# ZERO TRUST SPA™ — LAYER 3

*Trusted Data Management*

## Overview

**MIP Zero Trust SPA™ secures and orchestrates data across the MIP Stack using its Symmetrical Parallel Aggregation (SPA™) architecture, enabling policy-based access, modular flow, and segmentation. Built for regulated environments, it protects IP, ensures data integrity, and supports trusted, distributed operations. It serves as the architectural backbone for secure interoperability between edge, cloud, and air-gapped systems.**

## Key Features

- Protocol-agnostic encrypted telemetry pipeline
- Policy-driven access control across all layers of the MIP stack
- Multi-tenant and audit-ready with event logging
- Segmentation and isolation of critical data zones
- Built-in compliance tooling aligned with NIST, ISO, and CMMC

## How it Works

SPA™ secures all data traffic between modules using a Zero Trust model. It validates identity, context, and policy before allowing any read/write operation across the MIP Stack. All communications are encrypted, logged, and isolated by default unless explicitly configured. SPA™ also establishes the foundation for future-ready, quantum-resilient architectures through Quantum Secure SPA™ alignment.

## Use Cases

- Enforce secure, policy-based access across all MIP Stack data flows
- Segment network traffic to isolate sensitive or regulated operations
- Encrypt telemetry for secure transmission within and across facilities
- Align with regulatory frameworks (NIST, ISO, CMMC) for OT cybersecurity
- Prevent unauthorized access during audits or remote sessions

## Advantages

- Protects critical systems and sensitive data
- Reduces audit burden and access risks
- Enables secure remote and partner operations
- Aligns with NIST, ISO, and CMMC frameworks
- Enforces Zero Trust at every telemetry node

BC AUTOMATION