UPTAKE

Operational Technology Data, The Key To Your Digital Transformation

People of the world are becoming increasingly aware that there is data about them collected, kept, and used to keep track of them. As their understanding continues to improve, they are growing more concerned about their data privacy. Regulations like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and HIPAA all empower citizens to exercise their data rights.

In a similar fashion, companies are realizing that they've gathered a great deal of information about their production processes and all of the things that are necessary to keep them running. In the past, they've done this for reasons such as; maintaining compliance with applicable standards, product traceability, adherence to reliability standards, etc. Now there's a growing awareness that all of the data about what they've done could help them better perform in the future.

OT Data, or operational technology data, is data about a company's production processes. Operational or operating technology data is about the process control systems and their execution that a company utilizes to control its production equipment. OT data is also data used by the control systems to derive other data, to respond to process upsets, and to perform specific tasks. As products are produced, so too is data produced. The settings of the systems-the configuration settings for assets and control algorithms, all represent additional operational technology data that has been kept in history.

Companies operating today are under additional pressures beyond proving their compliance with government regulations and international standards. Now they need greater levels of empirical proof of their operating parameters as they relate to environmental concerns. It isn't enough to just produce things, and measure how much went into the things, or how many were produced. It's no longer enough to implement automation and control systems to run your production processes and set up those systems to 'log data to the historian'. Now, in order to survive, you need to use all of the data you've kept.

Competition, increasing costs, strained supply chains and labor shortages are all placing companies under more pressure. The pressure to operate profitably while being affected by all of these constraints has caused many companies to understand that in order to get better, they need to understand their operations and themselves better!

They've also finally realized that the best way by which to understand themselves is to analyze all the data about themselves and their operations that they've gathered and kept for twenty years! That data, a history of how they've operated, how well they've controlled all the processes that produce their products, also has trapped within it all the knowledge that would help them do it better. Now. So all of the production processes information they've logged and historized has a great deal of value. Anything valuable needs to be protected.

At Uptake, we believe industrial companies should exercise their operational technology (OT) data rights. Industrial machines produce operational data that can be analyzed for insights on how to make machines run better, how to make them run more efficiently. A company should analyze all of their data, in fact they have the right to analyze their data, in order to know what to do and where to do it next. Companies are realizing now that their operational data holds the key to unlock profit.

If you own the machine, you should also own the data coming from it. There's still the value of the data about the health and behaviors of the equipment now. The analysis of this data is something else that you 'own' and can do when you're ready. But that data and its unrealized value can be at risk if you don't take cyber security measures to protect access to it. No vendor, no competitor, and certainly no cyber criminal should take over ownership of your company's machine or its data for good or ill purposes. It's your data.

This paper outlines why Uptake honors your company's OT data rights. It discusses the business case for moving your OT data to the cloud and using it, and identifies some safety and security concerns that can impact your data. By the paper's end, you'll understand your data rights, and have a better idea of how to protect your OT data on-premise and in the cloud.

Treat Your Data Not Only As An Asset But A Protected One

See your company's industrial data as a proprietary asset, just like inventory, products, and equipment. Doing so will help you achieve what we believe in at Uptake. It's your data, regardless of whether it resides at your facilities, in your datacenter, and/or your cloud or a partner cloud environment.

Uptake's Dr. Dave Shook, Chief Digital Officer and a Microsoft MVP, puts your company's data rights this way.

“”

You should never have to surrender control of your data to anyone else.

As much as you should treat your data as a proprietary asset, its greatest value lies in open availability for consumption by your users. Digital transformation requires open access to data from across the organization. Data shared is knowledge gained. Past practices and technologies produced data silos, which created information silos and reinforced organizational silos. Open access to data allows digital transformation, breaking down silos and releasing the data, so that the knowledge and creativity of your users can be applied.

The challenge of data ownership stems from when industrial companies engage original equipment manufacturers (OEMs) and SaaS companies in digital transformation initiatives. From the perspective of the SaaS company, the digital transformation journey begins with you, the customer, sharing your data with them. The SaaS company needs your data so that it can do something with it, to show results with their solutions. It's as if SaaS companies have a rule regarding customers and cloud. Their rule: vendor cloud, multi-tenant. It means the SaaS company welcomes you to their cloud, and all the other customers in the vendor cloud are welcome. Your data cohabitates with other companies' data in the SaaS company's cloud.

At Uptake, we have our own rule that reflects our integrity with OT data rights in the cloud. Our rule: single tenant, customer tenant. It means when your data resides in the cloud, most likely on the Microsoft Azure platform or with Amazon Web Services (AWS), you're in complete possession of your data stored in your tenant-often referred to as a data lake or estate. The only time Uptake stores customer data on its cloud tenant is if the customer lacks one. Even then, it's a temporary basis with a noted transfer date.

When transferring data (time series, historical, real time) to the cloud for advanced analytics, there are other elements to consider. Your math computations, the applications you use, and the amount of data you analyze will all have an impact on your existing infrastructure. The problems that you can identify solutions for, additional benefits you may realize based upon actions you could take, all can have impacts upon your infrastructure. You own that infrastructure that moves and shares your data, you own all the data you've collected over the years, and you own everything that you learn from your data.

At Uptake, we treat a company's data and all its hardware/software and infrastructure as proprietary to the company, essential for protection by safety and security measures. It's our guiding principle.

Chevron transfers its time-series data to the cloud for advanced enterprise analytics

Chevron used Uptake Fusion when it needed to transfer its time-series data from the field to the cloud while exercising its data rights. Fusion securely extracted data from on-premise historians and assets for transfer to Chevron's data lake on the Microsoft Azure cloud platform. Once there, Uptake Fusion automatically organized the data for advanced analytics.

By minimizing security risk and transferring the data reliably to Chevron's Azure tenant, time-series data is made available enterprise-wide to Chevron users. Individuals of many expertise(s) within Chevron use data for their digital solutions. The solutions span the differing needs of Chevron. Examples of these needs include: digital twins, GIS visualization, connected worker, data science, analytics tools, and process control.

As part of Chevron's time-series plan, Chevron data moved to date includes 3.5 million tags, ten years of historical data, and 50,000 events per second. Chevron's time-series plan and reliance on Uptake Fusion continues to expand and grow.

Ellen Nielsen, Chevron's Chief Data Officer, explains the time-series program this way.

“”

> *By teaming with Uptake and Microsoft to connect and also automate our complex data, we're able to unlock the insights that help Chevron deliver on higher returns and lower carbon for our energy future.*

The Business Opportunity For Cloud-Based OT Data

Use cases have driven cloud adoption since 1999, when Salesforce used the Internet to deliver software programs to users. Nearly a quarter of a century later, OT use cases are in the spotlight-with a focus on industrial asset reliability and sustainability related to the environment.

Regardless of the OT use case, the requirement and the challenge is accessibility to quality data. Many companies have multiple processing sites, and therefore multiple on-premise sources. Each source has its own users. The users at a specific source will draw their conclusions from only the examination of their own data, losing the benefits of shared knowledge and insights from other individuals at other sites-who may be looking at a slightly better or clearer version of the not-quite-shared data. Traditionally it has been hard for a company to knit together dispersed knowledge-gathered at many on-premise sites-to develop a cohesive picture of process events and process trends. It's been harder still for a company to have the collaborative environment to develop insights about their processes and assets in a timely fashion, so oftentimes knowledge from one site isn't acted upon when there's the most value to gain.

The benefits to be realized by creating a system of unified data from previously separate pools of data, come with some heightened risks. One can create an environment of shared data and pooled insight, but this can create unintended consequences for the customer's networks. A company opening the access between sites and their specific users can also create cyber vulnerabilities.

A customer tries to improve his collaborative environment by creating multiple provisions for remote access to on-premise systems, and creates a network loading problem for himself. In addition, providing external access to on-premise systems can also be prohibitively expensive.

So a scalable computing environment can enable multiple users to have access to much larger amounts of multi-premise data. If that data can be accessed and transferred securely to an environment where advanced analytics tools can be applied to it, then there is much value that can be realized. However, access is not a guarantee of quality. Advanced analytics requires quality data. The challenge is getting quality on-premise data into the cloud without losing the data's granularity, and organizing the data for analytics and visualizations. Now consider that you're getting on-premise data from multiple sources, the scope of the challenge increases with each additional system you add.

In some ways, moving OT data to the cloud is like moving to a new home. All your household possessions arrive at the new place in boxes. Many of them are placed in the wrong room. Sometimes boxes seem to be in the right room, but upon opening you discover that the contents don't match the label. They weren't what you were looking for. Perhaps they were mis-labeled? And where are the contents that the label says should be there? Sometimes items are lost forever. In the same way, OT data transferred that lacks associated metadata will be misplaced. It may ultimately end up lost, with no data to aid in its identification and organization. So too, data often arrives in the cloud jumbled or missing, not unlike move-in day.

To ensure that the OT data that you transfer to the cloud can be used in the most effective ways, be certain that your data extractor also transfers the metadata associated with each OT data point. Many OT data measurements have location and equipment references built into their tag names and point definitions, so being able to interpret the 'data about the data' facilitates its use for interdependent users.

For example, OT data in the cloud is ideal for maintenance and reliability use cases. The reliability of an asset is enhanced or degraded by how well one maintains it, so making the data available to both organizations to analyze and understand makes it easier for them to collaborate and succeed together. Having asset data accessible anytime and anywhere increases coordination and collaboration across departments. Silos fade away with equal data access. Initiatives like predictive analytics involving data scientists, engineers, and maintenance supervisors enable plants to service equipment before failure, increasing uptime and meeting production goals.

A customer tries to improve his collaborative environment by creating multiple provisions for remote access to on-premise systems, and creates a network loading problem for himself. In addition, providing external access to on-premise systems can also be prohibitively expensive.

So a scalable computing environment can enable multiple users to have access to much larger amounts of multi-premise data. If that data can be accessed and transferred securely to an environment where advanced analytics tools can be applied to it, then there is much value that can be realized. However, access is not a guarantee of quality. Advanced analytics requires quality data. The challenge is getting quality on-premise data into the cloud without losing the data's granularity, and organizing the data for analytics and visualizations.

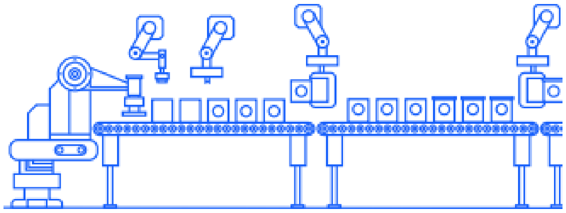
Now consider that you're getting on-premise data from multiple sources, the scope of the challenge increases with each additional system you add.

In some ways, moving OT data to the cloud is like moving to a new home. All your household possessions arrive at the new place in boxes. Many of them are placed in the wrong room. Sometimes boxes seem to be in the right room, but upon opening you discover that the contents don't match the label. They weren't what you were looking for. Perhaps they were mis-labeled? And where are the contents that the label says should be there? Sometimes items are lost forever. In the same way, OT data transferred that lacks associated metadata will be misplaced. It may ultimately end up lost, with no data to aid in its identification and organization. So too, data often arrives in the cloud jumbled or missing, not unlike move-in day.

To ensure that the OT data that you transfer to the cloud can be used in the most effective ways, be certain that your data extractor also transfers the metadata associated with each OT data point. Many OT data measurements have location and equipment references built into their tag names and point definitions, so being able to interpret the 'data about the data' facilitates its use for interdependent users.

For example, OT data in the cloud is ideal for maintenance and reliability use cases. The reliability of an asset is enhanced or degraded by how well one maintains it, so making the data available to both organizations to analyze and understand makes it easier for them to collaborate and succeed together. Having asset data accessible anytime and anywhere increases coordination and collaboration across departments. Silos fade away with equal data access. Initiatives like predictive analytics involving data scientists, engineers, and maintenance supervisors enable plants to service equipment before failure, increasing uptime and meeting production goals.

Data availability and data quality are the two greatest challenges facing a company's environmental and sustainability programs, according to a Deloitte study. OT data extracted correctly and transferred to an open major cloud environment addresses both availability and quality. With more high-quality information available, you can more easily monitor, track, and report metrics and KPIs on energy consumption, emissions, water use, and environmental impact.



OT data in the cloud opens the door to collaboration with third-party firms and applications like IBM Maximo. Third-party applications run most efficiently when they operate on curated data vs. non-curated data. Data curation ensures data is organized and ready for use. As business demands that your company move OT data to the cloud, keep data quality and accessibility top of mind. Having both will drive usage, acceptance, and results.

The Importance Of Cloud Data Security

When moving your company's industrial data to the cloud, the conversation invariably turns to security. "Is our data at risk in the cloud?" The short answer is yes. The longer answer, the one that helps you sleep better at night, requires more explanation.

First things first, your data on-premise is also vulnerable to hackers. It's why you have firewalls and an IT department that is vigilant and constantly performing security updates. That's why IT enforces onsite data and access security policies, multi-factor authentication, etc.

Your cloud provider helps with data security. For example, with the Azure platform, Microsoft is responsible for physical hosts, physical network, and physical data center. In addition, Microsoft has security covered for Azure tenant owners and stands ready to work with your IT department and OT engineers to ensure your data security. In other solutions, stack security is your responsibility, or belongs to a SaaS, PaaS, or IaaS provider.

Why is data security so important? A quote from Stephane Nappo, Global Head of Information Security for Societe Generale Group, clearly indicates security's importance.

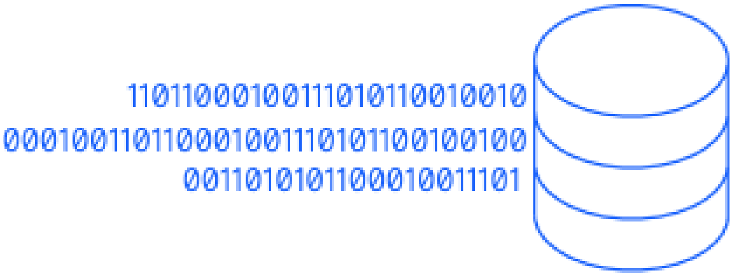
> ***"It takes 20 years to build a reputation and a few minutes for a cyber-incident to ruin it."***

Selecting a tenant for your industrial data isn't just about security; it's also about deciding between open and closed networks. Open networks like the Microsoft Azure platform and AWS give you autonomy and interoperability with your data, and provide access to exceptional data analysis capabilities. Closed networks like Apple's wall garden and OSIsoft's bolted-on cloud services for PI users work great as long as you stay within their network, and the analysis capabilities that you need are in their environment. However, if capabilities that you need are lacking, you'll have to accept limitations, or pay licensing fees for out-of-network activities.

Imagine a scenario where several departments use the same dataset from the cloud. So far, so good on a closed network. But what if your departments use an outside-the-network tool like IBM Maximo, or you need to involve another third party? On a closed network, you'll experience challenges and high costs with data sharing with outside parties. With a major open network like Azure, your data moves inside and outside the network freely and securely. Your tenant then becomes an extension of OT/IT operations.

The journey data takes from the on-premise world to the cloud also follows security protocols. Uptake Fusion utilizes private, secure endpoints, and provides an IEC 62443-secure environment and transport for your data. Part of that compliance is maintaining the security of your data in motion. To meet security requirements, Uptake Fusion encrypts the data it extracts and transfers to the cloud utilizing the latest transport layer security (TLS) protocol for privacy and data security.

Securing And Protecting OT Data In Industrial Environments



As a necessary part of any data or software threat modeling strategy, you need to ensure the security of both data in motion and data at rest. OT data extracted from historians and industrial assets, for bulk or real-time transfer to a cloud environment, should therefore be encrypted using the latest transport layer security (TLS) protocol as stated in Section 3. TLS covers the journey of OT data to the cloud. Once there, the platform provides data security.

That being said, OT data that resides on premise in industrial facilities with IT connections to the outside world is very much at risk from hackers, malware, and nefarious nation-states. It's imperative that industrial operations, especially in energy, shore up defenses. IT already has solid defense systems but is still subject to cyber attacks. Cyber risk to OT data is less known but an ever-present risk (see sidebar).

A good place for industrial organizations to start is by complying with regulations and standards like NIST, NERC CIP, and IEC 62443. The National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards is a respected security framework for IT and OT professionals. Moreover, the NERC CIP Standards map to the NIST Cybersecurity Framework, which many CISOs swear by and use as a benchmark for their own programs. IEC 62443 is another set of security standards for the secure development and deployment of Industrial Automation and Control Systems (IACS).

Third parties, the companies that industrial organizations often rely on, also present risk. From an IT perspective, third parties given access can create vulnerabilities. Imagine industrial companies with plants and warehouses running heating and cooling systems managed by outside parties.

Each plant or warehouse has hundreds of IoT devices connected to the Internet. Each one of those devices must be configured in a secure manner, or their vulnerabilities have reduced the security of the network. A network is only as secure as its weakest access point. It's a cyber risk that must be managed with steps like: threat modeling of your existing network infrastructure, regular assessments of the cyber vulnerabilities of your third parties, as well as internal reviews of your company policies and procedures.

Heavy industry does have an advantage that you should exploit. It's the company-wide focus on worker and operations safety, which fits well with security. Time has taught us that an exploited cyber security vulnerability could create a hazardous and unsafe situation for people, processes and equipment. With a safety/security management mindset, companies can build a cybersecurity infrastructure that is resilient to outside threats and vulnerable third parties. Building a cybersecurity infrastructure requires that they adopt standards and frameworks like NERC, NERC CIP, NIST Cybersecurity Framework,and IEC 62443. All are integral for achieving safe, secure, and cyber secure operations.

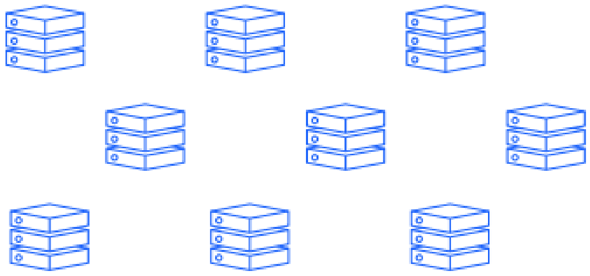
Risk can be greatly reduced, but it can never be totally eliminated. Any program should include an incident response process that encompasses a business continuity plan. For any industrial organization, a collaboration between IT and OT professionals makes the most sense. IT lives in a risk-filled world, and OT appreciates that it shares many of those risks.

US energy grid at risk of cyberattack

Cybersecurity for OT systems at energy facilities is woefully lacking compared to the established process for IT security.

Gartner predicts that by 2025 cyber attackers will be successful in weaponizing operational technology environments, resulting in human casualties. The energy grid is especially vulnerable. The Texas power grid and oil and gas transportation hubs are on high alert due to Russian hackers probing for weak points in the energy infrastructure.

Regulations follow incidents. Don't let an incident at your plant or facility lead to the company CEO testifying in front of a congressional subcommittee. Form a joint task force of IT and OT professionals tasked to deliver an action plan for protecting operational data.

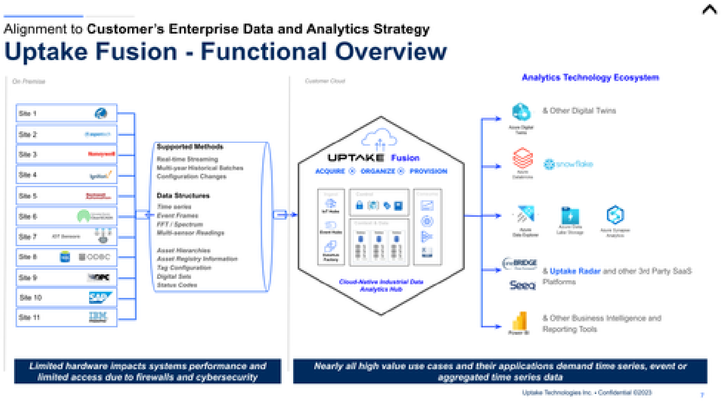


Final Thoughts

IT receives the fanfare and budget to protect a company's data, and rightfully so. Its cousin, OT, with data associated with heavy industry machines, offers enterprise benefits and increasingly comes with risk. We hope this paper has brought this promise and peril to your attention. IT and OT must come together to form a strategy and plan for protecting OT data.

Our final thought is, don't let a vendor request access to your data without questioning it.

When you work with Uptake, it's always your data, from its origin on premise through the journey to the cloud. We believe in your OT data rights, and we will protect them. Uptake's promise: it's always your data. Regardless of where the data resides, you still control it.



Alignment to Customer's Enterprise Data and Analytics Strategy

Uptake Fusion - Functional Overview

Supported Methods
Real-time Streaming
Multi-year Historical Batches
Configuration Changes

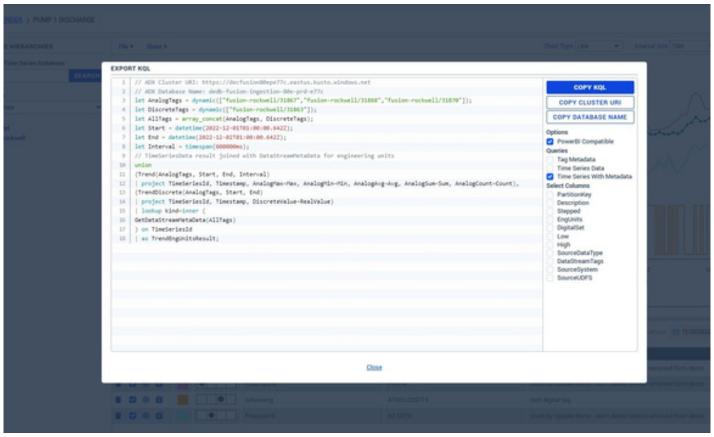
Data Structures
Time series
Event Frames
FFT / Spectrum
Multi-sensor Readings

Asset Hierarchies
Asset Registry Information
Tag Configuration
Digital Sets
Status Codes

Limited hardware impacts systems performance and limited access due to firewalls and cybersecurity

Nearly all high value use cases and their applications demand time series, event or aggregated time series data

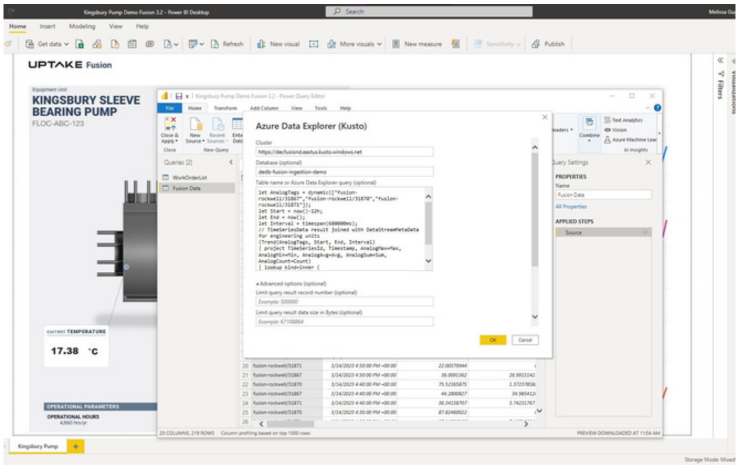
Uptake Technologies Inc. • Confidential ©2023



EXPORT KQL

```
// ADX Cluster URI: https://decfusion00epe77c.eastus.kusto.windows.net
// ADX Database Name: dedb-fusion-ingestion-00e-prd-e77c
let AnalogTags = dynamic(["fusion-rockwell/31867","fusion-rockwell/31868","fusion-rockwell/31870"]);
let DiscreteTags = dynamic(["fusion-rockwell/31863"]);
let AllTags = array_concat(AnalogTags, DiscreteTags);
let Start = datetime(2022-12-01T01:00:00.642Z);
let End = datetime(2022-12-02T01:00:00.642Z);
let Interval = timespan(600000ms);
// TimeSeriesData result joined with DataStreamMetaData for engineering units
union
(Trend(AnalogTags, Start, End, Interval)
| project TimeSeriesId, Timestamp, AnalogMax=Max, AnalogMin=Min, AnalogAvg=Avg, AnalogSum=Sum, AnalogCount=Count),
(TrendDiscrete(AnalogTags, Start, End)
| project TimeSeriesId, Timestamp, DiscreteValue=RealValue)
| lookup kind=inner (
GetDataStreamMetaData(AllTags)
) on TimeSeriesId
| as TrendEngUnitsResult;
```

Export a query from inside the Uptake Fusion Trender



Azure Data Explorer (Kusto)

Cluster: https://decfusiond.eastus.kusto.windows.net

Database (optional): dedb-fusion-ingestion-demo

Table name or Azure Data Explorer query (optional):

```
let AnalogTags = dynamic(["fusion-rockwell/31867","fusion-rockwell/31870","fusion-rockwell/31871"]);
let Start = now()-12h;
let End = now();
let Interval = timespan(600000ms);
// TimeSeriesData result joined with DataStreamMetaData for engineering units
(Trend(AnalogTags, Start, End, Interval)
| project TimeSeriesId, Timestamp, AnalogMax=Max, AnalogMin=Min, AnalogAvg=Avg, AnalogSum=Sum, AnalogCount=Count)
| lookup kind=inner (
```

Paste the query into any analysis tool such as Power BI

To learn more about Uptake Fusion
Vist our website: uptakefusion.com
Contact: fusion@uptake.com
Call: 780-862-9699