Adobe Experience Cloud

WHITEPAPER

Adobe Experience Manager as a Cloud Service Security Overview

Table of Contents

Adobe Security

At Adobe, we take the security of your digital experience very seriously. 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 our product and service offerings.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of your Adobe Experience Manager as a Cloud Service solution and your data.

About Adobe Experience Manager as a Cloud Service

Adobe Experience Manager (AEM) as a Cloud Service is a modern, cloud-native application that accelerates delivery of omnichannel personalized experiences throughout the customer journey. Built upon a container-based infrastructure that offers API-driven development and a guided DevOps process, AEM as a Cloud Service allows IT to focus on strategic business outcomes instead of operational concerns.

AEM as Cloud Service consists of industry-leading cloud applications for hybrid content management (CMS) and digital asset management (DAM), each of which can scale to help meet the demands of the largest global corporations. Informed by data insights, AEM as a Cloud Service optimizes both marketer and developer workflows throughout the entire content lifecycle.

About the Adobe Container Management Platform

To support building modern cloud-based applications that can easily run and scale across multiple cloud infrastructure providers, Adobe has developed a container-based application platform based on the Kubernetes container orchestration engine. Adobe Experience Manager as a Cloud Service is built on this new container-based platform, which provides built-in core security functionality to further strengthen applications. The platform also provides greater flexibility to implement security and compliance controls on-the-fly without disrupting existing applications and will serve as the foundation for future versions of Adobe products and services.

AEM as a Cloud Service Solution Architecture

AEM as a Cloud Service includes four (4) primary components:

- **AEM Sites**, the Adobe Web Experience Management solution
- **AEM Assets**, the Adobe Digital Asset Management solution
- **AEM Forms**, the Adobe Digital Enrollment solution
- **AEM Screens**, the Adobe Digital Signage solution

The architecture for these components delivered as a cloud service is based on three (3) primary tiers:

- An ***Author Tier*** where content management takes place
- A ***Preview Tier*** where content can be viewed and adjusted prior to publishing
- A ***Publish Tier*** where experiences are delivered and consumed

The ***Author Tier*** is comprised of two or more nodes within a single Author cluster, which scale automatically based on the volume of content management activity. The ***Preview Tier*** is comprised of a single preview node, which is used for quality assurance of content before publishing. The ***Publish Tier*** includes two or more nodes within a single Publish farm, each of which can operate independently. Each node consists of an AEM Publisher and a web server equipped with the AEM dispatcher module and scales automatically with site traffic requirements.

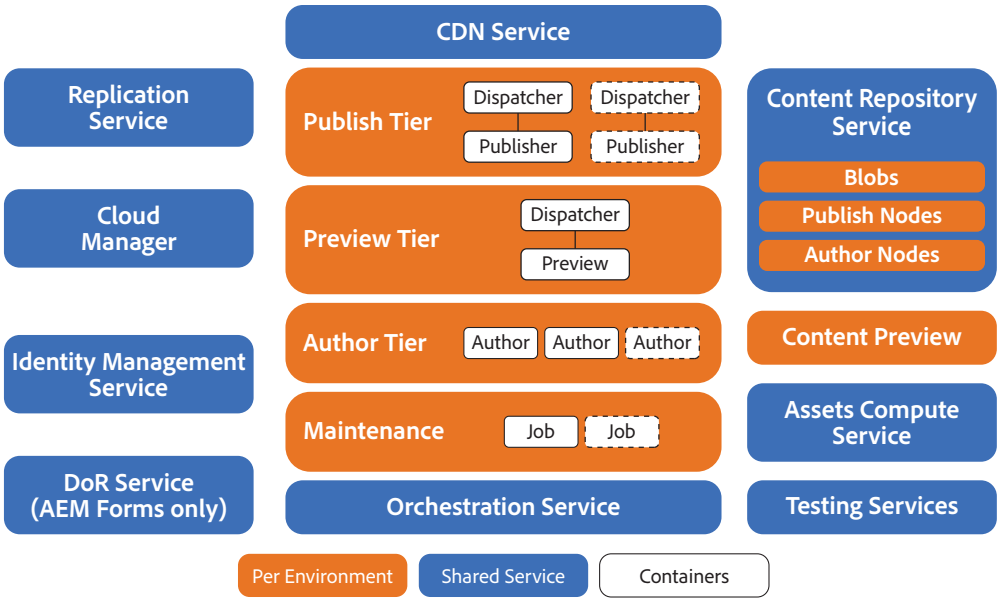


Figure 1: Adobe AEM as a Cloud Service Solution Architecture

AEM Sites, Assets, Forms, and Screens share a common underlying architecture and can each leverage additional related services, including:

- **Replication Service** — Manages the distribution of content from the Author Tier to the Publish Tier using a middleware pipeline. Individual Publish nodes subscribe to the content that has been pushed to the pipeline by Author nodes.
- **Content Delivery Network (CDN) Service** — Caches content and delivers it to site visitors and provides industry-leading traffic routing capabilities and network security.
- **Content Repository Service** — Provides a single, central repository for content created and published with AEM as a Cloud service. The Publish Tier only reads from the repository, while the Author Tier reads from as well as writes to it. BLOB storage, which hosts the actual files, is shared across both tiers.
- **Cloud Manager** — Allows customers to manage, monitor, maintain and troubleshoot the AEM as a Cloud Service through a Continuous Integration/Continuous Delivery (CI/CD) service made available via Cloud Manager. This includes code and configuration deployments using the Cloud Manager's CI/CD pipeline.
- **Adobe Identity Management Services (IMS)** — AEM as a Cloud Service uses Adobe Identity Management Services for authentication and supports legacy LDAP-compliant systems, SAML-compliant systems, and SSO.
- **Assets Compute Service** — Offloads ingestion and processing of content assets that are uploaded to AEM as a Cloud Service.
- **Document of Record Service** — Generates PDFs from the submitted forms for users to download.

- **Orchestration Service** — Helps with maintenance of the infrastructure and AEM instances, including auto-scaling and spinning up new instances as required.
- **Testing Services** — Automatically executes product functional tests during AEM as a Cloud Service deployment to validate that customer changes do not break core functionality. Customers are encouraged to supplement those tests with custom functional and UI tests. More information about creating and running custom tests is available online.

AEM as a Cloud Service Content Flow

AEM as a Cloud Service divides content management into four (4) distinct steps:

1. Developers configure the page templates to be used later for creating web content and web experiences. They develop the presentation templates for the main components using the Sightly open-source templating language;
2. Content authors log into the Author Tier and create web pages, content fragments, experience fragments, and adaptive HTML forms that are then stored in the AEM as a Cloud Service content repository;
3. Once the content is reviewed and approved in the Author Tier, as well as optionally published and previewed in the Preview Tier, it is then pushed to the Publish Tier to be included in the main web experiences;
4. Consumers and site visitors interact with the content in the form of web pages, HTML fragments, adaptive HTML forms, and APIs that can deliver content in a specific format for third-party applications (e.g., JSON). These content assets are delivered through a leading CDN provider that caches content to improve performance and delivers the content to site visitors.

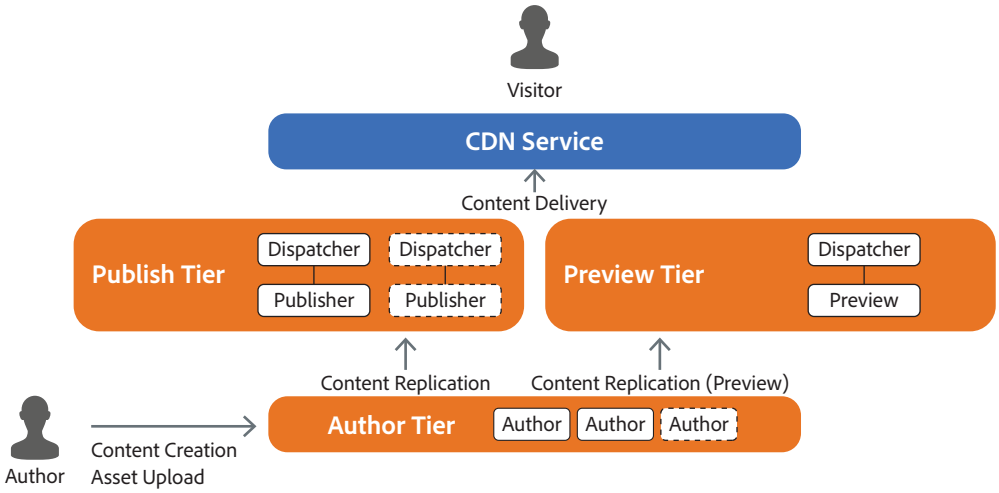


Figure 2: AEM as a Cloud Service Content Flow

For AEM Forms customers, users will also submit the form that will result in data coming back to the Publish Tier. A form submission could also result in a publish to Author Tier invocation of an API. This triggers workflows on an author.

AEM as a Cloud Service Application Deployment Model

When Adobe releases a new version of AEM as a Cloud Service or the customer updates an existing or releases a new version of their application, Cloud Manager creates a new build for the customer application and deploys it to both the Author and the Publish services.

To enable this functionality, Cloud Manager implements a deployment pipeline, which is coupled with each environment within an application. When a Cloud Manager pipeline is running, it creates a fresh version of the customer application by combining the latest customer packages with the latest baseline Adobe image. When the new application is built and tested, Cloud Manager automates the cutover to the latest version of the application, updating all service nodes using a rolling update pattern. Using this method, Adobe helps ensure no downtime for either the Author or the Publish service.

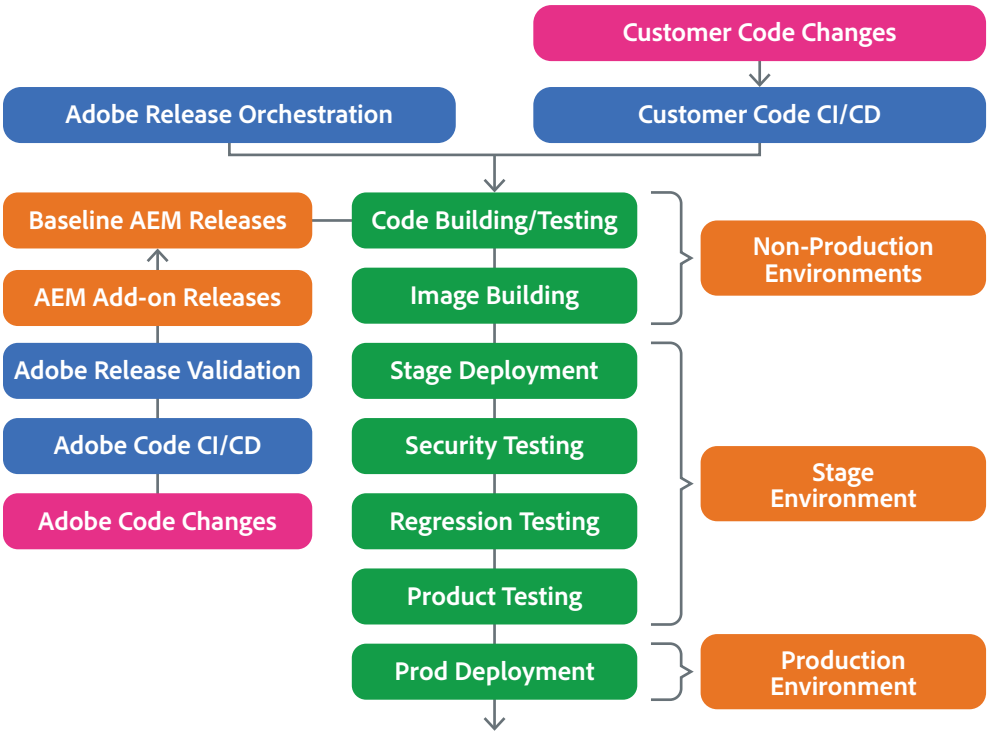


Figure 3: AEM as a Cloud Service Application Deployment Model

AEM as a Cloud Service Security Architecture

The AEM as a Cloud Service security model includes tenant- and node-level isolation for all services. Each AEM as a Cloud Service tenant exists within its own isolated namespace, including its own networking policies, computing, and storage.

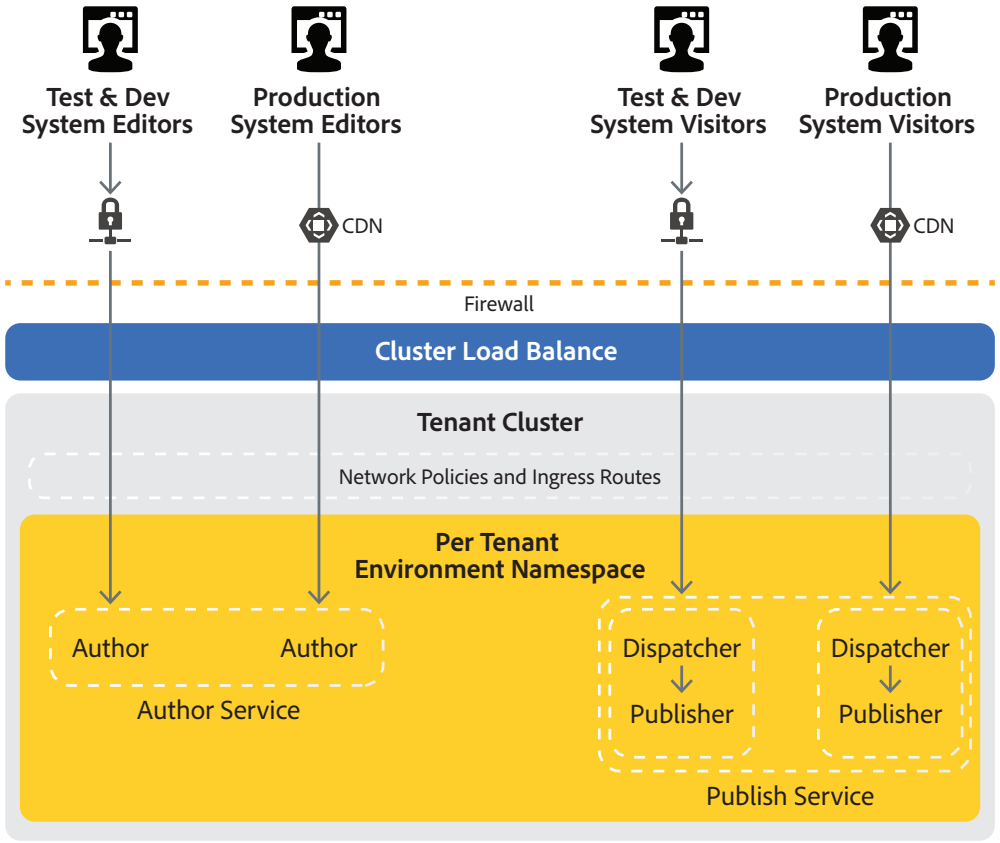


Figure 4: AEM as a Cloud Service Security Architecture

Data Encryption

All data in transit between AEM as a Cloud Service and external components is conducted over secure, encrypted connections using TLS 1.2. All data at-rest is encrypted by the cloud service provider. This includes any data that is transmitted upon submission of a form using AEM Forms.

In addition, AEM as a Cloud Service includes a FIPS-compliant crypto library and supports system-wide encryption keys, which can be used to encrypt any data in the AEM content repository, e.g., configurations and application data. Local user passwords are hashed using a configurable algorithm.

User Authentication

Access to AEM as a Cloud Service requires authentication with a username and password. Adobe continually works with our development teams to implement new protections based on evolving authentication standards. Users can access AEM as a Cloud Service in one of three (3) different types of user-named licensing:

Business ID is an Adobe-hosted, enterprise-managed option for organizations that either use email addresses outside of their own claimed domain as the user's ID or for customers that have not claimed a domain for identity purposes. Adobe Business ID is the preferred option for organizations that work with outside contractors or freelancers who do not have an organizational ID or email.

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 customer 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 AEM as a Cloud Service 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 customers' IT infrastructure. Adobe integrates with most any SAML2.0-compliant identity provider.

Enterprise IDs 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 IMS can be found in the Adobe Identity Management Services Security Overview.

AEM Roles and Permissions

AEM as a Cloud Service includes generalized use of Adobe IDs for accessing the Author Tier and therefore, the Adobe Admin Console, for managing users and user groups. Within the Admin Console, each environment is represented with one or multiple product context instances. Administrators are responsible for creating or importing the end-users' accounts in the Admin Console and assigning each user to one or multiple product context instances, giving them access to the associated AEM as a Cloud Service instance. Admins can also manage access for users with specific roles using product profiles in the Admin Console..

The Admin Console also enables admins to manage AEM environment access as a regular user or as an AEM administrator using profiles.

Once given access to AEM as a Cloud Service, user accounts can be leveraged in the same way as in the non-cloud-hosted version of AEM, including setting up roles and permissions. IUser privileges and AEM group memberships that are used to define the roles of users remain local to each particular instance of AEM as a Cloud Service.

Cloud Manager Security

Cloud Manager provides the first-generation of cloud-native functionality for Adobe Experience Manager. It includes features such as a continuous integration and continuous delivery (CI/CD) framework, flexible deployment modes, automated provisioning, API connectivity, and transparent service delivery that lets IT teams and implementation partners expedite the delivery of customizations or updates without compromising performance or security. For more information, please visit the Cloud Manager documentation online.

Git Repository

Adobe requires customers to check-in code to an Adobe-provided Git repository, powered by Azure DevOps. Customer separation is conducted within Azure DevOps, with each customer receiving a dedicated account. Validated and approved by Microsoft, this solution does not allow access between customer accounts.

Public API Security

Cloud Manager exposes a subset of its API to customers through an adobe.io endpoint (cloudmanager.adobe.io). This integration is done through the Adobe Developer Console and is available to all system administrator users and authorized developers with a valid product license.

Authentication

At the Adobe I/O Gateway level, checks are made to ensure that both a valid Adobe identity management service (IMS) access token and a valid profile exist. For the IMS access token, checks are made to ensure the signature is valid and that the token has not expired. For the profile, checks are made to ensure the service code and owning entity fields are valid. After the user is authenticated, each API validates that it has proper permissions. The permissions are based on roles, which corresponds to Product Profiles in the Admin Console.

For more information, please visit the Adobe Identity Management Services overview.

AEM as a Cloud Service Hosting

The AEM as a Cloud Service solution is hosted in the data centers of leading public cloud providers in the U.S. (Oregon & Virginia), Canada, Europe (London, Amsterdam, Frankfurt), Australia, Japan, and Singapore.

Figure 5 — Adobe AEM as a Cloud Service hosting locations

Segregated Client Data

User content is placed into separate databases. In some cases, more than one client may share a cloud cluster, but the content is segmented into separate databases. The only access to these servers and databases is via secure access by the AEM as a Cloud Service application.

Secure Network Routing

By default, inbound connections are only available on allowed ports, i.e., Port 443 for HTTPS, and outbound traffic is only allowed on HTTPS. Network Address Translation (NAT) masks the true IP address of a server from the client connecting to it.

Customers can optionally open additional outbound ports through which traffic passes through an encrypted tunnel before continuing to its destination. Customers can optionally egress traffic through a dedicated IP address, which is useful when customer infrastructure needs to limit the source of inbound connections. Learn more about dedicated egress IP addresses.

Customers may connect their own infrastructure to AEM as a Cloud Service through a VPN connection. Learn more about VPN support.

Load Balancers

The load balancers proxy incoming HTTPS connections and distribute requests that enable the network to handle momentary load spikes without service disruption. Adobe implements fully redundant load balancers, reducing the possibility that a single device failure can disrupt the flow of traffic.

AEM as a Cloud Service also offers reliable protection against (distributed) denial-of service (DDoS) attacks on three different levels:

- Edge filtering all non-HTTP/HTTPS traffic to block disruptive Layer 3 and Layer 4 attacks
- Protection against generic Layer 7 threats enforced by logic running on the CDNs cache nodes
- Additional Layer 7 filtering throughout the network stack to mitigate AEM specific attack vectors

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 6: 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.

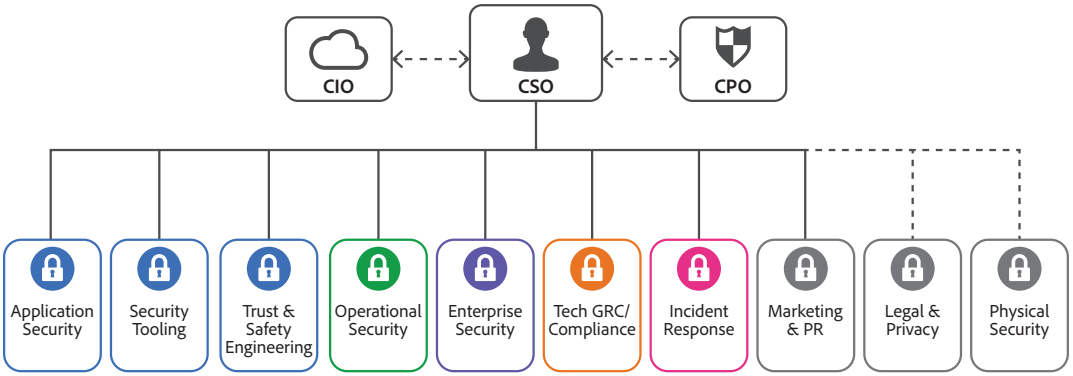


Figure 7: The Adobe Security Organization

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 recertification 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.

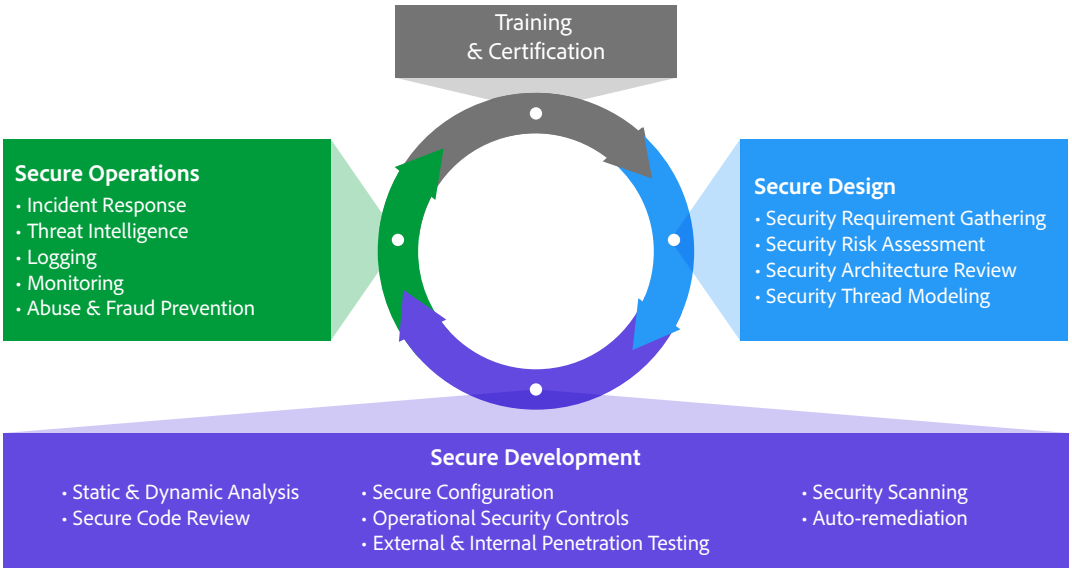


Figure 8: The Adobe Secure Product Lifecycle

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.

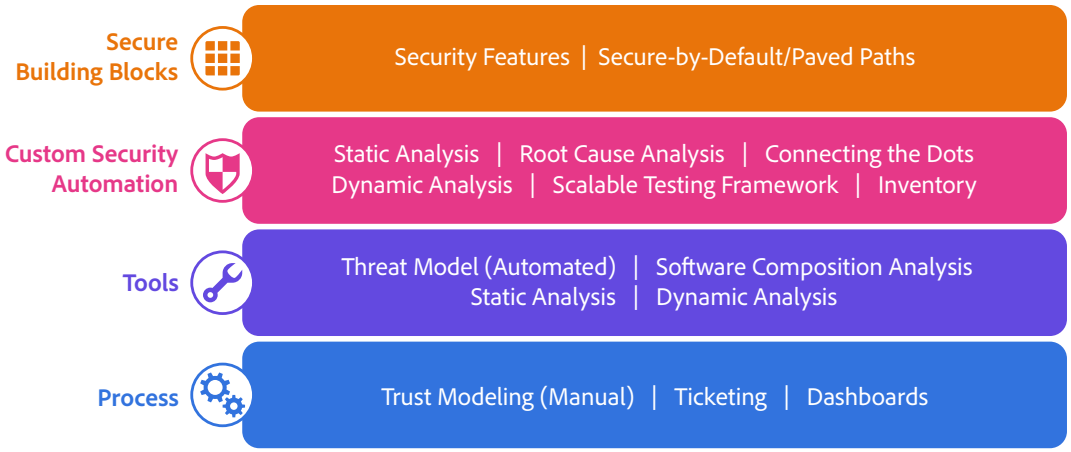


Figure 9: The Adobe Application Security Stack

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.

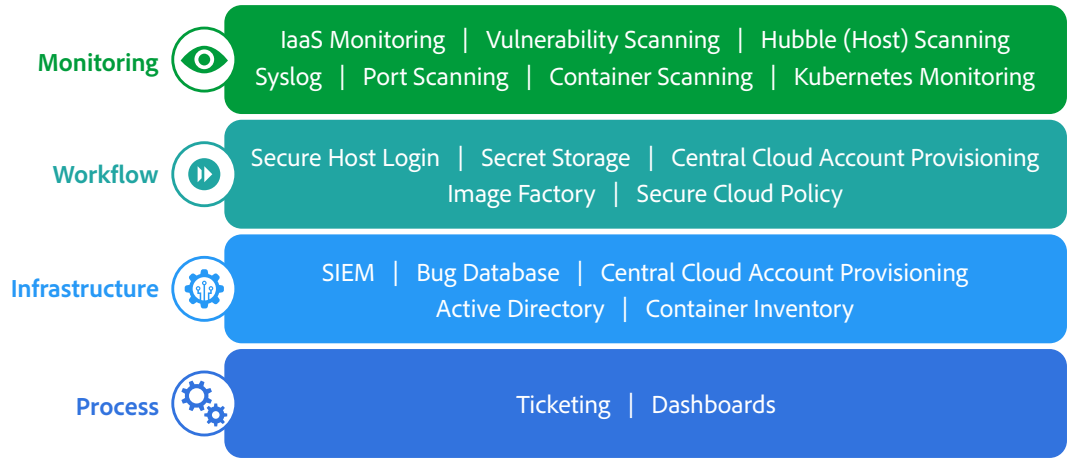


Figure 10: The Adobe Operational Security Stack

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.

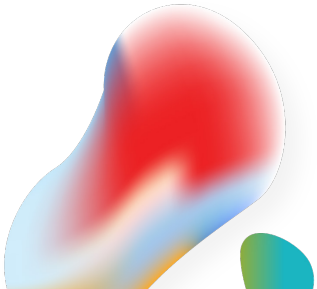
As much as possible, Adobe leverages leading-edge automation processes to alert teams to possible non-compliance situations and help ensure swift mitigation and realignment.

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 AEM as a Cloud Service solution 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 try to stay ahead of malicious activities and help ensure the secure our customers' data.

For more information about Adobe security, please visit the Adobe Trust Center.

Adobe