SafeLINC Cloud Service

Validating security controls when deploying Connected Services Gateway

Solution overview

SafeLINC Cloud Services is a service facilitated by the Connected Services Gateway (CSG) that brings the connectivity you expect in everyday life to fire alarm management, reducing labor over the life of the system. Real-time and historical fire alarm control unit data can be accessed from anywhere through a secure cloud platform.

Remote features monitoring can help identify and resolve issues faster. End users benefit from more proactive maintenance and gain peace of mind, knowing their systems are in compliance and ready to protect building occupants.

- Manage multiple locations
- Data enrichment
- Device management
- Prioritization and enhanced safety

General cybersecurity features

Security is designed into all Johnson Control products – hardware, software and hosted services.

- **End-to-end encryption:** Data in transit is encrypted at your local building and only decrypted once it reaches the Johnson Controls-managed cloud
- **Secure storage:** SafeLINC Cloud data is securely stored at rest using AES-256 encryption
- **Secure authentication:** Multi-factor authentication ensures that only authorized personnel can access the cloud application
- **Role-based access control:** User roles in SafeLINC Cloud can be customized granularly to fit the exact needs of the solution, to make sure that only users with proper authorizations are able to access specific features
- **Firmware updates:** Firmware updates can be pushed from the SafeLINC Cloud to the Connected Services Gateway, ensuring that your gateways always have the latest security patches and features
- **Secure protocols:** All data moving from site-to-cloud is carried via the AMQPS protocol which is the AES-256 encrypted (TLS/SSL) version of AMQP. All traffic is outbound-initiated on port 5671
- **Regular vulnerability assessments:** SafeLINC Cloud and gateway software is continuously reviewed for vulnerabilities as part of Johnson Controls Software Design Lifecycle (SDLC), as well as a robust cloud monitoring toolset designed to highlight any security issues or network anomalies

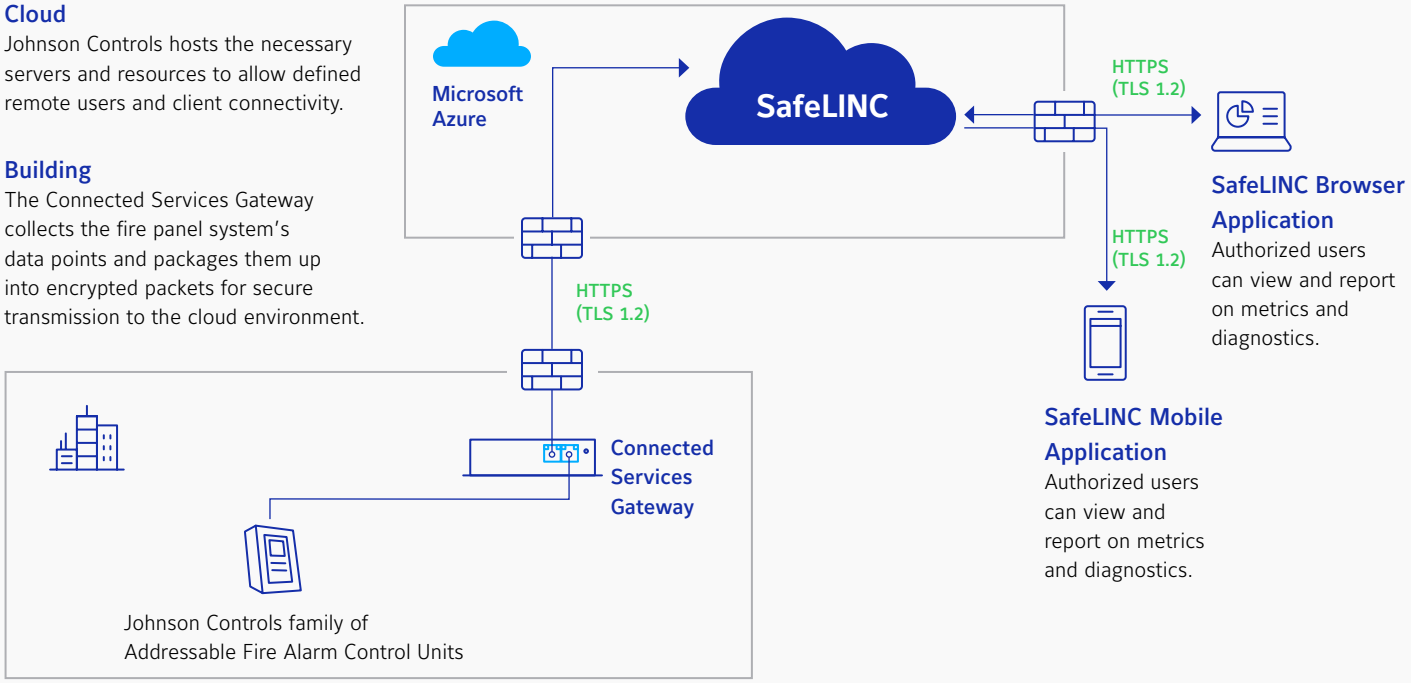
Architecture and data flow

Data flow specifics will depend on the components chosen by our customer and how we implement our solution in their facility.

Cybersecurity sales sheet diagram template – SafeLINC Cloud

Cloud
Johnson Controls hosts the necessary servers and resources to allow defined remote users and client connectivity.

Building
The Connected Services Gateway collects the fire panel system's data points and packages them up into encrypted packets for secure transmission to the cloud environment.



ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

All Johnson Controls global development locations complied with this security lifecycle development certification conforming with ISA/IEC 62443-4-1 and encompassing all associated brands. This certification reinforces our customer commitment to provide cyber-resilient solutions that follow best-in-class industry practices.

Visit our data privacy sheet for inquiries regarding SafeLINC Cloud

Visit **johnsoncontrols.com** or follow us **@johnsoncontrols**