

Inside the Telematics Attack Surface: Offensive Security Lessons for Preventing Fleet Disruption and Cargo Theft



Sean Herron
Chief Information Security Officer
Samsara



INSIDE THE TELEMATICS ATTACK SURFACE

Offensive security lessons for preventing fleet disruption and cargo theft

Sean Herron

Chief Information Security Officer, Samsara



A stolen account can result in a stolen load

© Samsara Inc. Confidential

Cargo theft losses rose in 2025

\$725M

Estimated losses in the U.S.
and Canada in 2025
Up 60% from 2024

2,646

Confirmed cargo thefts in
2025
Up 18% from 2024

\$274K

Average value per theft
Up 36% from 2024

Source: Verisk CargoNet, 2025 annual analysis. Includes all reported cargo theft, not just cyber-enabled theft.

© Samsara Inc. Confidential

THE TELEMATICS ATTACK SURFACE

Four connected systems, one fleet



Devices

Gateways, ELDs and trackers

Firmware and vehicle interfaces



Connections

Cellular, Wi-Fi and Bluetooth

Data and command channels



Cloud services

Fleet records and device management

APIs and integrations



People

Drivers, dispatchers and administrators

Accounts and permissions

© Samsara Inc. Confidential

Fleet data and device commands

The truck sends its location to dispatch

An attacker can use location data to target a load.

The cloud sends device updates and settings

Compromised admin access can disrupt reporting.

© Samsara Inc. Confidential

Public incidents and security research

Service outage

Microlise, 2024

A provider breach disrupted customer systems.

Admin access

Spireon research, 2023

Researchers gained access to fleet data and device controls.

Vehicle control

Fast and Vulnerable, 2015

Researchers demonstrated vehicle control through an aftermarket device.

Sources: Microlise company update, 18 Nov 2024; Curry et al., 2023; Foster et al., Fast and Vulnerable: A Story of Telematic Failures, USENIX WOOT 2015.

© Samsara Inc. Confidential

HOW TELEMATICS COMPROMISES UNFOLD

How stolen access can enable cargo theft

01

Gain access

A fake freight document delivers remote-access software.

02

Read shipment data

Access reveals loads, schedules and account details.

03

Arrange a pickup

An attacker impersonates a legitimate carrier.

04

Take the load

A crew collects the freight using false instructions.

Allow only approved remote tools. Verify pickup changes independently.

Composite scenario informed by Proofpoint, Remote access, real cargo (2025). Physical theft requires additional actions.

© Samsara Inc. Confidential

Testing access across fleets and user roles

Example: Fleet A dispatcher with view-only access

View Fleet A trucks	Allowed	Expected access
View Fleet B trucks	Allowed	Customer data leak
Change fleet settings	Blocked	Role check works

A valid login does not authorize access to every fleet.

© Samsara Inc. Confidential

A device accepts an attacker's software

01

Submit an update

An exposed interface lets the attacker submit an update.

02

Skip verification

The device installs an update without verifying its source.

03

Run attacker code

Malicious software changes or stops location reporting.

Reject updates altered after signing.

Composite scenario informed by Jepson, Chatterjee and Daily, VehicleSec 2024. Results depend on the tested device.

© Samsara Inc. Confidential

Firmware update and recovery checks

Reject

Altered update package

Unknown signing key

Disallowed older firmware

Install and recover

Authorized update installs

Expected version boots

Device recovers after power loss

Test failed updates as well as successful ones.

Aligned to NMFTA telematics requirements v1.5 and IETF RFC 9019 (firmware update guidance).

© Samsara Inc. Confidential

Blocking access and recovering a device

1. Block cloud access

Revoke its credentials and end active connections.

2. Recover the device

Restore verified firmware and replace compromised credentials.

Unaffected devices should keep reporting.

© Samsara Inc. Confidential

Example: test results and their limits

Observed
False location reports

Not tested
Braking or steering

Device access alone does not establish vehicle control.

© Samsara Inc. Confidential

AI IN SECURITY TESTING



AI can automate parts of an attack

Anthropic reports AI-assisted reconnaissance, exploitation and data theft.

Automation

Agents carry out repeated attack steps.

Parallel activity

Actors can run several tasks at once.

Defense

Retest known weaknesses after changes.

Source: Anthropic, September 2026 threat report. Observed cases are not specific to fleets.

© Samsara Inc. Confidential

Automating access-control tests

Define who can view each fleet's data and change its settings.

Test accounts

Create accounts for separate fleets and roles.

Expected permissions

Record which requests should succeed or fail.

An AI agent runs test cases.

An engineer confirms the findings and the fix.

Recommended approach: approved tests in an isolated environment.

© Samsara Inc. Confidential

SECURITY TESTING BEFORE RELEASE

Security checks during development

Design

Define access to fleet data and commands.

Build

Test permissions for each account and role.

Release

Test firmware updates and recovery.

Operate

Retest after software or integration changes.

Recommended workflow, aligned to NMFTA telematics security requirements.

© Samsara Inc. Confidential

An offensive security test cycle

01

Scope

Choose a control to test.

02

Test

Run allowed and forbidden actions.

03

Record

Record the response and operational effect.

04

Confirm

Reproduce the failure.

05

Retest

Verify the fix.
Retain the test.

Close the finding after the attack fails and normal operations still work.

© Samsara Inc. Confidential

Checks for builders, buyers and operators

Build

Test access between customer accounts

Test update failure and recovery

Retest fixes automatically

Buy

Match test results to deployed versions

Name incident and patch owners

Require proof that fixes work

Operate

Test account revocation

Verify pickup and route changes

Rehearse loss of tracking

Guidance informed by NMFTA telematics security requirements v1.5. Verify behavior in your deployment.

© Samsara Inc. Confidential

A 30-day security testing plan

- 01 Choose a test owner** Select one API, device update or dispatch process.
- 02 Run the agreed test** Record the expected result and what happened.
- 03 Assign the fix** Name the remediation owner and due date.
- 04 Verify the fix** Repeat the test and check normal operation.

Suggested schedule. Track unfinished tests and fixes with owners and due dates.

© Samsara Inc. Confidential

