Adobe Document Cloud

Adobe

WHITE PAPER

Adobe® Document Services APIs Security Overview

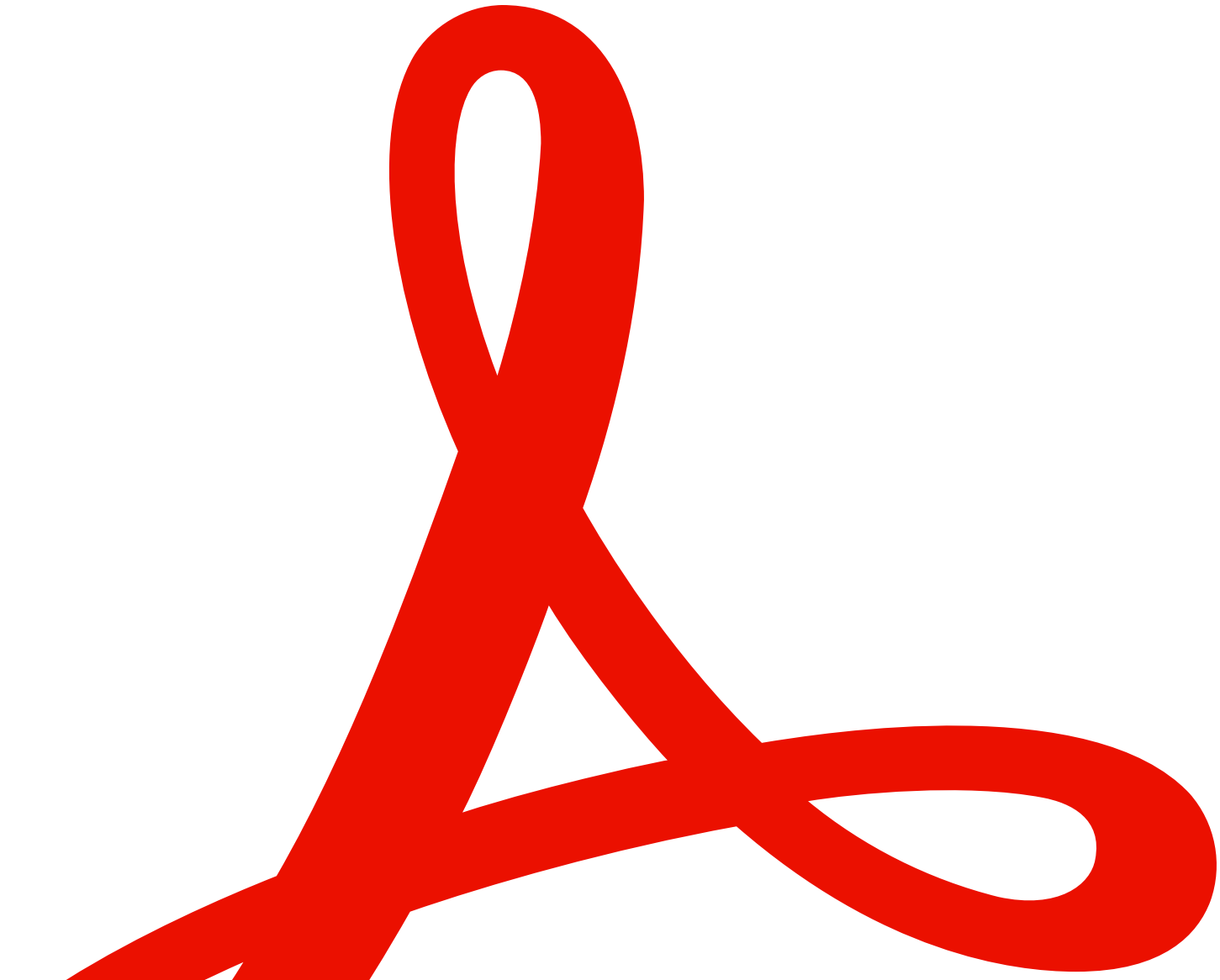

Table of Contents

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 Document Services APIs and their associated data.

About Adobe Document Services APIs

Adobe Document Services APIs help developers automate the generation, manipulation, and transformation of document content via a set of modern cloud-based web services. There are four (4) main Document Services APIs:

1. **Adobe PDF Services API**
   The Adobe PDF Services API is a cloud-based service that allows developers to manipulate PDFs in document workflows. Using the PDF Services API, you can:

   - Convert files from other formats to PDF files (e.g., HTML to PDF) and PDF files to other formats (e.g., PDF to Microsoft Word)
   - Compress PDF files
   - Combine multiple PDFs into a single PDF file or split a single PDF file into multiple PDFs
   - Perform OCR to create searchable and editable PDF files
   - Rotate or delete pages in a PDF file
   - Add encryption to, restrict permissions, or remove password protection on a PDF file

2. **Adobe PDF Extract API**
   Bundled with the Adobe PDF Services API, the PDF Extract API leverages the Adobe Sensei AI and machine learning platform to automatically extract text, tables, images, and document structure from PDF documents — native or scanned — and output the content in a structured JSON format.

3. **Adobe Document Generation API**
   Also bundled with the Adobe PDF Services API, the Document Generation API is a cloud-based web service that enables you to produce high-fidelity PDF and Word documents from Word templates and JSON data, or even merge JSON data with Word templates to create dynamic documents.

   Developers can embed the PDF Services API in any application via the PDF Services SDKs for Java, .NET, Node.js, and Python.

4. **Adobe PDF Embed API**
   The Adobe PDF Embed API allows developers to embed a PDF viewer into any web application and natively display their PDF in a controlled environment, enabling users to interact with and collaborate on PDFs within the application.

   With the PDF Embed API, you can:

   - Embed PDFs without forcing users to download additional plug-ins
   - Provide a rich PDF viewing experience within web applications
   - Enable digital collaboration and document analytics

   Developers embed PDFs into applications using web-based JavaScript code and in-page JS options, with support for React and Angular frameworks.

   For a complete list of functionality and other details for these APIs, please see the product documentation.

Adobe Document Services APIs Hosting and Security

All server-side components of PDF Services API and PDF Embed API are hosted in the data centers of leading cloud hosting providers. Publicly accessible and downloadable components, such as the PDF Services SDKs and the PDF Embed API JavaScript library are hosted on providers relevant to the component, such as library repositories and CDNs.

Data Encryption

All content in transit is encrypted using TLS 1.2 or greater.

PDF Services API Security

Authentication

The PDF Services API supports Service Account authentication. For more information on this authentication type, please refer to the Adobe I/O Authentication Overview.

User-Generated Content Storage

PDF Services API accepts and returns user-generated content (UGC). This content is uploaded to Adobe Document Cloud and temporarily cached as part of normal service operations.

PDF Embed API Security

Authentication

PDF Embed API is a client-side JavaScript- and WASM-based library and does not make any calls to cloud-based services. There are only three purposes for which the API makes network calls:

- Validating the client ID specified in JavaScript code upon loading
- Logging event data for out-of-the-box analytics and a pre-configured analytics dashboard, if given an Adobe Analytics report suite ID by the PDF Embed API integrator
- Loggin anonymous usage data in Adobe Analytics for internal use by Adobe for product improvement and feedback.

Iframe Security

The core functionality of PDF Embed API is contained within a sandboxed iframe. This helps prevent any vulnerabilities in the library from affecting the host website and vice versa. It also prevents unintended document object model (DOM) access and manipulation across the iframe boundary.

Content Security Policy (CSP)

Content loaded in the iframe is governed by CSP directives that help protect against certain kinds of attacks, including cross-site scripting (XSS).

Content Storage

The PDF Embed API does not manage content in cloud storage. Its primary functionality is restricted to loading and rendering PDF files supplied by the customer and, when asked to, saving a copy of the loaded file to local drives or external storage. Any controls or storage of the documents are dependent on either the website or the access controls of the browser to the PDF file.

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 1: 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.

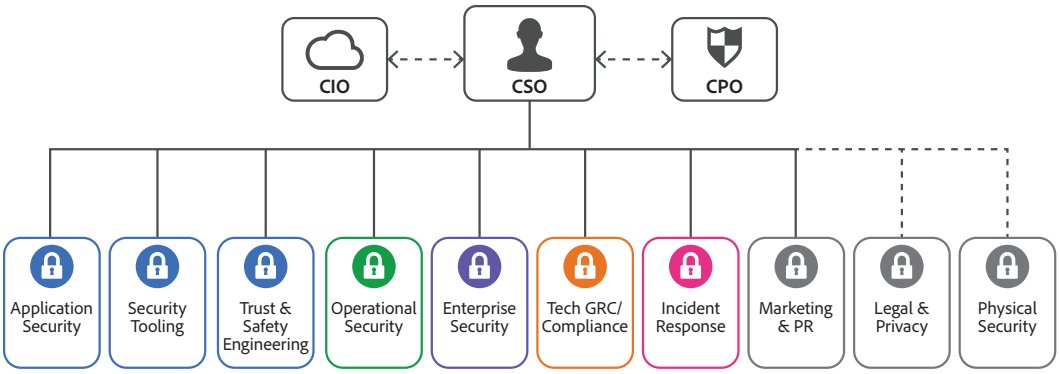

Figure 2: The Adobe Security Organization

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.

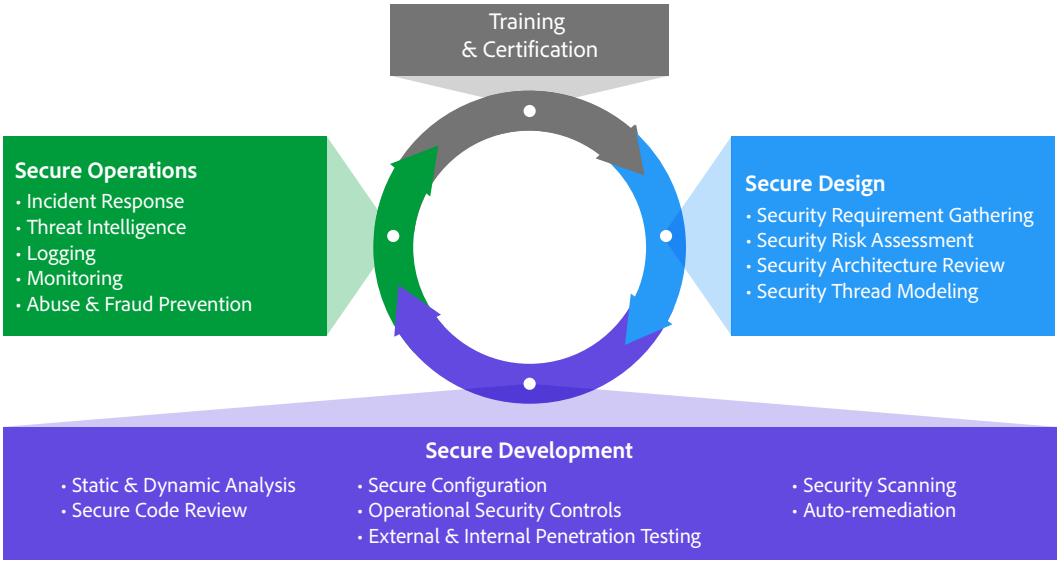

Figure 3: The Adobe Secure Product Lifecycle

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.

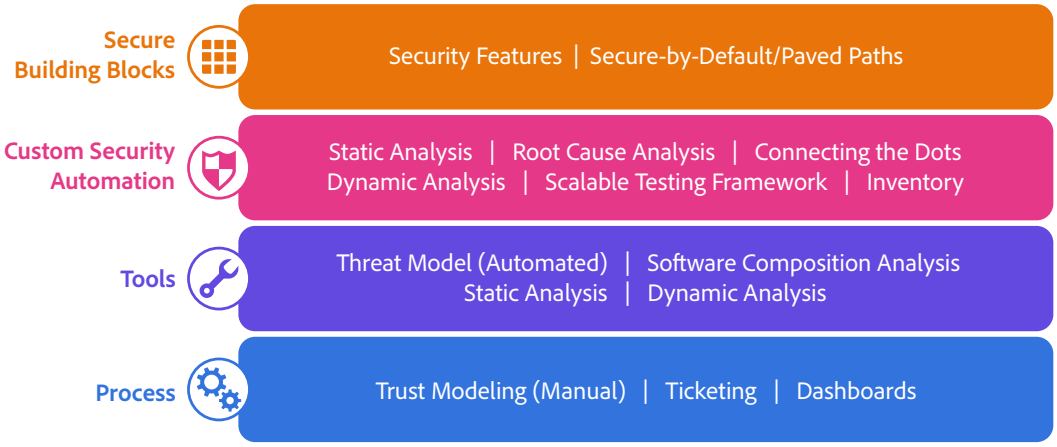

Figure 4: The Adobe Application Security Stack

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.

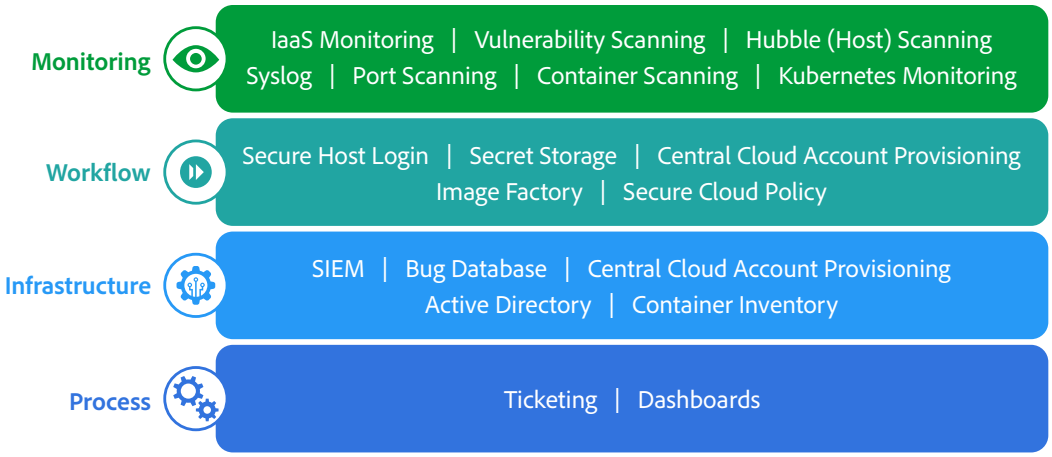

Figure 5: The Adobe Operational Security Stack

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 Document Services APIs 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.