VDOO

ERA™ – Embedded Runtime Agent

Essential Protection for Embedded Systems Against Known and Unknown Threats

DATASHEET

Runtime Protection for IoT Security

IoT devices and embedded systems are easy to hack, mainly because they were not necessarily meant to interact with the internet and therefore were not built with cybersecurity in mind. The rising number of IoT cyber-attacks, the complexity of the attacks, as well as the variety of malware samples and malware types crafted specifically for IoT devices reflect the attackers' awareness of the huge opportunity IoT technology holds for them. Threats are evolving most rapidly, and the entire IoT ecosystem is struggling to evolve its security at the same pace. Device manufacturers who want to offer their customers secure devices, as well as enterprises that use IoT devices, are advised to implement an on-device agent to protect against device breach attempts and to gain predefined and on-demand mitigation capabilities to deal with emerging threats, including known and unknown vulnerabilities.

Tailored for Your Device

As opposed to IT security solutions, having one agent type to protect all embedded devices is not possible; therefore, a tailored agent per device type is necessary. With VDOO, the agent is automatically tailored for each device based on an analysis of its firmware binary by Vision™, VDOO's analysis platform. This approach makes ERA™ the most suitable runtime protection layer for the device as it is focused on the specific threats the device is exposed to and the resources (CPU, storage, and memory) it has to avoid any significant performance or functionality loss to the device while providing runtime protection. To date, ERA™ is the only auto-generated runtime protection that is installed on the IoT device. IoT devices were not designed to run third-party endpoint security solutions and certainly not the traditional solutions which strengthens the need for a device-specific embedded runtime agent.

Protection from Different Threat Types

The VDOO agent provides a range of protection types against known and unknown threats. The protections can be adjusted by the device operator according to the chosen operation mode: “Prevent” in order for the agent to block an attempted attack, and “Alert Only” in order for the agent to alert on an attempted attack, without prevention.

The agent is based on a multi-layered approach that utilizes dozens of mechanisms to prevent each step of the attack separately. Among other things, it provides exploit mitigation capabilities to block the exploitation of IoT specific vulnerabilities, memory corruption vulnerabilities, and common logic flaws. It also detects and blocks many common attacks on IoT devices—the execution of undesired binaries and scripts, modification of critical assets, code injection, abuse of system and network resources, as well as network attacks such as man-in-the-middle (MITM).

Technical Description & Specifications

VDOO allows the device manufacturer, as well as the user's security team, to adjust the agent's fully granular protection policy according to the user needs and preferences. For example:

- Adjustable operation modes can be set to detect or prevent attacks.
- Locally stored logs can be sent to a Syslog/SIEM server or to an ELK Stack, according to the security team decision.
- Custom defined whitelists or blacklists can be made for specific device protection modules.

Supported OS	Linux | Android
Supported CPU architecture	MIPS | ARM | x86_64
CPU overhead	<1%
Storage overhead	<1MB
Operation modes	Online/Offline | Active/Passive/Learn

IoT Device Agents Are a Must

The typical advice for avoiding IoT device cyber-attacks continues to be installing the latest patches, although it is usually a very challenging task. Updating the device OS or firmware requires significant adaptations the user sometimes cannot allow because of lack of expertise and risk of data loss. This results in unpatched devices that are exposed to many known and unknown threats. Moreover, even if the resources were invested in the device to make it fully-patched, the device will still be exposed to zero-day vulnerabilities. For these reasons, an IoT agent becomes an essential layer in the security for IoT, as it protects against known and unknown threats.

Proprietary Research Approach

The VDOO IoT agent was built based on vast research of embedded device threats that includes the device components, hardware, OS, kernel, and software libraries. ERA™ blocks the execution of various IoT malware types, including the most recent ones such as Mirai, VPNFilter, Torii, and Chalubo.

About VDOO

VDOO was established in 2017 to pioneer embedded systems security, with an end-to-end solution of security automation, certification, and protection. The VDOO founders' backgrounds include an endpoint cybersecurity startup acquired by Palo Alto Networks, as well as notable experience serving in elite units in the Israeli Intelligence corps. For additional information, please contact us at info@vdoo.com or visit our website at vdoo.com.

Key Features

- Automatically tailored for each device
- Low CPU, storage & memory overheads
- Adjustable protection policy
- Various operation modes

Key Benefits

- On-device runtime protection
- Protects from a wide variety of threats
- Covers for unpatched vulnerabilities

Related Products

- VDOO Vision™
- VDOO CertIoT™
- VDOO Quicksand™