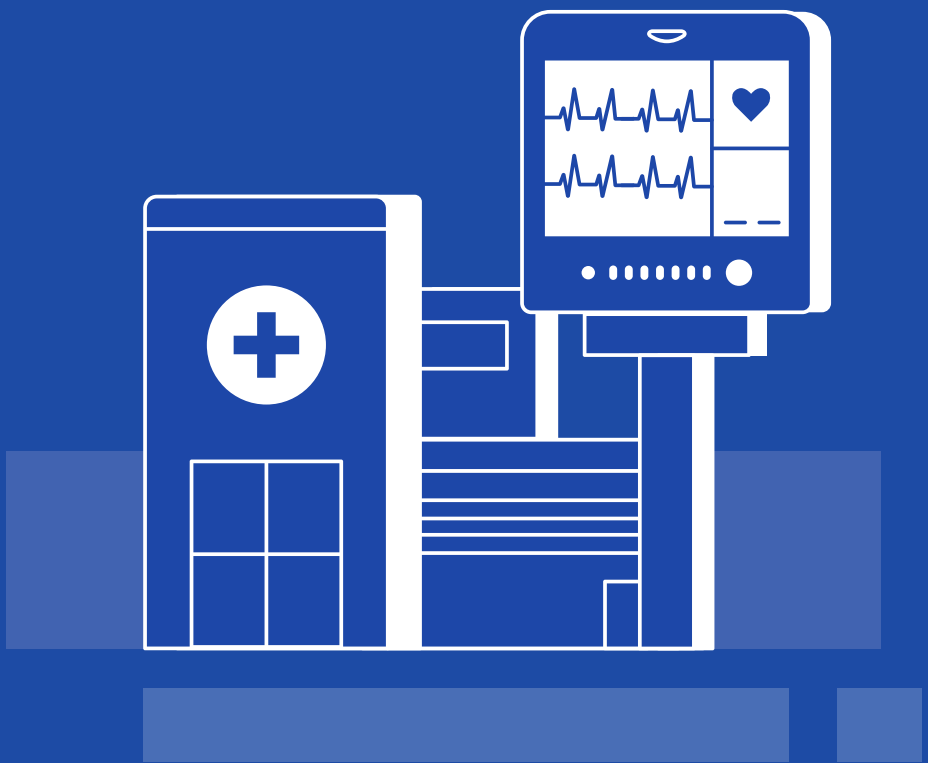
VDOO

VDOO's Security Platform for Internet of Medical Things (IoMT)



Introduction

Connected medical devices are used now more than ever, and there is rapid growth in the usage of such devices. The motivation for this abundance is clear: Connected medical devices used by patients allow constant monitoring of the medical situation of a patient, more precise anomaly recognition, and better supervision by the treating physician. Connected medical devices used in medical centers allow better flow of information and easier monitoring, and they also allow manufacturers to continuously update the devices with new features, making them safer and more precise. In the US, hospitals have an average of 15 connected medical devices per bed, and in the next decade, as many as 50 billion medical devices worldwide will connect to clinicians, health systems, patients, and each other (according to the Deloitte report).

This effect, by nature, constitutes a two-dimensional threat—privacy risk and physical threat. The potential privacy risk is the leakage of patients' sensitive medical information. The potential physical damage is also unprecedented; for example, compromising a connected drug pump or pacemaker can pose a threat of great magnitude and possibly death. Recent research on the matter has shown that such devices are vulnerable, and this led the FDA to recall pacemakers, NIST to publish a specific guide for Securing Wireless Infusion Pumps, and Former US Vice President Dick Cheney to disable his pacemaker's wireless capabilities to thwart possible assassination attempts.

Cyber attacks on health institutions, as shown in past years, can also disrupt vital services, impact patient confidence and regulatory inspection, cause significant financial losses, and above all, pose a risk to patient safety.

The growing number of attacks, zero-days discoveries, and malware crafted specifically for IoT devices indicate cybercriminals' intentions to exploit IoT devices' lack of security. This shift impacts the entire IoT ecosystem, which struggles to evolve its security at the same pace. The cyber criminals are the ones evolving most rapidly due to the security gaps mentioned, creating a very lucrative opportunity for them.

VDOO's Solutions for Internet of Medical Things (IoMT)

VDOO's platform enables trust in IoT devices by securing them throughout their entire lifecycle—from the design phase through the post-deployment phase when the device is used in its operational environment. The automatic technological capabilities VDOO's platform is based on make it suitable for any device type, including medical devices.

With Vision™, VDOO's analysis solution, device makers can analyze device firmware, regardless of its type or purpose, and receive an accurate description of the device's security status followed by mitigation guidance for device hardening. Beyond the described analysis process, the solution also helps in revealing important pieces of information on the analyzed device. This type of information is usually inaccessible to the device maker or the institute using the device since they usually do not have suitable tools to discover it; for example, the software and hardware bill of materials (BOM) listing all the components, as was recently published by the FDA as a way to ensure safety for devices that affect people's lives.

Upon meeting the security requirements, VDOO provides VDOO CertIoT™—a digital and physical security certification to help with signaling that the required security requirements have been met. The certification helps manufacturers position themselves as security innovators and leaders and gain a competitive advantage against their competitors that have not yet invested in security. In addition, CertIoT also helps device buyers, users, and integrators to make better decisions when considering which devices to use.

By using ERA™, VDOO's Embedded Runtime Agent solution, the device maker as well as the organization deploying the IoT devices can make sure they will remain safe and secure after deployment. To date, VDOO's agent is the only auto-generated agent protection that is installed on the IoT device. IoT devices were not designed to run traditional third-party endpoint security solutions, which strengthens the need for a device-specific agent.

Makers and medical institutes, such as hospitals, clinics, and health care providers, can rely on alerting 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 connected and secured medical devices.