SECURING DATA IN CONNECTED VEHICLES

OUR TEAM

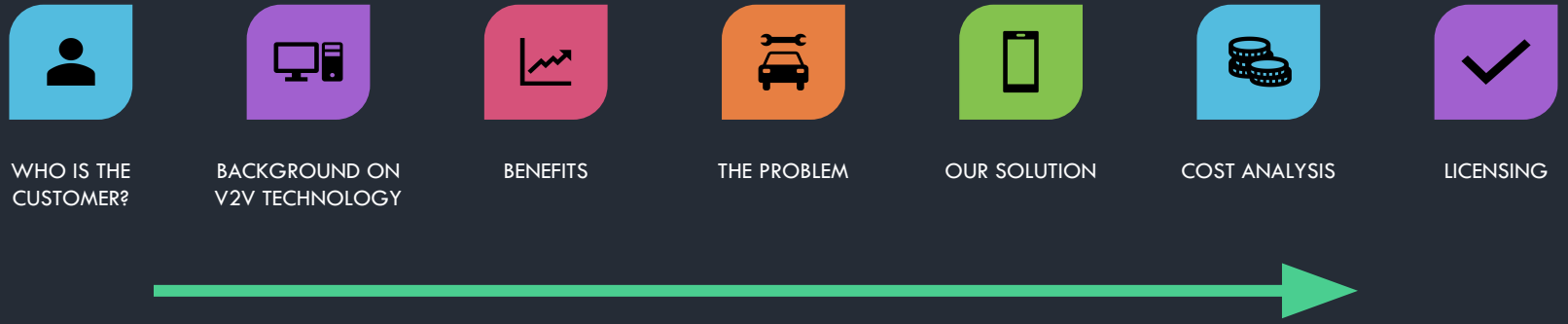
Minha Mir

Muhammed Mubeen

Youssef Clayb

Moeen El-Sharif

OVERVIEW


WHO IS THE CUSTOMER?
BACKGROUND ON V2V TECHNOLOGY
BENEFITS
THE PROBLEM
OUR SOLUTION
COST ANALYSIS
LICENSING

WHO IS THE CUSTOMER?

Electric Motor Vehicles 

Industry Leader of the best environmentally friendly automobiles

Producing the most reliable cars using ion batteries for the last decade

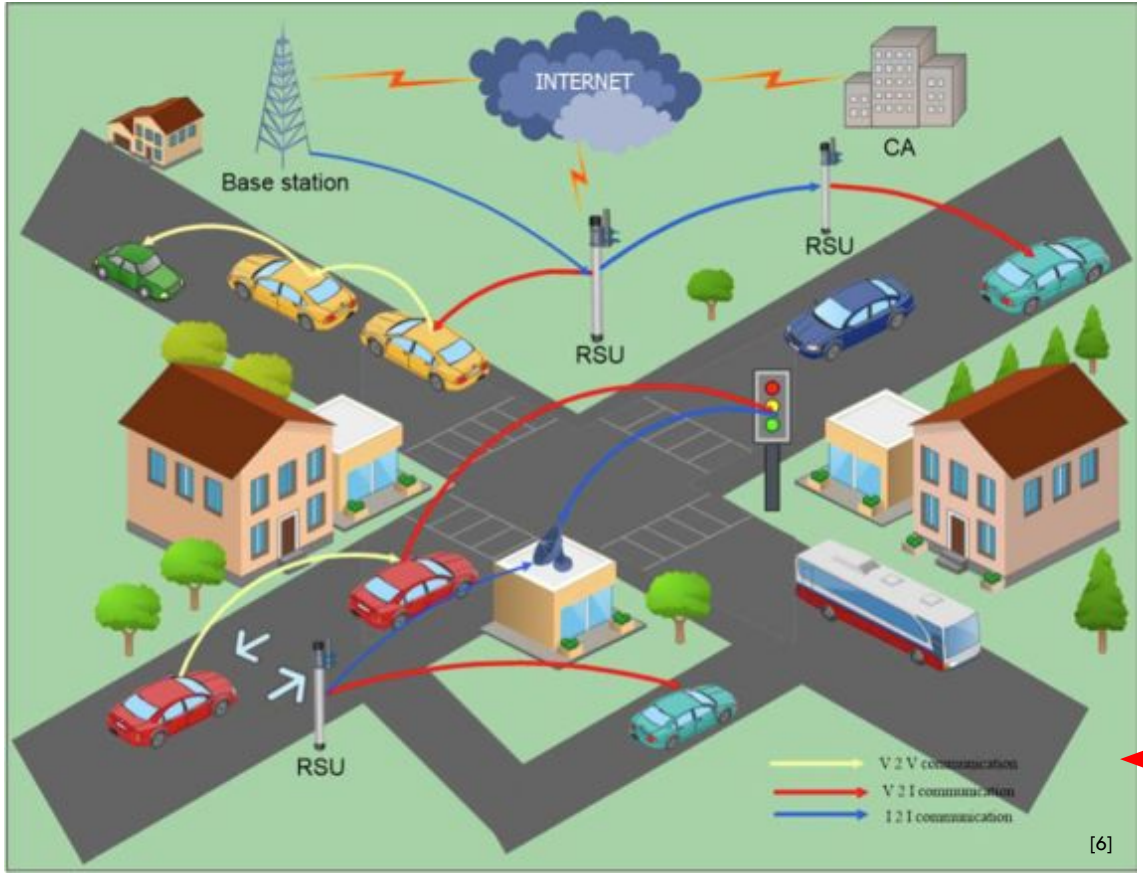
Owns 165 patents in the field of electric automobile industry

CONNECTED VEHICLES

- Communicate bidirectionally with other systems outside of the car.
  - Allows the car to share internet access, and hence data, with other devices both inside and outside the vehicle
- Vehicles are equipped with On-Board Units (OBUs) to communicate with each other and Road Side Units (RSUs) [6].
  - Validation and authentication of information exchange between the vehicles are a key concern for the traffic safety.
- Connected cars are a Data Mine and collect information about YOU, they need to be secured
- Due to their high mobility and dynamic network topology not all conventional cryptographic algorithms will be able to be applied [6].

BENEFITS OF CONNECTED VEHICLES

- In 2016, motor vehicle-related crashes on U.S. highways claimed 37,461 lives. Some of the benefits of connected vehicles include [7]:
  - Crash Elimination
  - Provide data encryption
  - Avoid traffic congestion
  - Reduce number of accidents
  - Reduce impact of fossil fuels on the environment
  - Reduce amount of lives lost each year due to accidents
- If every vehicle in the nation were equipped with V2V technology, as many as 600,000 crashes and 270,000 injuries could be prevented each year, and 1,080 lives could be saved [9]

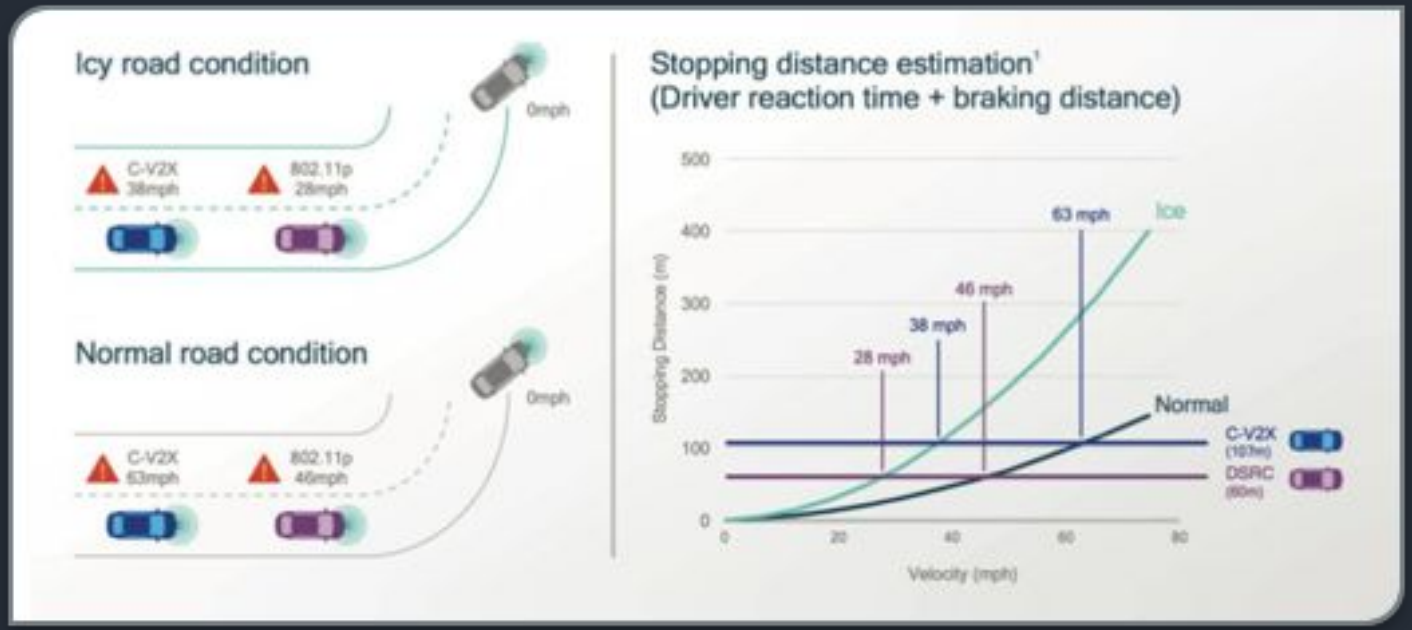

INTERNET
CA
Base station
RSU
RSU
RSU
V 2 V communication
V 2 I communication
I 2 I communication

[6]

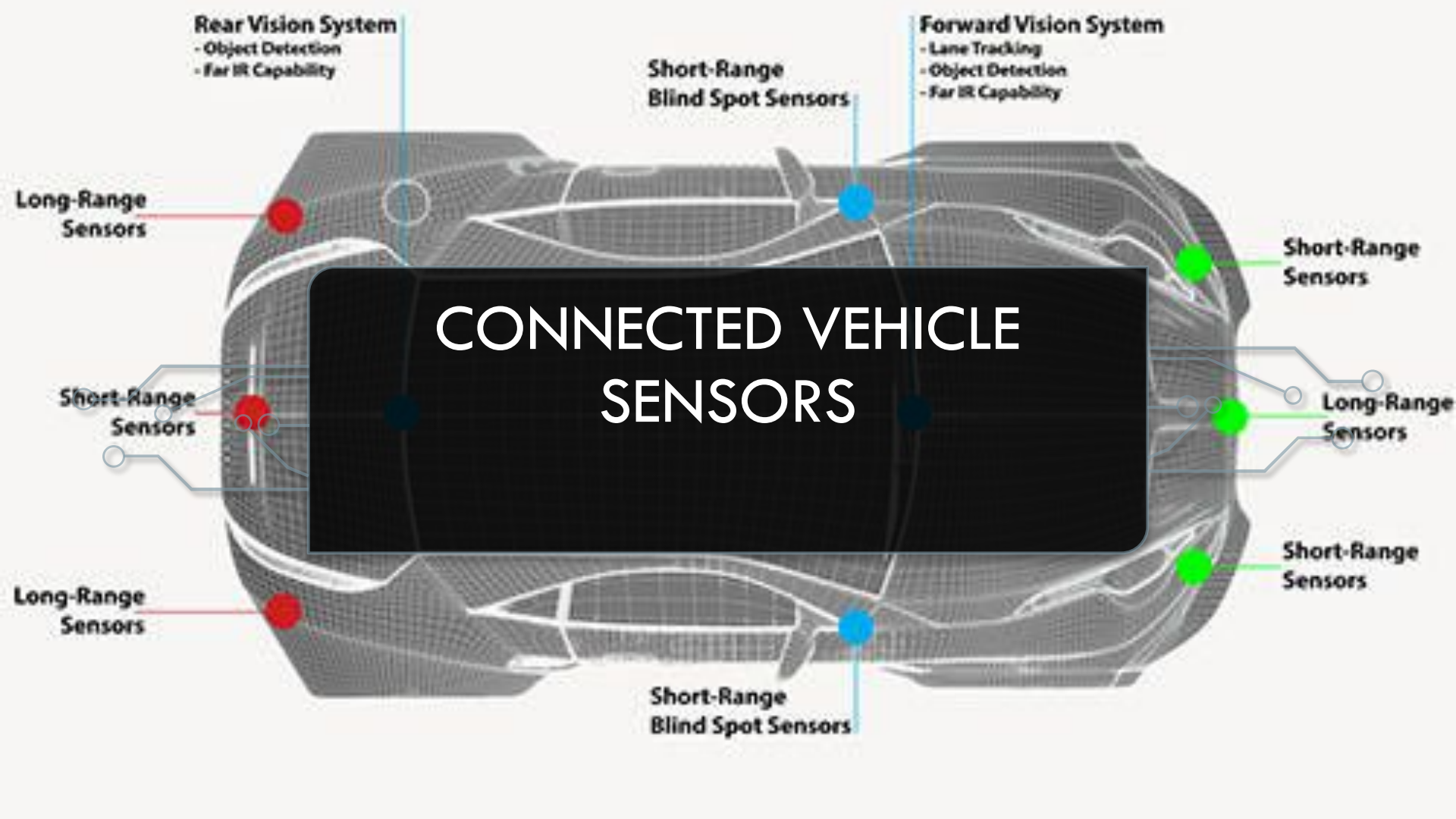
HOW IT WORKS

In addition to encryption. If there is a car about to turn into your lane and there is a possibility of an accident Car B in this scenario will be notified since they have our app installed.

HOW IT WORKS



A car that spun out due to black ice could alert other nearby vehicles of the road conditions to help them avoid making the same mistake


Rear Vision System
- Object Detection
- Far IR Capability
Short-Range
Blind Spot Sensors
Forward Vision System
- Lane Tracking
- Object Detection
- Far IR Capability
Long-Range
Sensors
Short-Range
Sensors
CONNECTED VEHICLE
SENSORS
Short-Range
Sensors
Long-Range
Sensors
Long-Range
Sensors
Short-Range
Sensors
Short-Range
Blind Spot Sensors

RISKS & VULNERABILITIES

- Theft of personal data because of lack of encryption
  - Vehicle Location (GPS coordinates, speed limit)
  - Metrics (drive status, engine RPM, fuel levels, fault codes)
  - Vehicle environment status
- Connection Risks

VEHICLE ATTACKS

- Common Cyber Threats related to V2V Communication [3]:
  - Hackers accessing drivetrain metrics (Drive status, engine RPM)
  - Having someone make your car suddenly brake or take control of the steering while you're driving
  - Hackers could disable sensors, so objects become invisible to your navigation systems

- V2V communication capability wirelessly exchange information about the Drive status, speed, and position of surrounding vehicles. If the above are compromised this can lead to car crashes and breach of privacy of personal information

Our Solution

1.) V2V Communication Security

Syber Safe Application

Provides secure transmission of data between connected vehicles through encryption

With our solution Vehicle communication such as metrics and sensors will be secured.

2.) Secure hosted environment to protect customer and vehicle data

Other solutions/procedures being implemented:

VPN

Update Antivirus software regularly

Vulnerabilities will be prioritized to invest time accordingly

SECURITY SOLUTION

- Symmetric encryption along with SPECK algorithm
  - This offers fast response time as well as highly constrained environments
  - SPECK:
    - More power and space efficient
    - Designed for constrained environments
  - Symmetric:
    - Simple, less demanding and fast
    - Fast and does not require exchange of kets or authentication but keys must be embedded on devices at the factory.
- If we were to go with Asymmetric it would be slower and more exposed to attacks.
- In V2V every millisecond is important for providing accurate, fast, and reliable information

OUR APP

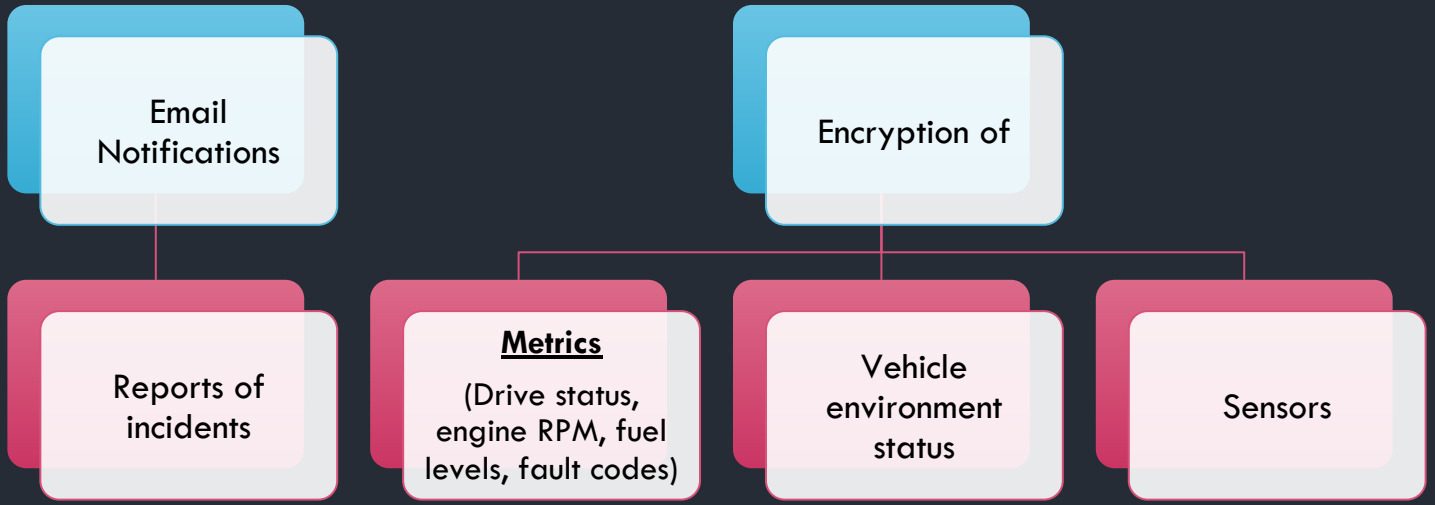
Once the driver has **parked** the car. This notifies them to check their email regarding any issues. Since the issue was not an emergency and was fixed the symbol is **green**.

The user will see a **red** symbol if it was a critical matter. They will receive an email and notification on the dashboard to pull the vehicle over.

HOW DOES IT WORK

1. The application will be built into the connected vehicles
   a) A Vehicle account will be made for the driver when the vehicle is bought or updated
2. The application will be seen in vehicles user interface
   a) The driver can access the application with a touch of a button on their user interface to see any alerts
3. Once the driver agrees to terms of accessing the new app encryption and other service will begin
4. Communication data will be encrypted between connected vehicles.
5. Any alerts will be shown on the dashboard

SYBER SAFE APP FEATURES



HARDWARE & SOFTWARE BEING USED

1

Google Cloud Platform (GCP)

- Virtual Server

2

SyberSafe

- Application for securing V2V communication data

3

Zeek

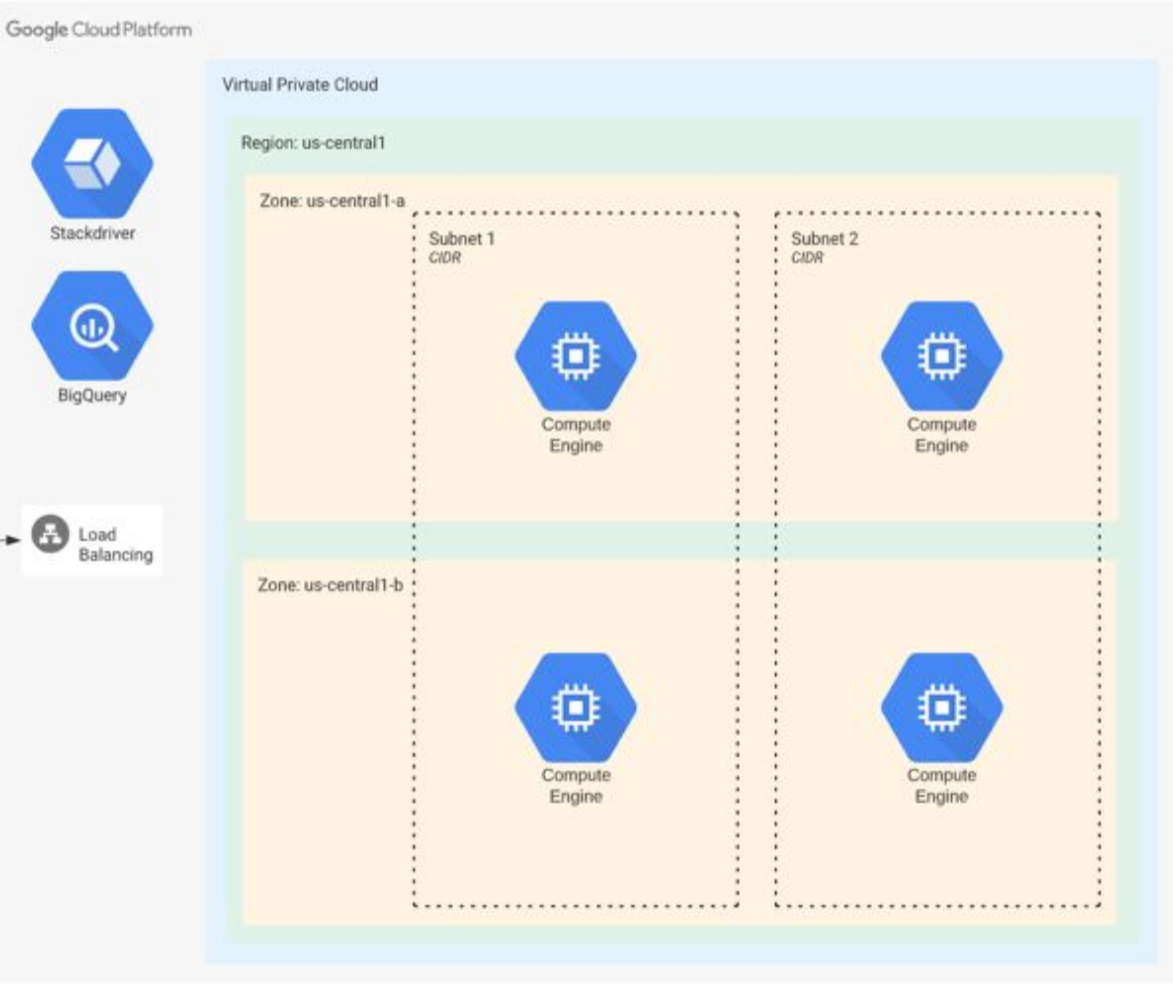
- Sits on a hardware, software, virtual or cloud platform and quietly and unobtrusively observes network traffic

4

Sophos (UTM)

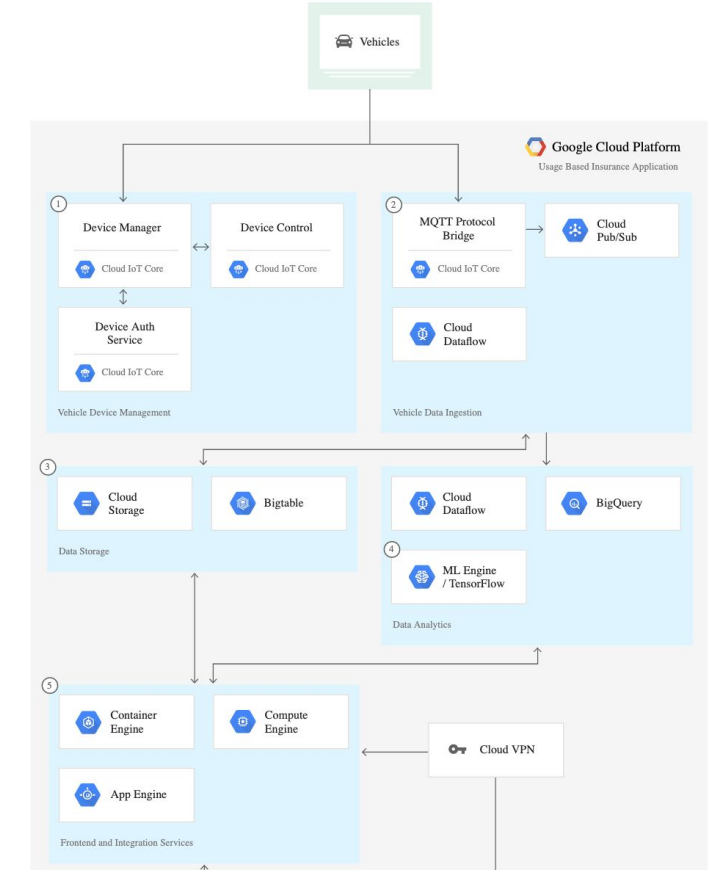
- Endpoint protection product that combines antimalware, web and application control, device control and much more.

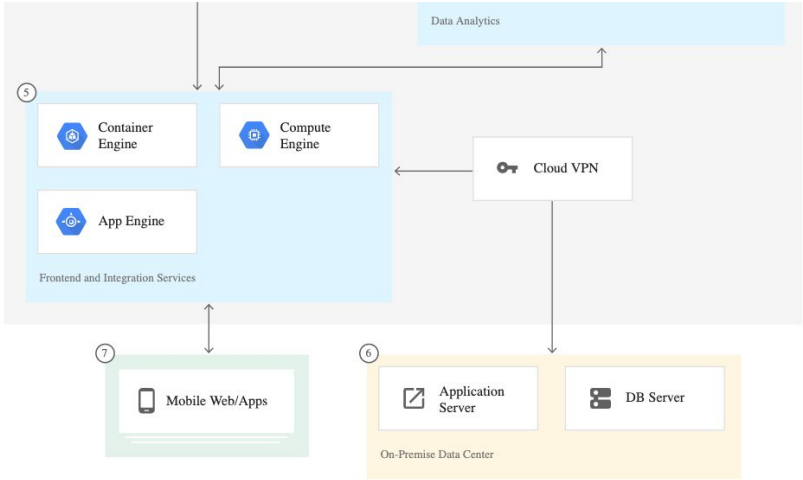
GOOGLE CLOUD PLATFORM (GCP)



- GCP provides a robust computing platform that takes advantage of Google's end-to-end security model for building and operating connected vehicle platforms.

- Solves the main challenges of developing a platform to connect and manage vehicle data include
  - Provides a platform for data ingestion, Internet of Things (IoT) device management, storage, analysis, and machine learning predictions





① **Device Management**
- Mutual authentication
- Device authorization
- 2-way communication

② **Vehicle Data Stream**
- Mutual authentication
- Device authorization
- 2-way communication

③ **Data Storage**
- Time-series telemetry data
- Historical accident data
- Select Customer data

④ **Machine Learning**
- Driver behavior analytics
- Risk modeling

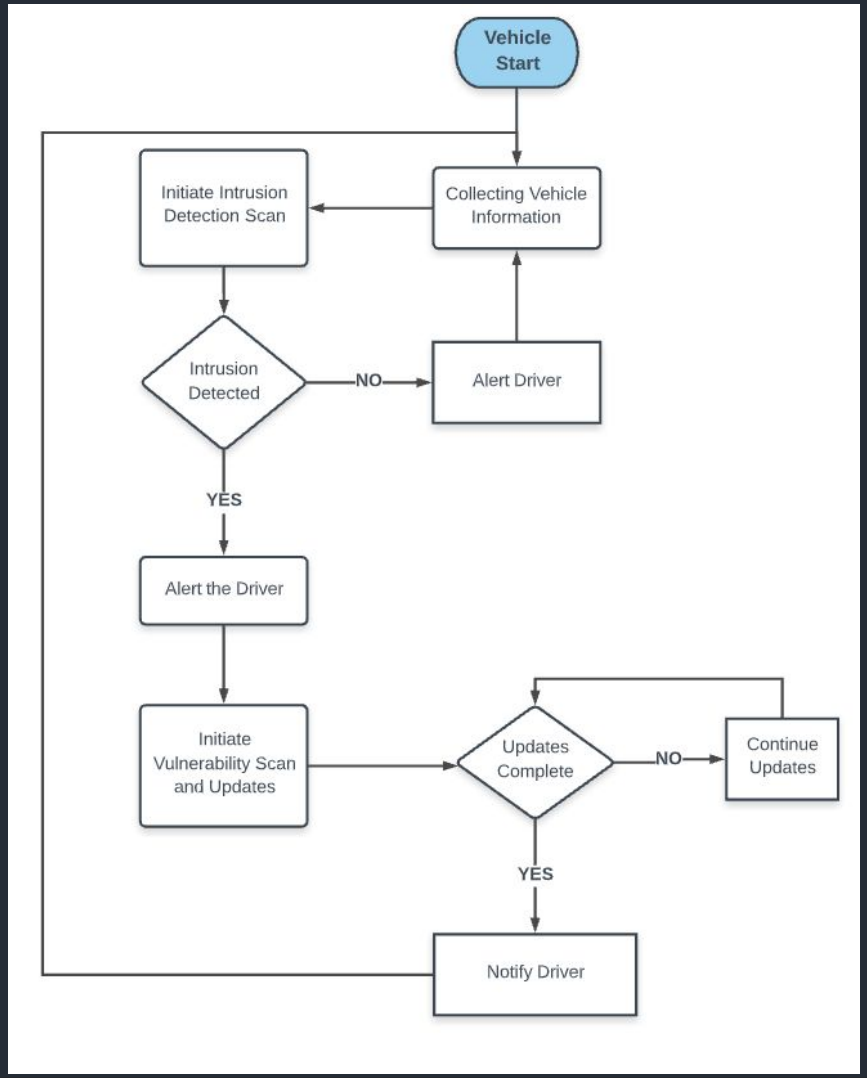
⑤ **Application**
- Frontend apps
- Backend services
- Integration services
- Mobile APIs

⑥ **Integrations**
- Integration with on-premise apps and databases
- Customer, vehicle, billing, services, policy data

⑦ **Web/Mobile Apps**
- Consumer website
- Consumer apps
- Field adjustor apps

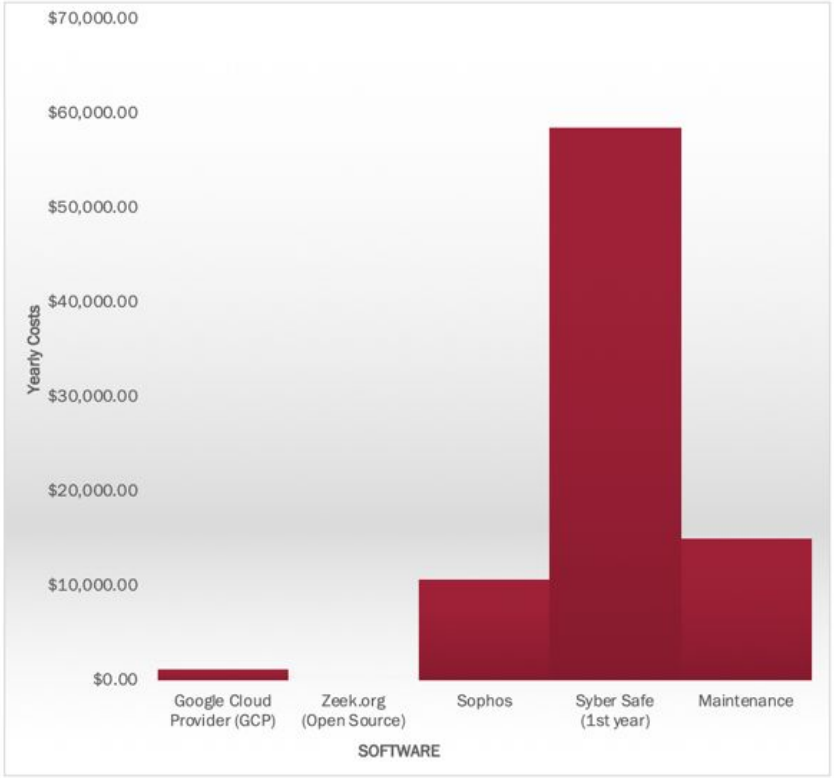
[8]

Example Flow Chart



Costs Analysis

COST BREAKDOWN

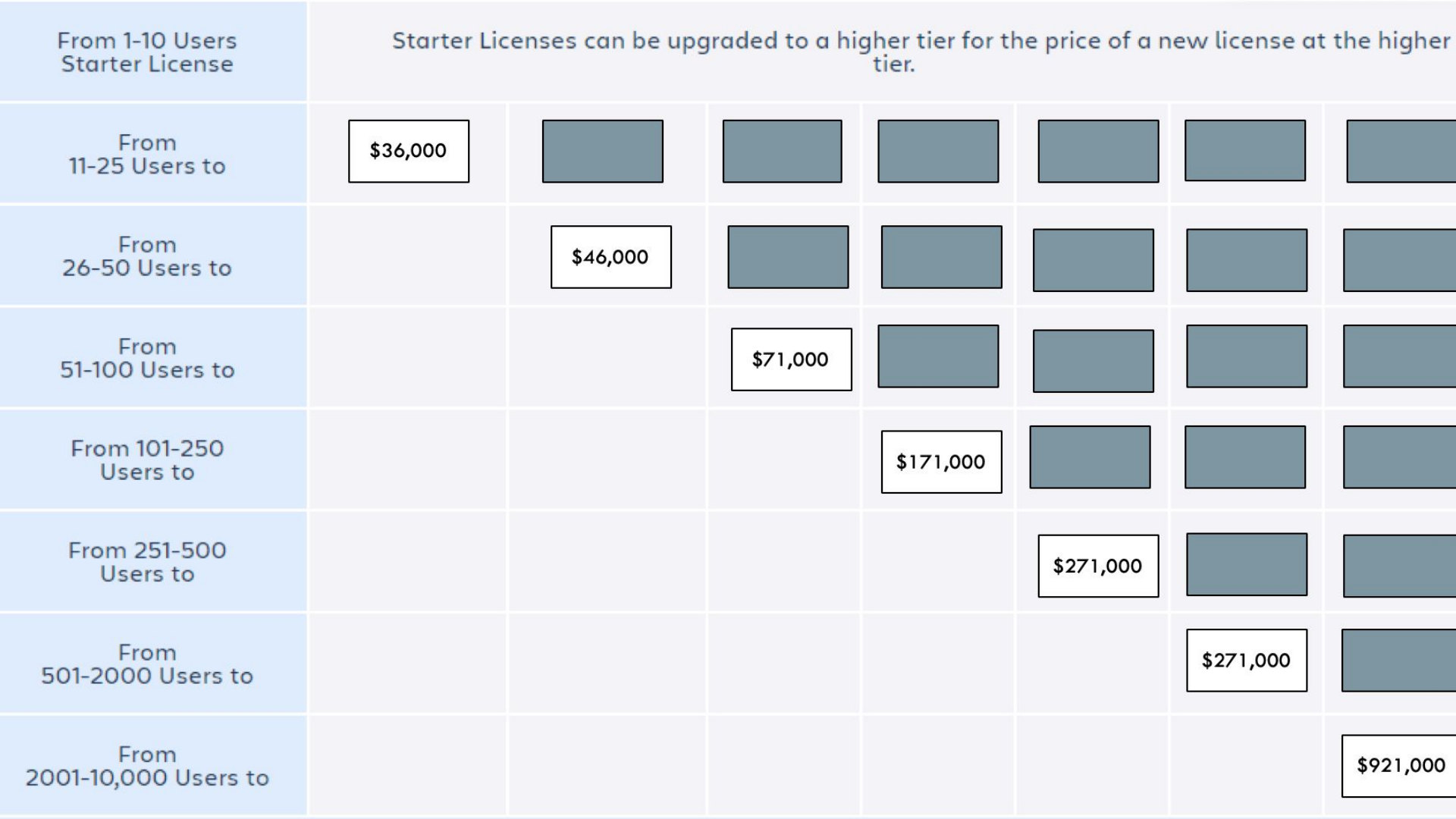


COST BREAKDOWN

Cost Center	Annual Cost
Google Cloud Provider (GCP)	$1,200.00
Zeek.org (Open Source)	$0.00
Sophos	$10,663.50
Syber Safe (1st year)	$58,500.00
Maintenance	$1,500.00
Total	**$71,863.50**

Syber Safe:
Software - $36,000
Maintenance- $1,500/m
Implementation & Training (30 hrs at 150/hr) - $4,500.00

Licensing


From 1-10 Users Starter License
Starter Licenses can be upgraded to a higher tier for the price of a new license at the higher tier.
From 11-25 Users to
$36,000
From 26-50 Users to
$46,000
From 51-100 Users to
$71,000
From 101-250 Users to
$171,000
From 251-500 Users to
$271,000
From 501-2000 Users to
$271,000
From 2001-10,000 Users to
$921,000

SOFTWARE LICENSE AGREEMENT

THIS AGREEMENT is entered into as of 8/01/2020 by and between SyberSafe Software Inc., with offices at 605 Maple, Suite 200, Farmington Hills, Michigan 48167 ("LICENSOR") and Electric Motor Vehicles, 100 EMV Ave, Troy, Michigan 48007 ("LICENSEE").

WHEREAS, Licensee wishes to license software for the purpose of data security and NEAR desires to license this software to licensee.

NOW THEREFORE, the parties hereto agree as follows:

1. GRANT OF LICENSE Subject to the terms and conditions of the Agreement, NEAR grants to Licensee a non-exclusive, non-transferable license to use the software identified in Exhibit A (the "Licensed Programs") for the purpose of data exchange. Licensee may use the Licensed Programs in executable format for its own use and may translate or modify the licensed programs or incorporate them into other software. Licensee may not, however, transfer or sublicense the Licensed Programs to any third party, in whole or in part, in any form, whether modified or unmodified.

2. CONSIDERATION TO NEAR

a. Licensee shall pay, upon delivery of the Licensed Programs, the license fees set forth in Exhibit A attached hereto.

b. License fees do not include any shipping, duties, bank fees, sales, use, excise or similar taxes due. If Licensor is required to pay any such amounts, Licensee shall reimburse Licensor in full.

3. COPIES Licensee may make copies of the Licensed Program in executable code form as necessary for use by Licensee and for backup or archive purposes. Licensee agrees to maintain records of the location and use of each copy, in whole or in part, of the Licensed Programs. Each Licensed Program is copyrighted but unpublished by NEAR. Licensee agrees to reproduce and apply the copyright notice and proprietary notice of NEAR to all copies made hereunder, in whole or in part and in any form, of Licensed Programs.

4. OWNERSHIP The original and any copies of the Licensed Programs, made by Licensee, including translations, compilations, partial copies, modifications, and updates, are the property of NEAR.

5. PROPRIETARY RIGHTS Licensee recognizes that NEAR regards the Licensed Programs as its proprietary information and as confidential trade secrets of great value. Licensee agrees not to provide or to otherwise make available in any form the Licensed Programs, or any portion thereof, to any person other than employees of Licensee without the prior written consent of NEAR. Licensee further agrees to treat the

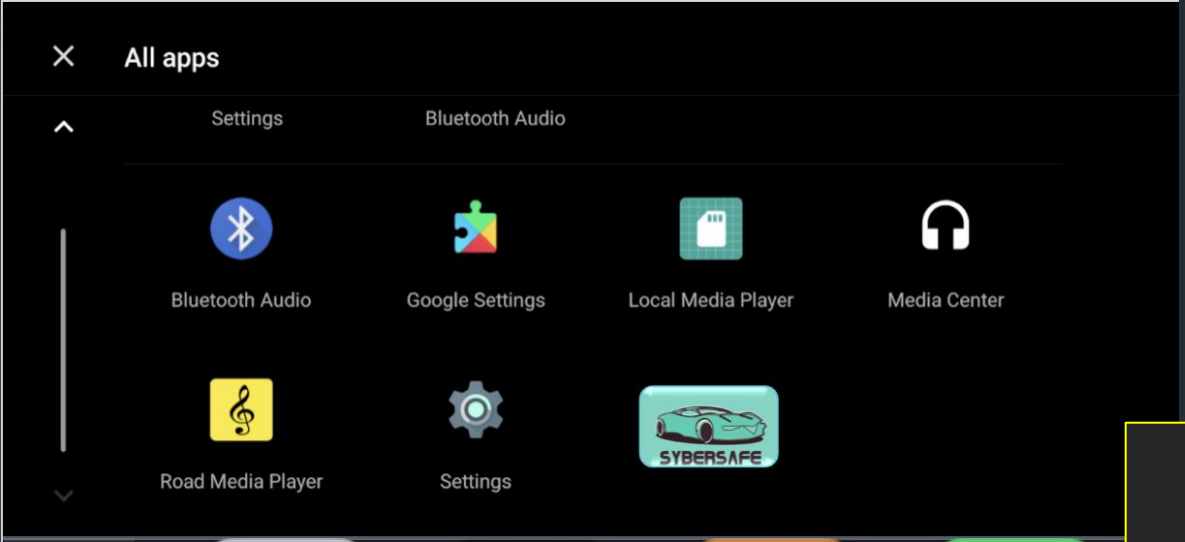
LICENSED PROGRAMS

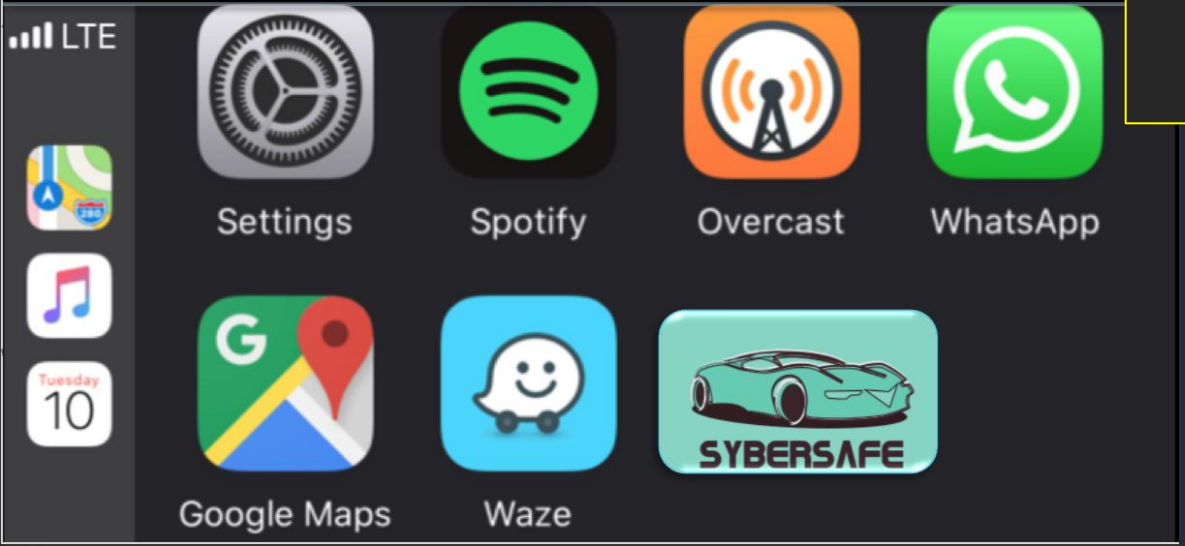
	One Time	Per Month
COMPUTER PROGRAMS	LICENSE FEE	MAINTENANCE FEE
SyberSafe (Executable format)	US $ 58,500	US $1,500.00

NOTES:

License fee excludes any taxes, shipping and/or insurance charges, and any bank transfer fees.

Code maintenance is free during the first year; thereafter, code maintenance is available annually with maintenance fee listed above.





developers

Next Steps….

Developer

CONTACT US

Syberquestions@SyberSafe.com

743.897.1234 Ext. 333
(Tech Dept.)

8908 Fire Blvd, Detroit
Michigan, 48232

SyberSafe.com

THANK YOU

References

1. https://www.trustonic.com/news/blog/top-10-security-challenges-for-connected-cars/
2. https://www.trendmicro.com/us/iot-security/news/2571
3. https://blog.guardknox.com/what-are-connected-vehicles-and-their-vulnerabilities
4. https://www.brandcrowd.com/maker/logo/5223e7c6-3cc7-41b2-bb43-9ca4fc8b2d99?text=SyberSafe
5. https://www.digicert.com/blog/connected-cars-need-security-use-pki/https://www.researchgate.net/figure/Flowchart-describing-the-working-of-V2I-I2V-Communication_fig2_296839370
6. https://www.hindawi.com/journals/wcmc/2018/1640167/
7. http://autocaat.org/Technologies/Automated_and_Connected_Vehicles/
8. https://cloud.google.com/solutions/designing-connected-vehicle-platform
9. https://totalsecurityadvisor.blr.com/security-hardware-and-technology/v2v-communications-crash-avoidance-cybersecurity/