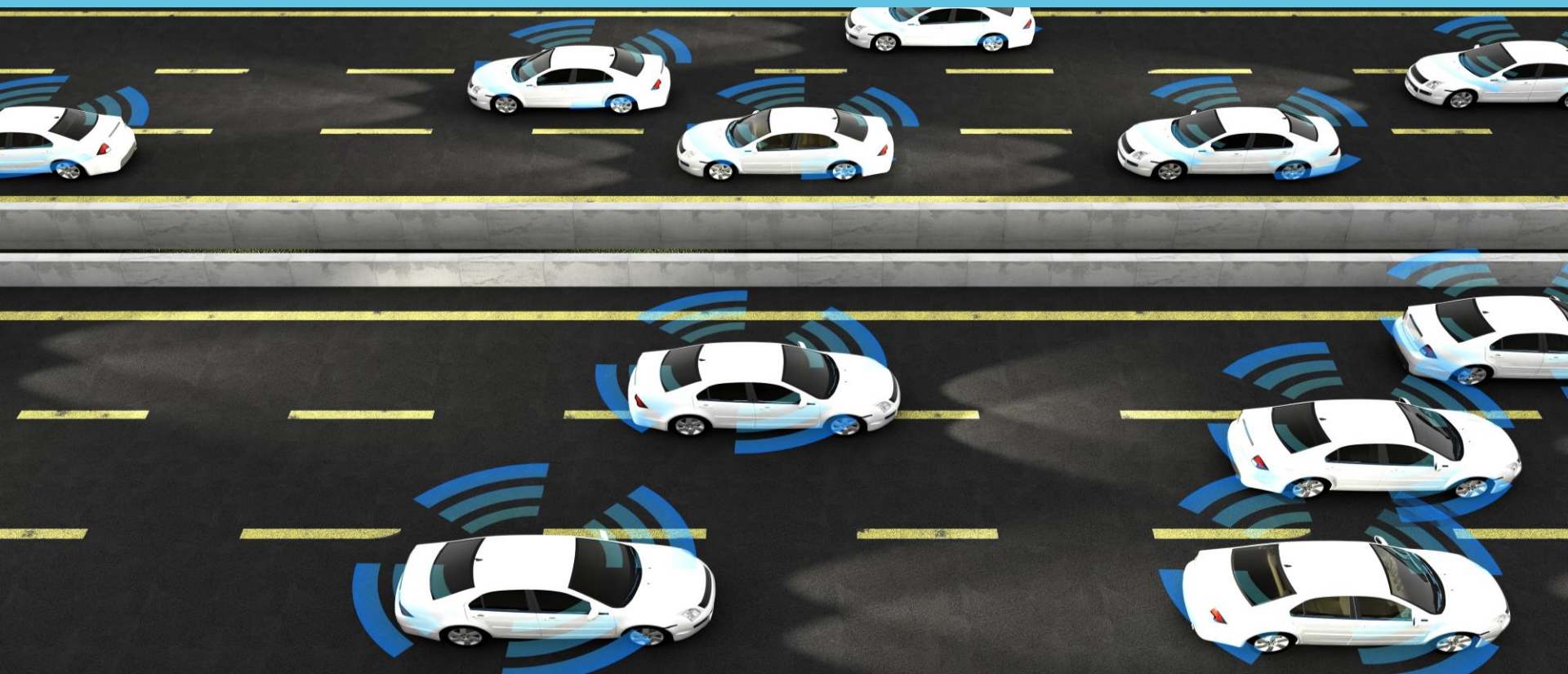


# ***Preventing Cyber Attacks on Aftermarket Connectivity Solutions***

**Zach Blumenstein, BD Director**

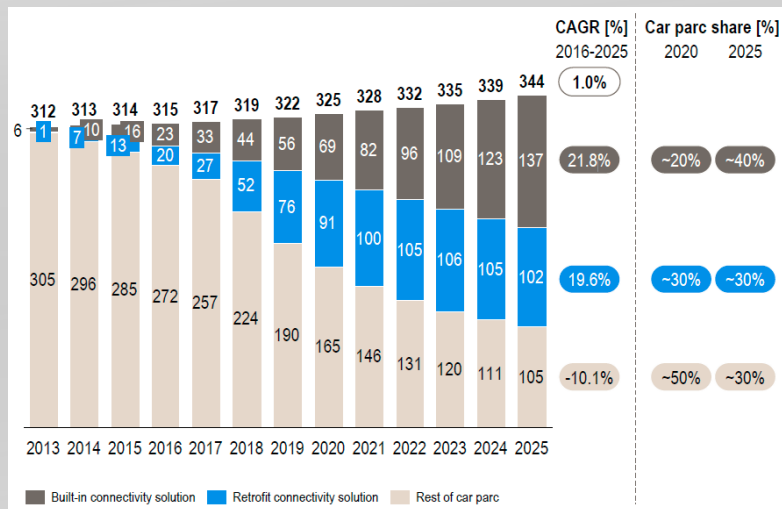
**Argus Cyber Security**

In less than a year, 100s of millions connected cars



# Aftermarket connectivity most prevalent until 2023

- Approx. 100 million connected cars in EU by 2018
- OBD II dongles used by 30% of EU car parc 2020-2025



# The opportunity

- Dongles are an attractive option
- 7 out of 10 consumers would **pay up to 10% of the car price** on services relevant to them
- 35% of consumers already willing to trade driving data for insurance benefits

	App based dongle solution	Proprietary solution
	<b>3</b> 	<b>5</b> 
Cost	10-150 EUR	2,000-3,000 EUR
Business focus	B2C and B2B	B2C and B2B
Level of integration	Fixed installed	Fully integrated (with delivery)
Functionalities	GPS tracking	GPS tracking
	Micro-billing	Micro-billing
	Speed control	Speed control
	Accident recognition	Accident recognition
	Braking behavior	Braking behavior
	Diagnosis/vehicle data	Diagnosis/vehicle data
		Entertainment
		Individual services
User examples		

# The challenge

***“...‘smart dongles’ provide an attacker with the capacity of easily performing a remote attack with...high impact.”***

➤ December 2017 – ENISA, Cyber Security and Resilience of Smart Cars

***“...the OBD-II port as it currently exists creates a growing risk to the safety and security of passengers.”***

➤ September 2016 – open letter from 4 US Congressman to NHTSA Administrator

## The challenge cont'd

***“...Aftermarket devices could be brought on to all ages and types of vehicles with varying levels of cybersecurity protections. Therefore, these devices should include strong cybersecurity protections since they could impact the safety of vehicles.”***

↘ October 2016 – NHTSA, Cybersecurity best practices for modern vehicles



60  
MINUTES

# Why hack a vehicle?



Cyber Ransom



Car Theft



Targeted Attacks



Hacktivism

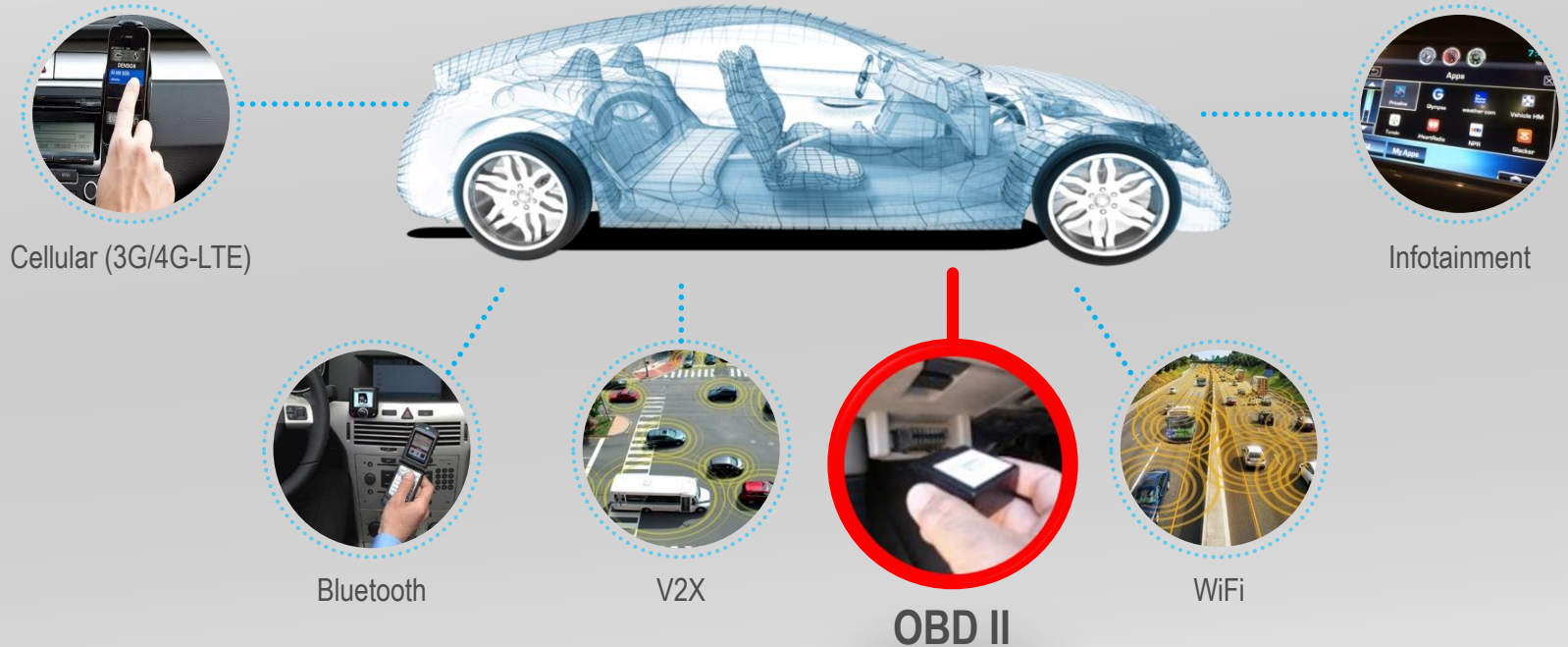


Data Theft / Privacy invasion



Mass Events

# ODB II dongles increase the attack surface



# Dongles have already been hacked

## Security challenges with telematics dongles

- Enlarge the attack surface
- Built on old hardware with weak security
- OBD II port is directly connected to safety critical functions
- No cyber security regulatory environment

**HACKERS CUT A CORVETTE'S  
BRAKES VIA A COMMON CAR  
GADGET**



**“...anything connected to...the Internet [enlarges the] attack surface...especially when it is plugged into the diagnostic port...”**

**-Chris Valasek**

# Argus exposes aftermarket device vulnerability



- Zubie aftermarket telematics dongle
- Communication based on non-secure HTTP protocol
- Provided direct access to the safety critical systems
- Braking, steering and acceleration could have been affected

# Progressive – two million cars open for exploit



- Progressive's UBI Snapshot device hacked
- No responsible disclosure, could affect on ~2 million cars
- Unlock the doors, start the engine, gather engine information

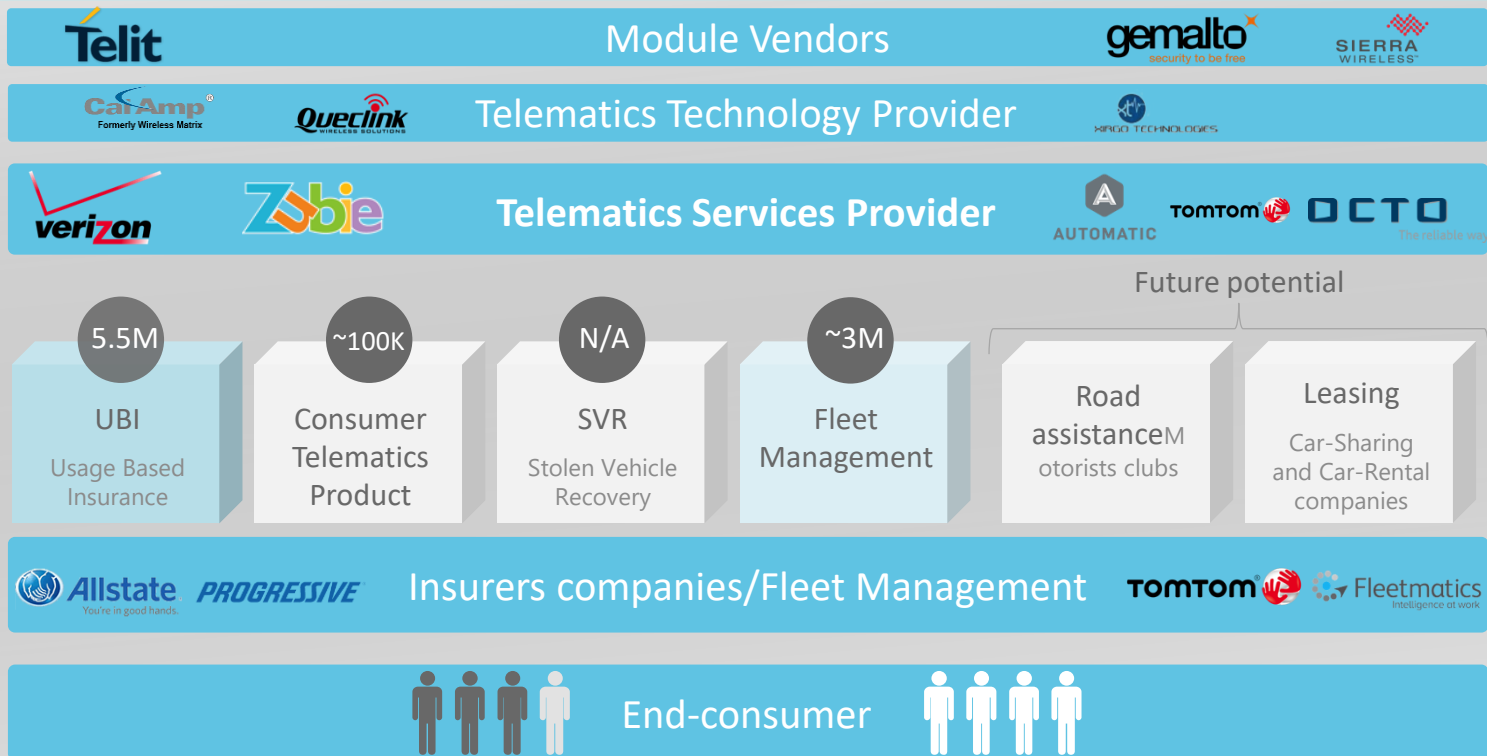
# UCSD researchers expose flaw

## HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET

- Mobile Devices OBD2 dongle
- Through malicious SMS messages researchers gained remote access
- Activating and disabling the brakes, turning on windshield wipers



## Aftermarket Food Chain



# 52% People Would Pay \$8/Month for Cyber Security



# Argus' Mission

- ✓ Keep Passengers Safe
- ✓ Protect Customer Privacy and Property
- ✓ Prevent Costly Cyber Recalls
- ✓ Maintain Business Continuity



# Argus Cyber Security Philosophy



## **Prevent**

Make it as hard as possible to attack



## **Understand**

Know you are being hacked and how, in real time



## **Respond**

Mitigate the damage and immunize the fleet in hours

# Maximum Prevention – Security in Depth



Prevent

**25** Granted and Pending Automotive Cyber Security Patents

## In-Vehicle



ECU  
Protection



In-Vehicle  
Network  
Protection



Aftermarket  
Protection

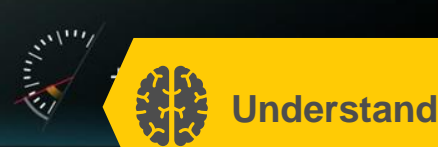


Connectivity  
Protection

## Out-of-Vehicle



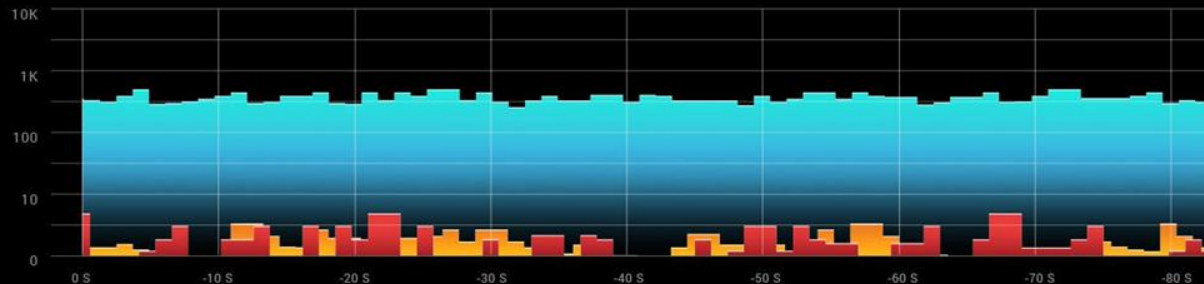
Lifespan  
Protection



## IN-VEHICLE TRAFFIC

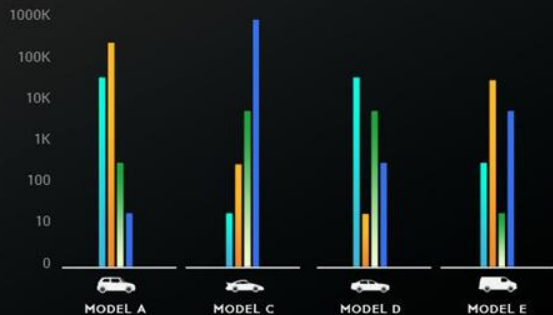
Allowed Anomalous Blocked

FLEET



## ATTACKS PER MODEL

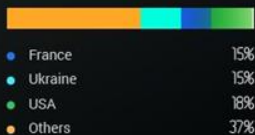
2015/09 2015/10 2015/12 2015/12



## CHECK POINT CAPSULE SECURITY INCIDENTS

SEVERITY	SOURCE	DESTINATION	MALWARE ACTIVITY
High	Argus Demo	192.117.2.58	Communicate with C&C
Low	Magna car	192.79.2.126	Access to malicious site
Low	Magna C	192.5.46.181	Communicate with C&C

### ATTACK ORIGINS

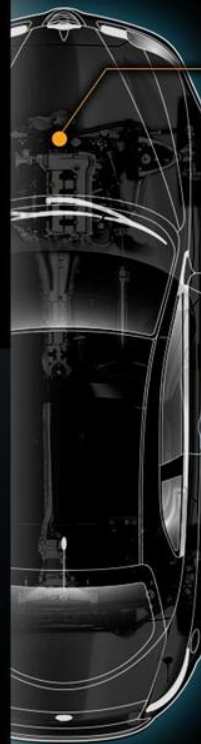


### ATTACKS TREND



## ATTACKED COMPONENTS

FLEET

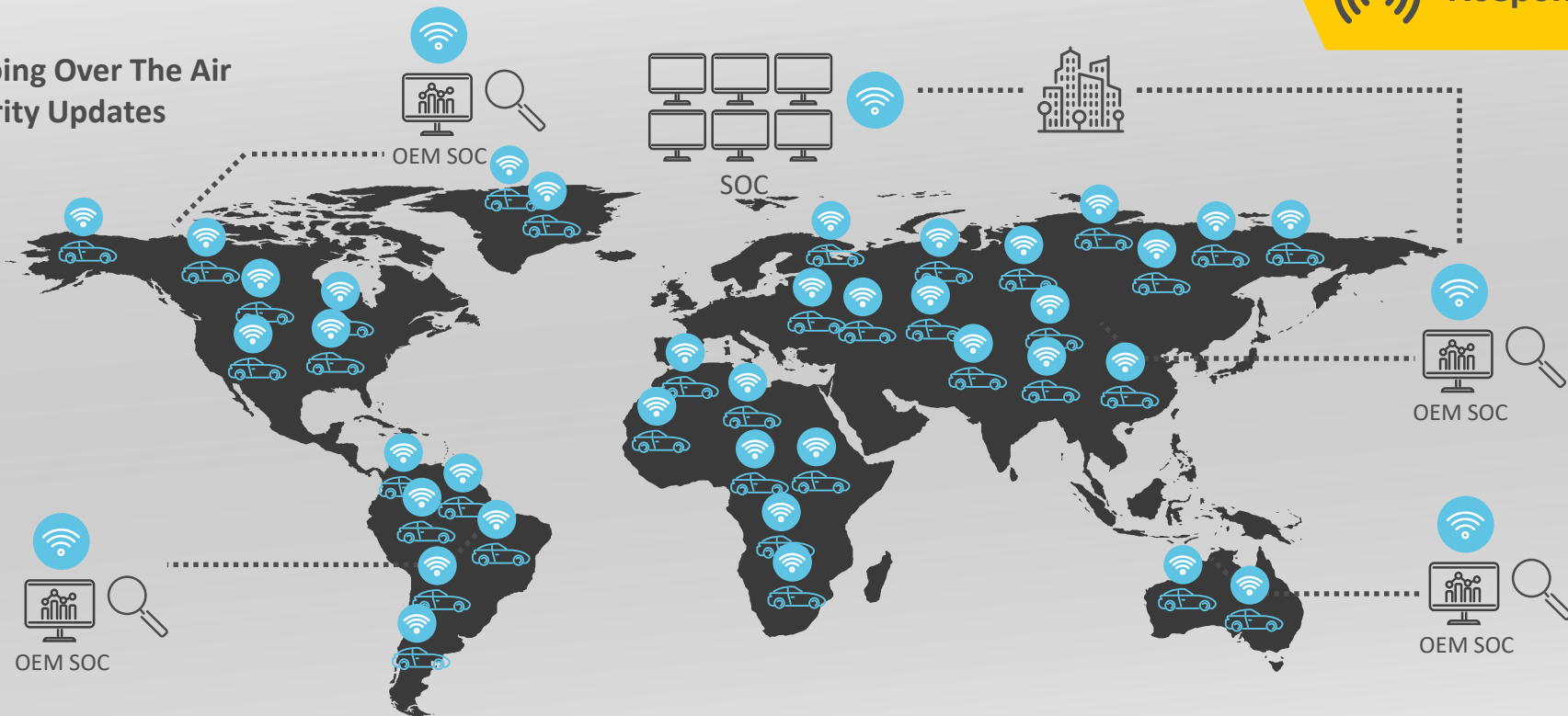


BRAKES	12
TEMP GAUGE	495
SPEED METER	1024
WINDOW	11
FUEL GAUGE	58
DOOR LOCK	4
TURN SIGNALS	78
A/C VENT	18

# Ongoing Monitoring & Mitigation

 Respond

Ongoing Over The Air  
security Updates



# Our Competitive Advantages

- ✓ Unique combination of cyber security & automotive experts
  - ✓ Industry's best team (founders, leadership, employees, investors, advisors)
- ✓ Widest array of solutions in the market
- ✓ Technologically superior, significant IP (25 pending / granted patents)
- ✓ Significant projects with OEM and Tier 1s
- ✓ Very strong partners
- ✓ Recognized as the market leader



# Drive Home Cyber Safe!

