Adobe® Target Security Overview

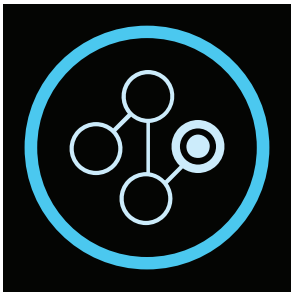

Table of Contents

Adobe Security

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

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

About Adobe Target

Adobe Target is an experience optimization solution that enables marketers, developers, and product owners to deliver a highly personalized user experience on any platform through testing and personalization. Each time a visitor requests a page that has been optimized for Adobe Target, a request is sent to the targeting system to determine what content to serve to a visitor. This process occurs in real time—every time a page is loaded, a request for the content is made and fulfilled by the system. An omni-channel solution, Adobe Target improves the visitor experience on any surface or screen customers use, including full websites, native mobile apps, set-top boxes, kiosks, and more.

There are two versions of Adobe Target, each of which provides a different level of functionality.

Adobe Target Standard includes the following targeting activity variations to help marketers deliver content and offers that match users' browsing, search, and product purchase history:

- A/B Testing—Adobe Target Standard supports two (2) types of A/B testing:
  - Manual traffic split—Compares two or more experiences to see which best improves conversions throughout a pre-specified test period.
  - Auto-Allocate—Identifies a winner among two or more experiences and then re-directs traffic to the winner.
- Experience Targeting (XT)—Delivers content to a specific audience based on a set of marketer-defined rules and criteria.
- Multi-Variate Testing (MVT)—Compares combinations of offers among elements on a page to see which combination performs the best for a specific audience. Also, identifies which element of the page best improves conversions throughout a pre-specified test period.

Adobe Target Premium includes all of the capabilities found in Adobe Target Standard plus advanced machine learning functionality powered by Adobe Sensei:

- A/B Testing—Adobe Target Premium adds support for Auto-Targeting, which identifies multiple high-performing, marketer-defined experiences and serves the most tailored experience to visitors based on their individual customer profiles and past behaviors of similar visitors.
- Automated Personalization (AP)—Personalizes content and drives conversions by combining specific offers or messages and then matches different offer variations to visitors based on their individual customer profiles.
- Recommendations—Automatically promotes, weights, and filters product recommendations and recommends content for subscribers based on what others are viewing and what's trending throughout the customer journey using AI-driven algorithms.

Adobe Target Solution Architecture

The Adobe Target solution includes the following components:

- The **Adobe Target user interface,** where customers define the activities that govern what content to deliver to website visitors; This interface is also used by administrators to determine who is authorized to use Adobe Target.
- **Admin Servers**, which persistently store all data authored using the Adobe Target UI and communicate with the Edge Servers to push the data of all active campaigns and activities. Reporting data, activity configuration, and segment configurations are all stored in the Admin Servers.
- **Edge Servers**, collect user ineractions based on defined activities and send corresponding reporting data to the Admin Servers.
- **Target Proxy Service**, which allows customer websites to be opened in the Adobe Experience Cloud user interface.
- **Adobe Target Mobile**, the mobile version of Adobe Target that enables marketers to define activities on the go.
- **Target Recommendation and Automated Personalization Servers**, which include Adobe Sensei and are only accessible by Adobe Target Premium customers.
- **The Adobe Target API**, which enables integration with other Adobe Experience Cloud solutions, including Adobe Analytics for Target, a set of reports that extends the basic reporting functionality built into Adobe Target.

All connections between Adobe Target components are conducted over secure, encrypted connections. Adobe Target does not store any Personally Identifying Information (PII) at any point in the Adobe Target architecture.

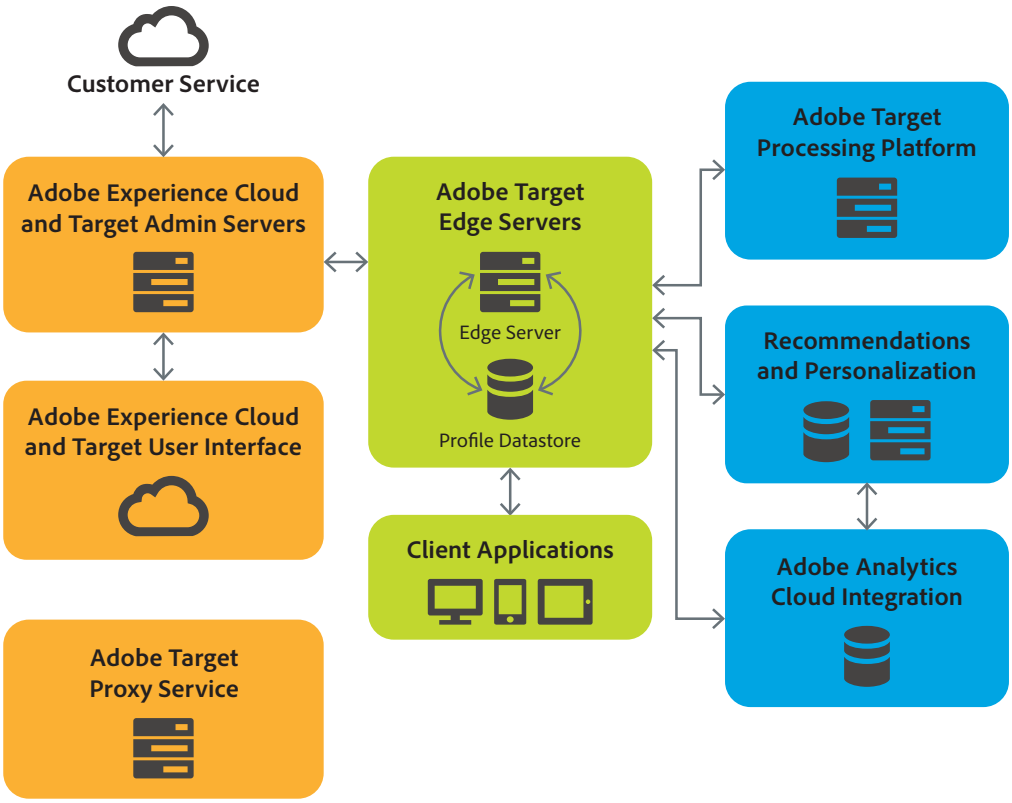

Figure 1: Adobe Target Architecture Diagram

Admin Servers are responsible for user management, cache management, IMS/SSO, REST APIs, and HAL Lookup functionality. Administrators create user profiles and grant varying levels of access to different users in the customer's organization using the Admin console. Cache management helps to decrease response times from Edge servers by allowing requests to be served from cache rather than latency-inducing database queries. The Identity Management Service (IMS) is the authentication and authorization data store that provides Single-Sign-On (SSO) functionality for Experience Cloud users. REST APIs are used to communicate with various platforms, applications, and server clusters. An Admin Server conducts a HAL Lookup when a customer administrator logs in to a server other than their assigned server in the cluster. The server searches for the username among the other Admin Servers and routes the login credentials from the customer's assigned server to the new server for authentication. All campaign information is saved in the MySQL database on the Admin Server cluster and then distributed to all nodes in each of the Edge Server clusters.

Edge Servers are located both in Adobe-owned and Adobe-leased data centers hosted by AWS and include cache management, profile management, and Mbox response functionality. As described above, cache management helps decrease response times by enabling requests to be served from cache. To keep track of website visitors, their profiles, and their actions, Edge Servers use Cassandra. Mbox response serves the appropriate Adobe Target content—as defined by the customer's campaign parameters—to the website visitor.

All Adobe Target Admin Servers and Edge Servers are continually kept updated using Adobe's patch management process (see Patch Management section below).

On the customer side of Adobe Target implementations, the customer must host a JavaScript library, at.js, which is responsible for making Mbox calls to Target Edge Server clusters and also applying the returned personalized content to the webpage. The at.js library can be self-hosted or deployed on Adobe servers. For server-side integrations, the customer may use use the Target API and process the returned content before applying it to webpages, mobile apps or iOT consoles/devices.

Customers can deploy the at.js library using any of the following three (3) methods:

- Using Adobe Launch: Adobe Launch is the next-generation tag management platform from Adobe and is the preferred method to implement Adobe Target. Launch gives customers a simple way to deploy and manage all of the analytics, marketing, and advertising tags necessary to power relevant customer experiences.
- Using Adobe Dynamic Tag Management (DTM): Adobe DTM is Adobe's legacy tag manager. Adobe Launch is the preferred, up-to-date method for implementing Target and the at.js library. For new Target implementations, use Adobe Launch.
- Not using a Tag Manager: Implement Target without using a tag manager (Adobe Launch or Dynamic Tag Management).

Legacy Adobe Target implementations that have deployed the mbox.js library should migrate to at.js, as the mbox.js library is not longer being developed.

For more information on deploying the jt.as library, please see https://docs.adobe.com/help/en/target/using/implement-target/client-side/deploy-at-js/how-to-deployatjs.html

Adobe Target Data Flow

The customer defines the content and parameters for a campaign (e.g., audience demographics and traffic allocation) in the Enterprise Cloud user interface, which communicates the campaign information to the Admin Server to which the customer has been assigned. This interface can be accessed either on a desktop or using Adobe Target Mobile on their mobile device. The campaign information is stored in the MySQL database on the Admin Server cluster and then distributed to all Edge Servers.

When a website visitor lands on a web page with Adobe Target functionality, an Mbox request is sent to the nearest geographical Edge Server, which searches through cache to find the appropriate response (content) for the visitor. If the content is not cached, the Edge Server forwards the request to the Admin Server cluster, where all content is stored, conducts a database query to find the appropriate content, and sends the response back to the Edge Server to present the personalized content to the visitor.

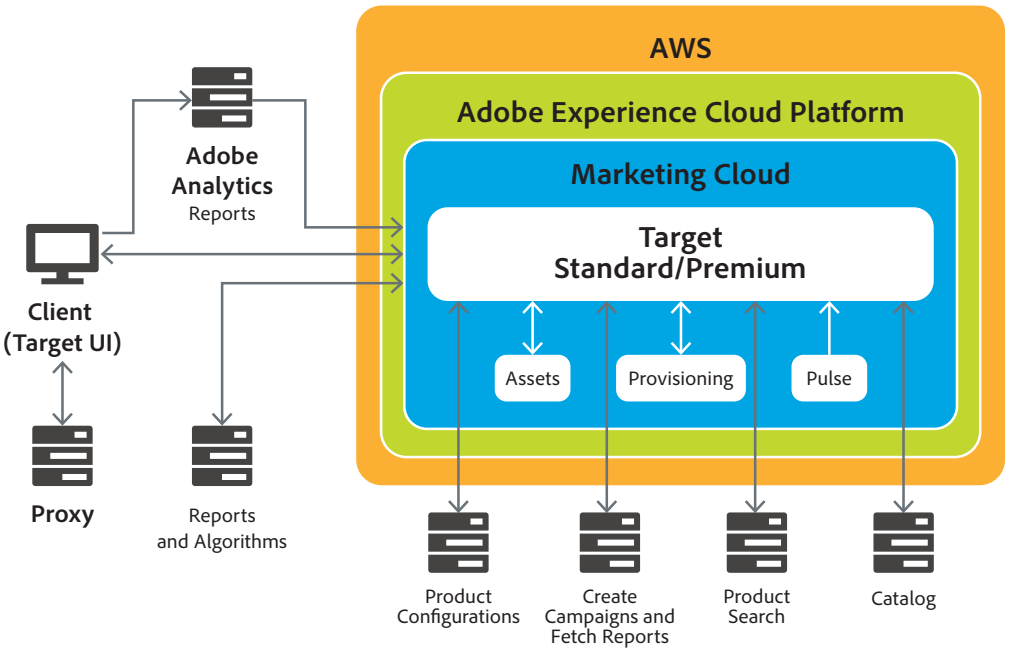

Figure 2: Adobe Target Data Flow Diagram

To automate the display of dynamic website content, Adobe Target traverses through the customer's website structure and aggregates the metadata from each traversal. This allows the system to learn about the subject matter of each different potential click-path. After the site's data has been collected, a score is associated to each of the smaller events within a click-path. When a visitor engages with a website that has the 1:1 product integration, the visitor's request will pass a special snippet of JavaScript library to the Edge Server cluster (physically closest to the visitor) that has a "scorer" label. When the Edge Sever cluster receives the "scorer," it evaluates the user's current web activity and determines how many of the events or click-paths have been executed. At that point, the visitor receives a score based on the activity, which dictates the type of content that the system will display to the user. Once the model is created and the website visitor has requested a response, Adobe Target automatically responds with the most appropriate content for the visitor based on the evaluation provided by the model.

On a regular basis, the Edge Server cluster transfers visitor activity and habit data (e.g., profiles, past-visited URLs, conversions, events, etc.) into Algol, which contains a Hadoop cluster and is responsible for developing models, model responses, interest areas, and gain charts. A model is similar to the scoring spectrum that is used to assign points (i.e., a score) for a visitor based on their current web activity. The model response delivers unique content based on the visitor's score within the model's spectrum. Interest area calculation is used to categorize sections of a website based on their content (i.e., metadata) and is used as part of the modeling process (e.g., a certain section or click-path of a website may be categorized as "Sports" and can help generalize the type of content that should be returned). Lastly, gain charts show the effectiveness of the customer's campaigns. The Edge Server clusters send report and metrics data to the Admin Server cluster, and customers access the gain chart information through the Target Admin Console, which connects directly to the Admin Server cluster.

User Authentication via Adobe Experience Cloud

Access to Adobe Target requires authentication with username and password. We continually work with our development teams to implement new protections based on evolving authentication standards.

Users can access Adobe Target 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 Target 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 customers' IT infrastructure. Adobe integrates with most any SAML2.0 compliant identity provider.

Adobe IDs and Enterprise IDs both leverage the SHA-256 hash algorithm in combination with password salts and a large number of hash iterations. Adobe continually monitors Adobe-hosted accounts for unusual or anomalous account activity and evaluates this information to help quickly mitigate threats to their security. For Federated ID accounts, Adobe does not manage the users' passwords.

More information about Adobe's identity management services can be found in the Adobe Identity Management Services security overview.

Roles and Responsibilities

System admininstrators must manually add Adobe Target user accounts; they are not automatically added. Users are invited by email from Adobe Experience Cloud and must confirm their email addresses before their accounts are registered. Only system administrators can set user roles in Adobe Target.

Role	Description
Observer	Can view activities, but cannot create or edit them
Editor	Can create and edit activities before they are live, but cannot approve the launch of an activity.
Approver	Can create, edit. and activate or stop activities.

Figure 3: Adobe Target Roles

Adobe Target Hosting and Security

The Adobe Target solution is hosted on Adobe-owned and Adobe-leased data centers around the globe. Admin Servers are hosted entirely within Adobe-owned data centers in London, Singapore, and multiple locations throughout the U.S, including Oregon and Virginia. Edge Servers are hosted both on Adobe-owned and Adobe-leased servers in Amazon AWS data centers in London, Hong Kong, Singapore, Tokyo, and Sydney.

Figure 4 — Adobe Target Admin and Edge Server Locations

Adobe Target Network Management

We understand the importance of securing the data collection, data content serving and reporting activities over the Adobe Target network. To this end, the network architecture implements industry best 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 secure access by the Target application. All other access to the application and data servers is made only by authorized Adobe personnel, and is conducted via encrypted channels over secure management connections. We also separate our testing environments from our production environments to avoid use of customer data in testing environments.

Secure Management

Adobe deploys dedicated network connections from our corporate offices to our data center facilities in order to enable secure management of the Adobe Target 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 Target network deny all Internet connections except those to allowed ports, Port 80 for HTTP and Port 443 for HTTPS. The firewalls also perform Network Address Translation (NAT). NAT masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming HTTP/HTTPS connections and also distribute requests that enable the network to handle momentary load spikes without service disruption. Adobe implements fully redundant firewalls and load balancers, reducing the possibility that a single device failure can disrupt the flow of traffic.

Non-routable, Private Addressing

Adobe maintains all servers containing customer data on servers with non-routable IP addresses (RFC 1918). These private addresses, combined with the Adobe Target 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 Target network to detect and alert our security team to unauthorized attempts to access the network. The security team follows up on intrusion notifications by validating the alert and inspecting the targeted platform for any sign of compromise. Adobe regularly updates all sensors and monitors them for proper operation.

Service Monitoring

Adobe monitors all of our servers, routers, switches, load balancers, and other critical network equipment on the Adobe Target network 24 hours a day, 7 days a week, 365 days a year

(24x7x365). The Adobe Network Operations Center (NOC) receives notifications from the various monitoring systems and will immediately attempt to fix an issue or escalate the issue to the appropriate Adobe personnel. Additionally, Adobe contracts with multiple third parties to perform external monitoring.

Data Backups

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

Change Management

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

Patch Management

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

Access Controls

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

Logging

In order to protect against unauthorized access and modification, Adobe captures network logs, OS-related logs, and intrusion detections. Sufficient storage capacity for logs is identified, periodically reviewed, and, as needed, expanded to help ensure that log storage is not exceeded. 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 Target Security Features for Administrators

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

Fire Suppression

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

Controlled Environment

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

Video Surveillance

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

Disaster Recovery

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

DNS record TTL (time to live) is set to allow this switch to the secondary location to happen quickly. For customers using Regional Data Collection ("RDC"), data collection will continue to queue data without intervention should the Data Processing Center be temporarily unavailable. If an RDC site should fail, data collection will continue to the other RDC sites. While data collection is in a failover mode, customers are notified of the ongoing situation with regular status updates. If it is expected that the primary data collection location will be back online within five (5) business days, no historical data will be transferred to, or data collection processed at, the secondary location. If the disaster at the primary data collection location is serious enough to have destroyed or make historical data there unavailable, Adobe will restore that data from backups stored at off-site locations.

Recovery Process

When the primary data collection location is available and stable again, the failover process will be reversed. All traffic collected at the secondary location will be merged with data in the primary location, DNS records will be restored, and 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. Page view processing will take approximately one day for every four hours the failover process was active. Time required to recover historical data from off-site may take up to an additional ten (10) days.

The Adobe Security Organization

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

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams, including the Adobe Target 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.

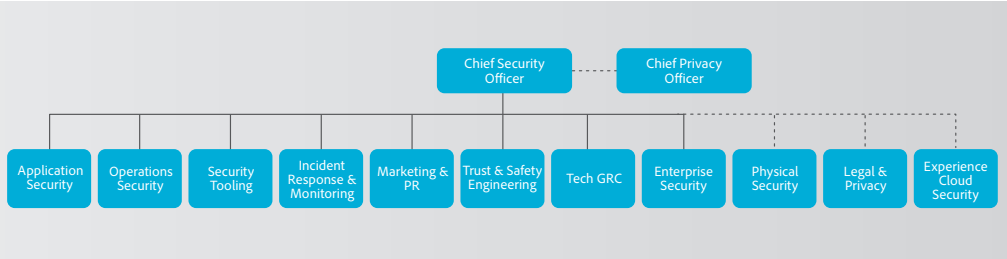

Figure 5: The Adobe Security Organization

Adobe Secure Product Development

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

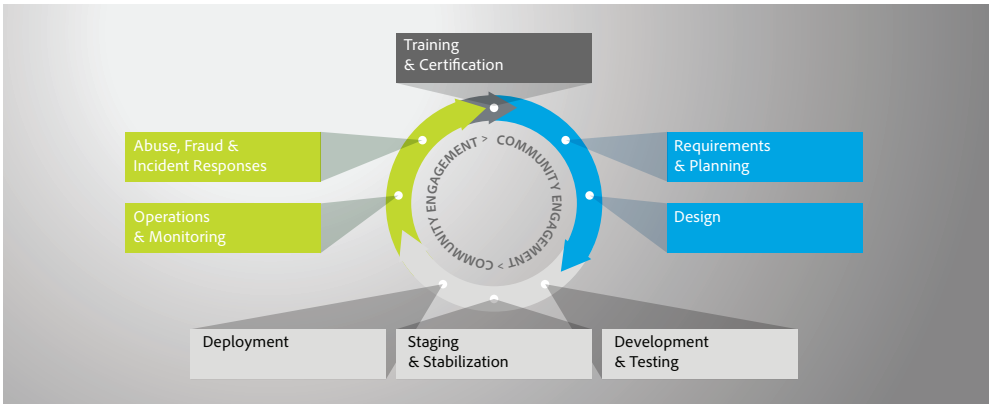

Figure 6: The Adobe Software Product Lifecycle (SPLC)

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 Adobe Target 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 Target 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.

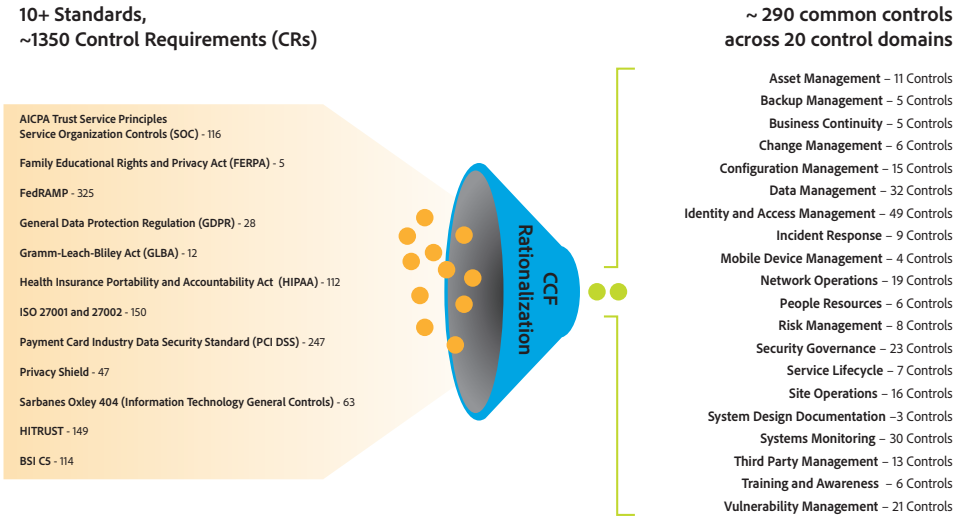

Figure 7: The Adobe Common Controls Framework (CCF)

Current Regulations and Compliance for Adobe Target

SOC 2 is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Target 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. Adobe Target is compliant with ISO 27001:2013.

The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions safeguard their customers' personal data. Adobe Target is GLBA-Ready, meaning that it enables our financial 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.

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. Adobe conducts a full penetration test annually.

Penetration tests are conducted at least annually or after every major release. Vulnerability scans are performed monthly while web and database scans are performed quarterly.

Internally, the Adobe Target security team performs a risk assessment of all Adobe Target components quarterly and prior to every release. The Target security team partners with technical operations and development leads to help ensure all high-risk vulnerabilities are mitigated prior to each release. For more information on Adobe penetration testing procedures, see the Adobe Secure Engineering Overview white paper.

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.

For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Forensic Analysis

For incident investigations, the Adobe Target 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 record.

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

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

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Adobe Target, 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.

Facility 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.

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.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Adobe Target 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 try 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
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com