STRAITUM

Security Whitepaper

Architecture, Controls & Data Protection

Version 1.0 · June 2026 · Straitum LLC

Executive Summary

Straitum is a unified security risk platform built for lean security teams. This document describes the security architecture, data protection controls, and operational practices Straitum uses to protect customer data.

We understand that our customers entrust us with sensitive security data — asset inventories, vulnerability scan results, CVE data, and risk register entries. This data represents the operational security posture of your organization. We treat it accordingly.

Key security facts at a glance:

- ✓ All customer data encrypted in transit (TLS 1.2+) and at rest (AES-256)
- ✓ Complete physical data isolation — each customer has a dedicated database
- ✓ No customer security data used to train AI models — ever
- ✓ JWT authentication with RBAC on every API endpoint
- ✓ 72-hour breach notification commitment per our DPA
- ✓ Audit logging on all API calls
- ✓ Rate limiting on all public endpoints
- ⏳ SOC 2 Type I audit targeted for Q1 2027

1. Data Architecture & Isolation

1.1 Per-Customer Database Isolation

Each Straitum customer receives a dedicated PostgreSQL database instance. No customer data is co-mingled in a shared database. This architecture provides the strongest possible tenant isolation:

- A security incident affecting one customer's instance cannot expose another customer's data
- No row-level security policies or tenant_id filtering required — data separation is physical
- Each database is provisioned, managed, and backed up independently

Shared Database (NOT used)	Dedicated Database (Straitum model)
✗ All customers in one DB	✓ One dedicated DB per customer
✗ tenant_id filtering required	✓ No shared tables, no filtering needed
✗ Bug could expose cross-tenant data	✓ Physical isolation prevents cross-tenant access

✗ Common in cost-optimized SaaS	✓ Standard for security-sensitive applications

1.2 What Data Straitum Stores

Straitum stores the following categories of customer data:

Data Category	Examples	Retention
Account data	Names, email addresses, hashed passwords	Duration of subscription
Asset inventory	Hostnames, IP addresses, OS versions, hardware details	Duration of subscription
Vulnerability data	CVE IDs, CVSS scores, affected software, severity	Duration of subscription
Risk register entries	Risk descriptions, owners, remediation plans	Duration of subscription
Vendor assessments	Questionnaire responses, risk scores	Duration of subscription
Lead form data	Name, company, email, tool preferences	Until account created or 1 year
Usage logs	API call timestamps, feature usage	90 days rolling

1.3 Data Deletion

Upon account termination or subscription cancellation, all customer data is deleted within 30 days. Deletion can be requested immediately by contacting hello@straitum.com. Written confirmation of deletion is provided on request. Database backups containing customer data are destroyed within 90 days of termination.

2. Encryption

2.1 Encryption in Transit

All data transmitted between your browser and Straitum is encrypted using TLS 1.2 or higher. This applies to:

- The Straitum platform at app.straitum.com
- The marketing site at straitum.com
- All API endpoints
- Email delivery via Resend

HTTP connections are automatically redirected to HTTPS. There is no option to use an unencrypted connection.

2.2 Encryption at Rest

All customer data stored in PostgreSQL databases is encrypted at rest using AES-256 encryption provided by Railway's infrastructure. This includes all tables: assets, vulnerabilities, applications, risk register entries, vendor assessments, and user accounts.

2.3 Password Storage

User passwords are never stored in plaintext. Straitum uses bcrypt with a cost factor of 12 — a deliberately slow hashing algorithm designed to make brute-force attacks computationally expensive. Even in the event of a database breach, passwords cannot be recovered from stored hashes.

3. Access Controls & Authentication

3.1 Authentication

All access to the Straitum platform requires authentication via JSON Web Tokens (JWT). JWTs are issued on login, expire after a configurable session duration, and are validated on every API request. Sessions survive browser refresh but are invalidated on explicit logout or password change.

3.2 Role-Based Access Control (RBAC)

Straitum implements a Groups → Roles → Permissions RBAC hierarchy. Permissions are granular per module — a user can be given view-only access to vulnerability data while having full edit access to the risk register. The sidebar and all API endpoints enforce permissions — a user cannot access data their role does not permit, regardless of knowing the URL.

3.3 Admin Controls

Administrative functions (user management, system resets, data imports) are protected by a separate requireAdmin middleware. Standard users cannot access admin endpoints regardless of their role permissions.

3.4 Public Endpoint Security

The only public endpoint (no authentication required) is the lead capture form at POST /api/v1/leads. This endpoint has additional protections:

- Rate limited to 5 submissions per IP address per hour
- Server-side input validation — rejects malformed data
- Uses a restricted database user (leads_writer) with INSERT and SELECT permissions on the leads table only — it cannot read, modify, or delete any platform data
- Personal email domains (gmail, yahoo, etc.) rejected server-side

4. Network Security

4.1 CORS Policy

Cross-Origin Resource Sharing (CORS) is enforced via an explicit allowlist. Only the following origins are permitted to make API requests:

- https://straitum.com
- https://app.straitum.com
- Localhost origins for authorized development

Requests from any other origin are rejected. The allowlist is configured via environment variables — not hardcoded — allowing it to be updated without code changes.

4.2 Rate Limiting

Straitum uses three independent rate limiters, each keyed appropriately to its context:

- Public routes (lead form, forgot password): 100 requests per 15 minutes per IP address
- Login endpoint: 20 attempts per 15 minutes per IP — brute-force and credential stuffing protection
- Authenticated routes: 500 requests per 15 minutes per USER ID — each authenticated user has an independent quota; users sharing a corporate VPN or office NAT do not consume each other's limits
- Lead form: 5 submissions per hour per IP — additional protection on the public intake endpoint

Clients exceeding these limits receive a 429 Too Many Requests response. Keying authenticated routes by user ID rather than IP address ensures that one user's activity cannot inadvertently block colleagues sharing the same network.

4.3 Security Headers

Straitum uses Helmet.js to set secure HTTP response headers on all responses, including:

- Content-Security-Policy — restricts resource loading
- X-Frame-Options: DENY — prevents clickjacking
- X-Content-Type-Options: nosniff
- Strict-Transport-Security — enforces HTTPS

4.4 Database Security

The PostgreSQL database is not publicly accessible. Connections require SSL (enforced via DB_SSL=true). The database listens only on the internal Railway network — it cannot be reached from the public internet.

5. AI Features & Third-Party Services

5.1 CVE Enrichment — What Is and Is Not Sent to AI

Straitum uses the Anthropic Claude API to generate contextual vulnerability descriptions. This is the only AI feature in the platform. It is critical to understand exactly what data is and is not sent:

NOT sent to Anthropic	ONLY this is sent
✗ Your hostnames or asset names	✓ CVE ID (e.g. CVE-2021-44228) — public information
✗ Your IP addresses	✓ CVSS score — public information
✗ Your network architecture	✓ NVD description — already public
✗ Any environment-specific data	✓ Generic impact/likelihood context
✗ Employee or user information	✓ No customer-identifying details

AI-generated CVE enrichments are cached globally by CVE ID — the same CVE is only enriched once, ever. The cache contains no customer-specific information.

5.2 Subprocessors

Straitum uses the following third-party subprocessors to deliver the service:

Provider	Purpose	Location	Data processed
Railway	Application hosting + database infrastructure	United States	All customer data (encrypted at rest)

Resend	Transactional email delivery	United States	Email addresses, email content
Anthropic	AI CVE enrichment only	United States	Public CVE IDs and NVD data only — no customer environment data

6. Audit Logging & Monitoring

Straitum logs all API calls including: timestamp, endpoint, HTTP method, authenticated user ID, response status, and client IP address. These logs are retained for 90 days and can be made available to customers upon request as part of a security review.

Specific security-relevant events that are logged:

- All authentication events (login, logout, failed attempts)
- All data imports and exports
- All risk score overrides (Expert Override mode)
- All user management actions (create, edit, deactivate)
- All admin-level actions
- All lead form submissions

7. Incident Response

Straitum maintains an incident response process designed to detect, contain, and communicate security incidents promptly.

7.1 Breach Notification

In the event of a confirmed security incident affecting customer data, Straitum commits to:

- Notifying affected customers within 72 hours of confirming the breach
- Providing details including: nature of the incident, data categories affected, approximate number of records, likely consequences, and steps taken or proposed
- Cooperating with customer incident response and regulatory notification requirements

This commitment is formalized in the Straitum Data Processing Agreement (DPA), available on request.

7.2 Vulnerability Disclosure

If you discover a security vulnerability in the Straitum platform, please report it responsibly to hello@straitum.com. We commit to acknowledging your report within 48 hours and providing a resolution timeline. We do not pursue legal action against good-faith security researchers.

8. Compliance Roadmap

Straitum is a pre-certification company. We are honest about where we are and where we are going.

Certification	Status	Notes

SOC 2 Type I	**Target: Q1 2027**	Controls implementation in progress. This whitepaper documents current control posture.
SOC 2 Type II	**Target: Q3 2027**	Follows Type I audit.
GDPR Compliance	**Controls in place**	DPA available. Data processed in United States. SCCs available on request.
HIPAA BAA	**Available on request**	BAA template available for healthcare customers. Contact hello@straitum.com before uploading PHI.
PCI DSS (as vendor)	**Not applicable**	Straitum does not process cardholder data. Customers use Straitum to track their own PCI scope assets.

We believe transparency about our certification roadmap builds more trust than overstating our compliance posture. The controls described in this document represent our actual implemented security program, not an aspirational statement.

9. Security Controls Summary

Control	Status	Implementation
Encryption in transit	**In Place**	TLS 1.2+ enforced on all connections
Encryption at rest	**In Place**	AES-256 via Railway PostgreSQL
Password hashing	**In Place**	bcrypt cost factor 12
JWT authentication	**In Place**	Required on all platform endpoints
Role-based access control	**In Place**	Groups → Roles → Permissions hierarchy
Admin route protection	**In Place**	requireAdmin middleware on sensitive routes
Rate limiting	**In Place**	Global + per-endpoint limits
Security headers	**In Place**	Helmet.js — CSP, X-Frame-Options, HSTS
CORS policy	**In Place**	Explicit allowlist, env-var driven
Audit logging	**In Place**	All API calls logged with user + timestamp
DB SSL enforcement	**In Place**	DB_SSL=true, rejectUnauthorized configurable
Trust proxy	**In Place**	Correct client IP behind load balancer
Public endpoint isolation	**In Place**	Restricted DB user on leads endpoint
Physical tenant isolation	**In Place**	Dedicated database per customer
Data deletion on termination	**In Place**	30-day deletion, 90-day backup purge
Breach notification (72hr)	**In Place**	Formalized in DPA
No AI training on customer data	**In Place**	Contractual + architectural commitment
Vulnerability disclosure process	**In Place**	hello@straitum.com responsible disclosure

Multi-factor authentication	In Place	TOTP-based via authenticator app. Per-user enforcement, admin controls, trusted devices (7 days), grace period, email reminders, step-up auth on destructive actions.
Penetration testing	Roadmap	Prior to SOC 2 Type I audit
SOC 2 Type I	Roadmap	Target Q1 2027
Per-tenant encryption keys	Roadmap	SOC 2 Type II phase

10. Contact & Additional Documentation

For security-related questions, vulnerability reports, or to request additional documentation:

- Security inquiries: hello@straitum.com
- Data Processing Agreement (DPA): available on request
- HIPAA Business Associate Agreement (BAA): available on request for healthcare customers
- Vulnerability disclosure: hello@straitum.com

Straitum LLC
straitum.com
hello@straitum.com