# Sepio VS. Lansweeper

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, LS relies depends heavily on traditional network scanning techniques (WMI, SSH, SNMP, etc.), creating critical blind spots, especially for OT assets,& risking misclassification & false positives, exposing organizations to cyber threats.

## POLICY ENFORCEMENT

While Sepio's solution provides extensive enforcement capabilities, Zero Trust hardware controls, and physical layer validation across multiple interfaces (USB/Ethernet/HWBOM), LS positions itself just as an asset management solution, and it's not equipped to handle advanced threat scenarios involving physical access.

## BUSINESS OPERATION CONTINUITY

Sepio's trafficless approach does not put sensitive OT network timing at risk, while LS depends on active asset scanning, which can lead network timing changes that can put business operations at risk.

Lansweeper

## ASSET INTELLIGENCE: LIMITATIONS AND CHALLENGES

- **Security Depth Gaps:** Lansweeper lacks built-in enforcement, real-time threat detection, and physical-layer inspection-making it insufficient for organizations seeking advanced risk mitigation.
- **Operational Blind Spots:** Without USB monitoring, rogue device detection, or HBOM awareness, Lansweeper cannot surface hidden or spoofed hardware that often bypasses traditional discovery methods.
- **Generalist by Design:** While versatile for ITAM and software asset management, Lansweeper is not purpose-built for cyber-physical infrastructure protection-offering breadth over depth and leaving critical infrastructure partially exposed.

## THE SEPIO ADVANTAGE

Sepio delivers true asset intelligence by going beyond inventory to provide **deep, hardware-level visibility and control**. While Lansweeper catalogues devices based on software and network presence, Sepio leverages **physical-layer data** to identify and validate all connected assets-including **spoofed, rogue, and unmanaged devices** invisible to scan-based tools. Sepio enforces Zero Trust Hardware Access policies in real time, ensuring every device is continuously verified and trusted. With built-in detection of **USB-borne threats, HBOM risks**, and **hardware-based impersonation**, Sepio eliminates operational blind spots and proactively reduces exposure—protecting what Lansweeper can't see.

Lansweeper

## LIMITED INCIDENT RESPONSE AND RISK EXPOSURE MANAGEMENT

Lansweeper provides broad asset visibility but lacks native incident response capabilities-there is no built-in mechanism to isolate, block, or contain suspicious assets. Any response action relies entirely on third-party integrations, creating delays and fragmented workflows that slow down remediation. Additionally, Lansweeper offers no real-time threat correlation or enforcement mechanisms, making it reactive by design. Without the ability to respond to rogue hardware, USB-based threats, or unauthorized asset connections, organizations are left with limited options to manage risk proactively, increasing exposure to physical-layer attacks and insider threats.

## THE SEPIO ADVANTAGE

While Lansweeper stops at asset discovery, Sepio goes further-delivering real-time mitigation and enforcement at the hardware level. Sepio enables organizations to define and enforce granular trust policies across multiple physical interfaces. When a rogue, spoofed, or unauthorized device is detected, Sepio can automatically trigger port blocking, isolate the device, or invoke external response workflows via SIEM/SOAR integrations. This ensures immediate containment of hardware-based threats-capabilities Lansweeper simply does not provide. With Sepio, visibility becomes action, and risks are neutralized before they escalate.

| Feature | Sepio | LS |
|---|---|---|
| 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 THE LANSWEEPER PRODUCT ?**
>
> Variance between cloud and on-premise interface, with lack of capabilities available in cloud version Cluttered on-premise interface.
>
> "

Gartner peerinsights™

Learn more at: **sepiocyber.com**

SEPIO