

A background image showing a blurred view of a road and a car, suggesting high speed and motion. The car is on the right side of the frame, and the road curves into the distance.

Why This Major Automaker Decided BlackBerry Cybersecurity Consulting was the Right Road to Protecting its Connected Cars

Industry Automotive
Services BlackBerry®
Cybersecurity Services

At a Glance

A global leader in the connected car market, this automaker is constantly seeking new ways to make driving both safer and more enjoyable for its customers. One of the greatest challenges it encountered in that regard was managing patches and updates. It worked with BlackBerry® Cybersecurity Consulting to create a secure platform for over-the-air updates.

A full-service cyber consultancy practice, BlackBerry Cybersecurity Consulting leverages BlackBerry's proven leadership in high-security organisations and use cases. Through extensive investigative experience and in-depth knowledge, BlackBerry's cybersecurity professionals assess the unique threat landscape and security challenges of each organisation they work with.



The Organisation

As a leading automaker and a leading manufacturer of connected cars, this organisation ships hundreds of thousands of vehicles to dealers and customers all over the world. It is a long-time partner of BlackBerry QNX®, and is constantly seeking ways to improve the driving experience for its customers. Given its leading position in the automotive space, it is familiar with the risks of software on the road.

It is also familiar with the complexities of addressing those risks. On the one hand, road safety is critical, and even a minor vulnerability can compromise that safety. On the other, they cannot introduce anything that will represent an inconvenience for their customers.

One of the most significant challenges faced by the automaker involved the delivery of security updates. The automaker knew that regular updates were necessary to keep its vehicles secure. However, it also knew that it needed to provide these updates in a way that was at once seamless, streamlined, and secure.

It struggled with how to achieve this.

"The cars of today are effectively big computers," explains James McDowell, Director of BlackBerry Cybersecurity Consulting. "The problem, of course, is that you can't update a car the same way you do a computer. It's not practical, and it's not safe – the automaker opted to work with us to find a solution."

“Fundamentally, the most important thing about a car is safety – there is no higher priority. Cybersecurity, now more than ever is tied up in that, and there’s a huge skills gap. We helped this automaker plug that gap, and make its vehicles both safer and more secure.”

James McDowell,
Director, BlackBerry®
Cybersecurity Consulting

The Challenge

Originally, the automaker attempted to update its vehicles when they were brought in for service – the driver would drop the car off at the garage, and staff would plug in a USB stick to apply any outstanding patches. Unfortunately, this method was both cumbersome and inefficient. The end result was that almost none of the automaker’s vehicles were up to date.

“The client quickly realised that it couldn’t keep asking customers to drive to a garage every time there was a patch,” McDowell says. “It needed a way to update its cars remotely at any time, from anywhere in the world. And it needed to be able to do so without the customer even knowing.”

An update for a car might contain information about embedded systems such as brakes, lights, or steering. If a hacker were able to intercept such an update, they could use it to brick a vehicle – or worse, cause a severe accident. But if, in the interest of preventing that scenario, the automaker interrupted the driving experience, it would alienate its entire customer base.

“Imagine a car that takes as long as a laptop to restart, or one that has to shut down every time there’s a patch,” says McDowell. “No one would buy it. There needs to be a balance between security and usability, and that balance is one that’s difficult to strike where connected cars are concerned.”

“Security is critical, but this is a consumer product,” he continues. “Convenience is just as important. You aren’t just thinking about security best practices – you’re also considering what you want your product to do for the customers at the same time.”

The automaker knew that it lacked the cybersecurity expertise to address these challenges, and decided to bring in outside help.

“Fundamentally, the most important thing about a car is safety – there is no higher priority. Cybersecurity, now more than ever is tied up in that, and there’s a huge skills gap. We helped this automaker plug that gap, and make its vehicles both safer and more secure.”

James McDowell,
Director, BlackBerry®
Cybersecurity Consulting

The Services

After speaking to BlackBerry QNX about BlackBerry Cybersecurity Consulting, the automaker created a shortlist of consultancies. It eventually narrowed that list down to BlackBerry and one other organisation. Although the other organisation’s services cost less, the automaker opted to work with BlackBerry.

“They came to us and told us they had two proposals on the table – ours and a competitor’s,” explains McDowell. “Although the competitor cost less than us, it was clear that they weren’t providing everything the automaker required. Ultimately, they decided to work with us – we had the expertise to give them exactly what they were looking for.”

BlackBerry’s Cybersecurity team then created a threat model that examined every potential risk of over-the-air updates, and presented that model to the automaker. From there, it was up to the automaker to decide what risks to address. Finally, they collaborated with the automaker’s engineering team to build a secure update platform from the ground up.

“We worked with the automaker to build security best practices in from the beginning,” says McDowell. “However, we only provided guidance – not commands. We explained the risk and impact of each decision, and allowed the client to make their own decisions about how to address them.”

“From a more general perspective, what we do for this automaker represents a shift in how people look at security. Historically, people have built products then tested to see if they were secure. Our approach with this automaker is the new approach – building in security while building the product.”

James McDowell,
Director, BlackBerry®
Cybersecurity Consulting

The Results

With help from BlackBerry Cybersecurity Consulting, the automaker was able to build a system capable of sending secure over-the-air updates to a vehicle without interrupting what that vehicle was doing. It can now ensure every vehicle it sells is consistently up to date, and readily push out security updates and quality of life patches. More importantly, it has also learned a great deal through collaboration with BlackBerry.

Security Without Sacrificing Convenience: BlackBerry has a long history in the security space. Much of what the company’s Cybersecurity Consulting does is simply an externalisation of its own internal security checks. What that means for clients like the automaker is that they can gain an understanding of where the boundaries lie when balancing security and convenience.

“For us, everything starts with security – we wouldn’t make a product and add functionality that compromises security in any way,” McDowell explains. “That’s the difference between us and other companies – they put security around something, but we put everything around security.”

“Working with us, the automaker has come around to this line of thinking – and it will serve them well, moving forward.”

Newfound Expertise: The greatest challenge of the connected car market and of the larger Internet of Things is the sudden requirement for engineering companies to become technology companies. There’s a massive learning curve involved in this. Many businesses are ill-equipped to deal with that learning curve.

Working with BlackBerry, the automaker is ready to excel in the connected car market.

“We don’t simply go in, perform an evaluation, and walk away – we’re interested in helping our clients understand what we’re doing,” notes McDowell. “The automaker’s engineering team is now better-placed on their next project. They’ve learned how to carry out threat modelling, and they’ve learned what to look for when designing a secure product.”

About BlackBerry Limited

BlackBerry Limited is an enterprise software and services company focused on securing and managing IoT endpoints. The company does this with BlackBerry® Secure™, an end-to-end Enterprise of Things platform, comprised of its enterprise communication and collaboration software and safety-certified embedded solutions.

Based in Waterloo, Ontario, BlackBerry Limited was founded in 1984 and operates in North America, Europe, Asia, Australia, Middle East, Latin America and Africa. The Company trades under the ticker symbol "BB" on the Toronto Stock Exchange and the New York Stock Exchange. For more information visit [BlackBerry.com](https://www.blackberry.com), and follow the company on [LinkedIn](#), [Twitter](#) and [Facebook](#).