deny.sh

SECURITY POSTURE OVERVIEW

April 2026 · Version 1.1 · Confidential

Security Posture

An overview of deny.sh's security architecture, compliance status, and cryptographic implementation for enterprise evaluation.

CRYPTOGRAPHIC IMPLEMENTATION

Encryption

AES-256-CTR with scrypt KDF (N=16384, r=8, p=1). XOR composition layer enables multiple plausible decryptions from a single ciphertext. 4-byte length prefix inside encrypted zone.

Verification

22 automated cryptographic tests: chi-squared distribution, Kolmogorov–Smirnov, Shannon entropy, serial correlation, avalanche effect, ciphertext invariance, and correctness verification. All tests run in-browser at deny.sh/verify.

SDK

8.4 KB TypeScript, zero runtime dependencies. Also available in Python, Go, and Rust. Published as deny-sh on npm. Full source on GitHub under AGPL-3.0 (commercial license available).

Architecture

Zero-knowledge design. Browser tools run entirely client-side. API processes in memory only. No plaintext logging, no key storage, no payload persistence. All sensitive data is ephemeral.

INFRASTRUCTURE & OPERATIONS

CONTROL	STATUS	DETAIL
Encryption at rest	✓ **Active**	Full-disk encryption on all servers.
Encryption in transit	✓ **Active**	TLS 1.3 enforced, HSTS preload, A+ SSL Labs rating.
API authentication	✓ **Active**	Bearer-token auth. Keys hashed with SHA-256 before storage; raw key never persisted.
Login brute-force defence	✓ **Active**	Per-IP limit (5 attempts / 15 min) plus per-account lockout (5 wrong passwords on one email → 60-min lock, regardless of source IP) to defend against distributed credential stuffing.
Rate limiting	✓ **Active**	Per-key burst (10 req/s) + monthly quota, per-IP registration limits.
Audit logging	✓ **Active**	IP, timestamp, action type, and API-key hash on every operation.
Input validation	✓ **Active**	Strict validation on all endpoints, body size limits (5 MB), CSP headers.
DDoS protection	✓ **Active**	Cloudflare proxy with WAF rules.
Backup & recovery	✓ **Active**	Automated daily backups, tested restore procedures.
Dependency scanning	✓ **Active**	Zero runtime dependencies in core SDK. Server dependencies audited regularly.
Penetration testing	**Scheduled**	Independent third-party review scheduled for 2026.

WEB APPLICATION SECURITY

Content Security Policy

deny.sh sets a strict same-origin Content Security Policy on every response. `script-src` and `style-src` currently permit `'unsafe-inline'` in addition to `'self'` and the Stripe.js origin. This is required for compatibility with Stripe.js (which uses inline scripts in the iframe-mediated checkout flow) and for per-page initialisation snippets across our 35-page static site. The carve-out is mitigated by: same-origin enforcement on every other directive, `X-Frame-Options: DENY`, `frame-ancestors 'none'`, strict server-side input validation on every endpoint, output escaping in all email templates, and SHA-256 hash-only API-key storage so a hypothetical injection cannot exfiltrate raw credentials. Long-term roadmap: extract all 49 inline scripts to external files served with Subresource Integrity hashes and a CSP nonce, removing `'unsafe-inline'` from `script-src` entirely. Tracked as a post-launch hardening item.

Other headers

HSTS with `preload`; `X-Content-Type-Options: nosniff`; `Referrer-Policy: strict-origin-when-cross-origin`; `Permissions-Policy` denies camera, microphone, geolocation, USB, and payment APIs site-wide. Cookies on authenticated consumer sessions are `HttpOnly; Secure; SameSite=Strict`.

COMPLIANCE

STANDARD	STATUS	DETAIL
GDPR	✓ **Compliant**	UK-registered data controller. Privacy policy covers all processing. Data deletion within 7 days on request.
SOC 2	**In progress**	Architecture designed with SOC 2 principles. Hash-only key storage, full audit logging.
ISO 27001	**Mapped**	Security controls mapped to Annex A. Documentation available for enterprise customers.
PCI DSS	✓ **N/A**	No payment-card data processed. Stripe handles billing under PCI DSS Level 1.
Export controls	**Aware**	Encryption software. UK OGEL covers most commercial use. Customer responsible for local compliance.

LICENSING

Open source (AGPL-3.0)

Free to use, modify, and distribute. AGPL requires derivative works to remain open source. Suitable for open-source projects and internal evaluation.

Commercial license

From $5,000/year. Embed deny.sh in proprietary products without AGPL obligations. Includes priority support, architecture review, and multi-language SDK access.

CONTACT

For enterprise inquiries, security questions, or to request a full architecture review under NDA:
Email: hello@deny.sh · **Web:** deny.sh/enterprise