Adobe Document Cloud

Adobe

WHITE PAPER

Adobe Acrobat Sign Security Overview

October 2023

Table of Contents

Adobe Security

At Adobe, we know the security of your digital experiences is important. 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 paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of Adobe® Acrobat® Sign and your data.

Note: This document describes features available in Acrobat Sign Solutions for Enterprise and Acrobat Sign Solutions for Business. If you have questions about the availability of a specific Acrobat Sign feature, please consult your Adobe representative.

About Acrobat Sign

Acrobat Sign helps your organization replace paper-and-ink signatures and deliver end-to-end digital experiences across all types of signing workflows — from basic electronic signatures (e-signatures) to digital qualified electronic signatures in the cloud. With Acrobat Sign, you can easily send, sign, track, and manage signature processes anywhere, anytime using a browser or mobile device. Acrobat Sign provides turnkey integrations and APIs to allow your organization to incorporate e-signature workflows into enterprise services, systems of record, and popular cloud productivity solutions, such as Microsoft 365.

Acrobat Sign complies with many regional, industry, and regulatory standards including supporting certificate-based digital signatures for increased signer identification and security. A robust cloud-based solution, Acrobat Sign helps your organization securely handle large volumes of online signature processes, including:

- Managing user identities, authentication, and access control
- Certifying document integrity
- Verifying e-signatures
- Logging recipient acceptance or acknowledged receipt of documents
- Maintaining audit trails
- Integrating with your most valued business applications and enterprise systems

Additionally, Acrobat Sign cloud signatures enable remote digital signatures backed by digital certificates from trust service providers (TSPs) with verified Cloud Signature Consortium (CSC) integrations to Acrobat Sign. More detailed information on e-signature compliance and global e-signature laws can be found on the Adobe Trust Center.

Acrobat Sign Solution Architecture

The Acrobat Sign architecture is designed to scale and handle large volumes of transactions without performance degradation. To provide a high level of availability and scalability, all Acrobat Sign transactional data is stored in multiple distributed redundant database clusters with automatic failover and recovery.

To help ensure the continued availability and delivery of Acrobat Sign, Adobe deploys and supports a comprehensive, ISO 22301-certified business continuity and disaster recovery (BCDR) program that enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information is available in the Acrobat Sign BCDR Fact Sheet (NDA required).

Each logical layer in the Acrobat Sign solution is monitored by an extensive suite of tools that keeps track of key indicators, such as average time to convert documents into PDFs or resource usage.

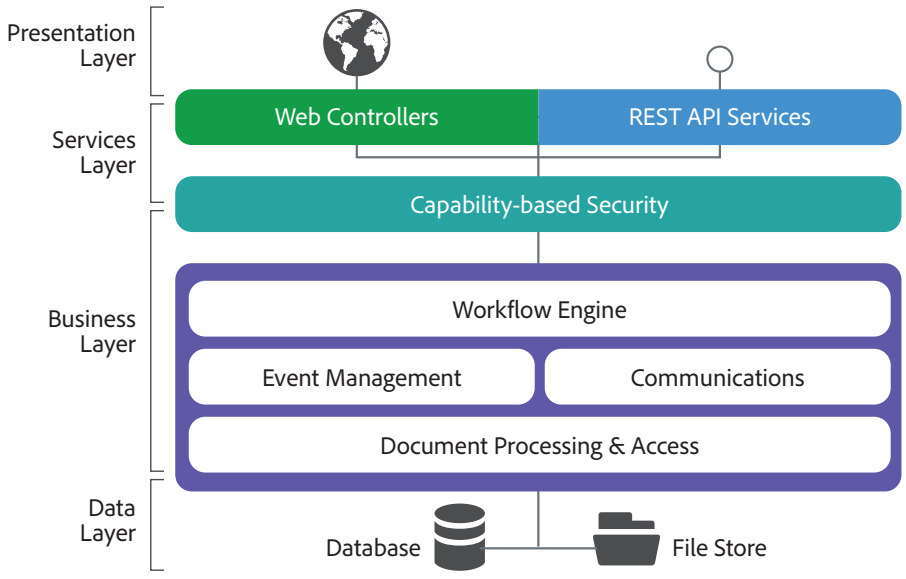

Figure 1: Acrobat Sign Solution Architecture

The monitoring dashboard allows Acrobat Sign operations engineers to easily view the overall health of the service. Real-time notifications alert operations engineers if any key indicator falls outside of its defined monitoring thresholds. If an issue cannot be averted, Acrobat Sign keeps extensive diagnostic and forensic logs to help engineers resolve the issue quickly and address the root cause to avoid a potential recurrence.

The following sections describe the functionality of each layer of the Acrobat Sign solution architecture.

Presentation Layer

The presentation layer manages the web user interface (UI) and generates and renders documents for signature collection and other workflows, including presentation of final PDF files with a tamper-evident seal.

Services Layer

The services layer handles the required controlling functions for the client and REST API services. The external-facing systems' web servers handle browser and API requests, and the email servers manage inbound and outbound communications.

Using load balancers, the web servers distribute complex dynamic requests to the Acrobat Sign application servers in the business layer. To prevent common web attacks, the services layer web servers also incorporate security-filtering rules as well as firewall protection to help strengthen access control.

Business Layer

The Acrobat Sign business layer handles the following functions:

- **Workflow engine** — Executes and manages all the business processes and steps that a document needs throughout the signature process. The workflow engine uses a declarative XML-based definition language to describe the preconditions for executing customer-specific flows and the sequence of events required to complete a signature or approval process.
- **Capability-based security** — Controls which resources are available and what operations are allowed to be performed on those resources by an authenticated user or application. Resources include any information in the form of documents, data, metadata, user information, reports, and APIs.
- **Document processing and access** — Provides stateless functionality for converting different file formats into PDF, for encrypting and decrypting files and for rasterizing images for viewing through a web browser. For document processing actions, Acrobat Sign relies on an asynchronous, queue-based messaging system to communicate across system resources. Additionally, all document processing and access to cloud file storage occurs in the background, allowing Acrobat Sign processing to appear instantaneous for users at each step in the workflow.
- **Event management** — Records and preserves an audit trail for relevant information pertaining to each user and document at each step in the workflow process. At each

stage in the workflow, Acrobat Sign generates an event and distributes messaging via an asynchronous messaging system to the appropriate system resources.

- **Communications** — Notifies users of signature events and optionally of signed and certified document delivery at the end of the process. To minimize spam and phishing, Acrobat Sign enables authenticated email with Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC), and Sender Policy Framework (SPF).

Data Layer

The data layer is responsible for transactional database access and the document store. Transactional data stored in the data access layer includes the original customer document, intermediate document versions generated during the signature process, document metadata, users, events, and the final signed PDF document processed by Acrobat Sign.

Integrations via REST API Services

Acrobat Sign includes turnkey integrations for a wide variety of business applications, enterprise systems, and trust service providers (TSPs). Additionally, Acrobat Sign exposes a comprehensive set of REST APIs that allow for custom integration with proprietary business systems or company websites via secure web services. Adobe maintains a complete list of business applications and enterprise systems supported by Acrobat Sign.

General Data Flow

The following data flow is how a customer often initiates the signing process for a document in Acrobat Sign. Step numbers correspond to the numbers in Figure 2, below:

1. **Create Repository:** Before using Acrobat Sign for the first time, users can create and save reusable custom workflow definitions, library templates, and web forms in the Acrobat Sign repository. Any user with access rights to these assets can then send an agreement from a library template, start a workflow, or post a web form to initiate signature processes.

2. **Compose Workflow:** To initiate a send agreement workflow through Acrobat Sign, the user defines the participants, the order in which they will participate, and the different options that define their participation. The workflow agreement may also be initiated through an Adobe-provided integration or through a partner or customer application built using the Acrobat Sign API. Agreements may also be sent out in bulk based on an uploaded list of email addresses.

Next, the user uploads the source document(s) to which the agreement pertains. Documents may be uploaded from a third-party cloud storage system, a customer or partner integration, from an existing library template, or from the user's desktop.

3. **Create Agreement:** Once a document is uploaded, it becomes an agreement within Acrobat Sign. If the agreement is generated from a library template form with predefined fields, Acrobat Sign instantiates fields into the agreement. If the agreement is not a library template form, the user must place the required fields into the agreement to help guide the signer through the signing experience.

   Acrobat Sign allows users to place form fields in their logical position in the agreement and add information and context to the agreement using typed form fields, such as email address, first name, last name, and title. This process is called "authoring."

   At a minimum, every agreement must have a signature field. The signature field can be placed through authoring or automatically by Acrobat Sign. If the user chooses to place the signature field automatically, Acrobat Sign places it at the bottom of the agreement (if space permits) or by adding an additional signing page to the agreement. This information can be exported later and used in downstream processes.

4. **Distribute Links:** When the user completes authoring the agreement, it is sent to all designated participants via email, web form, or by using the Acrobat Sign API in a custom application.

5. **Gather Signature:** Based on the agreement parameters, signers are asked to submit approval, provide a signature, and/or fill in form field values. These form fields may be optional or required, based on the originating user's instructions, and can be masked or formatted in a variety of ways. All values, along with the current agreement state (e.g., who has signed and who must sign next) are maintained in Acrobat Sign data storage in the cloud. Attachment documents may be collected at this stage.

6. **Present Fully Signed Agreement:** After all signers complete the signing workflow, the fully signed agreement is made available to all participants in the signing process and automatically stored in Acrobat Sign cloud storage. Users may download all artifacts related to the signing, including the signed agreement (certified PDF), an audit report (certified PDF) and a separate report of form field data values (exportable in CSV format), using Acrobat Sign clients. Optionally, users may move or copy the agreement into their chosen systems of record through Acrobat Sign APIs or a partner document vaulting service.

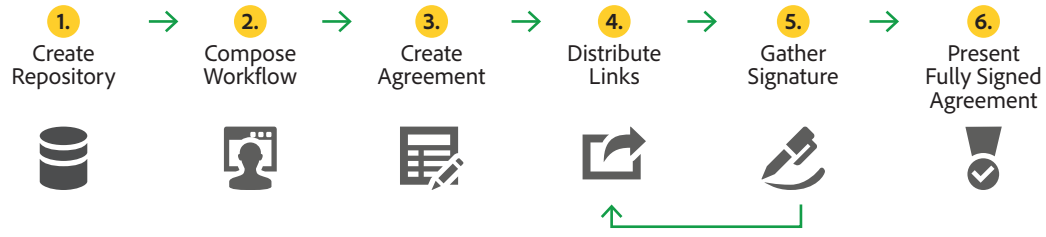

Figure 2: Acrobat Sign Data Flow

Acrobat Sign Security Architecture

The following network diagram describes the Acrobat Sign security architecture, including external- facing servers, cloud servers, and client access:

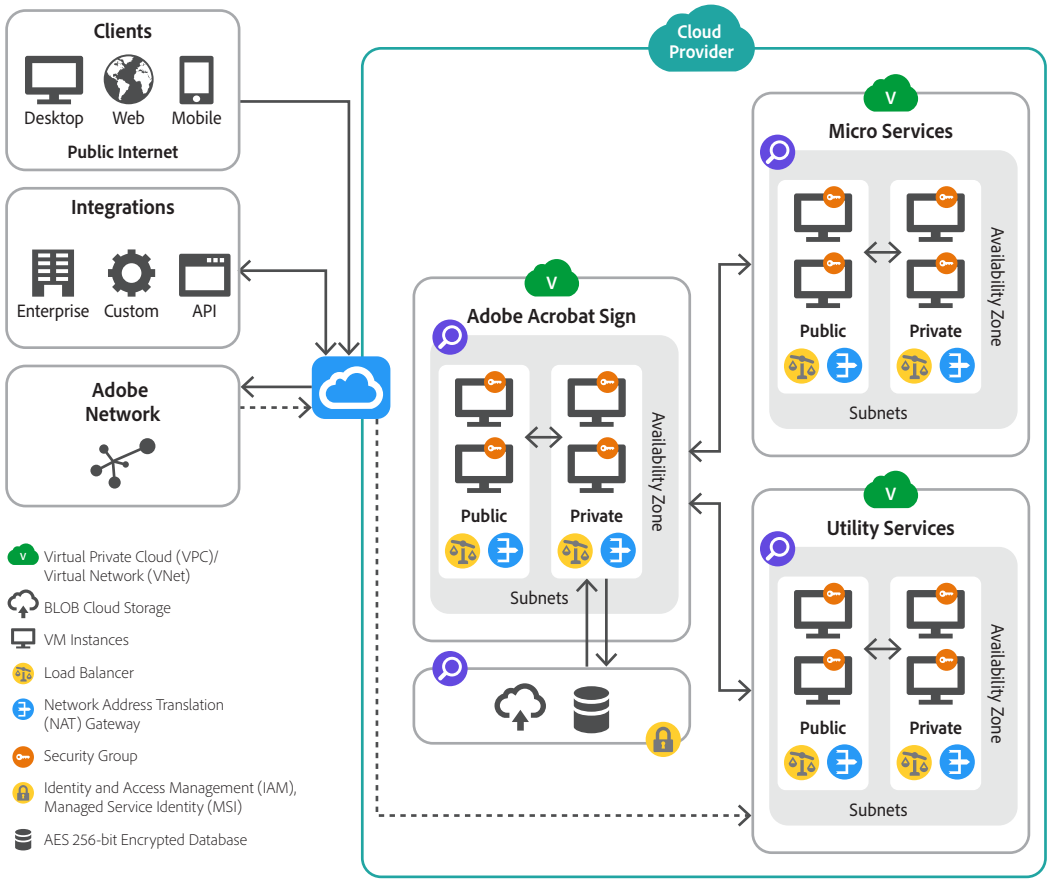

Figure 3: Acrobat Sign Security Architecture

External-Facing Servers

The external-facing systems within the hosted network architecture of Acrobat Sign include web servers to handle browser and API requests and email servers that handle inbound and outbound email traffic. The web servers and associated load balancers are responsible for distributing dynamic requests to the application servers. The web servers also include firewall protection to help ensure strong access control.

Virtualized Cloud Networks

The Acrobat Sign security architecture also relies on several virtualized cloud networks. In the AWS environment, these are referred to as Virtual Private Clouds (VPCs), while Microsoft Azure uses the term Virtual Networks (VNets).

A VPC/VNet is a logically isolated network, inaccessible from the outside except through tightly constrained entry and egress points. Within each VPC/VNet there are subnets, which contain a range of IP addresses. Subnets may be either public or private. A public subnet is connected to the Internet; a private subnet is not connected to the Internet. VPCs/VNets used by the Acrobat Sign service include:

- A core VPC/VNet supporting central Acrobat Sign business processes.
- A microservice VPC/VNet to support secondary services, such as digital signature integration with the Cloud Signature Consortium, signature validation and background removal of signature images.
- A utility services VPC/VNet to manage event monitoring and other administrative functions.

All these services run on scalable, secure virtual cloud servers that are accessible only as permitted by strict subnet and VPC/VNet network security restrictions.

To support high availability, VPC/VNet instances are divided into multiple, redundant availability zones (AZs). AZs are physically isolated from each other to ensure that power, network, or other infrastructure failures in one AZ do not affect operation in the others. All data is replicated across all AZs and across multiple servers within each AZ.

Network access within a VPC/VNet instance is locked down via security group rules. Similar to a virtual firewall, the security groups allow Adobe to further control inbound and outbound traffic to the VPC/VNet instance and to help ensure that only validated users are performing authorized actions. Additionally, the Acrobat Sign security architecture includes intrusion detection sensors at key locations to help ensure system integrity and visibility across the service.

Client Access

Acrobat Sign is accessible from a variety of client endpoints, including browsers, our REST API, and mobile apps. When a client connects to Acrobat Sign in its assigned region, it connects through an Internet gateway to a specific VPC/VNet. All client connections occur over HTTPS utilizing TLS v1.2 or higher with a minimum of AES 128-bit encryption.

Data encryption

Acrobat Sign 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 at rest can only be accessed with appropriate capability-based security permissions through the application data access layer in a private subnet. Acrobat Sign senders also have the option to add a private password to further secure a document.

Document encryption keys are stored and managed in a secure secrets management environment with restricted access requiring multifactor authentication.

Acrobat Sign email is normally sent via SMTPS and encrypted with TLS, using cipher suites with a minimum key length of 128 bits. However, since a small percentage of internet email providers do not support TLS encryption, email will be sent via unencrypted SMTP when necessary to ensure deliverability.

Identity Management

Acrobat Sign uses a role-based model for identity management that handles authentication, authorization, and access control throughout the Acrobat Sign solution. Capability-based security and authentication processes are defined and enabled for an organization by an Acrobat Sign administrator. Acrobat Sign defines general user roles including:

- **Sender**—Licensed user who is granted specific Acrobat Sign permissions by their administrator to create document-signing workflows and send documents for signature, approval or viewing.
- **Signer**—User who is provided access by a Sender to sign a specific document. By default, Acrobat Sign sends an email to the Signer that includes a unique URL to the document to be signed, which is comprised of exclusive identifiers specific to the transactions.
- **Approver**—User who is provided access by a Sender to approve a document.
- **Other**—Verified user who is provided specific access by a Sender to view a document or audit trail.

Licensed User Authentication

Acrobat Sign supports multiple methods to authenticate a user's identity, including both single- and multi-factor authentication.

Licensed users typically log into Acrobat Sign using one of the following authentication options:

- **Acrobat Sign ID**—A verified email address and password combination that is used by a licensed user to securely log in to an Acrobat Sign account.
- **Adobe ID**—An Adobe ID may be used to access all licensed Adobe services, including Acrobat Sign.
- **Single Sign-On (SSO)**—Enterprises seeking a tighter access-control mechanism can enable Security Assertion Markup Language (SAML) SSO to manage Acrobat Sign users through their corporate identity system.

Administrators may also choose to configure password strength and complexity, frequency of change, past password comparison, and lockout policies (such as login renewal expiration).

Location of Licensed User Identity Data

Licensed user identity data is stored within the same data center associated with the customer's geographical location. Typically, Acrobat Sign customers use Adobe Identity Management Services and the Adobe Admin Console for user management.

In this scenario, user identity data is also replicated in highly available data centers located in US-East (Virginia), US-West (Oregon), EU-West (Ireland), and SG-1 (Singapore).

Signer Identification

Depending on the type of signer (internal or external), the method and type of e-signature signers use to identify themselves can vary. Because most users have unique access to one email account, basic identification to Acrobat Sign typically occurs when an originator sends an email requesting a document signature to a specific individual.

To build on the security and help protect the integrity of e-signed documents, customers can require additional identity verification methods to confirm the identity of the signer, such as telephone, SMS, knowledge-based authentication (KBA), digital certificates, Government ID verification, or BankID/eID verification. Alternatively, customers can add other digital identity solutions, depending on availability in the customer's geographical location.

Acrobat Sign also offers many third-party digital identity solutions from providers with verified integrations to the Acrobat Sign Digital Identity Gateway or that Cloud Signature Providers that use the Cloud Signature Consortium (CSC) technical standard.

More information on digital identity solutions integrated into Acrobat Sign can be found on the Adobe Trust Center.

Acrobat Sign Document Certification

At each stage in the workflow, Acrobat Sign secures the document to help ensure both document integrity and proof of origin. Acrobat Sign uses public key infrastructure (PKI) to certify final signed PDF documents and audit trails with a digital signature before distribution of the document to a recipient.

The certification signature is created with the SHA-256 hashing algorithm that calculates a unique cryptographic fingerprint from the final signed PDF. Displayed graphically as a blue banner with a certification badge at the top of the final signed PDF, this digital signature

helps verify document integrity (see Figure 4 below), gives assurance that the document was generated within Acrobat Sign, and provides a final tamper-evident document. The final certified PDF can be further secured with a password, if the user requires additional document confidentiality.

Figure 4: Acrobat Sign Document Certification Banner

To generate the keys used to lock and certify the final signed PDF, Acrobat Sign uses certificates issued by trusted certificate authorities (CAs) and timestamp authorities (TSAs). In certain circumstances, administrators can configure Acrobat Sign to apply the certification signature using a specific certificate based on regional or compliance requirements. PKI keys used to certify the final PDF are stored in hardware security modules to meet the highest level of security and compliance.

Acrobat Sign Hosting and Security

The Acrobat Sign service infrastructure resides in American National Standards Institute (ANSI) Tier 4 data centers managed by our trusted cloud hosting providers, Amazon Web Services (AWS) and Microsoft Azure. Adobe's cloud service infrastructure partners maintain very strict controls around data center access, fault tolerance, environmental controls, and network security. Only approved and authorized Adobe employees, cloud service provider employees, and contractors with a legitimate, documented business are allowed access to the secured sites.

For more information on worldwide hosting locations, please see Adobe Acrobat Sign data centers.

Acrobat Sign Compliance

Industry and Regulatory Standards

As a global e-signature solution designed for verified signers to interact with digital documents from most any location or device, Acrobat Sign can be configured to help customers meet compliance requirements for many industry and regulatory standards. Customers maintain control over their documents, data, and workflow and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU, Health Information Protection Act (HIPAA) in the U.S., and FDA CFR 21 Part 11 (also in the U.S.). For more information on Adobe privacy policies, please see the Adobe Privacy Center.

To learn more about e-signature laws in a specific region and information about Acrobat Sign compliance, please see the Adobe Trust Center.

FedRAMP

Acrobat Sign is FedRAMP authorized at the Tailored level. Acrobat Sign for Government is authorized at the Moderate level and is hosted on Microsoft Azure Government Community Cloud. It is designated for the sole use of U.S. federal, tribal, state, and local government customers, as well as U.S. government contractors.

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.

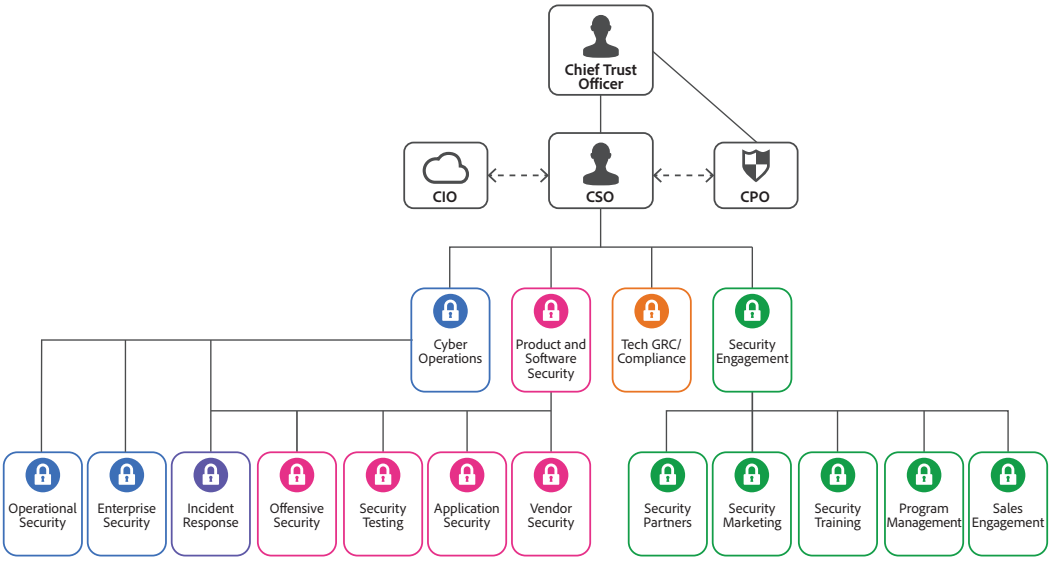

Figure 6: The Adobe Security Organization

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.

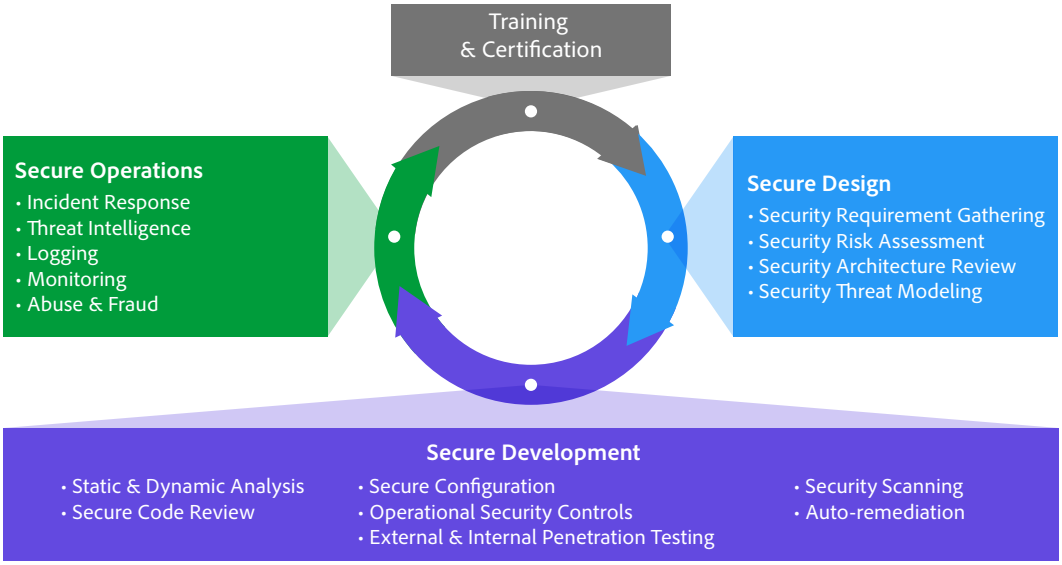

Figure 7: The Adobe Secure Product Lifecycle

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.

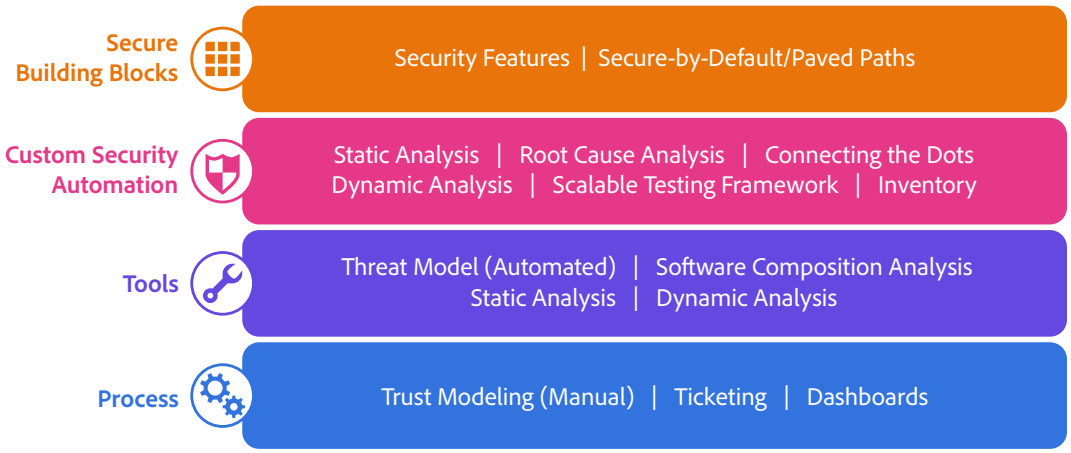

Figure 8: The Adobe Application Security Stack

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. 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.

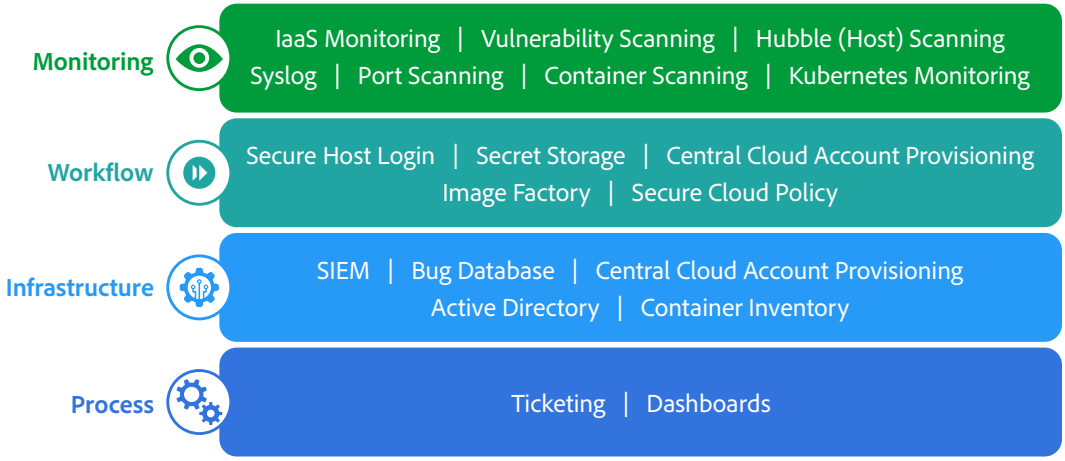

Figure 9: The Adobe Operational Security Stack

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 Acrobat Sign 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.

10/23