Vision™

Automated Security Analysis and Mitigation Platform for IoT Devices

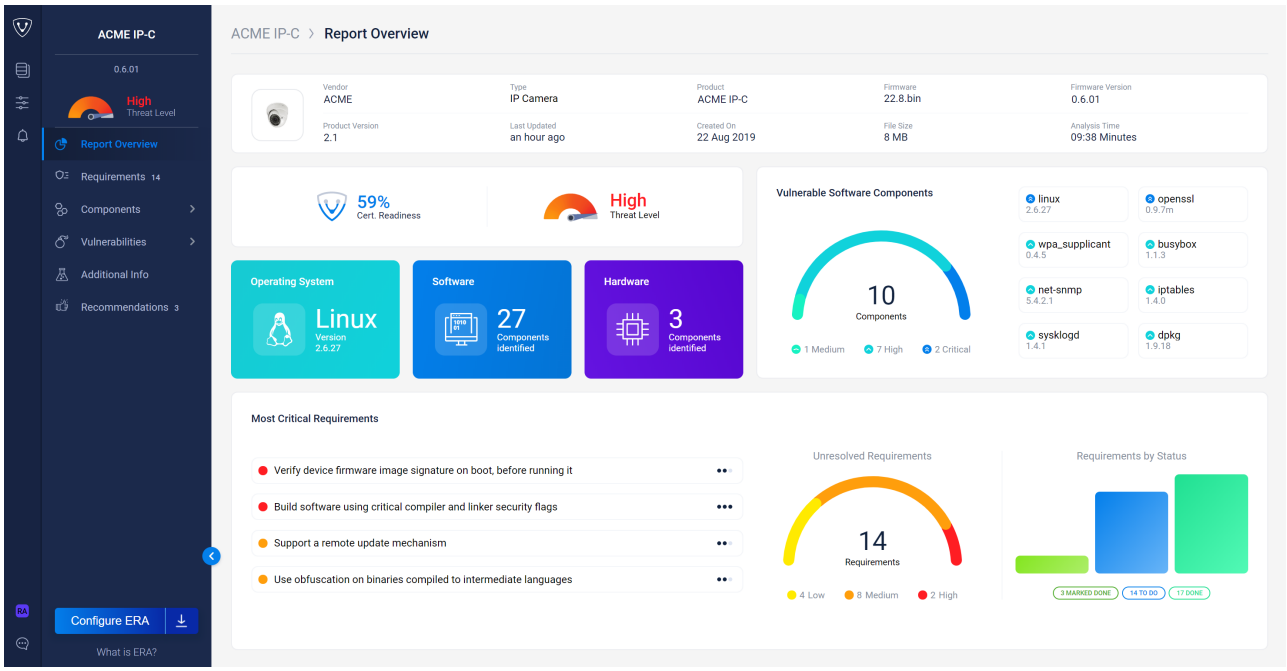
DATASHEET

Automated Approach for IoT Security

Connected 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 cyber security in mind. The wide variety of IoT devices and their nature (low resources: memory, storage, CPU) make it difficult to identify requirements for each device type and implement security. Therefore, manual security testing is not effective, and the time has arrived for an automated approach. We have built an automated analysis platform to meet your needs, whether you are a device manufacturer, integrator, or enterprise that uses devices—you can utilize our platform in a cost-effective way with no impact on the product's efficiency or time-to-market.

The Analysis Process

The platform's input is the device's firmware binary file, with no need to expose any source-code. After uploading the binary of any given IoT device, the platform analyzes it while classifying and extracting the device hardware components and software libraries. Then, based on VDOO's proprietary algorithms, the platform calculates the threats and creates a security outline for the specific device. Lastly, it conducts a deep analysis to identify concrete security gaps and provides the user with step-by-step guidance on how to fix them. Such gaps could be faulty architectures, security malpractices, wrong configurations, backdoors, missing security building blocks, exposure to known vulnerabilities (CVEs), and exposure to suspected new vulnerabilities, with emphasis on potential command injections. Upon meeting the security requirements, VDOO provides a digital and physical security-certification to help with signaling that the required security requirements have been met.



VDOO Vision™ analysis platform report overview

Get to Know Your Devices

Beyond the analysis process described, the platform also helps to reveal important pieces of information on the analyzed device. This type of information is usually inaccessible to the device maker or the enterprise using the device because they are simply not aware of it or do not have the tools needed to discover it. The VDOO analysis platform automatically produces a detailed analysis of the device security posture, including:

- **BOM auto-discovery:** Software and hardware, including specific package version, patch version and licenses, covering 1st party and 3rd party components
- **CVEs:** Details known vulnerabilities in the discovered software packages
- **Requirements:** Security needs that should be satisfied in order to mitigate various security gaps in architecture, software, network, authentication, procedures, and cryptography. The requirements can be filtered by the requirement's criticality and the required mitigation effort level. Each requirement includes:
  - Indicators and findings for checking whether the requirement has been properly implemented or not
  - References for similar requirements in leading standards and regulations
  - Knowledge base (KB) articles with a thorough, step-by-step explanation on how to mitigate the problem in the most cost-effective manner
- **Visibility:** Device internals, including initialization flow, unsafe APIs, critical assets for protection and hardening, coding malpractices, secrets and keys, permissions and users, suspected zero-day vulnerabilities, and more
- **Compliance:** Verification of the device's adherence to emerging global IoT security standards, such as NIST, ENISA, DCMS, and IoTSF
- **API:** Full integration with CI/CD platforms for ongoing security analysis, mitigation, and hardening
- **Executive summary:** Threat ranking, certification readiness, bill of materials (BOM) summary, number of identified CVEs, and number and status of security requirements
- **Dashboard:** A dashboard for the product manager and security stakeholders to review the status of all products

Security by Design

VDOO Vision™ includes a unique tool for designing new devices that allows the security architect and development teams to fully understand the device security threats and requirements in the initial design and development stages.

Cybersecurity Expert Know-How

In addition to the step-by-step mitigation guide provided for each security requirement, the platform allows access to VDOO's valuable knowledge base, where the curious user can find detailed information on security best practices, threats, and risks, organized into topics for convenient use.

Proprietary Research Approach

VDOO has conducted vast research combined with machine learning on embedded devices. As part of this research, over 15K firmware binaries consisting of more than 2.5M executables have been inspected to build the VDOO automated analysis engine. The engine is continuously enhanced with more and more new research findings. To date, the VDOO research team has discovered more than 120 IoT-specific 0-day vulnerabilities, as well as dozens of security findings per analyzed device.

Smooth Security Implementation Process

The analysis process does not require any access to source code and is performed as part of the CI (Continuous Integration) process, providing the development team with best practices and cybersecurity know-how via an actionable tool. VDOO's automated analysis platform carries out a neutral audit and cost-effective guidance for security implementation.

Specifications Table

Supported OS	Linux | Android
Supported CPU architecture	MIPS | ARM | x86
Max firmware binary size	Up to 100GB
Average analysis time	13 minutes

For additional information, contact us at info@vdoo.com or visit our website at vdoo.com.

VDOO

Key Features

- Security gap analysis within 30 min
- Suitable to any device type
- Covers 3rd-party threats
- No need to access source-code
- Device specific mitigation guide
- Requirements are sorted by criticality

Key Benefits

- Defines the device threat landscape
- Generates software and hardware bill of materials (BOM)
- Checks compliance with NIST, ENISA, DCMS, IoTSF, and more
- Does not impact product efficiency and time-to-market
- Used to discover over 120 IoT-specific 0-day vulnerabilities

Related Products

Once security risks are mitigated:

- VDOO CertIoT™

Device protection post-deployment:

- VDOO ERA™
- VDOO Quicksand™