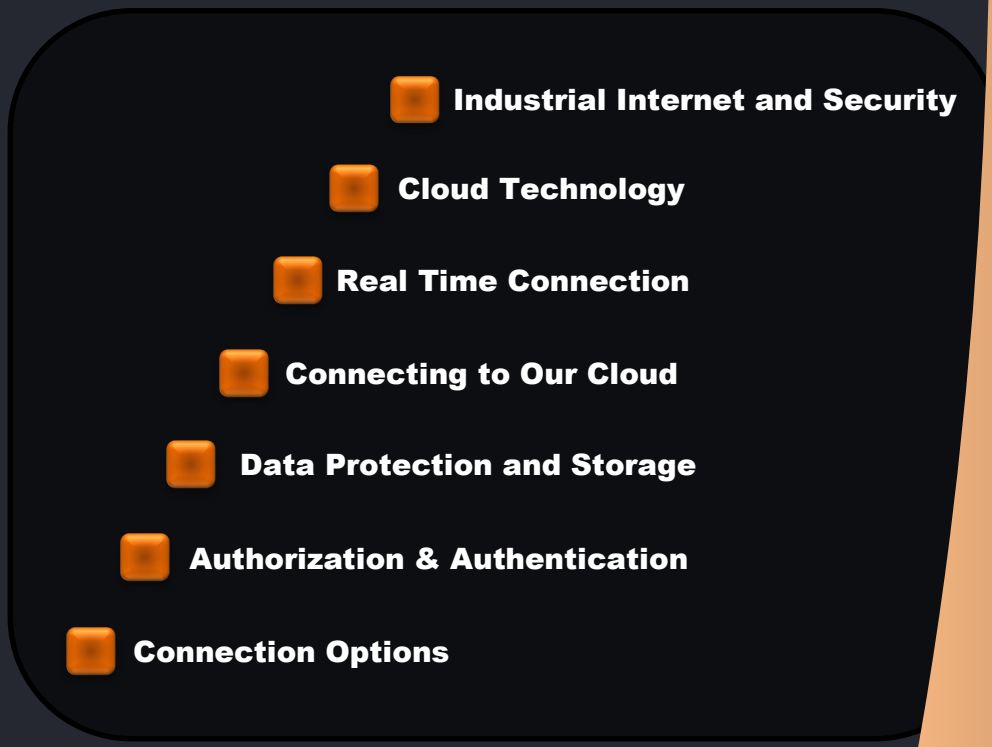
KAYE

Powered By FacilityConneX

Connection and Security

TECHNICAL WHITEPAPER



Document No. FCX-KAYE01-2020

INDUSTRIAL INTERNET AND CLOUD SECURITY

IoT and the Industrial Internet is here… but what is it?

The Industrial Internet, which represents the convergence of the global industrial systems with the power of advanced computing, analytics, low-cost sensing and new levels of connectivity, all permitted by the Internet. In short, it aims at transforming the way we connect and monitor critical machine data in order to make better business decisions. Typically, the industrial community has been burdened by fragmentation that creates islands of isolated data sources and individual applications that result in very high total costs of ownership (TCO). Now, by using a secure cloud-based solution, Operators and Managers can connect all that data into a "single source of knowledge" to drive transparency and full visibility into their operations at any time, and from anywhere!

So ask yourself …

- **What if you had complete operational visibility and control?**
- **What if you could utilize cloud applications more effectively to drive better operational insight?**
- **And what if you could get all this capability at the lowest total cost of ownership with no maintenance or upfront capital costs?**

That sounds great, but your first concern should be security!

In order to understand industrial cloud security, you must understand the Cloud Solution Provider's architecture and security practices. KAYE powered by FacilityConneX has been built "for" the cloud leveraging the most proven security technologies and practices to deliver a solution with security as the top priority.

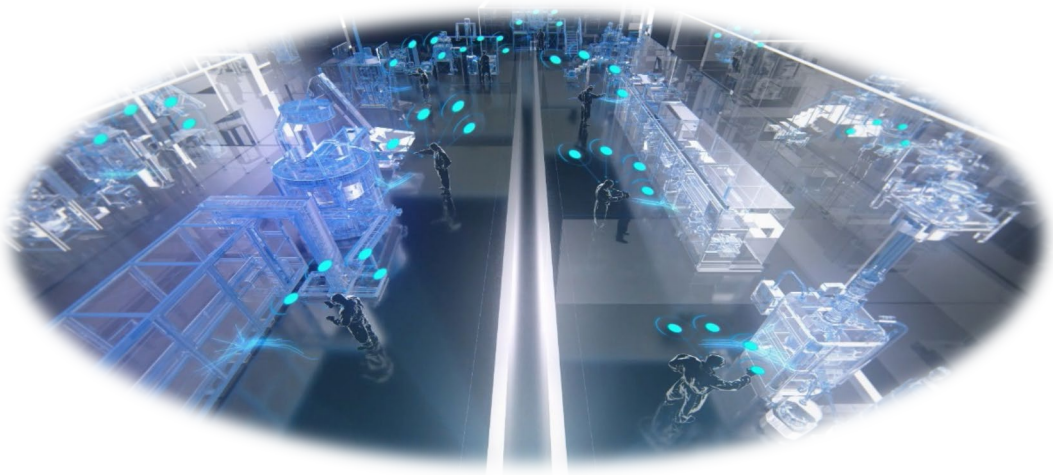
In this whitepaper, we will breakdown our cloud technology into the following sections:

- Cloud Core, Application, and GxP Technology
- Real Time Connection
- Drop and Go Method
- Data and Storage Protection
- Authorization & Authentication

CLOUD TECHNOLOGY

Technology defines your Protection.

Let us begin by defining a few basics and terminology that we will refer to: **Core Cloud Platform, Connectivity Solution, and the Visualization Application.**



The Core Cloud Platform forms the engines, databases, web services, and analytic services that provides knowledge through secure content delivery access. More importantly, the Core Cloud Platform is designed for security through a modular / micro-services architecture and application encoding schemes. The Core Cloud Platform is further broken into three secure layers that will be discussed in the next section.

Connectivity is the entry into your system - it must be secure. The Connectivity Solution has two sides - the server-side (cloud) and the edge-side (Customer machine) . Together they are designed to create a secure virtual private network tunnel in order to make the secure connection. Each session requires a digitally-signed certificate in both directions. In the upcoming section on connectivity, you will learn about this secure connection and how it uses trusted sessions, encryption, and encoding to secure your data into the cloud.

Access to your information is the reason why you buy our solution. Visualization comes with web browser clients and native mobile clients for tablets and smart phones. Each visualization solution is secure through multiple methods from encryption to encoding, making it more secure than your online banking connection. On top of the secure transfer methods, our solution is built with an intelligent authentication and authorization layer used not to only allow your access in but limits the information you see and have access to. The visualization section below will describe your access in detail.

LAYERING IS THE PROTECTION AND THE DIFFERENCE

Providing a Software-as-a-Service cloud solution puts the worry of security in our hands, **not yours**. Even in a cloud service like KAYE, the platform is secure through layering and protection. This solution is designed by security experts utilizing a secure modular architecture, with advanced firewall and protection services. Please note: For security reasons, not all layers and zones will be described here.

There are basically three layers making up the Core Platform.

The first secure layer is the **web services layer**. This internet facing layer is protected between two physical firewalls. Added protection on the secure point-to-point connection and authentication is built into the web service. This is described in the visualization section.

The second layer below the web service firewalls is a secure zone that incorporates the **intelligent engines and service applications**. These engines are modular by design, and are only accessible from the web service layer with unique encoding and port locations. The communication between these engines are proprietary encrypted and encoded.

The third layer is where **your data** is stored. This layer is protected behind another set of firewalls in a separate zone protected by another firewall. Here all storage is organized into multiple data stores and databases to assure security and data segregation.

Lastly, the Core Cloud Platform must be designed for Good Manufacturing Practices or what is typical referred to as the **“GxP Cloud”.** The Kaye Cloud is designed for GxP to ensure you meet your regulatory requirements.

Capabilities like complete audit trail at the system and application layers are available today. Core regulatory compliance capabilities such as Electronic Signature and Alert Acknowledgement Tracking are designed right into the platform. And with a complete reporting for verification, this cloud platform is designed for you. Now let’s talk about your connection…

CONNECTING INTO THE CLOUD

The Connection Solution is what connects your site, system, or equipment to ours. This Solution creates a virtual private tunnel with advanced encryption, encoding, and trusted certificates. So let's describe the life of a data packet that you entrust in our care:

THE LIFE OF YOUR DATA PACKET

- **A virtual private network tunnel originates from your local source ONLY, which is capable of connecting to our session control manager that is a digitally certified connection in both directions.**
- **A raw data packet is collected in a control server on your network.**
- **Then it is than converted into a 256-bit encrypted packet, and uniquely encoded ONLY to be deciphered on our cloud by our service applications.**
- **All of this is passed to the point-to-point VPN tunnel through an outbound only secure internet port and is encrypted before it leaves the source machine.**

When this data hits the cloud, it is protected by the first firewall zone - call it Zone A. This zone ensures only our certified tunnel sessions are connected. This session manager has the only connection to our second layered firewall called Zone B.

Your data is passed to our service application and engines before being stored away in **YOUR OWN** high performance proprietary and encrypted data stores. The data store technologies are used by tens of thousands of companies worldwide. The databases sit behind a third level protected firewall zone - called Zone C.

DATA PROTECTION AND STORAGE

YOUR DATA IS YOUR DATA!

As described in the previous section, your data is transported, encoded, and encrypted before it is stored. Once the data arrives, it is stored in a proprietary time-series database scheme designed for high performance and high security. This is your **own** data store.

Each data store is built and proven to hold millions and millions of tags over years of collection. This proprietary database is optimized for both insertion and retrieval by our applications. The data store can handle an insertion rate from thousands of controlled VPN sessions, and with the proprietary buffer technology, your data is protected from connection loss for several days.

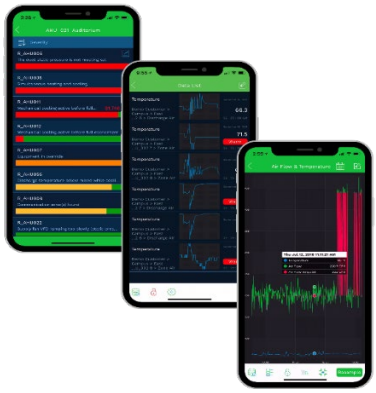
The data store is designed for high performance visual retrieval. This allows thousands of visualization clients to access this information for processing at micro-second rates. In addition to the insertion and retrieval performance, you can rest assured knowing your data is backed up from any potential failure or disaster. If it is ever required, our backup system is the leading technology in the market designed for no load backup and rapid restore.

Lastly, your data store has options. Our data store, by default, is an intelligent cache designed to only hold your data for processing and high performance visualization for a period of time. We then overwrite the data to process the next set of requests. Of course, our system is also designed to be a permanent store for your data for years of storage.

AUTHORIZATION & AUTHENTICATION

Anytime, Anywhere – Mobile and More!

Visualizing your information comes with the same rigor (with layers, trusted certificates, encryption, and authentication) as gathering your data. Your access is designed with one thing in mind - security. We will get to the layers and zones in a minute. Let us start with "who" you are.



Who you are matters...

KAYE/LabWatch IoT is a true role-based multi-tenant system. It is designed to authenticate you uniquely and based on **"WHO YOU ARE"**. You become authorized to access sets of information designed specifically for you - we call this the Customer Model - designed by you, for you. The model is secure by design. Every aspect of your model is authorized uniquely by you. Keep this in mind for later when we will talk about you sharing this model with others. For now, you have access to everything in your model. Once the model is defined for sites and equipment, we can describe the secure layers that protect access and information.

Your Authorization, Authentication, and Single Sign-on…

You may notice that your access requires you to login with your unique username and password, whether you are using your browser or smart device. The Authorization and Authentication service accommodates users to be defined directly in your user pool or you may choose to tie login credentials directly to your organizations single sign-on (SSO) provider via industry leading SAML 2.0 technology. Once authentication granted, rest assured each request to our server applications is verified with the Authorization service to assure that you have access to each feature and data request.

In addition to authorization assurance, all browser or mobile session data is secured and encrypted via our SSL certificate exchange featuring industry leading SHA-2 and 2048-bit encryption.

Now pause for moment and think about that, you have been through three layers of security already - a trusted connection complete with encryption, an authenticated login in, and authorization layer for access to your model. You have not even seen information yet - just a list from your model, your entry point into your data.

The Secure Request …

Our advanced, restful web services are designed to be connectionless and specifically looks for your signature and proprietary encoding on every request you make to the cloud. More importantly, in order for you to even hit our web service, you were first protected by physical and virtual firewalls in our cloud (remember Zone A). Once your request comes into the web service, it will pass the request through another firewall (Zone B) to highly scalable application engines for processing or data retrieval (across Zone C). By the time you see your data, you have been through several security layers, encrypted, encoded, and not to mention your authorized model!

KAYE cloud service uses authorized roles to extend security. As previously discussed, LabWatch IoT is built with your authorized customer model. But picture one thing first - each item in your model or application feature is uniquely authorized allowing you to extend your model to someone else without you losing any visibility. You can even extend your secure model to your customer. This means a piece of equipment can be visualized by people you distinctly allow to view and control.

Authorization is another key layer of security that is provided built in. It allows you full control over who sees your information – anytime, anywhere.

CONNECTION OPTIONS

Our Cloud Architecture is designed with security first, starting with the technology and with best in class practices of IT secure layering in mind. Our team of cloud experts monitors the security end to end, layer by layer, continuously. Hundreds of checks are made on the system continuously every week to ensure secure protocols and protections are tested and modified to keep the system secure at every layer. You can be confident in knowing that your data, access, and equipment is secure and powered by experts on Industrial Internet software and the Cloud Operations.

What are your secure connection options?

THE REAL-TIME CONNECTION

As described above. Our real time connection utilizes a continuous connection and highest level of encrypted technology. This real-time connection converts your data into an encrypted OPC outbound only into the Cloud. The advantages to this type of secure connection is no operator intervention, latest trending, instant alerts and notifications, and condition-based awareness

KAYE LabWatch IoT has multiple real-time connection options ranging from existing LabWatchPro systems to directing connecting to latest RF sensor technology. Please refer to the connection and IT architecture options on the website or talk with your KAYE account representative for details.

ABOUT KAYE

Powered by the Industrial Internet, KAYE is the first advanced operational intelligence-based system designed for continuous monitoring and detection of your Products. Using cloud-based technology, KAYE is an enterprise-level system designed to provide smart asset monitoring, alerts and notification, advanced predictive intelligence, continuous management. Ask your sales representative for details.

FOR MORE INFORMATION VISIT:

www.kayeinstruments.com

CONTACT US DIRECTLY AT:

https://www.kayeinstruments.com/en/contact