



# Sepio's MacOS Agent: The Industry's First Zero Trust Hardware Security Solution for Apple Devices

Full Device Visibility. True Asset Integrity.  
Unparalleled Protection.

## The MacOS Security Gap—Now Solved

Traditional endpoint security tools fail to provide true hardware-level protection. Attackers exploit blind spots in device security, using rogue peripherals, firmware manipulation, and supply chain vulnerabilities to bypass conventional defences. Sepio's MacOS Agent changes the game.

Unlike other security solutions that rely on software-based behavioural analysis alone, Sepio applies a Zero Trust Hardware Access (ZTHA) approach—leveraging physical layer insights to identify and neutralize threats at the hardware level.

With Sepio's MacOS Agent, organizations gain the first-ever full-spectrum visibility into all connected assets, ensuring that every device, peripheral, and interface is known, trusted, and continuously verified.



### True Hardware- Based Threat Detection

**Most** endpoint security tools monitor software behaviour. Sepio goes deeper, detecting malicious USB peripherals and other hardware-borne threats before they can execute an attack.



### Zero Trust for Devices & Peripherals

**Sepio** enforces a strict “never trust, always verify” policy for every asset connected to a MacOS system. This ensures that only authorized, verified hardware can interact with your endpoints—blocking rogue USB devices, hardware keyloggers, and tampered accessories.



### Instant Deployment & Seamless Integration

**Designed** for fast, frictionless adoption, Sepio's MacOS Agent deploys in minutes and integrates with your existing SIEM, SOAR, NAC, CMDB and asset management platforms for unified security operations.



### Complete AssetDNA Profiling

**Using** AssetDNA, Sepio maps every device's true identity—tracking its behavior, origin, and risk level from the moment it connects. Even sophisticated spoofing attempts fail against Sepio's hardware intelligence.



### Proactive Threat Prevention & Automated Response

**Sepio** doesn't just detect threats—it stops them in real time. The MacOS Agent enforces automatic response actions, such as:

- Blocking unauthorized hardware on the spot
- Quarantining risky assets before they can execute malicious actions
- Triggering security playbooks for rapid incident response

## // Why Enterprises Trust Sepio for MacOS Security

- **Patented Physical Layer Security**  
Only solution that validates device identity at the hardware level—beyond traditional software-based security.
- **Unmatched Speed to Value**  
Get complete visibility and automated protection within hours, not weeks..
- **CIS, NIST, & Zero Trust Aligned**  
Designed to meet the highest compliance and security standards, enabling robust cyber resilience for regulated industries.
- **MacOS Compatibility**
  - MacOS Version: MacOS 14 and above
  - Supported Devices: MacBook Pro with M-series processors.

### Ready to Eliminate Hardware- Based Threats?

Sepio's MacOS Agent is the first and only solution that provides full Zero Trust Hardware Access for Apple devices. Don't let invisible threats undermine your security posture.

Learn more at: [sepiocyber.com](https://sepiocyber.com)

