VDC Research
Insights for the Connected World

Press Release

Connected Vehicle Cybersecurity Creates Risks and Opportunities in Automotive Market, According to VDC Research

Carmakers finally coming to grips with security threats, but still have a long road ahead.

"The automotive industry should consider itself lucky that severe breaches have not yet occurred in the wild."

Natick, MA (PRWEB) January 29, 2016

Connected vehicles are an attack waiting to happen. The average new car in 2015 contained more than 30 microprocessors, and the cybersecurity of those embedded systems is severely challenged by in-vehicle Internet connectivity. By 2020 more than three-quarters of new vehicles will have Internet connectivity through an embedded modem and/or a smartphone interface, according to a new report by VDC Research (click here for more info).

The inexorable march to add connected features may continue to outpace the extent to which carmakers secure those features against hacking threats. Furthermore, the tiered supply chain of the automotive market distributes responsibility for developing electronic systems across numerous vendors who have only limited insight into the security implications of each others' systems. VDC's report highlights the most problematic aspects of vehicle cybersecurity, and presents business and technical areas of opportunity for vendors in the industry.

"Given the challenges of securing the many subsystems in connected vehicles, the automotive industry should consider itself lucky that severe breaches have not yet occurred in the wild," says Steve Hoffenberg, VDC's Director of IoT & Embedded Technology. While VDC believes it is possible to design and implement secure automotive systems, doing so will require C-suite executives to prioritize cybersecurity in product development and accept the cost consequences of implementing and maintaining security from chip to cloud. "Cybersecurity isn't a saleable feature in dealer showrooms," says Hoffenberg, "but lack of it may be devastating to brand image."

VDC's report examines the impact of both legacy and forthcoming automotive technologies on security vulnerabilities, and includes profiles of key technology vendors active in the many facets of vehicle cybersecurity.

About VDC Research
Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC's coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Natick, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.