Maskbreak Security Whitepaper

Sentinel Edge Networks LTD · Registered in England & Wales 17150600 · Version 1.8 · 17 September 2026 · canonical copy at maskbreak.com/security-whitepaper

Maskbreak is a real-time fraud detection API (maskbreak.com). This document states our security posture plainly for procurement and security review: the controls in place today, how data is handled, and — deliberately — what we do not yet have. It is written to be checked, not to impress: every claim here is verifiable on the linked public pages, and we do not list controls we don't have.

1. Certifications & audits — the honest version

> Maskbreak is **pre-audit for SOC 2 Type II** and holds no SOC 2, ISO 27001, HIPAA, or PCI DSS attestation today. No third-party penetration test has been commissioned yet. We say this here rather than imply otherwise with badge walls; this section will be updated as each milestone lands, with the change dated on our changelog. A responsible-disclosure program is active (/responsible-disclosure, RFC 9116 `security.txt` published).

2. Technical controls in place today

CONTROL	IMPLEMENTATION
Authentication	Email + bcrypt-hashed password, Google OAuth (RS256, JWKS verified), TOTP 2FA with recovery codes, passkeys (WebAuthn), reviewable active-session list with per-device revocation, account lockout on repeated failures.
API key management	Keys generated with `crypto.randomBytes` (prefix `sk_live_`); rotation and instant revocation via dashboard; key rotation and password change require re-authentication.
Password breach check	Have I Been Pwned k-anonymity (5-character SHA-1 prefix only) on signup and password reset — the password itself never leaves our infrastructure.
Transport security	TLS 1.2+; HSTS preload; CORP same-origin; CSP with allowlists and live violation reporting; X-Content-Type-Options nosniff; X-Frame-Options DENY; Permissions-Policy locks camera/mic/geolocation/payment.
Rate limiting	Per-API-key and per-source-IP caps on evaluation endpoints; fixed-window rate limits on authentication endpoints and a 30-minute account lockout after 10 failed password attempts.
Session invalidation	Password change/reset or admin suspension immediately invalidates all sessions (token-epoch bump).
Encryption at rest	Managed encryption at rest on the primary database (Turso / libSQL).

CONTROL	IMPLEMENTATION
Uptime transparency	Self-hosted status page with persisted 90-day probe history and real measured uptime at /status — no vanity numbers.

3. Data handling & retention

DATA	POLICY
Lookup IPs	Raw IPs retained 7 days, then reduced to a one-way hash.
Signup emails (API signal)	Checked transiently against disposable-domain feeds; never stored or logged.
Device linking	Per-customer only, stored as one-way hashes; never linked across customers.
Account deletion	GDPR Art. 17 self-service deletion with password re-auth; live-system deletion; the existing backup-expiry commitment is 60 days, with implementation verification pending as explained below.
Analytics & advertising	Fonts are self-hosted. Google Ads remains removed. Optional Widgo chat includes visitor analytics and browser identifiers only after explicit consent on each public page. Replay is disabled; microphone access is denied by site policy. No Widgo on private account or sign-in pages; see Cookie Policy §2.3–2.4.

Retention assurance — review dated 17 September 2026

The existing 60-day backup-retention commitment remains unchanged. The repository now audits all listed current and older backup versions and the storage expiry configuration, without a newest-snapshot exemption. A denied or incomplete inspection cannot pass. Scheduled uploads continue, but a successful upload alone does not establish retention compliance. This audit does not itself erase old versions or change the storage policy; end-to-end expiry still requires production evidence and remediation of any findings.

The repository restore tool now blocks downloads and restore instructions because an authoritative record of deletions after each snapshot has not yet been established. It permits a metadata-only inventory. Reopening recovery requires a reviewed deletion-reconciliation process and an isolated restore drill showing that erased accounts and records remain absent. This is a safeguard, not a completed recovery solution. These assurance items remain open, and do not authorise longer retention or restoration of deleted accounts.

4. Sub-processors

Cloudflare (CDN/edge), Railway (hosting), Turso (database, including keyed abuse-prevention counters), Resend (transactional email), Auth0 (emailed sign-in link, where offered), Widgo (optional public-page AI chat and visitor analytics after consent), Crisp (legacy support records only), Amazon Web Services / S3 (encrypted nightly DB backups, EU Stockholm eu-north-1, 60-day rolling retention),

Google (optional Sign-In only) and GitHub (Sign-In only, where offered — not currently enabled), Have I Been Pwned (k-anonymity check), plus network- and device-intelligence providers named to customers under DPA. The live list with a dated change log is public at /sub-processors; new customer-data processing sub-processors get 30 days' advance notice with right to object.

5. Compliance framework

UK GDPR / EU GDPR aligned (processor role for evaluation traffic; DPA with SCCs published self-serve at /dpa for every customer — countersigned copies via support@maskbreak.com). CCPA honored. Security questionnaires (SIG-Lite, CAIQ, bespoke) completed within 5 business days of request. MSA available where click-through Terms can't be accepted.

This document is a plain-language summary, not a contract; contractual commitments live in the Terms, DPA, and (for enterprise) MSA/SLA. Verify anything here against the live pages: /trust, /privacy, /status, /sub-processors. Questions: support@maskbreak.com.