



WHITE PAPER

Adobe Captivate Prime Security Overview

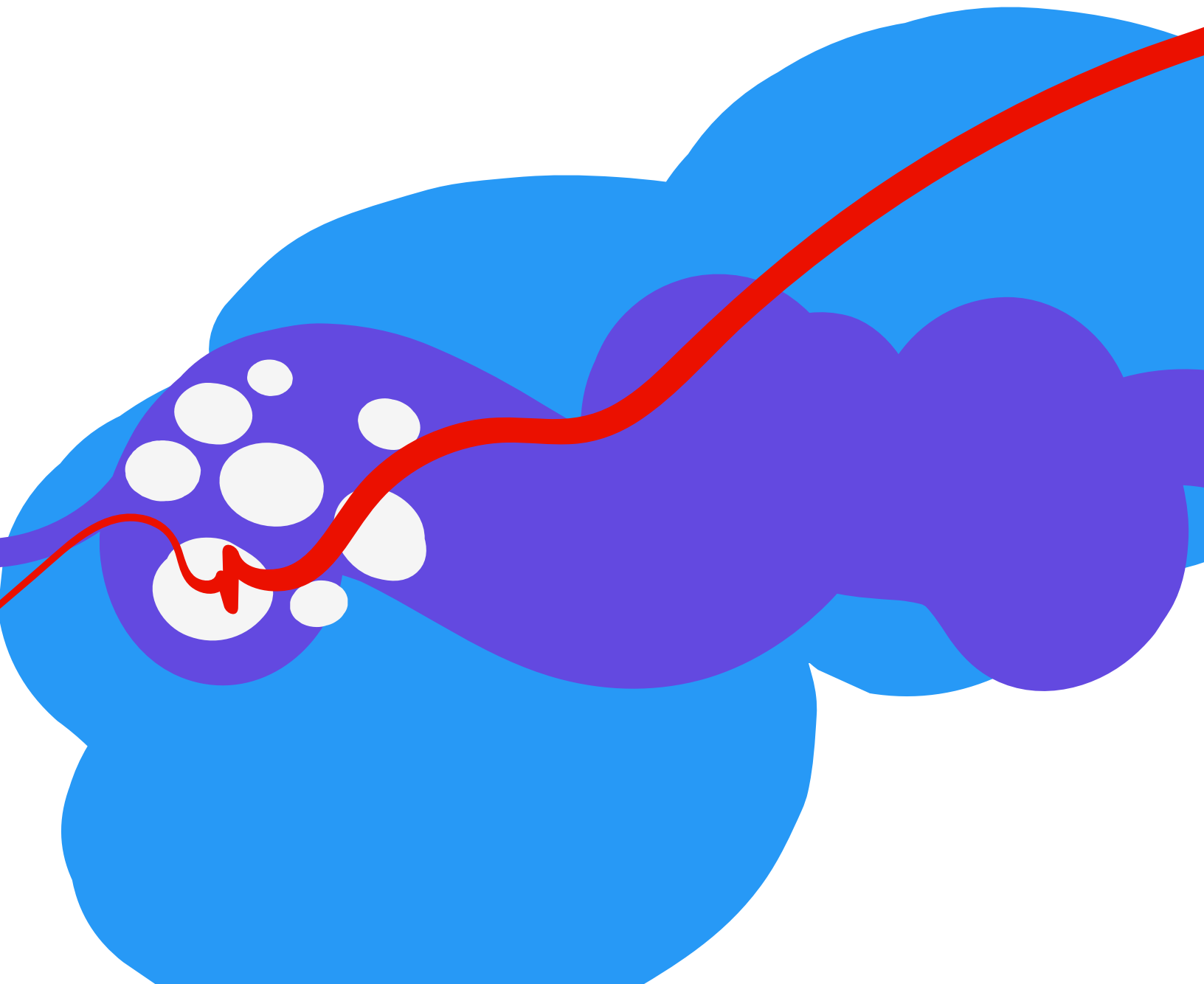
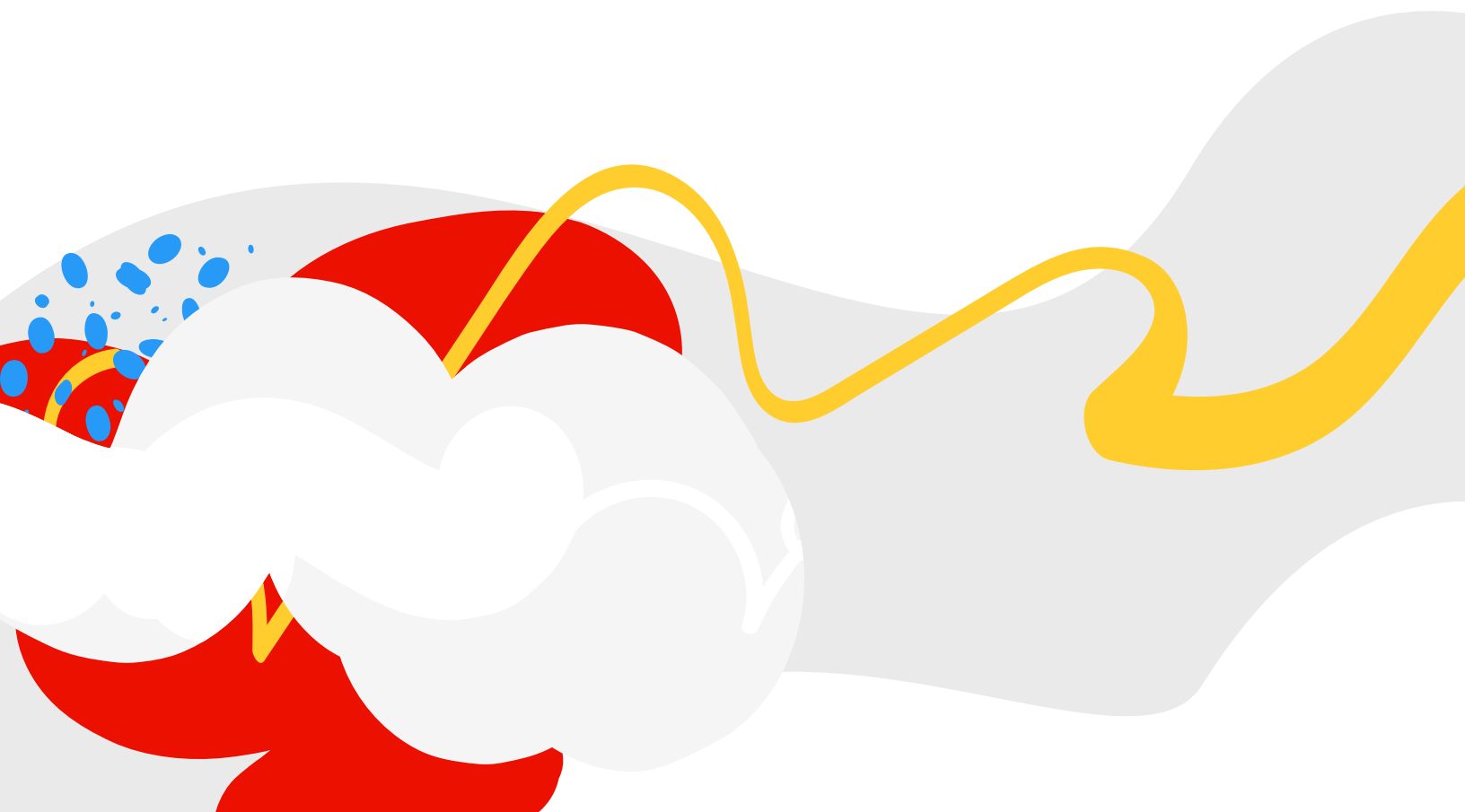


Table of Contents

Adobe Security	1
About Adobe Captivate Prime	1
Adobe Security Program Overview	6
Conclusion	12



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.

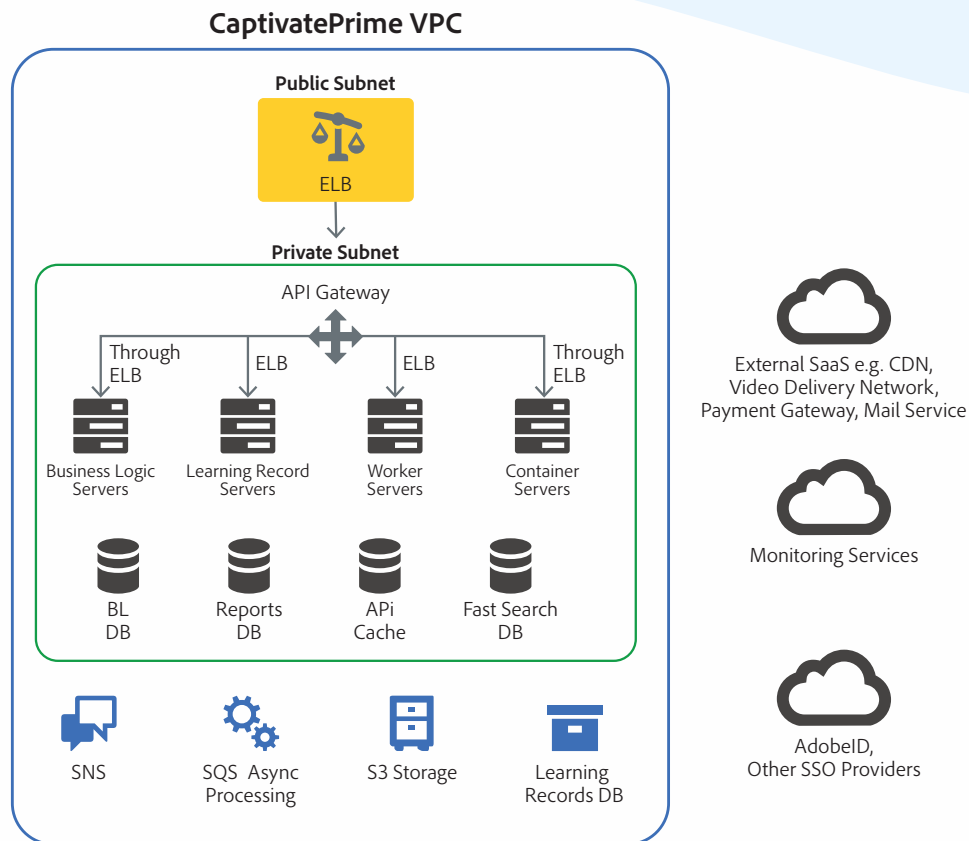


Figure 1: Adobe Captivate Prime application architecture

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.

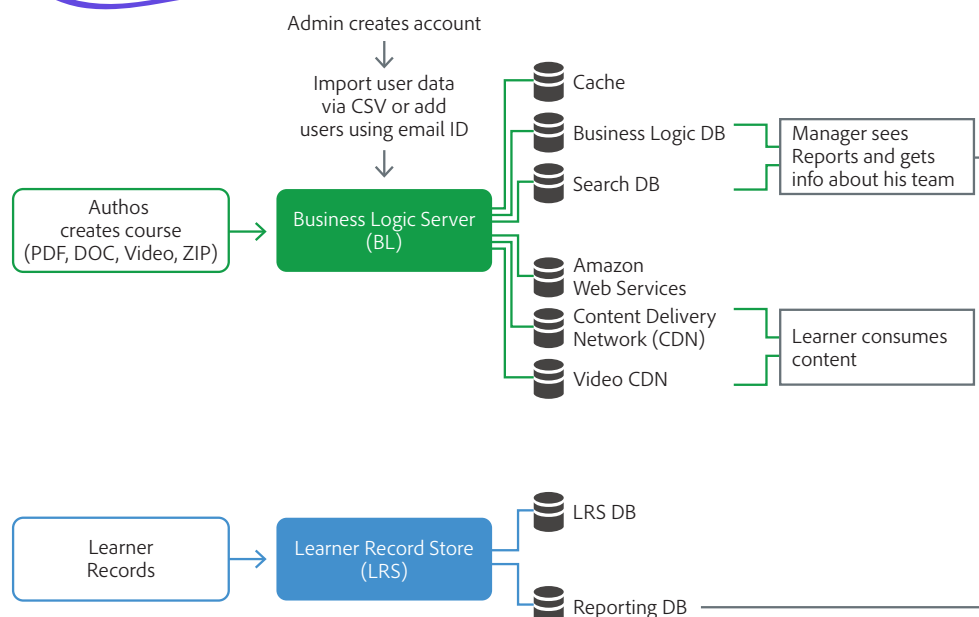


Figure 2: Adobe Captivate data flow

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 Cloud (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).

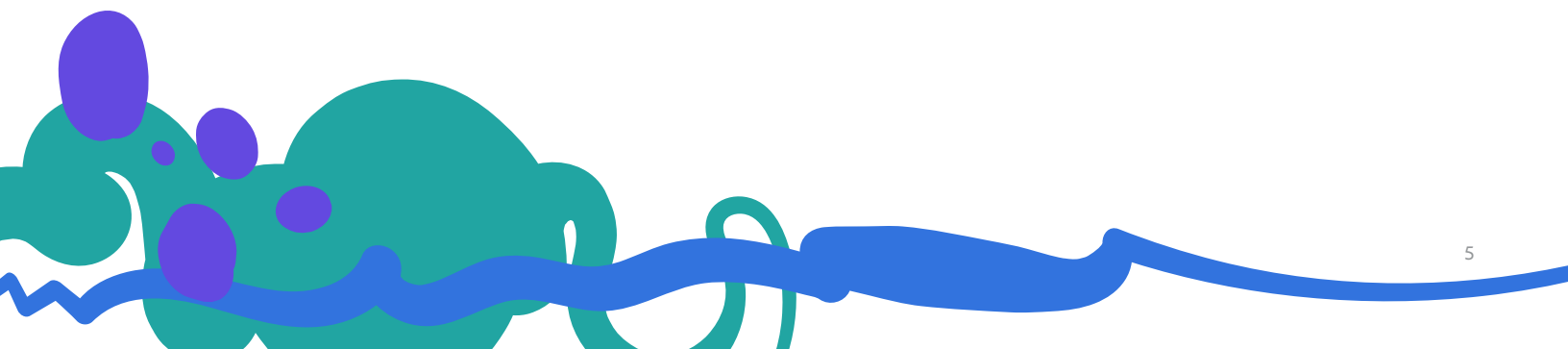
Isolation of Customer Data/Segregation of Customers

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.



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.

More information on Adobe security can be found on the [Adobe Trust Center](#).

