

Visibility & Security into Hardware Assets Hardware Access Control (HAC)

For Federal

Federal agencies and the nation’s critical infrastructure—such as energy, transportation systems, communications, and financial services—depend on IT systems to carry out operations and process essential data.

But the risks to these IT systems are increasing—including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks.

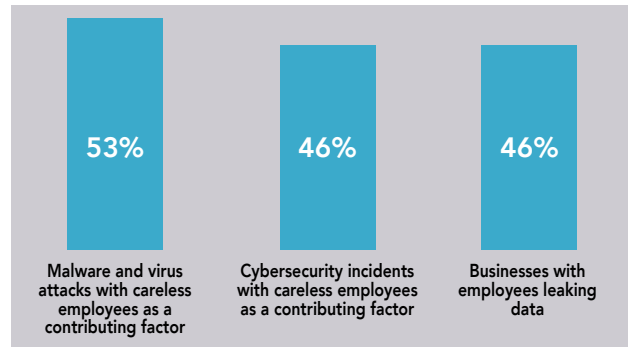
As per GAO’s recommendation – Establishing a comprehensive cybersecurity strategy and performing effective oversight with regards to mitigation of global supply chain risks and possible malicious hardware is of the utmost importance.

Tackling this challenge requires complete visibility to your Hardware assets, regardless of their characteristics and the interface used for connection, as attackers take advantage of the “blind” spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

Securing your network assets at the hardware layer by using a field proven solution developed by Cyber Physical Security experts, will be the first step in bringing your cyber security posture to the next level.

Key Challenges

- Total visibility is required to account for all of the agencies IT/OT/IoT assets - Knowing what you have, protecting what you own.
- Manipulated HID devices, which impersonate as legitimate devices, sharing the same logical identification, cannot be identified with existing solutions.
- Physical layer implants or spoofing devices cannot be identified by existing Network Access Control (NAC)/Intrusion Detection System (IDS) solutions, as they have visibility from L2 (MAC) and above.



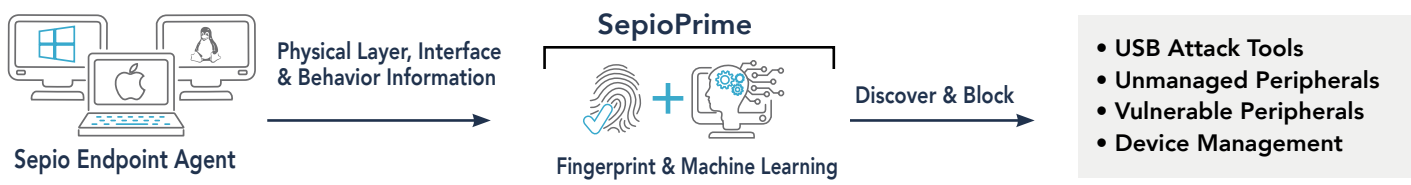
How Sepio Fixes the problem

By discovering rogue devices through physical layer hardware fingerprinting and behavior analytics, SepioPrime, which orchestrates Sepio’s solution, provides alerts for security threats, enforces policies and delivers risk insights and best practices recommendations. By supplying organizations with full visibility of the enterprise’s IT assets, a stronger cybersecurity posture is achieved with the following highlights -

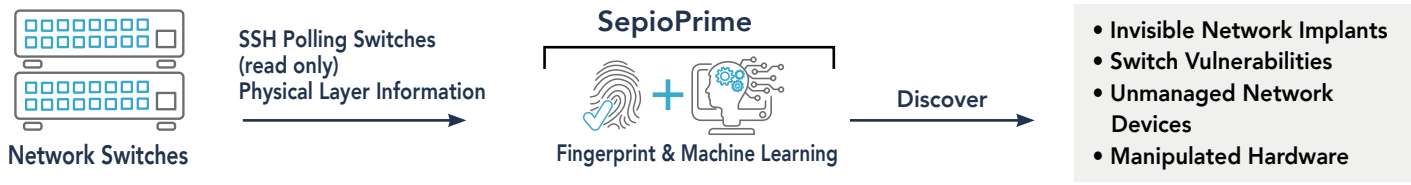
- Graphical dashboards
- Security status summary
- Policy management
- Risk insights
- Report engine
- Standalone or VM installation
- SIEM and NAC integrations
- Open APIs

How does it work

Peripheral Security



Network Security





```
# ... the end and back the deselected mirror
mirror_ob.select=1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier
mirror_ob.select = 0
bpy.context.scene.objects.active = mirror_ob
print("Active" + str(mirror_ob))
```

“ THE NETWORK VISIBILITY CREATED BY SEPIO’S SOLUTION IS A CRITICAL COMPONENT OF ANY EFFECTIVE ROUGE DEVICE MANAGEMENT SOLUTION. ”

Defense Research Analyst, Frost & Sullivan

- **Network Security:** works at the Physical Layer, polling switches to analyze what is happening at that layer and detecting all devices including rogue devices plugged into the Ethernet network.
- **Peripheral Protection:** guards against rogue devices connected to USB ports through multiple security layers, including real-time behavior analysis of suspicious devices. A Rogue Device being used to carry out an attack on an organization would be detected and blocked.
- **SepioPrime:** orchestrates Sepio’s solution and presents the overall status and security dashboards. It also alerts for security threats, defines and distributes the device usage policies and delivers risk insights and best practices recommendations.

Use Cases



Visibility Gap

Transparent Network Device that was found on a network in a Tier 1 bank.

- Can you detect it?
- Do you have a visibility to your hardware assets that are connected to your infrastructure?
- Do you have any idea about unmanaged devices in your network?
- Do you know how many and what peripherals are connected to your endpoints?



Insider Threat

In 2019 a US Federal Agency facility had been hacked by a Raspberry Pi device that was linked to the agency’s network without authorization. Attacker exploiting this device were able to facilitate a massive breach of classified data.

- Are you sure you don’t have hidden implants in your network?
- Are you sure you know what your endpoint devices really are?
- Can you be sure that you don’t have tapping devices inside your network?
- Do you know how many devices are being charged through a USB port on endpoints?



Supply Chain

A malicious peripheral device was found in an air-gapped network in a Power plant

- How do you know if you really received the hardware you bought?
- How do you know that your hardware was not modified/switched/tampered during upgrade or maintenance sessions?

Sepio phased Trial Program



NAICS CODES

511210 541519 541512 541511 541330
541690 541618 518210 541611

www.srccybersolutions.com

+91 120 2320960

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.

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.

