Billable CPQ

Security Overview

ENTERPRISE-GRADE INFRASTRUCTURE · LAYERED BY DESIGN

April 2026 · billablecpq.com/security · security@billablecpq.com

Billable CPQ is built on enterprise-grade infrastructure with security controls layered at every tier — from the global edge network down to row-level data access. This document outlines the specific technical measures in place to protect your data and your customers' data.

SCOPE

Billable CPQ inherits SOC 2 Type 2 controls from its infrastructure providers (Supabase, AWS, Cloudflare). Billable CPQ itself is early-stage and does not currently hold an independent SOC 2 Type 2 audit at the application layer; that audit is on our roadmap as the customer base justifies it.

BillableCPQ is built on enterprise-grade infrastructure with security controls layered at every tier — from the global edge network down to row-level data access. This document outlines the specific technical measures in place to protect your data and your customers' data.

1 Infrastructure & Hosting

BillableCPQ runs on two industry-leading platforms, both of which carry independent security certifications:

- **Cloudflare Pages** hosts our frontend and serves as the global edge layer.
- **Supabase** (built on PostgreSQL) hosts our database, authentication, and backend services.

Supabase is **SOC 2 Type 2 compliant** and is assessed annually against the SOC 2 security framework, which governs security, availability, processing integrity, confidentiality, and privacy. This means the environment hosting your data is audited by an independent third party every year.

2 Encryption

Encryption in transit

All traffic between your browser, our application, and our database is encrypted using **TLS 1.2 or higher**. SSL/TLS certificates are issued and auto-renewed through Cloudflare, eliminating any window of certificate

expiry risk.

Encryption at rest

All customer data — including your engagements, quotes, staffing plans, pricing, and customer records — is encrypted at rest using **AES-256**, the same encryption standard used by banks and the U.S. federal government. Database backups are encrypted using the same standard.

Application-layer encryption

Sensitive credentials such as API tokens and integration keys are encrypted at the application layer before being written to the database — meaning even if the database layer were somehow compromised, those values would remain unreadable.

3 Authentication & Access Control

Authentication

User authentication runs through Supabase Auth, which supports industry-standard OAuth 2.1 and OpenID Connect, plus password-based login with bcrypt-hashed credentials. Passwords are never stored in plaintext.

Role-based access control

BillableCPQ implements three distinct user roles at the application level — **Admin, Manager, and User** — enforced through the `company_users` table. Each role has a specific, limited set of permissions, so a user only sees and can act on what their role allows.

Row-Level Security (RLS)

At the database layer, we use PostgreSQL **Row-Level Security policies** to enforce multi-tenant data isolation. This means that even at the raw SQL level, a user from Company A cannot query, read, or modify data belonging to Company B — the database itself rejects the request before any application logic runs. This is a defense-in-depth pattern that prevents entire classes of data-leakage bugs.

Database isolation

Each Supabase project runs in an isolated Postgres instance — not a shared multi-tenant database — which further reduces the risk of cross-project data exposure.

4 Edge Security & DDoS Protection

All traffic to BillableCPQ is routed through Cloudflare's global network of 330+ data centers before reaching our application. This provides:

- **Always-on DDoS protection** at network, transport, and application layers (L3/L4/L7), with most attacks mitigated automatically in under three seconds.
- **Web Application Firewall (WAF)** protection against common attack vectors including SQL injection, cross-site scripting (XSS), and the OWASP Top 10 vulnerabilities.

- **Bot management** to identify and block automated scraping, credential-stuffing, and abuse attempts.
- **Rate limiting** on authentication and API endpoints to prevent brute-force attacks.
- **TLS termination at the edge**, keeping origin servers shielded from direct public exposure.

5 Data Backup & Recovery

- **Daily automated backups** of the production database, managed and monitored by Supabase.
- Backups are stored and encrypted at rest alongside the production database.
- **Geographically distributed** Cloudflare edge caching ensures the application remains available and performant even during regional network incidents.

As BillableCPQ scales into its first enterprise engagements, we plan to upgrade to Supabase's paid tier to enable **Point-in-Time Recovery (PITR)** — which provides second-level restore granularity and extended backup retention windows.

6 Code & Deployment Security

- **Private source code repository** on GitHub with branch protection and restricted commit access.
- **No public exposure of secrets.** All environment variables (Supabase keys, integration tokens, API keys) are stored as encrypted secrets in Cloudflare Pages — never committed to source control.
- **Automated deployments** via CI/CD: every commit is deployed through an auditable pipeline, so we have a complete record of what code ran in production and when.
- **Dependency scanning** via GitHub's built-in vulnerability alerts to catch known CVEs in third-party packages.

7 Penetration Testing & Monitoring

- Supabase, our backend provider, works with industry experts to conduct **regular penetration tests** of their platform.
- Supabase provides a **Security Advisor** that surfaces configuration issues proactively, and we review and remediate its findings as part of routine maintenance.
- Cloudflare provides real-time **Security Analytics** showing blocked requests, threat sources, and anomaly detection across all traffic.

8 Compliance Posture

BillableCPQ inherits the following compliance benefits from our infrastructure providers:

- **SOC 2 Type 2** — via Supabase (annually audited)

- **GDPR-ready** infrastructure — Supabase provides data-residency and data-subject-request tooling that helps us honor customer requests for data access or deletion.

BillableCPQ itself is early-stage and does not currently hold independent SOC 2 certification. We're transparent about this: the controls above are the same building blocks used by mature SaaS companies, and as BillableCPQ grows we plan to pursue our own SOC 2 audit.

9 Shared Responsibility

Security is a shared responsibility between BillableCPQ and our customers. We recommend all customers:

1. Enable **multi-factor authentication (MFA)** on their user accounts.
2. Assign the minimum role necessary to each user (principle of least privilege).
3. Remove user access promptly when employees leave.
4. Use strong, unique passwords and a password manager.
5. Report any suspicious activity to our team immediately.

✉ Contact

For security questions or to report a vulnerability, contact: **security@billablecpq.com**

We take security reports seriously and will respond within one business day.