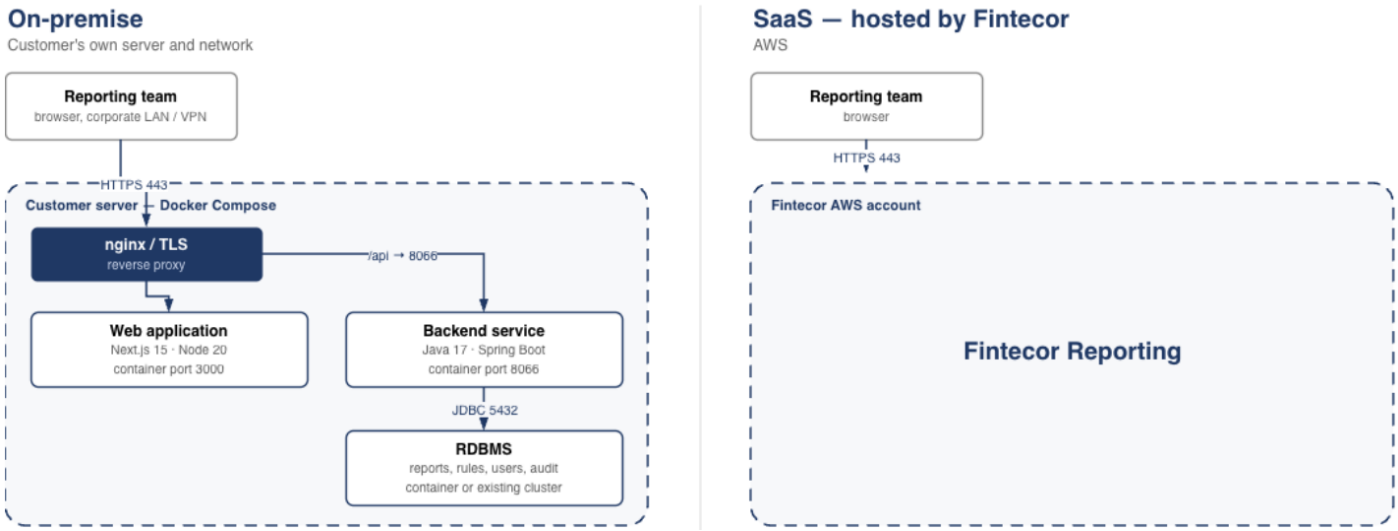
Technical Architecture

- Solution Architecture
- On-premises and SaaS Compared

Solution Architecture



The platform is a three-tier application. A browser client talks over HTTPS to a stateless REST backend, which is the only component that touches the database.

Tier	Responsibility	Technology and notes
Client	Report grid, editing, drill-down views, dataset comparison, Excel import/export in the browser	React 18.
Application	Authentication, calculation processes, validation rule execution, breakdown queries, server-side export, audit	Java 17, Spring Boot, Spring Security; runs stateless, so it can be scaled to more than one instance when volume requires it
Data	Templates, report data, validation rules, glossary, users, audit history etc.	RDBMS, schema owned and migrated by the application.

Security

Authentication	Named user accounts with password plus TOTP two-factor authentication. Failed second-factor attempts are counted and the account is locked out temporarily.
Authorisation	Role-based and enforced in the backend, so an API client cannot reach data the role does not permit. Access to reporting data requires an authenticated principal.
Transport	HTTPS end to end. The browser origins permitted to call the API are an explicit allowlist, not a wildcard.
Secrets	Database credentials, the token signing key and the key protecting stored two-factor secrets are supplied per installation and held outside the image. Two-factor secrets are encrypted at rest with AES.
Logging	Structured application logs to the container log stream, collectable by whatever you already run. Health is exposed at a dedicated endpoint for your monitoring system to poll.

On-premises and SaaS Compared

The two models differ in who operates the stack, not in what the software does.

	On-premise	SaaS (hosted by Fintecor)
Runs on	Customer server or VM, customer network	Dedicated instance in Fintecor's AWS account.
Data location	Entirely within the institution	AWS, data never leaves it.
Server, OS, Docker	Customer	Fintecor
Backups, monitoring, patching	Customer	Fintecor
Upgrades	Customer schedules; Fintecor supplies the image and performs the upgrade on request	Fintecor, in an agreed maintenance window
User and role administration	Customer	Customer
Report content and rule updates	Fintecor delivers, customer applies	Fintecor
Network exposure	Internal only if you wish — no internet access required	Published hostname over HTTPS; source-IP restriction available on request

Technical Requirements

On-premises

	Existing Database	Database on the same server
CPU	2 vCPU (x86-64 or ARM64)	4 vCPU
RAM	8 GB	16 GB
Disk	100 GB SSD	250 GB SSD, separate volume for the database
Operating system	64-bit Linux with Docker: Ubuntu 22.04/24.04 LTS, RHEL / Rocky / Alma 9, Amazon Linux 2023	Same, kept on the vendor's LTS update track
Software	Docker Engine 24+ with the Compose v2 plugin, TLS certificate	Same, DBMS
Database	Any RDBMS	Any RDBMS

SaaS

Hosting	Fintecor's AWS account.
Operations	Provisioning, OS and container patching, monitoring, capacity, backups and restore testing, and upgrades in an agreed window.
Backups	Automated database backups with defined retention.
Customer obligations	Managing its own users and roles, the TOTP enrolment of its staff.