Adobe Experience Cloud Security

Overview

At Adobe, we take the security of your digital experiences seriously. From our rigorous integration of security into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What’s more, our collaborative work with partners, researchers, and other industry organizations helps us understand the latest security best practices and trends and continually build security into the products and services we offer.

This white paper describes the proactive approach and procedures implemented by Adobe to address the security of Adobe Experience Cloud and your data.

Adobe Experience Cloud Solutions

Adobe Experience Cloud includes eight (8) primary solutions that help you give customers what they want—at the right moment. We have additional white papers that go into more detail about the security capabilities of individual solutions:

- Adobe Analytics
- Adobe Audience Manager
- Adobe Campaign
- Adobe Experience Manager
- Adobe Media Optimizer
- Adobe Primetime
- Adobe Social
- Adobe Target

Adobe Experience Cloud Platform/Core Services

Table of Contents

1 Overview
1 Adobe Experience Cloud Solutions
1 Adobe Experience Cloud Platform/Core Services
2 Authentication/Identity Management
3 Experience Cloud User Experience
3 Security and Compliance Strategy for Experience Cloud
4 Adobe Security Organization
4 Adobe Security Culture
4 Incident Response and Notification
5 Adobe Secure Product Lifecycle (SPLC) and Secure Engineering
6 Secure Operations
7 Adobe Experience Cloud Compliance
8 Conclusion
Adobe Experience Cloud solutions have access to five (5) core services, which are included in the platform:

**People** — Enables you to create a comprehensive view of individual customers by connecting Adobe and non-Adobe data in your Adobe Experience Cloud solutions. With the People core service, you can determine what matters most to your customers as they interact across touchpoints, recognize familiar consumers when they visit from unfamiliar devices, and group users into audiences for targeted marketing efforts.

**Places** — Helps you enrich your customer profiles across Adobe Experience Cloud solutions with location information from mobile devices. With the Places core service, you can develop location-enabled apps, add location data to your analytics, and engage users with location-based messaging. Places includes micro points of interest (e.g., beacons and stickers) as well as macro points of interest (e.g., GPS and geo-fencing). It also includes a database of points of interest so you don’t have to manually enter latitude and longitude coordinates for each one.

**Assets** — Lets you store your content in a central location that is automatically connected to the Adobe solutions you use every day. Not only can you find and organize your digital assets in one place, but you can also connect your files across Adobe Experience Cloud solutions and sync assets from Adobe Creative Cloud, making it easier for designers and marketers to collaborate.

**Mobile** — Provides the core technology stack necessary to deliver mobile interfaces for Experience Cloud applications and services to help enable customers to extend the experiences they want to provide to mobile devices for their users.

**Activation** — Lets you activate new technology across your website and connect it to the data you want, so you can trigger the right services at the right time and let your customers’ own behavior determine their web experience. With the Activation core service, it’s easier to launch customized actions based on what users do on your site — in real time — so you can launch a special offer, pop up a chat pod, or collect specific data at exactly the right time.

The platform also includes a set of services which enable you to create and intelligently deliver assets for personalized experiences in real time and at massive scale. The platform harnesses information from content and data assets — from high-resolution images to customer clicks. With the explosion of data, it can be tough for marketers to keep up. No worries. Behind the scenes, the platform crunches numbers and notifies you when it finds something interesting. Like a new lookalike audience you may want to approach. Or a specific message that will resonate better with a customer. And it also offers predictive modeling, to help you anticipate market changes and make better decisions.

**Authentication/Identity Management**

Users can access the Experience Cloud interface using one of three (3) different types of Client IDs. 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. Two-factor authentication options are supported for Adobe ID.

**Enterprise ID** is an Adobe-hosted, enterprise-managed option for accounts that are created and controlled by IT administrators from the customer enterprise organization. While the organization owns and manages the user accounts and all associated assets, Adobe hosts the Enterprise ID and performs authentication. Admins can revoke access by taking over the account or by deleting the Enterprise ID to permanently block access to associated data.

**Federated ID** is an enterprise-managed account where all identity profiles—as well as all associated assets—are provided by the customer’s Single Sign-On (SSO) identity management system and are created, owned, and controlled by IT. Adobe integrates with most any SAML2.0 compliant identity provider.
Experience Cloud User Experience

The Adobe Experience Cloud user interface provides a central location for users to access all of their Adobe Experience Cloud solutions and core services with user-friendly navigation. In addition, a centralized feed enables cross-channel collaboration between marketers and a notifications widget helps marketers stay in touch with events such as created posts, shared assets, and system updates.

The content and behavior of the Experience Cloud user experience is dynamically rendered based on the user’s profile. This enables seamless navigation between various Experience Cloud solutions and core services. This is realized by passing the user’s authorization token in the HTTP request’s header file. The destination application then performs the authorization itself via service-to-service authorization using a whitelisted Client ID. All solutions and services must whitelist a Client ID to be able to talk to it. Also, note that Client IDs can have variable scope to help prevent accidental misuse and malicious intent. These capabilities also enable integration of the various core services and feeds from Experience Cloud applications to be rendered in one user experience.

Security and Compliance Strategy for Experience Cloud

Adobe believes that a sound compliance and risk management strategy is as important to the success of an organization as the company’s product strategy. To this end, our Experience Cloud strategy includes a two-pronged approach to keeping your data safer, more secure, and available.

To protect from the physical layer up, we implement a foundational framework of security processes and controls called the Common Controls Framework (CCF) by Adobe. The CCF by Adobe helps protect the Adobe infrastructure, applications and services, as well as helps us comply with a number of industry-accepted best practices, standards, regulations and certifications.

Adobe complies with a range of important industry standards and government regulations concerning the security and privacy of data. While there are numerous industry standards and certifications comprising thousands of different requirements for compliance in the cloud, Adobe determined that significant overlap exists between these requirements and focuses on those that most significantly affect our Experience Cloud customers. As new security standards and regulatory requirements are developed and adopted by the industry, Adobe will review them and adopt those with relevance to our customers. Depending on the focus of a particular Adobe Experience Cloud solution, it may comply with some or all of the industry and regulatory standards described in the section below.

To protect from the software layer down, we use the Adobe Secure Product Lifecycle (SPLC), a rigorous set of several hundred specific security activities spanning software development practices, processes, and tools that are integrated into multiple stages of the product lifecycle. For more information on the Adobe SPLC, please see the Adobe SPLC section in this document, below.

Adobe Security Organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts under the Chief Security Officer (CSO). The office of the CSO coordinates all product and service security initiatives and the implementation of the Adobe Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security specialists who serve as consultants to key Adobe product security and operations teams. ASSET researchers work with individual Adobe product security and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations and incident response.
Security teams specifically assigned to Adobe Experience Cloud create controls, implement procedures, coordinate incident response, and oversee audits. These teams also help ensure the implementation of proper administrative, technical, and physical controls to help prevent unauthorized access to customer data. Many members of the security team earn and regularly maintain certifications as a Certified Information Systems Security Professional (CISSP®), a globally recognized, independent security certification given by the Information Systems Security Certification Consortium, Inc., (ISC)². Members with CISSP certifications renew their certifications every 3 (three) years. Members of the security team specialize in a broad range of security areas, including risk and vulnerability management, network security, monitoring, auditing, compliance and application security.

Adobe Security Culture

Adobe believes that every action taken on or interaction with data should be conducted with a lens of security to help ensure the security, privacy and availability of our customers’ data. To help achieve this goal, Adobe has created a culture of security that touches every corner of the company, beginning with regular security awareness training and seminars for all employees. Engineering and operations employees receive additional job- and/or function-specific security training and certification, helping them to be highly informed, adaptable and responsive to whatever vulnerabilities may arise. These employees can take advantage of many opportunities to demonstrate their ability to lead and create security projects that affect the entire company.

In addition, each product organization, including the Adobe Experience Cloud organization, includes a security champion, an Adobe employee who is specifically tasked with and responsible for the application and inclusion of the latest security mechanisms.

With this company-wide focus on security, Adobe tries to not only proactively prevent potential security issues from affecting both the company and our customers but is also able to more swiftly react to, remediate and resolve vulnerabilities and threats when they do appear.

Incident Response and Notification

As new vulnerabilities and threats evolve, Adobe strives to respond and mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT, Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

When a significant vulnerability is announced, the security team generates a customized environmental Common Vulnerability Scoring System (CVSS) score to identify the appropriate threat level and priority. Then, the team communicates the vulnerability to the appropriate teams both within and outside of the Adobe Experience Cloud organization to coordinate the mitigation effort.
Centralized Incident Response
Adobe Experience Cloud employs Adobe's centralized incident response, decision-making, and external monitoring with our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues. When an incident occurs, the SCC works with the involved Adobe product incident response and development teams to identify, mitigate, and resolve the issue as quickly as possible using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

Forensic Analysis
Adobe adheres to a forensic analysis process that includes complete image capture, evidence safe-holding, and chain of custody recording. Adobe may engage with third party forensics investigators as well as law enforcement in situations requiring further investigation or prosecution.

Adobe Secure Product Lifecycle (SPLC) and Secure Engineering
As with other key Adobe product and service organizations, the Adobe Experience Cloud organization employs the Adobe SPLC process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. Specific SPLC guidance is recommended per key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

A dedicated team of industry experts in building, deploying, and monitoring applications and services with robust security features, the Adobe Secure Software Engineering Team (ASSET) developed and constantly evolves the Adobe SPLC. They work with our digital marketing engineering teams to help achieve a high level of security for Adobe products and services.

A key part of the Adobe SPLC, the ASSET Software Security Certification Program includes ongoing training specifically designed for our engineering and operations teams to enhance security knowledge throughout the company and help improve the overall security of our products and services. The program provides a foundation for everyone at Adobe to understand security fundamentals, and it serves as a path for individuals who want to become security leaders. Participants achieve different certification levels called “belts” after completing in-person and online training as well as custom security projects.

Adobe SPLC
The Adobe SPLC controls include, depending on the specific Experience Cloud product or service, some or all of the following recommended best practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe Digital Publishing Suite security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture reviews and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness reviews, response plans, and release of developer education materials

Adobe Secure Product Lifecycle (SPLC)

Secure Operations

By employing the right level of processes and procedures in tandem with our overall security strategy, we provide a robust framework for continuous risk management and help the security of our operations. Our processes and controls are also designed to support many compliance frameworks and follow industry-standard operations practices.

System monitoring and logging

Our Ops Security teams use a set of monitoring alert criteria to define the critical security and availability standards for our services’ production environments. Ops Security personnel use third-party monitoring tools to closely monitor any spikes in activity above predefined thresholds. We also deploy Intrusion Detection System (IDS) sensors at critical points in the network to help detect and alert our security team to unauthorized attempts to access the network. Alerts are triggered for anomalies, and Ops Security uses established procedures to address them and any potential security threats they may represent.

Access control

We use access control measures so that the fewest number of operators have access to restricted data. Role-based access is defined and deployed to restrict privileged access to information resources based on the concept of least privilege. Authorization requires approval by the management directly responsible for the confidentiality, integrity, and availability of impacted resources.

Automation

As much as possible, we automate processes and procedures to help create efficiencies, maintain consistency and repeatability, and reduce human error. We use automation in areas including configuration and patch management, creation and hardening of baseline images, and system monitoring.
Change management

We enforce a comprehensive change management process to help ensure that changes to the network or production environment are documented, tracked, tested, authorized, and approved prior to migration to production. We monitor the states of the hardware, operating system, and configurations, and we log and execute changes in a controlled way. We also evaluate and check logs for potential misconfigurations.

Adobe Experience Cloud Compliance

The Adobe Common Controls Framework (CCF) is 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. In creating the CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,000 requirements down to Adobe-specific controls that map to approximately a dozen industry standards.

10+ Standards, ~1000 Control Requirements (CRs) & ~ 200 common controls across 11 control domains

<table>
<thead>
<tr>
<th>Standard</th>
<th>Approximate CRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 2 (5 Principles)</td>
<td>116 CR</td>
</tr>
<tr>
<td>ISO 27001 – 26 CRs</td>
<td></td>
</tr>
<tr>
<td>PCI DSS – 247 CRs</td>
<td></td>
</tr>
<tr>
<td>FedRAMP – 325 CRs</td>
<td></td>
</tr>
<tr>
<td>ISO 27002 – 114 CRs</td>
<td></td>
</tr>
<tr>
<td>SOX 404 (IT) – 63 CRs</td>
<td></td>
</tr>
<tr>
<td>Asset Management</td>
<td>12 Controls</td>
</tr>
<tr>
<td>Access Control</td>
<td>30 Controls</td>
</tr>
<tr>
<td>BCM</td>
<td>10 Controls</td>
</tr>
<tr>
<td>Cryptography</td>
<td>11 Controls</td>
</tr>
<tr>
<td>Data Privacy</td>
<td>10 Controls</td>
</tr>
<tr>
<td>Incident Response</td>
<td>6 Controls</td>
</tr>
<tr>
<td>Operations Management</td>
<td>70 Controls</td>
</tr>
<tr>
<td>Physical and Env. Security</td>
<td>16 Controls</td>
</tr>
<tr>
<td>People Resources</td>
<td>11 Controls</td>
</tr>
<tr>
<td>SDLC</td>
<td>11 Controls</td>
</tr>
<tr>
<td>Security Governance</td>
<td>31 Controls</td>
</tr>
</tbody>
</table>

The Adobe Common Controls Framework (CCF)

Current Standards and Regulatory Compliance for Adobe Experience Cloud

SOC 2 is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Experience Cloud solutions as well as Adobe Connect Managed Services and Adobe Experience Manager (AEM) Managed Services1 are SOC 2 – Type 2 (Security & Availability) compliant.

ISO 27001 is a set of globally adopted standards that outline stringent security requirements and provide a systematic approach to managing the confidentiality, integrity, and availability of customer information. Adobe Experience Cloud solutions1 as well as Adobe Connect Managed Services and AEM Managed Services1 are compliant with ISO 27001:2013.2

The Federal Risk and Authorization Management Program (FedRAMP) is a collection of mandatory standards established by the U.S. Federal Government for security assessment and purchase approval for cloud solutions. Adobe Connect Managed Services and AEM Managed Services1 are compliant with FedRAMP.

The Health Insurance Portability and Accountability Act (HIPAA) is legislation that governs the use of electronic medical records, and it includes provisions to protect the security and privacy of personally identifiable health-related data, called protected health information (PHI). Adobe Connect Managed Services and AEM Managed Services1 are HIPAA-compliant which means these products can enable our enterprise customers to use our solutions in a way that they can meet their obligations under HIPAA regulations. Ultimately the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.
The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions safeguard their customers’ personal data. Experience Cloud solutions, as well as Adobe Connect Managed Services and AEM Managed Services, are "GLBA-ready". These Adobe products enable our FSI customers to comply with the GLBA Act requirements for using service providers. Ultimately the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

The U.S. Family Education Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. Student education records and directory information. Under FERPA guidelines, Adobe can contractually agree to act as a "school official" when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements. Ultimately the customer is responsible for ensuring their compliance with their legal obligations, that our products meet their compliance needs, and that they secure the products in an appropriate way. Adobe Connect Managed Services and AEM Managed Services are FERPA-Ready.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Experience Cloud solutions 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 stay ahead of malicious activities and help ensure the security our customers' data.

For more information, please visit: http://www.adobe.com/security