

Zaphire

Sikker kommunikasjonsarkitektur - Zaphire BMS til Zaphire EMS



Introduksjon

Zaphires arkitektur er utformet for å sikre trygg, pålitelig og kontrollert dataflyt fra kundens lokale miljø til Zaphire sin skyplattform, uten behov for innkommende tilgang. Den støtter både en direkte API-kommunikasjonsmodell og en valgfri DMZ-basert API-gateway for organisasjoner med strengere sikkerhets- og styringskrav. All kommunikasjon er utgående og sikret med HTTPS (TLS).

Direct API Communication Model

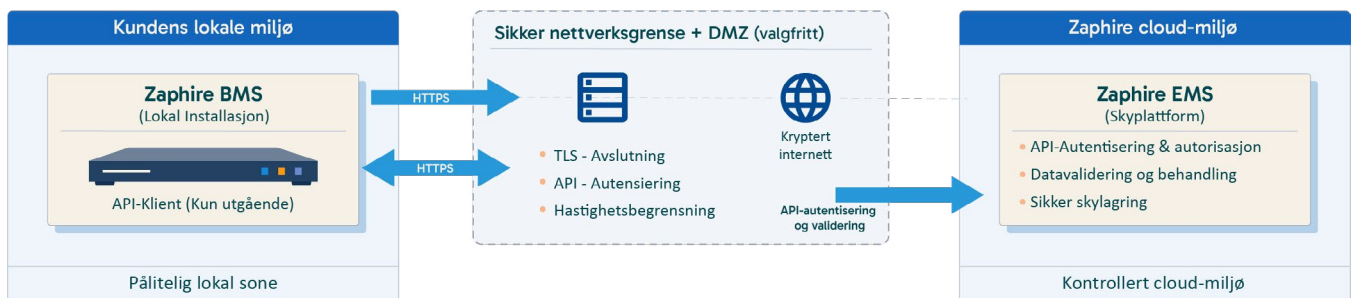
I denne modellen overfører en lokalt installert Zaphire BMS data sikkert direkte til den skybaserte Zaphire EMS ved hjelp av utgående HTTPS (TLS)-basert API-kommunikasjon. BMS initierer alle tilkoblinger, og det kreves ingen innkommende tilgang til kundens miljø. En kundeadministrert brannmur kan begrense trafikken slik at kun utgående HTTPS-tilkoblinger til Zaphire EMS-endepunktet er tillatt.



➡ Enveis dataflyt | 🛡️ Ingen innkommende tilgang | 🔒 Kryptert transport | 📋 Revidert og overvåket

API Gateway (DMZ) Communication Model (Optional)

I denne valgfrie utrullingsmodellen introduseres en API-gateway i en demilitarisert sone (DMZ) for å gi ekstra sikkerhetskontroller. Zaphire BMS fortsetter å initiere kun utgående HTTPS-tilkoblinger. API-gatewayen håndterer autentisering, hastighetsbegrensning og validering av forespørsler før godkjent trafikk videresendes til Zaphire EMS. Dette mønsteret brukes ofte i virksomhetsmiljøer som krever forbedret segmentering og sentralisert API-styring.



➡ Enveis dataflyt | 🛡️ Ingen innkommende tilgang | 🔒 Kryptert transport | 📋 Revidert og overvåket