Adobe Experience Cloud

WHITEPAPER

Adobe Journey Optimizer Security Overview

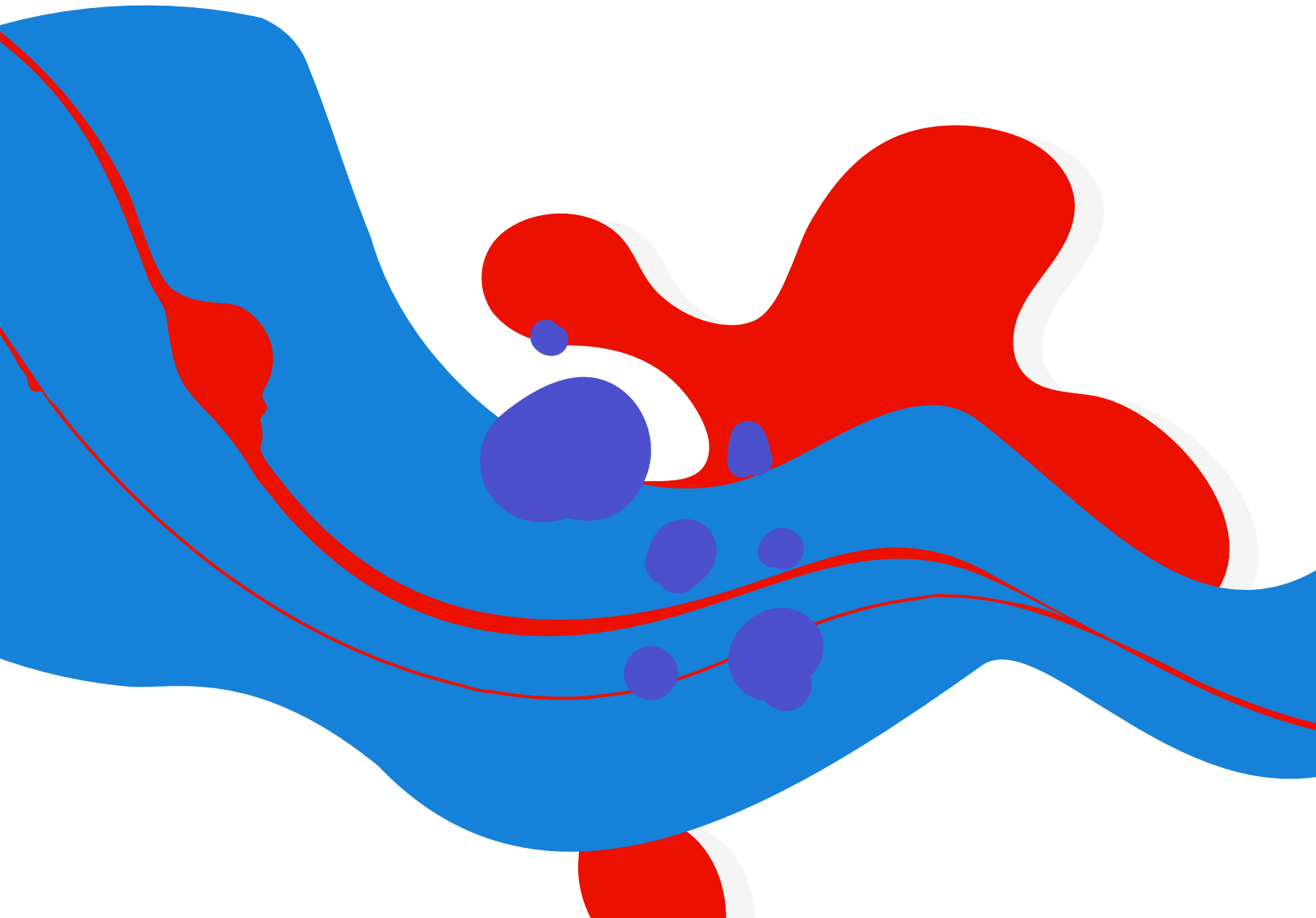
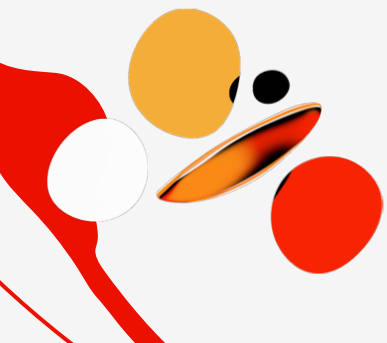


Table of Contents



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. Our cross-functional teams strictly follow these practices 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 and 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 secure Adobe Journey Optimizer and associated data.

About Adobe Journey Optimizer

Adobe Journey Optimizer (AJO) enables marketers to deliver personalized, contextual experiences to their customers. The customer journey is the entire process of a customer's interactions with a brand, from the first moment of contact until the customer leaves. Built natively on the Adobe Experience Platform (AEP), Adobe Journey Optimizer combines a unified, real-time customer profile; an API-first open framework; centralized offer decisioning; and artificial intelligence (AI) and machine learning (ML) for personalization and optimization. With Journey Optimizer, marketers can build real-time orchestration use cases that leverage contextual data stored in events or data sources.

Adobe Journey Optimizer Solution Architecture

The Adobe Journey Optimizer solution is comprised of six (6) components*:

- **Adobe Journey Runtime** — Progresses the customer profile through different steps of the customer journey. The progression of the profile can be triggered based on an external or time-based event.
- **Message Authoring** — Enables marketers to create messages for different channels optionally populating them with assets stored in AEM Assets. It also allows marketers to preview the messages for specific test profiles.
- **Message Runtime** — Pushes personalized messages to the customer via email, push, or a variety of other inbound and outbound communication channels.

* Message Authoring, Message Runtime, and Outbound Services are not available in AJO Starter.

- **Outbound Services** — Help deliver messages to the end-customer using multiple outbound channels.
- **Offers Service** — Enables marketers to create multiple offers for targeted profiles.
- **Reporting** — Provides robust reporting capabilities of customer journey measurements and engagement.

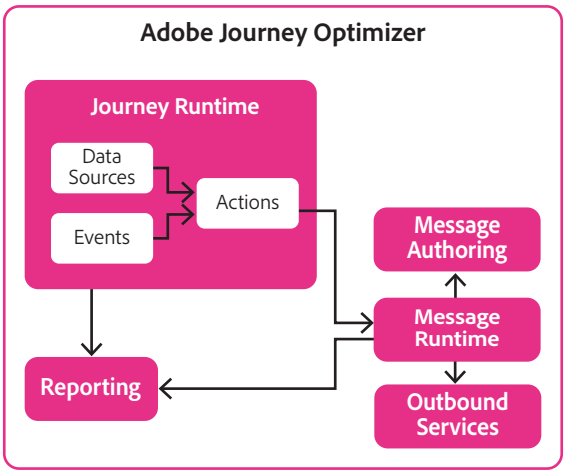


Figure 1: Adobe Journey Optimizer Solution Architecture

Other Integrations:

- Adobe Journey Optimizer integrates seamlessly with Adobe Experience Manager Assets, a collaborative workspace to store, discover, and distribute digital assets that marketers can use in authoring messages.
- Third-party APIs enable customers to easily integrate other business applications with Adobe Journey Optimizer to trigger custom actions.

Adobe Journey Optimizer Security Architecture and Data Flow

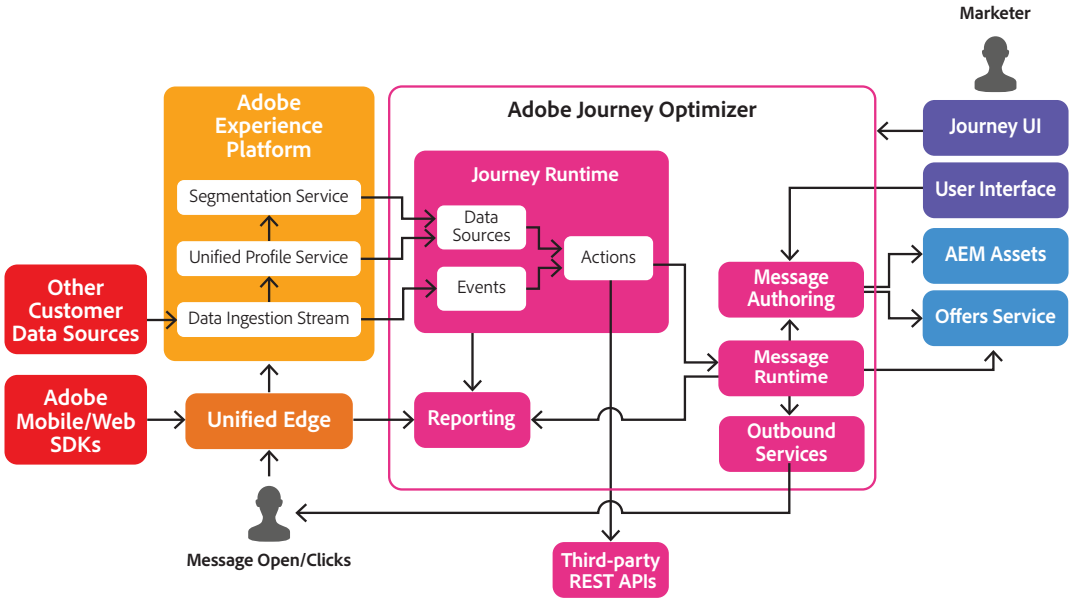


Figure 2: Adobe Journey Optimizer Data Flow

The following narrative describes how data flows throughout the Adobe Journey Optimizer solution, from message creation by the marketer to customer receipt of the message and click-through to receive the offer.

Note: Before creating content within Adobe Journey Optimizer, marketers must ingest the customer profiles to which they wish to send their message/s into Journey Optimizer from the Adobe Experience Platform (AEP) Unified Profile Service and upload any images or other content they wish to include in these messages into Adobe Experience Manager (AEM) Assets.

Step 1: The marketer logs into the Journey Optimizer UI using their username and password and authors a custom message along with the associated images and/or additional content that are stored in AEM Assets.

Step 2: Also within the Journey Optimizer UI, the marketer chooses a customer profile or set of profiles to target with the message and schedules a journey for the customer.

Step 3: The Journey Runtime sends the message to either the Message Service to trigger message execution to the customer or to a third-party application that has been integrated using a third-party REST API to trigger a custom action. Messages are sent to the customer via email, push, or other communication channels.

Step 4: Upon receipt of the message in email or in a text message, the customer clicks to open the message. If the customer clicks on any link in the message, they will be redirected to the website associated with the link. This action will also be captured for reporting purposes.

Step 5: AJO Reporting captures and logs all interactions automatically. The marketer can access logs using either the Journey Optimizer UI or the Adobe Experience Platform UI. If the marketer chooses to create custom reports, they can do so in the AEP UI or by integrating a third-party reporting solution using a REST API.

Data Encryption

All communications within Adobe Journey Optimizer use HTTPS TLS v1.2 or greater to protect data in transit.

User Interactions and Admin Source Configurations

Administrators and users with appropriate access permissions can authenticate to the Journey Optimizer UI and configure a variety of options. Users can also create content and trigger message execution in the Journey Optimizer UI.

IP Allowlists

IP allowlisting is not required for outbound actions because Adobe Journey Optimizer services run on servers with dynamically changing IP addresses. Additionally, third-party actions from Adobe Journey Optimizer are secured using an API key or token-based authentication, in accordance with best security practices.

About Adobe Experience Platform

Because Adobe Journey Optimizer is built natively on the Adobe Experience Platform, it inherits many attributes from AEP, including user authentication, data segregation and access control, and data governance. For more information, please see the Adobe Experience Platform Security Overview and the Adobe Experience Platform Data Governance White Paper.

Adobe Journey Optimizer Hosting Locations and Security

Adobe Journey Optimizer is hosted in enterprise-class data centers from public cloud service providers in U.S. East (Virginia), Canada (Toronto), Amsterdam (NL), and Sydney (AU). Upon provisioning, customers can designate the regional data center(s) where the data ingested into Adobe Journey Optimizer will be sent for storage.

Figure 3: Adobe Journey Optimizer Hosting Locations

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.

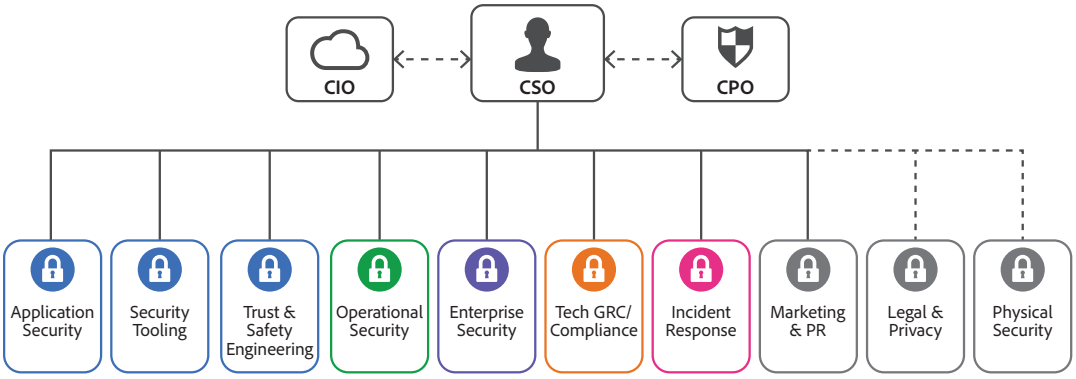


Figure 5: The Adobe Security Organization

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. 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.

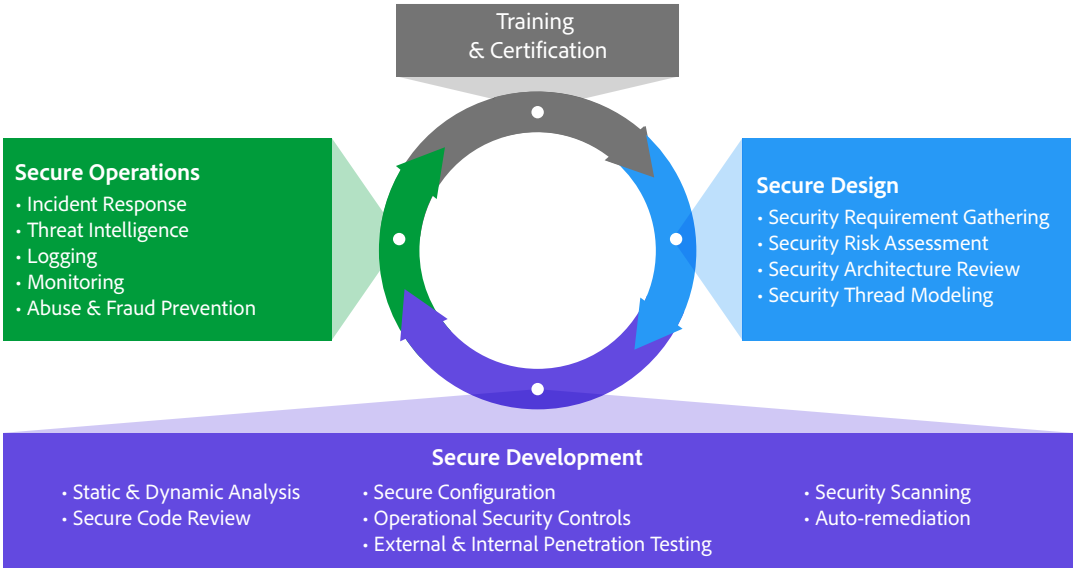


Figure 6: The Adobe Secure Product Lifecycle

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.

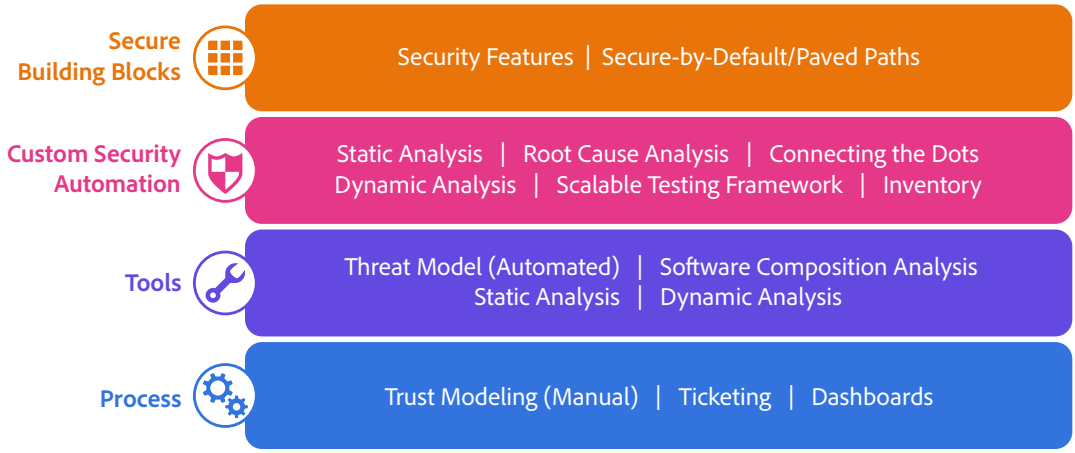


Figure 7: The Adobe Application Security Stack

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. 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.

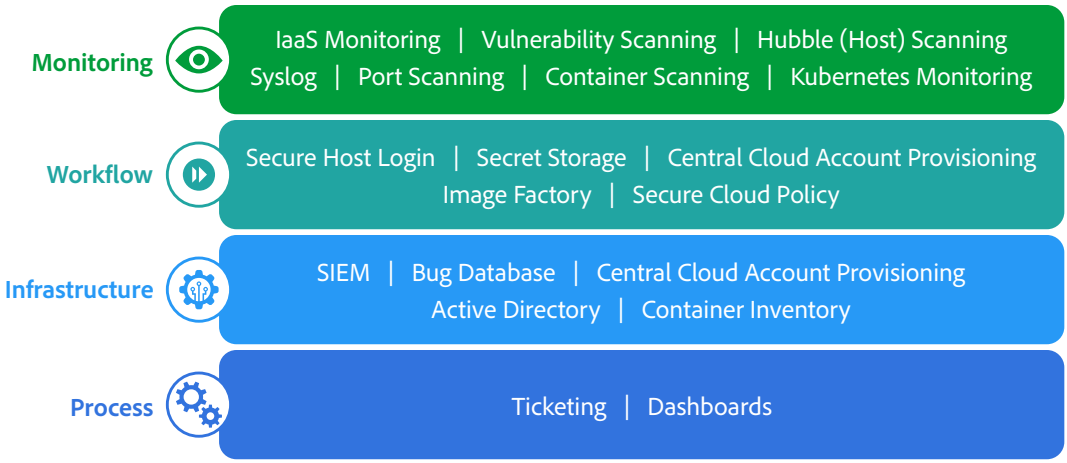


Figure 8: The Adobe Operational Security Stack

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 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 Journey Optimizer and your confidential data. At Adobe, we take the security of your digital experience data very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of our customers' data.

For more information about Adobe security, please go to the Adobe Trust Center.

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative.