

OpenBlue Bridge

Cybersecurity Sheet

Achieving next-generation performance
through innovative sub-system management



Solution overview

OpenBlue Bridge is an Internet of Things (IoT) connectivity platform designed to connect Operational Technology (OT) and Informational Technology (IT) systems into the OpenBlue Cloud, while managing those connections throughout the device lifecycle.

At Johnson Controls, we harness innovation to create connected solutions that maintain the health of critical equipment such as intelligent edge services, ensuring they last longer and perform better with our best-practice organization-wide strategies.



**Analytics
at the edge**



**Data
enrichment**



**Device
management**



**Enables command
and control**

General cybersecurity features

Security is designed into all Johnson Control products – hardware, software and hosted services. We work with expert partners in government and industry to maintain our customers' regulatory compliance.

- **Encrypted communications:** Building data is sent from site to cloud, encapsulated within a Zero-trust Host Identity Protocol (HIP) encrypted tunnel. A second layer of encryption is added by using Transport Layer Security (TLS), which provides additional protection
- **Site-to-cloud communications:** Only one outbound port is required to initiate site-to-cloud data exchange
- **Zero-trust policy-managed authorizations:** Only defined paths are permitted between OpenBlue Bridge and remote services
- **Forced password change:** Default user account passwords must be changed when commissioning OpenBlue Bridge
- **Remote updates:** When a new version of software is available, the OpenBlue Bridge gateway device periodically reviews and recommends security updates through the embedded secure connection
- **Secure remote management:** Technicians access to protected resources can be scheduled for specific dates and times based on explicit authorization in the network control plane
- **Custom-built Operating System:** The OpenBlue Bridge runs on a custom, minimal base image Linux operating system, enhanced with features such as secure boot, AES-256 partition encryption, and a Trusted Execution Environment

The power behind **your mission**

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.

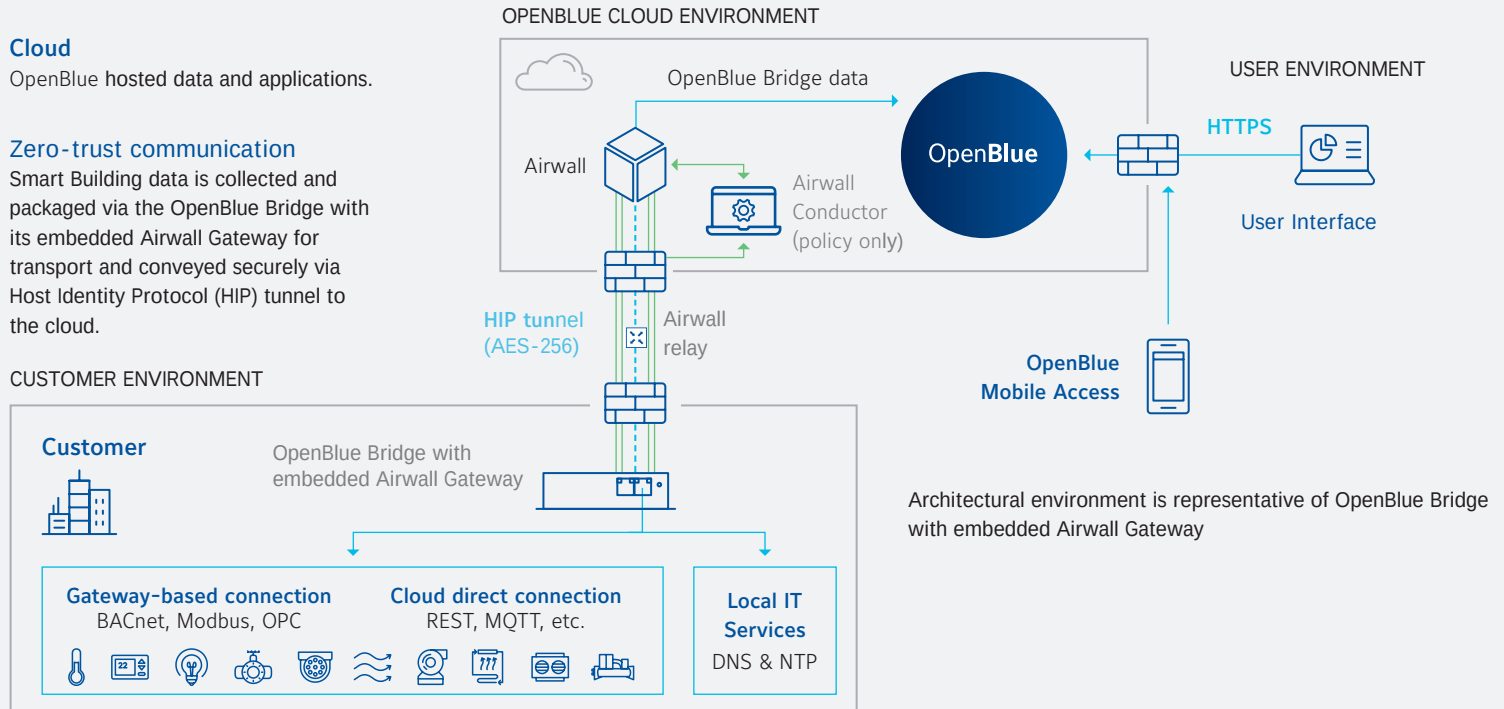
Cloud

OpenBlue hosted data and applications.

Zero-trust communication

Smart Building data is collected and packaged via the OpenBlue Bridge with its embedded Airwall Gateway for transport and conveyed securely via Host Identity Protocol (HIP) tunnel to the cloud.

CUSTOMER ENVIRONMENT



ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

All Johnson Controls global development locations were found to be in compliance 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.



SOC 2 Type 2 report

As part of the Johnson Controls journey to implement best-in-class cybersecurity controls, the first group of OpenBlue products, including OpenBlue Enterprise Manager, OpenBlue Companion, OpenBlue Cloud and OpenBlue Bridge, now have a SOC 2 **Type 2** report. This report provides assurance that Johnson Controls meets the standards for securing customer information and transparency in our practices for securely developing and supporting products across their lifecycle.*

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.

Cybersecurity and data privacy sheet

a. Personal data processing details of Connected Equipment Portal

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

Personal Data Category	Types of Personal Data	Purpose of Processing
User and account information	<ul style="list-style-type: none">• User ID• Password (static and defined by each user)	The information is used for authentication purposes only

b. Data retention and deletion

Johnson Controls has a Global Records Management Program, which includes a Global Records Retention 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 destruction of data, and to assign appropriate responsibilities to the right individuals.

When Johnson Controls processes personal data for our own purposes, the Johnson Controls Global Records Management Program applies to all records, on all media, and must be maintained in accordance with Johnson Controls Records Retention Policy and Records Retention Schedule for the specific country and business in which the record has been stored. The Records Management Program applies to all worldwide locations and legal entities controlled by Johnson Controls.

Similarly, when Johnson Controls processes personal data on behalf of a customer, or when our products are operating on customer site, those offerings can be configured to meet customer data retention periods.

See below the default retention periods applied to CEP:

Data Category	Retention Period	Reason for Retention
User and account information <ul style="list-style-type: none">• User login ID	n/a	The information is used for authentication purpose only. No data is retained.

c. 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 which can assist our customers:

Cybersecurity and data privacy sheet

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, 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 Cross-Border Privacy Rules (APEC CBRP)	The CBRP 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: United States of America, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines.
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 (DPF)	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.

Integrate the next-generation smart building with OpenBlue Bridge and discover technology that offers bidirectional edge-to-cloud and cloud-to-edge data communication. Visit www.johnsoncontrols.com/openblue today for more information.

*This excludes OpenBlue Services for BAS Optimization applications of OpenBlue Bridge.
Please note that this document is for customer guidance purposes only and is not legal advice. Johnson Controls is not a law firm and does not provide legal advice. While Johnson Controls products and solutions are designed for use in compliance with applicable law, implementation and deployment of Johnson Controls products and solutions should be reviewed by appropriate customer advisors and stakeholders for such compliance.

About OpenBlue

OpenBlue is a complete suite of connected solutions that serves industries from workplaces to schools, hospitals to campuses, and beyond. This platform includes tailored, AI-infused service solutions such as remote diagnostics, predictive maintenance, compliance monitoring, advanced risk assessments, and more. A dynamic new space from Johnson Controls, OpenBlue is how buildings come alive.



DS2306004