vdoo securing the connected everything

Vision

Automated Security Analysis and Risk Assessment for Connected Devices

info@vdoo.com

vdoo.com

Automated Approach to Connected and IoT Device Security

Driven by rapidly growing market adoption, and increased exposure to cyber threats, security has become a critical requirement for connected devices. Device manufacturers, vendors, operators and service providers need visibility into their devices' software components—many of them from third parties—and security posture, in order to manage risk and meet increasing security demands from both customers and regulatory bodies.

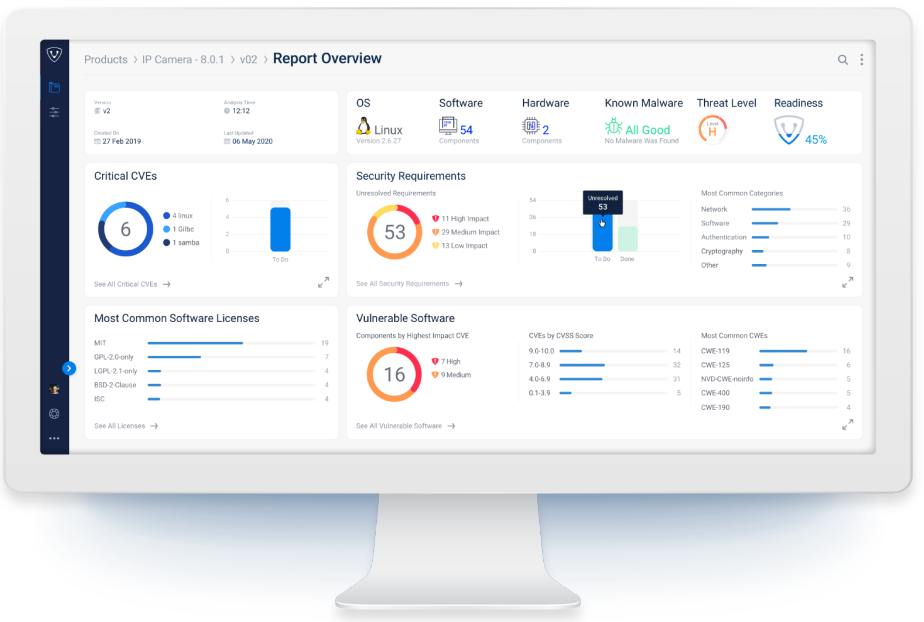
Vdoo addresses this need with Vision, an automated security analysis solution for connected devices. Vision provides full visibility into device composition, comprehensive security information, and rich vulnerability remediation capabilities, enabling quick detection of security risks and efficient resolution of the highest-impact issues in connected products.

Vision enables manufacturers and providers to secure the devices they deliver efficiently, consistently and at scale. It is fast, accurate (detecting high-priority issues with minimal false positives), actionable, and easy to integrate into existing development processes.

Quickly Identify and Mitigate Risks

Vision performs automated analysis on device images or other binary artifacts to identify their software composition and provide complete security information (CVEs, exposures, potential zero-days and more) in minutes, instead of the weeks to months it takes to get results from manual testing. This enables on-demand security assessment of devices from early stages of design and development through to product release, production, deployment and ongoing maintenance—reducing security implementation time and effort.

The Vision analysis reports provide relevant, actionable information for product security experts, developers, researchers, architects and business leaders, from high-level dashboards showing overall security levels and risk areas to detailed background, device-aware impact assessment, compliance information and step-by-step remediation guidance for specific security issues. Comparison views enable tracking of product security changes over time.



Product Highlights

Automated device security solution combining software composition analysis, static and dynamic security analysis

Detects a broad range of security issues: CVEs, configuration issues, security malpractices, potential zero-days & more

Smart device-aware impact analysis and issue prioritization, taking into account the full device context

Practical guidance to quickly resolve security gaps with minimal device impact and dependence on third-party vendors

Ongoing threat monitoring and vulnerability alerts for analyzed products

Compliance validation with industry standards and internal product security policies

Integrates into SDLC tools and automated workflows

Analyzes the device's binary image so access to the source code is not required

Easily Resolve Security Gaps

Vision provides clear remediation guidance for each issue, ranging from step-by-step remediation instructions to references to specific findings in the code to long knowledgebase articles, enabling quick gap resolution without the need for security expertise. Our goal is to provide the simplest issue resolution options, minimizing the need for software patching, re-coding, or architectural modifications, which can be difficult or impractical to implement while introducing new risks.

Reduce Risk with Comprehensive Security Coverage

Vision combines software composition analysis, static analysis and dynamic analysis techniques to produce accurate in-depth picture of a device's components and security posture. Vision detects a broad range of security issues including known vulnerabilities (CVEs), security exposures such as weak authentication and broken cryptography schemes, faulty configurations, malware instances, and potential zero-day vulnerabilities.

Gain Visibility into Third-Party Products and Components

Vision analyzes the binary artifacts, therefore it can be used to analyze products or components sourced from third-party suppliers without requiring access to their source code. Effectively manage your supply chain security by performing risk assessment as part of vendor or component selection processes, or by using analysis results to guide the definition and enforcement of security policies.

Focus on the Highest Risk Issues

By analyzing the device's binary image, rather than its source code, Vision can take into account the full device context—its attributes, components and configuration—and pinpoint the issues that would make most impact in real-world attack scenarios. Vision automates the analysis approach that a penetration tester (or an attacker) would take to find exploitable vulnerabilities in a finished product.

Simplify Compliance Validation

Vision helps streamline and speed up compliance validation efforts. The security issues detected by Vision are mapped to the specific requirements of dozens of industry standards such as OWASP ASVS, IEC 62443, UL-2900, FIPS 140-2, and ENISA Baseline Security Recommendations for IoT, enabling automated compliance checking. It is also possible to validate compliance with internal policies or customer demands by defining the set of requirements tracked by Vision that must be fulfilled.

Smoothly Integrate Security into Existing SDLC Systems

Using our API, Vision easily integrates with software development lifecycle (SDLC) tools and continuous integration / continuous development (CI/CD) workflows, enabling automated security implementation as a built-in part of the product development and release process.

The Vdoo Integrated Device Security Platform

Vdoo Vision is part of the Vdoo Integrated Device Security Platform, the only automated device security platform that covers the entire device lifecycle – from design, development and testing to deployment and maintenance.

Our platform provides everything companies need to secure their connected products consistently at scale. Our threat intelligence operations provide relevant and updated device-focused data which, combined with robust machine learning capabilities, becomes the basis on which the entire platform functions.

Built on Industry-Leading Device Security Expertise

Vdoo's offering is built on the extensive experience of our team that includes world-class experts in embedded system architecture and vulnerability research, reverse engineering, and binary code analysis. The team has analyzed thousands of firmware images, hundreds of millions of binaries, and thousands of vulnerabilities to generate a vast device security knowledgebase and has so far discovered more than 300 new zero-day vulnerabilities.

Vdoo Vision Benefits

Lower security risks
Detect and resolve threats and vulnerabilities throughout the entire connected device lifecycle

Increase efficiency
Focus on the highest priority issues and enable fast resolution without the need for internal security expertise

Control supply chain security
Gain visibility into the security of third-party products and components without access to their source code

Simplify security integration
Integrate device security capabilities into existing development, operational and asset management systems

Shorten time-to-market
Perform on-demand automated analysis in minutes rather than manual processes that take months

Speed up compliance
Quickly validate adherence to industry standards and internal security requirements

About Vdoo

Vdoo was founded by serial entrepreneurs who previously sold cybersecurity company Cyvera to Palo Alto Networks, bringing with them extensive knowledge of endpoint and embedded system security. The company has raised $45 million from top-tier investors including 83North, Dell Technology Capital, WRVI Capital, GGV Capital, NTT DOCOMO and MS&AD ventures. Vdoo has offices in the US, Europe, Japan and Israel, and dozens of well-known global customers.

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