Adobe Document Cloud

Adobe

WHITE PAPER

Panoramica sulla sicurezza di Adobe Acrobat con servizi Document Cloud

Indice

Sicurezza di Adobe 3

Panoramica di Acrobat con servizi Document Cloud 3

Esperienze utente basate su Acrobat 3

Servizi Document Cloud 4

Funzionalità di protezione dei documenti di Acrobat 4

Sicurezza dei servizi Adobe Document Cloud 7

Integrazioni tra Acrobat e Microsoft 8

Panoramica del programma di sicurezza Adobe 10

L'organizzazione della sicurezza targata Adobe 10

La procedura Secure Product Lifecycle di Adobe 11

Sicurezza delle applicazioni Adobe 12

Sicurezza operativa Adobe 13

Sicurezza aziendale Adobe 13

Conformità Adobe 14

Risposta in caso di incidenti 14

Continuità aziendale e disaster recovery 14

Conclusione 15

Sicurezza di Adobe

Noi di Adobe sappiamo che la sicurezza delle esperienze digitali è importante. Le pratiche di sicurezza sono profondamente radicate nei nostri strumenti e processi operativi interni e di sviluppo del software, e vengono seguite rigorosamente allo scopo di prevenire, rilevare e rispondere in modo tempestivo a eventuali incidenti. Inoltre, la nostra collaborazione con partner, importanti ricercatori, istituti di ricerca sulla sicurezza e altre organizzazioni del settore ci aiuta a rimanere sempre aggiornati sulle minacce e le vulnerabilità più recenti, consentendoci così di incorporare regolarmente tecniche di sicurezza avanzate nei prodotti e nei servizi che offriamo.

Questo white paper descrive l'approccio di "difesa dettagliata" e le procedure di sicurezza adottate da Adobe per rafforzare il livello di protezione di Adobe Acrobat con servizi Document Cloud e dei dati associati.

Panoramica di Acrobat con servizi Document Cloud

Acrobat con servizi Document Cloud è la soluzione PDF più completa per il mondo multidispositivo e connesso di oggi. Utilizzando il software desktop Acrobat e l'app mobile Adobe Acrobat Reader (potenziata con funzionalità avanzate pensate per i dispositivi mobili) con i servizi Document Cloud, le organizzazioni possono sviluppare flussi di lavoro più intelligenti e soddisfare l'esigenza di soluzioni mobile per gli utenti finali, garantendo allo stesso tempo la sicurezza dei documenti sui vari dispositivi.

Acrobat con servizi Document Cloud consente ai clienti di convertire praticamente qualsiasi contenuto in un documento elettronico da condividere con altri e di automatizzare facilmente la generazione, la manipolazione e la trasformazione di file PDF a partire da qualsiasi servizio cloud, applicazione desktop o app mobile Adobe.

Esperienze utente basate su Acrobat

I clienti possono utilizzare i servizi di Document Cloud in un'ampia gamma di esperienze utente basate su Acrobat:

- Acrobat Pro – Applicazione desktop per utenti che lavorano su laptop e PC
- Acrobat online – App web disponibile all'interno di browser supportati su PC e dispositivi mobili, tra cui Chrome, Microsoft Edge, Firefox e Safari
- Client Acrobat Reader per dispositivi mobili – App scaricabile gratuitamente da Apple App Store e Google Play per utenti che lavorano su dispositivi mobili e tablet

Adobe ha anche integrato Acrobat in diversi strumenti di produttività di Microsoft. Con queste integrazioni, l'archiviazione dei documenti funziona in modo diverso rispetto a quanto avviene nell'applicazione autonoma Acrobat. Le informazioni sulla sicurezza di ciascuna integrazione sono riportate in dettaglio nella sezione "Integrazioni tra Acrobat e Microsoft".

Servizi Document Cloud

I servizi Adobe Document Cloud comprendono:

- Invia PDF – Consente di inviare un PDF a un destinatario utilizzando un client di posta elettronica.
- Organizza PDF – Consente di inserire, eliminare, ruotare o riordinare le pagine in un PDF.
- Crea PDF – Consente di convertire documenti di Word, Excel e PowerPoint, nonché immagini o foto, in file PDF.
- Esporta PDF – Consente di convertire i PDF in file Microsoft Word, Excel, PowerPoint o RTF modificabili.
- Modifica PDF – Consente di modificare facilmente i PDF esistenti da un dispositivo mobile o laptop.
- Combina PDF – Consente di combinare più file in un unico documento PDF e di predisporre pacchetti di documenti provenienti da fonti diverse.
- Fill & Sign – Consente di completare un modulo e aggiungere una firma.
- Adobe Scan – Consente di acquisire e convertire qualsiasi documento in un PDF ricercabile di alta qualità.
- Adobe Acrobat Sign – Consente di preparare e inviare documenti per raccogliere firme elettroniche affidabili su qualsiasi dispositivo moderno, da firme semplici a firme digitali nel cloud.

Adobe aggiunge continuamente nuove offerte ai servizi di Document Cloud. L'elenco aggiornato di tutti i servizi Document Cloud è disponibile sul sito Adobe.com.

Funzionalità di protezione dei documenti di Acrobat

Redazione

I servizi Adobe Document Cloud offrono un insieme di strumenti per la redazione che consentono di proteggere le informazioni riservate o confidenziali. Ad esempio, è possibile eliminare definitivamente testo e immagini da un documento prima di distribuirlo. Gli utenti possono inoltre ricercare e redigere i contenuti in base a pattern specifici, ad esempio per numeri di telefono, numeri di carta di credito e indirizzi e-mail. Le informazioni selezionate vengono completamente rimosse dal file, anziché essere semplicemente mascherate come avviene con altri metodi o strumenti. La funzionalità di rimozione delle informazioni riservate dal documento consente inoltre ai clienti di eliminare informazioni nascoste e oggetti non grafici che possono essere presenti in un documento PDF, ad esempio i metadati.

Condivisione di file

I file Document Cloud archiviati su cloud vengono automaticamente etichettati come "privati" e questo significa che i contenuti sono visibili soltanto all'utente finale che li ha caricati. Per condividere questi contenuti, l'utente finale deve eseguire un'azione specifica, altrimenti resteranno privati. Per completare la condivisione di tutti i contenuti Document Cloud, è necessario inviare ai destinatari desiderati il link all'URL dei contenuti Document Cloud.

Gli utenti dei servizi Document Cloud possono condividere file in due modalità: Solo visualizzazione o Revisione. Se l'utente invia il link impostando la restrizione Solo visualizzazione, il destinatario potrà solamente visualizzare i contenuti come documento di sola lettura. Se invece l'utente invia il documento per la revisione, il destinatario potrà aggiungere commenti, ma non potrà modificare né alterare in alcun modo il documento. I link possono essere inviati ai destinatari via e-mail, SMS o tramite un software di collaborazione.

Impostazioni risorse e restrizioni di condivisione

Figura 1: Impostazioni risorse per i servizi Document Cloud

È possibile applicare restrizioni di condivisione ai contenuti archiviati in Document Cloud tramite la funzionalità Impostazioni risorse nell'Adobe Admin Console. Questa opzione consente all'IT dell'azienda di disattivare la condivisione di collegamenti pubblici e forzare la collaborazione DC solo all'interno del dominio registrato dall'azienda e di qualunque altro dominio autorizzato. Quando le restrizioni di condivisione sono abilitate, i destinatari devono eseguire l'accesso. In più, se viene attivata la modalità "Condivisione solo con utenti del dominio", i contenuti possono essere condivisi solo con altri utenti all'interno dell'organizzazione o altri domini affidabili, mentre la condivisione esterna è completamente disabilitata.

Microsoft Purview Information Protection

Microsoft Purview Information Protection (MPIP) è una soluzione Microsoft per la gestione dei diritti. Gli utenti di Azure Information Protection e altre soluzioni Microsoft Purview Information Protection possono usare Acrobat o Acrobat Reader per leggere contenuti contrassegnati e protetti. Con le versioni desktop più recenti di Acrobat Pro/Standard (versione 22.003.20258 e successive) ora è possibile applicare e modificare in modo nativo le etichette di riservatezza e i criteri di Information Protection ai PDF, senza un plug-in o un'installazione separata.

Modalità protetta

Per proteggere i clienti dai tentativi del codice dannoso di utilizzare il formato PDF per scrivere o leggere nel file system di un computer, Adobe offre un'implementazione della tecnologia di sandboxing, ovvero la Modalità protetta.

In Acrobat Reader, la Modalità protetta amplia la protezione contro aggressori che tentano di installare malware sul sistema informatico di un utente, impedendo a eventuali soggetti dannosi di accedere e sottrarre dati riservati e proprietà intellettuale anche dalla rete aziendale. Attivata in modo predefinito a ogni avvio di Acrobat Reader, la Modalità protetta limita il livello di accesso consentito al programma, salvaguardando i sistemi Microsoft Windows dall'intrusione di file PDF dannosi che potrebbero tentare di scrivere o leggere nel file system del computer, eliminare file o modificare in altri modi le informazioni del sistema.

La Modalità protetta di Acrobat Reader (su Windows 8.1 e versioni successive) può essere eseguita in isolamento in un AppContainer.

Vista protetta

Il sandboxing è un metodo di sicurezza estremamente apprezzato che crea un ambiente dedicato in cui eseguire i programmi caratterizzati da un basso livello di diritti o privilegi. I processi di sandboxing consentono di proteggere i sistemi degli utenti dai danni provocati da documenti non affidabili che contengono codice eseguibile. Nel contesto di Acrobat Reader, rientrano tra i contenuti non affidabili tutti i file PDF e i processi da essi richiamati. Reader tratta tutti i documenti PDF come file potenzialmente corrotti e relega l'intera elaborazione richiamata dal file PDF al sistema di sandboxing. Come la Modalità protetta di Acrobat Reader, la Vista protetta è un'implementazione della tecnologia di sandboxing per l'ampio kit di funzionalità di Acrobat.

In Acrobat, la funzionalità della Vista protetta è stata ampliata da Adobe per fare in modo che non vengano bloccati solo gli attacchi basati su scrittura che tentano di eseguire codice dannoso su un sistema informatico attraverso il formato di file PDF, ma anche gli attacchi basati su lettura che tentano di sottrarre dati riservati o proprietà intellettuale tramite file PDF. Come la Modalità protetta, la Vista protetta limita l'esecuzione di programmi non attendibili (ad esempio, qualsiasi file PDF e i processi da esso invocati) a un sandbox ristretto per impedire all'eventuale codice dannoso di utilizzare il formato PDF per scrivere o leggere nel file system del computer in uso. La Vista protetta presuppone che tutti i file PDF siano potenzialmente dannosi e confina la loro elaborazione al sandbox, a meno che l'utente non indichi specificamente l'attendibilità di un file.

La Vista protetta è supportata in entrambi gli scenari in cui gli utenti aprono i documenti PDF, ossia all'interno dell'applicazione autonoma Acrobat e all'interno di un browser. La Vista protetta su Windows 8 e versioni successive è sempre eseguita in un AppContainer. In questo modo gli utenti che attivano la Vista protetta hanno a disposizione un ambiente con blocchi ancora più avanzati. Quando si apre un file potenzialmente dannoso in modalità Vista protetta, in Acrobat appare una barra dei messaggi gialla nella parte superiore della finestra di visualizzazione. Questa barra indica che il file non è attendibile e ricorda all'utente che si trova nella Vista protetta e che, di conseguenza, molte funzionalità di Acrobat sono disattivate e la sua interazione con il file è limitata. In sostanza, il file è in modalità di "sola lettura" e la Vista protetta impedisce che il contenuto dannoso incorporato o correlato possa alterare il sistema.

Per rendere affidabile il file e attivare tutte le funzionalità di Acrobat, l'utente può fare clic sul pulsante Abilita tutte le funzioni nella barra dei messaggi gialla. Questa operazione determina l'uscita dalla Vista protetta e assegna uno stato di attendibilità permanente al file, che verrà dunque aggiunto all'elenco di posizioni privilegiate di Acrobat. Ad ogni successiva apertura del file PDF verranno disattivate le limitazioni della Vista protetta.

Sicurezza dei servizi Adobe Document Cloud

Autenticazione degli utenti

Gli amministratori autorizzano gli utenti finali ad accedere ai servizi Adobe Document Cloud distribuendo licenze nominative mediante l'Adobe Admin Console. Acrobat con servizi Document Cloud supporta quattro (4) diversi tipi di licenze nominative che prevedono l'utilizzo di Adobe ID, Business ID, Enterprise ID e Federated ID. Per maggiori informazioni su questi tipi di identità e sui servizi di gestione delle identità di Adobe, consultare la Panoramica sulla sicurezza dei servizi di gestione delle identità di Adobe.

Archiviazione di documenti e contenuti generati dagli utenti

I servizi Adobe Document Cloud sfruttano l'archiviazione multi-tenant. I contenuti generati dagli utenti e i documenti sono memorizzati in modo ridondante in più data center e su più dispositivi all'interno di ciascun data center. Tutto il traffico di rete è sottoposto a una verifica sistematica dei dati e a calcoli di checksum per prevenire la corruzione e garantire l'integrità. Infine, i contenuti memorizzati sono replicati in modo sincrono e automatico in altri data center compresi nell'area geografica del cliente, al fine di garantire l'integrità dei dati anche qualora i dati andassero persi in due posizioni.

I contenuti e i documenti generati dall'utente e caricati su Document Cloud sono generalmente archiviati nel data center regionale che corrisponde al codice paese associato all'utente che carica i dati, indipendentemente dal tipo di identità:

- Per gli utenti con codice paese Nord America, America Centrale o Sud America, l'archiviazione avviene in Virginia negli Stati Uniti.
- Per gli utenti con codice paese Europa o Africa, l'archiviazione avviene a Dublino in Irlanda.
- Per gli utenti con codice paese Asia-Pacifico o Medio Oriente, l'archiviazione è a Tokyo in Giappone.

Gli amministratori possono assegnare ad alcuni account Enterprise ID e Federated ID il relativo spazio di archiviazione cloud tramite l'Adobe Admin Console, ma non hanno accesso diretto a nessun contenuto o documento dell'utente finale archiviato nei servizi Document Cloud. Tuttavia, gli amministratori possono assumere il controllo dell'account dell'utente e revocare l'accesso. L'eliminazione di queste tipologie di account con un servizio di archiviazione condivisa rende i dati presenti nello spazio esistente inaccessibili all'utente finale: i dati di tale utente saranno cancellati dopo 90 giorni.

Gli amministratori possono utilizzare l'Admin Console anche per assegnare uno spazio di archiviazione agli account Adobe ID. Anche se non possono controllare gli account Adobe ID, gli amministratori possono eliminarli, revocando sia la quota di archiviazione aziendale concessa sia l'accesso alle applicazioni e ai servizi dagli account dell'utente finale, anche in questo caso con la cancellazione dei relativi dati dopo 90 giorni.

Cifratura dei dati

Per impostazione predefinita, i contenuti e i documenti generati dagli utenti dei servizi Document Cloud vengono cifrati in transito con il protocollo di crittografia HTTPS TLS 1.2. I contenuti dei servizi Document Cloud vengono cifrati a riposo utilizzando chiavi di sicurezza simmetriche AES a 256 bit univoche per ciascun cliente e per il dominio registrato di ciascun cliente. Questi metodi di crittografia si applicano all'archiviazione sia permanente che temporanea dei documenti.

Chiavi di crittografia dedicate

Oltre alle funzionalità di crittografia standard integrate, gli amministratori possono aggiungere un ulteriore livello di controllo e protezione per i documenti a riposo con una chiave di crittografia dedicata per alcuni o tutti i domini dell'organizzazione del cliente. I contenuti dei servizi Document Cloud possono essere quindi cifrati a riposo utilizzando la chiave di crittografia dedicata, che, se necessario, può essere revocata tramite l'Admin Console. La revoca di questa chiave rende inaccessibili agli utenti finali tutti i contenuti crittografati con quella chiave e impedisce sia l'upload che il download di contenuti fino a quando la chiave di crittografia non viene riattivata.

Nota: solo i file Adobe Document Cloud possono essere crittografati utilizzando la chiave di crittografia dedicata; i metadati non possono essere crittografati.

Per ulteriori informazioni sulla gestione della crittografia tramite una chiave dedicata, visitare il sito Adobe.com.

Firme elettroniche e digitali

Con i servizi Document Cloud, gli utenti possono usare due strumenti diversi per gestire le firme:

- **Strumento Fill & Sign** – Consente di aprire un PDF, compilare i campi modulo e firmare elettronicamente il documento.
- **Strumento Certificati** – Consente di firmare i documenti con una firma elettronica supportata da un certificato digitale vincolato crittograficamente al campo firma. Ogni certificato digitale (o ID digitale) identifica in modo univoco il firmatario ed è rilasciato da un fornitore di servizi fiduciari (TSP) o da un'autorità di certificazione (CA) elencati nell'Adobe Approved Trust List (AATL) o negli European Union Trusted Lists (EUTL). Lo strumento Certificati consente inoltre di aggiungere marche temporali ai documenti e di certificarli con un sigillo antimanomissione.

Integrazioni tra Acrobat e Microsoft

Adobe ha stretto una partnership con Microsoft per creare integrazioni con i suoi principali strumenti di produttività, consentendo l'accesso nativo ad Acrobat con servizi Document Cloud direttamente da:

- Microsoft SharePoint e OneDrive
- Microsoft Teams
- Microsoft Word, Excel e PowerPoint (solo per la creazione e la protezione di file PDF)

Con ciascuna di queste integrazioni, Adobe crea solo una copia temporanea del documento PDF e non raccoglie informazioni sul cliente o dati personali dall'utente.

Acrobat per SharePoint e OneDrive

Acrobat per SharePoint e OneDrive offre agli utenti la possibilità di accedere ai flussi di lavoro PDF all'interno di Microsoft 365 e consente loro di visualizzare, creare e modificare file PDF nel cloud.

Utilizzando questa versione integrata di Acrobat, i documenti vengono archiviati nella loro posizione originale su SharePoint o OneDrive. Azioni come la visualizzazione, l'inserimento di commenti e le ricerche avvengono sul computer dell'utente. Quando l'utente apporta modifiche a un documento, questo viene archiviato nuovamente nel suo account SharePoint o OneDrive.

Se l'utente crea, organizza, combina o esporta un documento, questo viene inviato ai server di Adobe Document Cloud nell'area geografica corrispondente al codice del paese dell'utente per l'elaborazione temporanea e viene poi eliminato entro 24 ore. Durante questo processo, il documento rimane cifrato sia in transito che a riposo (consultare la sezione "Cifratura dei dati"). Il documento modificato viene salvato nuovamente nell'account SharePoint o OneDrive dell'utente.

Per ulteriori informazioni sulla funzionalità specifica di Acrobat per SharePoint e OneDrive, visitare il sito Adobe.com.

Acrobat per Microsoft Teams

Acrobat per Microsoft Teams offre agli utenti la possibilità di accedere ai flussi di lavoro PDF all'interno di Microsoft Teams e consente loro di visualizzare, creare e modificare file PDF nel cloud. I clienti possono usare Acrobat per Microsoft Teams come scheda personale, bot, scheda, azione messaggio o estensione messaggio.

Per impostazione predefinita, tutti i PDF condivisi in una chat o un canale Microsoft Teams vengono archiviati nell'account OneDrive o SharePoint dell'utente. Tuttavia, se un PDF viene condiviso e più persone vi collaborano attivamente in Acrobat per Microsoft Teams (ad esempio condividendo commenti), il documento viene inviato ai server di Adobe Document Cloud nell'area geografica corrispondente al codice paese dell'utente per l'elaborazione temporanea e viene poi eliminato entro 24 ore. Durante questo processo, il documento rimane cifrato sia in transito che a riposo (consultare la sezione "Cifratura dei dati"). Il documento modificato viene salvato nuovamente nella sua posizione originale.

Se l'amministratore del cliente disattiva i servizi Document Cloud, gli utenti finali saranno in grado di visualizzare in anteprima e commentare i propri documenti, ma non potranno collaborare utilizzando le funzionalità per l'inserimento di commenti condivisi.

Per ulteriori informazioni sulle funzionalità specifiche di Acrobat integrate in Microsoft Teams, visitare il sito Adobe.com.

Acrobat per Word, Excel e PowerPoint

Gli utenti possono utilizzare il componente aggiuntivo Crea PDF per convertire facilmente un documento di Microsoft 365 in un PDF di alta qualità e poi salvare il PDF su OneDrive o scaricarlo sul disco rigido personale. Possono anche proteggere il PDF aggiungendo una password per impedire eventuali accessi non autorizzati al documento.

Panoramica del programma di sicurezza Adobe

Adobe ha definito un programma integrato di sicurezza composto da cinque (5) centri di eccellenza, ciascuno dei quali itera e migliora costantemente le modalità di rilevazione e prevenzione dei rischi sfruttando tecnologie nuove ed emergenti, come l'automazione, l'intelligenza artificiale e il machine learning.

Figura 2: Cinque centri di eccellenza per la sicurezza

I centri di eccellenza nel programma di sicurezza Adobe comprendono:

- **Sicurezza delle applicazioni** – Si concentra sulla sicurezza del codice dei nostri prodotti, conduce ricerche sulle minacce e porta avanti il programma bug bounty.
- **Sicurezza operativa** – Contribuisce al monitoraggio e alla protezione dei nostri sistemi, delle nostre reti e dei sistemi cloud di produzione.
- **Sicurezza aziendale** – Si concentra sull'autenticazione e sull'accesso sicuro all'ambiente aziendale Adobe.
- **Conformità** – Sovrintende il nostro modello di governance della sicurezza, i programmi di audit e conformità normativa e l'analisi dei rischi.
- **Risposta agli incidenti** – Include il nostro centro operativo di sicurezza e il personale pronto a intervenire in caso di minacce, attivi 24 ore su 24, 7 giorni su 7.

A dimostrazione dell'impegno profuso per la sicurezza dei nostri prodotti e servizi, i centri di eccellenza rispondono direttamente all'ufficio del Chief Security Officer (CSO), che coordina tutte le attività di sicurezza correnti e sviluppa la visione per l'evoluzione futura della sicurezza in Adobe.

L'organizzazione della sicurezza targata Adobe

Basata su una piattaforma con processi decisionali trasparenti, responsabili e consapevoli, l'organizzazione della sicurezza targata Adobe riunisce l'intera gamma di servizi di sicurezza in un unico modello di governance. A livello dirigenziale, il CSO collabora a stretto contatto con il Chief Information Officer (CIO) e il Chief Privacy Officer (CPO) per garantire l'allineamento della strategia e delle attività operative in materia di sicurezza.

Oltre ai centri di eccellenza sopra descritti, Adobe coinvolge i membri dei team legale, per la privacy, di marketing e di pubbliche relazioni nell'organizzazione della sicurezza, al fine di favorire la trasparenza e l'affidabilità di tutte le decisioni relative alla sicurezza.

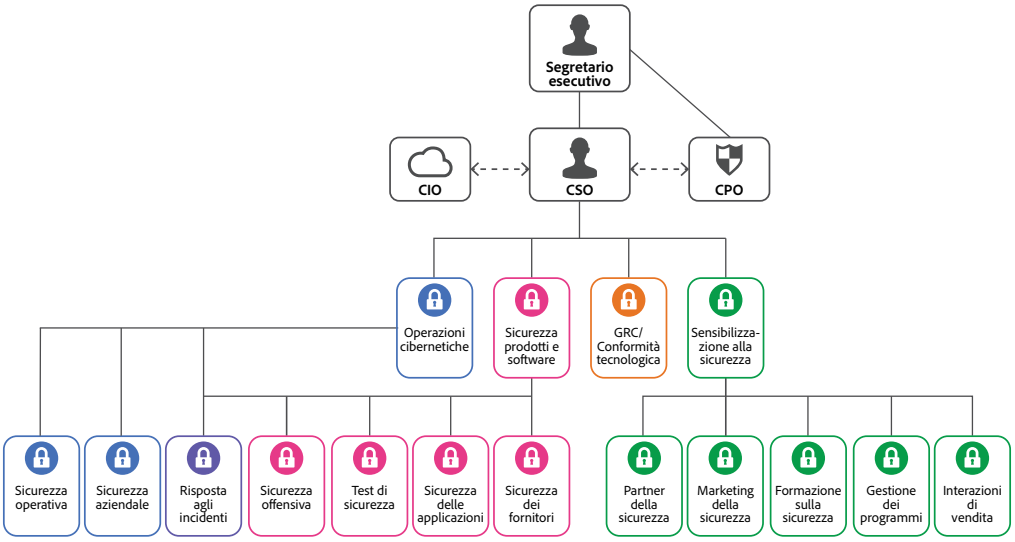

Figura 3: L'organizzazione della sicurezza targata Adobe

Adobe promuove una cultura della sicurezza a livello aziendale, per cui ciascun dipendente è tenuto a seguire il corso di sensibilizzazione e formazione sulla sicurezza, che deve essere completato con relativa ricertificazione a cadenza annuale, contribuendo così a garantire che ogni membro del personale si impegni attivamente a proteggere le risorse aziendali di Adobe, nonché i dati di clienti e dipendenti. Al momento dell'assunzione, il personale tecnico, compresi i team ingegneristici e addetti alle operazioni tecniche, vengono iscritti automaticamente a un programma di formazione approfondito in "stile arti marziali", con contenuti personalizzati in base ai ruoli specifici. Per ulteriori informazioni sulla nostra cultura della sicurezza e sui nostri programmi di formazione, consultare il white paper sulla cultura della sicurezza in Adobe.

La procedura Secure Product Lifecycle di Adobe

Integrata in molteplici fasi del ciclo di vita del prodotto, dalla progettazione allo sviluppo, fino al controllo qualità, al testing e alla distribuzione finale, la procedura Secure Product Lifecycle di Adobe (SPLC) è la colonna portante di tutte le iniziative di sicurezza intraprese da Adobe. Costituita da un insieme rigoroso di diverse centinaia di attività di sicurezza specifiche che interessano i criteri, i processi e gli strumenti di sviluppo software, la procedura Adobe SPLC definisce processi chiari e ripetibili per consentire ai team di sviluppo di integrare la sicurezza all'interno dei nostri prodotti e servizi ed è in costante evoluzione per incorporare le più recenti best practice del settore.

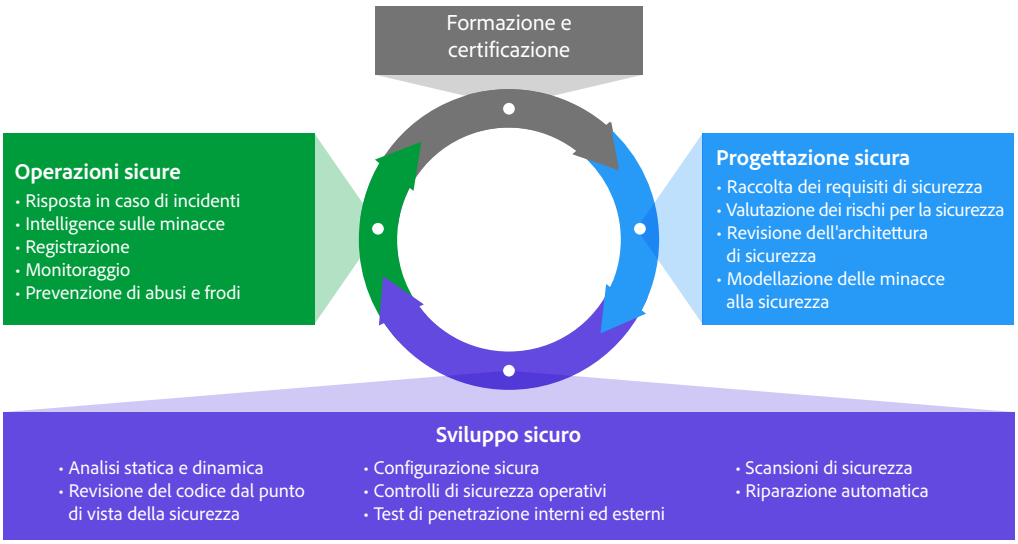

Figura 4: La procedura Secure Product Lifecycle di Adobe

Adobe ha pubblicato uno standard per la procedura Secure Product Lifecycle, disponibile per la consultazione su richiesta. Per ulteriori informazioni sui componenti della procedura Adobe SPLC, consultare la Panoramica sulla sicurezza delle applicazioni.

Sicurezza delle applicazioni Adobe

In Adobe, lo sviluppo di applicazioni "sicure di default" parte dallo Stack di sicurezza delle applicazioni Adobe. Combinando processi chiari e ripetibili basati su ricerche ed esperienze consolidate con automazioni che concorrono a garantire l'applicazione uniforme dei controlli di sicurezza, lo Stack di sicurezza delle applicazioni Adobe contribuisce a migliorare l'efficienza degli sviluppatori e a ridurre al minimo il rischio di errori sul fronte della sicurezza. Utilizzando blocchi di programmazione sicuri, testati e preapprovati che eliminano la necessità di scrivere codice da zero per i pattern e i blocchi più comunemente usati, gli sviluppatori hanno la certezza che il codice sia sicuro e possono quindi concentrarsi sulla loro area di competenza. Insieme a test, strumentazione specializzata e attività di monitoraggio, lo Stack di sicurezza delle applicazioni Adobe aiuta gli sviluppatori di software a creare codice sicuro di default.

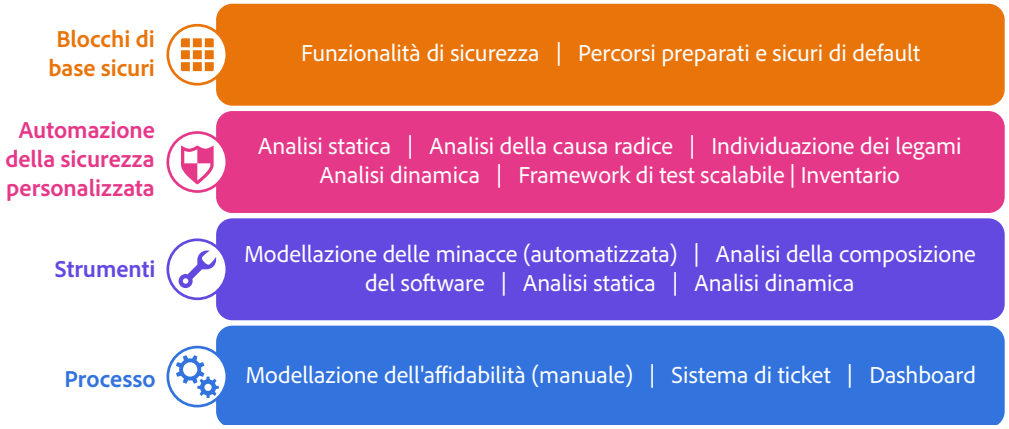

Figura 5: Lo Stack di sicurezza delle applicazioni Adobe

Adobe ha anche pubblicato diversi standard relativi alla sicurezza delle applicazioni, compresi quelli di lavoro specifici che disciplinano il nostro utilizzo dell'infrastruttura cloud pubblica. Questi standard sono disponibili per la consultazione su richiesta. Per ulteriori informazioni sulla sicurezza delle applicazioni Adobe, consultare la Panoramica sulla sicurezza delle applicazioni Adobe.

Sicurezza operativa Adobe

Per garantire che tutti i prodotti e servizi Adobe siano progettati fin dall'inizio secondo le best practice in materia di sicurezza, il team addetto alla sicurezza operativa ha creato lo Stack di sicurezza operativa Adobe. Si tratta di un insieme consolidato di strumenti che aiutano ingegneri e sviluppatori di prodotto a migliorare il proprio approccio alla sicurezza e a ridurre i rischi sia per Adobe sia per i clienti, contribuendo allo stesso tempo a promuovere il rispetto degli standard di conformità e privacy e l'adesione ad altri framework di governance in tutta l'azienda.

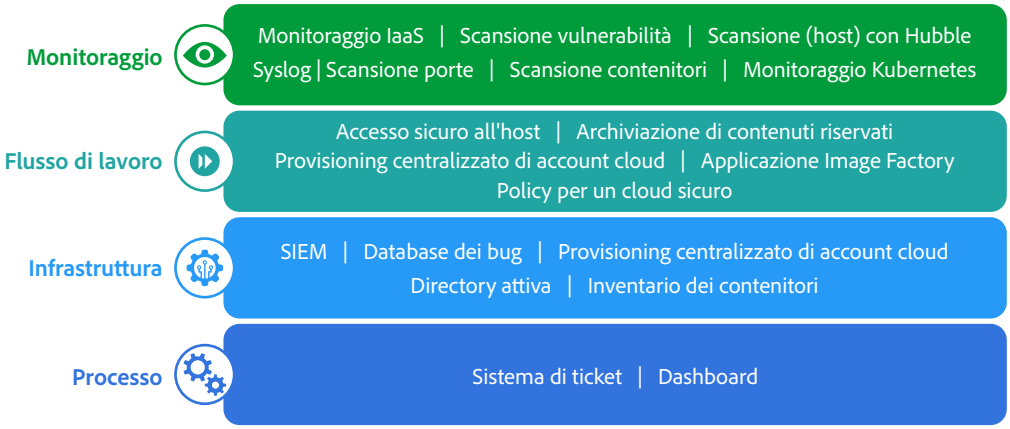

Figura 6: Lo Stack di sicurezza operativa Adobe

Adobe ha pubblicato diversi standard relativi alle attività operative nel cloud, disponibili per la consultazione su richiesta. Per una descrizione dettagliata dello Stack di sicurezza operativa Adobe e degli strumenti specifici utilizzati in Adobe, consultare la Panoramica sulla sicurezza operativa Adobe.

Sicurezza aziendale Adobe

Oltre a proteggere i propri prodotti e servizi, nonché le operazioni di cloud hosting, Adobe impiega anche una serie di controlli di sicurezza interni per garantire la sicurezza delle reti e dei sistemi interni, delle sedi fisiche aziendali, dei dipendenti e dei dati dei clienti.

Per ulteriori informazioni sui controlli di sicurezza a livello aziendale e sugli standard che abbiamo sviluppato per questi controlli, consultare la Panoramica sulla sicurezza aziendale Adobe.

Conformità Adobe

Tutti i prodotti e i servizi Adobe si attengono all'Adobe Common Controls Framework (CCF), un insieme di attività di sicurezza e controlli di conformità che vengono implementati all'interno dei nostri team di prodotto e, per vari aspetti, anche nei team che si occupano di infrastrutture e applicazioni. Per quanto possibile, Adobe sfrutta processi di automazione all'avanguardia per avvisare i team di possibili situazioni di non conformità e garantire l'adozione tempestiva di opportune misure di riduzione e riallineamento.

I prodotti e i servizi Adobe soddisfano gli standard legali applicabili o possono essere utilizzati secondo modalità che permettono ai clienti di soddisfare gli obblighi legali relativi all'utilizzo dei fornitori di servizi. I clienti mantengono il controllo sui propri documenti, dati e flussi di lavoro e possono scegliere la modalità migliore per garantire la conformità a normative locali o regionali, come il Regolamento generale sulla protezione dei dati (GDPR) nell'UE.

Adobe offre anche una formazione sulla conformità normativa, e i relativi standard sono disponibili per la consultazione su richiesta. Per ulteriori informazioni sull'Adobe CCF e sulle certificazioni principali, consultare l'Elenco di standard, regolamenti e certificazioni di conformità Adobe.

Risposta in caso di incidenti

Adobe si impegna a garantire che la gestione dei rischi e delle vulnerabilità, la risposta agli incidenti, la mitigazione e i processi di risoluzione siano agili e accurati. Monitoriamo costantemente il panorama delle minacce, condividiamo le conoscenze con gli esperti di sicurezza di tutto il mondo, risolviamo rapidamente gli incidenti quando si verificano e trasmettiamo queste informazioni ai nostri team di sviluppo per aiutare a raggiungere i massimi livelli di sicurezza per tutti i prodotti e servizi Adobe.

Manteniamo anche standard interni per la risposta in caso di incidenti e la gestione delle vulnerabilità, disponibili per la consultazione su richiesta. Per maggiori dettagli sul processo di risposta e notifica di Adobe in caso di incidenti, consultare la Panoramica sulla risposta agli incidenti di Adobe.

Continuità aziendale e disaster recovery

Il programma Business Continuity and Disaster Recovery (BCDR) di Adobe è composto dal piano di continuità aziendale Adobe (BCP) e dai piani di disaster recovery (DR) specifici per prodotto, che contribuiscono entrambi a garantire la disponibilità e la fornitura continua dei prodotti e servizi Adobe. Il nostro programma BCDR è certificato ISO 22301 e migliora la nostra capacità di risposta, riduzione degli impatti e ripresa in caso di interruzioni impreviste. Per ulteriori informazioni, consultare la Panoramica sul programma di continuità aziendale e disaster recovery di Adobe.

Conclusione

L'approccio proattivo alla sicurezza e le rigorose procedure descritte in questo documento permettono di garantire la sicurezza di Acrobat con servizi Document Cloud e dei dati riservati degli utenti. La protezione dei dati nelle esperienze digitali è una questione che Adobe affronta con grande serietà ed è per questo che monitoriamo costantemente l'evoluzione del panorama delle minacce per essere sempre informati di eventuali attività dannose e contribuire alla salvaguardia dei dati dei nostri clienti.

Per ulteriori informazioni sulla sicurezza Adobe, visitare il Centro protezione di Adobe.

Le informazioni presenti in questo documento sono soggette a modifiche senza preavviso. Per maggiori informazioni sulle soluzioni, sui controlli e sulle opzioni per l'acquisto di licenze Adobe, contattare il responsabile vendite Adobe di riferimento.

Adobe

© 2023 Adobe. Tutti i diritti riservati.

Adobe, il logo Adobe, Acrobat, il logo Adobe PDF, Adobe Document Cloud e Document Cloud sono marchi o marchi registrati di Adobe negli Stati Uniti e/o in altri paesi. Tutti gli altri marchi appartengono ai rispettivi proprietari.

8/23