Split Security

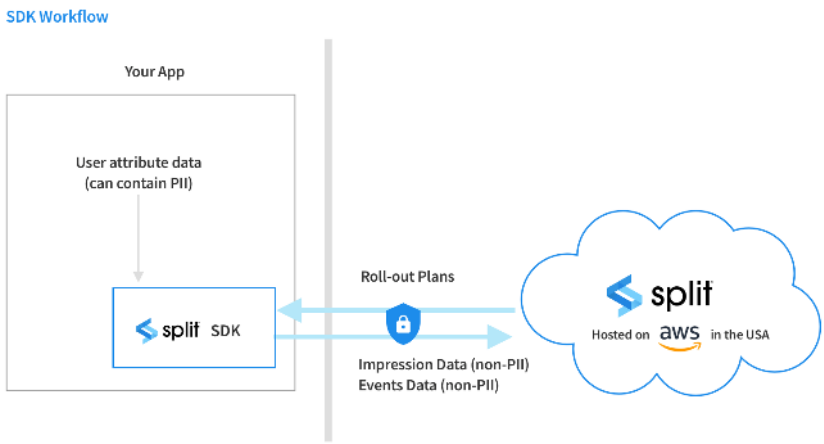
Split's Intelligent Security framework leverages industry-standard security practices and never requires user identifiable data to be sent to Split servers. We understand that with agility comes the need for rigorous access control and data security, and any unauthorized access can directly impact customer experience - which is why we approach security from these five vectors: Access Security, Data Privacy, Product Security, Infrastructure Security and Compliance.

Certifications:

SOC 2 Type 2
This certification underscores Split's dedication and commitment to security and Enterprise readiness.

Privacy Shield
Split agrees to resolve privacy-related issues in a timely manner through cooperation with European data protection authorities and binding arbitration.

Data Privacy
Split's platform was architected to support industry best practices in order to protect PII. Data is processed locally on the customer's servers using Split's SDK which supports 10 languages. Impression and event data is the only information being sent securely to Split's cloud.



2FA (two-factor authentication) and SSO (single sign-on)
Split accounts support two-factor authentication and administrators can view the 2FA status of any user at any time. Single sign-on is available via SAML 2.0 and Google account sign-in (OAuth).

Secure Data Encryption
Split employs SSL encryption in transit, with default communications handled over TLS 1.2 security. Split keys and secrets are stored using the Amazon AWS Key Management Service, and login tokens are salted and encrypted for increased security.

Yearly Penetration Testing
Gotham Digital Science performs an annual penetration test which includes OWASP-10 certification. GDS performs both authenticated and unauthenticated attacks.

10 California Street, Redwood City, CA 94063 I 650-399-0005 I security@split.io