

Enerbrain Cybersecurity Whitepaper

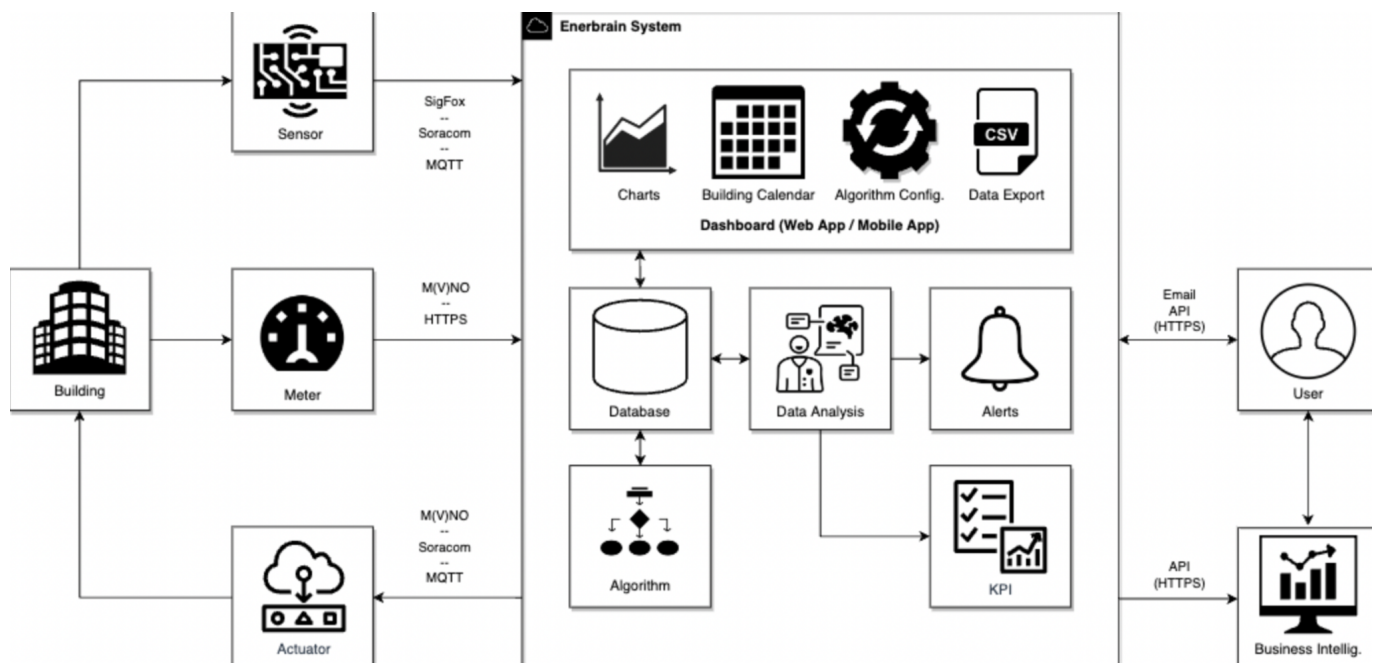
Introduction

Enerbrain, established in 2015 in Turin, Italy, was founded to make buildings in which we live high-performing and sustainable through an innovative hardware and software solution capable of automated and intelligent management of air conditioning and ventilation systems in buildings.

Via IoT devices we monitor environmental conditions and energy consumption by sending and collecting them in the cloud. There they are analyzed and used by our Enerbrain Algorithm to send inputs to controllers in the field to improve plant regulation, enabling:

- A 30% reduction (on average) in energy consumption;
- Decreased CO₂ emissions;
- Improved indoor comfort conditions;
- In-depth knowledge about the most energy-intensive processes or machinery;
- Decision-making from real data collected;
- Remote management of the entire building stock through a single Enerbrain Web App;

Below is the high-level diagram of our Enerbrain System:



The main components are:

- Energy and environmental monitoring devices that can collect comfort and energy consumption data and send it to the Cloud;
- Controllers for adjusting control systems in the field;
- Enerbrain architecture in the Cloud to interconnect devices, collect real-time data and, thanks to the Enerbrain Algorithm, send commands to controllers in the field;
- Web App, exposed on the Internet with verified access via Amazon Cognito, for visualization, downloading of plant monitoring and operation data;
- Back end and Database: storage and processing of data from the field.

Cybersecurity at Enerbrain

Enerbrain offers a number of standard products and services residing in the cloud and sold via license to the end customer. The main provider of cloud services and hosting is Amazon Web Services. The main cybersecurity operation and monitoring services are provided by them.

The instance is hosted at Irish datacenters, in compliance with GDPR regulations. The application is multitenant: a single instance and logical structure which accommodates via logon users from different clients.

Roles and guarantees for cybersecurity

Data confidentiality and security of the Enerbrain Web App are ensured by assigning user/building roles when they are created. Roles allow you to configure the ability to view or edit information for each building and client.

Our support performs a periodic check against user configuration. The ability to make interventions to the database is restricted to a limited number of internal Enerbrain employees for maintenance purposes only.

Several security adjustments have been made over the past year to raise the standards of our platform:

- Implemented a WAF for monitoring Internet traffic to the Enerbrain Web App;
- Implemented encryption of collected personal customer data (first name, last name, work email, work phone contact if provided). Based on a risk assessment done internally, we decided to safeguard data subject to legal requirements;
- Operational data, which are not subject to special regulations at this time, are instead in plain text also for performance reasons and guarantee of adequate service levels towards the end customer;
- Improvements to our password management policy to align it with corporate standards;
- Our technician and support accounts are authenticated with MFA;

VAPTs are performed annually to identify and correct possible threats.

A backup service is in place to restore any lost or altered data.

All Enerbrain personnel and any third parties are subject to assessment and profiling against the major systems through which we deliver our services and/or manage our business.

Enerbrain System Password Policy

We changed our user identification provider by adopting Auth0. A new password policy had been implemented:

- Last 4 passwords can't be used.
- Password complexity: uppercase, lowercase, numbers or special characters.
- Minimum length: 12 characters.
- Application administrator password length: 15 characters.
- Password expiration: unlimited according to last NIST guidelines.

Support

Also included in the Enerbrain Recurring Services, sold together with the Enerbrain System, is in-house support via a ticketing platform. Customer support is assisted by a team of developers and R&D, who step in for emergency fixes.

Monitoring

Mass access to data for easier consultation and/or report production is provided by access to a Tableau Enerbrain instance. Dedicated dashboards can be created according to customer requirements.

The Enerbrain Web App provides a number of APIs.

Authentication is done via API Key. The data stream is transmitted according to HTTPS protocol.

They are subject to a rate limiter to safeguard other customers and the performance of our product from misuse.

However, the use of these APIs is granted by us only for really specific cases and after evaluation of technical feasibility, where the Tableau solution cannot cover the standard needs of a customer.

Continuous improvement

Enerbrain also follows a philosophy of continuous improvement in terms of security, reliability and end-customer services.

To match the highest industry standards and react to the cybersecurity challenges posed by the current international environment, we have embarked on a path in order to comply with the ISO27001 standard.

Our goal is to achieve official certification during 2023.