Vdoo
Securing the Connected Everything

Customer Case Study

Vehicle Manufacturer Chooses Vdoo to Validate Security for Automotive Software Components

The Need

As a top innovator in the automotive industry, a leading global OEM is continually expanding its vehicle connectivity features to enhance customers' driving experiences and safety.

Recognizing the cybersecurity risks introduced by increasingly complex connected vehicle systems and functionality, the manufacturer's product security team has been working to incorporate processes and technologies designed to control and manage those risks.

In addition, increasing regulatory enforcement, notably the UNECE WP.29 cybersecurity regulation, has driven the OEM to focus on implementing new security processes and tools both before and after start of production.

The Challenges

With many ECUs in use in their vehicles and the increasing complexity of their software, the OEM was facing difficulties in keeping pace with vehicle cybersecurity and risk management requirements. The product security team realized that to achieve security at scale, they would need to automate cybersecurity tasks which were being handled manually or using multiple distinct tools, throughout all stages of the vehicle lifecycle.

Another significant challenge was the lack of transparency and control over the security of their growing supply chain. The manufacturer had to rely on suppliers for critical security information, with limited capability to test and validate this information internally.

Finally, they did not have effective mechanisms in place to quickly triage new vulnerabilities and identify the affected vehicles—a key capability needed to support continuous risk assessment and management requirements.

About the Customer

- Top global automotive manufacturer
- Headquartered in Europe
- Leading supplier of private and commercial vehicles
- Increasing focus on product security for connected vehicles due to growing risks and regulatory demands

Automating Product Security Analysis

The OEM's global product security team is tasked with obtaining a comprehensive and precise assessment of their vehicles' cyber-risk exposure. To achieve this goal, they require deep visibility into the security posture of their automotive ECUs, and the potential risk impact of existing software security gaps.

For third-party ECU software delivered by their suppliers, the team was lacking the means to gain the accurate security information they needed. Without access to the source code, they had limited ability to independently identify each ECU's software bill of materials (SBOM), detect vulnerabilities and exposures, and assess their impact.

In addition, their internal software testing and validation processes were resource-intensive and time-consuming. The team was using a mix of methods to validate the security of ECU software: white-box testing techniques such as static code analysis when source code was available, black-box testing techniques such as fuzzing on software provided by their suppliers as binaries, and more. The aggregation and analysis of results from multiple sources and tools required heavy manual effort.

The team decided to consider the Vdoo product security platform to help them increase their visibility, efficiency and scale. After a successful proof-of-concept, the team chose to start using the platform for automated security analysis of multiple ECUs.

Vdoo enabled them to analyze their ECUs simply by uploading their software images in binary form, and to receive comprehensive results in minutes. The platform provided them detailed information including:

- Software bill-of-materials (SBOM), known vulnerabilities, security exposures, and malicious files found in the ECU
- Potential zero-day vulnerabilities detected in the software, augmenting findings from their current pen-testing activities
- Smart prioritization for each issue based on its exploitability and potential impact in the context of the entire ECU and its configuration
- Clear issue resolution and hardening guidance, which the team found helpful to enable quick remediation of the actual important issues

Post-Production Vulnerability Monitoring and Triage

Beyond cybersecurity implementation in the development phase, the OEM and Vdoo are also collaborating to establish ongoing vulnerability management and accelerate triage efforts for newly discovered vulnerabilities in post-production assets.

To comply with the UNECE-WP.29 cybersecurity regulation and ISO/SAE 21434, the OEM is required to have the processes in place to identify new vulnerabilities, assess their true impact, and associate them with affected assets. This requires a combination of threat intelligence to know when new vulnerabilities arise, the ability to trace these vulnerabilities to affected vehicles based on the software components they have, and the ability to assess the actual risks created by the vulnerability.

The product security team was using labor-intensive manual methods to perform tasks such as determining if a new vulnerability affecting a specific software component impacted any of their ECUs. They desired to streamline and automate their processes to significantly improve their efficiency and speed.

They decided to leverage the continuous vulnerability monitoring capability offered by the Vdoo platform to automatically track vulnerabilities for all previously analyzed ECU software. This allowed them to benefit from both relevant, timely alerts based on continually updated security information gathered and researched by Vdoo, as well as readily available information on which ECUs are affected based on their software composition detected in the analysis phase.

To facilitate automated identification of on-road vehicles that contain the vulnerable components and thus are affected by a vulnerability, Vdoo and the OEM are working on integration of the Vdoo platform with an in-vehicle software management system.

Supporting Open-Source Compliance

To explore further use of the Vdoo platform's software composition analysis capabilities, the OEM's product security team introduced Vdoo to another group in the organization responsible for free and open-source software (FOSS) license compliance.

The group engaged in a proof-of-concept to see if the Vdoo platform could provide more accurate identification of open-source components than the vendor-provided SBOM lists. After performing automated scans of a few ECUs' software images, they investigated the findings from the automated analysis and cross-checked with the vendor-supplied data. They found that Vdoo provided more accurate SBOM information, giving them higher assurance of compliance with open-source license terms.

Benefits Gained fromUsing the Vdoo Platform

Increased efficiency

Leveraging automated security assessment, prioritization, hardening guidance, vulnerability monitoring and triage capabilities, the OEM augmented existing manual processes and reduced the time and effort for product security tasks

Improved risk management

With comprehensive security findings for both internally developed and third-party software, the OEM achieved new levels of visibility into supply chain risk, gaining additional assurance and independent vetting capability

Compliance readiness

With enriched FOSS component and license information, and the tools to implement automotive cybersecurity processes across all phases of the vehicle lifecycle, the OEM was able to address compliance requirements

About Vdoo

Vdoo delivers an automated device security platform enabling companies to ensure optimal security posture for their IoT, connected and embedded devices, with speed and at scale, from development to post-deployment. 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. Vdoo is backed by top-tier investors including 83North, Dell, WRVI, GGV, NTT DOCOMO, and MS&AD. 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

vdoo