WHITE PAPER

Adobe® Workfront 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 Workfront and associated data.

About Adobe Workfront

Adobe Workfront is an enterprise work management solution that helps customers manage the entire lifecycle of work in one place. Built for the way people work, the platform is intuitive, flexible, and customizable and provides a 360-degree view of all workplace activities, helping both team members and administration alike to better understand and organize their work.

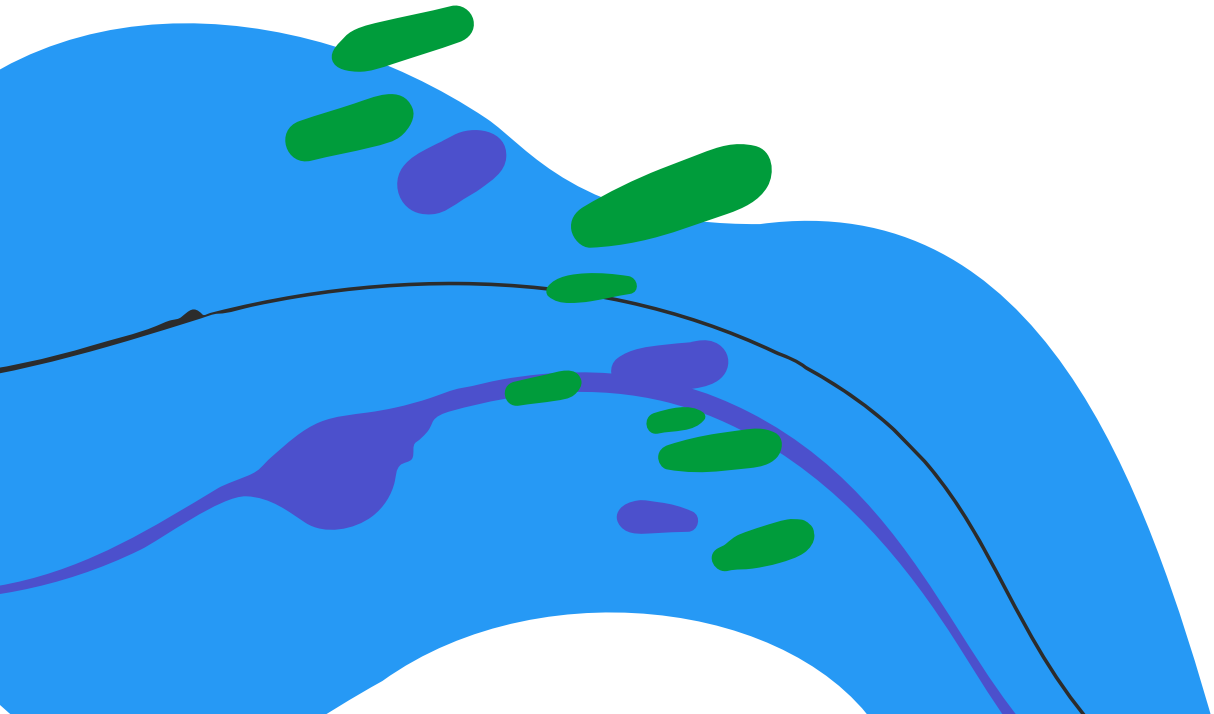
The solution includes the following functionality:

- **Project Management** — Enables planning and executing projects using feature-rich, interactive Gantt charts, real-time reporting, and custom project dashboards and views that give managers complete visibility to manage and bring projects in on-time and on-budget.
- **Reports and Dashboards** — Delivers custom reports and dashboards to unlock the data being tracked in Adobe Workfront. With more than 150 out-of-the-box yet customizable reports and dashboards, customers can change as programs mature and reporting needs grow.
- **Resource Management** — Allows resource managers to make business decisions that ensure the individual workers available today are budgeted against the highest priority work.
- **Team Collaboration** — Empowers teams with front-line conversational information, increasing their acceptance of and participation in the project management process, enabling greater accuracy in projections and more informed decision-making.
- **Time Management** — Allows customers to create and manage timesheets for anyone on the team through a built-in timesheet management portal.

- **Portfolio Management** — Helps prioritize projects and ensure that they are aligned with business goals and requirements.
- **Process Improvement** — Enables organizations to incorporate workflows within the solution, improving communication, coordination, and efficiency.
- **Product Integration** — Seamlessly integrates with a variety of business-critical applications, including turnkey connectors for popular applications.
- **Proofing** – Automatically notifies and updates collaborators and stakeholders on all pending and completed approvals outlined in the project workflow.
- **Auditing and Governance** — Provides a central repository for all project information, enabling the creation of an audit trail to authenticate compliance with corporate standards.

Adobe Workfront also includes three optional add-ons:

- **Workfront Fusion** — Lets customers create, manage, and monitor automated workflows within Workfront and across various third-party applications (Please see the section below for more information on specific security considerations for Workfront Fusion).
- **Workfront Goals** — Helps define, communicate, and achieve strategic outcomes by connecting strategy to work execution and delivery.
- **Workfront Scenario Planner** — Drives speed to execution by enabling the creation of different scenarios to find the optimal plan that delivers on the organizations' overall strategic outcomes.



Adobe Workfront Solution Architecture

The following diagram describes the components of the Workfront solution and the interconnections between them.

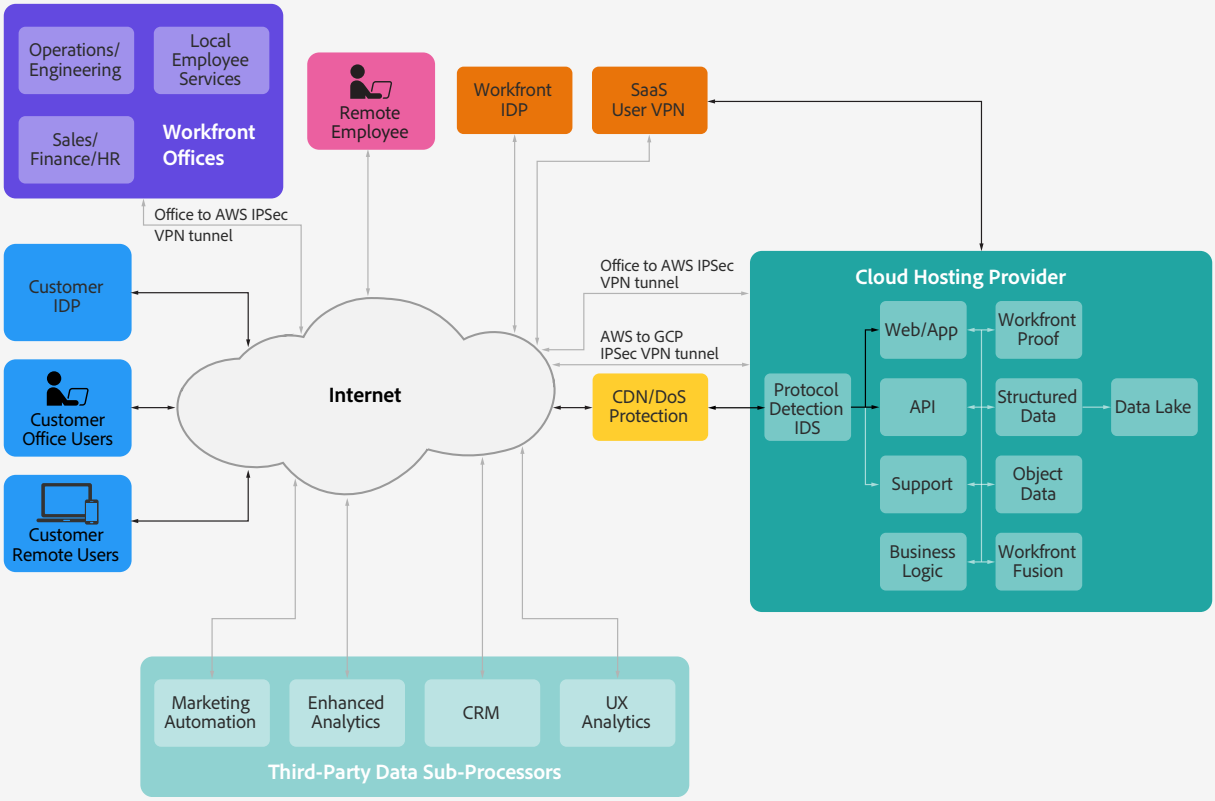


Figure 1: The Adobe Workfront Solution Architecture

Adobe Workfront Security Architecture and Data Flow

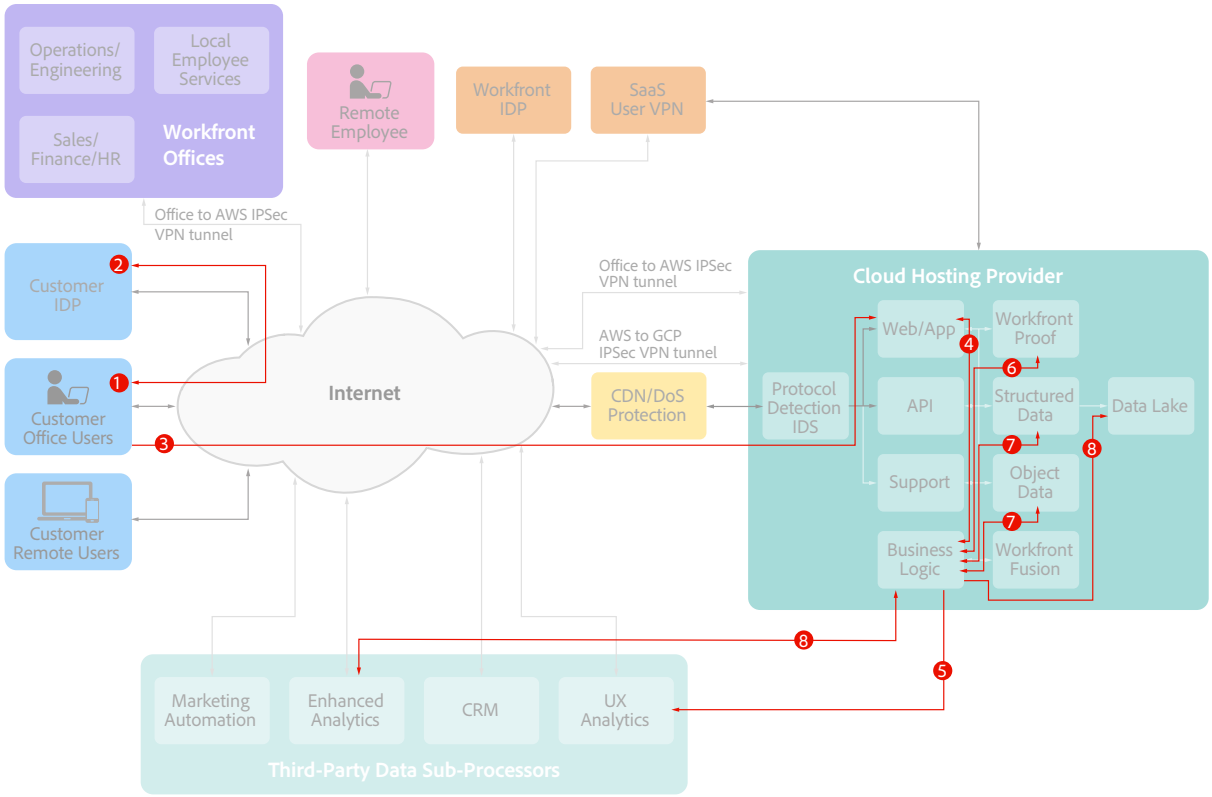


Figure 2: The Adobe Workfront Security Architecture and Data Flow

To protect the customer's Workfront URL from downgrade attacks, we implement HTTP Strict Transport Security (HSTS), which only allows access to the website using a secure HTTPS connection. In addition, Workfront protects customers from cross-site request forgery (CSRF/XSRF) and cross-site scripting (XSS) attacks.

Data Flow

Customers interact with Workfront in three ways:

- Workfront web UI
- Workfront mobile application
- Workfront API

1. In each case, the connection to Workfront begins with a TLS-1.2-secured HTTP request from the user's web browser to the customer company's Workfront URL.
2. Front-end load balancers and a CDN for static assets receive these HTTP requests and forward them to the Workfront application servers on the cloud hosting provider. Each request is filtered by the native firewall technology employed by the cloud hosting provider, helping ensure that only web requests using TCP port 80 or TCP port 443 are allowed.
3. The Workfront application servers handle the customer-configured authentication mechanisms (SSO, etc.) by initiating a new session or confirming an HTTP request against an existing authorized session.
4. Workfront application servers then route authorized requests between VPCs (virtual private clouds) to connect to Workfront backend databases or pull data from (using authenticated requests) cloud-native storage services.
5. Customers can view the events from these interactions either via the Audit Log (available via the Web UI) or the Event Subscription API.

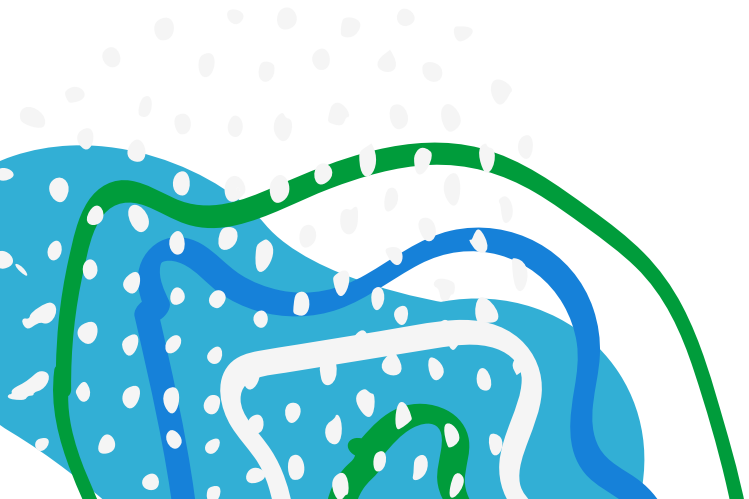
Adobe Workfront uses some third-party data sub-processors to provide certain functionality. A complete list of sub-processors used by Adobe can be found here.

Data Encryption

Adobe Workfront employs PCI DSS approved encryption algorithms to encrypt documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit.

Documents uploaded to Adobe Workfront are stored in cloud-native object storage services. Workfront databases are then encrypted with disk-level encryption technologies.

Workfront utilizes cloud-native key management systems (KMS) to centrally store and manage encryption keys. Workfront encryption keys are generated and stored in a FIPS-140-2 validated (or better) KMS managed by the cloud service provider and are automatically rotated on an annual basis.



User Authentication in Adobe Workfront

Access to Adobe Workfront requires authentication with username and password. We continually work with our development teams to implement new protections based on evolving authentication standards.

Users can access Workfront in one of three (3) different types of user-named licensing:

Adobe ID is for Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users.

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 to Workfront 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, controlled by the customer's IT infrastructure.

Adobe integrates with most SAML2.0 compliant identity providers. Adobe IDs and Enterprise IDs both leverage the SHA-256 hash algorithm in combination with password salts and a large number of hash iterations. Adobe continually monitors Adobe-hosted accounts for unusual or anomalous account activity and evaluates this information to help quickly mitigate threats to their security. For Federated ID accounts, Adobe does not manage the users' passwords. More information about Adobe's identity management services can be found in the Adobe Identity Management Services security overview.

API Authentication

Adobe Workfront provides a REST API interface that enables customers to integrate Workfront into their other corporate applications and services. The Adobe Workfront API interface offers three (3) different authentication mechanisms:

1. **Username + Password (+ Digital Certificate)** — The user must supply a valid username and password in order to access the Adobe Workfront API interface. For additional security, users can be required to supply a digital certificate in addition to username + password. Typically, this method of authentication is only used to:

a. Generate a session token (sessionID) for pre-authenticating future API calls
b. Generate an API key
c. Retrieve an API key

2. **Session Token** — The user presents a short-lived session token with each API call. Obtained using one of the two username + password authentication mechanisms mentioned above, the sessionID may be supplied as a URL parameter or in the HTTP header. Customers can configure sessionID lifetime based on their requirements.

3. **API Key** – Only available to users with system administrator-level privileges, the user supplies a valid API key to access the Adobe Workfront API interface. API keys are securely managed and generated within the Workfront application. Customers can configure these keys to automatically expire after a pre-determined amount of time to compel periodic API key rotation. API key expiration can also be configured to expire whenever the corresponding user's password expires. System administrators can revoke all users' API keys if needed.

Administrative Security Controls

Role-Based Access Controls — Workfront includes six (6) out-of-the-box access levels, which are geared toward users with various roles in the organization. The access level the user is assigned to in their user profile governs their rights and privileges in Workfront. By default, a user's access level affects which areas are visible to that user in the Global Navigation Bar. System administrators also can copy canned access levels and modify them to add/remove functionality.

IP Allowlists — In some cases, administrators must add certain IP addresses to their firewall's or mail server's allowlist in order to allow open communication between their environment and Adobe Workfront.

Administrators also have access to a variety of other system security preferences in Workfront. Changes made to these security preferences impact all users of the Workfront solution. Therefore, Adobe recommends that customers configure their system security preferences during initial implementation and only revisit them when absolutely necessary.

For more information on role-based access controls, IP allowlists, and specific security preferences available for Workfront, please visit Adobe Workfront One.

Adobe Workfront Hosting Locations

Adobe Workfront is hosted in data centers around the world managed by trusted and certified Adobe cloud hosting partners in the U.S. (Oregon, California, Iowa, and Virginia) and Europe (Ireland and Germany).

The specific data center region or location is determined by the customer's location, e.g., if the customer is based in the United States, their Workfront solution will be hosted in a data center located in the U.S. Similarly, if the customer is based in the E.U., their Workfront solution will be hosted in a data center in the E.U.

Figure 3: Adobe Workfront Hosting Locations

About Adobe Workfront Fusion

Adobe Workfront Fusion enables customers to create, manage, and monitor automated workflows within Workfront and across various third-party applications. With Workfront Fusion, data and information flow freely – yet securely – across systems and teams, increasing productivity and efficiency with a single, connected solution.

Adobe Workfront Fusion Solution Architecture

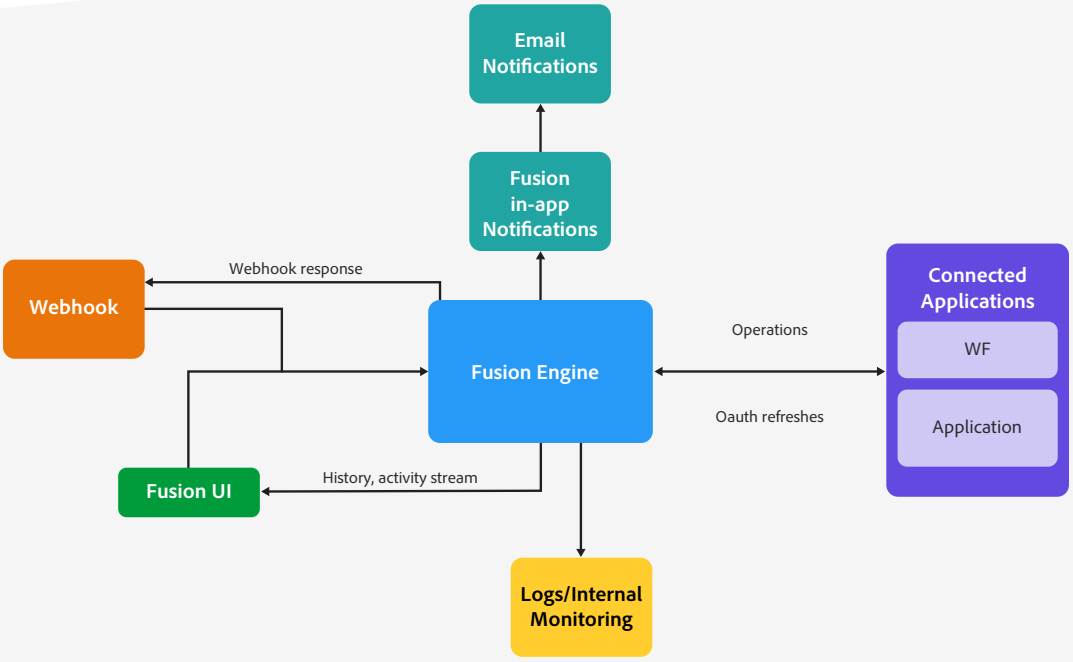


Figure 4: Adobe Workfront Fusion Solution Architecture

Adobe Workfront Fusion Data Flow

Fusion users use the Fusion visual designer to create and edit automation use cases called scenarios. A scenario is comprised of a series of modules that perform operations, including interactions with connected applications and data transformation. A Fusion module interacts with a web service via its API; The module defines what action is performed.

The Fusion engine executes scenarios based on trigger events. Scenarios with instant triggers are based on data received from another application. Scheduled scenarios are processed according to a schedule set using the Fusion designer.

During execution, Fusion operations sends data to and receives data from other systems. The Fusion engine also streams data to the Fusion user interface so that the user can view data that is currently being processed or that has already been processed, which can be accessed in Fusion's execution history.

Each connection between the user's browser and Workfront Fusion is encrypted using HTTPS TLS 1.2. Fusion also refreshes OAuth connections that support reauthorization.

Administrative Security Controls

Workfront Fusion provides administrators the same security controls as Workfront, which can be found above in the Workfront section of this document. For more information on role-based access controls, IP allowlists, and specific security preferences available for Workfront, please visit Adobe Workfront One.

Workfront Fusion Connectors

Workfront Fusion includes a pre-built set of application connectors that enable administrators to connect to other applications. For more information on how to add these connectors, please go to Adobe Workfront One.

Workfront Fusion also includes a set of universal connectors that enable administrators to connect to other applications for which a pre-built standard connector does not exist. These universal connectors support OAuth 2.0 Authorization Code Flow, Basic Authentication, and other forms of authentication based upon the specific needs of the target application.

In cases where an OAuth 2.0 Authorization Code Flow cannot be used, Workfront Fusion must store authentication credentials for the third-party application. Workfront Fusion uses cryptographically secure hash algorithms with AES encryption using PBKDF2 over SHA512 to encrypt credentials.

Regardless of the method of authentication used, once credentials for a third-party application are entered into Workfront Fusion, those credentials are never visible to any subsequent user, including the user that entered them originally.

All data between Workfront Fusion and connected third-party solutions is encrypted in transit using TLS 1.2. Mutual TLS is available for use in the HTTP connector.

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 5: 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.

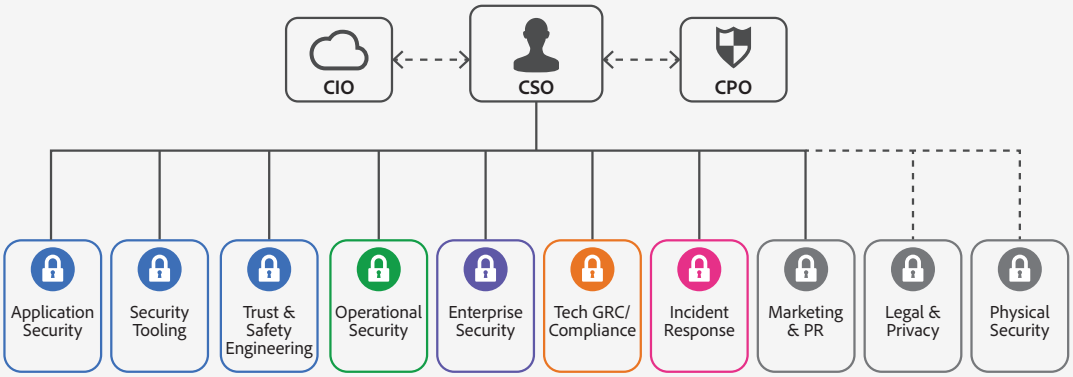


Figure 4: The Adobe Security Organization

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.

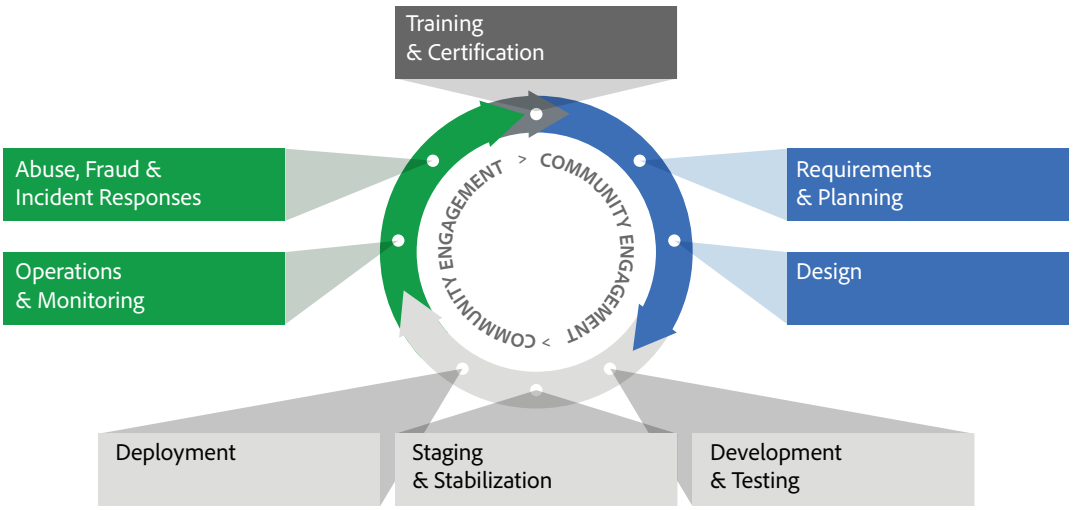


Figure 7: The Adobe Secure Product Lifecycle

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.

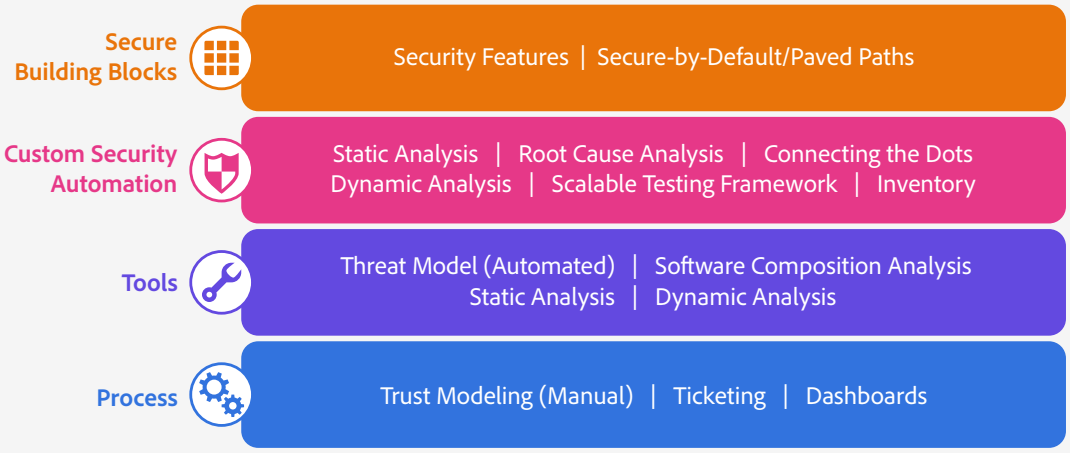


Figure 8: The Adobe Application Security Stack

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.

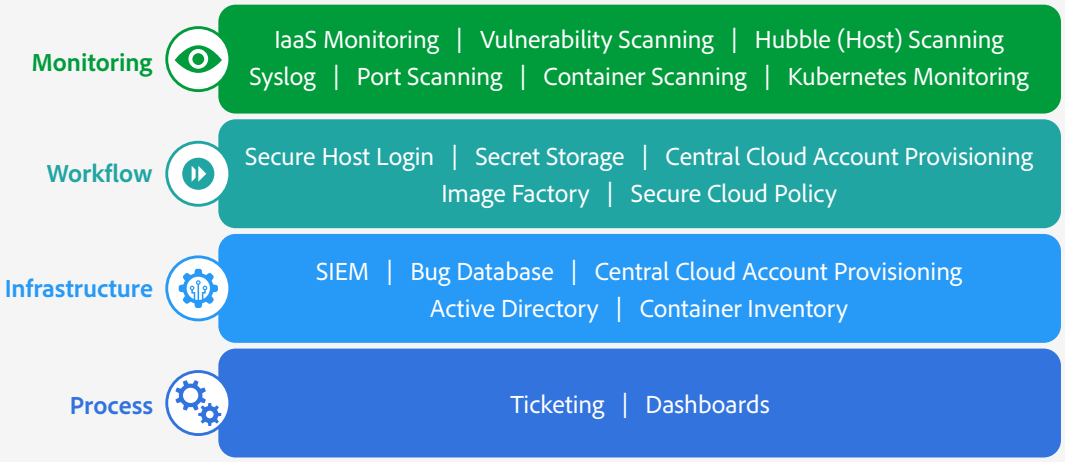


Figure 9: The Adobe Operational Security Stack

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.

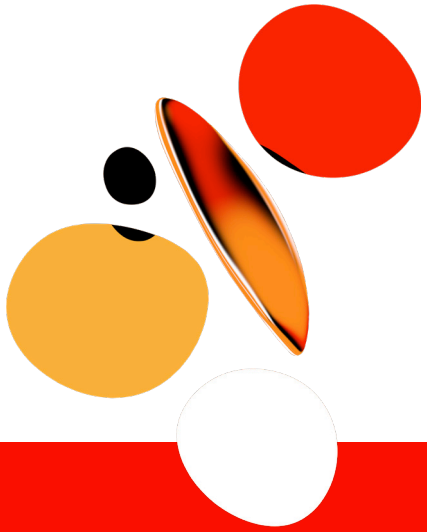
Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Workfront and Workfront Fusion 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 our customers' data.

For more information on:
Adobe security: www.adobe.com/security

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

Adobe
345 Park Avenue
San Jose, CA 95110-2704
USA www.adobe.com



Adobe