



archyl

Security Whitepaper

Comprehensive overview of security practices, infrastructure, and compliance measures

Version 3.0 • September 27, 2026

Classification: Public

EKO Consulting • EURL • SIRET 842 435 547 00026 • France

Executive Summary

Archyl is an AI-powered architecture documentation platform designed with security as a foundational principle. This document outlines our comprehensive approach to protecting customer data and maintaining a secure service.

Key Security Highlights

- TOTP-based Multi-Factor Authentication with single-use challenges and recovery codes
- AES-256-GCM encryption at rest for all sensitive fields, with Argon2id key derivation
- Object storage encryption at rest (AES-256) for uploaded file attachments
- Database SSL required by default (sslmode=require)
- OAuth 2.0, SAML 2.0 and OIDC single sign-on, with browser-bound state and PKCE
- Server-side session revocation on password change and MFA removal
- Tenant isolation enforced per resource and guarded by automated regression tests
- Outbound request protection (SSRF) on every user-configurable integration
- Strict Content-Security-Policy with hashed inline scripts and Subresource Integrity
- Automated security scanning in CI/CD: govulncheck, CodeQL, gitleaks, Trivy
- Ten rounds of internal penetration testing in 2026, all findings remediated
- Non-root, read-only, capability-dropped container execution

Infrastructure Overview

Archyl's infrastructure is built on containerized services with security hardening at every layer, from runtime to monitoring.

Component	Technology	Security Features
Backend Runtime	Go 1.26 / Fiber 3.5	Structured logging, panic recovery, read/idle timeouts
Database	PostgreSQL 18-alpine	SSL required, parameterized queries
Cache	Redis 8-alpine	Localhost-only binding
Object Storage	Google Cloud Storage (S3-compatible)	Private buckets, AES-256 at rest, short-lived signed URLs
Frontend	React 19.2 / TypeScript 6.0 / Vite 8	Hash-based CSP, SRI on CDN scripts, sanitized Markdown
Container Runtime	Alpine 3.24	Non-root (UID 10001), read-only root filesystem, multi-stage builds
Migration Tool	Atlas 0.31	Pinned version, SHA-256 checksum verified at build
Monitoring	Prometheus 3.9.1 / Sentry 0.47	Bearer token auth on metrics, disabled in production without a token
AI Provider	OpenAI (optional), or self-hosted Ollama	Code signatures, not full source; per-request size caps
Payment	Stripe SDK 86.4	Webhook HMAC-SHA256 verification

Data Protection

Encryption at Rest

Credentials and customer content are encrypted at the application level using AES-256-GCM with per-operation random 12-byte nonces. Field-level encryption is mandatory: the service refuses to start without an encryption key.

- **Credentials:** OAuth tokens, API keys, MFA secrets, recovery codes, marketplace credentials, repository access tokens, cloud connection settings
- **Customer content:** names, descriptions and tags of C4 elements and relationships; ADRs, documentation, comments, API contracts, flows, whiteboards, snapshots and change history — encrypted by the application before they reach the database
- **Not field-encrypted:** identifiers, links between elements, timestamps, diagram positions, and account e-mail addresses and names, which the database must index
- **Key derivation:** The field-encryption key is derived from the configured secret with Argon2id (memory-hard); older records remain readable and are re-encrypted on write
- **Encryption key:** Required at startup (minimum 32 characters)
- **Signing keys:** The JWT secret is required at startup (minimum 32 characters). MFA challenges, SSO/OAuth state and integration state are signed with separate purpose-bound keys derived via HKDF-SHA256, so no token type can be replayed as another
- **Secret hygiene:** Credentials are never serialized in API responses; integration settings are redacted on every read path

File Attachments

Files uploaded to documentation (images, PDFs, and other documents) are kept in S3-compatible object storage rather than in the database:

- **Storage:** Google Cloud Storage on Archyl Cloud; self-hosted deployments may configure any S3-compatible provider (AWS S3, MinIO, Cloudflare R2).
- **Encryption at rest:** AES-256, applied by the storage provider by default (customer-managed keys supported via Cloud KMS on Google Cloud Storage).
- **Access:** Buckets are private and never publicly listable; files are served only through short-lived, signed URLs generated on demand.

Encryption in Transit

All network communications are protected using modern encryption protocols:

- **External Traffic:** TLS 1.3 for all external connections
- **Database Connections:** SSL required by default (sslmode=require)

Data Classification

- **Customer Content:** Architecture diagrams, documentation, ADRs, API contracts, and uploaded file attachments — encrypted at rest and isolated per organization
- **Account Data:** User profiles protected by access controls; OAuth tokens and MFA secrets encrypted at rest
- **Usage Data:** Analytics and metrics — anonymized, no PII

Authentication & Access Control

User Authentication

Archyl implements a multi-layered authentication system:

Method	Implementation	Security Measures
Sessions (JWT)	HS256 only (algorithm pinned)	Configurable expiry; all earlier sessions revoked server-side on password change or MFA removal
OAuth 2.0	GitHub, GitLab, Bitbucket	Signed state bound to the initiating browser, verified provider email before account linking, server-side token storage
Enterprise SSO	SAML 2.0, OpenID Connect	SP-initiated only, InResponseTo and nonce checks, browser-bound single-use state, domain-bound identities
MFA	TOTP (RFC 6238)	Single-use challenge tokens, 8 bcrypt-hashed recovery codes, AES-256-GCM encrypted secret
Password reset	Emailed, time-limited link	No account enumeration; token invalidated once the password changes; no session issued
API Keys & MCP	Scoped (read by default)	Hash-based storage, project restrictions, write scope required for every mutation, OAuth 2.1 with mandatory PKCE S256 and allow-listed redirect URIs
Rate Limiting	Per IP, per account, per token	Login: 5/min per IP+email and 10/min per email; MFA: 5 per challenge; password reset: 3 per 15 min per email; 30/min per IP on all auth endpoints

Authorization Model

Archyl uses a role-based access control (RBAC) system:

- **Organization Owners:** Full administrative access, billing management
- **Team Admins:** Team and project management within their scope
- **Team Members:** Read/write access to assigned projects
- **Viewers:** Read-only access via share links

Tenant Isolation

Every request that addresses a resource by identifier is authorized against that resource's project or organization, not only against the caller's current organization. The same rule applies to the MCP server used by AI agents, where a central guard resolves the owning organization of every identifier argument and denies the call when it cannot:

- Authorization checks fail closed: an error while resolving ownership is a denial
- Resources that do not exist and resources the caller cannot see return the same response
- Automated tenancy and route-coverage tests fail the build if a guard is removed or a new identifier is left unchecked
- Membership uniqueness is enforced at the database level, so a role change always applies

Application Security

Secure Development Practices

- **CI/CD Pipeline:** go vet, golangci-lint, govulncheck, CodeQL, gitleaks secret scanning, Trivy image and IaC scanning, frontend lint, type checks and tests

- **Supply Chain:** GitHub Actions pinned to commit SHAs, build tools checksum-verified, third-party browser scripts version-pinned with Subresource Integrity
- **Input Validation:** go-playground/validator on all mutation endpoints; size caps on uploads, archives and AI requests
- **Container Security:** Non-root execution, pinned dependencies, multi-stage builds
- **Security Headers:** Content-Security-Policy (hash-based script-src), X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy
- **Outbound Requests:** Every integration that calls a customer-supplied URL (self-hosted git, AI endpoints, webhooks, cloud connectors, MCP connectors) uses a client that refuses private, loopback and cloud-metadata addresses, including after redirects
- **Code Execution Boundaries:** Repository URLs are validated before any git operation, git transports are restricted to HTTP(S), and agent workspaces reject paths that resolve into repository control files, including through symbolic links
- **Abuse Protection:** Metered AI quotas are reserved atomically in the database, and all public and webhook endpoints are rate limited

OWASP Top 10 Mitigations

Vulnerability	Mitigation
Injection	Parameterized queries via GORM, argument separators on every git command, sanitized e-mail headers
Broken Authentication	OAuth 2.0, SSO, MFA, layered rate limiting, bcrypt, session revocation, security event logging
Sensitive Data Exposure	AES-256-GCM with Argon2id-derived keys, TLS 1.3, server-side token storage, redacted API responses
XML External Entities	JSON APIs; SAML responses parsed by a hardened library with signature and request-ID validation
Broken Access Control	Resource-bound authorization on every identifier, fail-closed guards, automated tenancy tests, API key scoping
Security Misconfiguration	Mandatory secrets, security headers, hardened containers and Helm defaults (no default passwords)
XSS	React escaping, sanitized Markdown, hash-based CSP, sandboxed viewers
Insecure Deserialization	Type-safe JSON parsing with struct validation
Vulnerable Components	govulncheck, CodeQL and Trivy in CI, pinned dependency versions
SSRF	Outbound client blocking private, loopback and metadata addresses
Insufficient Logging	Structured security event logging, Sentry, Prometheus

Network Security

Archyl's network architecture follows defense-in-depth principles:

- **Port Binding:** Every published service port bound to 127.0.0.1 in the reference deployment
- **Database SSL:** SSL connections required by default
- **CORS Policy:** Restricting allowed origins to configured domains

- **Object Storage:** Private buckets accessed only via short-lived signed URLs
- **Metrics Protection:** Prometheus metrics require a bearer token and are not served in production when none is configured
- **Connection Timeouts:** Read and idle timeouts on every HTTP server (slow-client protection)
- **Error Handling:** Sanitized error messages, no stack traces in production

Container & Kubernetes Hardening

- All images run as a numeric non-root user (UID 10001)
- Helm chart defaults: runAsNonRoot, read-only root filesystem, all Linux capabilities dropped, no privilege escalation, RuntimeDefault seccomp profile, resource limits
- No default database password is shipped; credentials are generated or supplied as secrets

Third-Party Services

Archyl carefully selects third-party services based on their security posture and compliance certifications:

Service	Purpose	Data Location	Certifications
Google Cloud Storage	Object storage for documentation attachments	Configurable region	ISO 27001/27017/27018, SOC 2/3
Stripe	Payment processing	US (EU data center)	PCI-DSS Level 1, GDPR
OpenAI	AI analysis (optional)	US	DPA available
Mailgun	Transactional e-mail	US / EU	SOC 2, GDPR
Sentry	Error tracking	US / EU	GDPR, SOC 2
GitHub	OAuth & repo access	US	SOC 1/2, ISO 27001
GitLab	OAuth & repo access	US / EU	SOC 2, ISO 27001
Bitbucket	OAuth & repo access	US / EU	SOC 2, ISO 27001

AI Processing Note

- AI-powered features (architecture discovery, AI chat, coding agents) use OpenAI on Archyl Cloud, or a self-hosted Ollama instance. Organizations may also bring their own provider key, in which case they contract with that provider directly. Architecture discovery sends code signatures (imports, type and function declarations), the repository structure and existing architecture documentation — never full source code. OpenAI does not use API data to train its models.

Object Storage Note

- On Archyl Cloud, documentation file attachments are stored in Google Cloud Storage. Self-hosted deployments configure their own S3-compatible storage and remain the sole controller of that bucket; if storage is not configured, file attachments are simply unavailable.

Compliance & Certifications

GDPR Compliance

Archyl supports its customers' obligations under the General Data Protection Regulation:

- **Data Residency:** Configurable via SERVER_DATAREGION
- **Data Processing Agreement:** Available for all customers
- **Right to Access:** Users can export all data via /users/me/export
- **Right to Erasure:** Full cascade account deletion (including stored file attachments)
- **Data Portability:** JSON export
- **Privacy by Design:** Minimal data collection, purpose limitation
- **Cookie Consent:** Banner with accept/decline

SOC 2 Type 1

- Readiness assessment completed
- Independent CPA audit pending
- Security controls aligned with Trust Service Criteria

Security Testing

Between July and September 2026 Archyl ran ten rounds of internal penetration testing against the production application, the MCP server, the managed-agent runtime and the self-hosted distribution. Every finding was remediated and covered by a regression test before the round was closed.

Area	Controls added or strengthened
Tenant isolation	Resource-bound authorization across the HTTP API and the MCP server, fail-closed guards, tenancy and route-coverage tests in CI
Authentication	Login, MFA and password-reset rate limits; single-use MFA challenges; session revocation; self-service password reset; invitation-bound account verification
Federation	Browser-bound OAuth state, SP-initiated SAML with request-ID validation, OIDC nonce, token returned in the URL fragment only
Outbound requests	SSRF-safe HTTP client on every customer-configurable integration
Code execution	Repository URL validation, restricted git transports, symlink-safe agent workspaces
Cryptography	Argon2id key derivation for field encryption, purpose-separated signing keys
Business logic	Atomic AI quota reservation, unique memberships, request size caps, HTTP timeouts
Platform	Hash-based CSP with SRI, hardened containers and Helm chart, checksum-verified build tools, CI security scanning

An independent third-party penetration test is planned as part of the SOC 2 audit.

Incident Response

Response Process

Archyl maintains a documented incident response procedure:

1. **Detection:** Automated monitoring, security event logging, Sentry alerting
2. **Triage:** Severity classification and team notification
3. **Containment:** Immediate actions to limit impact
4. **Investigation:** Root cause analysis and evidence collection

- 5. **Remediation:** Fix implementation and verification
- 6. **Communication:** Customer notification within 72 hours for data breaches (GDPR Art. 33)
- 7. **Post-Mortem:** Lessons learned and preventive measures

Security Event Logging

The following security events are automatically logged:

- Failed login attempts (email, IP)
- Invalid/expired JWT tokens and use of revoked sessions (IP, user agent, path)
- Invalid/expired API keys (IP, user agent, path)
- Failed MFA verification and replayed MFA challenges (user ID, IP)
- Password-reset requests, failures and completions
- SSO/OAuth state that fails browser binding
- Rejected OAuth client registrations (disallowed redirect URIs)
- Credentials passed in URLs and cloud connections configured without TLS verification

Security Contact

Report Security Issues

- If you discover a security vulnerability, please report it responsibly.
- **Email:** security@archyl.com
- **Response Time:** Initial acknowledgment within 24 hours

We appreciate security researchers who help us maintain the security of our platform.

Document Control

Field	Value
Version	3.0
Last Updated	September 27, 2026
Classification	Public
Owner	Archyl Security Team
Review Cycle	Quarterly or upon significant changes

Company Information

- **Company Name:** EKO Consulting
- **Legal Form:** EURL (Entreprise Unipersonnelle à Responsabilité Limitée)
- **SIRET:** 842 435 547 00026
- **Country:** France