



QoE AI Insights v Beta

Functional Specification

Abstract

QoE AI Insights delivers a unified, privacy-first platform for measuring and improving real-world mobile experience. It combines lightweight device data, intelligent enrichment, and secure partner delivery with a robust control plane for licensing, governance, and analytics. Built on Microsoft Fabric, it enables operators and regulators to access high-resolution QoE intelligence and actionable insights through powerful dashboards.

support@qoeaiinsights.net
www.qoeaiinsights.net



1 Executive Summary

QoE AI Insights is an end-to-end quality-of-experience intelligence platform designed to give mobile operators, MVNOs, regulators, and enterprise connectivity providers unprecedented visibility into real-world network performance. It combines device-level telemetry, scalable cloud ingestion, and advanced analytics to create a continuously updated, crowdsourced digital twin of mobile network experience across regions, operators, and radio access technologies.

At the edge, the platform includes two complementary components: **QoEApp**, a fully compliant iOS and Android application for passive, movement-aware QoE measurement; and **QoESDK**, an embeddable Android library enabling partners to integrate the same high-fidelity telemetry capture directly into their own apps. Both components collect lightweight, privacy-preserving network performance signals and compute on-device QoE scores that reflect the user's lived experience of connectivity.

All telemetry flows into the **Core API backend**, a secure, multi-tenant service responsible for licensing, partner onboarding, device lifecycle management, and SAS token distribution. This backend orchestrates ingestion into **Microsoft Azure Blob Storage**, where crowdsourced data is stored efficiently and durably, ready for large-scale analytics. The architecture is designed for global deployments, with strong isolation between partners and full compliance with GDPR and regional data-handling requirements.

The analytics layer is powered by **Microsoft Fabric Real-Time Analytics (ADX)**, enabling high-volume ingestion, low-latency querying, and flexible data modelling. Network performance can be explored across operator identifiers (MNC/MCC), location areas (LAC/TAC), individual cells (CellID), and aggregated spatial tiles (Hex3). QoE scores are computed, aggregated, and benchmarked in real time, allowing operators and MVNOs to understand performance at a level of granularity previously unavailable without expensive drive-testing.

Insights are delivered through **Power BI dashboards** that provide intuitive filtering, comparison, and drill-down capabilities. Users can instantly compare QoE across operators, regions, or cells; identify performance anomalies; validate wholesale RAN agreements; and benchmark their service against competitors. The result is a living, data-driven view of network experience that supports churn reduction, NPS improvement, SLA enforcement, and strategic decision-making.

QoE AI Insights transforms raw crowdsourced telemetry into actionable intelligence. By combining device-level measurement, cloud-scale processing, and intuitive analytics, it empowers operators and MVNOs to understand—and improve—the real experience of their customers with unmatched precision and speed.

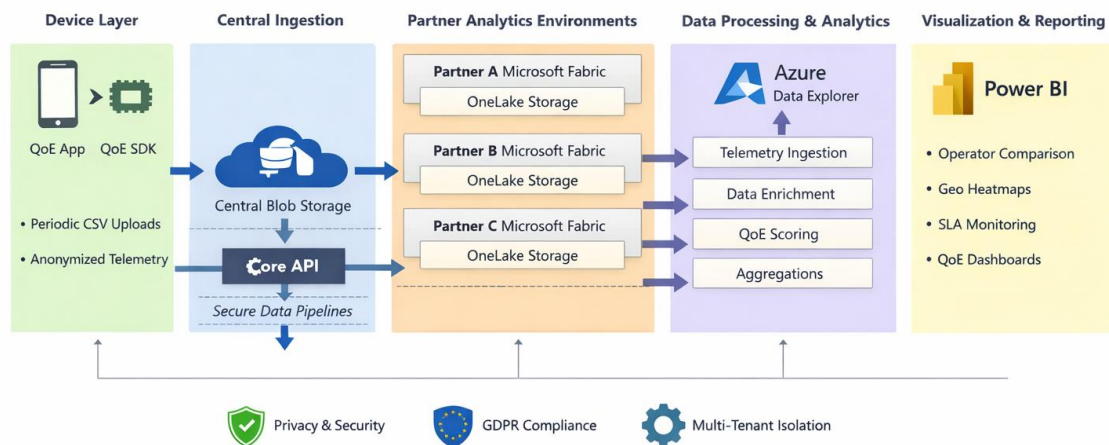
2 Contents

1	Executive Summary	1
3	Overview.....	4
4	Functional Architecture	5
4.1	High-Level Flow	5
5	QoEApp (iOS & Android)	6
5.1	Purpose	6
5.2	Core Functions.....	7
5.3	Platform Differences.....	8
6	QoESDK (Android)	8
6.1	Purpose	8
6.2	Key Functions.....	8
6.3	Differences vs QoEApp	8
7	Core API Backend.....	9
7.1	Role	9
7.2	Responsibilities.....	9
7.3	Security Model	9
8	Telemetry Ingestion Pipeline	11
8.1	Device Upload Workflow.....	11
8.2	File Format	11
8.3	Ingestion Jobs.....	11
9	Azure Blob Storage Layer	12
9.1	Structure.....	12
9.2	SAS Token Model	12
9.3	Operational Characteristics	12
10	Microsoft Fabric / ADX Analytics Layer	13
10.1	Ingestion	13
10.2	Data Modelling	13
10.3	Aggregations	14
10.4	Query and Data exploration.....	14
11	Power BI Dashboards	15
11.1	Audience.....	15
11.2	Key Visuals.....	15

11.3	Governance.....	16
12	Security, Privacy & Compliance.....	17
12.1	Data Minimization.....	17
12.2	Pseudonymization	17
12.3	GDPR & Regional Compliance.....	17
12.4	Access Control.....	17

3 Overview

QoE AI Insights is a modular, privacy-first platform for measuring, analysing, and improving real-world mobile network experience. It combines lightweight device telemetry, secure ingestion, multitenant data processing, and Fabric-based analytics to deliver actionable QoE intelligence for MVNOs, MNOs, regulators, and enterprise connectivity teams.



The system consists of four major components:

- **QoE AI Agent (aka QoEApp)** — standalone device based measurement AI Agent
- **QoESDK (Android)** — embeddable telemetry engine
- **Core API** — licensing, governance, and SAS token control plane
- **Analytics Layer (Fabric/ADX + Power BI)** — enrichment, scoring, dashboards

Key use cases include:

- **MVNO performance benchmarking**
Compare wholesale RAN performance across operators, regions, and cells.
- **SLA validation and RAN selection**
Support negotiations with host networks using objective QoE evidence, as well as alternative roaming partner / RAN selection.
- **MNO engineering and optimization**
Validate network changes, detect anomalies, and correlate QoE with radio conditions.
- **Regulatory and compliance monitoring**
Provide transparent, crowdsourced evidence of network quality.
- **Enterprise connectivity assurance**
Monitor employee or fleet connectivity across geographies.
- **Crowdsourcing deployments**
Collect large-scale, anonymized QoE data for market-wide insights.

4 Functional Architecture

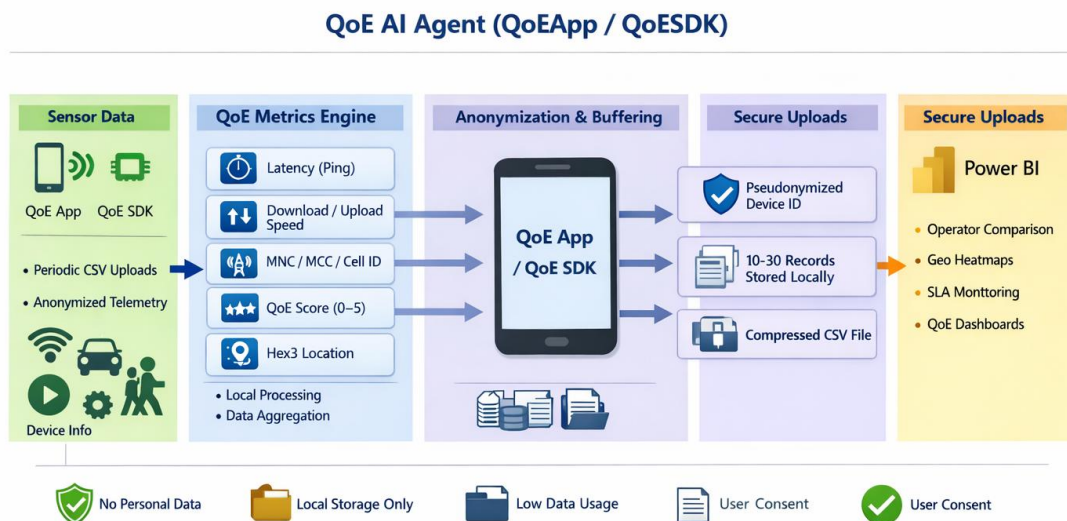
QoE AI Insights is built as a modular, AI-native architecture that connects device-level measurement with scalable ingestion, durable storage, and real-time analytics. Each component has a clear responsibility, and the interfaces between them are explicitly defined so the platform can evolve without breaking partners or deployed apps.

4.1 High-Level Flow

- 1. Device Measurement**
QoEApp and QoESDK collect network KPIs, compute QoE scores, and batch pseudonymized samples.
- 2. Secure Upload**
Devices request SAS tokens from the Core API and upload batches to Azure Blob Storage.
- 3. Crowdsourced Data Lake**
Blob Storage partitions data by partner, time, and geography.
- 4. Analytics & Modelling**
Fabric Real-Time Analytics (ADX) ingests, enriches, scores, and aggregates telemetry.
- 5. Insights Delivery**
Power BI dashboards expose operator comparisons, cell-level insights, and QoE trends.

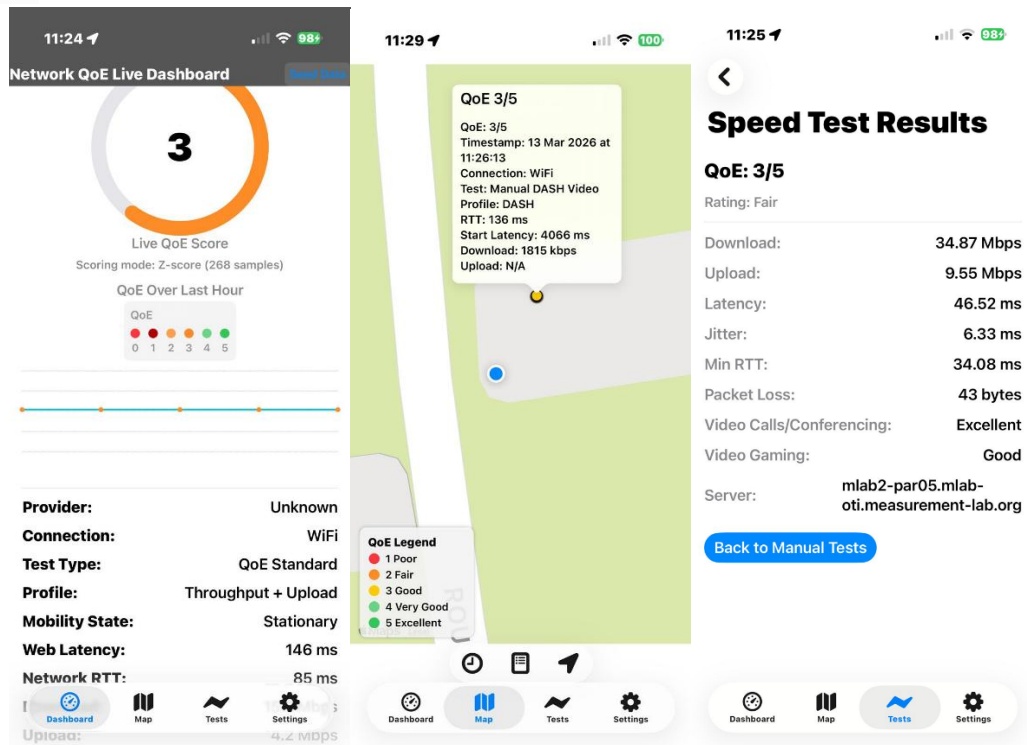
5 QoEApp (iOS & Android)

The QoEApp is the primary measurement client for the QoE AI Insights platform. Available on both iOS and Android, it provides passive background monitoring, high-precision active tests, local persistence, and map-based visualization. While the two platforms share a unified scoring model and consistent measurement philosophy, they differ in the depth of network metadata available due to OS-level restrictions — a key distinction highlighted in this section.



5.1 Purpose

- Passive, movement-aware QoE measurement
- On-device scoring
- Optional active tests (NDT7, DASH)
- Crowdsourcing mode for large-scale deployments



5.2 Core Functions

- **Passive Monitoring**
 - Android: distance and duration-based triggers
 - iOS: BGTaskScheduler + speed-based inference
 - Both perform periodic background monitoring of connectivity
 - QoE score (Latency, throughput UL/DL)
- **Active Tests**
 - NDT7 throughput and detailed TCP performance analysis
 - QoE score (Latency, jitter, drops/retransmission, throughput UL/DL),
 - Video Conference and Video gaming scoring
 - DASH video simulation
 - QoE score (stalls, start time, and throughput DL),
 - Quality (SD, HD 720, HD 1080, UHD),
- **On-Device Processing**
 - Local QoE scoring
 - Pseudonymization
 - Battery-aware scheduling



- **Upload Workflow**
 - Request SAS token
 - Batch 10–30 samples
 - Upload via HTTPS

5.3 Platform Differences

- **Android:** full radio metadata (MCC/MNC, LAC/TAC, CellID, RSSI/RSRP/RSRQ/SINR)
- **iOS:** limited radio metadata (RAT only), but full latency/throughput metrics

6 QoESDK (Android)

The QoESDK and the QoEApp share a unified measurement foundation, ensuring that all QoE data—whether collected by a standalone app or embedded inside a partner application—is directly comparable. However, the two components serve different purposes and operate under different constraints. This section highlights the shared capabilities and the critical differences between them.

6.1 Purpose

Provide partners with embedded QoE measurement identical to QoEApp, with minimal UX impact.

6.2 Key Functions

- Background execution model aligned with Android constraints
- Same scoring model and telemetry schema as QoEApp
- Partner-controlled configuration (sampling profiles, upload cadence)
- Lightweight API surface: start/stop monitoring, listen for live scores, trigger tests

6.3 Differences vs QoEApp

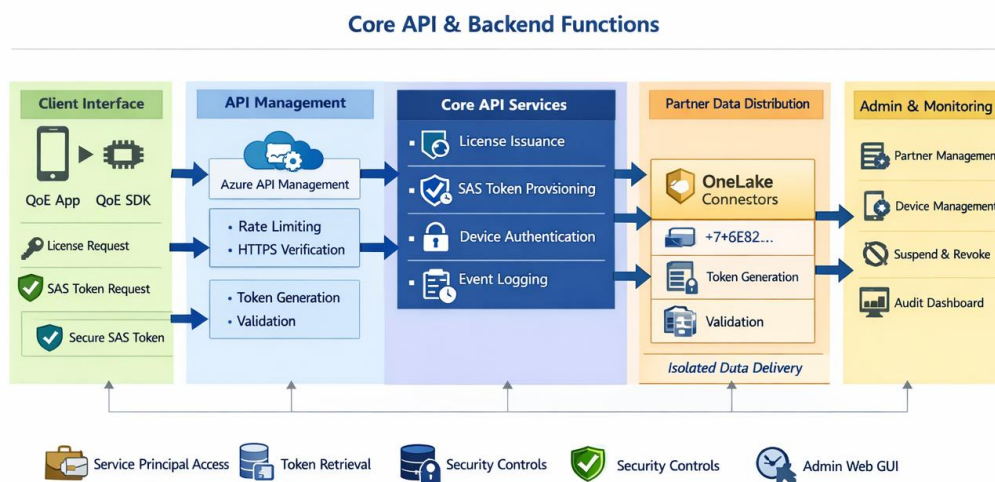
- No UI
- Partner app controls lifecycle
- Same telemetry, same scoring, same upload model

7 Core API Backend

The Core API is the control plane of the QoE AI Insights platform. Built as an Azure Functions backend with Cosmos DB as its primary data store, it provides secure, scalable services for partner management, device registration, licensing, SAS token issuance, and usage tracking. It is designed to support both the QoEApp/SDK clients and a React-based administrative UI.

7.1 Role

Central control plane for licensing, partner management, device lifecycle, and secure ingestion.



7.2 Responsibilities

- **Partner Management**
Create, suspend, revoke partners; manage entitlements.
- **Device Registration**
Issue device license, track lifecycle state.
- **License Issuance**
Validate partner quotas; enforce limits.
- **SAS Token Issuance**
Time-limited, write-only, partner-scoped tokens.
- **Rate Limiting & Abuse Detection**
Via Azure API Management.
- **Audit Logging**
All admin and device actions recorded.

7.3 Security Model

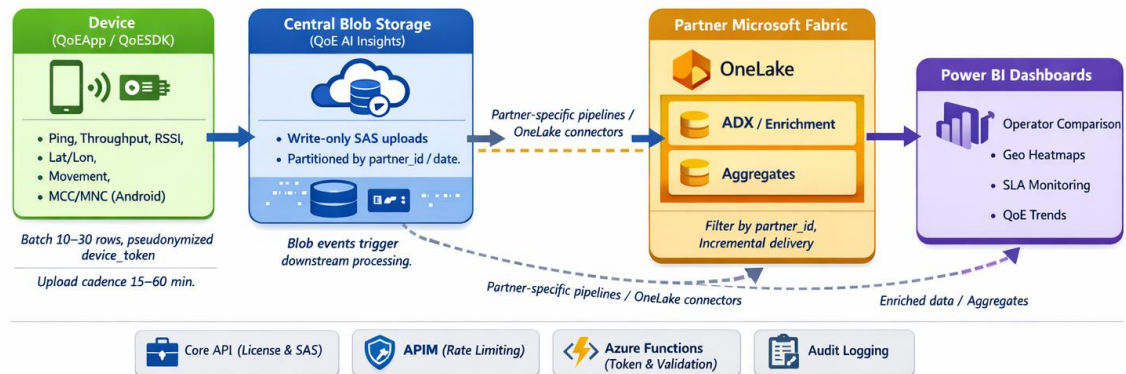
- OAuth2 for admin
- SAS tokens for devices



- Zero-secret client architecture
- Strict multitenant isolation

8 Telemetry Ingestion Pipeline

The telemetry ingestion pipeline is the backbone of the QoE AI Insights platform. It defines the complete, end-to-end flow of measurement data from devices in the field to the analytics environment in Microsoft Fabric. This pipeline is designed for scale, security, multi-tenant isolation, and cost efficiency, ensuring that millions of QoE samples can be ingested daily without bottlenecks or operational overhead.



8.1 Device Upload Workflow

1. Device requests license
2. Device requests SAS token
3. Device uploads batch to Blob Storage
4. Blob event triggers ingestion job

8.2 File Format

- Compressed CSV or JSON
- 10–30 samples per batch
- Includes partner_id, device_token, timestamp, metrics

8.3 Ingestion Jobs

- Schema validation
- Deduplication
- Enrichment (Hex3, operator lookup, movement smoothing)
- QoE scoring
- Write to ADX tables



9 Azure Blob Storage Layer

Azure Blob Storage serves as the **raw telemetry lake** for the QoE AI Insights platform. It is the first durable landing zone for all measurement data uploaded by the QoEApp and QoESDK. The design emphasizes multi-tenant isolation, zero-secret security, high throughput, and low operational cost.

This layer is intentionally simple, robust, and horizontally scalable — capable of ingesting millions of samples per day with minimal overhead.

9.1 Structure

- Per-partner containers
- Partitioned by date/hour
- Optional geography partitioning

9.2 SAS Token Model

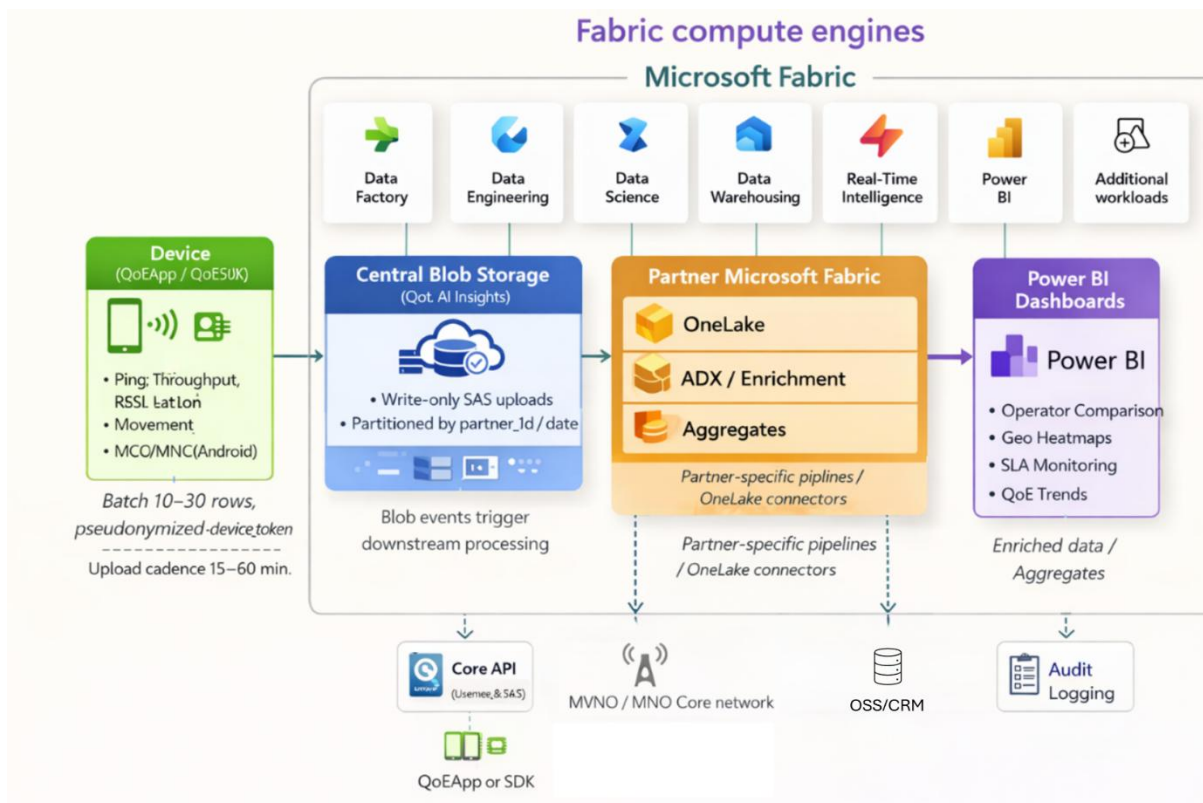
- Write-only
- Time-limited
- Scoped to partner container
- No secrets stored on device

9.3 Operational Characteristics

- Upload frequency: 15–60 minutes
- Typical batch size: 50–150 KB
- Local buffer: capped storage, oldest-first eviction

10 Microsoft Fabric / ADX Analytics Layer

Microsoft Fabric provides the analytics backbone for the QoE AI Insights platform. Each partner operates **their own Fabric workspace in their own tenant**, ensuring complete data isolation, governance autonomy, and compliance with regional or regulatory requirements. Real-Time Analytics (powered by Azure Data Explorer / ADX) ingests telemetry from Blob Storage, enriches it, and exposes curated datasets for dashboards, SLA reporting, and advanced analytics.



10.1 Ingestion

- Continuous ingestion from Blob
- Schema mapping and validation
- High-volume, low-latency processing
- Optional ingestion of network data (CDR, EDR, Alarms) to augment device QoE data.

10.2 Data Modelling

Dimensions include:

- MCC/MNC
- LAC/TAC
- CellID (Android only)
- Hex3 spatial tiles



- Movement state
- QoE score

10.3 Aggregations

- Per-sample
- Hourly
- Daily
- Per-cell (Android)
- Per-operator (Android)
- Per-region (gps)
- Per-Hex3 Cell (gps)

10.4 Query and Data exploration

- Direct KQL queries
- SQL endpoint access
- Spark notebook processing
- Real-time ingestion
- OneLake virtualisation shortcuts
- Power BI models
- ADX REST API
- Fabric item APIs
- External data pipelines
- Partner-scoped exports

More information and training for Microsoft Fabric can be found at [Microsoft Fabric documentation - Microsoft Fabric | Microsoft Learn](#)

11 Power BI Dashboards

Power BI provides the primary visualization layer for the QoE AI Insights platform. Each partner receives **their own Power BI workspace inside their own Microsoft Fabric tenant**, ensuring complete isolation of data, governance, and sharing boundaries. Dashboards are built on top of curated ADX/Fabric semantic models and expose real-time and historical QoE insights.

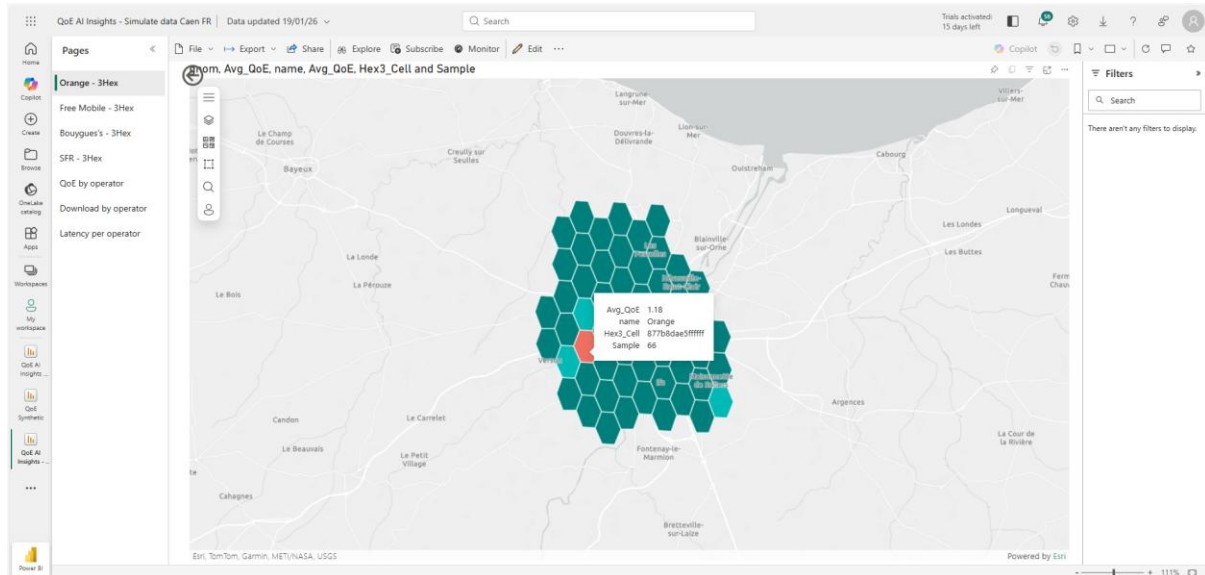


Figure 1: Hex3 Cell QoE analysis by region

11.1 Audience

- MVNO commercial, customer support, and engineering teams
- MNO commercial, customer support, and engineering teams
- Regulators
- Enterprise connectivity teams

11.2 Key Visuals

- Operator comparison
- MCC/MNC filtering
- LAC/TAC and CellID drilldowns
- Hex3 heatmaps
- QoE score distributions
- Trend analysis

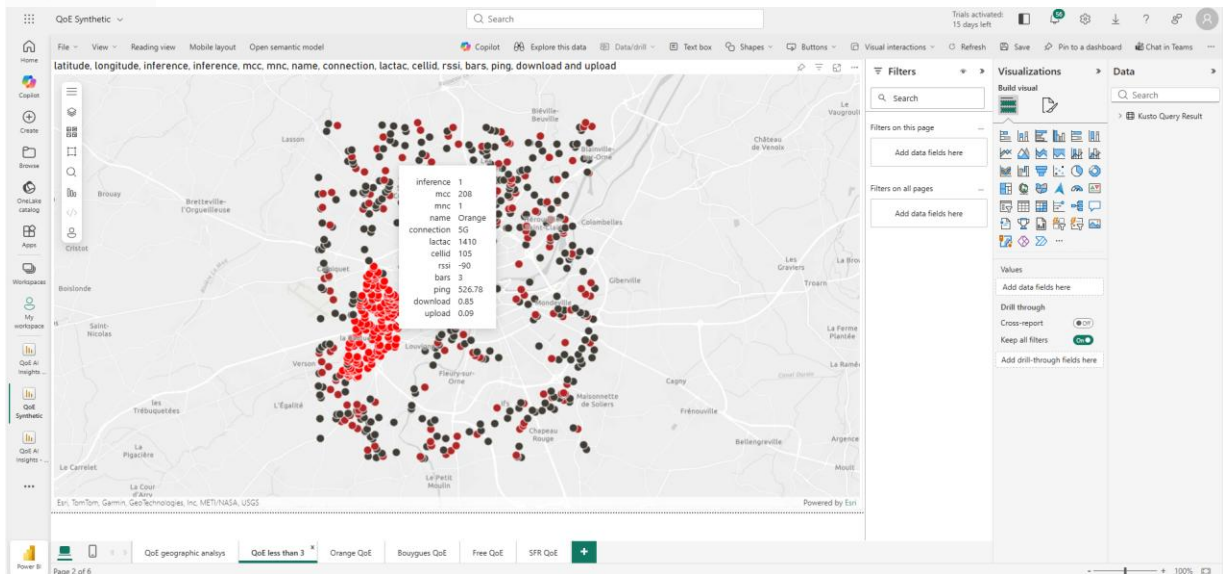


Figure 2 : Filtered view of low QoE scores

11.3 Governance

- Workspace-level access
- Row-level partner isolation
- Audit logging
- Optional Microsoft Purview (data governance)

More information and training about PowerBI can be found at [Power BI documentation - Power BI | Microsoft Learn](#)

12 Security, Privacy & Compliance

Security and privacy are foundational to the QoE AI Insights platform. The system is designed using **privacy-by-design**, **zero-secret architecture**, and **strict tenant isolation** principles. No personal data, content, or identifiers are collected; all telemetry is pseudonymized, minimized, and processed within each partner's own Microsoft Fabric tenant.

12.1 Data Minimization

- No personal identifiers
- No advertising IDs
- No reverse-geocoding on device

12.2 Pseudonymization

- Randomized device tokens
- No persistent identifiers

12.3 GDPR & Regional Compliance

- Regional deployment options
- Partner-scoped isolation
- Transparent data handling

12.4 Access Control

- RBAC for admin
- SAS tokens for devices
- Least-privilege model