

Deployment Architecture

Cargovate — supply chain and asset lifecycle, deployable on infrastructure you control.

Generated 2026-10-02 from Cargovate 7c2bd3e. Every figure in this document was read from the running system at build time, not transcribed.

1. Three deployment models

Model	Where it runs	Chosen by customers who
Managed cloud	Our infrastructure, the European Union (Finland). Shared, with tenants separated in the database (§2).	Want no infrastructure of their own.
Managed dedicated	Our infrastructure, one isolated stack per customer — their own database, credentials, backups and upgrade window.	Need physical separation but not their own operations team.
Self-hosted	Your servers, your VPC, or a site with no internet connection at all.	Have data residency obligations, or no outbound connectivity.

Managed dedicated and self-hosted run the **same artifacts** as the managed cloud. There is no reduced edition: the difference is where the stack runs and who operates it.

2. How tenants are separated

In the managed cloud, separation is enforced by the database rather than by application code. Of 141 tables, **89 carry a row-level security policy**, and every one of them is marked `FORCE ROW LEVEL SECURITY` — which means the policy binds even the table's owner, not only ordinary users. The application connects as a role that cannot bypass it.

The boundary has one definition per dimension, expressed through named functions, rather than a predicate copied into every table. Three automated guards assert it, and they run in the build.

How to check this yourself. In a trial or a self-hosted install, connect as the application role, set the tenant context to organisation A, and select from any shipment table. Rows for organisation B are not filtered by the query — they are not returned to the connection at all.

On managed dedicated and self-hosted there is one tenant per database, so the question does not arise.

3. Running with no outbound connectivity

The application talks to its database and — only if you configure them — to destinations you choose: an anchoring endpoint, where alerts and email are delivered, and the carrier tracking APIs you connect

with your own keys. With none configured it calls nothing else: no analytics, no error reporting, no licence check, no update ping.

A licence is verified **offline**, by signature. Nothing phones home to validate it, which is what makes an air-gapped installation possible at all. Updates arrive as a signed release bundle, verified against a public key held on the installation before anything is applied.

The limit of that claim, stated plainly. A build-time guard fails our build if the API's source gains an outbound call, and a test deliberately plants one to prove it catches it. The background workers that deliver alerts and poll carriers call only destinations you have configured. The guard cannot tell you what a third-party dependency does at runtime. A genuine air-gap guarantee is enforced by your network policy, egress-denied by default. We give you a codebase that does not fight it; your firewall is what proves it.

4. The audit trail

Every privileged action is recorded — reads and refusals, not only writes — with the actor, the credential used, the route, the outcome and the source address. Records are append-only by privilege: there is no update or delete policy on the table, so the application's own credential cannot rewrite history.

Each entry carries a hash of the one before it. Removing or altering a record breaks the chain, and the break is detectable by a request any customer can make against their own trail.

How to check this yourself. Export your audit trail, then ask the system to verify the chain. It reports whether the sequence is intact and where it is not. Tampering is designed to be *detectable*, not impossible — a distinction worth insisting on from any vendor who claims otherwise.

5. Your data, and getting it back

Operational data you enter remains yours. While your account exists — including while it is read-only for non-payment — you keep full read access, and you can export your audit trail and a shipment's compliance record from within the product. A complete copy of your organisation's data is available on request.

That export is produced by a tool that connects as a role which cannot bypass row-level security, so the boundary that separates tenants in normal operation is the same one that scopes the extract. It ships with a manifest naming every table included, every table excluded and why, and every column withheld.

Withheld deliberately: credential material — password hashes, second-factor secrets, recovery codes and passkeys. It is of no use to you and a copy of it is a liability to whoever holds the archive. The manifest names every column withheld, so nothing is missing silently.

6. Modules

Capabilities are licensed per organisation and can be switched off. Core is always present; every other module is optional, and **a module you have not licensed is not enabled by default** — including anchoring, which is off unless you ask for it and configure an endpoint. This list is generated from the running system, so it is what the software actually offers on the day this document was produced.

Module	What it does
Core platform core	Everything every customer gets: shipments and their itinerary, checkpoints, the party registry, documents, alerts, purchase orders, the dashboard, and the audit trail underneath all of it.
Custody & privacy envelope	Chain-of-custody handoffs between parties, and encrypted shipments that only named recipients can open.

custody	
Compliance compliance	Environmental envelopes with pass/fail verdicts, and manifest anchoring.
Tracking & telemetry tracking	Ingest from your own devices and from third-party fleet systems, with positions on the map. Seeing your positions is included with every plan; this module is what lets data arrive.
Warehouse management warehouse	Run the building, not just the shipment: stock held at a location, on a pallet, in a lot — with what is promised to somebody else tracked apart from what is free to sell.
Finance finance	Invoice escrow, and the ROI baseline that reports which savings inputs are measured from your own data rather than assumed.
Blockchain anchoring anchoring	Anchor evidence to the Vextaris chain so a third party can verify it without trusting us.
Import & onboarding import	Bring existing shipments in from spreadsheets or an ERP export, with a preview first.
Agency (act for your clients) agency	Work inside your customers' accounts without them handing over passwords — a forwarder sees and moves a principal's freight, and every action stays attributed to whoever really did it.
Manufacturing manufacturing	Build records that survive an audit: routings, operations, lots and units, with contract flow-downs that block release until they are resolved.
Asset maintenance maintenance	Assets, components, scheduled tasks and work orders — the fleet and equipment lifecycle.

Module control is per organisation. Control over what an individual person can see and do is separate, and is governed by their role within your organisation.

7. What we do not claim

This section exists because the fastest way to waste a security review is to discover, halfway through, that a vendor's document oversold something. The following are stated so they do not have to be found.

- We hold **no compliance certification**. The audit trail was built against the control families in NIST SP 800-171 §3.3, and building against a standard is not the same as holding a certification against it. Anyone telling you otherwise should be asked for the certificate number.
- The no-outbound property is enforced against our source, not our dependencies (§3).
- Shipment encryption happens in the browser: a manifest is encrypted before it leaves the page, our servers never receive it in the clear, and only the named recipients can open it. The code that does this is delivered by our web application, so it relies on the integrity of the page you load; on a self-hosted install, that page is served by you.
- Documents can be recorded or stored. For each document the product keeps its type, its name and a fingerprint of its contents, so any copy can be checked against it later. Files you upload —

to shipments, manufacturing units, lots or nonconformances — are stored for you, served only to your own organisation, and included when your data leaves with you.

- Managed-cloud customers do not choose their region. It is the European Union (Finland). If region matters to you, that is a self-hosted or managed-dedicated conversation.
- Optional capabilities are exactly that. A module not licensed to you is refused by the server, not hidden by the interface — and a capability described in our materials may not be switched on in your deployment. Ask, and ask us to show you.

8. Verifying any of this

Every claim above is either a property you can test in a trial, or a limit we have written down. We will give a technical evaluator a sandbox and the documentation set, without a sales call first.

Cargovate is a product of Cargovate LLC. This document describes deployment architecture and is not a contract. Generated 2026-10-02 · 7c2bd3e · questions: sales@cargovate.com