Sepio vs. Armis

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

While Sepio's software only approach, does not rely on traffic, Armis relies mainly on passive & agentless methods, creating critical blind spots, especially for OT assets, & risking misclassification & false positives, exposing organizations to cyber threats.

NO HIDDEN COSTS

Sepio's solution package is all inclusive, while Armis advanced features are sold separately, meaning customers need to make additional investments to reap the full benefits of Armis.

BUSINESS OPERATION CONTINUITY

Sepio's trafficless approach does not put sensitive OT network timing at risk, while Armis depends on network traffic probes for device visibility, which can lead network timing changes that can put business operations at risk.

ARMIS

ASSET INTELLIGENCE: LIMITATIONS AND CHALLENGES

- **Security Coverage Limitations:** Prioritizes asset visibility and risk assessment but lacks built-in proactive network security, real-time threat detection, and response mechanisms to prevent incidents before they arise.
- **Setup and Maintenance Challenges:** Relies heavily on third-party integrations, requiring significant fine-tuning, which adds complexity and raises the total cost of ownership (TCO).
- **Versatility Without Specialization:** Like a Swiss Army knife, it offers flexibility in asset visibility and vulnerability management but lacks deep specialization—making it a secondary option when a more tailored solution is unavailable.

THE SEPIO ADVANTAGE

Sepio redefines asset intelligence by delivering **unmatched accuracy and control** over connected devices. Unlike traditional solutions that rely on passive network monitoring, Sepio leverages **physical-layer visibility** to detect and classify all IT, OT, and IoT assets-**even those invisible to other tools**. With **real-time risk assessment and granular device trust enforcement**, Sepio prevents threats **before they materialize**, eliminating blind spots and reducing attack surfaces. When it comes to securing your critical infrastructure, **Sepio doesn't just identify risks-it neutralizes them.**

ARMIS

LIMITED INCIDENT RESPONSE: INCREASED RISK EXPOSURE

- **No Built-in Incident Response:** Armis relies solely on third-party integrations for incident response, lacking native capabilities to correlate multiple data sources and uncover hidden threats.
- **Slower Threat Resolution**: Dependence on external tools leads to longer response times, increased complexity, and disjointed workflows that slow down remediation efforts.
- **Reactive Rather Than Proactive:** Without integrated response capabilities, proactive threat mitigation and prevention are significantly limited, leaving organizations more vulnerable to evolving cyber risks.

THE SEPIO ADVANTAGE

Why accept blind spots in your asset security? Sepio takes a **proactive** approach to risk management, leveraging **physical-layer visibility** to detect and mitigate threats before they escalate. Unlike solutions that rely on network traffic monitoring, **Sepio uncovers rogue, hidden, and spoofed devices-eliminating attack surfaces at the hardware level.** Our zero-trust hardware access approach ensures **real-time risk assessment**, enforcement of granular policies, and seamless integration with your existing security stack for rapid, automated response.

With comprehensive compliance support for popular frameworks, Sepio ensures you're always audit-ready. **Risk isn't just managed-it's eliminated**.

Feature	Sepio	Armis
Short Deployment time	●●●●●	●●○○○
Asset discovery	●●●●●	●●●○○
Asset Protection	●●●●●	●●○○○
Vulnerability management	●●●○○	●●●○○
Peripherals detection	●●●●●	○○○○○
HBOM monitoring	●●●●●	○○○○○
MiTM and dormant device detection	●●●●●	●●○○○
Offline/Air gapped deployment	●●●●●	●●○○○
3rd. Party integrations	●●●●○	●●●●○

> **WHAT DO YOU DISLIKE MOST ABOUT ARMIS CPS PROTECTION PLATFORM?**
>
> The constant upkeep and administration of the tool and your span ports and collectors has become a real headache... When you manage 75-150 of these collectors that are in 45 different countries and start having random issues that require you to almost become a full time admin for this tool that was supposed to be "set it and forget it" has become quite the opposite.

Gartner peerinsights.

Learn more at: **sepiocyber.com**

SEPIO