Security Overview

Enterprise AI Platform Security & Compliance

GENERAL USE

March 2026

Version 1.2

Overview

monō ai is an enterprise AI platform designed for regulated industries. Security, privacy, and compliance are foundational to our architecture — not aftermarket additions.

This document provides an overview of monō's security posture and controls.

1. Platform Architecture

1.1 Deployment Models

monō offers two deployment models to meet varying client requirements:

Model	Description	Data Residency
Multi-Tenant SaaS	Hosted on app.monoai.co with logical tenant isolation	Australia (Sydney region)
Client Cloud	Containerised deployment within client's own cloud environment	Client-controlled

Both models inherit the same security controls at the application layer. The Client Cloud model provides additional sovereignty benefits for regulated industries.

1.2 Infrastructure

Cloud Provider: Google Cloud Platform (GCP)

Primary Region: australia-southeast1 (Sydney)

Disaster Recovery: Cross-region replication with < 4 hour RTO

Network: Private VPC with no public-facing databases; all traffic via load balancers with WAF

2. Security Controls

2.1 Data Protection

Control	Implementation
Encryption at Rest	AES-256 via Google Cloud KMS; client-managed keys available for Client Cloud deployments
Encryption in Transit	TLS 1.3 enforced on all connections; certificate pinning for API clients
Data Classification	Automated classification engine; PII detection and tagging
Data Retention	Configurable per-client; secure deletion with cryptographic verification
Backup	Daily encrypted backups; 30-day retention; tested quarterly

2. Security Controls

2.2 Identity and Access Management

Control	Implementation
Authentication	SSO via SAML 2.0 / OIDC; MFA enforced for all users
Authorisation	Role-based access control (RBAC) with principle of least privilege
Session Management	Configurable session timeouts; concurrent session limits
API Security	OAuth 2.0 with short-lived tokens; API key rotation policies
Privileged Access	Just-in-time access for administrative functions; all sessions recorded

2.3 Application Security

Control	Implementation
Secure Development	OWASP Top 10 coverage; mandatory security review for all releases
Code Analysis	Static analysis (SAST) in CI/CD; dependency vulnerability scanning
Penetration Testing	Annual third-party assessment; remediation SLAs defined
Vulnerability Management	Critical: 24 hours / High: 7 days / Medium: 30 days
Change Management	All changes via version control; peer review required; automated rollback

2. Security Controls

2.4 Infrastructure Security

Control	Implementation
Network Segmentation	Micro-segmented VPCs; zero-trust internal networking
Firewall	Cloud Armor WAF; DDoS protection; geo-blocking available
Intrusion Detection	Real-time monitoring via Google Chronicle; automated alerting
Endpoint Security	All administrative endpoints hardened; EDR deployed
Patch Management	Automated patching for OS and dependencies; < 72 hours for critical

3. Operational Security

- **Centralised Logging:** All application, infrastructure, and access logs aggregated
- **Retention:** 12 months online; 7 years archived (configurable for regulated clients)
- **Immutability:** Logs written to append-only storage; tamper-evident
- **Alerting:** 24/7 automated monitoring with escalation to on-call engineering

4. Privacy and Data Handling

4.1 Privacy Principles

monō operates under Privacy by Design principles:

Data Minimisation: Only collect and process data necessary for service delivery

Purpose Limitation: Client data used solely for contracted purposes; no secondary use

Client Ownership: All client data remains client property; portable on request

AI Training: Client data is never used to train monō models without explicit written consent

4.2 Data Residency

Deployment Model	Primary Location	Options
Multi-Tenant SaaS	Australia (Sydney)	—
Client Cloud	Client-specified	Any supported cloud region

For regulated clients requiring strict data sovereignty, Client Cloud deployment ensures data never leaves the client's designated environment.

5. Contact and Further Information

monō can provide further information on its security and compliance program under NDA.