MSSP USE CASES

A Sepio white paper

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

CONTENTS

ROGUE DEVICE RISKS 3

ROGUE DEVICE RISKS 4

USE CASES 5

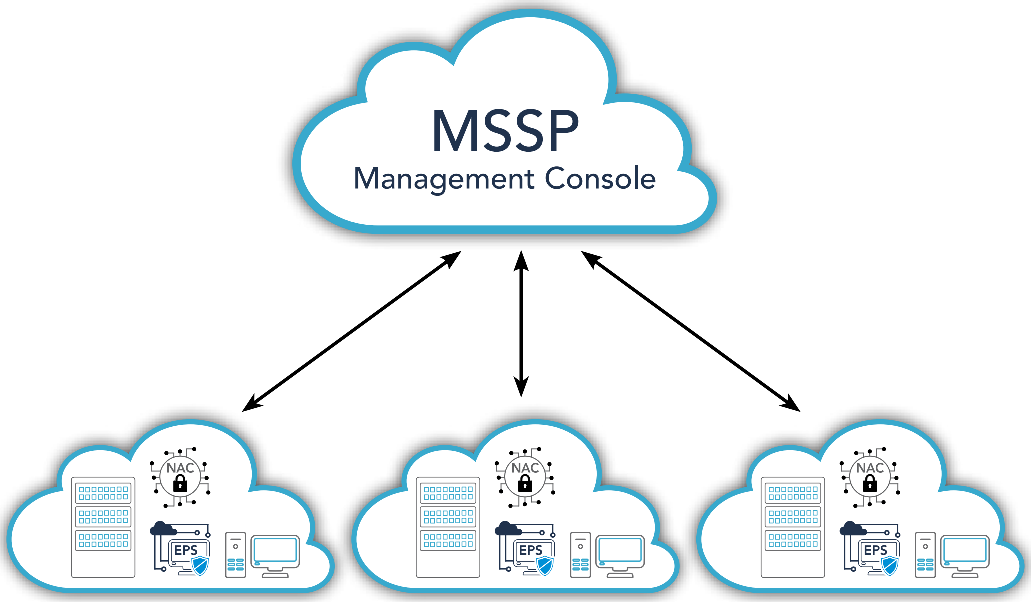
HAC-1 SOLUTION 8

USE CASES 10

INTRODUCTION

The number of organizations that are using MSSPs has increased over the years for various reasons. Importantly, due to the evolving nature of internal and external threats, cybersecurity is not only becoming progressively important, but increasingly complex. Governments, and organizations themselves, are implementing strict regulations regarding cybersecurity and the various components that accompany it. With this, internal security teams are often unable to meet every security requirement of the organization and the government. The complexity and difficulty of securing enterprise technology has led to frustration. This, and other staffing challenges, had caused the number of companies using MSSPs to increase. Additionally, MSSPs can cater to specific needs of an organization. Many companies are concerned with improving the security of customer-facing services and applications, or addressing existing threats and vulnerabilities – of which MSSPs can provide services for.

As such, the benefits of using MSSPs are in abundance, including incident resolution. According to Gartner, through 2021, organizations with MSSP operations that are sufficiently aligned with internal security operations will have a 50% superior incident resolution than organizations that are not. Moreover, a study on organizational security strategies found that organizations utilizing MSSPs made more accurate decisions; they were more equipped to comply with regulations and requirements, especially those who require an intimate visibility to all enterprises IT/OT/IoT assets; and, ultimately, customer experience had improved, and relationships were enhanced.



ROGUE DEVICE RISKS

Sepio Systems solution first establishes the visibility layer, upon which all other security related features are based upon – All devices will be accounted for – whether they are peripherals connected to an Endpoint, a Network element connected to the network, or through the Wireless access network (BYOD or other).

Once we gain visibility to what are our assets we can now deal with Rogue Devices – Spoofed Peripherals or Network Implants – which are malicious by nature. They have been intentionally compromised to carry out specific attacks including data breaches or the installation of various forms of malware, among other perilous risks. Rogue Devices, after being physically installed, provide bad actors with remote access to an organization's network; even after being removed. Spoofed Peripherals are recognized as genuine HIDs by existing security software solutions and, therefore, do not trigger an alert. Network Implants go completely undetected as they sit on the Physical Layer (Layer 1), which existing security software solutions do not cover. These transparent network devices have no network entity of their own – no IP or MAC address – and gain an invisible foothold on a target network to carry out attacks by creating an out-of-band connection to bypass an air-gapped network. Due to the range of attacks that these devices can carry out, no organization is free from the threat of them. Since there are no existing security software solutions that detect this type of attack, the threat is even more substantial. Hardware-based attacks are becoming more frequent, yet awareness surrounding them is not correlating with the rise in occurrence. As such, organizations do not only lack the protection against them, but are often even unaware that they need it. Adding to the threat of Rogue Device attacks is that they can originate from a myriad of sources including the supply chain; insiders; social engineering tactics; and BYOD and IoT devices. This increases the number of entry points for attackers, giving security teams an overwhelming surface area to cover.

> **“Sepio Systems' Visibility and Rogue Device Mitigation solution supports MSSPs architectures – Site-to-Site or Multi-tenant. With an easy and a speedy deployment process – Your customers will be able to enjoy a new level of asset visibility and a hardened Cyber Security posture.**
>
> **Use cases are important to identify to the provider the types of needs of the organizations to ensure that the appropriate MSSPs are provided. The various types of use cases that relate to Rogue Devices are explored below:”**

USE CASES

Advanced Persistent Threat (APTs)

APT attacks, as its name suggests, is a very advanced attack method that utilizes lesser-known and zero-day vulnerabilities. Due to the advanced nature of the attack, and that it typically continues for prolonged periods of time, it is the perfect method to carry out espionage. Although organizations can be the target for espionage, government agencies often fall victim to this type of attack, with state-sponsored hackers being the perpetrators. The nature of government agencies' information means that an attack of this type is extremely jeopardizing.

Consequences:

- Risk on national security.
- Decline of trust towards the government, should the attack become known to the public.
- An international shift on the perception of the victim state's ability to protect itself and its citizens.

Data Breach

A data breach could mean accessing, stealing or leaking confidential data either about clients, employees or the organization itself, such as intellectual property. The motives behind a data breach could be financial, whereby a bank would be a suitable target since the perpetrator can obtain credit card information to conduct credit card fraud. Healthcare facilities are another appealing target as here is where Personal Health Information is stored, which is highly valuable on the black market.

Another motive might be sabotage whereby intellectual property is accessed or stolen in order for the perpetrator to gain a competitive advantage.

Consequences:

- Loss of productivity due to clean-up time.
- Diminishing reputation as customers feel that their information is not securely stored.
- Loss of business due to the diminishing reputation.
- Legal consequences such as fines and lawsuits.
- Financial losses.

Malware

Malware comes in various forms including viruses, worms, and trojans. The installation of malware can impact the organization's systems. Additionally, malware can cause a data breach by providing bad actors with access to company information. Worms are an especially disruptive form of malware since they have the ability to replicate themselves and spread through the entire network, meaning the attack can reach far beyond the initial target endpoint.

Consequences:

- Loss of productivity due to systems being down.
- Diminishing reputation if there is a data breach.
- Loss of business due to the diminishing reputation.
- Legal consequences such as fines and lawsuits if there is a data breach.
- Financial losses.

Distributed Denial of Service (DDoS)

DDoS attacks occur when a large number of systems are compromised as used as a source of traffic on a synchronised attack. As a result, legitimate users are unable to access information systems, devices, or other network resources.

Consequences:

- Loss of productivity due to systems being down.
- Diminishing reputation as operations cannot be carried out.
- Legal consequences such as fines and lawsuits if there is a data breach.
- Financial losses.

Man-in-The-Middle (MiTM)

MiTM attacks are whereby the messages sent between the victim and the entity are intercepted, in this case by a Rogue Device, allowing the perpetrator to alter these messages without either party knowing. Attackers might carry out a MiTM attack to steal login credentials or personal information; spy on the victim; sabotage communications; or corrupt data.

Consequences:

- Diminishing reputation as customers feel that their information is not securely stored.
- Legal consequences such as fines and lawsuits.
- Financial costs.

Working From Home (WFH)

WFH policies, although bringing both the employer and employee benefits, can also present cyber risks. Using unknown peripherals – such as a mouse or keyboard – when connected to the network is hazardous as these peripherals might have been compromised and, having network access, can move laterally through the organization. As such, an unknown peripheral that has been manipulated has the potential to carry out any of the aforementioned attacks.

WFH presents increased risks since an employee is likely to be working on a personal device with fewer security features than a company-owned device. Furthermore, WFH means that the perpetrator does not need to gain physical access to the target organization, making the attack less challenging to carry out. Moreover, WFH means that there are fewer individuals in the office and, hence, fewer prying eyes – should an attacker gain access to the organization's premises, the likelihood of being caught is lower.

Consequence:

- National security risk should the attack be carried out against a government, or government-related agency.
- Legal consequences such as fines and lawsuits if there is a data breach.
- Diminishing reputation if there is a data breach.
- Loss of productivity if systems are shut down.
- Loss of business due to diminishing reputation.
- Financial costs.

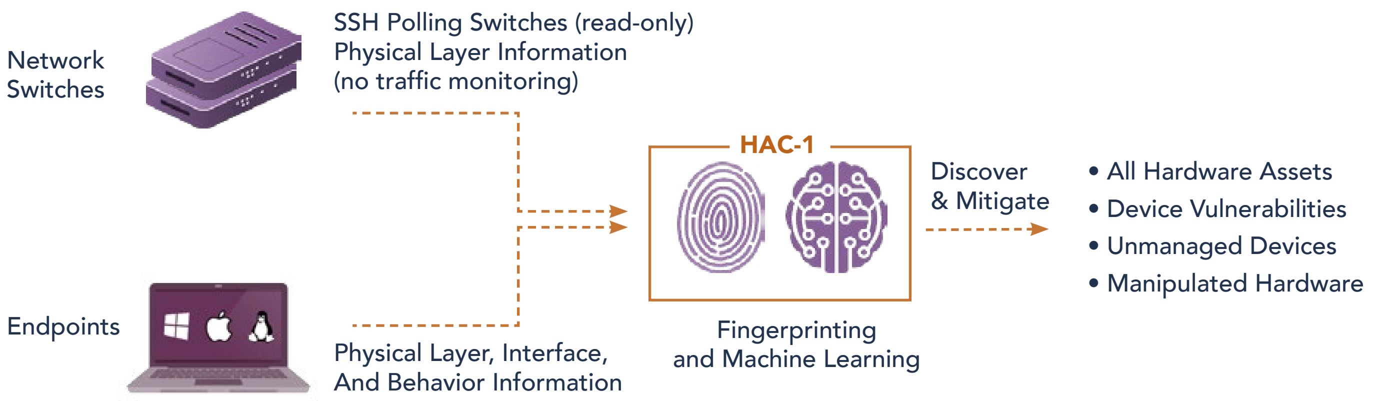
HAC-1 Solution

Many times, enterprises' IT and security teams struggle in providing complete and accurate protection of their hardware assets - especially in today's extremely challenging IT/OT/IoT environment. This is because, often, there is a lack of device visibility which leads to weakened policy enforcement of hardware access. This vulnerability may result in security incidents such as ransomware attacks, data leakage, etc. In order to address this challenge, ultimate visibility into your hardware assets is required, regardless of device characteristics and the interface used for connection. Moreover, malicious actors have adapted to the dynamic cybersecurity defenses deployed to block cyber-attacks by taking advantage of the "blind spots" – mainly through USB HID-emulating devices or Physical Layer network implants. These Rogue Devices are covert by nature and go undetected by existing security software solutions, thereby leaving the organization extremely vulnerable.

Sepio Systems has developed the Hardware Access Control (HAC-1) solution to provide a panacea to the gap in device visibility. As the leader in Rogue Device Mitigation, Sepio's solution identifies, detects and handles all peripherals; no device goes unmanaged.

HAC-1 uses Physical Layer fingerprinting technology and Machine Learning to calculate a digital fingerprint from the electrical characteristics of all devices and compares them against known fingerprints. In doing so, HAC-1 is able to provide organizations with ultimate device visibility and detect vulnerable devices and switches within the infrastructure. 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. When a device breaches the pre-set policy, HAC-1 automatically instigates a mitigation process which instantly blocks unapproved or Rogue hardware.

How It Works



Network Switches

SSH Polling Switches (read-only)
Physical Layer Information
(no traffic monitoring)

Endpoints

Physical Layer, Interface,
And Behavior Information

HAC-1

Fingerprinting
and Machine Learning

Discover
& Mitigate

- All Hardware Assets
- Device Vulnerabilities
- Unmanaged Devices
- Manipulated Hardware

HAC-1 - Visibility & Security of Hardware Assets

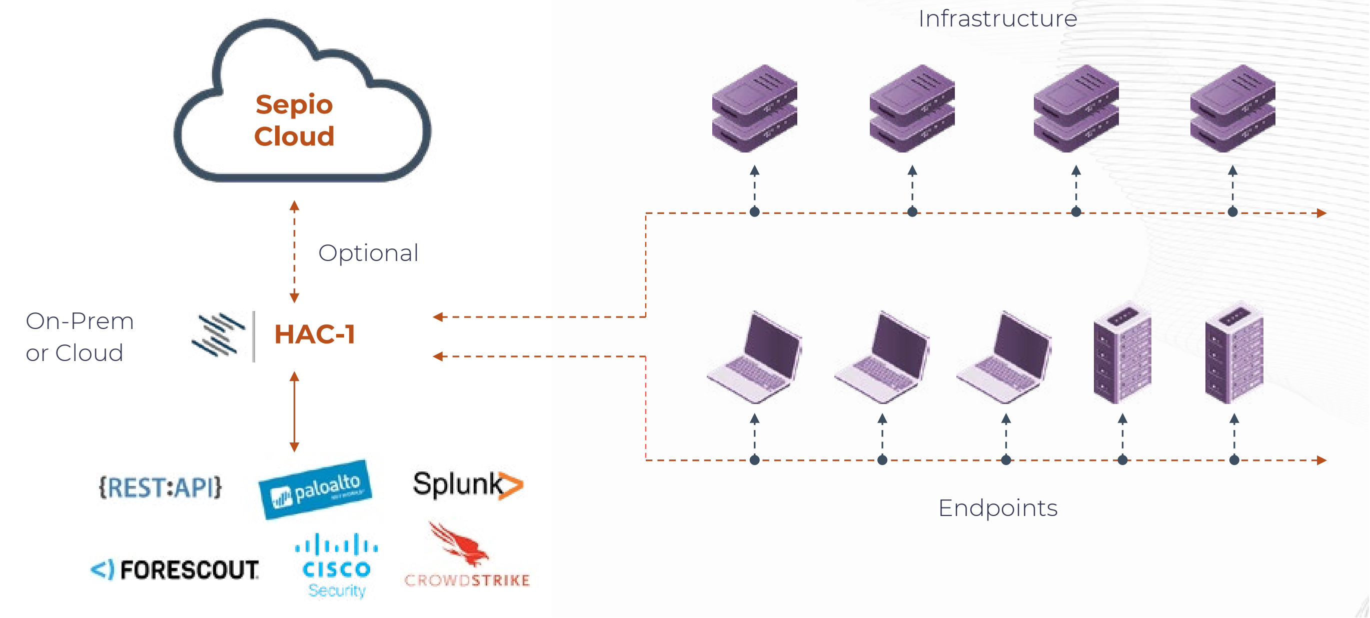
Main Benefits:

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



SUMMARY & CALL FOR ACTION

The risk of Rogue Device attacks is prevailing, and organizations can no longer rely on existing security measures to protect them from these hardware-based attacks. Since Rogue Devices can perform a number of different attacks, no organization is exempt from being a target.

Visit us at **www.sepio.systems** to find out more about our solution and the risks of Rogue Devices. Here, you can contact our sales team to further discuss the usage and benefits of Sepio Systems. Additionally, we provide demos to give a visual representation of how our solution works once deployed. Please do not hesitate to reach out to us with any questions or inquiries.

LEARN MORE

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.

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS