WHITE PAPER

Adobe Experience Platform Security Overview

October 2024

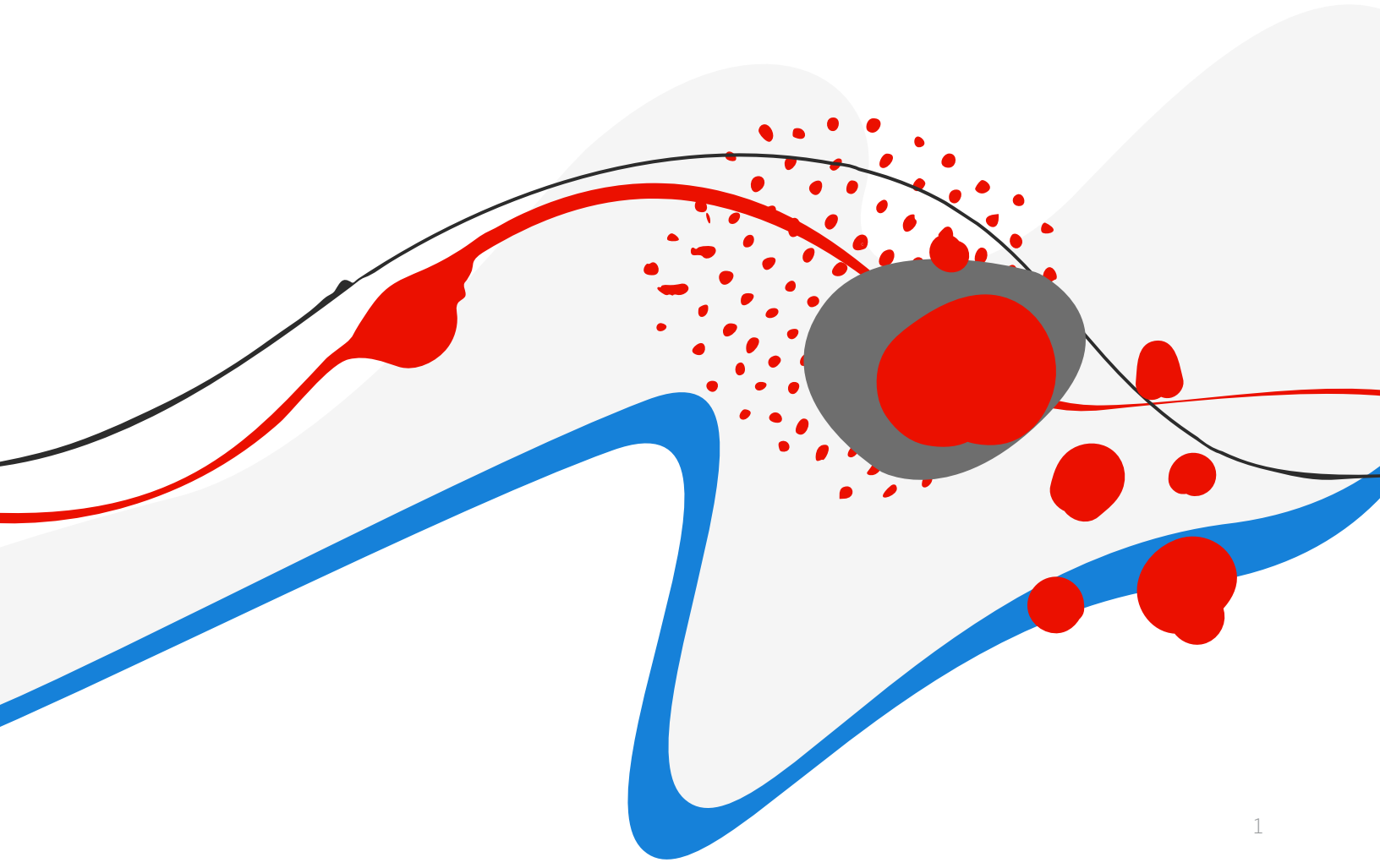


Table of Contents

Adobe Security

At Adobe, we take the security of your digital experience and assets seriously. Security practices are integrated into our internal software development processes, operations, and tools. Our cross-functional incident response teams are proactive and nimble in preventing, detecting, and responding to incidents. Furthermore, our collaborative work with partners, leading researchers, and other industry organizations helps us stay updated with the latest threats, vulnerabilities, and security best practices, thereby enabling us to continually build security into the products and services we offer. What's more, we regularly incorporate advanced security techniques into our product and service offerings.

This white paper describes Adobe's defense-in-depth approach and security procedures to secure your data and the Adobe® Experience Platform experience.

About Adobe Experience Platform

Adobe Experience Platform (AEP) is an open and extensible system designed to help brands build customer trust while delivering better, more personalized experiences. By centralizing and standardizing customer experience data and content across the enterprise, Experience Platform enables organizations to have an actionable, single view of their customer. Customer experience data can be enriched with intelligent capabilities that provide insights about customer interactions and the implications of customer engagement.

Experience Platform makes data, content, and insights available to delivery systems to act upon in real time, yielding compelling experiences at the right moment, and its robust data governance controls help organizations use data responsibly while delivering personalized experiences. Built on REST APIs, Adobe Experience Platform exposes the full functionality of the system to developers and partners, supporting the simple integration of enterprise solutions and other technologies using familiar tools.

Adobe Experience Platform Architecture

Adobe Experience Platform enables brands to ingest data from a variety of sources (in either batch or streaming format) to help them better understand the behavior of their customers. Typical sources include enterprise data sources, such as the customer's own web and mobile applications, CRM and other enterprise applications, cloud-based storage, and other Adobe applications.[1]

1 Source connectors, as well as ingestion run times and throughput management, are customizable in the Adobe Experience Platform UI.

Using Experience Platform services, customers can structure, label, and enhance incoming data. This data is then stored in the Experience Platform data lake or profile service for analysis and use by downstream services and applications, including:

- Native applications built on top of AEP, including Adobe Customer Journey Analytics (CJA), Adobe Journey Optimizer (AJO), and Adobe Real-time Customer Data Platform (RTCDP);
- Adobe Intelligent Services, including Customer AI and Attribution AI, which leverage the power of artificial intelligence and machine learning in customer experience use cases;
- Adobe Experience Cloud® applications and capabilities, such as Adobe Analytics, Adobe Target, Adobe Campaign, and Adobe Experience Manager; and customer- and partner-developed custom applications.

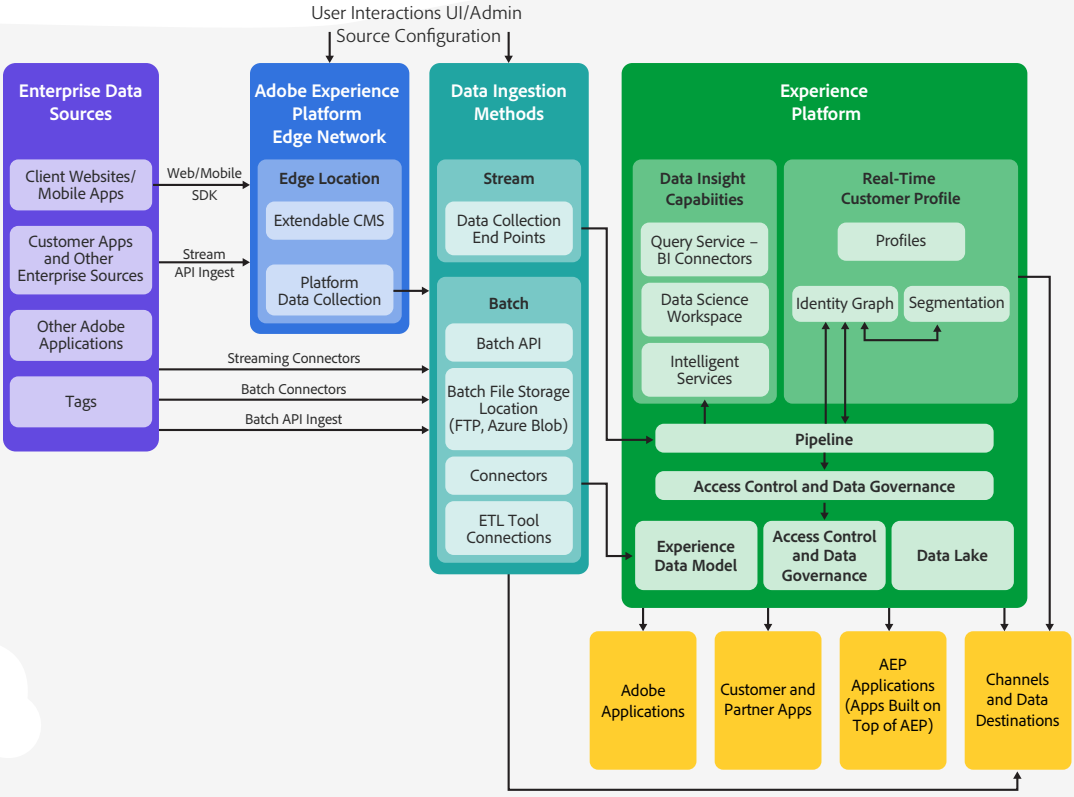


Figure 1: Adobe Experience Platform solution architecture

Experience Platform Security Architecture and Data Flow

Adobe Experience Platform enables customers to ingest and export data in the following ways:

Enterprise Data Source Ingestion

- **Client-side Data Collection**: Customer websites and mobile applications send data to the Adobe Experience Platform Edge Network for staging and preparation for ingestion using the web and mobile SDKs.
- **Server-side Data Collection**: Adobe Experience Cloud applications and enterprise data sources use built-in connectors to stream data directly to Experience Platform:
  - Adobe Experience Cloud applications, as well as enterprise data sources, send streaming and batch data to Experience Platform using built-in connectors.
  - User credentials are stored in the cloud provider's key vault.
  - Adobe Experience Platform application services use HTTPS TLS 1.2 to secure data in transit, where applicable.
- **Batch Ingestion via ETL Partners**: Data ingestion occurs using a non-Adobe ETL (extract, transform, and load) tool and the Experience Platform API for batch data consumption. The ETL tools and the corresponding dataflows reside in the customer environment.
- **Adobe Tags**: A service integrated into Experience Platform as a value-add feature, Tags provides a user interface and an API for customers to define what code should execute in a web or mobile property based on specific end-user interactions.

User Interactions and Admin Source Configurations

- Administrators and users with appropriate access permissions authenticate themselves to the Experience Platform UI and configure various options for data source collection. Using credentials stored in the cloud service provider's key vault, these individuals connect to enterprise data sources, ingest data, and create and modify dataflows.

Access Control and Data Governance

- The Experience Platform access control and data governance layer strictrly controls access to Experience Platform services, whether to write new data or read existing data.

Data Lake

- Based on the data model and configuration settings in the admin UI, Experience Platform writes data to the specific customer's location in the Experience Platform data lake.

Data Destinations

- Authenticated Adobe applications, customer and partner applications, and applications built natively on Experience Platform (including Adobe Customer Journey Analytics, Adobe Journey Optimizer, and Adobe RTCDP), can access results of analysis and processing as well as specific data sets.
- Experience Platform can also funnel results to customer-specific channels and data destinations, such as cloud storage or social media feeds.

Data Encryption

All data in transit between Experience Platform (in green in Fig. 1) and any external component, including the web and mobile SDKs, is secured over encrypted connections using HTTPS TLS v1.2. By default, all data at-rest is encrypted by the cloud service provider.

Optionally, Adobe provides the ability for customers to manage their own encryption keys. This customer-managed key (CMK) functionality enables businesses to control encryption and to grant and revoke access to data within their organization. Please contact your Adobe representative for more information.

User Authentication

IT administrators entitle end-user access to Adobe Experience Platform by utilizing named user licensing in the Adobe Admin Console. Detailed information about Adobe's identity management services is available in the Adobe Identity Management Services security overview

Data Governance in Experience Platform

Access Control

Adobe Experience Platform customers can use a robust set of access control capabilities to manage access to resources and workflows. Role-based access control ensures that only authorized users can access data and attribute-based access control enables administrators to control access to specific objects and/or capabilities based on attributes, such as metadata added to a schema field or segment.

Using the access control features, Experience Platform customers can manage data usage and prevent data leakage, helping ensure regulatory compliance. Administrators benefit from a centralized administration interface to seamlessly manage permissions required for users to access sandboxes and specific workflows, including data ingestion, data modeling, data management, profile management, identity management, and destinations.

Data Usage Label Enforcement (DULE)

Adobe Experience Platform allows customers to restrict the usage of data outside of the platform due to organizational needs or contractual obligations by applying data usage labels to datasets and fields andcategorizing each according to related data governance policies and access control policies. Using Adobe's patented Data Usage Labeling Enforcement (DULE) framework, customers can label data and enforce data usage policies based on those labels either through automatic policy enforcement or API-based enforcement. Customers can also customize labels and data usage policies based on their own standards and requirements.

For more information on policy enforcement, please see the data policy enforcement overview.

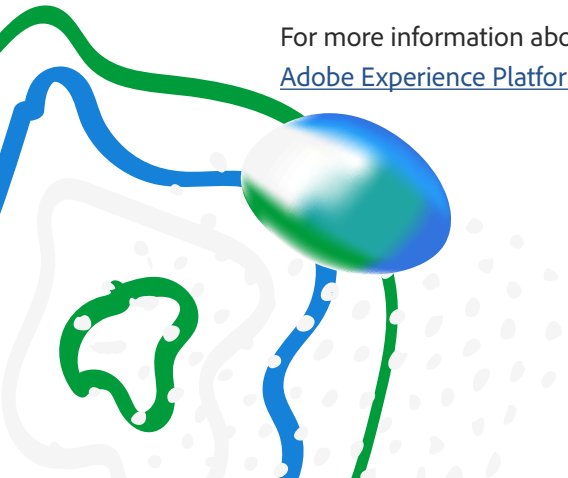
For more information on the "core" data usage labels available in Experience Platform out of the box and the governance policies they represent, please see the guide on core data usage labels.

Sandboxes

In Adobe Experience Platform, customer data is contained within sandboxes, or virtual partitions, within a single Experience Platform instance. These sandboxes are shared across Experience Platform services and applications and provide operational and data isolation to support market, brand, or initiative-focused marketing and digital experience operations.

Adobe provides two types of sandboxes to support software development lifecycle requirements: development and production. Experience Platform supports multiple production and development sandboxes, with each sandbox maintaining its own independent library of Experience Platform resources, including schemas, datasets, and profiles. Content and actions taken within any given sandbox are confined only to that sandbox and do not affect any other sandboxes.

For more information about Adobe Experience Platform data governance, please see the Adobe Experience Platform Data Governance white paper.



Adobe Experience Platform Hosting and Security

Data Center Locations

The Adobe Experience Platform service infrastructure resides in enterprise-class data centers from public cloud service providers in North America (Toronto and Virginia), EMEA (The Netherlands and the U.K.), and APAC (India and Australia). Upon provisioning, customers can designate the regional data center(s) where the data ingested into Experience Platform will be sent for storage.

Figure 2: Adobe Experience Platform Data Center Locations

Logical Isolation of Customers

Customer data in Adobe Experience Platofrm is logically isolated across customers.

Disaster Recovery

Adobe Experience Platform uptime data is available on the Adobe Status website. Additionally, for both planned and unplanned system downtime, the Experience Platform team follows a notification process to inform customers about the status of the service. If there is a need to migrate the operational service from a primary site to a disaster recovery site, customers will receive several specific notifications including:

- Notification of completion of the migration to the disaster recovery site
- Notification of the intent to migrate the services to the disaster recovery site
- Hourly progress updates during the service migration

The notifications will also include contact information and availability for client support and customer success representatives. These representatives will answer questions and concerns during the migration as well as after the migration to promote a seamless transition to newly active operations on a different regional site.

Audit Logs

To increase the transparency and visibility of activities performed in the system, Adobe Experience Platform allows customers to audit user activity. These logs form an audit trail that can help with troubleshooting issues as well as enable compliance with both corporate data stewardship policies and regulatory requirements.

The audit logs track which user performed what action and when. Each action recorded in a log contains metadata that indicates the action type, date and time, the email ID of the user who performed the action, and additional attributes relevant to the action type.

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.

10/24