escar USA
Ypsilanti, MI

SBD Automotive
Ann Arbor, MI, USA

Securing the Software-Defined Vehicle

Challenges and recommendations

June 17, 2022

SBD Automotive - Mission

Delivering **confidence** through **clarity, insight** and **vision**

Our Areas of Expertise

Connected

Autonomous

Shared

Electric

Secure

Why are we talking about the software-defined car?

- It's **not** just a buzzword – **everything is changing**
- Following the previous examples of software-defined X
- But safety presents new challenges
- New stakeholders, new processes, new suppliers, new software = cybersecurity risk

Defining the software-defined vehicle

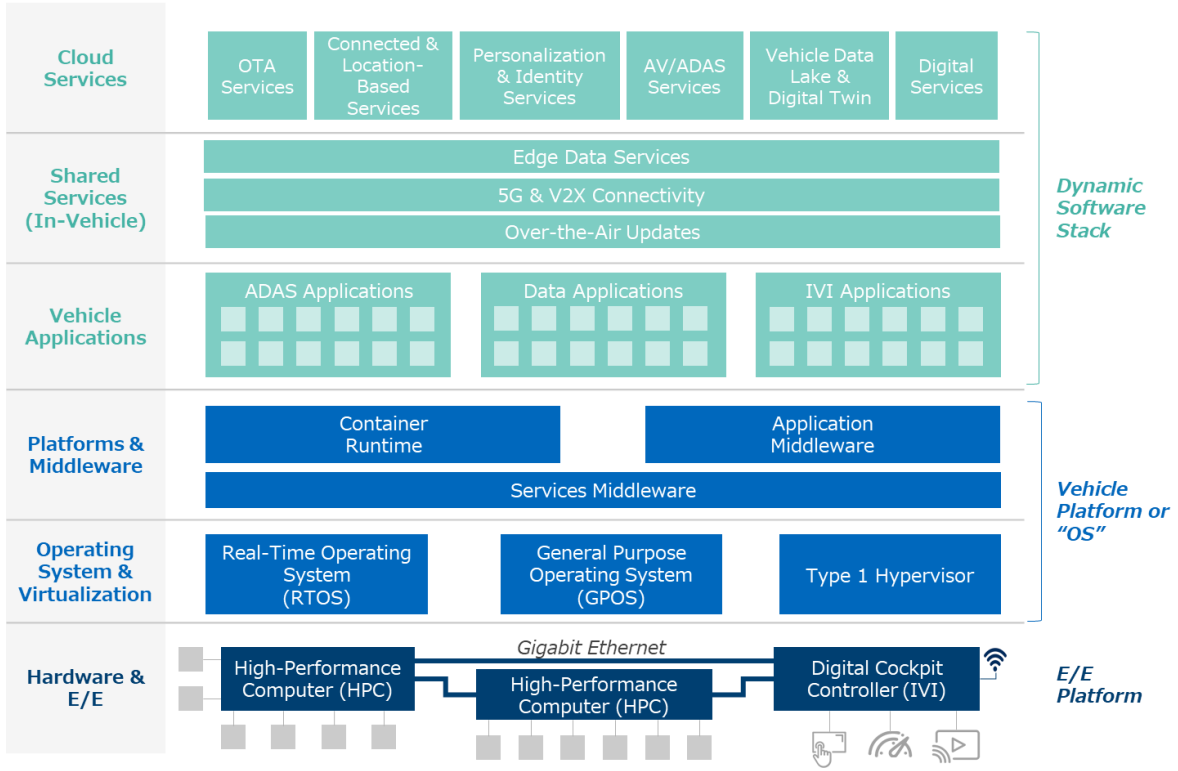
1. SDVs allow software to be **designed, developed and tested in a fully virtualized environment**, leveraging the scale of cloud services to simulate vehicle software

2. SDVs require **multiple layers of hardware and software across different domains** in order to implement this separation

3. SDVs allow OEMs to **dynamically implement new business models & customer experiences** much faster than before

4. SDVs create **significant disruption** in the traditional automotive electronics supply chain while creating **new "blue oceans"**

5. Much of the core SDV software stack is non-differentiating, making **standards & open-source software** attractive to OEMs



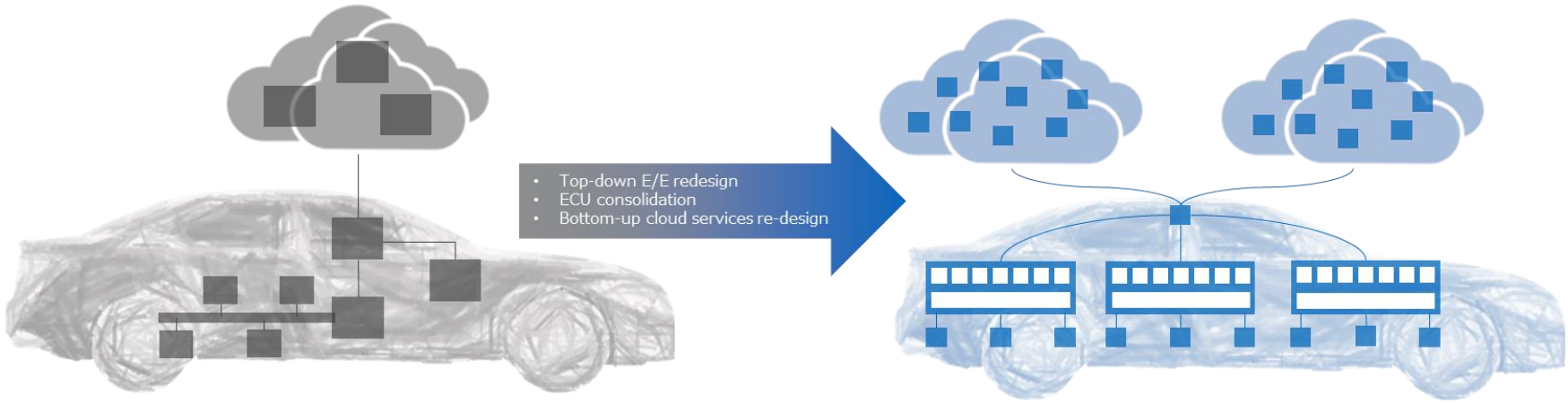
Source: SBD Automotive // The Software-Defined Vehicle (2021)

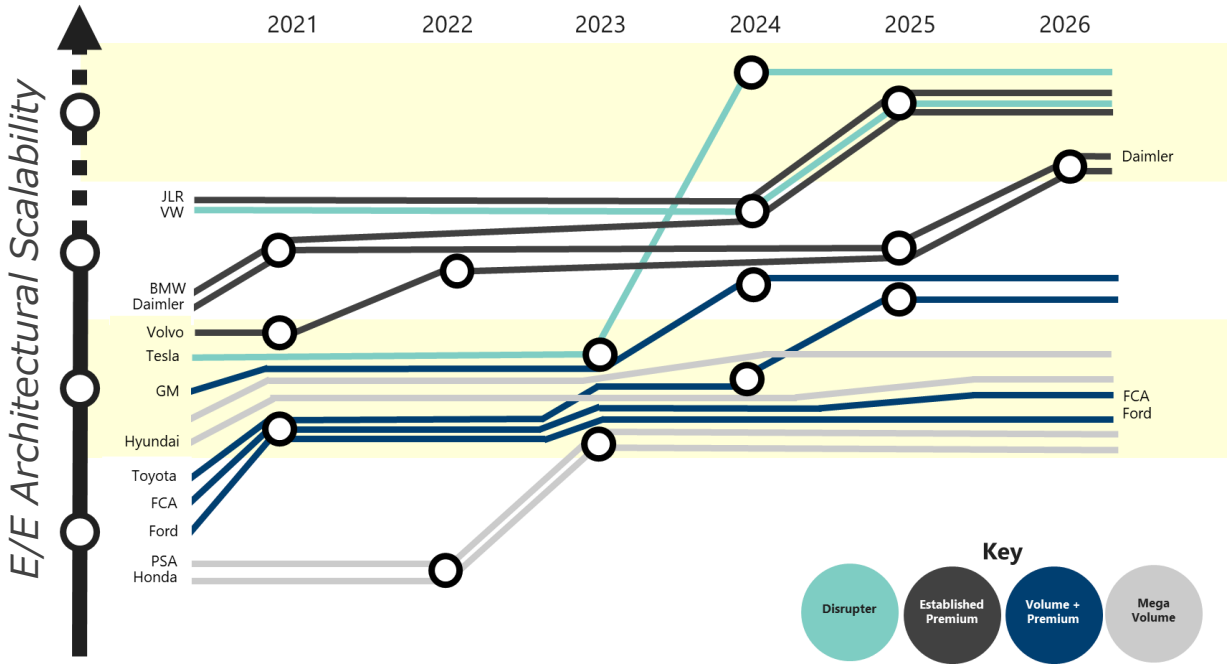
OEMs are just starting development of SDVs

Step 1:

Building the in-vehicle infrastructure ▶

▼





Source: SBD Automotive // Report 630 – E/E Architectures

Step 2: Maturation

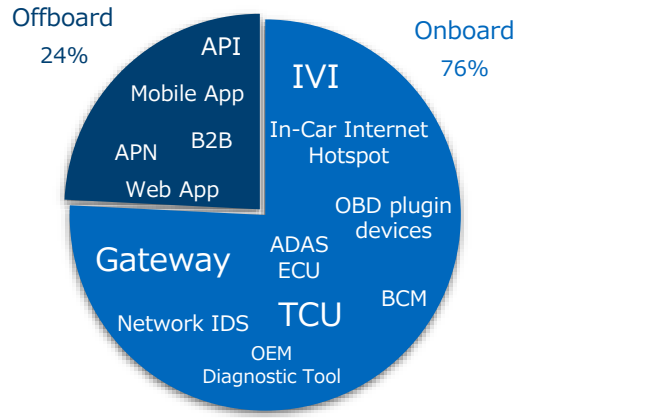
Maturity Challenges

- Organizational
- Process/lifecycle
- Talent
- Supplier
- Toolchain
- Consumer market

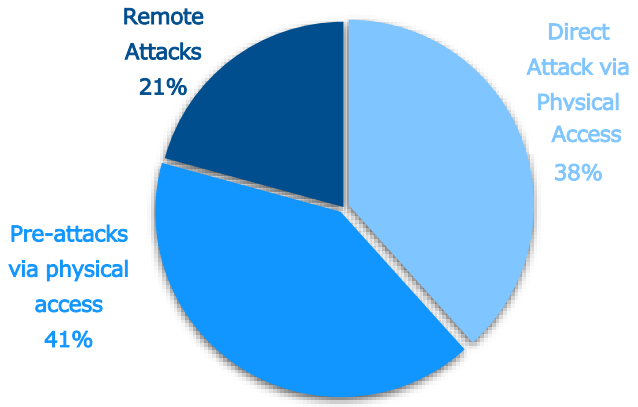
Architecture

We have uncovered significant vulnerabilities during recent pen tests

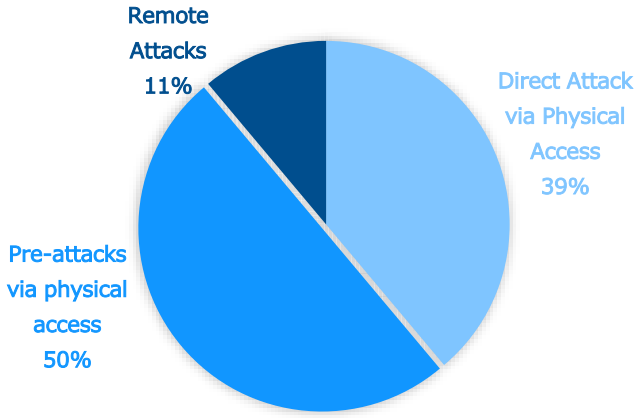
Pen Tests by SBD (last 3 years)



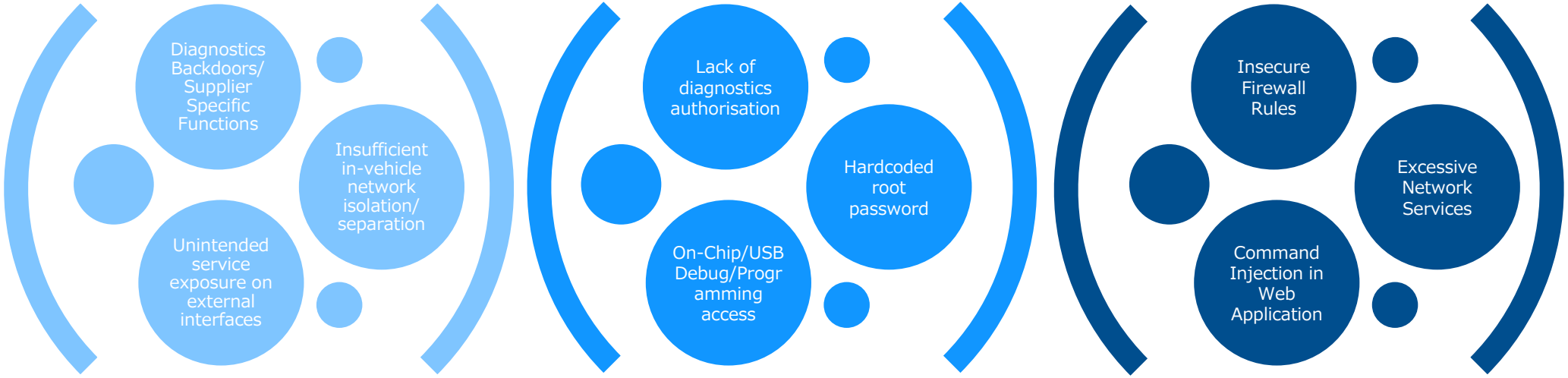
Vulnerability vs Attack Vector



High Severity Vulnerabilities vs Attack Vector



Top 3 High Severity Vulnerabilities

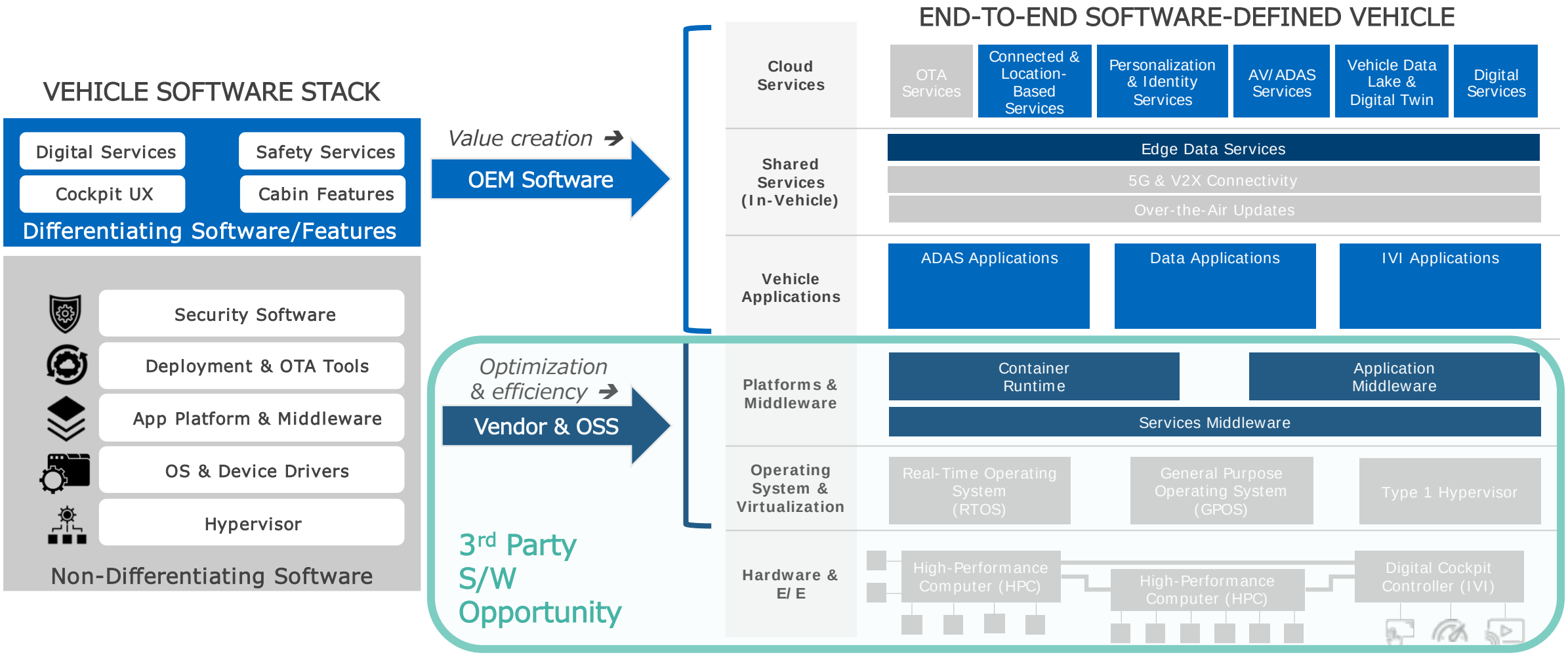


Direct Attack via Physical Access

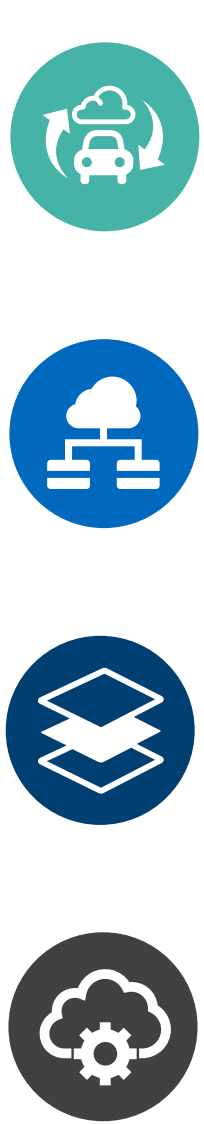
Pre-Attacks via Physical Access

Remote Attacks

New cloud-integrated s/w architecture = bigger attack surface



Key characteristics of SDV computing environments



Homogenous computing environments
between cloud and car

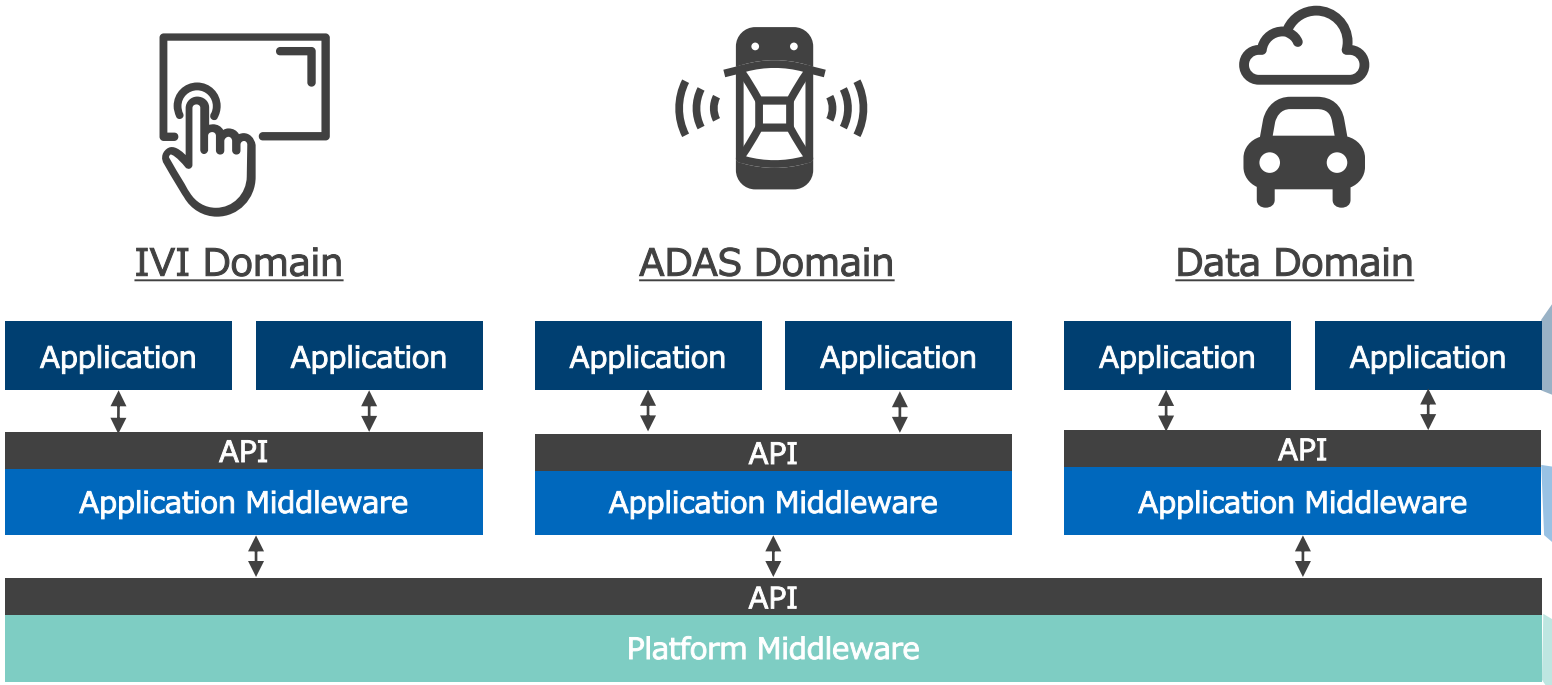
Cross-domain in-vehicle middleware
for distributed computing

Domain-specific runtime environments for specialized use cases

Cloud-integrated toolsets
for data processing, training, and reporting

- ✓ Simulation
- ✓ Portability
- ✓ Scalability
- ✓ Integration
- ✓ Efficiency

Middleware implements APIs as in-vehicle SOA enabler



- Vehicle data, functions for infotainment applications
- Access to infotainment domain functionality (i.e. HVAC)
- Access to vehicle data (i.e. for ADAS visualizations)

- Sensor data, cloud-integrated functions for autonomy applications
- Access to real-time and processed sensor data
- Access to vehicle control functions

- Access to all types of data generated by vehicle for data processing applications
- Integrated with cloud for simulation, diagnostics
- Anomaly, intrusion detection

Applications represents stand-alone software components developed, tested, and deployed as a single package

- ➢ Use APIs
- ➢ Expose services

Application middleware provides domain or use case-specific services as well as service discovery/APIs across applications

- ➢ Example: Adaptive AUTOSAR

Platform middleware provides infrastructure for communication between different physical components & software domains

- ➢ Example: Data Distribution Service, SOME/IP

3 key themes & their implications

1. Cloud-native computing principles are being applied to platforms in the vehicle

> Leverage abstraction, identity to establish defense in depth

2. Vehicles represent both a node and a hub in the edge computing environment

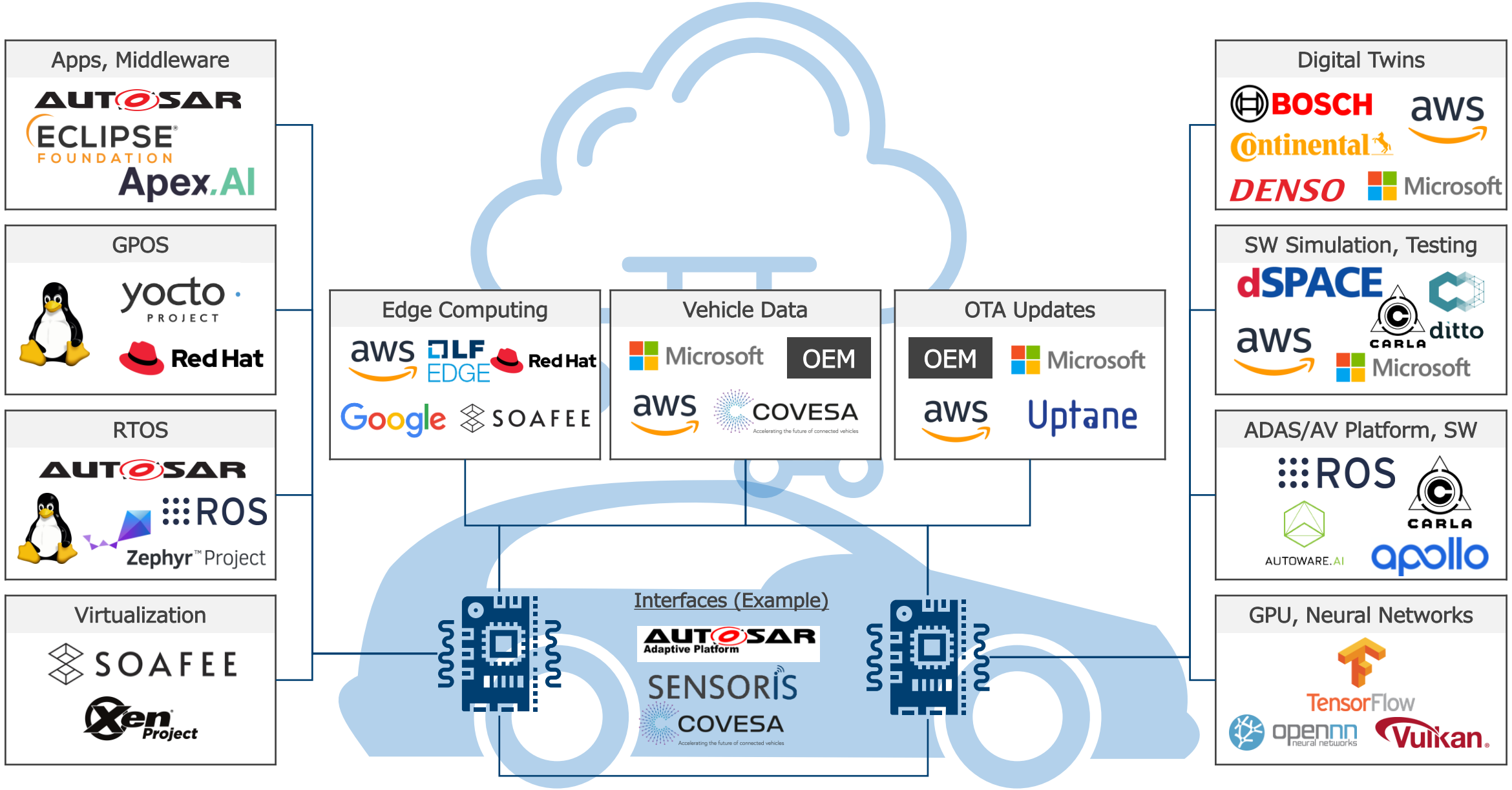
> The vehicle itself must be capable of sanitizing and protecting PII

3. Vehicle software systems can be fully simulated with a virtual workbench

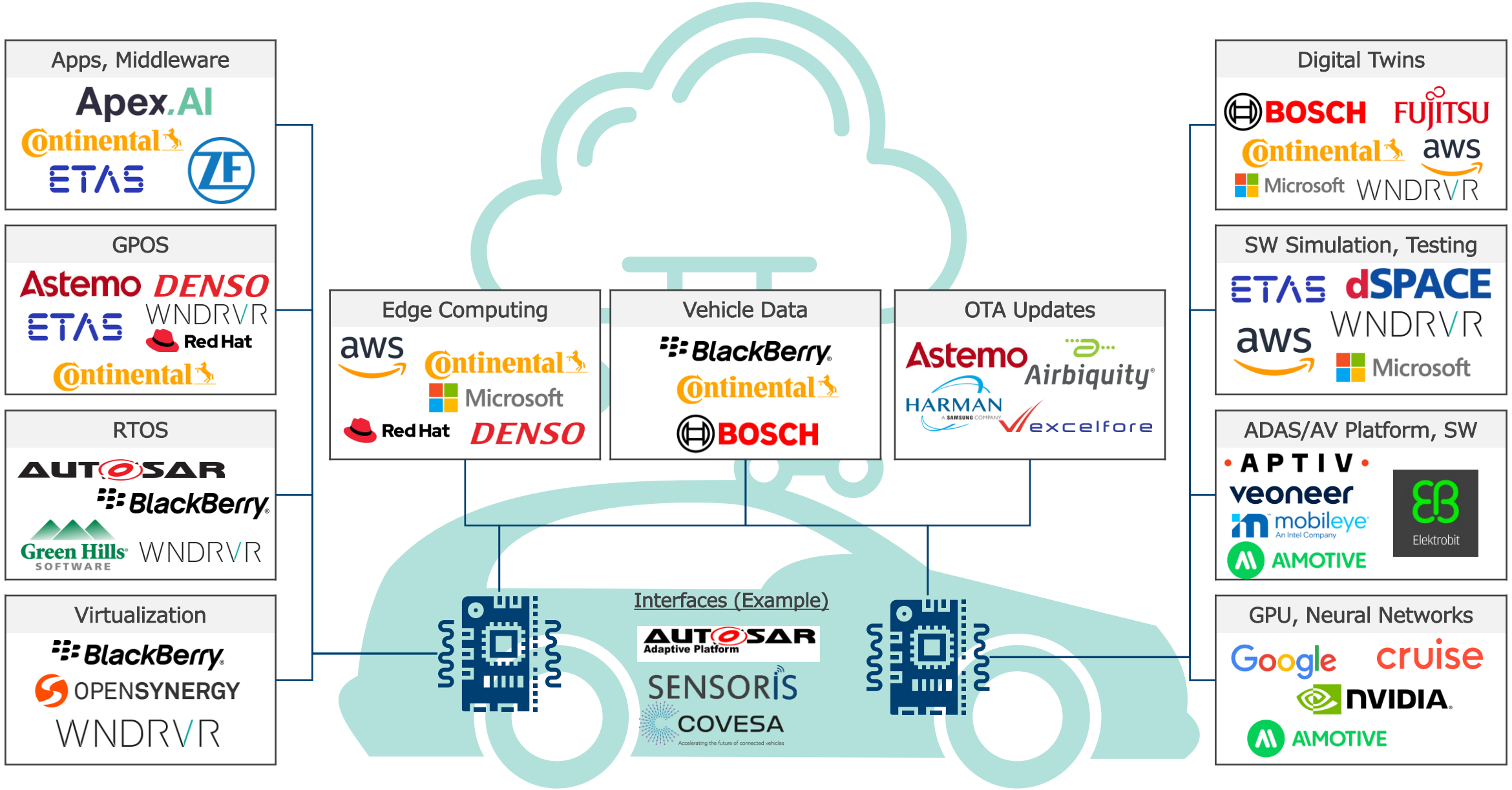
> Cybersecurity testing and incident response can be greatly accelerated leveraging scalable, automated simulation tools

Tools

OSS enablers & standards in the software-defined vehicle



Vendors in the software-defined vehicle



Organizations

Supporting SDVs requires a mature cybersecurity organization

Product cybersecurity division

Design

- Threat modelling & risk analysis
- Security requirements
- Design reviews & audits
- Internal standards
- DevSecOps
- Liaison with factory & service teams
- Legislation compliance (UNECE etc.)

Connected ECUs

Non-connected ECUs

Cloud, APIs & mobile apps

Test

- Coordination of 3rd party pen tests
- Fuzz testing
- Validation testing
- In-house SW testing
- Bug bounty management

R&D

- Next gen EE architecture study
- PoC studies with suppliers
- Advanced tech. research projects
- University projects
- Collaborative industry projects

Operations

- Digital key management (PKI, HSM etc)
- Identity & authentication management
- Code signing
- Cryptography

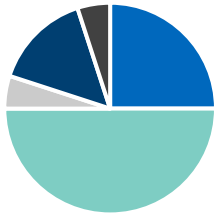
Risk management

- Threat intelligence & sharing
- Security Operations Center
- Incident response planning

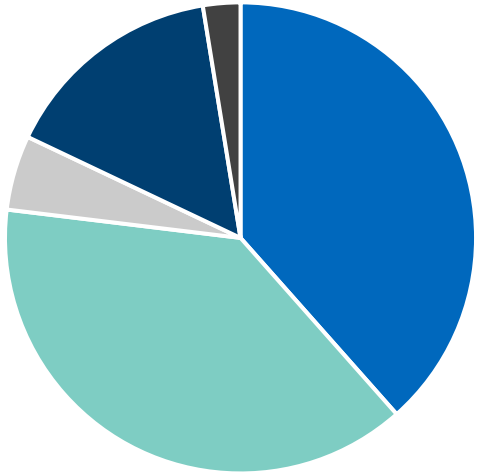
Cyber teams are growing and ‘shifting left’ over time

Estimated proportion of OEM cyber team involved in each work area

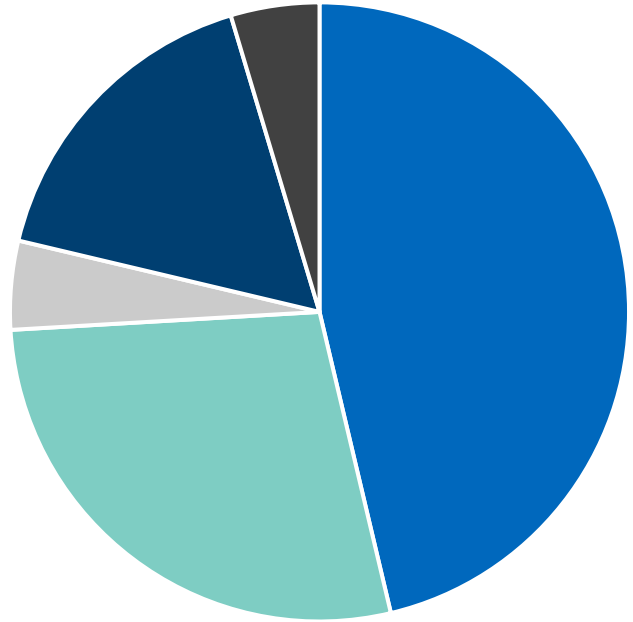
(The size of the pie chart illustrates the relative size of the cyber team each year.)



Typical OEM 2016
(Total staff = 20)



Typical OEM 2021
(Total staff = 80)



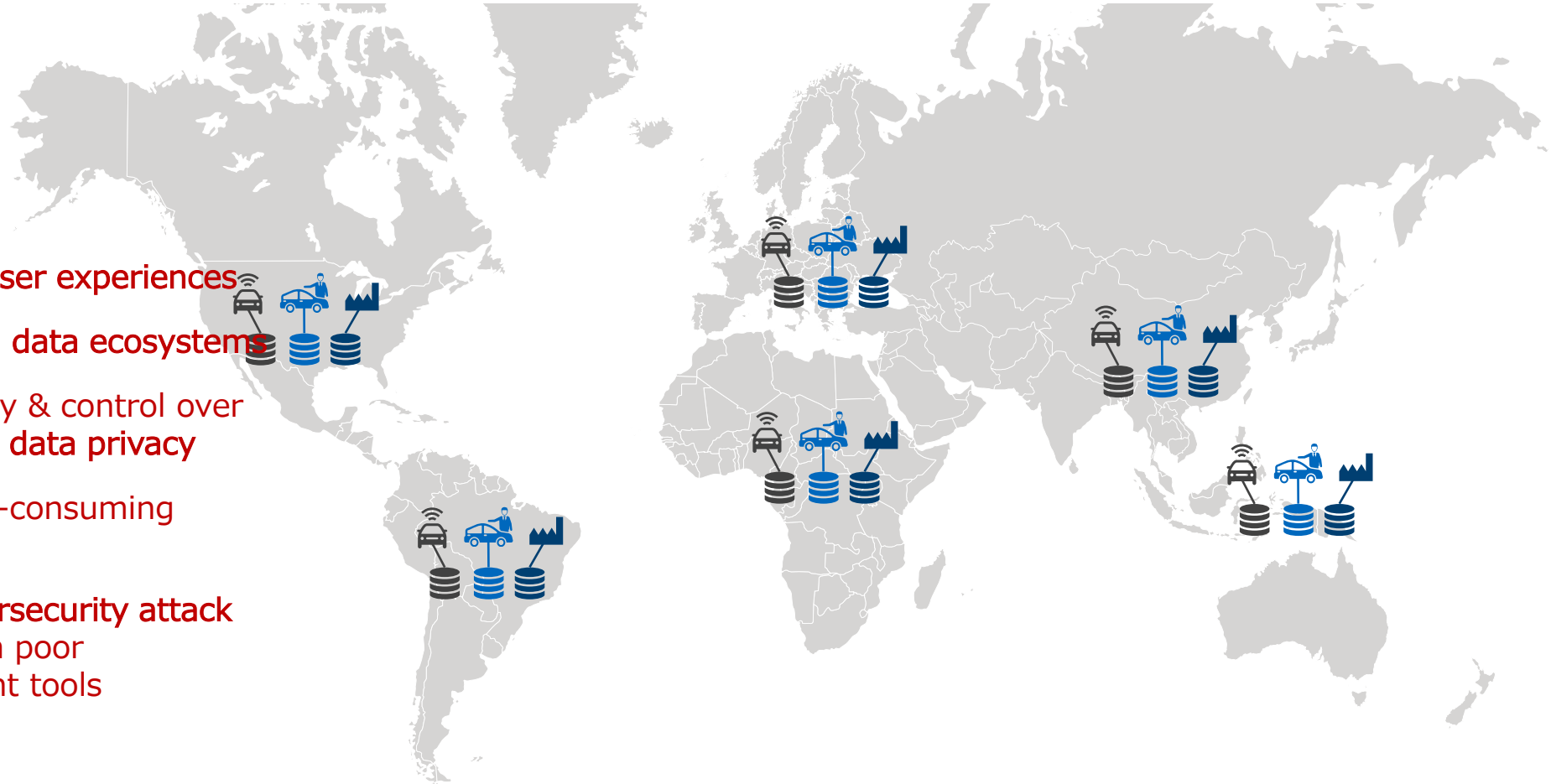
Typical OEM 2026
(Total staff = 120)

Design Test R&D Operations Risk management

Globalization

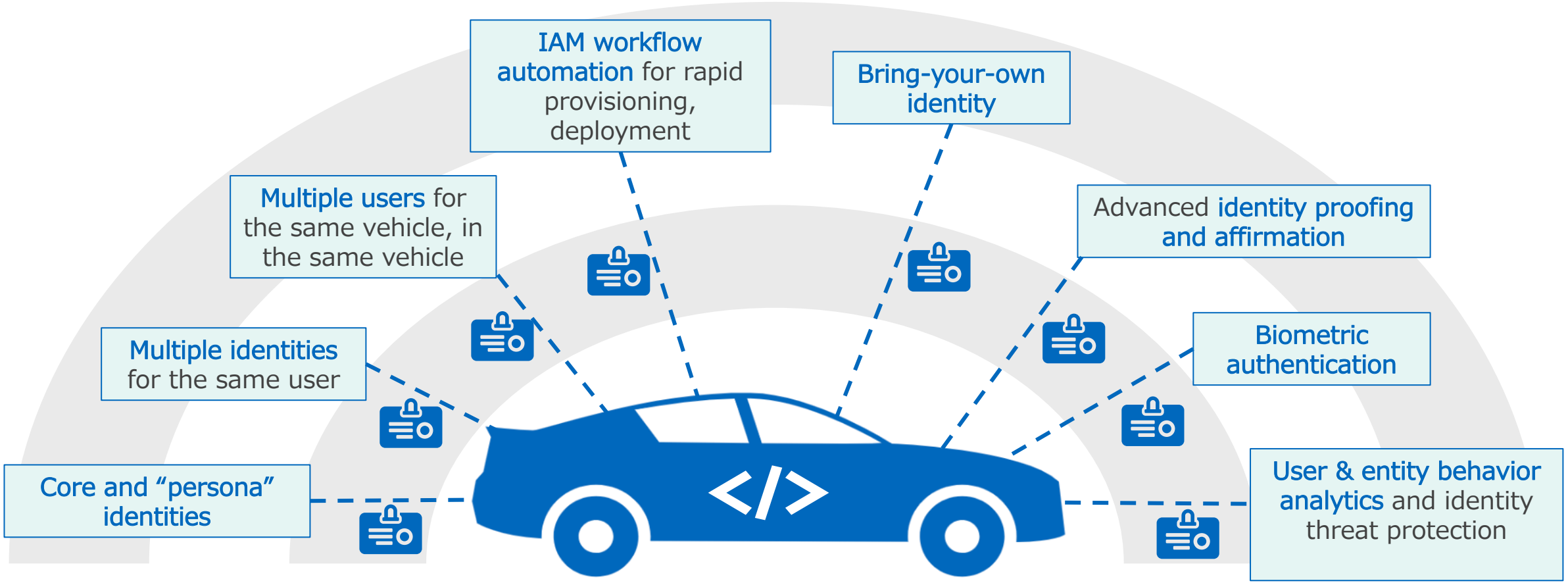
Most OEMs have had regionally fragmented tech ecosystems

- ! **Disjointed user experiences**
- ! **Fragmented data ecosystems**
- ! Poor visibility & control over **user-centric data privacy**
- ! Costly, time-consuming **audits**
- ! **Bigger cybersecurity attack surface** with poor management tools



Identity & access management underpins SDVs

- The emergence of the software-defined vehicle megatrend creates **massive demand for identity & access management services within and connected to the vehicle itself**.
- **One identity can be used for many vehicle services with a wide range of access security requirements**. To ensure appropriate cybersecurity measures for each service requires an IAM strategy that can efficiently handle a many-to-many interface of identities to electronic entities and services within a single vehicle journey.



Takeaways

Our three main takeaways for those supporting SDV security:

1. Emerging software and tools supporting software-defined vehicles enlarge the vehicle attack surface by enhancing offboard integration

2. These same tools enable modern cybersecurity countermeasures in & outside of the vehicle, empowering OEM cybersecurity organizations to act more quickly and efficiently

3. Key strategic and tactical design decisions are being made **now**, requiring urgent action by cybersecurity teams to add organizational and technical requirements

Thank you!

SBD Automotive
Global leaders in automotive technology research, consulting, and cybersecurity

Connectivity

Autonomy

Shared Mobility

Electrification

Security

Alex Oyler
Director, North America

alexoyler@sbdautomotive.com

SBD Automotive
Ann Arbor, MI, USA