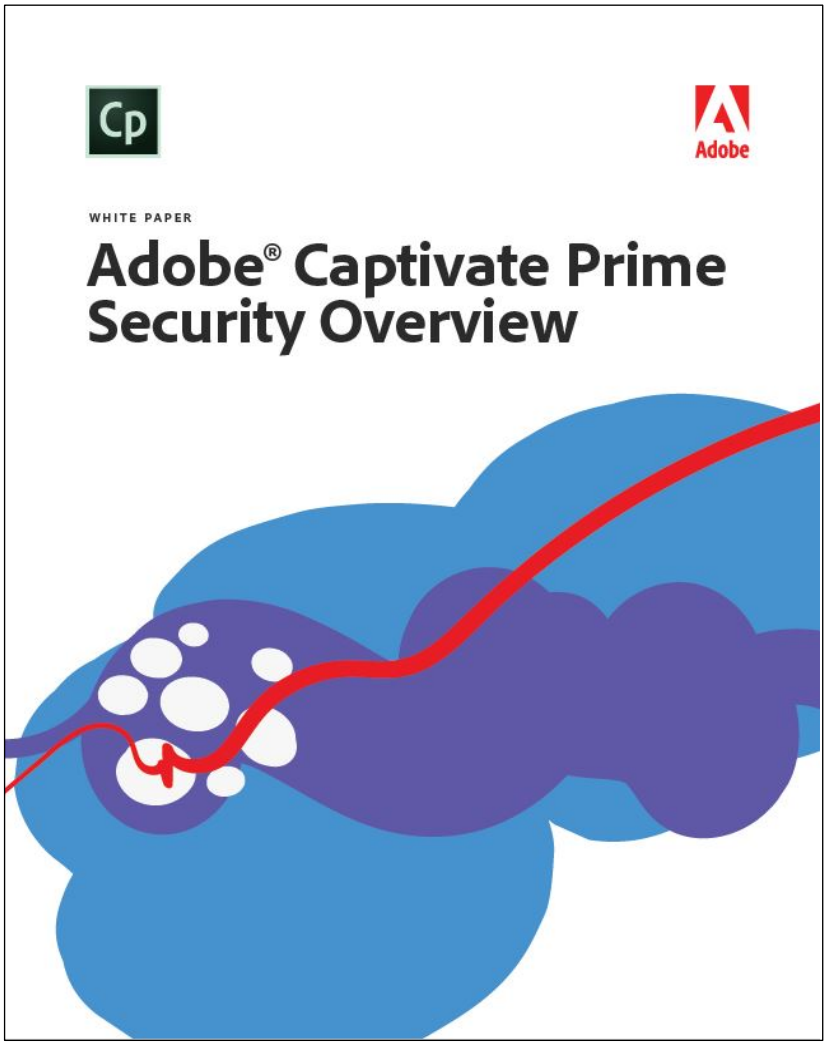
Adobe Captivate Prime Security Overview

White Paper



WHITE PAPER

Adobe® Captivate Prime Security Overview

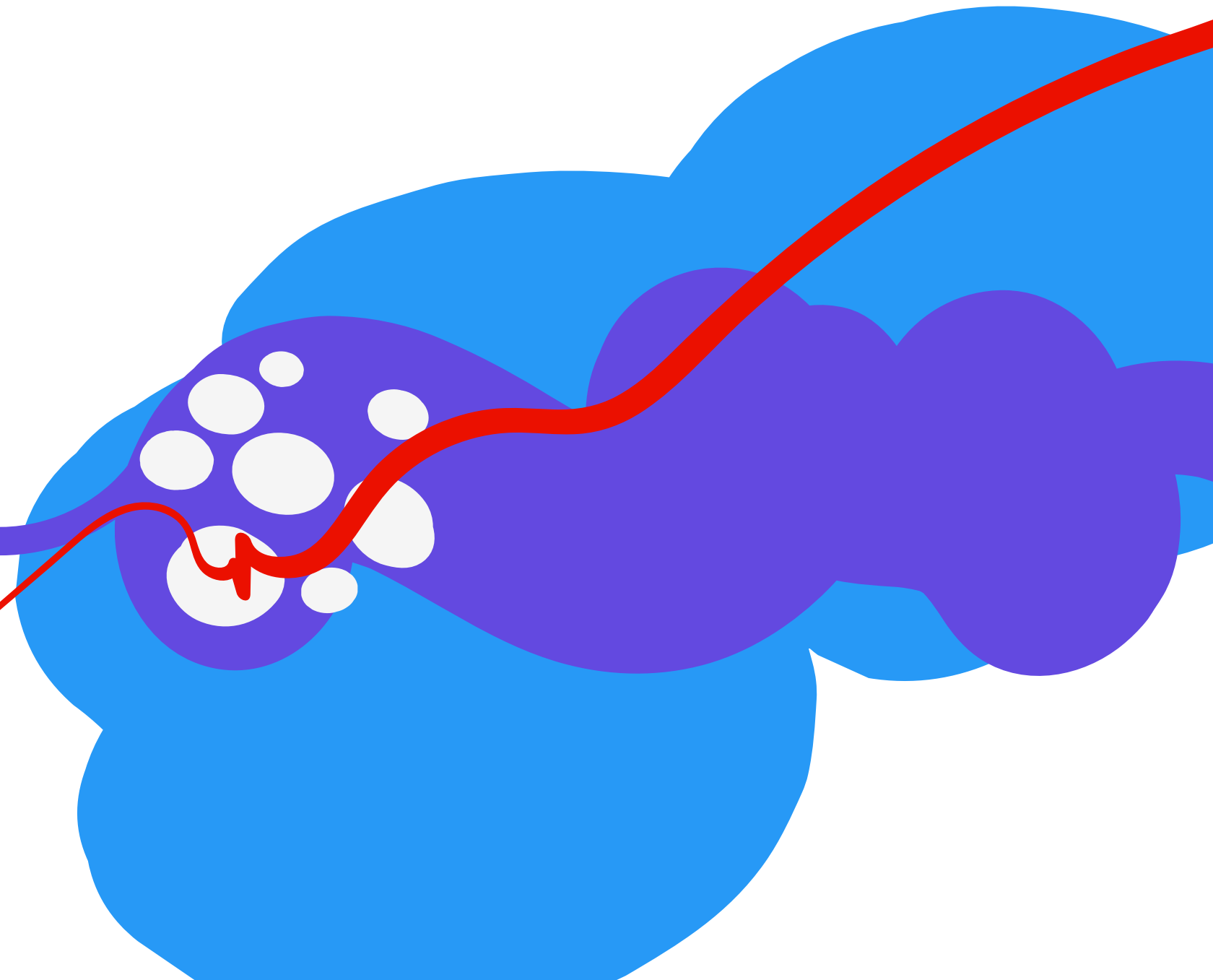
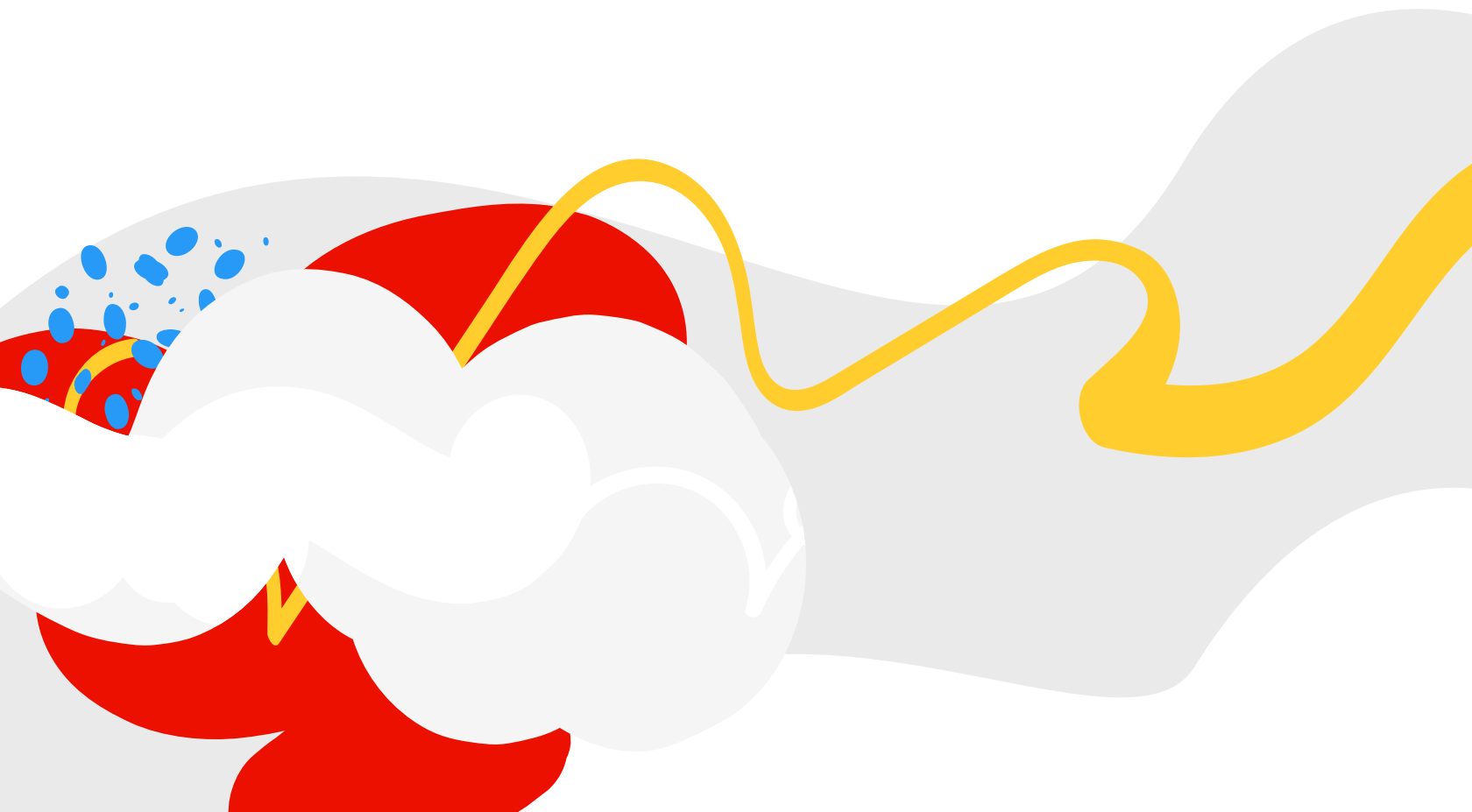


Table of Contents

Adobe Security	1
About Adobe Captivate Prime	1
Adobe Captivate Prime Network Management	5
Data Center Physical and Environmental Controls	8
The Adobe Security Organization	10
Adobe Software Security Certification Program	12
Adobe Captivate Prime Compliance	12
Adobe Risk & Vulnerability Management	13
Adobe Corporate Locations	14
Conclusion	16



Adobe Security

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

This white paper describes the defense-in-depth approach 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 set-up, delivery, and tracking of 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 static content formats into Captivate Prime, including PowerPoint, video, PDF, and Word documents, as well as interactive content, such 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.

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.

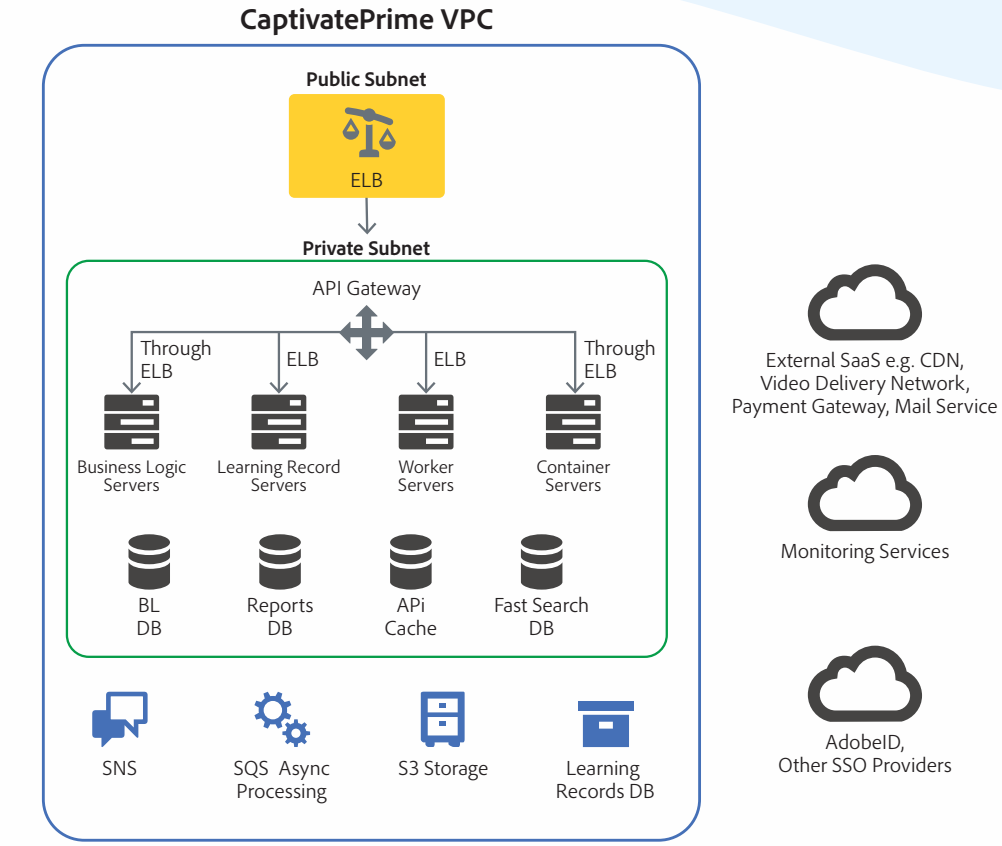


Figure 1: Adobe Captivate Prime application architecture

Adobe Captivate Roles

Adobe Captivate Prime supports six (6) different roles, each of which delivers and consumes various types of data. The roles and the specific data for which each is responsible include:

- **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 CSV format 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 a variety of customizable reports.
- **Instructors** — Manage sessions and modules, upload additional resources, grade activities, approve submissions and checklists, and mark session attendance.

Adobe Captivate Data Flow

The diagram 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.

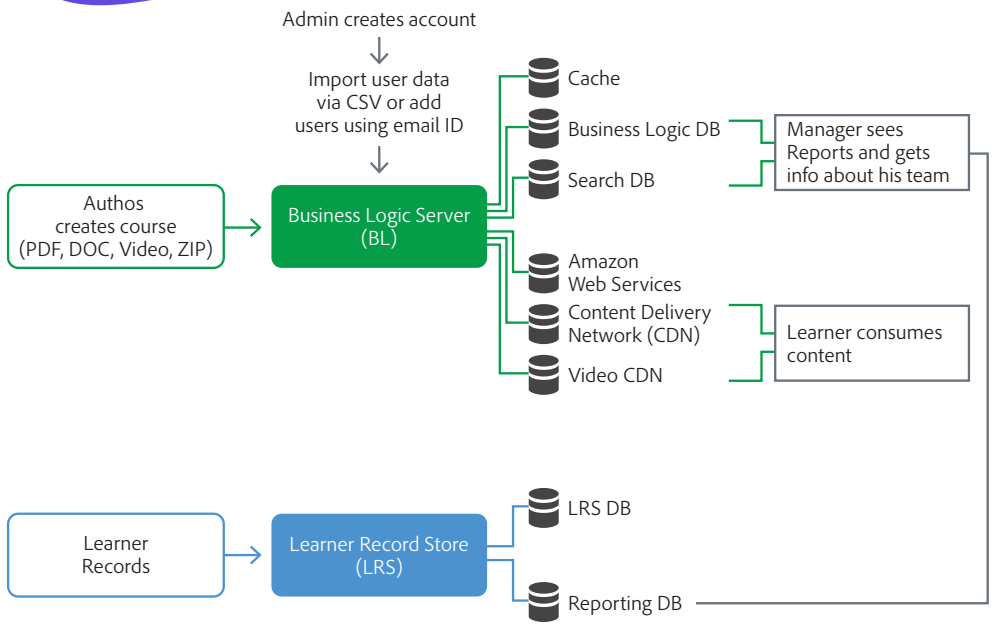


Figure 2: Adobe Captivate data flow

All client connections to Adobe Captivate Prime over the Internet are sent via HTTPS using SSL (Secure Sockets Layer), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. Any communication with a third-party service, such as Akamai, Brightcove, SendGrid, 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.

Administrative Security Controls

Adobe Captivate Prime provides role-based authentication and authorization and supports the above-mentioned six (6) user roles. The Administrator role has full control of the organization's Adobe Captivate Prime account, including adding, removing, enrolling, and updating users, creating learning objects, and viewing reports. Only those with Administrator privileges can provision and revoke roles, including the Integration Administrator role, which manages the integration of Adobe Captivate Prime with external systems, such as Salesforce and Workday. Users are only able to access functionality specifically granted to their role.

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.

- **Captivate Prime 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 Prime Network Management

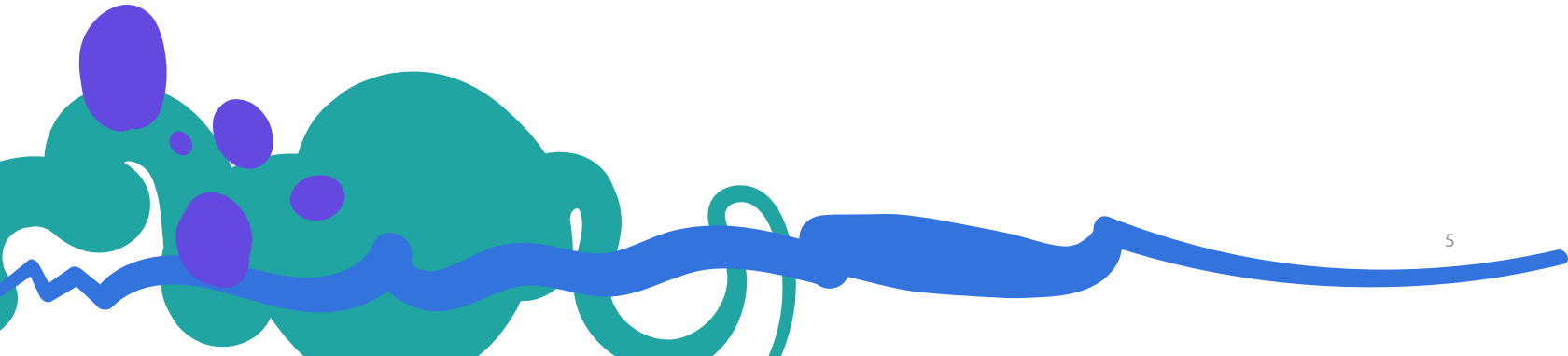
Adobe understands the importance of securing the data collection, data content serving, and reporting activities over the Adobe Captivate Prime network. To this end, the network architecture is designed with security as a top priority, including segmentation of development and production environments and authenticated RBAC.

Isolation of Customer Data/Segregation of Customers

Adobe provisions a separate Adobe Captivate Prime VPC for each customer using strong tenant isolation security and control capabilities, both those implemented by the hosting provider as well as Adobe-specific code that further restricts access to each customer VPC.

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.

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 any other Adobe Captivate Prime account.



Customer data resides in the same data center as the customer's Adobe Captivate Prime VPC, either US East (Virginia) or Frankfurt, Germany. Replication of Amazon S3 data objects occurs in the regional cluster in which the data is stored.

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 Captivate Prime 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 (2FA). Unless the connection originates from a list of trusted IP addresses, Adobe does not allow management access from the Internet.

Service Monitoring

Adobe monitors all servers, routers, switches, load balancers, and other critical network equipment on the Adobe Captivate Prime 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 promptly attempt to fix or escalate the issue to the appropriate Adobe personnel. Additionally, Adobe contracts with multiple third parties to perform external monitoring.

Further, Adobe uses state-of-the-art technologies and industry-leading providers for application-specific monitoring and alerting. SLIs and SLOs are constantly tracked, and violations result in alerts with the appropriate severity.

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 this change management tool to schedule maintenance blackouts outside of periods of high network traffic. Adobe also maintains a Status Health Dashboard for Adobe Captivate Prime.

Patch Management

In order to automate patch distribution to host computers within the Adobe Captivate Prime 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 aregular patch schedule. If required, Adobe releases and deploys emergency patch releases on short notice.

Firewalls (Secure Network Routing) and Load Balancers

Secure network routing is implemented to only allow connections to allowed ports, i.e., Port 443 for HTTPS. Outbound traffic is only allowed on HTTPS and NAT masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming 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 NAT and internal network policies, prevent an individual server on the network from being directly addressed from thexInternet, greatly reducing the potential vectors of attack.

Intrusion Detection

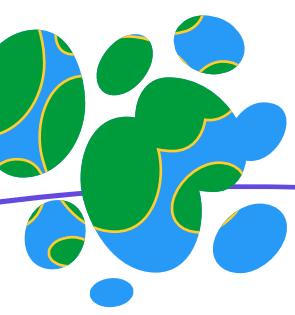
Adobe deploys Intrusion Detection System (IDS) sensors at critical points in the network to detect and alert our security team to unauthorized attempts to access the network. The security team follows up on intrusion notifications by validating the alert and inspecting the Adobe Captivate Prime platform for any sign of compromise. Adobe regularly updates all sensors and monitors them for proper operation.

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 Captivate Prime production server connections for auditing. For Captivate Prime environments, Adobe makes built-in security features available to implement permissions and access control using groups and privileges.

Logging

In order to help protect against unauthorized access and modification, Adobe captures and manages network logs, OS-related logs, and intrusion detections using a combination of industry-standard and Adobe-proprietary tools. Adobe periodically reviews log storage capacity and expands storage capacity if, and when, required. Adobe hardens all systems that generate logs and restricts access to logs and logging software to authorized Adobe personnel. Adobe retains raw logs for one year and all logs are managed and accessed only by Adobe personnel.



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 Captivate Prime 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. All 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 hint 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 promptly handle environmental issues 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 Captivate Prime 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

Captivate Prime utilizes multi-AZ deployment and backups are stored in multiple AZs in their respective regions, either US East (Virginia) or Frankfurt, Germany, thereby helping ensure the solution's resilience in the event of a data center failure. Service restoration is fulfilled within commercially reasonable best efforts and is performed in conjunction with the data center provider's ability to supply adequate infrastructure at the prevailing failover location.

Captivate Prime is hosted in state-of-the-art AWS data centers, which are highly resilient and designed to tolerate system or hardware failures with minimal impact. Each data center runs on its own physically distinct and independent infrastructure to help ensure business continuity in the event of an outage. Captivate Prime's recovery point objective (RPO) is 24 hours and recovery time objective (RTO) is 72 hours.

Availability and Notification

Captivate Prime uptime data is available at on the Adobe Status website. Additionally, for both planned and unplanned system downtime, the Captivate Prime team also follows a notification process to inform customers about the status of the service. If there is a need to migrate the operational service from a primary site to a disaster-recovery site, customers will receive several specific notifications including:

- Notification of the intent to migrate the services to the disaster recovery site
- Hourly progress updates during the service migration
- Notification of completion of the migration to the disaster recovery site

The notifications will also include contact information and availability for client support and customer success representatives. These representatives will answer questions and concerns during the migration as well as after the migration to promote a seamless transition to newly active operations on a different regional site.

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 Captivate Prime 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.

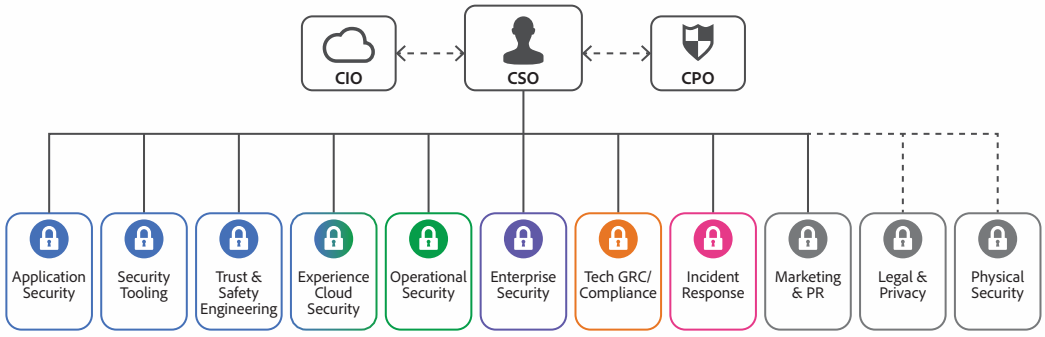


Figure 3: The Adobe Security Organization

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.

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 in general. For more information, please see the Adobe Security Culture white paper.

Adobe Captivate Prime Compliance

Captivate Prime meets or can be configured to meet compliance requirements for many industry and regulatory standards. Customers maintain control over their documents, data, and workflows and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU. For more information on Adobe privacy policies, please see the Adobe Privacy Center.

Adobe Common Controls Framework

Captivate Prime adheres to the Adobe Common Controls Framework (CCF), 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.

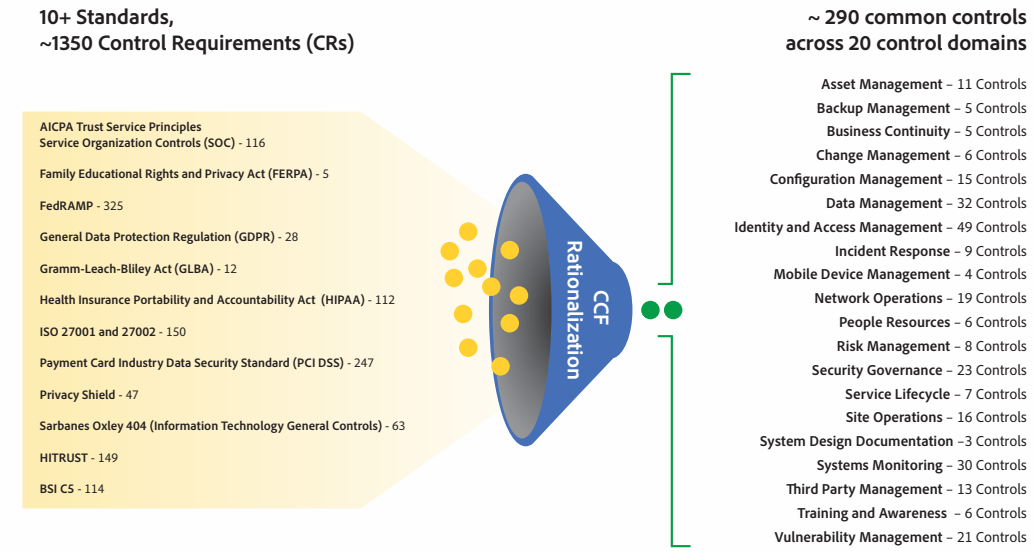


Figure 5: The Adobe Common Controls Framework (CCF)

Adobe Risk & Vulnerability Management

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. Adobe continuously monitors the threat landscape, shares knowledge with security experts around the world, swiftly resolves incidents when they occur, and feeds this information back to its 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 penetration test annually and before every major release. Vulnerability scans are performed monthly while web and database scans are performed quarterly.

The Captivate Prime security team performs a risk assessment of all Captivate Prime components prior to every release and also contracts with an industry-leading third-party vendor to conduct an annual external assessment. To help ensure high-risk vulnerabilities are mitigated prior to each release, the Captivate Prime security team partners with technical operations and development leads. For more information on Adobe penetration testing procedures, see the Adobe Secure Engineering Overview white paper.

Incident Response and Notification

New vulnerabilities and threats evolve each day and Adobe strives to respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Forensic Analysis

For incident investigations, the Captivate Prime team adheres to the Adobe forensic analysis process that includes, as appropriate, complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody record. We offer a data retention feature that helps automate deletion of Captivate Prime agreement data at a customer-specified interval after agreement completion. We also provide an administrative interface for customers to manually delete selected data.

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, Captivate Prime in and out with the receptionist, display a temporary Visitor ID badge, and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus Protection

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

Adobe Employees

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

Employee Access to Customer Data

Adobe maintains segmented development and production environments for 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 Adobe terminates an employee, Adobe People Resources sends a similar email notification torelevant 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, Captivate Prime 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.

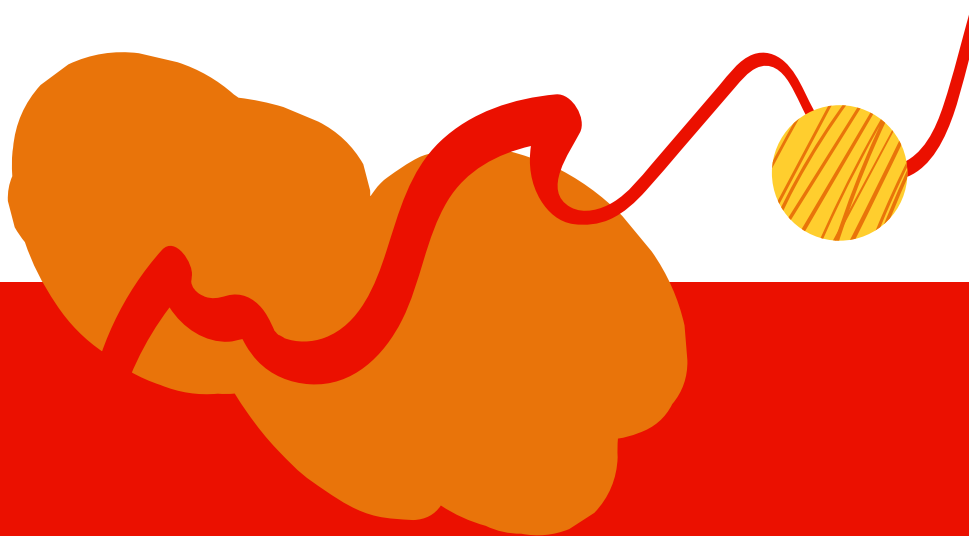
Customer Data Confidentiality

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.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Captivate Prime 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 the Adobe Trust Center.



Adobe

Adobe

Thank you for downloading this Adobe whitepaper! Carahsoft serves as the master GSA and SLSA Schedule Partner for Adobe Creative, Connect, Experience Manager, and Marketing Cloud products and services, supporting an extensive ecosystem of resellers and consulting partners committed to helping government agencies optimize constituent-facing applications while automating back-end processes.

To learn how to take the next step toward acquiring Adobe's solutions, please check out the following resources and information:

For additional resources:
carah.io/AdobeResources

For upcoming events:
carah.io/AdobeEvents

For additional Adobe solutions:
carah.io/AdobeSolutions

For additional CX solutions:
carah.io/CitizenExperience

To set up a meeting:
adobe@carahsoft.com
877-992-3623

To purchase, check out the contract vehicles available for procurement:
carah.io/AdobeContracts