Adobe® Captivate Prime Security Overview

Table of Contents

1 Adobe Security
1 About Adobe Captivate Prime
4 Adobe Captivate Core Operational Security
6 Adobe Risk & Vulnerability Management
7 AWS Physical and Environmental Controls
8 Adobe Corporate Security
8 Adobe Secure Product Development
9 Adobe Software Security Certification Program
10 Adobe Corporate Locations
10 Adobe Employees
12 Conclusion

Adobe Security

At Adobe, we take the security of your digital experience very seriously. Security practices are deeply ingrained into our internal software development and operations processes and tools and are rigorously followed by our cross-functional teams to prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities and we regularly incorporate advanced security techniques into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of your Adobe® Captivate Prime experience and your data.

About Adobe Captivate Prime

Adobe Captivate Prime is a Learning Management System (LMS) that streamlines the process of setting up, delivering, and tracking virtually any form of learning content. A self-service, cloud-based tool, Adobe Captivate Prime enables specialists in learning and development, training, and corporate HR departments to take charge of the learning environments they manage. Course authors can upload a variety of content formats into Captivate Prime, including PowerPoint, video, PDF, and Word documents, as well as AICC, TinCan/xAPI, and SCORM packages.

Adobe Captivate Prime Application Architecture

Adobe Captivate Prime is a hosted cloud solution that separates logical functions, such as presentation, application processing, and data management across independent processes. These processes run on multiple application servers, each of which provides a different service based on the different needs of LMS users, including administrators, authors, managers, and learners. Functions provided by Adobe Captivate Prime include content creation, management and on-demand delivery, user/group management, permissions and grants, and client session functionality.

Adobe Captivate Prime includes the following six (6) components:

- **Adobe Captivate Prime Business Logic Server** — Enables the creation and management of users, learning objects (e.g., courses, learning programs, and certifications), enrollments, and user groups.
- **Adobe Captivate Prime Learning Record Server** — Manages learning records captured while learners take courses (e.g., capture slide view, time spent on a slide, quiz scores, etc.) and handles all requests pertaining to real-time, customizable reports.
- **Adobe Captivate Prime Worker Server** — Performs all asynchronous jobs, such as course content conversion, large report generation, and bulk user import.
- **API Gateway Server** — Validates each connection request to determine user authenticity and session validity. The API gateway also authorizes and allows access to resources only to privileged users (e.g., only Authors can create a course, only Admins can add a learner, etc.).
- **Container Servers** — Hosts miscellaneous services, including external connectors (e.g., SFDC, FTP servers, and WorkDay), public APIs, and oAuth.
- **Fluidic Player** — Allows learning content to play on user devices with a uniform experience.

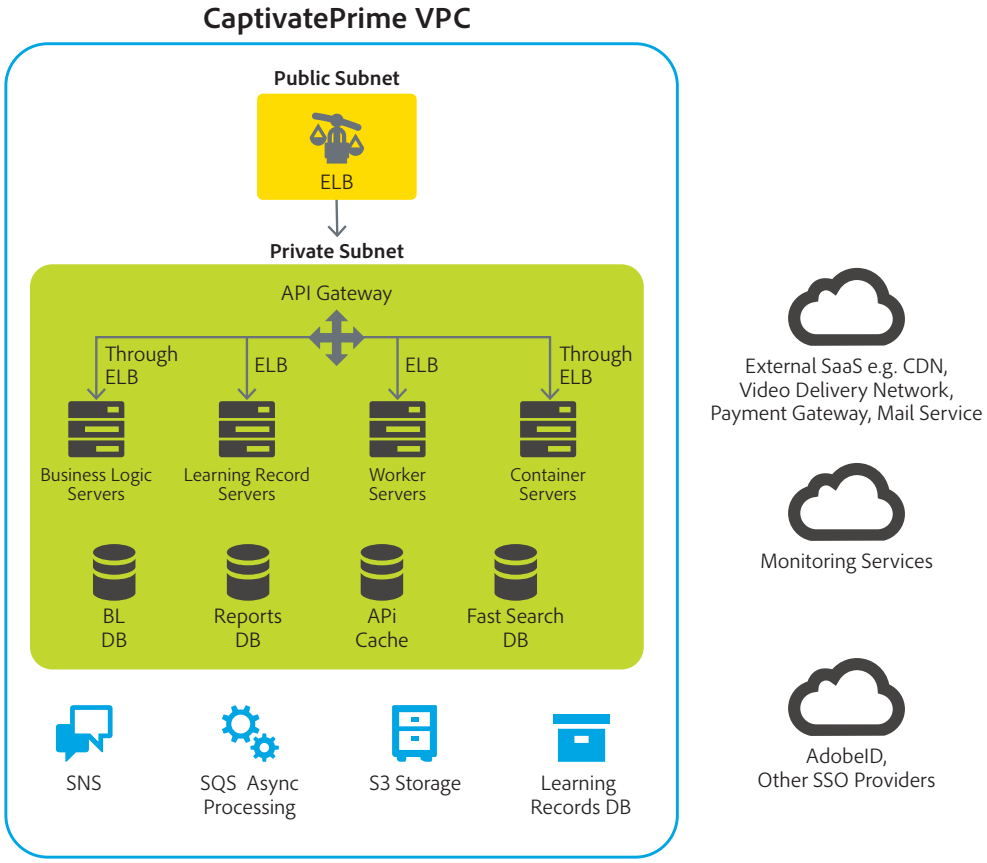

Figure 1: Adobe Captivate Prime application architecture

Adobe Captivate Data Flow

Adobe Captivate Prime supports five (5) different roles throughout the system, each of which provides and consumes various types of data. The roles and the specific data for which each is responsible includes:

- **Administrators and Integration Administrators** — Import user data into Adobe Captivate Prime and provision access to the account as well as course assets to other users of the system. User data is typically provided in the form of CSV or manually entered user details (e.g., email, name, designation, location, etc.).
- **Authors** — Create courses by uploading various eLearning content (e.g., PDF, video, .doc/.docx, PPT, Zip, etc.)
- **Learners** — Take courses based on their interest or based on assignments made by their manager or administrators. Adobe Captivate Prime records interactions between the learner and the course (e.g., time spent per slide/page, answers given to questions, time spent in video, etc.) for reporting purposes.
- **Managers** — View reporting data collected for their team using various customizable reports.

Figure 2, below, illustrates how data flows in the Adobe Captivate Prime system, including where it is stored and how it is consumed. Each color line describes one type of data flow into and out of the system.

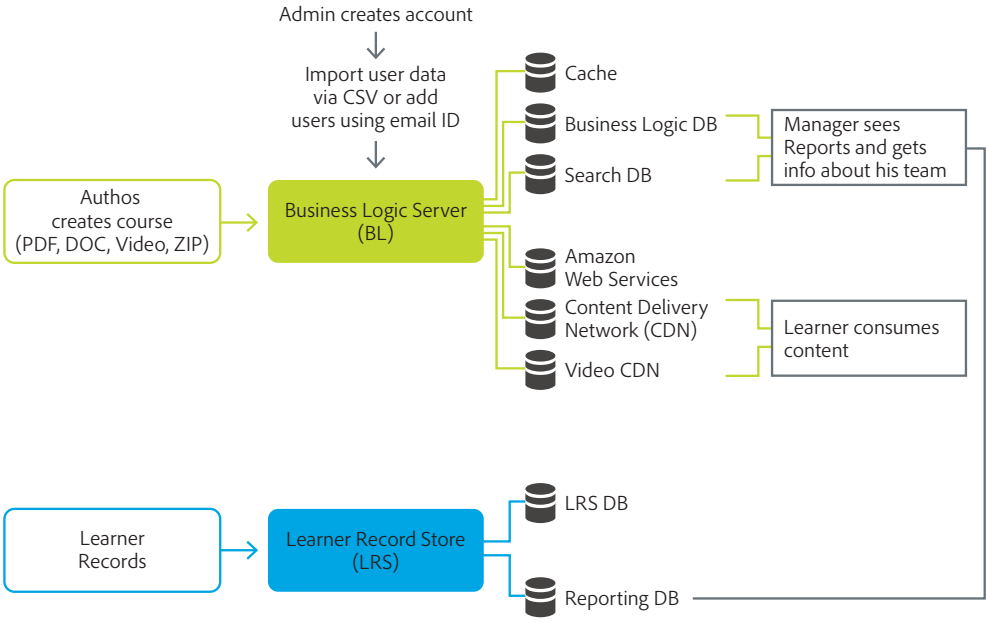

Figure 2: Adobe Captivate data flow

Any client connection to Adobe Captivate Prime over the Internet is sent via HTTPS using SSL (Secure Sockets Layer). Any communication with a third-party service, such as Akamai, Mandrill, Brightcove, FastSpring, and Box is also sent using HTTPS.

Adobe Captivate Security Architecture

Adobe Captivate Prime is hosted on Amazon Web Services (AWS) in an Amazon Virtual Private Could (Amazon VPC). All user-supplied content (e.g., courses, profile images, etc.) is made available via an authorization layer and can only be accessed by appropriately authorized individuals.

The Adobe Captivate Prime databases also reside inside the VPC and can only be accessed via authorized application server machines. These multi-tenant databases include special in-database security layers and additional code that helps restrict data access to the designated tenant. A user of one Adobe Captivate Prime account does not have permission to access data of any other Adobe Captivate Prime account.

Administrator security features

Adobe Captivate Prime provides role-based authentication and authorization and supports five (5) different roles throughout the system. Only those with Administrator privileges can provision and revoke roles. Users are only able to access functionality specifically granted to his or her role. Adobe Captivate Prime roles include:

- **Administrator** — Full control of the organization's Adobe Captivate Prime account, including adding, removing, enrolling, and updating users, creating learning objects, and viewing reports.
- **Author** — Create, upload, revise, and update courses.
- **Manager** — View reports of team members that report to him/her.
- **Integration Administrator** — Integrate Adobe Captivate Prime with external systems, such as Salesforce and Workday.
- **Learner** — Search for learning objects, enroll in them, and take courses.

User Authentication

Users can access Adobe Captivate Prime in one of three (3) different types of user-named licensing. Each of these types uses an email address as the user name and include:

Adobe ID is for Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users.

Federated ID is an enterprise-managed account where all identity profiles—as well as all associated asset—are provided by the customer's Single Sign-On (SSO) identity management system and are created, owned, controlled by the customer's IT department. Adobe Captivate Prime integrates with most any SAML 2.0-compliant identity provider.

CaptivatePrime ID enables external users (temporary users or partners) to create their Adobe Captivate Prime account by providing their email and setting a password. These credentials are stored in Adobe Captivate Prime and are used for authentication purposes. All the passwords are hashed and salted for encryption before storing in the database. The database is in private subnet and can only be accessed by the Adobe Captivate Prime authentication module.

All Protections implemented via the authentication and authorization layer help ensure content (e.g., courses, files, images, etc.) uploaded into Adobe Captivate Prime can only be seen by users logged into an Adobe Captivate Prime account with sufficient privileges to view that content (e.g., a user can only view course content when the admin specifically grants him or her the necessary permissions).

Adobe Captivate Core Operational Security

Adobe Captivate Prime is hosted on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the Northern Virginia, USA and Frankfurt, Germany regions, using multi-availability zone deployment to provide resilience in case an availability zone develops issues. 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.

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.

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 Target 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 the 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. AWS infrastructure can only be accessed from inside Adobe's corporate network to help prevent any un-authorized external access.

Geographic Location of Customer Data on AWS Network

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

Adobe Captivate Prime is deployed and data is stored in two separate, independent AWS regions: Northern Virginia, USA and Frankfurt, Germany. Data replication for Amazon S3 data objects occurs within the regional cluster where the data is stored and is not replicated to data center clusters in other regions.

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 from other AWS customers. Adobe uses the AWS Identity and Access Management (IAM) to further restrict access to compute and storage instances.

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 Adobe Captivate Prime using industry-standard Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Logging

Adobe conducts server-side logging of Adobe Captivate Prime 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 any restricted or confidential data, such as usernames and passwords. 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 Adobe Captivate Prime 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. Adobe also maintains a Status Health Dashboard for Adobe Captivate Prime at http://status.adobe.com/captivate_prime.

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.

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 help 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, the Adobe Captivate Prime security team performs a risk assessment of the Adobe Captivate Prime application prior to every release. Conducted by highly trained security staff trusted with creating a secure network topology and infrastructure and Adobe Captivate Prime application; the security reviews look for insecure network setup issues across firewalls, load balancers, and server hardware and also application level vulnerabilities. The security touch-points include exercises like threat modeling coupled with vulnerability scanning, static and dynamic analysis of the application. The Adobe Captivate Prime security team partners with the technical operations and development leads to help ensure high-risk vulnerabilities are mitigated prior to each release.

Availability and Application Monitoring

Health check URLs are set up for application health monitoring through automated systems that frequently ping service APIs and monitor page response time, page load time, error rate, and more. In case of any outage or abnormal monitored parameter value, the systems trigger an email alarm to the network operations team. These automated systems have been configured to monitor aspects of machine health, including CPU, memory, network, disk space, processes, etc.

Database

Amazon configures its databases with multi-availability-zone deployment to help ensure high availability and seamless failover. Learning records are transferred to an AWS database, which synchronously replicates data across three facilities within an AWS region to achieve high availability and durability. Granular data from Amazon is fetched and sent to create intelligent data aware store to facilitate retrieving and creating reports faster.

Incident Response and Notification

New vulnerabilities and threats evolve each day and Adobe strives to respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists,

including US-CERT, Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

When a significant announced vulnerability puts Adobe Captivate Prime at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Captivate organization to coordinate the mitigation effort.

For Adobe cloud-based services, including Captivate Prime, 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 Captivate 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.

AWS 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 Corporate Security

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 Target 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.

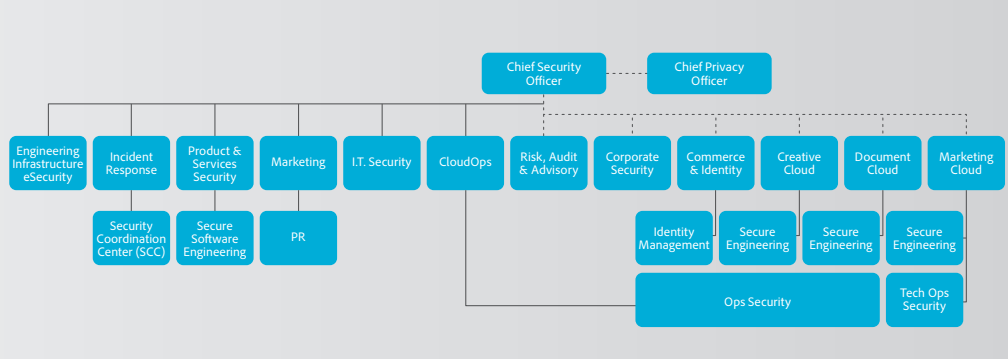

Figure 3: The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Captivate Prime 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 Captivate Prime 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 Captivate Prime 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

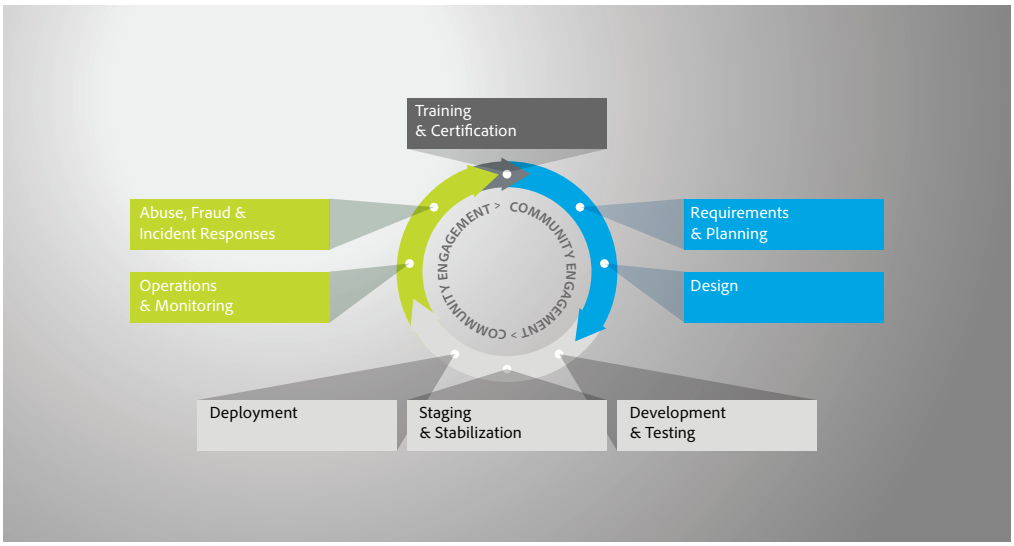

Figure 4: Adobe Secure Product Lifecycle (SPLC)

Adobe 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 Captivate Prime 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 Corporate Locations

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

Physical Security

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

Adobe Employees

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Captivate Prime, 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.

Compliance

Adobe Captivate Prime Compliance Posture

One way Adobe demonstrates our commitment to stronger security practices is by achieving compliance with security certifications, standards and regulations for our cloud products, services, platforms and operations.

At the time of this publishing, Adobe Captivate Prime has demonstrated the following:

- **SERVICE ORGANIZATION CONTROL (SOC) REPORTING** — The Service Organization Control (SOC) reporting standard is established by the American Institute of Public Accountants (AICPA). Adobe currently utilizes the SOC 2 reporting standard. SOC 2 reports are based on a third-party attestation of compliance with AICPA Trust Service Principles (TSPs) relevant to security, availability, confidentiality, privacy, and processing integrity.
- **ISO 27001** — This certification demonstrates a systematic approach toward managing information security risks that affect the confidentiality, integrity, and availability of the service and customer information. ISO 27001 certification includes the establishment of a formal information security management program, demonstrating Adobe's commitment to providing transparency into its security controls and practices.
- **FERPA** — The U.S. Family Educational Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. Student education records and directory information. Under FERPA guidelines, Adobe can contractually agree to act as a "school official" when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements.
- **GLBA** — The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard their customers' personal data. A "GLBA-Ready" Adobe service means that the service can be used in a way that enables the customer to help meet its GLBA Act obligations related to the use of service providers.

Adobe Common Controls Framework

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

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

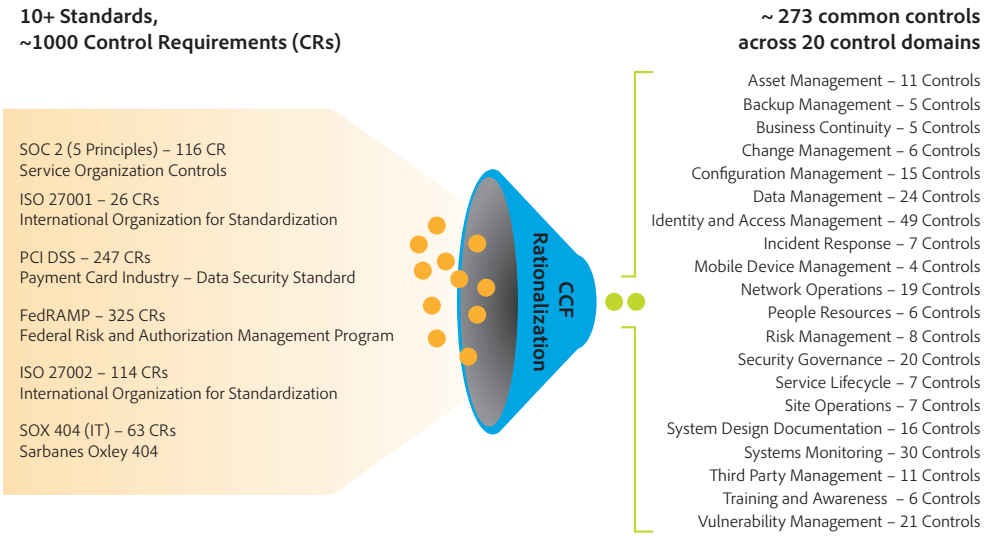

Figure 5: The Adobe Common Controls Framework (CCF)

Customer Data Confidentiality

Adobe treats customer data as confidential. Adobe does not access, 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. For more information on Adobe's privacy practices, please visit the Adobe Privacy Center.

Conclusion

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

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

Adobe

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