WHITE PAPER

Adobe® Advertising Cloud Security Overview

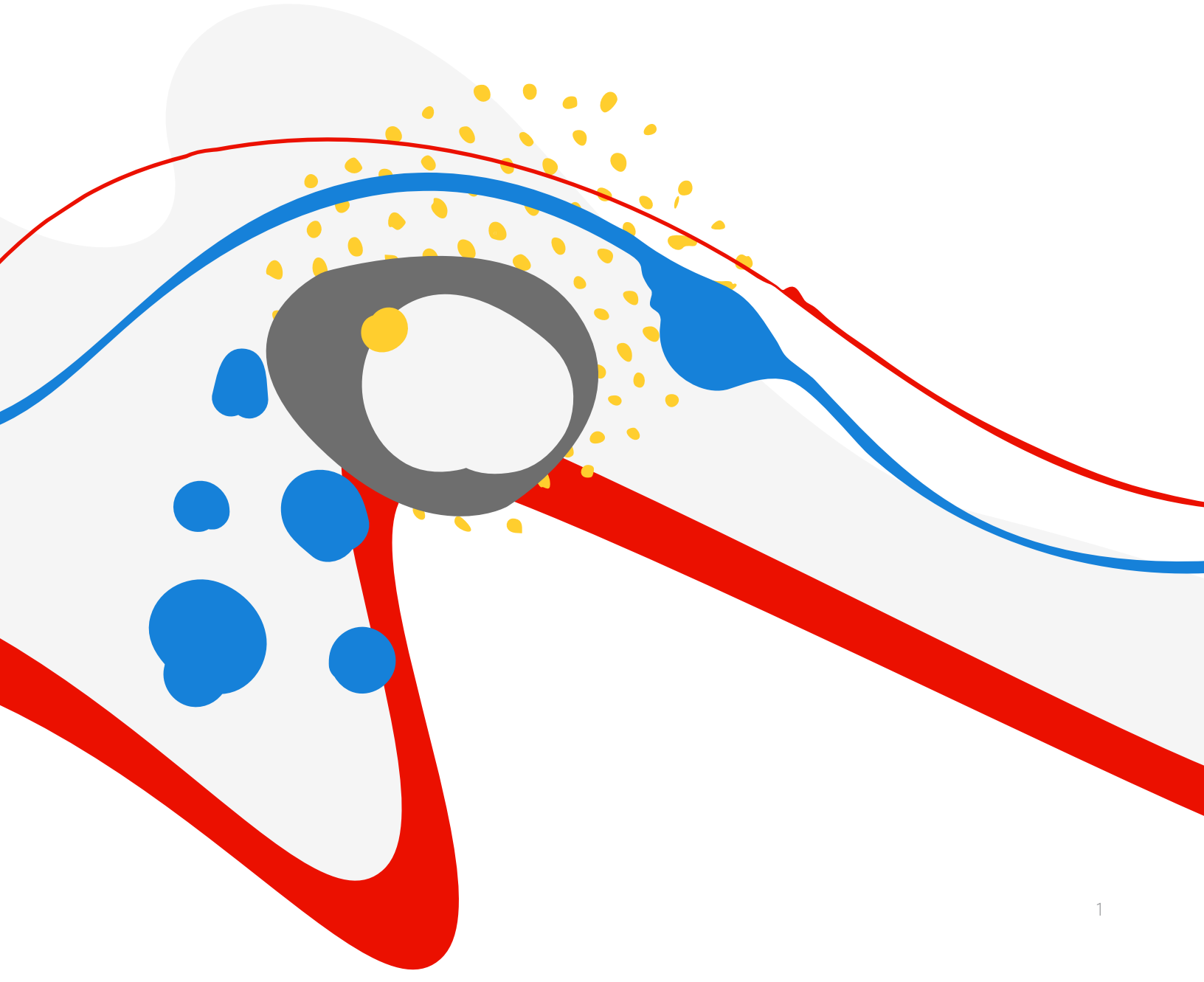
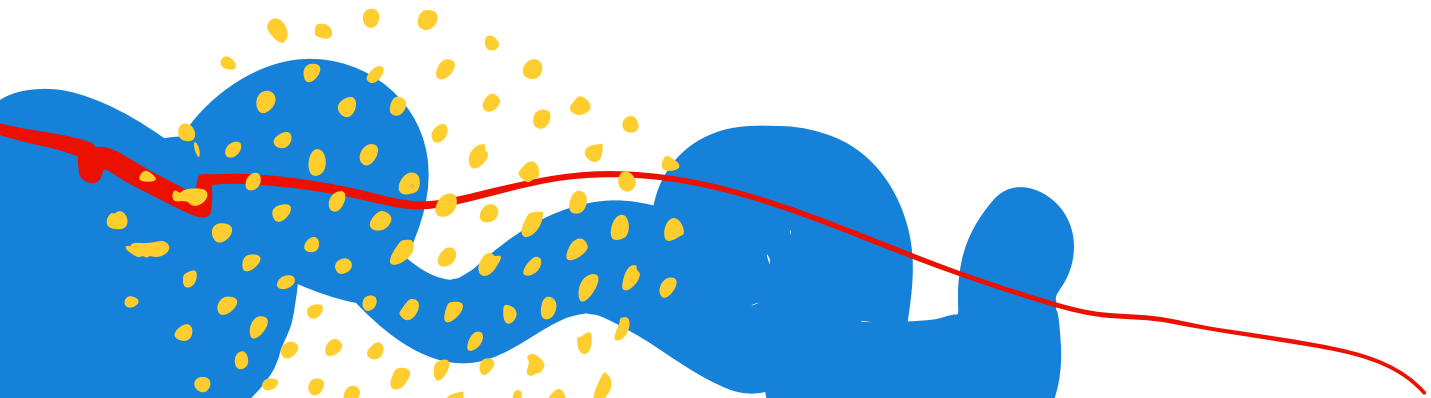


Table of Contents



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 and 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 bolster the security of Adobe Advertising Cloud and its associated data.

About Adobe Advertising Cloud

Adobe Advertising Cloud is the industry's first end-to-end platform for managing advertising across display, video, search, connected TV, and other digital formats. Advertising Cloud's breadth of experience in real-time bidding, APIs, and premium partnerships drives customer acquisition strategies across your preferred digital advertising channels and connects results and insights back to your sources of truth in Adobe Analytics and Experience Platform.

With this independent cross-channel platform, you can identify and engage the best audiences with a consistent and relevant ad experience—and integrate your media planning and buying into one programmatic solution. Adobe Advertising Cloud processes data from pixel tracking, publisher-provided reports, and advertiser-provided revenue feeds using predictive modeling algorithms to come up with spend and other configuration decisions for ad campaigns across both non-real-time and real-time bidding-based publishers.

Adobe Advertising Cloud Solution Architecture

The Adobe Advertising Cloud solution includes the following capabilities:

- **Search** — Allows users to simulate and quickly act upon the best and most profitable options in their search marketing strategy and offers the most comprehensive campaign optimization through industry-leading forecast models, scalable campaign automation, and integration with Adobe Analytics.
- **Demand-Side Platform (DSP)** — Automates display, social, video, and connected TV buying and lets users manage and optimize display and video programs to meet marketing goals and ROI objectives. DSP uses reliable re-targeting and data-reliant prospecting modeling to reach out to new and profitable audiences.

- **Feed-driven creative** — Automatically build thousands of digital ads that vary in real time for product-based retargeting, creative personalization, audience segmentation, and customer journey—all of which can be optimized with a feed-based algorithm using multivariate testing.
- **Adobe Creative Cloud integration** — Make collaboration between design and marketing teams a reality with the integration of Creative Cloud assets library and customer data from Adobe Analytics and Adobe Audience Manager. Combined, you get approved, campaign-ready creative elements that can build insight-led, personalized advertising sequences..

Adobe Advertising Cloud Data Flow

An advertiser typically uses Adobe Advertising Cloud as follows:

The advertiser creates ad campaigns on various publishing platforms using the campaign management capabilities of Advertising Cloud and/or directly creates campaigns on the publisher and grants Advertising Cloud access privileges to those campaigns. In the case of real-time-bidding-based publishing platforms, all campaign configuration is hosted by Advertising Cloud and so only the former is applicable. In the case of non-real-time-based publishers, Advertising Cloud also installs tracking hooks on these campaigns so that ad clicks will fire a beacon to the pixel tracking server in parallel with taking customers to the landing page. Advertising Cloud also downloads click reports from the publisher daily to help with reporting and optimization.

The advertiser also installs Advertising Cloud's pixel tracking on its website. This enables tracking of visitor behavior when the visitor reaches the site after clicking on an ad or other means. The pixel tracking captures page visits and conversions (revenue events quantified in terms of advertiser specific revenue metrics, e.g., "subscriptions," "ticket_purchase," etc.) by each visitor. The advertiser may also supplement or substitute this with periodic revenue feeds from his or her end. All revenue information is correlated in the back end with ad impressions and clicks of the same visitor, attributing value to each impression and click. The pixel tracking also segments visitors into categories based on their behavior on the site, which is critical in making bidding decisions for the visitor on real-time-bidding-based publishing platforms.

Portfolios, created by the advertiser, associate a set of ad campaigns with a budget and a maximization objective, usually expressed in terms of a weighted sum of the advertiser's revenue metrics. Advertising Cloud then applies predictive modeling techniques to the correlated click and revenue information to produce the bids and other campaign configuration for the following day. This process repeats daily, with campaign configurations adapting to changing conditions. The advertiser can run reports and forecasts on ad campaign performance through the Advertising Cloud web-based UI.

User Authentication

Access to Adobe Advertising Cloud 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 Advertising Cloud 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 Advertising Cloud 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.

Application and service entitlement is accomplished through the Adobe Enterprise Dashboard. More information on the dashboard is available here.

Adobe also maintains a Status Health Dashboard for Advertising Cloud, which can be accessed here.

Adobe Advertising Cloud Hosting

Demand-side platform (DSP) and search components of Adobe Advertising Cloud are hosted in Adobe data centers. Other components including television (TV) and Creative are hosted on public cloud service providers in the EMEA region.

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 1: 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.

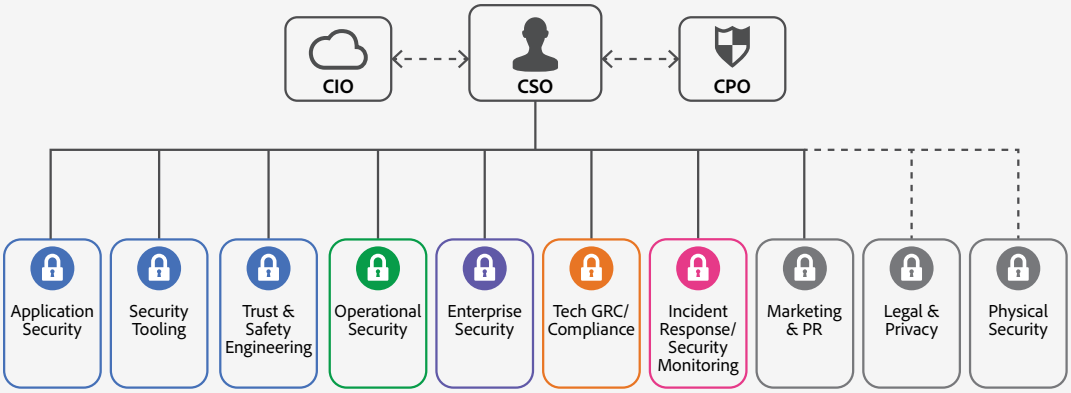


Figure 2: The Adobe Security Organization

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.

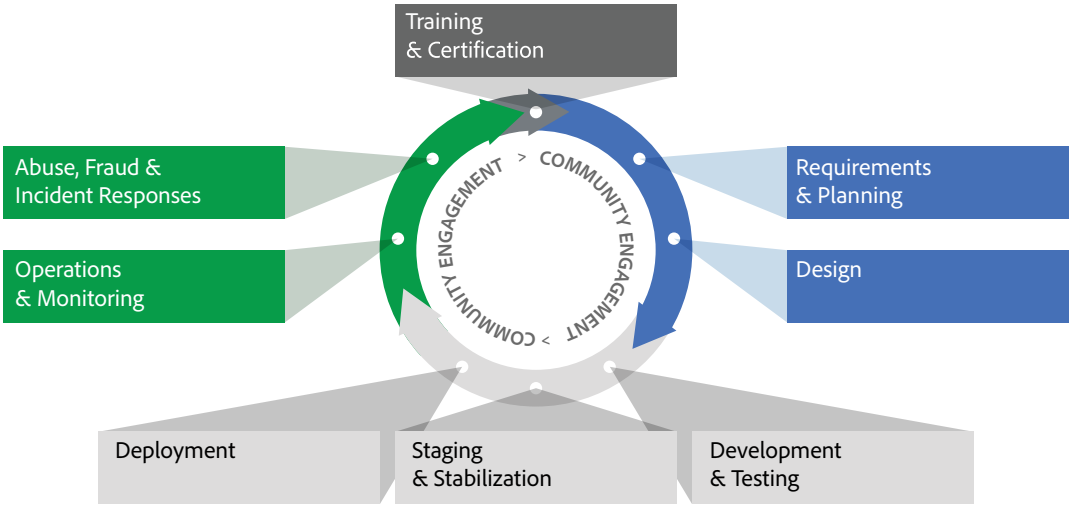


Figure 3: The Adobe Secure Product Lifecycle

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.

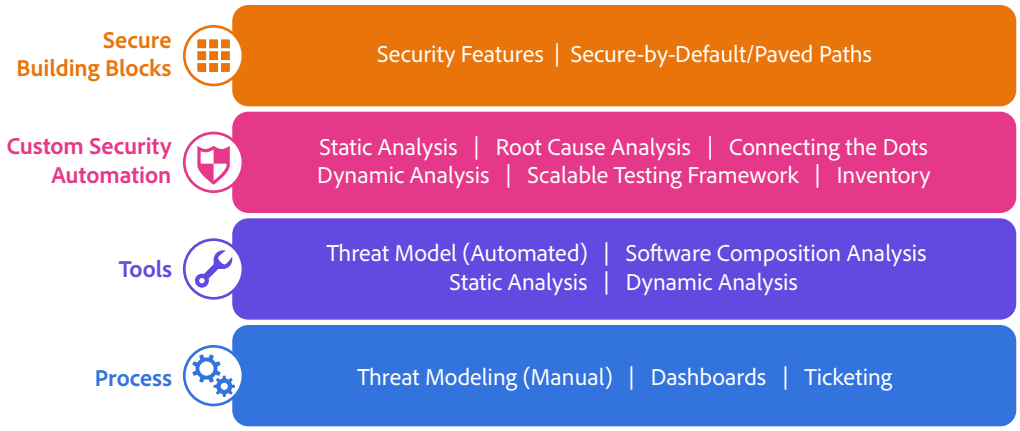


Figure 4: The Adobe Application Security Stack

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.

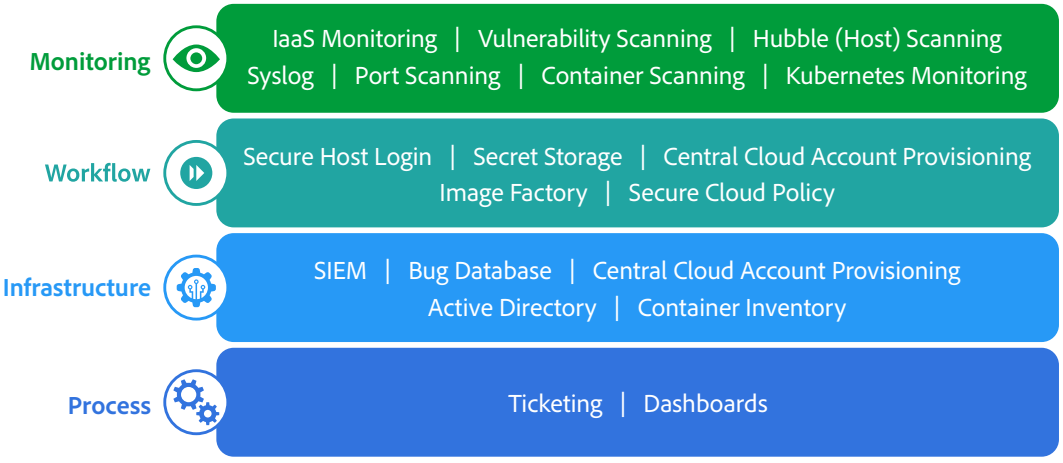


Figure 5: The Adobe Operational Security Stack

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.

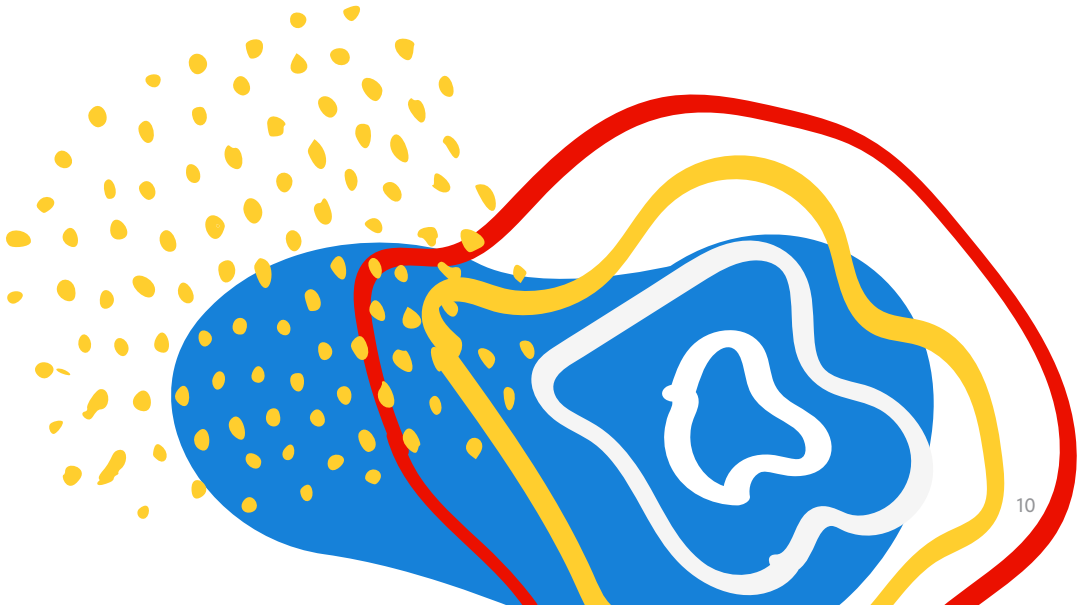
For more information on our enterprise security controls and standards we have developed for these controls, please see the Adobe Enterprise Security Overview.

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 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 Advertising Cloud 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 stay ahead of malicious activities and help ensure the secure our customers' data.

For more information, please visit the Adobe Trust Center.