WHITE PAPER

Adobe Analytics Security Overview

July 2024

Table of Contents

Adobe Security

At Adobe, we know the security of your digital experiences is important. Security practices are deeply ingrained into our internal software development and operations processes and tools and are rigorously followed by our cross-functional teams to prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities and we regularly incorporate advanced security techniques into the products and services we offer.

This paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of your Adobe Analytics experience and your data.

About Adobe Analytics

Adobe Analytics enables customers to apply real-time analytics and detailed segmentation across marketing channels to better understand how site visitors interact with their brand across multiple channels. By gathering, analyzing, and acting upon this visitor data, customers can better target these visitors and improve the effectiveness of their marketing. Used alone or in conjunction with other Adobe Experience Cloud solutions, Adobe Analytics turns vast streams of data from any channel into real-time, actionable insights based on true 360-degree visitor views, enabling organizations to improve their visitors' experiences.

Solution Architecture

The Adobe Analytics solution is comprised of three (3) primary processes that handle data collection, data processing, and data output:

Inputs:

- **Client-side code** — Code implemented on the customer's web or mobile property that sends data to Adobe Analytics. There are three ways to implement this client-side code:[1]
  - JavaScript (e.g., AppMeasurement.js)
  - Adobe Analytics Mobile SDK
  - Adobe Experience Platform Tags

- **Other Adobe solutions** — Adobe Analytics can be configured by customers to receive data from other Adobe solutions, including Adobe Target, Adobe Advertising Cloud, and Adobe Audience Manager.

[1] Detailed information about how to implement client-side code can be found on Adobe Experience League.

- **Customer-collected data** — Additional online or offline data collected by customers to use in their marketing analysis instead of or in combination with data collected by client-side JavaScript and the Adobe Analytics Mobile SDK.

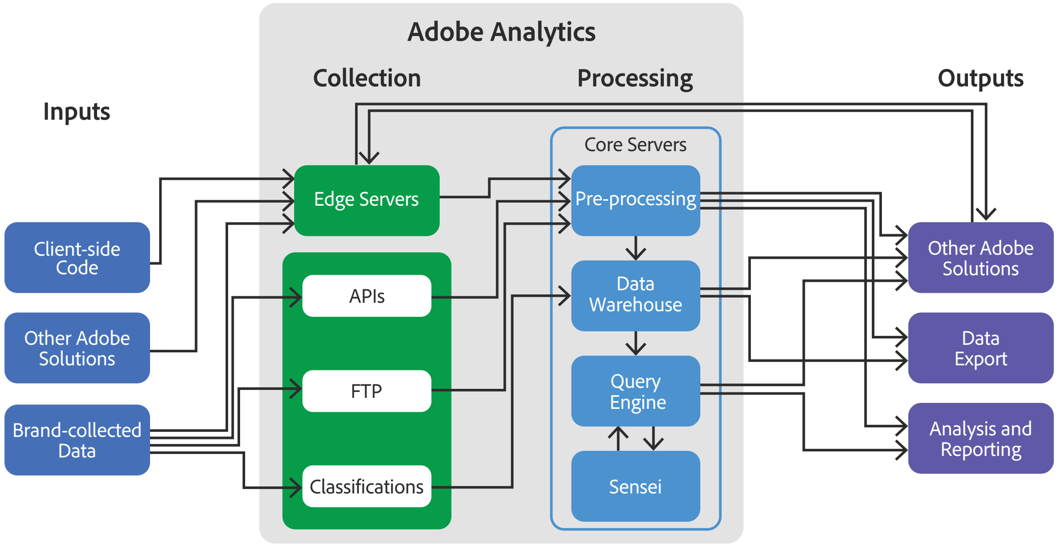

Figure 1: Adobe Analytics Solution Architecture

Data Collection:

- **Edge servers** — Collect data sent by the visitor's web browser or mobile apps that customers want to track and measure.
- **APIs** — Upload web or mobile traffic, or offline data such as, call center interactions, or in-store transactions to Adobe Analytics.
    - Data Insertion API sends data directly to Adobe servers, one event at a time.
    - Bulk Data Insertion API uploads data in batch format, such as in CSV-formatted files.
    - Data Sources API programmatically links applications and transfers data via methods such as HTTP, SOAP, or REST.
- **Data Sources** — Upload files via FTP file transfer to a designated Adobe FTP location. Adobe Analytics processes the file and makes the data available for reporting.
- **Classifications** — Upload classification data via HTTPS or FTP and categorize customer-collected data using variables to provide greater flexibility and visibility into customer interactions with site visitors and other trends. More information about Classifications in Adobe Analytics can be found on Adobe Experience League.

Data Processing:

- **Core sites** — Process, store, and report on visitor behavior data according to rules set by the customer, and include the following:
  - **Pre-processing** — Enhances data with visit and visitor information, device and browser details, rough geographic location, and other metadata and applies customer-defined processing rules and attribution calculations.
  - **Data warehouse** — Stores the processed data for query and analysis by the customer.
  - **Query engine** — Provides an interface for interactive ad hoc queries of data stored in the data warehouse. This is also used by the analysis and reporting tools described in the Data Output section below to access data.
  - **Adobe Sensei** — Analyzes data and detects anomalies through AI and ML methods.

Data Output:

- **Other Adobe solutions** — Send data from Adobe Analytics to other Adobe solutions, including Adobe Audience Manager, Adobe Advertising Cloud, and Adobe Experience Platform.

- **Data Export**[2]
  - **LiveStream** — Send Adobe Analytics raw data directly into custom dashboards or other reporting systems.
  - **Data Feeds** — Send raw data on an hourly basis in a batch fashion (typically in a single file) via FTP, sFTP, or cloud storage.
  - **Data Warehouse reporting** — Retrieve advanced data relationships from raw data via email or FTP based on specific, defined questions.

- Analysis and Reporting tools, which include the following:
  - **Analysis Workspace** — Provides a canvas for customers to drag components to meet reporting requirements
  - **Adobe Analytics Dashboards** — Allows access to intuitive scorecards with key metrics, detailed breakdowns, and trend reports via a mobile app.
  - **Activity Map** — Overlays which elements on the customer's site were clicked most often, using a browser plug-in
  - **Reports & Analytics** — Provides dozens of pre-built reports for novice users.
  - R**eport Builder** — A Microsoft Excel add-in that allows customers to retrieve Adobe Analytics data and place it directly into a workbook.
  - **Reporting AP**I — Sends Adobe Analytics data to third-party reporting or dashboard software.

[2] The security of data exported from Adobe Analytics to a third-party application becomes the responsibility of the customer.

Security Architecture and Data Flow

The following steps describe how data flows in a typical Adobe Analytics implementation. This section assumes that the customer has already defined the data they want to track:

1. When a visitor lands on a site on which the customer has incorporated Adobe Analytics client-side code, this code makes an image request to the Adobe Edge server located geographically closest to the visitor.[3] The image request includes a standard set of information about the visitor's machine configuration and the page they are viewing, as well as the pre-defined information the customer wants to track.

2. Along with the image, the Edge server returns a cookie containing a pseudonymous visitor ID, which is included in image requests on subsequent pages.

3. Throughout the visitor's web session, the Adobe Analytics client-side code relays the tracked information to the Edge server.

4. The Edge server forwards the visitor data to the Adobe Core site containing that customer's data. Communications between the client and Edge servers typically use the same communication method as the page itself (e.g., HTTP or HTTPS) however, it is possible for HTTPS to be used on HTTP pages.[4] The mobile SDK, however, always uses HTTPS.

5. The Core site server pre-processes the data, enhances it with additional metadata, and applies customer-defined processing rules. In addition, during pre-processing, Adobe applies visit, visitor, and attribution calculations. This data is then stored in a data warehouse within the Core site.

6. At this point, the customer can view or export the data gathered by Adobe Analytics using one of the reporting or export options included in the solution.

Data Encryption

All data in-transit between Adobe Edge sites and Core sites and through any ingress/egress point exposed to the public internet is encrypted using HTTPS TLS 1.2 or greater.

Data at-rest within the Core sites is generally stored unencrypted. Data at-rest within any cloud provider is always encrypted.

Data in the customer's control, which includes data sent from the custom JavaScript on the website to an Adobe Edge site, uses the protocol specified by the customer (HTTPS or HTTP). Communications from mobile applications to Adobe Edge sites using the Mobile SDK use HTTPS, as do all reporting APIs.

[3] Unless the customer chooses to restrict data collection to Edge sites in their preferred region (EU, US, or APAC).

[4] Adobe encourages customers to use HTTPS or similarly secure methods for all data they send to or export from Adobe Analytics.

User Authentication

Access to the Adobe Analytics user interface requires authentication with a username and password. We continually work with our development teams to implement new protections based on evolving authentication standards. Users can access Adobe Analytics in one of three (3) different types of user- named licensing:

Adobe ID is for Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users.

Enterprise ID is an Adobe-hosted, enterprise-managed option for accounts that are created and controlled by IT administrators from the customer enterprise organization. While the organization owns and manages the user accounts and all associated assets, Adobe hosts the Enterprise ID and performs authentication. Admins can revoke access to Adobe Analytics by taking over the account or by deleting the Enterprise ID to permanently block access to associated data.

Federated ID is an enterprise-managed account where all identity profiles—as well as all associated assets—are provided by the customer's Single Sign-On (SSO) identity management system and are created, owned, controlled by customers' IT infrastructure. Adobe integrates with most any SAML 2.0-compliant identity provider.

Adobe IDs and Enterprise IDs both leverage the SHA-256 hash algorithm in combination with password salts and a significant number of hash iterations. Adobe regularly monitors Adobe-hosted accounts for unusual or anomalous account activity and evaluates this information to help quickly mitigate threats. For Federated ID accounts, Adobe does not manage the users' passwords.

More information about Adobe's identity management services can be found in the Adobe Identity Management Services security overview.

Roles, Permissions and Entitlements

Administrators can provision the Adobe Analytics application and entitle users in the Adobe Admin Console. Admins can grant or restrict access to specific tools and datasets, as well as to specific fields within a dataset. For more information on specialized methods for accessing Adobe Analytics data and reporting via approved applications, please see the data sources guide on Adobe Experience League.

Hosting Locations

Adobe maintains eight (8) Edge sites for data collection and three (3) Core sites for data processing for Adobe Analytics. Edge sites are hosted in data centers of leading cloud service providers in locations around the world, while Core sites are hosted in an Adobe- owned data center in Oregon (for U.S. customers) and on Adobe-owned servers in leased data center space in London, England (for customers in the EU), and in Singapore (for customers in Asia), with some processing and storage happening in leading cloud service providers in the same region.

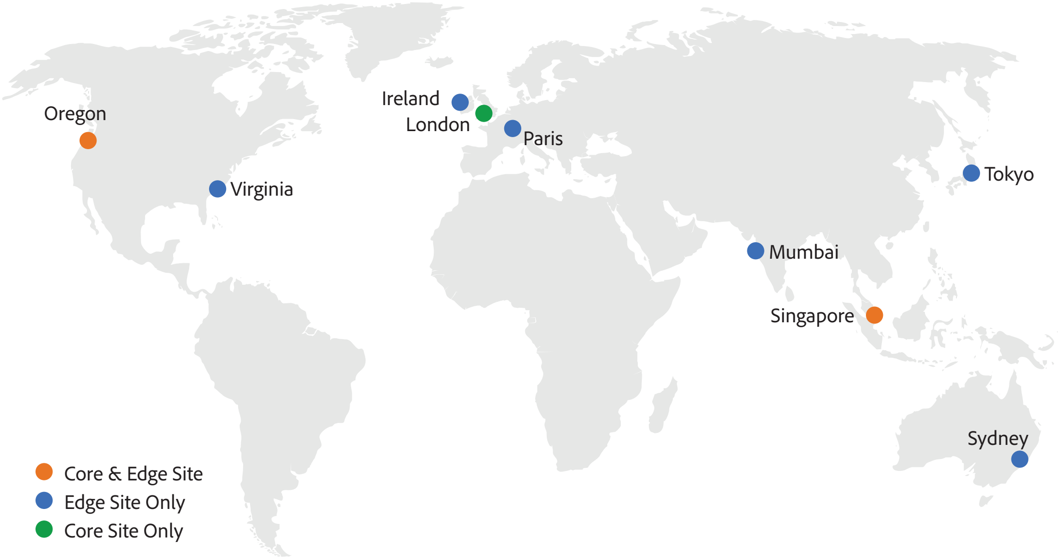

Figure 2 — Adobe Analytics Hosting Locations

Customers can configure data collection for their report suites to use the Edge site that is closest to each website visitor's location or restrict collection to the Edge sites in their preferred region (US, Europe, or Asia).

In the event of a disruption in communication between the Edge site and the Core site, data is saved locally and then forwarded to the customer-configured Core site when communication is restored.

For major disruptions, Adobe reconfigures the global DNS system used by Adobe Edge sites to route customer data through another Edge site (in the customer's preferred region, if applicable).

Roles, Permissions and Entitlements

Data is placed into separate databases (a.k.a., report suites), and a single customer's site reports are grouped together on one or more servers. In some cases, more than one customer may share a server, but the data is segmented into separate databases. The only access to these servers and databases is via secure access by the Adobe Analytics solution. All other access to the application and data servers is made only by authorized Adobe personnel and is conducted via encrypted channels over secure management connections.

Questions?

For more information about Adobe's operational, application, and enterprise security processes, compliance certifications, incident response program, security training and awareness program, and business continuity and disaster recovery program, please see the Adobe Trust Center.

Adobe

07/24