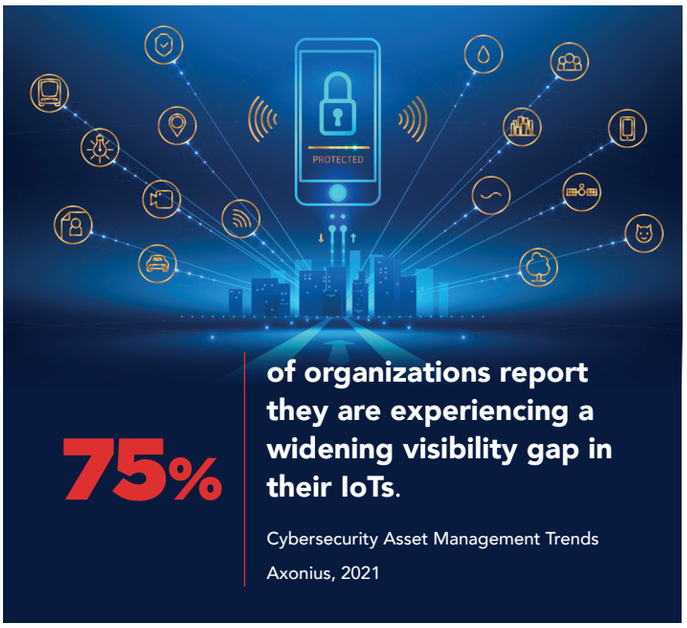
SMART BUILDING, SMART SECURITY

Sepio's HAC-1 solution gets to the root cause of the problem: visibility. Through Layer 1 visibility, HAC-1 goes deeper than any other security solution, offering unparalleled asset visibility. HAC-1 creates a digital fingerprint of all devices through multiple Layer 1 parameters and a unique machine learning algorithm to provide ultimate visibility of all IT/OT/IoT assets – managed, unmanaged, or hidden. In turn, HAC-1 generates a comprehensive and accurate hardware asset inventory that integrates with an enterprise's CMDB for automated asset management. For smart buildings and their interconnected environment, complete asset visibility and automated asset management is an imperative starting point to strengthening cyber hygiene.



Leveraging Layer 1 visibility enables HAC-1 to safeguard network integrity by offering greater control over all hardware assets through its Hardware Access Control feature. The system administrator defines a set of hardware access policies for the system to enforce based on a device's digital fingerprint and associated risk. This Zero Trust Hardware Access approach enables comprehensive access control of hardware assets, including non 802.1x compliant devices. When a device breaches the pre-defined rules or gets identified as malicious by the internal threat intelligence database, HAC-1 immediately initiates an automated mitigation process to block the device through integrated third-party tools. The Rogue Device Mitigation feature protects the entire network from potentially perilous hardware-based attacks that threaten the functionality of smart buildings.

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