Adobe Experience Cloud

WHITEPAPER

Adobe® Analytics Security Overview

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 multiple channels to better understand how site visitors interact with their brand. 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.

Adobe Analytics Solution Architecture

The Adobe Analytics solution is comprised of four (4) primary components that handle data input, collection, processing, and 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.

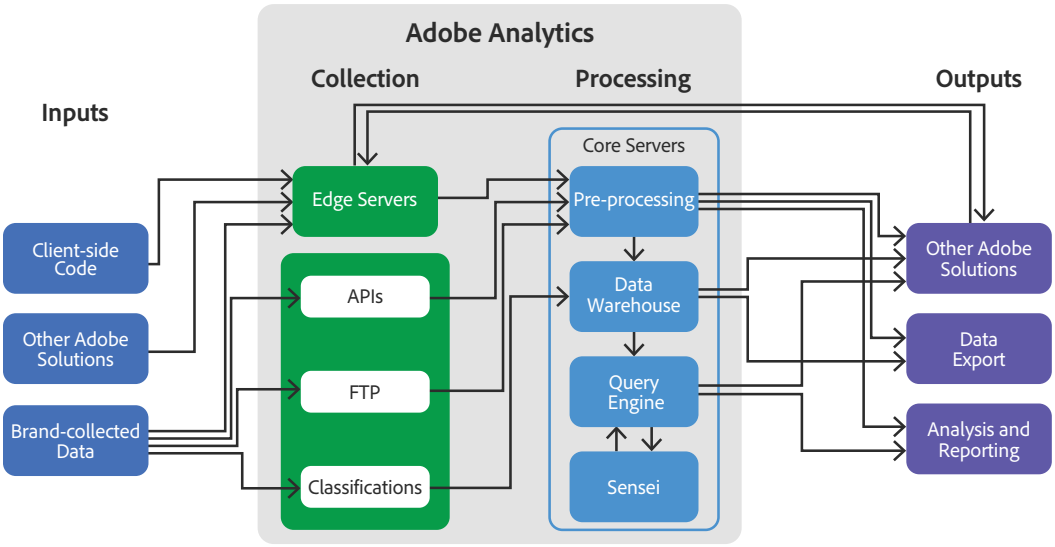

Figure 1: Adobe Analytics Solution Architecture

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** — Contain servers that 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.
  - **Report Builder** — A Microsoft Excel add-in that allows customers to retrieve Adobe Analytics data and place it directly into a workbook.
  - **Reporting API** — 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.

Adobe Analytics 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 Core sites is stored unencrypted, while data at-rest within Edge sites is always stored 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.

Adobe Analytics 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 to 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).

Segregation of Customer Data

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.

Adobe Security Program Overview

The integrated security program at Adobe is composed of five (5) centers of excellence, each of which constantly iterates and advances the ways we detect and prevent risk by leveraging new and emerging technologies, such as automation, AI, and machine learning.

Figure 3: Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

- **Application Security** — Focuses on the security of our product code, conducts threat research, and implements bug bounty.
- **Operational Security** — Helps monitor and secure our systems, networks, and production cloud systems.
- **Enterprise Security** — Concentrates on secure access to and authentication for the Adobe corporate environment.
- **Compliance** — Oversees our security governance model, audit and compliance programs, and risk analysis.
- **Incident Response** — Includes our 24x7 security operations center and threat responders.

Illustrative of our commitment to the security of our products and services, the centers of excellence report to the office of the Chief Security Officer (CSO), who coordinates all current security efforts and develops the vision for the future evolution of security at Adobe.

The Adobe Security Organization

Based on a platform of transparent, accountable, and informed decision-making, the Adobe security organization brings together the full range of security services under a single governance model. At a senior level, the CSO closely collaborates with the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) to help ensure alignment on security strategy and operations.

In addition to the centers of excellence described above, Adobe embeds team members from legal, privacy, marketing, and PR in the security organization to help drive transparency and accountability in all security-related decisions.

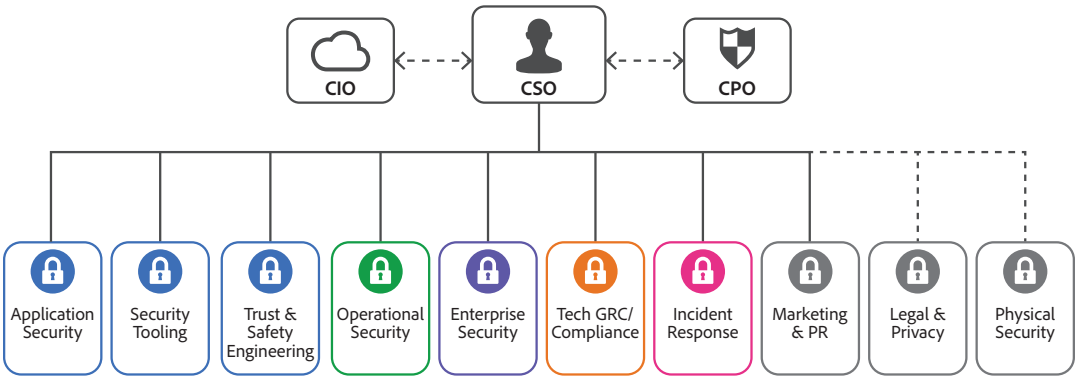

Figure 4: The Adobe Security Organization

As part of our company-wide culture of security, Adobe requires that every employee completes our security awareness and education training, which requires completion and re-certification on an annual basis, helping ensure that every employee contributes to protecting Adobe corporate assets as well as customer and employee data. On hire, our technical employees, including engineering and technical operations teams, are auto-enrolled in an in-depth "martial arts"-styled training program, which is tailored to their specific roles. For more information on our culture of security and our training programs, please see the Adobe Security Culture white paper.

The Adobe Secure Product Lifecycle

Integrated into several stages of the product lifecycle—from design and development to quality assurance, testing, and deployment— the Adobe Secure Product Lifecycle (SPLC) is the foundation of all security at Adobe. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC defines clear, repeatable processes to help our development teams build security into our products and services and continuously evolves to incorporate the latest industry best practices.

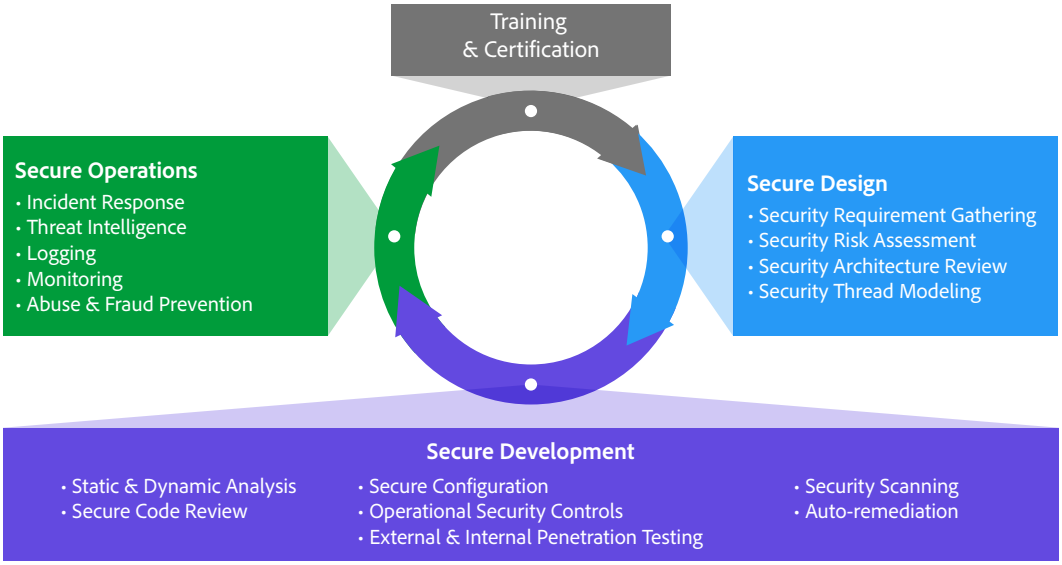

Figure 5: The Adobe Secure Product Lifecycle

Adobe maintains a published Secure Product Lifecycle Standard that is available for review upon request. More information about the components of the Adobe SPLC can be found in the Adobe Application Security Overview.

Adobe Application Security

At Adobe, building applications in a "secure by default" manner begins with the Adobe Application Security Stack. Combining clear, repeatable processes based on established research and experience with automation that helps ensure consistent application of security controls, the Adobe Application Security Stack helps improve developer efficiency and minimize the risk of security mistakes. Using tested and pre-approved secure coding blocks that eliminate the need to code commonly used patterns and blocks from scratch, developers can focus on their area of expertise while knowing their code is secure. Together with testing, specialized tooling, and monitoring, the Adobe Application Security Stack helps software developers to create secure code by default.

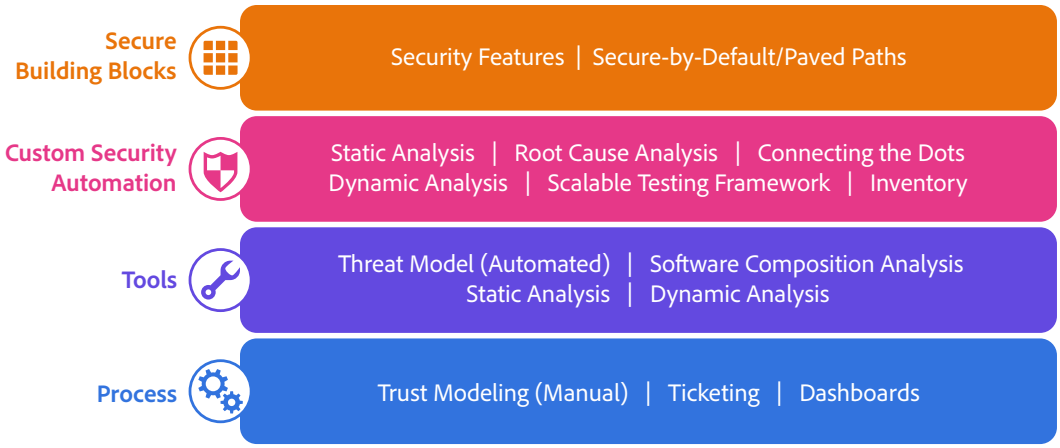

Figure 6: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of public cloud infrastructure. These standards are available for view upon request. For more information on Adobe application security, please see the Adobe Application Security Overview.

Adobe Operational Security

To help ensure that all Adobe products and services are designed from inception with security best practices in mind, the operational security team created the Adobe Operational Security Stack (OSS). The OSS is a consolidated set of tools that help product developers and engineers improve their security posture and reduce risk to both Adobe and our customers while also helping drive Adobe-wide adherence to compliance, privacy, and other governance frameworks.

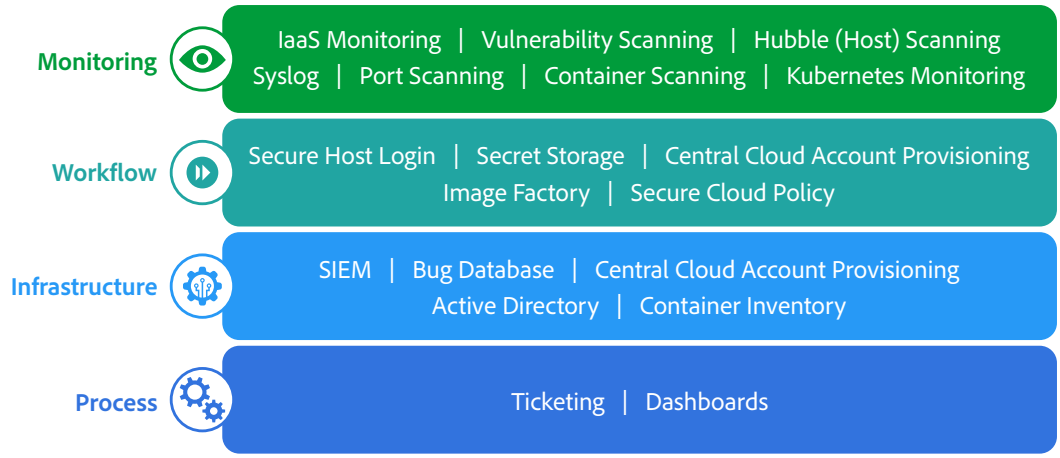

Figure 7: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. For a detailed description of the Adobe OSS and the specific tools used throughout Adobe, please see the Adobe Operational Security Overview.

Adobe Enterprise Security

In addition to securing our products and services as well as our cloud hosting operations, Adobe also employs a variety of internal security controls to help ensure the security of our internal networks and systems, physical corporate locations, employees, and our customers' data.

For more information on our enterprise security controls and standards we have developed for these controls, please see the Adobe Enterprise Security Overview.

Adobe Compliance

All Adobe products and services adhere to the Adobe Common Controls Framework (CCF), a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams. As much as possible, Adobe leverages leading-edge automation processes to alert teams to possible non-compliance situations and help ensure swift mitigation and realignment.

Adobe products and services either meet applicable legal standards or can be used in a way that enables customers to help meet their legal obligations related to the use of service providers. Customers maintain control over their documents, data, and workflows, and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU.

Adobe also maintains a compliance training and related standards that are available for review upon request. For more information on the Adobe CCF and key certifications, please see the Adobe Compliance, Certifications, and Standards List.

Incident Response

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution processes are nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help achieve the highest levels of security for all Adobe products and services.

We also maintain internal standards for incident response and vulnerability management that are available for view upon request. For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Business Continuity and Disaster Recovery

The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified BCDR Program enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information can be found in the Adobe Business Continuity and Disaster Recovery Program Overview.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Experience Manager as a Managed Service and your confidential data. At Adobe, we take the security of your digital experience data very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security our customers' data.

For more information about Adobe security, please go to the Adobe Trust Center.

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative.