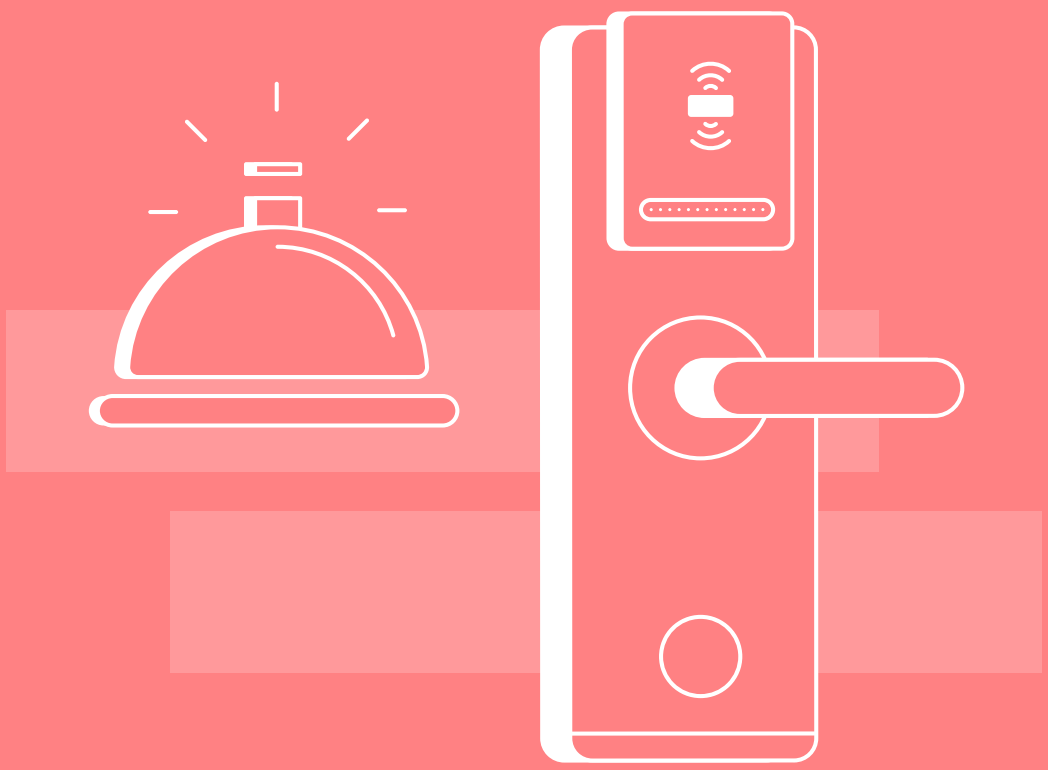
VDOO

IoT Security Platform for Hospitality



Introduction

Hospitality infrastructure uses connected devices in all aspects of the business, and these devices are used by both management and visitors. Management uses connected devices for security, access control, building management, stock management, and customer service. Customers use connected devices as part of the check-in process, room access, in-suite entertainment, lights, room HVAC (Heating, Ventilation, and Air-Conditioning) systems, and much more. The sheer number of connected devices used in hospitality locations by different users for multiple purposes usually means two things for attackers: many entry points and significant potential value.

In 2018, more than $1.6 billion was spent on smart hospitality projects globally. Under this wide category, there are dozens of different devices—smart HVAC, smart lighting, waste and recycling management, room access, in-suite entertainment, and more. The diversity in these projects is expressed in an abundance of IoT devices that networks can include, starting from cameras, sensors and detectors, alarm systems, and so on. It also means varied management, analysis, and data monitoring platforms, most of them cloud-based. These are, of course, added to the different network, communication, and storage components.

The complexity of securing devices in the hospitality ecosystem stems both from its varied network segmentation and from the different threat levels it holds—privacy, safety, and functionality. In order to secure hospitality devices, centralization is required, as there is an inherent requirement of connectivity. Hospitality, unlike other isolated grids, must be interconnected for efficiency and in order to provide a superior visitor experience.

Each device mentioned is an entry point for an attacker, which could extract confidential data or even disrupt device functionality and cause physical damage. The ability to use an embedded device for harming the entire network is particularly relevant for hospitality, since much of the communication between its different segments is done using extremely vulnerable M2M protocols, such as MQTT and CoAP.

VDOO's IoT security platform is designed with careful consideration of this condition, and therefore offers an automatic analysis of connected devices suitable to any device type, to generate its specific security requirements, including mitigation and hardening guidance applicable for both new devices and existing install bases, in a cost-effective manner.

A useful case for demonstrating VDOO's automated analysis approach are smart cameras, which are widely used as part of the hospitality IoT ecosystem. The approach can be relevant to any Linux-based firmware of any device, regardless of type or purpose.

VDOO's Solutions for Hospitality

By using Vision™, VDOO's analysis solution, the camera maker can analyze the device firmware to 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 camera maker as well as the hospitality management who deploy the IoT device can make sure the device will remain safe and secure after deployment. Hospitality managers as well as tenants can make sure any device installed in the accommodation area is certified by VDOO CertIoT™, which proves it has met a rigorous set of security requirements. 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 for 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 safe and secured hospitality.

IoT devices are a key element in hospitality, and dependency on IoT devices will continue to grow. Yet, along with their great benefits, they also carry a staggering risk to businesses and customers, and therefore must be secured. Today, VDOO IoT security platform is the only way to provide this type of holistic, scalable, and uncompromising security solution.