Microsoft

sqlbits 2023

Azure Data Explorer – a Torch in the Dungeon of Observational Analytics

Pawel Potasinski
Senior Program Manager
@pawelpotasinski
/in/pawelpotasinski

Guy Reiginano
Product Manager
@GuyReginiano
/in/reginiano


Long time ago, not so far away…

Necessity is the Mother of Invention

Do You Recognize This Person?

Jacques-Yves Cousteau -> Kusto

Proven Technology

In production since 2015 for internal Microsoft workload, GA since Feb 2019.

Battle tested for Microsoft internal workload

Windows
Skype
LinkedIn
Visual Studio
SQL
Bing
Microsoft Azure
Xbox
Power BI
Office

The platform for analytical solutions (SaaS)

Azure Monitor
Log Analytics,
Application Insights

Security Products
(MS Defender for Endpoint (MDATP),
MS Sentinel, MS Defender for IoT, MS Defender for Cloud Apps (MCAS))

Azure IoT Central

PLAYFAB
Gaming platform

Available as PaaS

esri
DocuSign
Check Point SOFTWARE TECHNOLOGIES LTD.
Taboola
ZOOMD KNOW MORE, DO MORE.
ECOLAB
BÜHLER
agl
BASF We create chemistry
Grab
BOSCH Invented for life
UPTAKE
Orchestrating a brighter world
NEC

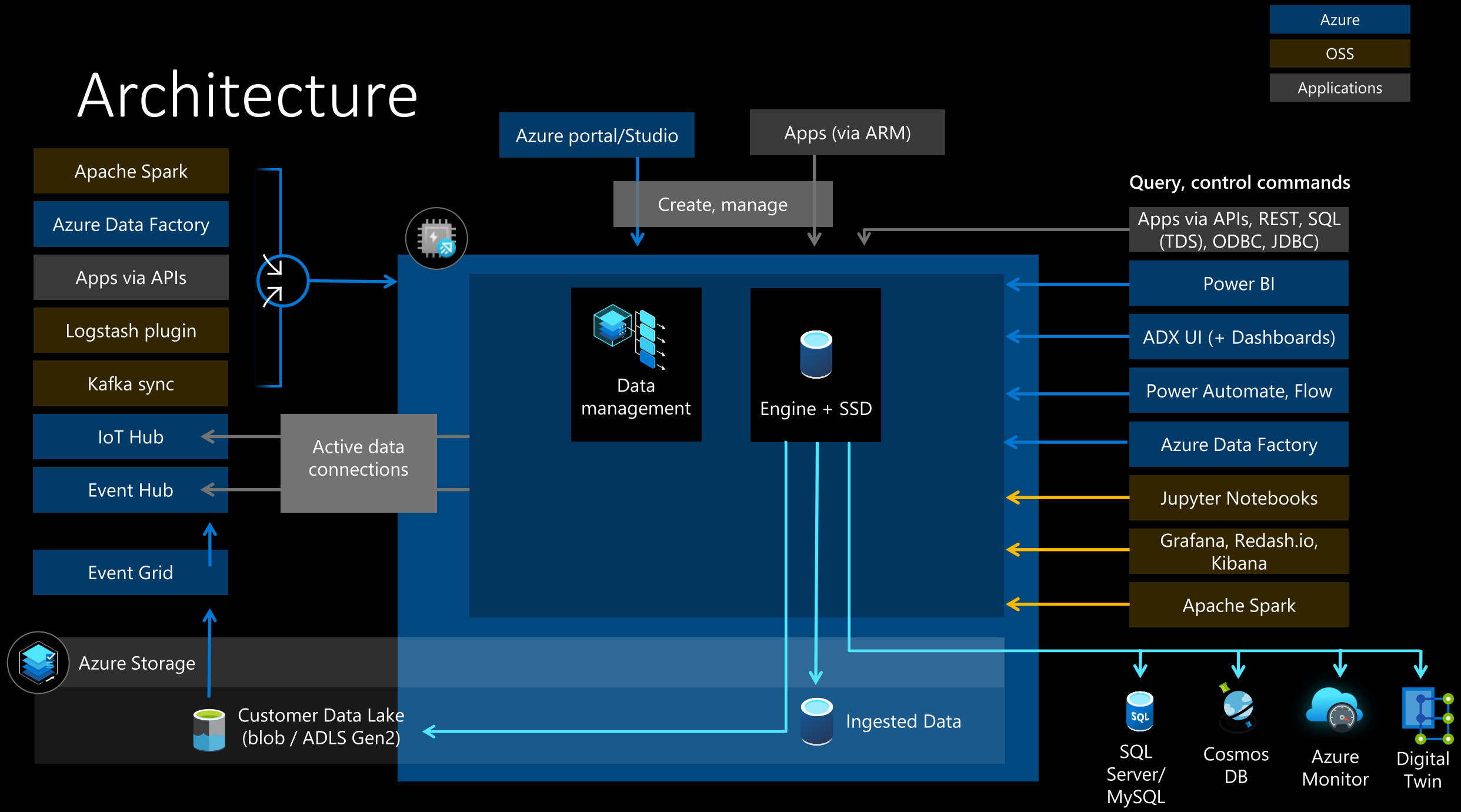
https://aka.ms/adx.customers

Introducing Azure Data Explorer aka Kusto!

A big data analytics cloud platform

optimized for interactive, ad-hoc queries

Architecture



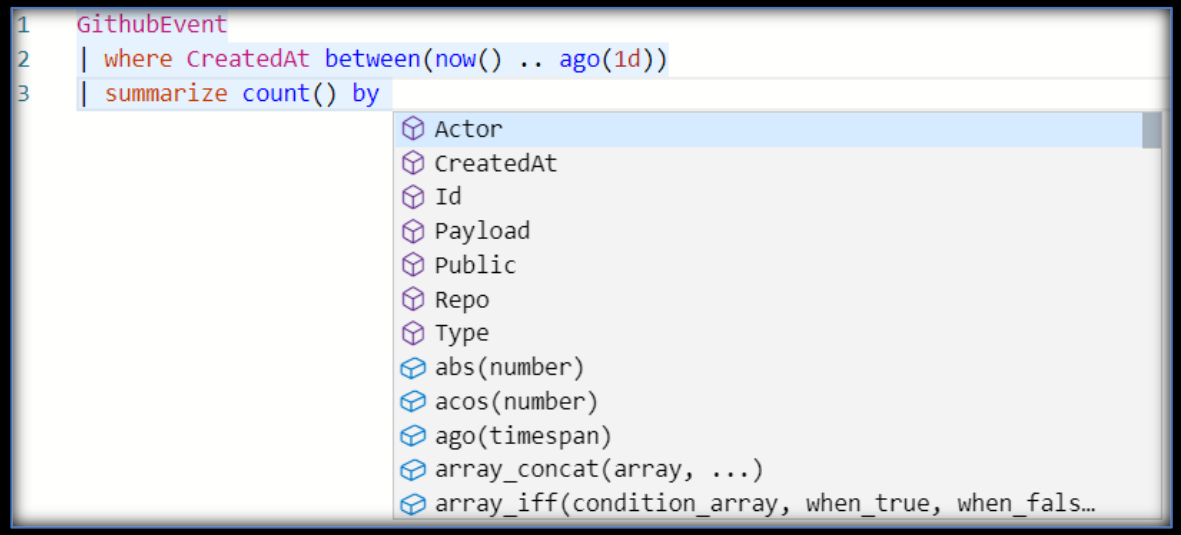
Kusto Query Language (KQL)

Simple and powerful

- Rich relational query language
- Built-in full-text search, time series, user analytics, geospatial, and machine learning operators
- Out-of-the box visualization
- Easy-to-use syntax + IntelliSense
- Highly recognizable hierarchical schema entities

Extensible

- T-SQL
- In-line Python and R

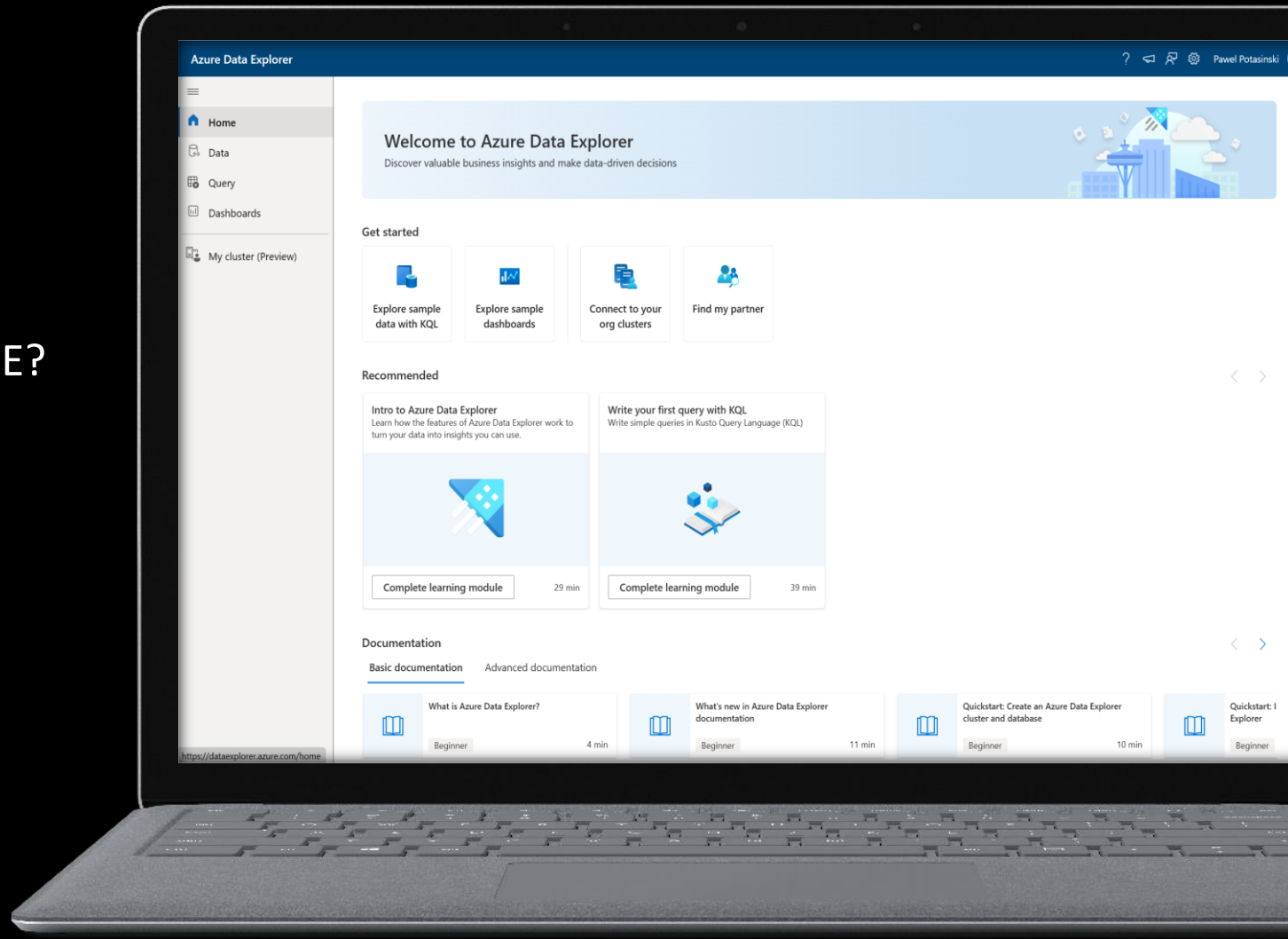


Example

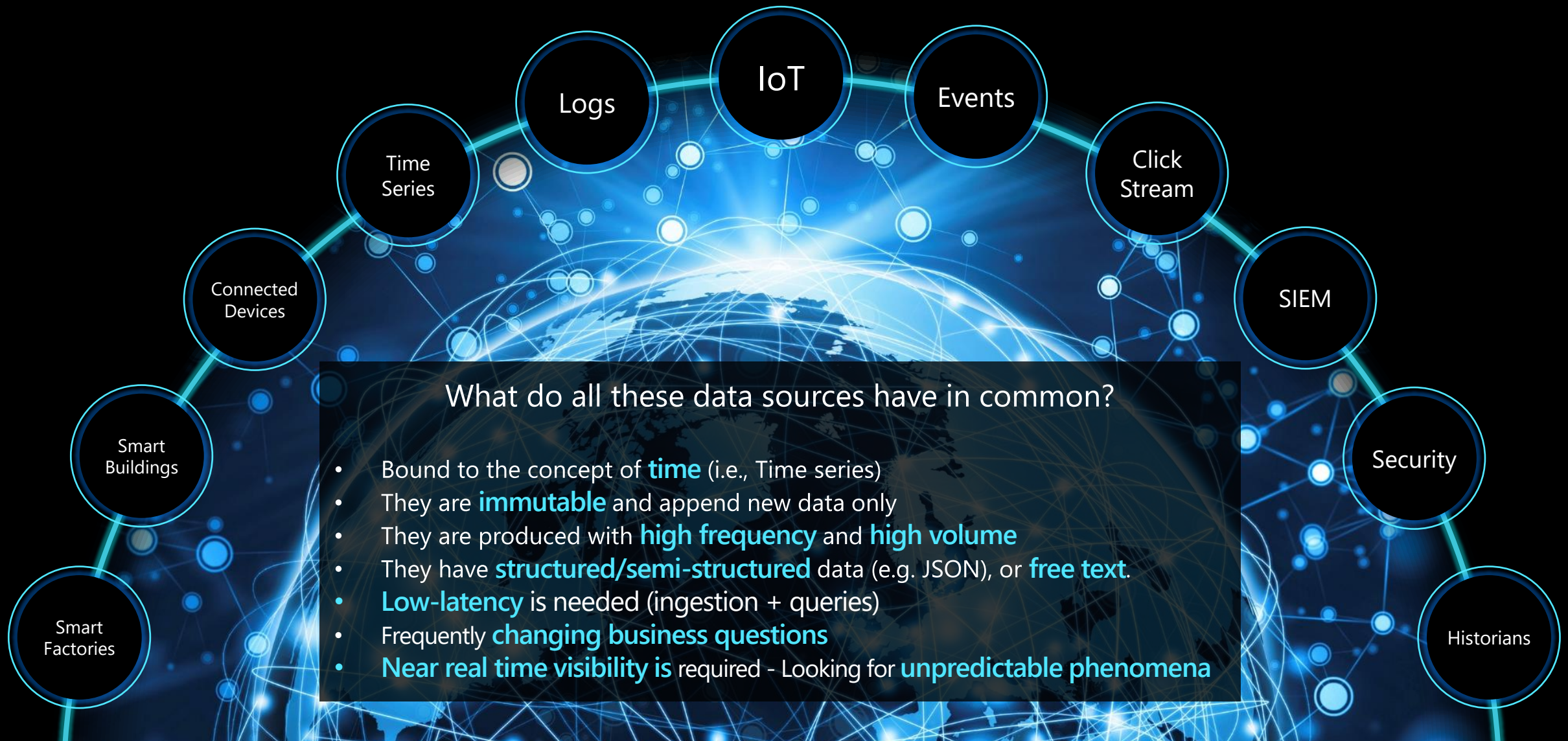
```
StormEvents
| summarize event_count=count(), mid = avg(BeginLat) by State
| sort by mid
| where event_count > 1800
| project State, event_count
| render columnchart
```

DEMO

1. How to start playing with Kusto for FREE?
2. Data ingestion
3. Observational analytics with KQL
4. ADX integration with other tools and services



Scenarios for Azure Data Explorer



What do all these data sources have in common?

- Bound to the concept of **time** (i.e., Time series)
- They are **immutable** and append new data only
- They are produced with **high frequency** and **high volume**
- They have **structured/semi-structured** data (e.g. JSON), or **free text**.
- **Low-latency** is needed (ingestion + queries)
- Frequently **changing business questions**
- **Near real time visibility is** required - Looking for **unpredictable phenomena**

Azure Data Explorer Community Resources

Product

- ADX Product Page: https://aka.ms/adx.pp
- ADX 101: https://aka.ms/adx.blog.101
- Documentation: https://aka.ms/adx.docs
- Technical whitepaper: https://aka.ms/adx.techwhitepaper
- Cost estimator: https://aka.ms/adx.cost
- Customer stories: https://aka.ms/adx.customers
- Preloaded open "help" ADX cluster: https://aka.ms/adx.try

Start for free: https://aka.ms/adx.free

Blogs, Videos, Forums

- Blog: https://aka.ms/adx.blog
- YouTube channel: https://aka.ms/adx.youtube
- ADX intro video: https://aka.ms/adx.intro
- Reference architectures: https://aka.ms/adx.architectures.video
- Stack overflow: https://aka.ms/adx.sof

Social Media

- Twitter: @AzDataExplorer
- LinkedIn: https://www.linkedin.com/company/adxkusto/

KQL

- KQL tutorial: https://aka.ms/adx/query.tutorial
- KQL cheat sheets:
  - https://aka.ms/SQL2KQL
  - https://aka.ms/ADX.KQL.Quick
  - https://github.com/marcusbakker/KQL
- Learn and practice KQL: https://github.com/rod-trent/MustLearnKQL
- KQL overview video: https://adx.kql.video

Free Online Learning

- Learn ADX for free: https://aka.ms/adx/start
- Learn how to query data using KQL: https://aka.ms/ADX.Learn.Queries
- Activate free benefit at Pluralsight: https://aka.ms/adx.pluralsight
- ADX courses at Pluralsight:
  - https://aka.ms/adx.pluralsight.how-to-start-with-adx
  - https://aka.ms/adx.pluralsight.azure-data-exploring
  - https://aka.ms/adx.pluralsight.kql-from-scratch
  - https://aka.ms/adx.pluralsight.advanced-kql

aka.ms/ADX.links

Join Kusto Detective Agency!

Solve complex riddles using Kusto and your data exploration skills!

https://detective.kusto.io/

Earn your badges and deserved fame if you dare!

Your Feedback Matters!

https://sqlb.it/?10314

Microsoft

sqlbits 2023

Azure Data Explorer – a Torch in the Dungeon of Observational Analytics

Pawel Potasinski
Senior Program Manager
@pawelpotasinski
/in/pawelpotasinski

Guy Reiginano
Product Manager
@GuyReginiano
/in/reginiano