Adobe Analytics Security Overview

Adobe Security

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

This white paper describes the proactive approach and procedures implemented by Adobe to increase the security of your Adobe® Analytics experience and your data.

Table of Contents

About Adobe Analytics

Adobe Analytics is a solution for applying real-time analytics and detailed segmentation across marketing channels. Part of the Adobe Marketing Cloud suite of solutions, Adobe Analytics enables you to gather, analyze, and act upon your customer data helping you better target customers and improve the effectiveness of your marketing.

There are three main versions of Adobe Analytics, each of which provides a different level of functionality:

Adobe Analytics combines the capabilities of multiple web analytics tools that have been available from Adobe to date: Reporting and analytics (previously available in SiteCatalyst), Ad hoc analysis (Discover), Report Builder (ReportBuilder — a Microsoft Excel plug-in), and DataWarehouse (Data warehouse — data repository) Each of these capabilities is now available centrally and seamlessly via Adobe Marketing Cloud when you use Adobe Analytics.

Adobe Analytics – Mobile Apps combines all of the features and functionality found in Adobe Analytics with advanced mobile app analytics and engagement capabilities to improve mobile app discovery, explore integrated cross-channel app insights, and engage app users with messaging and intelligent location marketing capabilities.

Adobe Analytics Premium Complete includes all of the capabilities found in Adobe Analytics and Adobe Analytics – Mobile Apps, but goes a step further by including customer analytics, multi-channel capabilities, and statistical/predictive modeling (primarily delivered through Data Workbench) to provide more complete views of your customers, allowing you understand their broader impact on the business. The following Adobe Analytics Premium bundles, which contain sub-sets of Adobe Analytics Premium Complete functionality, are also available for specific customer needs: Predictive Intelligence, Customer 360, Cross-channel Attribution.

Adobe Analytics Application Architecture

- **The Adobe Analytics user interface**, where customers define the rules that govern what information they wish to measure and gather on visitors
- **Adobe Analytics Application Measurement software**, which measures and collects end-user behavior and activity on the Adobe Analytics' customer's website(s)
- **Regional Data Collection (RDC) servers**, which collect the end-user behavior and activities measured; and
- **Regional Data Processing (RDP) servers**, which process the user behavior data according to the rules set by the customer in the Adobe Analytics user interface.

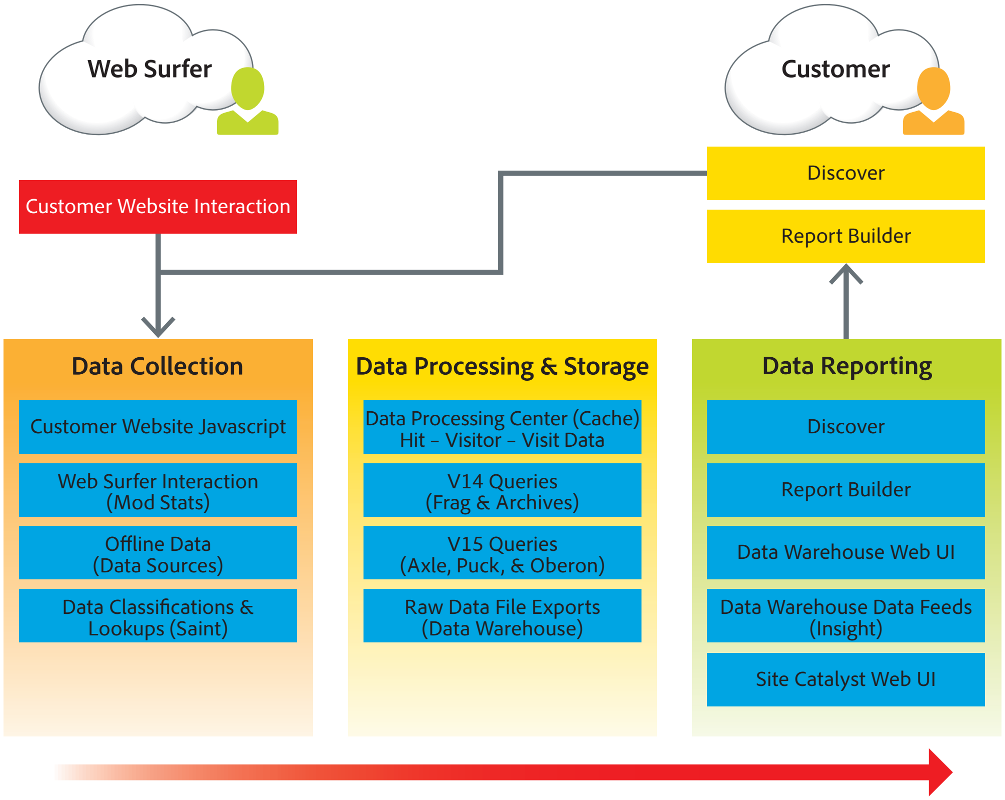

Web Surfer
Customer
Customer Website Interaction
Discover
Report Builder
Data Collection
Customer Website Javascript
Web Surfer Interaction (Mod Stats)
Offline Data (Data Sources)
Data Classifications & Lookups (Saint)
Data Processing & Storage
Data Processing Center (Cache) Hit – Visitor – Visit Data
V14 Queries (Frag & Archives)
V15 Queries (Axle, Puck, & Oberon)
Raw Data File Exports (Data Warehouse)
Data Reporting
Discover
Report Builder
Data Warehouse Web UI
Data Warehouse Data Feeds (Insight)
Site Catalyst Web UI

Figure 1 — The Adobe Analytics product architecture and data flow

All components of Adobe Analytics are hosted in Adobe-owned or -leased data centers, except Adobe Analytics Application Measurement software, which resides on the customer's web server.

Adobe Analytics Application Security and Network Architecture

When an end-user visits a website on which Adobe Analytics Application Measurement is used and after a customer has determined what data should be collected, Adobe Analytics sends tracked user behavior data back to the Adobe Analytics Application Measurement software. All communication between Adobe Analytics Application Measurement software and its related cookies inherits the same security rules as the customer's website. That is, if the customer implements HTTPS, then the communication between the App Measurement software and end-user cookies uses HTTPS as well.

Upon completion of the user's web session, the Adobe App Management software sends the user's behavior data to one of Adobe's worldwide RDC servers using HTTPS.

Once the user data is sent to Adobe, the Adobe Data Collection server pre-processes the data using the Adobe Analytics pre-processing rules engine, which applies all customer-defined rules that were created in the user interface. Location of RDC servers are chosen by the customer during implementation. Then, the RDC server sends the pre-processed user data to one of Adobe's RDP servers. If an RDP server is co-located with an RDC server (in the same facility), the data is sent there. If an RDP server does not exist at the same location as the RDC server, the data is sent to the RDP server nearest in geographic distance from the RDC server and is secured via HTTPS. The RDP server stores the database in the Adobe Analytics data warehouse on that server.

At this point, the user has several options for viewing the data gathered by Adobe Analytics. He/she can:

- Use the Adobe Analytics web application to run and view formatted reports. All interactions with the Adobe Analytics web application are secured via HTTPS.
- Implement a data warehouse reporting tool to pull data directly from the data warehouse using HTTPS or secure FTP.
- Receive a raw data feed that can be blended with other data feeds or sources for visualization or can be stored in a cloud-based data warehouse

Adobe Analytics Data Flow

Adobe Analytics provides two primary methods for collecting data to present a view of our customers' online properties. The primary methods are:

- **Directly on the customer's website** – Using a combination of embedded JavaScript code on customer's web pages, customized URLs and HTTP headers, and persistent cookies, the Adobe Analytics servers collect information about users' actions and behaviors as they interact on customers' web pages. This information is passed to Adobe Analytics Data Collection servers nearest to where activity occurs. The servers then pass the data they collect to the core Analytics Data Processing Center (DPC) to start processing for use. Locations of these servers is discussed later in this document.
- **From non-website channels** – Adobe Analytics supports collection and analysis of data via a Secure File Transfer Protocol (SFTP) interface. Customers provide this data in a prescribed file format with necessary classifications and upload it securely through this interface.

Once this data is sent to Adobe, it is analyzed and collated for reporting to our customers in the Adobe data warehouse. Customers are provided with the following methods for accessing data once it has been prepared and stored in the data warehouse:

- **Through the Marketing Cloud web interface** – Enables creation of reports, ad hoc queries, and other analysis of data stored in the data warehouse. This is the most common method of accessing data in Adobe Analytics.
- **Through web interface directly into the data warehouse** – Allows customers to work more directly with raw data and generate reports and feeds more complex than those offered through the Marketing Cloud interface.
- **Through the Adobe Analytics Ad Hoc Analysis desktop tool** – Allows customers to perform advanced analysis quickly on website activity data, including viewing multiple reports simultaneously, segmenting dimensions (campaigns, products, pages, etc.), and analyzing data from the micro and macro perspectives to view their impact on the target metrics. These features enable customers to answer questions about site traffic, graphics, revenue, and product movement.
- **Using the Excel plug-in** – Allows manipulation and reporting on data using the capabilities of Microsoft Excel.
- **Raw download from the data warehouse** – Allows customers to use their own advanced analysis and reporting suites for working with Adobe Analytics data.

Adobe Analytics Premium Data Flow

Adobe Analytics Premium offers an additional desktop tool called Data Workbench enabling more advanced usage of collected data and application services. The data flow and access options when using Data Workbench have some differences from Adobe Analytics as described below:

- **Data Feeds** - Most source log data comes through data feeds from Adobe Analytics. Analytics data is collected and stored in data processing centers for Analytics. Data feeds can be set up to feed into Data Workbench clusters. The feeds are sent internally from Analytics servers directly to Data Workbench via secure FTP.
- **Sensor** - Sensor refers to data collection done directly in Data Workbench. Sensors can be customer hosted on their web servers and sent directly to an Adobe hosted file server unit (FSU). Sensors can also be Adobe-hosted and are dedicated servers. In both cases, the sensor data is stored on the Network Attached Storage (NAS).
- **Offline Data** - Customers can upload data in a variety of sources but typically as flat files. Customers can send files via FTP or sFTP to the shared product FTP infrastructure. Scripts on Data Workbench (DWB) servers then pull the data from the FTP server into the DWB environment. Customers can also upload some files, such as like lookup files through the DWB Client interface.
- **Configuration Data** - Customers can set up specific rules around how their data will be read, filtered, and processed. These rules are stored as configuration files on the FSU. The configuration data on production servers is backed up and stored offsite. Customers can upload new rules and trigger a reprocessing event that pulls the source log data in according to the rules. The resulting dataset is stored on one or more data processing units (DPUs) and can then be queried/used by the customer.
- **Dataset Data** - This data lives on the DPUs. The data is in a proprietary database format to Data Workbench. Data can be queried by the DWB Workstation client software, or via API, or via a Report server that runs saved queries and distributes reports via email.
- **Export Data** - Customers can export data out of a DWB dataset and send this to external systems. This can be done via secure FTP directly from a server in a DWB cluster, or via the shared product FTP infrastructure.

User Authentication via Adobe Marketing Cloud

Access to Adobe Analytics requires authentication with username and password. For users accessing Adobe Analytics using Adobe IDs, Adobe leverages the SHA 256 hash algorithm in combination with password salts and a large number of hash iterations. We continually work with our development teams to implement new protections based on evolving authentication standards.

Users can access Adobe Analytics 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 Analytics 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, and controlled by IT. Adobe integrates with most any SAML2.0 compliant identity provider.

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

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

Adobe Analytics Hosted Data Centers

The Adobe Analytics solution is hosted on Adobe-owned and managed servers. Some of these locations include a data collection center as well as a data processing center. The five (5) locations that include both data collection and data processing centers are noted in the following map as **Core & Edge** sites.

The six (6) locations that only contain a data collection center, which may include more than one data collection server, are noted on the following map as **Edge** site only.

Each customer-defined data collection segment (report suite) is assigned to a specific data processing center as chosen by the customer during implementation. Therefore, a hit collected by a data collection center in Singapore might be sent to Oregon for processing, even though there is a data processing center at that site.

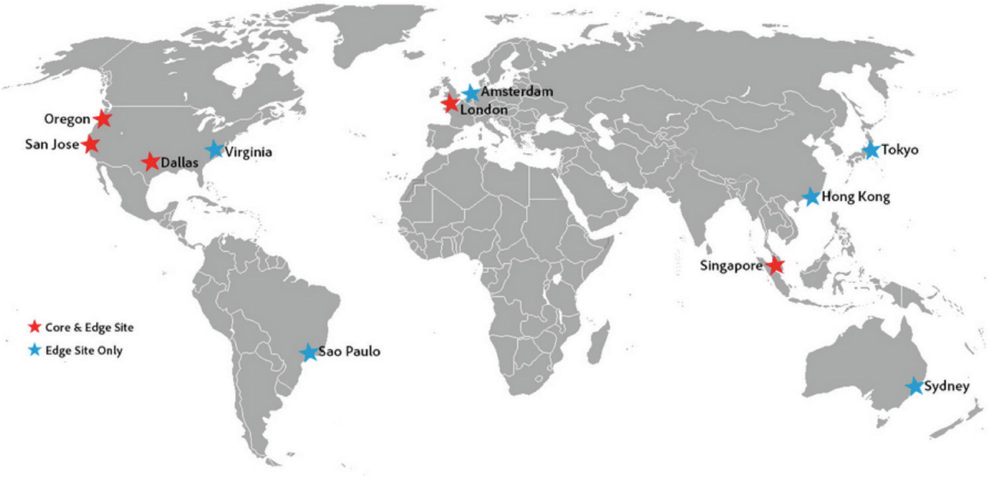


Figure 2 — The Adobe Regional Data Collection network

Regional Data Collection Process

The data collection process used by Adobe includes the following:

1. First, the Adobe Analytics customer must modify its Adobe collection code (s_code.js or AppMeasurement.js, AppMeasurement libraries, mobile SDK configuration, etc.) to use the RDC domain omtrdc.net.
2. Then, using advanced Domain Name Service (DNS) technology, Adobe maps the RDC domain to the data collection center nearest the visitor.
3. When a hit is sent, the Adobe image request automatically routes to the RDC center nearest the visitor.
4. The RDC center uses a secure data pipe to quickly forward the data to the regional data processing center, where it is processed and made available to Adobe Analytics and other Adobe Marketing Cloud solutions as customers choose.
5. The RDC domain also routes Data Insertion API requests through the nearest data collection center. Only HTTPS hits are encrypted between the browser and the data collection center. All data sent from RDC locations to DPC locations is also encrypted via HTTPS.

In event of a disruption in communication between the data collection center and the data processing center (DPC), the Adobe's RDC infrastructure attempts to route data to the DPC through another data collection center. Data is saved locally and then forwarded to the DPC when communication is restored. Due to limits on storage space, this option is available only for short-term disruptions.

For major disruptions, the Adobe Network Operations team reconfigures the global DNS system used by RDC to forward your data through another data collection center.

Adobe Analytics Network Management

We understand the importance of securing the data collection, data content serving, and reporting activities over the Adobe Analytics 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 Analytics 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 Analytics 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 Analytics 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 Analytics 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 Analytics 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 Analytics 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 Analytics 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 Analytics 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 Analytics 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 Analytics Security Features for Administrators

Adobe Analytics enables administrators to control access to reporting data. Options include strong passwords, password expiration, IP login restrictions, and email domain restrictions. For more information, please go to https://marketing.adobe.com/resources/help/en_US/reference/security_manager.html

Adobe Data Center Physical and Environmental Controls

The below description of data center physical and environmental access controls includes controls that are common to all Adobe data center locations. Some data centers may have additional controls to supplement those described in this document.

Physical Facility Security

Adobe physically secures all hardware in Adobe-owned or -leased hosting facilities against unauthorized access. All facilities that contain production servers for Adobe Analytics 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 Analytics 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 Analytics team. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.

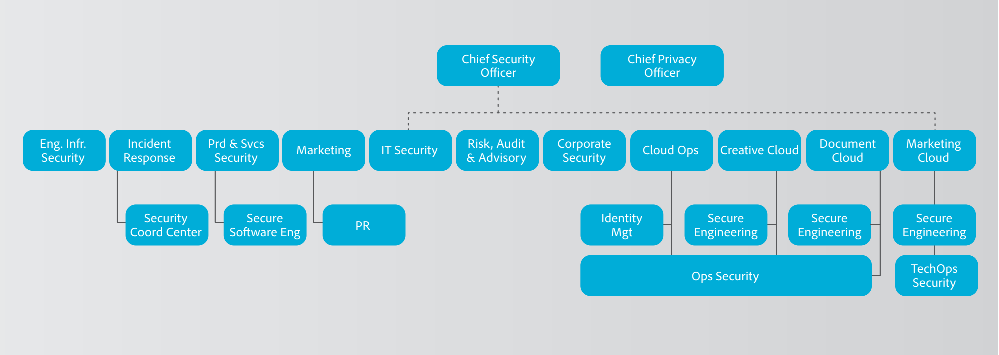


Figure 3 — The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Analytics 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 Analytics 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 Analytics security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials

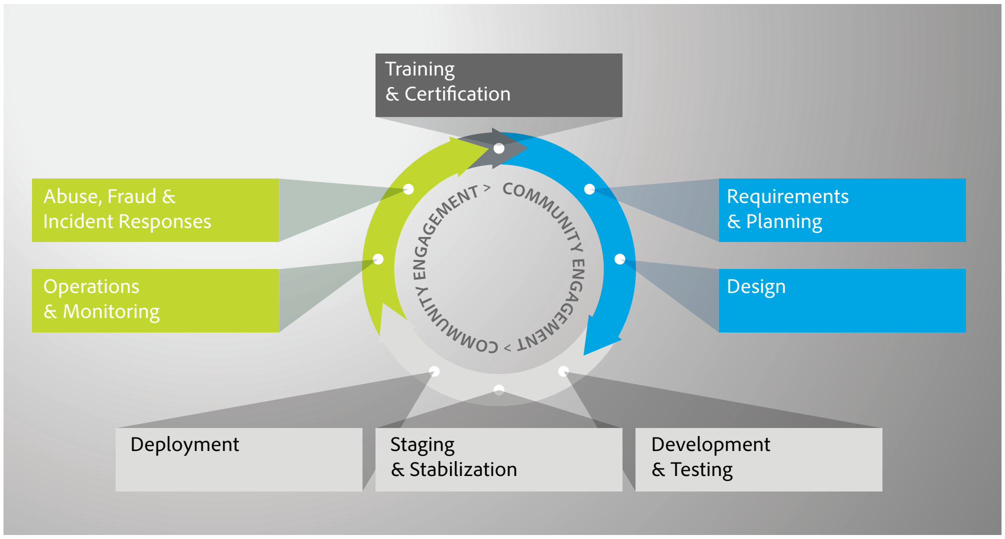


Figure 4 — Adobe Secure Product Lifecycle (SPLC)

Adobe Security Training

Adobe Software Security Certification Program

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

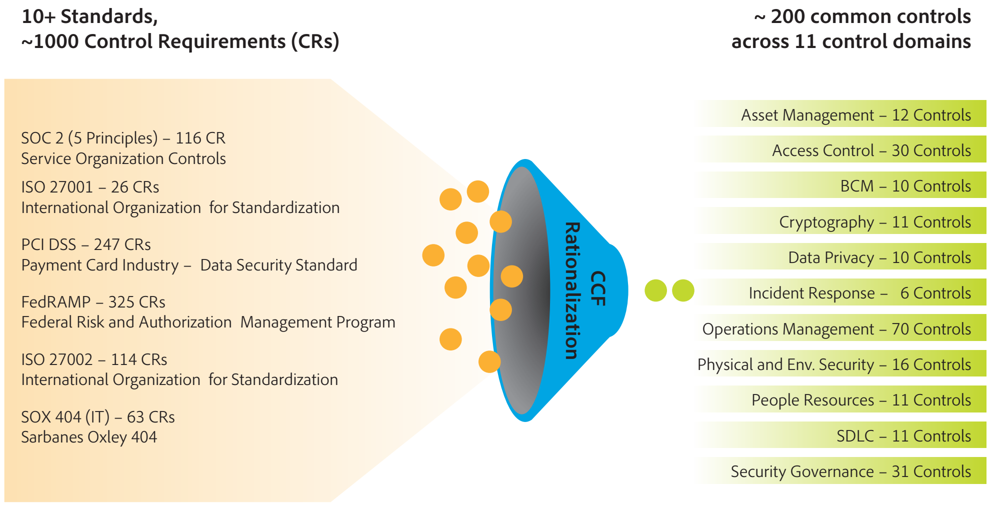
The program has four levels, each designated by a colored 'belt': white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months- or year-long hands-on security projects. Employees attaining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

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

Adobe Common Controls Framework

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

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


10+ Standards,
~1000 Control Requirements (CRs)
~ 200 common controls
across 11 control domains
SOC 2 (5 Principles) – 116 CR
Service Organization Controls
ISO 27001 – 26 CRs
International Organization for Standardization
PCI DSS – 247 CRs
Payment Card Industry – Data Security Standard
FedRAMP – 325 CRs
Federal Risk and Authorization Management Program
ISO 27002 – 114 CRs
International Organization for Standardization
SOX 404 (IT) – 63 CRs
Sarbanes Oxley 404
CCF
Rationalization
Asset Management – 12 Controls
Access Control – 30 Controls
BCM – 10 Controls
Cryptography – 11 Controls
Data Privacy – 10 Controls
Incident Response – 6 Controls
Operations Management – 70 Controls
Physical and Env. Security – 16 Controls
People Resources – 11 Controls
SDLC – 11 Controls
Security Governance – 31 Controls

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

For Adobe On-demand services, including Analytics, 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 Analytics team adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody recording.

Adobe Corporate Locations

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

Physical Security

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

Virus Protection

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

Adobe Employees

Employee Access to Customer Data

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

Security Compliance

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

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Analytics 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 security our customers' data.

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

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, change approval processes, access control procedures, and disaster recovery processes are available.

Adobe

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

www.adobe.com

Date: 11/2015