# Synthetic Users Internal Risk Assessment

**Version:** 1.0

**Assessment Date:** 15 February 2026

**Prepared by:** Artur Ventura, CTO & CISO

**Reviewed by:** Kwame Ferreira, CEO

**Next Review:** February 2027

---

## 1. Purpose

This document presents the results of Synthetic Users' annual internal risk assessment, identifying threats to the confidentiality, integrity, and availability of company and customer data, evaluating the effectiveness of existing controls, and documenting residual risks and remediation plans.

---

## 2. Scope

This assessment covers:

- SaaS platform infrastructure and operations
- Corporate systems and employee endpoints
- Third-party and subprocessor dependencies
- Data processing and storage
- Personnel and organizational risks
- Regulatory and compliance obligations (GDPR, SOC 2)

---

## 3. Methodology

The assessment was conducted using the following approach:

1. **Asset identification** — Catalogued all technology assets, data stores, and third-party dependencies from the asset inventory and subprocessor registry.
2. **Threat identification** — Identified threats across categories: external attacks, insider threats, operational failures, third-party risks, regulatory non-compliance, and natural/environmental events.
3. **Vulnerability analysis** — Reviewed penetration test results, vulnerability scans, incident history, and control documentation.
4. **Impact and likelihood scoring** — Each risk scored on a 5-point scale for likelihood and impact, producing a risk rating (Low / Medium / High / Critical).
5. **Control evaluation** — Assessed effectiveness of existing controls for each risk scenario.
6. **Residual risk determination** — Documented remaining risk after controls are applied.

### Risk Rating Matrix

| | Impact: Minimal | Impact: Low | Impact: Moderate | Impact: High | Impact: Critical |
|---|---|---|---|---|---|
| **Likelihood: Very Likely** | Medium | Medium | High | Critical | Critical |
| **Likelihood: Likely** | Low | Medium | High | High | Critical |
| **Likelihood: Possible** | Low | Medium | Medium | High | High |
| **Likelihood: Unlikely** | Low | Low | Medium | Medium | High |
| **Likelihood: Rare** | Low | Low | Low | Medium | Medium |

# 4. Risk Assessment Results

## 4.1 External Threats

| ID | Risk Scenario | Likelihood | Impact | Existing Controls | Control Effectiveness |
|---|---|---|---|---|---|
| R-01 | **Unauthorized access to production systems** | Unlikely | Critical | SSO with MFA (Google Firebase), RBAC, least privilege, no SSH access, Cloudflare WAF | Strong |
| R-02 | **Data breach / exfiltration of customer data** | Unlikely | Critical | Encryption at rest (AES-256) and in transit (TLS 1.2+), S3 Object Lock, Google Workspace DLP, GitHub secret scanning, RBAC | Strong |
| R-03 | **Ransomware attack** | Unlikely | High | Immutable backups (S3 compliance mode), endpoint anti-malware (macOS XProtect), no SSH access, containerized infrastructure | Strong |
| R-04 | **DDoS attack on platform** | Possible | Moderate | Cloudflare DDoS protection, WAF, rate limiting, bot management | Strong |

| | | | | | |
|---|---|---|---|---|---|
| R-05 | **Phishing / social engineering targeting employees** | Likely | Moderate | SSO+MFA, Google Workspace phishing protection, SPF/DKIM/DMARC, security awareness training, auto-forward disabled | Adequate |
| R-06 | **Supply chain attack (compromised dependency)** | Unlikely | High | GitHub secret scanning, Dependabot, automated dependency updates, code review, SDLC security scanning | Adequate |
| R-07 | **API abuse or scraping** | Possible | Low | Cloudflare rate limiting, bot management, API authentication, audit logging | Strong |

## 4.2 Insider Threats

| ID | Risk Scenario | Likelihood | Impact | Existing Controls | Control Effectiveness |
|---|---|---|---|---|---|
| R-08 | **Unauthorized data access by employee** | Unlikely | High | RBAC, least privilege, unique user IDs, semi-annual access reviews, audit logging | Strong |

| | | | | | |
|---|---|---|---|---|---|
| R-09 | **Accidental data exposure (misconfiguration, secret leak)** | Possible | Moderate | GitHub secret scanning, code review, infrastructure-as-code, no SSH, Render managed config | Adequate |
| R-10 | **Departing employee retains access** | Unlikely | Moderate | 24-hour access revocation on termination, SSO-based access (single revocation point), access review policy | Strong |

## 4.3 Operational & Infrastructure Risks

| ID | Risk Scenario | Likelihood | Impact | Existing Controls | Control Effectiveness | Re Ris |
|---|---|---|---|---|---|---|
| R-11 | **Primary hosting provider (Render) outage** | Unlikely | High | Pre-configured AWS failover (RTO: 4h), data stored on AWS not Render, DRP documented and tested | Strong | Lo |
| R-12 | **AI provider (OpenAI) outage** | Possible | Moderate | Multi-model failover (Anthropic, Google, Meta, | Strong | Lo |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Mistral), RTO: 2h | | |
| R-13 | **AWS regional outage** | Rare | Critical | Multi-AZ replication, regional data storage, immutable backups | Adequate | Me |
| R-14 | **Data loss or corruption** | Rare | Critical | Continuous backups (RPO: 15min), S3 Object Lock compliance mode, versioning, annual restore testing | Strong | Lo |
| R-15 | **Authentication provider (Google Firebase) outage** | Unlikely | High | Documented SSO configuration for rapid provider switch, cached sessions for short-term continuity | Adequate | Me |

## 4.4 Third-Party & Subprocessor Risks

| ID | Risk Scenario | Likelihood | Impact | Existing Controls | Control Effectiveness | Re Ris |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| R-16 | **Subprocessor data breach** | Unlikely | High | Third-party risk management policy, DPA requirements, SOC 2/ISO 27001 verification, annual vendor reviews | Adequate | Me |
| R-17 | **Subprocessor non-compliance with data protection** | Unlikely | Moderate | DPA contractual obligations, subprocessor disclosure, advance notice of changes, right to object | Adequate | Lo |
| R-18 | **Open-source dependency vulnerability** | Likely | Moderate | Dependabot automated scanning, SDLC dependency management, vulnerability SLAs (Critical: 24h remediation) | Adequate | Me |

## 4.5 Regulatory & Compliance Risks

| ID | Risk Scenario | Likelihood | Impact | Existing Controls | Control Effectiveness | Res Risk |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| R-19 | **GDPR non-compliance (breach notification failure)** | Unlikely | Critical | Incident response plan with 72-hour notification, DPA obligations, privacy policy, data deletion procedures | Strong | Lov |
| R-20 | **SOC 2 control failure** | Unlikely | High | Sprinto continuous monitoring, annual SOC 2 Type II audit, documented policies, evidence retention | Strong | Lov |
| R-21 | **Failure to meet client contractual SLAs** | Unlikely | Moderate | BCP with RTO/RPO/MTD, DRP, annual DR testing, multi-provider redundancy | Strong | Lov |

## 4.6 Personnel Risks

| ID | Risk Scenario | Likelihood | Impact | Existing Controls | Control Effectiveness | Resi Risk |
|---|---|---|---|---|---|---|
| R-22 | **Loss of key personnel (key-person risk)** | Possible | Moderate | Cross-training, documented procedures, infrastructure-as-code, BCP | Adequate | Med |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | personnel section | | |
| R-23 | **Insufficient security awareness** | Unlikely | Moderate | Annual security awareness training, monthly security focus topics, quarterly interactive sessions, phishing simulations | Adequate | Low |

## 5. Risk Summary

| Residual Risk Level | Count | Risk IDs |
|---|---|---|
| **Critical** | 0 | — |
| **High** | 0 | — |
| **Medium** | 9 | R-01, R-02, R-05, R-06, R-09, R-13, R-15, R-16, R-18, R-22 |
| **Low** | 14 | R-03, R-04, R-07, R-08, R-10, R-11, R-12, R-14, R-17, R-19, R-20, R-21, R-23 |

No critical or high residual risks identified. Medium residual risks are accepted with existing controls and monitored through ongoing review.

## 6. Remediation and Action Items

| ID | Risk | Action | Priority | Owner | Target Date |
|---|---|---|---|---|---|
| R-05 | Phishing / social engineering | Increase phishing simulation frequency from annual to quarterly | Medium | Security Lead | Q2 2026 |
| R-06 | Supply chain attack | Implement Software Bill of Materials (SBOM) generation for production builds | Medium | CTO | Q3 2026 |
| R-09 | Accidental data exposure | Implement pre-commit hooks for additional secret detection patterns | Low | CTO | Q2 2026 |
| R-13 | AWS regional outage | Document and test cross-region failover procedure | Medium | CTO | Q3 2026 |
| R-15 | Google Firebase outage | Document alternative authentication failover procedure | Medium | CTO | Q2 2026 |
| R-22 | Key-person risk | Expand cross-training program and document runbooks for all critical operations | Medium | CEO | Q2 2026 |

## 7. Assessment Participants

| Name | Role | Contribution |
|---|---|---|
| Artur Ventura | CTO & CISO | Lead assessor, technical risk evaluation, control effectiveness review |

| | | |
|---|---|---|
| Kwame Ferreira | CEO | Business impact evaluation, risk acceptance decisions |
| Zumbi Ferreira | CFO | Financial impact assessment, insurance coverage review |

## 8. References

- SOC 2 Type II Report 2025
- Penetration Test Report 2025
- Business Impact Analysis
- Incident Response Plan
- Third-Party Risk Management Policy
- Vulnerability Management Policy
- Data Loss Prevention Policy

## 9. Approval

This risk assessment has been reviewed and approved by the executive team. Residual risks are accepted within the organization's risk appetite. Remediation items will be tracked to completion and verified at the next assessment cycle.

| Name | Role | Date |
|---|---|---|
| Artur Ventura | CTO & CISO | 15 February 2026 |
| Kwame Ferreira | CEO | 15 February 2026 |