Yleiskuvaus Acrobat DC:n tietoturvasta

Maailman johtava PDF-ratkaisu dokumenttien luontiin, muokkaukseen ja hallintaan

Sisältö

1: Dokumenttien tietoturva
2: Sovellusten tietoturva
5: Pilvipalvelun tietoturva
5: Integraatio käyttöjärjestelmäarkkitehtuureihin
6: Kätevämpi käyttöönotto ja hallinta
7: Yhteenveto

Kun luotat yrityksesi tiedot kolmannen osapuolen sovellukselle, suojaus on ratkaisevan tärkeää. Adobe on ollut yli 20 vuoden ajan johtava suojattujen digitaalisten dokumenttien toimittaja ja edelläkävijä PDF-standardin ja digitaalisten allekirjoitusten kehityksessä. Sadattuhannet organisaatiot ovat tuottaneet miljardeja PDF-tiedostoja maailmanlaajuisesti luottaen Adobe Acrobat -ohjelmistoon ja siihen, että Adobe PDF:n avulla ne voivat valmistella, suojata ja jakaa kriittisimpiä dokumenttejaan joka päivä.

Adobe Acrobat DC ja Adobe Document Cloud -palvelut ovat täydellinen PDF-ratkaisu nykypäivän mobiilia ja yhdistettyä maailmaa varten. Se yhdistää Acrobat tietokoneohjelmiston ja Acrobat Reader -mobiilisovelluksen, jossa on premium-mobiilitoiminnot ja Document Cloud -palvelut. Niiden avulla organisaatio voi luoda älykkäämpiä dokumenttityönkulkuja, täyttää loppukäyttäjien mobiiliratkaisujen tarpeet ja varmistaa dokumenttien tietoturvan eri laitteissa. Acrobat DC:n avulla olet aina ajan tasalla. Saat uusimmat suojauspäivitykset ja viimeisimmät ominaisuudet, jotka voi ottaa käyttöön oman aikataulun mukaan.

Tämä dokumentti käsittelee Adoben lähestymistapaa tietoturvaan Acrobat DC -ohjelmiston kannalta. Dokumentissa käsitellään dokumenttien, sovellusten ja pilvipalvelun tietoturvaa tietojen ja kokemusten suojaamiseksi edelleen.

Dokumenttien tietoturva

Acrobat DC:n avulla dokumenttien laatijat voivat luoda PDF-dokumentteja ja soveltaa useita suojausmenetelmiä, kuten salausta, käyttöoikeuksia, sertifikaatin allekirjoituksia ja tekstin ja kuvien poistoa hävitystyökaluilla. Acrobat DC:n kätevät makrotoiminnot suojaustehtäväsarjojen määritykseen, joita käyttäjät voivat soveltaa vaivattomasti ilman muodollista koulutusta tai erikoistyökaluja, auttavat käyttäjiä säilyttämään tiedot yksityisinä ja luottamuksellisina.

Salaus

Acrobat DC:n tukemat suojausstandardit:

- 256-bittinen AES-salaus (Advanced Encryption Standard)
- Standardit, joita European Telecommunications Standards Institute (ETSI) tukee

Käyttöoikeudet

Dokumenttien jakaminen on luotettavaa, kun hallitset käyttöoikeuksia käyttämällä salasanoja ja lupia etkä salli muutoksia mihinkään PDF-dokumenttiin sekä rajoitat tulostusta, kopiointia tai dokumentin muokkausta.

Sähköiset ja digitaaliset allekirjoitukset

Acrobat DC:n käyttäjillä on valittavana kaksi työkalua suojattuun allekirjoituksilla työskentelyyn: Send for Signature ja Certificates.

Send for Signature -ratkaisun avulla käyttäjät hallitsevat koko allekirjoitusprosessia, joka on Euroopan unionin, Yhdysvaltojen ja useimpien teollisuusmaiden *sähköisen allekirjoituksen* lakien mukainen. Sen avulla he voivat pyytää allekirjoitusta muilta, seurata allekirjoitusprosessia ja arkistoida allekirjoitettuja dokumentteja ja kirjausketjuja automaattisesti. Koko prosessia hallitaan suojatusti, ja Adobe sertifioi dokumentit ja kirjausketjut koskemattomuuden osoittavalla sinetillä. Send for Signature perustuu *Adobe Signiin*, *Adobe Document Cloud* -ratkaisuun, jonka on puolueettomasti varmennettu täyttävän tiukat suojausvaatimukset, kuten ISO 27001, SOC 2 tyyppi 2 ja HIPAA sekä PCI DSS.

Certificates-työkalulla voit allekirjoittaa dokumentteja varmennepohjaisilla digitaalisilla tunnuksilla, jotka on saatu Adoben hyväksymän luotettavan luettelon (AATL) tai Euroopan unionin luottamusluettelon (EUTL) luottamuspalvelujen tarjoajilta. Allekirjoitus kolmannen osapuolen varmenteiden myöntäjän varmennetunnuksella on yksi suojatuimmista dokumenttien sähköisen allekirjoituksen menetelmistä. Tunnus on erityisesti linkitetty allekirjoittajaan ja tunnus pystyy tunnistamaan allekirjoittajan. Allekirjoittajan varmenne on kryptografisesti sidottu dokumenttiin allekirjoitusvaiheen aikana käyttämällä yksityistä avainta, joka on ainoastaan kyseisellä allekirjoittajalla. Acrobat DC vahvistaa allekirjoituksen – ja allekirjoitetun dokumentin alkuperäisyyden – luomalla automaattisesti yhteyden varmenteiden myöntäjään tarkistusta varten. Tämäntyyppinen allekirjoitus noudattaa PDF:n sähköisten allekirjoitusten standardeja, kuten PDF Advanced Electronic Signature (PAdES) osat 2, 3 ja 4 sekä Yhdysvaltain puolustusministeriön Joint Interoperability Test Command (JITC) -organisaation kryptografian käyttöä ja PKI AES-256-RSA-4096-/SHA-512-algoritmia. Certificates-työkalun avulla voit myös lisätä aikaleimoja dokumentteihin ja varmentaa ne koskemattomuuden osoittavalla sinetillä.

Lisätietoja sähköisistä ja digitaalisista allekirjoituksista on White paper -julkaisussa *Transform business processes with electronic and digital signature solutions*.

Todellinen hävitys

Acrobat DC sisältää sarjan hävitystyökaluja, joilla voi suojata arkaluonteisia tai luottamuksellisia tietoja. Voit poistaa pysyvästi sekä tekstiä että kuvia dokumentista ennen sen jakelua. Voit myös hakea ja hävittää tietoja kaavojen mukaan, kuten kaikki puhelinnumerot, luottokorttien numerot ja sähköpostiosoitteet. Valitut tiedot poistetaan kokonaan tiedostosta eikä vain peitetä, kuten muilla työkaluilla tai menetelmillä.

Dokumentin puhdistustoiminnolla voit poistaa piilotietoja ja muita kuin kuvaobjekteja, kuten metatietoja, joita voi olla PDF-tiedostossa.

Acrobat DC:n parannetut suojaustoiminnot auttavat suojauksessa hyökkäyksiltä, joissa hyödynnetään PDF-tiedostomuotoa asentamaan haittaohjelmia järjestelmään ja/tai poimimaan arkaluoteisia tietoja järjestelmästä.

Sovellusten tietoturva

Tietoturvakäytännöt ovat juurtuneet syvälle Adoben yrityskulttuuriin, ohjelmistokehitykseen ja suunnitteluprosesseihin. Acrobat DC ja Acrobat Reader on suunniteltu alan käyttöoikeuksien hallinnan, tietojen luottamuksellisuuden ja dokumenttien eheyden standardikäytäntöjen mukaisesti dokumenttien, tietojen ja henkilötietojen suojaamiseksi.

Suojaussuunnittelu

Adobe DC -sovellukset on suunniteltu käyttämällä Adobe Secure Product Lifecycle (SPLC) -prosessia. Se sisältää satoja tiukkoja suojaustoimintoja, jotka kattavat ohjelmistokehityksen käytännöt, prosessit ja työkalut. Adobe SPLC on integroitu useisiin Acrobat DC -tuotteen elinkaaren vaiheisiin suunnittelusta ja kehityksestä laadunvarmistukseen, testaukseen ja käyttöönottoon. Katso lisätietoja Adoben tietoturvaprosesseista, yhteisöön osallstumisesta ja Adobe SPLC -prosessista osoitteesta *www.adobe.com/security*.

Adobe Acrobat Reader DC:n suojattu tila

Adobe toimittaa hiekkalaatikkoteknologian uusimman toteutuksen, jota kutsutaan suojatuksi tilaksi ja joka esiteltiin Adobe Reader X:ssä. Sen tarkoituksena on suojata yksittäistä käyttäjää ja koko organisaatiota haittakoodilta, joka yrittää kirjoittaa tietokoneen tiedostojärjestelmään tai lukea siitä PDF-tiedostojen välityksellä.

Acrobat Reader DC:ssä suojattu tila laajentaa suojauksen sellaisia hyökkääjiä vastaan, jotka yrittävät asentaa tietokonejärjestelmään haittaohjelman, siten, että se estää ei-toivottuja henkilöitä käyttämästä ja poimimasta arkaluonteisia tietoja ja immateriaaliomaisuutta tietokoneesta tai yrityksen tietoverkosta.

Suojattu tila otetaan käyttöön aina, kun Acrobat Reader DC käynnistyy. Suojattu tila rajoittaa ohjelmalle annettavaa pääsytasoa. Tämä suojaa Windows®-käyttöjärjestelmän laitteita haitallisilta PDF-tiedostoilta, jotka saattavat yrittää kirjoittaa tietokoneen tiedostojärjestelmään tai lukea siitä, poistaa tiedostoja tai muuttaa järjestelmän tietoja muulla tavalla. Readerin suojattu tila (Windows 8.1- ja uudemmat versiot) voi toimia nyt AppContainerissa. Kun haluat lisätietoja AppContainerista: *https://msdn.microsoft.com/en-us/library/windows/desktop/mt595898(v=vs.85).aspx*.

Lisäksi Adobe suorittaa olemassa olevan koodin säännöllisiä tarkistuksia ja vahvistaa koodia tarpeen mukaan osana yrityksen jatkuvia toimenpiteitä turvallisuuden integroimiseksi tuotteen elinkaaren useaan vaiheeseen SPLC -prosessin kautta. Tämä parantaa edelleen sovelluksen tietoturvaa ja edistää datan turvallisuutta Adoben tuotteita käytettäessä.

Mitä hiekkalaatikko tarkoittaa?

Hiekkalaatikko on tietoturva-ammattilaisten arvostama menetelmä, joka luo toimiville ohjelmille rajoitetun suoritusympäristön vähäisillä oikeuksilla. Hiekkalaatikot suojaavat käyttäjien järjestelmiä, jotta suoritettavaa koodia sisältävät epäluotettavat dokumentit eivät vahingoita niitä. Acrobat Reader DC:n yhteydessä epäluotettava sisältö on mikä tahansa PDF-tiedosto ja sen käynnistämät prosessit. Reader DC käsittelee kaikkia PDF-tiedostoja potentiaalisesti korruptoituneina ja rajoittaa kaiken PDF-tiedoston käsittelyn hiekkalaatikkoon.

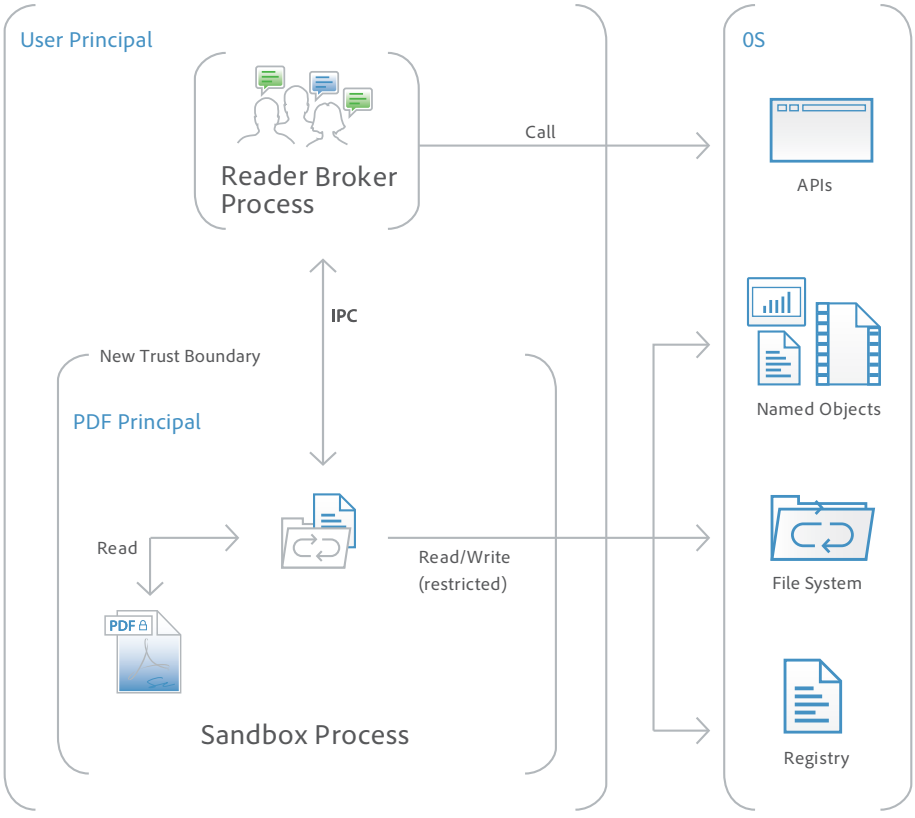
Acrobat DC:n suojattu näkymä

Suojattu näkymä vastaa Acrobat Reader DC:n suojattua tilaa. Se on hiekkalaatikkoteknologian toteutus monipuolisia Acrobat DC -ominaisuuksia varten. Acrobat DC -ohjelmistossa Adobe laajentaa suojatun näkymän toimintaa niin, että se tekee enemmän kuin kirjoituspohjaisten hyökkäysten eston. Näissä hyökkäyksissä yritetään suorittaa haitallinen koodi tietokonejärjestelmässä käyttämällä PDF-tiedostomuotoa lukupohjaisiin hyökkäyksiin, joissa yritetään varastaa arkaluonteisia tietoja tai immateriaaliomaisuutta PDF-tiedostojen avulla.

Suojatun tilan tavoin suojattu näkymä sulkee epäluotettavien ohjelmien (esim. mikä tahansa PDF-tiedosto ja sen käynnistämät prosessit) suorituksen rajoitettuun hiekkalaatikkoon, minkä ansiosta vältetään se, että haitallinen koodi voisi kirjoittaa tietokoneen tiedostojärjestelmään tai lukea siitä PDF-muodon avulla.

Suojattu näkymä olettaa, että kaikki PDF-tiedostot ovat mahdollisesti haitallisia ja rajoittaa käsittelyn hiekkalaatikkoon, ellei nimenomaisesti määritetä, että tiedosto on luotettava. Suojattua näkymää tuetaan molemmissa skenaarioissa, joissa käyttäjät avaavat PDF-dokumentteja – yksittäisessä Acrobat DC -sovelluksessa ja selaimessa. Suojattu tila Windows 8- ja uudemmissa versioissa toimii aina AppContainerissa. Tämä mahdollistaa vielä tehokkaamman lukitun ympäristön asiakkaille, jotka ottavat käyttöön suojatun tilan.

Kun avaat mahdollisesti haitallisen tiedoston suojatussa näkymässä, Acrobat DC näyttää keltaisen viestirivin (YMB) katseluikkunan yläreunassa. Keltainen viestirivi osoittaa, että tiedostoon ei voi luottaa ja muistuttaa, että olet suojatussa näkymässä, missä useat Acrobat DC -ominaisuudet eivät ole käytössä, ja käyttäjän vuorovaikutusta tiedoston kanssa on rajoitettu. Oleellista on, että tiedosto on vain-luku-muodossa ja suojattu näkymä estää upotettua tai liittyvää haitallista sisältöä kajoamasta järjestelmään. Jos luotat tiedostoon ja haluat ottaa kaikki Acrobat DC -toiminnot käyttöön, voit napsauttaa kaikkien toimintojen käyttöönottoa osoittavaa painiketta keltaisella viestirivillä. Tämä toiminto poistaa suojatun näkymän käytöstä ja suo tiedostolle pysyvän luotetun aseman lisäämällä sen Acrobatin etuoikeutettujen sijaintien luetteloon. Kaikki luotettavan PDF-tiedoston avaukset tämän jälkeen poistavat käytöstä suojatun näkymän rajoitukset.



JavaScriptin suoritus

Acrobat DC:ssä on hienostuneet ja granulaariset ohjaukset JavaScriptin suorituksen sallimiseen ja kieltämiseen useissa ympäristöissä, kuten Microsoft Windowsissa ja Macintoshissa. Adobe JavaScript Whitelist Framework ottaa JavaScriptin käyttöön valikoivasti tietyille PDF-tiedostoille, sivustoille, isännille tai dokumenteille, jotka on allekirjoitettu käyttämällä luotettavaa varmennetta. Lisäksi Adobe JavaScript Blacklist Framework -toiminnon avulla JavaScriptiä voi käyttää osana liiketoiminnan työnkulkuja. Se suojaa käyttäjiä ja järjestelmiä hyökkäyksiltä, jotka kohdistuvat tiettyihin JavaScript

Whitelist Framework

Voit ottaa JavaScriptin käyttöön valikoivasti luotetuille työnkuluille sallimalla dokumentit etuoikeutettujen sijaintien avulla, jotka sallivat luottamuksen myöntämisen Microsoft Windowsin suojausvyöhykkeiden tai sertifioitujen dokumenttien perusteella tai lisäämällä tiettyjä tiedostoja, kansioita tai isäntiä.

API -kutsuihin. Kun tietty JavaScript API -kutsu lisätään kielletylle listalle, voit estää sen toteutuksen ottamatta JavaScriptiä täysin pois käytöstä. Voit myös estää yksittäistä käyttäjää ohittamasta päätöstäsi hylätä tietty JavaScript API -kutsu, mikä suojaa koko yritystä haittakoodilta.

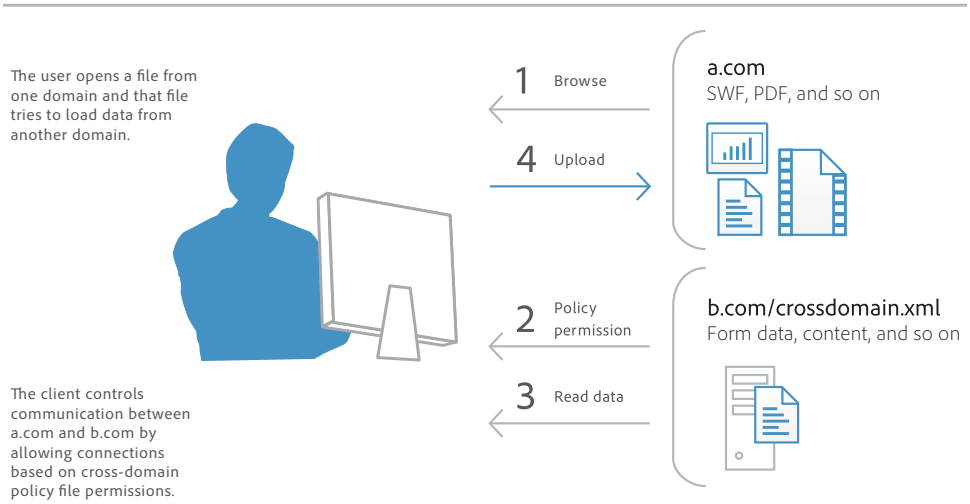
Toimialueiden välinen konfiguraatio

Acrobat DC poistaa käytöstä oletusarvoisesti rajoittamattoman toimialueiden välisen pääsyn sekä Windows- että Mac OS X -asiakkailta, mikä estää hyökkääjiä hyödyntämästä monipuolisia PDF-tiedostoja ja pääsemästä toisen toimialueen resursseihin.

Voit antaa Acrobat DC:lle ja Acrobat Reader DC:lle luvan datan käsittelyyn eri toimialueilla hyödyntämällä sisäistä tukea palvelinpohjaisille toimialueiden välisen menettelytavan tiedostoille. Tätä toimialueiden välistä menettelytapatiedostoa – XML-dokumenttia – isännöidään etätoimialueella. Tämä myöntää pääsyn lähdetoimialueeseen ja sallii Acrobat DC:n tai Acrobat Reader DC:n jatkaa tapahtumaa.

Adoben toimialueiden välinen tuki on hyvä ottaa käyttöön seuraavissa tapauksissa:

- Tarvitaan valikoiva toimialueiden välinen pääsy ja halutaan hyödyntää muita ominaisuuksia, kuten tunnistus, joka perustuu digitaaliseen sertifikaattiin.
- Tarvitaan toimialueiden välisten käyttölupien keskitettyä hallintaa yksittäisestä palvelinpohjaisesta paikasta.
- Toteutetaan työnkulkuja, joihin sisältyy datapyyntöjä useista toimialueista lomaketietojen palauttamiseen, SOAP-pyyntöjä, viitteitä suoratoistomediaan ja NET HTTP -pyyntöjä.



Käyttäjäystävälliset turvahälytykset

Adoben tietokoneohjelmistojen ongelmienkäsittelyn prosessin ja suojaushälytysten lisäksi Acrobat DC:n keltainen viestirivi on käyttäjäystävällinen menetelmä suojaushälytysten viestintään. Kun parannettu suojaus on otettu käyttöön eikä PDF-tiedosto ole etuoikeutettu tai luotettu, keltainen viestirivi tulee esiin, kun PDF yrittää suorittaa mahdollisesti vaarallisen toiminnon, kuten seuraavat:

- Toimialueiden välisen käytön käynnistys
- Etuoikeutetun JavaScriptin suoritus
- JavaScriptin synnyttämän URL:n käynnistys
- Kielletyn JavaScript API:n kutsu
- Datan lisäys
- Komentosarjojen lisäys
- Upotetun perinteisen multimedian toisto

Acrobat DC:ssä ja Reader DC:ssä varoitus- tai virheviestin sisältävä keltainen viestirivi tulee näkyviin dokumentin yläreunaan. Käyttäjä voi valita luottavansa dokumenttiin kerran tai aina. Jos valitaan "aina", dokumentti lisätään sovelluksen etuoikeutettujen dokumenttien luetteloon.

Valinnat-painikkeen avulla käyttäjät voivat asettaa luottamuksen nopeasti yhdeksi kerraksi tai jatkuvaksi. Voit määrittää ennalta tiedostojen, kansioiden ja isäntien luottamustason yrityksenlaajuisesti, jotta keltainen viestirivi ei tule koskaan esiin yrityksen totutuissa työnkuluissa.

Pilvipalvelun tietoturva

Adobe valvoo ja parantaa jatkuvasti pilvipalvelujaan, järjestelmiä ja prosesseja vastatakseen asiakkaiden kasvaviin tietoturvatarpeisiin ja -haasteisiin. Document Cloud -palvelut, kuten Adobe Sign ja PDF-palvelut, joita Acrobat DC käyttää, on suunniteltu varmistamaan dokumenttien luottamuksellisuus, eheys ja käytettävyys. Document Cloud -palvelut ovat ISO 27001-, PCI DSS- ja SOC 2 tyyppi 2 -yhteensopivia ja täyttävät monia muita alakohtaisia säännönmukaisuuden sertifiointeja, standardeja ja säännöksiä. Lisätietoja lähestymistavastamme pilvipalvelun tietoturvaan: *Adobe Document Cloud Security Overview*.

Tietokeskuksen tietoturva

Tällä hetkellä Document Cloud -datakeskus, joka isännöi PDF-palveluita ja tiedostojen tallennusta, sijaitsee American National Standards Instituten (ANSI) tason 4 datakeskuksessa. Sitä hallinnoi luotettu pilvipalveluiden toimittaja, Amazon Web Services (AWS), joka ylläpitää hyvin tiukkaa valvontaa datakeskukseen pääsylle, vikasietoisuudelle, ympäristövalvonnalle ja suojaukselle. Vain hyväksytyt, valtuutetut Adoben työntekijät, pilvipalveluiden toimittajien työntekijät ja alihankkijat, joilla on laillinen, dokumentoitu yritys, pääsevät suojattuihin tiloihin Virginiassa, Yhdysvalloissa. Katso lisätietoja AWS-datakeskuksen suojauksesta osoitteesta *https://aws.amazon.com/security/*.

Tietojen salaus ja tietosuoja

Adoben tuotteet ja palvelut, kuten Document Cloud -palvelut, on suunniteltu ottaen huomioon tietosuoja. Document Cloud salaa at-rest-dokumentit ja -resurssit käyttämällä National Institute of Standards and Technologyn (NIST) Advanced Encryption Standard (AES) 256-bittistä salausta ja tukee Hypertext Transfer Protocol (HTTP) -protokollaa yhteydellä, joka on salattu Transport Layer Security (TLS) -protokollalla sen varmistamiseksi, että myös in-transit-data on riittävästi suojattu.

Document Cloudin työntekijät ja luotetut toimittajat käyttävät asiakkaiden tietoja vain joidenkin liiketoiminta- ja tukitoimintojen suoritukseen tai lain niin vaatiessa. Adobe ei anna minkään maan julkiselle vallalle suoraa tai systemaattista pääsyä tallentamiinsa asiakastietoihin. Katso lisätietoja Adoben tietosuojakäytännöstä osoitteesta *www.adobe.com/fi/privacy*.

Integraatio käyttöjärjestelmäarkkitehtuureihin

Aina käytössä oleva tietoturva

Acrobat DC hyödyntää Windows- ja Mac OS X -käyttöjärjestelmien sisäisiä, aina päällä olevia suojauksia. Ne luovat lisäpuolustuskerroksen hyökkäyksille, jotka yrittävät hallita tietokonejärjestelmiä tai korruptoida muistia.

Tietojen suorituksen esto (DEP) estää datan tai vaarallisen koodin sijoituksen muistipaikkoihin, jotka on määritetty Windows-käyttöjärjestelmän suojaamiksi. Applella on vastaava suojaus Mac OS X Lion -käyttöjärjestelmälle, mukaan lukien Stack DEP ja Heap-based DEP, ja se laajentaa tämän suojauksen 32- ja 64-bittisille sovelluksille, mikä tekee kaikista sovelluksista paremmin hyökkäyksiä kestäviä.

Address Space Layout Randomization (ASLR) piilottaa muistin ja järjestelmäkomponenttien sivutiedoston paikat, mikä tekee kyseisten komponenttien löytämisen vaikeaksi hyökkääjille. Sekä Windows- että Mac OS X -käyttöjärjestelmät käyttävät ASLR-tekniikkaa. Mac OS X Lion -käyttöjärjestelmässä ASLR laajennetaan 32- ja 64-bittisille sovelluksille.

Rekisteritasoinen ja plist-konfiguraatio

Acrobat DC:llä on useita työkaluja turva-asetusten hallintaan, kuten rekisteritaso (Windows) ja plist (Mac OS) -määritykset. Näillä asetuksilla voit määrittää asiakkaat ennen käyttöönottoa ja sen jälkeen ja tehdä seuraavaa:

- Parannetun suojauksen kytkentä päälle tai pois
- Etuoikeutettujen sijaintien kytkentä päälle tai pois
- Ennalta määritettyjen etuoikeutettujen sijaintien määritys
- Tiettyjen ominaisuuksien lukitus ja sovelluskäyttöliittymän poisto käytöstä, jotta loppukäyttäjät eivät voi muuttaa asetuksia
- Melkein minkä tahansa turvallisuuteen liittyvän ominaisuuden poisto käytöstä, käyttöönotto tai konfigurointi

Kätevämpi käyttöönotto ja hallinta

Ohjelmiston suojauksen vahvistus

Tietoturvaparannukset, kuten suojattu näkymä, ovat vain yksi esimerkki laajoista teknisistä investoinneista, joita Adobe on tehnyt Acrobatin vahvistamiseksi uhkia vastaan. Kun Adobe tekee ohjelmistosta vahvemman hyökkäyksiä vastaan, se voi vähentää tai jopa poistaa tarpeen ylimääräisiin päivityksiin ja pienentää säännöllisesti ajoitettujen päivitysten kiireellisyyttä. Kaikki tämä lisää operatiivista joustavuutta ja pienentää kokonaiskustannuksia erityisesti laajoissa ympäristöissä, joilla on tiukat tietoturvavaatimukset.

Citrixin ja sovelluksen virtualisoinnin tuki

Voit toimittaa käyttäjien tarvitsemat Acrobat-toiminnot suojattuun etäkäyttöön nimetyn käyttäjän lisensoinnin tuen avulla Citrix XenApp-, Citrix XenDesktop-, VMware Horizon- ja Microsoft App-V -ympäristöille.

Enterprise Mobility Management (EMM) -ratkaisujen tuki

Adobe on sitoutunut auttamaan yritysasiakkaita täyttämään mobiilin liiketoiminnan tuottavuusratkaisujen kysynnän ja varmistamaan samalla yrityksen suojauksen ja säännönmukaisuuden. Acrobat Reader- ja Adobe Sign -mobiilisovellukset tukevat Androidia Work EMM -alustalle, ja Adobe Acrobat Reader for Microsoft Intune on saatavana iOS- ja Android-ympäristöihin. Acrobat Reader tukee myös AppConfig -ympäristöä. Lisätietoja *IT-resursseista*

Windows-ryhmäkäytännön objektien ja Microsoft Active Directory -toimialueen tuki

Windows Server -ryhmäkäytännön objektien (GPO) ja Microsoft Active Directory -toimialueen avulla voit automatisoida tietokonejärjestelmien one-to-many-hallinnan. Adobe on lisännyt tuen sertifioiduille Microsoft Active Directory Administrative (ADM) -malleille Acrobat DC:n ryhmäkäytäntöä varten, mikä mahdollistaa sen, että voit tarjota on-demand-ohjelmistoasennuksia ja sovellusten automaattisen korjauksen. Kun sovelluksia on määritettävä edelleen käyttöönoton jälkeen, voidaan soveltaa vaadittuja asetuksia koko organisaatiolle käyttämällä ADM-malleja.

Microsoft SCCM- ja SCUP-tuki

Acrobat DC:n avulla voi tuoda ja julkistaa tehokkaasti päivityksiä Microsoft System Center Configuration Managerin (SCCM) kautta ja varmistaa, että hallituissa Windows-tietokoneissa on uusimmat tietoturvakorjaukset ja päivitykset.

Microsoft System Center Updates Publisher (SCUP) -luettelojen tuen avulla voit automatisoida päivitykset Acrobat DC -ohjelmistoon koko organisaatiossasi sekä selkeyttää alustavia ohjelmiston käyttöönottoja. SCUP voi tuoda automaattisesti minkä tahansa Adoben julkistaman päivityksen heti, kun se on käytettävissä. Näin Acrobat DC:n käyttöönotosta tulee vaivattomampi ja tehokkaampi. Integrointi SCCM/SCUP:n kanssa auttaa pienentämään Adoben ohjelmistojen kokonaiskustannuksia, koska korjaukset voidaan toimittaa organisaationlaajuisesti yksinkertaisemmin ja nopeammin.

Apple Package Installer- ja Apple Remote Desktop -tuki

Acrobat DC:ssä Adobe on toteuttanut Mac OS X -käyttöjärjestelmän toimittaman standardin Apple Package Installerin sovelluskohtaisen Adobe Installerin sijasta. Tämän ansiosta Acrobat-ohjelmiston käyttöönotto yrityksen Macintosh-tietokoneissa on vaivattomampaa, koska Apple Remote Desktop -hallintaohjelmistoa voi käyttää alustavien ohjelmistokäyttöönottojen sekä jatkopäivitysten ja korjausten hallintaan keskitetystä paikasta.

Kumulatiiviset, säännöllisesti ajoitetut päivitykset ja korjaukset

Adobe toimittaa ennakoivasti säännölliset päivitykset, jotka sisältävät sekä ominaisuuksien päivityksiä että tietoturvakorjauksia, mikä auttaa ohjelmiston pitämisessä ajan tasalla. Adobe toimittaa säännöllisten päivitysten lisäksi tarpeen mukaan korjauksia, joiden on tarkoitus vastata nopeasti nollapäivähyökkäyksiin. Adobe hyödyntää kumulatiivisia korjauksia mahdollisimman paljon pienentääkseen järjestelmien päivityksen aiheuttamaa vaivaa ja kustannuksia. Adobe myös testaa tietoturvakorjauksia kattavasti ennen julkistusta, jotta varmistetaan yhteensopivuus nykyisten asennusten ja työnkulkujen kanssa.

Kunkin suunnitellun päivityksen päivämäärä julkistetaan Adobe Product Security Incident Response Team (PSIRT) -blogissa osoitteessa *blogs.adobe.com/psirt*.

Katso Adoben tuotteiden uusimmat tietoturvatiedotteet ja tiedotukset osoitteesta *www.adobe.com/ support/security*. Katso lisätietoja Adoben tuotteista ja tietoturvaominaisuuksista Adoben tietoturvakirjastosta osoitteesta *www.adobe.com/go/learn_acr_appsecurity_en*.

Adobe Customization Wizard ja Enterprise Toolkit

Adobella on seuraavat työkalut yrityksenlaajuisten käyttöönottojen tehokkaampaan hallintaan:

- **Adobe Customization Wizard** – Maksuton ladattavissa oleva apuohjelma, jonka avulla voi mukauttaa Acrobat-asennusohjelman ja määrittää sovelluksen ominaisuudet ennen käyttöönottoa.
- **Adobe Enterprise Toolkit (ETK) Acrobatille ja Windowsille** – Automaattisesti päivittyvä mukautettava sovellus, joka sisältää asetusten referenssit. Adobe ETK sisältää myös koko ajan laajenevan joukon muita yritysten hallintohenkilökuntaa kiinnostavia resursseja.

Lisätietoja näistä resursseista on osoitteessa *IT resources*.

Yhteenveto

Adobe siirtää PDF-dokumenttien ja tietojen turvallisuuden aivan uudelle tasolle Acrobat DC:n avulla. Acrobat DC tarjoaa korkeamman tietoturvatason pienemmillä kokonaiskustannuksilla kuin mikään sitä edeltävä Acrobatin versio. Sen tarjoaa mm. laajennetun sovellussuojauksen arkaluonteisten yritystietojen ja immateriaaliomaisuuden varastamista vastaan, vaarallisten haittaohjelmien asennuksen estämisen tietokonejärjestelmiin tai integroinnin lisätyökaluihin, jotka tekevät yrityksenlaajuisten käyttöönottojen hallinnan aikaisempaa vaivattomammaksi.

Lisätietoja
Ratkaisun yksityiskohdat:
www.adobe.com/security

Adobe

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

7/17