A P R I T Y

Aprity — Security Whitepaper

Enterprise Security Architecture & Controls

PUBLIC

Version 1.0 | March 2026 | aprity.ai

1. Executive Summary

Aprity is an enterprise SaaS platform that analyzes Salesforce metadata to produce functional, technical, and compliance-ready documentation. Security is foundational to the platform's design, not an afterthought.

Key security principles:

- **Metadata-only access** — Aprity never reads, stores, or processes your business data (Accounts, Contacts, Opportunities, etc.)
- **Zero-trust architecture** — Every API call is cryptographically signed and verified
- **Strict tenant isolation** — Your data is physically partitioned from other customers at the database level
- **No secrets in code** — All credentials are stored in a hardware-backed vault
- **Azure-native** — Built exclusively on Microsoft Azure with enterprise-grade security controls

2. What Data Does Aprity Access?

2.1 Accessed (Salesforce Metadata Only)

Category	Examples
Code	Apex classes, triggers, test classes
Automation	Flows, Process Builders, Workflow Rules
Configuration	Custom objects, fields, record types, page layouts
Security config	Permission sets, profiles, sharing rules
Validation	Validation rules, formula fields

2.2 Never Accessed

Category	Guarantee
Business records	No Accounts, Contacts, Opportunities, Cases, or any standard/custom object records
Files & attachments	No documents, images, or file content
User credentials	No passwords, tokens, or session IDs of your users
Personal data	No email content, phone numbers, or addresses

> *Aprity uses the **Salesforce Metadata API** (read-only). It is technically impossible for the platform to access record-level data through this API.*

3. Authentication & Authorization

3.1 Salesforce Package to Aprity Backend (HMAC-SHA256)

Every API call from your Salesforce org to Aprity is signed using **HMAC-SHA256**:

- A unique **256-bit secret** is generated during installation and stored in your Salesforce org's Protected Custom Settings
- Each request includes a cryptographic signature computed from: tenant ID, org ID, timestamp, nonce, and request body hash
- **Replay attack protection**: Every request includes a unique nonce (used once) and a 5-minute timestamp window
- The secret is returned **once** during initial registration and never transmitted again

3.2 Aprity Backend to Salesforce (JWT Bearer OAuth 2.0)

Aprity authenticates to your Salesforce org using the industry-standard **JWT Bearer flow**:

- **RSA-2048** key pair — private key stored exclusively in Azure Key Vault
- Each customer configures their own **Connected App** in Salesforce — no shared credentials
- Access tokens have a **15-minute lifetime** and are not stored
- Certificate rotation supported with **zero downtime** (dual-slot mechanism)

3.3 Admin Console

- Separate authentication layer with API key validation
- All administrative actions are logged in an immutable audit trail
- Role-based access control

4. Encryption

4.1 In Transit

Layer	Protocol
Client to Aprity	HTTPS / TLS 1.2+
Aprity to Salesforce	HTTPS / TLS 1.2+
Aprity to Azure services	Azure internal TLS
Aprity to AI providers	HTTPS / TLS 1.2+

4.2 At Rest

Storage	Encryption
Azure Cosmos DB	AES-256, Microsoft-managed keys
Azure Blob Storage	AES-256, Microsoft-managed keys
Azure Key Vault	HSM-backed (FIPS 140-2 Level 2)

5. Secret Management

All secrets are stored in **Azure Key Vault**, a FIPS 140-2 Level 2 certified service:

- Private keys for JWT authentication
- HMAC installation secrets
- AI provider API keys
- Third-party integration tokens (Confluence, etc.)

Secrets are never:

- Hardcoded in source code
- Written to log files
- Stored in the application database
- Returned in API responses (except the one-time installation secret)
- Included in error messages

Access to Key Vault uses **Azure Managed Identity** — no connection strings or credentials are needed in the application.

6. Network Security

Aprity is deployed on **Microsoft Azure** with enterprise-grade network isolation:

- **Virtual Network (VNet)** with dedicated subnets for compute, data, and management
- **Private Endpoints** for all data services (database, storage, cache) — no public internet exposure
- **DNS Private Zones** for internal service resolution
- **No inbound ports** open to the internet except the API gateway (HTTPS/443)

7. Audit & Monitoring

7.1 Application-Level Audit

Event	Logged
API authentication (success/failure)	Yes
Replay attack attempts	Yes
Scan lifecycle (start, progress, completion, failure)	Yes
Administrative actions	Yes
AI provider interactions (metadata only)	Yes

7.2 Infrastructure Monitoring

- **Azure Application Insights** for real-time telemetry
- **Structured logging** with tenant context on every log entry
- **Health endpoints** for uptime monitoring

8. Vulnerability Management

- OWASP ZAP security scanning performed regularly
- Salesforce AppExchange Security Review compliance
- Dependency scanning for known vulnerabilities
- Parameterized database queries (no SQL/NoSQL injection)
- Input validation on all API endpoints

9. Incident Response

In the event of a security incident:

1. **Detection** — Automated monitoring and alerting via Azure Application Insights
2. **Containment** — Affected tenant isolated; HMAC secrets can be rotated immediately
3. **Investigation** — Full audit trail available (API calls, scan events, admin actions)
4. **Notification** — Affected customers notified within 72 hours per GDPR requirements
5. **Remediation** — Root cause analysis and preventive measures documented

10. Compliance Summary

Standard	Status
GDPR	Compliant (see Data Privacy document)
Salesforce AppExchange Security Review	Passed
Azure SOC 2 Type II	Inherited from Microsoft Azure
HTTPS/TLS enforcement	Enforced globally
Data residency (EU)	Azure France Central region

Contact

For security questions or to request a penetration test authorization:

Email: security@aprity.ai

Website: https://aprity.ai

This document describes the security architecture of the Aprity platform as of March 2026. For the most current information, please contact our security team.