Zero Trust Hardware Access – Visibility.Control.Trust.

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, further emphasized by section 889b directive.

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. These challenges are also supported by the Comply-to-Connect and various Zero Trust guidelines.

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 agency's IT/OT/IoT assets - Knowing what you have, verifying what you own and only then trusting it.
- Spoofed devices, physical layer implants, "hiding" in the physical layer or impersonating as legitimate devices while sharing the same logical identification are hard to identify using existing technology.
- Rogue wireless AP's that can be used for attacks both in the enterprise and WFH environment.

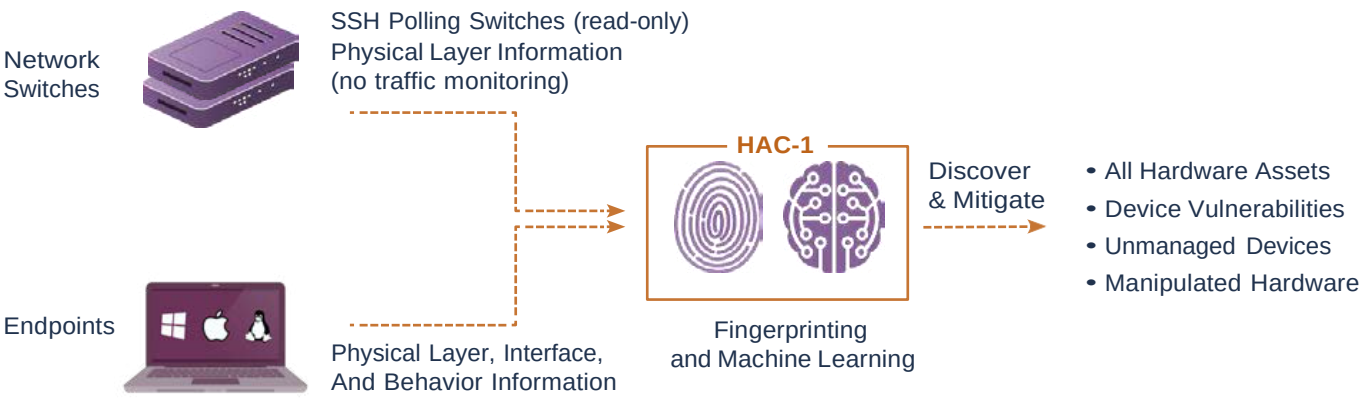
Sepio Systems Zero Trust Hardware Access approach to the challenges

Sepio's HAC-1 solution uses a unique algorithm based on physical layer fingerprinting module augmented by Machine Learning techniques. The unique approach allows HAC-1 to discover and report ALL devices, rogue devices included, enforce usage policies, deliver risk insights and device scoring.

By enabling organizations full visibility of their IT/OT/IoT assets, a stronger cybersecurity posture and true Zero Trust methodology are achieved with the following highlights -

- Asset visibility
- Policy management
- Device risk scoring
- Risk insights & actionable playbook
- Embedded Device Threat intelligence database
- Extensive device hunting, IR & Forensic features
- Fully integrated with popular orchestration & automation products

How It Works



Main Benefits of HAC-1

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.

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 Systems Phased Trial Program

Demo	POC - Lab/Production	Partial/Full production deployment
>> Demo Feedback report	>> PoC report	>> Complete Visibility & RDM coverage

CAGE CODE - 8FB16

GSA

SEWP V

DUNS # - 100288214

NAICS CODES

511210 | 541519 | 541512 | 541511 | 541330 | 541690 | 541618 | 518210 | 541611

About Sepio Systems

Founded in 2016 by cybersecurity industry veterans, Sepio HAC-1 is the first hardware access control platform that provides visibility, control, and mitigation to Zero Trust, Insider threat, C2C, BYOD, IT, OT and IoT security programs. Sepio's hardware fingerprinting technology discovers all managed, unmanaged and hidden devices that are otherwise invisible to all other security tools. Sepio is a strategic partner of Munich Re, the world's largest reinsurance company, and Merlin Cyber, a leading cybersecurity federal solution provider.

LEARN MORE