Adobe Experience Cloud

Adobe

WHITEPAPER

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

Adobe Campaign is a cross-channel marketing campaign management solution that enables organizations to bring customer data from different systems, devices, and channels into a single profile and deliver timely and relevant campaigns to these customers. With Adobe Campaign, companies can understand and define unique customer segments and then craft multi-step, cross-channel campaigns that make meaningful connections with each customer.

Adobe Campaign Solution Architecture

The Adobe Campaign platform is written on a flexible application layer and is easily configurable to meet any organization's specific business requirements, thereby accommodating the growing needs of the enterprise from a functional, as well as a technical, perspective. The distributed architecture ensures linear system scalability scaling from thousands to millions of messages.

The Adobe Campaign solution consists of the following three (3) components:

Personalized Client Environment — Intuitive graphical interface in which users can communicate and track marketing offers; create campaigns; review and manage all marketing activities, programs, and plans (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 communication channels, including emails, SMS, push notifications, direct mail, web, or social media, based on the rules and workflows defined in the user interface.

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

Each of these three components includes several functional modules that can be deployed on one or more computers, and in single or multiple instances, depending on scalability, availability, and service isolation requirements. In this service-oriented architecture (SOA), some modules operate continuously, while others spin up occasionally to perform administrative tasks (e.g., configuring the database connection) or to run a recurrent task (e.g., consolidating tracking information). With this flexibility, organizations can deploy the Adobe Campaign solution in multiple confirgurations, from a single, central computer to multiple dedicated servers over multiple sites. Visit our website for a complete list of Adobe Campaign modules.

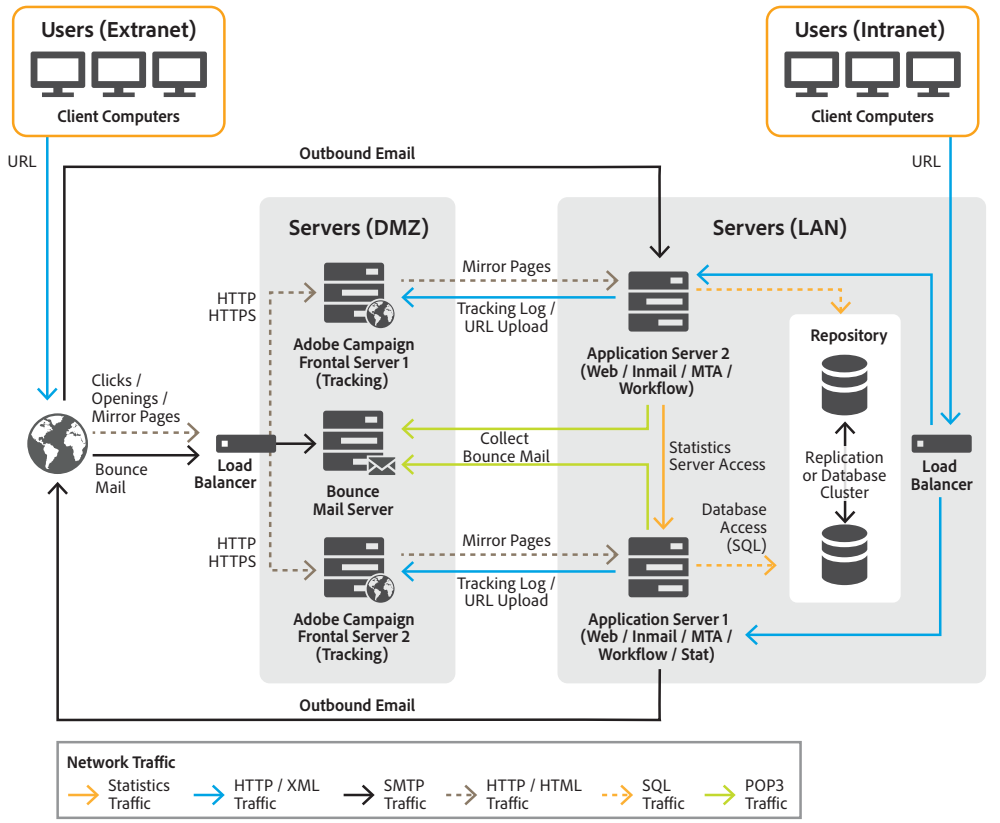


Figure 1: Adobe Campaign Solution Architecture

Personalized Client Environment

Users can access the Adobe Campaign solution in three different ways, depending on the user's needs:

- **Rich client** — Typically, users will use Adobe Campaign's primary user interface, a native Windows application that communicates with the Adobe Campaign application server using standard internet protocols, including SOAP and HTTP. The console works in a browser, updates automatically, and does not any require specific network configuration.
- **Thin client** — Some parts of the application, including the reporting module, delivery approval stages, functionality in the distributed marketing module (central/local), and instance monitoring, can be accessed via a simple web browser using an HTML user interface.
- **Integration via APIs** — Adobe Campaign can be integrated with external applications using the Web Services APIs exposed via the SOAP protocol.

Development Environment

Adobe Campaign relies on a set of server-side processes that work together. The primary processes include:

- **Application server** (nlserver web) — Exposes the full range of Adobe Campaign functionality via web services APIs (e.g., SOAP, HTTP, and XML). Furthermore, it can dynamically generate the web pages used for HTML-based access (e.g., reports, web forms, etc). To execute these functions, this process includes an Apache Tomcat JSP server. This is the process to which the Adobe Campaign console connects.
- **Workflow engine** (nlserver wfserver) — Executes the workflow processes defined in the Adobe Campaign application and handles periodically executed technical workflows, including:
  - Tracking — Enables retrieval of logs from the redirection server and creation of aggregate indicators used by the reporting module
  - Cleanup — Purges old records from the database to avoid exponential growth of the database
  - Billing — Automatically sends an activity report for the platform, including database size, number of marketing actions, etc.
- **Delivery server** (nlserver mta) — Functions as an SMTP mail transfer agent (MTA) to provide native email broadcast functionality. This process also performs "one-to-one" personalization of messages, handles their physical delivery, and manages automatic retries. In addition, when tracking is enabled, this process automatically replaces the URLs to point to the redirection server. If needed, the process can automatically send SMS, fax, and direct mail to a third-party router.

- **Redirection server** (nlserver webmdl) — Automatically handles click-tracking for email by incorporating rewritten URLs in email messages to point to this module, which registers the passing of the internet user before redirecting them to the required URL. Fully independent from the database, other server processes communicate with this process using SOAP calls (e.g., HTTP, HTTPS, and XML.

Database Containers

The Adobe Campaign database contains the functional data (profiles, subscriptions, content, etc.), the technical data (delivery jobs and logs, tracking logs, etc.) and the work data (purchases, leads) for the solution, and all Adobe Campaign components communicate with the database in order to perform their specific tasks.[1]

Customers can deploy Adobe Campaign using the predefined data mart or an existing data mart and schema using any of the major RDBMSs. All data within the data mart is accessed by the Adobe Campaign via SQL calls. Adobe Campaign also provides a full complement of Extract Transform and Load (ETL) tools to perform data import and export of data into and out of the system.

Adobe Campaign Data Flow

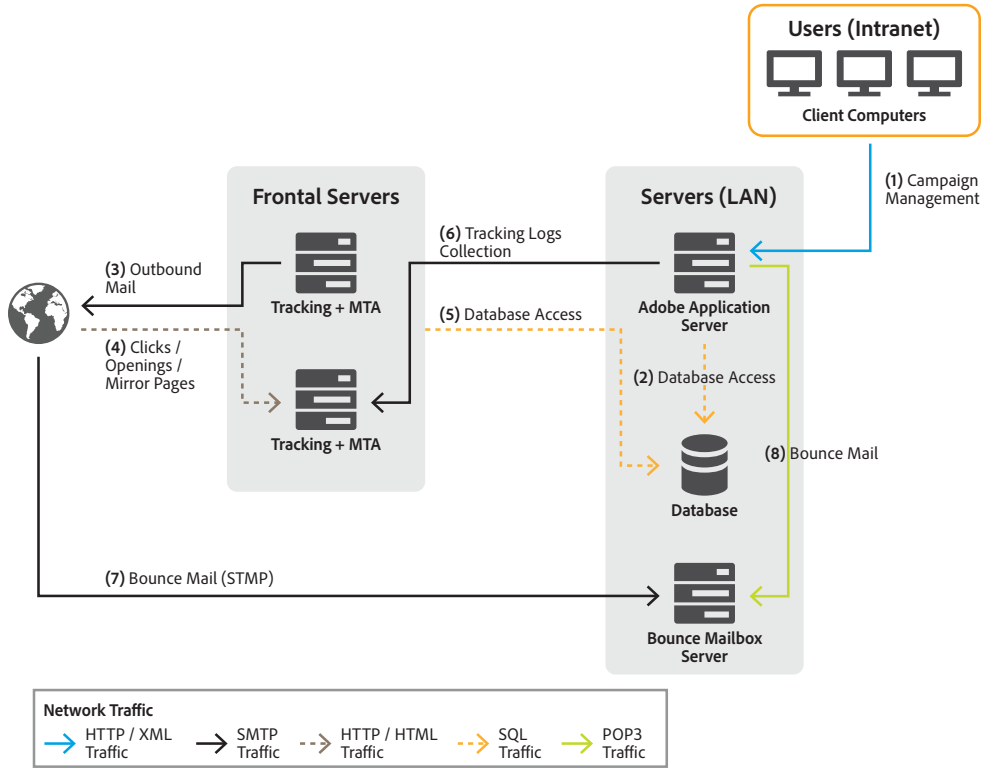


Figure 2: Adobe Campaign Data Flow Diagram

Data Encryption

Data in transit between different Adobe Campaign components is encrypted using TLS 1.2 over HTTPS. Data at-rest is encrypted by the cloud service provider hosting the solution using 256 bit AES encryption.

User Authentication

Customers can access Adobe Campaign through the following methods:

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 IT. Adobe integrates with most SAML2.0 compliant identity providers.

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.

Adobe Campaign Security Features for Administrators

Adobe Campaign enables administrators to control access to reporting data. Options include strong passwords, password expiration, IP login restrictions, and email domain restrictions. Please visit our website for more information.

User-exposed Security Options and Settings in Adobe Campaign

Short overview graph on what this is and why it's needed. The security options and settings that users can control in Adobe Campaign include:

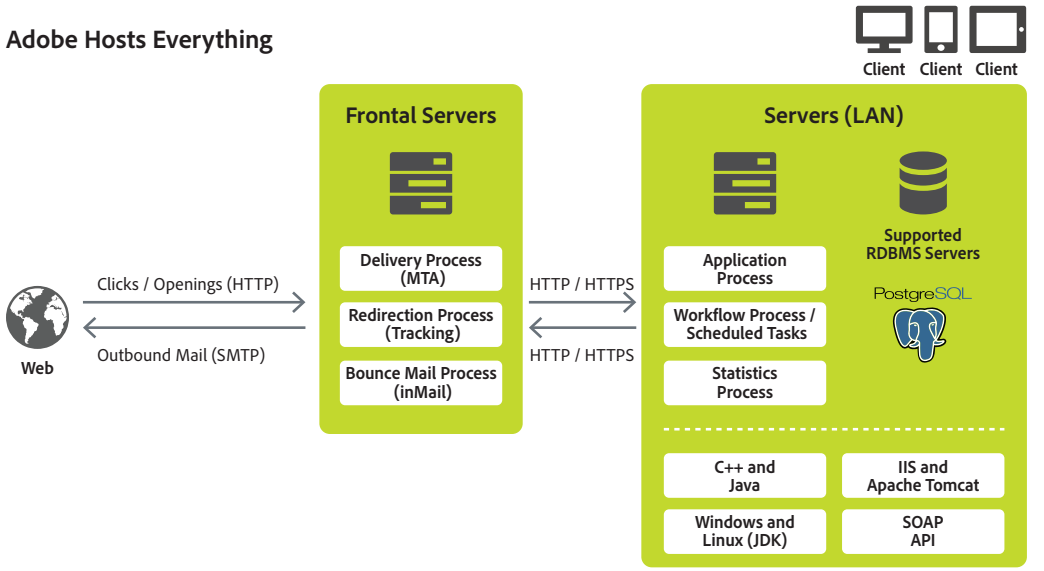
- **URL allow listing** — External URLs that need to be accessed via JavaScript should be allow listed in the Adobe Campaign config file. URLs that are not allow listed will not be allowed to access Campaign.
- **IP allow listing on infrastructure and application level** — To allow incoming traffic to the Adobe Campaign instance (e.g., via SFTP), the source IP must be allow listed at the infrastructure level. To access an instance of Adobe Campaign via SOAP or web API calls, the IP allow list is done at the application level, in the config file. Any IP address that is not allow listed cannot access the Adobe Campaign instance.
- **Hubble setup** — To install Hubble on all Adobe Campaign instances for security auditing, reporting, and compliance.
- D**omain-specific SSL certificates** — SSL certs can be installed at the infrastructure level to provide secure access using HTTPS.
- **GPG key** — Encrypted files that have been uploaded on an Adobe Campaign server via SFTP/workflow can be decrypted using a public GPG key installed on the server. Similarly, files can be encrypted using a GPG key before before sending them from Adobe Campaign.
- **SFTP key** — To securely access the Adobe Campaign file server, key-based authentication can be used by installing an SFTP user public key on the server.
- **On-demand addition of secret key and key ID for AWS S3 credentials** — If secure access to an AWS S3 bucket from Adobe Campaign instance is required, AWS keys can be installed on the Adobe Campaign server.
- **DKIM (Domain Key Identified Mail) configuration** — Used to ensure that Adobe Campaign emails have been sent from an authorized server. The private key is kept on application side to sign the email and the public key is installed on DNS side.

- **No regex on cloudfront** — Restrict redirection (regex) of URLs on cloudfront based on regex matching on query string part of URL. By default, cloudfront is configured to allow all redirects and there is no filtration on query string part.
- **Pipeline triggers configuration** — Analytics-triggered events on pipeline can be encrypted before sending to Adobe Campaign using keys provided by the customer, which are added to the configuration here. These events can be decrypted by Adobe Campaign using the public key configured in the config file.
-

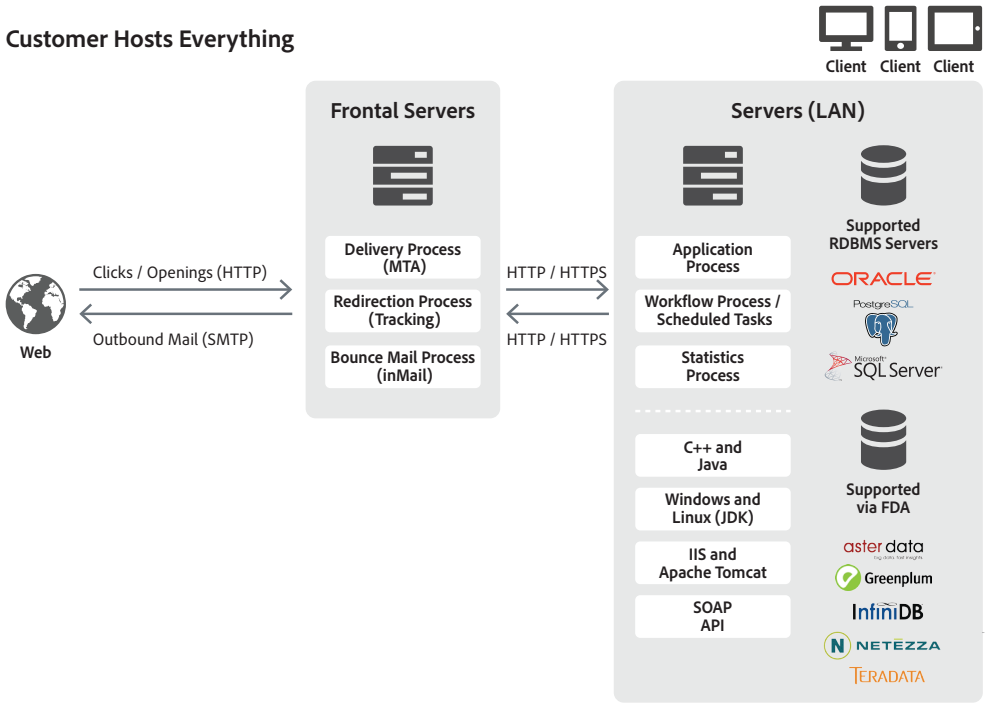
Adobe Campaign Deployment Models

Adobe Campaign Classic can be deployed in one of three (3) ways:

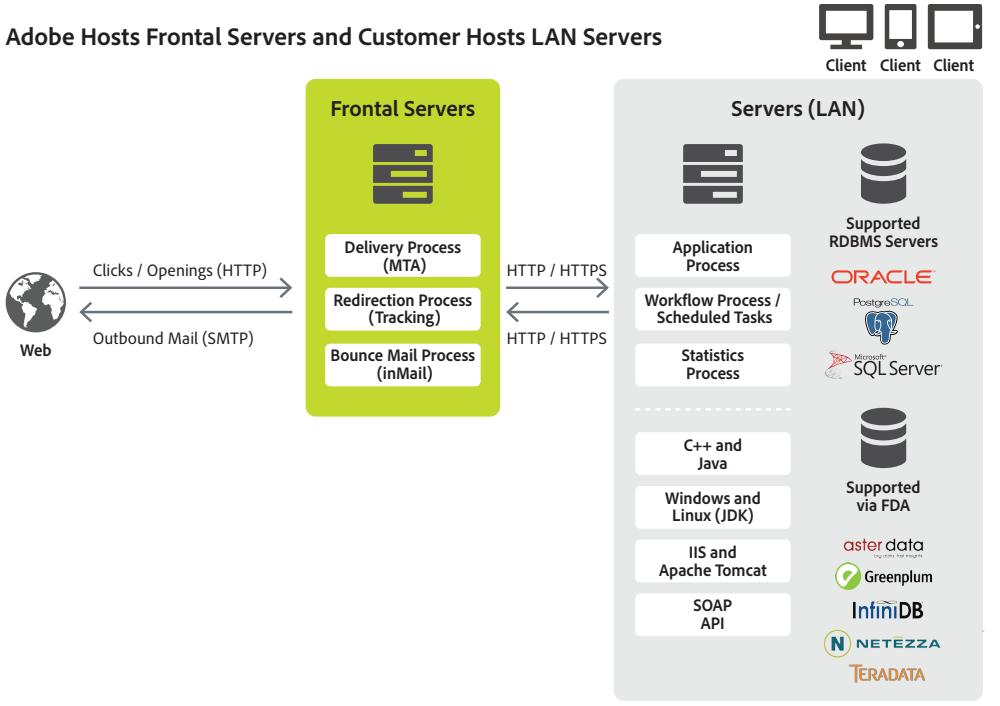
Managed Service: All components of Adobe Campaign, including the user interface, the execution management engine, and the customer's Campaign database are hosted in Adobe-managed data centers around the world.



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.



Hybrid: 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.



Adobe Campaign Standard is available only as a hosted application. All components are hosted on Adobe-managed servers closest to the customer's operating region.

Hosting Locations

For managed services, on-demand and hybrid deployments, Adobe hosts the appropriate Adobe Campaign software in a data center located in the customer's corresponding region.

Figure 4 — Adobe Campaign hosting locations

Adobe Campaign Network Management

We understand the importance of securing the data collection, data content serving and reporting activities over the Adobe Campaign 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

In Adobe Campaign Classic, each customer is deployed in a separate virtual machine or container using a single tenant configuration.

In Adobe Campaign Standard, 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.

Some people would consider ACS to be multi-tenant in that each customer uses the same application code base, however, each customer has their own separate database.

The only access to these servers and databases is via secure access by the 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 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 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 the Adobe Campaign 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 Campaign 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 Campaign 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 Campaign 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 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 customer data for Adobe Campaign on a daily basis. A 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 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 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 Campaign production server connections for auditing.

Logging

In order to protect against unauthorized access and modification, Adobe captures access logs and error logs in Splunk. All successful and unsuccessful access activities are recorded in the system and in application logs, including username, action, and date/time of access. Every data change is logged in the system and in application logs. Additionally, vendor actions and integration actions, including username, action, and date/time, are recorded and stored in application logs. Application logs are stored tamper-proof for six months. 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 personnel.

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 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 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 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 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.

For Campaign customers that are provisioned in AWS or Azure, each region is comprised of one or more availability zones. Generally a region has three availability zones and each availability zone is a physically separate location. In the event of an availability zone failure, a Campaign instance can be recovered in the same region to another availability zone, where backups are sent daily.

In addition, Adobe's Business Continuity and Disaster Recovery program is supported by governing documentation that covers business continuity, disaster recovery, testing, business impact analysis, data backup, and restoration processes. The plan is tested and reviewed annually. An overview of Adobe's program is available by contacting your Adobe sales representative.

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.

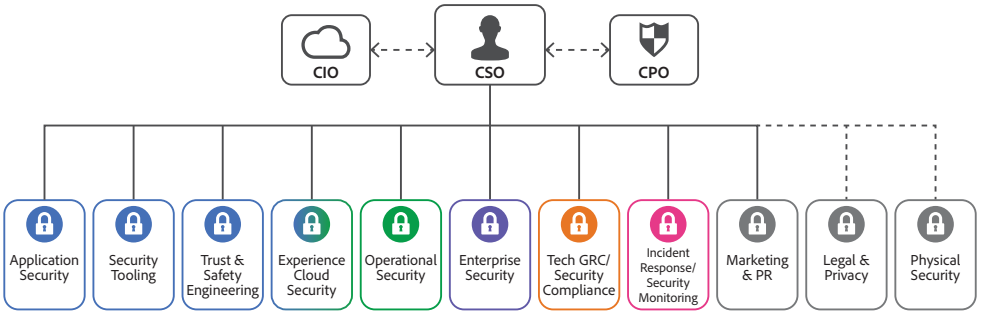


Figure 5: The Adobe Security Organization

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

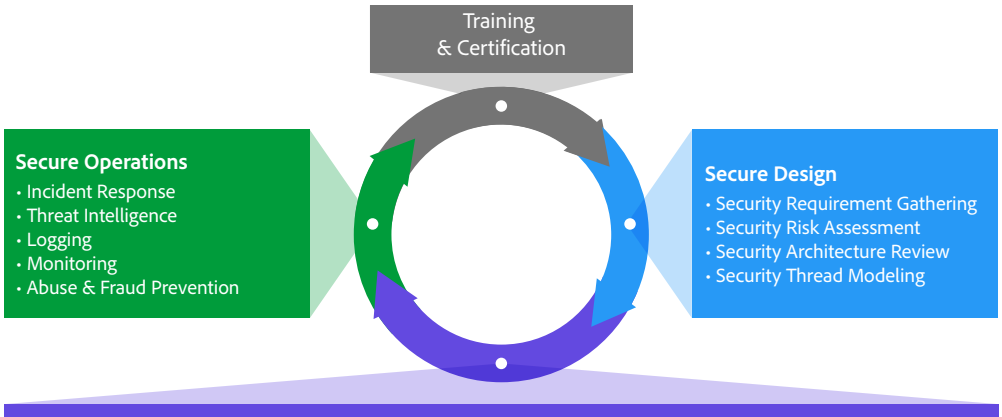


Figure 6: The Adobe Software Product Lifecycle (SPLC)

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 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 Campaign 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.

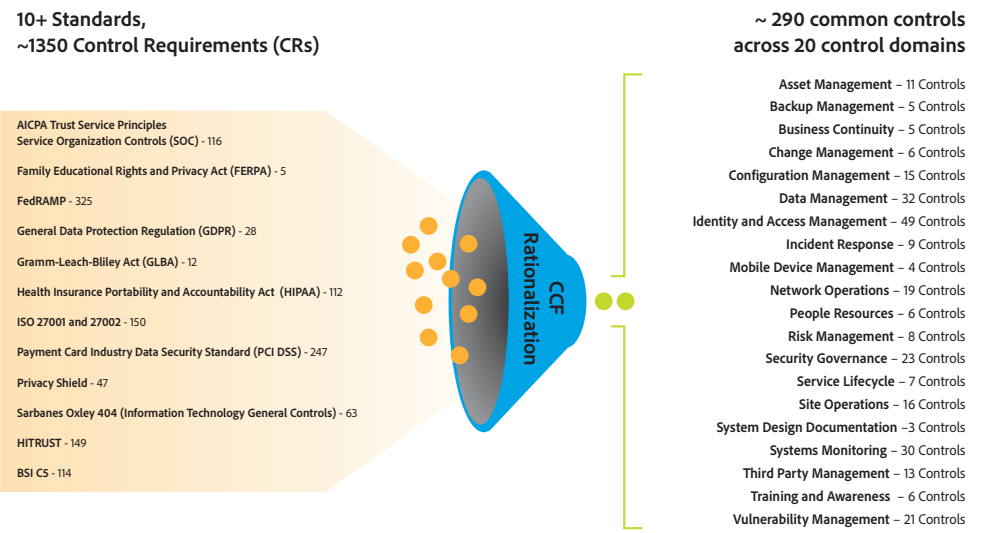


Figure 7: The Adobe Common Controls Framework (CCF)

Current Regulations and Compliance for Adobe Campaign

For the most up-to-date information about compliance, please see the Adobe Master Compliance List at:
https://www.adobe.com/content/dam/acom/en/security/pdfs/MasterComplianceList.pdf

Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that the Adobe 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 and after every major release, performs vulnerability scans monthly, and runs web and database scans quarterly.

Internally, the Adobe Campaign security team performs a risk assessment of all Adobe Campaign components quarterly and prior to every release. The Campaign 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 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 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

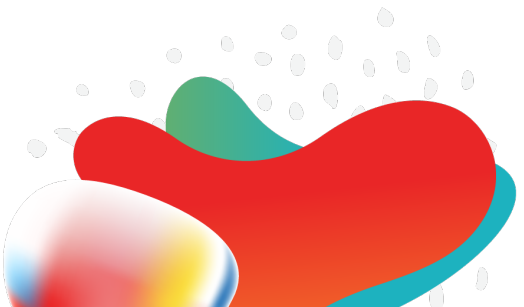
Adobe scans all inbound and outbound corporate email for known malware threats.

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 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.

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 Campaign 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

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.