Solution Brief

The OT Blind Spot

Executive Summary

As IT and OT networks converge, hidden device-level risks are growing. Rogue or spoofed hardware can bypass existing controls, exposing operations and compliance.

Sepio delivers device-level risk intelligence, uncovering every connected asset and detecting anomalies at the physical layer—so organizations gain true asset awareness, reduce risk, and maintain uptime without disruption.

The Challenge: Incomplete Visibility Across the Physical Layer

- Shadow Assets: Unmanaged controllers, sensors, and converters outside inventories.
- IT/OT Convergence: IP-based networks introduce IT threats into OT environments.
- Unverified Hardware: Legacy and vendor devices lack authenticity checks.
- Compliance Gaps: Standards like CISA, NIST, and ISA/IEC require full asset visibility.

Outcomes

- Full visibility of every device in the OT network.
- Smaller attack surface by removing rogue and unknown assets.
- Greater uptime through early detection of anomalies.
- Simplified compliance with accurate, verified inventories.
- Actionable insights for faster, smarter decisions.

The Sepio Approach: Risk Insight from the Physical Layer

Sepio provides a single source of truth for all connected hardware—across IT, OT, and IoT environments. Its patented Device DNA technology identifies, fingerprints, and classifies every device at the physical-signal level, revealing what traditional discovery tools miss.

- Asset Discovery: Finds every connected device—managed or unmanaged.
- DNA Identification: Authenticates hardware and detects spoofed devices.
- Risk Scoring: Quantifies exposure and prioritizes response.
- Integration: Strengthens NAC, SIEM, and SOC workflows.

Customer Example: Industrial Manufacturer

A global manufacturer deployed Sepio across its converged OT network and uncovered previously invisible assets—including unmanaged serial converters and unauthorized wireless bridges. These components were creating potential lateral-movement paths between production and corporate networks. Within weeks, Sepio's insights guided policy updates and segmentation improvements, resulting in a 42% reduction in unmanaged device risk exposure and full alignment with NIST and ISA/IEC requirements.

Conclusion

Protecting OT environments requires visibility that reaches beneath the software layer. By detecting and validating every device—legitimate or malicious—Sepio empowers organizations to secure critical operations, maintain compliance, and reduce risk.

See everything. Control everything. Trust nothing by default.

About Sepio

Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any scale. The only trafficless solution, Sepio is infinitely scalable to protect the company's decentralized, uncontrolled ecosystem as fast and often as anyone, anywhere connects any assets. Sepio provides actionable visibility with the asset risk score based on a unique AssetDNA generated for each asset at its physical layer source, reflecting actual business, location, and rules. Sepio radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust solutions that simply see only the assets they are there to protect.

Visit: www.sepiocyber.com