Adobe Experience Cloud

WHITEPAPER

Adobe Commerce on Cloud Security Overview

Table of Contents

Adobe Security 3

About Adobe Commerce on Cloud 3

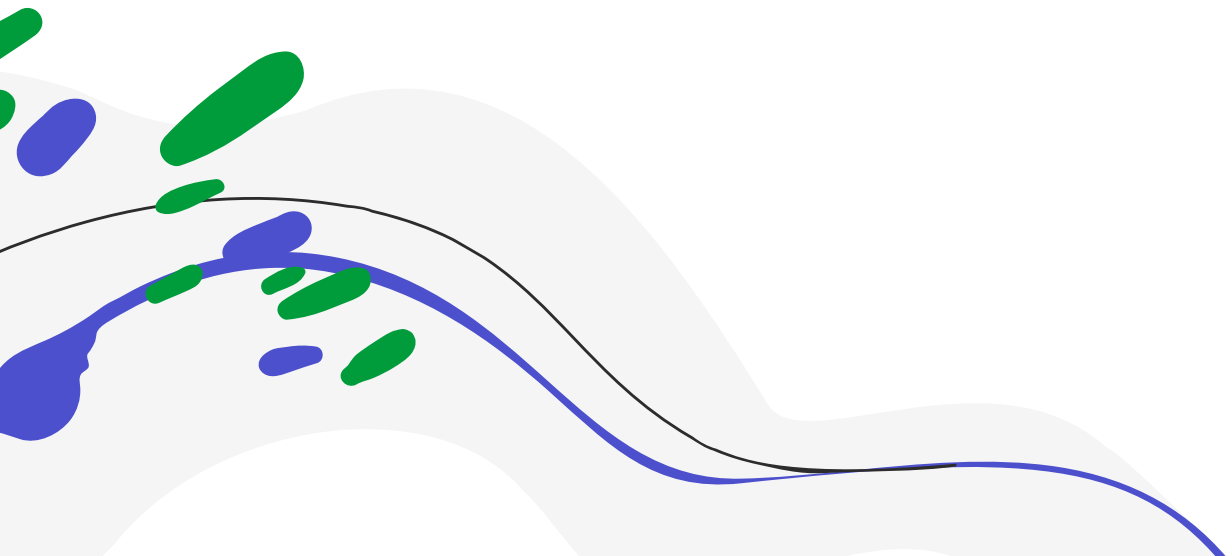
Adobe Commerce on Cloud Solution Architecture 3

Adobe Commerce on Cloud Data Flow and Security Architecture 5

Adobe Commerce on Cloud Hosting and Security 8

Adobe Security Program Overview 9

Conclusion 14



Adobe Security

At Adobe, we know the security of your digital experiences 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, and we regularly incorporate advanced security techniques into our products and services.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to secure Adobe® Commerce on Cloud and its associated data.

About Adobe Commerce on Cloud

Adobe Commerce on Cloud is a leading solution for digital commerce that supports B2C, B2B, and B2E use cases in a single platform. Built on an extensible architecture, Adobe Commerce on Cloud gives businesses of all sizes unmatched agility and scalability to go to market in highly differentiated ways. In addition, the tools and features included in Adobe Commerce on Cloud help enable companies to deliver personalized and unique shopping experiences to customers across all devices and digital touchpoints.

Adobe Commerce on Cloud Solution Architecture

The Adobe Commerce on Cloud solution includes the following ten (10) key functional services:

- **Product Catalog** — Contains the list of all products available for purchase online from the merchant.
- **Search and Navigate** — Allows potential customers to search for a specific product or products in an online store using keywords and then navigate to that product based on the search results.
- **Merchandising** — Helps merchants target a selection of products that are presented to the customer as related products, up-sells, and cross-sells, resulting in dynamic, targeted merchandising.

- **Cart and Checkout** — Enables merchants to customize the look and feel of the customer's shopping cart and automatically calculate the order total, along with discount coupons and estimated shipping and tax. Additional options for the checkout process include layout and placing constraints on checkout, such as allowing guest checkout and enforcing a terms and conditions agreement.
- **Account Management** — Helps merchants manage customer accounts, including analyzing and understanding purchase history to better discover trends and potential promotions based on customer attributes.
- **Pricing** — Enables merchants to price products using a variety of pricing options that can be used for promotions or to meet the minimum advertised pricing requirements of the manufacturer. Changes to product pricing can be made on schedule or by a price rule applied at the product level in the shopping cart.
- **Offers and Promotions** — Presents customers with special offers, promotions, and prices based on their specific attributes or assigned customer group.
- **Customer Profil**e — Includes information about customer activity, such as when the customer last signed in or out of their account, addresses, order statistics, recent orders, shopping cart contents, product reviews, newsletter subscriptions, and more.
- **Content Management and Page Builder** — Enables merchants to store, update, revise, and delete store and product content in the Adobe content management system (CMS) and push these changes to web pages in the online store.
- **Order Management** — Defines the order workflow and how to process orders, create invoices, and manage shipments.

Adobe Commerce on Cloud also includes:

- **Open GraphQL APIs** — Expose each of the core Adobe Commerce on Cloud services to a wide variety of end-customer applications; and
- **REST APIs** — Allow asynchronous syndication and bulk import/export of data between Adobe Commerce on Cloud and back-office systems of record, such as ERP, CRM, DAM, and pricing solutions.
- **Content Delivery Network (CDN)** — Adobe contracts with a leading CDN provider to optimize content flow between users and the Adobe Commerce on Cloud environment. The CDN includes a built-in web application firewall (WAF), which can be configured to scan and block malicious requests and/or traffic.

Adobe also offers Payment Services for Adobe Commerce as an optional add-on. For more information on this option, please see Adobe Experience League.

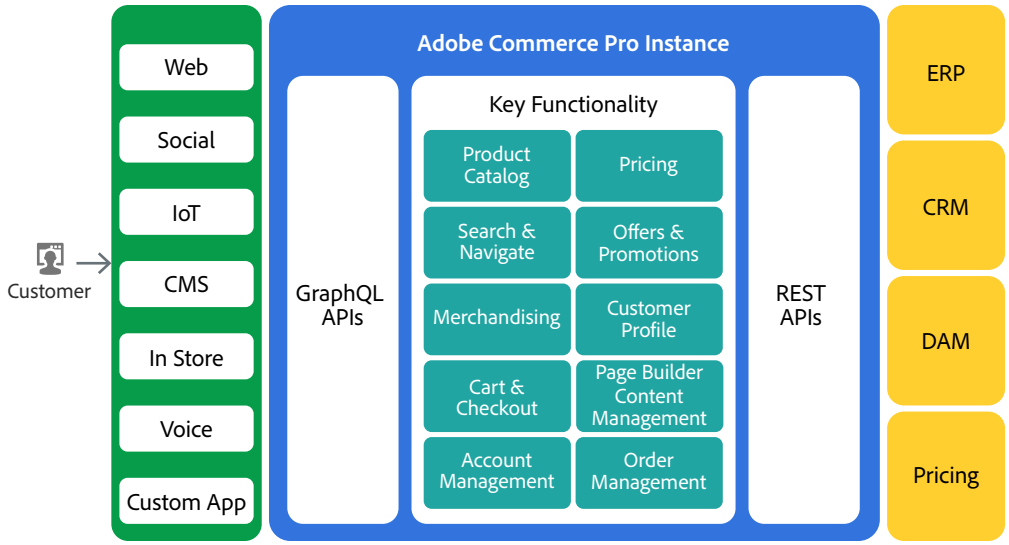


Figure 1: Adobe Commerce on Cloud Solution Architecture

Adobe Commerce on Cloud is built on a redundant architecture that includes three (3) separate instances of the environment for development, staging, and production. More detailed information about the solution architecture is available on Adobe Experience League.

Adobe Commerce on Cloud Data Flow and Security Architecture

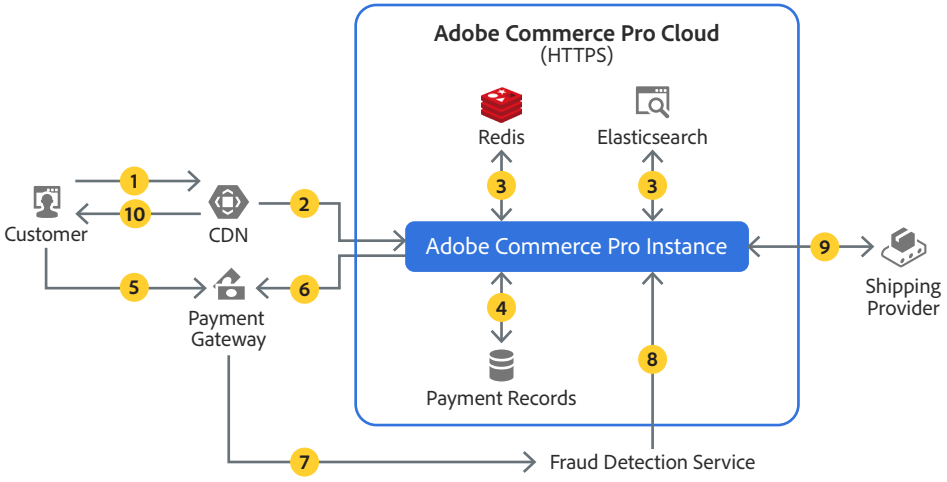


Figure 2: Adobe Commerce on Cloud Data Flow

Data Flow Narrative

The following narrative explains how data flows through the Adobe Commerce on Cloud solution:

1. The customer types in the URL of the online store (powered by Adobe Commerce on Cloud) they wish to visit in their web browser. The request is received by the CDN.
2. If the site URL is cached, the CDN simply returns it to the customer. If it is not cached, the CDN forwards the customer's request to the website via HTTPS. The Adobe Commerce on Cloud instance processes the request and serves the web page via HTTPS to the customer.
3. If needed, the Adobe Commerce on Cloud instance retrieves cached product information from Elasticsearch and cached configuration information from Redis.
4. Depending on the operation the customer wishes to complete (e.g., find product information, add a product to cart, submit payment information, etc.), Adobe Commerce on Cloud may access the database to retrieve or store information pertaining to the request.
5. If the operation is part of the checkout process, the customer selects their preferred payment option[1] and is redirected to the payment solution provider's site to enter payment information, including credit card number or bank routing information.
6. During payment processing, Adobe Commerce on Cloud may verify payment success with the payment gateway.
7. If configured, the payment gateway will interface with a fraud detection service to verify payment authenticity.
8. If the payment is determined to be fraudulent or suspicious, the fraud detection service will inform Adobe Commerce on Cloud instance for appropriate action to be taken.
9. The shipping provider will work with the Adobe Commerce on Cloud instance throughout the process to provide pricing, tracking numbers, and status updates.
10. Once payment is confirmed, the customer is redirected back to the Adobe Commerce on Cloud-powered store and receives a confirmation of their order.

Data Encryption

All inbound traffic from the user to Adobe Commerce on Cloud is secured using HTTPS, either using a TLS certification included with the Adobe Commerce on Cloud solution (and hosted on the CDN) or using the merchant's own TLS certificate.[2]

[1] Adobe Commerce on Cloud includes pre-built integrations for several third-party online payment solutions and gateways. More information on these integrations is available on Adobe Experience League.
[2] If the merchant chooses the latter option, the acquisition and management of this certificate to support HTTPS traffic is the merchant's responsibility.

Adobe Commerce on Cloud employs strong encryption as defined by PCI DSS 3.2.1 to encrypt documents and assets at rest with ChaCha20-Poly1305 256-bit encryption and HTTPS TLS v1.2 to protect data in transit.

Outbound traffic from Adobe Commerce on Cloud to the user is re-encrypted after communications are processed by the CDN. The CDN supports SHA-256 certificates signed by publicly trusted certificate authorities that have a minimum key size of 2048 bits for RSA. All pages are served using HTTPS, by default.

A NOTE ABOUT PCI-COMPLIANCE: Adobe Commerce on Cloud is PCI-compliant and does not store credit card information or process payments within the solution. All payments are processed through third-party payment processors. The customer is responsible for verifying that any custom code or extensions to Adobe Commerce on Cloud do not process and/or store payment information or are certified as PCI-compliant if they must handle PII data.

User Authentication

Adobe Commerce on Cloud uses Adobe Identity Management Services (IMS) to manage access and entitlements for users. Adobe Commerce on Cloud supports three (3) different types of user-named licensing. For more information about each identity type, please see this identity types overview. You can also find out more about Adobe's identity management services in the Adobe Identity Management Services Security Overview.

Administrator Authentication

Administrators use the Adobe Admin Console to manage the online store, including products, orders, shipments, CMS content, design of the storefront, and customer information. Role-based permissions enable admins to control access to specific features, options, and capabilities.

For administrative users only, access to the Adobe Commerce on Cloud Admin Console requires two-factor authentication (2FA) from all devices. This option is not available for storefront customer accounts.

Additional Security Options

Adobe Commerce on Cloud administrators have additional security options that can be implemented for both admin users as well as storefront customers. These options are detailed on Adobe Experience League.

Adobe Commerce on Cloud Hosting and Security

Adobe Commerce on Cloud is hosted in enterprise-class data centers from public cloud service providers in U.S. East (Ohio, South Carolina, and Virginia,), US-West (California, Oregon, and Washington), US-Central (Iowa and Texas), Canada (Montreal and Toronto), APAC (Hong Kong, India, Japan, Singapore, South Korea, and Sydney), EU (France, Germany, Ireland, Italy, The Netherlands, and Sweden), UK (London); ROW (Bahrain, Brazil, and South Africa).

Upon provisioning, customers can choose the specific data center region or location to host their Adobe Commerce on Cloud instance.

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.

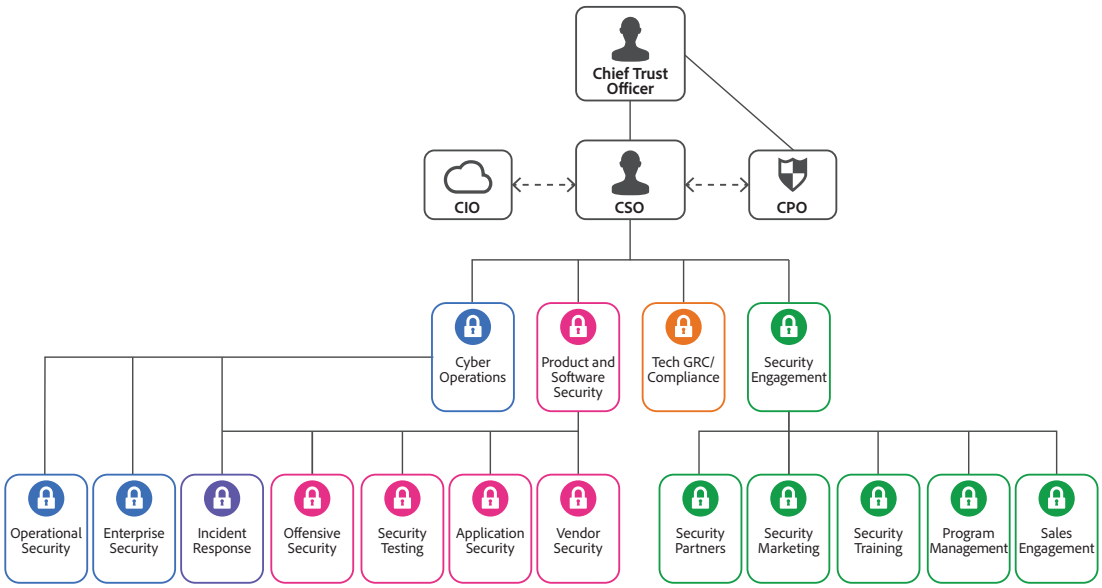


Figure 5: The Adobe Security Organization

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.

Adobe's culture of security and training programs are outlined in more detail in 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.

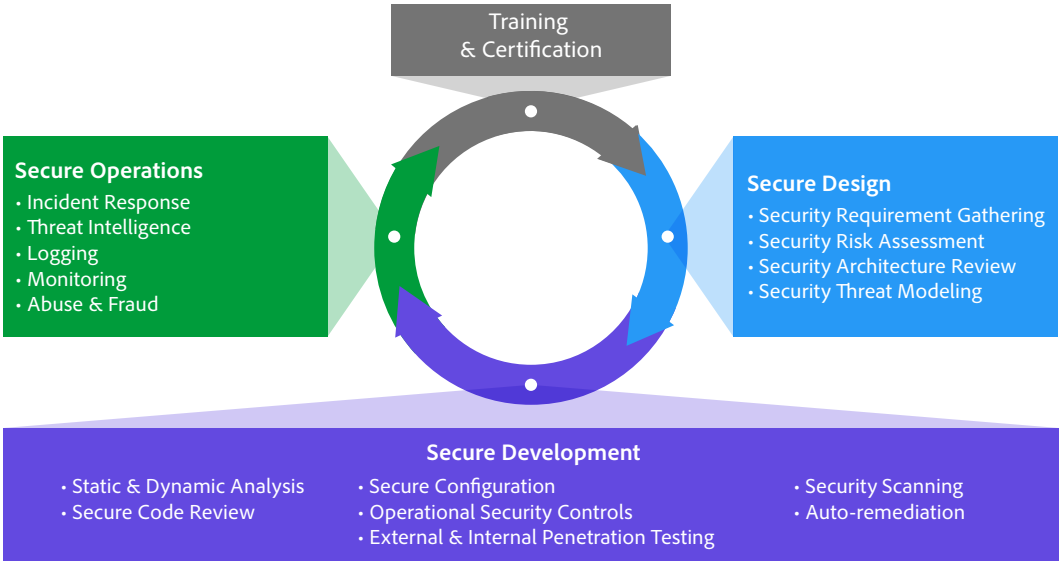
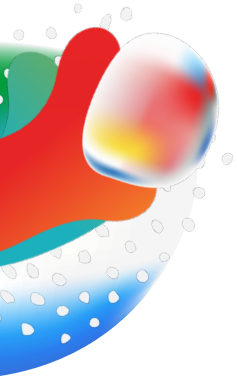


Figure 6: The Adobe Secure Product Lifecycle

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.



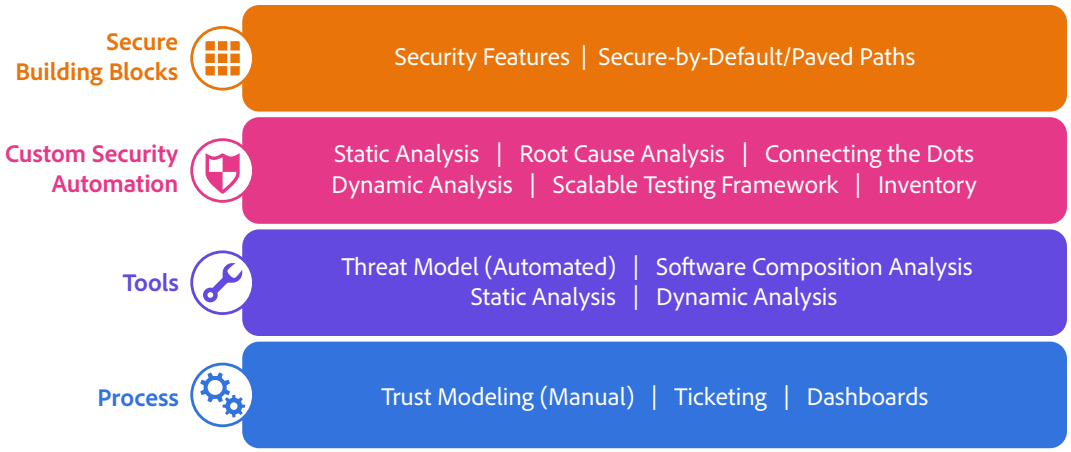


Figure 7: The Adobe Application Security Stack

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. The Adobe Application Security Overview contains more detailed information about Adobe's application security practices and processes.

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.

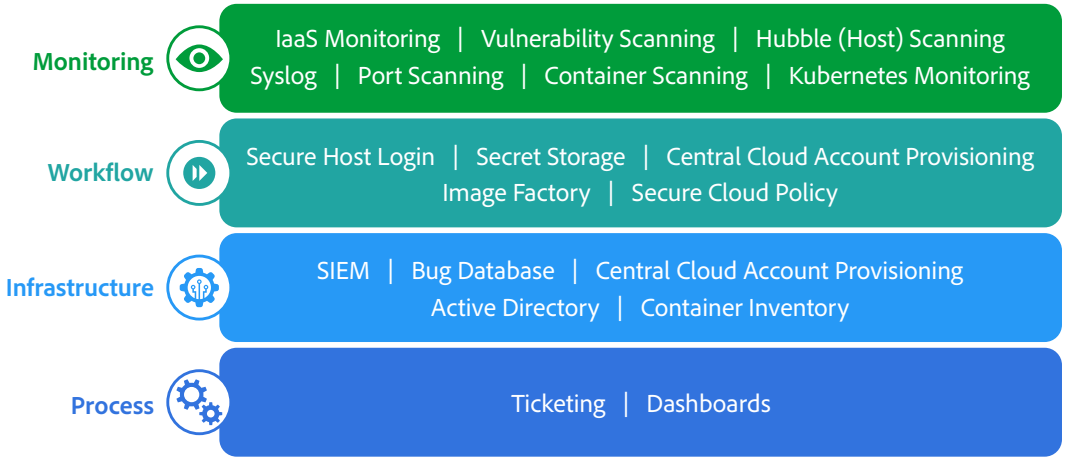


Figure 8: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. A detailed description of the Adobe OSS and the specific tools used throughout Adobe can be found in 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.

More information on our enterprise security controls and standards we have developed for these controls can be found in 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. More information on the Adobe CCF and key certifications can be found in the Adobe Compliance Certifications, Standards, and Regulations 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.

More details about Adobe's incident response and notification process are documented in the Adobe Incident Response Program Overview.

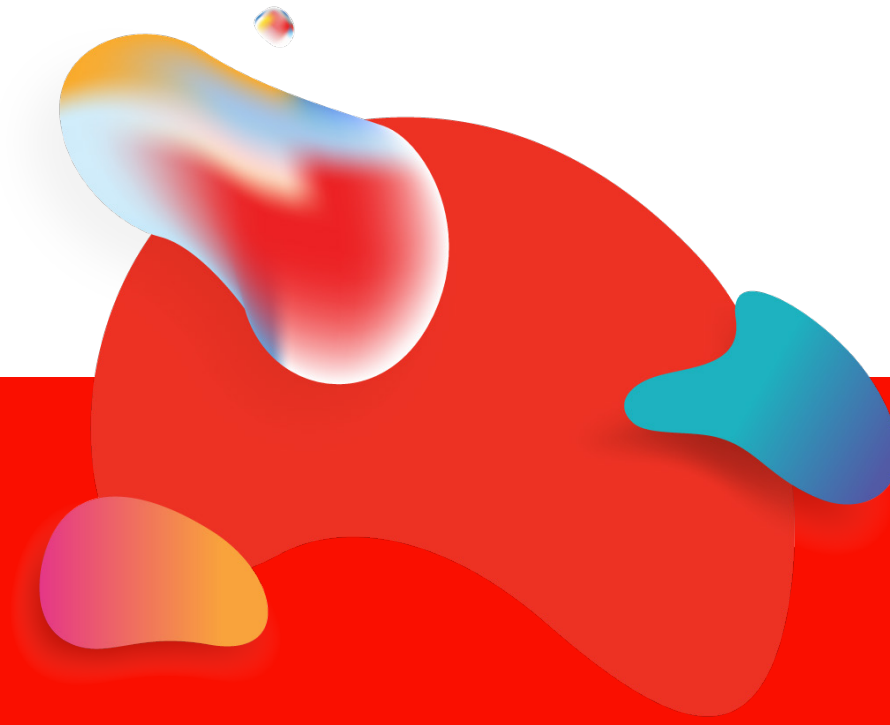
Business Continuity and Disaster Recovery

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 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 Acrobat Sign 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 security our customers' data.

For more information on Adobe security, please go to the Adobe Trust Center.



Adobe

3/23