Adobe Marketing Cloud Security

Adobe Security

At Adobe, we take the security of your digital experiences seriously. From our rigorous integration of security into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What’s more, our collaborative work with partners, researchers, and other industry organizations helps us understand the latest security best practices and trends and continually build security into the products and services we offer.

This white paper describes the proactive approach and procedures implemented by Adobe to address the security of your Adobe Marketing Cloud experience and your data.

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 specialists who serve as consultants to key Adobe product security and operations teams, including the Digital Marketing Information Security Team (DMIST) for the Adobe Marketing Cloud. ASSET researchers work with individual Adobe product security 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.
The DMIST Manager creates controls, implements procedures, coordinates incident response, and oversees audits for the Adobe Marketing Cloud.

DMIST ensures the implementation of proper administrative, technical, and physical controls to help prevent unauthorized access to customer data. Many members of the DMIST security team earn and regularly maintain certifications as a Certified Information Systems Security Professional (CISSP®), a globally recognized, independent security certification given by the Information Systems Security Certification Consortium, Inc., (ISC)²®. Members with CISSP certifications renew their certifications every 3 (three) years. Members of the DMIST security team specialize in a broad range of security areas, including risk and vulnerability management, network security, monitoring, auditing, compliance, and application security.

Product Development
As with other key Adobe product and service organizations, the Adobe Digital Marketing 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. Specific SPLC guidance is recommended per 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 controls include, depending on the specific Adobe Marketing Cloud service, 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 Marketing Cloud 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 reviews 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 reviews, response plans, and release of developer education materials
Training

Adobe Software Security Certification Program
As part of the Adobe SPLC, Adobe conducts ongoing security training 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 teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

Adobe Marketing Cloud teams 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.

The Adobe Marketing Cloud Network
Because of the data collection, data content serving, and reporting activities conducted over the Adobe Marketing Cloud network, the security of the network is important to us. To this end, the network architecture implements best practices for security design, including segmentation of development and production environments, DMZ segments, hardened bastion hosts, and unique authentication.

Password-Protected User Access
Access to Adobe Marketing Cloud services requires authentication with username and password. For services currently using Adobe IDs, Adobe leverages the SHA 256 hash algorithm in combination with password salts and a large number of hash iterations.

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 Marketing Cloud servers. Management connections to the servers occur over encrypted Secure Shell (SSH), Secure Sockets Layer (SSL), or Virtual Private Network (VPN) channels. 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 Marketing Cloud network deny all Internet connections except those to allowed ports, for example, 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
The Adobe Marketing Cloud maintains servers containing customer data on servers with non-routable IP addresses (RFC 1918). These private addresses, combined with the Adobe Marketing Cloud 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 Marketing Cloud network to detect and alert our security team to unauthorized attempts to access the network. The DMIST security team follows up on intrusion notifications by validating the alert and inspecting the targeted platform for any sign of compromise. Adobe regularly updates our sensors and monitors them for proper operation.

Service Monitoring
Adobe monitors our servers, routers, switches, load balancers, and other critical network equipment on the Adobe Marketing Cloud network 24 hours a day, 7 days a week, 365 days a year (24x7x365). The Adobe Network Operations Center (NOC) receives notifications from our monitoring systems and will immediately attempt to fix or escalate an issue to the appropriate Adobe personnel. Additionally, Adobe contracts with multiple third parties to perform external monitoring.

Data Backups
Customer data stored within our core Adobe Marketing Cloud product line is backed-up on a daily basis through the use of snapshots. Each snapshot is stored for up to 7 (seven) 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 system 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 system in order to schedule maintenance blackouts to avoid periods of high network traffic.

Patch Management
In order to automate patch distribution to host computers within the Adobe Marketing Cloud organization, Adobe uses internal patch and package repositories as well as patch and configuration management. Depending on the role of the host and the criticality of pending patches, the Adobe Marketing Cloud distributes patches to hosts at deployment and on a regular patch schedule. If required, Adobe Marketing Cloud 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 Adobe Marketing Cloud production server connections for auditing.

Risk & Vulnerability Management
Audits
Adobe performs internal audits and works with third parties to perform security audits as an additional check against the policies, procedures, and controls implemented on the Adobe Marketing Cloud network. These audits are performed at the corporate level, product level, or against identified specific threats.

Penetration Testing
Adobe engages with approved third-party vendors to perform penetration testing to find potential security vulnerabilities and improve the overall security of Adobe products and services. The vendors complete the tests according to industry best practices. Upon receipt of the vendor’s report, Adobe documents these vulnerabilities, evaluates severity and priority of each using internal processes, such as the Common Vulnerability Scoring System (CVSS), and then creates and implements an appropriate mitigation strategy or remediation plan. A customer may receive a Letter of Testing Completion from the vendor upon written request and under NDA, which may include information about the testing methodologies used and an overview of the findings.
Incident Response and Notification
As new vulnerabilities and threats evolve, Adobe strives to respond and 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 vulnerability is announced, the DMIST security team generates a customized environmental Common Vulnerability Scoring System (CVSS) score to identify the appropriate threat level and priority. Then, the team communicates the vulnerability to the appropriate teams both within and outside of the Adobe Marketing Cloud organization to coordinate the mitigation effort.

Incident Response
Adobe Marketing Cloud employs Adobe’s centralized incident response, decision-making, and external monitoring with our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues.

When an incident occurs, the SCC works with the involved Adobe product incident response and development teams to identify, mitigate, and resolve the issue as quickly as possible 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
Adobe adheres to a forensic analysis process that includes complete image capture, evidence safe-holding, and chain of custody recording. Adobe may engage with third party forensics investigators as well as law enforcement in situations requiring further investigation or prosecution.

Adobe Hosting Locations
Physical Facility Security
All hardware in Adobe-owned or Adobe-leased hosting facilities is physically secured against unauthorized access. All facilities that contain production servers for the Adobe Marketing Cloud 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.

Video Surveillance
All facilities that contain product servers for the Adobe Marketing Cloud provide video surveillance to monitor entry and exit point access, at a minimum. Data center facilities also monitor physical access to equipment. Adobe may review video logs when issues or concerns arise in order to determine access violations.

Fire Suppression
All data center facilities employ an air-sampling, fast-response smoke detector system that alerts facility personnel at the first sign of a fire. In addition, each facility has installed 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 includes an environmentally controlled environment, including temperature humidity control and fluid detection. Adobe requires a completely redundant heating, ventilation and air conditioning (HVAC) system and 24x7x365 facility teams to handle any environmental issue that might arise. If the environmental parameters move outside those defined, environmental monitors alert both Adobe and the facility’s Network Operations Center (NOC).
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 conducts regular testing of its generators under load to ensure availability of equipment.

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 at all times. Server equipment, development machines, phone systems, file and mail servers, and other sensitive systems are further kept locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus Protection
Adobe scans all in-bound and out-bound corporate email for known malware threats.

Adobe Employees
Production and Development Environments
Adobe maintains segmented development and production environments, using technical controls to limit network and application-level access to live systems. Employees have specific authorizations to access development and production systems. Adobe creates, maintains, and monitors logs for key systems in order to establish accountability for actions taken in the Adobe Digital Marketing environments.

Employee Access to Customer Data
Adobe helps ensure that only appropriate, authorized employees can access customer data. Adobe uses role-based access to limit employee access to data based on specific job function. Within Adobe, workers can only access the Adobe Marketing Cloud network after written approval of sufficient business justification for the access and successful passing of a background check. Adobe conducts periodic reviews of access privileges and upon any change of job responsibility.

Background Checks
Adobe obtains consumer 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
In the event that an employee resigns from 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 no longer access 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 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. For more information, please refer to the Adobe Privacy Policy (http://www.adobe.com/privacy/policy.html). Adobe does not share customer data except as described in the Adobe Privacy Policy or when asked to do so by the company using our Adobe Marketing Cloud services.

**Safe Harbor**

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

**Conclusion**

The proactive approach to security and stringent procedures described in this paper help protect the security of your Adobe Marketing Cloud data. At Adobe, we take the security of your digital experience seriously. Please visit the Adobe security site for more information about security efforts across our products and services.