The Rising Cybersecurity Challenge

The number of connected cars on the road is increasing rapidly, and with it the number of connected components, to the point where a single car can include hundreds of millions of lines of code. Several key car systems—whether related to critical controls, basic functions or driver systems—already enable Over the Air (OTA) software updates, and more and more Electronic Control Units (ECUs) are expected to enable this feature in the near future. This allows OEMs to continuously update their cars with new features that enable additional functionality and services and reduce the number of recalls.

As positive as these developments may be, the exponential growth in connectivity between the components of each car and between these components and external systems, have also created new data privacy and physical safety risks. Vulnerabilities in a seemingly low-risk component such as the car’s infotainment system may end up compromising critical functionality, posing an immediate physical threat to the car’s driver and passengers. The variety of interfaces and communication protocols used by the different car systems add even more critical risks, such as control takeover and interception of communications.

Implementing optimal security across increasingly complex connected car systems has become a challenging yet critical imperative for the entire automotive ecosystem. To achieve trust and protect their business, they must integrate security across all embedded components and during the car’s entire lifecycle, both before and after it is on the road.
The Vdoo Integrated Security Platform for Connected Cars

The automated Vdoo platform provides automotive OEMs and Tier 1 suppliers with the full visibility, deep security analysis and rich risk mitigation capabilities they need to ensure the security of all car components across the entire lifecycle – from design and development, all the way to production, deployment and until end-of-life.

Why Use the Vdoo Integrated Security Platform for Connected Cars?

- **Lower monetary, regulatory and legal risks**
  Enforce security policies and controls at every stage of each component’s lifecycle

- **Address security post production**
  Continuously monitor and manage threats for post-production assets; proactively stop threats with runtime agents

- **Gain visibility**
  Mitigate supply chain risks by gaining visibility into all third-party components

- **Simplify implementation**
  Automate and integrate security into every phase of the V-Model and the SDLC

- **Speed time-to-market**
  Reduce security analysis from weeks to minutes and quickly fix high priority issues

- **Comply with industry standards**
  Meet requirements of industry standards such as ISO 21434, UNECE WP.29 and more
Comprehensive Security

The Vdoo platform addresses the cybersecurity challenges of the automotive industry, considering the complexity of using many disparate components and software supply chains as well as the growing requirements to extend security beyond the production phase. It provides full visibility into connected car components and control over their security:

• Analyzes both proprietary and third-party components using advanced binary firmware analysis, without requiring the source code
• Identifies known CVEs and security issues as well as unknown zero-day vulnerabilities
• Creates component-specific risk assessment and mitigation guidance based on analysis findings
• Provides real-time component-specific vulnerability monitoring and threat alerts post-deployment
• Generates runtime protection agents per component for proactive threat detection and prevention on deployed vehicles

Efficiency and Automation Focused

Designed to simplify the process of implementing security, Vdoo enables OEMs and their suppliers to identify, manage, monitor and mitigate threats in an efficient and timely manner, across multiple car models and at scale:

• Performs automated firmware analysis in minutes, replacing manual security assessment and penetration testing methods that often take weeks
• Prioritizes security tasks and provides rich contextual guidance to accelerate security implementation, including practical information and resolution steps for each issue found during the scanning process
• Supports compliance efforts by mapping discovered security issues to industry regulations and standards to facilitate fast resolution, as well as providing needed security controls to achieve compliance
• Continuously delivers relevant vulnerability and threat alerts for deployed vehicles based on all their components, saving the hassle and expense of internal threat intelligence gathering
• Automatically generates a runtime agent for each component, tailored to its specific attributes and security needs, based on analysis results
• Integrates with development and operations systems including continuous integration/delivery (CI/CD), SIEM and asset management systems

Built by Device Security Experts

Vdoo’s offering is built on advanced binary analysis, sophisticated machine learning capabilities, and the extensive experience of a research team that includes some of the world’s leading embedded security experts. The team has analyzed thousands of firmware images, hundreds of millions of binaries, and thousands of vulnerabilities to generate the most comprehensive product security database available today and has so far discovered more than 300 new zero-day vulnerabilities. This continuously updated knowledge base feeds into the platform to ensure that decisions are made based on the most up-to-date component-specific threat landscape.
Automotive OEMs and suppliers can use the Vdoo platform to integrate security into every phase of the V-Model and the software development lifecycle (SDLC).

In the system and software design phases Vdoo provides security architecture and device hardening recommendations, while during unit implementation and testing the platform runs automated security testing, compliance verification and license analysis after each build. Detailed hardening guidance for the vulnerabilities and misconfigurations issues that were discovered can be used to improve product security as well as refine security requirements in the earlier design phases of future iterations.

The Vdoo solution also helps build supply-chain trust. When receiving a software package from a vendor, the OEM can perform a final risk assessment as part of the integration, system testing and acceptance testing phase, in order to ensure that security requirements are met and to manage supply chain risk. The platform also serves as a security gatekeeper for software packages during the production phase and for OTA software updates.

Finally, in the post-production phase the Vdoo platform provides ongoing vulnerability management, monitoring and threat intelligence. In addition, Vdoo provides a Hybrid Intrusion Detection and Prevention (H-IDS) solution for vehicle real-time protection using a host-based runtime agent.

Vdoo Integrated Security Platform for Connected Cars


System design - Requirements specification - Software architecture design - Software unit design - Software implementation - Acceptance testing - System testing - Software integration - Software unit testing

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 Ventures and MS&AD ventures. Vdoo has offices in the US, Europe, Japan and Israel, and dozens of well-known customers across the globe including multi-vertical and automotive-specific OEMs and Tier 1s.

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