Adobe Experience Cloud

WHITEPAPER

Adobe® Experience Manager as a Managed Service Security Overview

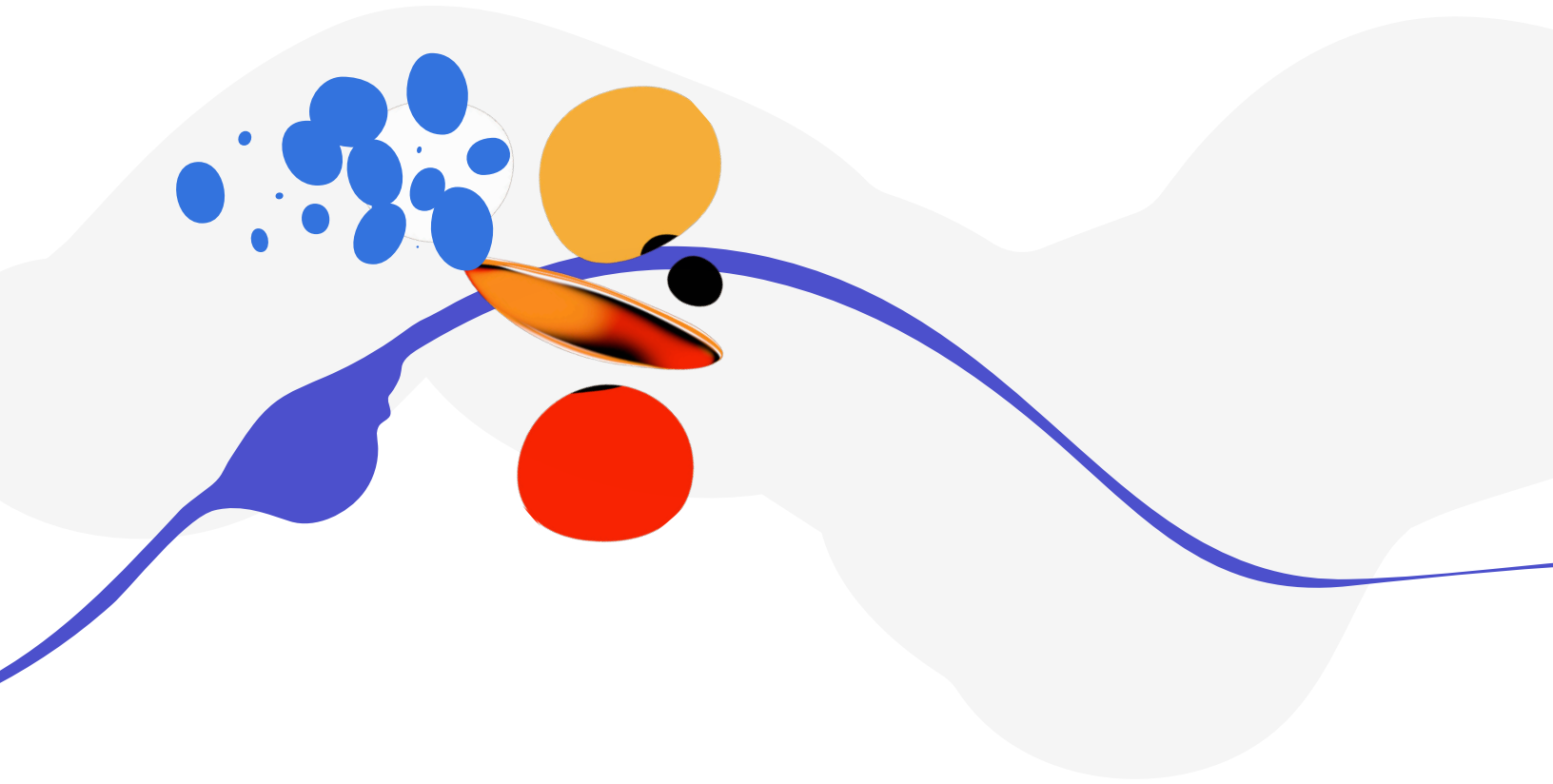

Table of Contents

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. These practices are strictly followed by our cross-functional teams 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. 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 Experience Manager as a Managed Service and its associated data.

About Adobe Experience Manager as a Managed Service

Adobe Experience Manager (AEM) is the industry-leading digital experience management solution for enterprises and midsize organizations. It provides a modern, scalable foundation to deliver compelling experiences that promote brand engagement, drive demand, and increase customer loyalty. Experience Manager includes a complete set of tools to create, manage, and deliver digital experiences across all channels. Built on the Java platform, AEM is powered by open-source standards and state-of-the-art frameworks and technologies, including the Java Content Repository (JCR) API, and a solid and structured REST architecture.

With Adobe Experience Manager as a Managed Service, the Adobe Experience Manager solution resides in a dedicated environment that is fully managed and supported by Adobe. Core infrastructure, such as web application hosting, redundancy, and storage, are enabled through Adobe-certified cloud service providers and managed by Adobe experts.

Adobe Experience Manager as a Managed Service Solution Architecture

AEM as a Managed Service includes four (4) primary solutions:

- 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 managed service is based on three (3) primary tiers:

- An Author Tier where content management takes place
- A Publish Tier where experiences are delivered and consumed
- A Web Server Tier where static content can be cached for faster delivery

The ***Author Tier*** is comprised of one or two nodes within a single Author cluster, which automatically fail over from the active to the passive Author node based on the availability of the active Author node. 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*** and scales automatically with site traffic requirements.

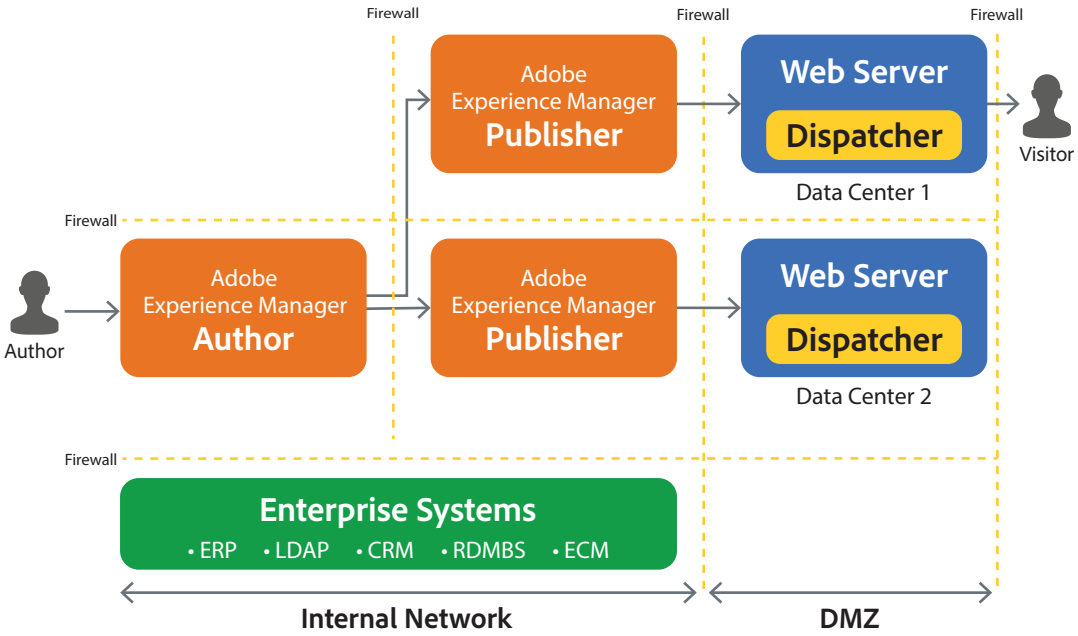

Figure 1: Adobe Experience Manager as a Managed Service Solution Architecture

AEM as a Managed Service Content Flow

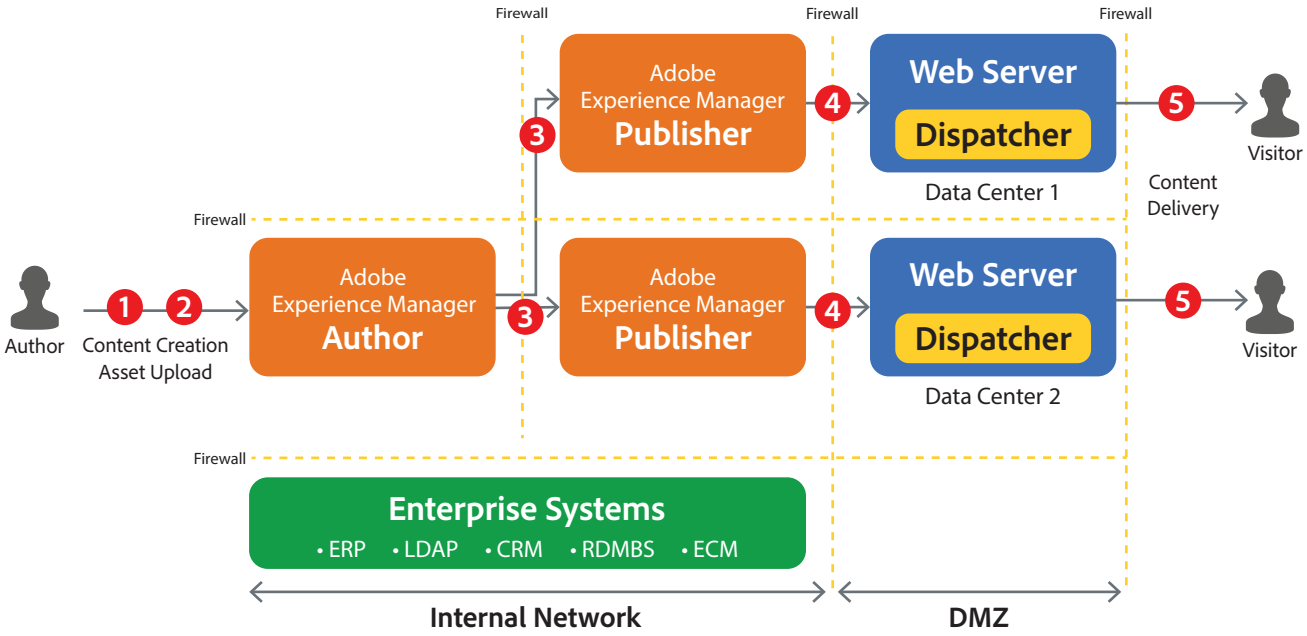

Figure 2: Adobe Experience Manager as a Managed Service Content Flow

The following narrative describes how content flows through the AEM as a Managed Service solution:

1. Developers configure the web page templates using the Sightly open-source templating language.
2. Content authors log into the Author user interface and create web pages, content fragments, experience fragments, and adaptive HTML forms that are then stored in the AEM as a Managed Service content repository.
3. After the content is reviewed and approved by the business requestor/s in the Author Tier, it is then pushed to the Publish Tier.
4. The Publish tier resolves the requests for dynamic content on any requested page. Static content is sent to the AEM Dispatcher to be cached. The AEM Dispatcher is also used to control access to all publicly exposed URL paths.
5. Consumers and other 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).

Data Encryption

All content is protected during upload using HTTPS TLS v1.2 or greater. The content remains protected and private on Adobe Experience Manager servers until the customer publishes the content, enabling consumers of the website to access it.

Cloud Manager

Customers can securely access and manage their cloud environment, including checking in, inspecting, and validating the security of new code and testing performance, using Cloud Manager. For more information about Cloud Manager for Adobe Managed Services (AMS) customers as well as the security and privacy controls in Cloud Manager, please see the Introduction to Cloud Manager.

User Authentication

Typically, customers choose to integrate Adobe Experience Manager into their existing enterprise identity management system. It supports legacy LDAP-compliant systems, SAML-compliant systems, SSO systems, and social integration via OAuth. Custom integrations are also possible.

LDAP Support

Adobe Experience Manager can leverage existing Lightweight Directory Access Protocol (LDAP) implementations, including Microsoft Active Directory, to authenticate user credentials. It also works with sophisticated authentication server deployments, such as synchronized, multi-server environments, to support massive scalability.

SAML Support for Federated Identity Management

Adobe Experience Manager is fully compatible with SAML (Security Assertion Markup Language) and can integrate with any SAML-compliant federated identity provider. SAML provides a standard XML representation for specifying the exchange of security information between a security system, such as an authentication authority, and an application that trusts the security system, and provides interoperable ways to exchange and obtain it. As such, SAML helps ensure the security of identity information between business partners, keeping federated identity cross-domain transactions more secure.

Adobe Experience Manager includes a SAML authentication handler that provides support for the SAML 2.0 Authentication Request Protocol including both Single Sign-On and Single Log-Out functionality.

SSO Authentication Handler

Adobe Experience Manager includes an SSO Authentication Handler service for organizations that do not implement LDAP or SAML but want to create a federated identity for their users. This service processes the authentication results provided by the trusted authenticator. Single Sign On (SSO) allows a user to access multiple systems after providing authentication credentials (such as a username and password) once. A separate system (known as the trusted authenticator) performs the authentication and provides Adobe Experience Manager with the user identity, generally in the form of an HTTP header. The SSO Authentication Handler can be used in concert with LDAP, if needed, or as part of a larger integration with bespoke identity management systems.

Social Integration via OAuth

The Social Login feature of Adobe Experience Manager enables organizations to provide a social login option on owned digital properties and then personalize the user experience based on profile information. Marketers can also combine social profile information with data from additional sources, such as a customer relationship management system or a website profile, to create a unified view of the customer.

Adobe Experience Manager includes built-in support for Social Login using Facebook and Twitter. This integration can be extended on a project basis to include other providers that support the OAuth standard. OAuth defines a framework for securing application access to protected resources, such as the identity attributes of a particular user. It allows an application that desires information to send an API query to a resource server hosting the desired information. The server can then authenticate that the client in fact sent the message.

Authentication in Single Sovereign Architecture

Adobe Managed Services Single Sovereign Architecture (SSA) deployments host the operational infrastructure that Adobe uses to manage the deployment in the same region as the deployment itself (e.g., customer is based in Australia, the tools are hosted in the same region). SSA enables a centralized authentication experience (delegated authentication) that allows users to log in to multiple applications with a single set of credentials. Compliant with SAML 2.0, delegated authentication in AEM as a Managed Service does not store or cache user credentials.

AEM as a Managed Service Hosting Locations

AEM as a Managed Service central servers are hosted in enterprise-class data centers from public cloud service providers in North America (US-West (California, Oregon, and Washington), US-East (Virginia), US-Central (Illinois), and Canada-Central (Toronto)), South America (Sao Paolo, Brazil), EMEA (Dubai, UAE; London, England; Paris, France; Frankfurt, Germany; Dublin, Ireland; Amsterdam, The Netherlands; Cape Town, South Africa; and Zurich, Switzerland) and Asia Pacific (Sydney, Australia; Beijing, China; Hong Kong; Mumbai, India; Indonesia; Tokyo, Japan; Seoul, South Korea; and Singapore).

Figure 3: Adobe Experience Manager as a Managed Service Hosting Locations

When a customer opts to deploy Adobe Experience Manager as a Managed Service, Adobe creates a single-tenant, virtual container to house the customer's instance of the solution. An Adobe Customer Success Engineer (CSE) works closely with the customer to configure the environment, including access control lists and port restrictions in Adobe Managed Services enterprise deployments. All components are hosted on a leading cloud service provider certified by Adobe. Core infrastructure, such as web application hosting, redundancy, and storage, is enabled through and supported by the cloud service provider.

Geographic Location of Customer Data

By default, all customer data is stored in cloud service provider regions within the country of customer operations. Data replication occurs within the regional cluster where the data is stored and is not replicated to data center clusters in other regions.

Segregation of Customer Data

Adobe utilizes strong tenant isolation security and control capabilities to maintain the segregation of its customers. Each AEM as a Managed Service instance is held in a single-tenant, virtual container, which isolates each customer from other customers. Adobe uses Identity and Access Management (IAM) tools provided by the cloud infrastructure provider to further restrict access to compute and storage instances.

Operational Responsibilities of Adobe Managed Services

Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and Adobe Experience Manager software, as well as the configuration of provided firewalls, and deployment of customer-developed code into production.

Secure Management

Adobe uses secure connections to manage and access customer instances. Multi-factor authentication (MFA) is required to connect to the cloud service provider.

Intrusion Detection

Adobe actively monitors both the AEM Content Producer Service and AEM Distribution Service using industry-standard Intrusion Detection Systems (IDS). Host-based Intrusion Detection Systems (HIDS) are also deployed on each production server for configuration file monitoring, virus and malware detection, and identification of root kits.

Logging

Adobe captures server-side logging of customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs do not contain username/password combinations, or other confidential information. A centralized SIEM solution is used to correlate and monitor the events logged. Only authorized Adobe technical support personnel, key engineers, and select developers can access the logs to diagnose specific issues that may arise.

Data Storage and Backup

By default, Adobe conducts a daily differential backup of all AEM data and retains this backup information for seven days. The unneeded backup files are deleted, purged from the system, and overwritten by the cloud service provider. This backup procedure can be adjusted, upon customer request, to cover virtually any frequency and retention period.

The backup creation snapshot process takes only a few seconds, during which time the repository is in read-only mode. This process typically occurs during minimum load hours and has minimal impact on normal system operation. The snapshot is then processed and distributed for availability in a second process that takes between 10 and 30 minutes.

Change Management

All changes to production instances of application sub-systems are controlled according to the requirements outlined in the Adobe Managed Services Configuration Management Plan. Only production systems are covered by this change control model; neither development/proof-of-concept or staging/pre-production systems are covered. Because management and control of customer instance changes are critical to meeting service-level agreement (SLA) commitments, the Adobe Managed Services Change Approval Board (CAB) must review and approve any change prior to implementation, including a technical assessment of the security impact of the proposed change. All qualifying changes are documented prior to implementation, including business justification, timeline, risks, and rollback procedures. Approval archives are maintained for the life of the customer engagement.

Patch Management

Adobe is responsible for patching its guest operating systems (OS), Adobe Experience Manager software, and applications running on provider infrastructure. New OS patches are being released every month and new AEM security patches are being delivered every quarter. Adobe also supplies a new, pre-hardened instance of the OS and application when requested.

Operational Responsibilities of Cloud Infrastructure Providers

Adobe-certified cloud service providers operate, manage, and control the components from the hypervisor virtualization layer down to the physical security of the facilities in which Adobe Experience Manager is deployed.

These providers also operate the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. This infrastructure includes facilities, network, and hardware, as well as operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources. Adobe requires these providers to adhere to industry-standard practices as well as a variety of security compliance standards.

Service Monitoring

Adobe cloud service providers monitor electrical, mechanical, and life support systems and equipment, and environmental states to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, our cloud providers are required to perform ongoing preventative maintenance.

Physical and Environmental Controls

Required physical and environmental controls are specifically outlined in a SOC Report. The following section outlines some of the security measures and controls in place at data centers of our cloud service providers around the world.

Physical Facility Security

Cloud service providers' data centers utilize industry-standard architectural and engineering approaches. These data centers are housed in nondescript facilities and the provider controls physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Only employees and contractors who have a legitimate business need for such privileges can access the data center and information contained within. When an employee no longer has a business need for these privileges, their access is immediately revoked, even if they continue to be an employee of the cloud service provider partner. All physical access to data centers is logged and routinely audited.

Fire Suppression

Cloud service providers provide automatic fire detection and suppression equipment in all data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Climate-Controlled Environment

Adobe cloud service providers employ a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. Data centers maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup Power

Data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Disaster Recovery

Adobe-certified data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built in clusters across several global regions, all data centers remain online 24/7/365 to serve customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Secure Network Architecture

Adobe requires cloud service providers to employ network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic. Adobe works with our cloud providers to enforce the most up-to-date ACLs.

Network Monitoring and Protection

A variety of automated monitoring systems are enabled by our cloud infrastructure providers to help ensure a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools provide significant protection against traditional network security issues, including:

- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet sniffing by other tenants

Data Storage and Backup

By default, Adobe stores all Adobe Experience Manager data using high-durability storage services provided by our cloud infrastructure partners. To help provide durability, PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in a provider region. In addition, providers calculate checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Change Management

Cloud service providers are responsible for authorizing, logging, testing, approving, and documenting routine, emergency, and configuration changes to existing infrastructure in accordance with industry norms for similar systems. Providers schedule updates to minimize any customer impact. Adobe maintains a Status Health Dashboard for Adobe Experience Manager, which can be accessed from the Adobe Experience Manager "Welcome" screen.

Patch Management

Adobe cloud infrastructure providers maintain responsibility for patching systems that support the delivery of IaaS services, such as the hypervisor and networking services.

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 4: Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

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

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

The Adobe Security Organization

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

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

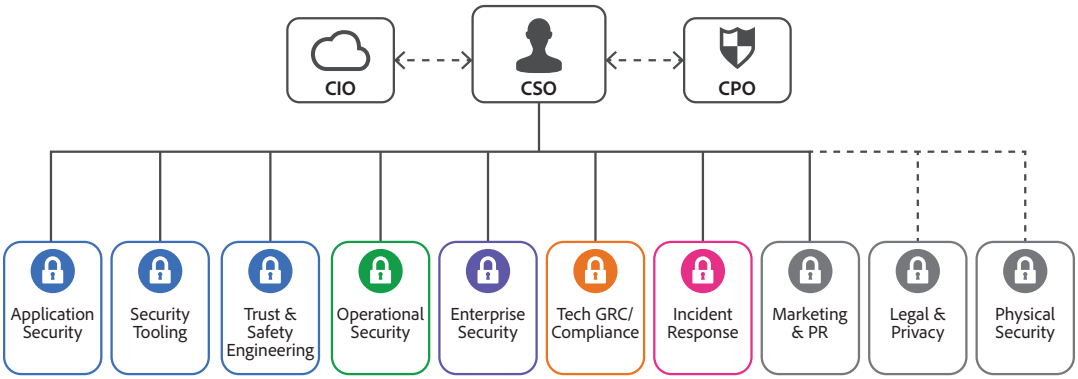

Figure 5: The Adobe Security Organization

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

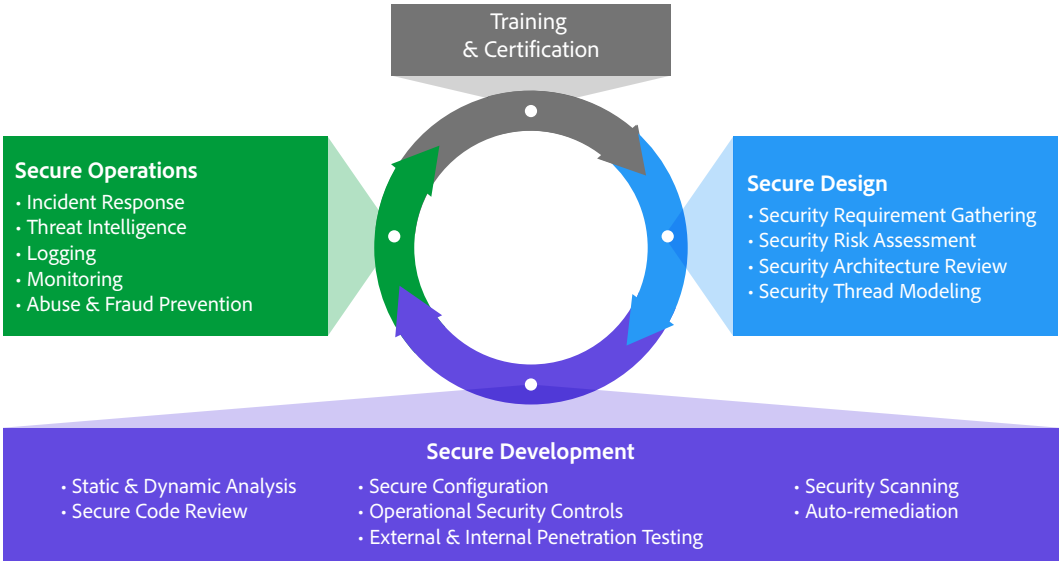

Figure 6: The Adobe Secure Product Lifecycle

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

Adobe Application Security

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

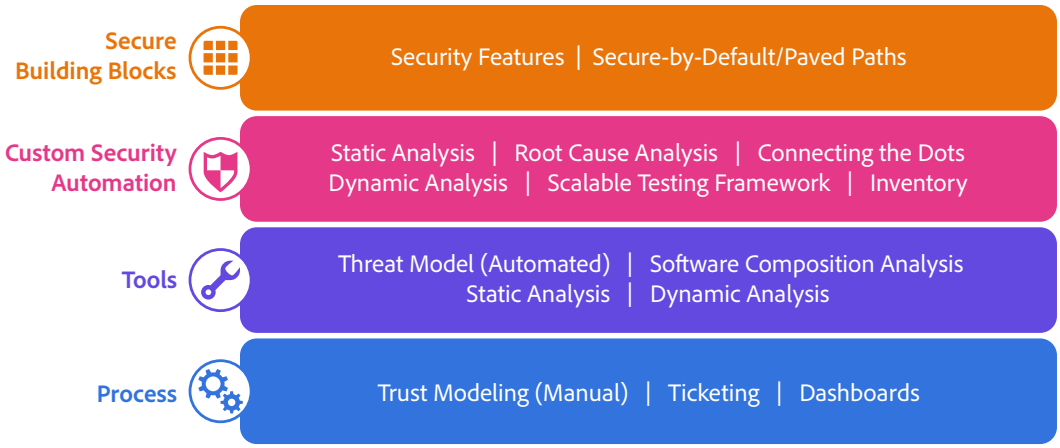

Figure 7: The Adobe Application Security Stack

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

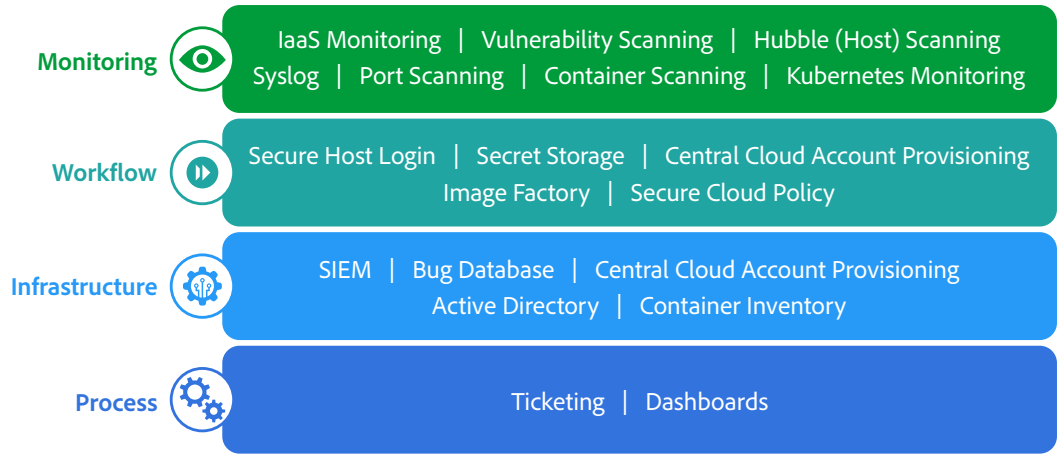

Figure 8: The Adobe Operational Security Stack

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 can be found in the Adobe Business Continuity and Disaster Recovery Program Overview.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Experience Manager as a Managed Service 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 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.