WHITE PAPER

Adobe® Learning Manager Security Overview

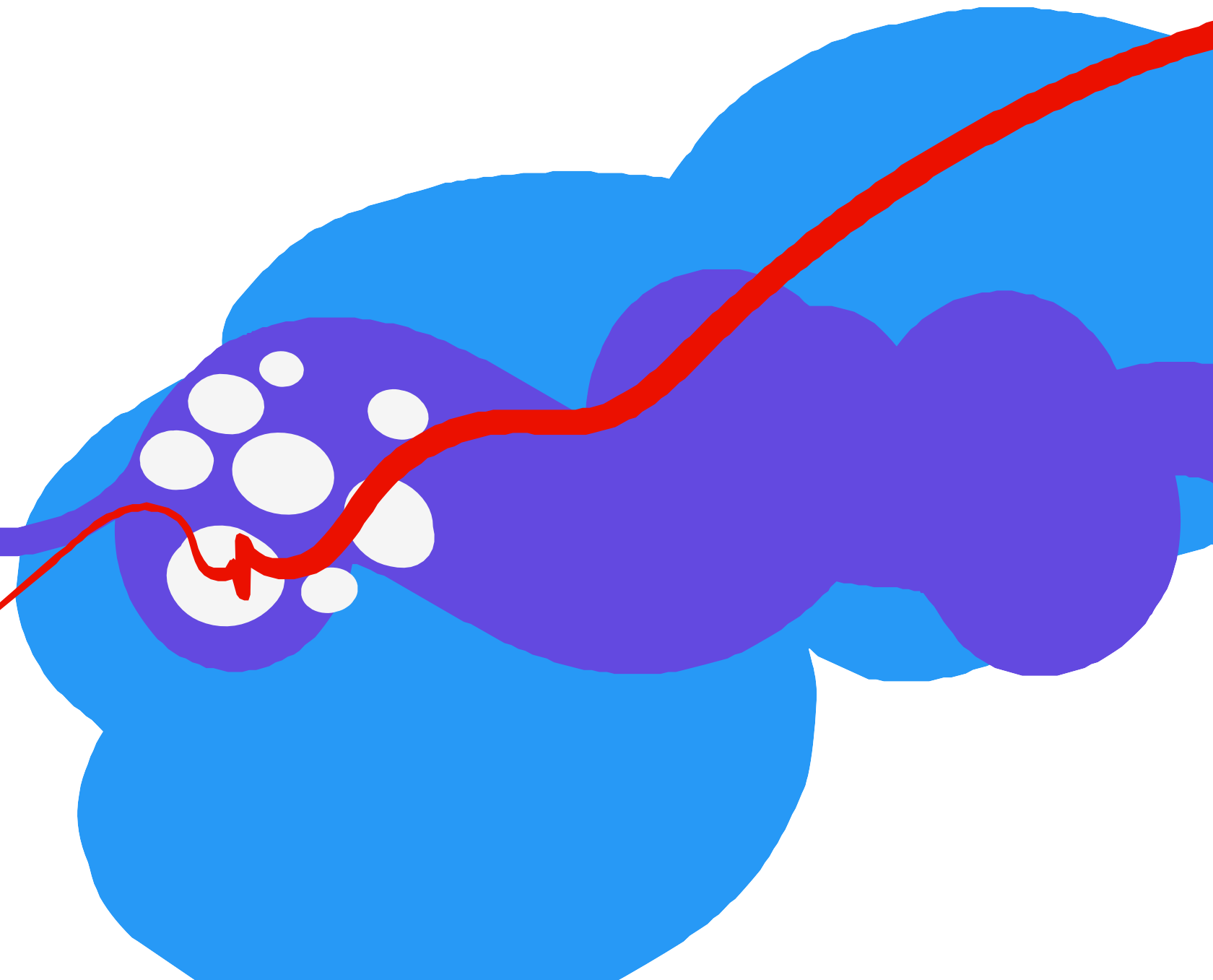
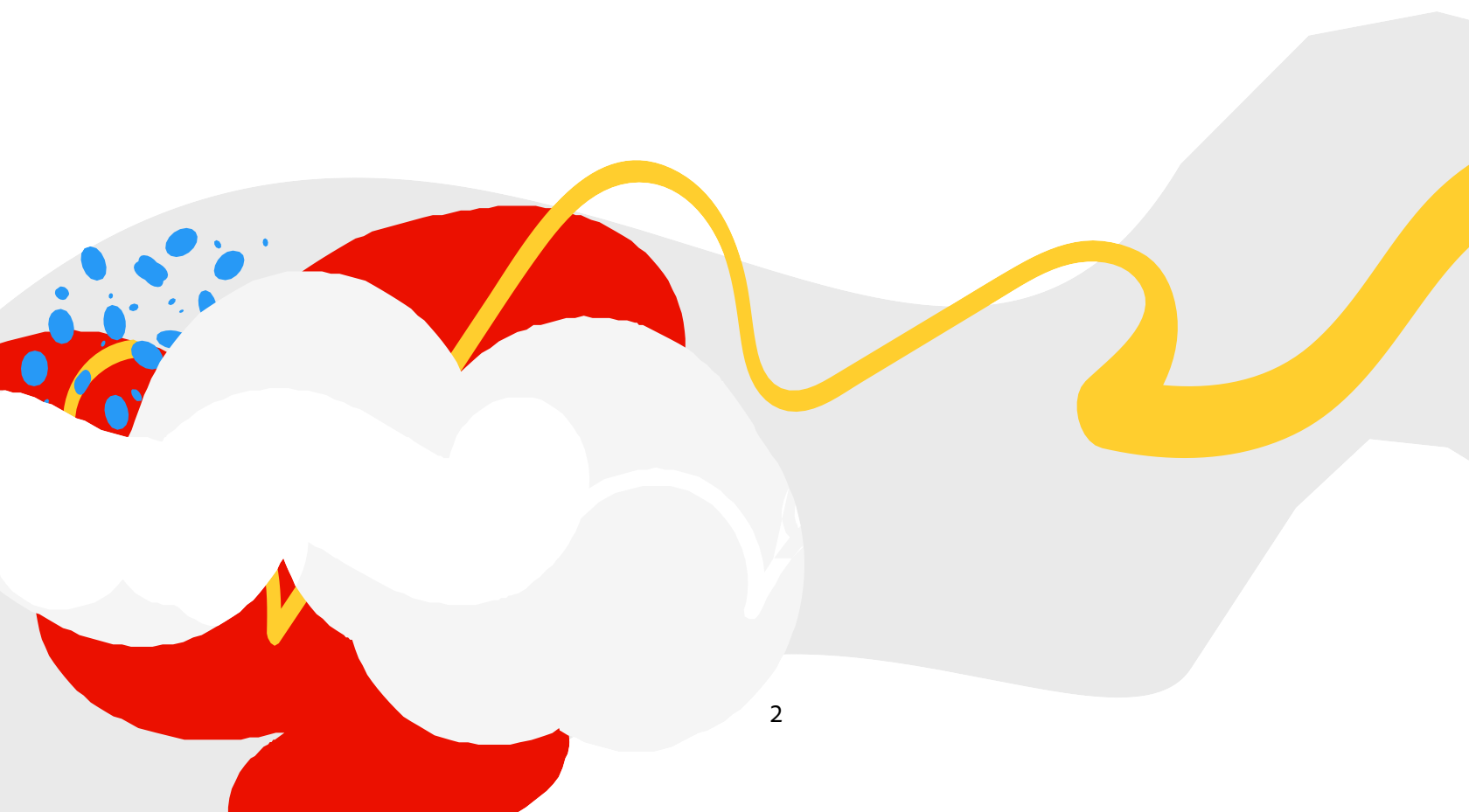


Table of Contents



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® Learning Manager experience and your data.

About Adobe Learning Manager

Adobe Learning Manager 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 Learning Manager 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 Adobe Learning Manager, including PowerPoint, video, PDF, and Word documents, as well as interactive content, such as AICC, TinCan/xAPI, and SCORM packages.

Adobe Learning Manager Application Architecture

Adobe Learning Manager 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 Learning Manager includes the following six (6) components:

- **Adobe Learning Manager Business Logic Server** — Enables the creation and management of users, learning objects (e.g., courses, learning programs, and certifications), enrollments, and user groups.

- **Adobe Learning Manager 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 Learning Manager 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.

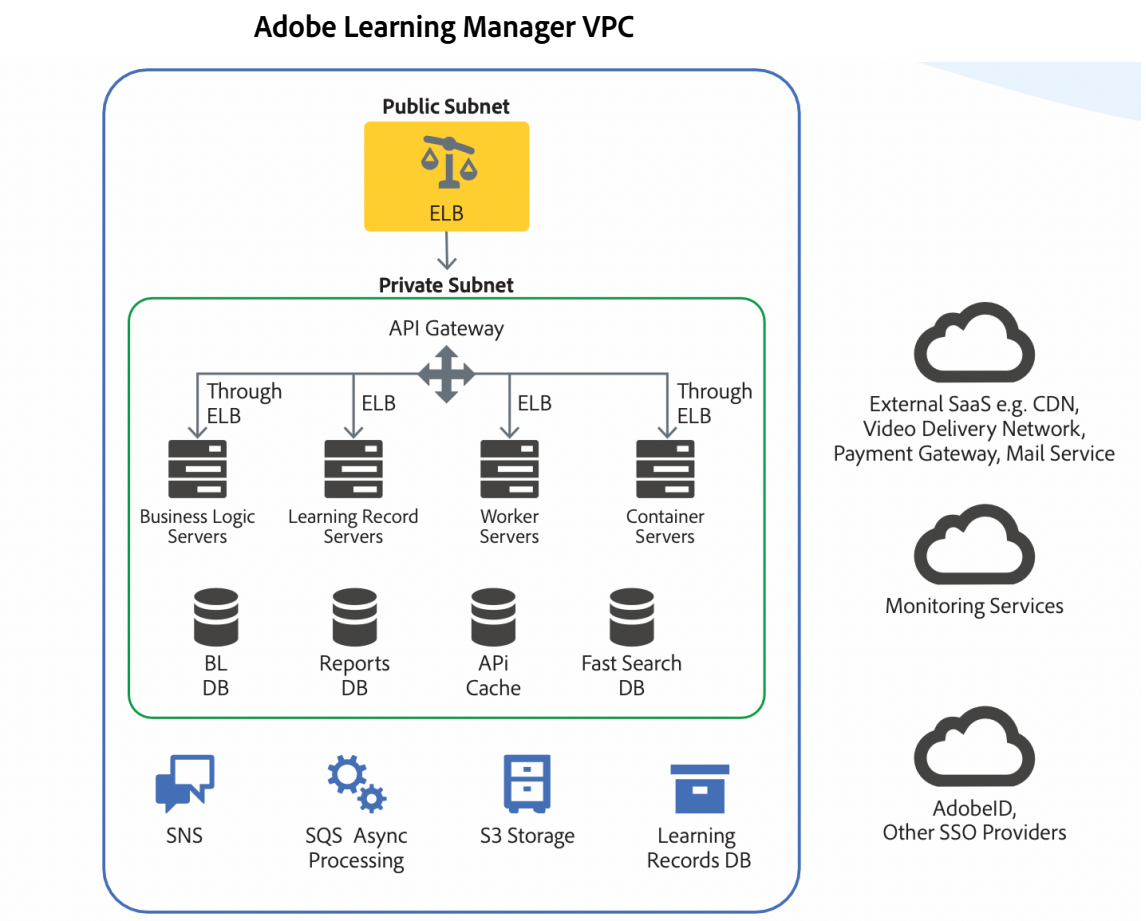


Figure 1: Adobe Learning Manager application architecture

Adobe Learning Manager Roles

Adobe Learning Manager 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 Learning Manager 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 (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 Learning Manager 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 Experience Manager Data Flow

The diagram below illustrates how data flows in the Adobe Learning Manager 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.

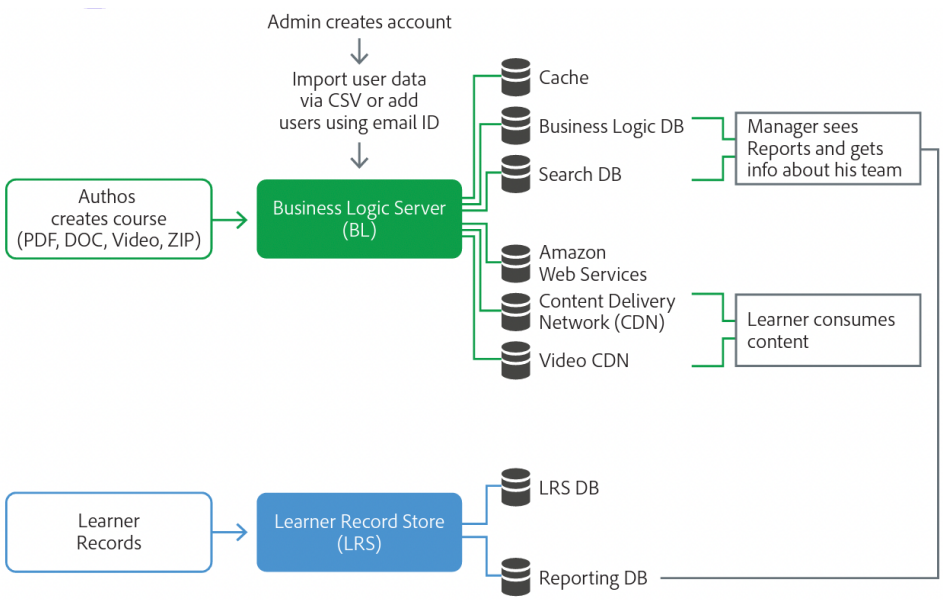


Figure 2: Adobe Learning Manager data flow

All client connections to Adobe Learning Manager 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 Learning Manager Security Architecture

Adobe Learning Manager 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 Learning Manager 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 Learning Manager account does not have permission to access data of any other Adobe Learning Manager account.

Administrative Security Controls

Adobe Learning Manager 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 Learning Manager 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 Learning Manager 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 Learning Manager 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 Learning Manager integrates with most any SAML 2.0-compliant identity provider.

- **Adobe Learning Manager ID** enables external users (temporary users or partners) to create their Adobe Learning Manager account by providing their email and setting a password. These credentials are stored in Adobe Learning Manager 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 Learning Manager authentication module.

All protections implemented via the authentication and authorization layer help ensure content (e.g., courses, files, images, etc.) uploaded into Adobe Learning Manager can only be seen by users logged into an Adobe Learning Manager 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).

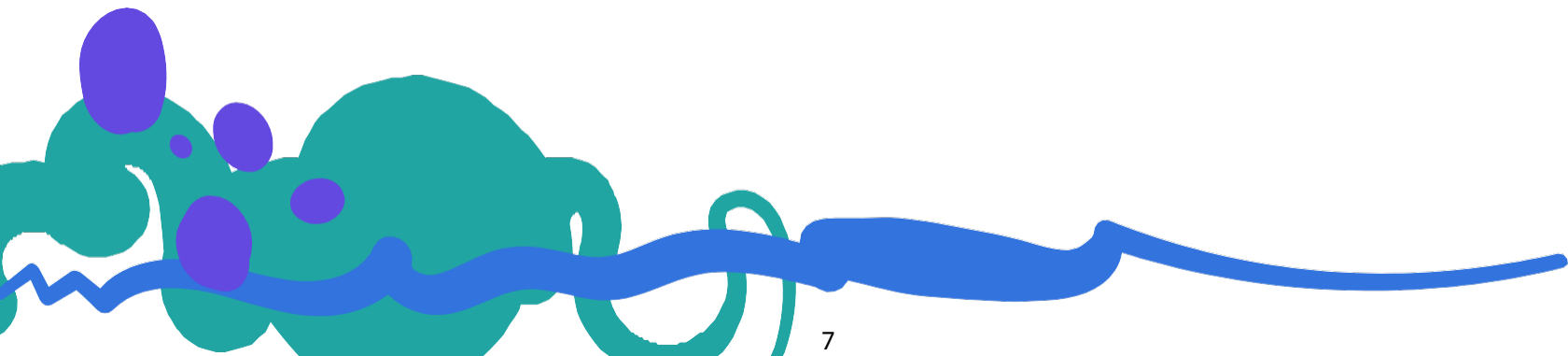
Isolation of Customer Data/Segregation of Customers

Adobe provisions a separate Adobe Learning Manager 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 Learning Manager 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 Learning Manager account does not have permission to access any other Adobe Learning Manager account.

Customer data resides in the same data center as the customer's Adobe Learning Manager VPC, either Virginia (US), Frankfurt (Germany), or Mumbai (India). Replication of Amazon S3 data objects occur in the regional cluster in which the data is stored.



Adobe Security Program Overview

The integrated security program at Adobe is composed of five (5) centers of excellence, each of which constantly iterates and advances the ways we detect and prevent risk by leveraging new and emerging technologies, such as automation, AI, and machine learning.

Figure 3: Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

- **Application Security** — Focuses on the security of our product code, conducts threat research, and implements bug bounty.
- **Operational Security** — Helps monitor and secure our systems, networks, and production cloud systems.
- **Enterprise Security** — Concentrates on secure access to and authentication for the Adobe corporate environment.
- **Compliance** — Oversees our security governance model, audit and compliance programs, and risk analysis; and
- **Incident Response** — Includes our 24x7 security operations center and threat responders.

Illustrative of our commitment to the security of our products and services, the centers of excellence report to the office of the Chief Security Officer (CSO), who coordinates all current security efforts and develops the vision for the future evolution of security at Adobe.

The Adobe Security Organization

Based on a platform of transparent, accountable, and informed decision-making, the Adobe security organization brings together the full range of security services under a single governance model. At a senior level, the CSO closely collaborates with the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) to help ensure alignment on security strategy and operations.

In addition to the centers of excellence described above, Adobe embeds team members from legal, privacy, marketing, and PR in the security organization to help drive transparency and accountability in all security-related decisions.

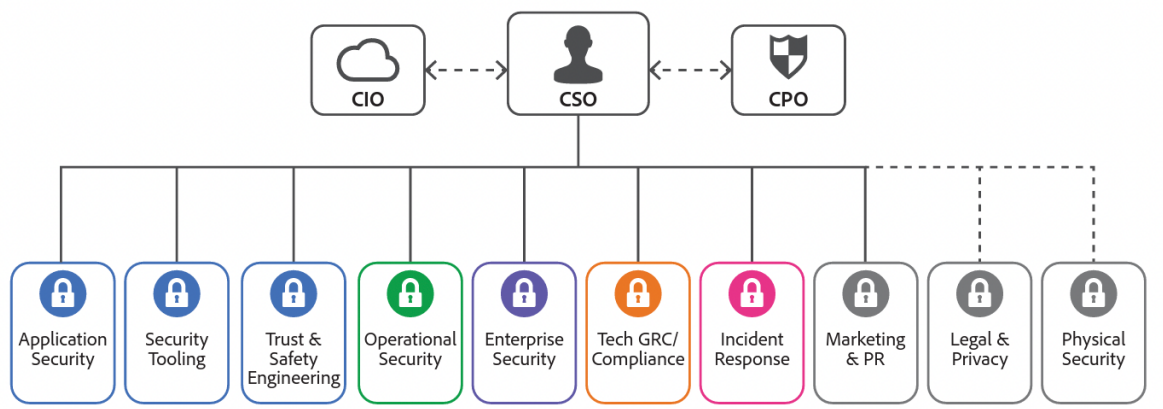


Figure 4: The Adobe Security Organization

As part of our company-wide culture of security, Adobe requires that every employee completes our security awareness and education training, which requires completion and re-certification on an annual basis, helping ensure that every employee contributes to protecting Adobe corporate assets as well as customer and employee data. On hire, our technical employees, including engineering and technical operations teams, are auto-enrolled in an in-depth 'martial arts'-styled training program, which is tailored to their specific roles. For more information on our culture of security and our training programs, please see the Adobe Security Culture white paper.

The Adobe Secure Product Lifecycle

Integrated into several stages of the product lifecycle—from design and development to quality assurance, testing, and deployment— the Adobe Secure Product Lifecycle (SPLC) is the foundation of all security at Adobe. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC defines clear, repeatable processes to help our development teams build security into our products and services and continuously evolves to incorporate the latest industry best practices.

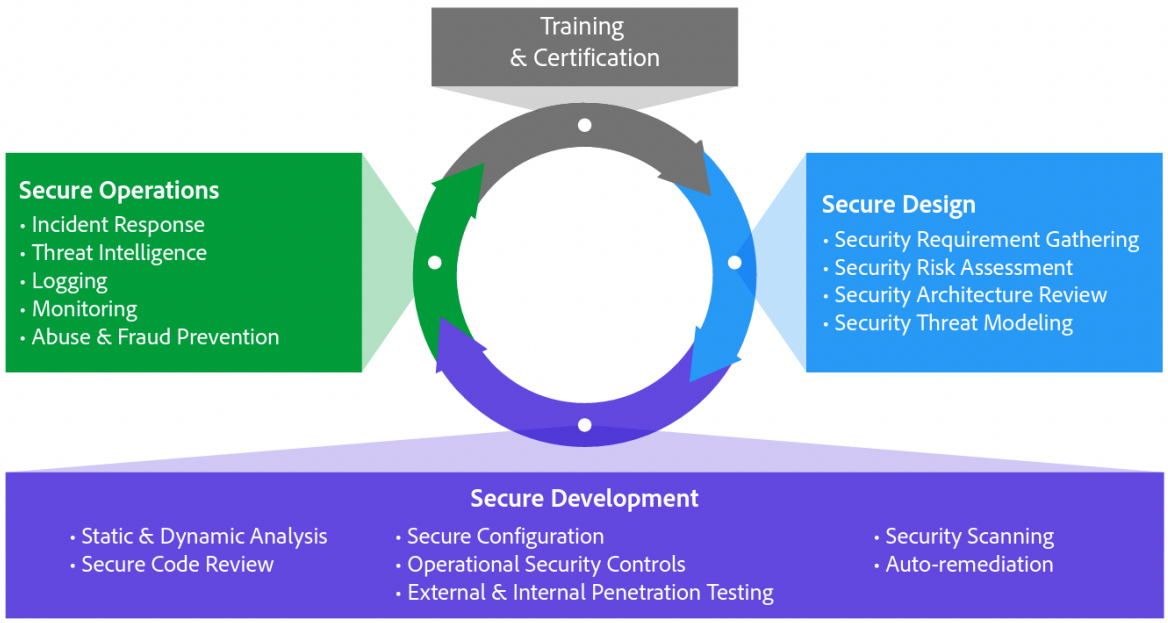


Figure 5: The Adobe Secure Product Lifecycle

Adobe maintains a published Secure Product Lifecycle Standard that is available for review upon request. More information about the components of the Adobe SPLC can be found in the Adobe Application Security Overview.

Adobe Application Security

At Adobe, building applications in a "secure by default" manner begins with the Adobe Application Security Stack. Combining clear, repeatable processes based on established research and experience with automation that helps ensure consistent application of security controls, the Adobe Application Security Stack helps improve developer efficiency and minimize the risk of security mistakes. Using tested and pre-approved secure coding blocks that eliminate the need to code commonly used patterns and blocks from scratch, developers can focus on their area of expertise while knowing their code is secure. Together with testing, specialized tooling, and monitoring, the Adobe Application Security Stack helps software developers to create secure code by default.

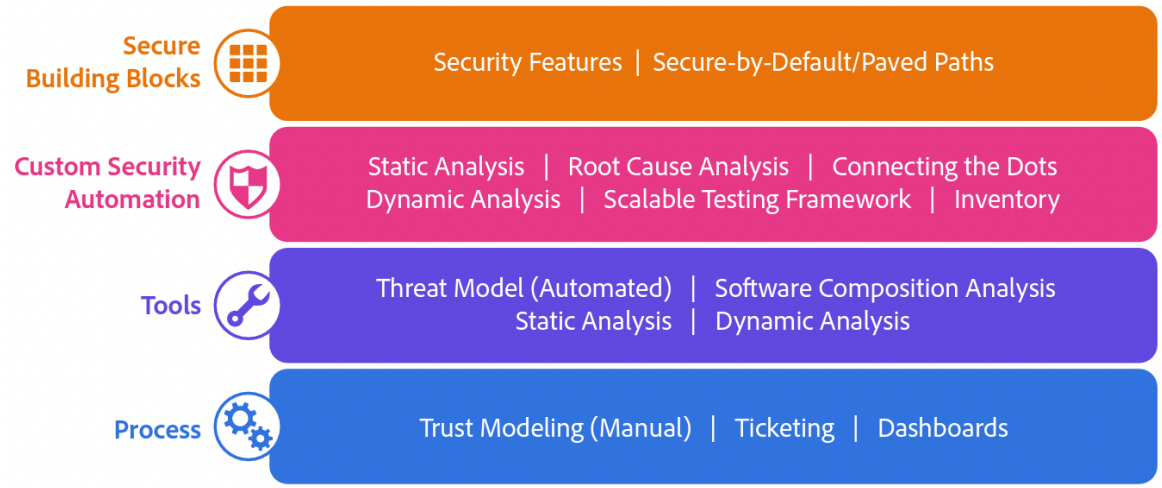


Figure 6: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of Amazon Web Services (AWS) and Microsoft Azure public cloud infrastructure. These standards are available for view upon request.
For more information on Adobe application security, please see the Adobe Application Security Overview.

Adobe Operational Security

To help ensure that all Adobe products and services are designed from inception with security best practices in mind, the operational security team created the Adobe Operational Security Stack (OSS). The OSS is a consolidated set of tools that help product developers and engineers improve their security posture and reduce risk to both Adobe and our customers while also helping drive Adobe-wide adherence to compliance, privacy, and other governance frameworks.

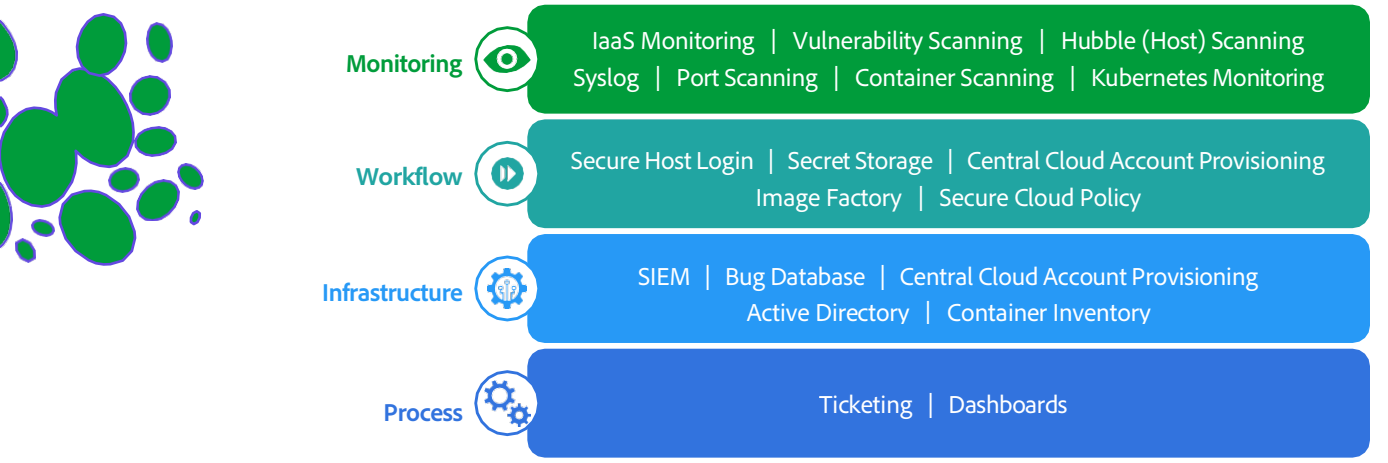


Figure 7: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. For a detailed description of the Adobe OSS and the specific tools used throughout Adobe, please see the Adobe Operational Security Overview.

Adobe Enterprise Security

In addition to securing our products and services as well as our cloud hosting operations, Adobe also employs a variety of internal security controls to help ensure the security of our internal networks and systems, physical corporate locations, employees, and our customers' data.

For more information on our enterprise security controls and standards we have developed for these controls, please see the Adobe Enterprise Security Overview.

Adobe Compliance

All Adobe products and services adhere 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.
As much as possible, Adobe leverages leading-edge automation processes to alert teams to possible non-compliance situations and help ensure swift mitigation and realignment.

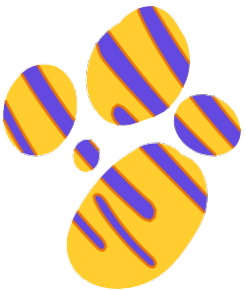
Adobe products and services either meet applicable legal standards or can be used in a way that enables customers to help meet their legal obligations related to the use of service providers. Customers maintain control over their documents, data, and workflows, and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU.

Adobe also maintains a compliance training and related standards that are available for review upon request. For more information on the Adobe CCF and key certifications, please see the Adobe Compliance, Certifications, and Standards List.

Incident Response

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution processes are 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.

We also maintain internal standards for incident response and vulnerability management that are available for view upon request. For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.



Business Continuity and Disaster Recovery

The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified BCDR Program enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information on the Adobe BCDR Program can be found here.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Learning Manager 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.

Adobe