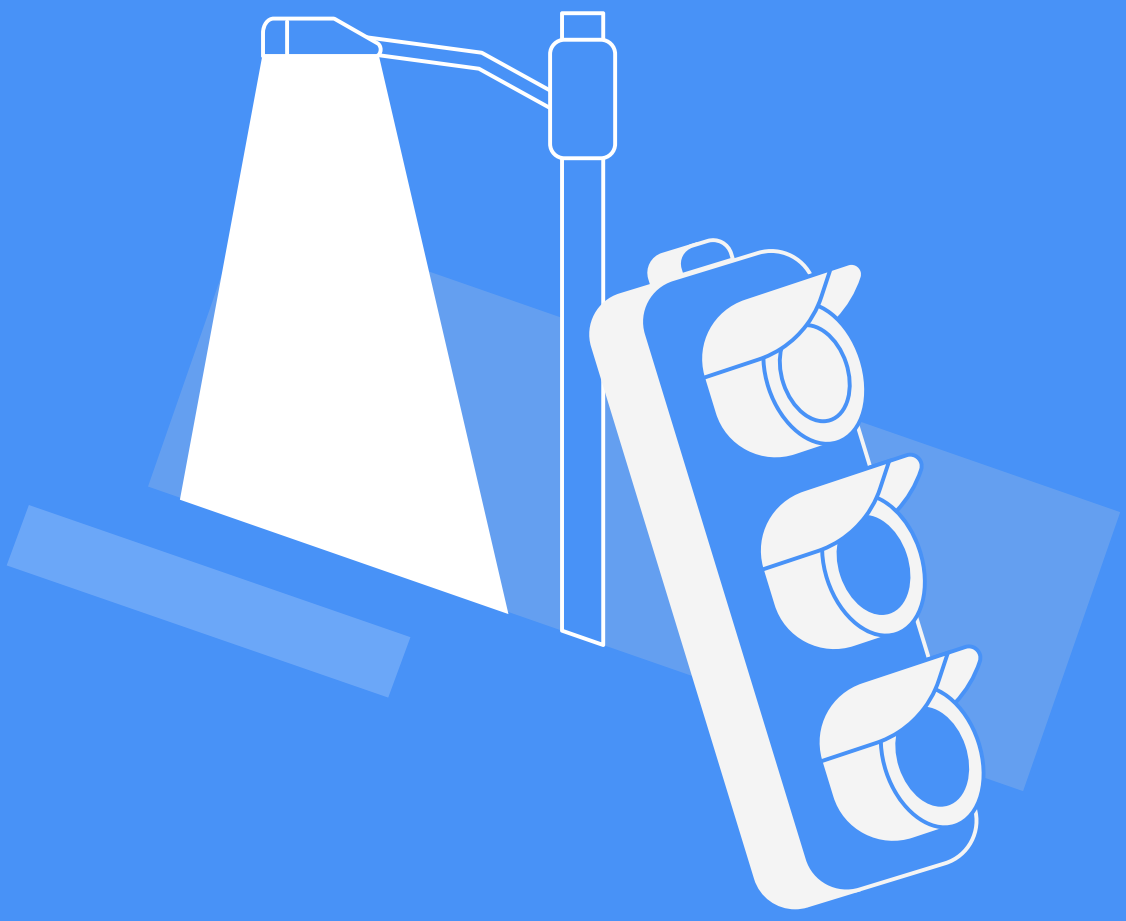
VDOO

IoT Security Platform for Smart Cities



Introduction

Smart cities IoT grids are complex, yet centralized. This combination usually means two things for attackers: many entry points and significant potential value. The complexity of the smart city ecosystem stems both from its varied network segmentation and from the different threat levels it holds—privacy, safety, and functionality. Its centralization stems from the inherent requirement of connectivity; smart cities, unlike other isolated grids, must be interconnected.

Over 2018, more than $80 billion was spent on smart cities projects globally. Under this wide category, there are dozens of different projects—smart parking, smart utilities, smart stadiums, smart lighting, waste and recycling management, noise monitors, air pollution controls, earthquake detection, and more. The diversity in projects is expressed in the abundance of IoT devices such networks can include, starting from cameras, sensors and detectors, alarm systems, and so on. It also means varied management, analysis, and data monitoring platforms for special occasions, such as the Olympic games, but also for constant monitoring. Most of the platforms are cloud-based, and of course, added to the different network, communication and storage components.

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 whole network is particularly relevant for smart cities since much of the communication between different segments is done using extremely vulnerable M2M protocols, such as MQTT, CoAP, WSN, TALQ, 3GPP and 6LoWPAN. VDOO's IoT security platform was designed with careful consideration of this condition, and therefore offers a three-level plan: comprehensive device analysis for device hardening and security gaps mitigation, device certification, and on-going device monitoring and active protection.

VDOO's Solutions for Smart Cities

A useful case for demonstrating this plan can be examined through smart cameras, which are widely used as part of the smart city's ecosystem but can be relevant to any Linux-based firmware of any device, regardless of type or purpose. VDOO's analysis solution, Vision™, can analyze any Linux-based firmware for any camera and provide an accurate description of the device's security status. If the device meets VDOO's standard, which is based on 600 rigorous security requirements, it would receive VDOO's CertIoT certification. After the camera is installed, VDOO would provide it with ERA™ - Embedded Runtime Agent protection, which would make sure it remains safe and secure after its deployment. This solution is valid for both known and unknown security threats and is possible due to the company's pioneering proven research capabilities.

Smart cities are here to stay, but for their advantages to outweigh the disadvantages, they must be secured. Today, VDOO is the only solution that can provide this type of holistic, scaled, and uncompromising security.