CYBERSECURITY AND DATA PRIVACY SHEET

SafeLINC Cloud Services

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 monitoring features 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 Controls 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 cloud managed by Johnson Controls
- 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: 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

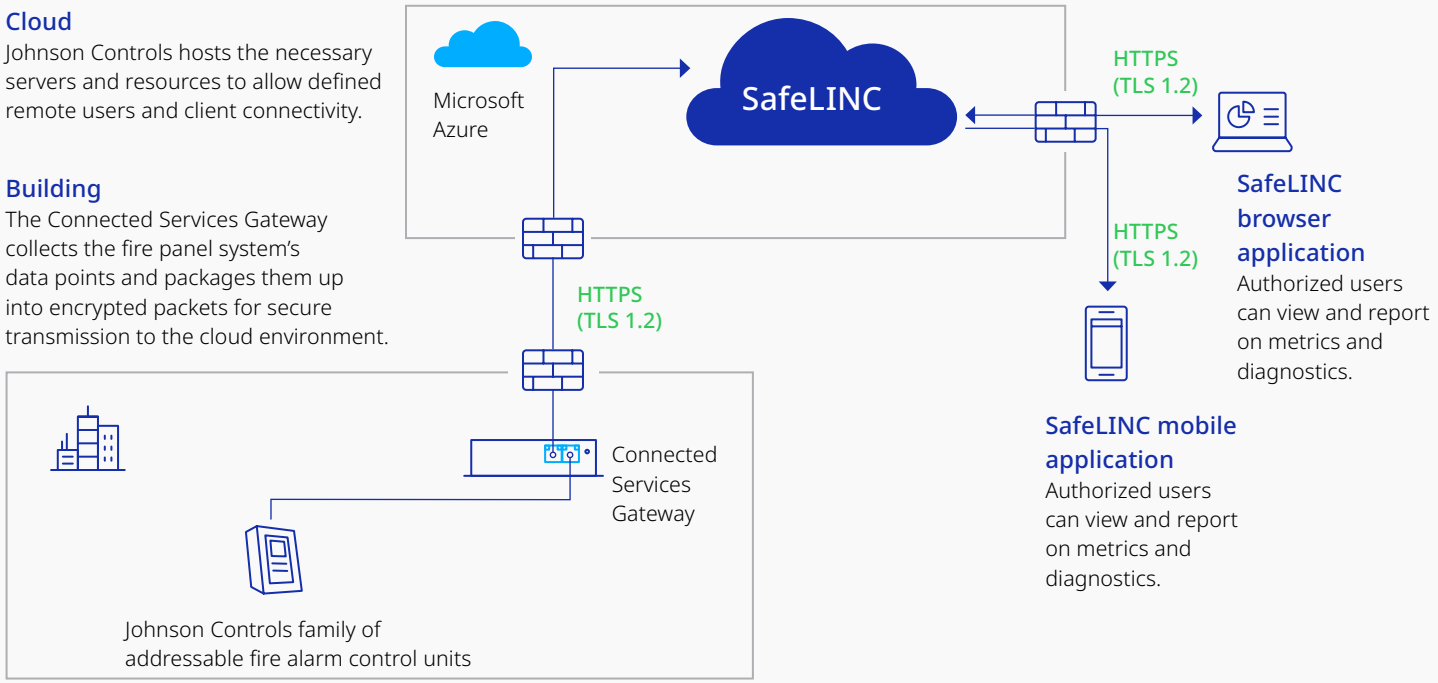
Architecture and data flow

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.



SafeLINC browser application
Authorized users can view and report on metrics and diagnostics.

SafeLINC mobile application
Authorized users can view and report on metrics and diagnostics.

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.

Data privacy

Johnson Controls has a Global Privacy Office and a Global Privacy Program, involved at the beginning and throughout the design and development of our processes, activities, products, services and solutions, in accordance with internationally accepted principles of Privacy by Design. The Johnson Controls Privacy Program is led by our privacy experts and designed with the most stringent global privacy and data protection laws. In addition to product-related information provided in this section please visit www.johnsoncontrols.com/privacy-center for more details on our Global Privacy Program.

a. Personal data processing details of SafeLINC Cloud Services

See below details on each category of personal data processed by SafeLINC Cloud Services, types of personal data within each category and the purpose of processing each type:

Personal data category	Type of personal data	Purpose of processing
Work-related identification details	User email address Preferred language	Account management

b. Data retention and deletion

Johnson Controls has a Global Records Management Program, which includes a Global Records Retention Policy and Procedures. The purpose of our Global Records Management Program is to detail the responsibilities and working instructions necessary for the use, maintenance, retention or deletion of data Johnson Controls is processing. The Global Records Management Program applies to all worldwide locations and legal entities controlled by Johnson Controls.
When Johnson Controls processes personal data on behalf of a customer, or when products are operating on a customer site, to the extent provided by a product's functionalities and upon a system's configuration, customers may access such data and delete it at any time on their own. The default retention periods as predefined by Johnson Controls apply. See the below table for the default retention periods applied to SafeLINC Cloud Services. If, during the 90 days following the end of a subscription, Johnson Controls received from a customer a request to export their personal data, Johnson Controls will provide a customer with an export of their personal data in a structured commonly used machine-readable format, as reasonably determined by Johnson Controls. Such request must be made to the JCI Digital Customer Support email currently at **CSGcloudsupport@jci.com**.
If not already deleted by the customer using available internal product deletion features, the customer's personal data will be deleted after such 90-day period or as otherwise agreed. During any retention period, the provisions of the underlying agreement that are applicable to the retention and product of a customer's personal data continue to apply.

Default retention periods for customer personal data are as set forth in the table below:

Data category	Retention period	Reason for retention
Work-related identification details	For the period of an active subscription + 90 days	Required to run an active subscription

c. Sub-processors for SafeLINC Cloud Services

Please see below the list of current sub-processors utilitized for SafeLINC Cloud Services:

Sub-processor	Service type	Location of data centers
Microsoft Azure Cloud	Third-party cloud hosting	United States or European Union (depending on customer's location)

d. Cross-border data transfers

Many countries and jurisdictions have laws governing the transfer of personal data. As a multinational organization, Johnson Controls has substantial experience in dealing with cross-border transfer issues and restrictions. When Johnson Controls processes personal data for our own purposes or on behalf of a customer, we utilize the following transfer mechanisms that can assist our customers:

Binding Corporate Rules (BCRs)	The Johnson Controls BCRs are designed to ensure an adequate level of protection of personal data no matter where in the world it is processed by Johnson Controls. With respect to the European Union (EU), the Johnson Controls BCRs have been specifically approved by the EU and Data Protection Authorities (DPAs) for transfer of EU personal data globally within Johnson Controls.
Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR)	The CBPR is a government-backed privacy certification which demonstrates that Johnson Controls complies with internationally recognized data privacy protections and is the framework approved for the transfer of personal data by Johnson Controls between participating APEC member economies: the United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines.
Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP)	The PRP is a government-backed privacy certification that enables Johnson Controls to demonstrate to customers our accredited enterprise-wide Privacy Program, and to transfer data processed on behalf of customers (including our cloud solutions) between the United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines. Please see the PRP Directory and the Johnson Controls TRUSTe validation page for more information.
EU Standard Contractual Clauses (SCCs)	Johnson Controls incorporates the EU's approved standard contractual clauses, also referred to as the "Model Contract," into the Johnson Controls Data Protection Agreement located at www.johnsoncontrols.com/dpa to afford the contractual protection under the SCCs to our customers.
US Data Privacy Framework	Johnson Controls is certified under the US Data Privacy Framework for transfers of personal data from the European Union (EU), United Kingdom (UK) and Switzerland.

We combine our critical focus on cybersecurity and privacy with digital innovation and building expertise to deliver smart building solutions.

To learn more, please visit our website at www.johnsoncontrols.com/trust-center or contact us at TrustCenter@jci.com.

Visit johnsoncontrols.com or follow us @johnsoncontrols