



ConnX Network Security Assessment

Unified Security Visibility Across IT, OT, and IoT

The Challenge Organizations Face

Modern organizations operate highly interconnected environments that span:

- **Enterprise IT systems**
- **Operational Technology (OT) and industrial networks**
- **IoT devices, sensors, and edge systems**

These environments were often built at different times, by different teams, with different security assumptions—creating blind spots, weak segmentation, and unmanaged risk.

Traditional security assessments frequently focus only on IT, leaving OT and IoT environments under-assessed or misunderstood.

YOU CANNOT SECURE WHAT YOU CANNOT SEE—AND YOU CANNOT DEFEND WHAT YOU DO NOT UNDERSTAND.

UNDERSTAND YOUR TRUE NETWORK RISK—BEFORE IT BECOMES AN INCIDENT.

A comprehensive, standards-aligned security assessment of IT, OT, and IoT networks—designed to identify risk, validate controls, and strengthen cyber and operational resilience.

The ConnX Difference

ConnX brings together **enterprise security rigor** and **operational technology awareness**—a critical combination in modern environments.

- **Integrated IT, OT, and IoT security expertise**
- **Standards-aligned, audit-ready methodology**
- **Vendor-neutral, objective assessment**
- **Clear translation of technical risk into executive insight**

What the ConnX Network Security Assessment Delivers

The ConnX Network Security Assessment provides a holistic, defensible evaluation of network security posture across IT, OT, and IoT environments.

THIS ENGAGEMENT HELPS ANSWER CRITICAL QUESTIONS SUCH AS:

- Where are our most significant cyber and operational risks?
- Are IT, OT, and IoT environments properly segmented and protected?
- How effective are our current network security controls?
- How aligned are we with recognized security standards and frameworks?

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

ConnX AI

Scope of the Assessment

Network Architecture, Design & Segmentation
- Audit of network topology, trust zones, and segmentation
- Validation of isolation controls between IT, OT, and IoT environments
- Identification of pathways that increase lateral movement risk

Perimeter & Internal Network Security
- Firewalls, gateways, VPNs, and secure remote access
- Internal network controls and east–west traffic restrictions
- Review of access pathways into critical environments

Network Devices & Configuration
- Routers, switches, industrial networking equipment, and IoT gateways
- Identification of misconfigurations, weak encryption, and insecure protocols
- Review of firmware, lifecycle status, and hardening practices

OT & Industrial Network Security
- Assessment of ICS and OT network security posture
- Review of industrial protocols using safety-aware methodologies
- Alignment with NIST SP 800-82 and OT-relevant ISO controls

IoT Network Security
- Device onboarding, authentication, and encryption
- Network access controls and segmentation
- Identification of unmanaged, shadow, or high-risk devices

Network Access Control & Identity
- Authentication mechanisms and role-based access
- Privileged access pathways
- Third-party, vendor, and contractor connectivity

Vulnerability, Logging & Detection
- Network-level vulnerability identification
- Risk analysis incorporating operational and safety impact
- Logging, monitoring, and anomaly detection capabilities
- Integration with SIEM, SOC, and incident response processes

Standards & Compliance Mapping
- Alignment with:
  - ISO/IEC 27001 & 27002
  - NIST Cybersecurity Framework (CSF)
  - NIST SP 800-53 and 800-82
- Identification of control gaps and maturity levels

Deliverables

Executive Summary
Overall network security posture and risk profile

Detailed Assessment Findings
Technical observations with evidence

Risk & Maturity Analysis
IT, OT, and IoT environments

Standards Mapping
ISO and NIST alignment overview

Prioritized Remediation Roadmap
Clear, actionable next steps

The Outcome

- **Unified visibility across IT, OT, and IoT security posture**
- **Reduced cyber, operational, and safety risk**
- **Increased confidence in audit and regulatory readiness**
- **Stronger segmentation and containment of threats**
- **A defensible, prioritized path to improved resilience**

The ConnX Assessment & Audit Process

Discovery & Intake
- Stakeholder interviews
- Architecture and documentation review
- Identification of regulatory and operational priorities

Security Audit & Assessment
- Network architecture and configuration analysis
- Control validation across IT, OT, and IoT
- Risk identification using standards-aligned methodologies

Findings & Risk Insights
- Identification of security gaps and exposure points
- Risk-based prioritization incorporating business and safety impact
- Security maturity observations

Actionable Security Roadmap
- Clear remediation recommendations
- Alignment to ISO and NIST controls
- Practical roadmap to strengthen security posture

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