MaestroIQ + SecurityIQ

CYBER DEFENSE AND OBSERVABILITY FOR CONNECTED TRANSIT INFRASTRUCTURE

The Challenge



Transit agencies today operate complex, hybrid infrastructures that span **IT networks** (back office, cloud, passenger Wi-Fi) and **OT systems** (signals, SCADA, CAD/AVL, fare collection, vehicle systems, CCTV).
As these environments converge, new vulnerabilities emerge that can impact safety, service continuity, and compliance.

Key Security Challenges

IT/OT Convergence Risks

Legacy operational systems like SCADA and PLCs weren't built with cybersecurity in mind.
When connected to enterprise networks for analytics or remote management, they expose new attack surfaces.
Limited segmentation means malware in IT can pivot into OT environments.

Ransomware and Supply Chain Attacks

Transit agencies have been targets of ransomware that halt fare systems, dispatch centers, or control operations.
Vulnerabilities in third-party hardware, software, or vendor portals create exploitable entry points.

Visibility Gaps

Most agencies lack a complete, continuously updated asset inventory across IT and OT.
Without real-time monitoring, unauthorized devices or rogue access points can persist unnoticed.

Compliance and Data Protection

FTA and TSA directives now require cyber incident reporting and periodic risk assessments.
Passenger data and payment systems demand strict protection of personally identifiable information (PII).

Insider Threats and Access Control

Contractors, vendors, and multiple departments share system access — often without consistent oversight.
Poor identity management enables privilege misuse and lateral movement across networks.

The ConnX Advantage

MaestroIQ
provides AI-driven observability and performance assurance.
Together, they help agencies modernize operations, enhance safety, and mitigate cyber risk — all within a unified platform.

SecurityIQ
delivers real-time threat detection and Zero Trust defense.

ConnX Bridges IT, OT, and IoT Into One Secure, Intelligent Fabric.

Together, they create an intelligent fabric that helpS agencies modernize operations, enhance safety, and mitigate cyber risk — all within a unified platform.

OUR CUSTOMERS GAIN:

- **Clarity across every connected system**
- **Confidence through AI-driven security**
- **Control with automated response and compliance insight**

www.connxai.com +1-609-438-6100 connxsales@connxai.com

ConnX AI

ConnX MaestroIQ

ConnX SecurityIQ

Core Capabilities

SecurityIQ Cyber Intelligence	• Continuous monitoring across IT, OT, and IoT networks • Real-time threat detection and automated response • Zero Trust access control and micro-segmentation • Risk-based analytics and mitigation workflows • SOC/SIEM integration (Splunk, QRadar, SecureX) • Compliance mapping to NIST, IEC 62443, ISO 27001, FTA/TSA
MaestroIQ AIOps Platform	• End-to-end observability and service assurance • Predictive analytics and performance monitoring • Automated correlation and root-cause analysis • Unified dashboards for operational and security metrics
Cisco Cyber Vision + Industrial Networking	• Deep visibility into industrial protocols (Modbus, PROFINET, OPC UA) • Ruggedized, encrypted connectivity across depots, substations, and vehicles
ConnX Managed Services	• 24×7 monitoring and lifecycle management • SOC integration and compliance reporting • Continuous improvement via monthly KPI dashboards

Key Benefits



Unified Visibility
End-to-end observability across IT, OT, and IoT



Proactive Defense
AI-driven detection, Zero Trust access, and automated incident response



Compliance Confidence
Audit-ready reporting aligned with leading security frameworks



Operational Resilience
24×7 monitoring, predictive maintenance, and lifecycle management

POSITIONING STATEMENT

ConnX SecurityIQ + MaestroIQ combine AI-powered observability with Zero Trust cyber defense to protect the modern transit ecosystem.

Together, they empower agencies to operate smarter, safer, and more resiliently — with full compliance and confidence.

www.connxai.com +1-609-438-6100 connxsales@connxai.com