AutoSec

Watching Your Vehicles by C2A

WHITEPAPER

THE FIRST AUTOMOTIVE CYBERSECURITY LIFECYCLE MANAGEMENT PLATFORM

INDUSTRY CHALLENGES

AutoSec

CONNECTED CARS MEAN MORE RISK

Today's sophisticated connected vehicle architecture is inherently more vulnerable to cyber-attack. Connected vehicles can host up to 150 electronic control units and run on 100 million lines of code; tomorrow's vehicles may contain up to 300 million lines of software code. Cyber-attacks that exploit the increasing digitization of vehicles present a significant risk to manufacturers, vehicle owners, other drivers and pedestrians. In response, automakers must assess attack vectors, analyze weaknesses, and work to prevent the emergence of new vulnerabilities.
Cybersecurity does not stop at the production of vehicles. Rather, it's paramount that security be accounted for throughout the entire vehicle lifecycle: through vehicle design, manufacturing, and even when it's on the road. All told, this can amount to over ten years of communication between manufacturers and suppliers to continually detect and react to cybersecurity vulnerabilities, which can be discovered at any given moment.

COMPLEX SUPPLY CHAIN

OEMs source vehicle components from a variety of Tier 1 and Tier 2 suppliers, as part of the industry's intricate supply chain. Though it is the responsibility of the vehicle manufacturer to ensure that their value chain partners follow and implement the best cybersecurity practices, all participants have a role to play in mitigating risks and producing vehicles that are secure from design to decommission. With so many automated safety systems as potential targets for cyber-attacks, cybersecurity has become a safety issue.
For the purpose of a successful cybersecurity management, Automotive manufacturers will have to own their cybersecurity lifecycle by ensuring an end-to-end, comprehensive and structured organizational processes. Together with additional technical measures, these processes will enable them to define, control, manage, and improve cybersecurity on an ongoing basis along the entire value chain.

REGULATION IS NOW TANGIBLE

Changes in the regulatory environment for automotive cybersecurity lingered for some time in the industry. Today, the first cut of standards are here and encompassed in the new ISO 21434 standard and UNECE WP.29, which define the categoric directive for implementing cybersecurity management systems for the protection of vehicles. Together with additional standards expected in the future, such as the Cybersecurity Act in the EU, the Chinese ICV program, new guidelines from JASPAR in Japan and legislative proposals in the US Congress, these are vivid examples of the industry-wide collaborative efforts to create a basis for automotive cybersecurity.
Now, OEMs need to independently find their practical way of tackling the challenge of cybersecurity lifecycle management while adhering to these standards.

INDUSTRY NEEDS

AutoSec

IS KEY TO CYBERSECURITY RESILIENCE

Visibility is crucial for cybersecurity management, which needs to be agile, efficient and anticipate future threats. Understanding the supply chain of a vehicle is essential to understanding how to monitor and protect it. Before professional cybersecurity teams can protect their products, they must have full oversight of the inner workings of a vehicle.

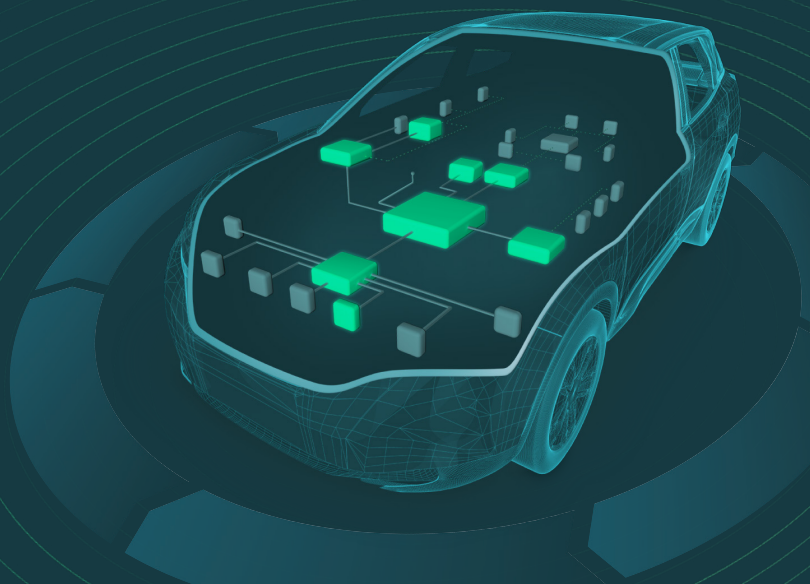
Visibility is key here: providing 360-degree oversight of the operation of security control to OEMs makes relevant information easily accessible and therefore manageable.

For OEMs, this is a main obstacle to overcome. When considering the number of vehicle models and topologies, complex supply chains, increasing connectivity and over the air updates, among other areas of consideration once the vehicle is on the road, visibility provides important means of constant and systematic analysis, allowing for strong security posture.

OWNERSHIP

OF THE CYBERSECURITY LIFECYCLE

Once they gain visibility into their vehicles' cybersecurity lifecycles, OEMs can perform risk assessment and analyze potential threats, **plan their desired security policy and enforce the chosen policy across the board to gain full ownership.**

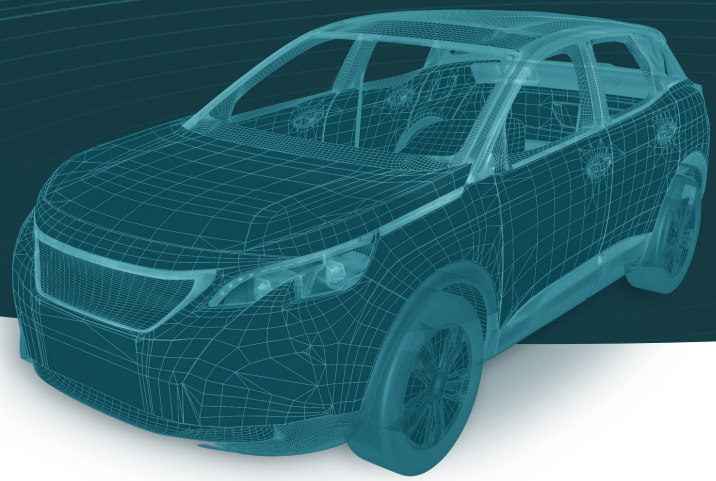


IMAGINE

FEASIBLE CYBERSECURITY MANAGEMENT

Cybersecurity management doesn't have to be difficult.
With the proper tools, risk assessments can take a matter of minutes, potential vulnerabilities can be identified and prioritized with ease, and custom security policies can be enforced across the board without hesitation. Analysis of the most complex multi-network systems doesn't have to be an arduous task; while easy visibility of cybersecurity status can be accessed and deployment of new cyber protection can happen at any place, any time.

With the right technology, **cybersecurity can become predictive rather than reactive,** can enable rapid innovation and, above all, can allow automotive manufacturers to focus on what matters.



AutoSec

A PRACTICAL, TRANSPARENT APPROACH TO LIFECYCLE CYBERSECURITY

AutoSec was designed to achieve C2A's vision of a practical approach for managing security throughout the vehicle lifecycle. AutoSec is the **first comprehensive cybersecurity lifecycle management platform** that empowers OEMs and Tier 1s with the visibility and control required to meet vehicles' lifelong cybersecurity needs.
The unique orchestration layer gives auto manufacturers unparalleled transparency to enable streamlined management of each phase: risk assessment, planning, policy creation and policy enforcement, allowing for true resilience needed to tackle the cybersecurity management challenge.

AWARD WINNING SOLUTION

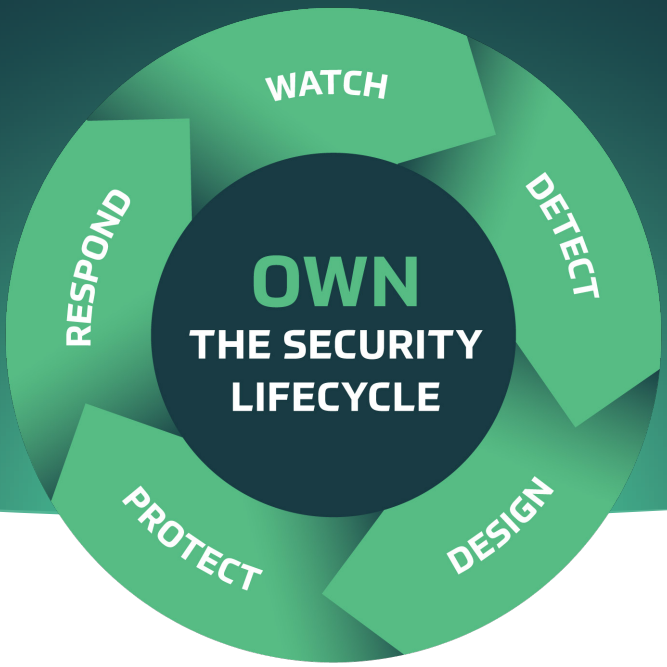
AUTOMOTIVE SECURITY SOLUTION 2021

CYBERSECURITY INDUSTRY SOLUTION 2021

INNOVATION OF THE YEAR 2020

FROM VISIBILITY TO ACTION

AutoSec



WATCH

OBTAIN VISIBILITY OVER CYBERSECURITY STATUS ACROSS ALL VEHICLE MODELS

AutoSec's asset based management approach provides full spectrum visibility into security across all car models using its cutting edge dashboard. It uncovers unique security insights, alerts users in the event of policy noncompliance or identified risk, and helps OEMs monitor the status of enforcement points, staying alert to potential threats, including:

- Automated visual analysis for all assets (Network, MCU and Binary)
- Real-time asset status view
- Cross-check assets: from full vehicle topology to single function level.

DETECT

ACCOUNT FOR ALL IN-VEHICLE COMPONENTS

With AutoSec's surgically accurate visibility, a full-scale analysis of a vehicle's threat model can now be performed, including:

- Risk Audits
- Simulation of in-vehicle component behavior
- Formulate required security features

DESIGN

PRIORITIES NEEDS, YOU CALL THE SHOTS

AutoSec allows you to customize in-vehicle cybersecurity architecture,and hand pick which security policies best suit your needs. With this new ability, OEMs and Tier 1s can deploy security where it is really needed, and configure embedded security products for all types of assets.

PROTECT

CONFRONT ATTACKS WITH THE RIGHT MEASURES

Deploy embedded cybersecurity solutions and appropriate configuration files inside the vehicles on a range of ECUs, including TCU, IVI, ADAS, GW, DC among others, to provide protection for vehicles on the road, preventing cyber-attacks in real time and protecting drivers' and passengers' safety.

RESPOND

KEEP PACE WITH FAST-EMERGING THREATS

Leverage AutoSec's scalable platform to easily maintain strong security posture across different car programs throughout the vehicle lifecycle:

- Perform ongoing risk assessment, quickly identify affected devices
- Maintain and deploy in-vehicle cybersecurity
- Manage all security products in one place

KEY BENEFITS

AutoSec

AutoSec

Full-spectrum visibility of the entire cybersecurity lifecycle

Simplified planning, designing and ongoing management of in-vehicle cybersecurity

Automation of threat identification and prevention

Implementation of security best practices using car-model based policies

Rapid translation of security policies into embedded security solutions

Continuous risk assessment

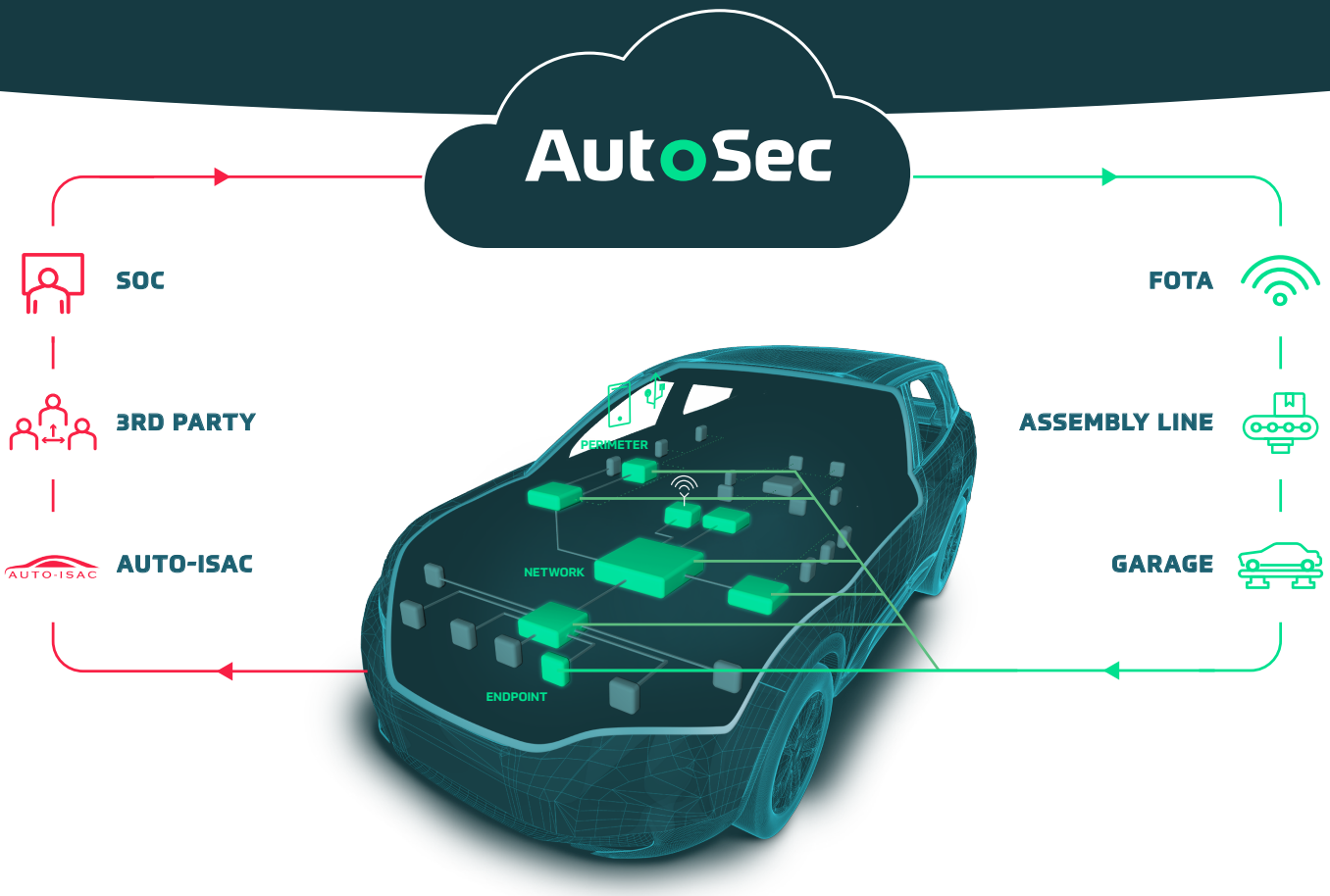
Deploy protection swiftly with an open cybersecurity ecosystem

Protection for today's and tomorrow's connected vehicles

MIND THE GAP

AutoSec

AutoSec creates the requisite linkage between the ever-changing reality of cybersecurity challenges and the ability to deploy protection quickly based on an open ecosystem approach. The platform acts as a liaison between vulnerability, threat information sources (SOC, 3rd party, AutoISAC) and security policy sources (FOTA, assembly line, garage). AutoSec is built to evolve with the needs of the vehicles' defenses, leveraging various data types onboarded into the system to generate insights and security policies and to deploy protections.



AutoSec is available as an on-premises or cloud solution.

AutoSec

Watching Your Vehicles by C2A

ABOUT C2A SECURITY

C2A Security is a trusted end-to-end automotive cybersecurity solutions provider. Its embedded cybersecurity solutions and cybersecurity lifecycle management platform empower the automotive industry with visibility and control over the bespoke solutions needed to protect today's and tomorrow's connected vehicles. Armed with the understanding that cybersecurity is a process, not a product, C2A's holistic approach includes a comprehensive, multi-layered technology suite scalable enough for the entire vehicle lifecycle.

C2A products' minimal footprint and compute resources consumption give them the flexibility to fit into any automotive ECU. With market neutrality, complete fluency in the needs of the automotive industry and ease of integration, C2A is redefining the automotive cybersecurity ecosystem as the sole provider of the most flexible, comprehensive, and transparent cybersecurity solution on the market.

C2A security

To learn more about AutoSec: info@c2a-sec.com www.c2a-sec.com