SEPIO SYSTEMS

# US FEDERAL AGENCY

## CASE SCENARIO

*Just a high-profile example of how RDM by Sepio Systems could have prevented a successful Cyber attack.*

# BACKGROUND

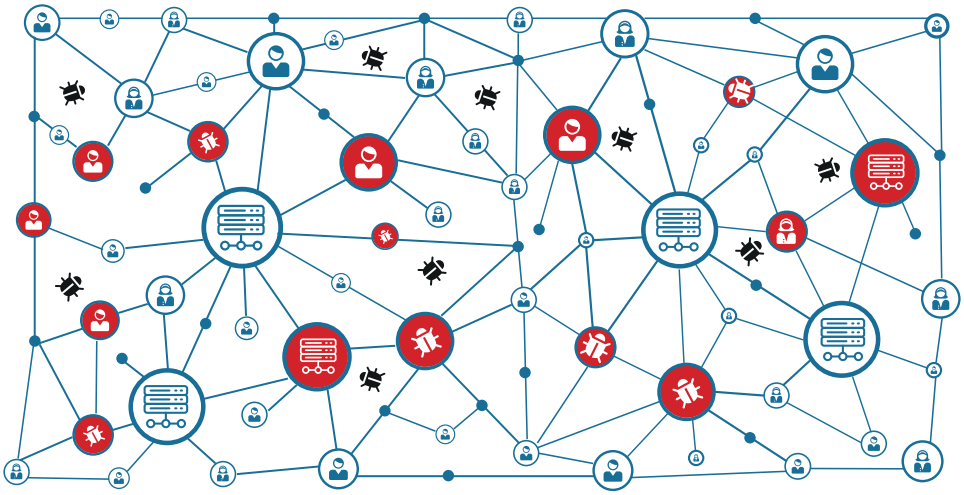
In 2019 it was announced that US Federal Agency facility had been hacked. The hackers went unnoticed for almost a year before eventually being discovered, but the damage was done. 500 megabytes of data from 23 different files from one of its major assets were stolen. Following the major security breach, several external entities chose to disconnect from the agency's network.

# ATTACK STUDY

Following a tedious audit investigation that underwent months, it was found that a Raspberry Pi device was linked to the agency's network without authorization. An account belonging to an external user had been compromised. As such, hackers we able to gain access and steal 500 megabytes of data from 23 different files. Furthermore, the network was shared, not a segmented environment, which allowed the attackers to move freely between the various systems within the network causing further damage.

The audit discovered that the agency had reduced visibility into devices connected to its network, thereby hindering the ability to comprehensively secure those networks. The considerable depth in which the attackers went provided them with access to several sensitive operations. When news broke, several connected agencies disengaged from the network to prevent further damage.

> *We found the database inventory incomplete and inaccurate, placing at risk the agency's ability to effectively monitor, report and respond to security incidents. Moreover, reduced visibility into devices connected to its networks hinders [the] ability to properly secure those networks.*
>
> *Audit report*



# TOOLS USED

The attackers used a Raspberry Pi device that can be bought on Amazon for as little as $25. A small barebones computer, it was originally developed with the intention of providing low-cost computers and free software to students, yet the device is now being used with malicious intent.

Hackers utilize this device, not only due to its credit card-like size, but also for the range of hacking tools it provides, notably being able to capture data on targeted networks.

The Raspberry Pi supports a variety of payloads and scripts. once mounted on, the device can perform Network Packet sniffing; used mainly for reconnaissance purposes. Some more advance payloads include an easy to use 802.1x bypassing module which helps the attacker overcome various MAC authentication procedures used by some of the NAC vendors.

Exfiltration of data from the Raspberry Pi can easily be done by connecting a mass storage device to it, use its on board WiFi capabilities or, for more covert operations, a dedicated USB-Wireless Dongle (non-WiFi) can be used, making its detection more difficult.


# HAC-1 SOLUTION

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment.

This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

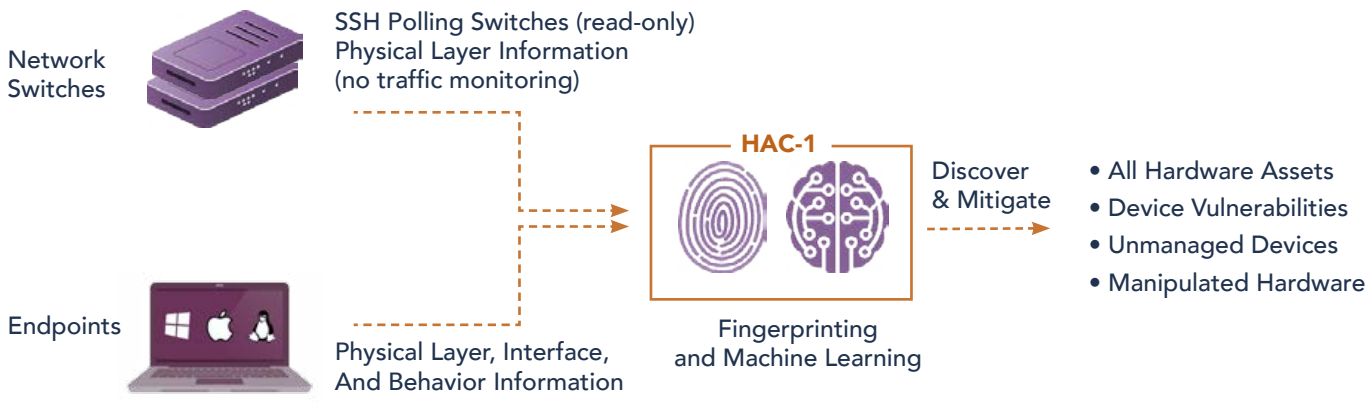
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.

Sepio Systems is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio Systems calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

## How It Works



# HAC-1 - Visibility & Security of Hardware Assets

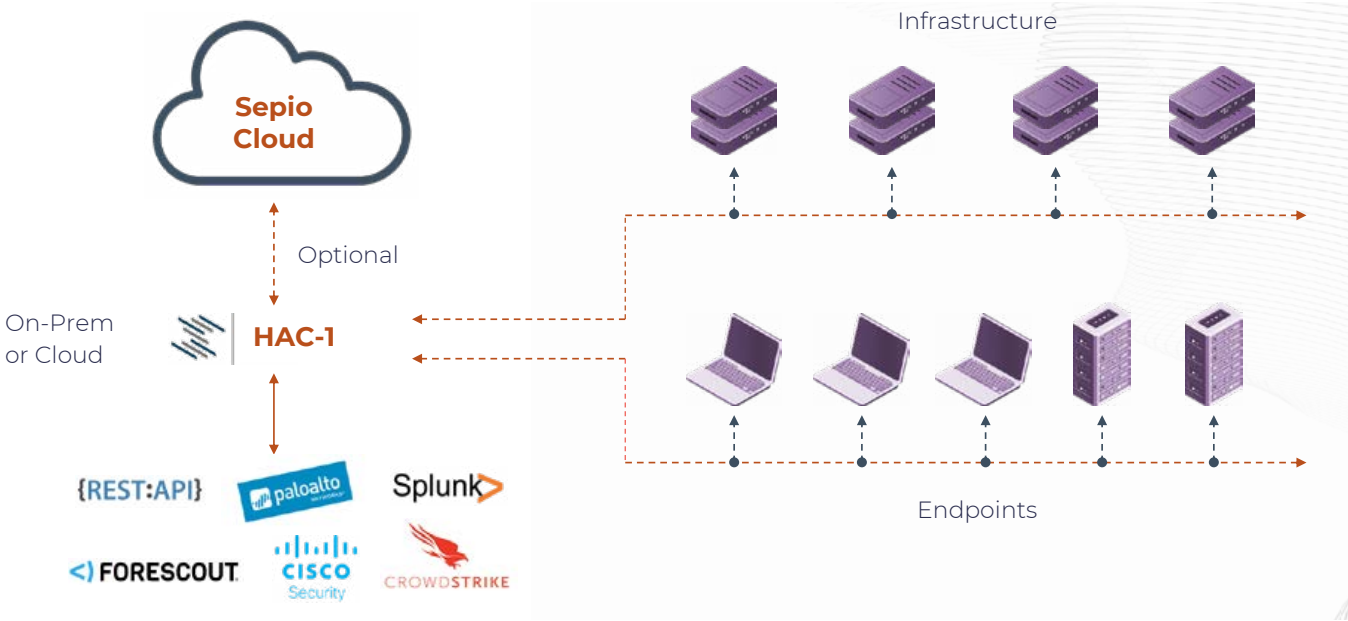
## Main Benefits

**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.

## System Architecture




LEARN MORE


SEPIO SYSTEMS