Security in Adobe Experience Platform

Contents

At Adobe, we take the security of your digital experiences very seriously. Security practices are deeply ingrained in our internal software development and operations processes and tools. They are rigorously followed by our cross-functional teams to prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities. We regularly incorporate advanced security techniques into the products and services we offer.

This paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of Adobe Experience Platform and your data.

ABOUT ADOBE EXPERIENCE PLATFORM

Today's digital landscape is teeming with people interacting across many devices—mobile phones, tablets, internet-enabled televisions, car dashboards, and countless other touchpoints. Consumers have higher expectations for their content and data than ever before—they want personalized and relevant experiences delivered to them in real time. These developments are exciting, but they also present enormous challenges to businesses that need to reach the right people with the right content at the right time, faster than ever. Massive amounts of data, a plethora of devices and screens, and skyrocketing customer expectations are forcing businesses to completely rethink their approach to interacting with their customers.

At the center of this challenge is the need to create a customer profile that represents everything you know about your customer -including behavioral data, CRM data, product usage, and commerce data. Experience Platform enriches that data with insights derived from past interactions and is available in real time to drive relevant and personalized experiences across any channel.

Experience Platform is the technology behind Adobe Experience Cloud that helps centralize and standardize all customer data, enabling enterprises to create and activate real-time customer profiles to deliver more personalized customer experiences in milliseconds. By bringing together all attribute and behavioral data—including data from the web, mobile devices, IoT , and systems of record like point-of-sale and CRM systems—into one place, Platform enables you to work with a vast array of experience data in real time and helps you deeply understand your customers and deliver the right experiences to them.

Experience Platform is open and extensible. Through its APIs, Platform's capabilities and services can interoperate with your entire tech stack, including enterprise data lakes. Using these APIs, Adobe customers, partners, and developers can extend and embed Adobe product functionality to build completely new customer experience applications.

Experience Platform is powered by open source standards and state-of-the-art frameworks and technologies, including the Java Content Repository (JCR) API and a solid and structured representational state transfer (REST) architecture through Adobe I/O.

Experience Platform allows enterprises to:

- Create actionable, intelligent, real-time customer profiles
- Enrich data and derive more insights with data queries and artificial intelligence (AI) and machine learning (ML) models
- Enhance the delivery and personalization of multichannel, real-time experiences
- Gain trust with governance, security, and privacy controls
- Innovate with open and composable components

HOW IT WORKS

Experience Platform provides services for preparing and delivering data to various systems for building real-time personalized digital experiences. These services leverage a combination of distributed data stores and file systems, powered by Open Source and state-of-the-art frameworks and technologies, an extensible set of REST APIs—including the Dataset API, Ingestion API, Infrastructure API, and Compute API—and a robust Data Access SDK for interacting with the data itself.

Experience Platform is built on the following concepts:

Data

Data is at the core of Experience Platform. Data that is collected through Adobe's: Analytics Cloud, Experience Cloud, and Advertising Cloud flows into the platform. Experience Platform Launch, is the next-generation tag management system and client-side platform that makes it easy to integrate Adobe and partner tools into your experiences to capture data. Experience Platform also provides a set of built-in connectors, streaming and batch APIs, and a rich ecosystem of data integration tools like Informatica, SnapLogic, and Unifi to ingest additional customer data from CRM, commerce, loyalty, voice of customer, offline purchases, and data sources across the enterprise to provide a complete view of your customer.

Customers that choose to tap into data from other Adobe solutions or ingest their data into the platform will take advantage of our data lake, powered by Microsoft Azure. Azure provides encryption at rest by default. The data lake provides a combination of various types of data stores of customer experience data. Using data stored in the data lake, businesses can query, configure, and manage their data at the speed of business.

Data governance

Experience Platform is organized into a common set of schemas known as Experience Data Model (XDM). XDM provides open, standardized, extensible schemas to represent all experience data, enabling an immediate semantic understanding of cross-channel data and fostering an ecosystem of prebuilt insights and services. XDM is a formal standard, published in JSON Schema, that allows data interoperability in Experience Platform. A schema registry and schema design tool let you manage and extend XDM to fit your needs.

Experience Platform also helps to govern and control how data is used. Data in today's world is subject to government regulations, contractual restrictions, and your internal policies which may limit data usage. These regulations often come with penalties or adverse consequences for noncompliance. The business value you can derive from your data is controlled by your ability to know what data you have and where it came from; catalog and categorize it; and manage the myriad of regulatory, contractual, and policy limitations on its use. Experience Platform was built with these considerations in mind. It provides a robust, powerful data governance framework that you can use to manage compliance with regulations such as GDPR, restrictions, and policies controlling the use of your data. With Experience Platform, you can catalog and categorize your data and define policies for how different categories of data can be used.

Queries, ML, and AI integrations

Experience Platform Data Science Workspace, powered by Adobe Sensei, helps brands enrich customer profiles by making predictions using AI and ML on their data assets.

Built on a common machine learning framework and runtime, Data Science Workspace delivers advanced workflow management, model management, and scalability. It gives data scientists of all skills levels the flexibility to create their own custom models, bring in their own models, or use prebuilt Adobe models and seamlessly train and deploy them with Adobe product data or any other data they want to use.

Without Experience Platform, it can typically take days to weeks to get data into a data lake, standardize the data, perform the modeling, and then pipe back the results to systems of engagement for influencing the customer experience. But because all customer data is already ingested into and standardized on Experience Platform, data scientists will be able to light up models without any extra data preparation required, shortening time to value.

In addition, with Experience Platform Query Service, data analysts have an easy-to-use SQL query tool built on top of XDM on our data lake to enable ad hoc omnichannel, multiplatform, serverless, petabyte-scale queries for filtered, aggregated, and jointed data sets. Query Service enables deeper insights in less time by eliminating the need to take the data out of Adobe products. You can natively use your favorite business intelligence (BI) tools, such as Tableau or Power BI, to visualize queries and bring added granular inspection and validation of the data and to enrich customer profiles.

Profile management

To provide personalized experience, an enterprise needs real-time access to a complete view of the customer. This holistic view is provided by the Profile Service. The Profile Service can ingest data from various enterprise repositories including first-party data as well any third-party data. This data may consist of CRM data; e-commerce transactions; offline transactions; loyalty program data; behavioral data from mobile, the web, or emails; social interaction data; and so on.

Data from multiple data sources is stitched together to provide a unified view of the customer. Each data source has its own notion of the identity of a customer. These identities are matched against each other. For first-party data, this requires de-duplication, data merge, and survivorship rules. For online behavioral data, identities are often based on cookies and require cookie-matching techniques. Mobile and IoT have their own notion of identities based on device. The Identity Service uses deterministic and probabilistic algorithms to match identities and model these relationships as a graph.

DATA FLOW NARRATIVE

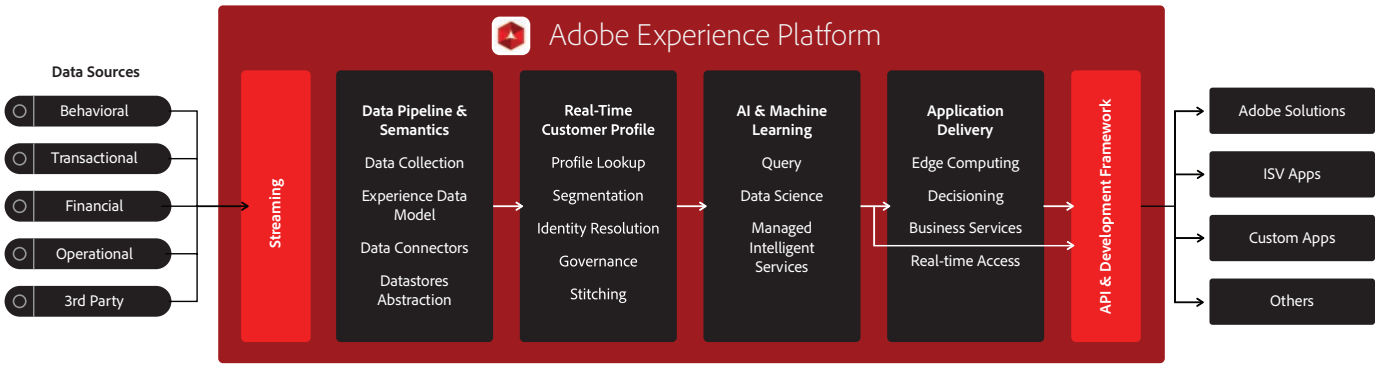
Experience Platform is a single, persistent, reliable repository of customer experience data. It provides an easily-accessible, current, fast, and complete data store that systems of activation can use to access, query, configure, and manage data. Experience Platform offers multiple types of databases (such as our data lake, NoSQL, Graph) to store data in different formats and support multiple data access patterns (real time, near real time, batch), depending on the use case. You don't need to build multiple databases—they already exist.

Experience Platform allows structured, semi-structured, and unstructured data to be onboarded from virtually any source in a variety of manners including streaming, Bulk Ingestion API, native third-party connectivity, Experience Platform Mobile SDK, and Experience Platform Launch. Experience Platform validates all data before it's ingested to help ensure onboarded data can be queried by the attributes and constraints specified in its related XDM Schema. During data ingestion, information about datasets, schemas, sample data, lineage, and metrics is cataloged in Adobe's catalog.

Brands using Experience Cloud products have the benefit of automatically ingesting their data into Experience Platform and making it available for use in real time. Thanks to XDM, brands can easily combine data from Adobe and non-Adobe customer data.

Once the data is standardized, ingested, and stored in Experience Platform, you can create and activate real-time customer profiles in virtually any channel via APIs. You can enrich customer profiles using Experience Platform services like Data Science Workspace and Query Service. In

addition, a powerful data catalog in Experience Platform manages the metadata of all data stored in the platform, allowing data discovery and data governance. Data stored in our data lake is encrypted at rest for security.

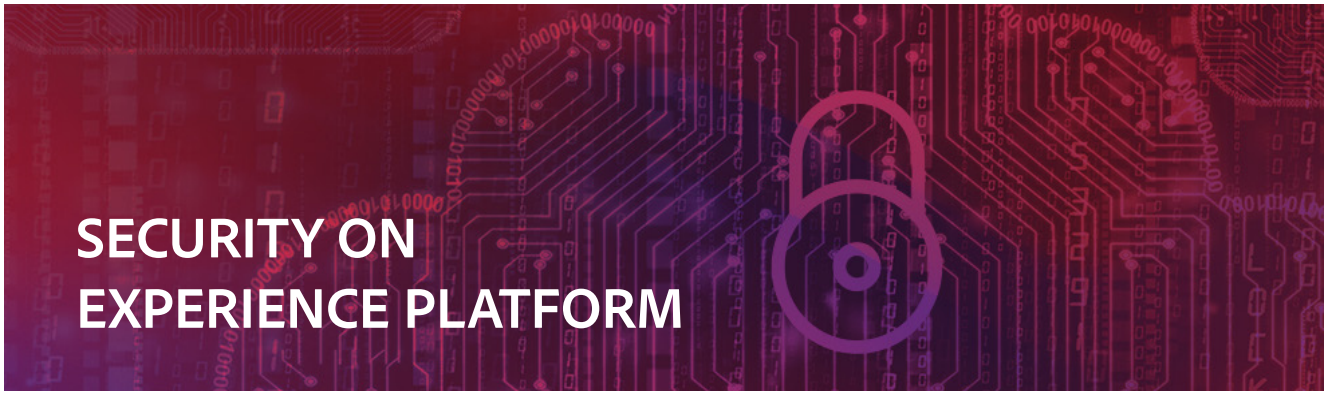


Adobe Experience Platform data work flow diagram

SECURE ARCHITECTURE

Experience Platform is based on a "shared architecture," which brings all experience data from systems of engagement together to create the Experience System of Record. The service model used by Experience Platform streamlines the approach to security. By using a single access gateway (Adobe.io), we're able to quickly understand intended versus unintended traffic. We've standardized our security models for both operation and application-level security in ways that allow us to apply security controls across Experience Cloud.

By taking advantage of Azure Blob Storage and network security capabilities, Experience Platform builds on robust security controls, programs, and processes to constantly improvise the security posture of Adobe systems and their customers.



SECURITY ON EXPERIENCE PLATFORM

Experience Platform uses enterprise cloud infrastructure services to deliver security infrastructure, data, and systems. From ingestion, data input is restricted to authorized users, systems, and services. These input connections come through the UI or secure REST APIs. Data is then stored in our data lake, which acts as a sandbox for data and algorithms. All data, schemas, configurations, and profiles are secured via an authorization layer and can only be accessed by appropriately authorized users.

Each customer's data is stored in a separate subscription. Role-based access control helps ensure access to data is restricted to authorized users only. Data in our data lake is governed by the rules defined by the customer. Experience Platform also encrypts data at rest by default.

SECURITY AT ADOBE

Authentication and access management

Adobe uses IMS for authentication. This allows for use of Adobe Enterprise ID, but customers who would like additional control around access to Experience Platform may choose to use Federated ID. Federated ID allows customers to leverage their existing identity provider for authentication to Experience Platform. Leveraging Adobe Identity Management Service (IMS), Experience Platform supports legacy LDAP-compliant, SAML-compliant, and SSO systems. Read more about Adobe IMS.

Operational responsibilities of cloud infrastructure providers

Adobe contracts with certified cloud infrastructure providers to operate, manage, and control components from the hypervisor virtualization layer to the physical security of the facilities in which Experience Platform is deployed.

These providers also operate the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. This infrastructure includes facilities, network, and hardware, as well as operational software (host OS, virtualization software) that supports the provisioning and use of these resources. Adobe has a strict third-party vendor security assessment program, called Guardrails, that validates that these providers to adhere to industry-standard practices as well as a variety of security compliance standards.

Service monitoring

Our cloud service providers monitor electrical, mechanical, and life support systems and equipment and environmental states to help with the immediate identification of service issues. To maintain the continued operability of equipment, our cloud providers are required to perform ongoing preventive maintenance.

Physical and environmental controls

Required physical and environmental controls are specifically outlined in a SOC report. The following sections outline some of the security measures and controls in place at data centers of our cloud service providers around the world.

Physical facility security

Cloud infrastructure partner data centers utilize industry-standard architectural and engineering approaches. These data centers are housed in nondescript facilities, and partners control physical access at the perimeter and building ingress points using professional security staff, video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Our infrastructure partners only provide data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of our partners. All physical access to data centers is logged and audited routinely.

Fire suppression

Adobe cloud infrastructure providers provide automatic fire detection and suppression equipment in all data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action or gaseous sprinkler systems.

Climate-controlled environment

Adobe cloud service providers employ a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. Data centers maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Backup power

Data center electrical power systems are designed to be fully redundant and maintainable with no impact on operations, 24 hours a day, seven days a week. Uninterruptible power supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Video surveillance

Professional security staff strictly control physical access at the perimeter and building ingress points for data centers using video surveillance, intrusion detection systems, and other electronic means.

Disaster recovery

Data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built in clusters in various global regions, all data centers remain online 24x7 to serve customers; no data center is "cold." If failure occurs, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Secure network architecture

Adobe requires cloud service providers to employ network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic. We work with our cloud providers to enforce the most up-to-date ACLs.

Network monitoring and protection

Our cloud infrastructure providers employ a variety of automated monitoring systems to help ensure a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools provide significant protection against traditional network security issues:

- Distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MITM) attacks
- IP spoofing
- Port scanning
- Packet sniffing by other tenants

Data storage and backup

By default, Adobe stores all Experience Platform data using high-durability storage services provided by our cloud infrastructure partners. To help provide durability, PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in a provider region. In addition, providers calculate checksums on all network traffic to detect the corruption of data packets when storing or retrieving data.

Change management

The cloud service provider is responsible for authorizing, logging, testing, approving, and documenting routine, emergency, and configuration changes to existing infrastructure in accordance with industry norms for similar systems. Providers schedule updates to minimize any customer impact.

Patch management

Experience Platform cloud infrastructure providers maintain responsibility for patching systems that support the delivery of IaaS services, such as the hypervisor and networking services.

Adobe risk and vulnerability management

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution process is 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 not only for Experience Platform but for all Adobe products and services.

Penetration testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can help uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe documents all vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan. Adobe also has an internal penetration testing team who engages regularly to perform penetration tests of Experience Platform.

Security Review

The Experience Platform security team performs regular risk assessments of all components of Platform. Conducted by experienced security engineers and architects dedicated to Experience Platform, the in-depth security reviews look for design flaws, vulnerabilities or insecure configurations across the entire stack. Security discovery activities include threat modeling coupled with vulnerability scanning and static and dynamic analysis of the application. The security team partners with operations and development leads to ensure high-risk vulnerabilities are mitigated swiftly.

Incident response and notification

New vulnerabilities and threats emerge each day, and Adobe strives to respond immediately to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT, Bugtraq, and SANS, Adobe subscribes to the latest security alert lists issued by major security vendors.

When a vulnerability puts Experience Platform at risk, the Adobe Product Security Incident Response Team (PSIRT) communicates the vulnerability to the appropriate teams within the organization to coordinate the mitigation effort.

For cloud-based services, Adobe centralizes incident response, decision-making, and external monitoring in its Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues.

When an incident occurs with an Adobe product or service, the SCC works with the involved Adobe product incident response and development teams to help identify, mitigate, and resolve the issue using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

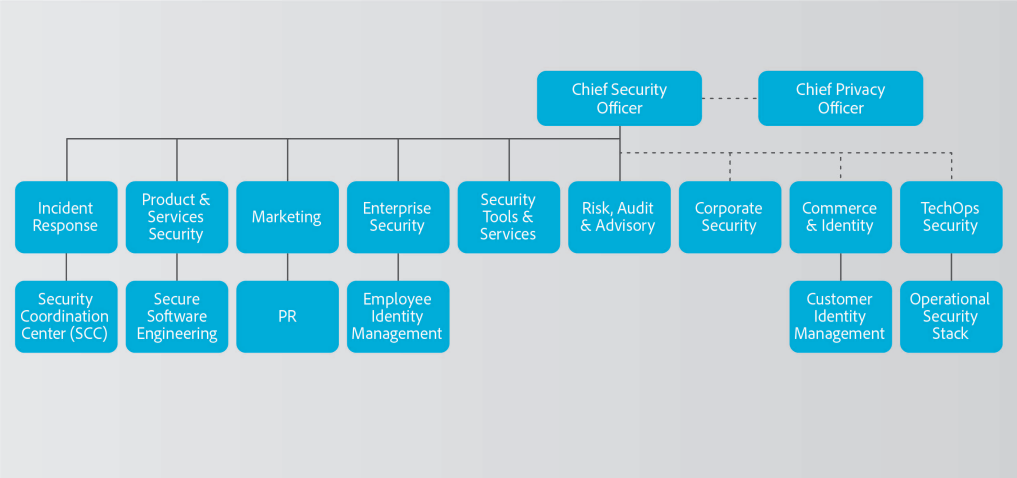
Forensic analysis

For incident investigations, the Experience Platform team adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody recording. Adobe may engage with law enforcement or third-party forensic companies when it determines that is necessary.

Adobe Security organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts under the chief security officer (CSO). The office of the CSO coordinates all product and service security initiatives and implementation of the Adobe Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams, including the Experience Platform team. ASSET researchers work with individual Adobe product and operations teams to achieve the right level of security for products and services and advise the teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.



Adobe secure product development

As in other key Adobe product and service organizations, the Experience Platform organization employs the SPLC process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment.

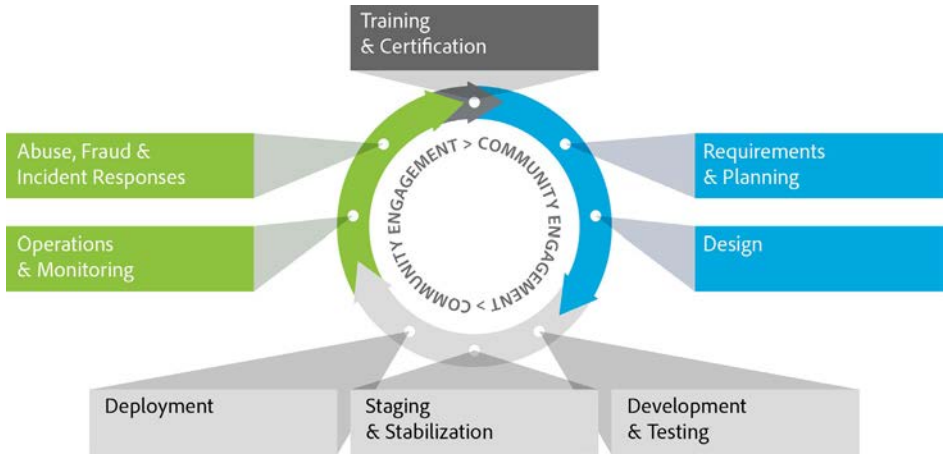
ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe SPLC

Adobe SPLC activities, depending on the specific Experience Platform component, include some or all of the following recommended best practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis

- Service roadmaps, security tools, and testing methods that guide the Experience Platform security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and the CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials



Adobe SPLC process

Adobe Software Security Certification Program

As part of the Adobe SPLC, we conduct ongoing security training in development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects.

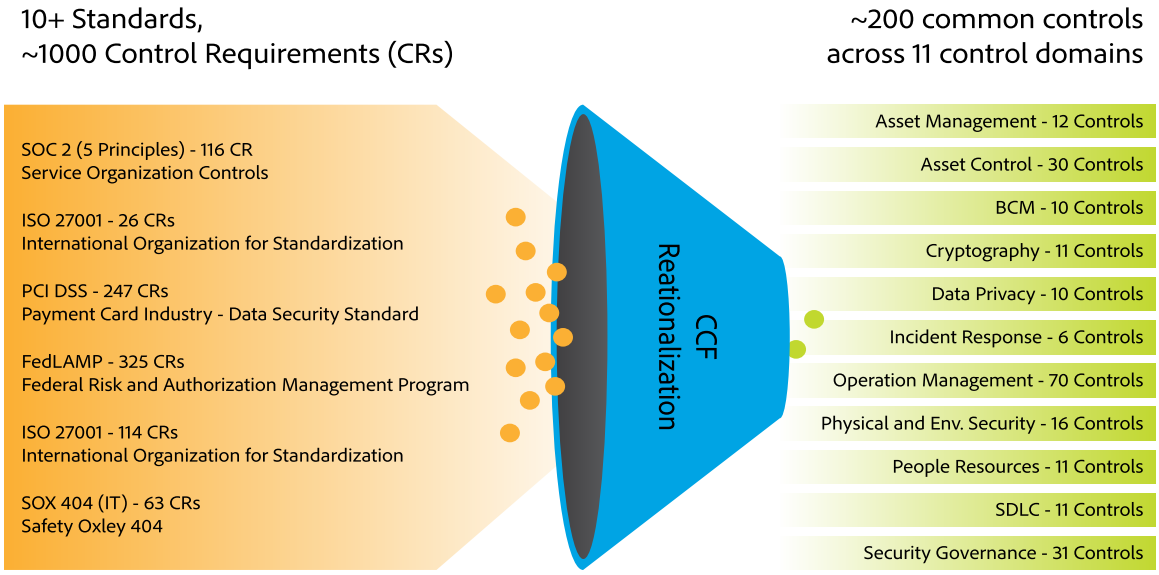
The program has four levels, each designated by a colored "belt": white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months to a year of hands-on security projects. Employees attaining brown and black belts become security champions and experts in their product teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

Various teams in the Experience Platform organization participate in additional security training and workshops to increase their awareness of how security affects their specific roles in the organization and the company as a whole.

Adobe Common Control Framework

To protect from the software layer down, Adobe uses the Adobe SPLC, as described previously. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls to protect the company's infrastructure, applications, and services and to help Adobe comply with a number of industry-accepted best practices, standards, and certifications.

In creating the Adobe Common Control Framework (CCF), we analyzed the criteria for the most common security certifications and found a number of overlaps. After analyzing more than 1,000 requirements from relevant cloud security frameworks and standards, we rationalized these down to approximately 200 Adobe-specific controls. The CCF control owners know exactly what is required to address the expectations of Adobe stakeholders and customers when it comes to implementing control.



Adobe CCF

Adobe corporate locations

Adobe maintains offices around the world and implements the following processes and procedures company-wide to protect the company against security threats.

Physical security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge, and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environmentally controlled server rooms accessible only by appropriate, authorized staff members.

Virus protection

Adobe scans all inbound and outbound corporate email for known malware threats.

Adobe employees

Employee access to customer data

Adobe maintains segmented development and production environments for Experience Platform, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

Background checks

Adobe obtains background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the United States, we conduct background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Employee termination

When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. In the event that Adobe terminates an employee, People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that upon conclusion of the employee's final day of employment, he or she can longer access Adobe confidential files or offices:

- Email access removal
- Remote VPN access removal
- Office and data center badge invalidation
- Network access termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

Customer data confidentiality

Adobe always treats your data as confidential. We don't use or share the information collected on behalf of any customer except as may be allowed in a contract with that customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy.

Standards compliance

All Adobe services are governed by a comprehensive set of documented security processes and have been subject to numerous security audits to maintain and improve quality. Adobe services are under continuing self-review to ISO 27001 standards, and the shared cloud underlying services infrastructure has a SOC 2 security certification.

Why Adobe

Adobe helps businesses better serve their customers and deliver amazing experiences. For customers and partners, Experience Platform offers a path towards a streamlined, seamless experience management process. Our platform starts by solving data and profile management challenges. It then lets you use Adobe Sensei services and custom ML models to enrich a customer's profile with actionable insights and surface it through the applications in Adobe Experience Cloud, Creative Cloud, and Document Cloud. Furthermore, the platform's seamless integration and open APIs allow you to build your own solutions and integrations.

The proactive approach to security and stringent procedures described in this paper help protect the security of the Experience Platform environment and your confidential data. We created Experience Platform with the strictest security in mind because we take the security of your digital experiences very seriously. In addition, we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of your data.

For more information, visit https://www.adobe.com/security.html.

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

5/19