Rhenari Security Overview

For IT, security, and procurement evaluation

Rhenari Built by Catalystium, Inc.
rhenari.com | security@rhenari.com

Rhenari is continuous roadmap monitoring for SaaS product leaders. It reads behavioral metadata from the collaboration, project management, and development tools teams already use and surfaces execution health in Microsoft Teams. This document summarizes Rhenari's security posture for initial evaluation. A detailed architecture review is available under NDA.

HOSTING & INFRASTRUCTURE

Platform	Fully Rhenari-hosted SaaS on Microsoft Azure
Deployment	Nothing is deployed into the customer's Azure subscription or cloud environment
Client install	Microsoft Teams personal app only
Data residency	Region-specific hosting available by contract
Disaster recovery	Geographically separated DR environment with defined RPO/RTO targets

DATA HANDLING

Rhenari reads signals — not content. It processes behavioral metadata: who communicated with whom, when, how often, and in what pattern.

- ✓ Message bodies, email text, and long-form content are never written to storage
- ✓ Source content is read ephemerally, processed in memory, and discarded
- ✓ Structured analytical output is persisted; source content is not
- ✓ Individual-level behavioral data is never surfaced to any user
- ✓ All outputs are team-level and anonymized; minimum group sizes enforced
- ✓ Customer data is never used to train AI models
- ✓ Customer data is never sold or shared with third parties

ENCRYPTION

At rest	AES-256
In transit	TLS 1.2+ across all application, bot, and integration traffic
Credentials	Integration secrets stored in Rhenari-managed vault, namespaced by tenant; never exposed through UI or API

AUTHENTICATION & ACCESS

User auth	Microsoft Teams SSO — no separate login or credentials
Access model	Role-based access with tenant and department scoping
Employee access	Production data access is restricted, role-gated, time-bound, requires justification, and is fully audited

TENANT ISOLATION

Every operation is scoped to a single tenant context. Tenant isolation is enforced across identity, API, credential storage, data processing, analytics, and serving layers. No cross-tenant data is ever in scope for any process or query.

COMPLIANCE POSTURE

Precise claims only. We do not overclaim.

SOC 2	Type II controls mapped and operating. Not yet certified. Architecture review available on request.
HIPAA	BAA available where applicable. Healthcare-grade privacy controls where contractually required.
GDPR	Rhenari acts as Data Processor. DPA available on request.
ISO 27001	Annex A controls mapped. Available for review.

INCIDENT RESPONSE

Documented incident response plan with defined severity levels, escalation timelines, and authority boundaries. Customers are notified of security incidents affecting their data in accordance with contractual commitments and applicable law.

SUBPROCESSORS

Rhenari's infrastructure runs on Microsoft Azure. A complete subprocessor list is available upon request as part of DPA execution.

OFFBOARDING

Upon cancellation, customers may request an export of scored output history, insights, alert history, workflow records, and configuration snapshots. Following the export window, Rhenari disables access and deletes tenant data per the offboarding policy and contractual terms.

PROCUREMENT

Available through Microsoft Marketplace. MACC-eligible. Billing managed through your existing Microsoft relationship. No separate

vendor contract required for self-service plans.

Detailed architecture review available under NDA

Full technical architecture documentation, privacy architecture, isolation model details, compliance control mappings, and infrastructure topology are available for qualified evaluators under mutual NDA.

Request a review

security@rhenari.com

rhenari.com/security