Adobe® Experience Manager 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 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 Experience Manager application and your data.

About Adobe Experience Manager as a Cloud Service

Adobe Experience Manager is a modern, cloud-native application that accelerates delivery of omni-channel personalized experiences throughout the customer journey. Informed by data insights, Experience Manager optimizes both marketer and developer workflows throughout the entire content lifecycle.

Adobe Experience Manager as Cloud Service consists of industry-leading cloud applications for hybrid content management (CMS) and digital asset management (DAM), each of which can scale up to help meet the demands of even the largest global corporations.

The modern cloud-native architecture of Experience Manager as a Cloud Service is built upon a container-based infrastructure offering API-driven development and a guided DevOps process. It allows IT to focus on strategic business outcomes instead of getting slowed down by operational concerns. This helps organizations achieve faster time to market while being flexible and extensible to meet unique business requirements.

With Experience Manager as a Cloud Service, your teams can focus on innovating instead of planning for product upgrades. New product features are thoroughly tested and delivered to your teams without any interruption so that they always have access to the state-of-the art application.

About Adobe's 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. This container platform provides core security functionality built-in to further strengthen applications built upon it. This platform also provides more flexibility in implementing stronger security and compliance controls on-the-fly without disrupting existing applications. This platform will serve as the foundation for future versions of Adobe's solutions helping to ensure that industry-standard security practices are built into everything we do.

Adobe Experience Manager: Cloud Service Solution Architecture

AEM as a Cloud Service includes two primary components:

- **AEM Sites**, Adobe's market leading Web Experience Management solution
- **AEM Assets,** Adobe's market leading Digital Asset Management solution

The architecture for AEM Sites and AEM Assets delivered as a cloud service is based on two primary tiers:

- An Author Tier where content management takes place, for AEM Sites and AEM Assets
- A Publish Tier where experiences are delivered and consumed, for AEM Sites

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 ***Publish Tier*** includes two or more nodes within a single Publish farm, which can operate independently from each other. Each node consists of an AEM publisher and a web server equipped with the AEM dispatcher module and scales automatically with site traffic requirements.

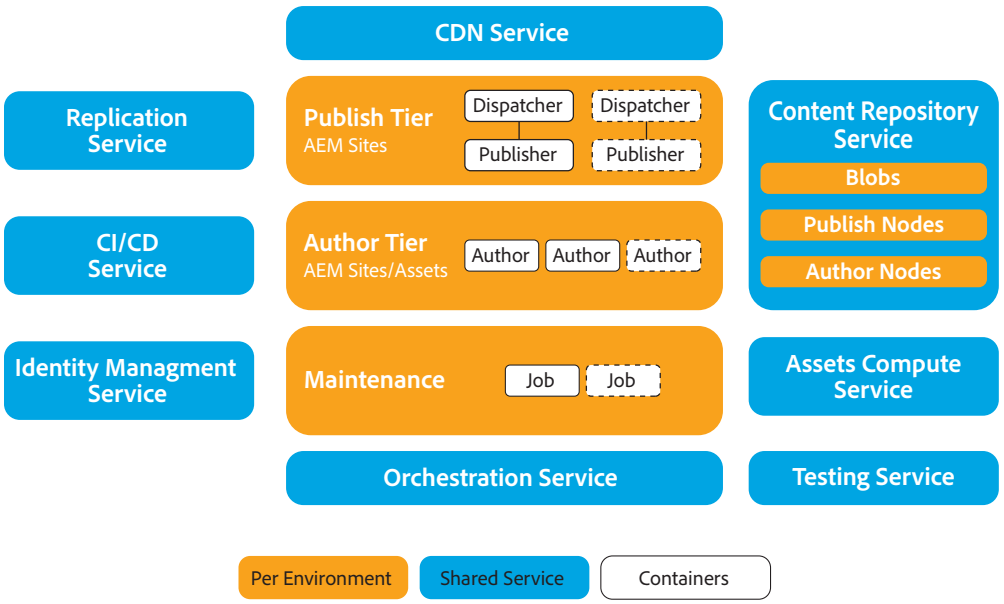

Figure 1: AEM as a Cloud Service Solution Architecture

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

- **Orchestration Service** — Helps with maintenance of the infrastructure and AEM instances, including auto-scaling and spinning up new instances as required.
- **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.
- **Cloud Manager** — Allows customers to self-provision AEM as a Cloud Service environments and instances as well to deploy application code and updates. Cloud Manager manages customer deployments as part of Programs that include a set of Non-Production and Production Environments (each of them hosting both the Author and Publish Tiers) with a common customer application codebase.
- **Continuous Integration (CI)/Continuous Delivery (CD) Service** — Enables developers and system administrators to manage the AEM Cloud Service application via Cloud Manager, including code and configuration deployments.

- **Adobe Identity Management Services (IMS)** — AEM as a Cloud Service uses Adobe Identity Management Services for authentication and also supports legacy LDAP-compliant systems, SAML-compliant systems, and SSO.
- **Content Delivery Network (CDN) Service** — Allows AEM as Cloud Service to cache content and deliver it to site visitors, along with 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.
- **Asset Compute Service** — Offloads ingestion and processing of content assets that are uploaded to AEM as a Cloud Service.

Adobe Experience Manager as a Cloud Service Content Flow

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

1. The 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. The content authors log into the Author Tier and create web pages, content fragments, experience fragments that get stored in the AEM as a Cloud Service content repository;
3. Once the content is previewed and approved in the Author 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, or APIs that can deliver content in a specific format for third-party applications (e.g., JSON)

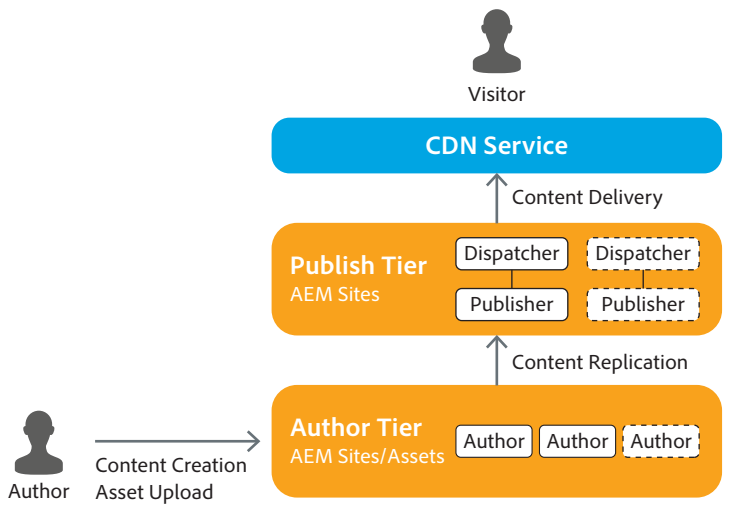

Figure 2: AEM as a Cloud Service Content Flow

Adobe Experience Manager 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

Cloud Manager implements a deployment pipeline to do this, 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.

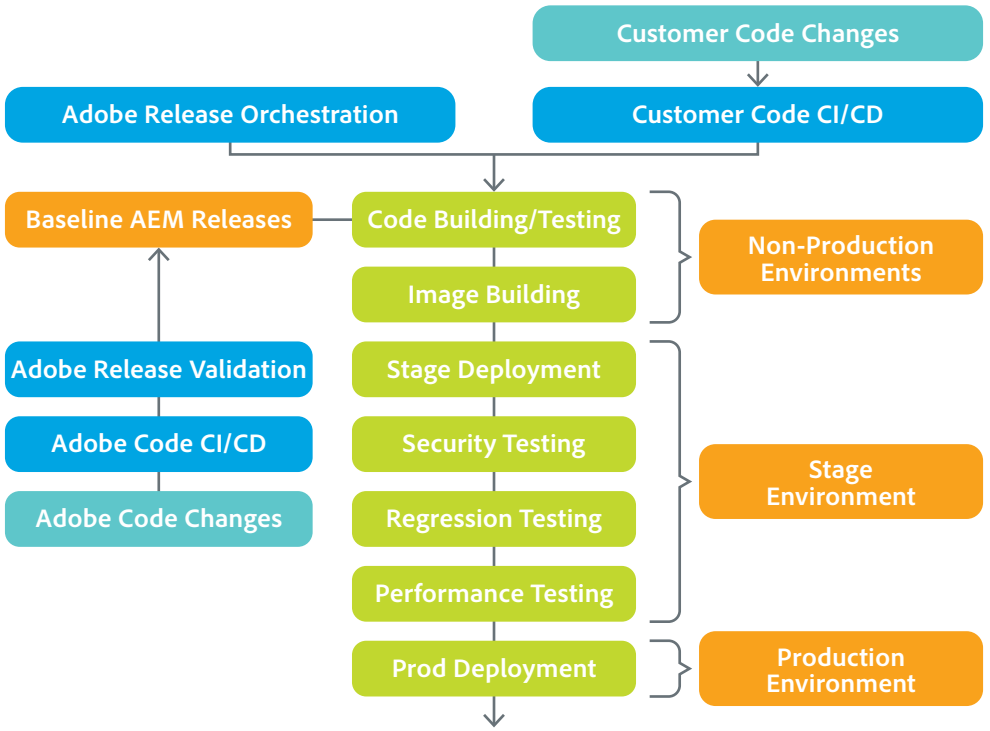

Figure 3: AEM as a Cloud Service Application Deployment Model

Adobe Experience Manager 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.

End consumers of content access AEM as a Cloud Service through a CDN that provides caching for better performance.

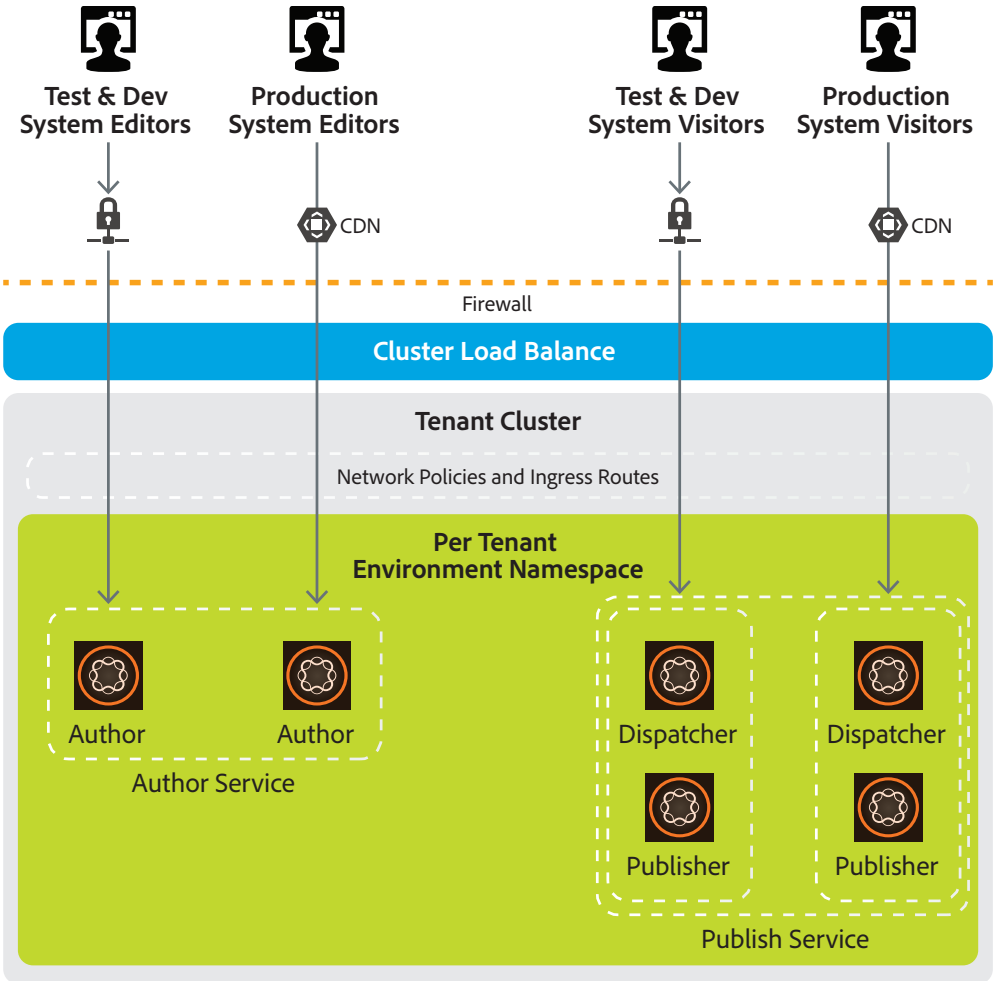

Figure 4: AEM as a Cloud Service Security Architecture

Data Encryption

All data in transit between AEM as a Cloud Service and external components is conducted over secure, encrypted connections using TLS. All data at-rest is encrypted by the cloud service provider

In addition, AEM includes a FIPS compliant crypto library and has support for a system-wide encryption key, which can be used to encrypt any data in the AEM content repository, e.g., configurations or any 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. We continually work with our development teams to implement new protections based on evolving authentication standards. Users can access AEM as a Cloud Service in one of two different types of user-named licensing:

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 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

One of the major updates in AEM as a Cloud Service is the 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, which gives them access to the associated AEM as a Cloud Service instance.

Once given access to AEM as a Cloud Service, the user accounts can be leveraged as in the non-cloud-hosted version of AEM, including setting up roles and permissions. In addition, all user profile information is centralized in Adobe IMS, but user 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.

Adobe Experience Manager as a Cloud Service Hosting and Security

The AEM as a Cloud Service solution is hosted on Adobe-leased data centers in the U.S, (Virginia) and in Amsterdam, The Netherlands and Sydney, Australia.

Figure 5 — Adobe AEM as a Cloud Service hosting locations

Adobe Experience Manager as a Cloud Service Network Management

We understand the importance of securing the data collection, data content serving and reporting activities over the AEM as a Cloud Service network. To this end, the network architecture implements industry best practices for security design, including segmentation of development and production environments and authenticated RBAC.

Segregating Client Data

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. All other access to the application and content 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 content in testing environments.

Secure Management

Adobe deploys dedicated network connections from our corporate offices to our data center facilities in order to enable secure management of the AEM as a Cloud Service. All management connections to the servers occur over encrypted TLS channels only accessible from the Adobe corporate network. All access requires two-factor authentication.

Firewalls (Secure Network Routing) and Load Balancers

Secure network routing is implemented, to only allow connections to allowed ports, i.e. Port 443 for HTTPS.

Outbound traffic is only allowed on HTTPS, NAT masks the true IP address of a server from the client connecting to it.

The load balancers proxy incoming HTTPS connections and also distribute requests that enable the network to handle momentary load spikes without service disruption. Adobe implements fully redundant firewalls and 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

See "DDoS mitigation" for more information about Edge filtering provided by the built-in CDN in AEM as a Cloud Service

Non-routable, Private Addressing

Adobe maintains all servers containing customer data on servers with non-routable IP addresses (RFC 1918). These private addresses, combined with NAT and internal network policies, prevent an individual server on the network from being directly addressed from the Internet, greatly reducing the potential vectors of attack.

Intrusion Detection

Adobe deploys Intrusion Detection System (IDS) sensors at critical points in the Adobe AEM network to detect and alert our security team to unauthorized attempts to access the network. The security team follows up on intrusion notifications by validating the alert and inspecting the AEM Cloud platform for any sign of compromise. Adobe regularly updates all sensors and monitors them for proper operation.

Service Monitoring

Adobe monitors all of our servers, routers, switches, load balancers, and other critical network equipment on the Adobe AEM network 24 hours a day, 7 days a week, 365 days a year (24x7x365). The Adobe Network Operations Center (NOC) receives notifications from the various monitoring systems and will immediately attempt to fix an issue or escalate the issue to the appropriate Adobe personnel. Additionally, Adobe contracts with multiple third parties to perform external monitoring.

In addition, AEM Cloud as a Service uses state of the art technologies and industry leading providers for application specific monitoring and alerting. SLIs and SLOs are constantly tracked and violations results in alerts with the right severity.

Data Backups

Adobe backs up customer data or AEM as a Cloud Service daily using snapshots. Each snapshot is stored up to seven (7) days. The combination of backup procedures provides quick recovery from short-term backup as well as off-site protection of data.

Change Management

Adobe uses a change management tool to schedule modifications, helping increase communication between teams that share resource dependencies and inform relevant parties of pending changes. In addition, Adobe uses the change management tool to schedule maintenance blackouts away from periods of high network traffic.

Patch Management

In order to automate patch distribution to host computers within the Adobe AEM organization, Adobe uses internal patch and package repositories as well as industry-standard patch and configuration management. Depending on the role of the host and the criticality of pending patches, Adobe distributes patches to hosts at deployment and on a regular patch schedule. If required, Adobe releases and deploys emergency patch releases on short notice.

For AEM as a Cloud Service instances, product updates, including security updates, are applied through the deployment pipeline (see above section on the deployment model for more details.

Access Controls

Only authorized users within the Adobe intranet or remote users who have completed the multi-factor authentication process to create a VPN connection can access administrative tools. In addition, Adobe logs all Adobe AEM production server connections for auditing. Our standard policy is to retain logs for one year. For AEM Cloud as a Service environments, Adobe makes built-in security features available to implement permissions and access control using groups and privileges.

Logging

In order to protect against unauthorized access and modification, Adobe captures and manages network logs, OS-related logs, and intrusion detections using industry-standard tools. Adobe periodically reviews log storage capacity and expands storage capacity if, and when, required. We harden all systems that generate logs and restrict access to logs and logging software to authorized Adobe Digital Marketing Information Security Team personnel. Adobe retains raw logs for one year and all logs are managed and accessed only by Adobe personnel. Customers can also retrieve AEM as a Cloud Service logs (e.g. access log, debug log) from Cloud Manager. These logs are maintained for the period agreed in your customer service agreement.

Disaster Recovery

AEM as a Cloud Service offers support for the following disaster scenarios:

Hardware failure

Handled by underlying Cloud Provider (e.g. Azure, AWS) and Container Orchestration (e.g. Kubernetes) infrastructure, i.e. each component is deployed across multiple physical nodes.

Data corruption

Synchronization of backups will be achieved by running an automated alignment procedure. AEM as a Cloud Service will allow to restore either at a snapshot (RPO) or point in time (PIT). RPO will restore the Author and Publish tiers at a backup timestamp. Point in time will restore the Author and Publish tiers to an arbitrary timestamp.

Customer code is hosted on the Cloud Provider's GIT repositories.

In-Region Protection

The Segment Store, Blob Store and Pipeline clusters are natively geo-redundant. Database snapshots of the Author tier node store are automatically replicated to the Cloud Provider's blob containers, which too, are geo-replicated to a secondary region. In case of failure of an entire Cloud Provider region, data loss or corruption in the main storage account, the backup storage account can be used to quickly restore the tenant environment.

Special Administrative Features

AEM as a Cloud Service provides capabilities for administrators to perform User Management and permission management in an AEM Environment.

In Admin Console, administrators can manage Cloud Manager access for users with specific roles using product profiles. They can also manage AEM environment access as a regular user or an AEM administrator using profiles.

Data Center Physical and Environmental Controls

The below description of data center physical and environmental access controls includes controls that are common to all Adobe data center locations. Some data centers may have additional controls to supplement those described in this document.

Physical Facility Security

Adobe physically secures all hardware in Adobe-owned or -leased hosting facilities against unauthorized access. All facilities that contain production servers for Adobe AEM include dedicated, 24-hour on-site security personnel and require these individuals to have valid credentials to enter the facility. Adobe requires PIN or badge credentials—and, in some cases, both—for authorized access to data centers. Only individuals on the approved access list can enter the facility. Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

Fire Suppression

All data center facilities must employ an air-sampling, fast-response smoke detector system that alerts facility personnel at the first sign of a fire. In addition, each facility must install a pre-action, dry-pipe sprinkler system with double interlock to ensure no water is released into a server area without the activation of a smoke detector and the presence of heat.

Controlled Environment

Every data center facility must include an environmentally controlled environment, including temperature humidity control and fluid detection. Adobe requires a completely redundant heating, ventilation, and air conditioning (HVAC) system and 24x7x365 facility teams to handle environmental issues promptly that might arise. If the environmental parameters move outside

those defined by Adobe, environmental monitors alert both Adobe and the facility's Network Operations Center (NOC).

Video Surveillance

All facilities that contain product servers for Adobe AEM must provide video surveillance to monitor entry and exit point access, at a minimum. Adobe asks that data center facilities also monitor physical access to equipment. Adobe may review video logs when issues or concerns arise in order to determine access.

Backup Power

Multiple power feeds from independent power distribution units help to ensure continuous power delivery at every Adobe-owned or Adobe-leased data center facility. Adobe also requires automatic transition from primary to backup power and that this transition occurs without service interruption. Adobe requires each data center facility to provide redundancy at every level, including generators and diesel fuel contracts. Additionally, each facility must conduct regular testing of its generators under load to ensure availability of equipment.

The Adobe Security Organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts under the Chief Security Officer (CSO). The office of the CSO coordinates all product and service security initiatives and the implementation of the Adobe Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams, including the Adobe AEM team. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.

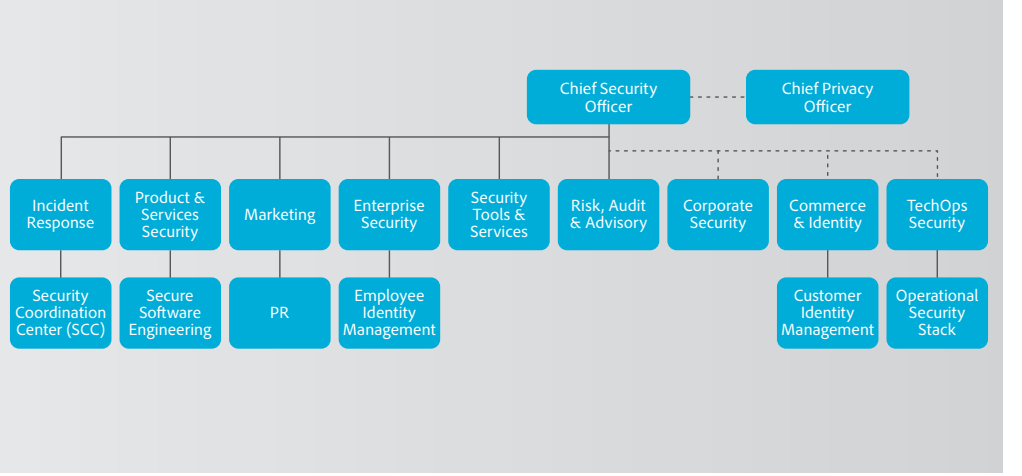

Figure 6: The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe AEM organization employs the Adobe Software Product Lifecycle (SPLC) process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe Secure Product Lifecycle

The Adobe SPLC activities include, depending on the specific Adobe AEM component, some or all of the following recommended best practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe AEM security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing

- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials

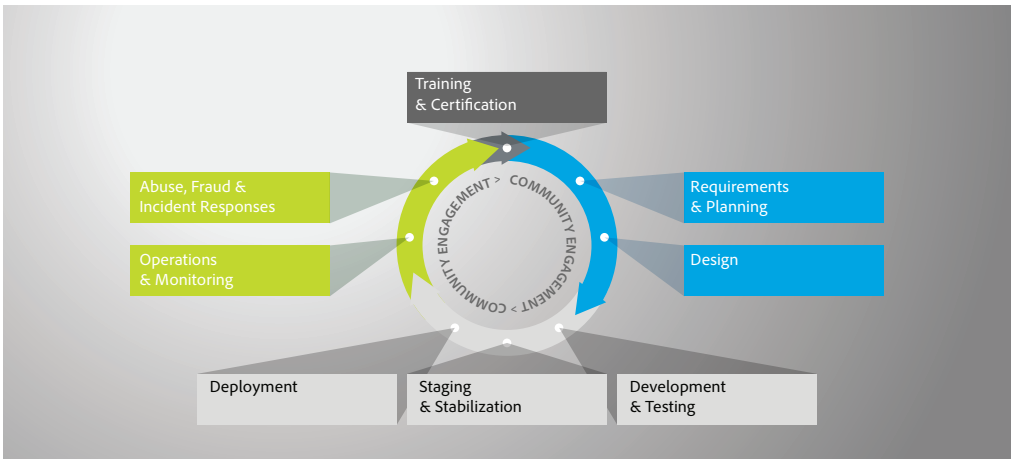

Figure 7: The Adobe Software Product Lifecycle (SPLC)

Adobe Software Security Certification Program

As part of the Adobe SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects.

The program has four levels, each designated by a colored 'belt': white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months- or year-long hands-on security projects. Employees attaining brown and black belts become security champions and experts within their product teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

Various teams within the Adobe AEM organization participate in additional security training and workshops to increase awareness of how security affects their specific roles within the organization and the company as a whole.

Adobe AEM as a Cloud Service Compliance

The Adobe Common Controls Framework (CCF) is 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. In creating the CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,000 requirements down to Adobe-specific controls that map to approximately a dozen industry standards.

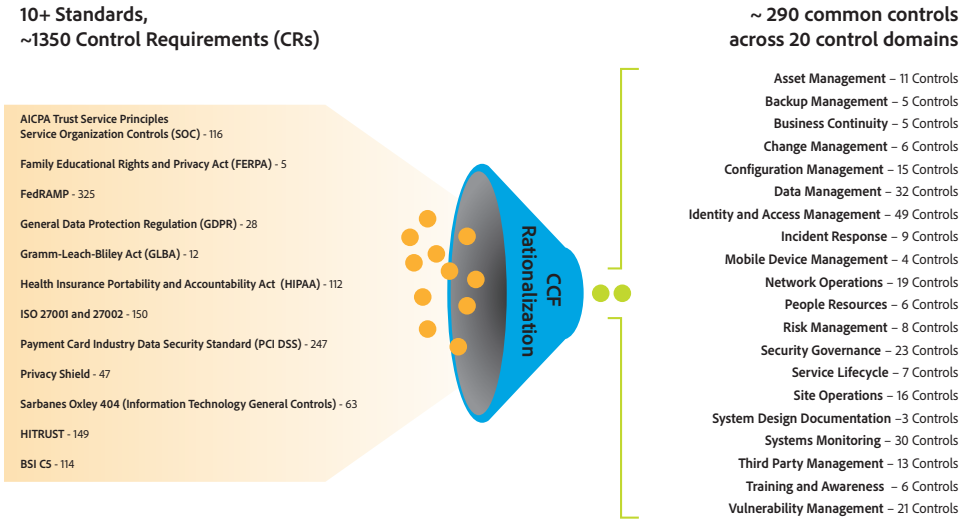

Figure 8: The Adobe Common Controls Framework (CCF)

Current Regulations and Compliance for Adobe AEM as a Cloud Service

For the most up-to-date information about AEM as a Cloud Service compliance, please see the Adobe Master Compliance List: https://www.adobe.com/content/dam/acom/en/security/pdfs/MasterComplianceList.pdf

Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

Adobe Risk & Vulnerability Management

Adobe strives to ensure that our risk and vulnerability management, incident response, mitigation, and resolution process is 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.

Penetration Testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe documents these vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan. Adobe conducts a full penetration test annually.

Penetration tests are conducted at least annually or after every major release. Vulnerability scans are performed monthly while web and database scans are performed quarterly.

Internally, the Adobe AEM security team performs a risk assessment of all Adobe AEM components quarterly and prior to every release. The AEM security team partners with technical operations and development leads to help ensure all high-risk vulnerabilities are mitigated prior to each release. For more information on Adobe penetration testing procedures, see the Adobe Secure Engineering Overview white paper.

Incident Response and Notification

New vulnerabilities and threats evolve each day and Adobe strives to respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT, Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Forensic Analysis

For incident investigations, the Adobe AEM team adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody record.

Adobe Corporate Locations

Adobe maintains offices around the world and implements the following processes and procedures company-wide to protect the company against security threats:

Physical Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge, and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus Protection

Adobe scans all inbound and outbound corporate email for known malware threats.

Adobe Employees

Adobe maintains employees and offices around the world and implements the following processes and procedures company-wide to protect the company against security threats:

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Adobe AEM, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

Background Checks

Adobe obtains background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background, work history, court records, including criminal conviction records and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Employee Termination

When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to

Adobe

Adobe
345 Park Avenue
San Jose, CA 95110-2704
USA
trust.adobe.com

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

www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.

© July 2020 Adobe. All rights reserved. Printed in the USA.

take specific actions leading up to the employee's last day. In the event Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, he or she can longer access to Adobe confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office and Datacenter Badge Invalidation
- Network Access Termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

Facility Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus Protection

Adobe scans all inbound and outbound corporate email for known malware threats.

Customer Data Confidentiality

Adobe always treats customer data as confidential. Adobe does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy.

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, please visit: http://www.adobe.com/security

Adobe

Adobe
345 Park Avenue
San Jose, CA 95110-2704
USA
trust.adobe.com

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

www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.

© July 2020 Adobe. All rights reserved. Printed in the USA.