ThreadSync — Security Overview

ThreadSync Security Overview (High Level)

This document provides a high-level overview of ThreadSync's security posture. Detailed evidence and additional documentation may be available for qualified prospects under NDA via the Trust Center.

Security principles

• Least privilege access and role separation
• Defense-in-depth controls across identity, network, and application layers
• Auditability and governance for automation and operational actions

Identity and access

• Support for SSO patterns (SAML/OIDC)
• Role-Based Access Control (RBAC)
• Multi-factor authentication (MFA) options and session controls

Data protection

• Encryption in transit (TLS) and at rest (AES)
• Scoped access to customer data and environment isolation patterns
• Data retention and export patterns aligned to enterprise requirements

Application security

• Secure SDLC practices and dependency hygiene
• Logging and monitoring for operational integrity
• Controlled automation boundaries with human verification where required

Auditability and governance

• Audit-friendly logs for administrative and operational actions
• Role-scoped permissions and approval workflows where applicable
• Documentation and standard questionnaires supported (e.g., CAIQ / SIG Lite where requested)

Subprocessors and documentation

• Subprocessors listed transparently in the Trust Center
• Security package requests supported via the Trust Center workflow

Trust Center: https://www.threadsync.io/trust-center.html **Security page:** https://www.threadsync.io/security.html **Contact:** security@threadsync.io