Torvus Security - Repository Audit & Enhancement Report

Date: 2025-09-23 (AEST)

1) Repo Snapshot

Tech stack & versions: Next.js 15.0.0-canary.36, React 19.0.0-rc.0, TypeScript 5.4.x, TailwindCSS 3.4.x, Vitest 1.6.x, Supabase JS 2.43.x. Runtime targets Node >=18.18.0.

Build/test commands: root scripts proxy to the console workspace (pnpm build:console, pnpm --filter @torvus/console test, etc.).

Structure (top two levels):
- Root: README.md, RUNBOOK.md, apps/, db/, docs/, node_modules/, pnpm-lock.yaml, supabase/, etc.
- apps/: Next.js app with app/, components/, lib/, middleware.ts, next.config.mjs, server/, styles/, tests/.
- docs/console/: Cloudflare Access policy, console README, status page embed notes.
- db/: verification SQL; supabase/migrations/: timestamped SQL migrations.

2) Findings by Severity

[Critical] Cloudflare Access identity is trusted without signature verification
Files:
- apps/console/lib/auth/cfAccess.ts:37-82
- apps/console/lib/auth.ts:34-40,168-188
- apps/console/app/api/admin/roles/route.ts:31-49
- apps/console/app/api/admin/settings/read-only/route.ts:12-48
Description: Cf-Access tokens decoded without signature validation, allowing forged staff identities.
Impact: Enables impersonation and privilege escalation.
Recommendation: Verify Cloudflare Access JWTs or require Supabase sessions before honoring headers.

[High] Passkey enrollment stub bypasses hardware-factor requirement
Files:
- apps/console/app/enroll-passkey/actions.ts:15-64
- apps/console/app/enroll-passkey/page.tsx:7-46
Description: Checkbox-only flow flips passkey_enrolled via service-role client.
Impact: Undermines mandatory hardware key enforcement.
Recommendation: Implement full WebAuthn ceremony and disable stub in production.

[High] Break-glass RLS helper references nonexistent column
Files:
- supabase/migrations/20250927_break_glass.sql:45-94
- supabase/migrations/2025-09-21-001_features_1_16.sql:44-80
Description: has_security_admin_role() compares against sr.role_name while table exposes sr.name.
Impact: Migration fails or helper always false, breaking dual-control.
Recommendation: Join on sr.name and add regression tests.

[Medium] CSP profile exists but is never emitted
File: apps/console/middleware.ts:194-279
Description: Middleware builds nonce yet omits Content-Security-Policy header.
Impact: Leaves console without promised CSP protections.
Recommendation: Emit CSP header on all responses.

[Medium] DB verification checklist drifts from schema
Files:
- db/verify/checklist.sql:42-50
- supabase/migrations/2025-09-21-001_features_1_16.sql:72-80
Description: Checklist asserts columns absent from migrations.
Impact: False positives obscure real drift.
Recommendation: Align checklist with schema or add columns.

[Medium] Cloudflare Access policy doc doesn't match implementation
Files:
- docs/console/CLOUDFLARE-ACCESS-POLICY.md:15-17
- apps/console/lib/auth.ts:34-39
Description: Docs reference X-Torvus headers while code expects cf-access-authenticated-user-email.
Impact: Misconfiguration risks lockouts or spoofing.
Recommendation: Align docs and code while verifying JWTs.

[Low] Root README misrepresents the project
File: README.md:1-8
Description: Claims repo is a static landing page, conflicting with Next.js console.
Impact: Misleads onboarding and audits.
Recommendation: Update README with accurate context.

[Low] Environment template omits secrets required by intake encryption
Files:
- .env.example:1-23
- apps/console/server/intake.ts:86-134
Description: Missing TORVUS_INTAKE_SECRET_KEY and fallback.
Impact: Dev/CI rely on insecure fallback.
Recommendation: Add required secret variables with guidance.

3) Security Review

Headers: HSTS, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, COOP/COEP/CORP, and X-Frame-Options configured; Content-Security-Policy absent despite nonce generation.

Authn/Authz: Supabase service-role clients bypass RLS while relying on unverified Cloudflare Access headers; FORCE RLS enabled but undermined by header spoofing.

Upload pipeline: Intake endpoints use AES-256-GCM with key fallback; antivirus hooks, MIME validation, SCAN_ENFORCEMENT gating, and storage ACL checks remain TODO.

Secrets & configs: Supabase keys required; intake encryption key defaults to dev constant and missing from env template.

Dependency audit: Using bleeding-edge Next.js canary and React 19 RC; no automated scanning configured.

Build/CI/CD: No GitHub Actions workflows; deployment parity with Vercel undocumented.

Logging & auditing: log_audit_event RPC records actor/email/IP with sanitized metadata.

Third-party embeds: Statuspage iframe depends on unenforced CSP.

RLS policies: FORCE RLS applied; break-glass helper bug undermines security_admin checks.

Rate limiting: No per-IP/user throttling evident.

Crypto: AES-256-GCM with strict key length for intake encryption.

Analytics: Limited set of events mapped to taxonomy; dev fallback host used.

4) Expected Features Cross-Check

Read-only dashboards for incidents/releases/queues - Implemented: metrics and listings provide read-only insights.

Privileged actions gated by staff roles & built_in flag - Partially implemented: UI checks roles but header spoofing and helper bug weaken controls.

Search and triage tools with PII redaction - Partial: Filters exist, no explicit redaction observed.

Audit visibility & impersonation safeguards - Partial: Audit trail exists; dual-control undermined by auth gaps.

Feature flags/toggles - Implemented: TORVUS_FEATURE_ENABLE_RELEASE_EXECUTION used across app.

Runbook links - Missing: No references to Uptime & Incident Response Runbook surfaced in UI.

Staff role schema with built_in column - Implemented: Migration adds built_in flag.

Impersonation approval safeguards - Missing: No code paths for impersonation approvals located.

5) Quick Wins (<=1 day)

Fix break-glass helper to reference sr.name instead of sr.role_name in supabase/migrations/20250927_break_glass.sql.

Emit Content-Security-Policy header from middleware with generated nonce.

Extend .env.example with TORVUS_INTAKE_SECRET_KEY and TORVUS_SECRET_ENCRYPTION_KEY placeholders.

6) Remediation Plan (1 week)

Day 1: Enforce verified authentication (Cloudflare Access JWT validation + Supabase session) and align documentation.

Day 2: Replace passkey stub with full WebAuthn enrollment and attestation validation.

Day 3: Repair break-glass migration, add regression tests, verify approvals in staging.

Day 4: Ship CSP enforcement, review directives via report endpoints, integrate SIEM logging.

Day 5: Update README/docs/env templates; surface runbook links in UI.

Day 6: Add rate limiting and enhance audit logging around sensitive endpoints.

Day 7: Establish CI pipeline (lint/tests/schema diff), run dependency audit, and finalize release checklist.

Testing

Warning: Tests not run (analysis-only security review).