SECURITY AT GTMETA

Security engineered into every layer

GTmeta is built for organizations that can't compromise on data protection. Authentication, encryption, and isolation aren't add-ons: they're part of the platform's foundation.

2FA · TOTP | AES-256 | scrypt | TLS 1.3 | JWT + IP-binding | Role-based access

DEFENSE IN DEPTH

Five layers, each independent

Security isn't a single wall but a series of them. A weakness in one layer is contained by the next, from the network edge down to every stored record.

Edge	**Network**	All traffic over `TLS 1.2 / 1.3`; HTTP is automatically redirected to HTTPS. Reverse-proxy isolation between the public edge and the application.
AuthN	**Identity**	Signed and encrypted `JWT` tokens bound to the client IP, plus two-factor authentication.
AuthZ	**Permissions**	Role-based access control and `row-level security`: users reach only what their profile allows.
Data	**Storage**	Credentials one-way hashed, other secrets encrypted at rest with `AES-256`, data separated by domain and by project.
Ops	**Operations**	Containerized services, encrypted off-site backups, and full audit logging of authentication and data access.

WHAT WE DO

The measures, in detail

Written for the people who ask the hard questions. Every claim below reflects how the platform actually works.

Authentication & access

Every request is verified: who you are, from where, and what you're allowed to touch.

- `JWT` tokens, signed *and* encrypted, bound to the client IP address.
- Two-factor authentication (`TOTP`) with per-user secrets and lockout after repeated failures.
- Role-based access control, scoped per project and per user.
- Single sign-on via Google and Microsoft (`OAuth 2.0`).
- Password policies: complexity, expiry, and automatic lockout.

Password protection

We can't read your users' passwords. And that's the point.

- Stored as one-way `scrypt` hashes with a unique per-user salt.
- Never reversible: not even an administrator can recover a password.
- Verified in constant time to resist timing attacks.
- Aligned with GDPR data-minimization: no recoverable personal credentials.

Encryption everywhere

Protected in transit and at rest.

- ✓ `TLS 1.2 / 1.3` for all traffic; HTTP redirected to HTTPS automatically.
- ✓ Stored secrets (database & mail credentials) encrypted with `AES-256`, unique initialization vector per record.
- ✓ Encryption keys kept outside the database and outside source control.

Data isolation & privacy

Your data stays yours: separated, scoped, and access-controlled.

- ✓ Authentication, application data, and audit logs held in separate databases.
- ✓ `Row-level security`: users see only the records their profile permits.
- ✓ Per-project isolation for multi-company and multi-tenant deployments.
- ✓ GDPR-aligned: data minimization, non-recoverable credentials, audit trails.

Application hardening

Built to withstand the common attack classes.

- ✓ SQL injection: queries use bind parameters throughout; dynamic grid filters additionally validate column names against a strict allow-list.
- ✓ Rate limiting on authentication endpoints to blunt brute-force attempts.
- ✓ Modern HTTP security headers (content-type, framing, transport security).
- ✓ Input validation and path-traversal protection on file operations.

Infrastructure & operations

Security continues after deployment.

- Containerized, isolated services.
- Encrypted, off-site backups replicated between data centers (public-key encryption).
- Secrets never committed to source control.
- Comprehensive audit logging: authentication, database access, and errors.

Have a harder question?

We're happy to walk your security team through the architecture in detail.

This page describes security measures implemented in the GTmeta platform. GTmeta is developed by GTsoftware di Giancarlo Thiella. Specific configurations may vary by deployment; contact us for details relevant to your environment.