DeRISK™ Platform — Security & Deployment Overview

How the DeRISK Platform deploys in your environment, what data it uses, and how it protects that data — for IT/OT security and infrastructure teams.

WHAT THE PLATFORM DOES

The DeRISK Platform translates OT cyber exposure into financial risk metrics — giving industrial organizations and their insurance partners a shared, quantified view of risk. Three products, each with a distinct role:

- **DeRISK™ CRQ** — Cyber risk quantification in financial terms
- **DeRISK™ QVM** — Vulnerability prioritization by financial impact
- **DeRISK™ UWA Agentic** — Agentic underwriting workflow augmentation

DEPLOYMENT OPTIONS

Product	SaaS	On-Premises	API
DeRISK CRQ	✓	—	—
DeRISK QVM	✓	—	—
DeRISK UWA Agentic	✓	✓ (AWS · Azure · GCP)	✓

SaaS hosted on AWS with US and EU data residency options. Data residency region selected at onboarding and does not change without customer consent.

↑ What leaves your network

Anonymized asset metadata · Vulnerability lists · Abstracted network topology · Control system categories · Configuration summaries. No raw values. No operational data.

✕ What never leaves

Raw OT traffic · Process values and setpoints · Historian data · PLC/HMI configurations · Credentials · Proprietary operational data of any kind

⊙ How connectors work

Read-only queries to your OT visibility platform APIs. No software installed on OT assets. No write access of any kind. Outbound HTTPS only.

SECURITY POSTURE

Data encryption — STANDARD

All customer data is encrypted at rest and in transit using current industry-standard algorithms. Data is anonymized at the point of ingestion — asset identifiers are replaced with internal references before any processing occurs.

Access control — AVAILABLE

Role-based access control (RBAC) is enforced across all platform functions. Multi-factor authentication (MFA) is required. Single sign-on (SSO/SAML 2.0) is available on Professional and Enterprise tiers.

Tenant isolation — ENFORCED

Each customer's data is logically isolated at the data layer. Enterprise customers receive dedicated compute environments. Cross-tenant data access is not architecturally possible in any deployment configuration.

Audit trail — IMMUTABLE

Every data access, model operation, API call, and user action is logged to an immutable audit trail. Logs are traceable to source, pipeline step, and model version. Export available on request.

Security certification — SOC 2 TYPE II

The platform is SOC 2 Type II certified, covering security, availability, and confidentiality trust service criteria. The certification report is available to qualified prospects on request.

Independent assurance — ANNUAL

Annual third-party security assessment by an independent firm. A full security review package — including assessment findings and data processing agreements — is available to prospects on request.

INTEGRATION & NETWORK REQUIREMENTS

Connector requirements (SaaS)

TRAFFIC Outbound HTTPS from your network to DeNexus. No inbound connections are initiated by DeNexus to your environment.

PROTOCOL HTTPS only. No additional firewall rules required beyond standard outbound web traffic.

AUTHENTICATION API key per connector, rotatable at any time. Keys are stored encrypted and are never logged in plaintext.

SYNC CADENCE Configurable: hourly, daily, or on-demand. Connectors transfer metadata only — no bulk data export.

ACCESS SCOPE Read-only API permissions to your OT visibility platform. No write operations are requested or possible.

UWA Agentic — on-premises deployment

RUNTIME Containerized deployment. Runs on your infrastructure — cloud-hosted (AWS, Azure, GCP) or private data center.

DATA RESIDENCY In on-premises mode, all data remains within your managed environment. No external connectivity is required once deployed.

AIR-GAP Fully air-gapped deployment is available on Enterprise tier for environments with strict isolation requirements.

API ACCESS RESTful API available for integration with internal systems. OpenAPI specification provided at onboarding.

REGULATORY & COMPLIANCE COVERAGE

Framework	Status	Scope	Notes
SOC 2 Type II	✓ **Certified**	Platform-wide	Security, availability, confidentiality. Report available under mutual NDA.
GDPR	✓ **Compliant**	EU data subjects	Data processing agreement available. EU data residency option available.
US / NAIC	✓ **Addressed**	UWA Agentic	Model law and guidance requirements addressed in workflow and audit outputs.
UK / FCA & Lloyd's	✓ **Addressed**	UWA Agentic	FCA AI principles and Lloyd's market requirements addressed in design.
EU / EIOPA	✓ **Addressed**	UWA Agentic	Solvency II data requirements and EIOPA guidance incorporated.
NERC CIP	Reference alignment	CRQ / QVM	Platform outputs support NERC CIP-013 supply chain risk documentation.

KEY COMMITMENTS

01 **Read-only access only.** Connector agents are granted read-only permissions. No write operations to your OT visibility platform or OT assets are ever requested or performed.

02 **Your OT data stays in your environment.** Raw OT traffic, process values, historian data, and device configurations never leave your network under any deployment model.

03 **Your data is not used to train shared models.** Data processed on your behalf is used exclusively to generate your outputs. It is never used to train or improve DeNexus models for other customers.

04 **Full security documentation available.** SOC 2 Type II report, independent assessment findings, and data processing agreements are available to qualified prospects prior to deployment.