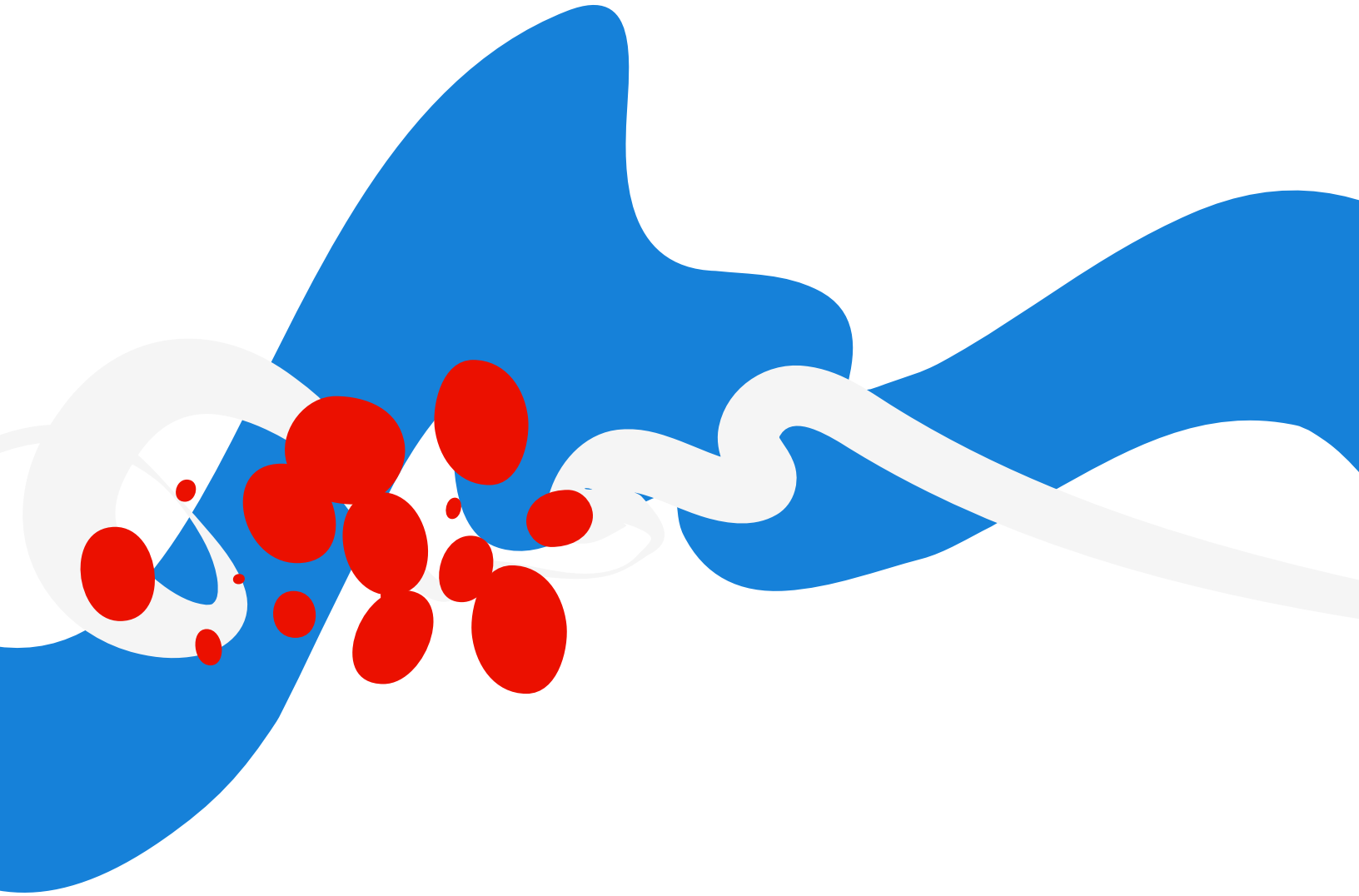
WHITE PAPER

# Adobe Target Security Overview

July 2024



# Table of Contents



# Adobe Security

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

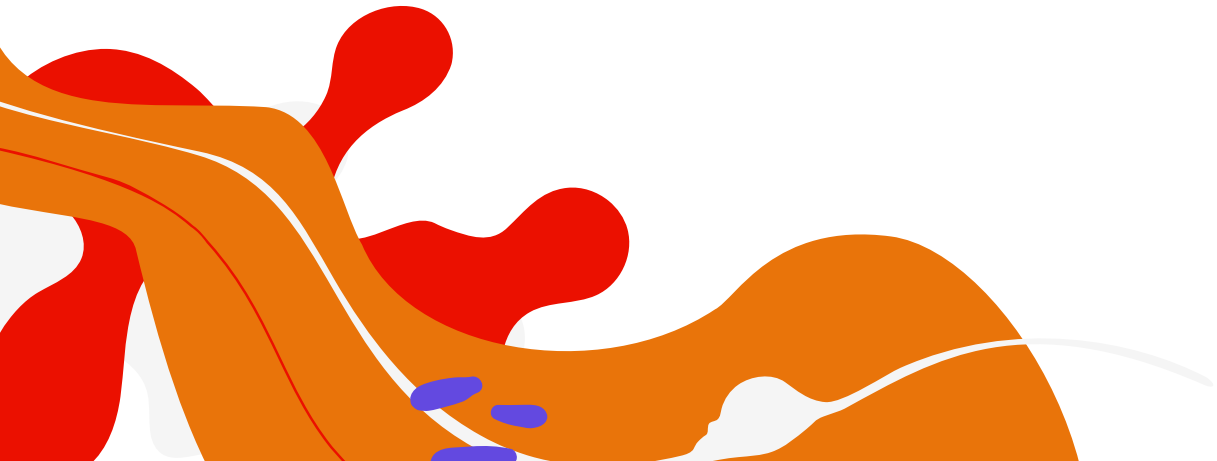
This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to secure the Adobe Target solution and associated data.

# About Adobe Target

Adobe Target enables marketers, developers, and product owners to deliver and optimize highly personalized experiences on any platform through testing and personalization. Using a variety of common testing methods, Adobe Target serves the most appropriate content and offers to audiences based on contextual data such as browsing, search, and product purchase history. An omni-channel solution, Adobe Target improves the visitor experience on any surface or screen customers engage with, including websites, native mobile apps, set-top boxes, kiosks, and more.

There are two versions of Adobe Target, each of which provides a different level of functionality to drive key business goals relating to acquisition, activation, retention, and revenue.

- **Adobe Target Standard** supports A/B testing, Experience Targeting (XT), and Multi-Variate Testing (MVT) capabilities delivering content to specific audiences with Rules-Driven Personalization.
- **Adobe Target Premium** includes all the capabilities of Adobe Target Standard plus advanced machine learning with Automated Personalization and Recommendations powered by Adobe Sensei.



# Solution Architecture

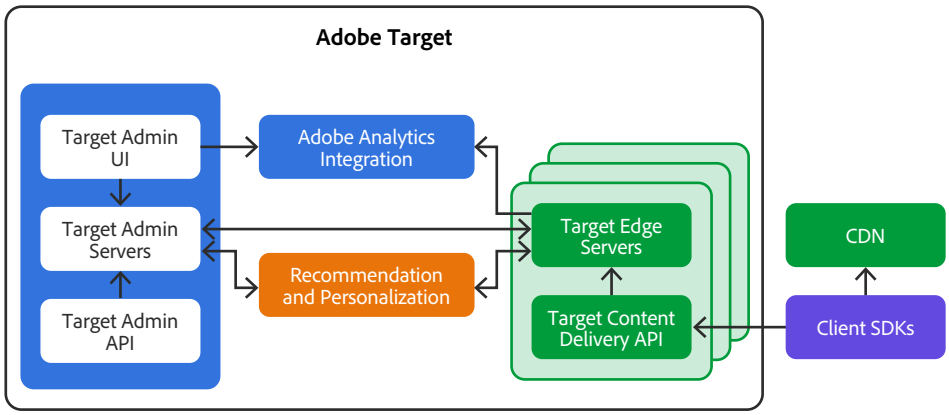



Figure 1: Adobe Target Solution Architecture

The Adobe Target solution includes the following components:

- **Target Admin UI** — Enables customers to define the activities that govern the content delivered to website visitors. This interface is also used by administrators to determine who is authorized to use Adobe Target.
- **Target Admin Servers** — Persistently store all data authored using the Admin UI or Admin API, publish activities to the Edge Servers for delivery, and process user interaction data to generate reports.
- **Target Admin API** — Enables customers to programmatically define activities and access performance reports.
- **Adobe Analytics Integration** — Sends Target user interaction data to Adobe Analytics so that customers can analyze Target activity performance in the context of their other Analytics reports.
- **Target Recommendation and Personalization** — Uses Adobe Sensei AI and machine learning to drive 1:1 personalization at scale, delivering content, product, or media recommendations across any channel with enhanced reporting and enterprise governance capabilities.
- **Target Edge Servers** — Power the Content Delivery API and persistently store user profiles containing website visitor behavior and customer CRM data. Edge servers are redundantly located in data centers around the world, and content delivery requests are served by the nearest Edge cluster to minimize network latency.
- **Target Content Delivery API** — Delivers personalized content to website visitors and other client applications based on defined activities. Collects user interactions that are sent to the Admin Servers for reporting.

- **Content Distribution Network (CDN)** — The Target solution communicates with a leading CDN provider for the distribution of static content and temporary customer-specific decisioning content.
- **Client SDKs** — For client-side content delivery integrations, the customer must embed a JavaScript library on their website, which is responsible for making calls to Target. The library can be self-hosted or deployed on Adobe servers. For server-side content delivery integrations, the customer may use Target's server-side SDKs or call the Target Content Delivery API directly and process the returned content before applying it to webpages, mobile apps or IoT consoles/devices. For mobile app integrations, the customer may use the Adobe Target Mobile SDK Extension. For more information on implementing Target, please see https://experienceleague.adobe.com/docs/target/using/implement-target/implementing-target.html.

# Security Architecture and Data Flow

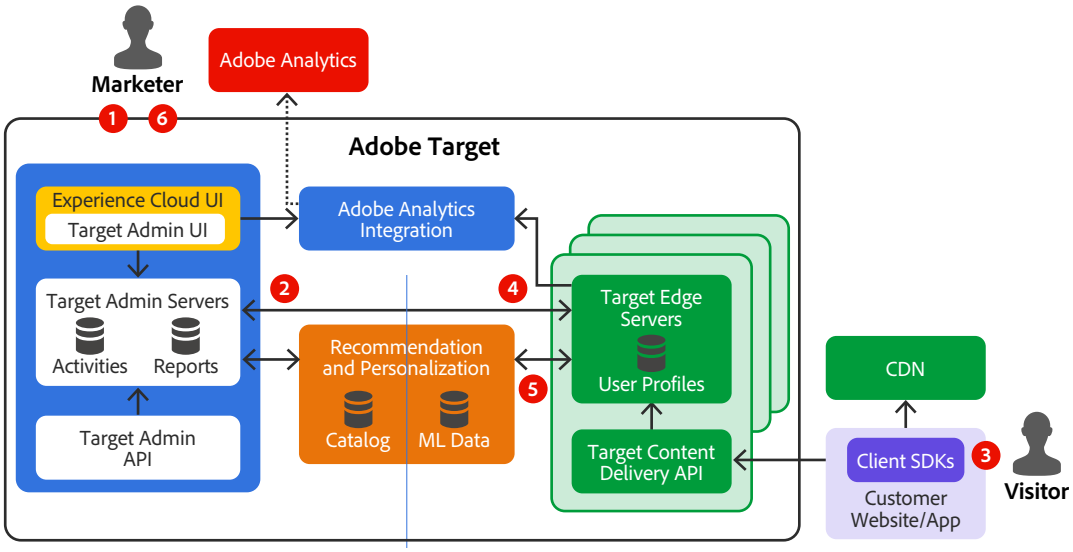



Figure 2: Adobe Target Data Flow Diagram

The following narrative describes how data flows through the Adobe Target solution.

**Step 1: Configuration.** The customer defines the content and parameters for an experiment or personalization activity (e.g., audience segment and traffic allocation) in the Target Admin UI, which communicates the activity information to the Target Admin Server cluster to which the customer has been assigned. The activity information is stored in a MySQL database on the Admin Server cluster.

**Step 2: Distribution.** The new activity is distributed to all Target Edge clusters around the world.

**Step 3: Delivery.** When a visitor loads a page that has been instrumented with the Target JavaScript SDK, a request is sent to the Target Content Delivery API on the nearest edge. The Target Edge Servers load the user profile for the visitor identity in the request, select and deliver a personalized experience based on configured activities, and update the user profile based on the latest interaction. This process occurs in real time. If the customer has decided to implement optional on-device decisioning, the experience selection is performed on the customer's own server, rather than the Target Edge Servers, based on an activity rule file periodically loaded and cached from the Adobe Target CDN.

**Step 4: Collection.** After processing a user interaction, the Target Edge Servers send activity impression and conversion data to the Target Admin Servers for reporting. Aggregate performance reporting data is processed and stored on the Target Admin Servers. The Edge Servers also send activity interaction data to Adobe Analytics if the customer has the Adobe Analytics Integration enabled. Finally, the Edge Servers send interaction data to the Recommendation and Personalization servers for analysis and optimization.

**Step 5: Optimization.** The Recommendation and Personalization servers continuously analyze user interaction data and optimize machine learning models used to determine the most relevant recommendations and experiences to deliver to users for each activity. New, optimized models are periodically distributed back to the Target Edge Servers for use in real-time experience selection.

**Step 6: Reporting.** The customer can access performance reports for an activity to see how many visitors interacted with the activity and whether the activity generated lift. Reports are generated by the Target Admin Servers and displayed in the Target Admin UI. If the customer has the Adobe Analytics Integration enabled, the customer can also analyze the effectiveness of Target activities through the Adobe Analytics user interface.

## Data Encryption

All connections between Adobe Target components are conducted over secure, encrypted connections HTTPS TLS v1.2 or greater.

## User Authentication

Users can access Adobe Target  in one of three (3) different types of user-named licensing:

**Business ID** is an Adobe-hosted, enterprise-managed option for organizations that either use email addresses outside of their own claimed domain as the user's ID or for customers that have not claimed a domain for identity purposes. Adobe Business ID is the preferred option for organizations that work with outside contractors or freelancers who do not have an organizational ID or email.

**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 customer 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 Target 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 SAML2.0-compliant identity provider.

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

More information about Adobe IMS can be found in the Adobe Identity Management Services Security Overview.

## Roles and Permissions

System administrators can add Adobe Target user accounts and manage roles and permissions in the Adobe Admin Console, which set the access for creating and managing activities in Adobe Target.

Administrators can also control access to reporting data. Options include strong passwords, password expiration, IP login restrictions, and email domain restrictions. For more information, please go to https://docs.adobe.com/content/help/en/target/using/administer/administrating-target.html

# Hosting Locations

Adobe Target Edge Clusters are hosted in enterprise-class data centers from public cloud service providers in US-East (Virginia) US-West (Oregon), Europe (Ireland), and Asia Pacific (Singapore, Tokyo, Mumbai, and Sydney). Visitor profile data is stored on the Edge Cluster closest to the site visitor.

The Central Clusters that manage and process site activity are also hosted by public cloud service providers in US-West (Oregon), Europe (Ireland), and Asia Pacific (Singapore).

Components of the Adobe Target Personalization service are located at an Adobe-managed location in US-West (Oregon).


Figure 3: Adobe Target Hosting Locations

# 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