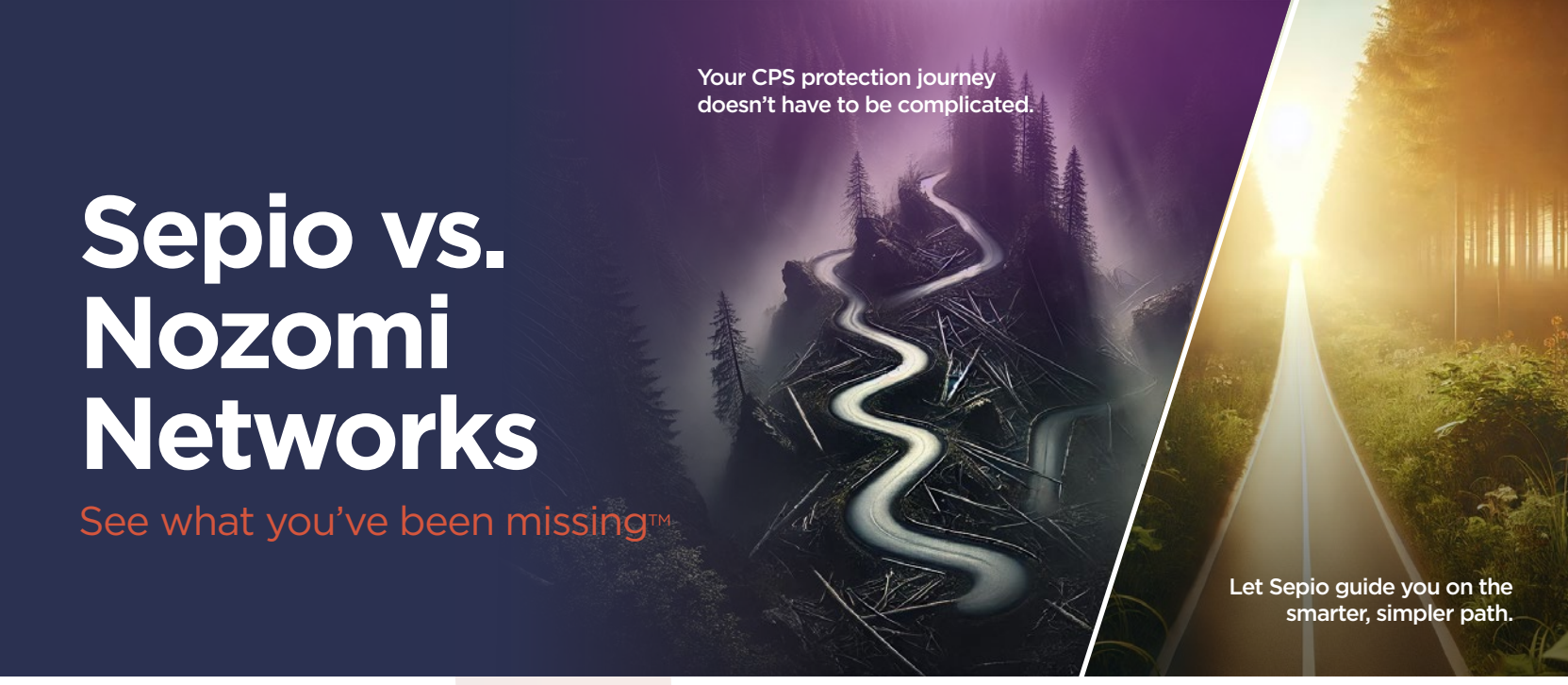

Sepio vs. Nozomi Networks

See what you've been missing™

Enjoying CPS protection with complete asset visibility and Zero Trust Hardware Access without relying on network traffic analysis or active scanning. Eliminate complexity and ensure seamless deployment, at scale.

Trafficless Approach

Sepio delivers full visibility and control across converged IT, OT, IoT, and CPS environments without depending on packet inspection, traffic mirroring, or sensor-heavy architectures. By leveraging physical-layer data and AssetDNA, Sepio reveals the actual identity of connected hardware, including rogue, hidden, unmanaged, and dormant devices that may otherwise evade detection.

Field-Proven And Scalable

Designed for distributed and complex environments, Sepio scales across sites, business units, and infrastructure types with minimal architectural burden. Its trafficless approach supports rapid deployment, low operational overhead, and consistent visibility across global environments.

Policy Enforcement

Sepio enables granular policy enforcement based on the actual hardware identity, location, and trust posture of each asset. With Zero Trust Hardware Access, organizations can move from visibility to control, integrating with existing security stacks while also supporting direct device-level enforcement at the hardware layer.

Nozomi

Asset Intelligence: Limitations And Challenges

- **Asset visibility limitations**
  Nozomi is well known for OT, IoT, and CPS visibility, but its approach is still largely centered on network-observable behavior and sensor-driven analysis. That can make it harder to identify assets that are silent, spoofed, MAC-less, intermittently connected, or intentionally designed to avoid generating meaningful traffic.

- **Detection of non-communicating and hardware-level threats**
  Where visibility depends on observed communications, devices such as passive implants, covert taps, unauthorized peripherals, and certain dormant hardware threats may remain difficult to identify in real time. Organizations seeking the hardware truth of a device, rather than just its declared or behavioral identity, may still face blind spots.

- **Architectural complexity**
  Deployments that rely on sensors, collectors, packet capture points, or mirrored traffic can introduce architectural and operational complexity. In large or segmented environments, that may increase deployment effort, create tuning overhead, and add long-term maintenance burdenensuring network taps at all critical points.

The Sepio Advantage

Sepio eliminates visibility blind spots by operating at the physical layer. Instead of inferring trust from traffic, behavior, or declared identity, Sepio validates what the device actually is. This allows organizations to discover rogue, hidden, unmanaged, spoofed, MAC-less, dormant, and non-communicating assets across IT, OT, IoT, and CPS environments.

Sepio's trafficless architecture removes the need for complex sensor placement, SPAN ports, TAPs, or packet-analysis-heavy deployments. The result is simpler rollout, faster time to value, lower operational overhead, and more scalable asset intelligence across distributed environments.

With Zero Trust Hardware Access, Sepio goes beyond visibility. It provides the ability to enforce policy based on hardware truth, helping organizations reduce risk before a threat escalates. This supports faster mitigation, stronger compliance alignment, and more precise control over connected infrastructure.

Nozomi

Risk Management And Vulnerability Prioritization: Limitations

- **Risk driven by observed behavior**
  Platforms focused primarily on network communications are often strongest when assets are active and producing observable signals. That can delay detection of risks associated with silent, dormant, or deception-based hardware threats.

- **Limited hardware trust validation**
  Without physical-layer validation, risk scoring may still depend on software-level attributes, traffic patterns, or inferred context. That can make it more difficult to distinguish between a legitimate device and a spoofed or tampered one.

- **Enforcement dependency**
  Where enforcement depends mainly on third-party tools and orchestration, the ability to take immediate action at the exact point of hardware trust failure may be less direct than in a platform designed around hardware-native trust and control.

The Sepio Advantage

Why accept blind spots in risk management? Sepio takes a proactive approach by using physical-layer visibility to identify risk before it becomes incident activity. Rather than waiting for suspicious communications, Sepio establishes hardware truth at the source.

Sepio's risk evaluation is based on actual device identity, trustworthiness, location, and policy context. This gives security teams actionable intelligence that supports faster prioritization, more precise mitigation, and stronger operational confidence.

Unlike architectures that depend primarily on traffic analytics, Sepio helps organizations address a class of threats that can otherwise persist unseen inside the environment. That is the foundation of Zero Trust Hardware Access: do not assume the device is what it claims to be.

Capability	Sepio	Nozomi
Short deployment time	●●●●●	●●○○○
Asset discovery	●●●●●	●●●●●
Rogue / shadow asset detection	●●●●●	●●●●○
Hardware identity validation	●●●●●	●●○○○
Response automation and scalable expansion	●●●●○	●●○○○
MITM / covert implant detection	●●●●●	●●○○○
No hardware sensors required	●●●●●	●○○○○
3rd-party integrations	●●●●○	●●●●○
Policy enforcement / mitigation	●●●●○	●●●●○

> **It lacks the capacity to respond to detected threats. Expansion capacity is too costly. The process is not automated.**

Gartner peerinsights™

Learn more at: **sepiocyber.com**

SEPIO