Adobe Connect Security Overview

Meeting your most demanding security requirements and providing a secure foundation for building your solutions

At Adobe, security is our highest priority. From the rigorous integration of security into our internal software development processes and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What's more, our collaboration with partners, researchers, and other industry organizations helps us understand the latest security best practices and trends to continually integrate best of breed security practices into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of your Adobe Connect Multi-tenant Hosted or Adobe Connect Managed Services private cloud experience and associated data.

CONTENTS

About Adobe Connect

Adobe Connect is a secure web conferencing platform that offers immersive online meeting experiences for virtual classrooms, collaboration, and large-scale webinars. Powering end-to-end, mission-critical web conferencing solutions on desktops and devices, Adobe Connect enables organizations to fundamentally improve productivity through collaboration. Adobe Connect is available in two primary deployment options:

Adobe Connect Hosted Multi-tenant, which serves as a SaaS offering in a shared cloud deployment.

Adobe Connect Managed Services (ACMS), which uses the Amazon Web Services (AWS) cloud infrastructure in a private cloud deployment. Each ACMS customer has private images provisioned for their Adobe Connect application, database, and storage.

The option to deploy Adobe Connect on-premise is also available.

Adobe Connect Solution Components

Adobe Connect includes two components, the Adobe Connect application suite and the Adobe Connect Server. All deployment options require both components, however, the location of the Adobe Connect Server changes based on the chosen deployment option (hosted, managed service, or on-premise).

ADOBE CONNECT APPLICATION SUITE

Adobe Connect Meeting - Conduct online meetings, webinars, and virtual classrooms with voice-over-IP, PowerPoint presentations, screen sharing, chat, polling, whiteboards, webcams, MP4 video playback, moderated Q&A, and more.

Adobe Connect Training - Create, manage, deploy, and track eLearning courses and curricula, complete with support for standard learning content formats, enrollment tracking capabilities, learner management, and reporting.

Adobe Connect Events - Manage the full lifecycle of large and small-scale events through highly customized landing pages, email notification, event catalogs, registration management, reporting, and analytics.

Adobe Connect Central – Administrative portal to create meetings, manage presentations, create courses and curricula, author and publish events, view and download reports, and more.

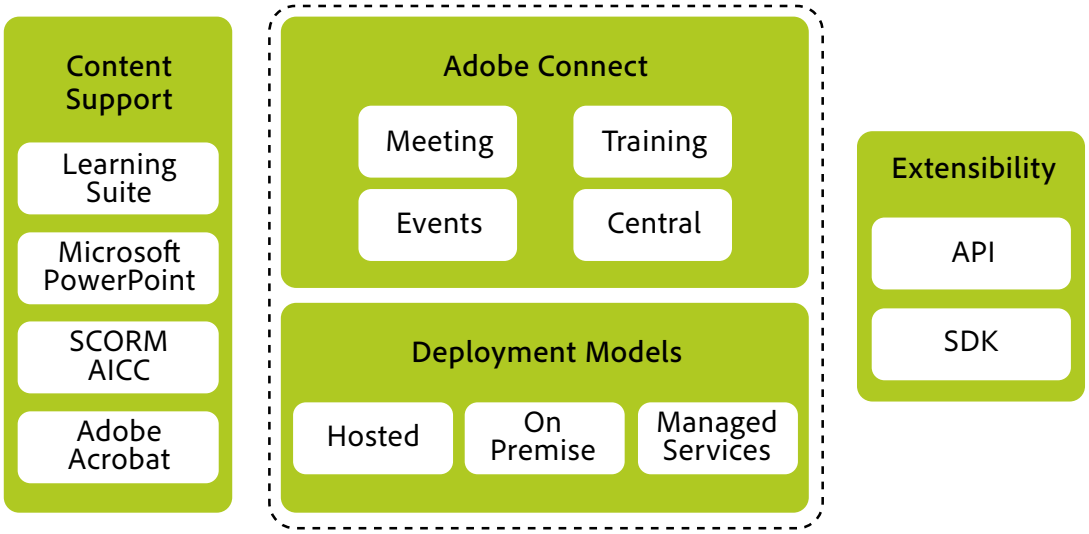

Figure 1: Adobe Connect Product Architecture

ADOBE CONNECT SERVER

Adobe Connect Server is an open platform server that delivers enterprise-class scalability with support for clustered environments and provides the reliability and redundancy needed to seamlessly support thousands of concurrent users.

In addition to the four Adobe Connect software solutions, you can also publish training content and multimedia presentations directly to an Adobe Connect Server from Adobe Captivate®. What's more, since Adobe Connect Server is an open platform, you can extend and integrate it with other, non-Adobe systems through a comprehensive set of APIs and a software development kit (SDK).

Adobe Connect Server Architecture

As a multi-tier server, Adobe Connect Server separates logical functions across independent processes. .

APPLICATION SERVER

Adobe Connect is a stand-alone Java application that embeds Apache as its web server. It can be installed as a service or run from the command line. Adobe Connect also embeds Tomcat as its application server, which contains and executes all the business logic necessary to deliver content, manages users, groups, on-demand content, and client sessions, among other tasks. Some of the application server's specific duties include access control, security, compliance, quotas, and licensing, as well as auditing and management functions, such as clustering, fail-over, and replication. It also transcodes media, such as Microsoft PowerPoint and Adobe PDF, to a format that allows viewing without the original application.

STREAMING COMMUNICATION SERVER

Adobe Connect Server includes two distinct streaming solutions.

The first, for rooms using Standard Audio/Video, is an embedded instance of Adobe Media Server that acts as the meeting server. This component handles all the real-time streaming of audio and video, synchronization of data, and delivery of rich media content. Adobe Media Server also plays a vital role in reducing server load and latency by caching frequently accessed streams and shared data. Adobe Media Server uses the Real-Time Messaging Protocol (RTMP) but can also be configured to use Secure Sockets Layer (SSL) for increased data security.

In addition, Adobe Connect offers another streaming solution using the latest WebRTC framework for providing enhanced Audio and Video capabilities. This Enhanced Audio-Video setup typically runs on multiple Linux nodes that have specific roles. There are signaling nodes, media nodes, and recording nodes. This setup also uses PostgreSQL and Redis databases that can be installed on one or separate machines depending on the usage.

DATABASE

The Adobe Connect Server database persistently stores transactional and application metadata, including user, group, content, and reporting information. Adobe Connect Server can use either the embedded database engine (Microsoft SQL Server Express) or the full version of Microsoft SQL Server. Check the Adobe Connect system requirements for the most up-to-date information.

When deploying Adobe Connect Server in a cluster, the full version of Microsoft SQL Server must be used and cannot be installed on the same computer as the Adobe Connect Server. Standard cluster and hot-swap configurations for a Microsoft SQL Server are supported for scalability and failover.

HTML AUTHORING/PUBLISHING

Adobe Connect Server uses Adobe Experience Manager (AEM), a web content management system, to create and manage HTML-based templates used for event email notifications, landing pages, and user self-registration. Users can also author and subsequently publish web pages using AEM. AEM requires at least one author and one publisher instance within the Adobe Connect Server deployment when the Adobe Connect Events module is enabled. All web-page authoring is done in the Adobe Experience Manager author instance and replicated in the publish instance. The publish instance is the read-only view of the web pages that have been authored in the Adobe Experience Manager author instance. Multiple Adobe Experience Manager author and publish instances can be configured behind a Dispatcher within a server cluster, to provide increased security, scalability, and failover, as well as to leverage the caching and load balancing capabilities provided by that component.

ANALYTICS

Adobe Connect provides a range of out-of-the-box reports as well as custom reports that can be configured by customers. Optionally, Adobe Analytics can be used with either Adobe Connect Hosted Multi-tenant or Adobe Connect Managed Service deployments to provide more robust reporting and analytics for Adobe Connect events. These analytics reports track viewing of landing pages, responses to registration questions, attendance, participation in polls, Q&A, and file download activity during meetings.

MEDIA TRANSCODING

Adobe Connect Server provides several file conversion utilities to automatically convert popular document formats into high-quality files to display in the meeting room. It converts the PowerPoint file format (e.g., .ppt and .pptx) into bitmap image files, providing a high-quality, resolution-independent display for all participants. The conversion also accurately reproduces hyperlinks and virtually all the original animations contained within each slide.

Each Adobe Connect client pre-caches the individual slides when they are loaded into a meeting room, using minimal bandwidth to maintain synchronization across all users and ensuring the lowest latency transitions. Adobe Connect Server displays animations exactly as they appear in the original slides and keeps all hyperlinks clickable. Other supported file formats, such as PDF, are similarly converted.

Adobe Connect Data Flow

When using Standard audio/video meetings, Adobe Connect uses the HTTP, HTTPS, WS, WSS, RTMP, and RTMPS protocols. RTMP is optimized to deliver real-time, rich media streams. RTMPS is the secure implementation of RTMP.

With Enhanced Audio/Video the goal is to ensure high throughput, low latency communication for Adobe Connect users that may (or may not) be behind restrictive firewall rules.

The following is the preferred precedence of network communication protocols between an Adobe Connect Client and Adobe Connect Media server:

UDP - Direct flow between Client and Media servers using the STUN based discovery.

UDP - Indirect (relayed) between Client and Media servers using the TURN server embedded in Connect Media server.

TCP - Indirect (relayed) between Client and Media servers via the TURN server embedded in Connect Media server using TCP.

TCP/TLS - Indirect (relayed) between Client and Media servers via the TURN server embedded in Connect Media server using TCP with an extra layer of encryption.

When using SIP, UDP and TCP are used for registration and calling.

The data flow paths for connections between both the Adobe Connect client for desktop browsers and the Adobe Connect HTML client and the Adobe Connect Server are described in this section.

Adobe Connect Client Connections

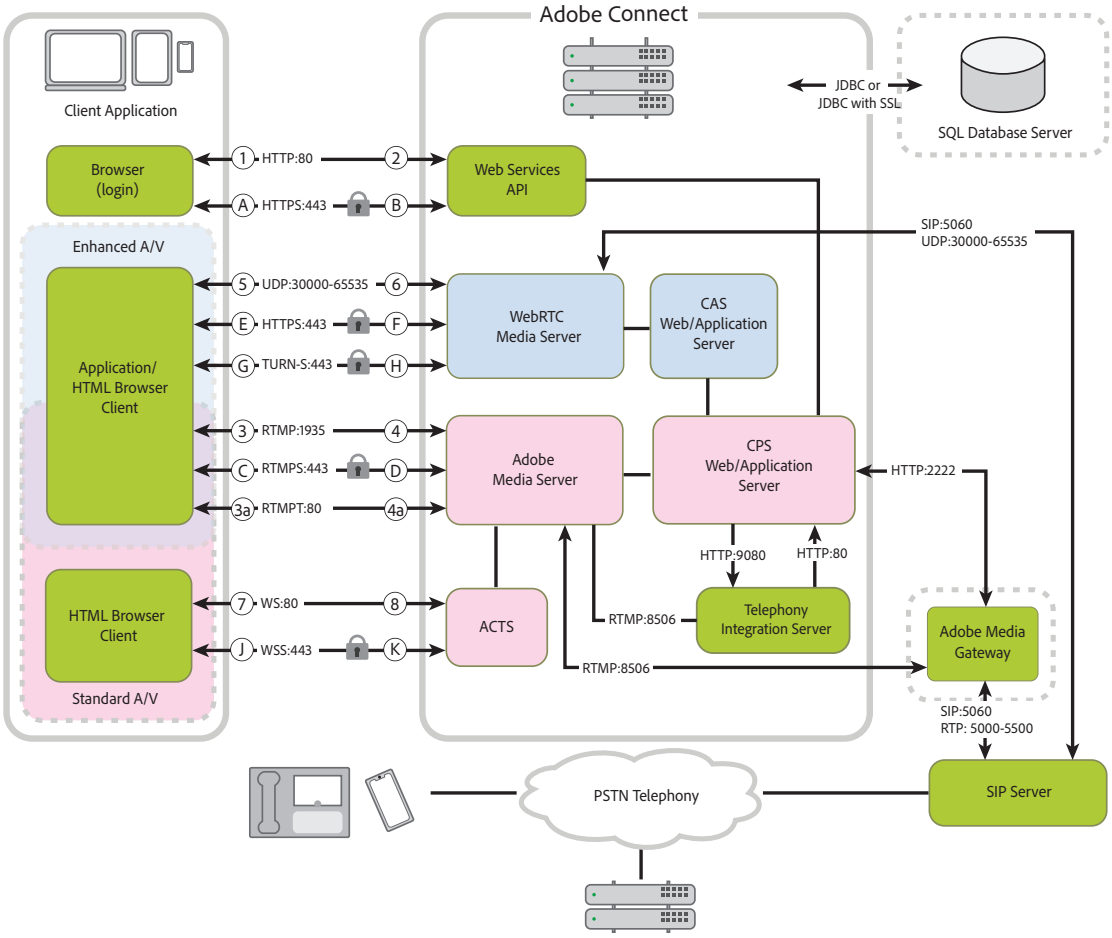

Figure 2: Adobe Connect data flow

UNENCRYPTED CONNECTIONS

In principle, Adobe Connect allows the use of unencrypted connections with the HTTP, RTMP or UDP protocols and follow the paths indicated by the associated numerals (e.g., 1, 2, 3, etc.) in the Adobe Connect Data Flow Diagram above. However, both the Adobe Connect Hosted Multi-tenant and ACMS deployments force clients to make secure connections by default, thereby ensuring encryption of data in transit.

1. The Adobe Connect client requests a meeting or content URL over HTTP:80.
2. The web server responds and transfers the content or provides the Adobe Connect client with information to connect to the meeting.

STANDARD MEETING CONNECTION USING AN APPLICATION

3. The Adobe Connect client requests a connection to the meeting over RTMP:1935.

3a. The Adobe Connect client requests a connection to the meeting but can only connect over RTMPT:80.

4. Adobe Media Server responds and opens a persistent connection for Adobe Connect streaming traffic.

4a. Adobe Media Server responds and opens a tunneled connection for Adobe Connect streaming traffic.

ENHANCED MEETING ADDITIONAL CONNECTIONS USING EITHER APPLICATION OR BROWSER

5. The Adobe Connect client requests a connection to the meeting over UDP: 30000-65535.

6. The Adobe WebRTC Media Server responds and opens a persistent connection for Adobe Connect streaming traffic.

STANDARD MEETING CONNECTION USING A BROWSER

7. The Adobe Connect browser client requests a connection to the meeting over WS:80.

8. The Adobe Connect Transmuxing Server (ACTS) responds and opens a persistent connection for Adobe Connect streaming traffic.

ENCRYPTED CONNECTIONS

Adobe Connect encrypted connections use HTTPS and RTMPS or TURN-S and follow the paths indicated by the associated letters (e.g., A, B, C, etc.) in the Adobe Connect Data Flow Diagram above.

A. The Adobe Connect client requests a meeting or content URL over a secure connection on HTTPS:443.

B. The web server responds and transfers the content over a secure connection or provides the Adobe Connect client with information to securely connect to the meeting.

STANDARD MEETING CONNECTION USING AN APPLICATION

C. The Adobe Connect client requests a secure connection to Adobe Media Server over RTMPS:443.

D. Adobe Media Server responds and opens a secure, persistent connection for Adobe Connect streaming traffic.

ENHANCED MEETING CONNECTION USING EITHER APPLICATION OR BROWSER

E. The Adobe Connect client requests a meeting or content URL over a secure connection on HTTPS:443.

F. The web server responds and transfers the content over a secure connection or provides the Adobe Connect client with information to securely connect to the meeting.

G. The Adobe Connect client requests a connection to the meeting over TURN-S:443.

H. The Adobe WebRTC Media Server responds and opens a persistent connection for Adobe Connect streaming traffic.

STANDARD MEETING CONNECTION USING A BROWSER

J. The Adobe Connect browser client requests a connection to the meeting over WSS:443.

K. The Adobe Connect Transmuxing Server (ACTS) responds and opens a persistent connection for Adobe Connect streaming traffic.

DATA ENCRYPTION

As information flows between Adobe Connect client applications and the Adobe Connect Server, industry standard data encryption methods safeguard the confidential information contained within the traffic. Adobe Connect uses SHA-256 hashing with a random salt to store passwords in the database, in addition to encrypting all other sensitive application data in both the database and file system using AES-256.

Adobe Connect Hosted Multi-tenant - provides encryption in transit with a single key for all customers, using Transport Layer Security (TLS) encryption 1.2 and 1.3.

Adobe Connect Managed Services - provides both encryption in-transit as well as encryption at rest using AES-256. For volume encryption - each customer is assigned a unique key. The customer can determine the version of TLS that is most appropriate for their needs.

Adobe Connect Security Architecture

ADMINISTRATOR FEATURES

Customers control users, content, access, and features through the administration controls of Adobe Connect. Customers retain ownership of their content and data. The compliance and control settings are account-wide settings that broadly consist of the following:

- Disable undesired functionality - Administrators can turn off certain functional modules as needed.
- Disable screen sharing - Administrators can prevent sharing of desktop, windows, or applications. They can also restrict screen sharing to specific applications or prevent specified applications from being shared.
- Record and retain communications for auditing purposes - Administrators can force recordings for all meetings, log all chat messages in files, and show a notice or disclaimer to all participants. Recordings can be prevented from public access or be disabled entirely for all meetings.
- Control access to meetings - Administrators and hosts can completely disable guest access so that guests can no longer request entry. Hosts can also automatically deny access to specific users and groups. Unlike the previous two categories, meeting access control settings are enforced on a per-meeting basis rather than for the entire system or hosted account.

An administrator or limited administrator can also customize the permissions list for a file or folder. These permissions include:

- Manage - Users or groups with Manage permission for a folder or file can view, delete, move, and edit the file or folder. They can also view reports for files in that folder, set permissions for the file or folder, and create new folders. However, they cannot publish to that folder.
- Denied - Users or groups with a Denied permission setting for a folder or file cannot view, publish, or manage this folder or file.
- Publish - Users or groups with a Publish permission setting for a folder or presentation can publish, update, and view presentations, as well as view reports for files in that folder. However, these users must also be members of the Built-in Author group, as well as have Publish permission, to publish content to this folder.
- View - Users or groups with a View permission setting for a folder or file can view any content in the folder or an individual file.

Administrators can allow or force meeting hosts to require a passcode for Adobe Connect sessions.

Adobe Connect User Authentication

Adobe Connect uses standard access control lists with password policy options and Transport Layer Security (TLS) encryption to secure access, content, and data.

PASSWORD POLICIES

Passwords can be set to expire after a period of days, as well as require certain characters. Administrators can mandate that a password include a number, a capital letter, and/or a special character as well as require passwords to be of a minimum and/or a maximum length. In addition, old passwords can be tracked to prohibit reuse.

Users can reset their passwords to create their own passwords based on the password policy set by the account administrator. Administrators can mandate a password change or set a temporary password for any user. Meeting hosts can lock out new participants, expel current participants, disable remote control, and disable the ability of participants to change their displayed name.

Administrators can configure the number of old passwords that can be tracked. Adobe Connect allows administrators to provision user accounts in several ways:

1. Manual provisioning through the use of a .csv file
2. Using the Adobe Connect Events module for self-registration
3. Using the webservice API
4. For Adobe Connect Managed Services, using LDAP/AD synchronization

If a user incorrectly enters a password five (5) times, the account can either be locked out for five (5) minutes, or suspended until reset by an administrator. The user is notified by email that the account has been temporarily suspended. It is possible to change these values and procedures with customization.

Authentication takes place on the login screen of the Adobe Connect client or through the webservice API. For Adobe Connect Managed Services, administrators can also enable HTTP header authentication as well as LDAP/AD authentication.

SINGLE SIGN-ON

Adobe Connect provides support for Security Assertion Markup Language (SAML). This feature must be enabled by a request to Adobe Customer Support. In addition, several of Adobe's trusted partners have developed custom solutions for single sign-on (SSO) for all deployment models. These solutions take advantage of the open and published webservice API.

For Adobe Connect Managed Services and on-premise deployments, HTTP header authentication and login page customization for the purpose of redirection, and LDAP synchronization and authentication are also available. Adobe Connect Central handles application and service entitlement. More information is available here.

Adobe Connect Hosted Multi-tenant Data Centers

Adobe focuses on securing data collection, serving, and reporting activities over the Adobe Connect network. To this end, the network architecture for this Adobe-hosted implementation leverages industry best practices for security design, including segmentation of development and production environments, DMZ segments, hardened bastion hosts, and unique authentication.

Adobe Connect Hosted is deployed in a shared cloud (multi-tenant) environment, utilizing Amazon Web Services (AWS) servers distributed across four (4) global locations. The data centers supporting the environments are located in the United States (2), Ireland, and Australia.

Adobe generally hosts each customer in a data center located in the customer's corresponding region. For Adobe Connect Hosted Multi-tenant, multiple customer accounts reside on the same cluster of servers.

Figure 3: Adobe Connect hosted multi-tenant data center locations

Adobe Connect Managed Services Data Centers

Adobe relies upon certified cloud infrastructure providers to operate, manage, and control the components from the hypervisor virtualization layer down to the physical security of the facilities in which Adobe Connect Managed Services operates. These providers also operate the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. This infrastructure includes facilities, network, and hardware, as well as operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources. Adobe requires these providers to adhere to industry-standard practices as well as a variety of security compliance standards.

Adobe Connect Managed Services data centers are in five (5) locations around the world: USA (3), and Ireland, and South Africa.

Data Center Security

Data Protection, Monitoring, and Availability

SEGREGATING CLIENT DATA

The Adobe Connect Hosted Multi-tenant service relies on application permissions to isolate one customer from another. The only external access to these servers and databases is via secure access using the Adobe Connect application, or a web browser. All direct access to the servers is made only by authorized Adobe personnel and is conducted via encrypted channels over secure management connections. Adobe also separates its corporate testing environments from its production environments to avoid use of customer data in testing environments.

DATA STORAGE AND BACKUP

Adobe backs up customer data for Adobe Connect on a daily basis for disaster recovery purposes. These backups are also replicated to a hot failover site that is geographically removed from the primary data center. Adobe tests backups quarterly. The combination of backup procedures provides quick recovery from short-term backup as well as off-site protection of data.

By default, Adobe stores all active customer content using high-durability storage services provided by its cloud infrastructure partners, also leveraging the file-system-consistent, durable, and incremental backup capabilities they offer. This includes point-in-time snapshots.

ACCESS CONTROLS

Only authorized users within the Adobe intranet or remote users who have completed the multi-factor authentication process to create a VPN connection can access administrative tools. In addition, Adobe logs all server connections for auditing.

LOGGING

To protect against unauthorized access and modification, Adobe captures network logs, OS-related logs, and intrusion detections. Sufficient storage capacity for logs is identified, periodically reviewed, and as needed, expanded to help ensure that log storage is not exceeded. Systems generating logs are hardened and access to logs and logging software is restricted to authorized Adobe Digital Marketing Information Security Team personnel.

SECURE MANAGEMENT

Adobe deploys dedicated network connections to enable secure management of Adobe Connect. All management connections to the servers occur over encrypted Secure Shell (SSH), Secure Sockets Layer (SSL), or Virtual Private Network (VPN) channels and remote access always requires two-factor authentication. Unless the connection originates from a list of trusted IP addresses, Adobe does not allow management access from the Internet.

CHANGE MANAGEMENT

Adobe Connect follows a Change Approval Board (CAB) process for all changes that could impact customer experience. The CAB process focuses upon enforcing stability and availability, while permitting an agile response to emerging issues and providing internal process transparency and accountability.

The Adobe Connect release schedule is typically one major release every 12 to 18 months, with a minor release following the major release by six months and patches as needed.

While most maintenance does not require downtime, when it does, a typical downtime maintenance window will fall during low load periods for the regions in question (e.g. Sunday 9 PM PST for North America, Friday 11 PM-GMT for EMEA, and Saturday 12 AM AEST for APAC). Adobe Connect maintenance windows that include downtime are scheduled on an as-needed basis and are typically used for more involved maintenance (major releases) that will require part of the system to be unavailable for a number of hours. There is no option for delaying or scheduling maintenance on the hosted service. All patches, updates, and hotfixes are tested prior to deployment. Prior to deployment, manager approval is required.

All Adobe certified cloud service providers are responsible for authorizing, logging, testing, approving, and documenting routine, emergency, and configuration changes to existing infrastructure in accordance with industry norms for similar systems. Providers schedule updates to minimize any customer impact.

PATCH MANAGEMENT

To automate patch distribution for Adobe Connect components, Adobe uses internal patch and package repositories as well as industry-standard patch and configuration management. Depending on the role of the host and the criticality of pending patches, Adobe distributes patches to hosts at deployment and on a regular patch schedule. If required, Adobe releases and deploys emergency patch releases on short notice.

Adobe cloud infrastructure providers maintain responsibility for patching systems that support the delivery of IaaS services, such as the hypervisor and networking services.

FIREWALLS AND LOAD BALANCERS

Adobe Connect clusters rely on Web Application Firewalls offered by the cloud service provider to monitor and block/allow web requests based on specific criteria - such as originating IP addresses or the values of query strings, etc. Qualifying requests are forwarded to Application Load Balancers to be distributed across different clusters. In addition, the WAF also enforces rate-based rules to protect the application against DDoS attacks. The rules also deny all internet connections except those to authorized ports for the relevant protocols: port 80 for HTTP/RTMPT, port 443 for HTTPS/RTMPS, port 1935 for RTMP, etc.

NON-ROUTABLE, PRIVATE ADDRESSING

All Adobe servers containing customer data are configured with non-routable IP addresses (RFC 1918). These private addresses, combined with firewalls and NAT, help prevent an individual server on the network from being directly addressed from the Internet, greatly reducing the potential vectors of attack.

INTRUSION DETECTION

Both network intrusion detection and host intrusion detection (NIDS and HIDS) are integrated into our centralized security incident and event management system (SIEM) and are continuously monitored by the Digital Marketing Information Security Team. The security team follows up on intrusion notifications by validating the alert and inspecting the targeted platform for any sign of compromise. Adobe regularly updates all sensors and monitors them for proper operation.

NETWORK MONITORING

Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points. Adobe ensures its infrastructure providers offer protection against traditional network security issues, including:

- Distributed Denial of Service (DDoS) attacks
- Man-in-the-Middle (MITM) attacks
- IP Spoofing
- Port Scanning
- Packet sniffing by other tenants

Adobe monitors all its servers, routers, switches, load balancers, and other critical network equipment on the Adobe Connect network 24 hours a day, 7 days a week, 365 days a year. The Adobe Network Operations Center (NOC) receives notifications from the various monitoring systems and will immediately attempt to fix an issue or escalate the issue to the appropriate Adobe personnel. Additionally, Adobe contracts with multiple third parties to perform external monitoring.

Risk & Vulnerability Management

PENETRATION TESTING

Adobe conducts internal penetration tests performed by Adobe researchers as well as external penetration tests performed by leading third-party security firms that can uncover potential vulnerabilities and improve the overall security of Adobe products and services.

In addition, Adobe also collaborates with the broader security community to encourage the finding and disclosure of security issues privately and in a manner that minimizes risk to both Adobe and its customers.

Upon receipt of any report provided by these testers, Adobe documents these vulnerabilities, evaluates their severity, considers their priority, and then creates a mitigation strategy or remediation plan. Please review our white paper on secure engineering practices for more information.

INCIDENT RESPONSE AND NOTIFICATION

New vulnerabilities and threats evolve each day and Adobe strives to respond to 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. You can learn more about our incident response programs and systems on Adobe.com.

FORENSIC ANALYSIS

For incident investigations, the Adobe Connect team adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe holding, and chain-of-custody recording.

CUSTOMER DATA CONFIDENTIALITY

Adobe treats customer data as confidential. Adobe does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy. Adobe Systems Incorporated also certifies to the Privacy Shield Framework.

Adobe publishes details about our GDPR compliance on our website.

Adobe Security Organization

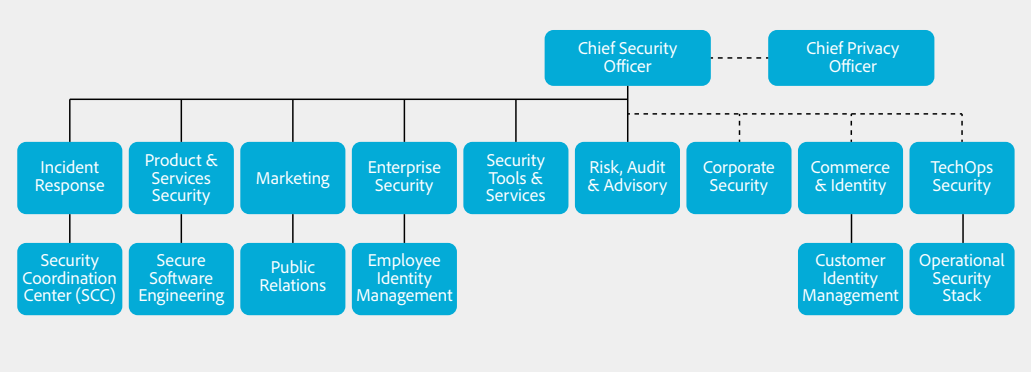

Figure 4: Adobe Security Organization

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 experts who serve as consultants to key Adobe product and operations teams, including the Adobe Connect team. ASSET researchers work with individual Adobe product 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.

ADOBE SECURE PRODUCT DEVELOPMENT

As with other key Adobe product and service organizations, the Adobe Connect organization employs the 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. ASSET security researchers provide specific SPLC guidance for each 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.

ADOBE SECURE PRODUCT LIFECYCLE

A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC was designed from the ground up to help keep your information safe and secure when you use Adobe products and services and is integrated into multiple stages of the product lifecycle. Adobe's SPLC must meet the standard of due care that is reasonably expected by customers, shareholders, partners, Adobe workers, and the business itself within the product lifecycle. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape. Please review our secure engineering white paper for more information about the Adobe SPLC.

Adobe Software Security Certification Program

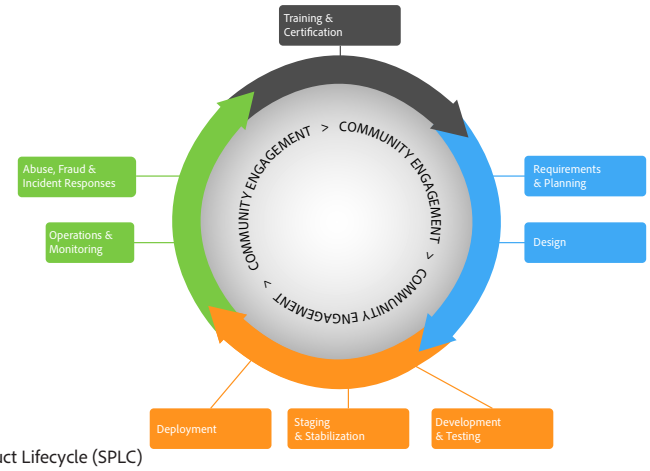

Figure 5: Adobe Secure Product Lifecycle (SPLC)

As part of the Adobe SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects.

The program has four levels, each designated by a colored 'belt': white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months- or year-long hands-on security projects. Employees attaining brown and black belts become security champions and experts within their product teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages. You can learn more about our security certification program here on Adobe.com.

Various teams within the Adobe Connect organization participate in additional security training and workshops to increase awareness of how security affects their specific roles within the organization and the company as a whole.

Adobe Employees

Adobe maintains employees and offices around the world and implements the following processes and procedures company-wide to protect the company against security threats:

EMPLOYEE ACCESS TO CUSTOMER DATA

Adobe maintains segmented development and production environments for Adobe Connect, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

BACKGROUND CHECKS

Adobe obtains background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background, work history, court records, including criminal conviction records and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Current Regulations and Compliance for Adobe Connect Hosted Multi-tenant

SOC 2 is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Connect Hosted is compliant with SOC 2-Type 2 (Security & Availability).

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 Connect Hosted is compliant with ISO 27001:2013.

The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions safeguard their customers' personal data. Adobe Connect Hosted is "GLBA-ready," meaning that it enables our financial service customers to comply with the GLBA Act requirements for using service providers. Ultimately, the customer is responsible for ensuring compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

Current Regulations and Compliance for Adobe Connect Managed Services

SOC 2 is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Connect Managed Services is compliant with SOC 2-Type 2 (Security & Availability).

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 Connect Managed Services is compliant with ISO 27001:2013.

The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions safeguard their customers' personal data. Adobe Connect Managed Services is GLBA-Ready, meaning that it enables our financial 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 Federal Risk and Authorization Management Program (Fed RAMP) 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 is compliant with Fed RAMP.

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 is HIPAA-compliant, which means it 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 solution 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 is FERPA-Ready.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Adobe Connect solution and your confidential data. At Adobe, we take the security of your digital experiences very seriously and we continuously monitor the evolving threat landscape to stay ahead of malicious activities. For more information, please visit: https://trust.adobe.com.

Adobe Systems Incorporated
345 Park Ave.
San Jose, CA 95110-2704
www.adobe.com