FAQ page #3

Are connected and autonomous cars a current trend? What is their expected adoption rate?

A research conducted by Navigant Research in 2016, estimates there'll be 188 million connected vehicles with built-in telematics on our roads by 2020; and that completely autonomous cars will account for 15% of all cars shipped globally each year by 2025, and 70% of all shipped cars in 203. Gartner predicts that 220 million connected vehicles on the roads by 2020.

Whether you go with 188 million or 220 million by 2020, that's a lot of connected cars driving around.

Analysts projections indicate partially autonomous cars. What are partially autonomous cars?

The National Highway Traffic Safety Administration (NHTSA) and SAE International have each outlined 5 levels of connectivity, ranging from no automation to completely driverless cars.

The interim levels, levels 1 through 4, each specify increasing levels of connectivity. Level 2 on both charts is the first level identified as partially autonomous, applying to cars with steering and acceleration/deceleration functions performed by the driver assistance system rather than the human driver.

What are the cyber attack risks for connected and autonomous cars?

The greatest risk of a hacked autonomous platform is loss of lives. One attack may affect hundreds of thousands of cars, and can wreak serious havoc. The FBI, in conjunction with the National Highway Traffic Safety Administration (NHTSA), has already issued a public service announcement warning of the massive impact a car with exploited vulnerabilities can have.

What does the automotive industry do to address those risks?

The automotive industry has been gearing up to mitigate the risks posed by connected vehicles. Various automotive cybersecurity boards, consortiums, and information sharing and analysis centers have been established in an effort to improve the industry's cybersecurity knowledge and capabilities.

Automotive companies have also been beefing up their security teams and training, and launching "Bug Bounty" reward programs designed to encourage hackers to help them identify and correct software vulnerabilities. They have also started using static code analysis to try to protect the traffic within the connected cars.

Couldn’t the automotive industry adopt enterprise security methods?

Enterprise security is based on heuristics models of detecting anomalies from normal traffic patterns and is focused on protecting data and commercial services. Heuristics modeling make it acceptable – and expected – to absorb a certain measure of false positives and other detection errors. More so, enterprise security approach is based on constant updates to malware to adapt to the perpetual creativity of hackers.

Autonomous and connected cars’ security needs to protect lives. False positives and detection errors are not acceptable risks. It must also secure the transportation platform regardless of whether it's actively connected to the cloud (as cars may drive in spotty coverage areas without frequent cellular connectivity to the Internet). Security solutions that make critical decisions in the cloud or require anti-malware updates aren't providing ultimate security.

Why do false positives create a major risk for the car industry?

A false positive happens when a security solution misidentifies a permitted call or function as a potential hack and stop its operation.

False positive in a connected or autonomous car means a necessary car operation, like brakes or deceleration, malfunctions. It just can't be allowed to happen.

What is Autonomous Security?

The Carwall product suite is built based on the Autonomous Security framework, which outlines the following criteria required of any security solution that can protect against the high risks that come with autonomous and connected cars:

- The ECU protects itself: It's unique security policy is embedded within the ECU, so all detection and prevention decisions are made locally on the ECU.
- Always-on security: The ECU remains fully capable of protecting itself against potential hacks at all times, no external connectivity is required.
- Zero false positives: Each ECU gets a customized security policy based on its own factory settings. All foreign code is blocked. Even functions that don't follow an approved path are blocked.
- OS and hardware agnostic: Runs on every ECU without requiring any changes or upgrades to its software or hardware.
- Negligible performance impact: Operates reliably on the ECU without interfering with any of its other functions or storage needs.

What make Autonomous Security suitable for the car industry?

Autonomous Security eliminates the risks of a cyberattack on a connected or autonomous vehicle, which is the only acceptable standard for car security. It locks down all a car's ECUs, regardless of connectivity, making a deterministic decision in runtime whether a call or function is permitted under factor settings.

Once Carwall is installed and generates an ECU's unique security policy, that ECU is always able to protect itself from hackers.

How does Carwall Autonomous Security suite work?

Carwall is a security software offered by Karamba Security, that automatically secure a car’s ECUs against hackers. Carwall seals the ECU to provide early detection of cyberattack attempts and to prevent hackers from infiltrating the ECU to gain control over the vehicle’s safety systems.

Carwall’s automated sealing approach provides a deterministic way to protect a car’s ECUs from cyberattack, including in-memory attacks. The patent-pending software is embedded during the ECU’s software build process. It automatically learns the factory settings and creates a security policy that detects and prevents any deviation from those settings. Because Carwall seals the ECU’s software, security bugs contained in that code are also hardened, so they can’t be exploited to infiltrate the car’s safety systems.

What do you mean by factory settings?

Factory settings are the legitimate programs, scripts and function calling sequences the car manufacturers and tier-one system providers intend to run in the car. Because Carwall becomes part of the software build, it automatically learns everything that is allowed in that system, so it can detect and then prevent any foreign codes or calls that don't comply.

Does Carwall also protect against in-memory attacks?

Yes. When Carwall generates an ECU's unique security policy according to its factory settings, it creates a call graph of all acceptable function call paths.

When a function call is made, Carwall checks it, in runtime, against the function call map it created during the build process. If the function call hasn't followed a legitimate path, Carwall detects and prevents it from executing, since it’s an indication a hacker has infiltrated a process in the ECU’s memory.

How does Carwall ensure no false positives?

Carwall bases its security policies on complete factory settings. There’s no ambiguity and no false alarms. If a piece of code or a function calling sequence isn't part of the factory settings, Carwall won't allow it to run, period.

What effort is required to deploy Carwall security policy?

None. Carwall doesn’t add any steps or require any special processes to deploy.

Car manufacturers and system providers follow a rigorous process when they are building or updating automobile software. With one line of code, Carwall integrates seamlessly into this process, becoming part of the software image.

Once deployed, Carwall’s patent-pending technology enables the software to automatically learn the factory settings and create a security policy with no action needed by developers.

Should developers change their development practices?

No need. You seamlessly integrate Carwall into your build server, and Carwall autonomously generates the ECU's security policy according to its factory settings. You don't need to change or add any new developer resources.

Does Carwall require any hardware or software upgrade?

No. A key principle of Autonomous Security is that it can't have any discernable performance impact. In our tests, Carwall only requires ±1% processing power. No need to spend more on an upgraded CPU.

Carwall also works on any operation system, as well as ECUs that run on schedulers. They can all be locked down with Carwall.