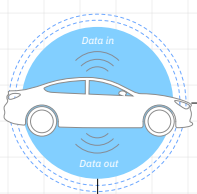
Data Story

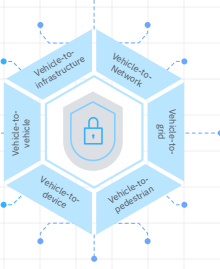
Securing connected vehicles

Designing the future of mobility



The era of the software-defined vehicle is here. With 367 million connected vehicles projected to be on the road by 2027, the volume of vehicle endpoints will expand significantly. This exposes hundreds of millions of new attack surfaces—inside and outside vehicles—to cyber threats. The increasing use of generative AI further complicates the threat landscape.

Advanced mobile technologies, such as autonomous vehicles and electric vertical takeoff and landing vehicles, will add further complexity to connectivity. However, when addressing connected vehicle security and privacy, most OEMs and auto suppliers focus on research standards and regulations, while not planning adequately to secure future systems against cyberattacks.



Auto industry executives recognize that connected vehicle security enhances product and brand value.[1]

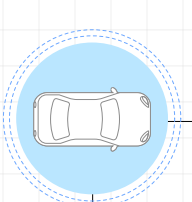
72%

agree that security is a revenue enabler rather than a cost center.

86%

agree that security, assurance, and trust are brand attributes that differentiate their organizations.

Consumers will choose brands with superior security and privacy

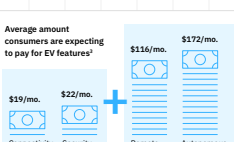


As the connected vehicle industry prioritizes cybersecurity to help ensure the security and privacy of drivers, passengers, and other road users, it is also clear that this is a top brand differentiator for consumers. In fact, 53% of consumers would request a specific brand if that brand offers superior security and privacy with shared mobility and autonomous driving.[2]

Security and connectivity are the keys to unlocking higher value

For future mobility solutions, data security and privacy are the leading criteria for consumers prioritizing one automotive brand over another. Core services like security and connectivity are essential for realizing revenue from higher-value adding services like autonomy and remote diagnostics.

Average amount consumers are expecting to pay for EV features[3]



Foundational features

Higher-value features

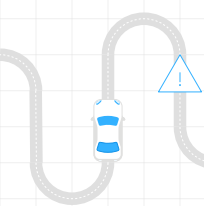
Actions to accelerate

1. Embed security and privacy throughout the product lifecycle. Elevate security by emphasizing that security is everyone's responsibility—stakeholders, partners, and even customers.

2. Adapt a bi-modal mindset. While focusing on addressing current regulatory requirements, prepare a broader, security-by-design strategy to protect future mobility solutions.

3. Secure all physical and digital supply chains. Plan for the connected, autonomous, shared, electric (CASE) ecosystem. Use common standards, tools, and partner expertise to drive efficiencies.

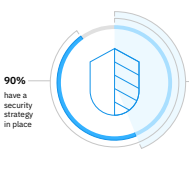
Automotive CEOs see security and privacy as top challenges



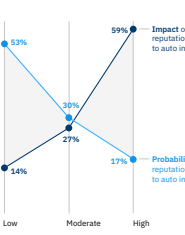
After sustainability, automotive CEOs see security and privacy as their top challenges. As data breaches become more consequential, leaders recognize that vehicle cybersecurity and privacy impact revenue-generating operations and brand reputations. The complexity of edge connectivity, over-the-air software updates, and telco connectivity coverage requires committed leadership, collaborative teamwork, and design thinking to address divergent stakeholder needs.

A wide gap exists between ambition and action

Most automotive organizations have a security strategy, but less than half have started executing on that strategy.[4]



Too often, security and privacy are afterthoughts and are not integrated into product development and production from the start. Barriers include a lack of tools, resources, expertise, and organizational alignment. For example, 63% of auto executives point to lack of resources, 56% indicate lack of common tools, 51% see lack of integration between business units, and 47% view lack of common governance as obstacles.[5]



Roadblock ahead?

The vehicle attack surface is expanding rapidly due to more connectivity features on more connected vehicles. When considering cybersecurity risks, auto executives understand the impact of reputational damage is high, but they may be underestimating the likelihood of future mobility threats. To mitigate risks, connected vehicle security features should be embedded by design and enabled by default.[4]

Actions to take now

1. Build core platforms and services like a hyperscaler. Quantify risks to understand the technical constraints of operating vehicle software, edge, and cloud at scale. Use data insights to design a robust infrastructure that fuses data, network, and end users without compromising security, performance or reliability.

2. Tap the potential of generative AI and automation to improve security and privacy operations. Harness the collective brainpower of ecosystem stakeholders and make sure they are equally invested and incentivized to make the whole ecosystem resilient.

3. Address the future when making your business case. Anticipate the vulnerabilities of connected, software-centric vehicles. Consider how security and privacy will differentiate your brands and incorporate this value in your base case.

Interested in more insights and discussion on this topic?

Check out:

Helping to secure privacy for data generated by electric cars

Accelerating security

Subscribe now to receive research driven insights to help you make smarter business decisions.

To learn more about AI and automation for cybersecurity, check out:

AI and automation for cybersecurity

The CEO's guide to generative AI: Cybersecurity

The power of AI: Security

IBM

IBM Institute for Business Value

Sources: 1: IBM IBV *The new era of cloud security*. 2: IBM IBV *Automotive 2030: Racing to a digital future*. 3: IBM IBV *Electric vehicles: An on-ramp to sustainable mobility*. 4 and 5: IBM IBV *Prosper in cyber economy, 2022*. 6: IBM *IBV open standards benchmarking, IT and OT risk, security, and resilience 2020*, unpublished.

DRQOOEOZ-USEN-00