Metrovolo

Security Overview

Private AI Infrastructure for Professional Services

This document describes the security architecture, data isolation guarantees, and compliance alignment of Metrovolo deployments.

Prepared for prospective clients and their compliance teams.

info@metrovolo.com | 713-938-8988 | metrovolo.com

Houston, TX | April 2026 | Confidential

ARCHITECTURE

How your data stays private.

Metrovolo deploys a private AI environment on cloud infrastructure dedicated to your firm. The AI model, your documents, your conversations, and all processing happen entirely within this environment. No data is transmitted to any third-party AI provider. No data is used to train external models. Your firm controls who has access and how data is handled.

How it works

When a user at your firm sends a query or uploads a document, the request is processed by an AI model running inside your private environment. The model generates a response and returns it directly to the user. The entire exchange happens within your dedicated infrastructure.

The inference engine is stateless — it processes each request independently and retains nothing between requests. No prompts, no responses, no conversation history is stored by the model layer. All persistent data (conversations, documents, user accounts) is stored in your firm's isolated application environment with dedicated database and document storage.

What never happens

✘ Your data is never sent to OpenAI, Google, Anthropic, or any other AI provider.

✘ Your data is never used to train or improve any external model.

✘ Your documents are never stored on infrastructure outside your environment.

✘ Your conversations are never accessible to other firms or to Metrovolo staff (except for explicit technical support with your authorization).

Data isolation

Each client firm receives a fully isolated application environment. This includes a dedicated database, dedicated document storage, dedicated vector embeddings for knowledge base search, and dedicated user accounts. No firm can access another firm's data. This isolation is enforced at the infrastructure level, not the application level — meaning it cannot be bypassed through the user interface or API.

All infrastructure runs on Amazon Web Services (AWS) in US-based data centers, inheriting AWS's physical security controls, SOC 2 certifications, and compliance framework coverage.

SECURITY CONTROLS

Technical safeguards.

Every Metrovolo deployment implements the following security controls. These are not configurable tiers — every client receives the same security architecture.

Encryption and data protection

Control	Implementation	Details
Encryption at rest	AES-256	All stored data encrypted via AWS EBS encryption with KMS-managed keys. Encryption keys are managed by AWS Key Management Service and never exposed.
Encryption in transit	TLS 1.2+	All traffic between users and the platform is encrypted via TLS, terminated at an AWS Application Load Balancer with certificates managed by AWS Certificate Manager.
Data residency	US-based	All data processing and storage occurs in AWS US-based data centers. Data does not leave the region.
Backup encryption	AES-256	Automated daily backups are encrypted at rest using the same KMS-managed keys as primary storage.

Access controls and network security

Control	Implementation	Details
Authentication	Admin-managed accounts	User accounts are created and managed by firm administrators. Self-registration is disabled. No public access.
Network isolation	Private infrastructure	AI infrastructure is not directly internet-accessible. All user traffic routes through a managed load balancer with strict routing rules.
Firewall	Restrictive security groups	Inbound traffic restricted to HTTPS via the load balancer only. Administrative SSH access limited to a single authorized IP address.
SSH hardening	Key-pair only	Password-based SSH authentication is disabled. Access requires cryptographic key-pair authentication.

Monitoring, patching, and recovery

Control	Implementation	Details
Audit logging	Comprehensive	All AI interactions (queries, document uploads, responses) are logged within the firm's application environment. Logs are available for compliance review.
Automated backups	Daily, 7-day retention	Encrypted snapshots of all firm data are taken daily and retained for 7 days. Recovery from backup can be performed within hours.
OS patching	Automated	Operating system security patches are applied automatically via unattended upgrades. No manual intervention required.
Model updates	Managed by Metrovolo	As improved open-source AI models are released, Metrovolo tests and deploys updates to client environments. Clients are notified before any model change.

COMPLIANCE

Regulatory alignment.

Metrovolo's architecture is designed to support compliance with the regulatory frameworks that govern professional services firms. Below is a summary of how key requirements are addressed.

ABA Model Rule 1.6 — Client confidentiality

Rule 1.6 requires attorneys to make reasonable efforts to prevent unauthorized disclosure of client information. Consumer AI tools transmit data to third-party servers for processing, potentially implicating this obligation. With Metrovolo, all AI processing occurs within the firm's private environment. No client data is transmitted to any third-party AI provider, no data is used for model training, and all interactions are logged for audit purposes. This architecture supports the "reasonable efforts" standard by eliminating third-party data exposure at the infrastructure level.

SEC and FINRA — Data handling and supervision

Registered investment advisors are subject to Regulation S-P (safeguarding customer records) and FINRA requirements for supervision of client communications and protection of customer information. Metrovolo deployments keep all client data within the firm's controlled environment, with no third-party data transmission. Full audit logging of AI interactions supports the supervision and recordkeeping requirements that SEC and FINRA examiners expect.

HIPAA — Protected health information

For healthcare practices handling protected health information (PHI), Metrovolo provides HIPAA-eligible infrastructure including encryption at rest and in transit, access controls, and comprehensive audit logging. A Business Associate Agreement (BAA) is available for HIPAA-covered entities upon request.

Cloud infrastructure compliance

All Metrovolo deployments run on Amazon Web Services infrastructure, which maintains SOC 1, SOC 2, and SOC 3 certifications, along with ISO 27001, HIPAA, and FedRAMP compliance. Metrovolo deployments inherit these infrastructure-level certifications and controls.

See it in action.

Book a 20-minute walkthrough and we'll show you the platform live, walk through the security architecture with your team, and discuss how Metrovolo fits your firm's specific compliance requirements.

Book a demo: metrovolo.com/book
Email: info@metrovolo.com
Phone: 713-938-8988

Metrovolo LLC | Houston, TX | metrovolo.com