

# CASE STUDY

## Invisible network devices

- Industry**  
 Financial.
- Scenario**  
 Man in The Middle (MiTM) network attack.
- Attack Tool**  
 PocketPort2 Cellular Modem Bridge from Proxicast. The device pair was configured to run in virtual cable mode and to use a private switchboard server to ensure that there will be no traces back to the origin of the attacker.
- Duration**  
 Undetected within environment for several months.
- Challenge**  
 The attack tool was placed between the CFO printer and the switch and has no IP address nor MAC address and went undetected by traditional IDS, NAC, and network monitoring tools. The entire manipulation is conducted on the Physical Layer (Layer 1) and the Data-Link Layer (Layer 2); so all higher-level communications are considered authentic and safe.
- Result**  
 Highly sensitive documents sent to printer was exfiltrated to the attacker cloud environment.
- HAC-1 Solution**  
 HAC-1 detected the attack tool by examining physical layer 1 information located on the switch which determined the presence of the MiTM device.



**MiTM attack using Virtual Cable Mode of PP2 device**



### 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 Systems 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.

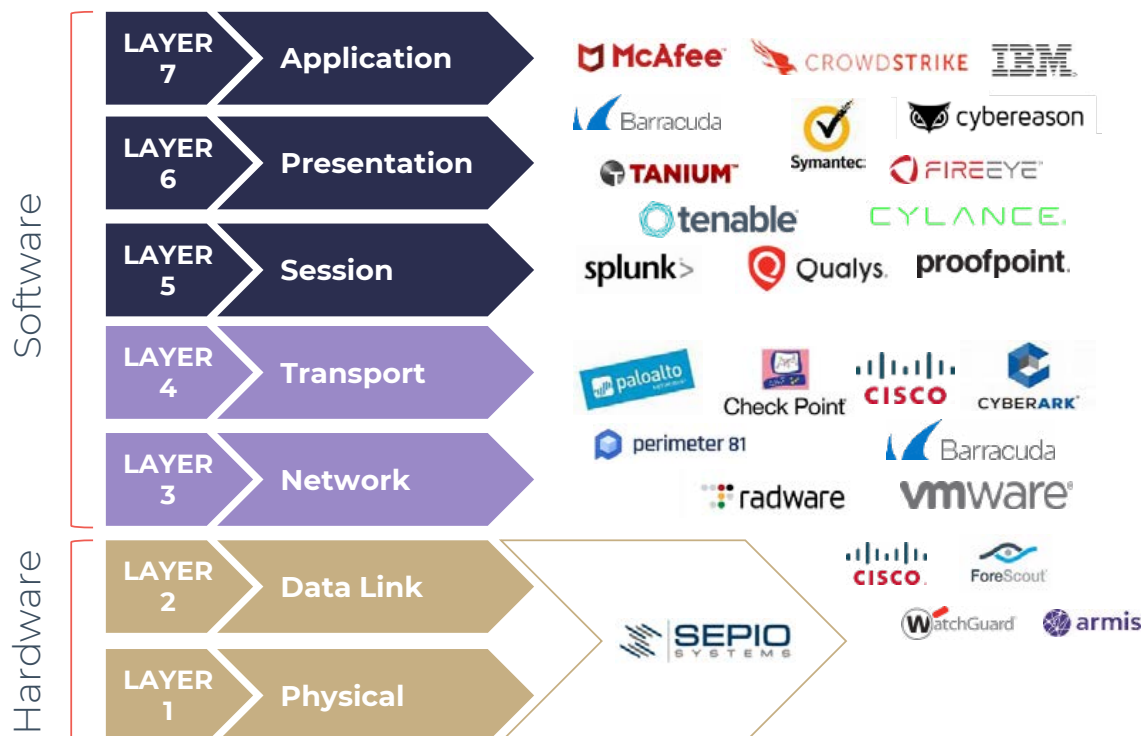


**Full Control through Predefined Policies:** Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.



**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"?



## About Sepio

Sepio delivers hardware access control (HAC) platform that reduces the risk of unapproved and rogue devices by providing complete visibility, control, and mitigation of all hardware assets. Sepio's hardware fingerprinting, augmented by machine learning, discovers all managed, unmanaged and hidden devices that are invisible to all other security tools. Sepio's solution enhances zero trust, insider threat, BYOD, IT, OT and IoT security programs.

[LEARN MORE](#)

