Adobe Experience Cloud

Adobe

WHITEPAPER

Adobe® Analytics Security Overview

Table of Contents

Adobe Security

At Adobe, we know the security of your digital experiences is important. Security practices are deeply ingrained into our internal software development and operations processes and tools and 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 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 your Adobe Analytics experience and your data.

About Adobe Analytics

Part of the Adobe Experience Cloud suite of solutions, Adobe Analytics enables customers to apply real-time analytics and detailed segmentation across marketing channels to better understand how visitors interact with their brand across multiple channels. By gathering, analyzing, and acting upon this visitor data, customers can better target visitors and improve the effectiveness of their marketing.

Solution Architecture

The Adobe Analytics solution is comprised of the following components:

- **Adobe Analytics client-side implementation** – JavaScript code that customers add to their website in order to measure and collect end-user behavior and activity.[1]
- **Adobe Analytics reporting solutions**
  - **Analysis Workspace,** the default analysis and visualization tool for Adobe Analytics, providing a robust, flexible canvas for building custom analytics projects and accessible using a web browser.
  - **Reports & Analytics,** designed for beginner users who need access to pre-built reporting that is easier to navigate.
  - **Report Builder,** a Microsoft Excel plug-in that enables automatic updating of tracked data from Adobe Analytics that corresponds to cells in an Excel spreadsheet.
  - **Reporting API,** a REST API that allows customers to send Adobe Analytics data to third-party reporting or dashboard software.
  - **LiveStream,** a raw data stream that sends Adobe Analytics data directly into custom dashboards or into other reporting systems.
  - **Data Feeds,** a data stream that is similar to LiveStream in that it delivers raw data to the customer, but in a batch fashion rather than streaming data. Typically, Data Feeds sends a single file containing the raw data on an hourly basis via FTP, sFTP, Amazon S3, or Azure Storage.
  - **Data Warehouse,** a batch processing system that supports custom queries which often can't be composed in the interactive applications above. The customer can configure the system to send the report via email, FTP, sFTP, or Amazon S3 when it is complete.
- **Adobe Regional Data Collection** centers (RDC) – Adobe servers that collect the data customers want to track and measure, sent by the visitor's web browser or mobile apps.
- **Adobe Data Processing Centers** (DPC) – Adobe servers that process user behavior data according to the rules set by the customer in the Adobe Analytics application. Adobe then stores the processed data in a data warehouse for querying and analysis by the customer.

[1] For mobile applications, customers use the Mobile SDK. Alternatively, customers can use Adobe Launch to manage their client-side JavaScript updates. Please see the Adobe Launch website for more information.

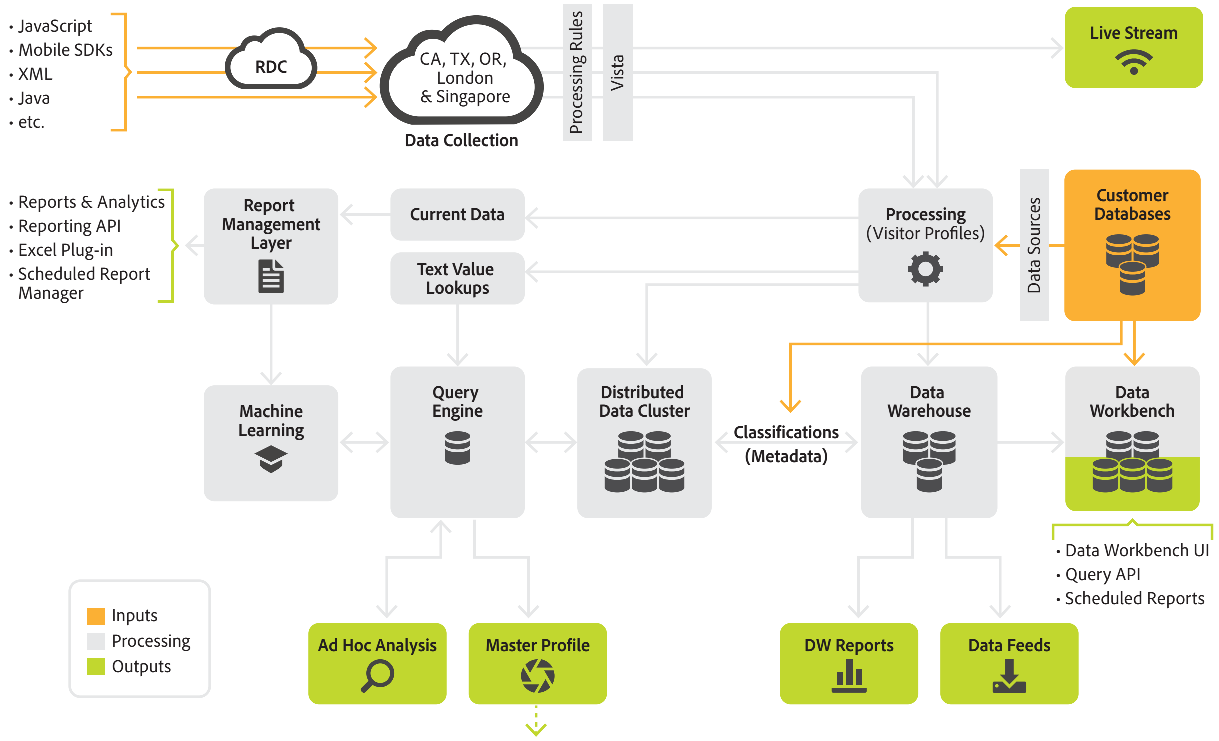


Figure 1: Adobe Analytics Solution Architecture Diagram

Data Flow

The following steps describe how data flows in a typical Adobe Analytics implementation. This section assumes that the customer has already defined the data they want to track:

1. When a visitor lands on a website on which the customer has incorporated the Adobe Analytics client-side implementation,[2] the code makes an image request to one of Adobe's RDC servers. This image request includes a standard set of information about the user's machine configuration and the page they are viewing, as well as the pre-defined information the customer wants to track.

   Along with the image, the RDC server returns a cookie containing a pseudonymous visitor ID, which is included in image requests on subsequent pages.[3]

   Most customers use a CNAME DNS entry to map Adobe's RDC servers into their own domain, so that the calls are first-party calls and the cookies are first-party cookies. For example, MyCompany might have a DNS entry that maps omtrdc.net to metrics.mycompany.com, and then they configure their JavaScript and/or mobile apps to send the Analytics data to metrics.mycompany.com.

2. Throughout the visitor's web session, the Adobe Analytics client-side code relays the tracked information to the Adobe RDC server. Communications to the RDC servers typically use the same communication method as the page itself (e.g., HTTP or HTTPS) however, it is possible for HTTPS to be used on HTTP pages. The mobile SDK uses HTTPS.

[2] Adobe Analytics requires code within the website, mobile app, or other application to send data to data collection servers. There are several methods to implement this code, depending on platform and organizational needs. Please see XXXX for the different implementation methods.

[3] Customers using the Adobe Visitor ID Service use a different cookie in a different way but the end-result is the same.

3. The RDC server forwards the user data to the Adobe DPC containing that customer's data using HTTPS.
4. The DPC pre-processes the data enhancing it with additional metadata and applying customer-defined processing rules. In addition, Adobe applies visit and attribution calculations. The data is then stored in Adobe Analytics data processing centers.
5. At this point, the customer can view the data gathered by Adobe Analytics using one of the reporting options listed above.

Data Encryption

Data in the customer's control, which includes data sent from the custom JavaScript on the website to the Adobe RDC, uses the protocol specified by the customer (HTTPS or HTTP). Adobe encourages customers to use HTTPS or similarly secure methods for all data they send to or pull from Adobe Analytics.[4]

Communications from mobile applications to Adobe RDCs using the Mobile SDK use HTTPS, as do all reporting APIs.

Data within an Adobe DPC is generally stored unencrypted. Data in-transit within the DPC is not always encrypted.

All communications between Adobe DPCs and Adobe RDCs are encrypted as are all communications with Adobe Analytics services running in Amazon Web Services (AWS) or Azure.

User Authentication

Access to the Adobe Analytics user interface requires authentication with a username and password. We continually work with our development teams to implement new protections based on evolving authentication standards. Users can access Adobe Analytics 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 Adobe Analytics 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,

[4] Adobe continues legacy support for sending data using HTTP and FTP and for extracting data using FTP. However, secure alternatives are available and preferred.

owned, controlled by customers' IT infrastructure. Adobe integrates with most any SAML2.0 compliant identity provider.

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 regularly monitors Adobe-hosted accounts for unusual or anomalous account activity and evaluates this information to help quickly mitigate threats. 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.

Roles, Permissions and Entitlements

Application provisioning and user entitlement is accomplished in the Adobe Admin Console.

For more information on specialized methods for accessing Adobe Analytics data and reporting via approved applications, please refer to the data sources guide at https://marketing.adobe.com/resources/help/en_US/sc/user/home.html

Cloud Hosting and Security

Adobe maintains eight (8) Regional Data Collection centers and three (3) Data Processing Centers for Adobe Analytics. The RDCs are hosted in AWS in locations around the world, while the DPCs are hosted in an Adobe-owned data center in Oregon (for U.S. customers) and on Adobe-owned servers in leased data center space in London, England (for customers in the EU), and in Singapore (for customers in Asia).

Customers can configure data collection for their report suites to use the RDC that is closest to each website visitor's location or restrict collection to the RDCs in their preferred region (US, Europe or Asia).

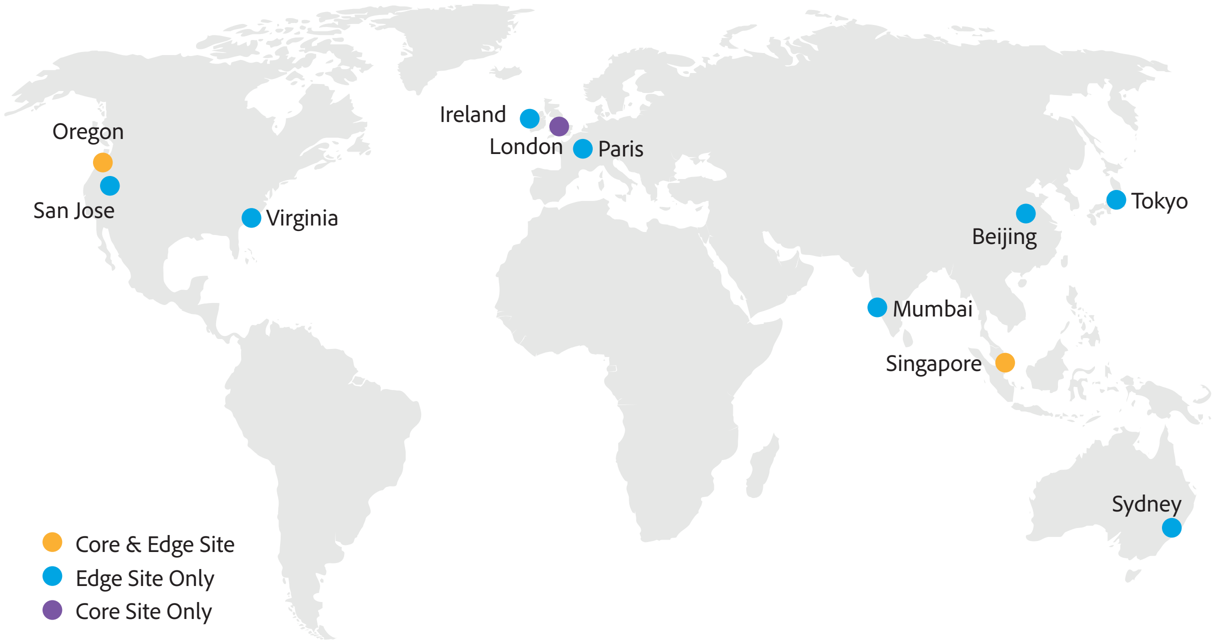


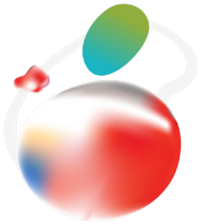
Figure 2 — Adobe Analytics hosting locations

In the event of a disruption in communication between the RDC and the DPC, data is saved locally and then forwarded to the customer-configured DPC when communication is restored.

For major disruptions, the Adobe Operations team reconfigures the global DNS system used by Adobe RDCs to route customer data through another data collection center.

Segregating Client Data

Data is placed into separate databases (a.k.a., report suites), and a single client's site reports are grouped together on one or more servers. In some cases, more than one client may share a server, but the data is segmented into separate databases. The only access to these servers and databases is via secure access by the Analytics application. All other access to the application and data servers is made only by authorized Adobe personnel, and is conducted via encrypted channels over secure management connections. We also separate our testing environments from our production environments to avoid use of customer data in testing environments.



Adobe Security Program Overview

The integrated security program at Adobe is composed of five (5) centers of excellence, each of which constantly iterates and advances the ways we detect and prevent risk by leveraging new and emerging technologies, such as automation, AI, and machine learning.

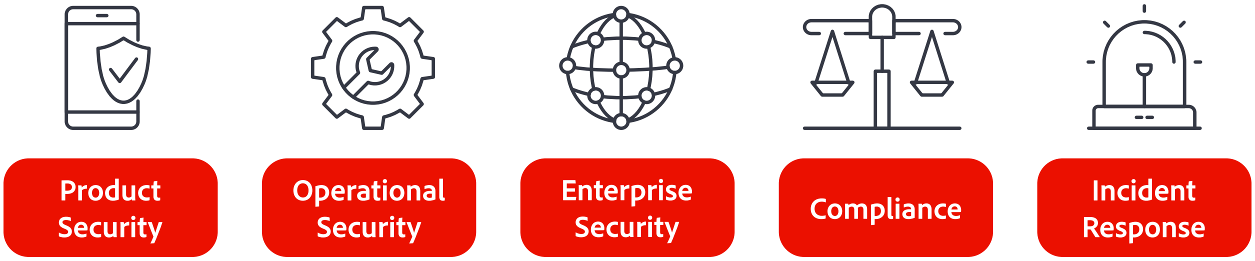


Figure 3 - Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

Application Security — Focuses on the security of our product code, conducts threat research, and implements bug bounty.

Operational Security — Helps monitor and secure our systems, networks, and production cloud systems.

Enterprise Security — Concentrates on secure access to and authentication for the Adobe corporate environment.

Compliance — Oversees our security governance model, audit and compliance programs, and risk analysis; and

Incident Response — Includes our 24x7 security operations center and threat responders.

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

The Adobe Security Organization

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

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

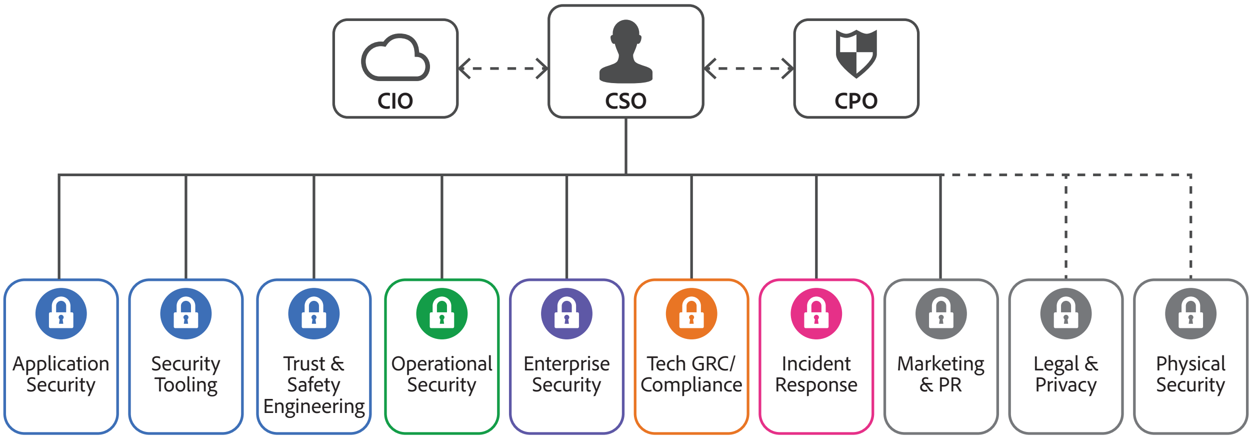
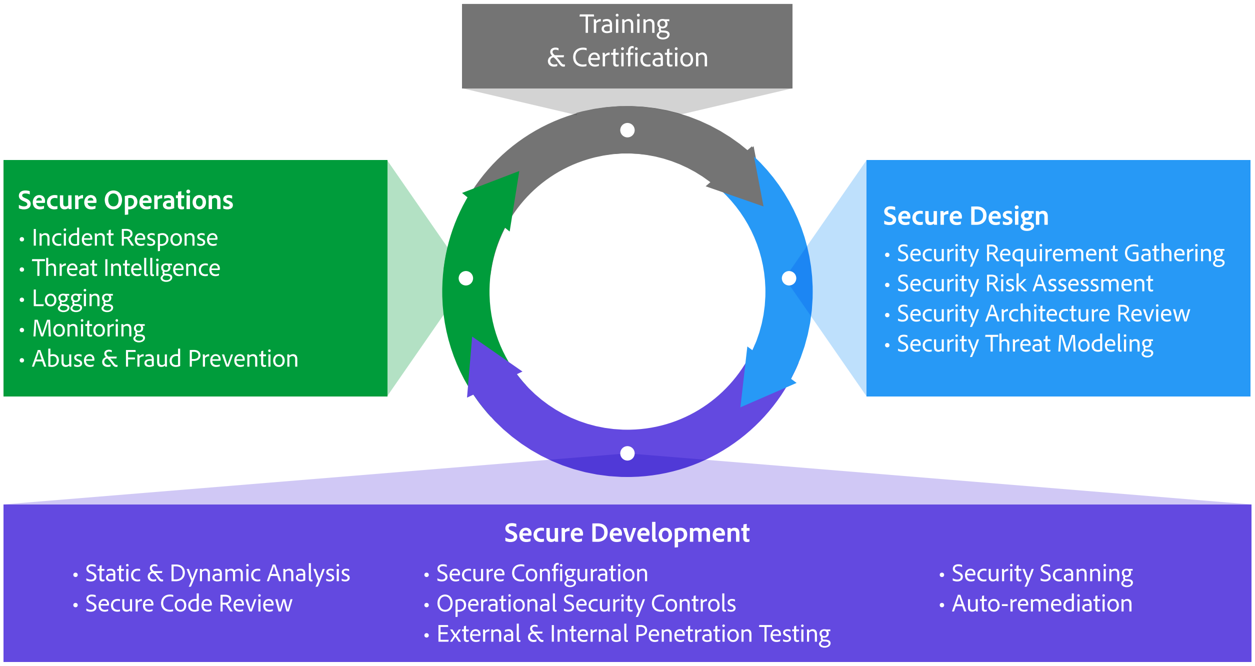


Figure 4 - The Adobe Security Organization

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



Training & Certification

Secure Operations

- Incident Response
- Threat Intelligence
- Logging
- Monitoring
- Abuse & Fraud Prevention

Secure Design

- Security Requirement Gathering
- Security Risk Assessment
- Security Architecture Review
- Security Threat Modeling

Secure Development

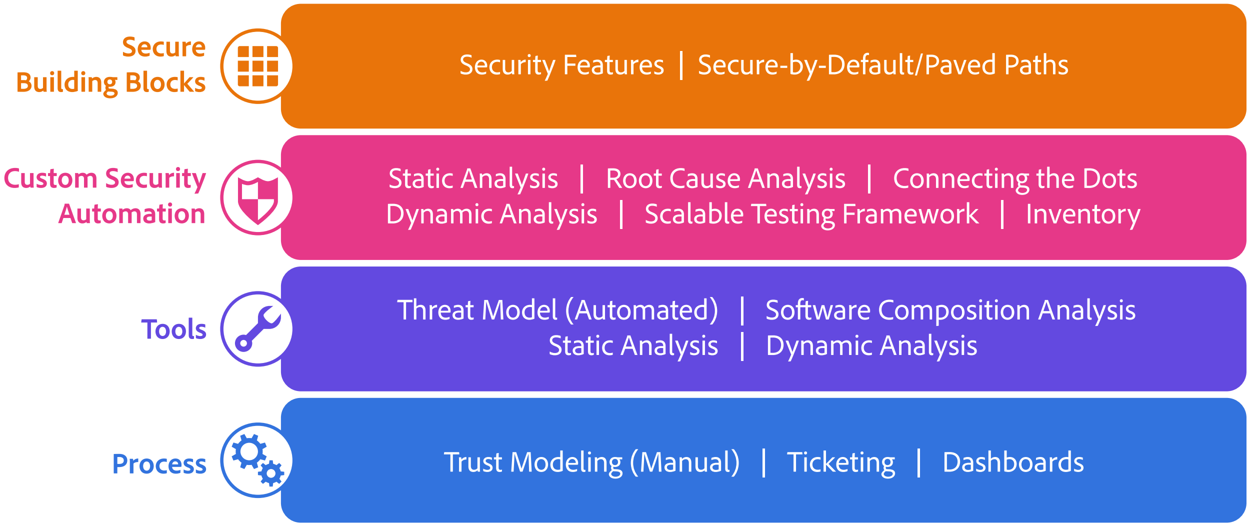
- Static & Dynamic Analysis
- Secure Code Review
- Secure Configuration
- Operational Security Controls
- External & Internal Penetration Testing
- Security Scanning
- Auto-remediation

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

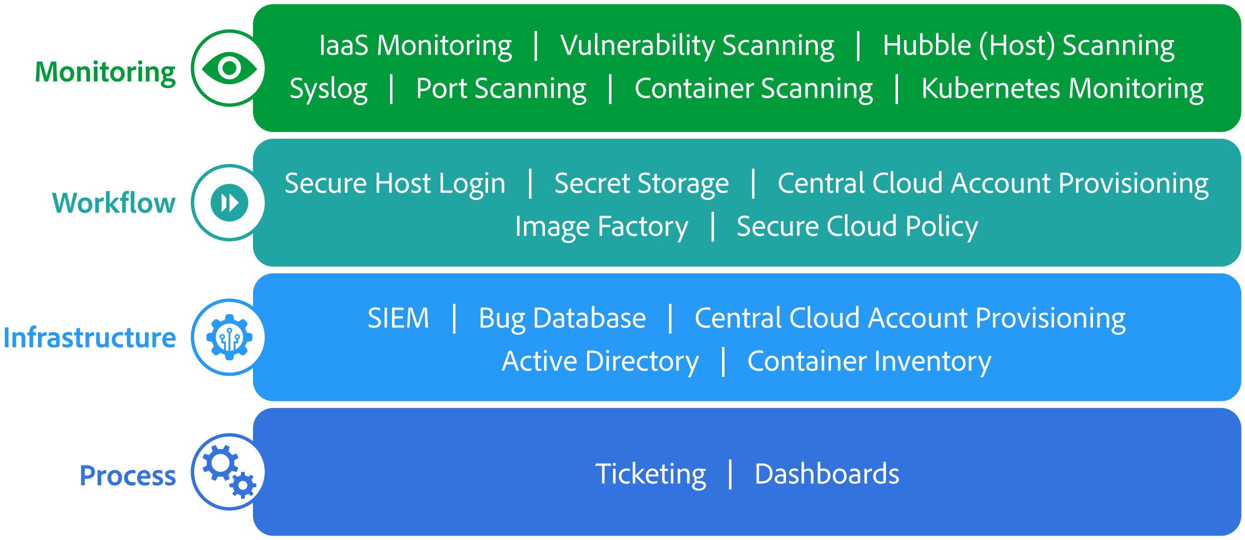
Process: Trust Modeling (Manual) | Ticketing | Dashboards

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.

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 the Adobe Analytics solution and your customer data. At Adobe, we take the security of your digital experience very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and to help ensure the security of our customers' data.

For more information, please visit the Adobe Trust Center.

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