threadfin

Threadfin Business Solutions | Trust & Security

Last updated: January 2026
This page describes Threadfin Business Solutions' general security, privacy, and risk management practices. It is provided for informational purposes only and does not supersede any specific Master Services Agreement (MSA) or Statement of Work

Threadfin Business Solutions – Trust & Security

At Threadfin Business Solutions, trust is the baseline for execution. For more than 20 years, enterprise organizations have relied on our senior engineering teams to design, modernize, and support critical environments where the cost of failure is high.

Our approach prioritizes **Governance, Security, and Operational Readiness**. This page explains how we manage risk and protect your data throughout the delivery lifecycle so your stakeholders can engage with confidence.

Security & Governance

Threadfin designs its services and operating practices around modern security best practices and secure-by-default configurations. Our program focuses on preventing unauthorized access, maintaining data integrity, and ensuring that what we build is supportable and secure long after handoff.

Key execution controls:

- **Access Management:** Threadfin engineers operate under the principle of least privilege. We prefer using client-managed credentials or Just-In-Time (JIT) access to ensure a full audit trail within your environment.
- **Encryption:** Any customer data handled within approved Threadfin delivery tools is encrypted in transit using TLS 1.2+ and encrypted at rest using industry-standard AES-256.
- **Secure Architecture:** We follow documented delivery guardrails and secure coding standards, conducting peer reviews for all complex infrastructure-as-code and platform configurations.
- **Environment Integrity:** We enforce strict separation between production, development, and testing environments to prevent cross-contamination of data.
- **Personnel Security:** All senior engineers undergo background checks, receive regular security awareness training, and are required to follow internal acceptable-use policies.

AI Data Sovereignty & Privacy

We respect customer privacy and are committed to handling data responsibly and transparently, while prioritizing the protection of your intellectual property. Where third-party AI services are used, requests are processed via customer-controlled tenants or approved enterprise endpoints.

- **Data Ownership:** Your data remains your property. For RAG and AI engagements, we ensure your private data stays within your designated tenant (Azure or Google) and is never used to train public LLM models.
- **Data Minimization:** We only access the specific data necessary to execute the defined scope of work.
- **Retention & Deletion:** Customer data within our project management systems is retained only for the duration of the engagement or as required by contract. Upon project completion, data is securely decommissioned.
- **Regulatory Alignment:** Where contractually required, we support customer compliance efforts aligned with applicable regulations (e.g., GDPR, CCPA, HIPAA).

Compliance & Attestations

Threadfin does not currently maintain standalone SOC 2 or ISO certifications.

Where required, we support customer security reviews, questionnaires, and contractual security addenda as part of the engagement process. Threadfin does not operate long-term hosting of customer production data outside of approved delivery tooling and engagement needs.

Operational Readiness & Availability

Threadfin understands that delivery is only successful if the system is usable and supportable.

- **Resilient Design:** We architect solutions on reputable cloud platforms (Azure/Google) using high-availability and redundant configurations to minimize downtime.
- **Documented Handoff:** Our “Readiness” pillar ensures your internal team receives complete documentation and operational training for every system we deploy.
- **Continuous Monitoring:** We utilize monitoring and alerting to track the performance and health of the environments we support.
- **Disaster Recovery:** We maintain and regularly test documented recovery procedures to ensure service continuity in the event of an incident.

Risk Management & Partners

We proactively identify and mitigate risks to protect our customers and our firm.

- **Incident Response:** We maintain a defined incident response plan for detection, investigation, and timely customer communication consistent with contractual obligations.
- **Services-Only Neutrality:** As a services-only firm, we have no licensing bias or hardware channel conflict. Our recommendations are based solely on engineering-informed outcomes.
- **Vendor Oversight**: We carefully vet our primary partners (Microsoft, Google, AWS) and sub-processors for security and compliance alignment.

Questions? Let's Talk.

We welcome direct conversations about our security and governance practices.

security@threadfin.com – Security inquiries or requests.
privacy@threadfin.com – Privacy and data handling questions.