TECHNICAL OVERVIEW

IT Infrastructure & Security Overview

Jifeline Networks infrastructure for Remote Vehicle Diagnostics
Architecture, data protection and network requirements

Document	IT Infrastructure & Security Overview
Version	1.1
Date	November 2026
Intended audience	IT administrators, network engineers and information security officers of customers and partners
Publisher	Jifeline Networks · www.jifeline.net

1 Introduction

1.1 Purpose

This document describes the IT infrastructure that supports the Jifeline Networks infrastructure for remote vehicle diagnostic services and the security measures that protect the data exchanged between workshops, the Jifeline Cloud Platform and remote diagnostic centers.

It is intended for IT administrators, network engineers and information security officers who assess the service or prepare their network environment for it.

1.2 Scope

The document covers the following topics:

- Solution architecture and system components
- Data flows between the workshop, the cloud platform and the diagnostic center
- Hosting and data residency
- Encryption of data in transit and at rest
- Firewall and network requirements

2 Solution architecture

2.1 Overview

The Jifeline service enables a diagnostic specialist in a remote diagnostic center to diagnose a vehicle that is physically located in a workshop, as if the specialist's diagnostic equipment were connected directly to that vehicle.

The solution consists of three domains:

- **Workshop (customer site):** the location of the vehicle, the *Remote Vehicle Communication Interface* (Remote VCI) and the workshop technician.
- **Jifeline Cloud Platform:** the central infrastructure, hosted on Amazon Web Services (AWS), that connects workshops and diagnostic centers.
- **Remote Diagnostic Center:** the location of the diagnostic specialist, *Local Tool Communication Interface* (Local TCI) and the (IAM/OEM) Diagnostic Tool.

Communication takes place over two logically separated channels: a *diagnostic data channel* for vehicle communication and an *application channel* for the web applications used by the workshop and the diagnostic specialist.

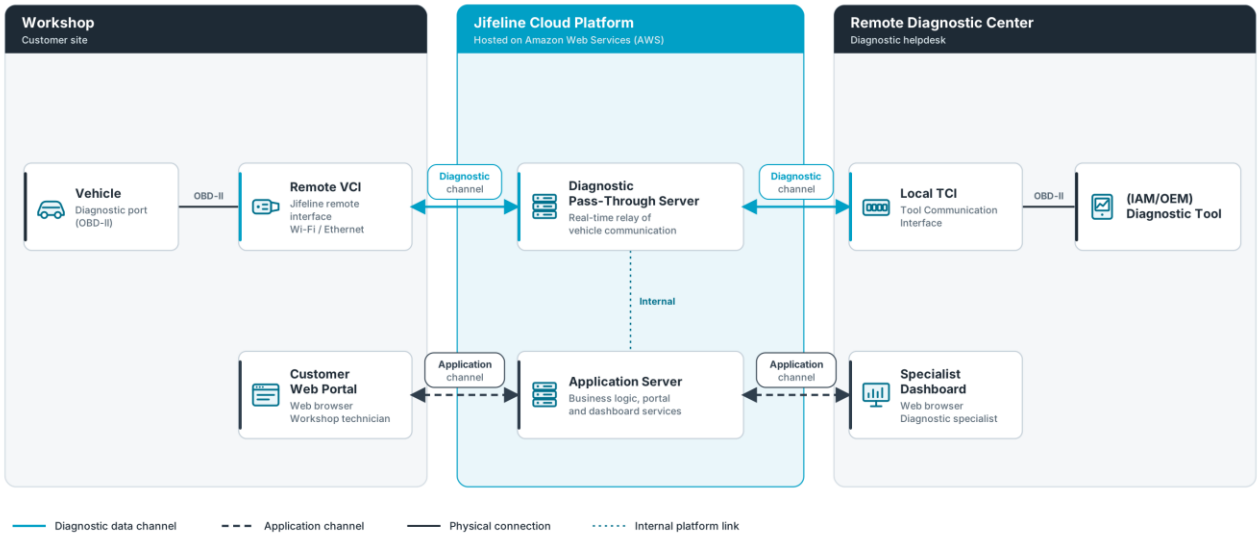


Figure 1 Solution architecture and data flows

2.2 System components

Component	Domain	Function
Remote VCI (Remote Vehicle Communication Interface)	Workshop	Connects to the vehicle's OBD-II diagnostic port and to the Jifeline Cloud Platform via the workshop's Wi-Fi or wired Ethernet network.
Customer Web Portal	Workshop	Browser-based application used by the workshop technician to communicate with the remote diagnostic center about diagnostic sessions.
Diagnostic Pass-Through Server	Cloud platform	Relays vehicle communication in real time between the Remote VCI in the workshop and the Local TCI in the diagnostic center.
Application Server	Cloud platform	Hosts the business logic of the service and serves the Customer Web Portal and the Specialist Dashboard.
Local TCI (Tool Communication Interface)	Diagnostic center	Interface in the diagnostic center to which the (IAM/OEM) Diagnostic Tool is connected. It presents the remote vehicle to the tool as a locally connected vehicle.
(IAM/OEM) Diagnostic Tool	Diagnostic center	Independent Aftermarket (IAM) or Official Manufacturer's (OEM) diagnostic tool, connected to the Local TCI.
Specialist Dashboard	Diagnostic center	Browser-based application used by the diagnostic specialist to manage diagnostic sessions and communicate with the workshop.

3 Data flows

3.1 Diagnostic data channel

The diagnostic data channel carries the communication between the vehicle and the (IAM/OEM) Diagnostic Tool. The Remote VCI reads the vehicle through the OBD-II port and exchanges this data with the Diagnostic Pass-Through Server. The server relays the data in real time to the Local TCI in the diagnostic center, where the (IAM/OEM) Diagnostic Tool is connected.

Path: **Vehicle** → **Remote VCI** → **Diagnostic Pass-Through Server** → **Local TCI** → **(IAM/OEM) Diagnostic Tool** (bidirectional).

3.2 Application channel

The application channel carries the communication between the people involved in a diagnostic session. The workshop technician uses the Customer Web Portal and the diagnostic specialist uses the Specialist Dashboard. Both are browser-based applications served by the Application Server.

Path: **Customer Web Portal** ↔ **Application Server** ↔ **Specialist Dashboard**.

3.3 Separation of channels

Diagnostic data and application traffic are processed by separate servers and use separate network ports and encryption mechanisms. This separation limits the impact of a disruption in one channel on the other and allows each channel to be secured according to its own requirements.

4 Hosting and data residency

Both the Diagnostic Pass-Through Server and the Application Server are hosted in Amazon Web Services (AWS) data centers in Europe. The platform is reachable through fixed public IP addresses, which allows customers to restrict outbound traffic to known destinations in their firewall policy.

Cloud provider	Amazon Web Services (AWS)
Data center locations	Frankfurt, Germany (AWS region eu-central-1) London, United Kingdom (AWS region eu-west-2)
Public addressing	Fixed (static) public IP addresses
Data at rest	Encrypted (see section 5.2)

5 Data protection and encryption

5.1 Encryption in transit

All connections between the sites and the Jifeline Cloud Platform are encrypted. Each channel uses the encryption mechanism best suited to its traffic:

Channel	Connection	Protection
Diagnostic data channel	Remote VCI ↔ Diagnostic Pass-Through Server	512-bit encryption
Diagnostic data channel	Diagnostic Pass-Through Server ↔ Local TCI	512-bit encryption
Application channel	Customer Web Portal ↔ Application Server	TLS (HTTPS)
Application channel	Specialist Dashboard ↔ Application Server	TLS (HTTPS)

5.2 Encryption at rest

Data stored on the Jifeline Cloud Platform, on both the Diagnostic Pass-Through Server and the Application Server, is encrypted at rest.

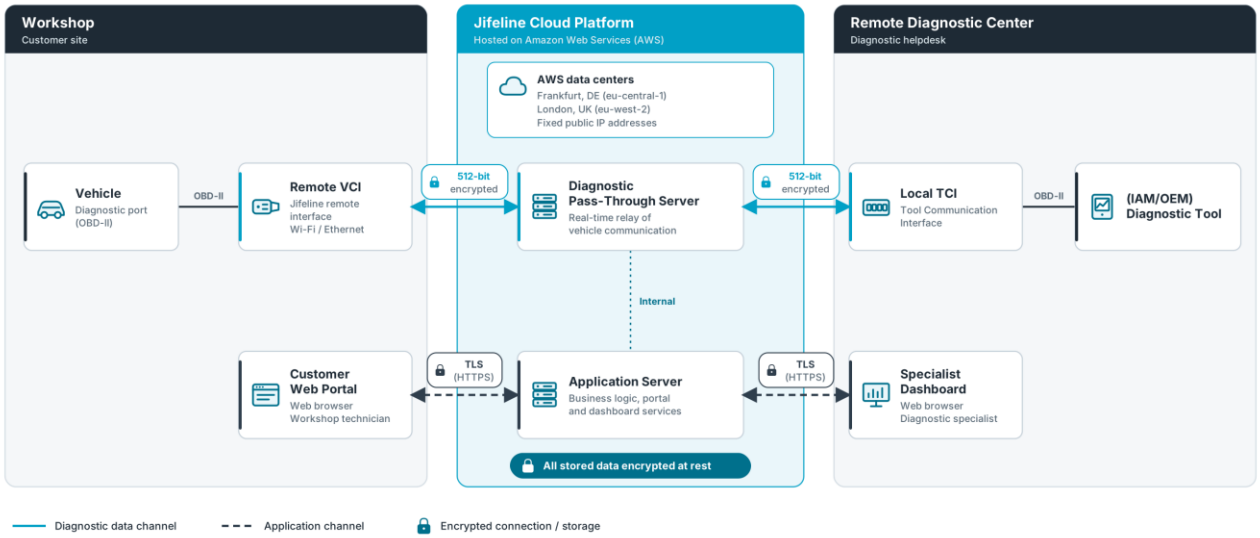


Figure 2 Encryption in transit and at rest

6 Network and firewall requirements

6.1 Connection model

All connections to the Jifeline Cloud Platform are initiated outbound from the workshop and the diagnostic center. No inbound ports need to be opened and no inbound firewall rules are required at either site.

6.2 Required outbound ports

The following outbound connections must be permitted by the firewall at both the workshop and the diagnostic center:

Traffic	Source	Port	Remarks
Diagnostic data channel	Remote VCI (workshop) / Local TCI (diagnostic center)	TCP 46329	Primary port
Diagnostic data channel (fallback)	Remote VCI (workshop) / Local TCI (diagnostic center)	TCP 80	Used automatically if port 46329 is blocked
Application channel	Web browser (Customer Web Portal / Specialist Dashboard)	TCP 443	HTTPS

6.3 Recommendations

- Allow outbound TCP 46329 explicitly for the diagnostic data channel. TCP 80 is intended as a fallback only.
- Where the firewall policy restricts outbound destinations, use the fixed IP addresses of the Jifeline Cloud Platform. More information about these IP addresses is available in the Jifeline Network Support pages (login required). A public list of the fixed IP addresses is available at: https://resources.obd.help/public/network/iplist.txt

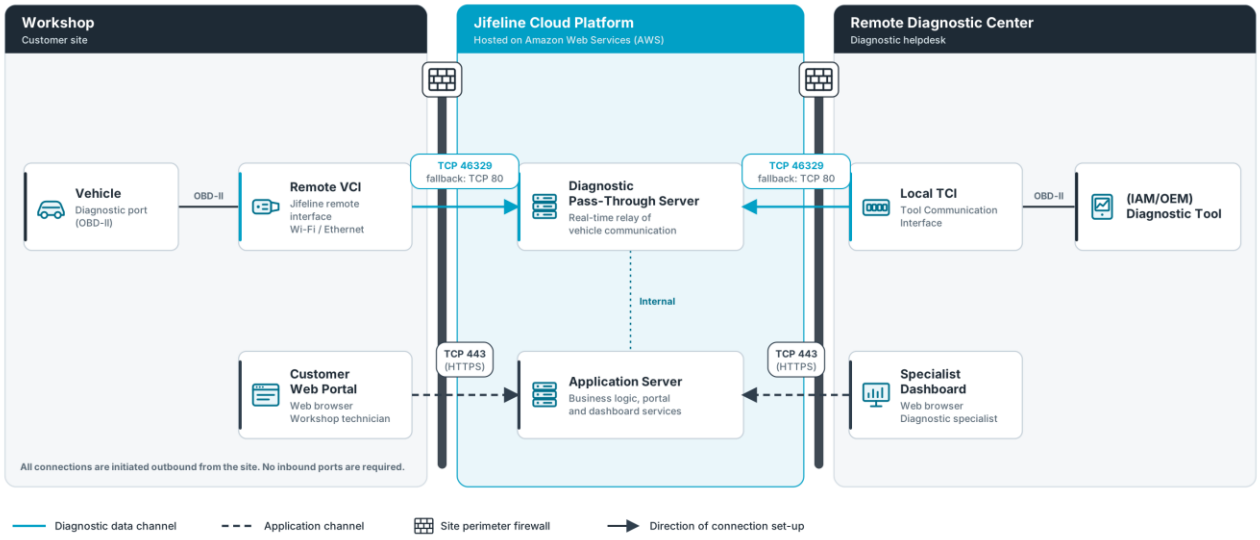


Figure 3 Firewall and port requirements

7 Summary of security measures

Measure	Description
Channel separation	Diagnostic data and application traffic run on separate servers and ports.
Encryption in transit	512-bit encryption on the diagnostic data channel; TLS (HTTPS) on the application channel.
Encryption at rest	All data stored on the Jifeline Cloud Platform is encrypted.
Outbound-only connectivity	Sites only initiate outbound connections; no inbound ports are required.
European hosting	Hosted on AWS in Frankfurt (Germany) and London (United Kingdom).
Fixed IP addresses	Allow outbound traffic to be restricted to known destinations.

Appendix A Glossary

Term	Definition
AWS	Amazon Web Services, the cloud infrastructure provider that hosts the Jifeline Cloud Platform.
Encryption at rest	Encryption of data while it is stored on disk or in a database.
Encryption in transit	Encryption of data while it travels over a network.
(IAM/OEM) Diagnostic Tool	Independent Aftermarket / Official Manufacturer's Diagnostic Tool: a diagnostic tool from an independent aftermarket supplier (such as Bosch, Hella, Autel) or the vehicle manufacturer's official diagnostic tool (OEM).
HTTPS	HTTP secured with TLS; the standard protocol for secure web traffic.
OBD-II	On-Board Diagnostics, the standardized diagnostic port and protocol set of a vehicle.
Pass-through	Technique whereby diagnostic communication is forwarded transparently between a vehicle and a diagnostic tool.
TCI	Tool Communication Interface, the hardware in the diagnostic center that connects the (IAM/OEM) Diagnostic Tool to the platform (Local TCI).
TLS	Transport Layer Security, the cryptographic protocol that secures web connections (successor to SSL).
VCI	Vehicle Communication Interface, the hardware that connects the vehicle to the platform (Remote VCI).