Adobe Experience Cloud

WHITEPAPER

Adobe Experience Manager Assets Essentials Security Overview

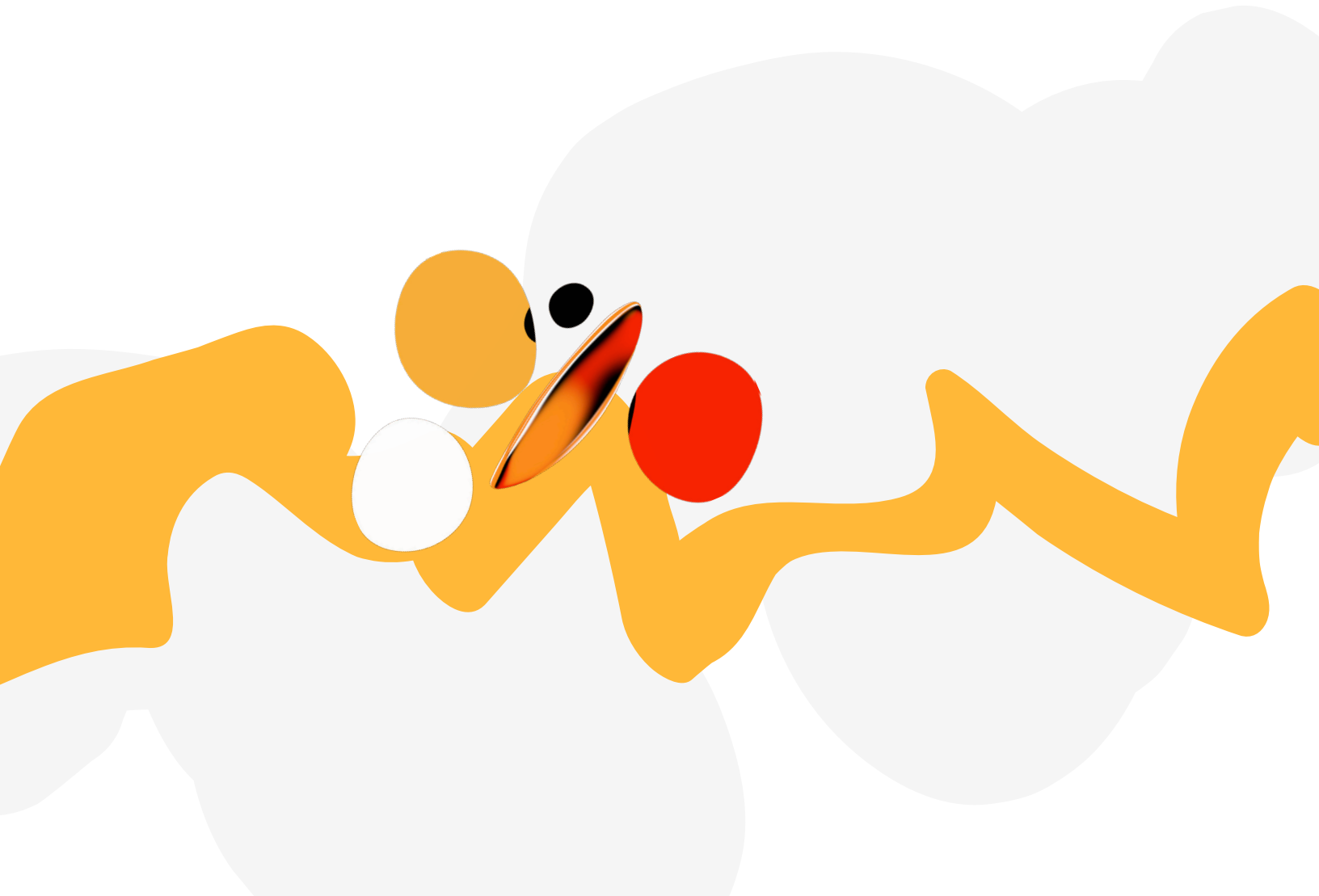

Table of Contents

Adobe Security

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

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of your Adobe Experience Manager Assets Essentials experience and your data.

About Adobe Experience Manager Assets Essentials

Adobe Experience Manager Assets Essentials is a lightweight, cloud-native digital asset management solution, providing unified asset management and collaboration with a streamlined, modern user interface. Seamless integrations with other Adobe solutions improve the content creation process from concept to design to delivery.

Built on the Adobe Experience Manager as a Cloud Service infrastructure and services, Assets Essentials shares its fundamental security approach, procedures, and architecture, which are described in the Adobe Experience Manager as a Cloud Service Security Overview. Focusing on simplifying the end-user and administrator experiences, Assets Essentials leverages a subset of AEM capabilities. This overview outlines the security controls specific to Assets Essentials.

Assets Essentials Solution Architecture

Assets Essentials includes three (3) primary components with which users and administrators interact:

- **Assets Essentials User Interface (UI)** — Provides full access to the solution's capabilities for end-users
- **Assets Essentials Integration UI components** — Give end-users access to Assets Essentials services from within other Adobe solutions
- **Adobe Admin Console** — Enables administrators to manage users, groups, and entitlements

Additional components that help comprise the architecture of the solution include:

- **Backend Service and APIs** — Exposes internal solution APIs and related content management services through a specially provisioned Adobe Experience Manager as a Cloud Service environment. The Assets Essentials UI and Integration UI components connect to these APIs.
- **Cloud Manager** — Provides administrators with a view of the backend service status and provides additional capabilities like the ability to download access logs.

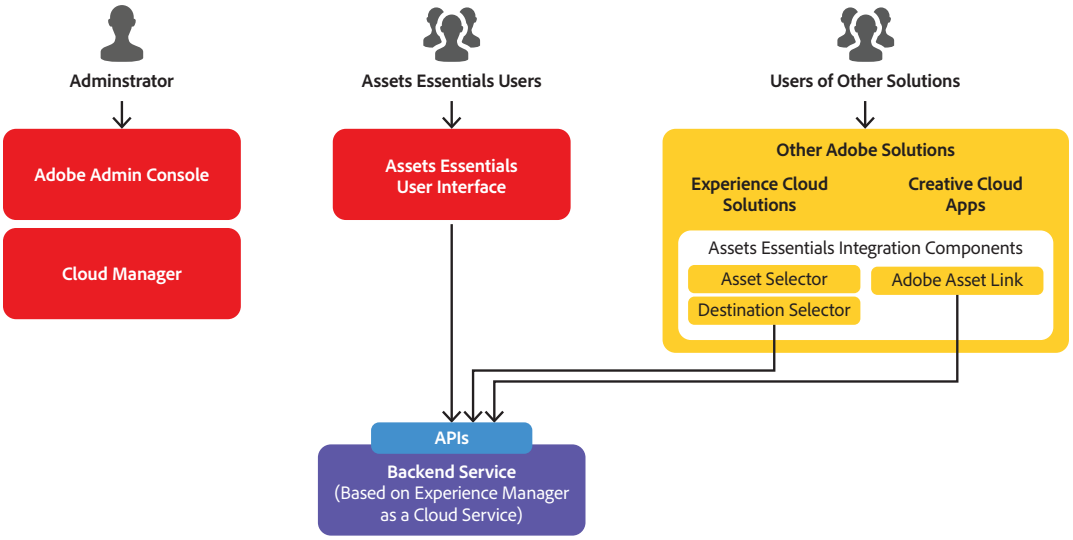

Figure 1: Adobe Experience Manger Assets Essentials Solution Architecture

Assets Essentials Data Flow and Security Architecture

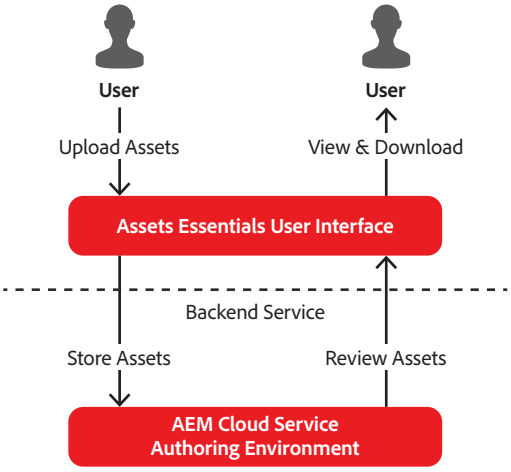

Figure 2: Adobe Experience Manger Assets Essentials Data Flow

Data Encryption

Data transmitted between Assets Essentials servers and client machines are secured in transit using HTTPS with TLS 1.2 or higher.

User Authentication

Administrators create and manage user access to Assets Essentials in the Adobe Admin Console. More detailed information about Adobe's identity management services is available in the Adobe Identity Management Services Security Overview.

Roles and Permissions

Assets Essentials uses the Adobe Admin Console to manage users and user groups. Within the Admin Console, the Assets Essentials environment is represented by the corresponding product instance.

Administrators create or import end-user accounts in the Admin Console and assign each user to product profiles, giving them access to the associated Assets Essentials instance.

The Admin Console also enables admins to manage Assets Essentials environment access as a regular user (Assets Essentials Users and Assets Essentials Consumer Users) or as an AEM administrator (Assets Essentials Administrators) using product profiles.

Assigning users to user groups in Admin Console allows for configuring group-level permissions to folders in Assets Essentials. Users assigned to Assets Essentials Administrator profile can use Assets Essentials permissions management features to set up access level to folders and assets that they contain for user groups and users, with granular permissions with read, read/write, or deny permissions for the application's users.

Assets Essentials Hosting Locations

The Assets Essentials solution is hosted in the data centers of leading public cloud providers in the United States (Oregon & Virginia), Canada, EMEA (Germany, Switzerland, The Netherlands, and the U.K.), and APAC (Australia, India, Japan, and Singapore).

Figure 3: Assets Essentials Hosting Locations

Segregation of Customer Data

User-generated content is placed into separate databases. In some cases, more than one customer may share a cloud cluster, but the content is segmented into separate databases. The only access to these servers and databases is via secure access by the Assets Essentials solution.

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 4: 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.

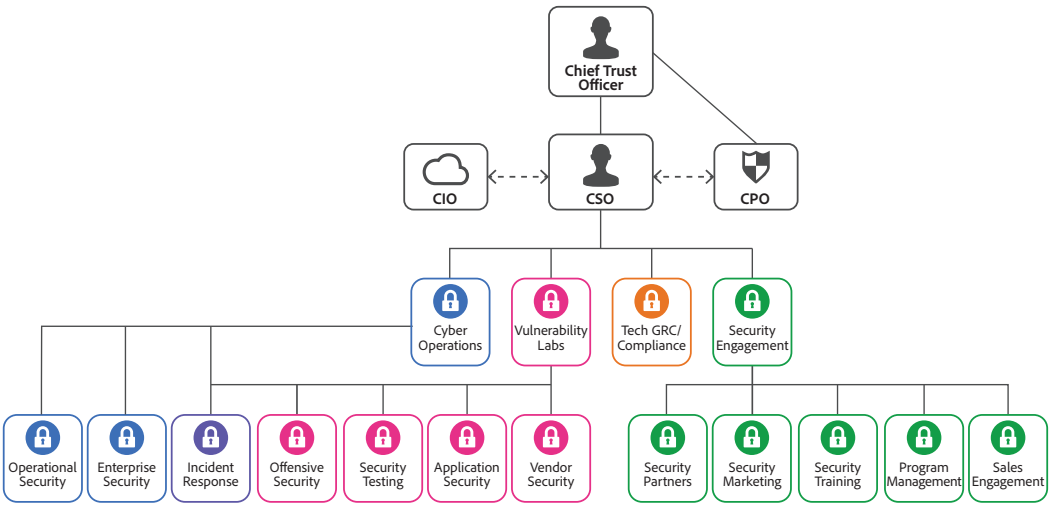

Figure 5: The Adobe Security Organization

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.

Adobe's culture of security and training programs are outlined in more detail in 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.

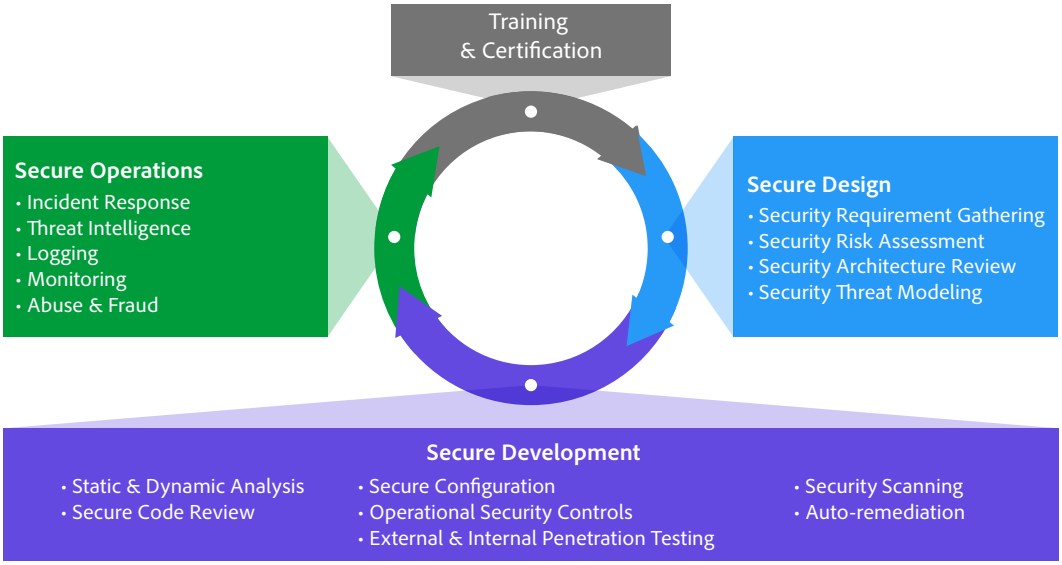

Figure 6: The Adobe Secure Product Lifecycle

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.

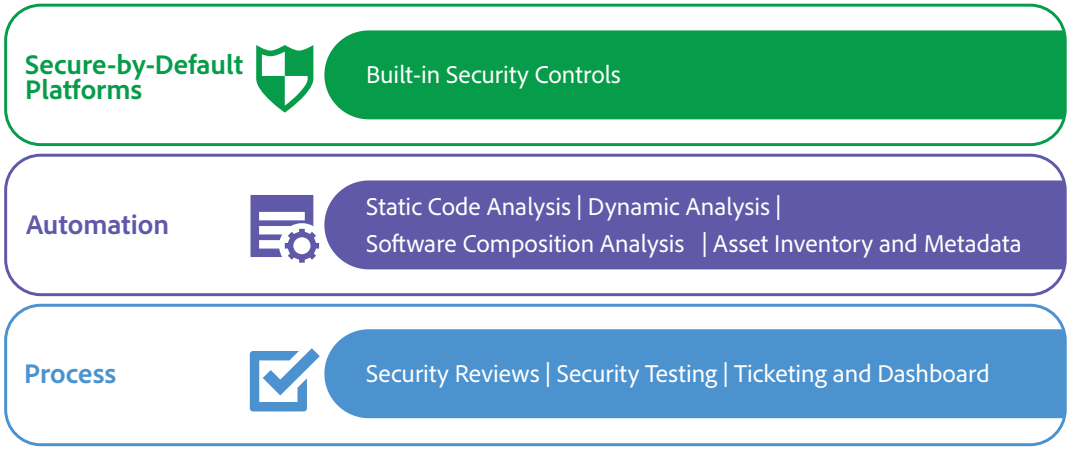

Figure 7: The Adobe Application Security Stack

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. The Adobe Application Security Overview contains more detailed information about Adobe's application security practices and processes.

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.

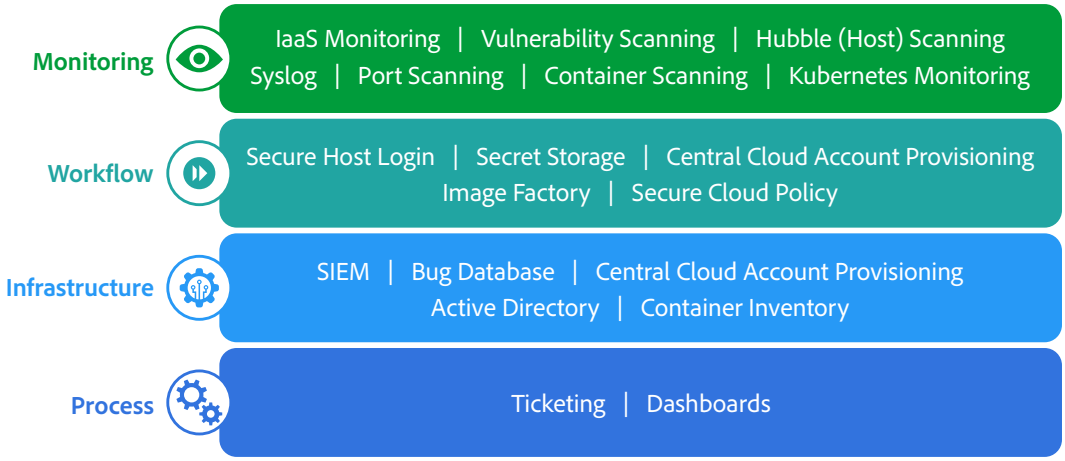

Figure 8: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. A detailed description of the Adobe OSS and the specific tools used throughout Adobe can be found in 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.

More information on our enterprise security controls and standards we have developed for these controls can be found in 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. More information on the Adobe CCF and key certifications can be found in the Adobe Compliance Certifications, Standards, and Regulations 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.

More details about Adobe's incident response and notification process are documented in the Adobe Incident Response Program 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 in the Adobe Business Continuity and Disaster Recovery Program Overview.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Experience Manager Assets Essentials 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 on Adobe security, please go to the Adobe Trust Center.

Adobe

11/22