REPORT REPRINT

Vdoo launches integrated platform to ensure IoT device security

AUGUST 17 2020

By Johan Vermij, Aaron Sherrill

Israeli startup Vdoo targets integrated device security across the entire device lifecycle for OEMs and vendors of connected devices, embedded systems and IoT products. The platform empowers OEMs to offer ongoing managed security services or partner with MSPs and MSSPs to deliver these services.

451 Research

S&P Global
Market Intelligence

Introduction

The Israeli startup Vdoo launched its security analysis platform Vision in 2018 and released ERA, an embedded runtime agent, in 2019. As both products gain traction across multiple verticals, the company has now launched its Integrated Device Security platform to support original equipment manufacturers and vendors in designing, building and sustaining secure connected devices.

451 TAKE

In an ever more connected world, the attack surface is growing exponentially, and IoT security is becoming more important. According to 451 Research's Voice of the Enterprise: IoT, Budgets and Outlook 2020 survey, improved security now tops the list as most important business driver to increase IoT spending. Many security vendors take a passive approach to device security by providing endpoint protection, passive network monitoring, segmentation and threat discovery, but in the end, the devices themselves are still insecure. The logical next step is securing the device per se, but hundreds of thousands of OEMs lack the in-house expertise to address all vulnerabilities. Vdoo is an early entrant to the emerging embedded security segment, which is taking on the challenge of securing connected devices. Vdoo is inserting itself into primary production processes by offering OEMs an integrated security platform that supports the entire device lifecycle from secure design to real-time monitoring of deployed assets. This will likely position it more as a strategic partner than as a security vendor.

Context

Tel Aviv-based Vdoo, which means 'verification' in Hebrew, was founded in 2017 by industry veterans Netanel Davidi and Uri Alter, who sold their endpoint security company, Cyvera, to Palo Alto Networks in 2014 for $200m. The third cofounder, Asaf Karas, has an extensive background in security research with a focus on reverse engineering, embedded security and forensics with the Israeli Defense Forces.

The company received initial funding of $13m in 2018 backed by 83North (formerly Greylock IL) and Dell Technology Capital. A second round of $32m series B funding followed in 2019, led by GGV Capital and WRVI Capital with participation from NTT DOCOMO Ventures and MS&AD Ventures. Vdoo has grown to approximately 75 employees and has a presence in the US, EU and Japan and is looking to expand further into these territories.

Strategy

Vdoo primarily targets large device manufacturers, vendors, operators and service providers across multiple verticals given that device security is a problem across the board. The company says its growing customer base shows a fairly even spread of tier one and two vendors across the medical, industrial, automotive, utilities, telecom and electronics sectors.

With the launch of a more integrated platform approach to device security, Vdoo provides an opportunity for device manufacturers to monetize device security as a business model. The platform empowers OEMs to offer ongoing managed security services or partner with managed service providers (MSPs) and managed security service providers (MSSPs) to deliver these services.

Technology

The billions of connected devices deployed around the globe represent a large potential security risk. These devices collect data, control physical environments, influence supply chains, improve healthcare, and maintain safety and security. As these IoT devices start bridging the digital and the physical worlds, the level of risk and liability for organizations rapidly increases as attacking or disrupting these devices can result in real-world consequences. Vdoo believes the best way to secure these devices is with a device-centric, lifecycle platform approach that provides ongoing risk analysis and actionable insights both during development and after deployment.

The Vdoo Integrated Device Security platform is a SaaS offering that helps manufacturers identify security flaws throughout the design and production stage of new devices, as well as on existing products. A device usually consists of many third-party components and chipsets to which the device maker adds its own software and device capabilities. During the Vdoo analysis, which is done by uploading the firmware binaries, the device is analyzed as a whole, including the third-party components, credentials, crypto mechanisms and boot components. Vdoo can identify known vulnerabilities by matching the individual components to common vulnerabilities and exposures (CVE) databases and assess whether these vulnerabilities are exploitable in the specific context of the device. Beyond identifying known vulnerabilities, Vdoo detects faulty device configuration, general hardening issues and potential zero-day software vulnerabilities. In addition, the platform provides device-aware prioritization of detected issues, as well as remediation instructions using a step-by-step approach so engineers without specific security knowledge can see how to resolve identified issues. The platform integrates with multiple build and ticketing systems to make implementing fixes an integral part of the development process.

Vdoo's core capability is its ability to perform binary analysis of embedded software. Binary analysis is required in this case to inspect third-party components and compiled software to understand their inner workings and find vulnerabilities without having access to the source code. Analyzing the binaries instead of the source code allows Vdoo to mimic the attacker's approach, covering components that are not included in source code analysis, and protecting vendors' intellectual property by helping to reduce potential exposure of their source code. Additionally, it can detect the use of outdated cryptography and crosscheck databases for leaked passwords. In considering the full device context, Vdoo claims to eliminate many false positives.

The platform not only helps manufacturers eliminate or mitigate vulnerabilities during the production stage, but also during device deployment; the embedded runtime agent continuously provides real-time protection against new threats, informs the Vdoo platform regarding suspicious device behavior and can also prevent such behavior. The company says the platform provides proactive vulnerability mitigation, compliance validation, real-time protection and monitoring, and actionable insights across the entire device lifecycle. With an embedded agent that is automatically customized for each device based on its analysis findings, Vdoo delivers multilayered protection blocking threats and providing relevant alerts based on its focused, device-aware threat intelligence.

Competition

Although Veracode was among the first vendors to offer widely applicable binary analysis as part of the application security landscape, binary analysis is a relatively new approach to tackling security vulnerabilities in IoT/IIoT devices per se. In this area, Vdoo's main competitor is Synopsys, which provides a variety of tools for software and application security analysis. Other early firmware analysis tools include spinoffs of the Fraunhofer Institute for Applied and Integrated Security Firmware Analysis Framework (FAF). There is a large community of open source developers offering tools to device manufacturers to perform firmware analysis, but Vdoo is among the first to commercialize binary analysis and integrate it into a full platform to help manufacturers build more secure devices step by step. Additional vendors offering firmware analysis tools include Attify, IoT Inspector, ReFirm Labs and SecuriThings, which also offers real-time monitoring through an embedded-agent approach.

As IoT security has become more important, other vendors have developed a similar vision to secure the device throughout its lifecycle through design, build and sustain stages. Mocana and Sequitur Labs are among those to take on this challenge starting at the silicon level.

SWOT Analysis

STRENGTHS

Device manufacturers are being increasingly challenged to ensure the confidentiality, integrity and availability of their products. Vdoo's automated platform enables manufacturers to integrate security into product design and ensure devices remain secure after deployment.

WEAKNESSES

In offering a relatively new approach to securing IoT devices, Vdoo not only needs to win over manufacturers, but it also needs to help them convey the value of ongoing security services to its downstream customers.

OPPORTUNITIES

The need for IoT device security is gaining visibility and recognition. For example, in the US, the FCC, DHS and Cyberspace Solarium Commission have all recently campaigned for better device security, even recommending legal mandates and laws regarding IoT device security. These moves could be advantageous for Vdoo as it looks to grow its market share.

THREATS

Some of Vdoo's strengths rely on an embedded agent on the device; however, many manufacturers are opposed to that approach. The company will need to invest in educating the market on the value and expanded capabilities an embedded agent can provide.