Adobe® Experience Manager Livefyre Security Overview

Table of Contents

Overview

At Adobe, we take the security of your digital experiences 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 security best practices and trends and continually build security 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 Adobe® Experience Manager Livefyre experience and your data.

About Adobe Experience Manager Livefyre

Part of Adobe Marketing Cloud, Adobe Experience Manager Livefyre (lets you engage consumers through a combination of real-time content, conversation, and social curation. Experience Manager Livefyre puts the billions of pieces of content created each day at your fingertips, enabling you to integrate that content into your digital marketing assets, websites, and mobile apps to increase traffic, user engagement, and revenue.

Adobe Experience Manager Livefyre Application Architecture

The Experience Manager Livefyre solution includes the following eight (8) sets of capabilities:

Content Curation and Asset Management: Experience Manager Livefyre helps you find, store, organize, and tag user-generated content (UGC), transforming UGC into assets you can use time and again. You can find content that fits your brand from Twitter, Facebook, Instagram, YouTube, or any other site and then narrow down the results by filtering for language, location, and more. With Experience Manager Livefyre, you can collect and find the kind of content you want using granular rules and then automatically stream it to your digital properties or store it in your library for future use.

Publishing: Experience Manager Livefyre simplifies content creation by giving your teams everything they need to craft, curate, and live-blog engaging stories. Multiple editors can work and collaborate on the same stories simultaneously, updating, reviewing, and publishing content instantly, and from anywhere. It's a breeze to search, sort, and share UGC or upload your own assets. Preset feeds can scan nonstop for relevant content that you can then incorporate into your stories.

Moderation: The sophisticated moderation tools in Experience Manager Livefyre allow you to turn user-generated content into a safe source of high-quality assets that are everything you're looking for and nothing you're not. You can moderate continuously, without a dedicated team, because Livefyre works automatically — all day and all night.

Engagement: With the embedded applications of Experience Manager Livefyre, you can get your audiences more involved all across your sites. It's easy with flexible and responsive features that fuel engagement. Applications such as Comments, Reviews, Sidenotes, Mediawalls, Polls, and Chat provide engaging social experiences that inspire loyalty and build a valuable community that grows over time.

Rights Management: User-generated content requires consent of the author for use in many contexts. Experience Manager Livefyre provides a rich feature set that enables customers to request and negotiate usage rights to content generated on social networks.

Federated Single-Sign-On: If you have a user management system, you can federate it with Experience Manager Livefyre, enabling seamless user handoff to Experience Manager Livefyre's embedded applications while retaining full control over login and registration processes.

Identity Management: If you don't have an existing user management system, Experience Manager Livefyre provides Livefyre Identity, a software-as-a-service (SaaS) user management system. Through Livefyre Identity, your users can log into applications either using one of their social media accounts or a site-specific email-based account.

Content Pipeline: Powering the solution is a robust data pipeline, which enables real-time features across the platform. These features include automatic analysis and tagging; rich rule-based routing to power artificially intelligent and human moderation activities; and scalable real-time distribution to millions of concurrent users.

Adobe Experience Manager Livefyre Data Flows

Each component of Experience Manager Livefyre has a unique data flow, unified by the Content Pipeline. These data flows are detailed in the following sections:

UGC Ingestion and Curation Data Flow

End-users engaging with Experience Manager Livefyre embedded applications produce a variety of content including posts, likes, and flags. These users post to Experience Manager Livefyre servers, where content is injected into the Content Pipeline for processing.

Enabled through configuration options, users may also upload photos and videos that can be attached to their posts. Users trigger a file upload button, which opens a dialogue provided by Filestack. The user locates the selected media and then streams it to Filestack servers, which validate content types and transmit the media to an Adobe Experience Manager Livefyre-owned and managed AWS S3 bucket. During this process, Filestack may require credentials to 3rd party services which are stored temporarily on Filestack's servers and attached to the user's session to complete the transaction. After media is located and transferred, Filestack returns metadata about the upload and attaches it to the user's submission of content.

Experience Manager Livefyre collects social content directly from social networks (e.g., Twitter, Instagram, Facebook, YouTube, and others) based on customer-defined rules and pushes this data into the Content Pipeline.

This content is collected via API calls to the networks or via streaming APIs. Specific APIs, such as the Instragram API, require OAuth credentials. To collect from these sources, a user with administrator privileges authenticates through a browser and approves Livefyre to act on their behalf. The source then passes Adobe Experience Manager Livefyre OAuth credentials through a server-to-server call. The credentials are stored and encrypted using AWS KMS, a key management service implementing the 256-bit AES-GCM encryption algorithm. For more details on KMS, see http://docs.aws.amazon.com/kms/latest/developerguide/crypto-intro.html. Adobe Experience Manager Livefyre retains these credentials until they expire or upon customer termination.

Ultimately, streamed content may be stored in the Experience Manager Livefyre Asset Library or ModQ, or it may be delivered to an Experience ManagerLivefyre engagement app.

Asset Library Data Flow

The Livefyre Asset Library is a repository of content that users can manage and organize for future use and reuse.

Adobe Experience Manager Livefyre supports ad-hoc queries of content on social networks through a search interface. Results of these searches may be optionally filtered for nudity in imagery, in which case images are downloaded temporarily by a server that performs in-memory analysis.

Users may also upload content directly to the Asset Library. Filestack, as described above, negotiates this process with the user via the browser. A reference (as URL) to the uploaded content is saved in the asset library. All metadata is saved in an Elasticsearch cluster.

Publishing Data Flow

Adobe Experience Manager Livefyre supports a collaborative editing experience for media-rich publishing via Storify, a tool specifically designed for live blogging. Storify allows multiple editors to draft content in real time and publish to the range of Experience Manager Livefyre embedded apps. Editors draft content and store it in a local Storify database until publication. When the editor decides to publish a post, the content then enters the Content Pipeline and Publishing data flows.

Delivery Data Flow

Adobe Experience Manager Livefyre provides several mechanisms by which data can be published or delivered to end-users or external systems:

- **Engagement Applications** – Enables users to publish content to in-browser visualizations and embedded widgets, such as Comments, Reviews, Media Walls, etc., which deliver the content to consumers through streaming APIs. Experience Manager Livefyre optimizes load times by prerendering to content in batch to S3 for optimized delivery and fronted S3 with Varnish HTTP accelerators and Fast.ly CDN.
- **Opt-in Emails** — Delivers personalized content to end-users (based on their subscriptions) using the Sendgrid email delivery service.
- **Syndication APIs** — Enable users export content to non-Adobe systems.
- **Real-time Activity Stream** — Let end-users to consume streams of content and activity via API in real time.
- **Rights Request Stream** — Provides users with a stream of rights-requested content.
- **Fyrehose** — Publishes all activities in the system, including content creation, moderation actions, and login activity, to files in an AWS S3 bucket readable only by the customer.

Moderation Data Flow

Adobe Experience Manager Livefyre provides many tools for automated and manual moderation, which are designed to reduce moderation workloads and enhance brand trust and affiliation. Users can choose from a wide range of options for automatically managing content, including pre-moderation, filtering, banning, and bozo'ing, which configure the *UGC Ingestion and Curation Data Flow*.

Pre-moderation can be set globally or at various points in the system. Pre-moderated content will not be distributed to end users until that content is approved by privileged reviewers, at which point the content will be distributed to embedded applications or stored in the asset library.

Engagement Data Flow

Embedded Adobe Experience Manager Livefyre applications connect content delivery APIs to in-browser experiences. By embedding Experience Manager Livefyre Javascript via an HTML script tag, along with an embed code (instructions for loading a specific application), browsers' Javascript engines will load published content via API and render rich media experiences with a host of engagement features, depending on the application.

Rights Management Data Flow

Using the rights request functionality in Adobe Experience Manager Livefyre, customer can secure usage rights to content produced in Twitter and Instagram. Initially, the customer creates a link between social accounts from which they will be requesting rights. Through an OAuth2 negotiation, tokens are conveyed to Experience Manager Livefyre and stored encrypted with AWS KMS. After the account is set up, the customer can request rights to content.

To request rights, a customer curates content into their Asset Library, and then crafts a message which will be posted to the social network as a tweet or comment. The message is posted via authenticated API on the customer's behalf, and then Experience Manager Livefyre listens for replies via credentialed API calls. Experience Manager Livefyre matches replies back to the original rights request, and the replies are persistent as annotations with the content. If the end-users reply contains predefined signals of acceptance or rejection, Experience Manager Livefyre updates the state of the contents as granted or rejected.

Customers with the latest Adobe Experience Manager Assets installation can configure their system to connect to Experience Manager Livefyre to download rights requested assets into their repository. When enabled, and Adobe Experience Manager instance contacts Experience Manager Livefyre with a privileged token, and requests content which has not already been synced. On download Adobe Experience Manager retrieves the metadata in Experience Manager Livefyre, as well as the binaries of attached media and persists it to the local JCR repository.

Content Pipeline Data Flow

The Adobe Experience Manager Livefyre Content Pipeline powers all Experience Manager Livefyre capabilities, processing and distributing hundreds of millions of user-generated content activities per day. Experience Manager Experience Manager Livefyre encodes and routes all actions performed on content through the pipeline, where listeners analyze, enrich, store, and/or route the content through the system. Presets and configurable business rules dictate how and what data is processed. The pipeline itself uses Apache Kafka and Redis for the queuing and distribution of messages among sub-systems. In some cases, small amounts of data or metadata are stored in Redis clusters for very low-latency distribution or ephemeral caching.

Content flowing through the system, such as social media posts, comments, and reviews, travel the pipeline in JSON or binary formats. These formats included authorship information, text content, and possibly URLs to websites or media. URLs to media—such as avatar images, photos, or videos—are linked to the original source; for example, Instagram photos are referenced by URLs to the original media served via the Instagram CDN.

In the content enrichment phase, Experience Manager Livefyre fetches and scrapes embedded links found in content for Oembed metadata, OpenGraph tags, and HTML meta-tags. This data is only extracted if the embedded URL is publicly accessible via uncredentialed HTTP requests. In the majority of cases, Experience Manager Livefyre fetches the content directly. For a subset, Experience Manager Livefyre uses Embed.ly to extract the information. This derived information is persisted with content to enable rich media embeds, such as thumbnails and video players.

The pipeline includes sub-systems for content normalization and automated content analysis. The content analysis engine checks for spam, abuse, and objectionable content. Media linked via URL may also be downloaded to process memory for automated classification and content recognition. The derived information will be attached to the content as text enrichments. The content, classifications, and enrichments are retained in S3 for tuning and further development of the classification engine.

After classification, and based on presets defined by the customer, Experience Manager Livefyre stores the user-generated content in one of three (3) database clusters, depending on its intended use:

- **ModQ** — Temporarily stores content for review by the user, who can then publish the best content to an app or save the content to the asset library. ModQ stored for up to six (6) months before purging.
- **Asset Library** — Permanently stores content for use and reuse.
- **Engagement Application** — Publishes content directly to an app without human intervention.

Experience Manager Livefyre indexes all content to Elasticsearch clusters in order to power full-text queries. In addition, Experience Manager Livefyre partitions content within these clusters by customer identifier: all queries by applications are filtered with that identifier. After persistence and indexing, content progresses through the pipeline through one or more flows for delivery.

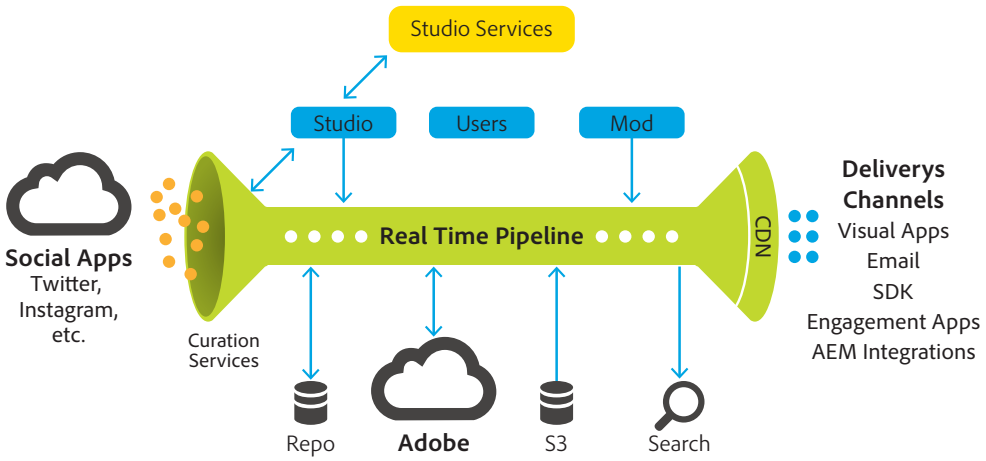

Figure 1: Adobe Experience Manager Livefyre Data Flow

End-User Single Sign On for Engagement Applications

Experience Manager Livefyre.js Auth, a library that enables Single Sign On (SSO) within the end user's browser, enables your end-users to interact with Experience Manager Livefyre embedded applications on your digital properties, such as posting comments, writing reviews, and "liking" your content.

To sign in, the end user registers and logs in through the process defined by his or her user management system (UMS), which then generates a JSON Web Token that is used by Experience Manager Livefyre for authentication and authorization. This token contains an ID, a display name, an avatar URL, and a user handle. The token is signed using the SHA 256 hashing algorithm and is passed along to Experience Manager Livefyre.js Auth to be used for authenticated HTTPS calls to Experience Manager Livefyre's servers. Additional profile details can be passed in SSL-enabled server-to-server calls.

Adobe Experience Manager Livefyre Identity

Customers without their own user management system may use Experience Manager Livefyre Identity, a SaaS UMS. To integrate Experience Manager Livefyre Identity functionality, the customer embeds the appropriate JavaScript on their site. When an end-user authenticates, an SSO token is exchanged with the Livefyre engagement application/s according to the process described above. More information on integrating Livefyre Identity can be found at http://answers.livefyre.com/developers/identity-integration/livefyre-identity/

Experience Manager Livefyre Identity gives customers the choice of which OpenID Connect provider/s to enable, as well as whether or not to enable and disable password login. To enable third-party identity providers, Experience Manager Livefyre Identity must be configured with application keys and secrets in order to perform OAuth2 negotiations. Experience Manager Livefyre stores all credentials and user passwords encrypted with AWS KMS. All personal information beyond basic identifiers in Livefyre Identity are encrypted.

Adobe Experience Manager Livefyre User Authentication

Access to Experience Manager Livefyre's management console requires authentication with username and password. For users accessing Experience Manager Livefyre using Adobe IDs, Adobe leverages the SHA 256 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 Experience Manager Livefyre 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 Adobe Livefyre 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 customer's IT department. Adobe integrates with most SAML 2.0 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

For more information on specialized methods for accessing Experience Manager Livefyre data and content via approved applications, please refer to the product documentation at https://marketing.adobe.com/resources/help/en_US/livefyre/

Adobe Experience Manager Livefyre Core Operational Security

Adobe hosts Experience Manager Livefyre in Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), and Amazon Simple Storage Service (Amazon S3), in the United States. Amazon EC2 is a web service that provides resizable compute capacity in the cloud, making web-scale computing easier. Amazon Relational Database Service provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. Amazon S3 is a highly redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere. Additionally, Adobe Experience Manager Livefyre applications make use of other services in the AWS ecosystem, such as AWS Cloudfront, AWS Route 53 (DNS), AWS Key Management Store (KMS), and AWS Kinesis.

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 Experience Manager Livefyre resides. In turn, Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and Adobe Experience Manager Livefyre 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.

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.

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

Data is logically partitioned by client, and sharded into highly available and replicated database clusters. These servers and databases can only be accessed via the Experience Manager Livefyre application. All other access to the application and data servers by authorized Adobe personnel can only occur at the request of a customer due to a reported issue and, when necessary, via encrypted channels. Adobe separates testing from production environments, and we do not use customer data in testing environments unless the customer specifically grants permission to do so.

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.

Firewalls and Load Balancers

The firewalls implemented on the Experience Manager Livefyre servers 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 servers containing customer data with non-routable IP addresses (RFC 1918). These private addresses, combined with the Experience Manager Livefyre 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 Experience Manager Livefyre 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 sensors and monitors them for proper operation.

Service Monitoring

Adobe monitors its servers, routers, switches, load balancers, and other critical network equipment on the Experience Manager Livefyre 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 multiples other services and tools to perform external 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.

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 Experience Manager Livefyre, which can be found here.

Experience Manager Livefyre Managed Services follows a Change Approval Board (CAB) process for any and all changes that could impact customer experience. The CAB process focuses upon enforcing stability and availability, while permitting an agile response to emerging issues, and providing internal process transparency and accountability.

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

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.

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.

Adobe conducts server-side logging of Experience Manager Livefyre 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.

Data Storage and Backup

Adobe stores all Experience Manager Livefyre customer 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.

Access Auditing

Only authorized users can access administrative tools. In addition, Adobe logs all Experience Manager Livefyre production server access attempts for auditing.

Disaster Recovery

In the event that one of the AWS zones 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 facilitate an effective and accurate recovery.

Failover Process

In a routine small-scale operational failure or degredation within the environment, failover processes are automatic to redundant and highly available instances in other AWS zones. Most cases are automatic, while some require minimal manual intervention. When an event is determined to result in long-term service disruption, Adobe will reconfigure DNS and internal networks to a location not affected by the disaster. Adobe will instantiate new instances to restore the cluster to full capacity. During this time, queue-based systems may experience delays in processing or delivery, such as search indexing, curation streams, and realtime updates.

Recovery Process

When the affected 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 the environment rebalanced across availability zones. This process may be completed over days or weeks, with negligible impact to the users of the service.

Adobe Experience Manager Livefyre Administrative Security Features

Adobe Experience Manager Livefyre enables administrators to control access to customer UGC. Options include strong passwords, password expiration, IP login restrictions, and email domain restrictions. For more information, please go to https://marketing.adobe.com/resources/help/en_US/reference/security_manager.html

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 Experience Manager Livefyre security team performs a risk assessment of the Livefyre application prior to every release. Conducted by highly trained security staff trusted with securing the network topology and infrastructure as well as the Livefyre 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 Experience Manager Livefyre 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 Experience Manager Livefyre at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Captivate organization to coordinate the mitigation effort.

For Adobe cloud-based services, including Adobe Experience Manager Livefyre, 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 Adobe Experience Manager Livefyre 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.

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 Corporate Security

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 Experience Manager Livefyre 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.

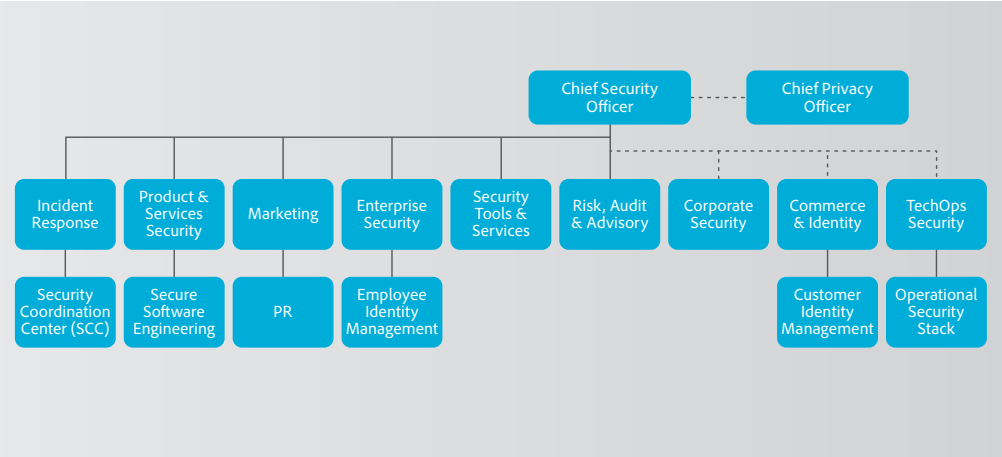

Figure 2: The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Experience Manager Livefyre 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 Connect 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 Experience Manager Livefyre 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

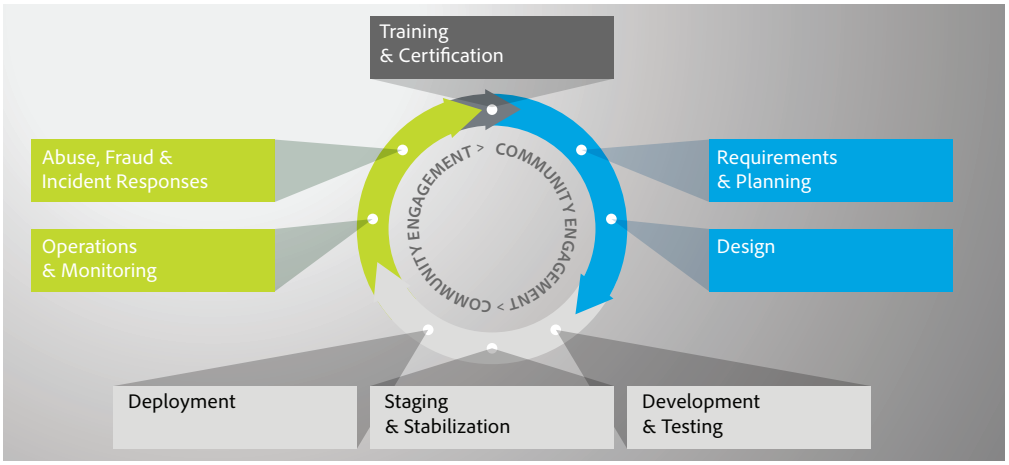

Figure 3: Adobe Secure Product Lifecycle (SPLC)

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 Connect 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 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 Connect, 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.

Adobe Experience Manager Livefyre Compliance

The Adobe Common Controls Framework (CCF) is 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. In creating the CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,000 requirements down to Adobe-specific controls that map to approximately a dozen industry standards.

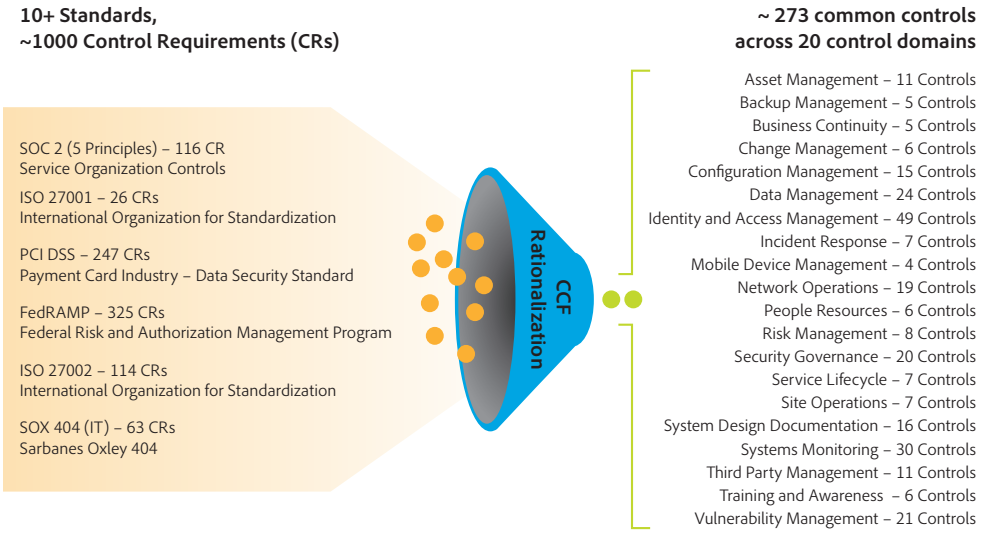

Figure 4: The Adobe Common Controls Framework (CCF)

Current Regulations and Compliance for Adobe Experience Manager Livefyre

SOC 2 is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Experience Manager Livefyre is SOC 2 – Type 2 (Security & Availability) compliant.

ISO 27001 is a set of globally adopted standards that outline stringent security requirements and provide a systematic approach to managing the confidentiality, integrity, and availability of customer information. Experience Manager Livefyre is compliant with ISO 27001:2013.

The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions safeguard their customers' personal data. Experience Manager Livefyre is GLBA-Ready, meaning that it enables our FSI customers to comply with the GLBA Act requirements for using service providers. Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

The Federal Risk and Authorization Management Program (FedRAMP) is a collection of mandatory standards established by the U.S. Federal Government for security assessment and purchase approval for cloud solutions. Experience Manager Livefyre is compliant with FedRAMP.

The Health Insurance Portability and Accountability Act (HIPAA) is legislation that governs the use of electronic medical records, and it includes provisions to protect the security and privacy of personally identifiable health-related data, called protected health information (PHI). Experience Manager Livefyre is HIPAA-compliant, which means it can enable our enterprise customers to use our solutions in a way that they can meet their obligations under HIPAA regulations. Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

The U.S. Family Education Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. Student education records and directory information. Under FERPA guidelines, Adobe can contractually agree to act as a "school official" when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements. Ultimately the customer is responsible for ensuring their compliance with their legal obligations, that our products meet their compliance needs, and that they secure the products in an appropriate way. Experience Manager Livefyre is FERPA-Ready.

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. Adobe Systems Incorporated (our U.S. company) also adheres to the European Union Safe Harbor Privacy Program.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Experience Manager Livefyre solution and your confidential data. At Adobe, we take the security of your digital experience very seriously and we continuously monitor the evolving threat landscape to 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