IOT Jetstream Cybersecurity Product Brief

IOT Jetstream is a cloud-based integration platform developed with robust cybersecurity features that protect your data and your building. This document explains how our innovative platform achieves high-level security at each data handoff point.

User Authentication

Jetstream leverages Okta's authentication platform to manage access to its API. Specifically, OAuth 2.0 is used by clients to authenticate with the Authorization Server and retrieve a secure token. The token can be used to interface with Jetstream APIs without sharing passwords or API keys. These measures also enable building and role-focused access management for tightened security.

Encryption

IOT Jetstream uses the TLS 1.2+ protocol to encrypt all external traffic and keep data secure during transfer.

TLS 1.2+ protocols prevent third parties from viewing data between client and server applications during transmission. You can be confident that any information transmitted between Jetstream APIs and an API client is protected from eavesdroppers and hackers. Enforcing the use of recent versions of the TLS protocol eliminates obsolete cryptographic algorithms and enhances security over older versions of the security protocol.

TLS Auth

In addition to the standard TLS, IOT Jetstream can utilize mutual TLS (mTLS) authentication for traffic going from public clouds to private clouds. Unlike standard TLS, where only the server has a TLS certificate, with mTLS both the client and server have certificates. This allows authentication on both sides when using public/private key pairs and ensures traffic between clients and servers is secure in both directions.

mTLS authentication is excellent for preventing cyberattacks, including:

- Brute force attacks
- Credential stuffing
- Malicious API requests
- On-path attacks
- Phishing
- Spoofing

This sophisticated authentication method is particularly valuable for verifying connections that do not use a login process, like Internet of Things (IoT) devices.

JSON Web Tokens

A JSON web token (JWT) is a security token that enables information about identity and claims to be shared across security domains. Encoded like a JSON object, the claims within a JWT are used as the basis for web signature structures or JSON web encryption structures. These enable users and systems to sign claims digitally or offer integrity protection through a message authentication code (MAC), which can also be encrypted.

IOT Jetstream uses standard JWT bearer tokens to represent claims between two parties securely, using the industry standard RFC7519 method.

Subnets and Load Balancer

IOT Jetstream allows incoming traffic through the public subnet via a hypertext transfer protocol secure (HTTPS) port on the load balancer. Private subnets only accept connections on behalf of IOT Jetstream's load balancer, ensuring microservices are kept secure.

Buildings IOT's state-of-the-art integration software helps buildings become smart while keeping data safe. Contact our team of experts at hello@buildingsiot.com to learn more about what we can do for you.