Sepio Vs. Claroty

See what you've been missing™

Enjoying CPS protection platform 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.

> "Sepio's trafficless approach takes away the need for traditional sensors, probes or crawlers. This supports easy deployment and low architectural complexity."
>
> Leading analyst covering the CPS PP market.

TRAFFICLESS APPROACH

Sepio delivers full visibility and control across your converged IT, OT, and IoT infrastructure. No need for multiple tools or complex deployments — our trafficless solution , based on physical layer data ,uncovers the complete hardware-based attack surface, boosting security and operational efficiency across your entire environment.

FIELD-PROVEN AND SCALABLE

Designed for complex, globally distributed environments, Sepio scales effortlessly—supporting multiple sites with ease. From local facilities to multinational operations, organizations rely on Sepio to deliver consistent visibility and control without compromising performance.

POLICY ENFORCEMENT

Sepio provides the ability to set and enforce granular policies across CPS environments. This helps teams respond more efficiently to potential risks, reduce noise, and maintain alignment with internal controls and compliance needs.

CLAROTY

ASSET INTELLIGENCE: LIMITATIONS AND CHALLENGES

- **Asset Inventory:** Claroty does not have full asset visibility across converged IT,IoT and OT environments, organizations may face blind spots that leave them exposed to unmanaged(shadowIT) or unauthorized devices —particularly at the physical layer.
- **Limited Detection of Non-Communicating Devices:** Claroty's asset discovery relies on network activity, making it ineffective at identifying non-communicating, MAC-less, or passive hardware implants. Devices such as unmanaged switches, covert network taps, or rogue USB peripherals can remain undetected, creating security gaps in critical infrastructure.
- **Scaling Constraints:** Deployment requires network access (SPAN ports, etc.), which can be complex. Potential for alert fatigue if not tuned for OT environments. Scaling requires ensuring network taps at all critical points.

THE SEPIO ADVANTAGE

Sepio eliminates visibility blind spots by operating at the physical layer (Layer 1), ensuring complete asset inventory across IT, OT, and IoT environments—including non-communicating, MAC-less, and passive hardware devices that traditional network-based solutions miss. Unlike platforms that rely on traffic monitoring, Sepio detects rogue, hidden, and unmanaged devices the moment they connect, providing instant visibility into Shadow IT and unauthorized hardware.

Sepio's trafficless approach removes the need for complex network access configurations like SPAN ports or network taps, making deployment simple, scalable, and infrastructure-agnostic. Because Sepio does not rely on packet analysis, it avoids alert fatigue caused by excessive network noise, instead providing accurate, actionable intelligence on every connected device. Whether across a single site or globally distributed environments, Sepio scales effortlessly, delivering continuous asset trust verification and risk management at any scale.

CLAROTY

Risk Management and Vulnerability Prioritization: Limitations

- **Limited Enforcement Capabilities:** Claroty's reliance on third-party tools for enforcement (e.g., NAC, firewalls) may limit the ability to take immediate action at the device level, especially in environments where segmentation or access control needs to be tightly enforced.
- **Reactive Rather Than Proactive Approach:** Without real-time physical layer insights, risk detection is often based on observed network activity, potentially delaying the identification of rogue or stealthy threats that operate outside traditional monitoring methods.
- **Risk Prioritization Challenges:** The absence of comprehensive, actionable risk metrics can make it difficult to accurately prioritize threats, potentially delaying response to critical issues.

THE SEPIO ADVANTAGE

Why accept blind spots in risk management? Sepio takes a proactive approach by leveraging physical-layer visibility to detect and mitigate threats before they escalate. Unlike solutions that rely on network activity for risk detection, Sepio identifies rogue, hidden, and MAC-less devices-whether or not they communicate-eliminating blind spots at the hardware level. Sepio's real-time risk prioritization goes beyond software vulnerabilities, assessing each asset's physical identity and trustworthiness to provide granular, actionable risk metrics. Unlike platforms that depend on third-party enforcement tools, Sepio enables immediate policy enforcement and device blocking at the hardware layer. Our Zero Trust Hardware Access approach ensures real-time threat mitigation, enforcement of granular security policies, and seamless integration with your existing security stack for rapid, automated response. With comprehensive compliance support for frameworks like NIST, NERC CIP, and NDAA 889, Sepio provides the full visibility and control needed to eliminate risk—before it becomes a threat.

Feature	Sepio	Claroty
Short Deployment time	●●●●●	●●○○○
Asset discovery	●●●●●	●●●○○
Asset Protection	●●●●●	●●○○○
Vulnerability management	●●●○○	●●●○○
Peripherals detection	●●●●●	○○○○○
HBOM monitoring	●●●●●	○○○○○
MiTM and dormant device detection	●●●●●	●●○○○
No hardware sensor	●●●●●	○○○○○
3rd. Party integrations	●●●●○	●●●●○

> "It has weakness for insight menu. I mean, there has too much insights to follow-up that the solution show us. It need to be more prioritize in the future. It is hard to manage things like this. Its integration limitations can be a challenge for organizations seeking a more comprehensive, cross-network solution."

Gartner peerinsights.

Learn more at: **sepiocyber.com**

SEPIO