# SMART SECURITY FOR SMART BUILDINGS

## What are Smart Buildings?

Industry 4.0 facilitated the convergence of IT and OT through smart, connected devices collectively referred to as the Internet of Things (IoTs). The technological advancement has sparked widespread digitalization, and buildings are no exception. Smart buildings, as they are known, rely on IoT sensors and artificial intelligence to simplify or automate building functions and processes using real-time data. Naturally, this allows for the more efficient and economical use of resources while also enhancing safety and comfort.

## Cybersecurity Risk of Smart Buildings

IoTs are the foundation of smart buildings. This, however, means there is an increased number of devices in use, which, in turn, expands the attack surface. Any smart device, being that it is connected, provides an attacker with network access; and as IoTs typically lack sufficient security features, they are highly vulnerable. Additionally, the interconnected environment means IoTs are exposed to other attacks on the network. In short, breaching one device (smart or not) puts the entire network in jeopardy.

The challenge with protecting a smart building starts with a lack of visibility. A worrying 75% of organizations report a widening visibility gap in their IoTs, thus making it difficult to manage such devices and their associated risk. Existing security solutions, such as NAC, IDS, IoT Network Security, fail to provide Layer 1 visibility, further contributing to the issue as hardware risks go unaccounted. Additionally, rogue devices (hardware attack tools) exploit the Layer 1 blind spot, bypassing security solutions and access controls by spoofing or hiding their identity through Layer 1 manipulation.


For hardware-based attackers, smart buildings are an attractive target. IoTs, which are not 802.1x compliant, can effortlessly gain unauthorized network access by spoofing a legitimate MAC address.

Additionally, rogue devices require physical access, and the large attack surface offers countless opportunities. Interconnectivity means the rogue device only needs access to one endpoint - the most accessible one. Through clandestine lateral movement, rogue devices are capable of deep infiltration, in which all devices on the network become vulnerable. This is a serious concern as disruptive attacks, such as ransomware and DDoS, can cause IoT downtime and put the building at risk of becoming inoperable. Such a situation has significant consequences for productivity, business continuity, and even physical safety.

## Smart Building, Smart Security

Sepio's solution gets to the root cause of the problem: visibility. Through Layer 1 visibility, Sepio goes deeper than any other security solution, offering unparalleled asset visibility. Sepio 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, Sepio 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.


***Additionally, rogue devices require physical access, and the large attack surface offers countless opportunities. Interconnectivity means the rogue device only needs access to one endpoint - the most accessible one.***

Leveraging Layer 1 visibility enables Sepio 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, Sepio 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.