

# CASE STUDY BRIEF

## Zero Trust Security

- Industry**  
 Financial institution.
- Scenario**  
 Man-in-The-Middle (MiTM) network attack over a network printer.
- Attack Tool**  
 Raspberry Pi 4, configured in transparent bridge mode, spoofing a legitimate printer. Leaking PCL files being sent to the enterprise's network printer. Exfiltration done through the built-in AP functionality in the RP4 device.
- Duration**  
 Undetected by existing cybersecurity products (NAC/IDS/Other) runs completely passive with no inbound traffic manipulation – allowing it to operate for a long period of time.
- Challenge**  
 Enforcing a Zero Trust architecture for IoT devices that are being manipulated on the physical layer.
- Result**  
 The “printer” is considered a trusted device, bypassing micro-segmentation and Zero Trust security policy measures.
- HAC-1 Solution**  
 HAC-1 implements a Zero Trust Hardware Access policy by verifying the device's true identity with physical layer (L1) information. Extensive built in threat intelligence database for known-to-be-vulnerable devices provides additional valuable risk scoring.



### Key Challenges

- Total visibility is required into all IT/OT/IoT assets – Knowing what you have , protecting what you own.
- Compromised devices impersonating as legitimate devices cannot be identified with existing solutions.
- Physical layer MAC-less devices cannot be identified by existing NAC/IoT security solutions as they are MAC-based.

Enterprises are challenged with gaining accurate visibility into hardware assets, especially in today's extremely challenging IT/OT/IoT environment. In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers.

Sepio is the leader in visibility, control and mitigation of hardware assets and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. HAC-1, which orchestrates Sepio's solution, identifies, detects and handles all network devices including peripherals; no device goes unmanaged.



**Give us 24hrs.**  
 We will provide you with complete visibility and control for hardware devices and augment hardware risk mitigation.





## HAC-1 Benefits:



**Complete Visibility of All Hardware Assets:** With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

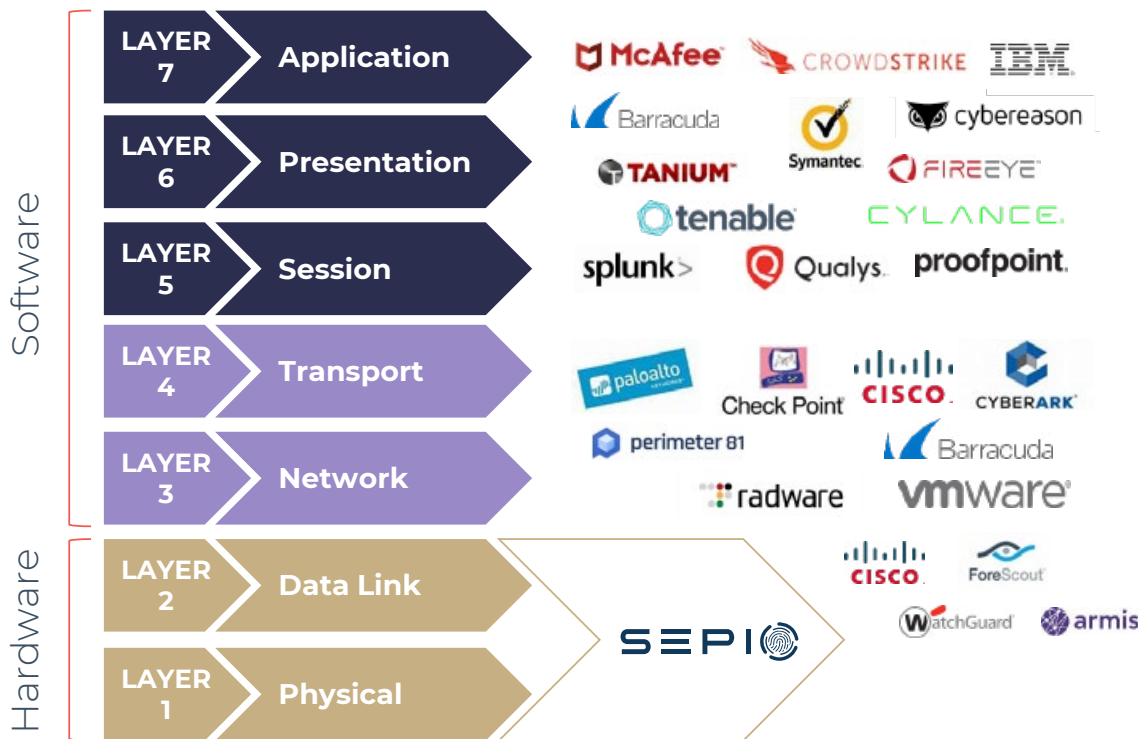


**Full Control through Predefined Policies:** Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.



**Rogue Device Mitigation (RDM):** Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

## Where Are We in the Cyber Security "Jungle"?



[www.srccybersolutions.com](http://www.srccybersolutions.com)

+91 120 2320960

[sales@srccybersolutions.com](mailto:sales@srccybersolutions.com)



### ABOUT SEPIO

Founded in 2016 by cybersecurity industry experts, Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any stage. The only trafficless solution, Sepio is infinitely scalable to protect the company's decentralized, uncontrolled ecosystem as fast and often as anyone, anywhere connects any assets. Sepio provides actionable visibility with the Asset Risk Factor (ARF) score based on a unique Asset DNA generated for each asset at its physical source, reflecting actual business, location, and rules. Sepio radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust layer solutions that simply see only the assets they are there to protect. Visit: [www.sepiocyber.com](http://www.sepiocyber.com).

### ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, and User-Friendly Solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, SEPIO for Asset Risk Management (ARM) to assess and mitigate all known and shadow assets at any scale, THREATX for WAAP (WAF++) for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

