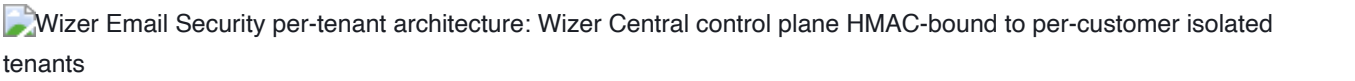
Wizer Email Security — Security Overview

A one-pager for prospective customers' security teams. Designed to answer the common questions that come up during a vendor security review. Counter-signed DPA, privacy policy, and detailed sub-processor list available on request to `security@wizer-training.com`.

What the product is

Wizer Email Security is a SaaS phishing- and business-email-compromise detection layer that runs alongside Google Workspace mail. It reads inbound mail metadata via the Workspace API (Domain-Wide Delegation), applies a combination of deterministic detection rules and AI-assisted second-opinion analysis, and surfaces warnings as in-line banners, quarantine routing, or block actions. End-user reports feed an authoring agent that proposes new detection rules for the customer's IT/security team to approve.

Architecture in one diagram


Wizer Email Security per-tenant architecture: Wizer Central control plane HMAC-bound to per-customer isolated tenants

Three load-bearing properties:

1. **Per-tenant isolation.** Every customer has a dedicated Postgres database, a separate serverless application deployment, isolated credentials, and a separate inbound Pub/Sub subscription. A compromise of one customer's tenant cannot reach another.
2. **No email content at the central control plane.** The central management surface (used for license, billing, sub-processor coordination) has no access to per-row customer message data. This is architectural, not a policy promise.
3. **All AI usage runs under Zero-Data-Retention.** Every Wizer AI call — both the inline detection second-opinion and the optional admin agent — goes to Anthropic via the Vercel AI Gateway under a Zero-Data-Retention contract. Prompts and responses are not stored or used for model training. Before any message data reaches an AI provider, a structural anonymization layer replaces real domains and addresses with placeholders; raw message bodies are not transmitted. The optional admin agent may invoke a `web_search` tool routed through a separate third-party search provider; the ZDR contract is with Anthropic specifically and does not extend to that provider, but search queries are derived from the same anonymized inputs.

Data handling

What we read

Email message metadata only — sender, recipients, subject, headers (authentication results, routing, structural), hyperlinks (URLs only), attachment metadata (filename, MIME type, size).

What we don't read or store

Email body text, attachment contents, or any data unrelated to detection. Messages are parsed in-memory, scored, and the parsed body is discarded.

Where data lives

Within the United States, in the customer's dedicated tenant database. Specific regional placement available on request for customers subject to data-residency requirements.

Retention

Data	Retention
Detection records / audit log	Term of subscription
Raw `.eml` retained for triage	30 days OR until admin disposition (whichever is sooner)
Per-mailbox spam-filter state	While the mailbox is monitored
Sign-in records	While the account is active

On termination: 30-day wind-down then permanent deletion, or earlier on written request.

Security controls

Domain	Control
Encryption in transit	TLS 1.2+ end-to-end
Encryption at rest	Database and blob storage encrypted at the provider level
Authentication	Google Domain-Wide Delegation for mailbox access; per-tenant admin allow-list for console
Authorization	Least-privilege internal access; named operators only
Audit logging	Every administrative action stamped with operator + timestamp; retained 7 years
Backup	7-day point-in-time recovery per tenant DB; protected production branches
Recovery	Documented runbook; tested restore < 5 minutes from incident detection
Secret hygiene	No customer credentials in central; per-tenant credential isolation

---

Sub-processors

A sub-processor is a third party that processes personal data on our behalf. Listed by function.

Sub-processor	Category	Purpose	Personal data processed
Vercel, Inc.	Infrastructure	App hosting; AI Gateway routing; encrypted file storage	Email content + metadata (encrypted at rest)
Neon, Inc.	Infrastructure	Per-tenant database hosting	Email metadata, encrypted message bodies, mailbox addresses
Google LLC	Product functionality	Workspace API access via DWD + Cloud Pub/Sub inbound	Mail metadata and content of monitored mailboxes
HubSpot, Inc.	Customer management & support	Support, success, CRM, sales	Account + contact data
Twilio Inc. (SendGrid)	Customer management & support	Transactional / customer emails	Customer contact email addresses
Stripe, LLC	Customer management & support	Payment processing and billing	Billing and payment data

Not sub-processors (no personal data): Anthropic (all AI usage; structurally anonymized inputs under a Zero-Data-Retention contract — message bodies not transmitted), the third-party web search invoked by the optional admin agent (anonymized queries), Google Safe Browsing (URLs only), and GitLab (source code, no customer data).

DPA Annex III is the authoritative list. We notify customers 30 days in advance of any sub-processor addition or replacement.

Operational posture

- **Detection latency**: < 1 second from message arrival to verdict (median).
- **Banner application latency**: < 5 seconds from verdict to in-mailbox banner.
- **Per-mailbox kill switch**: Reversible suspension at the tenant level with zero data loss. Used for incident response and end-of-billing-cycle freezes.
- **Health monitoring**: Tenant-level heartbeat with automated alerts for AI failures, push lag, and prolonged dark periods.

Compliance posture

- **GDPR (EU/UK):** DPA available; standard contractual clauses (Module 2) incorporated by reference. EU/UK data subjects accommodated under processor framework.
- **CCPA/CPRA:** Wizer acts as a "service provider" under CCPA/CPRA; will not sell, share, or use customer data outside the direct business relationship.
- **SOC 2:** Type 1 preparation underway; status updated as the audit progresses.

Wizer Email Security is operated by Wizer Training, Inc., a Delaware corporation. Wizer Training has been operating in security-awareness training since 2018 and runs Wizer Email Security on its own corporate mailboxes (~4,000+ messages processed across 11 mailboxes, real phishing caught, reported, and converted into deployed detection rules).

Incident response

- **Notification timeline**: Within 72 hours of confirming a security incident affecting customer data.
- **Escalation channel**: Direct line to the customer's named security contact on the Order Form.
- **Mitigation**: Per-tenant kill switch can isolate a tenant immediately while investigation proceeds.

Customer self-service

Tenant administrators have access to:

- All data Wizer Email Security holds for the tenant (via the admin console at `app.wizer-emailsecurity.com`)
- Per-mailbox ledger of every email evaluated, banner applied, and report filed
- Audit log of every admin action
- "Forget forever" action to permanently delete individual mailbox records
- Export tools for ledger and audit data

Contacts

Purpose	Address
Security questions / report a finding	`security@wizer-training.com`
DPA / legal	`legal@wizer-training.com`
Sales	`sales@wizer-training.com`
Support	`support@wizer-training.com`

This document and its references are current as of the date below. Reach out to `security@wizer-training.com` for the most recent version or to receive notice of material changes.

Wizer Training, Inc. · 131 Dartmouth St, Boston, MA 02116, USA · `wizer-emailsecurity.com`