Adobe Experience Cloud

Adobe

WHITEPAPER

Adobe® Audience Manager Security Overview

Table of Contents

Adobe Security 3

About Adobe Audience Manager 3

Adobe Audience Manager Solution Architecture 4

Adobe Audience Manager Security Architecture and Data Flow 5

- Data Encryption 6
- User Authentication 7
- Roles and Permissions 7

Audience Manager Hosting and Security 7

Adobe Security Program Overview 8

The Adobe Security Organization 9

The Adobe Secure Product Lifecycle 10

Adobe Application Security 10

Adobe Operational Security 11

Adobe Enterprise Security 12

Adobe Compliance 12

Incident Response 12

Business Continuity and Disaster Recovery 13

Conclusion 13

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. Our cross-functional teams strictly follow these practices 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 secure Adobe Audience Manager and its associated data.

About Adobe Audience Manager

Adobe Audience Manager is a data management platform that helps customers build unique audiences from multiple data sources to create valuable segments that can be targeted consistently across channels. Audience Manager supports a variety of pseudonymous identifiers (first- and third-party cookies, device IDs, hashed email) but never stores Personally Identifying Information (PII) anywhere in the Audience Manager network.

Advertisers use Audience Manager to help grow their revenue and customer base through unified, actionable views of their audiences by combining attributes from their data sources into high-value audience segments for ad targeting. Publishers use Audience Manager to identify the audience segments that are unique to their business and sell advertisers the opportunity to reach those unique, valuable audiences.

Adobe Audience Manager Solution Architecture

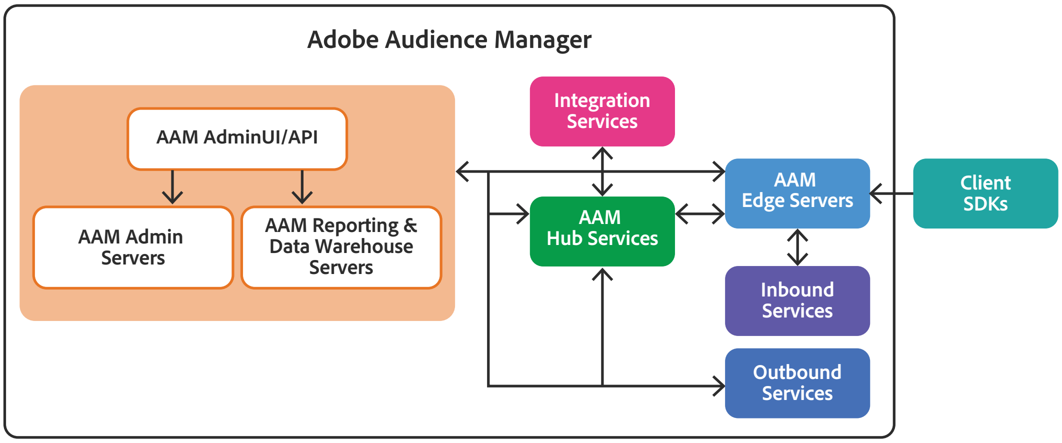


Figure 1: Adobe Audience Manager Solution Architecture

The Adobe Audience Manager (AAM) solution includes the following components:

- **Admin UI/API** — Enables customers to define and classify the types of data they wish to track on their digital properties, to configure the destinations where segmented data is sent, and to access audience reports for their segments. This interface is also used by administrators to determine who is authorized to use AAM.
- **Admin Servers** — Persistently store all data authored using the Admin UI/API.
- **Reporting & Data Warehouse Servers** — Generate standard and advanced audience reports for customer defined segments.
- **Integration Services** — Send configuration, audience, and identity data between Audience Manager and other Adobe solutions.
- **Hub Services** — Process and store long-term historical activity from specific users around the world, which can be joined with audience data previously collected from Edge Servers or on-boarded through inbound services. The audience data is then processed based on the rules defined by the customer in the Admin UI. All processed data is stored in the hub and can be pushed back to the Edge Servers to be joined with incoming on-line data.
- **Edge Servers** — Obtain real-time audience information from multiple sources, including customer websites, third-party data providers, customers' partners, and other Adobe solutions. Audience data is then processed based on the rules defined by the customer in the Admin UI and joined with the historical data stored on the Edge Servers.
- **Inbound Services** — Onboard data in batches from multiple sources, including customer's systems, third-party data providers, partners, and other Adobe solutions.
- **Outbound Services** — Publish audience and identity data to destinations configured by customers using server-to-server HTTP streams or using SFTP or batch files to public cloud providers' blob storage locations.

Adobe Audience Manager Security Architecture and Data Flow

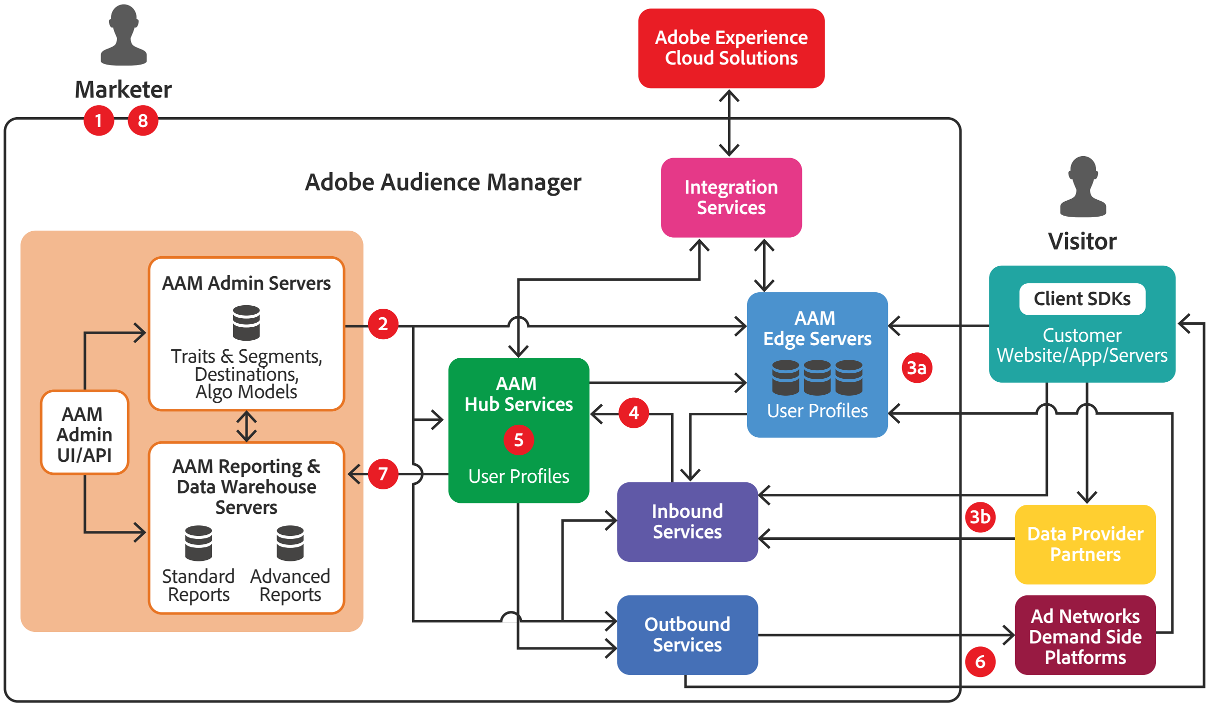


Figure 2- Audience Manager Data Flow Diagram

The following narrative describes how data flows through the Adobe Audience Manager solution.

Step 1: Configuration. Customers log into the Audience Manager web interface to configure rule sets using defined attributes, such as signals, traits, and segments.

- A **signal** is a key-value pair that identifies certain web activity (e.g., page = "sports" or event = "form submission").
- A **trait** is a combination of signals (e.g., page = sports + location = North America).
- A **segment** is the aggregation of both traits and signals (e.g., audience/ segment = "North American customers who have purchased soccer jerseys from the sports page"). Once defined, the rules are then stored in the Admin Servers.

Step 2: Rule distribution. The newly defined rule sets are distributed to all Audience Manager Edge Servers and Hub Services instances.

Step 3a: Online data collection. When a user visits the customer's website, Audience Manager places code on the user's computer to create behind-the-scenes communication and data collection with Adobe and its partners. Edge Servers process all incoming data into segments based on the customer-defined rules and any prior user data stored in Edge Servers and add cookie values to each user.

Step 3b: Offline data collection. To enrich the site visitor data collected online, customers and data provider partners can onboard offline activity and identity data through Inbound Services.

Step 4: Data aggregation and trait qualification. Inbound Services process collected online and offline data, attempt to match activity signals with traits defined by customers, augment activity data with matching trait qualifications, and prepare data to be ingested into Hub Services. *(Note: A trait qualification is a logged event indicating that one or more activity signals belonging to a visitor profile matches a trait rule.)*

Step 5: Data consolidation and segmentation. Hub Services instances ingest and merge all incoming data from customers, partners, and end-users and attempt to match the stored historical data to incoming data, thereby building and storing a more robust visitor profile. Based on segments defined by customers and trait qualifications from incoming and historical data, Hub Services process visitor profile data into segments and augment profile data with segment qualifications. *(Note: A segment qualification is a logged event indicating that one or more traits belonging to a visitor profile matches a segment rule.)*

Step 6: Destination updating. Outbound Services send updated activities, segments, and identities to customer-defined destinations.

Step 7: Reporting. Customers can access various audience reports about their defined traits and segments. Reports are generated by the Reporting and Data Warehouse Servers and displayed in the Admin UI. Customers that have enabled integrations with other Adobe solutions can also access performance reports for their segments in the user interface of each of these solutions.

Data Encryption

All connections between Adobe Audience Manager components are conducted over secure, encrypted connections using HTTPS TLS v1.2 or greater.

Audience Manager uses server-side encryption to encrypt data at-rest in outbound files published in batch to the object storage services managed by the public cloud provider. The encryption service is run by the public cloud provider, which also automatically generates and manages the encryption keys.

Inbound data files sent to Audience Manager can be encrypted with PGP encryption using Audience Manager 4096 RSA public key and the Advanced Encryption Standard (AES) data-encryption algorithm.

Audience Manager never stores Personally Identifying Information (PII) anywhere in the Audience Manager network.

User Authentication

Access to Adobe Audience Manager requires authentication with username and password. Users can access Adobe Audience Manager in one of three (3) different types of user-named licensing: Adobe ID, Enterprise ID, or Federated ID. You can find more information about Adobe Identity Management Services in the Adobe Identity Management Services security overview.

Roles and Permissions

System administrators can add user accounts and manage roles and permissions, which set the access for creating and managing activities in Audience Manager, in the Admin Console.

Administrators can also control access to reporting data using strong passwords, password expiration, IP login restrictions, and email domain restrictions.

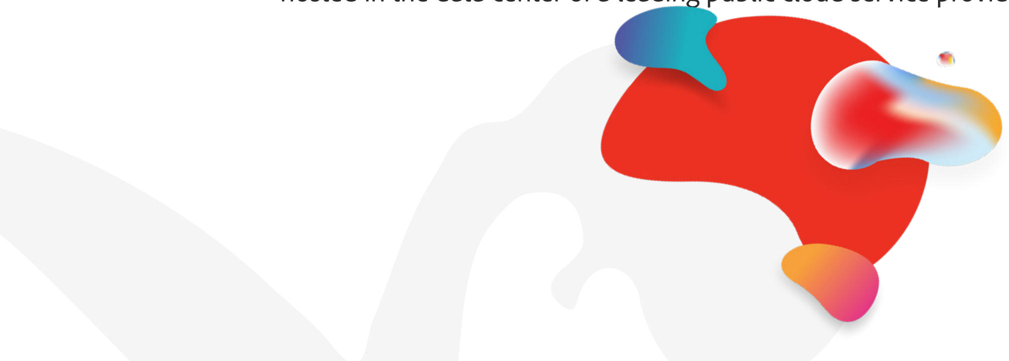
Audience Manager allows customers to control the visibility of the different data elements to specific business units through group permissions, referred to as Role-Based Access Control (RBAC). Group permissions are tied to objects (e.g., traits, segments) and to actions that users can perform on those objects (e.g., edit, view). Administrators can manage how their users view, create, read, write, and edit specific data sets, as well as restrict users from accessing data sets that should not be available to them.

Audience Manager also includes export control functionality to provide finer-grained control over which data can be distributed externally.

Audience Manager Hosting and Security

Adobe Audience Manager Edge Servers are hosted in enterprise-class data centers from public cloud service providers in US-East (N. Virginia), US-West (Oregon), Europe (Ireland), South America (São Paulo, Brazil) and Asia Pacific (Singapore, Tokyo, Mumbai, and Sydney). Visitor profile data is collected and stored by the Edge Servers closest to the site visitor.

Audience Manager Central Servers, which contain Hub Services, Admin Servers, Reporting and Data Warehouse Servers, Inbound and Outbound Services, and Integration Services, are also hosted in the data center of a leading public cloud service provider in US-East (N. Virginia).



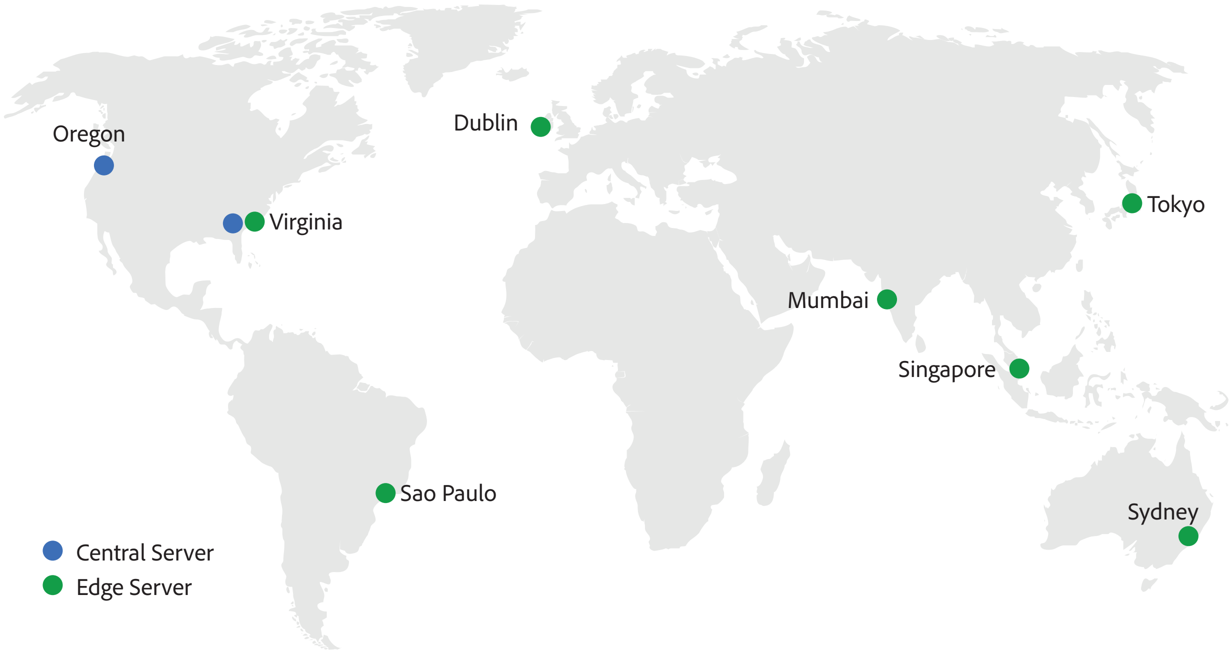


Figure 3-Adobe Audience Manager Hosting Locations

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 5: 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.

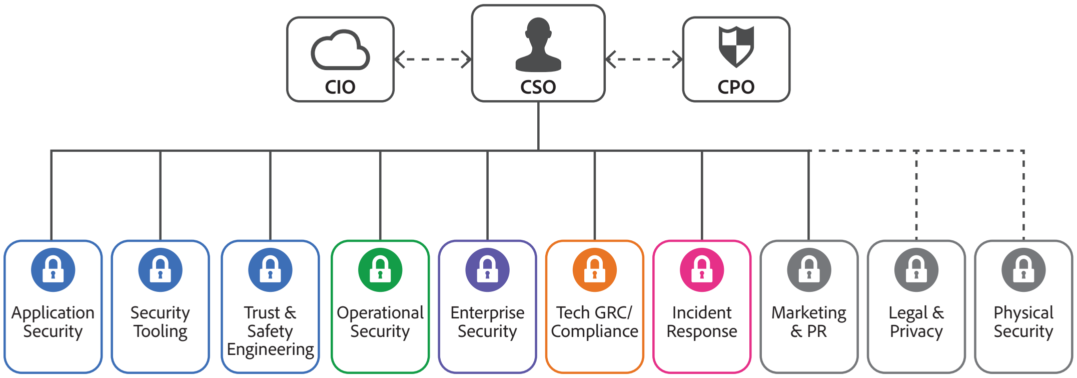
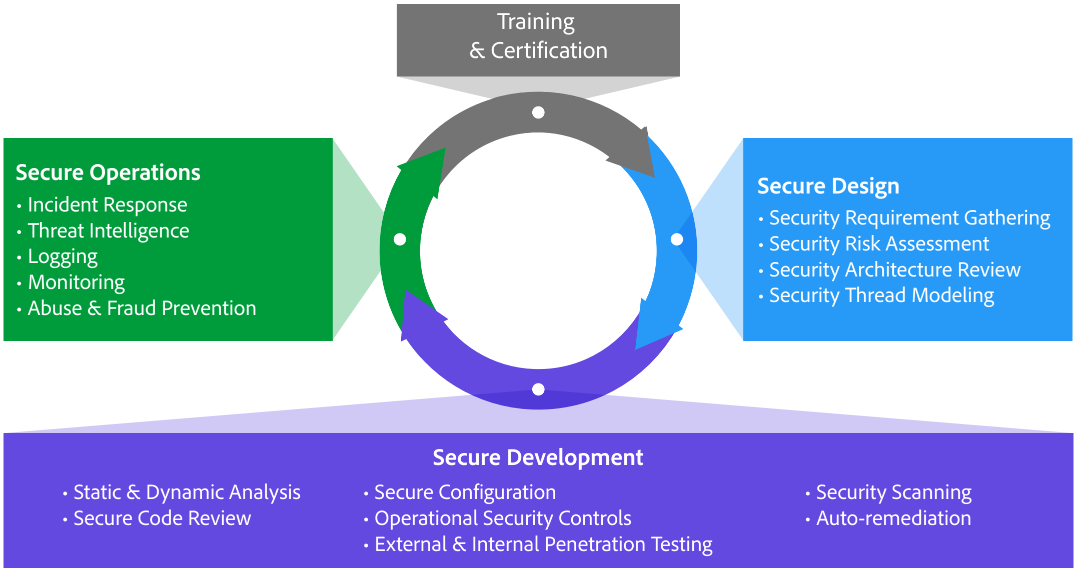


Figure 6: The Adobe Security Organization

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 Thread Modeling

Secure Development

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

Figure 7: 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.

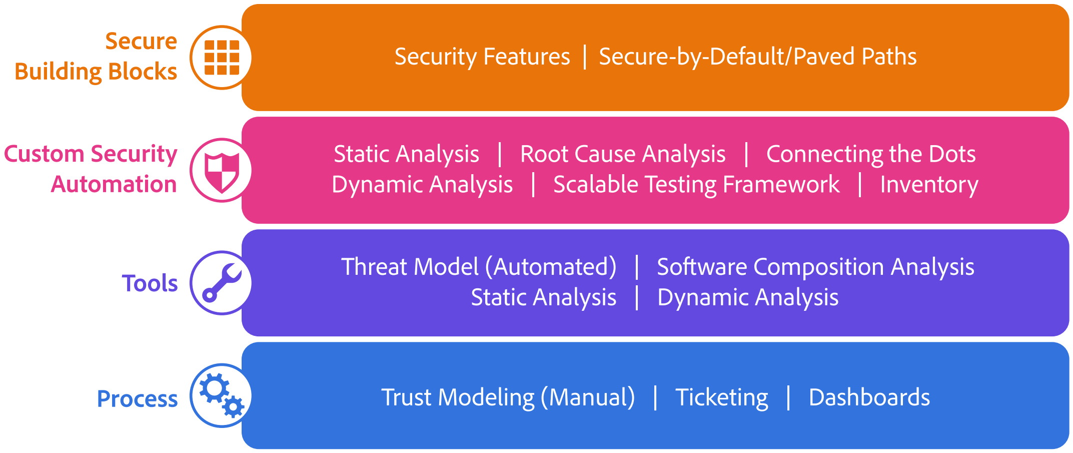

Secure Building Blocks
Security Features | Secure-by-Default/Paved Paths
Custom Security Automation
Static Analysis | Root Cause Analysis | Connecting the Dots
Dynamic Analysis | Scalable Testing Framework | Inventory
Tools
Threat Model (Automated) | Software Composition Analysis
Static Analysis | Dynamic Analysis
Process
Trust Modeling (Manual) | Ticketing | Dashboards

Figure 8: 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.

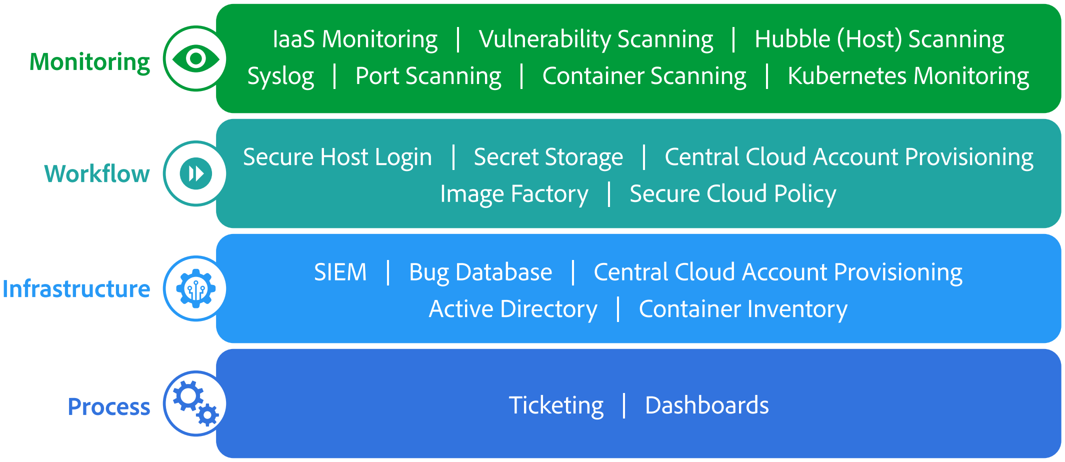

Monitoring
IaaS Monitoring | Vulnerability Scanning | Hubble (Host) Scanning
Syslog | Port Scanning | Container Scanning | Kubernetes Monitoring
Workflow
Secure Host Login | Secret Storage | Central Cloud Account Provisioning
Image Factory | Secure Cloud Policy
Infrastructure
SIEM | Bug Database | Central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

Figure 9: 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 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 Adobe Journey Optimizer and your confidential data. At Adobe, we take the security of your digital experience data very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of our customers' data.

For more information about Adobe security, please go to 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 sales representative.

Adobe

Adobe