BlackBerry. Intelligent Security. Everywhere.

24 OF THE TOP 25 EV OEMs CHOOSE BLACKBERRY QNX.

Read the top 10 reasons why.

ELECTRIC VEHICLE WHITE PAPER

THE TOP 10 REASONS WHY 24 OF THE TOP 25 EV OEMs CHOOSE BLACKBERRY QNX.

A diversity of teams—from traditional automakers to Silicon Valley start-ups—are racing to build electric vehicles (EVs). Without the paradigm disruption enabled by electrification, other innovations like autonomy, connectivity and sharing would come at a glacial pace. To enable rapid yet reliable innovation, the majority of these mobility leaders—in fact, 24 of the top 25 EV OEMs—choose BlackBerry® QNX® for their EV software, services and knowledge.

This white paper will explore the top 10 reasons why. First, it's important to briefly mention two industry trends that have set the stage for this domination.

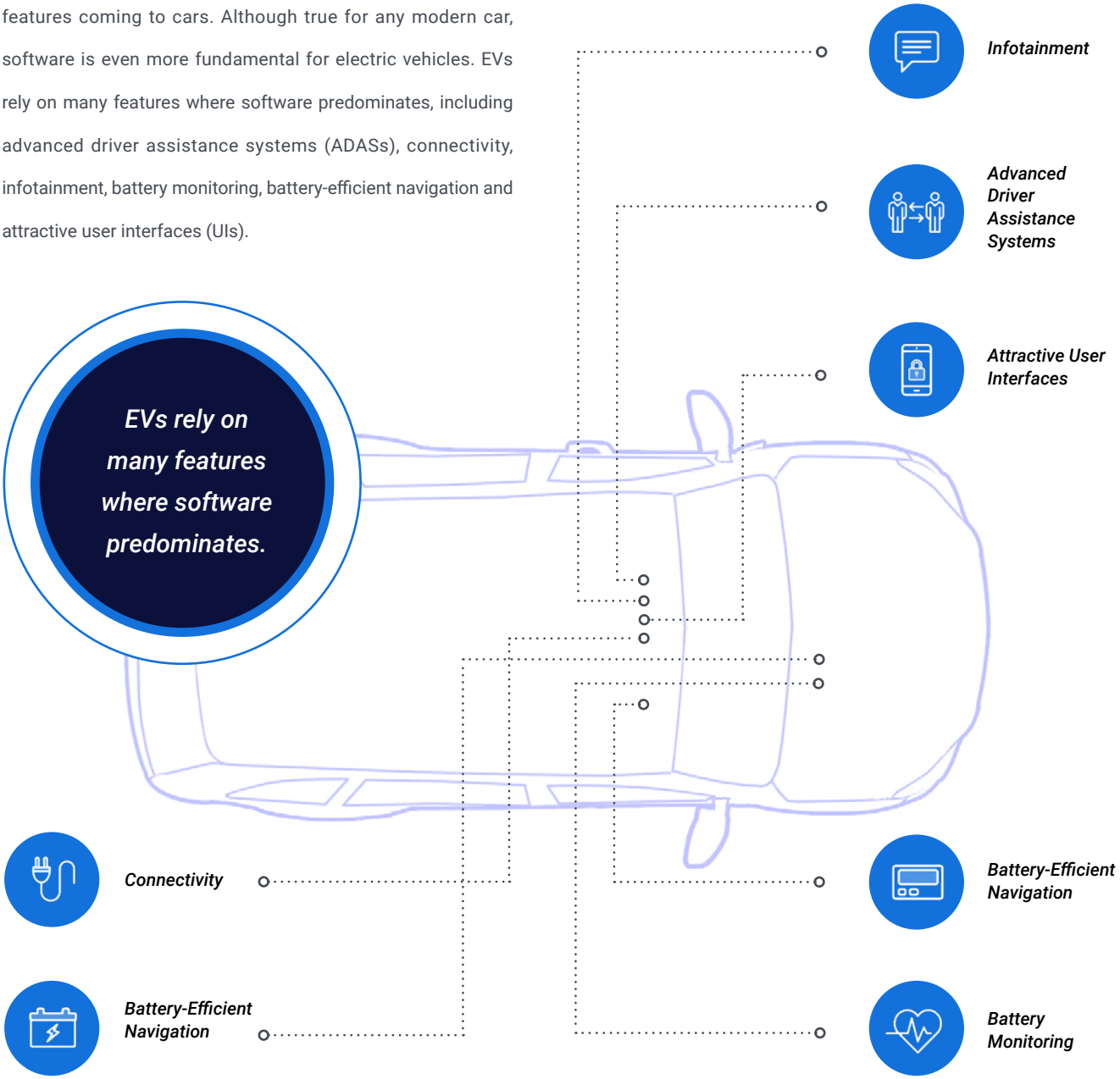
> *"EV OEMs are looking for partners with deep automotive software experience and successful track records to help solve some of their thorniest issues. Here's why BlackBerry QNX is at the top of the list for many EV OEMs in 2021."*

24 of the top 25 EV OEMs

are choosing BlackBerry QNX for their software, services and knowledge.

TREND #1: INCREASED SOFTWARE RELIANCE

There has been an explosive increase in software-dependent features coming to cars. Although true for any modern car, software is even more fundamental for electric vehicles. EVs rely on many features where software predominates, including advanced driver assistance systems (ADASs), connectivity, infotainment, battery monitoring, battery-efficient navigation and attractive user interfaces (UIs).



TREND #2: SOFTWARE OWNERSHIP

Automakers traditionally outsourced vehicle hardware and software development to others. This model, however, failed as soon as software became a defining and differentiating feature. Since then, automakers have decided to design and own the car's software so it can be built, fixed, extended and maintained over the life of a car and across different product lines. Now that automakers are responsible for software, they're carefully selecting its components, designing how it should interact and planning for its adaptation and evolution.

ADDRESSING AUTO TECH MARKET CHALLENGES

It's important to note that these new developments within traditional automakers mirror a software-first strategy chosen by brand-new EV companies. From California to China, companies that approach the problem of building vehicles from a fresh perspective are consistently applying software to solve old problems in car design, manufacturing and customer appeal. However, traditional automakers have not cultivated the software expertise needed to support this new direction. And although new automakers may have software competency, they are lacking automotive-specific domain expertise.

EV OEMs are therefore looking for partners with deep automotive software experience and successful track records to help them *solve some of their thorniest issues.* Here's why BlackBerry QNX is the operating system of choice for many EV OEMs in 2021.

REASON 1:
SAFETY FIRST

REASON 2:
DEEP COMPETENCE

REASON 3:
WHOLE-CAR SOFTWARE

REASON 4:
HYPERVISORS AND MODULE CONSOLIDATION

REASON 5:
BUILT FOR SECURITY

REASON 6:
CLOUD CONNECTED

REASON: 7
SENSOR FUSION

REASON 8:
RELIABLE SELF-DRIVING

REASON 9:
POWER EQUALS DISTANCE

REASON 10:
TIME-TO-MARKET

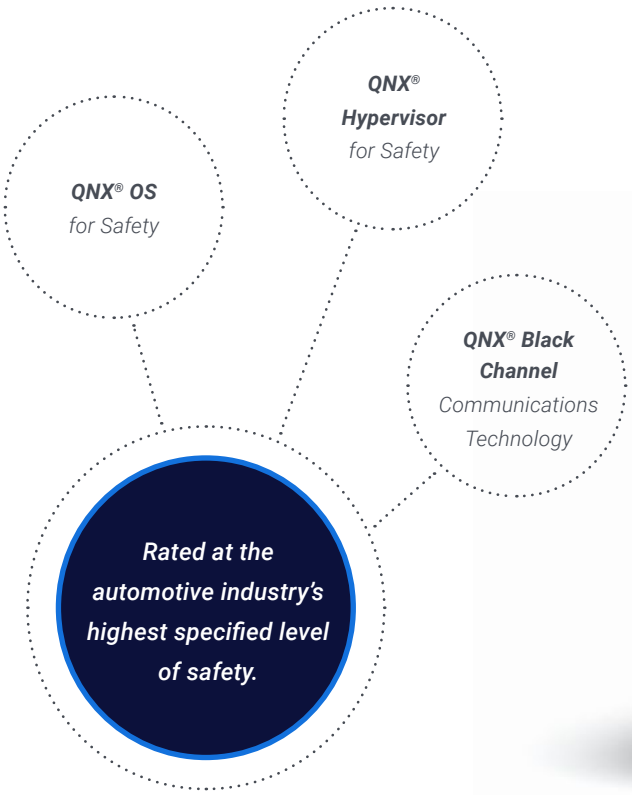
REASON #1:
SAFETY FIRST

One of the most critical requirements of any vehicle system is safety. This is one of the top reasons why automakers turn to BlackBerry QNX, a company known for its massive investment in safety certifications and industry reputation in building safe products. BlackBerry QNX has helped automakers streamline their safety certification processes and meet aggressive start of production dates with a combination of pre-certified software and unique safety expertise.

> ***"The reliable BlackBerry track record is why global automakers including Baidu, WM Motor, Arrival and many others rely on BlackBerry QNX to help run their cars."***

From a product perspective, the *QNX® OS for Safety, QNX® Hypervisor for Safety* and *QNX® Black Channel Communications Technology* are rated as *ISO 26262* ASIL-D certified, the automotive industry's highest specified level of safety—a bar that is met by few software vendors. This certification is complemented by BlackBerry® QNX® Professional Services, a team that has deep expertise and experience in certifying their own software as well as their customers'.

Safety considerations are what drove *BlackBerry QNX customer Desay SV Automotive* to use BlackBerry QNX technologies in the design of its EV sports sedan. But it isn't just automakers that recognize the value of reliability. Key component suppliers also have chosen BlackBerry QNX to form the basis of their autonomous driving platforms. The AI-powered *NVIDIA DRIVE* is a case in point, selected by *Daimler for its next-generation vehicles*.



Automakers rely on BlackBerry QNX Professional Services *as a trusted guide to produce safety-certified software.*

Advanced Driver Assistance Systems

REASON #2: ***DEEP COMPETENCE***

Just as important as safety-certified software is the engineering staff behind it. This is as true for new EV OEMs that sometimes lack rigorous software discipline as it is for established automakers building out their own software engineering capacity. Having been a key part of building software for *over 195 million cars*, the *BlackBerry QNX Professional Services team* has faced and solved thousands of challenging automotive problems in products from advanced LiDAR systems to large, integrated infotainment systems.

However, building today's electric car is not just about embedded development experience, it's also about the knowledge of certification processes, safety requirements and preeminent safety expertise. Most automakers' in-house EV engineering staff may not have the necessary experience with the difficult process of certification. That is why automakers rely on BlackBerry QNX Professional Services as a trusted guide to produce safety-certified software through engineer training, safety assessments and development methodologies as well as custom software components that meet special safety and security requirements.

After 35 years of building safe and secure systems, the BlackBerry QNX Professional Services team creates the quickest and smoothest path to safe EVs.

REASON #3:
WHOLE-CAR SOFTWARE

Every car is supported by dozens of separate subsystems that control every aspect of the car: door locks, windows, braking systems, lighting, engine, suspension, airbags, ADASs, instrument clusters and much more. A *single software architecture* holistically considers the software across every module, including both safety-critical under-the-hood modules as well as consumer-facing applications. Without an overarching plan, in-vehicle software development can quickly get out of control, making it extremely difficult to maintain, update and fix.

This is another critical reason why the QNX® Neutrino® RTOS underpins new EV architectures. Although it can easily support safety-critical and real-time applications like engine control, airbag deployment and ABS brakes, it's just as adept at managing the modern protocols and high-powered graphics needed for smartphone connectivity, infotainment and telematics. Customers like *Byton selected the QNX Neutrino RTOS for this reason*—it's one of the only real-time operating systems (RTOSs) that can be used for all car software, no matter where in the car it is. This flexibility allows Byton to rely on the same set of software libraries and services, reorganize module structures and use engineering talent across its entire car software development effort.

QNX Neutrino RTOS:
One of the only RTOSs that can be used for all car software.

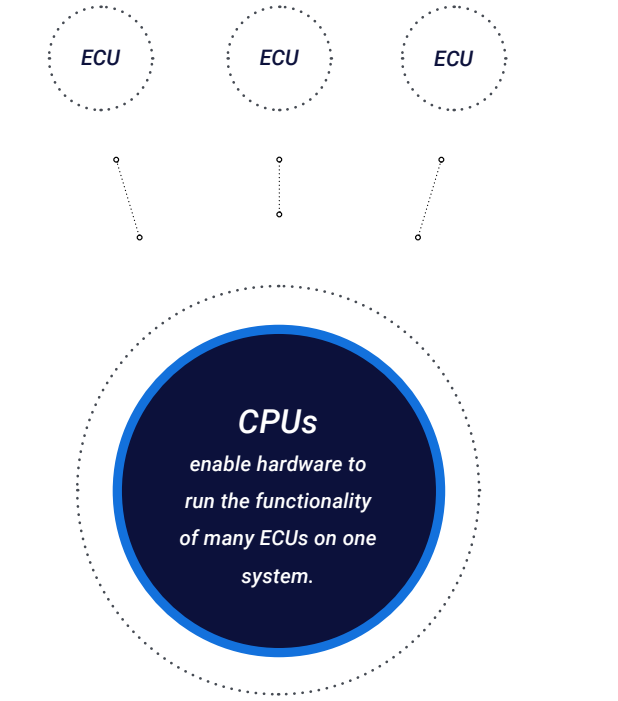
REASON #4:
HYPERVISORS AND MODULE CONSOLIDATION

Virtualization is another architectural change seen across the industry that is reducing costs and simplifying electronics. In earlier car designs when automakers placed all subsystems in separate electronic control units (ECUs), each black box required its own hardware, connectors, microcontroller or microprocessor, RAM memory, flash storage and supporting electronics. Although this traditional automaker structure was good at driving down individual module costs, it was unable to recognize a benefit across the many ECUs within the vehicle.

The commoditization of high-powered 32- and 64-bit CPUs as well as large RAM and flash chips now makes it possible for hardware to run the functionality of many ECUs on one system. But it's the introduction of hypervisor technology—letting a single CPU run multiple virtual machines protected and isolated from each other—that allows the consolidation of ECU software to be realized, removing the cost and complexity of dozens of hardware boxes in the car.

The hypervisor's job is to keep each subsystem isolated. It allows one chip to run many disparate functions such as instrument clusters, infotainment, rear seat entertainment and heads-up displays, to name a few. Hypervisor isolation also supports the development of virtual modules by independent teams, something that is critical for the global distributed workforce. And because it allows distinct modules to run without interfering with each other, a hypervisor can help prevent failures in one module from affecting others as well as contain security vulnerabilities. Because of their many strengths in creating isolated software domains, hypervisors are even being used in under-the-hood battery management ECUs to ensure the EV's fuel source—its battery—is kept at maximum operating capacity and within safe operating conditions.

Although a handful of hypervisor options are available, BlackBerry QNX has the industry's *first commercially available ISO 26262 ASIL-D safety certified hypervisor.* This combination of isolation and safety is crucial for automakers building architectures with ECU consolidation, and it's why *ARCFOX chose the automotive-designed BlackBerry QNX Hypervisor* for its intelligent electric SUV.



REASON #5:
BUILT FOR SECURITY

When cars weren't connected, there was little worry about remote attackers stealing data or disabling cars. That's no longer the case; new, always-connected and software-heavy EV architecture must be designed for defense. Although automakers take cybersecurity concerns seriously and organizations like Auto-ISAC, SAE and ISO provide best practice recommendations, automakers haven't been required to follow any cybersecurity guidelines to date. That situation is due to change. *The WP.29 regulation* released in 2020 by the United Nations establishes cybersecurity requirements for vehicles sold in the EU, the UK, Japan and South Korea. It includes a wide variety of requirements for automakers on items such as cybersecurity process, risk mitigation strategy, cyber-safe vehicle design and certification compliance. Because most automaker vehicle architectures have a global footprint, this regulation will have a huge impact on automotive cybersecurity programs worldwide.

BlackBerry security credentials play a big role in automaker cybersecurity considerations, with an array of security products that EV makers worldwide have come to rely on. *BlackBerry® Jarvis®* scans and flags software binaries for security vulnerabilities. *QNX Black Channel Communications Technology* secures critical data streams to prevent tampering. And the BlackBerry QNX Professional Services team assists in the many tasks needed to implement a cybersecure car, from secure boot through open-source audits and software security assessments to penetration testing. These products and services were a factor for *Karma Automotive in its selection of BlackBerry QNX technology* to keep the Revero luxury EV safe from cybersecurity exploits.

When it comes to the issue of protecting the data and the car, EV OEMs also need to safeguard the connection to the vehicle to safely and privately transfer vehicle diagnostics, sensor fusion streams and private user information. *Certicom®* by BlackBerry has been a key player in securing automaker data since the first telematics systems rolled off the assembly line decades ago, providing elliptical encryption, public key infrastructure (PKI), asset management systems, code signing and certificate authority services. BlackBerry also brings its authoritative security experience to automakers through *BlackBerry® Persona*, a security solution that actively adapts to protect the car by using machine learning to recognize and remove malware.

As a result, BlackBerry technology is being used by automakers to secure software in the vehicle, in the automaker cloud backend—even on the manufacturing line. Because these certification, cryptography and cyberdefense pieces smoothly integrate across its entire automotive software offering, BlackBerry makes it easy for EV OEMs to get their safety and security needs met by a single supplier.

> ***"One of the most critical requirements of any vehicle system is safety. This is one of the top reasons why automakers turn to BlackBerry QNX, a company known for its massive investment in safety certifications and industry reputation in building safe products."***

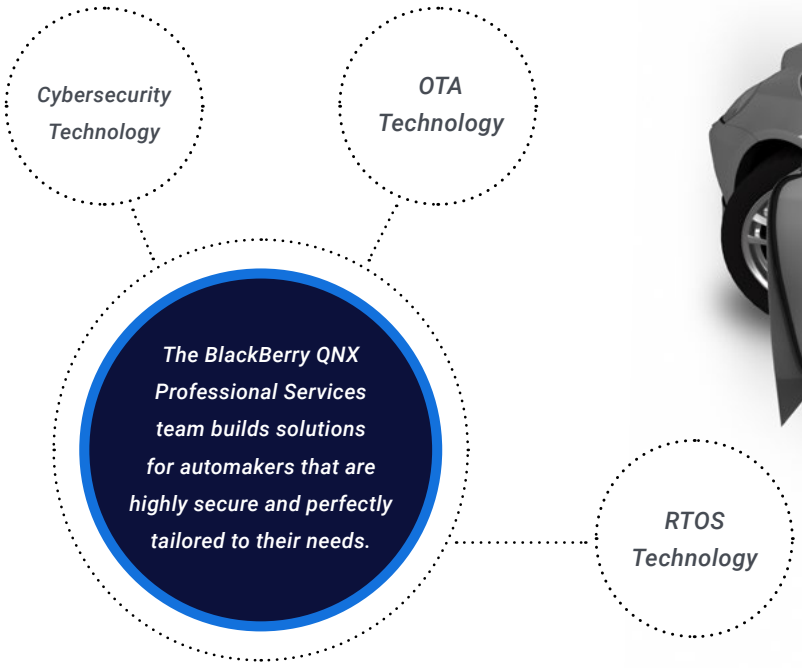
REASON #6:
CLOUD CONNECTED

Everyone regularly relies on over-the-air (OTA) software updates for their phones, laptops and other connected devices. These updates allow software providers to fix bugs, patch security vulnerabilities, add new features and improve the customer experience to keep products running optimally. Software update expectations have also carried over to the car. OTA updates let cars increase in perceived value after their purchase as well as generate brand loyalty. This fact has made EV OEMs both old and new sit up and take notice.

BlackBerry QNX helps automakers deliver an OTA experience that's automotive-specific. Although phone or computer OTA updates may be commonplace, they are often intrusive, leading to many minutes of unavailability as the system rewrites critical software components. Nobody wants to wait in their car for a half-hour update when they're trying to rush their child to the doctor, hurry to an important meeting or pick up groceries for dinner.

Because of its microkernel operating system, the QNX Neutrino RTOS is unique in its ability to enable incremental OTA updates. It is designed to support hot-swapping of running software components—even at the system or device driver level—which allows for maximum flexibility when it comes to software updates. Another factor is the QNX Neutrino RTOS's fast boot. With a boot time measured in milliseconds rather than seconds, any updates that must restart the system result in a momentary hesitation rather than a lengthy delay. These technical advantages are unique to the QNX Neutrino RTOS, making it the perfect choice as the backbone for automakers' OTA solutions.

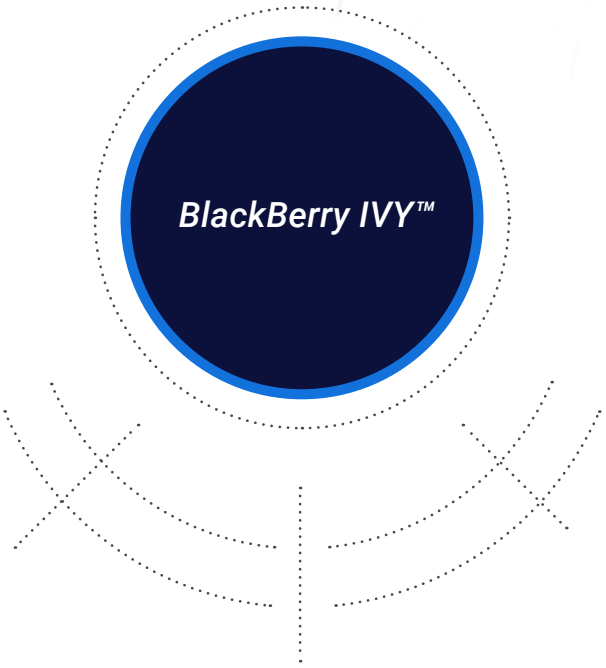
Finally, with a complex system such as an EV, an OTA solution will never be an off-the-shelf technology. BlackBerry has been able to combine its deep automotive knowledge with years of mobile device OTA experience to create a world-class OTA deployment team. The BlackBerry QNX Professional Services team draws from a large portfolio of distinct RTOS, OTA and cybersecurity technologies to *build OTA solutions* for automakers that are highly secure and perfectly tailored to their needs. A number of automakers have deployed custom BlackBerry OTA solutions that manage their unique demands, whether they are manufacturing plant tie-ins, bespoke in-vehicle architectures or customer cloud portals.



REASON #7:
SENSOR FUSION

An autonomous vehicle uses many different sensors that continually collect data from the car and its surroundings: camera, LiDAR, radar, gyroscopes, GPS location and accelerometers. Sensor fusion is the merging of these continuous data sources into a single organized and condensed data stream. This data then drives the autonomous car's recognition, decision and control mechanisms. Once fed to the cloud, that vital data also feeds the machine-learning algorithms that allow our cars to continually improve.

To solve this complex task, BlackBerry has developed *BlackBerry IVY™*, a scalable, cloud-connected software platform that allows automakers to provide a consistent and secure way to read vehicle sensor data, normalize it and create actionable insights from that data both locally in the vehicle and remotely in the cloud. Automakers can use this information to create responsive in-vehicle services that enhance driver and passenger experiences. This product, jointly developed and marketed by Amazon Web Services (AWS), allows automakers to simultaneously solve the in-car and in-cloud challenges involved in developing, running and refining autonomous machine-learning algorithms. The reliable cloud capability provided by BlackBerry IVY and directly backed by AWS helps EV OEMs build self-driving systems, create customer-personalized services and monetize vehicle data.



REASON #8:
RELIABLE SELF-DRIVING

An autonomous system requires software that is reliable and safe. Yet a car's self-driving system uses different software technologies than normal automotive embedded software. For instance, machine-learning algorithms often use the Python programming language and machine vision systems usually need graphics processing unit (GPU) programming. However, these systems still require real-time performance and high reliability. This combination of attributes and technologies can really only be found in one vendor—BlackBerry QNX.

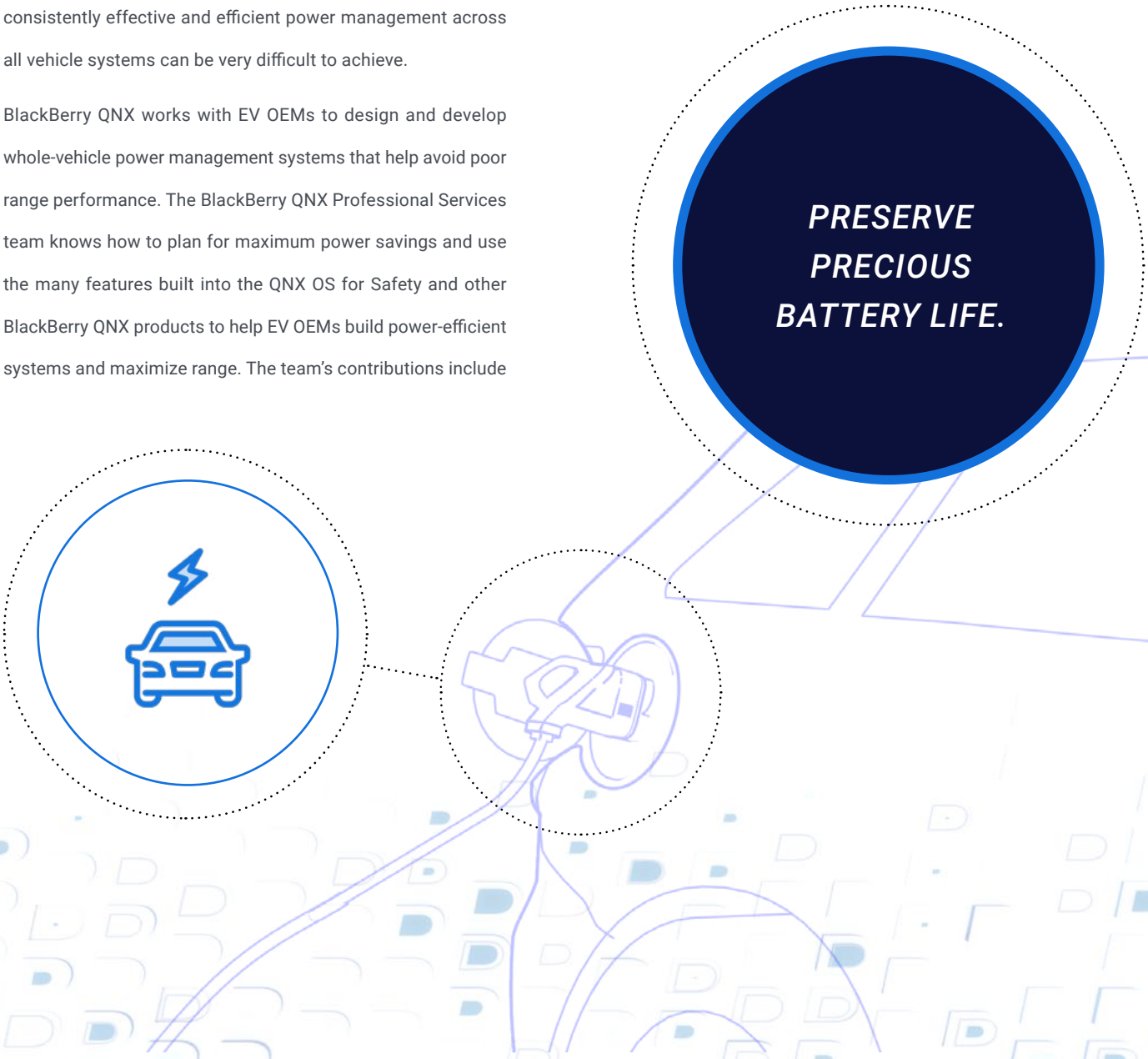
The *QNX OS for Safety* and the *QNX® Platform for ADAS* are used by automakers to help ensure their self-driving systems meet highly rigorous safety requirements such as the *Federal Motor Vehicle Safety Standards*. The QNX Platform for ADAS, built on the QNX OS for Safety, provides automated driving systems with a solid software foundation as well as reference implementations for a well-designed starting point. This reliability is why EV OEMs *Canoo* and *Damon* use BlackBerry QNX products and services to implement their vehicles' ADAS and autonomous features. It's also why EV OEMs rely on BlackBerry QNX software to keep their mission-critical components always running—like *Leddartech's autonomous LiDAR* and *Renovo's vehicle data management system.*

> ***"With decades of proven expertise and a huge array of technologies at its disposal, BlackBerry QNX is at the forefront of helping OEMs build electric cars."***

REASON #9:
POWER EQUALS DISTANCE

Electronics designed for internal combustion engines (ICEs) could always rely on a running engine to provide a steady power supply. This setup meant the car's electrical components weren't maximally energy efficient—they didn't need to be. Switching the fuel source from gasoline to battery makes energy efficiency a significantly higher priority. The more power an EV uses for electronic systems, the less is available for propulsion. Poorly designed hardware and needlessly executing software soak up excessive power, shortening an EV's range and, as we all know, limited range is already a key customer concern. Yet maintaining consistently effective and efficient power management across all vehicle systems can be very difficult to achieve.

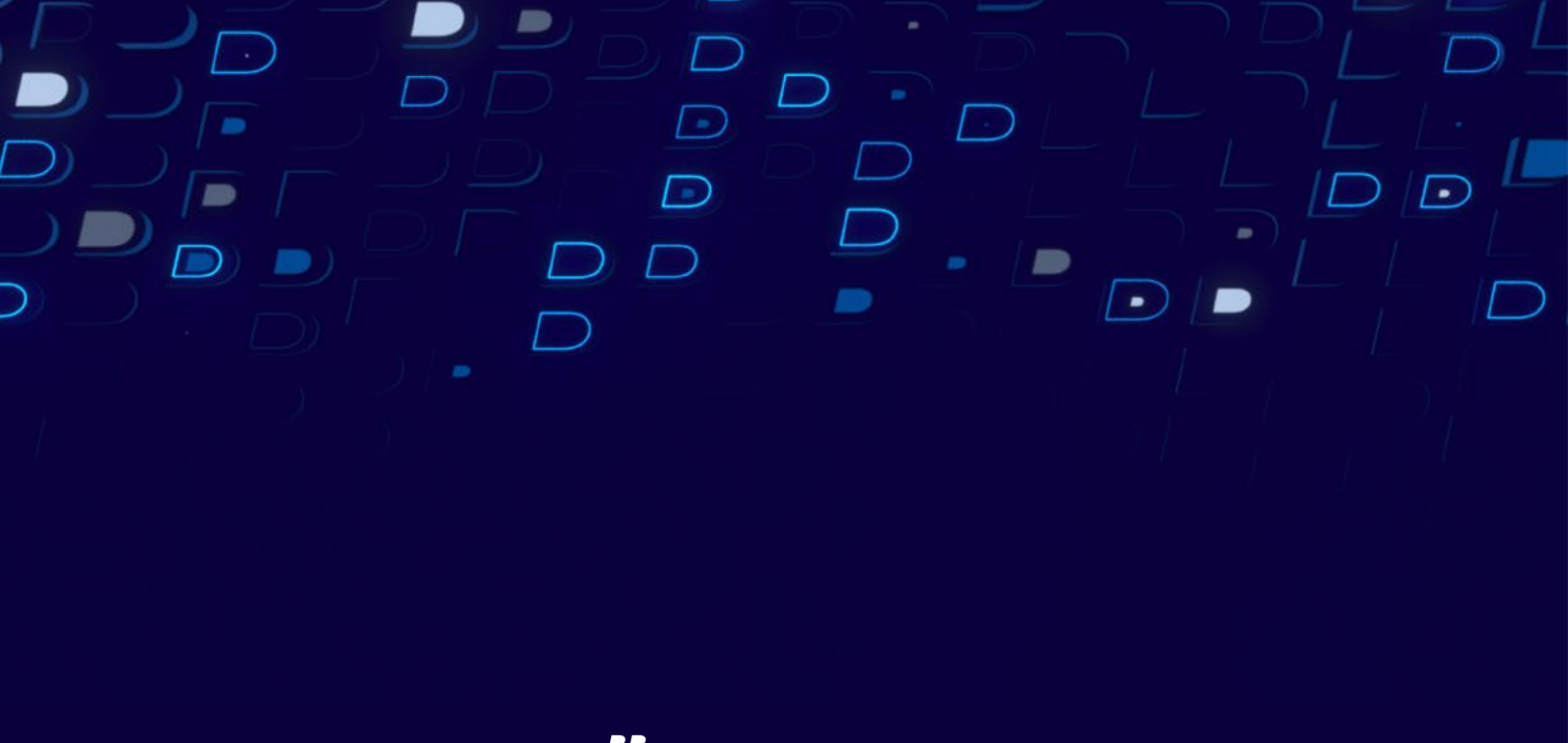
BlackBerry QNX works with EV OEMs to design and develop whole-vehicle power management systems that help avoid poor range performance. The BlackBerry QNX Professional Services team knows how to plan for maximum power savings and use the many features built into the QNX OS for Safety and other BlackBerry QNX products to help EV OEMs build power-efficient systems and maximize range. The team's contributions include precisely controlling powered-on CPU peripherals and low power modes, implementing dynamic voltage and frequency scaling techniques to match performance requirements to power draw and using fast-boot optimizations to keep systems turned off as long as possible—all to preserve precious battery life.



REASON #10:
TIME-TO-MARKET

Whether old or new, EV OEMs need to meet regulatory requirements and appeal to customers who may be purchasing an EV for the first time. With the exponentially expanding amount of software in new vehicles, EV OEMs can't afford the time to piece together the millions of details involved in building electric car software. The cost of homegrown solutions and extensive integration lessons is high: at best it comes with added cost and wasted time, and at worst can lead to public mistakes and brand damage. EV OEMs can make much better use of their time and finances by using industry-trusted products and road-tested suppliers to get their vehicles to market faster.

With decades of proven expertise and a huge array of technologies at its disposal, BlackBerry QNX is at the forefront of helping OEMs build electric cars. The reliable BlackBerry track record is why global automakers including *Baidu*, *WM Motor*, *Arrival* and many others rely on BlackBerry QNX to help run their cars. And it's why many EV OEMs today have BlackBerry QNX powering their vehicles' software.



Intelligent Security. Everywhere.

About BlackBerry: BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 195M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear—to secure a connected future you can trust.

.For more information, visit ***BlackBerry.com*** *and follow* ***@BlackBerry****.*