Septembre 2024

Au carrefour de la technologie et de la cybersécurité : quels sont les enjeux de la mobilité connectée ?

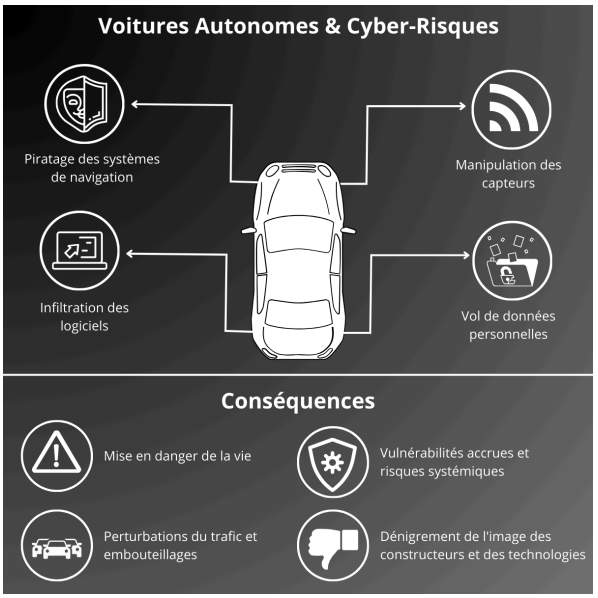
Romain LAFITTE
Managing Director chez Via ID

Sommaire

Dans un monde où la technologie et la connectivité redessinent les contours de l'industrie automobile, les récentes préoccupations exprimées par les autorités américaines à l'égard des voitures connectées chinoises mettent en avant les enjeux qui se situent à l'intersection de la mobilité et de la cybersécurité. L'évolution de ces technologies pose des questions essentielles sur la sûreté et la sécurité des informations et des infrastructures dans un monde où chaque véhicule constitue le nœud d'un réseau vaste et interconnecté.

Luca de Meo, CEO du groupe Renault, estime que "Le véhicule défini par le logiciel, nommé Software Defined Vehicle, représente l'avenir de l'industrie automobile," et annonce une montée en puissance spectaculaire du marché des véhicules connectés[1]. Cette transformation ne marque pas seulement une révolution technologique ; elle initie un changement de paradigme dans notre façon de concevoir, d'utiliser et d'interagir avec nos moyens de transport. Toutefois, **la promesse d'une mobilité plus efficace, plus personnalisée et plus connectée** vient avec son lot de défis, en particulier dans le domaine de la cybersécurité.

La croissance exponentielle de la connectivité des véhicules, tout en ouvrant de nouveaux horizons pour l'innovation et l'amélioration de l'expérience utilisateur, **introduit également un niveau de vulnérabilité accru aux cybermenaces**. Au-delà de la protection des données personnelles des utilisateurs, ces préoccupations en matière de cybersécurité touchent également à la sécurité des systèmes de transport eux-mêmes, susceptibles d'être la cible d'attaques visant à les perturber ou à les paralyser. Face à ce défi, l'industrie de la mobilité connectée doit **trouver le juste équilibre entre innovation technologique et impératifs de sécurité**, s'engageant dans une lutte constante pour préserver les infrastructures et les données contre les nouvelles menaces.

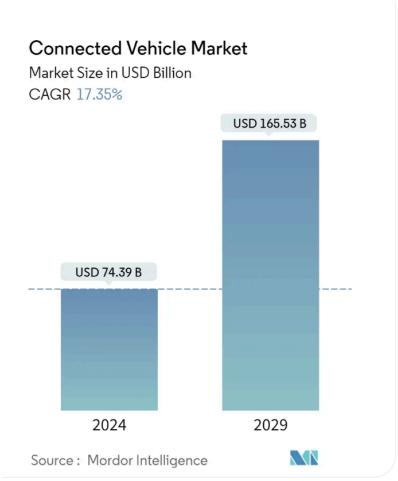


Source : Blog Cybersecurity

[1] Un véhicule connecté est un véhicule qui intègre des technologies de communication pour échanger des données avec d'autres dispositifs, améliorant ainsi la sécurité, l'efficacité et le confort.

Accélérer vers le futur : tendances actuelles et projections du marché des véhicules connectés

L'expansion rapide du marché des véhicules connectés marque une révolution dans l'industrie automobile, redéfinissant les fondements de la mobilité moderne. À l'horizon 2027, le nombre de véhicules connectés en service dans le monde devrait presque doubler, passant de 192 millions en 2023 à 367 millions. Cette croissance spectaculaire est appuyée par un marché en pleine ascension, dont la valeur est estimée à 74,39 milliards USD en 2024 et devrait s'élever à 165,53 milliards USD d'ici 2029, avec un TCAM (Taux de Croissance Annuel Moyen) impressionnant de 17,35% sur la période 2024-2029.



Période d'étude	2019 - 2029
Taille du Marché (2024)	USD 74.39 milliards de dollars
Taille du Marché (2029)	USD 165.53 milliards de dollars
TCAC(2024 - 2029)	17.35 %
Marché à la Croissance la Plus Rapide	Asie-Pacifique
Plus Grand Marché	Asie-Pacifique

Ce développement fulgurant témoigne d'une adoption accrue à l'échelle mondiale, même si le taux de pénétration des véhicules connectés varie significativement d'une région à l'autre. Alors qu'il est de seulement 30% au Japon, des pays comme la France et l'Allemagne affichent des taux bien plus élevés (respectivement 71,8% et 84,3%). Ces différences mettent en lumière **les disparités dans l'adoption des technologies connectées, reflétant ainsi la diversité des approches et des stratégies à l'échelle internationale**.

Mary Barra, DG de General Motors, encapsule parfaitement l'essence de cette transformation : "**L'avenir de la mobilité sera déterminé par ceux qui parviendront à intégrer avec succès connectivité, électrification et conduite autonome**." Cette vision souligne tout le potentiel de la mobilité connectée, non seulement pour révolutionner l'industrie automobile, mais également pour façonner la société dans son ensemble. Les implications vont bien au-delà des véhicules eux-mêmes, promettant des avancées vers **des villes plus intelligentes, plus efficaces et plus durables**. Dans cette perspective, l'expansion du marché des véhicules connectés n'est pas juste une tendance, mais un pivot vers un avenir où la technologie et la connectivité redéfinissent les contours de notre environnement urbain et de notre vie quotidienne.

L'impact de la connectivité sur l'industrie automobile marque une évolution sans précédent dans les changements technologiques et les modèles d'affaires. L'avènement des véhicules connectés, devenant de véritables ordinateurs sur roues, redéfinit les perspectives de mobilité. **Aujourd'hui, une voiture connectée est équipée de pas moins de 200 capteurs**, surveillant une gamme étendue de paramètres, depuis la température du moteur jusqu'à l'état des ceintures de sécurité. Ces dispositifs collectent une quantité phénoménale de données, promises à une croissance exponentielle avec le développement de la conduite autonome.

De nouveaux entrants et des investissements massifs pour la connectivité des véhicules

Cette transformation donne naissance à de nouvelles sociétés spécialisées dans la connectivité des véhicules, tandis que les géants technologiques comme Google investissent massivement dans ce domaine. Un acteur comme Waymo, filiale d'Alphabet (maison mère de Google), spécialisée dans le développement de technologies de conduite autonome, est à la pointe de cette révolution. Ces sociétés technologiques proposent des solutions allant de la gestion de flotte autonome à la navigation avancée, exploitant la connectivité pour offrir une mobilité plus sûre, plus propre, et plus efficiente. Il est évident que la présence accrue de ces acteurs souligne un changement de paradigme, où les voitures ne sont plus de simples moyens de transport mais des hubs connectés, intégrant et interagissant avec un écosystème numérique plus large.

Les véhicules peuvent se connecter et communiquer avec leur environnement de diverses manières, révolutionnant la sécurité routière, la gestion de flotte, et l'efficacité énergétique. La connectivité du véhicule à l'infrastructure fournit des **données vitales sur la sécurité et les conditions environnementales**. Entre les véhicules, cet échange **améliore la sécurité et réduit les embouteillages**. De plus, la connexion au cloud offre des avantages en termes de gestion des performances et d'entretien, tandis que la communication avec les piétons vise à **prévenir les accidents**. Enfin, la capacité d'interconnexion à tout autre dispositif ouvre des possibilités infinies pour l'intégration de la voiture dans le réseau global de l'Internet des objets (IoT).

Une infrastructure permettant une connectivité optimale des véhicules

Afin de répondre aux exigences des voitures connectées qui génèrent des millions de points de données chaque jour, la connexion internet doit s’adapter. L’arrivée de la 5G est une première réponse, mais comme le précise Damien Garot CEO de la société Stellar, “elle n’offre pas une couverture suffisante sur l’ensemble de nos routes”. C’est pourquoi la startup se propose d’offrir à ses partenaires du marché automobile **une solution de connectivité hybride intelligente**. “Un internet parfait sur les routes ne peut être atteint qu’en combinant toutes les technologies sans fil disponibles (cellulaire 4G/5G, Wi-Fi et

satellite) grâce à des algorithmes avancés basés sur l'intelligence artificielle et une cartographie précise des réseaux télécoms sur les routes."

De nouveaux services et modèles économiques émergent

Cette ère de connectivité promet non seulement d'**améliorer l'expérience de conduite mais aussi de proposer de nouveaux modèles économiques**. Des services basés sur les données, tels que l'assurance au kilomètre, l'assurance ajustées au comportement de conduite (avec des données permettant de récompenser les pratiques de conduite sûres). Mais aussi un service de maintenance prédictive. **L'analyse des données opérationnelles permet d'anticiper les besoins de réparation, améliorant ainsi la fiabilité du véhicule et réduisant les coûts d'entretien pour les propriétaires**. Enfin, les plateformes de divertissement embarquées tirent parti des préférences des utilisateurs pour proposer des contenus personnalisés, transformant le temps passé en voiture en une expérience récréative. Cette transformation vers une mobilité connectée et intelligente représente à la fois un défi et une opportunité majeure pour l'industrie automobile, nécessitant une adaptation rapide pour rester à l'avant-garde de l'innovation. Cependant, elle introduit aussi des défis majeurs en matière de cybersécurité.

La cybersécurité automobile : les enjeux d'une réponse aux menaces croissantes dans un monde connecté

Les risques d'un contrôle à distance d'un véhicule connecté

L'importance cruciale de la cybersécurité dans le domaine de la sécurité routière est mise en exergue par Chris Valasek, expert reconnu pour ses recherches sur la vulnérabilité des véhicules aux attaques à distance. Il souligne que "la sécurité des véhicules connectés transcende la simple protection des données personnelles pour devenir **une fondation de la sécurité routière elle-même**." Cette affirmation souligne l'indispensabilité de la cybersécurité, non seulement pour la confidentialité, mais aussi comme **garant de la sécurité physique des occupants**. Face à des menaces en constante évolution, l'adoption de stratégies de défense robustes et adaptables est devenue impérative.

C'est pourquoi, le secteur de la cybersécurité automobile connaît une croissance exponentielle. Estimée à 2,9 milliards de dollars en 2022, une projection à 10,3 milliards est envisagée d'ici 2032. Cette tendance marque l'urgence de concevoir des solutions avancées pour faire face aux menaces grandissantes. En effet, à mesure que les automobiles s'intègrent davantage dans le réseau numérique mondial, elles sont exposées à des risques accrus de piratage et de vol de données.

Source : [Global Market Insights]

Ces risques de piratage et vol de données se manifestent principalement sous deux formes critiques : la protection des données et la sécurité routière. Avec l'intégration des systèmes d'infodivertissement et des Unités de Commande Électronique (ECU), contenant jusqu'à 40 millions de lignes de code, les véhicules connectés sont extrêmement vulnérables. Ces systèmes complexes peuvent être **exploités pour le vol d'informations personnelles ou, plus dangereux encore, pour la prise de contrôle à distance de fonctions vitales telles que les systèmes de freinage ou de direction**. Ainsi, la sophistication croissante des véhicules connectés, dotés de réseaux complexes de capteurs et d'algorithmes, augmente leur vulnérabilité aux cyberattaques. Les Systèmes d'Aide à la Conduite Avancés (ADAS), utilisent des capteurs comme le LiDAR[2], des caméras et des radars pour collecter des données sur l'environnement du véhicule et prendre des décisions de conduite. Ces systèmes s'appuient sur des algorithmes complexes pour traiter les données et agir en conséquence, comme l'ajustement automatique de la vitesse, le freinage d'urgence ou l'assistance au maintien de la voie. Si un pirate parvient à compromettre ces systèmes, il pourrait désactiver le freinage d'urgence ou manipuler le système d'assistance au maintien de la voie pour provoquer un accident.

De même, **les communications Véhicule à Véhicule (V2V) et Véhicule à Infrastructure (V2I) sont essentielles pour la sécurité et l'efficacité de la conduite connectée**. Elles permettent aux véhicules de partager des informations sur leur position, vitesse et direction, ainsi que sur les conditions de la route et les signaux de trafic. Ces informations permettent d'éviter les collisions et d'optimiser les flux de trafic. Cependant, un pirate pourrait, par exemple, envoyer de fausses informations à un véhicule, lui faisant croire qu'un obstacle se trouve sur sa trajectoire, poussant ainsi le véhicule à effectuer une manœuvre d'évitement inutile et potentiellement dangereuse.

Un exemple concret de ces vulnérabilités a été démontré par des chercheurs en sécurité ayant réussi à prendre le contrôle à distance d'une Jeep Cherokee. En exploitant une vulnérabilité dans le système d'infodivertissement connecté à l'internet du véhicule, ils ont pu accéder aux fonctions critiques du véhicule, comme le contrôle de la direction, l'accélération et le freinage, démontrant ainsi les risques potentiels liés à la cybersécurité des systèmes embarqués. **Le journaliste Andy Greenberg qui s'était prêté à l'exercice à connu une expérience choquante**. Alors qu'il roulait sur une autoroute américaine à une vitesse de 100 km/h, plusieurs fonctions de bord du Cherokee se sont mises en route tout seul. La ventilation s'est mise à souffler au maximum, la radio s'est allumée à pleine puissance, le lave-glace a vidé son réservoir et les essuie-glaces se sont affolés. Mais ce n'est pas tout... les chercheurs sont parvenus à mettre la transmission hors service et à désactiver les freins.

[2] Le terme LiDAR est un acronyme anglais pour « LIght Detection And Ranging » signifiant en français « détection et estimation de la distance par la lumière ». Le Lidar est une méthode de télédétection sous forme de capteur laser consistant à mesurer le « temps de vol » (TOF ou « Time-Of-Flight ») des faisceaux lumineux.

Quelles solutions pour renforcer la cybersécurité des véhicules connectés ?

Face à cette menace ciblant l'industrie automobile, la mise en place de solutions et mesures de sécurité robustes pour les véhicules connectés est devenue une priorité. Le secteur automobile répond par l'adoption de normes et réglementations strictes, ainsi que par le déploiement de technologies avancées pour protéger les utilisateurs et leurs données.

Plusieurs normes et réglementations structurent désormais la cybersécurité dans le secteur automobile. Ces dernières se positionnent sur toutes les phases du cycle de vie des véhicules, de leur conception à leur maintenance pour être le plus efficace possible.

- Par exemple, la norme ISO/SAE 21434, issue d'une collaboration entre l'Organisation Internationale de Normalisation (ISO) et la Society of Automotive Engineers (SAE), définit des directives cruciales pour la gestion de la sécurité des informations. Elle promeut une analyse approfondie des risques et l'adoption de mesures de protection adaptées.
- La National Highway Traffic Safety Administration (NHTSA), l'agence fédérale américaine chargée de la sécurité routière, et la norme SAE J3061, spécifique à la cybersécurité dans l'automobile, proposent quant à elles des orientations pour **identifier et gérer les risques liés à la cybersécurité**, en insistant sur l'importance de rester proactif face aux menaces numériques.
- Ces efforts sont complétés par les recommandations du WP.29, le forum mondial pour l'harmonisation des réglementations des véhicules des Nations Unies, qui établit des principes pour la sécurité **des véhicules connectés et pour les mises à jour logicielles effectuées à distance**

(Over-The-Air, OTA). Ces mises à jour OTA sont cruciales pour corriger rapidement les vulnérabilités. En parallèle, les meilleures pratiques de l'Automotive Information Sharing and Analysis Center (Auto-ISAC) aident les constructeurs et fournisseurs à renforcer leurs défenses contre les cyberattaques en favorisant le partage d'informations et la collaboration en matière de cybersécurité automobile.

Ces cadres et directives jouent un rôle vital dans la prévention des cyberattaques et la protection des utilisateurs dans un paysage technologique en constante évolution.

Des opportunités pour les acteurs du secteur

Les constructeurs automobiles déploient des mesures innovante

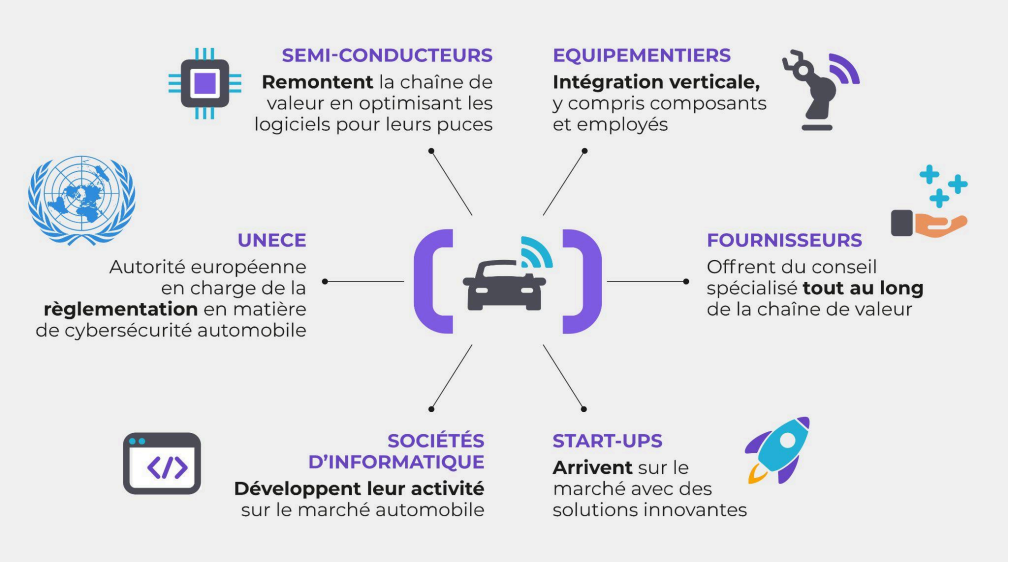
Dans le sillage des réglementations établies par les normes et les recommandations évoquées plus haut, les constructeurs automobiles déploient des mesures innovantes pour la cybersécurité. Ces efforts visent à protéger efficacement les véhicules contre les cybermenaces tout au long de leur cycle de vie.

- L'adoption de **systèmes de chiffrement avancés, comme l'Advanced Encryption Standard (AES)**, sécurise les communications vitales. Parallèlement, comme préconisé par l'ONU, les mises à jour logicielles à distance (OTA) permettent une réponse rapide aux vulnérabilités, sans intervention physique.
- **Les Systèmes de Détection d'Intrusion (IDS)** surveillent les activités du système pour identifier et contrer les tentatives d'attaques, tandis que la segmentation des réseaux internes isole les fonctions critiques des moins sensibles, réduisant le risque d'exploitation des vulnérabilités.
- En complément, **l'utilisation de l'intelligence artificielle** aide à détecter les schémas d'attaque, renforçant la prévention contre les menaces émergentes.
- L'engagement vers une cybersécurité proactive se manifeste aussi dans **la sensibilisation des utilisateurs**, les informant des bonnes pratiques pour minimiser les risques.

Ces initiatives illustrent l'engagement des constructeurs à suivre et surpasser les standards de cybersécurité, combinant conformité réglementaire et innovation pour assurer la sécurité des véhicules connectés dans un environnement numérique en évolution.

Dans un contexte où la connectivité dans la mobilité connaît une croissance fulgurante, l'importance de la cybersécurité devient plus évidente que jamais. Les risques liés à la sécurité des données et des infrastructures dans ce secteur en pleine expansion ont poussé les acteurs clés à prendre des mesures significatives pour contrer les menaces croissantes. Les entreprises, les régulateurs et les organismes de normalisation travaillent de concert pour élaborer des solutions robustes et adaptatives qui garantissent la sécurité et la protection des utilisateurs et de leurs données.

Emergence de nouveaux acteurs / startups spécialisé.es dans la cybersécurité automobile



Source : Expleo

Parmi les réponses apportées, nous observons l'émergence et le développement de sociétés spécialisées dans la cybersécurité automobile, telles que Argus Cyber Security, C2A Security, Upstream Security, GuardKnox, ProvenRun, ou encore SAIFLOW. Ces entreprises apportent des innovations technologiques cruciales et des solutions de cybersécurité sur mesure pour répondre efficacement aux défis uniques posés par l'ère des véhicules connectés.

Argus Cyber Security, acquis par Continental en 2017 pour 450 millions de dollars, illustre parfaitement l'intégration de solutions de cybersécurité avancées dans l'industrie automobile. Cette société collabore étroitement avec des constructeurs automobiles de renom pour y intégrer ses solutions de sécurité. De même, C2A Security, met en avant des partenariats avec AUTOSAR pour l'élaboration de normes de cybersécurité et avec Valeo pour renforcer la sécurité des systèmes automobiles en intégrant ses **solutions de sécurité directement au niveau du matériel**. De son côté, Upstream Security s'est **associée à plusieurs plateformes cloud majeures pour renforcer la surveillance et la sécurité des données des véhicules connectés à distance**. Ces collaborations illustrent parfaitement comment les sociétés de cybersécurité automobile

travaillent de concert avec les acteurs traditionnels du secteur et les innovateurs technologiques pour répondre aux défis uniques posés par l'ère des véhicules connectés.

Ces startups qui s'imposent comme des acteurs incontournables de l'écosystème sont suivies de plus en plus près par les sociétés historiques du secteur. D'après des projections récentes réalisées par Mc Kinsey, l'importance accrue de la cybersécurité dans le secteur automobile devrait entraîner une augmentation considérable des investissements, **passant de 4,9 milliards de dollars en 2020 à près de 9,7 milliards de dollars d'ici 2030**. Cette croissance sera largement soutenue par l'adoption de nouveaux règlements établis par les Nations Unies, qui encourageront une dynamique d'innovation. Ce contexte législatif ouvre de nouvelles perspectives économiques, notamment pour les fournisseurs de l'industrie automobile, les entreprises technologiques et les start-ups spécialisées, particulièrement dans les domaines du développement de logiciels et des services associés.

En forgeant des liens avec des entreprises de premier plan et des entités gouvernementales, ces startups renforcent l'écosystème global de la mobilité, positionnant **le marché de la cybersécurité automobile comme un domaine d'investissement de plus en plus attractif**. Avec la montée des enjeux liés à la protection des données et à la sécurité routière dans un monde connecté, ces partenariats stratégiques mettent en lumière l'urgence et l'importance d'investir dans des solutions avancées de cybersécurité, annonçant un avenir prometteur pour le secteur.

Un secteur prometteur pour les investisseurs

Je suis persuadé que le marché de la cybersécurité dans la mobilité représente un véritable marché d'avenir, promettant de nombreuses opportunités d'investissement. La demande pour des solutions de protection des données et la sécurisation des systèmes de mobilité ne cesse de croître, rendant ce secteur particulièrement attractif pour les investisseurs à la recherche de domaines porteurs. La protection des données, au cœur des préoccupations des utilisateurs et des fabricants, devient un enjeu majeur qui définit la valeur et la compétitivité des solutions de mobilité sur le marché.

Je garde un œil attentif sur ce marché, convaincus de son potentiel significatif. La cybersécurité automobile ne se limite pas à un enjeu de protection ; elle représente **une opportunité d'innovation et de différenciation** dans un secteur en constante évolution. Les sociétés qui se sont développées dans ce domaine au cours des dernières années, en particulier en Israël, leader reconnu dans l'innovation de la cybersécurité, illustrent la dynamique et le potentiel de croissance de ce marché.

En conclusion, l'investissement dans la cybersécurité automobile s'annonce comme une démarche stratégique pour anticiper les besoins futurs de la mobilité connectée et assurer une avance technologique dans le domaine. **La capacité à protéger efficacement les données et les systèmes sera un facteur clé du succès dans l'ère de la mobilité intelligente et connectée**, offrant des opportunités sans précédent pour les investisseurs visionnaires prêts à contribuer à façonner l'avenir de la mobilité.

Nous contacter :

rlafitte@via-id.com

Romain Lafitte

Écrit par Romain LAFITTE
Managing Director chez Via ID

Découvrez notre site internet :

www.via-id.com

Suivez-nous sur les réseaux sociaux !