It’s Not Your Father’s Connected Car...

Since the automobile was first introduced to the public in the late 19th century, it has gone through a series of transformations. What was once merely a mechanical transport system built upon a single cylinder has evolved into a rolling computer designed by engineers and developers alike, running on over a million lines of code.

With every release, technological advancements have made vehicles much safer to drive; antilock braking systems, electronic stability controllers, backup sensors, and voice controls all have contributed to making our roads safer. Many of those systems now rely heavily on complex software, leading to the inevitable question, For most organizations, the answer is

In the following guide, we will discuss the security risks that are associated with the software within connected cars and introduce development and vulnerability management techniques that are being adopted by leaders in the automotive industry. By integrating these practices earlier and throughout the software development life cycle, you can maximize the benefits of open source software while effectively managing its risks.

Today, any car on the road can contain unpatched software vulnerabilities, putting it at exploitation risk. Because automakers have been focusing their attention on differentiating features, the disparity between innovation and security is growing at an accelerated speed. Open source software is at the heart of this race and enables developers to spend less time reinventing the wheel and more time on innovative, differentiating features.

BMW's iDrive, Tesla's Model X, Apple CarPlay, and Android Auto have turned a car's dashboard into a technological hub for entertainment, navigation, cellular communication, intelligent climate control, and more. Because these features are often built on a core of open source, software security vulnerabilities hidden within the code can put the entire automotive system at risk. To ensure the safety of the passengers and the performance of the vehicle, automakers must vet the code before, while, and after the vehicle goes to market.

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.