Adobe Creative Cloud

Adobe

WHITE PAPER

Creative Cloud for enterprise

Security Overview

Table of Contents

Executive Summary

At Adobe, we take the security of your digital assets seriously. From our rigorous integration of security into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What's more, our collaborative work with partners, researchers, and other industry organizations helps us understand the latest threats and security best practices as well as continually build security into the products and services we offer.

We built Adobe Creative Cloud for enterprise with security considerations at its core, and we utilize industry-standard software security methodologies for both development and management of the Creative Cloud for enterprise solution. From desktop and mobile apps to cloud services, your assets are protected, managed, and monitored by state-of-the-art security.

Adobe services that touch customer content have completed multiple standards certifications. Please see the Current List of Certifications, Standards, and Regulations for a detailed list of all compliance certifications and standards, as well as government regulations currently supported by Adobe products and solutions. For information on GDPR, please see the Adobe GDPR Readiness page.

This whitepaper describes the proactive approach, as well as procedures and security architecture, implemented by Adobe.

Creative Cloud for enterprise Overview

Creative Cloud for enterprise is a modern creative platform for businesses that want to design stand-out experiences across devices and customer touchpoints. With a collection of desktop and mobile apps, built-in templates, and cloud services, Creative Cloud for enterprise unlocks the content velocity required for today's digital transformation.

Desktop Applications

Packaged for deployment by IT via standard methods, such as Microsoft SCCM/JAMF Casper Suite, or utilized in a self-service scenario in which end-users download the apps directly from Adobe, Creative Cloud for enterprise desktop apps run on the end-user's desktop system. Each user is assigned a desktop application license via the Admin Console based on their identity (see Entitlement and Identity Management section below). When a user launches a Creative Cloud for enterprise app, such as Photoshop, the app communicates with Adobe Identity Services to determine if the user is entitled to use that application. Adobe encrypts all Creative Cloud data transmissions and handles user information by applying industry standards and best practices for security and privacy.

Mobile Apps

Adobe mobile apps run on users' mobile devices (including smartphones and tablets) and may be managed by a Mobile Device Management (MDM) solution. Content created by any of the mobile applications is stored both on the mobile device and in the cloud using encrypted storage (see the Cloud Services section below). Data transmissions are encrypted and access to the mobile services is determined by user identity as configured in the Admin Console. Adobe also leverages tooling to regularly scan and secure our mobile applications. This helps ensure they are following security best practices and properly leveraging the security controls provided by their underlying operating systems.

Cloud Services

Cloud services available in Adobe Creative Cloud for enterprise include a variety of productivity features that increase the efficiency of users. Using the Admin Console, administrators entitle users for Creative Cloud for enterprise services, including those that enable designers to access files, collaborate on projects, and leverage multiple fonts and stock images. Access to services is based on each user's unique identification, which means that only users entitled to a service may access it.

All data transmissions are encrypted and user generated content (UGC) is encrypted at-rest. As detailed in the *Dedicated Encryption Key* section below, both transmissions and UGC may be additionally encrypted with a dedicated encryption key.

Admin Console

The Adobe Admin Console is used to manage named user accounts as well as to configure license and service entitlements. It provides role-based access to Creative Cloud for enterprise apps and services and enables user management and entitlement access to Adobe Document Cloud, Adobe Marketing Cloud, and Print & Publishing applications. IT staff can also utilize the Admin Console to open support cases with Adobe Customer Care or schedule Expert Services sessions, so they can quickly resolve problems and issues.

Not only does the Admin Console integrate with any SAML 2.0-compliant enterprise identity management system for authentication, but it also works with the different ID types described in the *Entitlement and Identity Management* section below.

IT staff can set up product license groups to either mirror the enterprise directory groupings or create separate groups specifically tied into creative workgroups. Additionally, Adobe exposes a user management API that enables administrators to quickly configure license and service entitlements. The API also allows the admin to revoke all content access, if required.

If needed, the Admin Console can control a customer-specific, dedicated encryption key that encrypts all cloud content with a FIPS 140-2-compliant key utilizing envelope encryption. The Admin Console also allows administrators to view logs of all uploaded content as well as restrict the ability of end-users to share cloud content with anyone outside of the organization.

Administrators can download detailed reports, called content logs, from the Admin Console. These reports give information on how end-users are working with corporate assets. As end-users interact with the assets (e.g., create, update, etc.) the details are recorded in log files. Administrators can export these log files to track actions that users perform on the Creative Cloud assets owned by an organization. Logs can be generated for user activities that occurred in the past 90 days.

All communication with the Admin Console is encrypted using AES 128-bit GCM for symmetric key cryptographic block ciphers over TLS 1.2. Administrator access is limited to assigned users, which are set up and controlled by the customer.

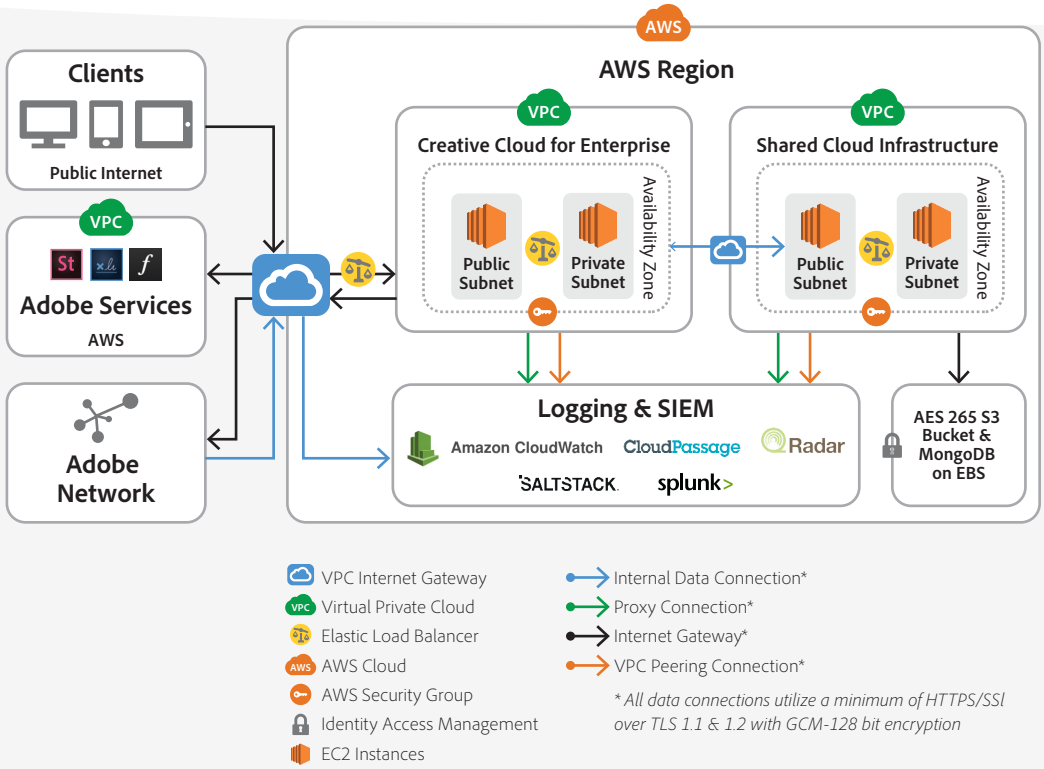
Enterprise Storage Management

Enterprise Storage Management (ESM) is an update to Adobe storage that provides users with more control, insight, and security over their Creative Cloud for enterprise accounts. Inaddition to pooling storage allocation at the organizational rather than the individual level, ESM also enables Creative Cloud for enterprise administrators to:

- Run per-user storage reports and generate alerts on a storage dashboard when a user exceeds their granted storage limit
- Reclaim assets by transferring one employee's cloud content to another employee
- Designate a storage administrator whose sole role is to handle storage administration tasks

Currently, ESM does not enable individuals to manage their own storage quota or provide a mechanism to entirely prohibit cloud data storage. In addition, whether you are using the enterprise storage (ESM) or user storage (USM) management model, all current compliance certifications apply to both configurations. More information about current compliance certifications can be found on the Adobe Trust Center.

Creative Cloud for enterprise Architecture and Data Flow



Creative Cloud for enterprise solution architecture

Creative Cloud for enterprise Architecture

Creative Cloud for enterprise leverages multi-tenant storage in which customer content is processed by an Amazon Elastic Compute Cloud (EC2) instance and stored on a combination of Amazon Simple Storage Service (S3) buckets and through a MongoDB instance on an Amazon Elastic Block Store (EBS).

Creative Cloud for enterprise is deployed regionally, as noted in the Data Center Locations and Your Data section below. Each region contains two VPC (Virtual Private Cloud) instances, a Creative Cloud for enterprise VPC and a Shared Cloud VPC. Both VPCs are logically isolated networks within an AWS region.

The Creative Cloud for enterprise VPC hosts the websites and APIs where end-users interact with the solution, and the Shared Cloud VPC hosts the services that perform common tasks across Creative Cloud for enterprise, such as storage.

In practice, availability zones exist as isolated locations within a region. However, from a network architecture perspective, they reside in a VPC. Physically, each availability zone has multiple different redundant data centers, enabling all data to be replicated across all data

centers as well as within multiple servers within each data center. This redundant backup ensures that Creative Cloud for enterprise customer data is safe from disasters, floods, power failures, etc.

Everything within each VPC is locked down by an AWS Security group, represented by orange keys in the chart above. A security group is another layer of security that allows Adobe to control the inbound and outbound traffic through the VPC, much like a virtual firewall.

The actual code within the VPC is housed in Amazon EC2 instances in specific subnets (or ranges of IP addresses). While public subnets are connected to the internet, private subnets are not and are only accessible through authenticated connections originating from the public subnet. This prevents an unauthorized user from connecting directly to the Creative Cloud for enterprise storage service, for example, and allows Adobe to make sure that only authorized users can perform certain actions, such as storing UGC.

UGC is stored in Amazon S3 buckets and the metadata about the content is stored in Amazon EBS via MongoDB. The UGC is then protected by Identity and Access Management (IAM) roles within that AWS region. Implementing per-user content security, IAM roles ensure that any content an end-user uploads to the cloud is considered private and is only accessible by that user, unless they take explicit steps to share it.

Content and assets stored in S3 are encrypted with AES 256-bit symmetric security keys that are unique to each customer and their claimed domain. The dedicated keys are managed by the Amazon Key Management Service (KMS), which provides additional layers of control and security for key management. Adobe automatically rotates the key on an annual basis. If necessary, IT administrators can revoke their key via the Admin Console, which will render all data encrypted with that key inaccessible to end-users. For more information, see the below section on dedicated encryption keys.

Metadata and support assets are stored in EBS using AES 256-bit encryption and Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms, both of which are consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations.

For more information on the underlying Amazon services, please see:

- MongoDB: http://www.mongodb.org
- Amazon S3 service: https://aws.amazon.com/s3/faqs
- Amazon KMS service: http://aws.amazon.com/kms/faqs/
- Amazon EC2 service: http://aws.amazon.com/ec2/

Data Center Locations and Your Data

User generated content is redundantly stored in multiple data centers within a region and on multiple devices in each data center. All network traffic undergoes systematic data verification and checksum calculations to prevent corruption and ensure integrity. Finally, stored content is synchronously and automatically replicated to other data center facilities within the customer's region so that data integrity is maintained even in the event of data loss in two locations.

UGC created using Creative Cloud for enterprise can be stored in the US (US-East VA), Europe (EMEA-West IE), or Japan (APAC-West JP) regions. An end-user's regional data store is determined when the user is created in the Adobe Admin Console and remains consistent throughout the user's lifetime. In other words, content created by a user account in the US will always be stored in the US data center, regardless of where the user is located when they upload the content.

Dedicated Encryption Key

As mentioned above, Adobe encrypts all UGC stored in Creative Cloud for enterprise at rest. For an additional layer of control and security, IT administrators can enable a dedicated encryption key for some or all the domains in the organization. Content is then encrypted using that dedicated encryption key which, if required, can be revoked from the Admin Console. Revoking the key will render all content encrypted with that key inaccessible to all end-users and will prevent both content upload and download until the encryption key is re-enabled.

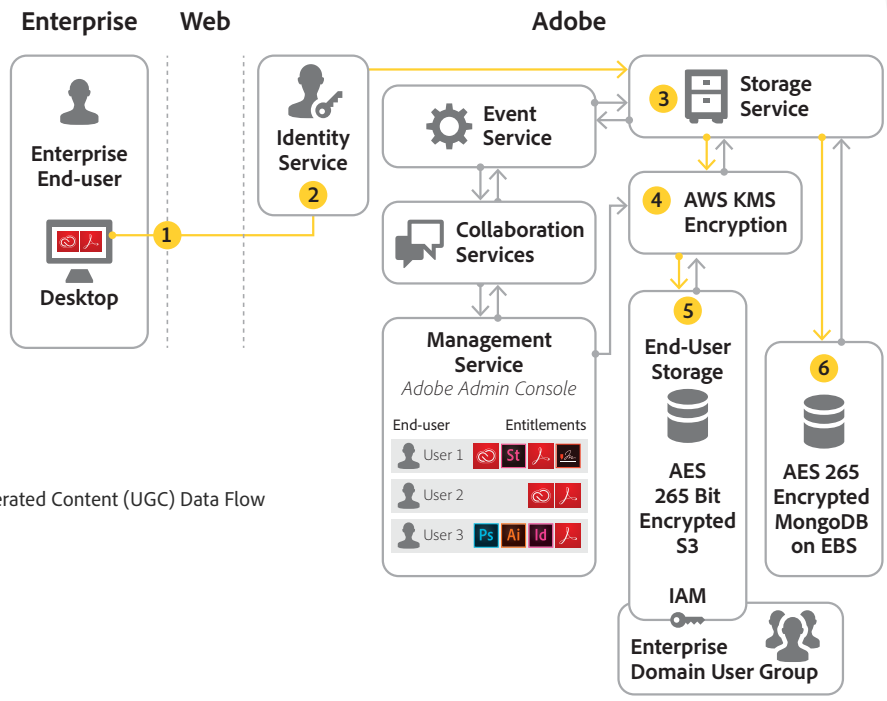
The key service employed utilizes FIPS 140-2 validated hardware security modules (HSMs) to protect key integrity and confidentiality. Plain-text keys are never written to disk and are only used in the HSM volatile memory on the server in the regional data store.

For more information on managing encryption using a dedicated key, please see:

- https://helpx.adobe.com/enterprise/help/encryption.html
- https://helpx.adobe.com/enterprise/help/encryption-faq.html

User Generated Content (UGC) Data Flow

1. End-users store the content they create in a Creative Cloud folder on their system's hard drive. If the user chooses to upload this content to cloud storage in Creative Cloud for enterprise, a background process uploads the UGC to the cloud. All UGC is encrypted in-transit using AES 128-bit GCM over TLS 1.2.
2. The Adobe Identity Service validates the user and their entitlements.
3. Adobe Creative Cloud for enterprise scans the content for viruses and sends the content to the AWS Key Management System (KMS) for encryption.
4. AWS KMS encrypts the user's content with the customer-managed encryption key. For more detail on KMS, go to http://aws.amazon.com/kms/faqs/.
5. Creative Cloud for enterprise stores the encrypted content in AES 256-bit Amazon S3 storage. In order to update or retrieve the content, the user must use Creative Cloud for enterprise; there are no external links to the content.
6. Metadata about the content is stored in MongoDB on an Amazon EBS using AES 256-bit encryption.



User Generated Content (UGC) Data Flow

Creative Cloud for enterprise Identity Systems

Entitlement and Identity Management

IT administrators entitle end-user access to Creative Cloud for enterprise desktop applications, such as Adobe Photoshop and Adobe Illustrator, as well as to cloud services, by utilizing named user licensing in the Adobe Admin Console. There are three (3) enterprise ID management options:

- **Adobe 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. With a Business ID, enterprises can separate users' business content from their personal content and can control and manage all business content created by the user (up to 2TB storage each).
- **Adobe Enterprise ID** is an Adobe-hosted, enterprise-managed option for organizations that use email addresses inside their own domain. The accounts are created and controlled by IT administrators from the customer enterprise organization, and the organization owns and manages both the user accounts and all associated assets. While a Business ID does not require a user to login with an email address from the organization's claimed domain, an Enterprise ID does.
- **Adobe Federated ID** is a Single-Sign-On (SSO) identity in which identity profiles are provided by the customer's identity management system. Federated IDs and associated assets are created, owned, and controlled by the customer's IT department. Adobe integrates with most any SAML 2.0-compliant identity provider. See the steps used to migrate to a customer identity provider at https://helpx.adobe.com/enterprise/using/set-up-identity.html

Application and service entitlement for any of the above methods is managed using the Adobe Admin Console.

Most enterprise organizations use Federated IDs for their employees and use Business IDs for their contractors and freelancers. You can learn more about each identity type at https://helpx.adobe.com/enterprise/help/identity.html.

Please visit the Adobe Trust Center for more information about Adobe's identity services.

Password Lockout Procedures

Organizations can enforce password policies for both Business IDs and Enterprise IDs with three (3) different password policies, shown here:

Password Requirements

Password Requirements:	Most Secure	More Secure	Easiest for Users
Minimum Number of Characters	✓ (8+)	✓ (8+)	✓ (8+)
Symbol & Number	✓ (1+ of both)	✓ (1+ of both)	✓ (1+ of both)
Lower & Upper Case Characters	✓	✓	✓
Cannot Match Previous Passwords	✓ (last 5)	✓ (last 5)	✓ (last 5)
Expiration	✓ (60 days)	✓ (90 days)	X

Creative Cloud for enterprise password policies

Both Business IDs and Enterprise IDs leverage the SHA-256 hash algorithm in combination with password salts and a large number of hash iterations. Adobe continually monitors accounts hosted on its infrastructure for unusual or anomalous account activity and evaluates this information to help quickly mitigate security threats. Conversely, Adobe does not manage user passwords for Federated ID accounts.

Account Management

IT departments can create, manage, and delete Business ID, Enterprise ID, and Federated ID accounts through the Adobe Admin Console. Cloud storage for these accounts is allocated as individual storage, which means IT staff does not have direct access to any files in the user's Creative Cloud for enterprise storage. However, IT staff may assume ownership for the employee's account and revoke access or, with ESM, remove a user and transfer their assets to another user.

Removing a user either involves removing entitlements for that user or completely deleting the user account. Removing the entitlements of a user with existing shared services storage renders any data in cloud storage inaccessible to that user and prohibits them from using the desktop applications, but it does not delete the user or their cloud content. Completely deleting a user removes that user from the Admin Console and deletes their data. A deleted user's data is erased from disk 14 days after their account is deleted.

Creative Cloud for enterprise Content Sharing and Collaboration

All Creative Cloud for enterprise content stored in the cloud is automatically labeled "Private," which means the content is only visible to the end-user who uploaded it. The user must take explicit actions to share content or it will remain private. Sharing in Creative Cloud for enterprise is accomplished in the following two ways:

Collaborate

Collaborated content remains private and the content owner must specifically invite named recipient/s to view or edit the content. Only the invited recipients can view the content and the collaborators must authenticate themselves to view it. If any collaborator changes the content, all collaborators can view the changes. Collaborated content in the cloud physically remains in the regional data center of the content owner—it is never relocated to a collaborator's regional storage.

A user can only be invited to collaborate on a Creative Cloud (CC) Folder, CC Library, or certain Cloud Documents. Individual pieces of content within a shared CC Folder or CC Library are accessible by the invited collaborator but CC Collaboration is at the folder or "group" level. Adobe Experience Design (XD) Prototypes and Design Specs are also enabled for CC Collaboration.

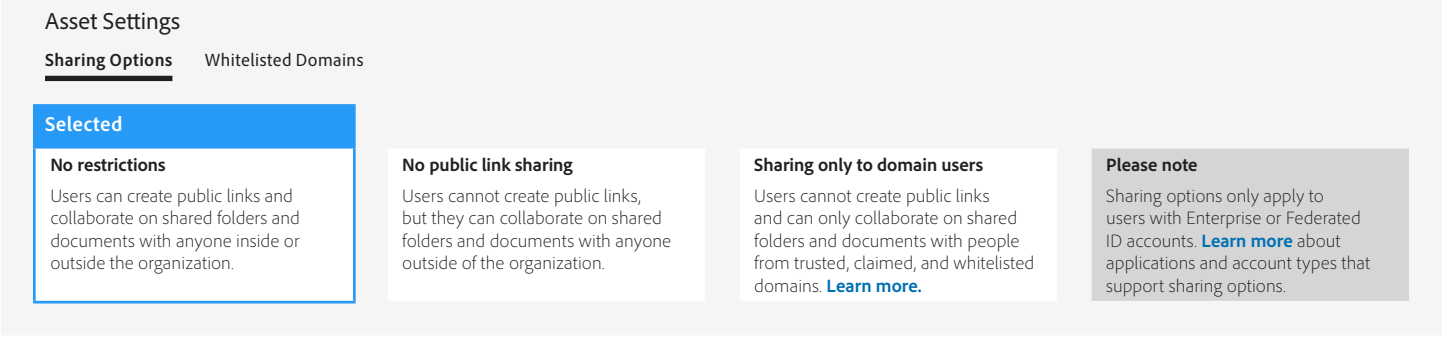
If a user wants to share an individual file or a mobile creation, they must use the "Send Link" function instead.

Send Link

Creative Cloud for enterprise also gives users the ability to share content with other users through the "Send Link" option. Unlike collaboration, sending a link creates a public link to the content and anyone with that link address can view the content. Linked content can be shared with the option to "Allow Download" or "Allow Save" which, if enabled, allow the recipient to download the content to either their desktop or their own Creative Cloud storage. In either case, the connection to the original content is broken and the recipient is now considered to be the owner of the content, with that content residing in the recipient's assigned data center. When sending a link to a CC Library, the "Allow Follow" option enables recipients to access a read-only view of the CC Library and receive any updates made by the owner. Unless downloaded as noted above, a "followed" CC Library will remain in the data center of the owner.

The ability to perform a Send Link on content can be controlled by the enterprise administrator using the **Asset Settings** feature in the Admin Console.

Asset Settings and Sharing Restrictions



Administrators can manage sharing restrictions for content stored in Creative Cloud for enterprise using the Asset Settings feature in the Admin Console.

Enterprise IT departments can turn off public link sharing and limit collaboration to the enterprise-claimed domain and any other whitelisted domains. Limiting collaboration

to claimed domains means that designers can only share content with other users within their organization; external sharing is completely disabled.

Access Request Policy

Administrators can also choose between two (2) access request policies:

- **Allow access requests** — The default setting, "Allow access requests," allows users to request access to folders or documents that have not been specifically shared with them. Users with sharing permissions on the asset receive notifications for each access request and can decide whether to grant access or not.
- **No access requests** — For added privacy, administrators can prevent users from being able to request access to a document that has not been specifically shared with them.

Hosting Services

All components of Creative Cloud for enterprise are currently on Amazon Web Services (AWS), including Amazon EC2 and Amazon S3, in the United States, the European Union (EU), and Asia Pacific. Amazon EC2 is a web service that provides automatically scalable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly reliable data storage infrastructure forstoring and retrieving any amount of data.

The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits. You can find additional information about AWS and Amazon's security controls on the AWS security site and can obtain a SOC 2 report by entering into an NDA with AWS.

Geographic Location of Customer Data on AWS Network

The following information is from the AWS: Overview of Security Processes White paper. For more details, please consult the AWS white paper.

Regardless of the geographic location of the customer, all Identity data is stored in multi-region, load-balanced, cloud infrastructure providers with data centers located in US-East (Virginia), US-West (Oregon), EU-West (Ireland), and Singapore. Content is backed up within each data center, in other data centers within the region, and in cross-region data centers for load balancing and redundancy. Adobe complies with applicable laws regarding cross-border data transfers, as outlined in greater detail at https://www.Adobe.com/privacy/eudatatransfers.html.

UGC uploaded to Creative Cloud for enterprise is generally stored in the AWS regional data center that corresponds to the country code associated with the user uploading the data, regardless of identity type:

- UGC for users with a North American, Central American or South American country code is stored in the AWS US-East 1 (Virginia) data center
- UGC for users with a European or African country code is stored in the AWS EU – West 1 (Dublin, Ireland) data center
- UGC for users with an Asia-Pacific or Middle Eastern country code is stored in the AWS — Asia Pacific Northeast 1 (Tokyo) data center

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.

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.

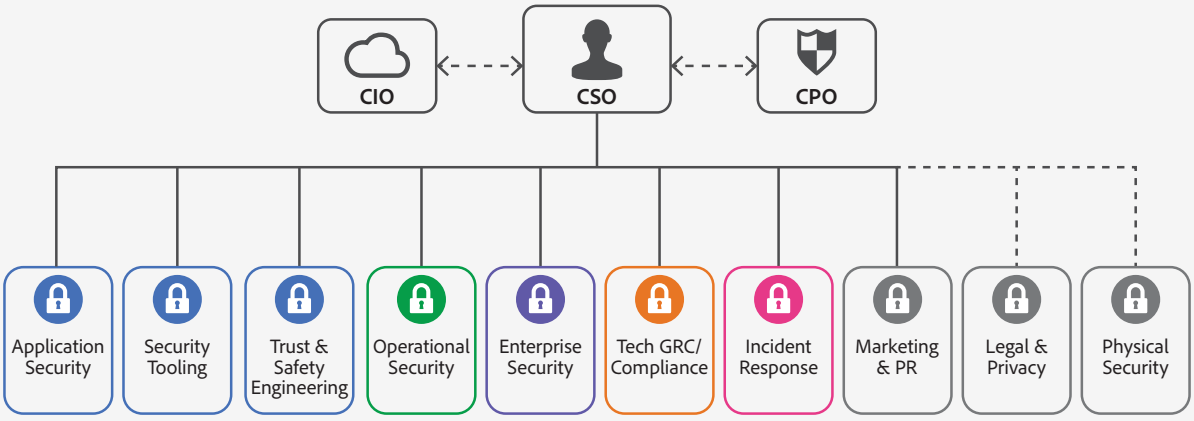
The Security Centers of Excellence

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.

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.

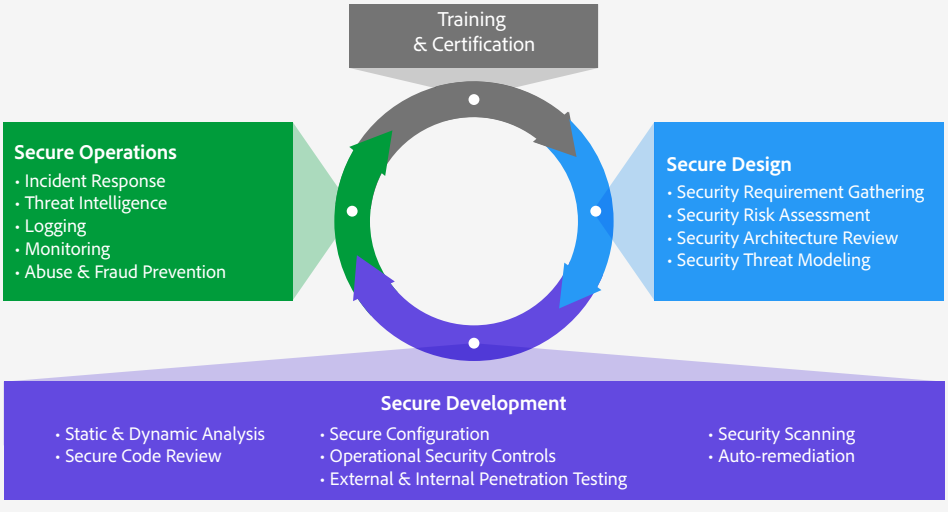


The Adobe Security Organization

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.

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.

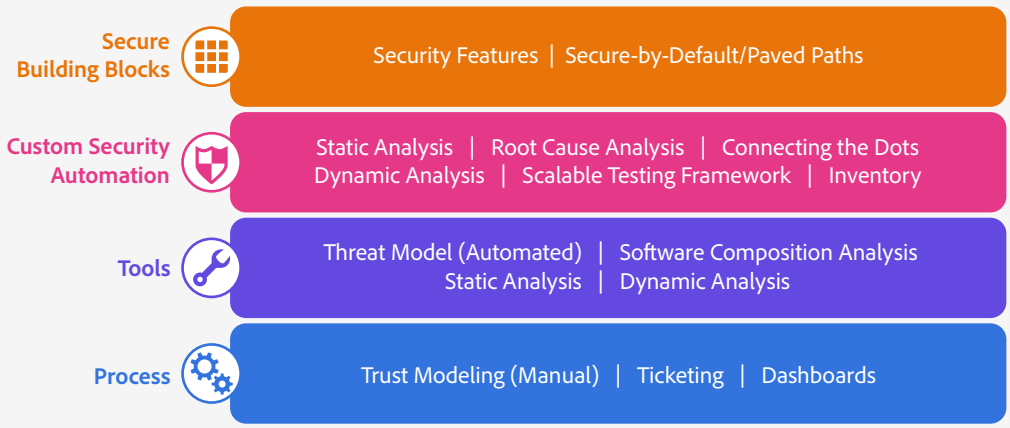


The Adobe Secure Product Lifecycle (SPLC)

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.

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.



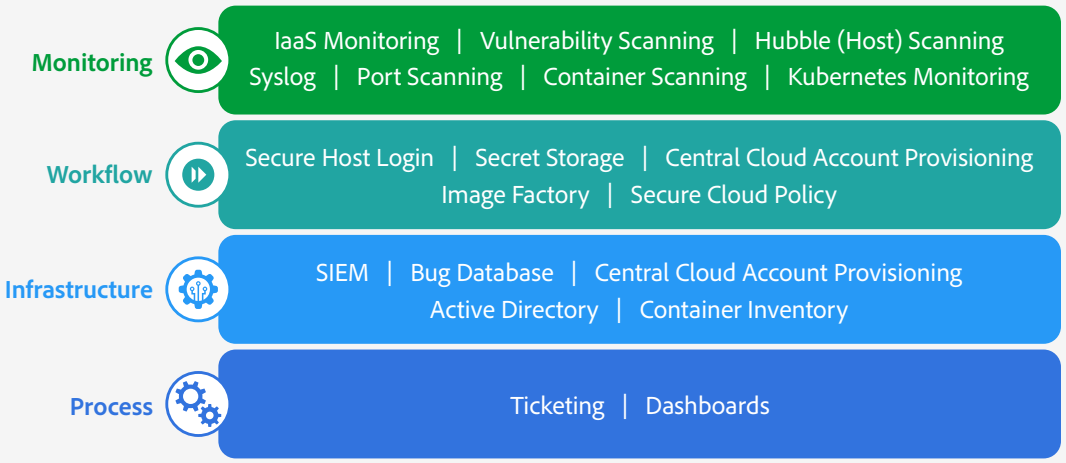
The Adobe Application Security Stack

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.

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.

The Adobe Operational Security Stack



Adobe Enterprise Security

In addition to securing our products and services as well as our cloud hosting operations, Adobe also employs a variety of internal security controls to help ensure the security of our internal networks and systems, physical corporate locations, employees, and our customers' data.

For more information on our enterprise security controls and standards we have developed for these controls, please see the Adobe Enterprise Security Overview.

Adobe Compliance

All Adobe products and services adhere to the Adobe Common Controls Framework (CCF), a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams. As much as possible, Adobe leverages leading-edge automation processes to alert teams to possible non-compliance situations and help ensure swift mitigation and realignment.

Adobe products and services either meet applicable legal standards or can be used in a way that enables customers to help meet their legal obligations related to the use of service providers. Customers maintain control over their documents, data, and workflows, and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU.

Adobe also maintains a compliance training and related standards that are available for review upon request. For more information on the Adobe CCF and key certifications, please see the Adobe Compliance, Certifications, and Standards List.

Incident Response

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution processes are nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help achieve the highest levels of security for all Adobe products and services.

We also maintain internal standards for incident response and vulnerability management that are available for view upon request. For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Business Continuity and Disaster Recovery

The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified BCDR Program enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information on the Adobe BCDR Program can be found here.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Adobe Creative Cloud for enterprise 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 the Adobe Trust Center.