Zaphire

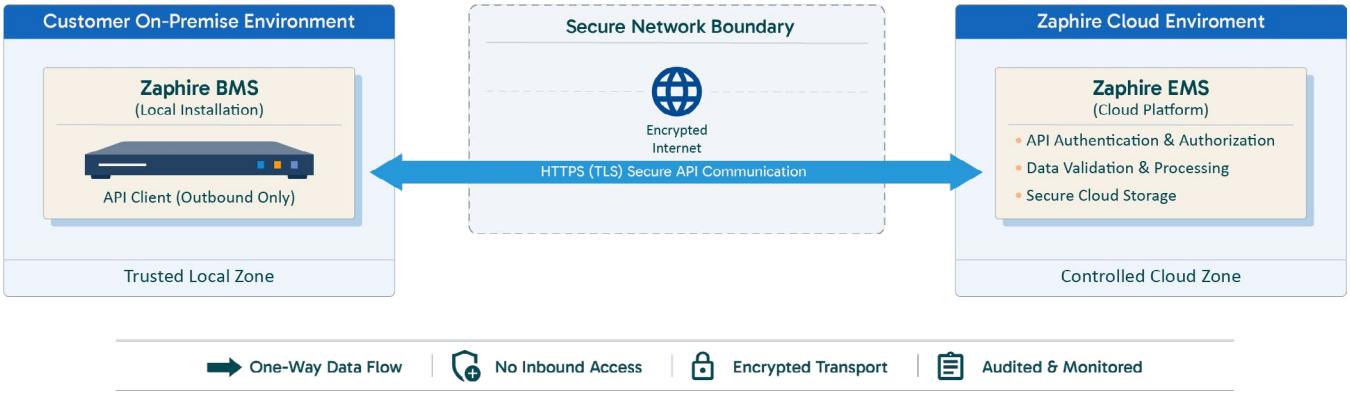
Secure Communication Architecture - Zaphire BMS to Zaphire EMS

Introduction

Zaphire's architecture is designed to ensure secure, reliable, and controlled data flow from the customer's local environment to the Zaphire cloud platform, without requiring inbound access. It supports both a direct API communication model and an optional DMZ-based API gateway for organizations with stricter security and governance requirements. All communication is outbound-only and secured using HTTPS (TLS).

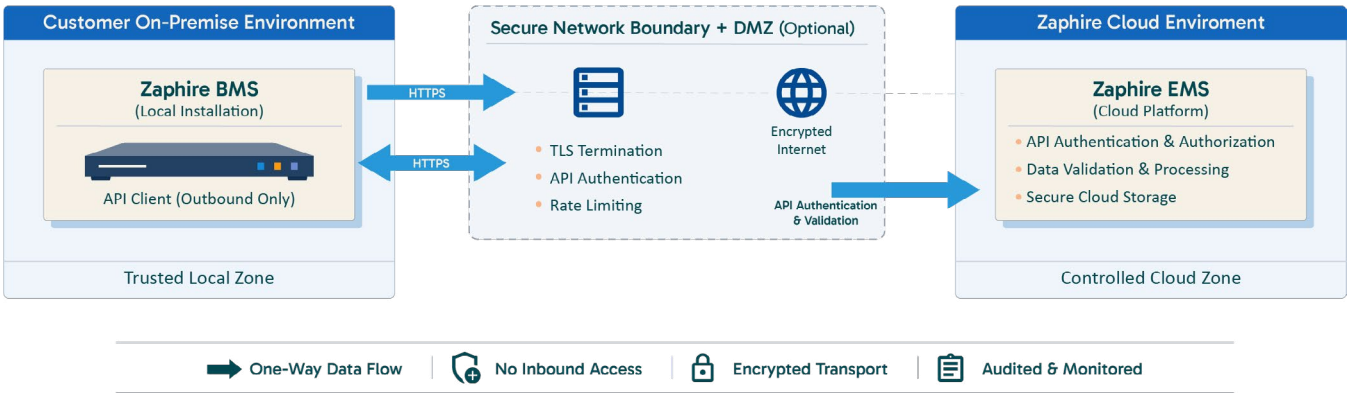
Direct API Communication Model

In this model, a locally installed Zaphire BMS securely transmits data directly to the cloud-based Zaphire EMS using outbound HTTPS (TLS) API communication. The BMS initiates all connections, and no inbound access to the customer environment is required. A client-managed firewall can restrict traffic so that only outbound HTTPS connections to the Zaphire EMS endpoint are permitted.



API Gateway (DMZ) Communication Model (Optional)

In this optional deployment model, an API gateway is introduced within a demilitarized zone (DMZ) to provide additional security controls. The Zaphire BMS continues to initiate outbound HTTPS connections only. The API gateway enforces authentication, rate limiting, and request validation before forwarding approved traffic to the Zaphire EMS. This pattern is commonly used in enterprise environments requiring enhanced segmentation and centralized API governance.



zaphire