WHITE PAPER

Adobe® Experience Platform Security Overview

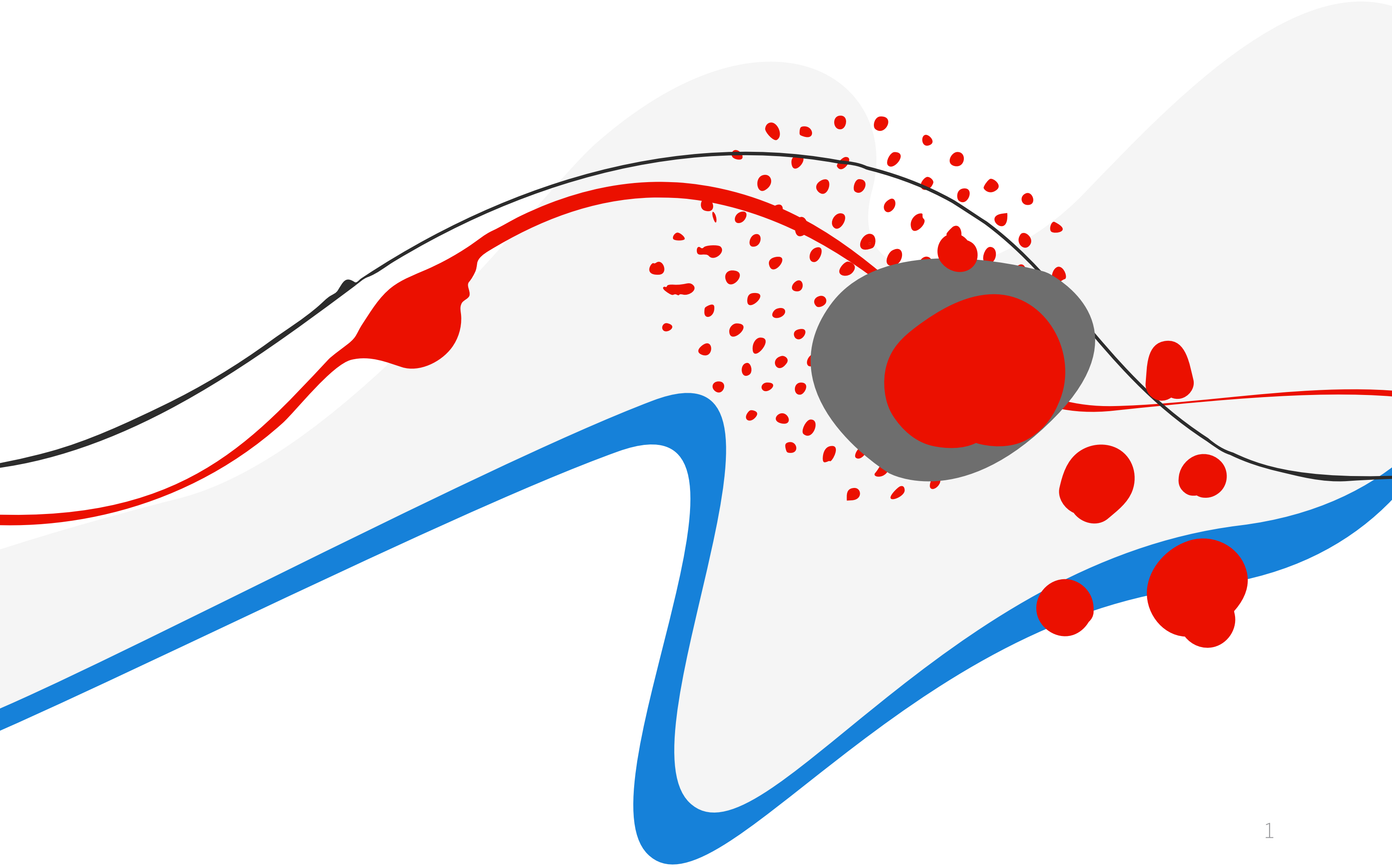


Table of Contents

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. These practices are strictly followed by our cross-functional teams 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. We 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 Adobe Experience Platform and its associated data.

About Adobe Experience Platform

Adobe Experience Platform is an open and extensible system designed to help brands build customer trust while delivering better 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 the 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, 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 ingests data from a variety of sources in order to help brands better understand the behavior of their customers. Typical sources include enterprise data sources, including the Experience Platform customer's own web and mobile applications, CRM and 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:

- Adobe Customer Journey Analytics (CJA), Adobe Journey Optimizer (AJO), and Real-time Customer Data Platform (RT CDP), which are applications built on top of Experience Platform
- Adobe Intelligent Services, including Customer AI, Attribution AI, and Content and Commerce AI, that 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
- Customer and partner applications

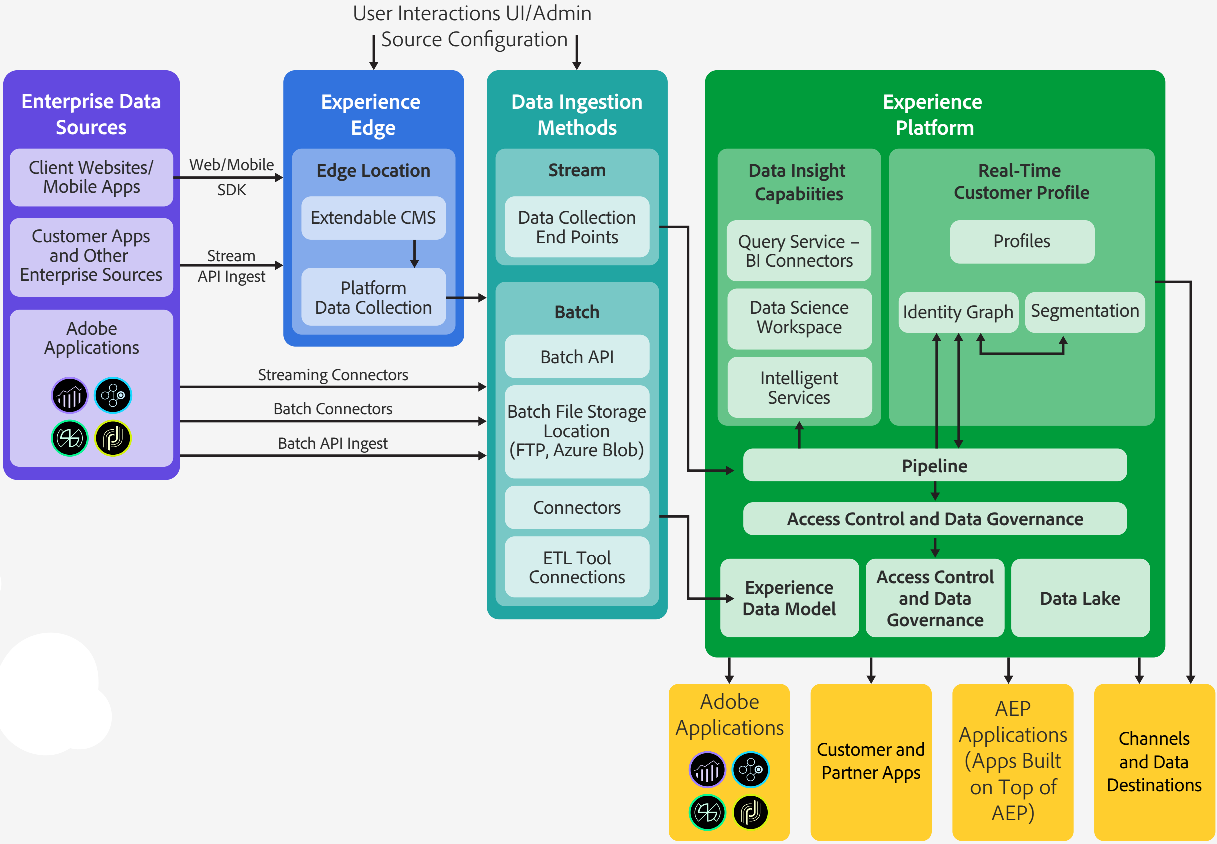


Figure 1: Adobe Experience Platform solution architecture

Experience Platform Security Architecture and Data Flow

Adobe Experience Platform ingests and exports 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.
- 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 batch data (i.e., data collected over time) using built-in connectors.
    - Credentials are stored in the public cloud provider’s key vault.
    - If the cloud data store supports HTTPS or TLS, all data transfers between data movement between AEP services and the cloud data store are conducted via secure channel HTTPS or TLS (1.2).
- 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 consumption. The ETL tools and the corresponding data flows reside in the customer environment.

User Interactions and Admin Source Configurations

- A customer’s administrators and users with appropriate access permissions can authenticate to the Experience Platform UI and configure various options for data source collection. These individuals provide credentials to connect to enterprise data sources, which are persisted in the cloud service provider’s key vaults after encrypting sensitive data. The credentials are used on the user’s behalf to create and modify data flows during design time and ingest data at run time.

Access Control and Data Governance

- All access to the Experience Platform data lake, whether to write new data or read existing data, is strictly controlled using the Experience Platform access control and data governance layer.

Data Lake

- Data is written to the appropriate location in the Experience Platform data lake for the specific customer, based on the Experience Platform data model and the configuration settings in the admin UI.

Pipeline

- Batch data is available by request for analysis or processing by the Experience Platform data insight and real-time customer profile services.
- Streaming data is available for immediate analysis by the Experience Platform data insight and real-time customer profile services.

Data Destinations

- Results of analysis and processing as well as specific data sets are made available to authenticated Adobe applications, customer and partner applications, and native Experience Platform applications, such as Adobe Customer Journey Analytics and Adobe Journey Optimizer.
- Results can also be funneled to customer-specific channels and data destinations, such as S3 buckets or social media feeds.

Data Encryption

All data in transit between Experience Platform and any external component is conducted over secure, encrypted connections using HTTPS TLS v1.2. All data at-rest is encrypted by the cloud service provider. All customer data at-rest is isolated in single-tenant cloud instances.

User Authentication for Adobe Experience Platform

Access to Adobe Experience Platform requires authentication with username and password. We continually work with our development teams to implement new protections based on evolving authentication standards.

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

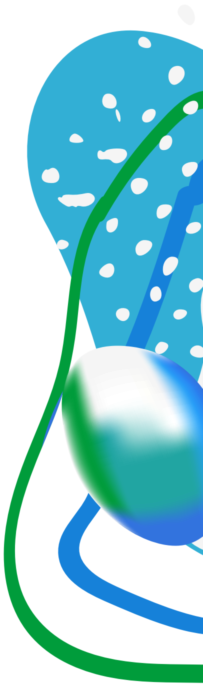
Adobe ID is for Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users.

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 Experience Platform 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 the customers' IT infrastructure.

Adobe integrates with most SAML2.0 compliant identity providers. Adobe IDs and Enterprise IDs both 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's identity management services can be found 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.

Using the access control feature, 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.

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), Amsterdam (NL), and Sydney (AU). Upon provisioning, customers can designate the regional data center(s) where the data ingested into Experience Platform will be sent for storage.

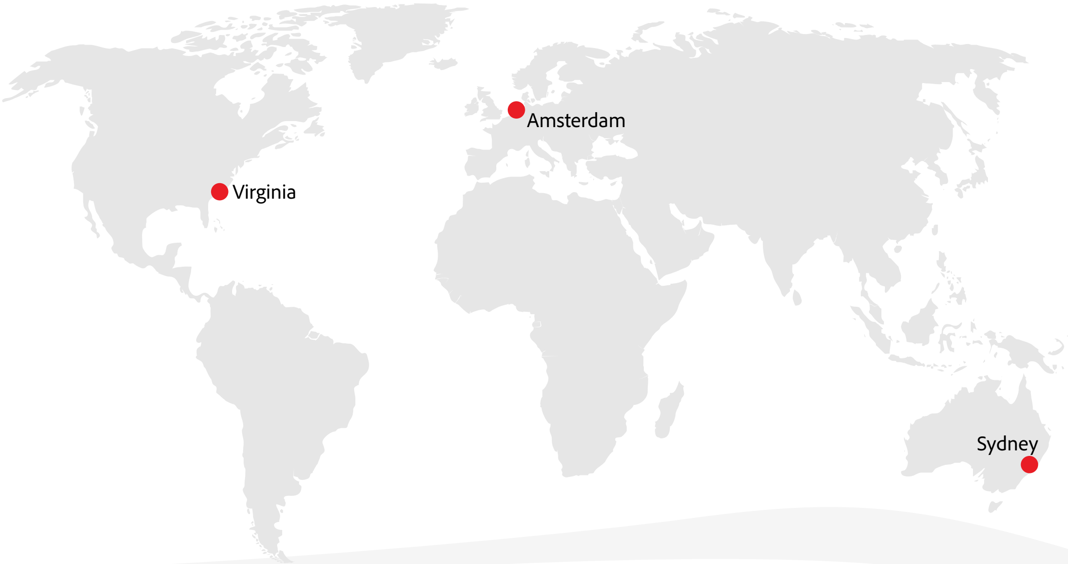


Figure 2: Adobe Experience Platform Data Center Locations

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.

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.

Product Security
Operational Security
Enterprise Security
Compliance
Incident Response

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.

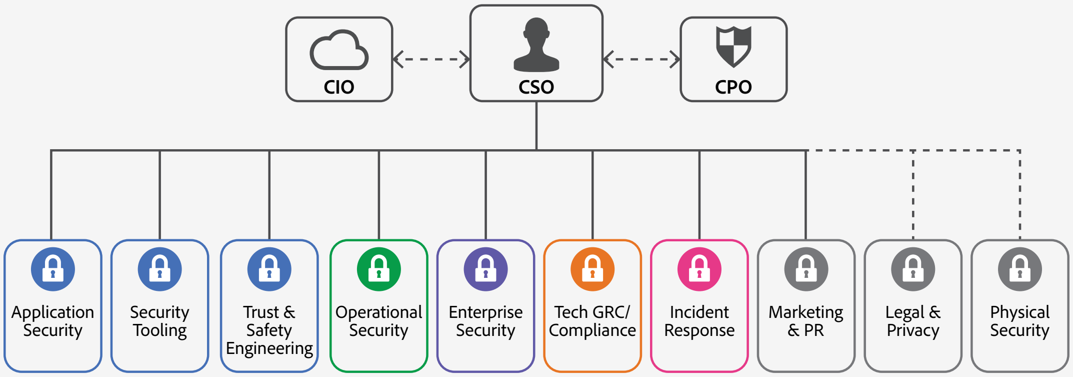


Figure 4: The Adobe Security Organization

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. 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.

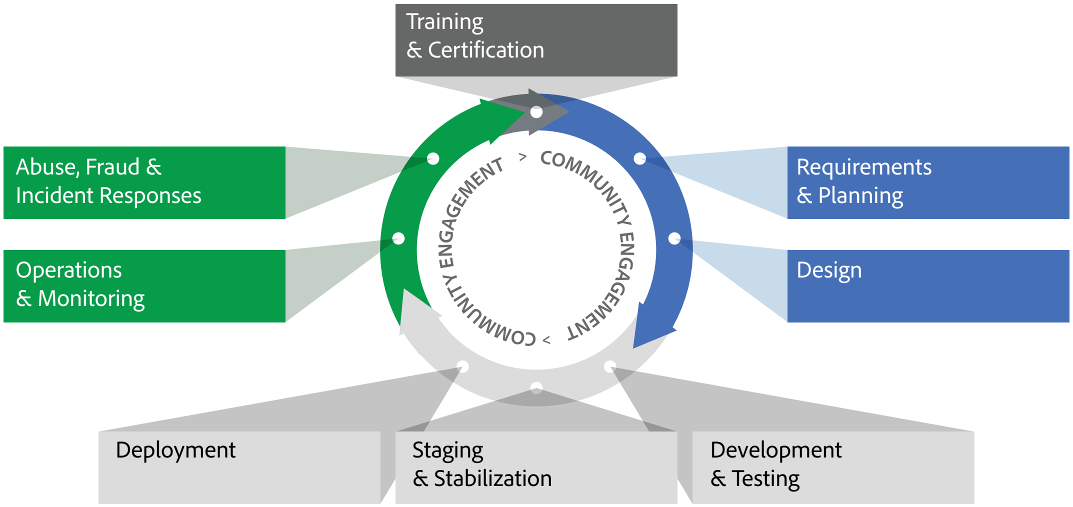
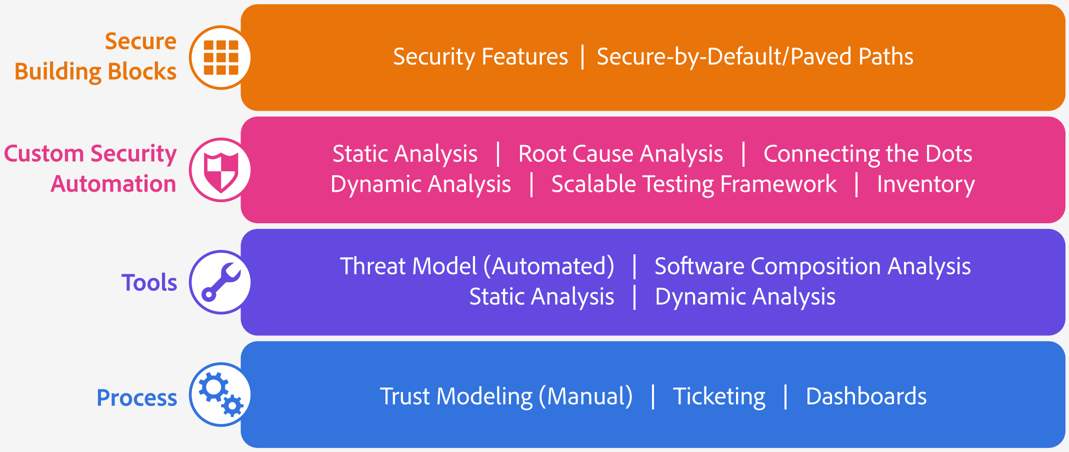


Figure 5: The Adobe Secure Product Lifecycle

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.



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 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.
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.

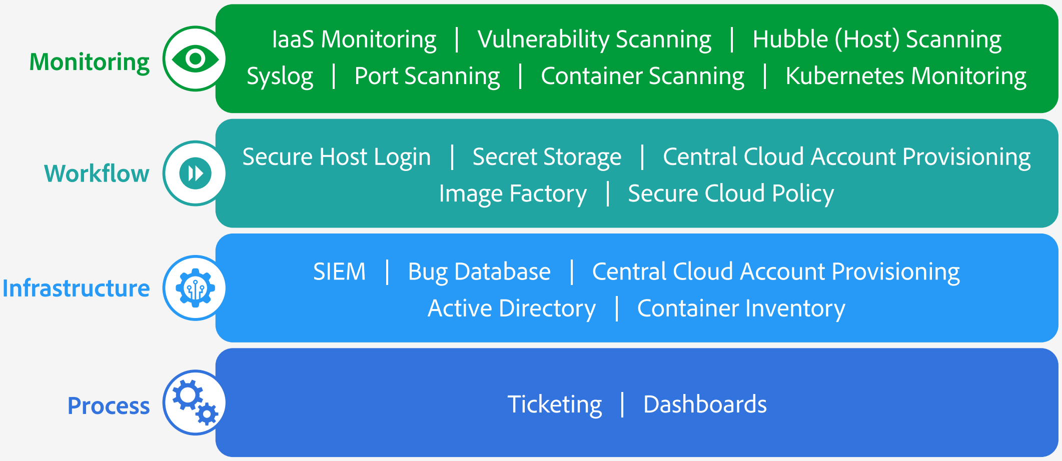

Monitoring
IaaS Monitoring | Vulnerability Scanning | Hubble (Host) Scanning
Syslog | Port Scanning | Container Scanning | Kubernetes Monitoring
Workflow
Secure Host Login | Secret Storage | Central Cloud Account Provisioning
Image Factory | Secure Cloud Policy
Infrastructure
SIEM | Bug Database | Central Cloud Account Provisioning
Active Directory | Container Inventory
Process
Ticketing | Dashboards

Figure 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.

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 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 on:
Adobe security: www.adobe.com/security

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

Adobe
345 Park Avenue
San Jose, CA 95110-2704
USA www.adobe.com