities are agreed during onboarding.
- Critical production incidents receive priority handling within the support window.
- Out-of-hours response can be added for critical incidents.

Add-ons and Boundaries

The package can be extended with add-ons. Boundaries are intentionally explicit so customers understand which risks are covered by the selected service level.

Available add-ons

- Warm disaster recovery environment in a second region
- 24/7 critical incident support
- Advanced log aggregation and dashboards
- Cloudflare Pro/Business WAF package
- Quarterly security review
- Long-term audit log retention

Important boundaries

- Primary production remains single-region unless disaster recovery is added
- High-availability database clustering is not included by default
- 24/7 response is an add-on or Enterprise feature
- Major architecture changes are scoped separately

Not included by default

- New product features and application refactoring are scoped separately.
- Third-party service subscriptions, cloud overages, and paid security tools are not bundled by default.
- Formal audits, penetration tests, and legal compliance reviews are optional add-ons.

Shared responsibility

- DevCorp manages the hosting platform, monitoring, backups, and agreed operational processes.
- The customer remains responsible for business content, third-party account ownership, and timely approval of changes.
- Final support windows, response targets, and legal commitments are defined in the service agreement.

Typical onboarding path

- Confirm application architecture, domains, DNS, secrets, integrations, and expected traffic.
- Select compute platform, region, backup target, firewall model, and monitoring scope.
- Deploy the environment, run smoke checks, validate backups, and document access.
- Agree support contacts, maintenance windows, incident priorities, and escalation path.