Fellowwind

Real-Time Analytics at scale in Fabric

A unified analytics solution for the era of AI

smart
casual
datadesign

redgate

TIMEXTENDER

b.telligent

Brian Bønk Rueløkke

Principal & Enterprise architect, Data & AI

Fellowmind

https://linkedin.com/in/brianbonk
https://brianbonk.dk
https://github.com/brianbonk

MVP Microsoft Most Valuable Professional

Microsoft
FastTrack Recognized
Solution Architect
Power BI
2022 >>

Microsoft
Certified Trainer
Data Platform

2018 >>

Jaques Cousteau
1910-1997

Fellowwind

Jaques Cousteau
1910-1997

The history of Kusto

Azure Sentinel

Log Analytics

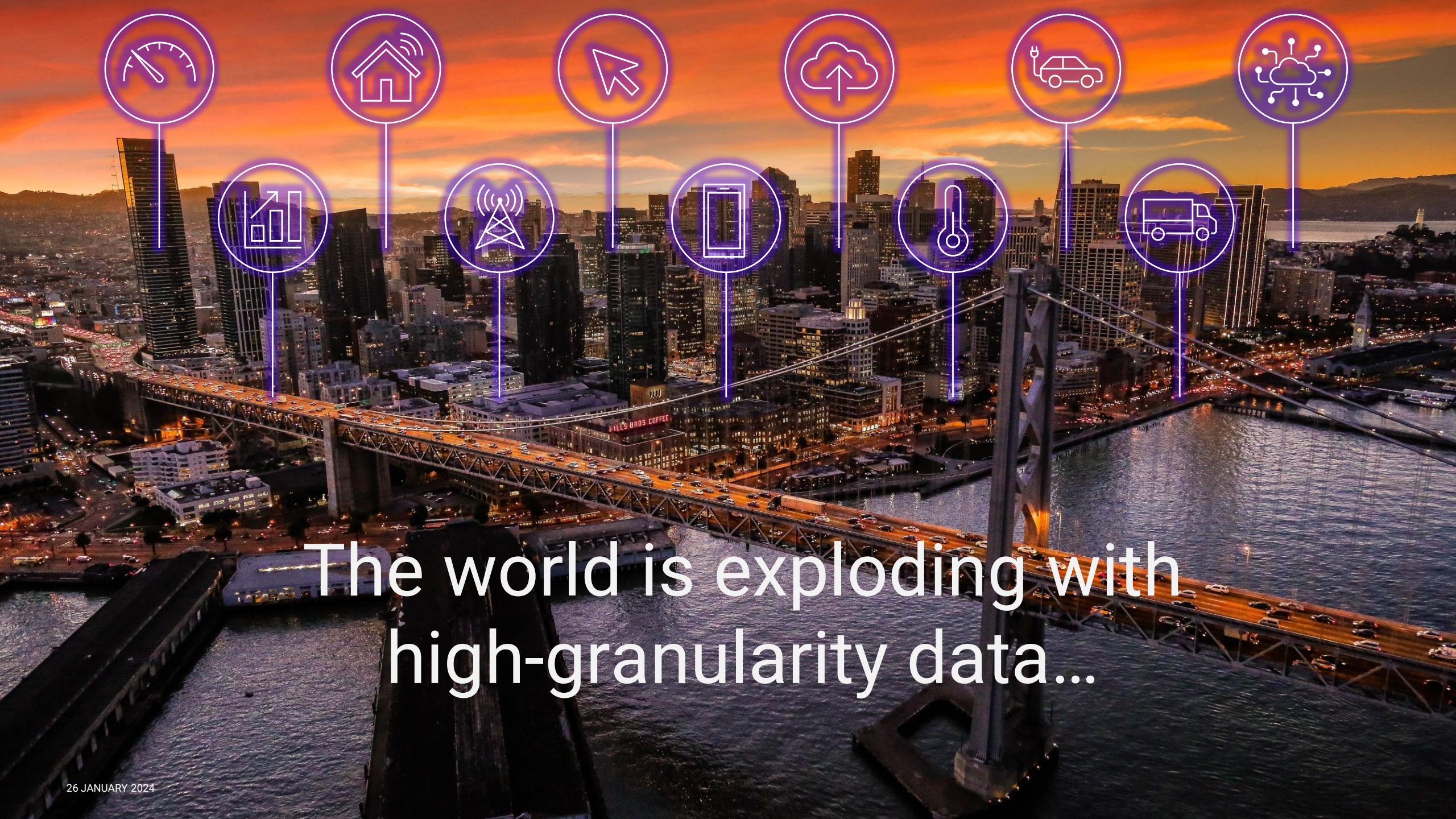
Real-Time Analytics

Azure resource graph

Microsoft 365 Defender

CMPivot

CMPivot



The world is exploding with high-granularity data…

It all starts with data

Telemetry – a key data for digital transformation

Telemetry – a key data for digital transformation

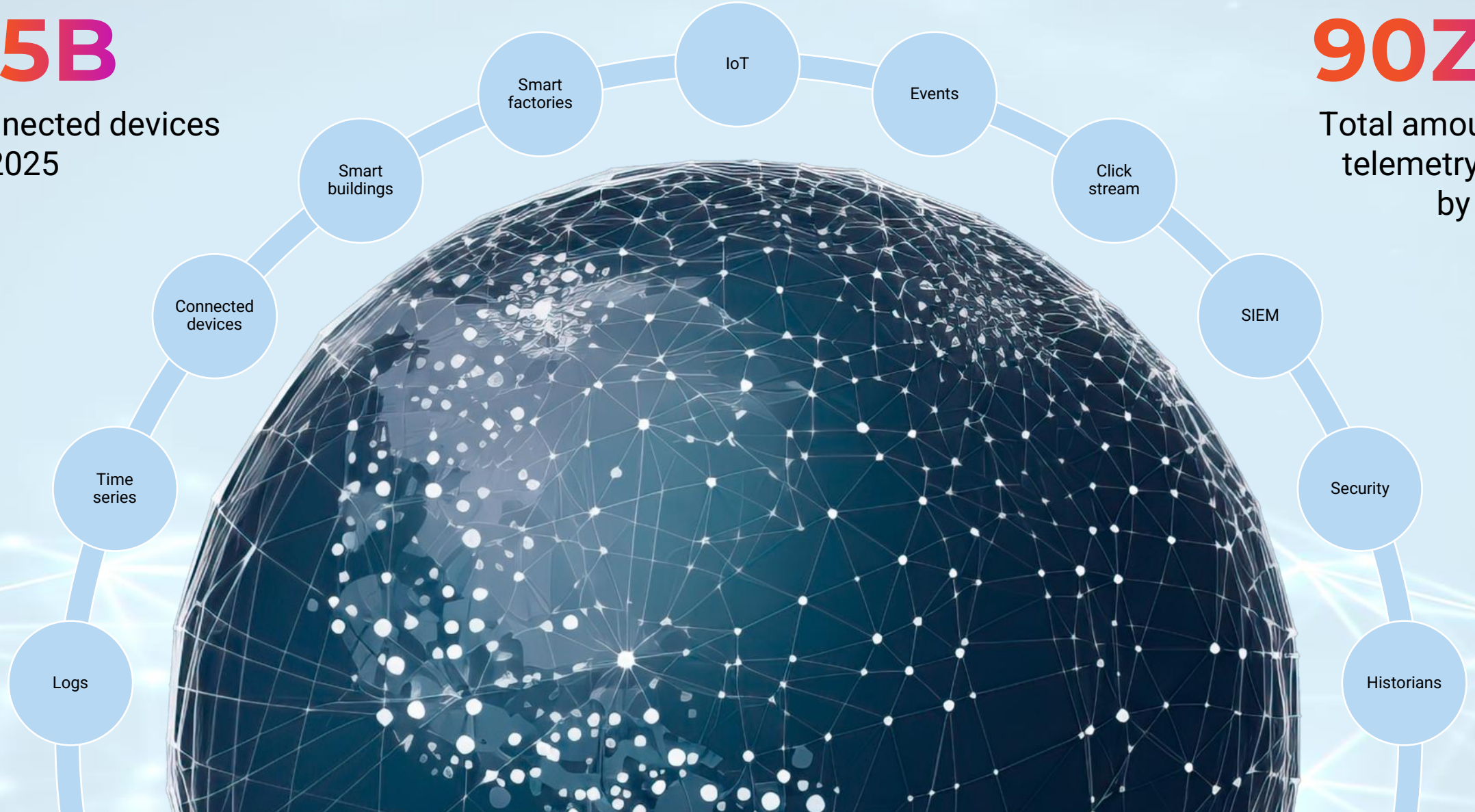
Telemetry – a key data for digital transformation

75B

Connected devices by 2025

90ZB

Total amount of telemetry data by 2025



Digital transformation

Cybersecurity
Asset tracking and management
Predictive maintenance
Supply chain optimization
Customer experience
Energy management
Inventory management
Quality control
Environmental monitoring
Fleet management
Health and safety

Microsoft Fabric

Get data

Data Factory

Prepare data

Synapse Data Engineering

Synapse Data Warehouse

Synapse Data Science

Synapse Real-Time Analytics

Use data

Power BI

Data Activator

Store data

OneLake

Microsoft Fabric

Get data

Data Factory

Prepare data

Synapse Data Engineering

Synapse Data Warehouse

Synapse Data Science

Synapse Real-Time Analytics

Use data

Power BI

Data Activator

Store data

OneLake

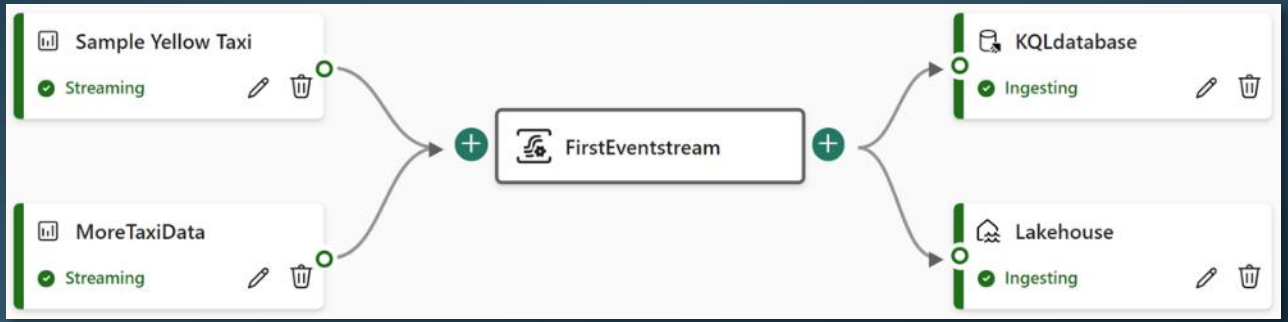
Fabric Real-time Analytics solution enables organizations to consume **vast amount of data**, focus and **scale up** their Analytics solution with **data in motion, empower** their business analysts, and **democratize their data** for citizen data scientists and Data Engineers

Synapse Real-Time Analytics

Streaming data with ease

EVENTSTREAM

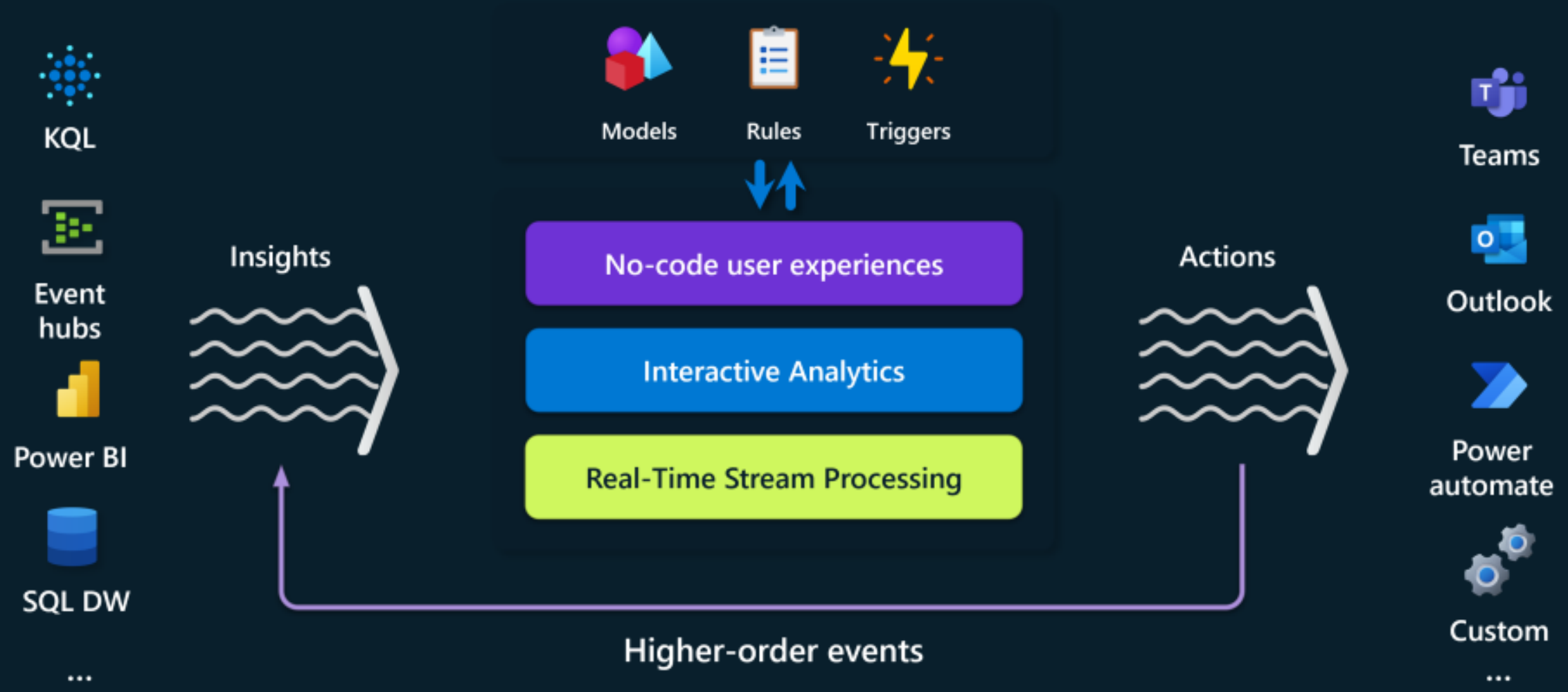
The brand-new event stream service, leverages the ability to get data from several sources of streaming data and save it to a wide variety of destinations, including OneLake, KQL databases and Azure services.



The service computes the data once and can pipe it out to several destinations at once. All configured and maintained from within the Microsoft Fabric portal and “coded” with your mouse.

Imagine scenarios of IoT devices loading data to both the data warehouse and other 3-rd party destinations – this can now be done using the low-code approach from Event Stream.

Data Activator



KQL database
Key capabilities

Unlimited Scale (query, ingestion and storage)

Any data source

Any data format

Structured
Semi-structured
Free-text

Real-time transformation og complicated data strcutures

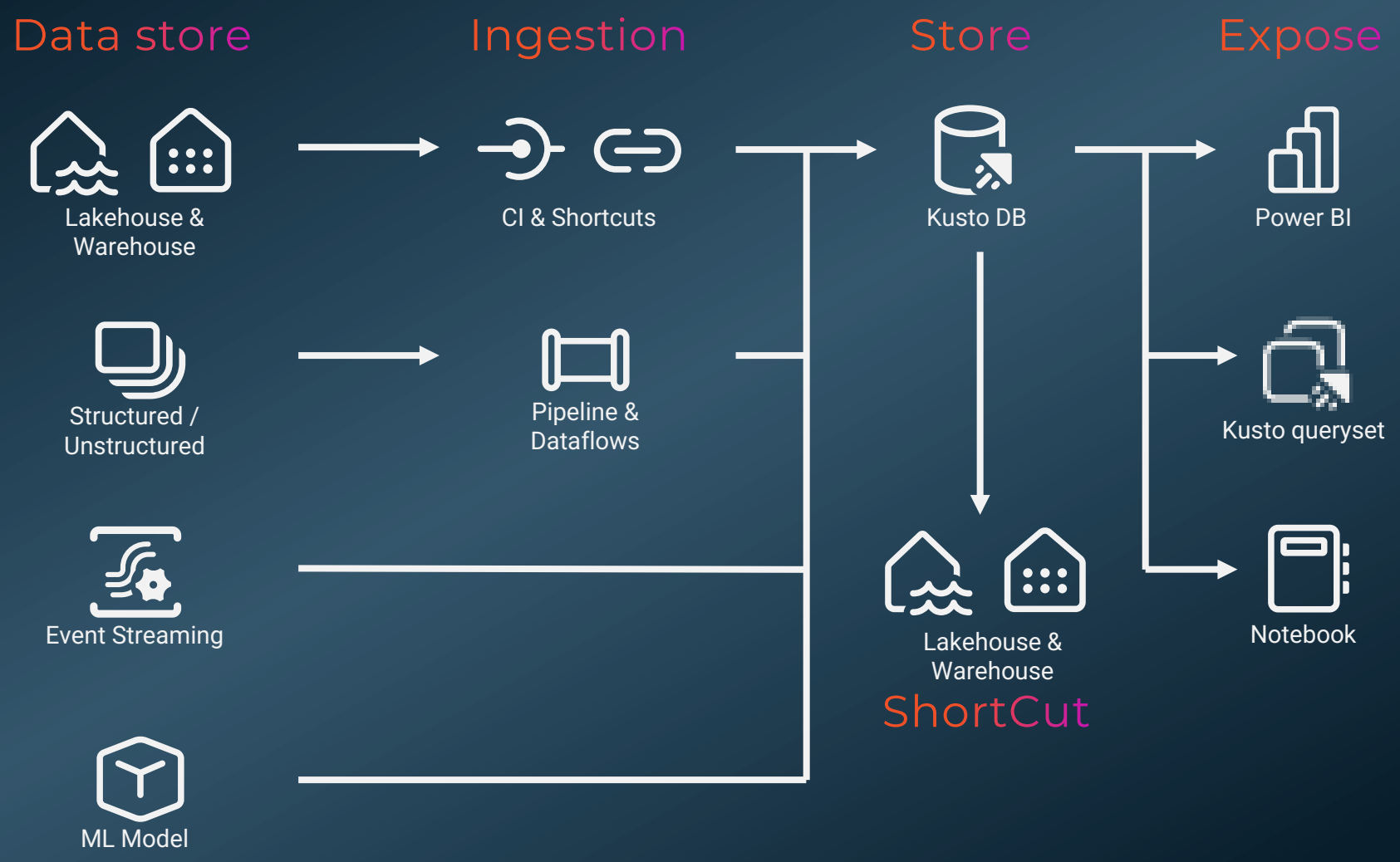
Streaming analytics in Near-Real-Time

High performance
Low latency
High freshness

Timeseries database

Everything is indexed and partitioned

Real-Time Analytics

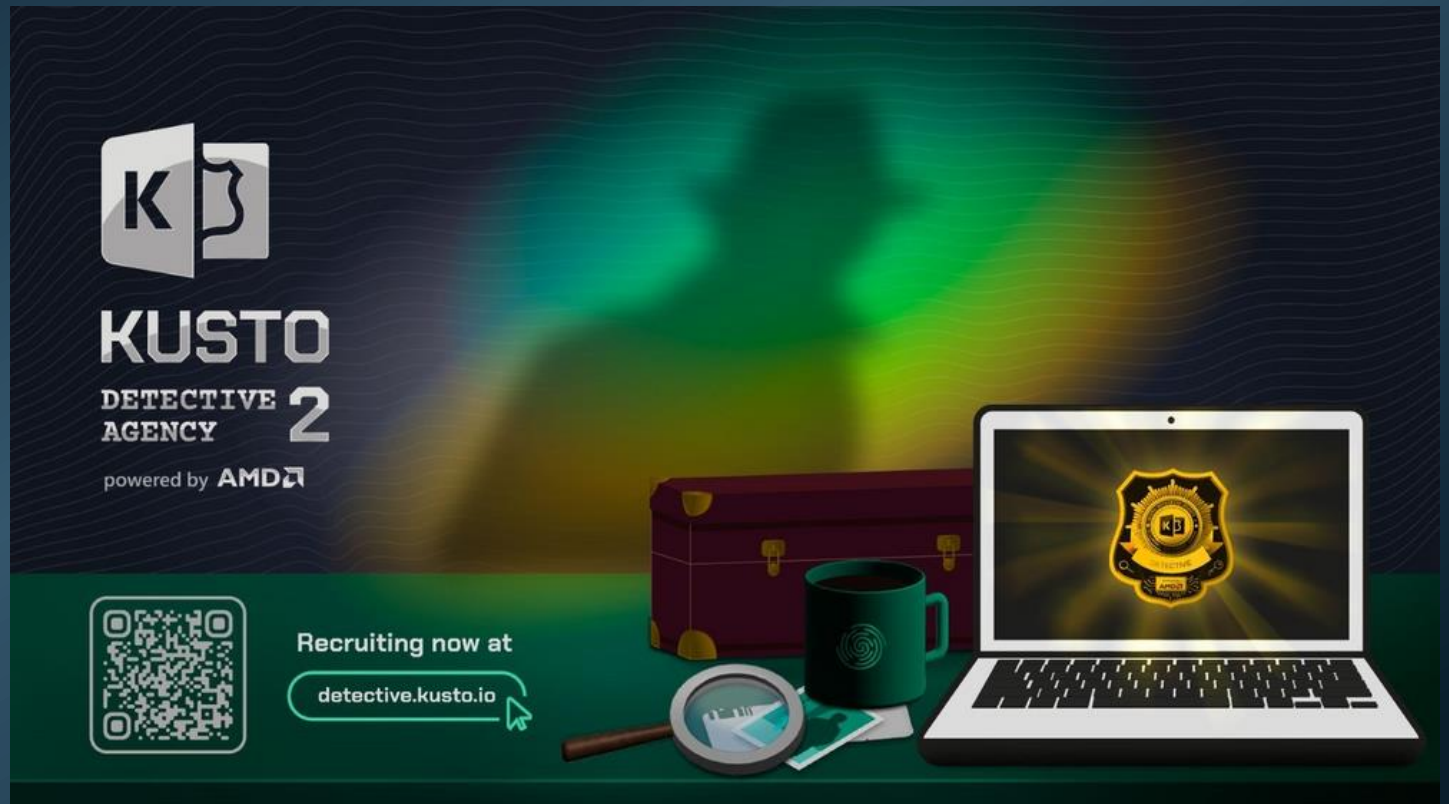


Fellowwind

Get started for free

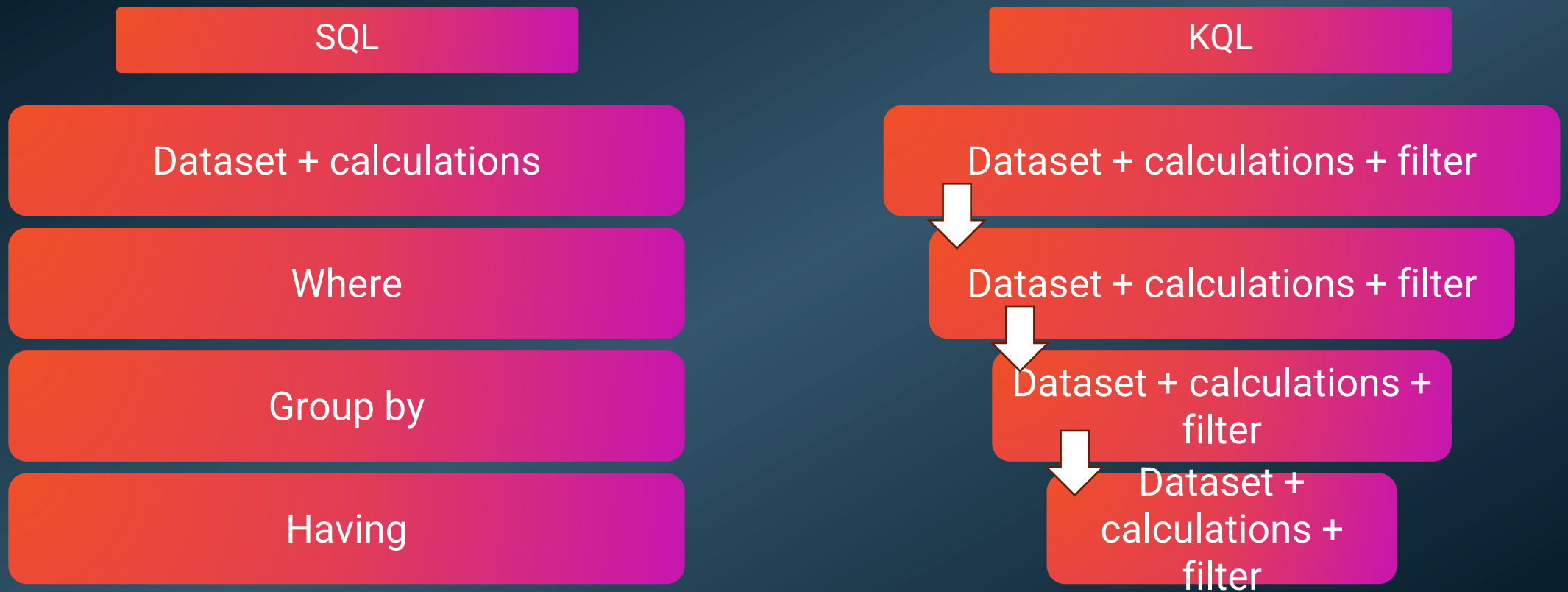
https://dataexplorer.azure.com/freecluster

https://detective.kusto.io



Fellowwind

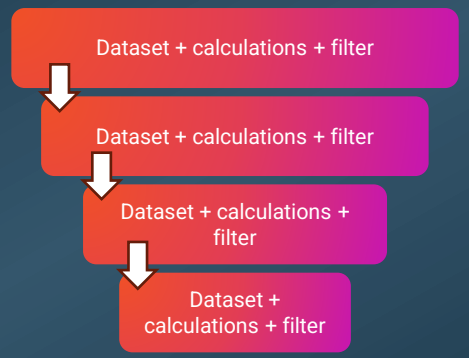
The language and structure



SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

KQL




```
NYCTaxi
| where passenger_count > 1
| project passenger_count, total_amount, VendorID, fare_amount
| extend AmtPsngr = total_amount / passenger_count
| where AmtPsngr > 10
| summarize TotalAmount = sum(total_amount), AvgAmtPsngr = avg(AmtPsngr) by VendorID
| where VendorID  <> 1
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

Forget everything you know about

query performance vs data types
&
data modelling best practices

Data modelling Kusto in Power BI

- Single table reporting can be a good option, if you can include all columns from dimensions to the table
- M:M relations are hard to avoid, but not a big deal → all queries will be translated to KQL
- All dimensions must be tagged with “IsDimension=true”
- Dimensions can be imported if they are <1 mio rows.
- INTEGER and DECIMAL er slow joins compared to STRING

Harness the Power (BI) of Kusto

Let Power BI build the KQL

- In Power Query
- Using DAX

Or build a Kusto function

DEMO

Live coding

(hopefully no demo-ghost 👻)

Harness the Power (BI) of Kusto

```
.create-or-alter function GetSysLogs(TimeWindow:string , Bucket:string )
{
cluster('help').database('SampleLogs').RawSysLogs
| where timestamp > ago(totimespan(TimeWindow))
| summarize LogCount=count() by name, bin(timestamp,
totimespan(Bucket))
| order by timestamp asc
}

GetSysLogs('5d','1h')
```

Analysis and reporting

Dashboards in RTA - planned - to come…

Real-Time Analytics

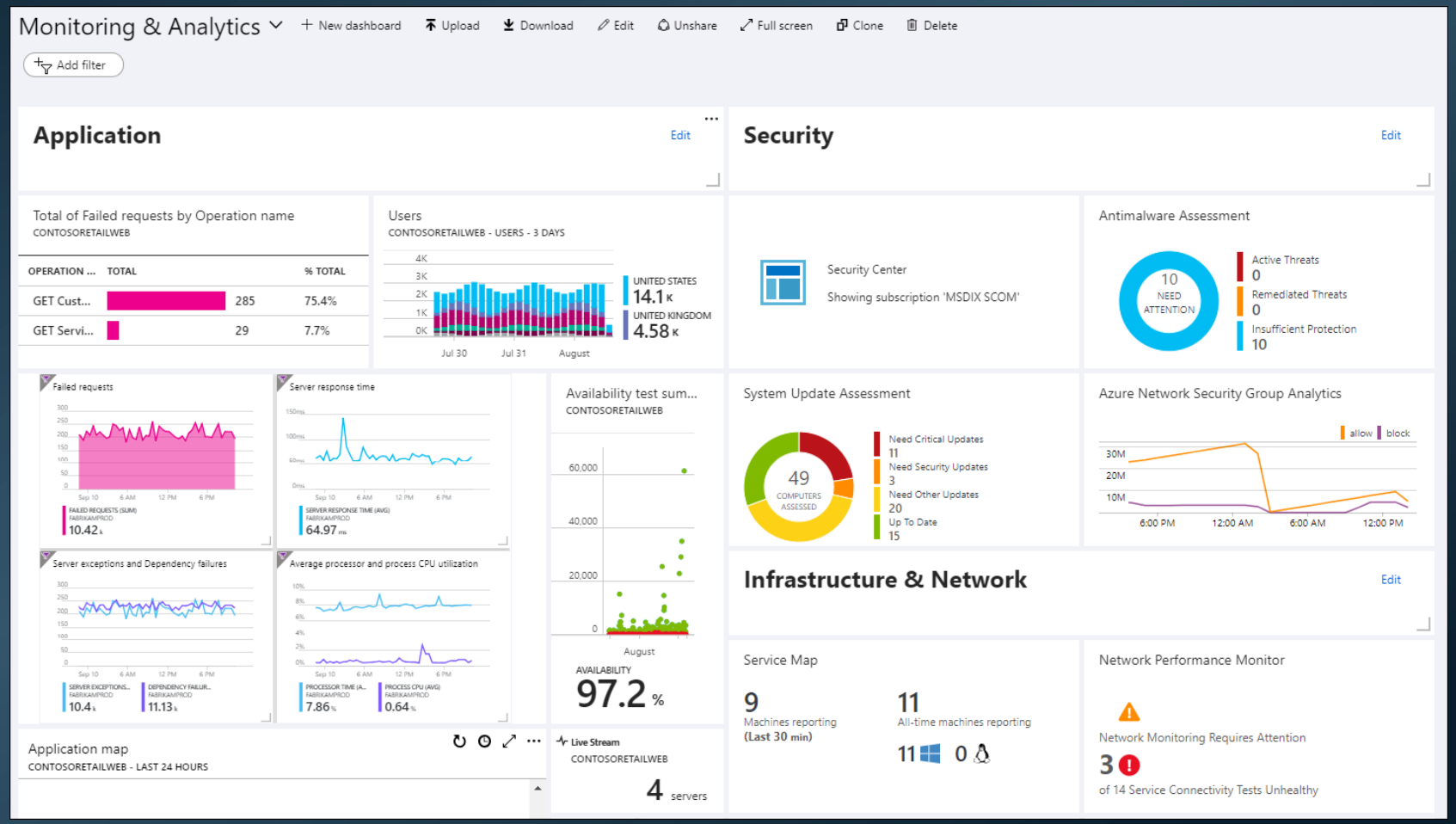


Image from James Westall

Fellowwind

Thank you

Connect with me at:

https://linkedin.com/in/brianbonk
https://brianbonk.dk
https://github.com/brianbonk

Session feedback