SEPIO

Gartner COOL VENDOR 2020

FROST & SULLIVAN 2019 BEST PRACTICES AWARD
EUROPEAN ROGUE DEVICE MITIGATION ENABLING TECHNOLOGY LEADERSHIP AWARD

HAC-1

Visibility, Control, and Mitigation of all Hardware Assets

> **How confident are you that you have total asset visibility?**
>
> **Phil Packman**
> CISO, commercial contracts, BT

In today's extremely challenging IT/OT/IoT environment, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets. This is driven by the fact that lack of visibility leads to a crippled policy enforcement of hardware access which may result in security incidents, data theft, sabotage, ransomware etc.

Tackling this challenge requires ultimate visibility into your Hardware assets, regardless of their characteristics and the interface used for connection as attackers, being pragmatic and adopting to the changing Cyber security defenses put in place to block them, take advantage of the "blind" spots – mainly through endpoint peripherals emulating legitimate devices or rogue network implants hiding in plain sight.

Give us 24hrs.

We will provide you with complete visibility and control for hardware devices and augment hardware risk mitigation.

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.

> **Sepio has solved one of the longest standing issues within the cybersecurity arena – hardware security visibility and remediation.**
>
> **With the company's new solution, enterprises will be able to see what, until now, has been invisible.**
>
> **Dr. Edward Amoroso**
> CEO, TAG Cyber

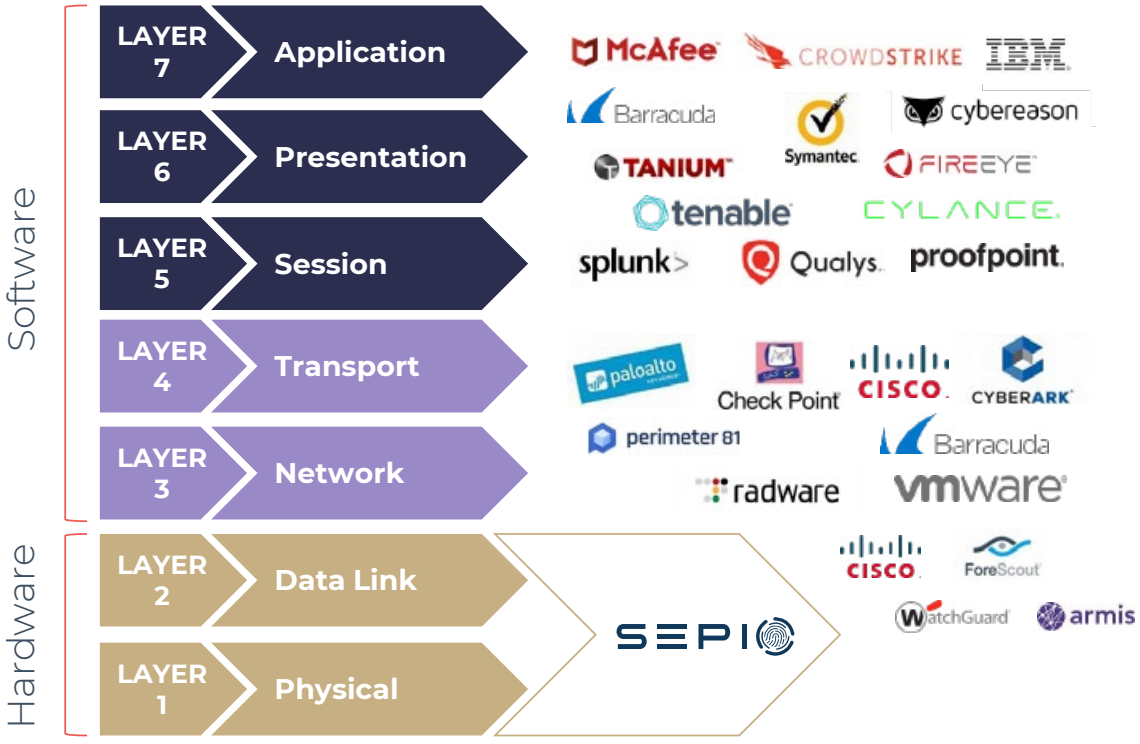
HAC-1 Benefits:

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

Founded in 2016 by cybersecurity industry veterans from the Israeli Intelligence community, Sepio's HAC-1 is the first hardware access control platform that provides visibility, control, and mitigation to zero trust, insider threat, 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 re-insurance company, and Merlin Cyber, a leading cybersecurity federal solution provider.

LEARN MORE