Adobe Primetime Security Overview

Adobe Security

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 enables us to continually build security into the products and services we offer.

This white paper describes the proactive approach and procedures implemented by Adobe to help increase the security of your data and Adobe Primetime experience.

About Adobe Primetime

Adobe Primetime helps operators and programmers reach viewers on IP-connected screens, creating more value for pay-TV service and strengthening brand affinity for content owners. With a unified, highly secure workflow for live, linear, and video-on-demand (VOD) programming, Adobe Primetime delivers an engaging, personalized viewing experience on desktops and a wide range of devices.

Adobe Primetime includes five (5) distinct capabilities:

- **Adobe Primetime Authentication** — Delivers a universal, user-friendly system for unlocking pay-TV content on devices using integrated authentication and authorization to easily verify subscribers in Pay-TV operator sites and apps.
- **Adobe Primetime Ad Decisioning** — Provides Primetime management, creative trafficking, forecasting, inventory management, partner management, reporting, and TV Everywhere support to improve operational efficiency and visibility.
- **Adobe Primetime Ad Insertion** — Allows the monetization of TV programming across digital devices by dynamically inserting ads into live, linear, and VOD content.
- **Adobe Primetime Cloud Digital Rights Management (DRM)** — Provides a scalable and efficient workflow for delivering and protecting premium video content across desktops and devices and platforms.
- **Adobe Primetime TVSDK** — Enables access to the key features necessary for premium video delivery, including content preparation, DRM, ad insertion, variable bitrate selection, hooks to collect engagement and quality-of-experience data, and more.

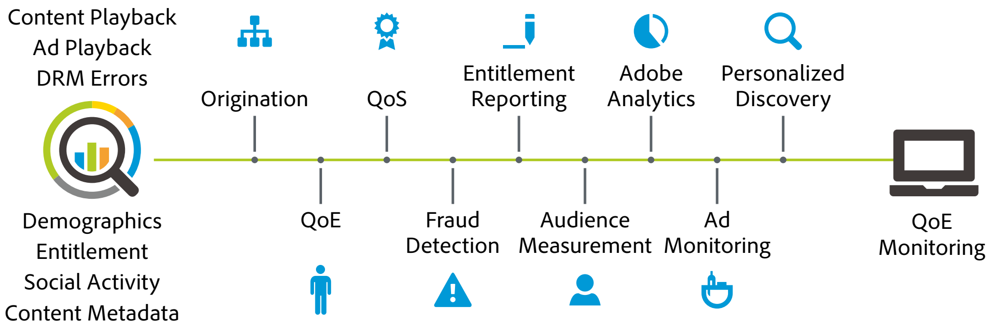

Figure 1: Adobe Primetime application architecture

Application Security and Network Architecture

Adobe Primetime components are hosted in one of three locations based on the specific component. Primetime DRM is hosted on Amazon Web Services (AWS) infrastructure; Primetime Authentication and Primetime Ad Decisioning are hosted at Adobe's own data centers; and Adobe Ad Insertion is hosted on both AWS and Adobe's secure data centers in a hybrid hosting model.

For information on AWS and Adobe hosting location security, please see the Adobe Primetime Hosting section below.

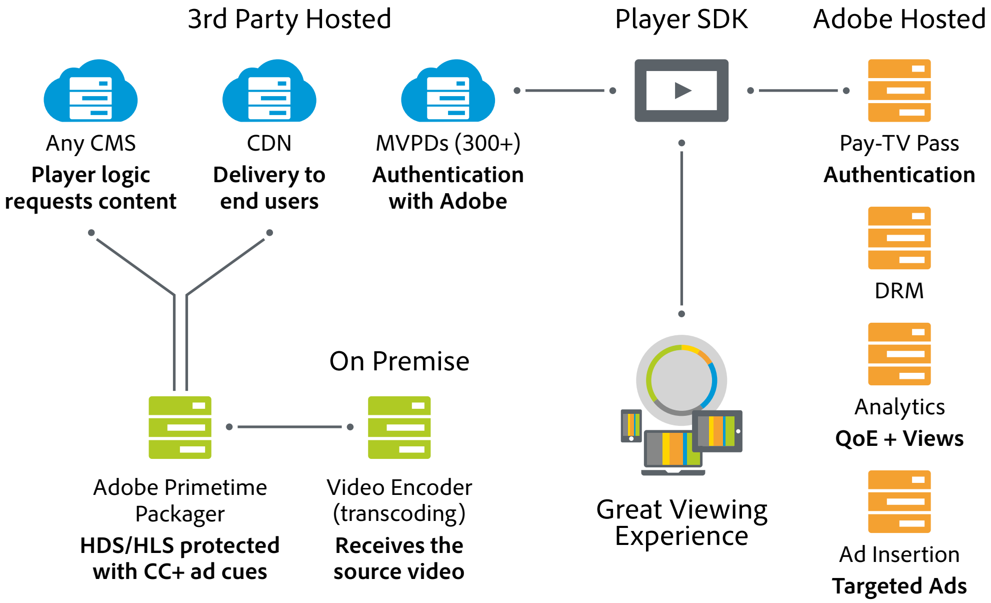

Figure 2: A typical Adobe Primetime deployment

Adobe Primetime Data Flows

Each Adobe Primetime component has its own, specific data flow. These data flows are outlined in the sections below:

Primetime Authentication

Primetime Authentication mediates entitlement transactions (authentication and authorization) between programmers and Pay TV providers, facilitating viewer access to subscription content. The Primetime Authentication services can be accessed through an SDK (multiple platforms) or directly through an API. Programmers then integrate the SDK or use the API in their own applications to query subscription databases to determine access rights to content.

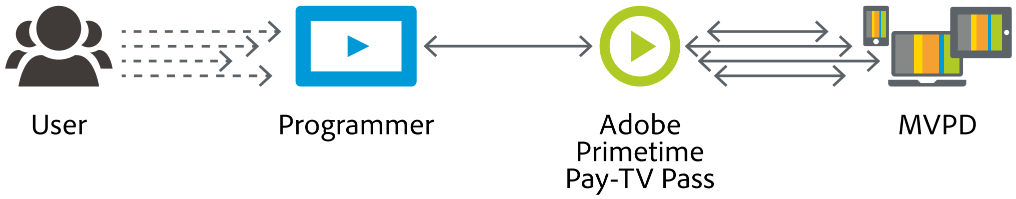

Figure 3: Primetime Authentication data flow

Primetime Ad Decisioning

Adobe Primetime Ad Decisioning provides a player plug-in and SDKs enabling communication between the player and Adobe Primetime ad server. It handles the request and playback of ads as well as the pinging of impression calls as instructed by Adobe Primetime Ads server ad response or 3rd party ad response. These player SDKs/plug-ins are used by third-party online video players to interface with the Primetime Ad Decisioning ad platform. SDKs are available for multiple platforms, including Adobe Flash® Player, iOS, HTML5, Silverlight, Android. The SDKs are provided to clients via the Adobe support organization. The plug-in sends a GET request (**Ad Call request**) to the server. When there are key-values specified through the player, the plug-in attaches them as POST parameters and sends a POST request to the adserver. The XML response from adserver is parsed by the plugin. Once the XML is parsed, the plug-in informs the player that ads are ready to be played.

The Adobe Primetime ad server is the core component of Adobe's ad serving platform. It manages the incoming ad request and the return of a proprietary (SMIL based) ad response or IAB standard-compliant (VAST or VMAP) ad response for player ad playback. The Ad Server receives and ad-request from an Ad Player and processes it. It decides the ads by running auction and returns result to Ad Player according to requested protocol. Auction happens on the list of Ads that are present in server's in-memory database considering the targeting criteria. The session continues as interaction between player and asset server. New updates are delivered in real time from content server and ingested into Ad Server's fast in-memory database. User sessions are logged and sent to proc server for further processing.

The entire process is monitored by M/Monit agent capable of conducting automatic maintenance and taking action in case of errors. Ad server produces one log record for each event (such as ad call, impression tracking, stat event, etc.). Log records are separated by empty line (\n\n). Each log record starts with one main line (ADP, EAD, ST, AS, etc.) and might be followed secondary lines (ADA, K, ADU, WARN, etc.) that contains additional information.

These logs are sent to procserver which processes them to calculate monetizable asset calls.

Adobe Primetime's processing servers fetch, parse, filter, and pre-aggregate log data from our ad serving hubs. They compute real-time summaries and load the summaries into the applicable databases for further processing and reporting:

- Processing servers — Responsible for fetching raw logs from ad server and filtering the invalid and fraud logs. All the logs which are left will be processed further and that data is ingested in Database and S3 outbox. All the raw logs will be kept in outbox folder so that log archive can pull them and keep them for future.
- Logarchive servers — Pull all the logs from procserver and aggregate these logs on the basis of month, hour. These logs are then backed up by tech ops for any further requirement.
- Postproc servers — Pull logs from logarchive server and analyze these logs for any fraudent activity done by unknown entity and create daily log files so that these can be analyzed on monthly basis.

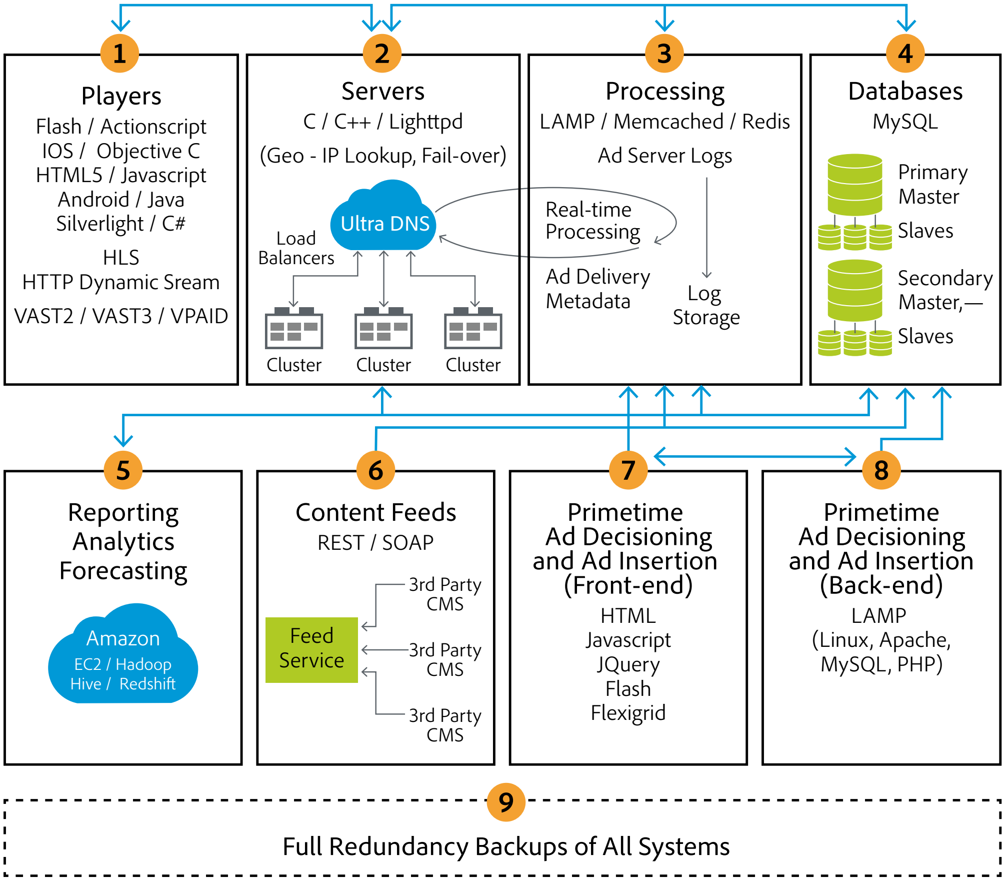

Figure 4: Primetime Ad Decisioning data flow

Primetime Ad Insertion

Primetime Ad Insertion includes a manifest server component, which coordinates the systems that provide content, provide ads, play video, and track ads. The server receives M3U8-encoded playlists (manifests) that client video players receive from content providers, stitches in ads from ad providers, and passes those manifests, with ads stitched in, to video players. It supports both client-side and server-side ad tracking and communicates with CDNs (Content Delivery Networks) using an HTTP-based web service interface.

To use Primetime Ad Insertion, the publisher sends the content URL and information for the ad server to the client. The client uses the information from the publisher to generate a Manifest Server URL, sends a GET request to that URL, and establishes a session with the Manifest Server. The server then obtains content from the CDN, including information about where to place ad breaks, passes the client-supplied information to the ad server, and receives ads and ad-tracking URLs from the ad server. If a supplied ad is not in HLS format, the manifest server sends it to CRS for conversion to that format. After stitching ads into the playlist, the Manifest Server sends the new playlist to the client as a file in M3U8 format. The client then plays the content with the stitched-in ads and sends reports at the specified times to the specified URLs.

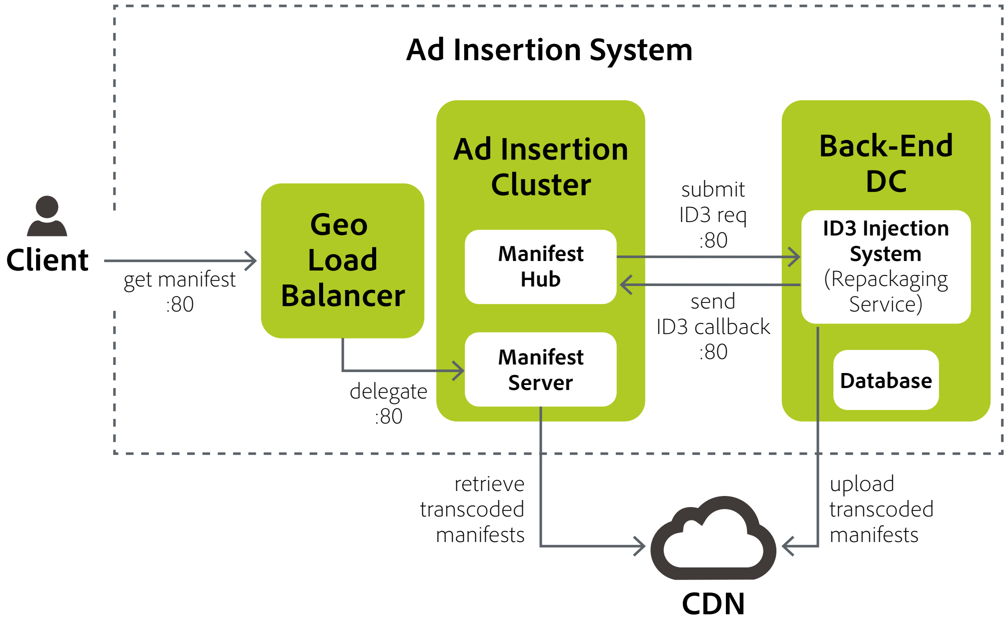

Figure 5: Primetime Ad Insertion data flow

Primetime Cloud DRM

Primetime Cloud DRM issues DRM licenses to video applications that wish to play DRM-protected content. The video application may optionally include custom data into the request to Cloud DRM before making the license request. This custom data may be derived locally on the device, or by querying a third-party custom service designated by the video application. When Cloud DRM receives a license request, the presence of additional custom data (Authentication Token) will determine whether or not Cloud DRM communicates with a third party Custom Authentication and Entitlement server to determine if this particular license request shall be granted a license.

Primetime Cloud DRM retrieves configuration data from a database which is administered by the Adobe Administration Service for Cloud DRM.

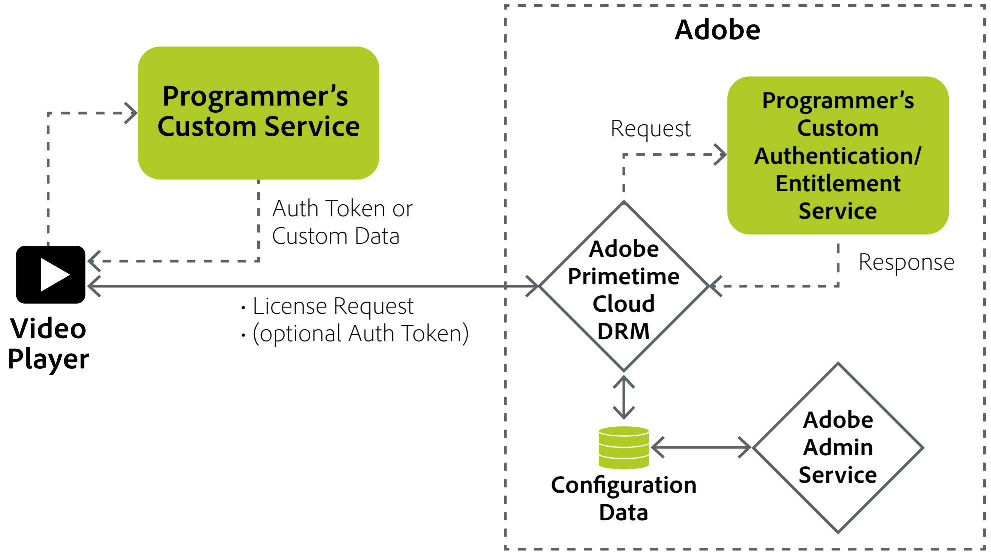

Figure 6: Primetime DRM data flow

User Authentication

Customers primarily access and use Adobe Primetime through the interface included in Adobe Marketing Cloud. Users of Primetime Ad Decisioning tools gain access via separate HTTPS-secured web UI or web services interfaces.

User Identity Services: Accessing Adobe Primetime through Marketing Cloud

Users can access the Marketing Cloud interface to Adobe Primetime in one of three (3) different types of user-named licensing. Each of these types uses an email address as the user name and include:

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 Adobe Primetime 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 asset—are provided by the customer's Single Sign-On (SSO) identity management system and are created, owned, *controlled by the customer.* 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

User Identity Services: Accessing Adobe Primetime Ad Decisioning

Users of the Ad Decisioning tool use a separate username and password based authentication mechanism unique to the product and managed by Adobe.

Adobe Primetime Products Hosted in Adobe Data Centers

Primetime Authentication, Primetime Ad Decisioning and Primetime Ad Insertion are hosted in Adobe-hosted data centers.

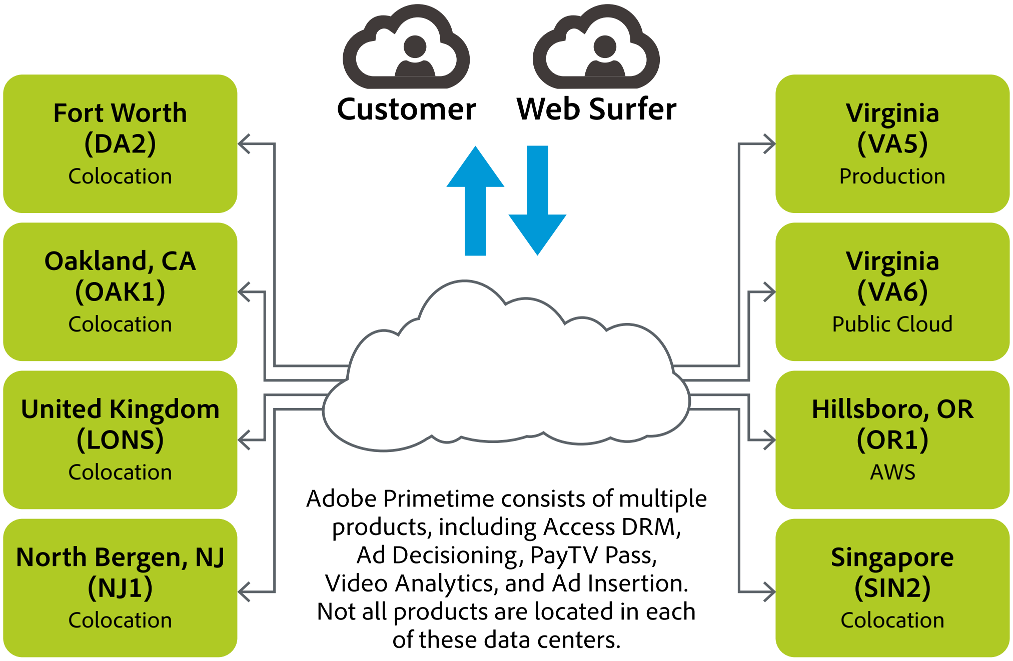

Figure 7: Adobe Primetime hosted data center locations

Adobe stores all Adobe Primetime customer data in data centers located closest to the customer's geographic location (e.g., North America, Europe, or Singapore) except for Primetime Ad Decisioning customer data, which is hosted in the Fort Worth, TX location.

Inter-Product Communication Security

Any data that is transmitted between Adobe Primetime components over the Internet is secured via HTTPS using 256-bit AES encryption.

For Primetime Ad Decisioning: Hub and spoke architecture (Hub= back end, spokes = Adobe adservers worldwide). Intra-product communication occurs via IPSEC tunnels between Adobe data centers managed by Adobe Network Engineering.

For Primetime Ad Insertion: Hub and spoke architecture (Hub= back end, spokes = Adobe adservers worldwide). Intra-product communication occurs via IPSEC tunnels between Adobe data centers managed by Adobe Network Engineering.

For Primetime Authentication: Active/active architecture. The DA2 and OAK1 data centers communicate via IPSEC tunnels managed by Adobe Network Engineering.

For Primetime DRM: No communication with other product components.

Adobe Primetime Hosted Network Management

Because of the data collection, data content serving, and reporting activities conducted over the Adobe Primetime network, the security of the network is important to us. To this end, the network architecture 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

For Primetime Authentication and Primetime Ad Decisioning, all data is stored in the same server cluster, with access granted on a per customer basis. The only access to these servers and databases is via the Primetime application. All other access to the application and data servers is made only by authorized Adobe personnel and is conducted via encrypted channels. We separate our testing environments from our production environments, and we do not use customer data in testing environments unless specifically granted permissions by the customer.

Secure Management

Adobe deploys dedicated network connections from our corporate offices to our data center facilities in order to help enable secure management of the Adobe Primetime 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 Primetime 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 without service disruption. 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 Primetime 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 Primetime 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. In addition, the Ad Decisioning tool uses its connected ad servers to help detect suspicious traffic. Adobe regularly updates all sensors and monitors them for proper operation.

Service Monitoring

Adobe monitors all of the servers, routers, switches, load balancers, and other critical network equipment on the Adobe Primetime 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 contracts with multiple third parties to perform external monitoring.

Data Backups

Data backup policies differ slightly per Adobe Primetime component based upon customer needs and obligations. Below are the general backup policies for most Primetime product components:

- Adobe backs up Adobe Primetime customer data on a daily basis. Each backup is stored for up to seven (7) days by default. An encrypted copy (using GPG) of the database backup is sent offsite daily as well. In case of database loss, the last daily backup can be restored. Point-in-time recovery can be done if data loss results from a customer action. Any of the last seven (7) backups can be used.
- Adobe also backs up the Primetime infrastructure configuration files on a daily basis. Backups are done using snapshots. A snapshot of all configuration data is backed up daily and transferred off-site using encrypted transmission.
- Because all backups are performed online, for both the database and the Adobe Primetime configuration, the application and servers are available to users for the duration of the backup period.

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 try to schedule maintenance blackouts away from periods of high network traffic.

Patch Management

In order to automate patch distribution to host computers within the Adobe Primetime 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.

The Adobe Primetime team conducts scans on many critical production system components at a minimum of once per month. These scans are configured to pull the latest vulnerabilities from external industry sources, such as US CERT, detect vulnerabilities in production systems, and score these vulnerabilities according to risk impact and likelihood. Scores range from 0 to over 10,000. Higher scores represent higher impact vulnerabilities. Vulnerabilities with a score of 2500 or higher have JIRA tickets automatically generated for solution teams to patch the associated vulnerability appropriately. On a bi-weekly basis, these vulnerabilities are reviewed with the technical operations security champion to address. Once vulnerabilities are addressed scans are preformed again to validate the vulnerabilities have been corrected.

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 Primetime 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 exceeded. Only authorized Adobe Digital Marketing Information Security Team personnel can access the hardened logs generated by Primetime systems. Adobe retains raw logs for one year.

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 controls access to all hardware in Adobe-owned or -leased hosting facilities against unauthorized access. All facilities that contain production servers for the Adobe Primetime 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 help 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 Primetime 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 help 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 is 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 facilitate an effective and accurate recovery.

Failover Process

When an event is determined to result in long-term service disruption, Adobe will reconfigure DNS to send requests to a secondary data center location not affected by the disruption.

DNS record TTL (time to live) is set to allow this switch to the secondary location to happen quickly. While product components are in a failover mode, customers are notified of the ongoing situation with regular status updates. If the disaster at the primary server locations is serious enough to have destroyed or make any needed historical data there unavailable, Adobe will work to restore that data from backups stored at off-site locations.

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 held requests will be processed sequentially. Time required to recover historical data from off site may take up to an additional ten (10) days.

Adobe Primetime Products Hosted on AWS

Adobe hosts the Primetime Ad Insertion and Primetime DRM products on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the United States, EU, and Asia Pacific. 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 Adobe Primetime components 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 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.

About Amazon Web Services (AWS)

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 Primetime customer data in Amazon Web Services' US East Region. For customers within the United States, Adobe stores analytic data in AWS's San Jose, California or Dallas, Texas facilities. For customers outside the U.S., Adobe stores analytic data in the London, U.K. facility of Amazon Web Services.

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, such as Primetime, 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 Primetime components using industry-standard intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Logging

Adobe conducts server-side logging of Primetime 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 stores all Primetime data in Amazon S3, which provides a storage infrastructure with high durability. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in an Amazon S3 region. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper.

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 Adobe Primetime.

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 Data Center 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 traffc 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, Adobe Primetime security team performs a risk assessment of the Primetime application prior to every release. Conducted by highly trained security staff trusted with securing the network topology and infrastructure and Primetime application; the security reviews look for insecure network setup issues across firewalls, load balancers, and server hardware and also application level vulnerabilities. The security touchpoints include exercises like threat modeling coupled with vulnerability scanning, static and dynamic analysis of the application. The Primetime security team partners with the 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 Primetime at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Primetime organization to coordinate the mitigation effort.

For Adobe cloud-based services, including Primetime, 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 Primetime 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.

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 Primetime 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.

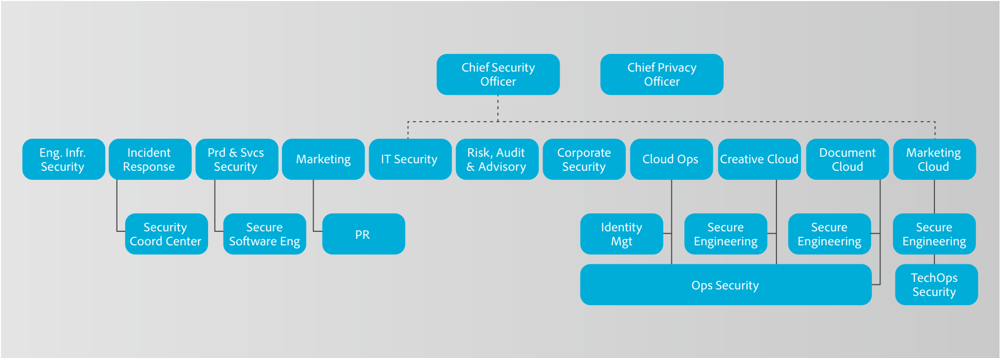

Figure 8: The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Primetime 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 Primetime 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 Primetime 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

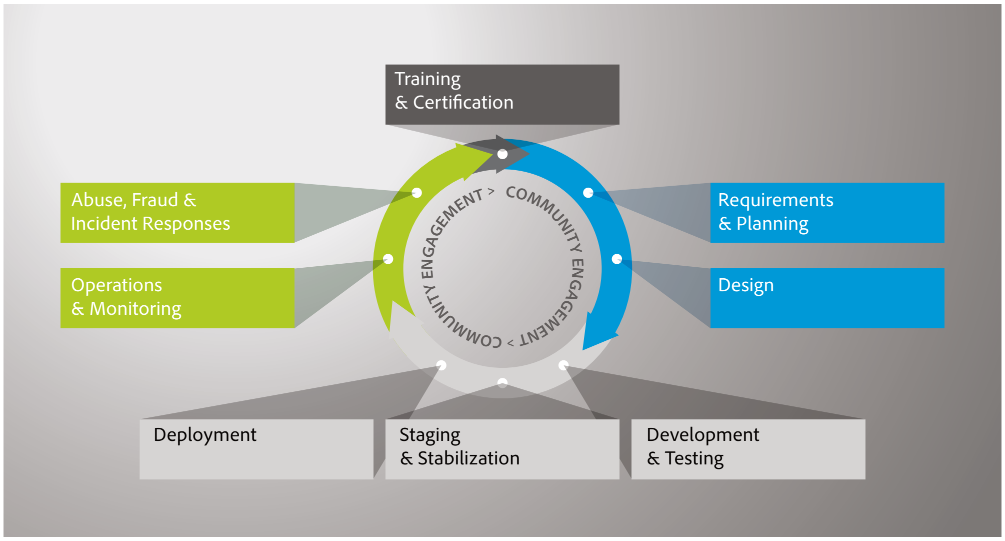

Figure 9: Adobe Secure Product Lifecycle (SPLC)

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 Primetime 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 previous 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.

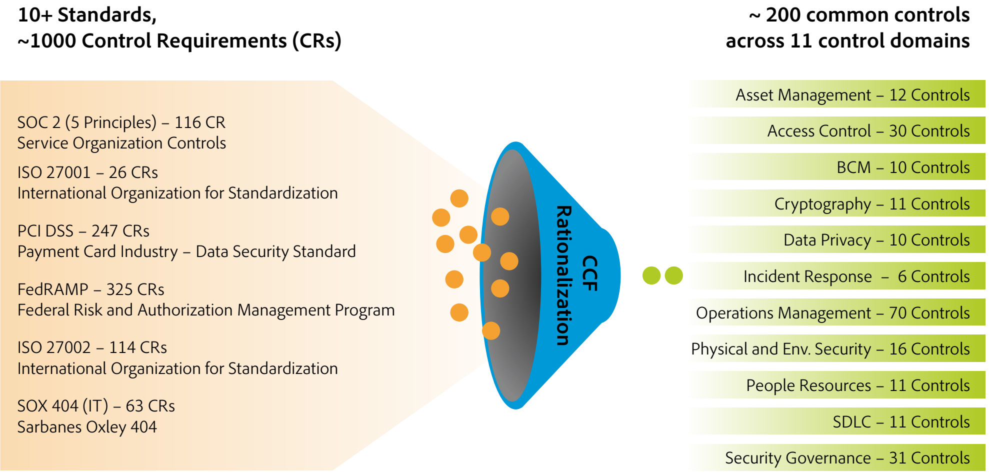
10+ Standards,
~1000 Control Requirements (CRs)
~ 200 common controls
across 11 control domains
SOC 2 (5 Principles) – 116 CR
Service Organization Controls
ISO 27001 – 26 CRs
International Organization for Standardization
PCI DSS – 247 CRs
Payment Card Industry – Data Security Standard
FedRAMP – 325 CRs
Federal Risk and Authorization Management Program
ISO 27002 – 114 CRs
International Organization for Standardization
SOX 404 (IT) – 63 CRs
Sarbanes Oxley 404
CCF
Rationalization
Asset Management – 12 Controls
Access Control – 30 Controls
BCM – 10 Controls
Cryptography – 11 Controls
Data Privacy – 10 Controls
Incident Response – 6 Controls
Operations Management – 70 Controls
Physical and Env. Security – 16 Controls
People Resources – 11 Controls
SDLC – 11 Controls
Security Governance – 31 Controls

Figure 10: The 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.

Adobe Employees

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Primetime, 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 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

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Primetime application 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 stay ahead of malicious activities and help ensure the secure 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

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

www.adobe.com