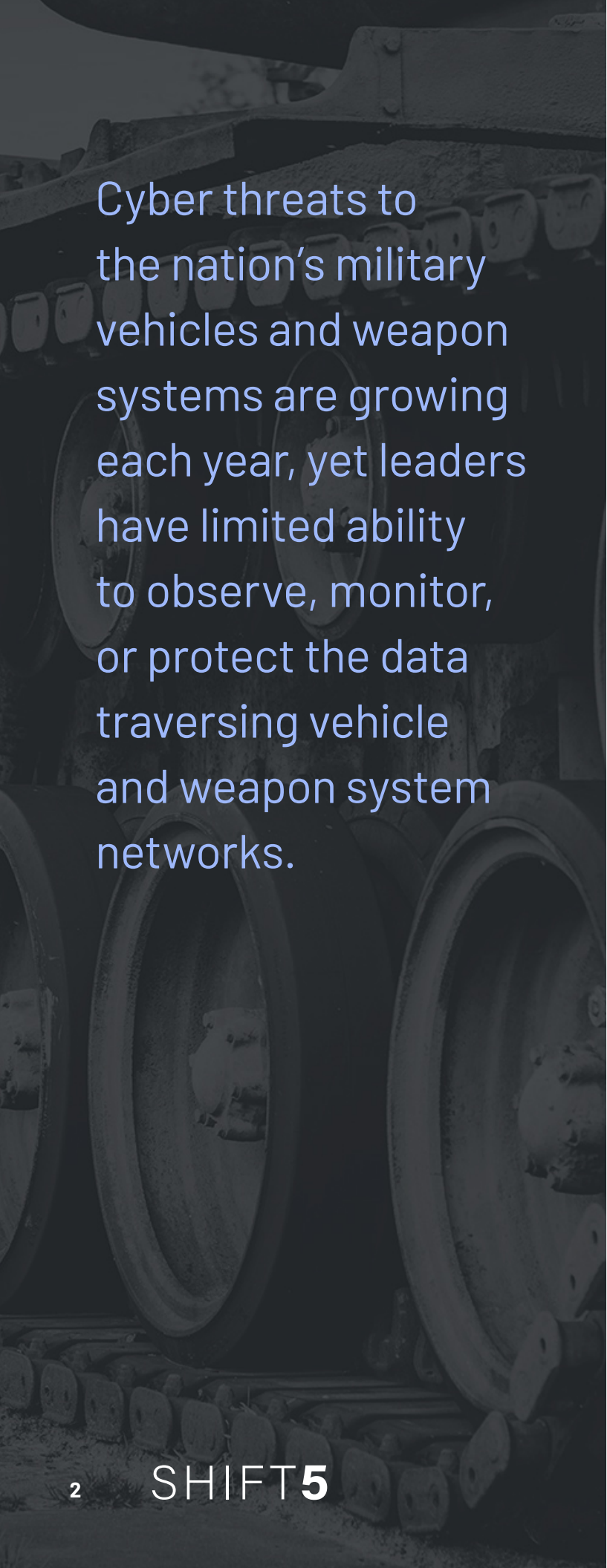


Customer Case Study:

# ENSURING THE CYBER RESILIENCE OF HEAVY GROUND VEHICLES



SHIFT**5**



Cyber threats to the nation's military vehicles and weapon systems are growing each year, yet leaders have limited ability to observe, monitor, or protect the data traversing vehicle and weapon system networks.

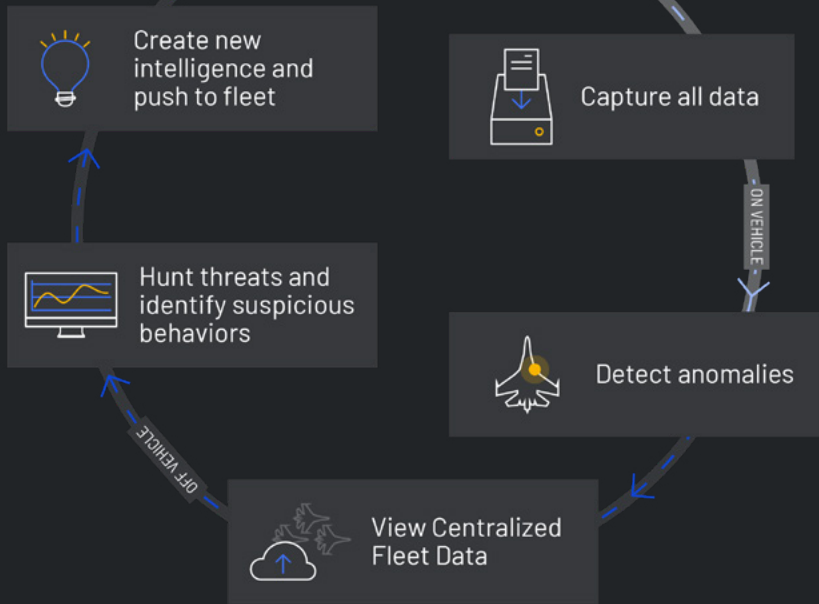
**Shift5 changes that by unlocking the data that controls planes, tanks, and other weapon systems. This allows organizations to hunt for anomalies and alert crew and maintenance personnel so they can take action to mitigate or eliminate cybersecurity threats.**

## The Customer Challenge

Heavy ground vehicles are powered in part by serial bus networks that use embedded protocols to ensure various components are working together to operate the vehicle. These networks employ few cybersecurity protections, leaving vehicles open to cyber attacks that can degrade, deny, disable, disrupt, manipulate, or even destroy vehicles by compromising their embedded software and affecting physical outcomes.

Due to urgent and emerging threats, the customer required enhanced security for heavy ground vehicles within a short time period. Shift5 delivered a single piece of low Size, Weight, and Power (SWaP) hardware to enable cyber resilience and cyber situational awareness across several vehicles. The Shift5 prototype is scalable across the entire fleet and was tailored for integration with the specific vehicle platform for the purpose of detecting cyber attacks conducted on the vehicle's serial bus network. Because of the sensitive nature of the data, the customer had additional requirements around the security of data collection, storage, analysis, and retrieval. Shift5 therefore followed and implemented the policies established by U.S. Executive Order 13556, U.S. Department of Defense Manual 5200.01, and NIST SP 800-53.

## SHIFT5 COMPLETE OBSERVABILITY



## About Shift5

Shift5 is the onboard OT data and cybersecurity company for planes, trains, and tanks. Created by founding members of the U.S. Army Cyber Command who pioneered modern weapons system cyber assessments, Shift5 defends military platforms and commercial transportation systems against malicious actors and operational failures. Customers rely on Shift5 to detect threats and maintain the readiness and availability of today's planes, trains, tanks, and weapons systems and tomorrow's next-generation vehicles.

For more information, visit [shift5.io](https://shift5.io).

## The Shift5 Solution and Results

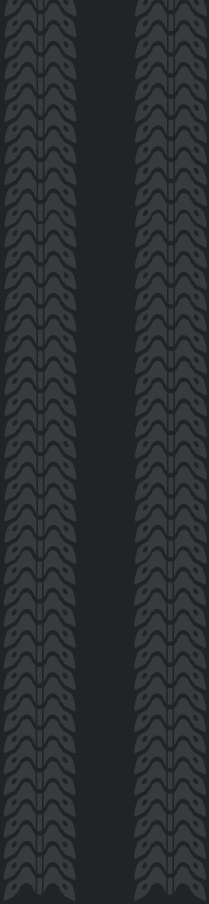
### DURING THIS ENGAGEMENT, Shift5:

- Installed hardware to monitor multiple Controller Area Network (CAN) serial buses on the vehicle. Hardware was certified according to military requirements, including MIL-STD-461E
- Used a variation of commercially-available compact computers for on-vehicle collection, detection, and alerting. These computers weighed less than 2 lbs, consumed between 15-20 Watts of power, and ranged in size from 55 to 63 cubic inches
- Translated communications for the vehicle's unique J1939 protocol implementation, which provides serial data communication between various Electronic Control Units (ECUs) powering the vehicle

### AS A RESULT OF THIS ENGAGEMENT,

Shift5 successfully demonstrated the following capabilities:

- Full-packet J1939 bus data capture
- Compression and storage of J1939 bus data on-vehicle in the Shift5 product
- Transformation, loading, translation, and visualization of J1939 vehicle data in a centralized, off-vehicle environment
- Detection of malicious and anomalous J1939 messages
- Alerts to crew about vehicle cyber readiness
- Ability to enable cyber incident response functions



Customer Case Study:

# ENSURING THE CYBER RESILIENCE OF HEAVY GROUND VEHICLES

## SHIFT**5**

<http://shift5.io>

*"Ensuring the Cyber Resilience of Heavy Ground Vehicles" Version 3.0 // Nov 2022*  
© Shift5, Inc.