SEPIO

Gartner
COOL VENDOR 2020

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

CASE STUDY

Asset Visibility - Network and Peripherals

Scenario

Complete and accurate visibility into network and peripheral devices.

Challenge

Network visibility is a foundational element of an IT organization. As devices exponentially increase, enterprises struggle to know with full confidence what is connected to their network. Traditional visibility tools use Layer 2 (MAC) and Layer 3 (TCP/IP) network data to discover and identify their devices. This is problematic as at Layers 2 and above, devices without a digital existence, such as passive taps, unmanaged switches, MiTM attack tools or 'spoofed' devices go undetected.

Result

Enterprises lack 100% visibility. Absent of an examination of Layer 1, IT organizations do not have all of the information necessary to mitigate risk coming from their hardware infrastructure – you cant secure what you cant see.

HAC-1 Solution

HAC-1 collects physical Layer 1 (analog) information from a network switch and endpoints to detect and identify all devices. This approach provides continuous real-time visibility of all network and peripheral devices within the environment. No additional hardware needs to be deployed. HAC-1 provides accurate visibility, control, and risk mitigation of all devices

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.

Enterprises are challenged with gaining accurate visibility into hardware assets, especially in today's extremely challenging IT/OT/IoT environment. 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.

Sepio Systems is the leader in Visibility, Control and Mitigation of hardware assets and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. HAC-1, which orchestrates Sepio's solution, identifies, detects and handles all network devices including peripherals; no device goes unmanaged.

Give us 24hrs.

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

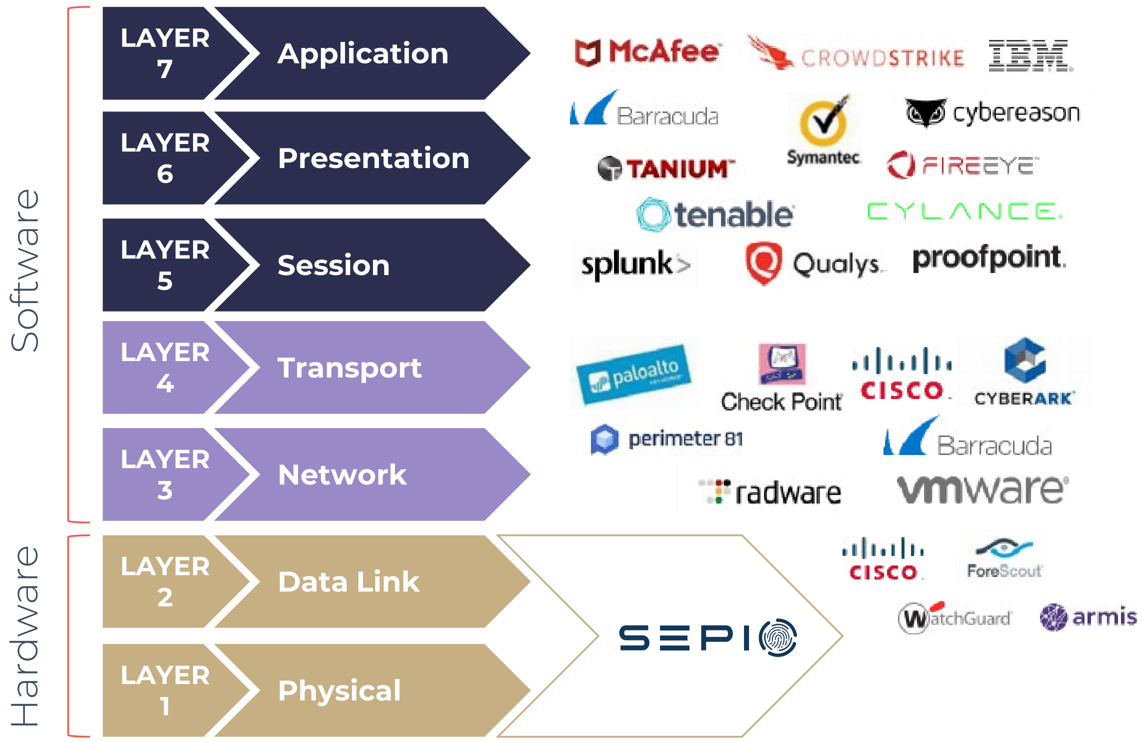
HAC-1 Benefits:

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

Sepio delivers hardware access control (HAC) platform that reduces the risk of unapproved and rogue devices by providing complete visibility, control, and mitigation of all hardware assets. Sepio's hardware fingerprinting, augmented by machine learning, discovers all managed, unmanaged and hidden devices that are invisible to all other security tools. Sepio's solution enhances zero trust, insider threat, BYOD, IT, OT and IoT security programs.

LEARN MORE