Adobe Experience Cloud

Adobe

WHITEPAPER

Adobe® Experience Manager Dynamic Media Security Overview

Table of Contents

Adobe Security

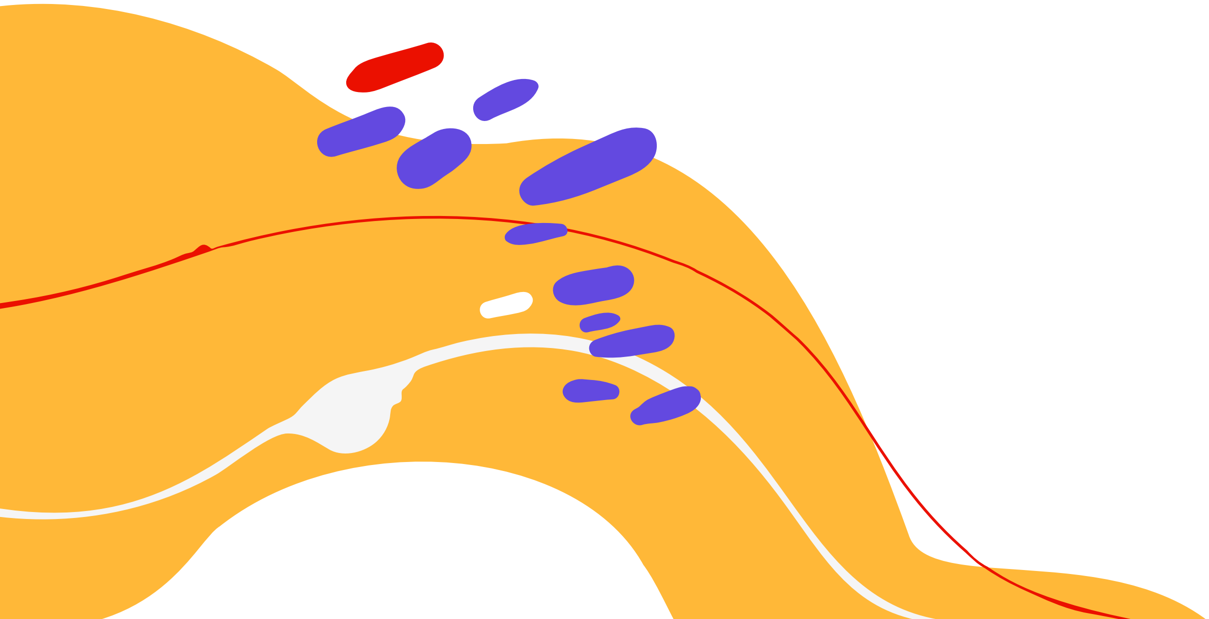
At Adobe, we know the security of your digital experience is important. Security practices are deeply ingrained into our internal software development, operations processes, and tools. Our cross-functional teams strictly follow these practices to help prevent, detect, and respond to incidents in an expedient 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 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 the Adobe Experience Manager Dynamic Media solution and its associated data.

About Adobe Experience Manager Dynamic Media

Adobe Experience Manager (AEM) Dynamic Media is a content-serving service that allows marketers to manage and publish digital experiences designed in AEM Assets, Adobe's highly scalable, cloud-native digital asset manager (DAM). Customers can deliver rich visual merchandising and marketing assets on demand, automatically scaled for consumption on web, mobile, and social sites.

AEM Dynamic Media generates and delivers multiple variations of rich content in real time through its global, scalable performance-optimized network. A joint solution from Adobe and a leading content delivery network (CDN) provider, AEM Dynamic Media helps reduce the cost of running a digital property by enabling customers to offload content-serving to Adobe's network.



AEM Dynamic Media Solution Architecture

Adobe AEM Dynamic Media is comprised of the following components:

AEM Assets — Enables customers to manage assets to create, manage, deliver, and optimize dynamic digital experiences in a cloud-native digital asset management (DAM) solution.[1]

AEM Dynamic Media Cloud Service — Processes and publishes the media assets created in AEM Assets for delivery to target web properties. It includes two services:

- **Image Production System (IPS)** — Ingests digital assets (images, videos, PDF files, etc.) stored in AEM Assets using SOAP APIs and transforms them into an optimized format for web delivery.
- **Image Serving** — Sends images, videos and other static content to target digital properties defined by the customer. Operating from one master file allows Dynamic Media to seamlessly create unlimited versions of an asset for any media, automatically. Smart imaging technology automatically detects the available bandwidth and device type to dramatically minimize image file size by up to 70 percent upon delivery, with no loss in visual fidelity to ensure smooth and quick loading.[2]

Content Delivery Network (CDN) — Delivers performance-optimized content to end-users.

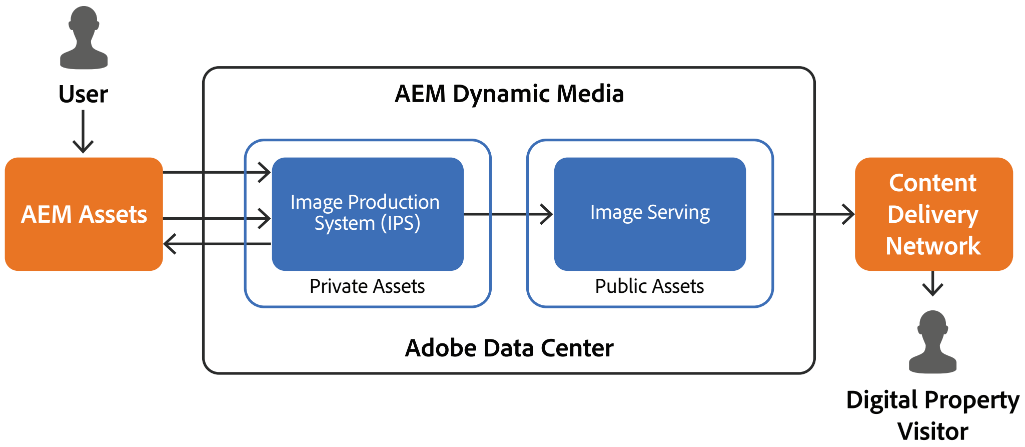


Figure 1: AEM Dynamic Media Solution Architecture

[1] The customer must configure AEM Assets to integrate with Dynamic Media Cloud Service.

[2] For video, Image Serving includes the Adobe Media Server.

AEM Dynamic Media Content Flow: Image Processing

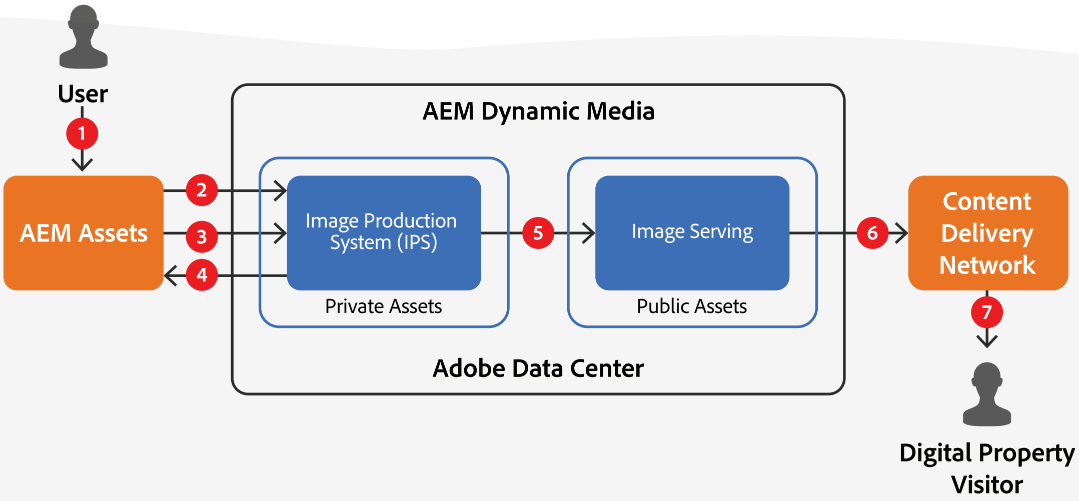


Figure 2: AEM Dynamic Media Image Processing Content Flow

1. The customer uploads their visual content (image) to AEM Assets using the AEM user interface.

2. AEM Dynamic Media automatically synchronizes the image stored in AEM Assets to Dynamic Media IPS, which is hosted in an Adobe-managed data center.

3. Dynamic Media IPS then converts the image to the PTIFF format, which enables the solution to manage a single primary source image and generate infinite renditions on-the-fly without additional storage.

4. At this point, authenticated users can preview the image as well as dynamic renditions of the asset.[3]

5. After approving the image and its renditions, the customer can publish the image to Image Serving. Once published, the asset becomes publicly available.

6. All published assets are served directly to the digital property via the AEM Dynamic Media built-in CDN. When the CDN receives the first dynamic image generation request or "hit" from a visitor to the digital property, it checks to see if the content is in the CDN cache. If it is in the cache, Dynamic Media immediately delivers the content. If it is not in the CDN cache, then the CDN will pull the content from cloud-based origin servers, which are optimized for memory, disk, and software-caching.

7. The CDN serves the content to the digital property visitor.

[3] For earlier versions of Adobe Dynamic Media (e.g., 6.5.x), the IP addresses of AEM instances must be allowlisted in the Dynamic Media settings. Preview will be allowed only to the configured IP addresses.

AEM Dynamic Media Content Flow: Video Processing

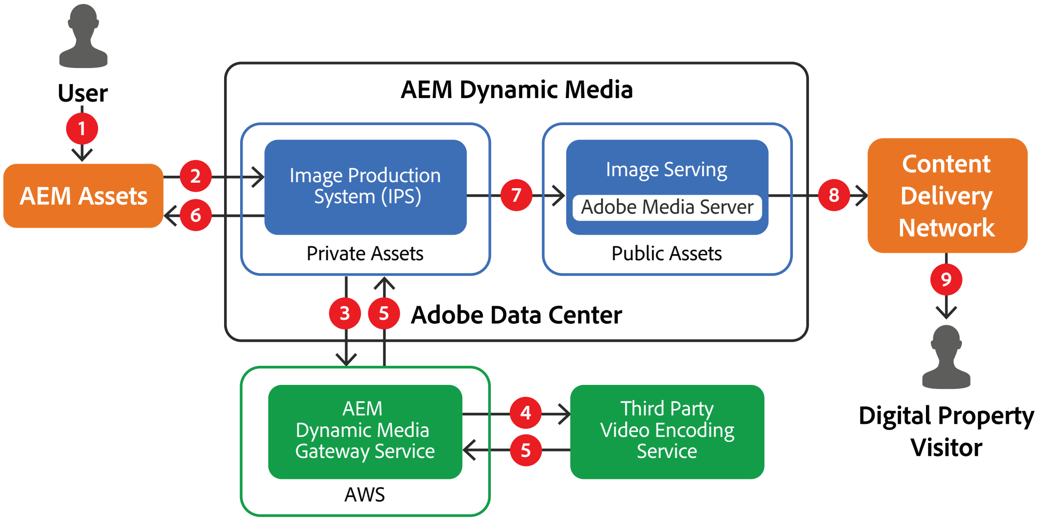


Figure 3: AEM Dynamic Media Video Processing Content Flow

1. The customer uploads their video content to AEM Assets using the AEM user interface.
2. AEM Dynamic Media automatically synchronizes the video stored in AEM Assets to Dynamic Media IPS, which is hosted in an Adobe-managed data center.
3. IPS sends the video processing request to the AEM Dynamic Media Gateway Service hosted in AWS.
4. The AEM Dynamic Media Gateway Service shares the uploaded videos with a third-party encoding service using S3-signed URLs.
5. The third-party encoding service generates transcodes for the source video. Source video and output videos are stored temporarily in private S3 buckets in AWS while processing occurs. Once processed, the transcodes are copied to IPS and the source video and transcodes are deleted from AWS.
6. The customer can now preview and then publish the video and its transcodes. The published video is now publicly available.
7. All published assets are served directly to users via AEM Dynamic Media's built-in CDN. The video transcodes are streamed by Adobe Media Server, which is part of Image Serving.
8. When the CDN receives the first dynamic image generation request or "hit" from a visitor to the digital property, it checks to see if the content is in the CDN cache. If it is in the cache, Dynamic Media immediately delivers the content. If it is not in the CDN cache, then the CDN will pull the content from cloud-based origin servers, which are optimized for memory, disk, and software caching. Video streaming is also backed by CDN.
9. Video is streamed to the digital property visitor.

AEM Dynamic Media Security Architecture

Data Encryption

AEM Dynamic Media protects all data in transit with HTTPS.

DDoS Protection

Adobe Dynamic Media employs a service provided by our CDN partner that uses pattern matching and rate limiting to protect against DDoS (Distributed Denial of Service) attacks.

Virus/Malware Scanning

All input files are scanned for viruses and malware as part of the Dynamic Media upload workflow to IPS. Any compromised file is discarded.

User Authentication

The number of end-user accounts with access to AEM Dynamic Media is controlled by the customer's Adobe AEM administrator. AEM Assets must be configured using one of these appropriately provisioned accounts to integrate with Dynamic Media Cloud Service.[4] We continually work with our development teams to implement new protections based on evolving authentication standards.

Users can access AEM Assets in one of three (3) different types of user-named licensing:

Adobe ID is for Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users.

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 organization owns and manages the user accounts and all associated assets, Adobe hosts the Enterprise ID and performs authentication. Admins can revoke access to Dynamic Media 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 the customers' IT infrastructure.

[4] Access to the Dynamic Media Cloud Service, through the Adobe Dynamic Media user interface within the AEM UI, requires authentication with username and password. There is no IMS/SSO/SAML support at the Dynamic Media Cloud Service level.

Adobe integrates with most SAML2.0 compliant identity providers. Adobe IDs and Enterprise IDs both 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's identity management services can be found in the Adobe Identity Management Services security overview.

The AEM Dynamic Media Content Delivery Network

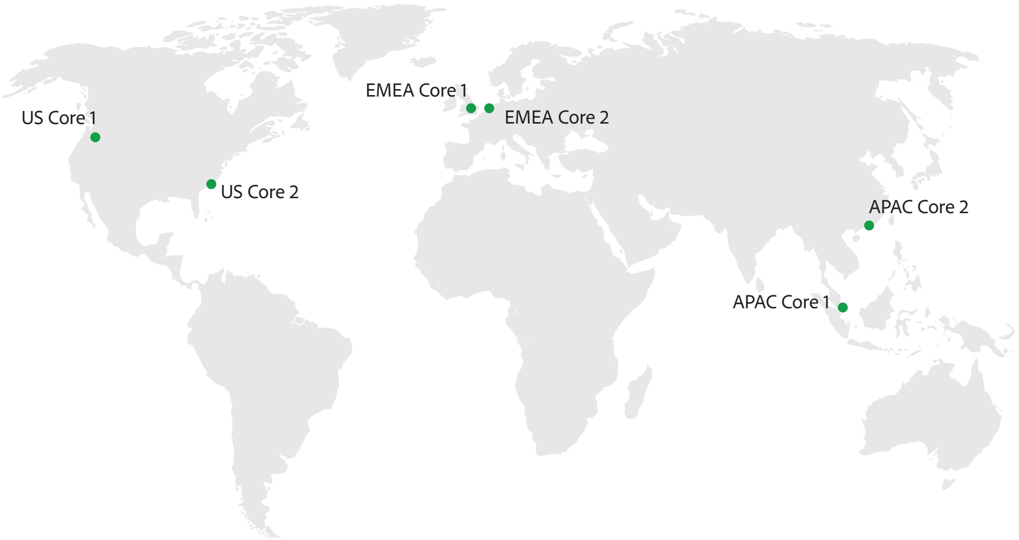


Figure 4: AEM Dynamic Media Content Delivery Network

AEM Dynamic Media is hosted in Adobe-owned or -leased data centers in North America, Europe, and Asia-Pacific. Each region includes a primary data center and a secondary data center within the region (for failover). Upon provisioning, customers are assigned to the primary data center geographically closest to them.

Primary servers host both IPS and Image Serving components of AEM Dynamic Media. Secondary servers only host the Image Serving component.

- In North America, the primary server is located in the US-West region (Oregon) and the secondary server is located in US-East (Virginia).
- In Europe, the primary server is located in London and the secondary server is located in Amsterdam.
- In Asia-Pacific, the primary server is located in Singapore and the secondary server is located in Hong Kong.

AEM Dynamic Media deploys a third-party global server load-balancing solution that routes customer requests based on dynamic metrics obtained by constant monitoring of host servers.

Video encoding workflows also use a video encoding gateway service that is deployed in AWS.

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.

Application Security
Operational Security
Enterprise Security
Compliance
Incident Response

Figure 5: 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.

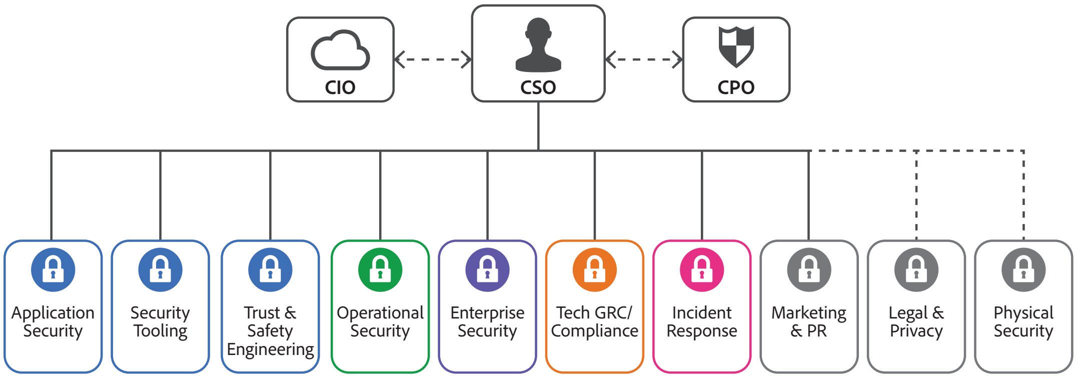


Figure 6: The Adobe Security Organization

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.

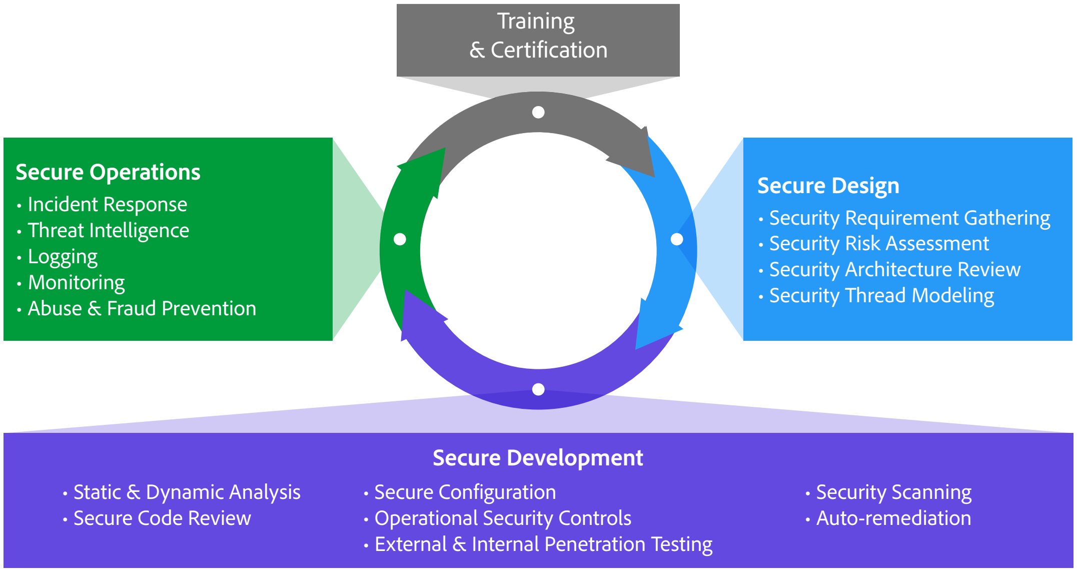

Training
& Certification
Secure Operations
• Incident Response
• Threat Intelligence
• Logging
• Monitoring
• Abuse & Fraud Prevention
Secure Design
• Security Requirement Gathering
• Security Risk Assessment
• Security Architecture Review
• Security Thread Modeling
Secure Development
• Static & Dynamic Analysis
• Secure Code Review
• Secure Configuration
• Operational Security Controls
• External & Internal Penetration Testing
• Security Scanning
• Auto-remediation

Figure 7: 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.

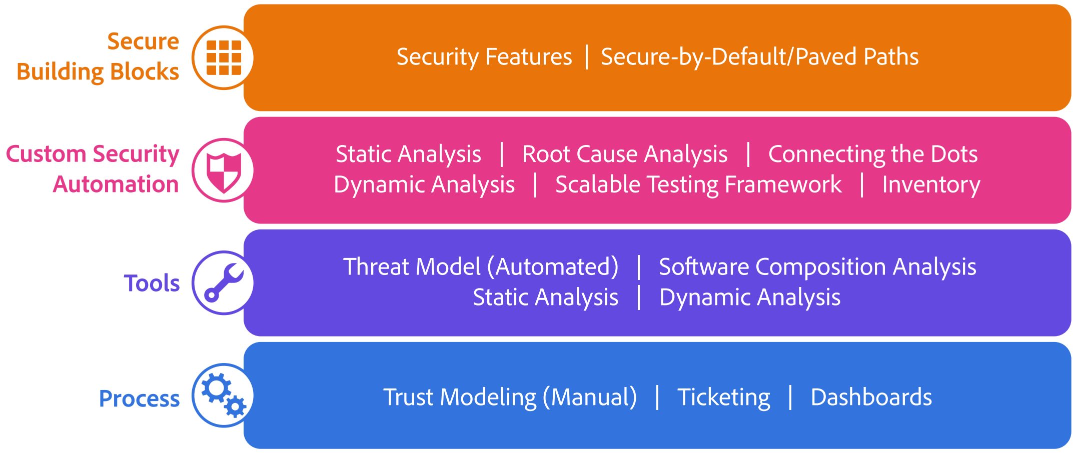

Secure
Building Blocks
Security Features | Secure-by-Default/Paved Paths
Custom Security
Automation
Static Analysis | Root Cause Analysis | Connecting the Dots
Dynamic Analysis | Scalable Testing Framework | Inventory
Tools
Threat Model (Automated) | Software Composition Analysis
Static Analysis | Dynamic Analysis
Process
Trust Modeling (Manual) | Ticketing | Dashboards

Figure 8: 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.

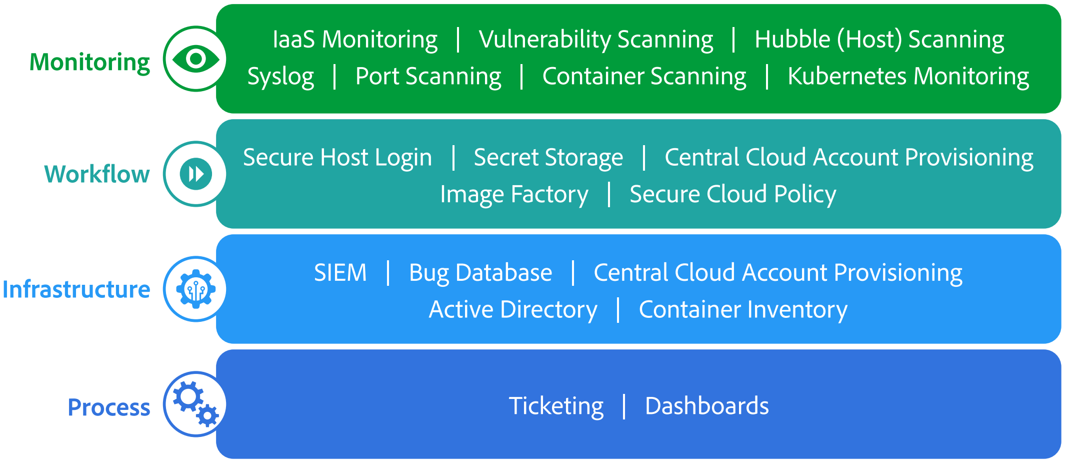

Monitoring
IaaS Monitoring | Vulnerability Scanning | Hubble (Host) Scanning
Syslog | Port Scanning | Container Scanning | Kubernetes Monitoring
Workflow
Secure Host Login | Secret Storage | Central Cloud Account Provisioning
Image Factory | Secure Cloud Policy
Infrastructure
SIEM | Bug Database | Central Cloud Account Provisioning
Active Directory | Container Inventory
Process
Ticketing | Dashboards

Figure 9: 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 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

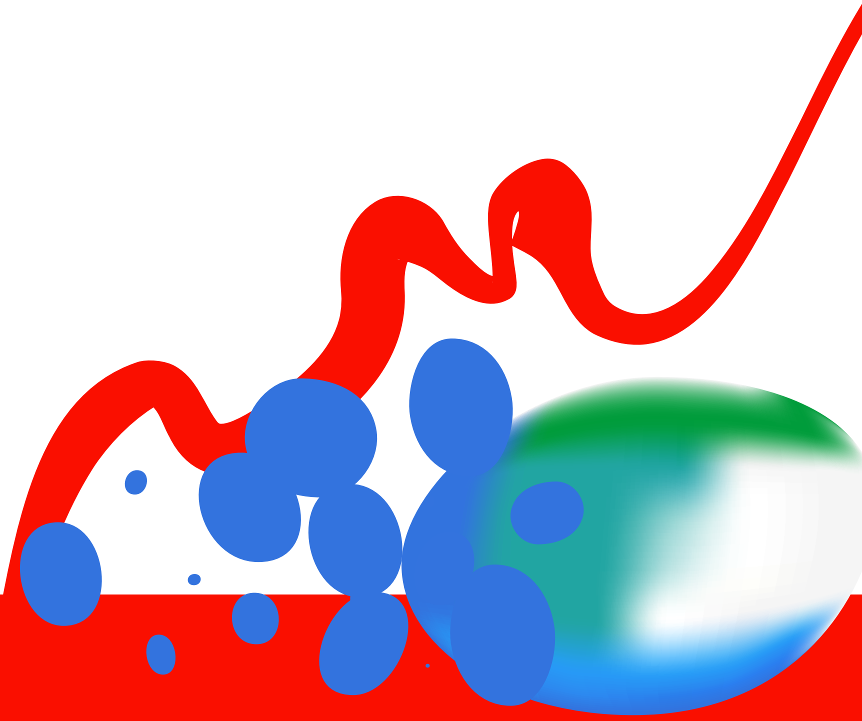
The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified 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 Dynamic Media 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 of 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.



Adobe