Finmail Security Whitepaper

Version 1.1 · July 2026 · For security reviewers and compliance officers

This online edition summarizes the Finmail security architecture for PE, VC, hedge fund, and compliance officer diligence. Version 1.1 · Last updated 2026-07-12. For the downloadable PDF, use the Security Trust Center.

Executive summary

Finmail is an AI-native enterprise webmail platform for regulated finance. Production design prioritizes:

• Mail body non-persistence in SQL — bodies remain on Dovecot IMAP;

• MariaDB as system of record for indexes, queues, compliance, and settings;

• HttpOnly transport credentials sealed in JWT for in-process IMAP/SMTP only;

• Append-only compliance hashing (CM6) with client-verifiable chains;

• Privacy gateway header scrubbing, tracking-pixel neutralization, and Shield relay aliases;

• Client-side Vault — AES-GCM ciphertext only; no platform decryption;

• AI egress controls — optional PII masking; mailbox content not used to train generalized models.

Innovation & intellectual property

Finmail holds US invention patent US12542755B2 (granted February 3, 2026) for email-based value transfer and remittance-mail cluster technology. A full patent portfolio — including JP7308496B2 — is listed on the trust center. Current Webmail features (indexing, privacy gateway, collaboration) are documented elsewhere on that page and do not represent the full patent scope.

Data residency & entity isolation

Entity	Location	Role
R&D	Shanghai	Source code and engineering IP — segregated from production data plane
Operations	Hong Kong	Finmail Limited — contracts, billing, support
Data plane	US (Virginia)	Production hosting — MariaDB, application tier, compliance logs

The Shanghai R&D entity maintains engineering assets only; R&D environments do not hold production mailbox credentials, HttpOnly session secrets, or IMAP decryption keys. Production access on US-hosted infrastructure is limited to designated operational roles (least privilege, MFA, audit logging) and is not required for routine engineering. Processing is designed for alignment with US CCPA/CPRA and Hong Kong PDPO where applicable.

System of record architecture

Layer	Technology	Stores

Mail bodies & attachments	Dovecot IMAP	RFC822 content (customer-controlled retention)
Business truth	MariaDB 10.11	`mail_index`, `mail_outbox`, `compliance_audit_logs`, settings, collaboration
Browser cache	Dexie (encrypted)	Performance cache and offline outbox — not authoritative
Sessions	HttpOnly JWT + Cookie	Sealed `mp` claim for transport — not plaintext in DB

Clearing browser storage must not destroy business truth; all recoverable data restores via API from MariaDB and IMAP.

Compliance audit chain (CM6)

Material mail actions — open, download, forward, secure-link send — append to `compliance_audit_logs` with:

• Monotonic `sequence` (server-assigned only);

• `previousHash` linking to the prior entry;

• `entryHash` = SHA-256 over canonical row data.

Concurrent writes retry on duplicate sequence. Platform administrators cannot alter history without breaking verification. Damaged chains are repaired only through documented, auditable runbooks — never silent edits.

Compliance Officer views (Enterprise tier) expose chain verification and export for regulatory review.

Privacy gateway & Shield aliases

The Privacy Enhancement Gateway reduces metadata leakage:

• Header scrubbing removes sensitive MIME headers (client IP traces, device fingerprints, unnecessary Received hops) before SMTP relay.

• HTML sanitization blocks passive tracking pixels where configured; blocked events are counted for review.

• Shield shadow aliases (`shield-*@relay`) mask analyst real addresses on outbound mail while preserving deliverability.

Gateway features complement — but do not replace — MTA-grade TLS and SPF/DKIM/DMARC transport authentication.

Session model & encrypted Vault

At login, mailbox passwords are verified against MariaDB (supporting legacy Dovecot `$6$` and Finmail standard hashes with silent upgrade). The password is sealed in an HttpOnly JWT (`mp` claim) for IMAP/SMTP transport only — never exposed to client JavaScript or stored as reusable plaintext in profile fields.

Cross-device Vault sync uploads AES-GCM ciphertext derived from the user's local master password. Finmail servers store encrypted blobs only.

AI processing & egress

When AI features are enabled (summaries, Ask Finmail, pre-send checks):

• Processing is scoped to provide the Service for the authenticated account;

• External AI egress may apply PII masking per tenant settings;

• Finmail does not use mailbox content to train or improve generalized LLMs;

• Usage is metered via `ai_usage_logs` with monthly quotas and daily safety valves (see product pricing).

Customers must independently verify AI outputs before regulatory or tax filings.

Secure Share & outbound controls

Secure Share links support burn-after-read, access badges, and optional watermarking. Secure-link sends append compliance audit entries (`mail.send.secure_link`) without blocking delivery on audit failure (best-effort logging).

Outbound mail flows through `mail_outbox` !' worker !' Postfix SMTP with rate limits per `users.role`.

Transport & infrastructure controls

• Dovecot IMAP — mail read/write boundary; QUOTA and IDLE for sync;

• Postfix SMTP — outbound delivery with TLS;

• Edge proxy — JWT/Cookie gating only; no database or IMAP in Edge Runtime;

• API authentication — `resolveRequestAuth()` on all mail and settings routes;

• Rate limiting — login, send, AI, and sensitive endpoints;

• 2FA — TOTP and backup codes where required.

SOC 2 & certification program

Finmail maps architecture and operations to a SOC 2 Type II control matrix with an active certification program (in progress — not yet attested). Implemented controls include append-only audit, mandatory 2FA, API session gates, TLS transport, PII masking on AI egress, Secure Share controls, and documented audit repair procedures.

Operational transparency

Public system status at `/status` reports production probes (IMAP TCP, SMTP TCP, MariaDB, AI configuration, privacy relay) with 90-day uptime history. Architecture claims on this page describe design intent; live status reflects runtime health.

Contact

Security inquiries: security@finmail.com Privacy / DPA: privacy@finmail.com Abuse (spam / phishing / forged mail): abuse@finmail.com Trust center: /security