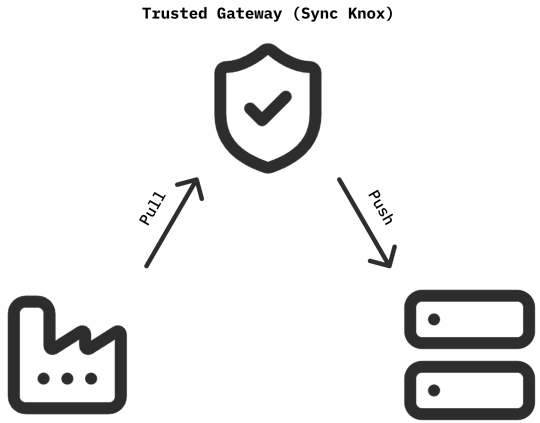
Cybersecurity at Sync Motion

Security by Design

Security is not an afterthought in our solutions, it is the foundation of everything we build. Every component is built with a secure by design approach, ensuring that protection is embedded at every level rather than added as an extra layer. We follow a strict zero-trust philosophy, meaning no device or application is inherently trusted, even in airgapped networks. Every interaction must be verified, authenticated, and authorized. This principle applies consistently across networks, transport layers, and applications.

Communication Model

Our network topology is designed with one guiding principle: strict separation between industrial environments and software environments. Communication takes place exclusively through a trusted gateway device, ensuring no direct network traffic can flow between the two domains.



The gateway operates on a secure pull-and-push model. It collects data from shop-floor devices and forwards it to application devices, while blocking all incoming traffic from both directions. By enforcing this one-way data flow, the gateway provides a robust safeguard that protects critical operations from external threats while ensuring reliable availability.

Layered Security Model

All communication across our environments is protected by a strict three-layer security model, ensuring end-to-end protection at every stage:

Network Security

We enforce rigorous firewall rules that block any traffic from untrusted networks, protocols, or devices. Fine-grained checks on both source and destination guarantee that only authorized communication paths are permitted.

Transport Security

To achieve a true zero-trust communication model, we implement mutual TLS (mTLS) with X.509 authentication between all applications and endpoints, using Envoy proxy in sidecar deployments. This means both client and server must authenticate with trusted certificates, which are validated for the correct tenant.

We configure TLS manually to allow only version 1.3, hardened cipher suites, and secure certificate algorithms. Certificates are rotated regularly to maintain the highest level of cryptographic security.

Application Security

At the application protocol level, we enforce strict authentication mechanisms, such as OPC-UA or MQTT with strong policy requirements. These include robust password standards, minimum security specifications, and protocol-specific safeguards to ensure that only verified applications can communicate.

SYNC MOTION

Business Impact

Certification-Ready

Our security framework is fully aligned with internationally recognized standards such as ISO/IEC 27001 and NIS-2 Directive requirements. This reduces certification effort and accelerates audit readiness.

Regulatory Peace of Mind

With security controls built into every layer, we stay ahead of evolving EU and global regulations. Customers gain assurance that our solutions comply with stringent industrial cybersecurity obligations.

Trust & Reputation

A zero-trust, secure-by-design architecture signals to partners and clients that data and operations are protected by industry best practices. This builds long-term trust and confidence.

Operational Continuity

By minimizing cyber risk at the architecture level, we safeguard uptime and reliability - ensuring critical industrial processes remain protected from disruption.

Future-Proof Standard

Our layered model represents a gold standard in industrial cybersecurity, embedding resilience, compliance, and risk management into every deployment.