Visão geral da segurança no Acrobat DC

A solução de PDF líder de mercado para criar, editar e gerenciar documentos

Índice

Quando você confia suas informações de negócio a um aplicativo de terceiros, a segurança é um ponto crítico. A Adobe tem mais de 20 anos de liderança em documentos digitais seguros e foi a pioneira na criação do padrão para PDF e assinaturas digitais. Milhares de organizações produziram bilhões de PDFs no mundo todo, pois confiam no software Adobe Acrobat e no Adobe PDF para ajudá-las a preparar, proteger e compartilhar seus documentos mais importantes diariamente.

O Adobe Acrobat DC com serviços da Adobe Document Cloud é a solução de PDF completa para o mundo atual, móvel e conectado. Ela combina o software de desktop do Acrobat com o aplicativo Adobe Acrobat Reader e recursos premium para dispositivos móveis e os serviços da Document Cloud para ajudar as organizações a criar fluxos de trabalho de documentos mais inteligentes e atender à demanda dos usuários finais por soluções móveis enquanto garante a segurança dos documentos em todos os dispositivos. Com o Acrobat DC, você sempre fica atualizado com acesso às atualizações de segurança e os recursos mais recentes que podem ser implantados de acordo com o seu cronograma.

Este documento contém informações abrangentes sobre segurança e como ela se relaciona com o Acrobat DC, abrangendo segurança de documentos, aplicativos e nuvem, para ajudá-lo a proteger ainda mais suas informações e sua experiência.

Segurança de documentos

Autores de documentos podem usar o software Acrobat DC para criar documentos em PDF e aplicar inúmeras medidas de segurança, incluindo criptografia, controle de acesso, assinaturas de certificado e remoção permanente de textos e imagens por meio de ferramentas de remoção. A conveniência de usar a funcionalidade Ações no Acrobat DC para definir um conjunto de tarefas de segurança que os usuários podem aplicar facilmente sem treinamento formal ou ferramentas especiais facilita para as organizações manterem a privacidade e a confidencialidade das informações.

Criptografia

Padrões de segurança compatíveis com o Acrobat DC:

- Padrão de Criptografia Avançada (AES) de 256 bits
- Padrões compatíveis com o European Telecommunications Standards Institute (ETSI)

Controle de acesso

Compartilhe documentos de maneira confidencial, aplicando facilmente senhas e permissões para controlar o acesso ou impedir modificações em documentos PDF, restringindo impressões, cópias e alterações de documento.

Assinaturas digitais e eletrônicas

No Acrobat DC, os usuários podem escolher entre duas ferramentas diferentes para trabalhar de maneira segura com assinaturas: Envio para assinatura e Certificados.

O Envio para assinatura permite que os usuários gerenciem todos os processos de assinatura em conformidade com as leis de *assinatura eletrônica* nos Estados Unidos, na União Europeia e nos demais países industrializados. Com ele, é possível solicitar assinaturas de outras pessoas, monitorar o processo de assinatura e arquivar documentos assinados e trilhas de auditoria automaticamente. O processo é gerenciado de modo seguro e os documentos e as trilhas de auditoria são certificadas pela Adobe com um

selo inviolável. O Envio para assinatura é capacitado pelo *Adobe Sign*, uma solução da *Adobe Document Cloud*, que é certificado de modo independente para atender aos requisitos de segurança mais rigorosos, como ISO 27001, SOC 2 Tipo 2 e HIPAA, além de PCI DSS.

A ferramenta Certificados permite a você assinar documentos com IDs digitais baseadas em certificados de provedores de serviço confiáveis na lista aprovada da Adobe (AATL) ou nas listas aprovadas da União Europeia (EUTL). Assinar com uma ID de certificado emitida por uma autoridade certificadora confiável é um dos métodos mais seguros para assinar documentos eletronicamente. A ID é vinculada exclusivamente ao signatário, permitindo sua identificação. O certificado do signatário é vinculado de maneira criptografada ao documento durante a etapa de assinatura usando a chave privada exclusiva do signatário em questão. O Acrobat DC valida a assinatura e a autenticidade do documento assinado conectando-se automaticamente à autoridade certificadora para verificação. Esse tipo de assinatura tem conformidade com os padrões de assinatura eletrônica em PDF, incluindo PDF Advanced Electronic Signature (PAdES) Parts 2, 3 e 4, além do uso da criptografia U.S. Department of Defense Joint Interoperability Test Command (JITC) e PKI com AES-256/RSA-4096/SHA-512. A ferramenta Certificados também permite que você adicione marcações de data e hora aos documentos e os certifique com um selo inviolável.

Para saber mais sobre assinaturas eletrônicas e digitais, leia o white paper *Transformar processos de negócios com soluções de assinatura eletrônica e digital*.

Remoção de verdade

O Acrobat DC apresenta um conjunto de ferramentas de remoção que ajuda na proteção de informações sensíveis e confidenciais. Você pode excluir permanentemente textos e imagens gráficas em um documento antes de distribuí-lo. Você pode até pesquisar e remover com base em padrões, como números de telefone, números de cartão de crédito e endereços de email. As informações selecionadas são totalmente removidas do arquivo, não apenas disfarçadas, como acontece em outras ferramentas ou métodos.

Com o recurso Limpar documentos, remova informações ocultas e objetos não gráficos, como metadados possivelmente presentes no PDF.

Os recursos aprimorados de segurança no Acrobat DC auxiliam na proteção contra ataques que tentam explorar o formato de arquivo PDF para instalar malwares no sistema e/ou extrair dados confidenciais do sistema.

Segurança de aplicativos

Na Adobe, as práticas de segurança estão enraizadas em nossa cultura, nosso desenvolvimento de software e nos processos de engenharia. O Acrobat DC e o Acrobat Reader foram criados com as práticas de segurança padrão do setor para gerenciamento de acesso, confidencialidade de dados e integridade de documentos para ajudá-lo a proteger documentos, dados e informações pessoais.

Engenharia segura

Os aplicativos Adobe DC foram criados com os processos Adobe Secure Product Lifecycle (SPLC), que incluem centenas de atividades de segurança rigorosas que englobam práticas, processos e ferramentas de desenvolvimento de software. O Adobe SPLC é integrado a várias fases do ciclo de vida dos produtos Acrobat DC, desde o design e o desenvolvimento ao controle de qualidade, ao teste e à implantação. Para obter mais informações sobre os processos de segurança da Adobe, o envolvimento da comunidade e o Adobe SPLC, consulte *www.adobe.com/security*.

Modo protegido no Adobe Acrobat Reader DC

Para proteger você e sua organização de códigos maliciosos que tentam usar o formato PDF para gravar ou ler no sistema de arquivos do computador, a Adobe fornece uma implementação inovadora de tecnologia para áreas restritas chamada "Modo protegido", o qual foi introduzido no Adobe Reader X.

No Acrobat Reader DC, o Modo protegido amplia a proteção contra invasores que tentam instalar malwares no sistema do computador e impede que indivíduos mal-intencionados acessem e extraiam dados confidenciais e propriedade intelectual do computador ou da rede corporativa.

O Modo protegido é ativado por padrão quando o Acrobat Reader DC é iniciado. Ele limita o nível de acesso concedido ao programa, protegendo os sistemas com Microsoft Windows® de arquivos PDF que tentam gravar ou ler no sistema de arquivos do computador, excluir arquivos ou, de modo geral, modificar informações do sistema. O Modo protegido do Reader (no Windows 8.1 e posterior) pode ser executado em um AppContainer. Para saber mais sobre AppContainer: *https://msdn.microsoft.com/en-us/library/windows/desktop/mt595898(v=vs.85).aspx*.

E, como parte dos esforços contínuos da empresa para integrar a segurança aos vários estágios do ciclo de vida do produto por meio do processo SPLC, a Adobe realiza revisões regulares dos códigos existentes e fortalece-os conforme apropriado, aprimorando ainda mais a segurança de aplicativos e de dados no uso de produtos da Adobe.

Exibição protegida no Acrobat DC

Similar ao Modo protegido no Acrobat Reader DC, a Exibição protegida é uma implementação de tecnologia para área restrita para o amplo conjunto de recursos do Acrobat DC. No Acrobat DC, a Adobe estende a funcionalidade da Exibição protegida para fazer mais do que bloquear ataques baseados em gravação que tentam executar códigos maliciosos no sistema do computador usando o formato de arquivo PDF para ataques baseados em leitura que tentam roubar dados confidenciais ou propriedade intelectual por meio de arquivos PDF.

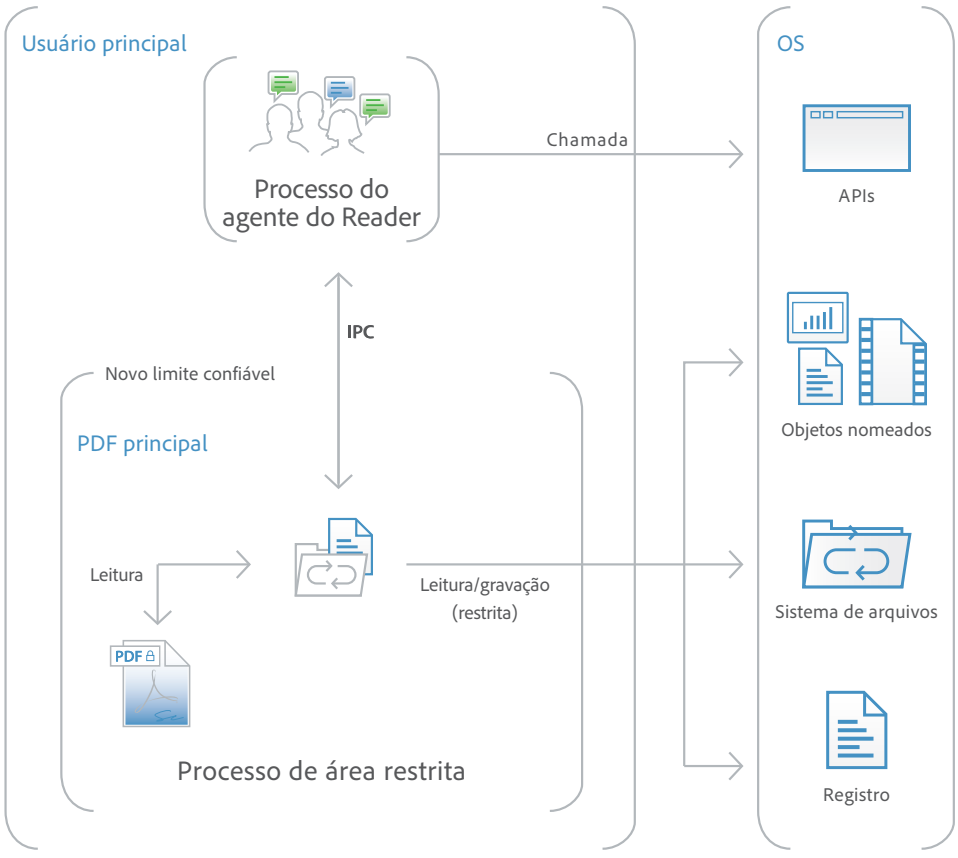
Como o Modo protegido, a Exibição protegida limita a execução de programas não confiáveis (por exemplo, arquivos PDF e os processos que eles iniciam) a áreas de segurança restritas para evitar que códigos maliciosos usem o formato PDF para gravar ou ler no sistema de arquivos do computador.

A Exibição protegida assume que todos os arquivos PDF são potencialmente maliciosos e limita o processamento às áreas restritas, a menos que seja especificamente indicado que o arquivo é confiável. A Exibição protegida é compatível nos dois cenários em que os usuários abrem documentos PDF: nos aplicativos individuais do Acrobat DC e em navegadores. A Exibição protegida no Windows 8 e posterior sempre é executada em um AppContainer. Isso fornece um ambiente ainda mais restrito para clientes que ativam o Modo protegido.

Ao abrir um arquivo possivelmente malicioso na Exibição protegida, o Acrobat DC exibe uma barra de mensagem amarela (YMB) na parte superior da janela em exibição. A YMB indica que o arquivo não é confiável e lembra que você está na Exibição protegida, a qual desativa muitos recursos do Acrobat DC e limita a interação entre usuário e arquivo. Basicamente, o arquivo está no modo "somente leitura", com a Exibição protegida impedindo que o conteúdo malicioso incorporado ou agregado adultere seu sistema. Para tornar o arquivo confiável e habilitar todos os recursos do Acrobat DC, basta clicar no botão Habilitar todos os recursos na YMB. Essa ação desativa a Exibição protegida e torna o arquivo permanentemente confiável, adicionando-o à lista do Acrobat de locais privilegiados. Cada abertura subsequente do arquivo PDF confiável desabilita as restrições da Exibição protegida.

O que é uma área restrita?

A área restrita é um método altamente respeitado por profissionais de segurança que cria um ambiente limitado para a execução de programas com poucos direitos ou privilégios. As áreas restritas ajudam a evitar que os sistemas dos usuários sejam prejudicados por documentos não confiáveis que contêm código executável. No contexto do Acrobat Reader DC, o conteúdo não confiável é qualquer PDF e os processos que ele inicia. O Reader DC trata todos os arquivos PDF como potencialmente corrompidos e limita à área restrita todos os processos que o arquivo PDF requisita.



Execução de JavaScript

O Acrobat DC apresenta controles sofisticados e granulares para whitelist e blacklist de execução de JavaScript em vários ambientes, como Windows e Macintosh. A estrutura de whitelist de JavaScript da Adobe ativa seletivamente o JavaScript de arquivos PDF, sites, hosts ou documentos específicos que foram assinados com um certificado confiável. Além disso, a estrutura de blacklist de JavaScript da

Estrutura de whitelist
Ative seletivamente o JavaScript para os fluxos de trabalho confiáveis ao incluir documentos na whitelist usando locais privilegiados, que permitem que a confiabilidade seja concedida com base nas zonas de segurança do Microsoft Windows, documentos certificados ou adicionando arquivos, pastas ou hosts específicos.

Adobe permite o uso do JavaScript como parte de fluxos de trabalhos comerciais protegendo usuários e sistemas de ataques direcionados a chamadas de API JavaScript específicas. Adicionando uma chamada de API JavaScript específica à blacklist, é possível impedir que ela seja executada sem a necessidade de desativar completamente o JavaScript. Você pode impedir que usuários individuais ignorem sua decisão de bloquear uma chamada de API JavaScript específica, ajudando a proteger toda a empresa de códigos maliciosos.

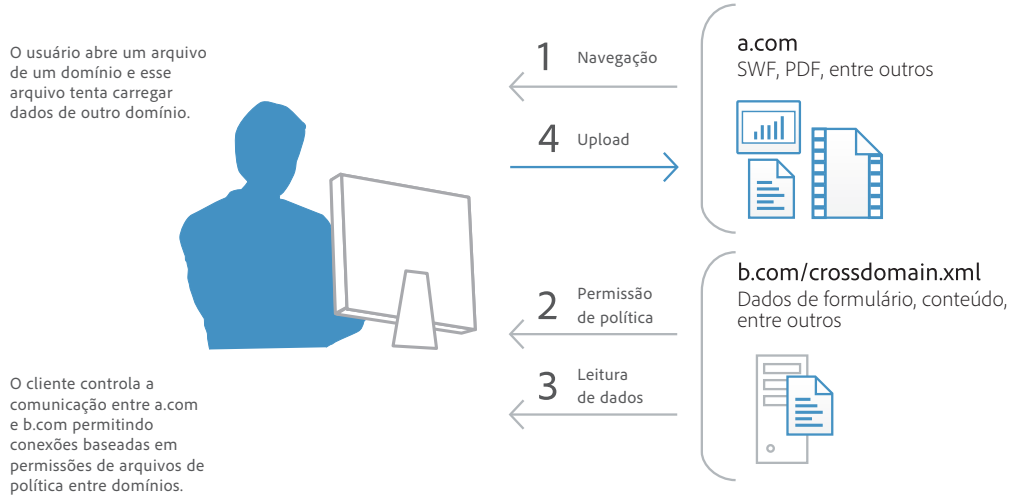
Configuração entre domínios

Por padrão, o Acrobat DC desabilita o acesso irrestrito entre domínios para clientes do Windows e Mac OS X, evitando que invasores explorem os arquivos PDF importantes para acessar recursos em outro domínio.

Aproveitando o suporte integrado de arquivos de política entre domínios baseados em servidor, é possível permitir que o Acrobat DC e o Acrobat Reader DC manipulem dados entre os domínios. Esse arquivo de política entre domínios, um documento XML, está hospedado no domínio remoto, concedendo acesso ao domínio de origem e permitindo que o Acrobat DC ou o Acrobat Reader DC deem continuidade à operação.

Você precisa ativar o suporte entre domínios da Adobe nos seguintes cenários:

- Para obter acesso seletivo entre domínios e aproveitar outros recursos, como reconhecimento baseado em certificado digital.
- Para gerenciar, de forma centralizada, as permissões de acesso entre domínios de um único local baseado em servidor.
- Para implementar fluxos de trabalho que incluem pedidos de dados de vários domínios para restituição de dados de formulário, solicitações SOAP, referências a streaming de mídia e solicitações de HTTP .NET.



Alertas de segurança de fácil utilização

Além dos processos de resposta a incidentes e os alertas de segurança, o Acrobat DC implementa métodos de fácil utilização para alertas de segurança por meio de YMBs. Se a segurança aprimorada estiver ativada e o arquivo PDF ainda não estiver definido como local privilegiado ou confiável, a YMB aparece no momento em que os arquivos PDF tentam executar uma ação com risco potencial, o que inclui:

- Requisitar acesso entre domínios
- Executar JavaScript privilegiado
- Requisitar URL invocado por JavaScript
- Chamar uma API JavaScript em uma blacklist
- Inserir dados

- Inserir scripts
- Reproduzir multimídia incorporada de legado

No Acrobat DC e Reader DC, a YMB aparece na parte superior do documento com o aviso ou a mensagem de erro. O usuário pode escolher tornar o documento confiável uma vez ou sempre. A escolha sempre resulta na adição do documento à lista de documentos privilegiados do aplicativo.

O botão Opções permite aos usuários definir rapidamente como confiável, uma vez ou sempre. Você também pode tornar arquivos, pastas e hosts confiáveis em toda a empresa para que a YMB não seja exibida em fluxos de trabalho confiáveis.

Segurança em nuvem

A Adobe monitora e aprimora constantemente os serviços, os sistemas e os processos em nuvem para ajudar os clientes a atender às crescentes demandas e aos desafios de proteger e manter os dados em segurança. Os serviços da Document Cloud, incluindo o Adobe Sign e os serviços de PDF usados pelo Acrobat DC, foram criados para garantir confiabilidade, integridade e disponibilidade dos documentos. Os serviços da Document Cloud estão em conformidade com ISO 27001, PCI DSS e SOC 2 Tipo 2, e atendem a outras normas, padrões e certificações de conformidade específicas do setor. Para obter mais informações sobre nosso método de segurança em nuvem, consulte a *Adobe Document Cloud Security Overview* (Visão geral sobre segurança na Adobe Document Cloud).

Segurança em data center

Atualmente o data center da Document Cloud que hospeda os serviços de PDF e o armazenamento de arquivos está localizado em um data center American National Standards Institute (ANSI) Tier 4 gerenciado por nosso provedor de serviços em nuvem confiável, o Amazon Web Services (AWS). O AWS mantém controles restritos de acesso ao data center, tolerância a falhas, controles de ambiente e segurança. Somente funcionários da Adobe autorizados e aprovados, funcionários do parceiro de serviços em nuvem e fornecedores de empresas legítimas e documentadas têm acesso permitido ao local seguro na Virgínia, EUA. Para obter mais informações sobre a segurança do data center do AWS, consulte *https://aws.amazon.com/security/*.

Criptografia e privacidade de dados

Os produtos e serviços da Adobe, incluindo os serviços da Document Cloud, foram criados focados em privacidade. A Document Cloud criptografa documentos e ativos em repouso usando o Padrão de Criptografia Avançada (AES) de 256 bits do National Institute of Standards and Technology (NIST) e é compatível com o protocolo HTTP com uma conexão criptografada pela Segurança da camada de transporte (TLS) para garantir que o tráfego de dados esteja adequado e protegido.

Os funcionários da Document Cloud e fornecedores confiáveis acessam os dados dos clientes apenas para executar algumas funções de suporte e de negócio ou se exigido por lei. A Adobe não fornece a nenhum governo acesso direto ou sistemático aos dados dos clientes que armazenamos. Para obter mais informações sobre as políticas de privacidade da Adobe, consulte *www.adobe.com/privacy*.

Integração com as arquiteturas dos sistemas operacionais

Segurança permanente

Para fornecer uma camada adicional de defesa contra ataques que visam obter controle sobre sistemas de desktop e corromper memória, o Acrobat DC beneficia-se de proteções de segurança incorporadas e permanentes nos sistemas operacionais Windows e Mac OS X.

A prevenção à execução de dados (DEP) evita que dados ou códigos perigosos sejam inseridos em locais de memória considerados protegidos pelo sistema operacional Windows. A Apple fornece proteção semelhante para o Mac OS X Lion, incluindo DEP de pilha e DEP baseada em heap, estendendo essa proteção a aplicativos de 32 e 64 bits e tornando-os mais resistentes a ataques.

A randomização de layout do espaço de endereço (ASLR) oculta locais de memória e de arquivos de paginação dos componentes do sistema, dificultando a localização desses componentes e protegendo-os de ataques. O Windows e o Mac OS X Lion usam a ASLR. No Mac OS X Lion, a ASLR é estendida a aplicativos de 32 e 64 bits.

Configuração de nível de registro e lista de propriedades

O Acrobat DC fornece diversas ferramentas para o gerenciamento de configurações de segurança, incluindo preferências de nível de registro (Windows) e lista de propriedades (Mac OS). Com essas definições, é possível configurar clientes, antes e depois da implantação, para:

- Ativar ou desativar a segurança aprimorada
- Ativar ou desativar locais privilegiados
- Especificar locais privilegiados predefinidos
- Bloquear determinados recursos e desativar a interface do aplicativo para que os usuários finais não possam alterar as configurações
- Desativar, ativar ou configurar os outros recursos relacionados a segurança

Administração e implantação facilitadas

Fortalecimento da segurança do software

Os aprimoramentos de segurança, como a Exibição protegida, são um exemplo de extensos investimentos em engenharia feitos pela Adobe para fortalecer o Acrobat DC contra ameaças. Com esse fortalecimento, a Adobe pode reduzir, ou até mesmo eliminar, a necessidade de atualizações de segurança fora de banda e diminuir a urgência de atualizações agendadas regularmente. Tudo isso aumenta a flexibilidade operacional e reduz o custo total de propriedade (TCO), principalmente em grandes ambientes que requerem a mais alta segurança.

Suporte ao Citrix e virtualização de aplicativos

Com o suporte a licenciamento por usuário nomeado no Citrix XenApp, Citrix XenDesktop, VMware Horizon e Microsoft App-V, você pode fornecer acesso remoto seguro aos recursos do Acrobat de que seus usuários precisam.

Suporte a soluções de gerenciamento de mobilidade corporativa (EMM)

A Adobe tem o compromisso de ajudar os clientes corporativos a atender à demanda por soluções de produtividade móvel enquanto garante a segurança e a conformidade da corporação. Os aplicativos para dispositivos móveis do Acrobat Reader e do Adobe Sign são compatíveis com a plataforma Android for Work EMM. O Adobe Acrobat Reader for Microsoft Intune está disponível para iOS e Android. O Acrobat Reader também é compatível com a plataforma AppConfig. Saiba mais sobre os *recursos de TI*.

Suporte para Group Policy Objects do Windows Server e Microsoft Active Directory

Os objetos de política de grupo (GPO) do Windows Server e o Microsoft Active Directory permitem a automatização de gerenciamento um-para-muitos de sistemas de computador. A Adobe acrescentou suporte para modelos certificados de Microsoft Active Directory Administrative (ADM) para política de grupo no Acrobat DC, possibilitando a instalação de softwares por demanda e o reparo automático de aplicativos. Se ainda houver necessidade de configurar aplicativos após a implantação, use os modelos de ADM para propagar por toda a organização as configurações requisitadas.

Suporte para Microsoft SCCM e SCUP

Com o Acrobat DC, é possível importar e publicar eficientemente as atualizações por meio do Microsoft System Center Configuration Manager (SCCM) para garantir que os desktops gerenciados com Windows tenham sempre as correções e atualizações de segurança mais recentes.

O suporte para os catálogos do Microsoft System Center Updates Publisher (SCUP) permite automatizar as atualizações do software Acrobat DC em sua organização, bem como aprimorar as implantações iniciais de software. O SCUP pode importar qualquer atualização enviada pela Adobe assim que ela é disponibilizada, o que facilita e torna mais eficiente as atualizações do Acrobat DC. A integração com SCCM e SCUP ajuda a reduzir o custo total de propriedade do software da Adobe, uma vez que você pode distribuir as correções por toda a organização de forma mais rápida e fácil.

Suporte para Apple Package Installer e Apple Remote Desktop

No Acrobat DC, a Adobe implementou o Apple Package Installer padrão fornecido pelo Mac OS X em vez do instalador exclusivo da Adobe. Isso facilita a implantação do software Acrobat nos desktops Macintosh da empresa, já que é possível usar o software de gerenciamento Apple Remote Desktop para administrar implantações iniciais de software e atualizações e correções subsequentes em um local central.

Atualizações e correções cumulativas programadas regularmente

Para ajudar a manter o software atualizado, a Adobe fornece, de maneira proativa, atualizações programadas regularmente que contêm atualizações de recursos e correções de segurança. Para respostas rápidas a ataques de dia-zero, a Adobe fornece correções fora do ciclo conforme necessário. A Adobe aproveita as correções cumulativas ao máximo para reduzir o esforço e o custo necessários para manter os sistemas atualizados. A Adobe também testa ativamente as correções de segurança antes de lançá-las para ajudar a garantir a compatibilidade com as instalações e os fluxos de trabalho existentes.

A data de cada atualização planejada é anunciada previamente no blog Adobe Product Security Incident Response Team (PSIRT) em *blogs.adobe.com/psirt*.

Para ver os boletins e relatórios de segurança mais recentes sobre os produtos da Adobe, acesse *https://helpx.adobe.com/br/security.html*. Para obter informações mais detalhadas sobre os produtos e recursos de segurança da Adobe, visite a Biblioteca de Segurança da Adobe em *www.adobe.com/go/learn_acr_appsecurity_en*.

Assistente de personalização da Adobe e kit de ferramentas corporativas

Para maior controle sobre as implantações em toda a empresa, a Adobe fornece as seguintes ferramentas:

- **Assistente de personalização Adobe**, uma ferramenta gratuita disponível para download que permite personalizar o instalador do Acrobat e configurar os recursos de aplicativos antes da implantação.
- **Kit de ferramentas corporativas (ETK) para Acrobat e Windows**, um aplicativo personalizável e atualizado automaticamente que contém a referência de preferências da Adobe. O ETK da Adobe também inclui uma lista cada vez maior de recursos que interessam aos administradores corporativos.

Saiba mais sobre essas ferramentas em *recursos de TI*.

Conclusão

Com o Acrobat DC, a Adobe leva a segurança de documentos PDF e dados para um nível completamente novo. Da ampliação de segurança para ajudar na proteção contra o roubo de dados confidenciais e propriedade intelectual da empresa, bem como o bloqueio de instalações de malwares perigosos no computador, à integração com ferramentas adicionais que facilitam, de modo inédito, a administração de implantações em toda a corporação, o Acrobat DC fornece níveis mais elevados de segurança a um custo total de propriedade menor que o de qualquer versão anterior do Acrobat DC.

Para obter mais informações
Detalhes da solução:
www.adobe.com/security

Adobe

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

7/17