Adobe Social Security Overview

Table of Contents

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 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® Social experience.

About Adobe Social

Adobe Social is a social management platform that ties data to your bottom line. A part of the Adobe Marketing Cloud suite of services, Adobe Social goes beyond just likes and follows to manage the deep relationship between your customers' sentiments and your business goals. With Adobe Social, you can monitor and moderate conversations, publish and promote content, and analyze engagement and conversion data in a single, mobile-friendly interface. What's more, Adobe Social lets you truly measure the impact of your social content by automatically attaching tracking codes to each piece of content, enabling you to identify what activities drive engagement and conversion. And with integration with other Adobe Marketing Cloud services, you can use these social insights to improve targeting strategies and optimize the customer experience.

Adobe Social Application Architecture

The Adobe Social solution includes four (4) components:

- **Listening:** Collects and categorizes public and private social data. The Listening component collects social data through the Twitter API and directly from other social networks (including Facebook, Google+, YouTube, LinkedIn, and Sina Weibo) and then sends all collected data through a categorization engine. This engine checks for spam, categorizes emotion, determines language, categorizes sentiment, and adds geographic data. The categorized data is then stored where it can be accessed by other systems via API calls and, when appropriate, sent to Adobe Analytics and other data sources for reporting purposes.
- **Publishing:** Proactively publishes social network communications, such as Facebook posts, Twitter tweets, Google+ content, YouTube videos, LinkedIn post, and Sina Weibo posts either immediately or on a customer-defined schedule. The Publishing component tracks incoming social data against published content and any other content that has been specifically configured for tracking by the customer. Security and group management allow different users of an organization to be set up with different roles within a social network. Other functionality includes reports and dashboards, as well as a URL shortening service. All social content is provided in a single application, which handles authentication, navigation, and the framework UI.
- **Moderation:** Enables the customer's social community manager to react to social data, develop a social data feed based on specific filters, and interact with the company's consumers or users on all defined social feeds. The social community manager can view, reply, retweet, escalate, prioritize, mark as spam, and star any social interactions that come in through the defined feeds. Additionally, the manager can pull up additional user profile information to add comments and store internally.

- **Social Analytics:** Collects, processes, and reports insights and metrics related to social content. Social content is composed of user-generated content (e.g., Tweets and posts by consumers or users of the brand) and owned content (e.g., Tweets and posts generated by the brand itself). Adobe Social tracks three (3) types of analytics:
  - **Property Analytics** — Includes insights related to Facebook pages, Twitter handles, YouTube channels, LinkedIn profiles, Google+ pages, Sina Weibo handles (i.e., properties owned by the Adobe customer);
  - **Post Analytics** — Allows the customer to view and report on insights based on posts originating from customer-owned social properties; and
  - **Social Buzz** — Creates a report based on customer-defined terms, including graphs, posts, tracked terms, and mentions by platform and by geography. By default, the report shows data for the last 12 hours, but this timeframe can be changed by the customer. Adobe Social maintains 30 days of verbatim posts. Data from Social Buzz can also be sent to Adobe Analytics for deeper analysis and reporting.

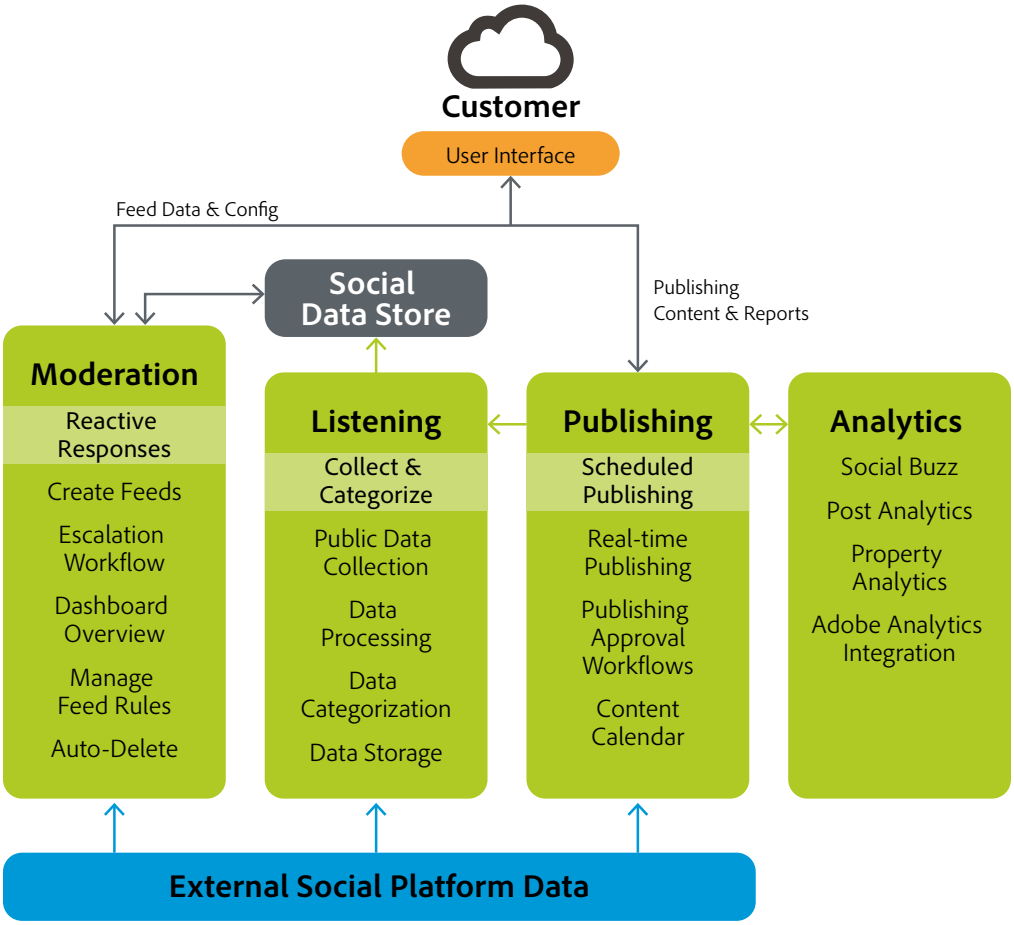

Figure 1: The Adobe Social product architecture and data flow

Adobe Social Application Security and Network Architecture

Adobe Social Data Flow

Adobe Social collects social content in two primary ways: It collects Twitter public content via GNIP and other social network content (e.g., Facebook, LinkedIn, YouTube, Google+, and Sina Weibo) directly via API calls. Adobe Social collects the raw data from each social network and pushes this data into a queuing system for internal processing on Adobe servers. All content deemed to come from social properties owned by the Adobe customer (the customer's Facebook account or Twitter handle, for example) is also sent to Adobe Analytics.

After collecting the social content, the Listening component sends all data through a categorization engine, which checks for spam, categorizes emotion, determines language, categorizes sentiment, and adds geographic data. The content is then stored in an Adobe Social database on one of Adobe's servers. If the content is determined to be customer-owned, it is sent via HTTPS API endpoints to Adobe Analytics for further analysis and reporting. The data is sent to the specific data center to which the customer is assigned based on Adobe Analytics.

The Publishing component of Adobe Social enables customers to create, schedule, and publish social content from a single dashboard. The customer creates the schedule and workflow (e.g., author and approver) in the component's user interface. These schedules and workflows are synced to the Adobe Social servers. When a scheduled submission is ready for posting, the server sends the selected content to the Publishing back end, which then publishes the content to the selected social network. The URL shortening service within Adobe Social launches when a user clicks a shortened URL. The long URL includes the Adobe Analytics Campaign ID and redirects the user to the actual customer website. The customer website then forwards the included Campaign ID and data directly to Adobe Analytics for tracking and metrics.

The Moderation component pulls social content from the Social database as well as receives Twitter Direct Messages and profile information directly from Twitter APIs. Social content is pulled based on listening rules defined by the customer. The Moderation component can also communicate back to Twitter and update the Social database with events and information. As social content comes in, it is filtered based on the defined feed criteria and is stored in the database. Customers view their social feeds through the Moderation UI, which allows them to engage with users and take action—such as reply, retweet, etc.—on certain feed events, which are either sent back via the Twitter API (for immediate posting) or pushed into the Publishing component (for scheduled posting).

User Authentication via Adobe Marketing Cloud

Access to Adobe Social requires authentication with username and password. For users accessing Adobe Social 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 Adobe Social 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 Campaign 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 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

For more information on specialized methods for accessing Adobe Social data and reporting via approved applications, please refer to the product documentation at https://marketing.adobe.com/resources/help/en_US/sc/user/home.html

Adobe Social Hosted Data Centers

The Listening and Publishing components of the Adobe Social solution are hosted on Adobe servers in six (6) data centers around the world. The Moderation component is hosted in Amazon Web Services (AWS). For information on AWS security controls that impact the Moderation component, please see the section entitled, "Adobe Social Moderation Component Hosting."

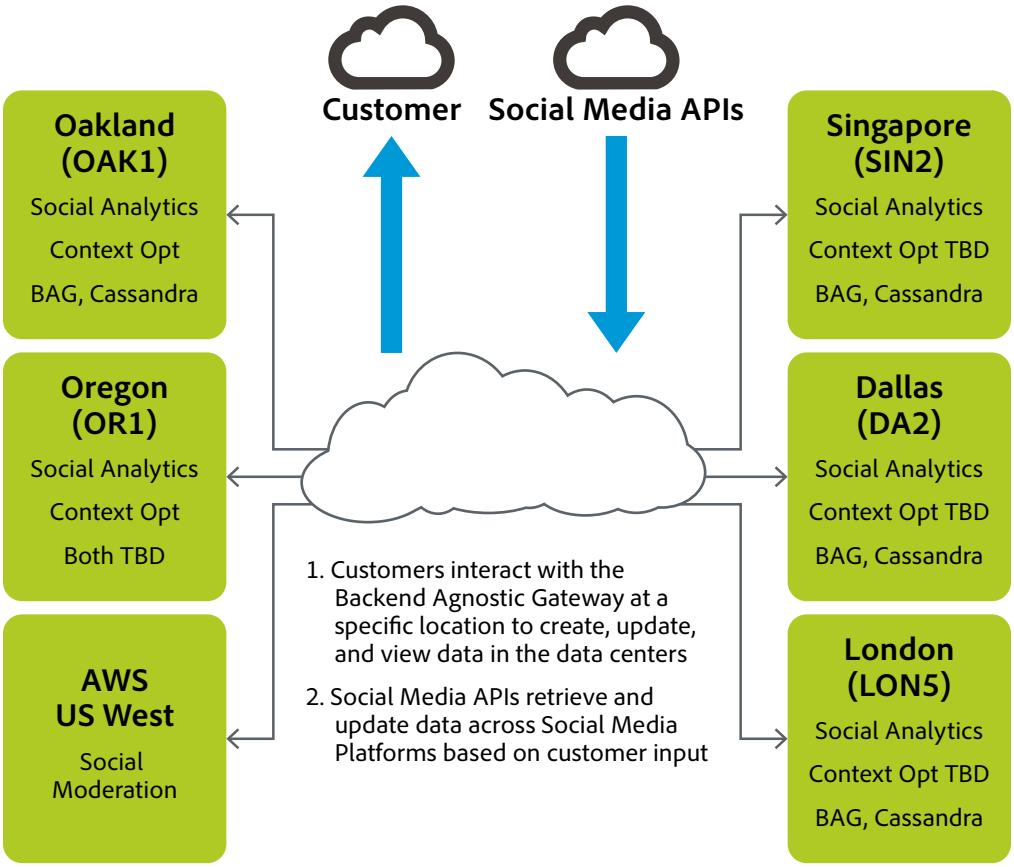

Figure 2: The Adobe Social network

Geographic Location of Customer Data on the Data Center Network

Adobe stores all Adobe Social customer data in data centers located closest to the customer's geographic location.

Adobe Social Network Management

Because of the data collection, data content serving, and reporting activities conducted over the Adobe Social 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

Data is placed into separate databases (report suites), and a single client's site reports are grouped together on one or more servers. In some cases, more than one client may share a server, but the data is segmented into separate databases. The only access to these servers and databases is via the Social application. All other access to the application and data servers is made only by authorized Adobe personnel at the request of a customer due to a reported issue, and when necessary 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 Social 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 Social network deny all Internet connections except those to allowed ports, Port 80 for HTTP and Port 443 for HTTPS. The firewalls also perform Network Address Translation (NAT). NAT masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming HTTP/HTTPS connections and also distribute requests that enable the network to handle momentary load spikes. Adobe implements fully redundant firewalls and load balancers, reducing the possibility that a single device failure can disrupt the flow of traffic.

Non-routable, Private Addressing

Adobe maintains servers containing customer data on servers with non-routable IP addresses (RFC 1918). These private addresses, combined with the Adobe Social 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 Social 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 Adobe Social 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.

Change Management

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

Patch Management

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

Access Auditing

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

Logging

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

Adobe Social Administrative Security Features

Adobe Social enables administrators to control access to reporting data. 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 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 Social 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 includes 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 production servers for Adobe Social 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 Adobe-owned or Adobe-leased data center facilitites. Adobe also requires automatic transition from primary to backup power and that this transition occurs in a way that helps mitigate potential service interruption. Adobe requires each data center facility to provide redundancy at every level, including generators and diesel fuel contracts. Additionally, each facility must conduct regular testing of its generators under load to ensure availability of equipment.

Disaster Recovery

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

Failover Process

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

Recovery Process

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

Adobe Social Moderation Component Hosting

Adobe hosts the Adobe Social Moderation component 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 the Moderation component of Adobe Social resides. In turn, Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and Adobe Social Moderation component 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 Adobe stores all Adobe Social Moderation component 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 AWS.

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 Adobe Social, 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 both the Content Producer Service and the Distribution Service using industry-standard intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Logging

Adobe conducts server-side logging of Adobe Social Moderation customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs only store user 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 Adobe Social Moderation 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.

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.

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 Social team. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.

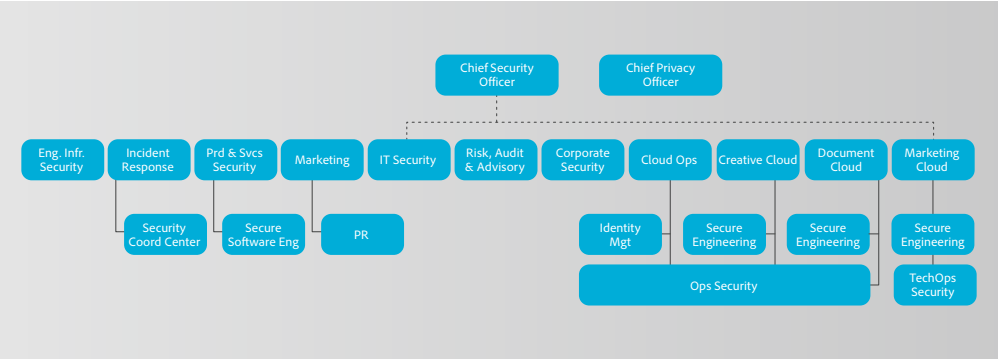

Figure 3: The Adobe Security Organization

Adobe Secure Product Development

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

Adobe Secure Product Lifecycle

The Adobe SPLC activities include, depending on the specific Adobe Social 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 Social security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials

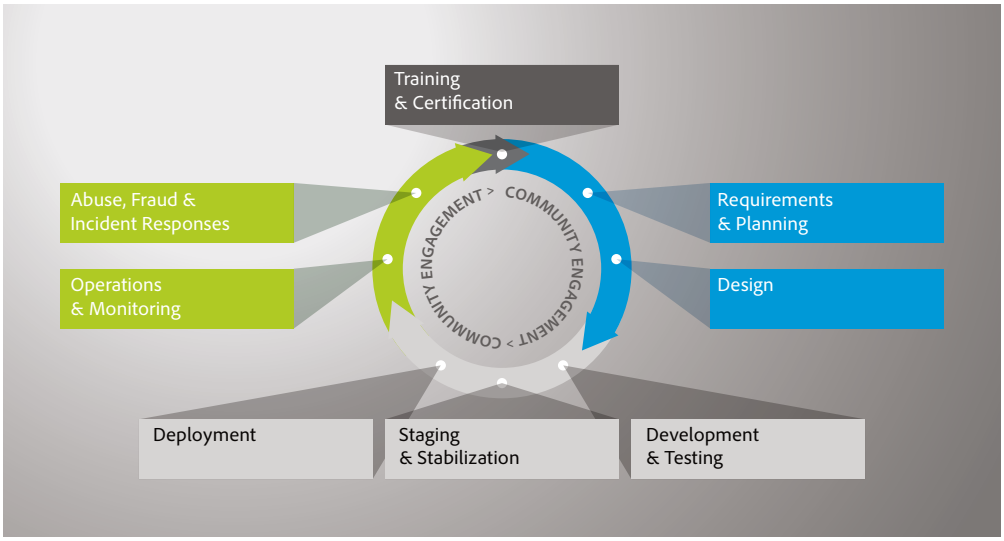

Figure 4: Adobe Secure Product Lifecycle (SPLC)

Adobe Security Training

Adobe Software Security Certification Program

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

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

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

Adobe Common Controls Framework

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

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

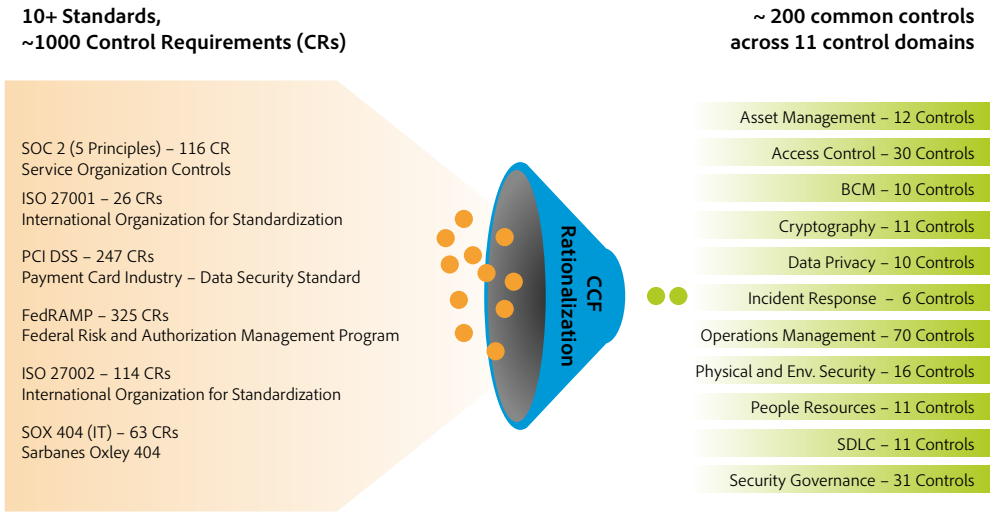

Figure 5: The Adobe Common Controls Framework

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 help 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 Social security team performs a risk assessment of all Social components prior to every release. Conducted by highly trained security staff trusted with creating a secure network topology and infrastructure and Social application, the security reviews look for insecure network setup issues across firewalls, load balancers, and server hardware as well as application-level vulnerabilities. The security touchpoints include exercises such as threat modeling coupled with vulnerability scanning and static and dynamic analysis of the application. The Social security team partners with technical operations and development leads to help ensure 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 Social at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Social organization to coordinate the mitigation effort.

For Adobe cloud-based services, including Social, 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, Social team adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody recording. Adobe may engage with law enforcement or third-party forensic companies when it determines it is necessary.

Adobe Corporate Locations

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

Physical Security

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

Virus protection

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

Adobe Employees

Employee Access to Customer Data

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

Background Checks

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

Employee Termination

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

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

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

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

Customer Data Confidentiality

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

Safe Harbor/Data Transfers

On October 6, 2015 the European Court of Justice (ECJ) ruled that the U.S.-EU Safe Harbor Framework was invalid with immediate effect. Prior to this ruling, Adobe relied primarily on its certification to the Safe Harbor Framework to ensure adequate protection for the transfer of personal data from the European Union (EU)/European Economic Area (EEA) to the United States. Since the ruling, Adobe is authorizing these personal data transfers using European Commission-approved Standard Contractual Clauses (also referred to as Model Contracts). For more information, please refer to the Adobe Safe Harbor FAQ.

Security compliance

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

Adobe is in the process of developing, implementing, and refining the security processes and controls to meet various security and privacy certifications. Please visit http://www.adobe.com/security/resources.html to view a list of security white papers including the Adobe Security and Privacy Certifications white paper for more information on compliance and Adobe's overall security strategy.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Adobe Social 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 try to stay ahead of malicious activities and help ensure the security our customers' data.

For more information, please visit: http://www.adobe.com/security

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.

Adobe

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

www.adobe.com

Date: 02/2016