Adobe Experience Cloud

WHITEPAPER

Adobe® Target Security Overview

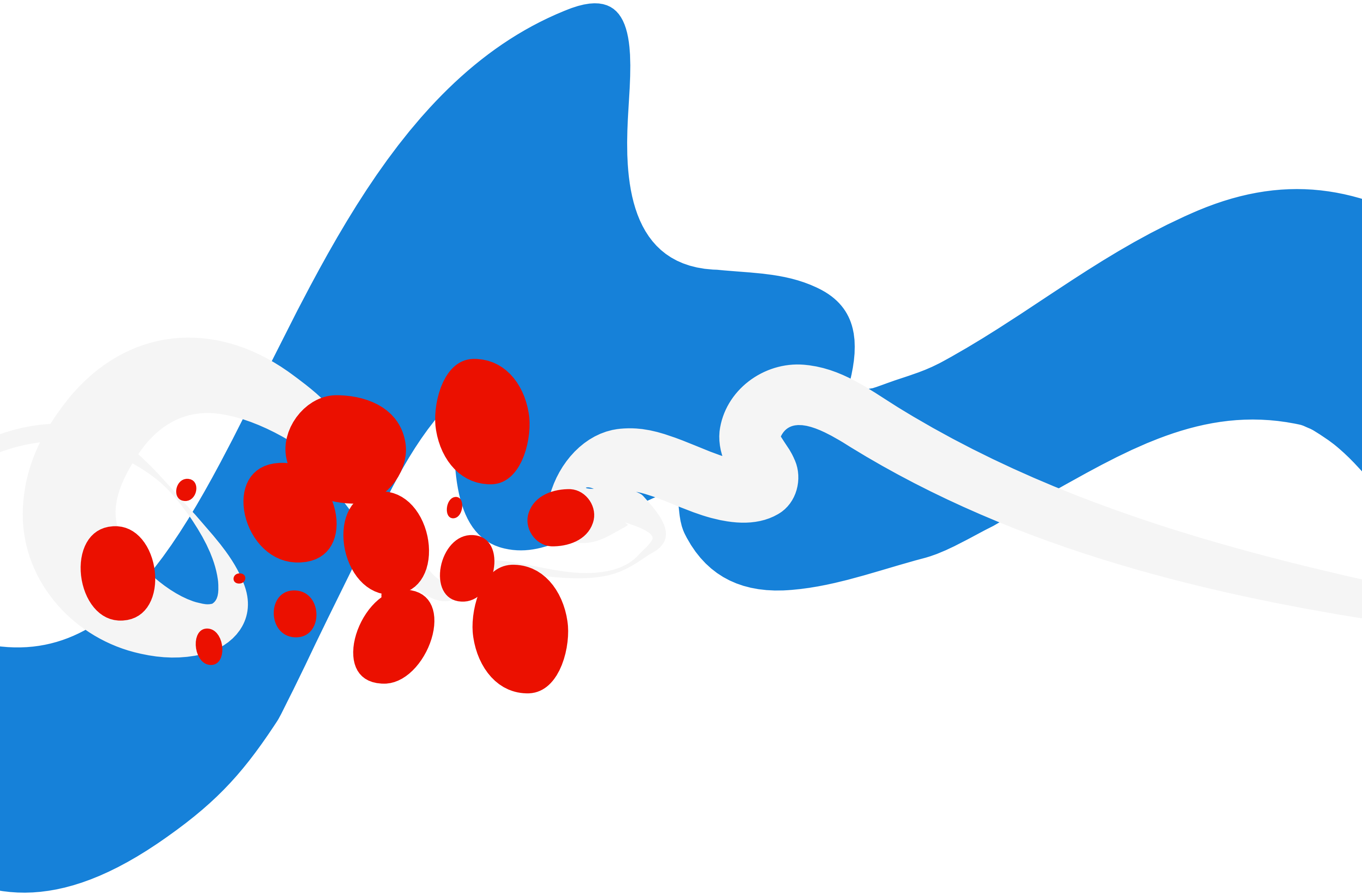


Table of Contents

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.

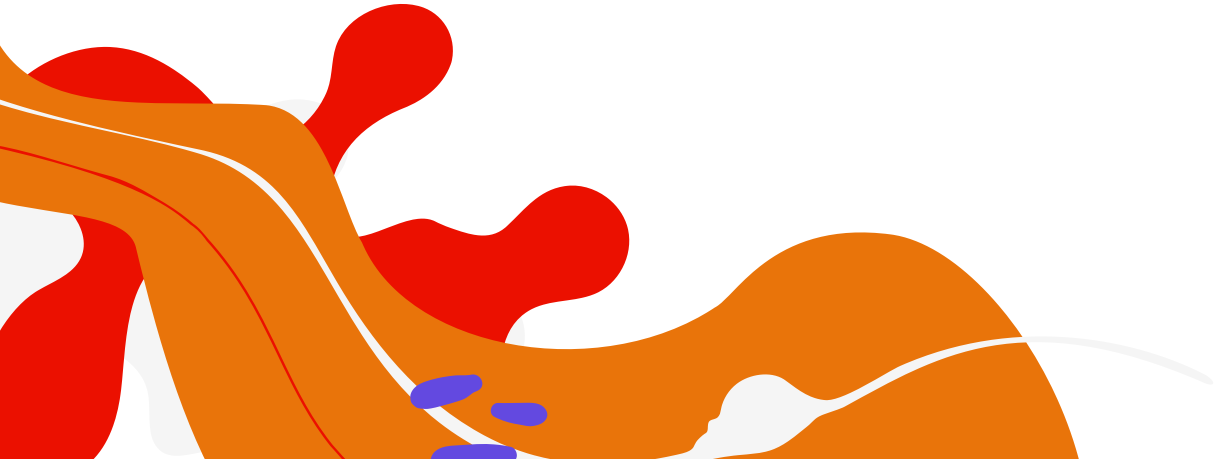
This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to secure your Adobe Target experience and associated data.

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.



Adobe Target Solution Architecture

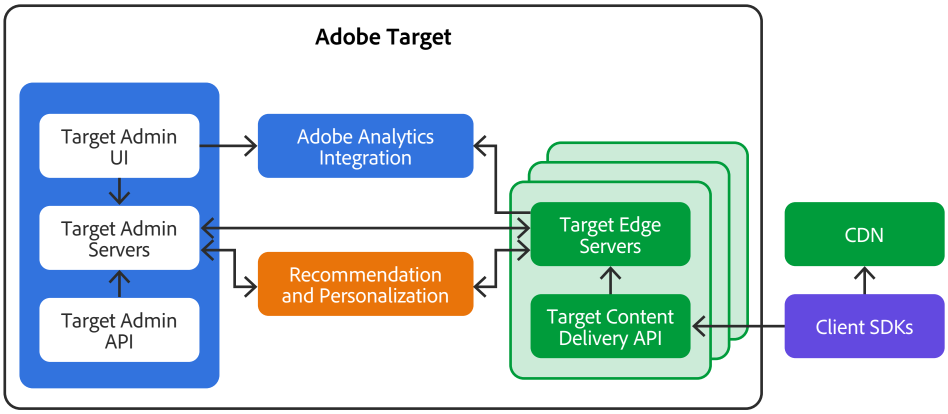


Figure 1: Adobe Target Solution Architecture

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 Adobe Target user interaction data to Adobe Analytics so that customers can analyze Adobe 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 Target 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.

- **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 Adobe Target. The library can be self-hosted or deployed on Adobe servers. For server-side content delivery integrations, the customer may use Adobe Target's server-side SDKs or call the Adobe 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 the Implementing Target Overview.
- **Content Distribution Network (CDN)** — The Adobe Target solution communicates with a leading CDN provider for the distribution of static content and temporary customer-specific decisioning content.

Adobe Target Security Architecture and Data Flow

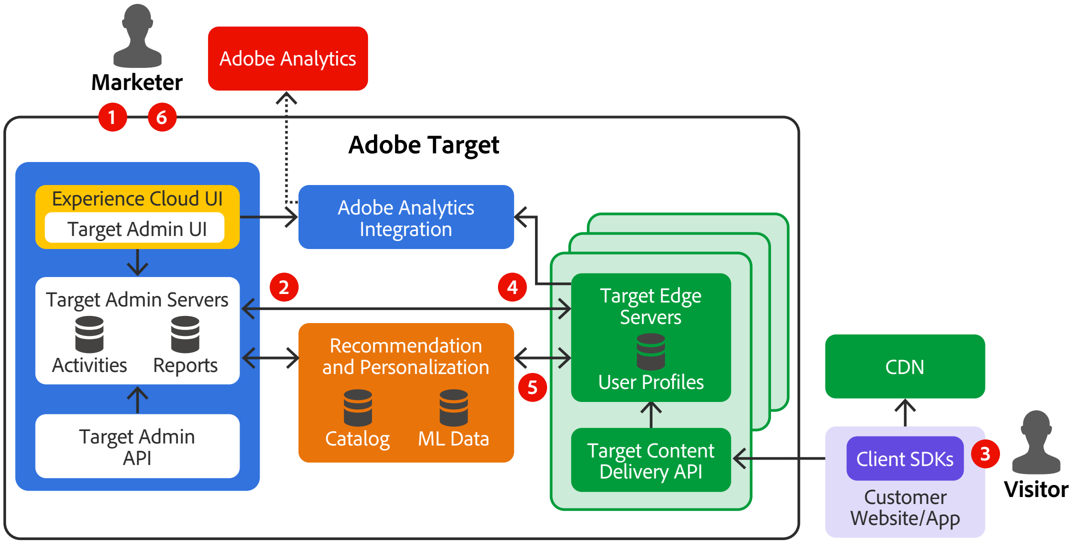


Figure 2: Adobe Target Data Flow Diagram

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 from the visitor's browser 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 back to the Target JavaScript SDK in the browser 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

Access to Adobe Target requires authentication with username and password. Users can access Adobe Target in one of three (3) different types of user-named licensing: Adobe ID, Enterprise ID, or Federated ID. You can find more information about Adobe Identity Management Services in the Adobe Identity Management Services security overview.

Roles and Permissions

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

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 the Administering Target Overview.

Adobe Target Hosting and Security

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).

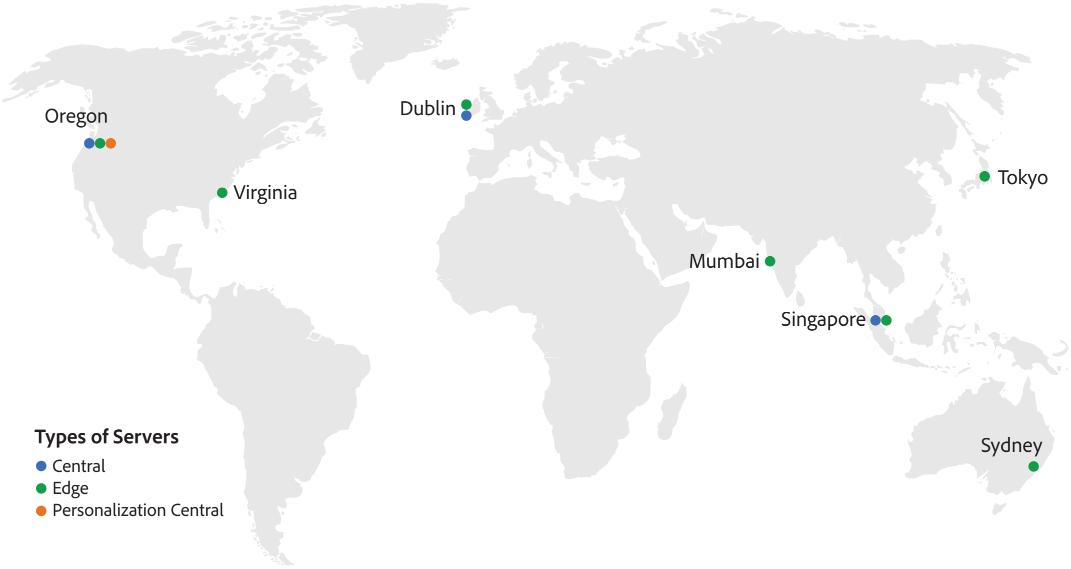


Figure 3: Adobe Target Hosting Locations

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.

Application Security
Operational Security
Enterprise Security
Compliance
Incident Response

Figure 4: 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; and
- **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.

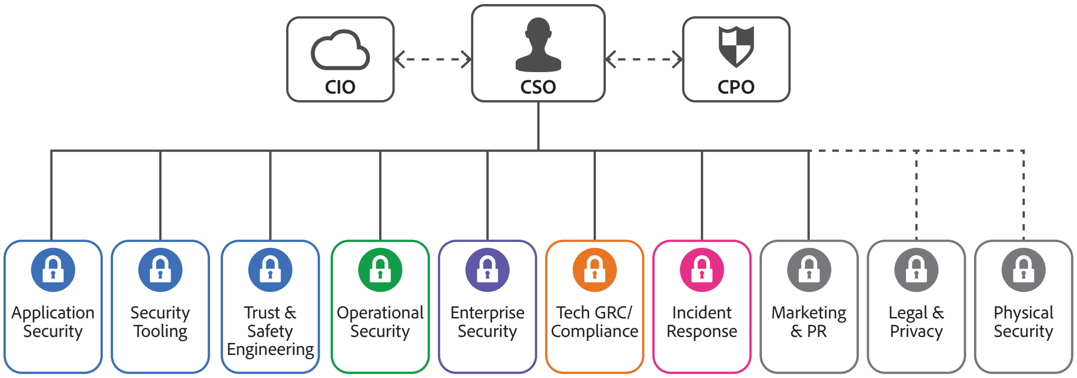
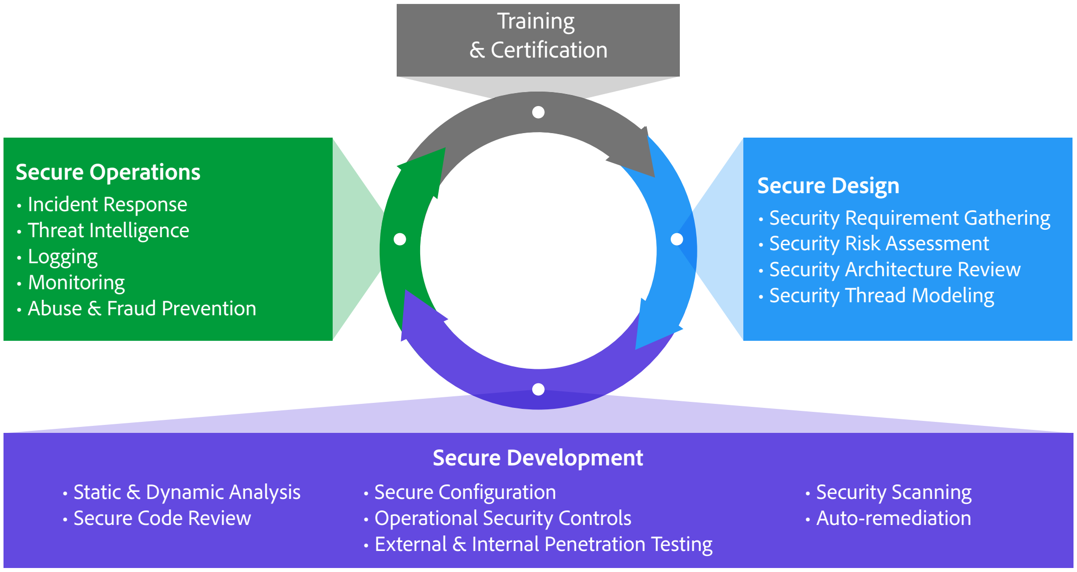


Figure 5: The Adobe Security Organization

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.



Training & Certification

Secure Operations

- Incident Response
- Threat Intelligence
- Logging
- Monitoring
- Abuse & Fraud Prevention

Secure Design

- Security Requirement Gathering
- Security Risk Assessment
- Security Architecture Review
- Security Thread Modeling

Secure Development

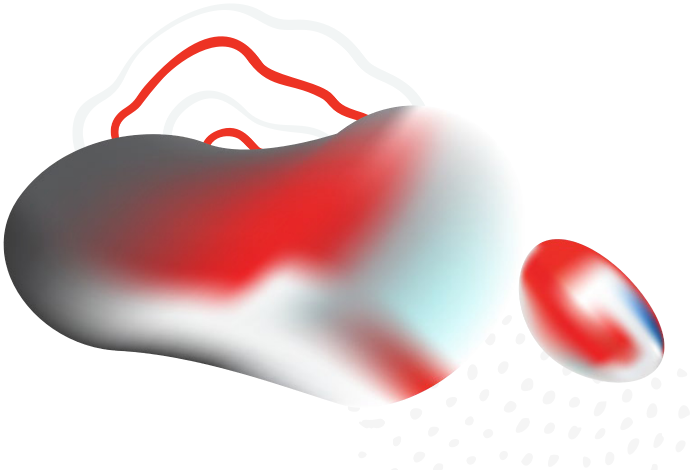
- Static & Dynamic Analysis
- Secure Code Review
- Secure Configuration
- Operational Security Controls
- External & Internal Penetration Testing
- Security Scanning
- Auto-remediation

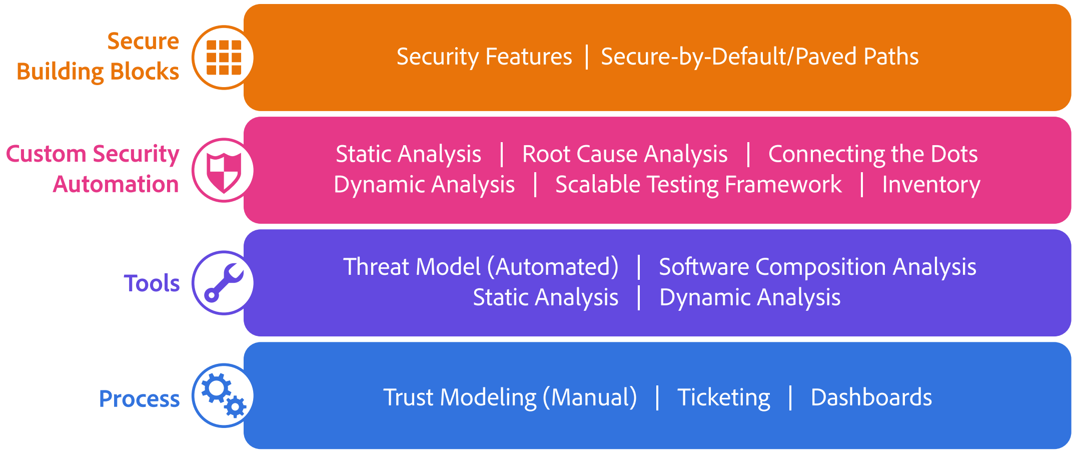
Figure 6: The Adobe Secure Product Lifecycle

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.





Secure Building Blocks: Security Features | Secure-by-Default/Paved Paths

Custom Security Automation: Static Analysis | Root Cause Analysis | Connecting the Dots | Dynamic Analysis | Scalable Testing Framework | Inventory

Tools: Threat Model (Automated) | Software Composition Analysis | Static Analysis | Dynamic Analysis

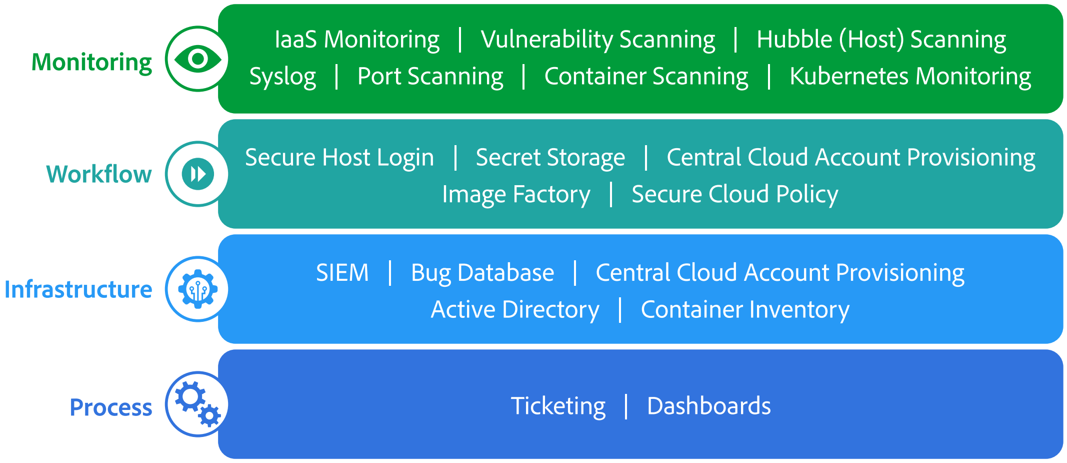
Process: Trust Modeling (Manual) | Ticketing | Dashboards

Figure 7: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of Amazon Web Services (AWS) and Microsoft Azure 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.



Monitoring: IaaS Monitoring | Vulnerability Scanning | Hubble (Host) Scanning | Syslog | Port Scanning | Container Scanning | Kubernetes Monitoring

Workflow: Secure Host Login | Secret Storage | Central Cloud Account Provisioning | Image Factory | Secure Cloud Policy

Infrastructure: SIEM | Bug Database | Central Cloud Account Provisioning | Active Directory | Container Inventory

Process: Ticketing | Dashboards

Figure 8: 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 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 on the Adobe BCDR Program can be found here.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Target 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 of 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.

Adobe