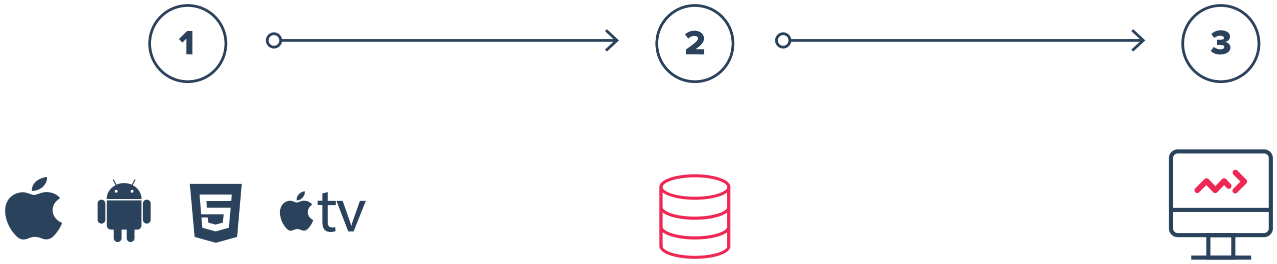
Security

As an enterprise-class customer data platform, the security of our clients' customer data is one of mParticle's primary objectives. As such, our architecture was built with security at its core. This document provides a high-level overview of the security protocols implemented throughout the data journey from the client app to mParticle.



DATA COLLECTION
WITH THE MPARTICLE SDK

THE MPARTICLE
DATA STORE ON AWS

INTERNAL MPARTICLE
PERSONNEL & SYSTEMS

Security begins with the data collection via the mParticle SDK

The mParticle SDK automatically collects anonymous lifecycle data: advertising IDs (Apple IDFA/Google Ad ID), app version, device data (e.g. OS, OS Version, Carrier), and session information (session start/session end).

Our customers explicitly control what custom events are collected by mParticle's SDK beyond the aforementioned data points.

All data is encrypted via Transport Layer Security (TLS) for transport to the mParticle data store. TLS v1, TLS v1.1 and TLS v1.2 are supported.

The SDK further ensures security by ensuring that encryption is signed by a specific Certification Authority (CA), which ensures third parties are unable to inspect data packets via proxies.

All server-to-server endpoints require encryption and authentication.

Upon arrival in the mParticle data store

All data is encrypted via Advanced Encryption Standard 256 bit (AES-256) encryption while in our data store.

All of our customers' data is stored with unique AWS Identity and Access Management (IAM) credentials.

Each customer's data resides on its own partition and data from one customer is never co-mingled with data from another customer.

mParticle employees are prohibited from storing any customer data on their workstations.

Access to mParticle systems is controlled and secured

The ability to access internal systems is restricted to whitelisted internal IP addresses.

Only trusted, background checked operations personnel can access customer accounts, with all access logged and available for auditing purposes.

Multi Factor Authentication (MFA) via mobile tokens is required for all mParticle personnel.

No non-employees have access to internal mParticle systems. No customer data is ever transmitted to employee computers.

User Authentication and Authorization

Role based permissioning is supported (admin, read-only, and custom rights)

Integration partner tiles exposed to clients can be configured to ensure no data is sent to unauthorized vendors

Multi-Factor Authentication Supported

Single Sign-on via SAML 2.0 is supported

Outbound data is sent securely

All data is sent with the strongest data encryption made available by the partner.

Whenever supported, hashed device and user identifiers are sent instead of raw identities