Adobe Experience Cloud

Adobe

WHITEPAPER

Adobe Primetime Advertising Security Overview

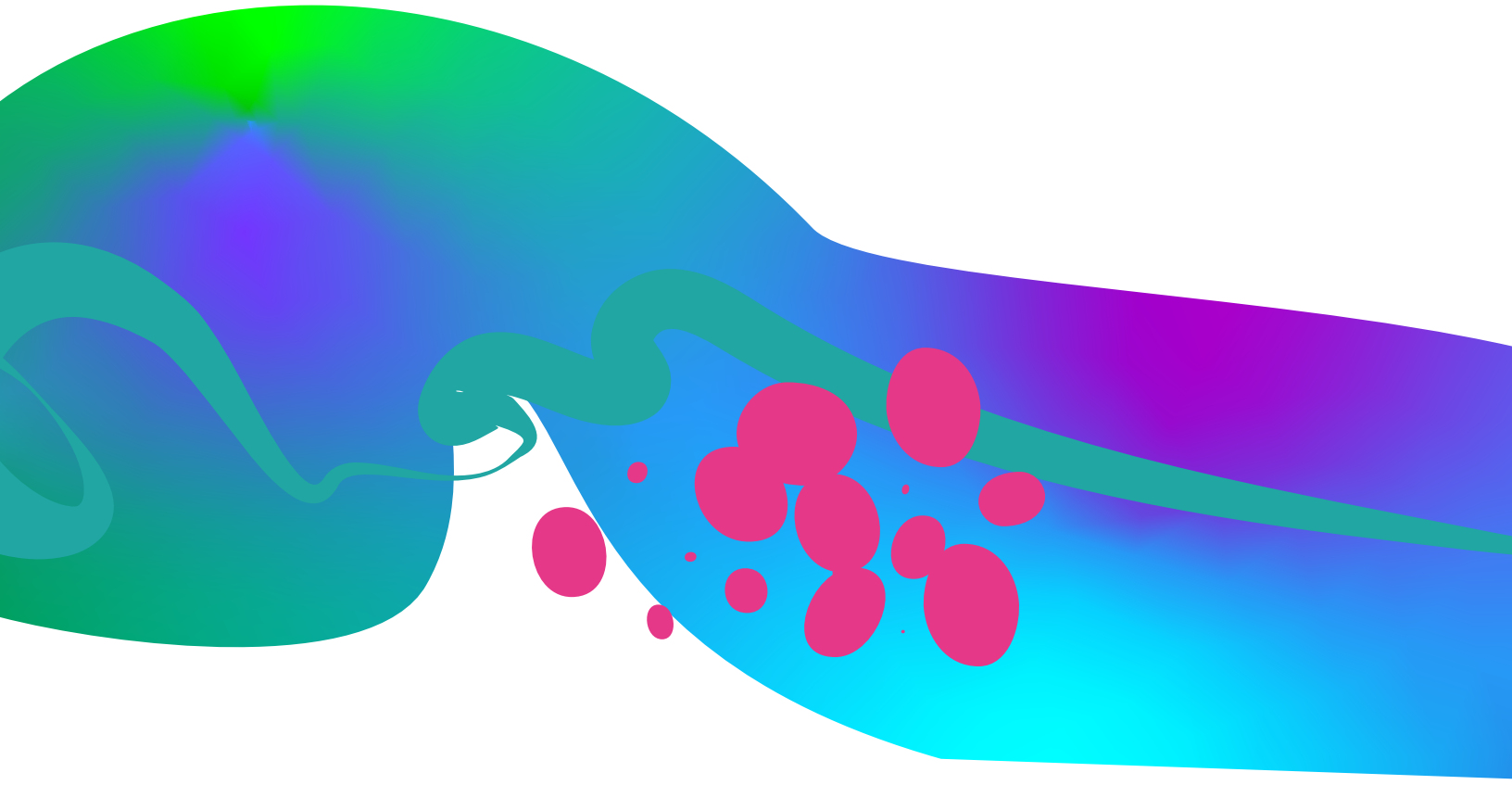


Table of Contents

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 and 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 Primetime Advertising solution experience.

About Adobe Primetime Advertising

Adobe Primetime Advertising helps content providers deliver and monetize viewer experiences and boost revenue by providing TV-quality, targeted ad experiences — even during big events and mega-launches. By dynamically inserting ads into live, linear, and VOD (video on-demand) content, Adobe Primetime Advertising allows the monetization of TV programming across a range of digital devices.

Adobe Primetime Advertising Solution Architecture

Adobe Primetime Advertising includes the following two (2) primary products:

- **Adobe Primetime Ad Insertion (PTAI)** enables publishers to stitch targeted ads into any video stream and includes two components:
  - **Server-Side Ad Insertion (SSA**I) — Conducts server-side insertion of ads into HLS- (HTTP Live Streaming) and DASH- (Dynamic Adaptive Streaming over HTTP) encoded manifests (a.k.a. playlists).
  - **Monetization & Experience Optimizer (MEO**) — Receives ad request calls, routes them to the proper ad server, and returns the ad details to be stitched into the content stream.
- **Adobe Primetime TVSDK** enables publishers to create a custom video playback experience and deploy it to a broad range of devices. TVSDK can be used with Primetime Ad Insertion for playback of server-side ad-inserted content or can leverage native client-side ad insertion capabilities to directly personalize manifests.

Adobe Primetime Advertising also includes an optional add-on service:

- **Adobe Content Repackaging Service (CRS)** conducts just-in-time transcoding to ensure that incompatible ad creatives can be properly played back in content streams. The Adobe CRS can be used with either Primetime Ad Insertion or Primetime TVSDK.

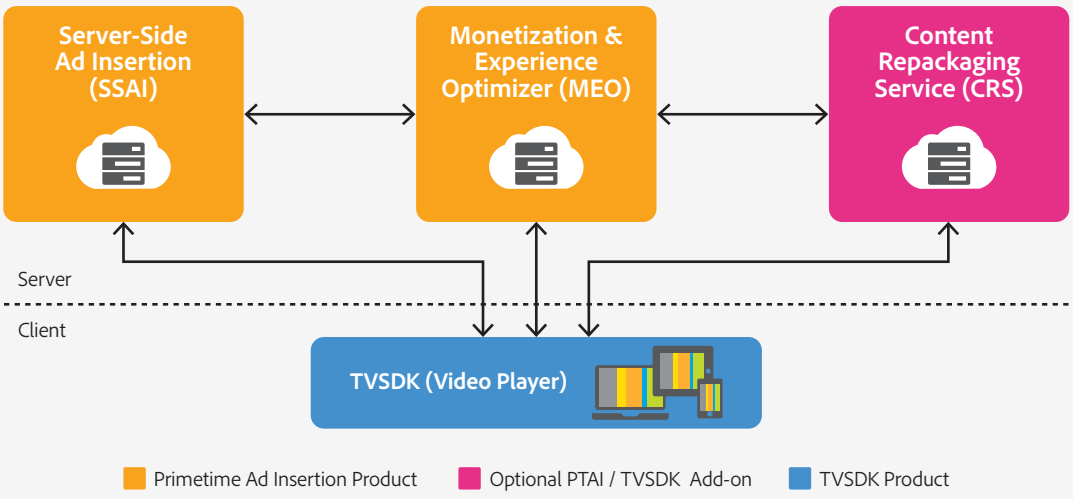


Figure 1: Adobe Primetime Advertising Solution Architecture

Additional third-party components with which Adobe Primetime Ad Insertion communicates include:

- **CDN** — Stores the physical assets for the entertainment content and advertising content. Adobe Primetime Ad Insertion does not store entertainment content; rather, it pulls the manifest files for the content and ads from the CDN. Adobe Primetime Ad Insertion works with all major CDNs and supports their typical token security schemes for ensuring protected access to content.
- **Ad Server** — Provides both the information that determines the specific ads to show each viewer as well as the location of the ad asset on the CDN to Primetime Ad Insertion for stitching into the manifest files. Adobe Primetime Advertising works with all major ad servers and supports IAB VAST/VMAP communication standards.
- **Video Players** — Similar to Primetime TVSDK, third-party or home-built video players make a call to Primetime Ad Insertion for ads and deliver personalized HLS/DASH manifests with targeted ads to viewers. A third-party video player is not needed if the customer chooses to use Primetime TVSDK.

Adobe Primetime Advertising Security Architecture and Data Flow

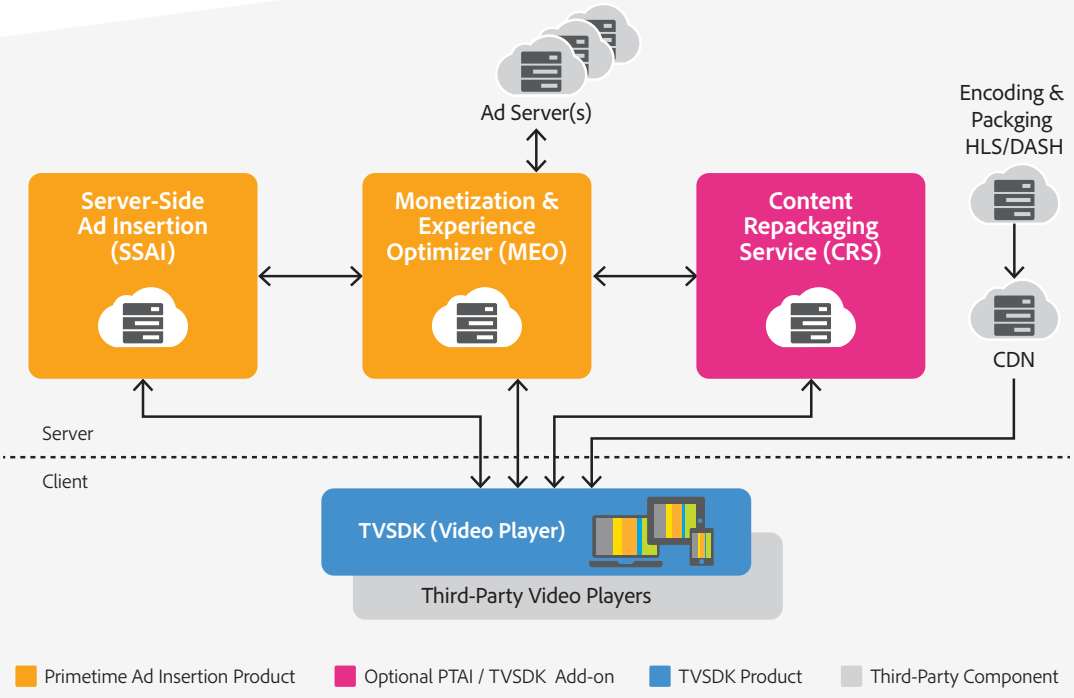


Figure 2: Adobe Primetime Advertising Data Flow

Data Flow Narrative

The following data flow narrative for server-side ad insertion using Primetime Ad Insertion assumes the customer has already configured the system using the instructions on Adobe Experience League.

1. The client application generates a Bootstrap URL with information about the video stream and sends a GET request to Primetime Ad Insertion. Primetime Ad Insertion supports HLS and DASH with a variety of ad signaling formats.
2. Primetime Ad Insertion responds by sending the content manifest from the publisher's CDN back to the client application.
3. The client application chooses appropriate streams in the generated manifest to play and makes requests to Primetime Ad Insertion.

4. Primetime Ad Insertion fetches the requested stream(s) from the content CDN, parses/reads any cue information, makes calls to the ad server and replaces ad breaks as necessary.
5. If the customer has enabled CRS, Primetime Ad Insertion normalizes the manifest by rewriting resource URLs and detecting whether the ad creative requires transcoding, see Just-in-time Ad Transcoding.
6. Primetime Ad Insertion fetches the required ad creative and inserts the appropriate fragments into the manifests.
7. Primetime Ad Insertion delivers the final stitched manifests, including ads, to the client application for playback.
8. Ad delivery and viewability can be measured via either client or server-side ad tracking, see Setting up Ad Tracking.

For more detailed information about setting up and operating the Primetime Advertising solutions, please consult the documentation at the Adobe Experience League.

Data Encryption

Data transmitted between Primetime Ad Insertion components are secured in transit using HTTPS TLS 1.2 or higher.

By default, communications between Primetime TVSDK or a third-party video player and Primetime Ad Insertion use the protocol used by the video player to initiate the request, either unsecured HTTP or HTTPS using TLS 1.2 or higher.

Similarly, by default, communications between Primetime Ad Insertion and third-party CDNs and ad servers, as well as the return response from Primetime Ad Insertion to the video player, use the protocol used by the video player to initiate the connection to Primetime Ad Insertion.

Optionally, customers can force calls between TVSDK and Primetime Ad Insertion to use HTTPS and calls between Primetime Ad Insertion and CDNs and ad servers to use HTTP for reduced latency and improved performance. For more information on this option, please contact your Adobe sales representative.

User-exposed Security Options

Primetime Ad Insertion egress IP addresses are shared with third-party ad servers.

User Authentication

End-users access Adobe Primetime Advertising by utilizing named user licensing in the Adobe Admin Console. Adobe Primetime Advertising 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

Adobe Primetime Advertising Hosting and Security

Data Center Locations

Primetime Ad Insertion is deployed on data centers of leading cloud service providers in US West (Oregon), US East (Virginia), and EMEA (UK) regions.

Figure 3: Primetime Advertising Hosting Locations

Segregation of Client Data

All data for Primetime Ad Insertion is stored in the same server cluster, with access granted on a per-customer basis.

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 4s: Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

- **Application Security** — Focuses on the security of our product code, conducts threat research, and implements bug bounty.
- **Operational Security** — Helps monitor and secure our systems, networks, and production cloud systems.
- **Enterprise Security** — Concentrates on secure access to and authentication for the Adobe corporate environment.
- **Compliance** — Oversees our security governance model, audit and compliance programs, and risk analysis; and
- **Incident Response** — Includes our 24x7 security operations center and threat responders.

Illustrative of our commitment to the security of our products and services, the centers of excellence report to the office of the Chief Security Officer (CSO), who coordinates all current security efforts and develops the vision for the future evolution of security at Adobe.

The Adobe Security Organization

Based on a platform of transparent, accountable, and informed decision-making, the Adobe security organization brings together the full range of security services under a single governance model. At a senior level, the CSO closely collaborates with the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) to help ensure alignment on security strategy and operations.

In addition to the centers of excellence described above, Adobe embeds team members from legal, privacy, marketing, and PR in the security organization to help drive transparency and accountability in all security-related decisions.

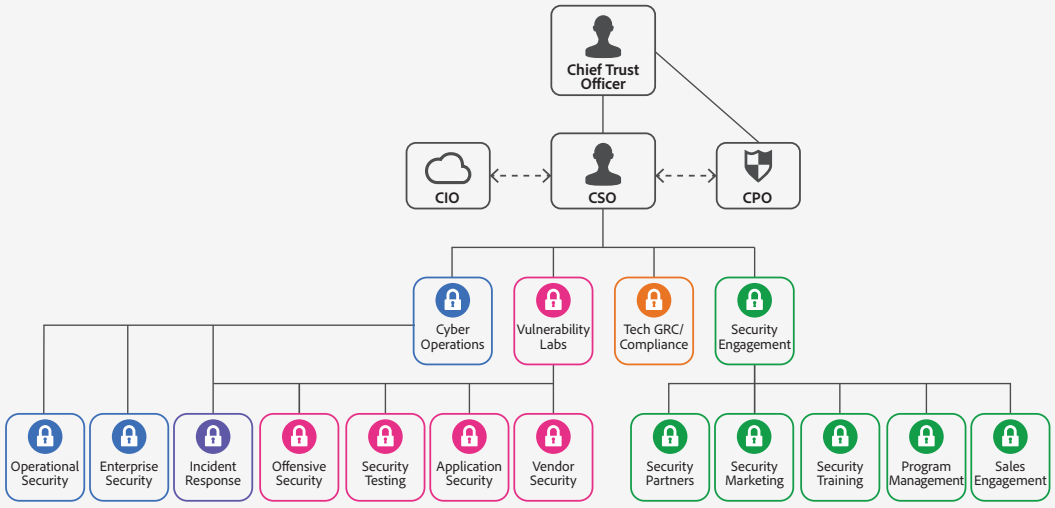


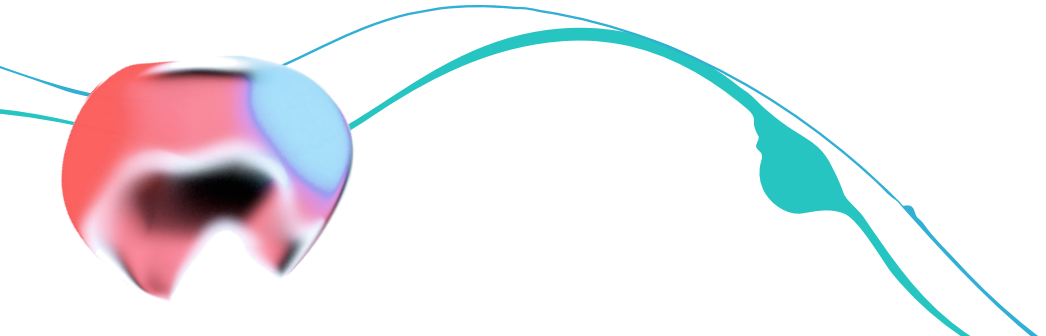
Figure 5: The Adobe Security Organization

As part of our company-wide culture of security, Adobe requires that every employee completes our security awareness and education training, which requires completion and re-certification on an annual basis, helping ensure that every employee contributes to protecting Adobe corporate assets as well as customer and employee data. On hire, our technical employees, including engineering and technical operations teams, are auto-enrolled in an in-depth 'martial arts'-styled training program, which is tailored to their specific roles.

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.



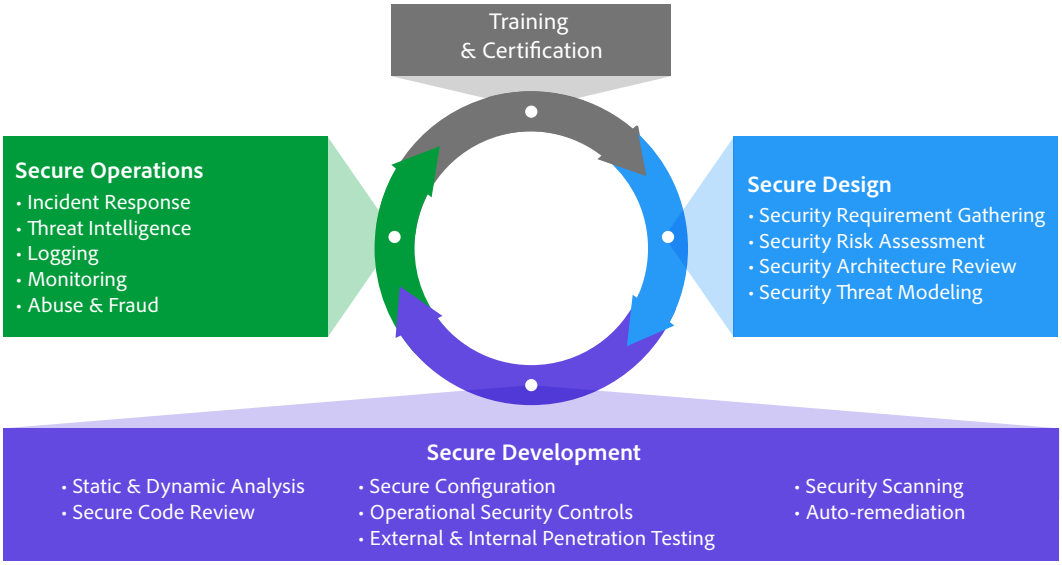


Figure 6: The Adobe Secure Product Lifecycle

Adobe maintains a published Secure Product Lifecycle standard that is available for review upon request. More information about the components of the Adobe SPLC can be found in the Adobe Application Security Overview.

Adobe Application Security

At Adobe, building applications in a "secure by default" manner begins with the Adobe Application Security Stack. Combining clear, repeatable processes based on established research and experience with automation that helps ensure consistent application of security controls, the Adobe Application Security Stack helps improve developer efficiency and minimize the risk of security mistakes. Using tested and pre-approved secure coding blocks that eliminate the need to code commonly used patterns and blocks from scratch, developers can focus on their area of expertise while knowing their code is secure. Together with testing, specialized tooling, and monitoring, the Adobe Application Security Stack helps software developers to create secure code by default.

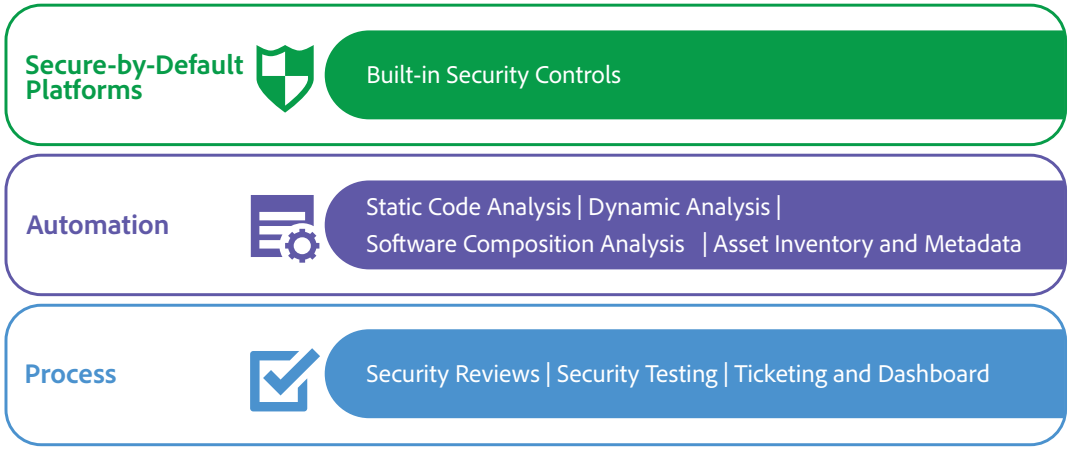


Figure 7: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of Amazon Web Services (AWS) and Microsoft Azure public cloud infrastructure. These standards are available for view upon request. 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.

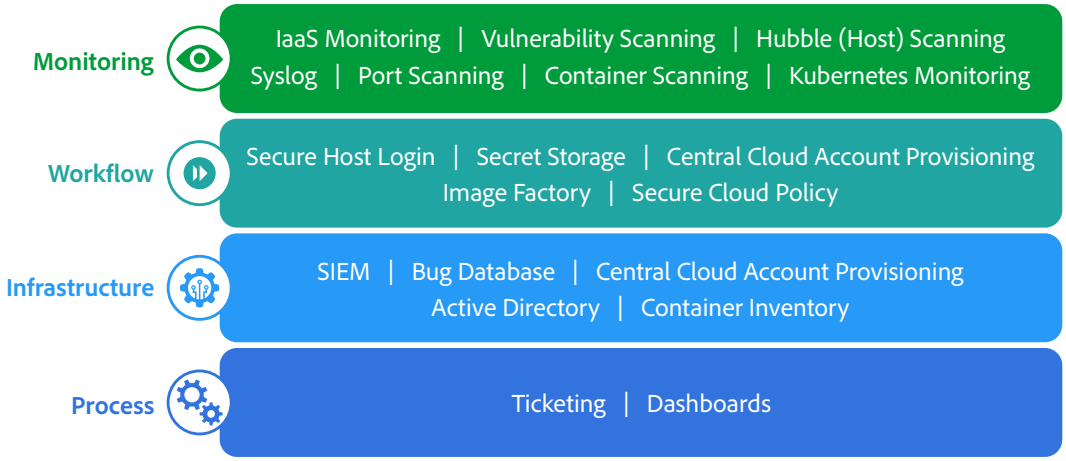


Figure 8: The Adobe Operational Security Stack

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 Primetime Advertising and your confidential data. At Adobe, we take the security of your digital experience data very seriously and we continually monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of our customers' data.

For more information, visit the Adobe Trust Center.

Adobe

11/22