FlowTux Security Overview

Last updated June 16, 2026

FlowTux ingests signals from the tools your team already uses, stores integration credentials, and can run remediation actions on enrolled devices. This one-pager summarises the controls in place today.

AT A GLANCE

SOC 2 TYPE II
Audit in progress
Not yet certified - we do not claim it until the audit completes.

DATA RESIDENCY
US · EU · India
Chosen at workspace creation. Ticket data and backups stay in region.

SSO & SCIM
SAML 2.0 + SCIM 2.0
Okta, Microsoft Entra ID, Google Workspace. Enforce SSO per domain.

AI TRAINING ON YOUR DATA
Never
Customer data is not used to train foundation models, and not sold.

DPA WITH SCCS
Available
GDPR, UK GDPR, and India DPDP Act aligned.

BREACH NOTIFICATION
Within 72 hours
Documented incident handling, with live uptime and incident history.

CONTROLS

Infrastructure	Google Cloud Platform and Microsoft Azure. Data region chosen at workspace creation (US, EU, India); ticket data and backups stay in region. Automated encrypted backups.
Encryption	TLS 1.2+ in transit. AES-256-GCM for integration credentials and sensitive data at rest. Third-party secrets held in an encrypted credential store.
Access control	Role-based access across member, admin, and workspace-admin roles on least privilege. Email verification and lockout after repeated failed sign-ins. Per-team permissions.
Enterprise SSO	SAML 2.0 with Okta, Microsoft Entra ID, and Google Workspace. SCIM 2.0 provisioning and deprovisioning. Enforce SSO per domain. Just-in-time role mapping.
Application security	HMAC-verified inbound webhooks with timing-safe comparison and timestamp windows. OAuth 2.0 with scoped least-privilege permissions. Validated input, parameterized queries, per-organization isolation.
Device agent	Remediation limited to a fixed allow-list of safe commands; arbitrary execution is not possible. Every action is a tracked job with acknowledgement, timeout, and a log entry.
Monitoring	Continuous error and performance monitoring with security alerting. Administrative and privacy-relevant operations written to an append-only audit trail.
Data privacy	Customer data is never used to train foundation models and is not sold. Self-serve export, consent management, and erasure. Configurable retention windows.
Compliance	Aligned with GDPR, UK GDPR, and India DPDP Act. DPA with Standard Contractual Clauses available. SOC 2 Type II audit in progress - not claimed as certified until complete.
Incident response	Documented detection, triage, containment, remediation, and communication procedures. Personal data breaches notified without undue delay and within 72 hours of awareness.

SUB-PROCESSORS

Google Cloud Platform (Google LLC)	United States	Application hosting and infrastructure, and AI processing of ticket, diagnostic, and assistant content. All customers.
Google Cloud Platform (Google Cloud EMEA Limited)	European Union	Application hosting and infrastructure for workspaces created in the European Union region. Customers on the EU data region.
Microsoft Azure (Microsoft Corporation)	India	Cloud hosting and infrastructure. All customers.
Meta Platforms, Inc. (WhatsApp Business)	United States	WhatsApp message delivery. Only where the customer enables WhatsApp notifications.

Customer-connected systems (Slack, GitHub, Sentry, Jira, PagerDuty, Notion, Microsoft Teams) are integrations chosen and controlled by the customer and are not FlowTux sub-processors.

Full details	https://flowtux.com/security
Uptime & incidents	https://status.flowtux.com
DPA	https://flowtux.com/dpa
Security contact	security@flowtux.com