Adobe Acrobat DC med Document Cloud-tjenester sikkerhedsoversigt

Indholdsfortegnelse

1: Executive summary
1: Acrobat DC med Document Cloud-tjenester oversigt
1: Acrobat dokumentsikkerhedsfunktioner
2: Elementindstillinger og delingsbegrænsninger
2: MIP (Microsoft Information Protection)
3: Document Cloud-tjenestearkitektur
3: Document Cloud-tjenestesikkerhed
4: Indholdslagring af Document Cloud-tjenester
5: Amazon Web Services
5: Driftsansvar for AWS og Adobe
8: Adobe risiko- og sårbarhedsstyrin
9: Adobes sikkerhedsorganisation
9: Adobe sikker produktudvikling
9: Adobe SPLC (sikker produktlevetid)
10: Adobe certificeringsprogram for softwaresikkerhed
10: Document Cloud-tjenesteoverholdelse
11: Adobe medarbejdere
12: Konklusion

Selvom Adobe Sign er en del af Document Cloud PDF-tjenester, er dens sikkerhedsfunktionalitet uafhængig.

Executive summary

Hos Adobe tager vi dine digitale oplevelsers sikkerhed meget alvorligt. Sikkerhedsprocedurer er tæt integreret i vores interne softwareudvikling, driftsprocesser og værktøjer. Disse metoder følges nøje af vores tværfunktionelle teams for at hjælpe med at forhindre, registrere og reagere på hændelser på en hensigtsmæssig måde. Vi holder os ajour med de seneste trusler og svagheder gennem vores samarbejde med partnere, førende forskere, sikkerhedsforskningsinstitutioner og andre brancheorganisationer. Vi integrerer jævnligt avancerede sikkerhedsteknikker med de produkter og tjenester, som vi tilbyder.

Adobe-tjenester, som berører kundeindhold, har gennemført adskillige branchecertifikationer. For en detaljeret oversigt over alle overensstemmelsescertificeringer og -standarder samt offentlige bestemmelser, der understøttes af Adobe-produkter og -løsninger, bedes du se Aktuel oversigt over certifikationer, standarder og bestemmelser. For oplysninger om GDPR bedes du se siden om GDPR-parathed.

Denne hvidbog beskriver tilgangen til dybdegående forsvar og sikkerhedsprocedurer, der er implementeret af Adobe, med henblik på at forbedre sikkerheden af Adobe Acrobat DC, Acrobat Reader DC, Document Cloud, Document Cloud-tjenester og dertilhørende data.

Acrobat DC med Document Cloud-tjenester oversigt

Adobe Acrobat DC kombinerer den seneste Acrobat-computersoftware med premiumfunktioner i Acrobat Reader-mobilappen og Adobe Document Cloud online-tjenesterne med henblik på at hjælpe organisationer med at opfylde slutbrugernes behov for at være forbundne og produktive på enhver enhed, og samtidig hjælpe med at opretholde sikkerheden på tværs af enheder. Ved at bruge Adobe Acrobat DC and Document Cloud-tjenester kan kunderne lave indhold om til et elektronisk dokument, der kan deles med andre og nemt generere, manipulere og transformere PDF-filer fra enhver Adobe cloud-tjeneste, computerapplikation eller mobilapp.

Acrobat dokumentsikkerhedsfunktioner

Redigering

Adobe Acrobat DC indeholder et sæt redigeringsværktøjer, som hjælper kunderne med at beskytte følsomme eller fortrolige oplysninger, herunder permanent sletning af både tekst og grafiske billeder i et dokument inden distribution. Derudover kan brugere søge og redigere indhold baseret på mønstre, som f.eks. telefonnumre, kreditkortnumre og e-mailadresser. De redigerede oplysninger er helt fjernet fra filen, ikke bare maskeret som med andre værktøjer eller metoder. Med funktionen dokumentrensning kan brugerne også fjerne skjulte informationer og ikke-grafiske objekter som f.eks. metadata, der kan være i PDF'en.

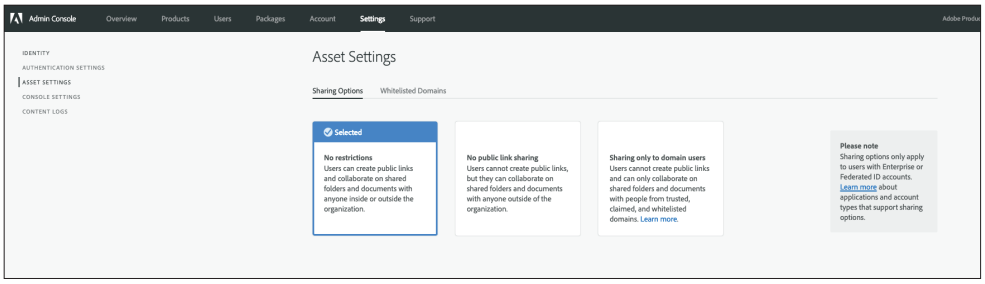
Fildeling

Alle Document Cloud-filer, der er lagret i skyen markeres automatisk med "Privat", hvilket betyder, at indholdet kun er synligt for den slutbruger, som uploadede det. En slutbruger skal træffe udtrykkelige foranstaltninger for at dele dette indhold, da det ellers vil forblive privat. Alt Document Cloud-indholdsdeling foretages ved at sende et link til Document Cloud-indholdet til modtageren/-ene via e-mail, sms eller en anden samarbejdssoftware.

Brugere af Document Cloud-tjenesterne kan dele filer med to muligheder: Se kun eller Gennemgå. Hvis brugeren sender linket med Se kun-begrænsning, kan modtageren kun se indholdet som et skrivebeskyttet dokument. Alternativt kan modtageren, hvis brugeren sender dokumentet til korrektur, kommentere dokumentet, men kan på ingen måde redigere eller ændre det.

Elementindstillinger og delingsbegrænsninger

Elementindstillinger giver en organisation kontrol over, hvordan medarbejdere deler elementer uden for organisationen. IT-administratoren kan vælge en begrænset indstilling, som begrænser medarbejdere i at bruge specifikke delingsfunktioner i Document Cloud, herunder begrænsning af invitationsbaseret deling til modtagere i de benyttede, pålidelige og hvidlistede domæner. Når denne politik er sat op, forhindres brugere i at dele organisationsejede elementer med eksterne brugere, som ikke er med på listen over tilladte domæner.



Elementindstillinger i Administratorkonsollen

MIP (Microsoft Information Protection)

For at kunder, som bruger Acrobat DC eller Acrobat Reader DC, skal kunne åbne filer, der er beskyttet med MIP-løsninger (Microsoft Information Protection), herunder AIP (Azure Information Protection) og informationsbeskyttelse vha. Microsoft Office 365, se i dette dokument.

Beskyttet tilstand i Acrobat Reader DC

For at hjælpe med at beskytte kunder mod skadelig kode, der forsøger at anvende PDF-formatet til at skrive til eller læse fra en computers filsystem, leverer Adobe en implementering af sandbox-teknologi, der kaldes Beskyttet tilstand, hvilket blev introduceret i Adobe Reader X.

Sandboxing er en sikkerhedsmetode, der skaber et indesluttet driftsmiljø til kørsel af programmer med begrænsede rettigheder eller privilegier. Sandboxe hjælper med at beskytte brugernes systemer, så de ikke bliver skadet af ikke-sikre dokumenter, der indeholder eksekverbar kode. I forbindelse med Acrobat Reader DC vil det ikke-sikre indhold være enhver form for PDF-fil og den proces, som den muligvis aktiverer. Acrobat Reader DC behandler alle PDF-filer som potentielt farlige og begrænser alle processer, som PDF-filen aktiverer, til sandboxen.

Acrobat Reader DC Beskyttet tilstand hjælper med at forsvare mod angribere, der forsøger at installere malware på et computersystem, som understøtter organisationens bestræbelser på at forhindre skadelige brugere i at få adgang til og trække følsomme data og ophavsrettigheder ud af deres netværk. Beskyttet tilstand aktiveres som standard, når en bruger starter Acrobat Reader DC og begrænser programmets adgangsniveau, hvilket sikrer systemer, der kører Microsoft Windows mod skadelige PDF-filer, der måske forsøger at skrive til eller læse fra computerens filsystem, slette filer eller på anden vis ændre systeminformationer.

Beskyttet tilstand på Windows 8 og højere kan også køre i en Windows AppContainer, hvilket giver et endnu stærkere låst miljø til kunder, som aktiverer Beskyttet tilstand.

Beskyttet tilstand i Acrobat DC

Næsten ligesom Beskyttet tilstand i Adobe Reader DC er Beskyttet visning en implementering af "sandboxing"-teknologien for det righoldige Acrobat DC funktionssæt. I Acrobat DC udvider Adobe funktionaliteten af Beskyttet tilstand lige fra blokering af skrivebaserede angreb, der forsøger at køre skadelig kode på et computersystem vha. PDF-filformatet, til også at omfatte læsebaserede angreb, der forsøger at stjæle dine følsomme data eller intellektuelle ophavsrettigheder via PDF-filer.

Ligesom Beskyttet tilstand begrænser Beskyttet visning mod kørslen af ikke-sikre programmer (f.eks. enhver PDF-fil og de processer, den vækker) til en begrænset sandbox for at forhindre, at skadelig kode anvender PDF-formatet til at skrive til eller læse fra computerens filsystem. Beskyttet visning går ud fra, at alle PDF-filer er potentielt skadelige og begrænser processerne til sandboxen, medmindre brugeren specifikt angiver, at en fil er pålidelig.

Beskyttet tilstand er understøttet i begge scenarier, hvor brugerne åbner PDF-dokumenter - i den enkeltstående Acrobat DC-applikation og i en browser. Beskyttet visning på Windows 8 og højere kan nu køre i en AppContainer. Det giver et endnu stærkere låst miljø for kunder, der aktiverer Beskyttet visning.

Når du åbner en ikke-sikker fil i Beskyttet visning, viser Acrobat DC en meddelelsesbjælke øverst i visningsvinduet. Denne meddelelsesbjælke angiver, at filen ikke er sikker og minder brugeren om, at han/hun er i Beskyttet visning, og deaktiverer dermed mange Acrobat DC-funktioner og begrænser brugerinteraktion med filen. I bund og grund er filen i læsebeskyttet tilstand og Beskyttet visning beskytter mod at integreret eller medfølgende indhold manipulerer med dit system.

For at indikere at brugeren har tillid til, at filen er sikker, og aktivere alle Acrobat DC funktioner, kan vedkommende klikke på knappen Aktiver alle funktioner i meddelelsesbjælken. Denne handling lukker Beskyttet visning, og giver filen status som permanent sikker ved at tilføje den til Acrobats liste sikre steder. Enhver efterfølgende åbning af den PDF-fil, du har tillid til, deaktiverer begrænsninger i Beskyttet visning.

Document Cloud-tjenestearkitektur

Adobe Document Cloud-tjenester omfatter:

- **Organiser PDF** - indsæt, slet, omstrukturer eller roter sider i en PDF
- **Skab PDF -** konverter Word, Excel og PowerPoint-dokumenter, og billeder eller fotos til PDF-filer
- **Eksporter PDF** - konverter nemt og enkelt PDF'er til redigerbare Microsoft Word, Excel, PowerPoint eller RTF-filer
- **Rediger PDF** - rediger nemt og enkelt eksisterende PDF'er fra din mobile eller bærbare enhed
- **Kombiner PDF -** kombiner flere forskellige filer til en enkelt PDF og saml dokumentpakker overalt
- **Send og spor** - send, spor og bekræft levering af dokumenter
- **Adobe Scan** - fang og konverter alt til en søgbar PDF i høj kvalitet
- **Adobe Sign** - klargør og send dokumenter til sikre og pålidelige, juridisk bindende elektroniske underskrifter på enhver enhed

Document Cloud-tjenestesikkerhed

Rettigheds- og identitetsadministration

IT-administratorer giver slutbrugere adgang til Adobe Document Cloud-tjenester ved at anvende navngivne brugerlicenser i Adobes administratorkonsol. Acrobat Document Cloud understøtter tre (3) forskellige typer af brugernavngivne licenser:

- **Adobe-id** - til Adobe-hostede, brugeradministrerede konti, der er skabt, ejet og kontrolleret af individuelle brugere. Adobe Id-konti har kun adgang til Acrobat Document Cloud-tjenester, hvis en IT-administrator giver adgang.
- **Enterprise-id** - en Adobe-hosted, virksomhedsadministreret mulighed til konti, der er oprettet og kontrolleret af IT-administratorer fra kundens virksomhed. Din organisation ejer og administrerer brugerkontiene og alle tilknyttede elementer.
- **Federated-id** - en virksomhedsadministreret konto, hvor alle identitetsprofiler stammer fra kundernes SSO-identitetsadministrationssystem (single sign-on) og oprettes, ejes og kontrolleres af kundernes IT-infrastruktur. Adobe integrerer med de fleste SAML 2.0 kompatible identitetsudbydere.

De fleste virksomheder anvender Enterprise-id eller Federated-id til deres medarbejdere, leverandører og freelancere, under forudsætning af at e-mailadressen ligger inden for virksomhedsdomænet, da det giver dem mulighed for at bevare kontrollen over såvel rettigheder som det brugergenererede indhold (UGC), der er gemt på vegne af det pågældende id. For yderligere oplysninger om hver enkelt id-type, bedes du se under Adobes kundesupportside.

Adobe-id og Enterprise-id adgangskodelagring anvender begge SHA-256 hashalgoritme i kombination med adgangskode-salte og et stort antal af hashgentagelser. Adobe overvåger kontinuerligt Adobe-hostede konti for usædvanlig eller uregelmæssig kontoaktivitet, og evaluerer disse oplysninger for at hjælpe med at reducere sikkerhedstrusler hurtigt. I forbindelse med Federated-id-konti administrerer Adobe ikke brugeres adgangskoder. For yderligere oplysninger se venligst Sikkerhedsoversigt over identitetsadministrationstjenester.

Elektroniske og digitale underskrifter

Med Document Cloud-tjenester kan brugere vælge mellem to forskellige værktøjer til at arbejde sikkert med underskrifter:

- **Værktøjet Udfyld og signer** - genereret af Adobe Sign giver brugerne mulighed for at administrere underskriftsprocesser fra ende til anden, der er beregnet til at hjælpe med at overholde lovene om elektroniske underskrifter i USA, EU og de fleste industrialiserede lande i verden. Med denne funktion kan de bede om underskrifter fra andre, spore underskriftsprocessen og arkivere underskrevne dokumenter og revisionsspor automatisk. Sikkerhedsforanstaltninger anvendes i hele processen, og dokumenter og revisionsspor certificeres af Adobe med en forsegling, der er sikret mod manipulation.

Sporing er ikke mulig på mobile enheder.

For yderligere oplysninger om Adobe Sign og dens sikkerhedsfunktionalitet, bedes du se Adobe Sign teknisk oversigt.

- **Certifikat-værktøjet** - giver brugere mulighed for at underskrive dokumenter med certifikatbaserede digitale underskrifter fra anerkendte serviceudbydere på enten AATL-listen (Adobe Approved Trust List) eller på EUTL-listen (European Union Trusted List). At underskrive med et certifikat-ID udstedt af en anerkendt tredjeparts certifikatmyndighed er generelt anerkendt som en sikker metode til at underskrive dokumenter elektronisk. Id'et er unikt knyttet til, og i stand til at identificere, underskriveren. Underskriverens certifikat er kryptografisk knyttet til dokumentet under underskriftsfasen med den private nøgle, der er unikt knyttet til den pågældende underskriver.

  Acrobat DC validerer underskriverens underskrift - og ægtheden af det dokument, han/hun underskrev - ved automatisk at kontakte certifikatmyndigheden for godkendelse. Denne type underskrift overholder elektroniske underskriftstandarder for PDF'er, herunder PAdES (PDF Advanced Electronic Signature) del 2, 3 og 4 samt det amerikanske forsvars JITC (Joint Interoperability Test Command) brug af kryptografi og PKI (Public Key Infrastructure) med AES-256, RSA-4096, SHA-512, og RSA-PSS. Med Certifikat-værktøjet kan brugere også føje tidsstempler til dokumenter, og certificere dem med en forsegling, der er sikret mod manipulation.

Indholdslagring af Document Cloud-tjenester

Selvom administratorer allokerer individuel cloud-lagring til Enterprise-id og Federated-id-konti gennem Adobe administratorkonsollen, har de ikke direkte adgang til filer i brugerens Document Cloud-tjenestelagring. Ved at slette et Enterprise-id eller Federated-id med eksisterende fælles tjenestelagring renderes alle data i cloudlagring, der ikke er tilgængelige for brugeren, og den pågældende brugers data slettes efter 90 dage.

Administratorer kan også anvende administratorkonsollen til at allokere lagring til Adobe-id-konti. Selvom de ikke kan slette Adobe-id-konti, kan administratorer tilbagekalde både den bevilligede virksomhedslagringskvote samt adgang til applikation og tjeneste. De forbundne data med disse konti slettes efter 90 dage.

Adobe Document Cloud-tjenesterne gør brug af multitenantlagring. Kundeindhold behandles af en Amazon Elastic Compute Cloud (Amazon EC2) hændelse og gemmes vha. en kombination af Amazon Simple Storage Services (Amazon S3) grupper og gennem en MongoDB hændelse på en Amazon Elastic Block Store (Amazon EBS). Selve indholdet er gemt i Amazon S3 grupper, og metadataene om indholdet er gemt i Amazon EBS via MongoDB - alt sammen beskyttet af IAM-roller (Identity and Access Management) i den pågældende AWS-region (Amazon Web Services).

Metadata og supportelementer, der er gemt i Amazon EBS, krypteres med AES 256-bit kryptering vha. FIPS-standarder (Federal Information Processing Standards) 140-2 godkendte kryptografiske algoritmer, der følger 800-57 anbefalingerne fra National Institute of Standards and Technology (NIST).

Data lagres redundant i flere datacentre og på flere enheder i hvert datacenter. Al netværkstrafik er underlagt systematisk datagodkendelse og tjeksumsberegninger for at forebygge ødelæggelse og sikre integritet. Endelig kopieres lagret indhold synkront og automatisk til andre datacenterfaciliteter

inden for kundens område, så dataintegriteten også vil blive vedligeholdt, selv om der har været datatab to forskellige steder.

For yderligere oplysninger om de underliggende Amazon-tjenester skal du se:

- MongoDB
- Amazon S3
- AWS Key Management Service (KMS)
- Amazon EC2-tjeneste

Dedikeret krypteringsnøgle

Som standard er det indhold og elementer, der er gemt i Amazon S3, krypteret med AES 256-bit symmetriske sikkerhedsnøgler, som er unikke for hver enkelt kunde og det domæne, som hver enkelt kunde gør krav på. Hvis administratorer ønsker at tilføje et ekstra lag med kontrol og sikkerhed for nogle af eller alle domænerne i deres organisation, kan de bruge en dedikeret krypteringsnøgle, der administreres af AWS KMS og automatisk går på omgang på årlig basis.

Administratorer kan også tilbagekalde denne dedikerede krypteringsnøgle via administratorkonsollen, der vil rendere alle data, der er krypteret med den pågældende nøgle, som ikke er tilgængelig for slutbrugere, og forhindrer både upload og download af indhold, indtil krypteringsnøglen er reaktiveret.

Bemærk: Modsat Adobe Document Cloud-filer, der kan krypteres vha. den dedikerede krypteringsnøgle, kan metadata ikke krypteres vha. nøglen.

For yderligere oplysninger om, hvordan man håndterer kryptering vha. en dedikeret nøgle, se disse sider med Adobe hjælp:

- Håndtering af kryptering
- Dedikerede krypteringsnøgler OSS

Amazon Web Services

Som tidligere nævnt er alle komponenter tilhørende Adobe Document Cloud-tjenester hostet på AWS, herunder Amazon EC2 og Amazon S3, i USA. Amazon EC2 er en web-tjeneste, der tilbyder automatisk skalerbar databehandlingskapacitet i skyen, hvilket gør webbaseret databehandling lettere. Amazon S3 anerkendes generelt som en yderst pålidelig databehandlingsinfrastruktur til lagring og genfinding af enhver mængde data.

AWS-platformen tilbyder tjenester, der overholder praksis for branchens standardarder, og er underlagt faste branche-anerkendte certifikationer og kontroller. Du kan finde flere detaljerede informationer om AWS og Amazons sikkerhedskontroller på hjemmesiden om AWS Cloud-sikkerhed.

Driftsansvar for AWS og Adobe

AWS driver, administrerer og kontrollerer komponenterne fra hypervisorens virtualiseringslag og ned til den fysiske sikkerhed for de anlæg, hvor Adobe Document Cloud-tjenesterne kører. Omvendt påtager Adobe sig ansvaret for og administrationen af gæsteoperativsystemet (herunder opdateringer og sikkerhedsrettelser) og applikationssoftware, samt konfigurationen af den AWS-leverede sikkerhedsgruppefirewall.

AWS driver også cloud-infrastrukturen, der anvendes af Adobe til at skaffe en lang række basisressourcer til databehandling, herunder behandling og lagring. AWS-infrastrukturen omfatter anlæg, netværk og hardware, samt operationel software (for eksempel, host OS, virtualiseringssoftware osv.), som understøtter anskaffelsen og brugen af disse ressourcer. Amazon designer og administrerer AWS i overensstemmelse med branchens standarder, samt en lang række standarder for sikkerhedsoverholdelse.

Sikker håndtering

Adobe anvender SSH (Secure Shell) og SSL (Secure Sockets Layer) til håndtering af forbindelser til at styre AWS-infrastrukturen.

Geografisk placering af kundedata på AWS-netværket

Alt brugergenereret indhold (UGC), der er uploadet til Document Cloud, er gemt i AWS USA-østs (Virginia) regionale datacentre. Indholdet ligger som backup hos hvert enkelt datacenter, og i andre datacentre i området, for balancering af belastning og redundans.

Geografisk placering af identitetsdata på AWS-netværket

Identitetsdata lagres i multiregionale, belastningsbalancerede AWS-datacentre, der er placeret i Virginia (USA-øst), Oregon (USA-vest), Irland (EU-vest) og Singapore (AP-sydøst). Identitetsdata kopieres på tværs af alle datacentre. Adobe overholder gældende love med hensyn til dataoverførsler over landegrænserne, som det fremgår i detaljer på https://www.adobe.com/dk/privacy/eudatatransfers.html.

Isolation af kundedata/opdeling af kunder

AWS anvender et højt sikkerhedsniveau for tenant-isolationssikkerhed og kontrolfunktioner. Som et virtualiseret multitenant-miljø implementerer AWS processer for sikkerhedshåndtering og andre sikkerhedskontroller, der er designet til at isolere den enkelte kunde fra andre AWS-kunder. Adobe anvender AWS Identity and Access Management (IAM) for yderligere at begrænse adgangen til behandling og lagring af hændelser.

Sikker netværksarkitektur

AWS gør brug af netværksenheder, herunder firewalls og andre grænseenheder, til at overvåge og kontrollere kommunikationer ved netværkets eksterne grænse og ved vigtige interne grænser i netværket. Disse grænseenheder gør brug af regelsæt, adgangskontrollister (ACL'er) og konfigurationer til at realisere informationsflowet til specifikke informationssystemtjenester. Der forefindes ACL'er eller politiker for trafikflow på hver enkelt administreret interface for at administrere og underbygge trafikflowet.

Amazon Information Security godkender alle ACL-politikker og skubber dem automatisk til hvert enkelt administreret interface vha. værktøjet AWS ACL-Manage, der hjælper med at sørge for, at disse administrerede grænseflader underbygger de mest opdaterede ACL'er.

Netværksovervågning og beskyttelse

AWS anvender en lang række automatiserede overvågningssystemer for at levere et højt serviceniveau for præstation og tilgængelighed. Overvågningsværktøjer hjælpe med at registrere usædvanlige eller uautoriserede aktiviteter, samt betingelser ved indgang og udgang fra kommunikationspunkter. AWS-netværket tilbyder betydelig beskyttelse mod traditionelle netværkssikkerhedsproblemer:

- DDoS-angreb (distributed denial-of-service)
- MITM-angreb (man-in-the-middle)
- IP-spoofing
- Port-scanning
- Packet sniffing af andre tenants

For yderligere oplysninger om netværksovervågning og beskyttelse, kan du besøge AWS Cloud Security-hjemmesiden.

Indbrudsregistrering

Adobe overvåger aktivt Adobe Document Cloud-tjenester vha. IDS-systemer (indbrudsregistreringssystemer) og IPS-systemer (indbrudsforebyggelsessystemer).

Logføring

Adobe udfører serverrelateret logging af Adobe Document Cloud-tjenesters kundeaktivitet for at lave diagnose på serviceafbrydelser, specifikke kundeproblemer og rapporterede fejl. Disse logs lagrer kun Adobe id'er for at hjælpe med at lave diagnose for specifikke kundeproblemer, og indeholder ingen kombinationer af brugernavne/adgangskoder. Kun Adobes autoriserede tekniske supportpersonale, nøgleteknikere og udvalgte udviklere kan tilgå de forskellige logs for at lave diagnose af specifikke problemer, der måtte opstå.

Serviceovervågning

AWS overvåger elektriske og mekaniske systemer samt driftstøttesystemer og udstyr til at hjælpe med umiddelbar identificering af serviceproblemer. For at opretholde udstyrets fortsatte funktionsdygtighed foretager AWS løbende forebyggende vedligeholdelse.

Datalagring og backup

Adobe lagrer alle Adobe Document Cloud-tjenesters data i Amazon S3, der tilbyder en lagringsinfrastruktur med høj holdbarhed. For at øge holdbarheden lagrer Amazon S3 PUT og COPY-operationer synkront, kundedata på tværs af flere forskellige anlæg og lagrer redundante objekter på flere forskellige enheder på tværs af flere forskellige anlæg i et Amazon S3-område.

Amazon S3 beregner tjeksummer på al netværkstrafik for at registrere ødelæggelse af datapakker ved lagring eller genfinding af data. Datakopiering i forbindelse med Amazon S3 dataobjekter forekommer i det regionale cluster, hvor data gemmes og ikke kopieres til datacenterclustre i andre områder.

Metadata kopieres ved at tage øjebliksbilleder af Amazon EBS-volumener, og lagres på en måde, der minder om Amazon S3. For yderligere oplysninger om AWS-sikkerhed, bedes du se AWS Cloud Security-hjemmesiden.

Administration af ændringer

AWS autoriserer, logger, tester, godkender og dokumenterer ændringer af rutiner, nødsituationer og konfigurationsændinger for eksisterende AWS-infrastruktur i overensstemmelse med branchestandarder for lignende systemer. Amazon planlægger opdateringer af AWS for at minimere enhver kundepåvirkning. AWS kommunikerer med kunder, enten via e-mail eller gennem AWS Service Health Dashboard, når det er sandsynligt, at tjenestebrug har den modsatte virkning. Adobe opretholder også en Adobe systemstatus for Adobe Document Cloud.

Administration af rettelser

AWS bærer ansvaret for rettelsessystemer, der understøtter leveringen af AWS-tjenester, såsom hypervisoren og netværkstjenester. Adobe er ansvarlig for rettelse af sine gæsteoperativsystemer (OS), software og applikationer, der kører i AWS. Når det er nødvendigt med rettelser, leverer Adobe hellere en ny, præ-hærdet hændelse af operativsystemet og applikationen end en aktuel rettelse.

AWS fysiske og miljømæssige kontroller

AWS fysiske og miljømæssige kontroller fremgår specifikt i SOC Type 1 og SOC Type 2 rapporter. Følgende afsnit fremhæver nogle af de sikkerhedsforanstaltninger og -kontroller, der findes hos AWS-datacentre over hele verden. For yderligere oplysninger om AWS-sikkerhed, bedes du se AWS Cloud Security-hjemmesiden.

Fysisk anlægssikkerhed

AWS-datacentre bruger arkitektoniske og tekniske tilgange iht. branchestandarden. AWS-datacentre er placeret i ukarakteristiske anlæg, og Amazon kontrollerer fysisk adgang både ved perimeter og ved bygningernes indgangspunkter vha. professionelt sikkerhedspersonale, videoovervågning, IDS'er og andre elektroniske anordninger. Autoriseret personale skal bestå to-faktor-godkendelse minimum to gange for at tilgå datacentergulve. Alle gæster og leverandører skal fremvise identifikation og tilmeldes og konstant ekskorteres af autoriseret personale.

AWS tilbyder kun datacenteradgang og informationer til medarbejdere og leverandører, som har et berettiget virksomhedsbehov for sådanne privilegier. Når en medarbejder ikke længere har et virksomhedsbehov for disse privilegier, tilbagekaldes hans eller hendes adgang straks, selvom han eller hun forsætter med at være medarbejder hos Amazon eller AWS. Al fysisk adgang til datacentre fra AWS-medarbejderes side logges og kontrolleres rutinemæssigt.

Brandbekæmpelse

AWS installerer automatisk branddetektion og -bekæmpelse i alle AWS-datacentre. Branddetektionssystemet anvender røgdetektorer i alle datacentermiljøer, mekaniske og elektriske infrastrukturområder, kølerum og generatorudstyrsrum. Disse områder er beskyttet af enten våd-rørs-, dobbeltlåste, offensive eller gassprinklersystemer.

Kontrolleret miljø
AWS anvender et system til klimakontrol for at opretholde en konstant driftstemperatur for servere og anden hardware, som forhindrer overophedning og reducerer muligheden for serviceafbrydelser. AWS-datacentre opretholder atmosfæriske betingelser ved optimale niveauer. AWS-personale og systemer overvåger og kontrollerer såvel temperatur som fugtighed ved passende niveauer.

Nødstrøm
AWS-datacentrenes elkraftsystemer er designet, så de er helt redundante og kan vedligeholdes uden at påvirke driften - 24 timer i døgnet, syv dage om ugen. UPS-enheder (nødstrømsforsyninger) sørger for nødstrøm i tilfælde af strømsvigt til kritiske og altafgørende belastninger i anlægget. Datacentre bruger generatorer til at skaffe nødstrøm til hele anlægget.

Genskabelse af data ved nedbrud
AWS-datacentre omfatter et højt tilgængelighedsniveau og kan klare system- eller hardwarenedbrud med minimal påvirkning. Da de er bygget i clustre i forskellige globale områder, er alle datacentre altid online 24×7×365 for at servicere kunderne - ingen datacentre er deaktive. I tilfælde af nedbrud flytter automatiserede processer kundedatatrafikken væk fra det påvirkede område.

Der anvendes kerneapplikationer i en N+1 konfiguration, så i tilfælde af et datacenternedbrud er der tilstrækkelig kapacitet til at sørge for, at trafikken er belastningsbalanceret til de resterende steder. For yderligere oplysninger om AWS-protokoller om genskabelse af data ved nedbrud, bedes du se AWS Cloud Security-hjemmesiden.

Adobe risiko- og sårbarhedsstyring
Adobe bestræber sig på at sikre, at vores risiko- og sårbarhedsstyring, hændelsesreaktion, begrænsning og løsningsproces er hurtig og præcis. Vi overvåger løbende trusselsbilledet, deler viden med sikkerhedseksperter over hele verden, løser hurtigt hændelser, når de opstår og sender disse oplysninger tilbage til vores udviklingsteams for at hjælpe med at opnå de højeste sikkerhedsniveauer for alle Adobes produkter og tjenester.

Indtrængningstest
Adobe godkender og arbejder sammen med førende tredjepart sikkerhedsfirmaer om at udføre indtrængningstest, der kan afsløre potentielle sikkerhedssvagheder og forbedre den overordnede sikkerhed af Adobes produkter og tjenester. Efter modtagelse af rapporten, som stammer fra tredjeparten, dokumenterer Adobe disse svagheder, evaluerer alvorsgraden og prioriteten, og udarbejder derefter en begrænsningsstrategi eller udbedringsplan. Adobe gennemfører en komplet indtrængningstest hvert år og udfører sårbarhedsscanninger på en månedlig basis.

Internt udfører Adobe Document Clouds sikkerhedsteam en risikovurdering af alle Document Cloud-komponenter og tjenester hvert kvartal og inden hver frigivelse. Document Clouds sikkerhedsteam samarbejder med førende eksperter inden for teknisk drift og udvikling for at hjælpe med at sikre, at alle højrisiko-sårbarheder begrænses inden hver frigivelse. For yderligere oplysninger om Adobes indtrængnings-testprocedurer, bedes du se Adobe Secure Engineering-oversigten.

Hændelsesreaktion og underretning
Der udvikles nye sårbarheder og trusler hver eneste dag, og Adobe bestræber sig på at reagere på og begrænse nyopdagede trusler. Udover at abonnere på branchedækkende lister med sårbarhedsunderretning, herunder United States Computer Emergency Readiness Team (US-CERT), Bugtraq og SANS, abonnerer Adobe også på de seneste sikkerhedsalarmeringslister, der udsendes af de vigtigste sikkerhedsleverandører.

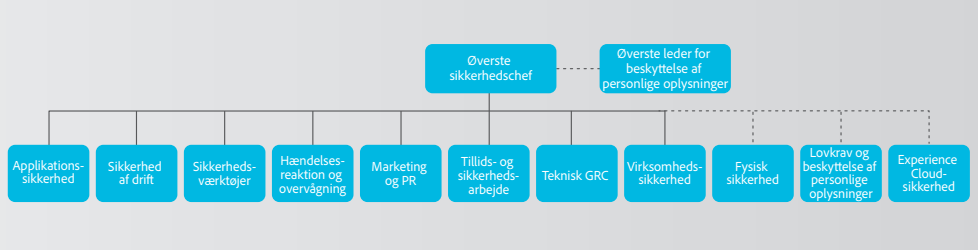
For yderligere oplysninger om Adobes hændelsesreaktion og underretningproces, bedes du se Adobes hændelsesreaktionsoversigt.

Kriminaltekniske analyser
I forbindelse med hændelsesefterforskninger følger Document Cloud-teamet Adobes kriminaltekniske analyseproces, som omfatter komplet billedoptagelse eller hukommelsesdump for en berørt maskine(r), bevissikring og sporbarhedsoptagelse(r).

Adobes sikkerhedsorganisation

Som en del af vores indsats for vores produkters og tjenesters sikkerhed, koordinerer Adobe alle sikkerhedsbestræbelser under den sikkerhedsansvarlige chef (CSO). CSO'ens kontor koordinerer alle sikkerhedsinitiativer for produkter og tjenester og implementeringen af Adobe Secure Product Lifecycle (SPLC).

CSO'en styrer også Adobe Secure Software Engineering Team (ASSET), et dedikeret, centralt team med sikkerhedseksperter, der fungerer som konsulenter for de vigtigste Adobe produkt- og driftsteams, herunder Adobe Document Cloud-teamet. ASSETs efterforskere arbejder med individuelle Adobe produkt- og driftsteam og bestræber sig på at opnå det rette sikkerhedsniveau for produkter og tjenester, og rådgive disse teams om sikkerhedsrutiner for tydelige og repeterbare processer med henblik på udvikling, udrulning, operationer og hændelsesreaktion.



Adobe sikkerhedsorganisation

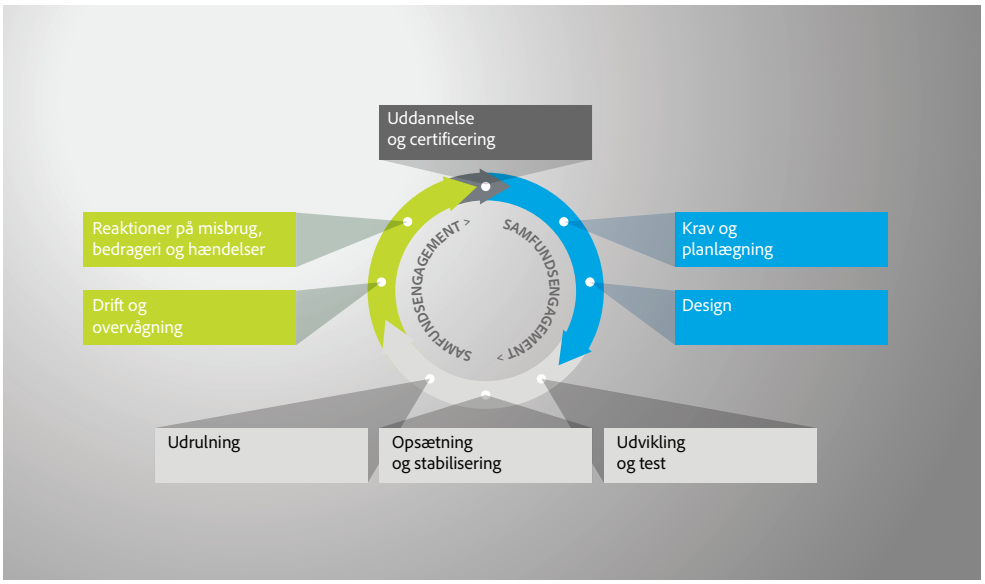
Adobe sikker produktudvikling

Som med andre vigtige Adobe produkt- og tjenesteorganisationer anvender Adobe Document Cloud-organisationen Adobe SPLC-processen. Med et omfattende sæt af adskillige hundrede specifikke sikkerhedsaktiviteter, der spænder lige fra praksis for softwareudvikling, processer og værktøjer, er Adobe SPLC integreret i flere forskellige trin af produktlevetiden, fra design og udvikling til kvalitetssikring, testning og udrulning. ASSETs sikkerhedsspecialister giver specifik SPLC-vejledning for hvert enkelt hovedprodukt eller -tjeneste på basis af en vurdering af de potentielle sikkerhedsproblemer. Suppleret af et kontinuerligt samfundsmæssigt engagement udvikler Adobe SPLC sig, så den er up-to-date, når der sker ændringer i teknologi, sikkerhedspraksis og trusselsbillede.

Adobe SPLC (sikker produktlevetid)

Adobe SPLC-aktiviteter omfatter, afhængig af den specifikke Adobe Document Cloud-komponent, nogle af eller alle de følgende, anbefalede best practices, processer og værktøjer:

- Sikkerhedstræning og certificering for produktteams
- Produktsundhed, risiko og trusselsbilledeanalyse
- Sikre kodevejledninger, regler og analyse
- Tjenesteplaner, sikkerhedsværktøjer og testmetoder, der vejleder Adobe Document Cloud sikkerhedsteamet om at hjælpe med at håndtere Open Web Application Security Project (OWASP) de 10 mest kritiske webapplikationssikkerhedsrisici og CWE/SANS de 25 farligste softwarefejl
- Gennemgang af sikkerhedsarkitekturen og indtrængningstest
- Gennemgang af kildekoder for at hjælpe med at begrænse kendte fejl, som kunne medføre sårbarheder
- UGC-validering
- Applikation og netværksscanning
- Gennemgang af fuld parathed, reaktionsplaner og frigivelse af udviklers uddannelsesmaterialer



Adobe SPLC (sikker produktlevetid)

Adobe certificeringsprogram for softwaresikkerhed

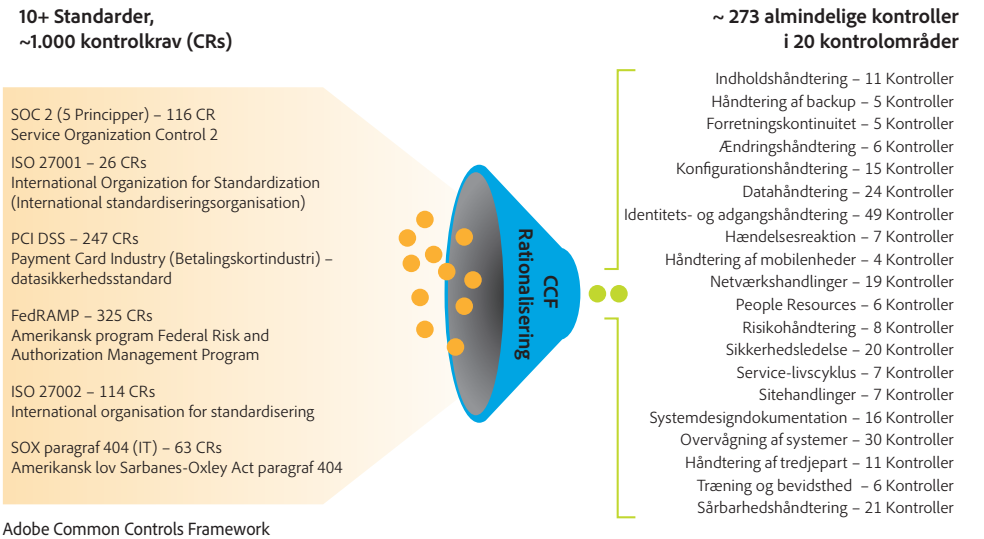
Som en del af Adobe SPLC afholder Adobe løbende sikkerhedstræning i udviklingsteams for at forbedre sikkerhedskendskabet i virksomheden og forbedre vores produkters og tjenesters overordnede sikkerhed. Medarbejdere, der deltager i Adobe certificeringsprogram for softwaresikkerhed opnår forskellige certificeringsniveauer ved at fuldføre sikkerhedsprojekter. For yderligere oplysninger om vores produktsikkerhedspraksis kan du læse Adobe Secure Engineering-oversigten.

For yderligere oplysninger om Adobes certificeringsprogram for softwaresikkerhed, kan du læse hvidbog om Adobes sikkerhedskultur.

Document Cloud-tjenesteoverholdelse

Adobe CCF (Common Controls Framework) er et sæt sikkerhedsaktiviteter og overholdelseskontroller, der implementeres i vores produktdriftsteams samt i forskellige dele af vores infrastruktur- og applikationsteams.

Ved oprettelsen af CCF analyserede Adobe kriterierne for de mest almindelige sikkerhedscertificeringer for cloudbaserede virksomheder og skar de mere end 1.000 krav ned til Adobes specifikke kontroller, der refererer til cirka en halv snes branchestandarder.



Adobe Common Controls Framework

Aktuelle bestemmelser og overholdelse for Adobe Document Cloud-tjenester

SOC 2 er et sæt sikkerhedsprincipper der definerer de vigtigste praksiskontroller med henblik på sikkerhed, fortrolighed og datasikkerhed. Adobe Document Cloud-tjenester lever op til SOC 2 Type 2 (sikkerhed og tilgængelighed).

ISO 27001 er et sæt bestående af globalt anvendte standarder, som definerer skrappe sikkerhedskrav og giver en systematisk tilgang til håndteringen af kundeinformationers fortrolighed, integritet og tilgængelighed. Adobe Document Cloud-tjenester lever op til ISO 27001:2013.

Industristandarden for datasikkerhed for betalingskort (PCI DSS) er en egenudviklet standard for informationssikkerhed for organisationer, der håndterer betalingskortoplysninger, som f.eks. kreditkortnumre. Ved at være en serviceleverandør, der overholder PCI DSS, kan Adobe hjælpe kunder med at leve op til PCI-krav for sikker håndtering af personligt identificerbare data, der henviser til en kortholder.

Den amerikanske GLBA-lov (Gramm-Leach-Bliley Act) kræver, at finansielle institutioner sikrer deres kunders personlige data. Adobe Document Cloud-tjenester er GLBA-forberedt, hvilket betyder, at de sætter vores finansielle kunder i stand til at overholde GLBA-krav til brug af serviceudbydere.

Det amerikanske FedRAMP-program (Federal Risk and Authorization Management Program) er et offentligt program, som har en standardiseret tilgang til sikkerhedsvurdering, godkendelse og kontinuerlig overvågning i forbindelse med cloudprodukter og -tjenester. Adobe Document Cloud-tjenester er skræddersyet til FedRAMP, hvilket betyder, at de sætter vores kunder i stand til at overholde FedRAMP-kravene.

Den amerikanske FERPA-lov (Family Educational Rights and Privacy Act) er beregnet til at bevare fortroligheden af uddannelsesdokumenter og adresseoplysninger for amerikanske studerende. Inden for FERPAs retningslinjer kan Adobe kontraktligt indgå aftale om at fungere som "skoletjenestemand" i forbindelse med håndteringen af regulerede data om studerende, så vores uddannelseskunder er i stand til at overholde FERPA-kravene.

Den amerikanske SAFE-BioPharma-standard beskriver krav for standardiseret identitetstillid i forbindelse med enten identitetsgodkendelse eller digital underskrivelse. Adobe Document Cloud er certificeret, så den overholder den digitale identifikationsstandard SAFE-BioPharma. Adobe Acrobat DC er sikker at bruge i og overholder SAFE-BioPharma-arbejdsgange. Adobe Document Cloud-tjenester og Adobe Sign overholder desuden SOC 2 Type 2.

For information om den aktuelle overholdelsesindstilling til Adobe Sign bedes du se Adobe Sign teknisk oversigt.

I sidste ende er det kundernes ansvar at sørge for at overholde deres juridiske forpligtelser og at sikre, at vores løsninger lever op til deres behov for overholdelse og er sikret på den korrekte måde.

Adobe medarbejdere

Adobe har medarbejder og kontorer over hele verden, og implementerer de følgende processer og procedurer på virksomhedsplan for at beskytte virksomheden mod sikkerhedstrusler.

Medarbejderadgang til kundedata

Adobe opretholder segmenterede udviklings- og produktionsmiljøer for Adobe Document Cloud, ved hjælp af tekniske værktøjer for at begrænse adgang på netværks- og applikationsniveau til aktive produktionssystemer. Medarbejdere har specifikke rettigheder til at tilgå udviklings- og produktionssystemer, og medarbejdere uden et legitimt forretningsformål har ikke adgangsrettigheder til disse systemer.

Baggrundstjek

Adobe får rapporter med baggrundstjek til ansættelsesmæssige formål. Den specifikke karakter og omfanget af rapporten, som Adobe typisk søger, omfatter forespørgsler om uddannelsesmæssig baggrund, arbejdshistorik og retsprotokoller, herunder straffeattester og referencer, der stammer fra professionelle og personlige associerede, i overensstemmelse med gældende ret. Disse krav for baggrundstjek gælder for almindelige amerikanske nyansatte medarbejdere, herunder dem som skal administrere systemer eller have adgang til kundeoplysninger. Nye amerikanske vikarer er underlagt krav om baggrundstjek gennem det pågældende vikarbureau, i overensstemmelse med Adobes retningslinjer om baggrundsscreening. Uden for USA udfører Adobe baggrundstjek af visse nye medarbejdere i overensstemmelse med Adobes praksis for baggrundstjek og gældende lokale love.

Medarbejderopsigelse

Når en medarbejder forlader Adobe, sender medarbejderens chef en aftrædelsesformular. Når den er godkendt, indleder Adobe People Resources et e-mailforløb med at informere relevante interessenter om at træffe specifikke handlinger, forud for medarbejderens sidste arbejdsdag. Såfremt Adobe opsiger en medarbejder, sender Adobe People Resources en lignende e-mail ud til relevante interessenter med oplysninger om den specifikke dato og tidspunkt for ansættelsesforholdets ophør.

Adobe Corporate Security planlægger derefter følgende handlinger med henblik på at sikre, at vedkommende, efter afslutning af medarbejderens sidste ansættelsesdag, ikke længere har adgang til Adobes fortrolige filer eller kontorer:

- Fjernelse af e-mailadgang
- Fjernelse af VPN-fjernadgang
- Ugyldiggørelse af kontor- og datacenterskilt
- Ophør af netværksadgang

På forespørgsel kan chefer anmode bygningssikkerhedsvagter om at eskortere den opsagte medarbejder ud af Adobes kontor eller bygning.

Anlægssikkerhed

Hvert enkelt Adobe virksomhedskontor har ansat vagter på stedet for at beskytte lokaliteterne 24×7. Adobes medarbejdere har et id-adgangskort til bygningen. Besøgende kommer ind gennem hovedindgangen, registreres hos receptionisten, når de kommer og går, viser et midlertidigt gæste-id-kort og ledsages af en medarbejder. Adobe holder alt serverudstyr, udviklingsmaskiner, telefonsystemer, fil- og mailservere samt andre følsomme systemer låst til hver en tid i klimastyrede serverrum, hvortil kun personale med de behørige rettigheder har adgang.

Virusbeskyttelse

Adobe scanner alle ind- og udgående forretnings-e-mails for kendte malwaretrusler.

Hemmeligholdelse af kundedata

Adobe behandler altid alle kundedata fortroligt. Adobe hverken anvender eller udveksler informationer, der er indsamlet på vegne af en kunde, medmindre det er tilladt i en kontrakt med den pågældende kunde og fremgår af Adobes Betingelser for brug og Adobes Politik om personlige oplysninger.

Konklusion

Adobes proaktive tilgang til sikkerhed og skrappe procedurer, der er beskrevet i dette dokument, er med til at beskytte sikkerheden af Adobe Acrobat DC, Acrobat Reader DC og Document Cloud-tjenester - og dine fortrolige data. Hos Adobe tager vi dine digitale oplevelsers sikkerhed meget alvorligt. Vi overvåger kontinuerligt udviklingen af trusselsbilledet, så vi er på forkant med skadelige aktiviteter og er med til at sørge for vores kundedatas sikkerhed.

For yderligere oplysninger kan du besøge Adobe Trust Center.

Adobe

Adobe Systems Nordic AB
Box 47, 164 93 Kista, Sverige
www.adobe.dk, www.adobe.com