Adobe Campaign 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® Campaign experience and your data.

About Adobe Campaign

Used by over 650 of the world's leading brands, Adobe Campaign provides best-in-class campaign, offer, and personalization management capabilities for sophisticated automation and execution of marketing programs across virtually all channels—digital and traditional. Adobe Campaign addresses a key challenge for marketers: how to build and extend relationships with their customer base to drive top-line revenue growth and ROI. Allowing every company to select the best fit based on their marketing strategy, IT ecosystem, and business and legal requirements, Adobe Campaign is a complete, integrated yet flexible solution and the only one on the market today to offer four deployment models: on-premises, cloud, and hybrid.

Adobe Campaign Application Architecture and Deployment Models

The typical Adobe Campaign solution deployment consists of the following components:

Personalized Client Environment — Easy-to-use, graphical interface in which customers can communicate and track marketing offers, create campaign content, review and manage all marketing activities, programs, and campaigns (including emails, workflows, and landing pages), create and manage customer profiles, and define customer audience types.

Development Environment — Server-side software that executes the marketing campaigns through chosen channels including email, SMS, direct mail, call center, web, push notification, and/or social based on the rules and workflow defined in the user interface.

Database Containers — Based on relational database technology, the Adobe Campaign database stores all customer information; campaign components, offers, and workflow; and campaign results in customer database containers.

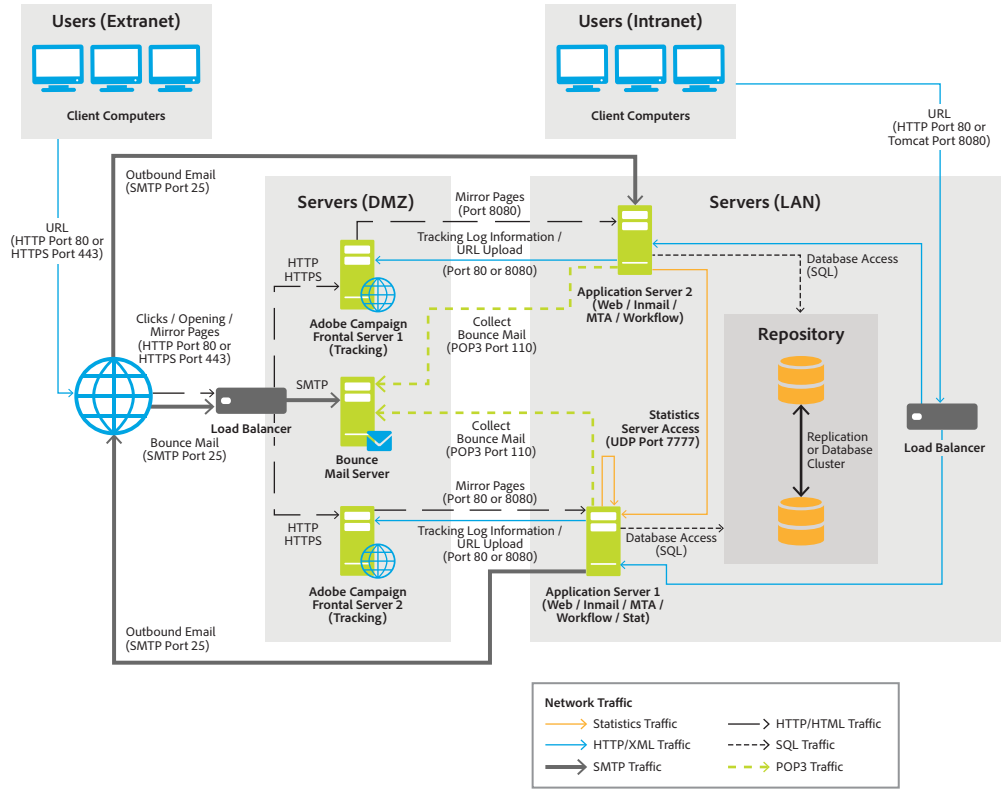

Figure 1 — Adobe Campaign application architecture

Deployment Models

Adobe Campaign can be deployed in one of four ways: as a managed service, on-premise, on-demand, or in a hybrid model.

When deployed as a managed service, all components of Adobe Campaign, including the user interface, the execution management engine, and the customer's Campaign database are hosted in Adobe-managed data centers around the world (see Adobe Campaign Hosting section below). Adobe hosts the customer's deployment in a data center located in the customer's corresponding region (e.g., North America, Europe, or Australia).

When deployed on-premise, all components of Adobe Campaign, including the user interface, execution management engine, and database reside on-site in the customer's data center. In this deployment model, the customer manages all software and hardware updates and upgrades.

When deployed on-demand, all components are hosted on Adobe-managed servers closest to the customer's operating region.

When deployed as a hybrid model, the Adobe Campaign solution software resides on-premise at the customer site, execution management is delivered as a cloud service by Adobe, and all data remains in the Campaign database in the customer's own data center until the moment of campaign execution. At that point, only the data required for the specific campaign is transmitted to the Adobe service infrastructure. No data of any kind is permanently stored in the cloud.

For more detailed information about Adobe Campaign deployment options, please see the white paper entitled, "Deployment Options for Managing Cross-Channel Campaigns."

Application Security and Network Architecture

When customers choose to deploy a completely hosted or hybrid hosting model for their Adobe Campaign deployment, these components are hosted in one of Adobe's SSAE 16 Type II SOC 2-audited and compliant data centers. For specific data center locations, please see the Adobe Campaign Hosting section below).

Any data that is transmitted between Adobe Campaign components over the Internet—typically between the client user interface software and the execution management engine—is secured via HTTPS using 256-bit AES encryption.

User Authentication

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

Customers can access and use Adobe Campaign either through the interface included in Adobe Marketing Cloud (called Adobe Campaign Standard) or by using the standalone Adobe Campaign client application (called Adobe Campaign V6), using 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 asset—are provided by the customer's Single Sign-On (SSO) identity management system and are created, owned, controlled by IT. Adobe integrates with most SAML2.0 compliant identity providers.

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

Adobe Campaign Hosted Data Centers

Adobe maintains data centers that host Adobe Campaign components in locations around the world.

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

Adobe Campaign Network Management

Adobe Campaign understands the importance of protecting your data. To this end, the network architecture for Adobe Campaign 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 secure access by the Adobe Campaign 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 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 enable industry-standard secure management of the Adobe Campaign 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 our 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 help 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

Customer data is hosted on servers with non-routable IP addresses (RFC 1918). These private addresses, combined with 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 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 the servers, routers, switches, load balancers, and other critical network equipment on the Adobe Campaign 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 Adobe Campaign customer data hosted by Adobe on a daily basis. Each backup is stored for up to seven (7) days by default. An encrypted copy (using GPG) of the database backup is sent offsite daily as well. In case of database loss, the last daily backup can be restored. Point-in-time recovery can be done if data loss results from a customer action. Any of the last seven (7) backups can be used.

Adobe also backs up the Adobe Campaign infrastructure configuration files on a daily basis. Backups are done using snapshots. A snapshot of all configuration data is backed up daily and transferred off-site using SSL encryption in transit. Backups can be stored in an encrypted format upon request.

Because all backups are performed online for both any Adobe Campaign customer data hosted by Adobe and the Adobe Campaign configuration; the application and servers are available to customer for the duration of the backup period.

Change Management

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

Patch Management

In order to automate patch distribution to host computers within the Adobe Campaign 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 network 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 Campaign 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. Adobe identifies, periodically reviews, and as needed, expands storage capacity to ensure that sufficient capacity always exists and is never 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 Risk & Vulnerability Management

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

Penetration Testing

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

Internally, Adobe Campaign security team performs a risk assessment of the Adobe Campaign application prior to every release. Security risk assessments are conducted by trained security staff trusted with securing the network topology and infrastructure and Adobe Campaign application. These 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 Adobe Campaign security team partners with the technical operations and development leads to ensure all identified 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 may put Adobe Campaign at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Adobe Campaign organization to coordinate the mitigation effort.

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

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 the Adobe Campaign include dedicated, 24-hour on-site security personnel and require these individuals to have valid credentials to enter the facility. Adobe requires PIN or badge credentials—and, in some cases, both—for authorized access to data centers. Only individuals on the approved access list can enter the facility. Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

Fire Suppression

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

Controlled Environment

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

Video Surveillance

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

Backup Power

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

Disaster Recovery

A disaster is defined as an incident that results in loss of computer processing at an Adobe Campaign hosting site. Disasters can result from a number of accidental, malicious, or environmental events, including fires, floods, terrorist attacks, human errors, employee strikes, and software or hardware failures.

The primary objective of the Adobe Campaign disaster recovery (DR) and business continuity plans is to ensure the continued operation of business critical systems in the event of a disaster. The goals include minimizing the disruption of the Adobe Campaign hosting capabilities and to ensure the operation of the standby facility as quickly as possible. Both plans are reviewed on an annual basis as well as upon any change to the Adobe Campaign hosting infrastructure.

The decision to initiate DR procedures is taken by the person responsible for company operation for the region after an initial assessment of the impact by the DR team. If this individual decides to initiate DR procedures, then all members of the team will follow the procedures described below until complete recovery.

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 Campaign 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.

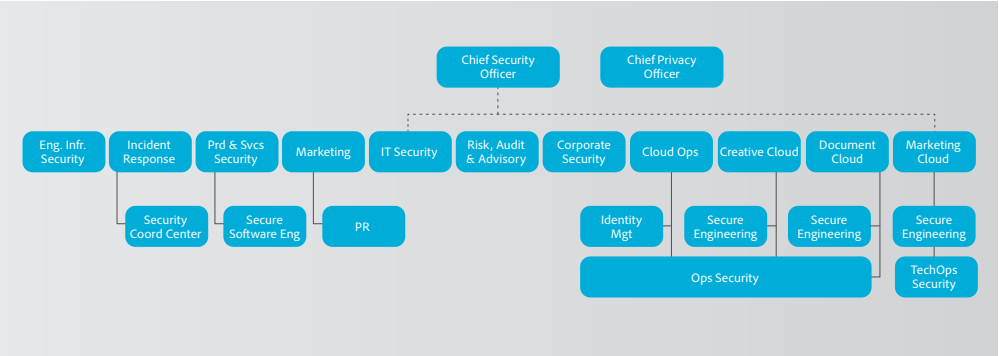

Figure 2 — The Adobe Security Organization

Adobe Secure Product Development

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

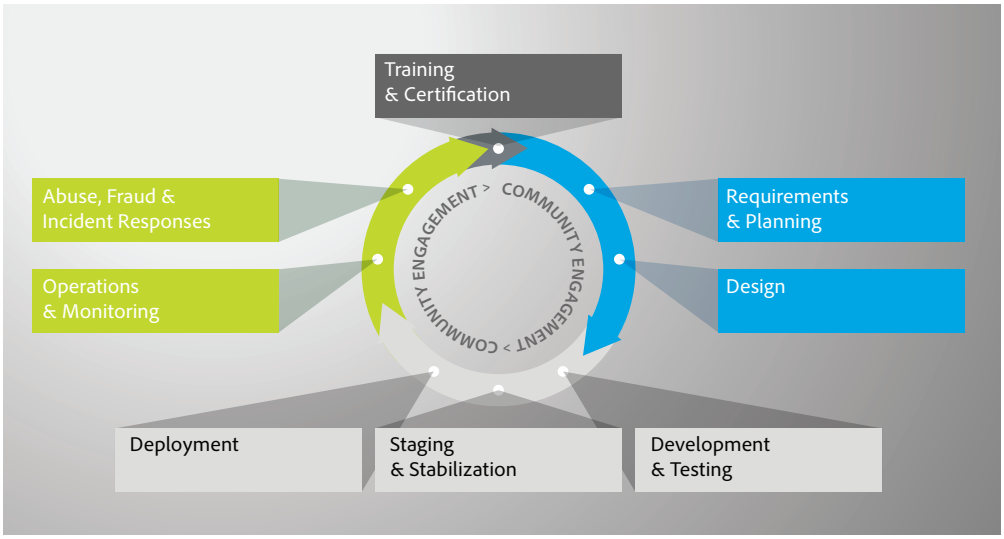

Figure 3 — Adobe Secure Product Lifecycle (SPLC)

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

Adobe Common Controls Framework

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

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

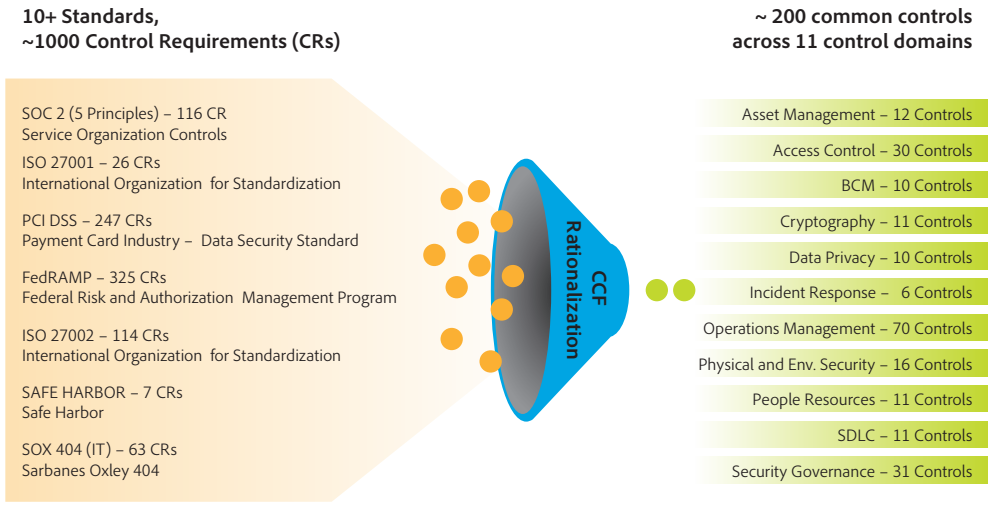

Figure 4 — The Adobe Common Controls Framework (CCF)

Adobe Corporate Locations

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

Physical Security

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

Adobe Employees

Employee Access to Customer Data

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

Background Checks

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

Employee Termination

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

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

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

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

Customer Data Confidentiality

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

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Campaign application and your confidential data. At Adobe, we take the security of your digital experience very seriously and we continuously monitor the evolving threat landscape to stay ahead of malicious activities and help ensure the secure our customers' data.

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

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

Date: 1/2017