# Säkerhet i Zaphire

Zaphire gör molnbaserad byggautomation säker genom att bygga plattformen på Zero Trust, där all åtkomst verifieras, krypteras och begränsas till det som är strikt nödvändigt. Med end-to-end-krypterad kommunikation, inga öppna VPN-åtkomster och kontinuerliga säkerhetsuppdateringar får du ett system som kombinerar hög tillgänglighet med modern cybersäkerhet.

zaphire


## Säg hej till ditt säkra, allt-i-ett toppsystem för byggautomation

Zaphire är byggt som en modern molnplattform baserad på mikrotjänster i en Azure Kubernetes-miljö, och kan köras i molnet, lokalt eller som en hybridlösning. Denna arkitektur ger hög skalbarhet, flexibilitet och möjlighet att isolera funktioner, så att problem i en modul inte påverkar hela systemet. Systemet har dokumenterad upptid på över 99,99 % och redundans i flera led för att säkerställa tillgänglighet även vid fel eller underhåll. Zaphire bygger på principen ”Zero Trust”, där utgångspunkten är att inga enheter eller användare automatiskt är betrodda – även om de befinner sig “på insidan”.

I praktiken innebär detta bland annat: inga öppna VPN-åtkomster, segmenterade anläggningar, strikt åtkomstkontroll, krypterad kommunikation hela vägen och ett system som inte är beroende av en enskild “yttervägg” som brandvägg.

Detta minskar konsekvenserna om en användare, enhet eller komponent skulle kompromitteras. Zaphire lägger stor vikt vid att kombinera IT-säkerhet och driftsäkerhet i en helhetslösning, så att man slipper välja mellan “säkert” och “praktiskt i drift”.

## Vem är Zaphire?

Zaphire är ett norskt företag med bas i Drammen. Sedan 2018 har vi utvecklat moderna system för byggautomation och energiuppföljning, med fokus på användarvänlighet, säkerhet och tillförlitlighet.

Zaphire drivs av ambitionen att skapa ett toppsystem byggt på moderna IT-principer och öppna standarder. Innan vi började utveckla Zaphire såg vi att traditionella system för bygg- och energistyrning var ineffektiva och komplexa. De befintliga lösningarna upplevdes som föråldrade, svåra att använda och saknade den effektivitet som krävs för att möta dagens behov. År 2018 bestämde vi oss för att lösa dessa utmaningar och startade utvecklingen av ett system för automatisering av bygg och energi – resultatet blev Zaphire.

Idag är Zaphire en etablerad aktör på marknaden, med lösningar som används av både kommuner och större fastighetsförvaltare. Med Zaphire får du en komplett lösning för styrning, övervakning och energiuppföljning av bygg, med hög driftsäkerhet, full mobil åtkomst och lägre livscykelkostnader än traditionella system.


# Arkitektur & säkerhetsprinciper

Zaphire är utvecklat som en flexibel plattform som kan köras i molnet, lokalt eller som en hybridlösning. Arkitekturen bygger på containerteknologi och mikrotjänster, vilket säkerställer både skalbarhet och återanvändning av tjänster på tvärs av systemnivåer. För att uppnå stabil drift är lösningen konstruerad med mekanismer för hög tillgänglighet (High Availability), där redundans och automatiserad failover säkerställer att eventuella fel inte påverkar användarupplevelsen.

All kommunikation mellan systemets komponenter är krypterad med HTTPS och moderna säkerhetsstandarder (TLS 1.2 eller högre, alltid med Forward Secrecy). Detta möjliggör säker datautväxling utan behov av VPN-lösningar – som ofta tillför komplexitet och ökar risken i mer traditionella system.

Nätverksarkitekturen bygger på principerna om segmentering och isolering. Dedikerade VLAN för tekniska system i kombination med strikt brandväggsskydd hindrar inkommande trafik och skyddar anläggningarna mot obehörig åtkomst. Dessutom används avancerad trafikfiltrering för att skydda både Zaphire och kunderna mot distribuerade attacker (DDoS), så att driften förblir stabil även under hög belastning.

Zaphire är utvecklat som ”managed code” och uppdateras kontinuerligt. Kända sårbarheter åtgärdas därmed snabbt och automatiskt, utan behov av manuell inblandning från driftspersonal. Resultatet är en plattform som kombinerar modern IT-säkerhet med praktisk driftsäkerhet – och som ger rådgivare en robust grund för planering och specifikation i sina projekt.

# Nätverkssäkerhet och VPN

Traditionellt har fjärråtkomst till SD-anläggningar ofta skett via VPN, vilket i praktiken ger bred nätverksåtkomst när en användare väl är inloggad. Detta ökar risken om en dator eller ett konto komprometteras, eftersom en angripare då kan röra sig vidare i nätverket.

Zaphire har därför medvetet valt en arkitektur utan traditionell VPN-åtkomst för leverantörer och användare. I stället sker all kommunikation via applikationslagret och säkra API:er, vilket innebär att användare aldrig får direkt åtkomst på nätverksnivå till byggens tekniska nät.

Åtkomst begränsas till en specifik session och en definierad endpoint, och det är inte möjligt att hoppa mellan anläggningar eller system via portalen. Detta följer principerna om segmentering och ”least privilege”, där användaren endast får den minsta åtkomst som krävs för att utföra en uppgift, och attackytan hålls mycket liten.

# Krypterad kommunikation

All information som utväxlas mellan användare, anläggningar och molntjänster i Zaphire är krypterad över HTTPS med TLS 1.2 och 1.3. Detta gäller både extern kommunikation mot portal och API samt intern trafik mellan mikrotjänster i molnlösningen, så att ett eventuellt intrång i en del inte ger fri tillgång vidare.

Zaphire följer principen ”stängt som standard” – API:er och funktioner måste explicit öppnas genom behörighetsstyrning innan de kan användas. Detta minskar risken för felkonfiguration och gör det enklare att ha kontroll över vem som kan göra vad, särskilt i miljöer med många användare, integrationer och bygg. Systemet öppnar inte heller portar direkt mot internet från anläggningarna, utan kommunikationen sker via kontrollerade och säkra endpoints i plattformen.

# DDoS-skydd

På nätverksnivå bygger Zaphire på principer om segmentering och isolering. Tekniska system placeras på egna VLAN, och inkommande trafik till anläggningarnas nät begränsas kraftigt med brandväggsregler, så att obehörig trafik stoppas tidigt.

Plattformen är dessutom skyddad mot volymattacker genom avancerad trafikfiltrering och DDoS-skydd i underliggande infrastruktur, vilket säkerställer att tjänsten förblir tillgänglig även under hög belastning. Detta bidrar till att SD-anläggningen upplevs stabil även när det finns ökad risk eller pågående attacker mot internetexponerade tjänster.

# Implementeringsmodell och skalbarhet

Traditionella SD-projekt har ofta långa utrullningsfaser, komplexa integrationer och tidskrävande idrifttagningar. Zaphire gör det annorlunda. Lösningen är byggd för att vara snabb, säker och enkel att ta i bruk – utan att kräva stora förändringar i befintlig infrastruktur.

Tack vare den modulbaserade arkitekturen och öppna protokoll kan Zaphires lösning faktiskt kopplas till ett befintligt SD-system på under 20 minuter. Allt som krävs är att en elektriker etablerar fysisk anslutning mot byggens SD-system, till exempel via BACnet/IP, Modbus, SRD-link eller MQTT.

Elektrikern ansvarar för fysisk anslutning och signalåtkomst, medan Zaphire ansvarar för datainsamling, säkerhet, analys och visualisering. När signalerna är tillgängliga kopplas Zaphires molnplattform automatiskt upp, och datainsamlingen startar omedelbart. Därmed finns inget behov av VPN, tunga IT-konfigurationer eller komplexa integrationsprojekt.

### Skalerbarhet

När ett bygg är anslutet kan lösningen enkelt skalas till fler lokationer. Zaphire använder samma säkra anslutningsmetod, vilket gör att nya bygg kan aktiveras med minimalt avtryck och utan behov av nya installationer. Detta gör systemet idealiskt för portföljer som önskar snabb utrullning, standardiserad datatillgång och enhetlig rapportering.

zaphire

## Intresserad av att veta mer?
## Kontakta oss idag!

info@zaphire.no
+47 40 00 88 00