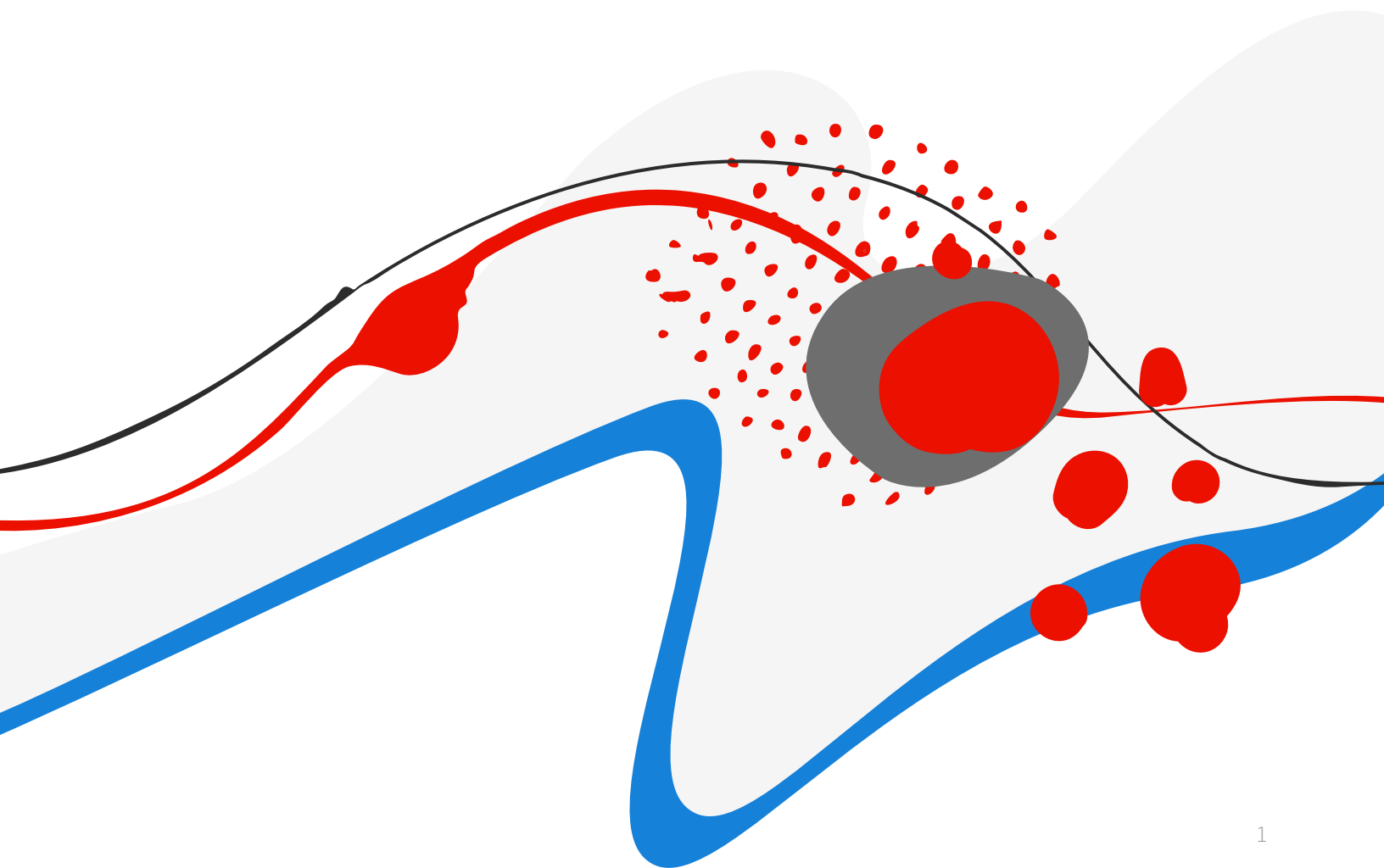


WHITE PAPER

# Adobe Experience Platform Security Overview



# Table of Contents

<b>Adobe Security</b>	<b>3</b>
<b>About Adobe Experience Platform</b>	<b>3</b>
<b>Adobe Experience Platform Architecture</b>	<b>3</b>
<b>Experience Platform Security Architecture and Data Flow</b>	<b>5</b>
Data Encryption	6
User Authentication	6
<b>Data Governance in Experience Platform</b>	<b>7</b>
<b>Adobe Experience Platform Hosting and Security</b>	<b>8</b>
<b>Adobe Security Program Overview</b>	<b>9</b>
The Adobe Security Organization	10
The Adobe Secure Product Lifecycle	11
Adobe Application Security	13
Adobe Operational Security	14
Adobe Enterprise Security	14
Adobe Compliance	14
Incident Response	15
Business Continuity and Disaster Recovery	15
<b>Conclusion</b>	<b>16</b>

# 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.<sup>1</sup>

<sup>1</sup> 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.

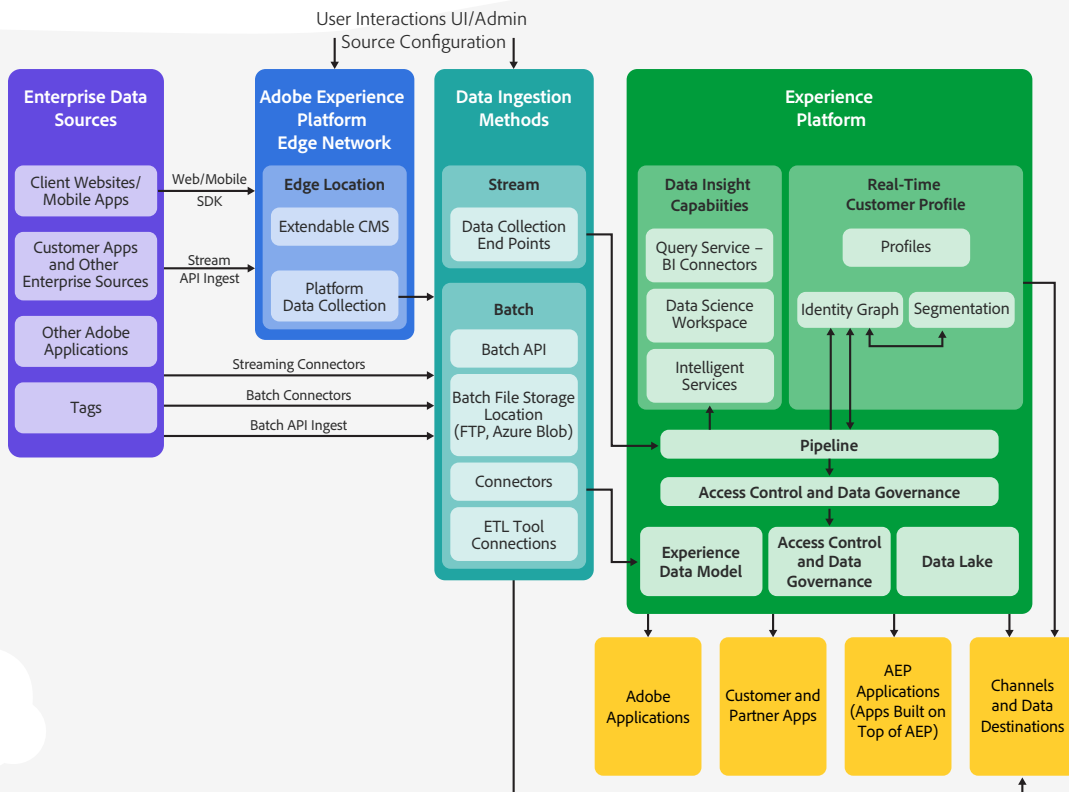


Figure 1: Adobe Experience Platform solution architecture

# 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 strictly 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 see 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. Experience Platform supports [four \(4\) different types of user-named licensing](#). More 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 and categorizing 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](#).

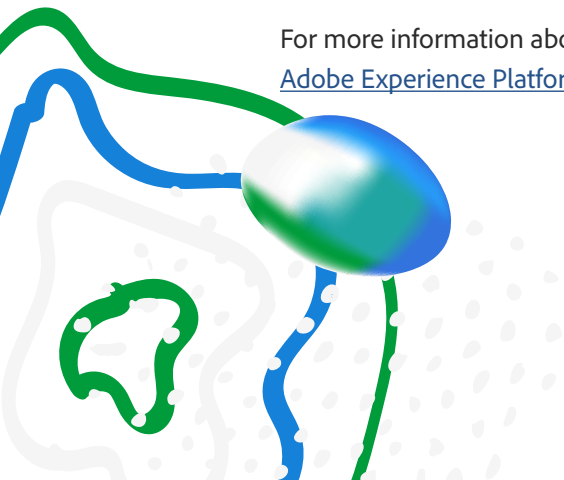
For more information on the "core" data usage labels available in Experience Platform out of the box and the governance policies they represent, please see the guide on [core data usage labels](#).

## 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 U.S. East (Virginia), EMEA (The Netherlands), and APAC (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 Platform 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 the intent to migrate the services to the disaster recovery site
- Hourly progress updates during the service migration
- Notification of completion of the migration to the disaster recovery site

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.

# 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; 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.

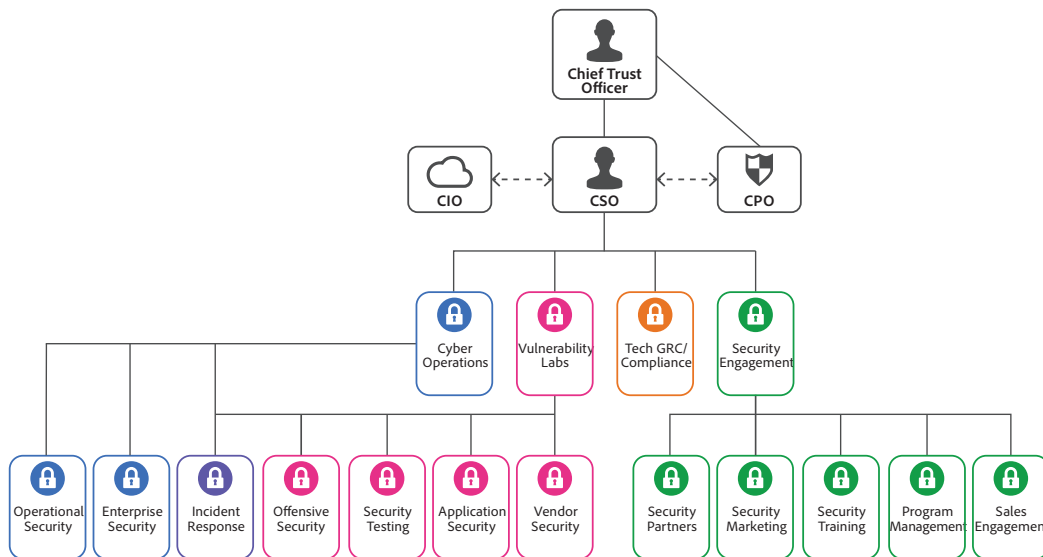


Figure 4: The Adobe Security Organization

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.

Adobe's culture of security and training programs are outlined in more detail in 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.

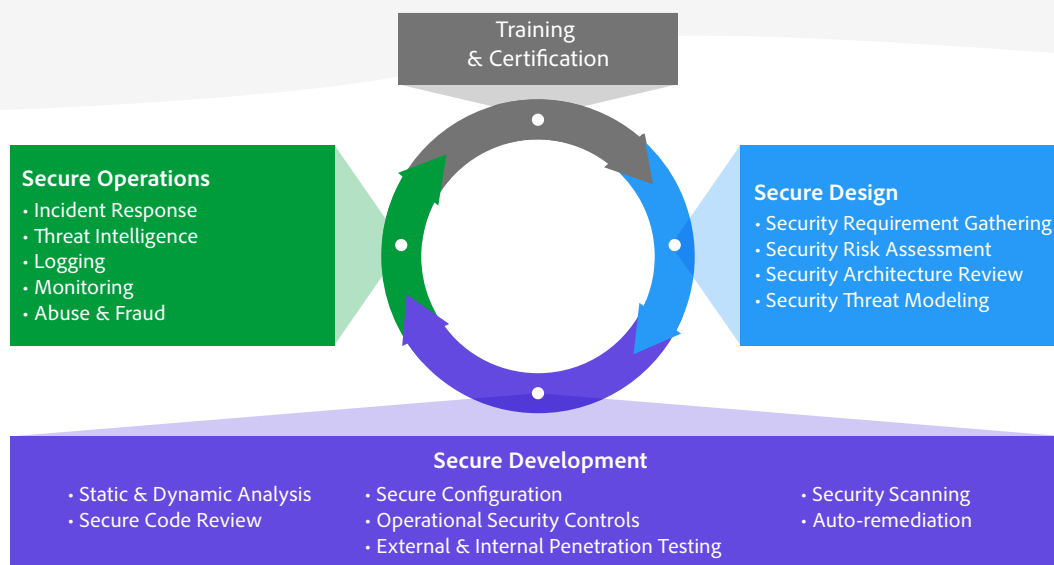


Figure 5: The Adobe Secure Product Lifecycle

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.

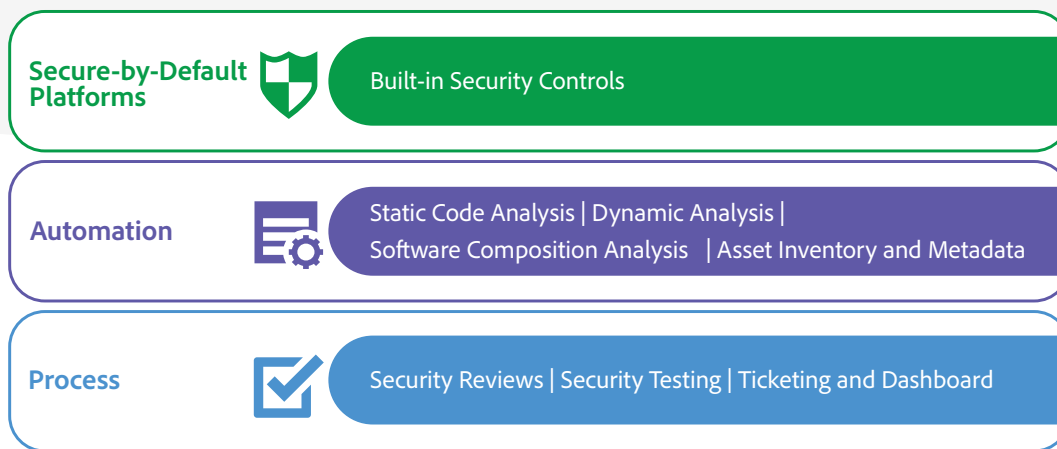


Figure 6: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of Amazon Web Services (AWS) and Microsoft Azure public cloud infrastructure. These standards are available for view upon request. The [Adobe Application Security Overview](#) contains more detailed information about Adobe's application security practices and processes.

# 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.

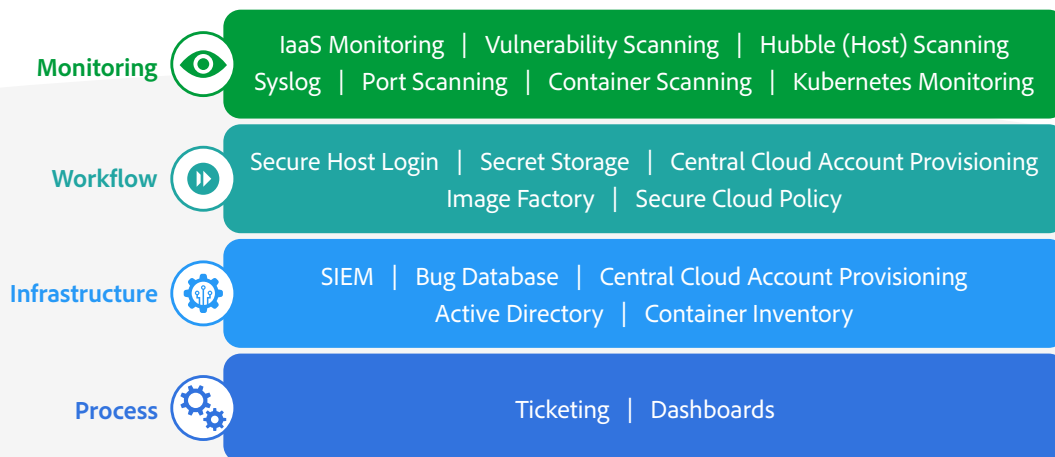


Figure 7: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. A detailed description of the Adobe OSS and the specific tools used throughout Adobe can be found in 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.

More information on our enterprise security controls and standards we have developed for these controls can be found in 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. More information on the Adobe CCF and key certifications can be found in the [Adobe Compliance Certifications, Standards, and Regulations 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. More details about Adobe's incident response and notification process are documented in the [Adobe Incident Response Program 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 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 Platform and your confidential data. At Adobe, we take the security of your digital experience 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 on Adobe security, please see the [Adobe Trust Center](#).





© 2023 Adobe. All rights reserved.

Adobe, Experience Cloud, the Experience Platform logo, and the Adobe logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.