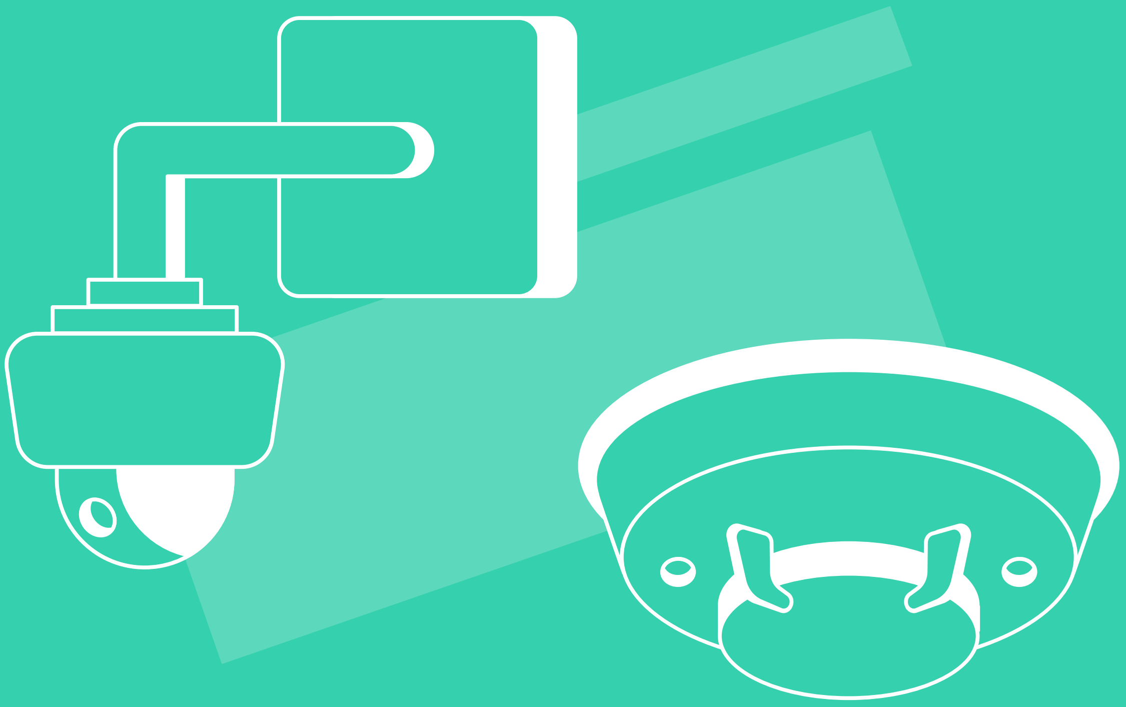
VDOO

IoT Security Platform for Physical Security and Saftey Devices



Introduction

Often, the IoT ecosystem is referred to as “cyber-physical,” since it connects these two dimensions. However, physical security and safety devices, such as door locks, surveillance cameras, smart safes, access control systems, and fire alarm systems, provide a new meaning to the term, since in their case, the physical safety they provide depends heavily on the device’s virtual safety. Considering their important role, one might expect their entry into the market would depend on their cyber-security status. However, reality shows otherwise. Over the past few years, each of the mentioned device types was either exploited or proven to be vulnerable. Naturally, and contrary to other cases, such attacks may go beyond the cyber dimension and can lead to real harm to human life.

According to different predictions, the number of connected devices in 2020 will stand at around 31 billion devices, with millions of them related to physical security and safety in homes, cities, office buildings, factories, and more. While everyone describes 2020, already now in 2019, there are over 20 billion devices connected, imposing great risks to businesses and individuals. Ironically, these devices, which have been created to serve one of our most primary needs, are posing a major threat to privacy, security, and safety.

Most security cameras, for example, are currently considered one of the easiest targets for attack, when even basic techniques can lead to huge damages. This phenomenon says more about the state of the market and lack of regulation than manufacturers. VDOO’s research team has discovered many zero-days vulnerabilities in several IP camera leaders. This also applies in the case of smart door control systems, where common and popular brands were also found to be highly vulnerable. Such attacks could range from disabling a specific device in order to bypass a security mechanism, to utilizing the device as an entry point for disrupting the entire network, whether in a smart home, school, financial institution, or hospital.

VDOO’s Solutions for Physical Security and Safety Devices

The key requirements for securing such devices are proactiveness and real-time alerts, both embedded in VDOO’s IoT security platform. By using Vision™, VDOO’s analysis solution, device makers can analyze any firmware in the 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. Users 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. IoT device makers and users can also 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. In the case of physical security and safety devices, real-time alerts and proactive security are not only an advantage, they could be life-saving.

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 smart and secured devices.