FRENOS

OPTICA – THE RAPID OT VISIBILITY SERVICE

SECURE OT WITHOUT PERFECT VISIBILITY

The OT Security Visibility Challenge

Traditional OT security approaches force organizations to choose between operational stability and security confidence. Active scanning tools risk disrupting essential processes or networks, while deploying passive monitoring sensors across hundreds or thousands of locations proves neither feasible nor scalable. This visibility gap creates fundamental business risks, preventing organizations from quantifying their security posture, demonstrating regulatory compliance, or making informed security investments.

The Optica Solution— Bridging The OT Visibility Gap

Optica provides what has long eluded OT security teams: scalable, comprehensive asset visibility. Using sophisticated modeling techniques on your existing OT datasets, Optica creates detailed representations of your network environment including:

- Precise hardware specifications & configurations
- Accurate software inventories with version details
- Protocol implementations and communications pathways

Unlike traditional OT discovery tools that require extensive scanning or time-consuming sensor deployments, Optica builds this intelligence through a template-based approach that leverages existing knowledge while filling critical gaps.

ABOUT OPTICA

Optica isn't another asset inventory tool or appliance. It's the OT security industry's first **"tech-enabled rapid visibility service"** providing a framework allowing asset owners to begin assessing, prioritizing, and proactively defending their operational technology networks.
By creating high-fidelity virtual representations of critical infrastructure, Optica enables what was previously impossible; comprehensive OT security analysis without complete asset visibility.

Optica + Frenos Platform
Continuous OT Security Posture Management

TRANSCENDING THE LIMITATIONS THAT HAVE HISTORICALLY HAMPERED CRITICAL INFRASTRUCTURE SECURITY

THE VISIBILITY BARRIER:	No more waiting for perfect asset inventory before conducting meaningful security analysis
THE RISK QUANTIFICATION CHALLENGE:	Replace subjective assessments with simulation-based evidence of actual attack feasibility
THE OPERATIONAL VS. SECURITY DIVIDE:	Test security improvements without impacting operational systems
THE COMPLIANCE DOCUMENTATION BURDEN:	Generate comprehensive assessment documentation automatically through simulation