

GhostAI Security Whitepaper

Aeon AI Risk Management Corporation

Version 0.5 (V0.5) | airiskmanagement.ca/ghostai | info@airiskmanagement.ca

Overview

GhostAI is an AI exposure and usage intelligence platform for mid-market companies. It cross-references a customer's existing DNS security posture against a curated registry of the top 1,000+ AI domains and reports what is blocked, what is logged, and what is completely invisible to their stack. If DNS logs are connected, it also reports which AI tools are actually being used on the network.

This document describes the security posture of the V0.5 release. Our guiding principle is a minimal trust surface: we collect the least data needed to deliver the product, we never run code on customer endpoints, and we are explicit about what we store and what we do not.

Architecture at a glance

- Frontend and API: Next.js (App Router) hosted on Vercel.
- Database: PostgreSQL hosted on Railway, accessed over TLS.
- Cache and rate limiting: Upstash Redis.
- Object storage (exports, reports): Cloudflare R2.
- Authentication: Clerk (passwordless and SSO).
- Payments: Stripe.
- Transactional email: Resend.

All detection runs through the customer's existing DNS infrastructure (Cloudflare Gateway, Cisco Umbrella) or a static block-list CSV upload. We never install agents, browser extensions, or scripts on customer networks or endpoints.

The minimal trust surface

V0.5 deliberately omits high-risk integrations:

- No identity provider integration (no Google Workspace or Microsoft 365 APIs).
- No email or calendar scanning.
- No OAuth grant enumeration.
- No endpoint agents and no kernel or browser hooks.

This eliminates entire classes of risk (mailbox access, broad OAuth scopes, endpoint privilege) before they exist.

What we collect, and what we never store

We collect:

- The customer's block-list or DNS policy data (domain names and their block/log status), used to compute exposure.
- Optional DNS query aggregates (domain plus daily query count) when the customer connects a DNS platform.
- Account and billing metadata (organization name, user email, plan).

We never store:

- The content of any prompt, document, or message sent to an AI tool.
- Full packet captures or raw per-query DNS logs (we aggregate to daily per-domain counts).
- Payment card data (handled entirely by Stripe).

Per-user attribution is OFF by default. When a customer's privacy officer explicitly enables it, DNS usage is bucketed by user; otherwise all usage collapses into a single anonymous aggregate per domain per day.

Data handling and encryption

- In transit: TLS for all connections (browser to app, app to database, app to third-party APIs).
- Platform credentials at rest: customer DNS-platform API keys are encrypted with AES-256-GCM before they are written to the database. The encryption key is held in the application environment, never in the database.
- Feed and SIEM tokens at rest: stored only as a SHA-256 hash. The raw token is shown to the customer exactly once, at generation. A lost token is rotated, not recovered.

Multi-tenancy and isolation

GhostAI is a multi-tenant single-database system. Every tenant-scoped row carries a tenant identifier, and every authenticated query filters on the caller's tenant. Authorization is role-based: an organization owner controls billing and destructive actions; admins have full operational access otherwise.

Authentication

User authentication is delegated to Clerk, which provides passwordless sign-in and Google SSO with organization and team support. GhostAI does not store passwords.

The auto-updating feed and SIEM events endpoints

The block-list feed (an External Dynamic List that firewalls poll) and the SIEM events feed are public endpoints authenticated by a per-tenant token embedded in the URL. The token is:

- Stored only as a SHA-256 hash, and looked up by hash (never compared as a raw string).
- Revocable and expirable, and rotatable at any time by the customer.
- Rate limited per source address.

Because the URL carries a secret, feed responses are marked private and are not held in shared CDN caches.

Billing

Billing is handled by Stripe. GhostAI stores only Stripe customer and subscription identifiers, never card data. Webhook events are signature-verified and processed idempotently so a replayed event cannot re-trigger a plan change.

Subprocessors

Vercel (hosting), Railway (database), Clerk (authentication), Stripe (payments), Upstash (cache and rate limiting), Cloudflare (R2 storage), Resend (email). Each processes the minimum data needed for its function.

Vulnerability management

Dependencies are tracked and audited; the dependency tree is kept free of known advisories at release. Security-relevant changes are reviewed before merge. We monitor advisories for our framework and direct dependencies and patch on a risk-prioritized basis.

Compliance status

GhostAI is a young product. We do not yet hold a SOC 2 Type II report, and we say so plainly rather than imply otherwise. Our architecture (minimal data collection, encryption at rest, no endpoint footprint) is designed to make that certification path straightforward as the company matures.

Responsible disclosure

If you believe you have found a security issue, please email info@airiskmanagement.ca with details and steps to reproduce. We will acknowledge receipt and work with you on a coordinated fix. We do not pursue legal action against good-faith security research.