Adobe Media Optimizer Security Overview

Table of Contents

Adobe Security

At Adobe, we take the security of your digital experience very seriously. Security practices are deeply ingrained into our internal software development and operations processes and tools and are rigorously followed by our cross-functional teams to prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities and we regularly incorporate advanced security techniques into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of your data and Adobe® Media Optimizer experience.

About Adobe Media Optimizer

Adobe Media Optimizer gives advertisers the ability to assess, forecast, and optimize online advertising spend across channels. Advertisers can manage all their display, search engine, and social ad campaigns from a single unified interface. Data from pixel tracking, publisher-provided reports, and advertiser-provided revenue feeds are processed by predictive modeling algorithms to come up with spend and other configuration decisions for ad campaigns across both non-real-time and real-time bidding based publishers.

Adobe Media Optimizer Application Architecture

The Adobe Media Optimizer solution includes the following capabilities:

Display Management — Lets users manage and optimize display programs to help meet marketing goals and ROI objectives. Display Management uses reliable re-targeting, data-reliant prospecting, and look-alike modeling to reach out to new and profitable audiences.

Search Ad Management — Allows users to simulate and quickly act upon the most profitable options in their search marketing strategy and offers comprehensive campaign optimization through industry-leading forecast models, scalable campaign automation, and integration with Adobe Analytics.

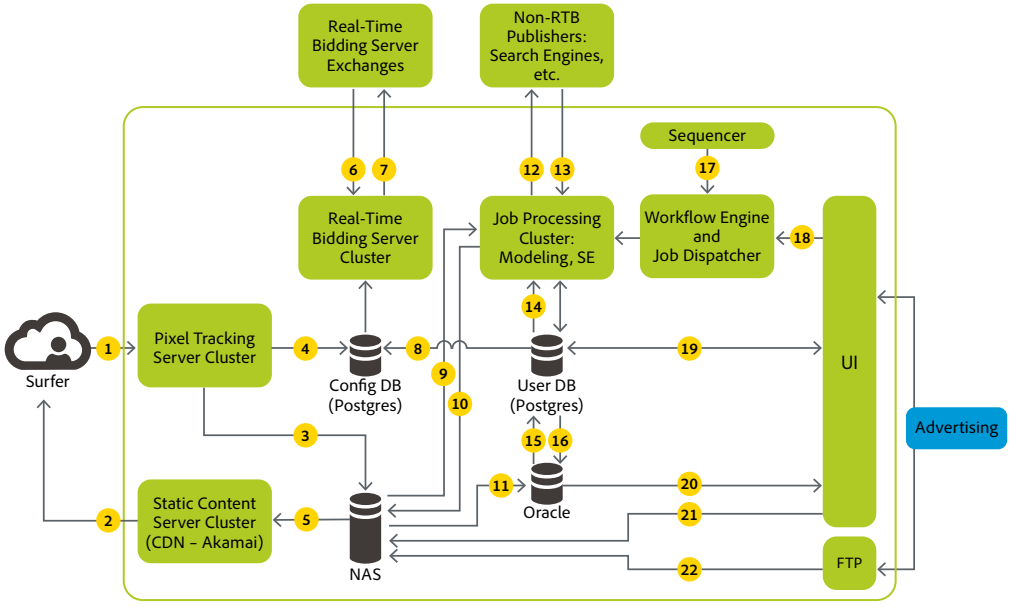
Social Ad Management — Allows users to confidently create, manage, optimize, and scale ads for Facebook using Adobe's unique preview environment, which enables users to edit ads in bulk prior to launch.

Tag Management — Enables users to manage an unlimited number of Adobe and third-party tags. Tag Management gives user more control and flexibility to optimize almost anything online, all while reducing dependency on IT resources.

Reporting — Helps users to know when to bet or when to hold on any campaign using the accuracy reporting feature.

Real-Time Bidding — Enables users to retarget their most valuable customers by optimizing display ad campaigns to meet their goals. Adobe Media Optimizer uses unified campaign tracking and reporting, real-time bidding, impression-level decisioning abilities, attribution reporting and simulations, and integration with the top ad exchanges to help users meet display objectives.

Dynamic Content Optimizer — Tool to seamlessly build, personalize and deliver creative assets in real time to help drive higher user engagement and conversion rates across devices. Allows customers to scale and optimize ad creative.



1. Impressions, Clicks, Conversions, Events, etc.
2. Tracking Javascript, RTB Rich Media Assets
3. Event Logs
4. Surfer Profile Info
5. RTB Rich Media Assets
6. Bid Request
7. Bid Response
8. RTB Campaign Config and Bids
9. Campaign Config Reports and Click Reports
10. Customer Campaign Config Feeds
11. Pixel Events, Customer Revenue Feeds Campaign Config Reports and Click Reports
12. Config Reports and Click Reports
13. Campaign Config and Bids
14. RTB Bids
15. Campaign Performance Warehouse
16. Portfolio Config
17. Periodic Tasks
18. Deferred Tasks
19. Portfolio Config, Campaign Config, User Preferences, Tagging, etc.
20. Campaign Performance Data and Reports
21. RTB Rich Media Assets
22. Revenue Feed Files and Campaign Config Feeds

Figure 1: Adobe Media Optimizer Application Architecture and Data Flow

Adobe Media Optimizer Application Security and Network Architecture

An advertiser typically uses Adobe Media Optimizer as follows:

The advertiser creates ad campaigns on various publishing platforms using the campaign management capabilities of Media Optimizer and/or directly creates the campaigns on the publisher and grants Media Optimizer access privileges to those campaigns. In the case of real-time-bidding-based publishing platforms, all campaign configuration is hosted by Media Optimizer and so only the former is applicable. In the case of non-real-time-based publishers, Media Optimizer also installs tracking hooks on these campaigns so that ad clicks will redirect through the pixel tracking server before going to the customer's landing page. Media Optimizer also downloads click reports from the publisher on a daily basis to help with reporting and optimization.

The advertiser also installs Media Optimizer's pixel tracking on its website. This enables tracking of visitor behavior when the visitor reaches the site after clicking on an ad or other means. The pixel tracking captures page visits and conversions (revenue events quantified in terms of advertiser specific revenue metrics, e.g., "subscriptions," "ticket_purchase," etc.) by each visitor. The advertiser may also supplement or substitute this with periodic revenue feeds from his or her end. All revenue information is correlated in the back end with ad impressions and clicks of the same visitor, attributing value to each impression and click. The pixel tracking also segments visitors into categories based on their behavior on the site, which is critical in making bidding decisions for the visitor on real-time-bidding-based publishing platforms.

Portfolios, created by the advertiser, associate a set of ad campaigns with a budget and a maximization objective, usually expressed in terms of a weighted sum of the advertiser's revenue metrics. Media Optimizer then applies predictive modeling techniques to the correlated click and revenue information to come up with the bids and other campaign configuration for the following

day. This process repeats daily, with campaign configurations adapting to changing conditions. The advertiser can run reports and forecasts on ad campaign performance through the Media Optimizer web-based UI.

User Authentication via Adobe Marketing Cloud

Access to Adobe Media Optimizer requires authentication with username and password. For users accessing Adobe Media Optimizer using Adobe IDs, Adobe leverages the BCrypt hash algorithm in combination with password salts and a large number of hash iterations. We continually work with our development teams to implement new protections based on evolving authentication standards.

Users can access Adobe Media Optimizer in one of two (2) different types of user-named licensing:

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

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 customer'sITdepartment. Adobe integrates with most any SAML2.0 compliant identity provider.

Application and service entitlement is accomplished through the Adobe Enterprise Dashboard. More information on the dashboard is available here: https://helpx.adobe.com/enterprise/help/aedash.html

Adobe Media Optimizer Hosted Data Centers

All components of Adobe Media Optimizer, except for some components of Dynamic Content Optimizer (DCO), are hosted on Adobe servers in six (6) data centers around the world. The DCO edge servers are hosted in Amazon Web Services (AWS). For information on AWS security controls that impact DCO, please see the section entitled, "Dynamic Content Optimizer Hosting."

When a customer chooses to have Adobe host all or part of their Adobe Media Optimizer deployment, Adobe generally hosts the customer's deployment in a data center located in the customer's corresponding region.

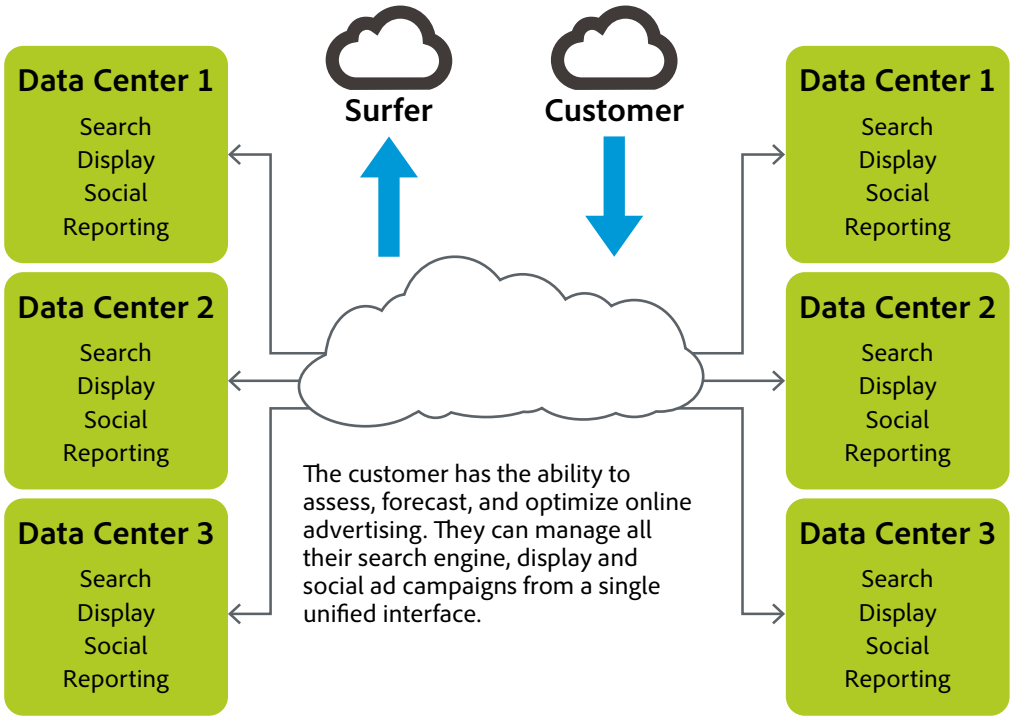


Figure 2: The Adobe Media Optimizer network

Geographic Location of Customer Data on the Data Center Network

Adobe stores all Media Optimizer customer data in data centers currently located in the United States and the United Kingdom.

Adobe Media Optimizer Network Management

Adobe understands the importance of protecting your data. To this end, the network architecture for Adobe Media Optimizer implements industry standard practices for security design, including segmentation of development and production environments, DMZ segments, hardened bastion hosts, and unique authentication.

Segregating Client Data

Data is placed into separate databases (report suites), and a single client's site reports are grouped together on one or more servers. In some cases, more than one client may share a server, but the data is segmented into separate databases. The only access to these servers and databases is via authenticated access by the Media Optimizer application. All other access to the application and data servers is made only by authorized Adobe personnel, andwhen necessary is conducted via encrypted channels. We separate our testing environments from our production environments.

Secure Management

Adobe deploys dedicated network connections from our corporate offices to our data center facilities in order to enable help secure management of the Adobe Media Optimizer servers. All management connections to the servers occur over encrypted Secure Shell (SSH), Secure Sockets Layer (SSL), or Virtual Private Network (VPN) channels and remote access always requires two-factor authentication. Unless the connection originates from a list of trusted IP addresses, Adobe does not allow management access from the Internet.

Firewalls and Load Balancers

The firewalls implemented on the Adobe Media Optimizer network deny all Internet connections except those to allowed ports, Port 80 for HTTP and Port 443 for HTTPS. The firewalls also perform Network Address Translation (NAT). NAT masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming HTTP/HTTPS connections and also distribute requests that enable the network to handle momentary load spikes. Adobe implements fully redundant firewalls and load balancers, reducing the possibility that a single device failure can disrupt the flow of traffic.

Non-routable, Private Addressing

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

Intrusion Detection

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

Service Monitoring

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

Data Backups

Adobe backs up customer data for Adobe Media Optimizer on a daily basis through the use of snapshots. Each snapshot is stored for up to seven (7) days. The combination of backup procedures helps provide quick recovery from short-term backup as well as off-site protection of data.

Change Management

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

Patch Management

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

Access Controls

Only authorized users within the Adobe intranet or remote users who have completed the multi-factor authentication process to create a VPN connection can access administrative tools. In addition, Adobe logs all Adobe Media Optimizer production server connections for auditing.

Logging

In order to help protect against unauthorized access and modification, Adobe captures network logs, OS-related logs, and intrusion detections. Sufficient storage capacity for logs is identified, periodically reviewed, and, as needed, expanded to help ensure that log storage is not exceed. Systems generating logs are hardened and access to logs and logging software is restricted to authorized Adobe Digital Marketing Information Security Team personnel. Adobe retains raw logs for one year.

Dynamic Content Optimizer (DCO) Hosting

The edge servers for the Dynamic Content Optimizer capability within Adobe Media Optimizer is hosted on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the EMEA region. Amazon EC2 is a web service that provides resizable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere.

The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits. You can find more detailed information about AWS and Amazon's security controls on the AWS security site.

Operational Responsibilities of AWS and Adobe

AWS operates, manages, and controls the components from the hypervisor virtualization layer down to the physical security of the facilities in which we operate. In turn, Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and application software, as well as the configuration of the AWS-provided security group firewall.

AWS also operates the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. The AWS infrastructure includes facilities, network, and hardware, as well as the operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources. Amazon designs and manages AWS according to industry-standard practices as well as a variety of security compliance standards.

Secure Management

Adobe uses Secure Shell (SSH) and Secure Sockets Layer (SSL) for management connections to manage the AWS infrastructure.

Geographic Location of Customer Data on AWS Network

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

Adobe stores all Media Optimizer DCO component customer data in Amazon Web Services' US East Region.

Data replication for Amazon S3 data objects occurs within the regional cluster where the data is stored and is not replicated to data center clusters in other regions.

Isolation of Customer Data/Segregation of Customers

AWS uses strong tenant isolation security and control capabilities. As a virtualized, multi-tenant environment, AWS implements security management processes and other security controls designed to isolate each customer from other AWS customers. Adobe uses the AWS Identity and Access Management (IAM) to further restrict access to compute and storage instances.

Secure Network Architecture

AWS employs 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 (ACL), 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. Amazon Information Security approves all ACL policies and automatically pushes them to each managed interface using AWS's ACL-Manage tool, helping to ensure these managed interfaces enforce the most up-to-date ACLs.

Network Monitoring and Protection

AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points. The AWS network provides significant protection against traditional network security issues:

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

You can find more information about Network Monitoring and Protection in the AWS: Overview of Security Processes white paper on the Amazon website.

Intrusion Detection

Adobe actively monitors the DCO component of Media Optimizer using industry-standard intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Logging

Adobe conducts server-side logging of DCO customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs only store Adobe IDs to help diagnose specific customer issues and do not contain username/password combinations. Only authorized Adobe technical support personnel, key engineers, and select developers can access the logs to diagnose specific issues that may arise.

Service Monitoring

AWS monitors electrical, mechanical, and life support systems and equipment to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, AWS performs ongoing preventative maintenance.

Data Storage and Backup

Adobe collects all DCO data in Amazon S3, which provides a storage infrastructure with high durability. Final storage and backup of data is handled via secure Adobe-managed data centers in Oregon and Ireland.

Change Management

AWS authorizes, logs, tests, approves, and documents routine, emergency, and configuration changes to existing AWS infrastructure in accordance with industry norms for similar systems. Amazon schedules updates to AWS to minimize any customer impact. AWS communicates with customers, either via email, or through the AWS Service Health Dashboard when service use is likely to be adversely affected. Adobe also maintains a Status Health Dashboard for DCO.

Patch Management

AWS maintains responsibility for patching systems that support the delivery of AWS services, such as the hypervisor and networking services. Adobe is responsible for patching its guest operating systems (OS), software, and applications running in AWS. When patches are required, Adobe supplies a new, pre-hardened instance of the OS and application rather than an actual patch.

AWS Physical and Environmental Controls

AWS physical and environmental controls are specifically outlined in a SOC 1, Type 2 report. The following section outlines some of the security measures and controls in place at AWS data centers around the world. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper or the Amazon security website.

Physical Facility Security

AWS data centers utilize industry standard architectural and engineering approaches. AWS data centers are housed in nondescript facilities and Amazon 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.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Fire Suppression

AWS installs automatic fire detection and suppression equipment in all AWS 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.

Controlled Environment

AWS employs a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. AWS data centers maintain atmospheric conditions at optimal levels. AWS personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup Power

AWS 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.

Video Surveillance

Professional security staff strictly controls physical access both at the perimeter and at building ingress points for AWS data centers using video surveillance, intrusion detection systems, and other electronic means.

Disaster Recovery

AWS data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built in clusters in various 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. You can find more information about AWS disaster recovery protocols on the Amazon Security website.

Adobe Risk & Vulnerability Management

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

Penetration Testing

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

Internally, the Adobe Media Optimizer security team performs a risk assessment of all Media Optimizer components prior to every release. Conducted by highly trained security staff trusted with securing the network topology and infrastructure and Media Optimizer application, the security reviews look for insecure network setup issues across firewalls, load balancers, and server hardware as well as application-level vulnerabilities. The security touchpoints include exercises such as threat modeling coupled with vulnerability scanning and static and dynamic analysis of the application. The Media Optimizer security team partners with technical operations and development leads to ensure all high-risk vulnerabilities are mitigated prior to each release.

Incident Response and Notification

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

When a significant announced vulnerability puts Media Optimizer at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Media Optimizer organization to coordinate the mitigation effort.

For Adobe cloud-based services, including Adobe Media Optimizer, Adobe centralizes incident response, decision-making, and external monitoring in our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues.

When an incident occurs with an Adobe product or service, the SCC works with the involved Adobe product incident response and development teams to help identify, mitigate, and resolve the issue using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

Forensic Analysis

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

Adobe Data Center Physical and Environmental Controls

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

Physical Facility Security

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

Fire Suppression

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

Controlled Environment

Every data center facility must include an environmentally controlled environment, including temperature humidity control and fluid detection. Adobe requires a completely redundant heating, ventilation and air conditioning (HVAC) system and 24x7x365 facility teams to handle any environmental issue that might arise. If the environmental parameters move outside those defined by Adobe, environmental monitors alert both Adobe and the facility's Network Operations Center (NOC).

Video Surveillance

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

Backup Power

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

Disaster Recovery

In the event that one of our data collection environments are unavailable due to an event, whether a problem at the facility, a local situation, or a regional disaster, Adobe follows the process described here to allow for continuation of data collection and to ensure an effective and accurate recovery.

Failover Process

When an event is determined to result in long-term data collection disruption, Adobe will reconfigure DNS to send data collection requests to a secondary location not affected by the disaster. Adobe will also manually place a hold on data processing in the primary environment to preserve the chronological order of page views, which is necessary for the recovery process to work successfully.

Recovery Process

When the primary data collection location is available and stable again, the failover process will be reversed. All traffic collected at the secondary location will be merged with data in the primary location, DNS records will be restored, and page views will be processed sequentially in time order. During page view processing, reports will not be real time until page view processing is complete. Page view processing will take approximately one day for every four hours the failover process was active. Time required to recover historical data from off-site may take up to an additional ten (10) days.

The Adobe Security Organization

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

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

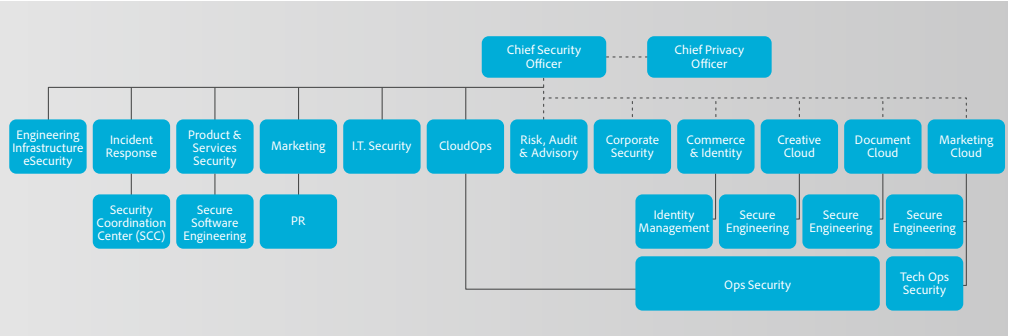


Figure 3: The Adobe Security Organization

Adobe Secure Product Development

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

Adobe Secure Product Lifecycle

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

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe Media Optimizer security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials

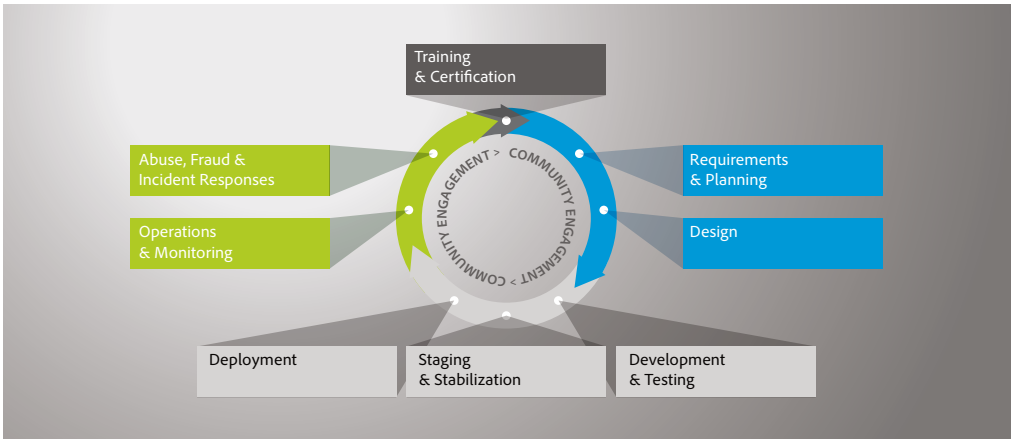


Figure 4: Adobe Secure Product Lifecycle (SPLC)

Adobe Security Training

Adobe Software Security Certification Program

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

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

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

Adobe Common Controls Framework

To protect from the software layer down, Adobe uses the Adobe Secure Product Lifecycle, which is described in the following section. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls to protect the company's infrastructure, applications, and services and help Adobe comply with a number of industry accepted best practices, standards, and certifications.

In creating the Adobe Common Controls Framework (CCF), Adobe analyzed the criteria for the most common security certifications and found a number of overlaps. After analyzing more than 1000 requirements from relevant cloud security frameworks and standards, Adobe rationalized these down to approximately 200 Adobe-specific controls. The CCF control owners know exactly what is required to address the expectations of Adobe stakeholders and customers when it comes to implementing controls.

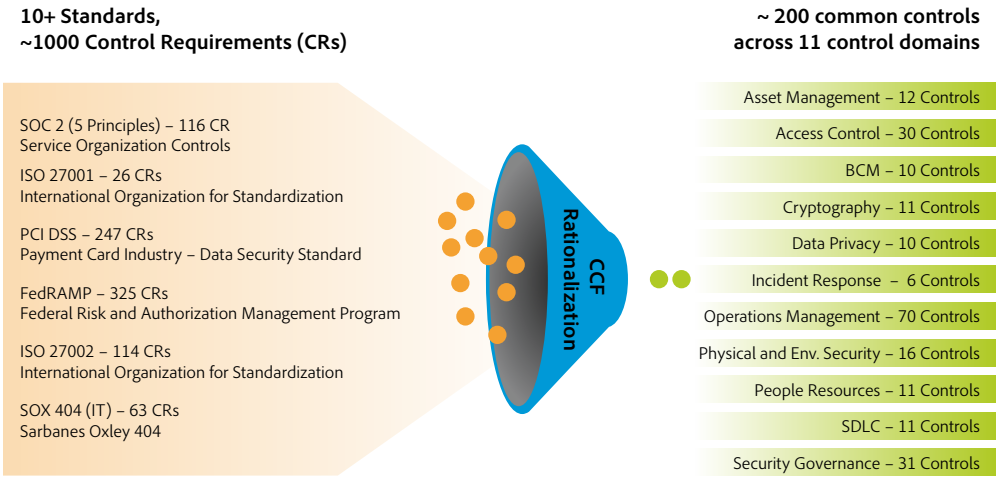


Figure 5: Adobe Common Controls Framework (CCF)

Adobe Corporate Locations

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

Physical Security

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

Virus protection

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

Adobe Employees

Employee Access to Customer Data

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

Background Checks

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

Employee Termination

When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. In the event that Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

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

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

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

Customer Data Confidentiality

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

Security compliance

All Adobe services are governed by a comprehensive set of documented security processes and have been subject to numerous security audits to maintain and improve quality. Adobe services are under continuing self review to ISO 27001 standards and the Shared Cloud underlying services infrastructure has a SOC 2 - Security certification.

Adobe is in the process of developing, implementing, and refining the security processes and controls for Creative Cloud operations in order to comply with the requirements for SOC 2 Trust Services Principles and the ISO 27001 security standard. Please visit http://www.adobe.com/security/resources.html to view a list of security white papers including the Adobe Security and Privacy Certifications white paper for more information on compliance and Adobe's overall security strategy.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Media Optimizer 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, please visit: http://www.adobe.com/security

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com