SYNTRIX Security Overview

Our Approach to Security

SYNTRIX is designed for environments where trust matters. Security is treated as a foundational system property, not an optional feature.

Our approach emphasizes **risk reduction, controlled access, and operational discipline**.

Core Security Principles

Least Privilege
Access is limited to what is required for platform functionality.

Secure Authentication
Modern authentication patterns are used. Raw credentials for third-party platforms are not requested.

Isolation by Design
Customer environments are logically isolated.

Defense-in-Depth
Security controls exist at multiple layers.

Data Handling Philosophy

- Data is processed only to deliver platform functionality
- Customer data is not sold or monetized
- Access to data is restricted and logged

Integrations & Permissions

SYNTRIX connects to external systems only with explicit authorization.

Permissions requested align with documented platform functionality.

Incident Handling

We maintain internal procedures for:

- Issue detection
- Impact assessment
- Remediation actions

We do not publicly disclose sensitive response details.

Responsible Disclosure

We encourage responsible vulnerability reporting through private channels.

Important Clarifications

SYNTRIX does not:

- Certify compliance
- Replace internal security controls
- Guarantee threat prevention

It provides **decision-support and visibility**, not security enforcement.