VDOO

IoT Security Platform for Smart Buildings

Introduction

The impact of smart buildings can be drawn using multiple circles—starting from the building's tenants, whether living or working there, to property owners and facility managers, to construction and engineering industries, and subsequently to urban and smart cities planning. Parallel to all of these are the smart device makers, which vary across device types. A single smart building can include dozens of different smart devices, such as lighting, fire protection, security systems, HVAC (Heating, Ventilation, and Air-Conditioning) systems, elevating systems, EV (Electric Vehicle) connected chargers, and more. Smart technology is also an increasingly significant part of the building construction process itself, with machines like mobile-controlled cranes and smart drilling machines coming into use.

The motivation for this abundance is clear: smart solutions increase comfort, efficiency, sustainability, and safety. However, ensuring their proper functioning depends on securing each link in the smart building chain. When estimating the opportunities and challenges smart buildings bring, two major trends that were predicted by well-known research firms must be noted—first, more people would spend more time in buildings, and second, more buildings would include smart technologies. The combination of the two means an increasingly extensive direct effect on the everyday life of millions in the foreseeable future.

This effect, by nature, constitutes a three-dimensional threat—privacy risk, physical threat, and commercial risk. One of the benefits of having a smart building system is the ability to enhance performance and improve tenant experience; both require big data collection and analysis. In 2020, data collected by buildings is predicted to stand at 37.2 zettabytes, which could be exposed and exploited. The potential physical damage is also unprecedented, and while taking control over smart door systems might lead to property loss, compromising fire protection systems might pose a threat of a completely different magnitude. An additional trait that distinguishes smart buildings is the emphasis given to interoperability. Since smart buildings encompass many different connected technologies, they also facilitate various, unstandardized communication protocols, starting from basic and simple one-way protocols such as Infrared, common and vulnerable protocols like WiFi and Bluetooth, and open protocols like Z-Wave, BACnet, and KNX.

VDOO's Solutions for Smart Buildings

The smart building industry's unique characteristics are deeply rooted in VDOO's IoT security platform design and development, built to serve both users, managers, and makers in the ecosystem. By using Vision™, VDOO's analysis solution, device makers can analyze any Linux-based firmware of any device, regardless of its type or purpose, and receive an accurate description of the device's security status followed by mitigation guidance for device hardening. By using ERA™, VDOO's Embedded Runtime Agent solution, the device maker as well as the organization that deployed the IoT devices can make sure they will remain safe and secure after deployment. Tenants can make sure any device installed in the building is certified by VDOO CertIoT™, which proves it has met a rigorous set of security requirements. Property and network managers can rely on proactive solutions like Quicksand™, a threat detection honeypot that lures the attacker and provides real-time monitoring and alerts, and Whistler™, a device-specific push alerts system on any new threat. This end-to-end solution was built to handle both security and safety related threats, whether known or unknown, to allow laying the foundations for a smart and secured building.