Adobe® Audience Manager

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 help bolster the security of your data and use of Adobe® Audience Manager.

About Adobe Audience Manager

Adobe Audience Manager is a data management platform that helps customers build unique audience profiles so they can identify their most valuable web traffic segments, or "audiences," and use them across any digital channel. Audience Manager also enables customers to upload other transactional datasets and combine them with web traffic to better identify customer segments.

Advertisers use Audience Manager to help grow their revenue and customer base through unified, actionable views of their audiences by combining attributes from all of their data sources into high-value audience segments for ad targeting. Publishers can sell advertisers their unique, targeted audiences—not just impressions—and identify the audience segments that are unique to their business.

Adobe Audience Manager is part of Adobe Analytics Cloud, a "customer intelligence engine" that helps empower businesses to move from insights to actions in real time by combining audience data across multiple information sources.

Adobe Audience Manager Application Architecture

The Adobe Audience Manager solution includes the following components:

Audience Manager User Interface—Enables customers to define and classify the types of data they wish to track on their website.

Data Collection Servers (DCS)—Obtain audience information from multiple sources, including customer websites, third-party data providers, customers' partners, and other Adobe Digital Marketing Solutions. The audience data is then processed based on the signal, trace, and segment rules defined by the customer in the Audience Manager user interface.

Profile Cache Servers (PCS)—Store two-week historical activity from specific users, which can then be joined with DCS data.

Outbound Publisher—Publishes content using server-to-server HTTP in real time.

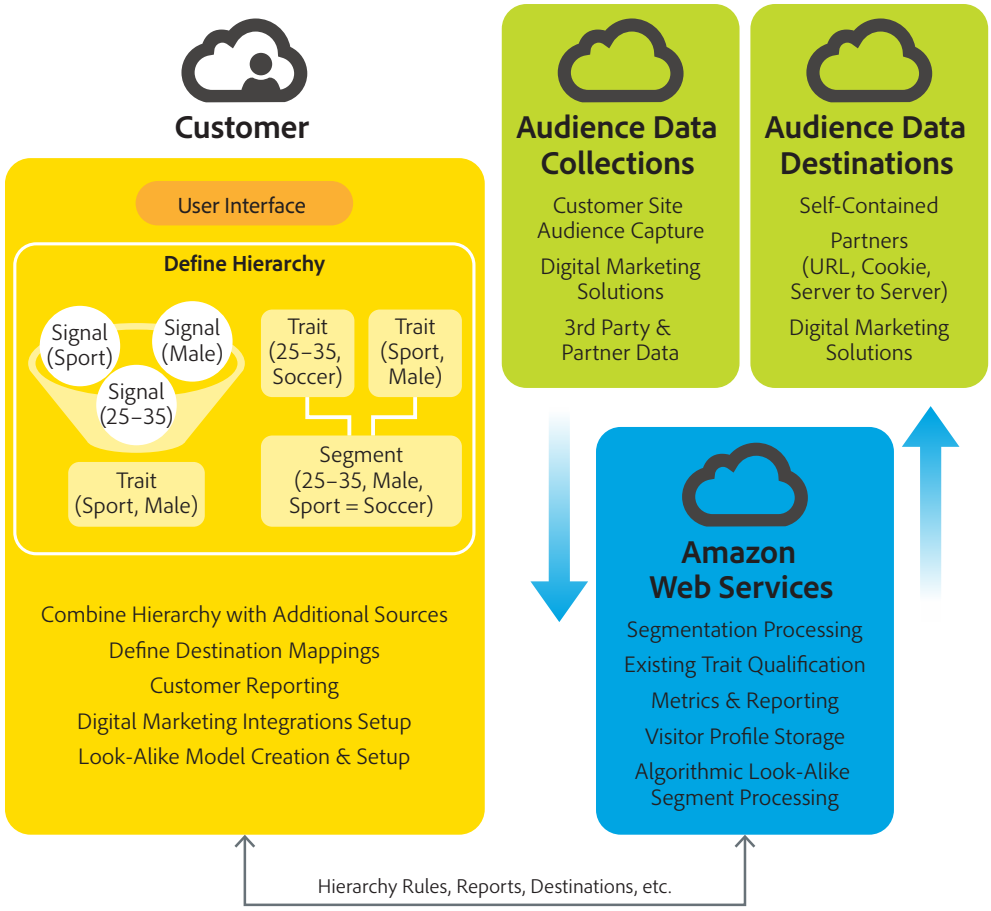

Figure 1: The Adobe Audience Manager Application Architecture

Adobe Audience Manager Application Security and Network Architecture

Adobe Audience Manager Data Flow

Customers log into the Audience Manager web interface to configure rule sets using defined attributes, such as signals, traits, and segments. A ***signal*** is a key-value pair that identifies certain web activity (e.g. page = "ports" or event = "form submission"). A ***trait*** is a combination of signals (e.g. page = sports + location = North America). A ***segment*** is the aggregation of both traits and signals (e.g. audience/segment = "North American customers who have purchased soccer jerseys from the sports page"). Customers can also combine signals, traits, and segments from customer web site interactions with other data sources as well as identify destination mappings, generate custom reports, configure digital marketing integration setup, and use a look-alike model creation and setup.

Once defined, the rules are then sent to a control database and distributed throughout the Audience Manager network via proprietary configurator software. When a user visits the customer's website, Audience Manager then places code on the computer to create behind-the-scenes communication and data collection with Adobe and its partners.

Edge data centers, hosted on Amazon Web Services (AWS), process all incoming data into segments, based on the customer-defined rules. These data centers collect the external data, marry the incoming data in the DCS to any prior user data stored in the PCS, process the information, add cookie values to each user, and send report data. Once Audience Manager processes the data, it returns the data to the customer via a distributed search index that provides real-time segment estimates.

Audience Manager also enables customers to track partner data. Partners are third-party entities that share inbound and outbound audience data with the customer. As with other incoming data from the customer's website, Audience Manager collects inbound data from the customer's partners. The DCS receives all incoming external data from both partners and the end user, and the PCS in the edge data center attempts to match the stored two weeks of historical prior trait data to incoming DCS data, thereby building a more robust web surfer profile. When required, the DCS pushes data to an external real-time reporting function.

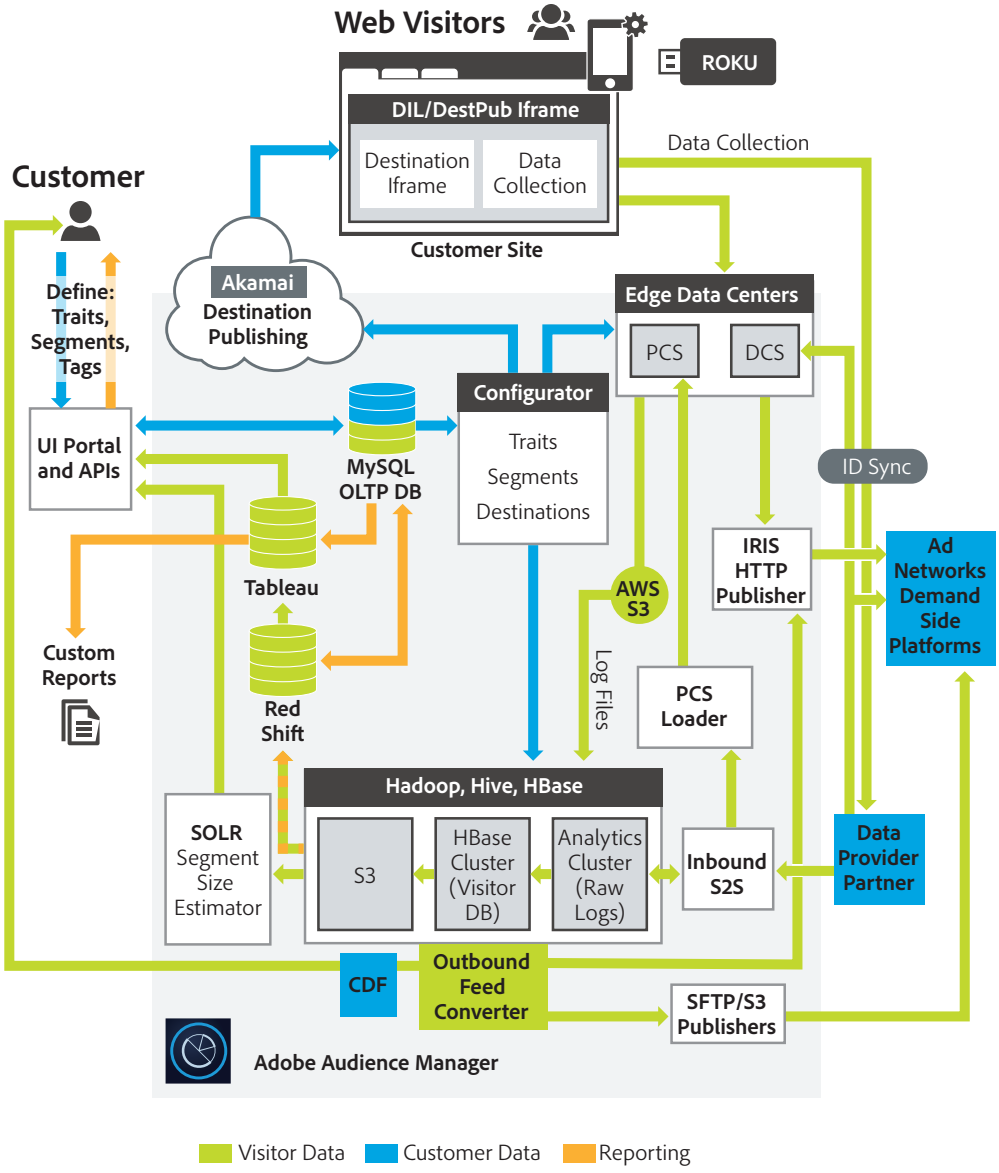

Figure 2: Adobe Audience Manager Data Flow

As information flows through Audience Manager components, Adobe relies on advanced industry-standard data encryption methods to help safeguard the confidential information when in motion. The technical safeguards include:

Data security in motion—Audience Manager supports TLS 1.2 with 128-bit key encryption when transmitting data over the Internet. It also includes export control functionality to provide finer-grained control over which data can be distributed externally.

Audience Manager never stores Personally Identifying Information (PII) anywhere in the Audience Manager network.

User Authentication

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

Users can access Adobe Audience Manager 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 Audience Manager by taking over the account or by deleting the Enterprise ID to permanently block access to associated data.

Federated ID is an enterprise-managed account where all identity profiles—as well as all associated assets—are provided by the customer's Single Sign-On (SSO) identity management system and are created, owned, controlled by customers' IT infrastructure. Adobe integrates with most any SAML2.0 compliant identity provider.

More information about Adobe Identity Management Services (IMS) can be found in this technical overview.

Adobe Audience Manager Hosting and Security

All components of Adobe Audience Manager are hosted on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the United States, EU, and Asia Pacific. Amazon EC2 is a web service that provides resizable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere.

Edge servers within the Adobe Audience Manager network are responsible for:

- Collecting new data and segmenting according to this new data as a result of real-time interaction with the digital properties (e.g. web sites, mobile apps, etc.) belonging to Audience Manager customers
- Sending this new real-time information from all Edge regions to a central location for data consolidation and for reporting purposes
- Receiving updates from the central location as a result of the data centralization process
- Publishing aliasing information to make this data available to other Adobe Marketing Cloud solutions
- Publishing data (real-time and batch) to Audience Manager partners

Core servers manage profile information and enable the platform to perform operations on those profiles to make real-time decisions.

Some hosting locations include only Edge server functionality, while others include both Edge and Core servers. Adobe uses AWS components communicating via secure HTTP (HTTPS) to facilitate transfer of information between components.

The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits. You can find more detailed information about AWS and Amazon's security controls on the AWS security site.

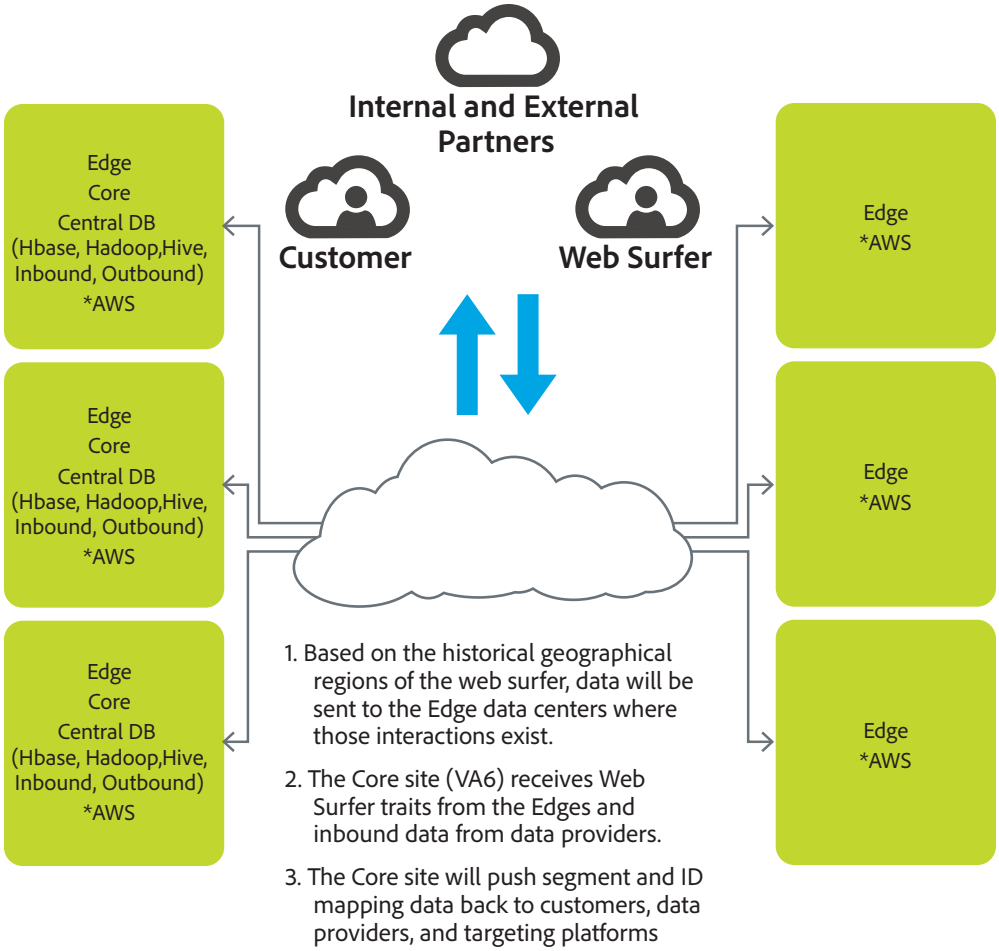

Figure 3: The Adobe Audience Manager Network

Operational Responsibilities of AWS and Adobe

AWS operates, manages, and controls the components from the hypervisor virtualization layer down to the physical security of the facilities in which Adobe Audience Manager operates. In turn, Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and application software, as well as the configuration of the AWS-provided security group firewall.

AWS also operates the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. The AWS infrastructure includes facilities, network, and hardware, as well as operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources. Amazon designs and manages AWS according to industry-standard practices as well as a variety of security compliance standards.

Secure Management

Adobe uses Secure Shell (SSH) and Secure Sockets Layer (SSL) for management connections to manage the AWS infrastructure.

About Amazon Web Services (AWS)

The following information is from the AWS: Overview of Security Processes White paper. For more detailed information about AWS security, please consult the AWS security site.

Isolation of Customer Data/Segregation of Customers

AWS uses strong tenant isolation security and control capabilities. As a virtualized, multi-tenant environment, AWS implements security management processes and other security controls designed to isolate each customer, such as Audience Manager, from other AWS customers. Adobe uses the AWS Identity and Access Management (IAM) to further restrict access to compute and storage instances.

In addition, Adobe Audience Manager implements the following additional partitioning to help prevent accidental information exposure:

- Trait Data Partitioning: Your data (traits, IDs, etc.) is partitioned by client. This helps prevent accidental information exposure between different clients. For example, trait data in cookies is partitioned by customer and stored in a client-specific sub-domain. It cannot be read or used accidentally by another Audience Management client. Furthermore, trait data stored in the Profile Cache Servers (PCS) is also partitioned by customer. This prevents other clients from accidentally using your data in an event call or other request.
- Data Partitioning in Reports: Client IDs are part of the identifying key in all reporting tables and report queries are filtered by ID. This helps prevent your data from appearing in the reports of another Audience Management customer.

Secure Network Architecture

AWS employs network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic.

Amazon Information Security approves all ACL policies and automatically pushes them to each managed interface using AWS's ACL-Manage tool, helping to ensure these managed interfaces enforce the most up-to-date ACLs.

Network Monitoring and Protection

AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points.

The AWS network provides significant protection against traditional network security issues:

- Distributed Denial of Service (DDoS) attacks
- Man-in-the Middle (MITM) attacks
- IP Spoofing
- Port Scanning
- Packet sniffing by other tenants

You can find more information about Network Monitoring and Protection in the AWS: Overview of Security Processes white paper on the Amazon website.

Intrusion Detection

Adobe actively monitors all components of Audience Manager using industry-standard intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Logging

Adobe conducts server-side logging of Audience Manager customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs only store Adobe IDs to help diagnose specific customer issues and do not contain username/password combinations. Only authorized Adobe technical support personnel, key engineers, and select developers can access the logs to diagnose specific issues that may arise.

Service Monitoring

AWS monitors electrical, mechanical, and life support systems and equipment to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, AWS performs ongoing preventative maintenance.

Data Storage and Backup

Adobe stores all Audience Manager data in Amazon S3, which provides a storage infrastructure with high durability. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in an Amazon S3 region. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper.

Change Management

AWS authorizes, logs, tests, approves, and documents routine, emergency, and configuration changes to existing AWS infrastructure in accordance with industry norms for similar systems. Amazon schedules updates to AWS to minimize any customer impact. AWS communicates with customers, either via email, or through the AWS Service Health Dashboard when service use is likely to be adversely affected.

Patch Management

AWS maintains responsibility for patching systems that support the delivery of AWS services, such as the hypervisor and networking services. Adobe is responsible for patching its guest operating systems (OS), software, and applications running in AWS. When patches are required, Adobe supplies a new, pre-hardened instance of the OS and application rather than an actual patch.

AWS Data Center Physical and Environmental Controls

AWS physical and environmental controls are specifically outlined in a SOC 1, Type 2 report. The following section outlines some of the security measures and controls in place at AWS data centers around the world. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper or the Amazon Security website.

Physical Facility Security

AWS data centers utilize industry standard architectural and engineering approaches. AWS data centers are housed in nondescript facilities and Amazon controls physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Fire Suppression

AWS installs automatic fire detection and suppression equipment in all AWS data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Controlled Environment

AWS employs a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. AWS data centers maintain atmospheric conditions at optimal levels. AWS personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup Power

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Video Surveillance

Professional security staff strictly controls physical access both at the perimeter and at building ingress points for AWS data centers using video surveillance, intrusion detection systems, and other electronic means.

Disaster Recovery

AWS data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built in clusters in various global regions, all data centers remain online 24/7/365 to serve customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load- balanced to the remaining sites. You can find more information about AWS disaster recovery protocols on the Amazon Security website.

Adobe Audience Manager Backup and Disaster Recovery Procedures

Audience Manager's DCS servers leverage GSLB (Global Service Load Balancing) to send visitors to the network-closest DCS cluster. Both DCS and PCS servers are spread across availability zones within a given AWS region, which makes up a cluster. Adobe takes regular nightly snapshots of the data within PCS clusters and stores these on S3.

In the event of a disaster affecting a single data center, the DCS and PCS real-time systems will automatically fail over to other active data centers without any manual intervention. Expected time for full failover is less than 20 minutes.

Adobe Risk & Vulnerability Management

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

Penetration Testing

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

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

Internally, Adobe Audience Manager security team performs a risk assessment of all Audience Manager components quarterly and prior to every release. The Audience Manager 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 white paper provides here.

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 go here.

Forensic Analysis

For incident investigations, Audience Manager 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.

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 Audience Manager 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.

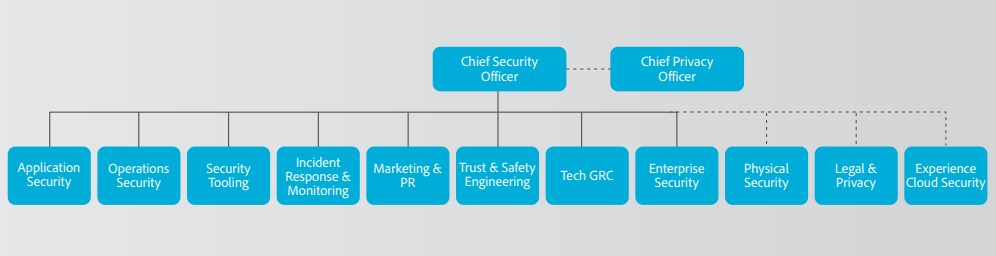

Figure 4: Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Audience Manager 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. More information on our secure engineering practices can be found in this white paper on Adobe.com.

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 Audience Manager 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. You can learn more about our security certification program here on Adobe.com.

Adobe Audience Manager 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.

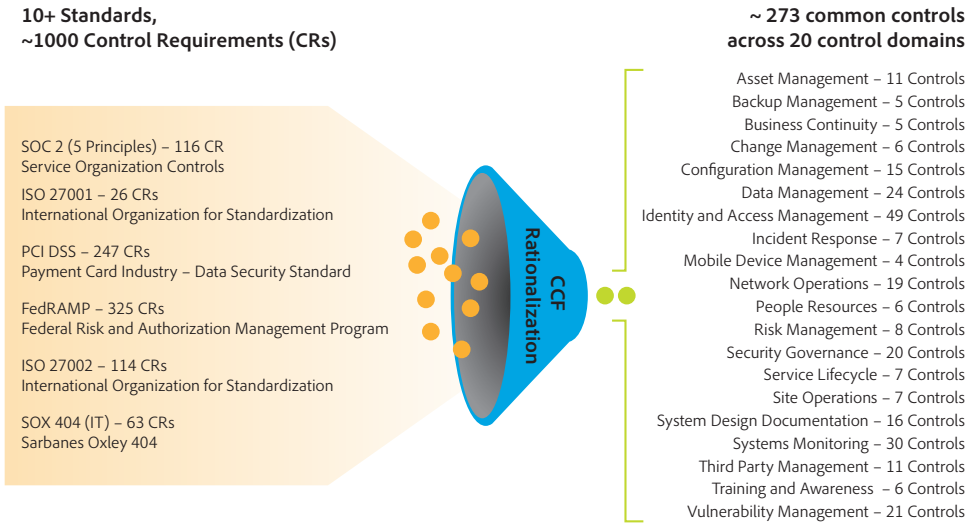

Figure 5: The Adobe Common Controls Framework (CCF)

Current Regulations and Compliance for Adobe Audience Manager

SOC 2 is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Audience Manager is SOC 2 – Type 2 (Security & Availability) compliant.

ISO 27001 is a set of globally adopted standards that outline stringent security requirements and provide a systematic approach to managing the confidentiality, integrity, and availability of customer information. Adobe Audience Manager is compliant with ISO 27001:2013.

The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions safeguard their customers' personal data. Adobe Audience Manager is GLBA-Ready, meaning that it enables our financial customers to comply with the GLBA Act requirements for using service providers.

Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

Adobe 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 Audience

Manager, 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 Audience Manager 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 try to stay ahead of malicious activities and help ensure the secure our customers' data.

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

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