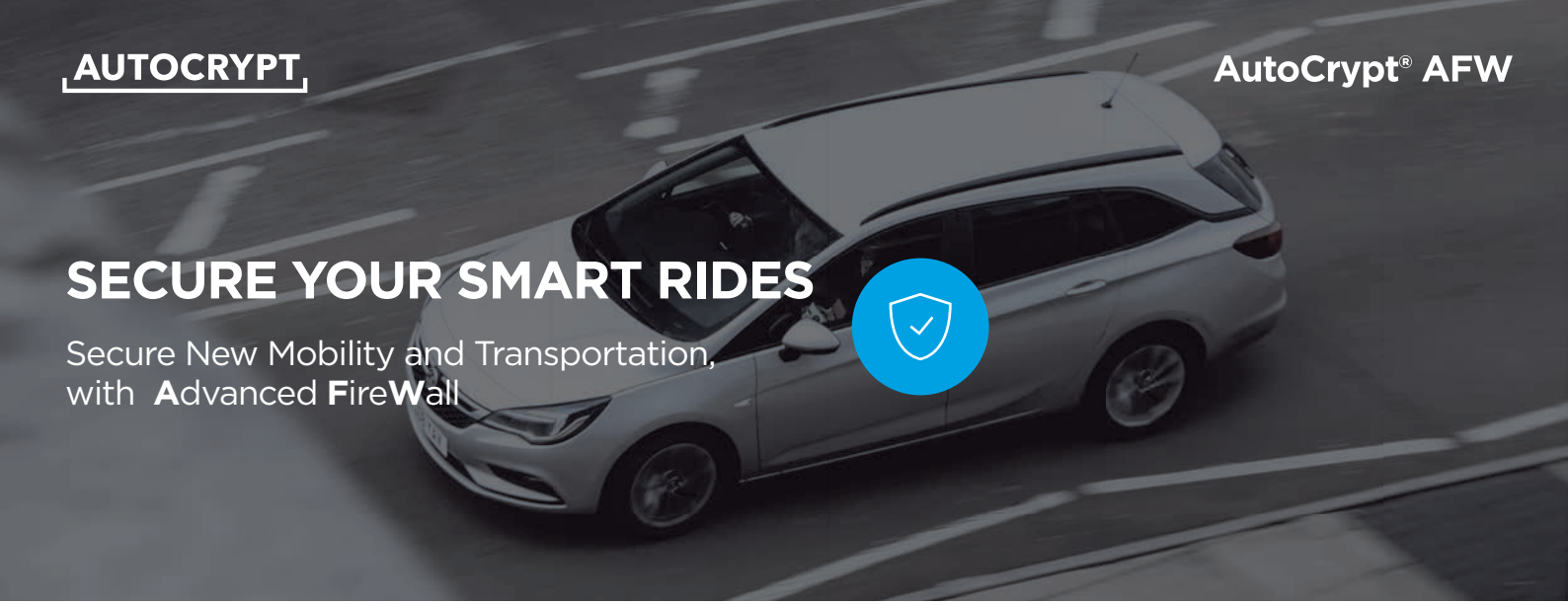
AUTOCRYPT

AutoCrypt® AFW



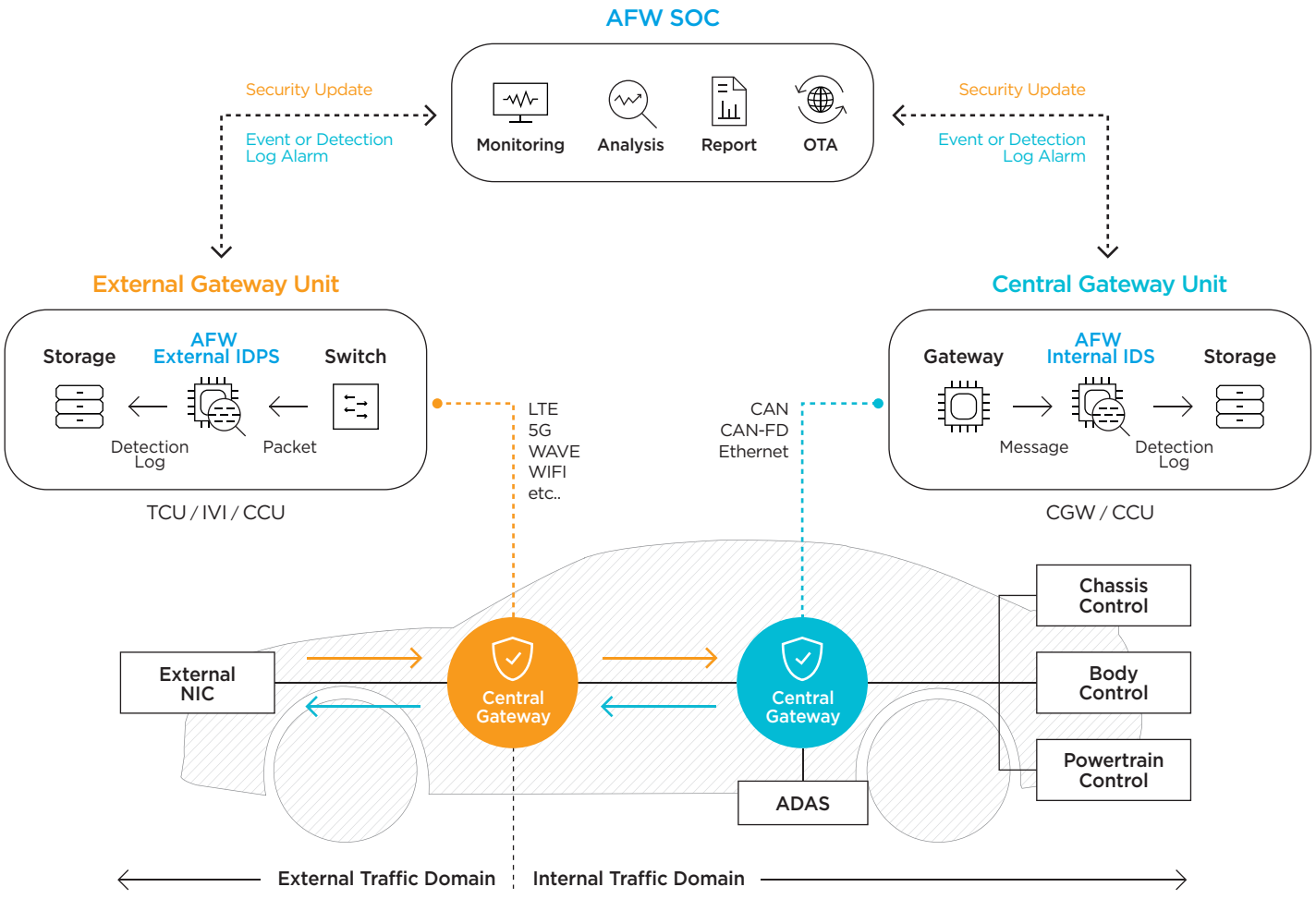
SECURE YOUR SMART RIDES

Secure New Mobility and Transportation,
with **A**dvanced **F**ire**W**all

OVERVIEW

As vehicles become increasingly more intelligent and connected through the advent of self-driving cars, electric vehicles and connected cars, the security threat to vehicles continues to evolve accordingly. All devices and technologies external to the vehicle can be the source of new threats, providing more opportunities for malicious agents.
The AutoCrypt AFW suite protects your vehicle's assets with integrated solutions that detect, manage and respond to cyber attacks from both internal and external security threats.

SYSTEM ARCHITECTURE



- **AFW External IDPS –** Firewall, Intrusion Detection and Blocking Solutions for Traffic Control from Outside the Vehicle
- **AFW Internal IDS –** Anomalous signal and intrusion detection solution for in-vehicle communication such as CAN, CAN-FD and Ethernet
- **AFW SOC –** Integrated control solution for big data analytics and monitoring, alarms and policy updates based on machine learning

FEATURES & BENEFITS

Features

The AutoCrypt AFW suite is optimized for automotive communication protocols to detect and respond to cyber attacks, including attacks from outside the vehicle as well as abnormal communications from inside the vehicle. It also monitors and analyzes cybersecurity threats in conjunction with the AutoCrypt SOC solution to update firmware and security policies online to protect and manage the safety of the vehicle at all levels.

AFW External IDPS

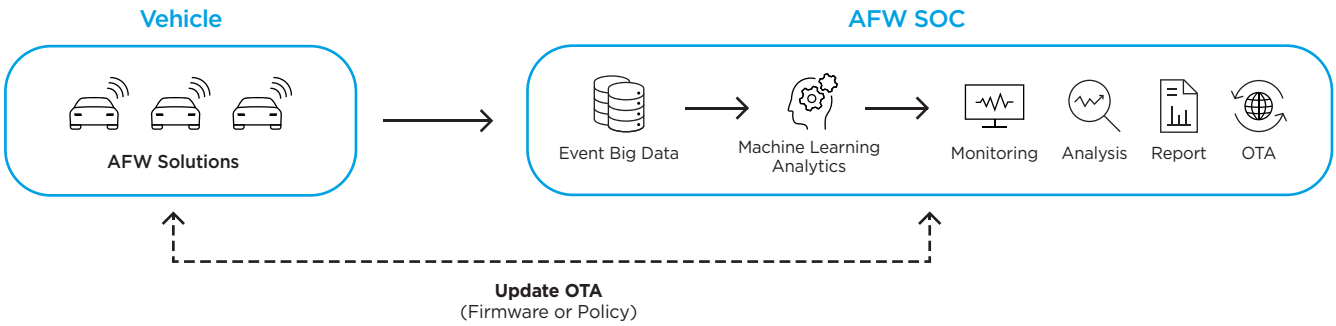
- Applies to TCU, IVI, CCU to defend against attacks via external communications such as LTE, 5G, WAVE, and WIFI
- White list-based access control and TCP level DDoS attack prevention
- Equipped with an intelligent detection engine based on logical analysis of application levels

AFW Internal IDS

- Applicable to systems such as CGW and CCU for detecting anomalies and intrusion of in-vehicle networks such as CAN, CAN-FD, Ethernet (SOME/IP, DoIP)
- Detected for all message information in the specified network domain
- Identification of the identity, length, period, serial number, data change rate, message status continuity and correlation of messages to provide optimized detection for the in-vehicle network

AFW SOC

- Applicable to systems such as CGW and CCU for detecting anomalies and intrusion of in-vehicle networks such as CAN, CAN-FD, Ethernet (SOME/IP, DoIP)
- Detected for all message information in the specified network domain
- Identification of the identity, length, period, serial number, data change rate, message status continuity and correlation of messages to provide optimized detection for the in-vehicle network



Advantages

- Supports a variety of embedded platforms applicable to E/E architecture
- Logical analysis-based detection engine reduces false positive detection rate for trusted identification of attack
- Forensics data for post-analysis
- Compliance with legal regulations and requirements for vehicle security

SYSTEM REQUIREMENTS

AFW External IDPS	• Embedded Linux, Android • CPU: ARM, PowerPC • Memory: 20 MB+ • Storage: 10 MB+
AFW Internal IDS	• AUTOSAR, FreeRTOS • CPU: ARM, PowerPC • Memory: 128 kB+ • Storage: 256 KB+

* Information is for reference purposes and may vary according to system environment and feature requirements.

AUTOCRYPT

Eusu Holdings Bldg., 20th Fl. 25 Gukjegeumyung-ro 2-gil, Yeongdeungpo-gu, Seoul, Korea
Tel. 02-2125-6500 e-mail: sales@autocrypt.io

www.autocrypt.io