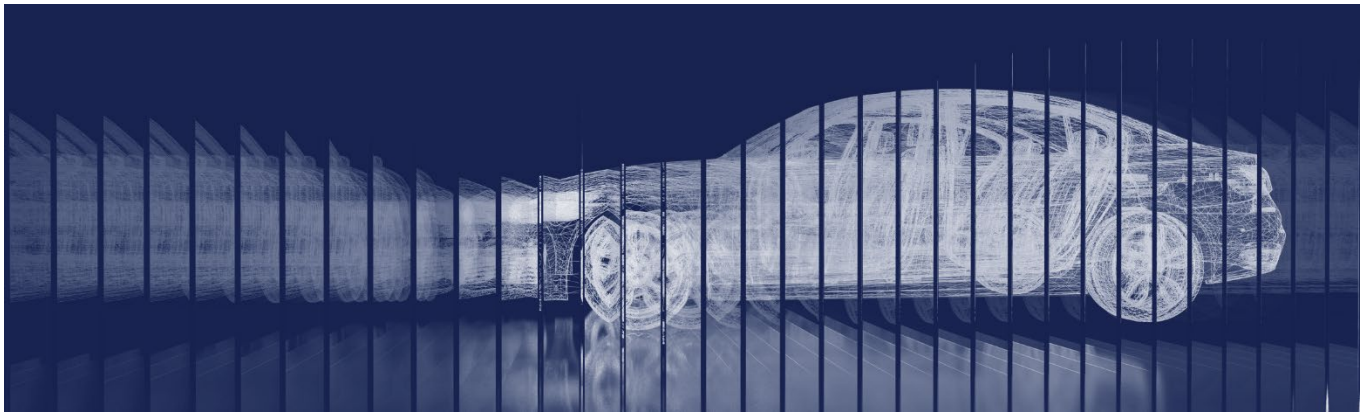
The Protected Connected Car

David A. Hoffman Steed Family Professor of the Practice of Cybersecurity Policy at Duke University



June, 2024

AMERICAN CAR RENTAL ASSOCIATION

Executive Summary

Operators of fleets of vehicles as owners of the cars should be able to control the data they produce. As operators of fleets of vehicles own their cars, they should also own and be able to fully control the data that is produced during vehicle operation.

But the car owners may not be able to get access to usable data from their vehicles to provide reasonable cybersecurity protections. The extent to which car manufacturers will grant usable access to telemetry data owned by fleet operators remains uncertain. This uncertainty raises significant concerns due to fleet owners' need for real-time access to the data they own so they can effectively protect their networks, the vehicles, and their customers.

Vehicles are increasingly connected to each other and central computing networks and produce increasingly useful and informative data. These connected vehicles employ many different sensors and data collection capabilities that describe the operation of the vehicles, the environments in which they drive, and the individuals with whom they come into contact including the driver, passengers and pedestrians. Modern cars are connected to digital networks in numerous ways, and these network "endpoints" create both cybersecurity vulnerabilities and access to data that is vital to securing an owner's network.

That data has privacy implications and can help reduce cybersecurity risks. The increasing presence of advanced computing power and connected arrays of sensors in cars introduces both privacy and cybersecurity challenges for fleet owners, as well as opportunities to use data to better protect their networks. Targeted attacks on individual vehicles can compromise critical driving systems and increase costs, and the potential to leverage a compromised vehicle to breach broader IT networks can threaten an entire fleet. However, the connected car also offers a unique source of telemetry data, aiding in the identification of potential cyber threats and its analysis contributing to overall network cybersecurity.

Fleet owners have unique cybersecurity risks and needs for access to usable data.
Cyberattacks can disproportionately impact fleet owners by increasing their maintenance costs, disrupting operations, decreasing consumer satisfaction, exposing personal data, and stealing sensitive corporate information. To manage the vulnerabilities inherent throughout an extensive network, owners require manufacturers and vendors to provide access to sufficient telemetry data to make informed decisions on patching, updates, or component replacement. For example, a cyberattack that disrupts a tire pressure reader can decrease the lifespan of the car, incurring costs for the owners while potentially creating additional revenue for car manufacturers.

Access to vehicle telemetry data is particularly important. Usable telemetry data is essential for effective cybersecurity risk management. Organizations, especially fleet owners, must gather and utilize telemetry data from endpoints to develop tailored and robust security practices. As the sensors and computing inside connected cars continue to evolve, the integration of advanced analytics and artificial intelligence solutions will become pivotal in leveraging telemetry data for real-time insights and proactive cybersecurity measures. Access to telemetry data will also help owners unlock the potential of Artificial Intelligence (AI) services that improve endpoint detection and response (EDR) to protect vehicles against evolving cyber threats.

The Protected Connected Car[1]

David A. Hoffman Steed Family Professor of the Practice of Cybersecurity Policy at Duke University

Abstract:

As operators of fleets of vehicles own their cars, they should also own and be able to fully control the data that is produced during vehicle operation. The increasing presence of advanced computing power and connected arrays of sensors in cars introduces both privacy and cybersecurity challenges for fleet owners, as well as opportunities to use data to better protect their networks. Targeted attacks on individual vehicles can compromise critical driving systems and increase costs, and the potential to leverage a compromised vehicle to breach broader IT networks can threaten an entire fleet. However, the connected car also offers a unique source of telemetry data, aiding in the identification of potential cyber threats and its analysis contributing to overall network cybersecurity. Despite the potential benefits, the extent to which car manufacturers will grant usable access to telemetry data owned by fleet operators remains uncertain. This uncertainty raises significant concerns due to fleet owners' need for real-time access to the data they own so they can effectively protect their networks, the vehicles, and their customers.

Modern cars are connected to digital networks in numerous ways, and these network "endpoints" create both cybersecurity vulnerabilities and access to data that is vital to securing an owner's network. The relationships between car manufacturers, component vendors, fleet owners, and data analytics providers shape how owners address their vulnerabilities by influencing which actor has access to which data at what times. Connected cars generate various types of data, ranging from operational metrics to sensitive information about drivers, passengers, and the environment. These data are controlled by different entities along a vehicle's supply chain and provide different value to owners, manufacturers, and vendors. A manufacturer might control data needed by an owner to secure their network, but have little incentive to share access.

Access to usable telemetry data is essential for effective cybersecurity risk management. Organizations, especially fleet owners, must gather and utilize telemetry data from endpoints to develop tailored and robust security practices. As the sensors and computing inside connected cars continue to evolve, the integration of advanced analytics and artificial intelligence solutions will become pivotal in leveraging telemetry data for real-time insights and proactive cybersecurity measures.

Rental car owners have an obligation to invest in the privacy and cybersecurity of their networks. Established privacy and data protection laws require organizations to implement "reasonable security safeguards" for data protection. The Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework underline the importance of usable telemetry data in identifying, protecting, detecting, responding to, and recovering from cybersecurity threats.

Connected car owners face unique challenges in mitigating cybersecurity risks. Cyberattacks can disproportionately impact fleet owners by increasing their maintenance costs, disrupting operations, decreasing consumer satisfaction, exposing personal data, and stealing sensitive corporate information. To manage the vulnerabilities inherent throughout an extensive network, owners require manufacturers and vendors to provide access to sufficient telemetry data to make informed decisions on patching, updates, or component replacement. The relationships governing data access between car manufacturers, vendors, and owners are thus critically important to owners like rental car companies. Additionally, owners and manufacturers might not

[1] Support for the research and preparation of this independent assessment of connected cars' data flows and related cybersecurity issues was provided by the American Car Rental Association. https://www.acraorg.com/. Views presented are solely those of the author unless otherwise noted

have the same incentive to safeguard different vehicle systems. For example, a cyberattack that disrupts a tire pressure reader can decrease the lifespan of the car, incurring costs for the owners while potentially creating additional revenue for car manufacturers.

Access to telemetry data will also help owners unlock the potential of Artificial Intelligence (AI) services that improve endpoint detection and response (EDR) to protect vehicles against evolving cyber threats. Integrating AI-driven EDR services, often through cloud-based platforms, will help owners proactively detect, respond to, and prevent cyberattacks, given sufficient telemetry data. AI will play an increasing role in threat hunting, vulnerability detection, and defense against ransomware attacks, providing owners with real -time insights to make informed decisions and choose cybersecurity solutions tailored to their specific risk exposure.

Owners of connected car fleets must have access to usable vehicle telemetry to ensure comprehensive cybersecurity protection. The integration of cloud-based AI services is essential for Owners to defend against cyber threats, maintain regulatory compliance, and demonstrate the implementation of reasonable cybersecurity safeguards. The concept of the "protected connected car" emerges as a key objective, emphasizing the pivotal role of usable access to telemetry data in securing vehicles, data, and the safety of individuals associated with connected cars.

Introduction

Rental car fleet operators must be able to control the data that is produced by the vehicles they own in order to protect their highly connected fleets from privacy and cybersecurity risks. Modern vehicles now include a variety of technologies including sensors that analyze what happens inside cars, outside cars, and how cars are running. Vehicle manufacturers and owners can access much of this data. There are also an increasing number of methods to connect to cars, including using the internet. Due to this increased connectivity, cars that operate as part of commercial fleets have become endpoints of the company IT networks, like phones, servers, and laptops.

As with any network endpoint, connected cars can create privacy and cybersecurity risks for fleet operators in two ways. First, malicious actors can attack specific vehicles to impact their operations or steal their data. Second, once gaining access to cars attackers can use the vehicles' connectivity to attack the overall network. However, connected cars can also be useful in protecting against cybersecurity attacks. Network cybersecurity depends on gathering and analyzing data from endpoints to help defend against attacks. Connected cars create useful data to understand when a malicious actor may be preparing for an attack. Therefore, connected cars create both cybersecurity risk, and the data from them can be used by fleet owners to protect their overall network. It is important to note that cyberattacks can also impact drivers. Attacks that compromise personal data such as a driver's location history, contacts, and conversations pose serious privacy and safety concerns for individuals. Companies who directly engage with the drivers will need to help protect them from those risks.

Rental car companies are an example of the type of fleet owner that requires the ability to access usable vehicle telemetry and to provide that data to cybersecurity service providers. New cloud-based cybersecurity services utilizing artificial intelligence are coming to the market. Fleet owners will not just need usable access to vehicle data but will need to provide real-time access to these service providers to deliver robust cybersecurity protections for drivers, passengers, and the company itself.

There are no guarantees, however, that car manufacturers will provide enough access to usable telemetry to fleet owners. There are several different individuals and entities that play roles with the connected car, such as the manufacturer and service providers. Those roles may provide them with access to data produced by the fleet owner's vehicles. Depending upon

commercial relationships, there may not be sufficient market incentives to make certain the entity that most needs usable access to the data to provide greater cybersecurity will be able to demand that access. For example, cyberattacks that diminish the user experience for drivers or obstruct owners' ability to monitor their fleet may create significant risks for owners and require data controlled by vendors or manufaturers who do not have sufficient incentives to provide usable access.

What is the Connected Car?

Advanced Computing, Sensors and Data

The connected car has arrived. With it comes increased concerns about how to provide adequate cybersecurity to protect vehicles, drivers, passengers, and the information technology networks of companies which operate fleets of vehicles.

Cars have seen dramatic changes over the past few years with the inclusion of advanced computing power and a variety of sensors to collect information to assist with driving, provide better customer service, enhanced entertainment experiences, and enhance safety for the driver, passengers, and pedestrians.[2] These new features include lane and braking assistance, passenger internet connectivity, GPS aided directions, satellite radio, and automated roadside assistance. Modern vehicles include thousands of semiconductor chips running a wide variety of software that analyzes data gathered by sensors that monitor the environment surrounding the car, and other sensors that measure different aspects of the car's performance.

The external environment sensors range from cameras to LiDAR (light detection and ranging) to RADAR.[3] The sensors that measure aspects of vehicle operations include those analyzing oxygen level in exhaust, air intake level, air intake temperature, engine oil level, engine oil pressure, coolant temperature, coolant level, tire pressure, battery level, and throttle position.[4] These sensors create a large amount of useful data to understand how the car is operating.

Along with the data collected by these environment and operational sensors there are other categories of information that connected vehicles increasingly collect. For example, new safety capabilities will require vehicles to communicate with each other, and with infrastructure, such as traffic lights, lane markers, and road signs, to know what is ahead on the road.[5] Those categories of data include information about the driver, passengers, pedestrians, and the environment outside the vehicle. For example, data about the driver can include information about the individual's use of the vehicle.[6] It can also include seat adjustments, conversations, video from inside the vehicle, and entertainment choices. Advanced analytics and potential combinations of the information with other data sources can provide insight into sensitive areas about the driver such as where the person travels, their health status, and their political affiliation (by for example noting changes in the way that individual sits in their seat or by access to entertainment choices). The vehicle may obtain similar sensitive data about passengers and pedestrians. The ability for data from connected cars to reveal sensitive insights into drivers and passengers highlights the need for fleet owners to secure this data from unauthorized access so as to best protect their customers.

The connected car also offers an increasing number of methods for data to be imported or exported from the vehicle. Traditionally, vehicles used on-board diagnostics (OBD) to inform repair technicians on what may need attention in the car.[7] OBD gives technicians access to subsystem information for the purpose of performance monitoring and analyzing repair needs.

---

[2] https://www.acko.com/car-guide/connected-cars-features-benefits/
[3] https://www.foresightauto.com/an-overview-of-autonomous-sensors-lidar-radar-and-cameras/
[4] https://autochimps.com/car-sensors/
[5] https://www.techtarget.com/whatis/definition/vehicle-to-infrastructure-V2I-or-V2X#:~:text=Vehicle%2Dto%2Dinfrastructure%20(V2I,streetlights%2C%20signage%20and%20parking%20meters
[6] https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/
[7] https://www.noregon.com/what-is-obd/

Since the 1980s the On-Board Diagnostics Port (OBD Port) has provided repair technicians with a simple way to test emissions data for compliance with state and federal laws.[8] Over time, the OBD port (now in its second generation and called OBD-II Port) allows for access to a wide variety of information that explains how aspects of the vehicle are performing, including speed, pedal position, spark advance, and coolant temperature. [9][10]

The OBD-II Port can be found in a variety of locations in different vehicles, but primarily near the steering column and underneath the dashboard. The port includes 16 pins which an OBD-II scanner can access to collect information.[11] Vehicle manufacturers make scanners available to their dealerships, and aftermarket scanners are available for purchase for under $200 by vehicle owners to access information to assist them with the repair of the vehicles.[12] In addition to the OBD-II Port, the modern connected car has additional ways to transmit data to or from the vehicle. These data transmission methods include WiFi, Bluetooth, USB ports, cellular network access, and satellite connectivity.[13] While vehicle owners have had access to data through the OBD-II Port, it is unclear the extent they will have access to information transmitted through these other mechanisms. This potential lack of future access may restrict the ability for fleet owners to have usable access to data they own.

The intersection of increased vehicle sensors, new methods to transmit data to and from the vehicle, and inferences from advanced analytics can provide tremendous insight to make driving more enjoyable and safer. However, as with any computing platform, integrating more technology increases the risk of cybersecurity attacks.[14] The variety of devices integrated into a connected car, and the software running on them, results in a greater available attack surface for malicious actors. Fortunately, the data created by the computing devices in the modern car is also useful, and increasingly necessary, to provide robust cybersecurity as analysis of it reveals suspicious or anomalous device behavior. For companies that operate fleets of vehicles, such as rental car companies, the individual cars operate in a distributed information technology network, like phones and laptops used by employees of all large companies. Protecting the vehicles from cybersecurity attacks is a critical objective for any fleet owner. Fleet owner access to usable data from the vehicle is a foundational element for that protection.

Connected Car Roles

Owners of connected cars are only one of many groups which come into contact with the data from the owners' vehicles. Much like other computing platforms, the connected car increasingly brings together various individuals and companies throughout its lifecycle, spanning from development to the end user's experience of driving a vehicle on the roads. To understand how the market left to itself may not provide the Owners with enough useful access to their own data to provide robust cybersecurity protections it is important to differentiate between:

The car manufacturer *(the Original Equipment Manufacturer (OEM))*
The vehicle purchaser *(the Owner)*
Component vendors to the OEM *(the OEM Supplier)*
Owner data analytics vendors *(the Owner Vendor)*

[8] https://ww2.arb.ca.gov/resources/fact-sheets/board-diagnostic-ii-obd-ii-systems-fact-sheet
[9] https://www.geotab.com/white-paper/vehicle-privacy-security/
[10] https://www.obdsol.com/knowledgebase/on-board-diagnostics/what-data-is-available-from-obd/#:~:text=OBD%2DII%20offers%20a%20standard,Emission%20readiness%20status
[11] https://www.autopi.io/blog/what-is-obd-2/
[12] https://www.tomsguide.com/best-picks/best-obd2-scanners
[13] https://www.mdpi.com/1424-8220/21/22/7712
[14] https://www.researchgate.net/publication/314272204_Cyber_Threats_Facing_Autonomous_and_Connected_Vehicles_Future_Challenges

Individuals in the vehicle *(the Driver or the Passenger)*

The OEM – The car manufacturer assembles components from suppliers and sells the vehicle to an owner.

The Owner – This can be an individual or an entity that operates a fleet of vehicles. State and local government organizations are examples of Owners which operate many purchased vehicles for which they are responsible for the maintenance and repair, as well as the safety of the drivers. Rental car companies, companies and government agencies all maintain fleets of vehicles. In situations where the government or a rental car company owns the vehicle, the Owner has the direct relationship with Driver instead of the OEM.

OEM Supplier – OEMs primarily assemble vehicles from components they do not make themselves. The computing hardware, software, and sensors in a connected vehicle are often developed, sold and serviced by companies with which the OEM contracts for products and services. The OEM will likely have vendors that supply hardware, software and services that will be deployed in the vehicle, in the data center, or from a cloud services provider to analyze data created by connected cars. These companies often provide ongoing services for this technology, including data analysis and the provision of software security updates. It may be the same suppliers providing services for vehicles sold to retail customers and to fleet owners, even though fleet owners will have a need to contract with their own suppliers such as cybersecurity services companies.

Owner Vendor – Effective operation of a fleet of vehicles requires data analysis about the condition of the cars and how they are used. The result of this analysis allows the Owner to increase customer satisfaction, maintain vehicle safety and maximize operational efficiency. To do so in a competitive market, the Owner often will need to contract with best in class and innovative data analytics vendors to provide insight from the information. These Owner Vendors may provide software and services onsite at the Owner's facilities, but increasingly, especially with cybersecurity analytics vendors, they will provide these services through real time data transmission from cloud services providers.

Driver and Passenger – In situations where the driver or passenger is not the Owner of the vehicle, they likely have little to no relationship with the OEM. Instead, their engagement is primarily with the Owner and their expectation is that the Owner will be accountable to them for their driving experience. This experience includes not just safety, but also ease of use, comfort, enjoyment, and efficiency.

Categories of Connected Car Data

As noted above, connected cars capture data about the vehicle, the driver, passengers, other cars, pedestrians, and the environment in which cars travel (temperature, air quality and road condition). All of these categories of data are a valuable resource to train artificial intelligence algorithms for products and services for connected car customers.[15] These categories of data present different risks. Cybersecurity attacks that change vehicle data can create safety issues and damage to the car. Theft of data relating to the driver, passengers, individuals in other cars, and pedestrians can reveal sensitive personal information.[16] There are both business and legal reasons to protect this information. Applying artificial intelligence solutions and advanced analytics to the data may provide firms a competitive edge. Securing data collected on Drivers or Passengers, meanwhile, is essential to preventing harm from malicious uses of their information.

[15] https://www.visteon.com/machine-learning-algorithms-in-autonomous-cars/
[16] https://www.autopi.io/blog/the-meaning-of-vehicle-data/

Telemetry Data is Particularly Valuable

Telemetry is the aggregation of data from remote sources to better understand a system's performance.[17] Telemetry involves taking data from many different decentralized sources and bringing it to a central system so that advanced analytics can gain insight from patterns or anomalies. Doing this allows firms to gain a comprehensive view of their systems which means they can preemptively identify weak points, early onsets of issues, or escalating problems. Telemetry is also useful for postmortems after an attack/breach to identify what went wrong, how, and what an organization should do to protect against further attacks.

Telemetry provides insight into the functioning of an organization's applications and systems. The distributed computing systems outside of the datacenter are often referred to as "endpoints". Endpoint computing devices include desktops, laptops, smartphones, tablets, servers, workstations, and Internet-of-things (IoT) devices.[18] Analyzing this endpoint telemetry data enables IT departments in many industries to understand potential malicious activities and identify patterns of threats.

Example 1 – Endpoint Telemetry in Healthcare

Healthcare providers routinely collect endpoint telemetry for cybersecurity.[19] Patient monitoring devices and internet connected medical equipment, such as scales, thermometers, wearable health trackers or medical sensors, are considered endpoints that produce valuable telemetry data.[20] These distributed devices collect particularly sensitive patient information including vital signs, sleep monitoring, menstrual cycle tracking, and physical activity levels. These devices also create useful telemetry data to demonstrate how well they are operating.[21] As noted above, the telemetry is crucial to defend against malicious actors and protect the sensitive patient data created by the devices.

Example 2 – Endpoint Telemetry in Manufacturing

Large manufacturing enterprises increasingly use connected Internet of Things (IoT) and Operational Technology (OT) devices which produce valuable telemetry.[22] Even for OT devices that are not connected to the internet there are cybersecurity risks from individuals who gain physical access to the system and load malware through mechanisms like the use of USB drives.[23] Cybersecurity experts increasingly view usable access to the telemetry data from these manufacturing IoT and OT devices as a critical component of providing cybersecurity protection for the overall manufacturing facility and network.[24][25]

For Owners of fleets of vehicles, the individual car is an endpoint that produces substantial amounts of useful telemetry.[26] Connected car telemetry is a valuable tool to gain a better understanding of the car's performance and usage.[27]

Vehicle OEMs recognize the criticality of usable access to telemetry data from the vehicle. For example, Tesla's user manual outlines this practice:

[17] https://www.splunk.com/en_us/blog/learn/what-is-telemetry.html
[18] https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint#:~:text=An%20endpoint%20is%20a%20remote,Laptops
[19] https://www.gehealthcare.com/insights/article/managing-clinical-it-and-telemetry-infrastructure
[20] https://nationaltelemetryassociation.org/how-telemetry-is-changing-in-todays-health-care-system/
[21] Id.
[22] https://www.databricks.com/blog/2023/03/01/cybersecurity-manufacturing.html
[23] Id
[24] https://www.tualcom.com/telemetry-and-remote-monitoring-the-future-of-industrial-processes/
[25] https://verveindustrial.com/resources/blog/adapting-xdr-for-ot-cybersecurity/
[26] https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/mobile-internet/driving-profits-from-connected-vehicles.pdf
[27] https://www.autopi.io/blog/the-meaning-of-vehicle-data/

> "Model 3 is equipped with electronic modules that monitor and record data from various vehicle systems, including the motor, Autopilot components, Battery, braking and electrical systems. The electronic modules record information about various driving and vehicle conditions, including braking, acceleration, trip and other related information regarding your vehicle. These modules also record information about the vehicle's features such as charging events and status, the enabling/disabling of various systems, diagnostic trouble codes, VIN, speed, direction and location.
>
> The data is stored by the vehicle and may be accessed, used and stored by Tesla service technicians during vehicle servicing or periodically transmitted to Tesla wirelessly through the vehicle's telematics system. This data may be used by Tesla for various purposes, including, but not limited to: providing you with Tesla telematics services; troubleshooting; evaluation of your vehicle's quality, functionality and performance; analysis and research by Tesla and its partners for the improvement and design of our vehicles and systems; to defend Tesla; and as otherwise may be required by law. In servicing your vehicle, Tesla can potentially resolve issues remotely simply by reviewing your vehicle's data log.[28]"

Cybersecurity and Connected Cars

The Requirement to Provide "Reasonable Security"

Having usable access to data brings with it obligations to protect that information. Cybersecurity protections are necessary to protect confidentiality, integrity, and availability of networks and computing devices. Failure to provide adequate cybersecurity can create risks to the organization, to individuals using those devices, and to the people to whom the data relates.

Privacy and data protection laws generally place cybersecurity responsibility on the organization in direct relationship with the individual to whom the data relates. Many of these laws and enforcement regimes require organizations to take "reasonable security safeguards" to protect data and systems. In the privacy and data protection area many of these requirements track back to the 1980 OECD Guidelines on the Protection of Privacy and the Transborder Flow of Data[29], which were the first internationally recognized set of privacy principles for use by countries to form the foundation for national legislation.[30] Privacy experts have referred to the eight OECD principles at the core of the guidelines as "the common global language of privacy.[31]" One of the eight principles is "Security Safeguards". The OECD's definition of that principle states, "[p]ersonal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."

Over the past four decades many legislatures and regulators, including many states, have incorporated the concept of "reasonable security safeguards" into privacy and data protection requirements.[32] For example, California's state privacy law requires, "[a] business that collects a consumer's personal information shall implement reasonable security procedures and

[28] https://www.tesla.com/ownersmanual/model3/en_au/GUID-2E8E5E0B-DAA8-40B8-9804-45F5960538DF.html#:~:text=Vehicle%20Telematics&text=The%20data%20is%20stored%20by,through%20the%20vehicle's%20telematics%20system.
[29] OECD (2002), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en.
[30] https://www.oecd.org/general/data-protection.htm
[31] https://www.worldprivacyforum.org/2021/05/from-the-filing-cabinet-to-the-cloud-updating-the-privacy-act-of-1974/
[32] https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/reasonable-data-security-measures/

practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure." [33]

The U.S. Federal Trade Commission (FTC) is the primary U.S. federal consumer protection regulator. One of the legal provisions the FTC enforces is Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." [34] The FTC states on its website, "(t)he FTC has brought legal actions against organizations that have violated consumers' privacy rights or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury."[35]

As a result of the examples above, and many other laws and regulatory requirements, organizations need to implement cybersecurity programs that align with the evolving definition of "reasonable security safeguards." Access to usable device data is a fundamental component of those programs.

It Takes Data to Protect Data

Companies in all industries rely upon their employees, customers, and vendors having access to computing devices. These endpoints include phones, laptop computers, desk workstations, industrial control systems, routers, switches and IoT devices such as cameras and motion sensors.[36] Those devices create a wide variety of data as they serve their computing functions. IT departments routinely use this data to remotely determine how individual endpoints perform and to understand whether there is anomalous behavior that may indicate cybersecurity attacks on hardware or software.

This collection of endpoint data allows network administrators to quickly detect problems, and to decrease the likelihood of those issues spreading through the network. Endpoint telemetry has been used for decades to better understand network operations and detect anomalous activity that would indicate cybersecurity attacks.

However, recently advanced analytics and artificial intelligence solutions have increased what can be done with endpoint data to provide for more robust cybersecurity. IT administrators now use telemetry to observe network traffic in real-time to monitor availability and performance. Some of these cybersecurity systems can automatically detect cybersecurity threats and separate individual devices to protect the rest of the network. Analysis of the data also provides insight into types of new threats and whether software updates are required for the device.

Adequate Cybersecurity Protection Requires Access to Usable Telemetry

In 2015, the FTC provided guidance on how to interpret the concept of reasonable security in its document, "Start with Security: A guide for business. Lessons learned from FTC cases."[37] That guidance specifically calls out the need to have the ability to segment the network and to use information to monitor for threats.[38] In its description of the need to monitor for threats, the guide refers to the FTC's consent orders with Dave & Buster's and Cardmember Solutions. The guide states, "In each of these cases, the businesses could have reduced the risk of a data compromise or its breadth by using tools to monitor activity on their networks."[39] The reference to the Dave and Buster's case is even more specific when it states the company "didn't monitor

[33] The California Consumer Privacy Act of 2018, Section 1798.100(e).
[34] 15 U.S.C. 45(a)(1)
[35] https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement
[36] https://www.techtarget.com/whatis/definition/telemetry
[37] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[38] Id. at pp. 7-8
[39] Id. at p.8

system logs for suspicious activity."[40] Usable access to telemetry data from endpoint devices is critical to monitor logs, detect suspicious activity, and to predict where attacks are likely in the future.

Telemetry's Role in the NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) further clarifies why organizations require access to telemetry information to protect their data and networks.[41] The CSF is a voluntary set of guidelines and best practices for mitigating cybersecurity risks. While the CSF is voluntary, countries around the world have referenced it as the recommended approach for managing cybersecurity risk. The framework provides a high-level, comprehensive, and flexible approach to cybersecurity risk management and is widely adopted across various industries. The CSF outlines five main functions for cybersecurity risk management processes: Identify, Protect, Detect, Respond, and Recover. This five-step framework provides a lens through which organizations can evaluate whether their internal program provides "reasonable security". It highlights fundamental tenets of cybersecurity practice and operations such as the importance of continuous adaptation to emerging threats, integration of cybersecurity risk management into organizational culture, emphasis on proactive measures, and an increased focus on supply chain security. Access to explainable and usable telemetry plays a crucial role in each of the five components of the framework.[42]

Identify: Telemetry is a useful tool for identifying potential threats, vulnerabilities, and risks. Telemetry provides insights into the security state of a server and devices, allowing organizations to better understand their cybersecurity state and better employ best practices for managing risks. Importantly, third-party vendors will face cybersecurity threats necessitating access to telemetry data for sufficient protection. The sharing of usable telemetry data provides a second line of defense in identifying cybersecurity threats, especially if the company relies upon the vendor's services to provide a good experience for the company's customers.[43]

Protect: Telemetry is used to enforce security controls and protect systems from threats. This use of telemetry includes implementing access controls, closely monitoring for malicious activity, and ensuring security applications are up to date.[44]

Detect: Organizations use telemetry to detect threat actors attempting to gain access to systems. Real-time monitoring of telemetry data helps organizations quickly identify malicious activity, impose additional access controls, and act immediately.[45]

Respond: Organizations use telemetry to respond to cyberattacks. Telemetry is useful to understand the impact of mitigation efforts and to protect against future risks. It provides detailed information about the attack which is critical to sufficiently addressing it.[46]

Recover: After a cyberattack has been addressed, telemetry provides data for a root-cause analysis and guides the system's restoration after an attack. Telemetry is used to evaluate the efficacy of recovery efforts and is the foundation for post-incident assessments. These reflective efforts improve resilience to mitigate against future attacks.[47]

[40] Id.
[41] https://www.nist.gov/cyberframework
[42] Id.
[43] Id.
[44] Id.
[45] Id.
[46] Id.
[47] Id.

Telemetry plays a critical role in each element of the CSF, underscoring the importance of Owners having access to the data. This access is crucial to protecting driver safety and their sensitive personal data.

When adhering to the CSF, gathering telemetry from the data center and network devices (such as routers and switches) is not enough for successful risk management; companies need telemetry specifically from endpoint devices to successfully mitigate potential cybersecurity risks. Endpoint data is the best way to analyze system status and have a more granular understanding of potential risks. This data allows for a more tailored approach, as general best practices are often not enough to deter more sophisticated attacks, especially on complex systems working with emerging technology like connected cars.

Telemetry plays a critical role in managing cybersecurity risk. Telemetry stands out as a crucial instrument in the battle against cyber threats, thanks to its capacity for real-time insights and its support for incident response and compliance monitoring. This is only achievable through gathering data at the endpoints. As organizations continue to grapple with the complexities of implementing cybersecurity, gathering and utilizing telemetry emerges as a key strategy for developing robust security practices that minimize risk.

On February 26, 2024, NIST published CSF 2.0.[48] This updated version of the framework puts particular focus on a new governance function as part of its core structure.[49] This governance focus places particular attention on organizational context, including roles and responsibilities across the supply chain.[50] The CSF 2.0 describes the governance function as "(t)he organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored." As part of the release of CSF 2.0, NIST also created implementation examples, including for the new governance function and with a focus on supply chain issues.[51] Various of those examples speak to the importance of understanding the roles of supplier and their access to data, including the statement of "Ex1: Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission."[52] As evidenced by NIST's modifications in CSF 2.0 it appears there is even more focus on companies understanding what data access they have to achieve the necessary outcomes of better protecting their organizations.

Cybersecurity Best Practices and Standards Require Access to Usable Telemetry

Similar to the FTC's security requirements many other laws provide only vague requirements that organizations provide "reasonable security".[53] Due to the vagueness in these legal requirements, a number of organizations and standards bodies have developed more specific guidance and best practices. These efforts highlight the importance of access to usable endpoint telemetry to protect devices, networks, and data with a focus on both threat detection and vulnerability management. Three important and representative examples of this guidance are the efforts from the U.S. Department of Homeland Security, the CIS Center for Information Security, and the International Organization for Standardization.

U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)

In consultation with industry, government, and substantive experts, CISA has developed a set of cybersecurity performance goals. Those goals make clear the need to have access to information to detect threats, and they state, "(o)rganizations

[48] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[49] Id. at p.3.
[50] Id.
[51] https://www.nist.gov/document/csf-20-implementation-examples-xlsx
[52] Id. at GV.SC-04 Ex. 1
[53] https://www.jdsupra.com/legalnews/let-s-be-reasonable-clearer-guidance-32633/

document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats."[54]

The goals also call out the need for effective cybersecurity vulnerability management with the inclusion of the statement, "(a)ll known exploited vulnerabilities (listed in CISA's Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first."[55]

CIS Center for Information Security (CIS)

CIS authored a set of best practices to assist in delivering robust cybersecurity known as the CIS Critical Security Controls.[56] CIS Control number 13 is Network Monitoring and Defense and encourages organizations to "(o)perate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base."[57] CIS Control number 7 is Continuous Vulnerability Management, and recommends an organization "(d)evelop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information."[58]

International Organization for Standardization (ISO)

ISO 27001:2022 is an ISO voluntary standard to provide guidance to organizations on how to identify cybersecurity risks and adopt controls to address them. Those practices are outlined in Annex A, which contains 114 controls divided into 14 areas. The implementation guidance for these controls makes clear the need to effectively manage endpoint computing devices to monitor them for malicious activity and to allow for the patching of vulnerabilities.

The implementation guidance for the Annex A 8.1 control calls for regular monitoring of endpoint devices when it states, "[i]nformation stored on, processed, or accessible via user endpoint devices should be protected. Annex A 8.8 makes clear the need to invest in protecting networks against internal and external exploitation of vulnerabilities."[59]

Each of these efforts makes clear that organizations must be able to both monitor endpoint devices and quickly react to effectively patch vulnerabilities on those machines. Connected car Owners need to have usable access to endpoint information to meet reasonable security expectations.

Owners Have Specific Needs to Address Cybersecurity Risks

The harms of cybersecurity risks and corresponding incentives to invest in protection are not shared evenly between Owners and OEMs. Researchers observed a significant increase in cybersecurity attacks on distributed endpoint technology such as internet of things devices.[60] Many of these attacks are enabled by increased use of vulnerability scanners to detect weaknesses in internet applications and application programming interfaces.[61] Connected car fleet owners are likely to face these types of distributed endpoint attacks. These attacks will impact Owners and OEMs differently, as an attack that takes vehicles out of

[54] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (3)
[55] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (1.E.)
[56] https://www.cisecurity.org/controls
[57] https://www.cisecurity.org/controls/network-monitoring-and-defense
[58] https://www.cisecurity.org/controls/continuous-vulnerability-management
[59] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection - Information security management systems (ISO Standard No. 27001:2022). https://www.iso.org/standard/27001
[60] https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the- education-sector/
[61] Id.

operation immediately and directly impacts the fleet owner's business, while OEMs most often will have time to address the vulnerability before seeing an impact on revenue.

Connected car Owners should not have to rely upon others to protect them from cybersecurity risk. Market forces and commercial relationships left to themselves will not in all situations incentivize OEMs to invest in sufficient endpoint security to mitigate the risks to Owners, Drivers, Passengers, and Pedestrians. Cyberattacks will often create risks and costs for Owners that are less impactful to OEMs. The unique impact of the risk to the Owner can significantly increase when the cyberattack is targeted at just the Owner's vehicles, instead of all vehicles of that model coming from an OEM. Owners must have the ability to quickly respond to cybersecurity attacks and proactively address vulnerabilities discovered in connected cars. Effective vulnerability management and cybersecurity operations for OEMs both require usable access to vehicle telemetry.

Vulnerability Management

As cars become increasingly connected, the increase in software running in the vehicle expands the "attack surface" and the likelihood for malicous actors to discover software vulnerabilities.[62] These vulnerabilities vary in significance and can impact organizations in different ways. The "criticality and urgency" of a threat can be subjective. A system vulnerability might impact an Owner and the OEM differently and similar vulnerability risk management programs may lead to different decisions by an Owner rather than an OEM on whether to patch a detected vulnerability.[63]

For example, vulnerabilities impacting sensors that assist with braking or staying in a lane can be especially hazardous. It is likely OEMs would prioritize patches to these safety or regulation compliance issues. Conversely, some software vulnerabilities are less likely to impact vehicle safety. Depending upon the amount of resources necessary to develop and test software patches, OEMs may deprioritize patches for vulnerabilities in vehicle components that primarily create inconveniences or costs for Owners, Drivers, and Passengers, such as vulnerability in the system used for fleet management. In other situations, patching may not be possible and risk management may require replacing certain vehicle components. Owners require usable telemetry to make these decisions.

Cybersecurity programs prioritize "identifying, classifying, remediating, and mitigating" vulnerabilities based on the evaluation of the level of risk.[64] Telemetry collected from endpoints is often a critical component of executing a comprehensive and successful vulnerability risk management program. Such a program usually contains four parts: identifying, evaluating, treating, and reporting.[65] This process allows an organization to identify and evaluate the harm of each system vulnerability as it is discovered.

The following are factors that are often used to determine the amount of resources an organization will place on developing a software patch.[66]

- **Patch Availability:** Not all identified vulnerabilities have patches to address them.
- **End-of-Life Software:** Some vulnerabilities are detected in systems that are no longer supported by a vendor, thus making a patch not possible.

[62] https://www.fortinet.com/resources/cyberglossary/attack-surface
[63] https://www.esecurityplanet.com/threats/vulnerability-patching/
[64] https://www.rapid7.com/fundamentals/vulnerability-management-program-framework/
[65] Id.
[66] Id.

- **Resource Constraints:** Organizations face staffing and budgetary constraints, which require prioritization based on the difficulty in developing the patch and their business needs.
- **Criticality and Urgency:** Some vulnerabilities are far more critical and urgent than others. However, assessing the criticality and urgency of a vulnerability depends on the perspective of the entity doing the evaluation and the determination of how much risk it creates.
- **Vendor Coordination:** Sometimes, companies cannot patch a vulnerability until vendor systems/software are updated; therefore, coordination between the Owner and Owner Suppliers is essential to address certain vulnerabilities.

Due to how vulnerabilities often impact OEMs and Owners differently, Owners need access to enough information to understand whether a vulnerability exists and the type and degree of impact it creates. With access to that information the Owner can determine the resources it should expend to either patch the vulnerability, request the OEM or an Owner Vendor to develop and supply the software update, or decide to replace certain software or hardware.

Usable access to vehicle telemetry will ensure Owners can conduct their own vulnerability risk management process and prioritize which vulnerabilities must be patched and on what timeline Owners engaging in the vulnerability assessment process benefits all parties by providing the necessary information to the right entity to best decrease cybersecurity risk. Telemetry data plays a critical role in safeguarding fleets, specifically for vulnerabilities that, if exposed, are a significantly higher priority for the fleet owner (and usually the customer) than for the car manufacturer.

Cybersecurity Operations and Attack Response

Not all cybersecurity attacks require the use of a vulnerability to gain access to the system. For example, company employees who already have access to systems can execute an insider attack. Similarly, malicious actors can use social engineering to trick employees into giving them access, such as a phishing email that appears to come from a work colleague. In these instances, access to usable data from endpoints is critical to allow an organization to respond quickly and effectively. The following are examples of where cyberattacks may disproportionately impact Owners vs. OEMs, and thereby demonstrate why Owners require usable access to vehicle telemetry.

Cyberattacks Can Create Increased Maintenance Costs for Vehicle Owners

One example of an attack that creates disproportionate risks for the Owner is an attack that impacts vehicle maintenance. As noted previously, a cyberattack can lead to inaccuracies in a tire pressure reader, resulting in tires wearing out prematurely and necessitating more frequent balancing. This will adversely affect the lifespan of the car, creating significant costs for the Owner while potentially creating additional revenue for the OEM. Other cyberattacks capable of causing a comparable impact include attacks targeting a vehicle's telematics, or an attack that changes the reading of the oil pressure in the vehicle. While such cyberattacks do not necessarily pose immediate customer safety concerns, they can cause significant financial impact to Owners. Reducing the need for maintenance and extending the life of a car uniquely benefits Owners while having at most an indirect impact on OEMs, and possibly being counter to their financial interests.

Cybersecurity Attacks Can Impact Fleet Operations

An attack that makes individual vehicles difficult to identify remotely will create challenges for the Owner’s fleet asset management. Owners rely heavily on accurate and real-time tracking of their cars for operational efficiency. In the event of such an attack, the Owner’s operations may be substantially impacted, leading to delays, insufficient resource allocation, and increased operational costs.

Cybersecurity Attacks Can Decrease Consumer Satisfaction

Another reason an Owner needs access to usable vehicle telemetry is that any cyberattack has the potential to harm the relationship between the Owner and their customer, in a way that may not impact the OEM to the same degree. An attack that affects the end-user experience can be detrimental to maintaining customer loyalty and future business. Inconveniences can become deciding factors influencing customer loyalty, especially in tight markets with competition from other fleet owners and ride-sharing companies.

Examples that don't pose immediate safety risks but can harm customer loyalty include cyberattacks to impact climate control manipulation, GPS tampering, smart key malfunction, and infotainment system disruption. The possibilities for these customer experience attacks are numerous with connected cars. As noted above, these impacts fall most directly on Owners, especially when the attacks target vehicles in a particular Owner's fleet rather than all cars of a specific model from the OEM. These types of attacks impose costs for which the Owner may want to expend resources to protect against them, or to quicky remediate them, while the OEM may not be similarly motivated.

Cybersecurity Attacks Can Impact Driver and Passenger Privacy

As noted above in the description of privacy and data protection laws, in the event of a cyberattack on a connected car, the Owner will often have direct responsibility for the protection of their customer's personal information. An attack on a connected car could provide access to a wide variety of sensitive personal information that relates to the Driver and Passengers. For example, an attack could exfiltrate contact folders from phones connected to the car entertainment system. The attack poses immediate privacy concerns not just for the Driver or Passenger, but also for their contacts. Obtaining that contact information could lead to phishing and social engineering attacks, identity theft, and financial scams. Another example of the impact to Driver and Passenger privacy is when a cyberattack records conversations or video from inside a connected car.

U.S. State data breach notification laws will often require the Owner to notify individuals and/or regulators of unauthorized access to personal data. Also, the Owner will likely be the entity regulators contact to investigate the breach, and to whom plaintiff's lawyers will direct lawsuits. Having access to usable telemetry from endpoint devices provides a defense to detect and prevent these attacks where the consequences of those attacks fall largely on the Owner.

Cybersecurity Attacks Can Obtain Owner Trade Secrets

Attacks can provide insight into an Owner's business operations that would have great value to competitors. Data from vehicles can provide insight into market demand, fleet management, and operational efficiency efforts. The Owner is the entity motivated to protect this valuable corporate information. Protecting against corporate cyber espionage and the theft of data that reveals trade secrets is another reason why the Owner cannot rely upon other entities to use vehicle telemetry to provide the best cybersecurity protection for the vehicle and the data it produces.

In summary, along with the need to effectively manage software and hardware vulnerabilities, the Owner is often the entity most incentivized to address cybersecurity risks in connected cars to mitigate a variety of risks to Drivers, Passengers and themselves.

Examples of Attacks that Disproportionately Impact Vehicle Owners

Example 1 – Single Owner Attacks – Attacks that impact the fleet of only one Owner. This impact to one Owner could be due to the unique configuration of systems and software because of the integration of a specific after-market entertainment or navigation system. It also could be that the threat actor is seeking to only impact one owner and in that situation the OEM may be less likely to detect the attack or may not prioritize addressing the issue.

Example 2 – The Driving Experience – Attacks that impact the driving/riding experience, but do not rise to the level of a safety concern. This category of attacks includes the ability to adjust temperature control systems in the car, the ability to control seat adjustments, and whether the onboard entertainment system functions properly.

Example 3 – Increased Operational and Maintenance Costs – Attacks may cause economic consequences for the Owner that do not directly impact the OEM. This category could include a vulnerability that leads to lower fuel economy for all vehicles in a rental car company's fleet.[67] Another example may be an attack that adjusts the performance of the vehicle to cause an increase in maintenance costs, such as decreasing the reliability of tire pressure readings or adjusting tire alignment.

Example 4 – Theft of Personal Data – Attacks may gain access to sensitive information about the Driver and/or the Passenger. Connected vehicle telemetry could gain insight into driving habits such as acceleration and braking habits.[68] This category could also include the ability to acquire data from devices such as personal phones that individuals connect to the vehicle or attacks that take control of cameras or microphones in the vehicle.

Artificial Intelligence Increases Telemetry Value for Owners

Owners increasingly have access to artificial intelligence enabled services that can make use of connected vehicle data to provide increased cybersecurity.

Endpoint Detection and Response to Protect Vehicles

This use of endpoint telemetry to detect and protect against cybersecurity threats is commonly known as endpoint detection and response (EDR).[69] Cybersecurity companies offer specific EDR products and services to gather telemetry, analyze the data, and make decisions based on what threats the analysis discovers.[70] IT departments use the insights from EDR products to identify suspicious endpoint activity and minimize threats and impacts of cyberattacks. Telemetry collected by EDR products and services allows for the detection of suspicious activity (preventing intrusions before they occur) and enables the robust investigation and patching of system vulnerabilities. Since 2013, EDR has been a core part of threat mitigation and has evolved from deployment of relatively simple antivirus capabilities to more advanced artificial intelligence implementations that analyze telemetry to predict future threats.[71]

[67] https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/mobile-internet/driving-profits- from-connected-vehicles.pdf
[68] https://www.autopi.io/blog/the-meaning-of-vehicle-data/
[69] https://www.paloaltonetworks.com/cyberpedia/what-is-end point-detection-and-response-edr
[70] https://www.paloaltonetworks.com/cyberpedia/what-is-end point-detection-and-response-edr
[71] https://www.paloaltonetworks.com/cyberpedia/what-is-end point-detection-and-response-edr

These EDR products and services also assist with software and hardware vulnerability management. Owner analysis of telemetry allows for the robust monitoring of system logs which can be used to identify misconfigurations or software that is not operating within its specifications. Owner access to telemetry is necessary not just to protect against attacks, but also to reduce the harm from successful attacks. Breaches are possible even within the most secure networks. Telemetry collected from endpoint devices allows for in-depth forensic analysis while a malicious actor is perpetrating the attack.[72] Advanced EDR systems allow for the network to isolate a particular device or number of devices and decrease the amount of the network at risk.

Utilizing Artificial Intelligence Tools to Defend Against Cyberattacks

EDR functionality is increasingly offered as a service available from companies utilizing commercial cloud computing providers. Direct data exchange and transfer between vehicles and cloud-based platforms or services provides greater access to EDR service for Owners. Cloud providers also allow for new cybersecurity services market entrants to quickly make their services broadly available. Both OEM Suppliers and Owner Vendors can utilize cloud computing providers to deliver these services. These cloud-based EDR services will be just a small segment of the overall group of cloud based analytics vendors to whom Owners should have access to not just improve their cybersecurity, but also to improve their operational efficiency and enhance the customer experience.

These services now use artificial intelligence to perform threat hunting, vulnerability detection, and to block incoming attacks. Ransomware continues to cause risks for organizations around the world.[73] For connected car Owners, ransomware creates the risk of not having access to the data from an entire fleet of vehicles, or to impact the operations of a specific vehicle.[74]

Cloud-based EDR services using artificial intelligence are now coming to the market to specifically address ransomware attacks.[75] Owners require real-time access to usable telemetry to contract with these innovative service providers. Relying on OEMs or other entities to determine which EDR providers to engage does not allow an Owner to choose the best solution for its specific risk exposure. Owners need full flexibility in selecting Owner Vendors to defend themselves, ensure compliance, and demonstrate to customers and regulators they are implementing reasonable cybersecurity safeguards.

Conclusion

Owners of fleets of connected cars require access to usable data from the vehicle to provide robust cybersecurity protection for their network, the vehicles, the data relating to Drivers and Passengers, and the safety of all individuals in contact with the vehicle while it is operating. Connected cars now utilize a wide diversity of sensors to collect data about the vehicle and the environment in which it is driven. This data also has privacy implications for Drivers, Passengers, and Pedestrians. Much of this information is also critical to provide robust cybersecurity as new products and services can analyze it to detect attacks and mitigate their impact. Those cybersecurity threats create unique risks for the Owners of the vehicle. Owners need to have the ability to mitigate risks to Drivers, Passengers, Pedestrians and themselves by having real-time access to data from the vehicle to engage with innovative new cybersecurity service providers utilizing cloud computing and artificial intelligence. Policy stakeholders should pursue providing Owners with rights to demand usable access to the data produced by the cars they own. With usable access to that information, the “connected car” can then be the “protected connected car.”

[72] https://www.sophos.com/en-us/cybersecurity-explained/telemetry
[73] https://securityandtechnology.org/ransomwaretaskforce/
[74] https://www.cybersecurity-insiders.com/connected-cars-are-vulnerable-to-ransomware-attacks/
[75] https://expel.com/solutions/ransomware-protection/