ARANIS

Security Posture Document

Public description of the security, privacy, and continuity controls of the Aranis platform

VERSION	2.1	CLASSIFICATION	Public
ISSUE DATE	November 19, 2026	NEXT REVIEW	May 2027 (or upon material change)
OWNER	Paulo Nascimento — Founder / Security Owner / DPO	CONTACT	security@aranis.ai

1. Identification and scope

Aranis (aranis.ai) is a B2B SaaS platform for third-party risk management (TPRM) and cyber risk management, operated by **Aranis Tecnologia em Desenvolvimento de Software Não Customizável Ltda** (Brazil). This document describes the technical, organizational, and privacy controls applied to the platform's production environment.

The scope covers the applications `aranis.ai`, `app.aranis.ai`, `tools.aranis.ai`, `docs.aranis.ai`, and `trust.aranis.ai`, the cloud infrastructure supporting them, and the customer data processed within them.

This document is not an independent audit report. It describes self-declared controls, supported by formalized internal policies, a risk register, and operational evidence available upon request under NDA.

2. Certifications and attestations

Attestation	Status	Detail
CSA STAR Level 1	ACTIVE	CAIQ v4.0.3 self-assessment published on the CSA STAR Registry on July 6, 2026. Publicly verifiable at `cloudsecurityalliance.org/star/registry/aranis`.
LGPD compliance	IMPLEMENTED	Brazilian Law 13.709/2018. DPA, privacy policy, legal basis mapped per processing purpose, and a documented data subject request process.
SOC 2 (TSC) crosswalk	MAPPED	Internal control catalog mapped to all five Trust Services Criteria categories. Preparatory to a formal audit.
GDPR crosswalk	MAPPED	Control catalog mapped to the applicable articles of Regulation (EU) 2016/679.
Independent external penetration test	PLANNED	Engagement planned as the customer base grows. Current coverage is continuous automated scanning.
SOC 2 Type I	PLANNED	Next formal certification milestone following CSA STAR.

> **Transparency on maturity.** As of this date, Aranis does not hold an audited third-party certification (SOC 2, ISO 27001). The controls described below are real and internally documented, and the company commits to never representing planned controls as implemented.

3. Architecture and production stack

The platform is cloud-native and runs entirely on Amazon Web Services (AWS), in the **us-east-1** region (United States). Aranis does not manage any on-premises infrastructure, and the shared responsibility model of its providers is explicitly accounted for in control design.

Layer	Technology	Function
Application	Next.js (App Router)	Frontend and API routes
Hosting / network / perimeter	Amazon Web Services (us-east-1), Cloudflare	Compute, load balancing, TLS termination, perimeter protection, DNS
Database / Auth	Supabase, self-hosted on AWS (PostgreSQL)	Persistence, authentication, Row Level Security
Object storage	Amazon S3	Assessment evidence and attachments
Job orchestration	Inngest	Asynchronous execution and workflows
AI layer	Amazon Bedrock (primary); Anthropic, OpenAI (contingency)	Assessment, evidence, and reporting agents
Payments	Stripe	Billing; card data tokenized, never traverses Aranis
Transactional email	Resend / Amazon SES	Notifications and invitations
Observability	Amazon CloudWatch, BetterStack	Logs, metrics, alerting, and public status page
DevSecOps	GitHub, Semgrep, Gitleaks, Dependabot	SAST, secret scanning, software composition analysis

4. Security governance

Aranis maintains a set of formalized, versioned, and periodically reviewed security policies, approved by the Security Owner:

- Information Security Policy
- Access Control and Identity Policy
- Encryption and Data Protection Policy
- Secure Development Policy (SSDLC)
- Vulnerability Management Policy
- Security Incident Response Policy
- Third-Party and Subprocessor Management Policy
- Data Retention and Disposal Policy
- Acceptable Use and Confidentiality Policy
- Formal definition of RTO and RPO
- Disaster Recovery Runbook

Enterprise risk management is conducted through a formal **Risk Register**, with risks classified by likelihood and impact, a defined treatment (mitigate, accept, transfer, avoid), and a named owner. The register is reviewed quarterly.

5. Encryption and data protection

- **In transit:** only TLS 1.2 and TLS 1.3 are accepted on all public endpoints; TLS 1.0 and 1.1 are refused, and plain HTTP is redirected to HTTPS. Mandatory headers: `Strict-Transport-Security`, `X-Content-Type-Options`, `X-Frame-Options`.
- **At rest:** AES-256 across the production database storage, backups, and object storage, with encryption keys managed by AWS (AWS KMS for database volumes).
- **Key and secret management:** secrets are stored in AWS Secrets Manager and in protected environment configuration, never in code. Continuous scanning for exposed secrets in commits and Git history.
- **Multi-tenant isolation:** logical segregation per tenant, with Row Level Security (RLS) enabled on every table containing customer data as a second line of defense behind application-level controls.
- **Payment data:** processed entirely by Stripe. Aranis does not store, transmit, or process primary cardholder data.

6. Access control and identity

- Multi-factor authentication (MFA) is mandatory on all administrative accounts of critical providers.
- RBAC model within each tenant, with the roles `owner`, `admin`, `member`, and `viewer`.
- Least-privilege principle applied to API keys, service tokens, IAM roles, and OAuth integrations, scoped by function.
- Scheduled rotation of API keys and immediate revocation upon exposure or termination of a third-party relationship.
- Periodic (quarterly) review of access, permissions, and active credentials.

7. Secure development and vulnerability management

Every code change is scanned before reaching production. Static application security testing (Semgrep, including AI-specific security rules) and exposed secret detection across the full Git history (Gitleaks) run on every pull request and block the merge on critical findings. Software composition analysis runs continuously through Dependabot and dependency audits.

Remediation SLAs

Severity	CVSS	Maximum window	Handling
Critical	9.0 – 10.0	24 hours	Immediate isolation of the affected component if required; affected customers notified within 72 hours
High	7.0 – 8.9	7 days	Remediation started immediately, tracked as P1
Medium	4.0 – 6.9	30 days	Tracked as P2, included in the next development cycle
Low	0.1 – 3.9	90 days	Backlog, prioritized by capacity

Exposed secrets are always treated as **critical**, regardless of CVSS score, requiring immediate revocation and rotation of the affected credential and an audit of the preceding 30 days of access. Every vulnerability is triaged within 48 hours of detection. Exceptions and formal risk acceptances require documented justification, compensating controls, and a reassessment date no later than 90 days out.

8. Artificial Intelligence security and governance

- The platform's AI controls are designed against the **NIST AI RMF**, which is also present in the product's control catalog.
- Model inference runs primarily on **Amazon Bedrock** in the AWS us-east-1 region, where prompts and outputs stay within AWS and are not shared with model developers. The Anthropic and OpenAI APIs are configured as contingency providers and may be used for continuity.
- Customer data is not used for model training, per the commercial terms of every AI provider in use.
- A model can only be enabled after a compliance and subprocessor review; unreviewed models remain blocked in the platform's model routing.
- Guardrails and content tokenization/minimization are applied before model calls, reducing unnecessary exposure of personal data to processing.
- AI operations are recorded in an audit log storing hashes of inputs rather than the original content, avoiding the persistence of personal data in logs.
- Every agent output that influences a risk decision is traceable back to the control and evidence that produced it.

9. Business continuity and resilience

Parameter	Commitment
Target availability (SLA)	99.5% monthly
RTO — Recovery Time Objective	Under 4 hours
RPO — Recovery Point Objective	Under 24 hours
Backup	Automated daily backups of the production database, encrypted at rest
Public status page	status.aranis.ai — independent external monitoring
Recovery runbook	Documented and reviewed after every P0/P1 incident

10. Incident response

Aranis maintains a formal incident response process covering detection, triage, containment, eradication, recovery, and communication, aligned with Article 48 of the LGPD.

- **Detection sources:** continuous security scanning, infrastructure and application logs and alarms (Amazon CloudWatch), external availability monitoring, subprocessor security bulletins, and customer reports.
- **Classification:** severities P0 through P3, with automatic escalation to critical when customer data is at risk.
- **Communication:** affected customers are notified within the applicable regulatory windows; the national authority (ANPD) is notified when required.
- **Recordkeeping:** every incident is logged with detection and resolution timestamps, severity, affected systems, root cause, and corrective actions.
- **Post-incident:** mandatory review of the runbook and the Risk Register after P0/P1 incidents.

11. Privacy and personal data protection

- Legal basis mapped per processing purpose, in accordance with the LGPD.
- A Data Processing Agreement (DPA) is made available to customers, including subprocessing and international transfer clauses.
- Customer data is hosted in the United States (AWS us-east-1). International transfers are supported by Standard Contractual Clauses (SCCs) in provider DPAs and by adequacy assessment of the receiving country.
- Data subject rights (access, correction, deletion, portability) are served through a documented process.
- Customers can delete their data and their account at any time, directly in the platform. Retention and disposal are governed by the Data Retention and Disposal Policy.
- Customers are notified 30 days in advance of the addition of any new subprocessor.

12. Subprocessors

Active subprocessors as of the issue date of this document. The complete and current list is maintained at trust.aranis.ai.

Subprocessor	Category	Data processed	Location
Amazon Web Services	Hosting, database, storage, AI (Bedrock), email (SES)	Customer, user, and assessment data; evidence; AI prompt content	USA (us-east-1)
Cloudflare	DNS / CDN / perimeter	Data in transit, traffic	Global
Anthropic	AI / LLM (contingency)	AI prompt content, when routed	USA
OpenAI	AI / LLM (contingency)	AI prompt content, when routed	USA
Stripe	Payments	Billing data; tokenized card	USA
Resend	Transactional email	Email addresses and message content	USA
Inngest	Job orchestration	Event payloads	USA
BetterStack	Availability monitoring / status page	Uptime telemetry (no customer data)	EU / USA
GitHub / Microsoft	Version control and code security	Source code (no customer data)	USA
Atlassian	Documentation / management	Internal documentation (no customer data)	USA / AU

13. Reference frameworks

Aranis controls — both those applied internally and those offered by the product — are anchored in the following frameworks:

- **NIST CSF 2.0** — Govern, Identify, Protect, Detect, Respond, Recover functions
- **ISO/IEC 27001:2022** — control clauses applicable to a cloud-native environment
- **ISO 22301** — business continuity
- **NIST AI RMF** — AI systems governance
- **CSA CCM / CAIQ v4** — basis of the CSA STAR Level 1 self-assessment
- **LGPD** (Brazilian Law 13.709/2018) and **GDPR** (Regulation EU 2016/679)
- **AICPA Trust Services Criteria** — preparatory crosswalk for SOC 2
- **MITRE ATT&CK** — mapping of adversary techniques to controls

14. Contact and verification

Purpose	Channel
Security questions and due diligence	security@aranis.ai
Privacy and data subject rights (DPO)	privacy@aranis.ai
Vulnerability disclosure	security@aranis.ai
Trust Center and public documentation	trust.aranis.ai
Real-time operational status	status.aranis.ai

Detailed control evidence, the full CAIQ, and internal policies can be made available to customers and prospects under a confidentiality agreement.

15. Revision history

Version	Date	Changes
2.1	November 19, 2026	Production migrated to AWS (us-east-1): database (self-hosted Supabase), Amazon S3 storage, and AI on Amazon Bedrock, with Anthropic and OpenAI as contingency providers. Updated DevSecOps tooling, observability, backup description, data deletion, and subprocessor list. Operating entity updated. CSA STAR registry date corrected to July 6, 2026.
2.0	July 8, 2026	Initial public version in PT/EN/ES.