Security in Zaphire

Zaphire makes cloud-based building automation secure by building the platform on Zero Trust, where all access is verified, encrypted, and limited to what is strictly necessary. With end-to-end encrypted communication, no flat VPN access and continuous security updates, you get a building management system that combines high availability with modern cybersecurity.

zaphire

Say hello to your secure, all-in-one top system for building automation

Zaphire is built as a modern cloud platform based on microservices in an Azure Kubernetes environment, and can run in the cloud, locally or as a hybrid solution. This architecture provides high scalability, flexibility and the ability to isolate functions, so that a problem in one module does not spread to the entire system. The system has documented uptime of over 99.99%, and redundancy at several levels to ensure availability also during failures or maintenance.

Zaphire is built on the philosophy of "Zero Trust principles", where the starting point is that no devices or users are automatically trusted, even if they are located "on the inside".

In practice this means among other things: no flat VPN access, segmented installations, strict access control, encrypted communication throughout, and a system design that is not dependent on a single "outer wall" such as a firewall. In this way the consequence is reduced if a single user device, account or local component becomes compromised.

Zaphire places great emphasis on combining IT security and operational reliability in one holistic solution, so that the building owner and consultants do not have to choose between "secure" and "practical in operation".

Who is Zaphire?

Zaphire is a Norwegian company. Since 2018, we have developed modern systems for building automation and energy monitoring, with a focus on usability, security and reliability.

Zaphire is driven by the desire to create a top system built on modern IT principles and open standards. Before we started developing Zaphire, we saw that the processes in traditional building and energy management systems were inefficient and complex. The existing solutions appeared outdated, difficult to use and lacked the efficiency required to meet modern needs. In 2018 we decided to solve these challenges and started the work of developing a system for automation of buildings and energy. The result was Zaphire.

Today, Zaphire is an established player in the market, with solutions used by both municipalities and larger property managers. With Zaphire you get a complete solution for control, monitoring and energy follow-up of buildings, with high operational reliability, full mobile access and lower lifecycle costs than traditional systems.

Architecture & security principles

Zaphire is developed as a flexible platform that can run in the cloud, locally or as a hybrid solution. The architecture is based on container technology and microservices, which ensures both scalability and reuse of services across system levels. To achieve stable operation, the solution is constructed with mechanisms for high availability (High Availability), where redundancy and automated failover ensure that potential errors do not affect the user experience.

All communication between the system's components is encrypted with HTTPS and modern security standards (TLS 1.2 or higher, always with Forward Secrecy). This enables secure data exchange without the need for VPN solutions, which often add complexity and increase risk in more traditional systems.

The network architecture is based on the principles of segmentation and isolation. Dedicated VLANs for technical systems combined with strict firewall protection prevent incoming traffic and shield installations from unauthorized access. In addition, advanced traffic filtering is used to protect both Zaphire and customers from distributed attacks (DDoS), so that operations remain stable even under high load.

Zaphire is developed as "managed code" and is continuously updated. Known vulnerabilities are therefore closed quickly and automatically, without the need for manual intervention from operating personnel. The result is a platform that combines modern IT security with practical operational reliability, and which gives consultants a robust foundation for planning and specification in their projects.

Network security and VPNs

Traditionally, remote access to building management systems has often taken place via VPN, which in practice provides broad network access once a user is logged in. This increases the risk if a PC or account becomes compromised, because the attacker can move laterally further within the network. Zaphire has therefore deliberately chosen an architecture without traditional VPN access for suppliers and users.

Instead, all communication takes place through the application layer and secure APIs, so that users never get direct network-level access to the buildings' technical networks. Access is limited to one specific session and one defined endpoint, and it is not possible to jump between installations or systems through the portal.

This follows the principles of segmentation and "least privilege", where the user only receives the minimum level of access required to perform a task, and the attack surface at the network level is kept very small.

Encrypted communication

All information exchanged between users, installations and cloud services in Zaphire is encrypted over HTTPS with TLS 1.2 and 1.3. This applies both to external communication with the portal and API, and internal traffic between microservices in the cloud solution, so that a potential compromise in one part does not provide free access further.

Zaphire follows the principle of "closed by default", APIs and functions must be explicitly opened through access control before they can be used. This reduces the risk of misconfiguration and makes it easier to maintain control over who can do what, especially in environments with many users, integrations and buildings. In addition, the system does not open ports directly to the internet from installations; communication goes through controlled and secure endpoints in the platform.

DDoS protection

At the network level, Zaphire is built on principles of segmentation and isolation. Technical systems are placed on their own VLANs, and incoming traffic to installation networks is heavily restricted with firewall rules, so that unauthorized traffic is stopped early.

The platform is also protected against volume attacks through advanced traffic filtering and DDoS protection in the underlying infrastructure, so that the service remains available even under high load. This contributes to the building management system being experienced as stable, even when there is increased risk or ongoing attacks against internet-exposed services in general.

Implementation model and scalability

Traditional building management projects often have long rollout phases, complex integrations and time-consuming commissioning. Zaphire does it differently. The solution is built to be fast, secure and easy to take into use, without having to make major changes to existing infrastructure.

Thanks to our modular architecture and open protocols, Zaphire's solution can actually be connected to an existing building management system in under 20 minutes. All that is required is that an electrician establishes a physical connection to the building's system (for example via BACnet/IP, Modbus or MQTT).

The electrician is responsible for the physical connection and signal access, while Zaphire takes responsibility for data collection, security, analysis and visualization. When the signals are available, Zaphire's cloud platform automatically connects and data collection starts immediately. This means there is no need for VPN, heavy IT configurations or complex integration projects.

Scalability

Once one building is connected, the solution can easily be scaled to additional locations. Zaphire uses the same secure connection method, so that new buildings can be activated with minimal footprint and without the need for new installations.

This makes the system ideal for portfolios that want rapid rollout, standardized data access and consistent reporting.

zaphire

Interested in learning more?
Contact us today!

info@zaphire.no
+47 40 00 88 00