

Combatting new types of (cyber) car crime

As vehicles become more connected, their attack surface expands. Cyber threats to cars, drivers, and their data will likely increase, so carmakers need to prioritize security



Automotive manufacturers want to provide complete, connected experiences to drivers and passengers. The more digitalized the vehicle, the more data it gathers, which can inform improvements and innovations.

A rise in sophisticated attacks on cars is mirroring this rise in connectivity. These range from the physical, where the digital nature of the vehicle is used against it to allow theft, to true cyber threats, where the data, access, and even usage of entire fleets are targeted.

The nightmare for OEMs is the thought of fleets of vehicles being hacked, their controls seized while driving, and drivers and manufacturers being held to ransom. Yet many more threats can disrupt their businesses, impact revenues, and damage customer trust.

Where are the threats?

OEMs need to know what is most at risk to combat these potential attacks.

There are three areas likely to be targeted in the connected car:

- 1 Onboard the vehicle:** Software, sensors, and systems that control everything from access to ignition, infotainment to safety controls
- 2 Connectivity and third parties:** Connecting the car to the OEM and other service providers, including the smartphones used to manage the vehicle
- 3 Off-board the vehicle:** Clouds, databases, systems, and infrastructure that run entire fleets

“Cyber attacks on vehicles and OEMs increased by 225% between 2018 and 2021, driven by the interconnected nature of cars and OEMs.”

Upstream

Taking responsibility for car cybersecurity

Protecting the connected car is like protecting an enterprise: the first step is identifying your assets. Having done that, steps can be taken to review how secure these elements are, analyze the likelihood of attacks, and then take steps to prioritize the areas most at risk.

OEMs' big challenge is that securing an asset and delivering differentiated experiences can come into conflict. Take infotainment apps; car makers want to offer drivers and passengers as much choice as possible, whether streaming content, finding a rest stop, or paying for a service. To do that requires apps, and for the most part, OEMs are likely to turn to the expertise of third-party developers. For example, why try to build a streaming service if Netflix can develop an app that works with car operating systems?

Finding the right partners

Threat intelligence, monitoring, assessments of assets and vulnerabilities, and pentesting are all necessary. Many organizations, however, do not have the capabilities and expertise to undertake them. Working with the right partner can make it easier while giving OEMs access to dedicated cybersecurity professionals and constantly updating tools. Specifically, car makers should look for companies that:

-  Have proprietary threat intelligence
-  Continually monitor for evolving threats
-  Experienced in addressing IT and connected car vulnerabilities
-  Equipped with specialist automotive Security Operations Centers (SOC) to support 24/7 threat detection and response
-  Working with a variety of OEMs and ecosystem security partners to ensure that both manufacturers and their suppliers are secured
-  Are experts in pen-testing to find potential weaknesses in existing systems






Four steps to securing the connected car

- 1 Test regularly:** The digital world doesn't stand still. Software updates and new integrations create new openings, and threats constantly evolve. Regular pen-testing can assess existing systems for vulnerabilities, identify risks and provide vital insights into how to protect assets and networks against evolving threats.
- 2 Continually monitor:** With attack methods changing, keeping up to date with how they work and what they strike is critical. Ongoing monitoring will help spot new threats and highlight weaknesses and gaps in existing security systems.
- 3 Embed security:** Too often, security is seen as a bolt-on, added at the end. This leaves solutions vulnerable to being outdated, not integrating effectively with the system it is supposed to protect, and less likely to be updated regularly. Embedding security, by design, helps avoid those situations.
- 4 Understand and anticipate risks:** It can be challenging for OEMs to protect against attacks if they don't know what is at risk; no company can protect against everything, and a complete security lockdown would hamper the overall connected car experience. Instead, car makers need to anticipate where there are risks, the likelihood of them being exploited and respond accordingly.



Why you should choose Orange Business

Orange Business has more than ten years of experience working with automotive leaders, supporting traditional and newer OEMs in developing and deploying new business models. Alongside Orange Cyberdefense, the European leader in cybersecurity, we offer customers:

-  **Unique threat intelligence** from 500+ proprietary, private, and public sources
-  **3000 security specialists** based around the globe
-  **25+ years track record** in cybersecurity

-  **250 researchers and analysts** identifying the latest threats agreements and partnerships
-  **18 SOCs, 14 CyberSOCs and 8 CERTs** spread around the world

Orange Business is the digital partner for OEMs seeking a secure connected car solution.

1. Upstream: 2022 Global Automotive Cybersecurity Report (https://info.upstream.auto/hubfs/Security_Report/Security_Report_2022/Upstream_Security-Global_Automotive_Cybersecurity_Report_2022.pdf)