RELATÓRIO TÉCNICO

Segurança e privacidade da Asana

Como a Asana protege seus dados

asana

Índice

Introdução 4
Infraestrutura 5
- Servidores Web 6
- Bases de dados 6
  - Master 6
  - Dados dos clientes 6
  - Dados dos usuários 6
- Armazenamento de arquivos 6
- Infraestrutura Europeia 6
- Segurança de dados 7
  - Criptografia em trânsito 7
  - Criptografia em repouso 7
- Multilocação 8
- Escalabilidade e confiabilidade 8
  - Grau de disponibilidade do sistema 8
  - Página de Confiança 8
- Backups 8

Recursos de segurança do produto 9
- Administradores 9
- Provisionamento e desprovisionamento de usuários 9
- Segurança do login 9
  - Proteções de senhas 9
  - SSO do Google 10
  - Single Sign-On via SAML 10
- Permissões de acesso 10
  - Elementos da Asana 10
    - Tarefas 10
    - Projetos 10
    - Equipes 11
    - Organizações 11
    - Usuários 11
- Gerenciamento de convidados 12
- Aplicativos permitidos 12
- Controle de dados 12

Segurança do aplicativo 13
Plataforma Asana 14

Integrações 14
Contas de serviço 14
Aplicações de terceiros 15
Segurança operacional 16
Segurança das informações da Asana 16
Informações confidenciais 16
Recursos humanos 16
Revisões e política de acesso dos usuários 16
Segurança física 16
Escritórios da Asana 16
Segurança dos centros de dados 17
Segurança da rede 17
Segurança da Tecnologia da Informação 17
Gestão de riscos e vulnerabilidades 17
Testes de penetração 17
Recompensas por vulnerabilidades 17
Ciclo de desenvolvimento de software 18
Resposta a incidentes 18
Recuperação após desastres e continuidade do negócio 18
Retenção e remoção de dados 19
Retenção de dados 19
Remoção de dados 19
Monitoramento 19
Gestão de subcontratantes e fornecedores 19
Privacidade, certificações e conformidade 20
Política de privacidade 20
Certificações e conformidade legal 20
Estrutura do Escudo de Proteção da Privacidade 20
Controles do serviço e da organização (SOC 2) 20
RGPD 21
Adendo de Processamento de Dados 21
Aplicação da lei 21
Conclusão 22

Última atualização: fevereiro de 2020[1]

[1] Este relatório técnico descreve o estado atual da segurança da Asana, que está sujeito a alterações com lançamentos de recursos e produtos futuros.

Introdução

Atualmente, empresas do mundo todo estão adotando novas ferramentas para gerenciar e organizar o trabalho, de tarefas diárias a iniciativas estratégicas, de maneira mais colaborativa e versátil. Essas ferramentas se enquadram em uma nova categoria de softwares conhecida como soluções de gerenciamento de trabalho, sendo a Asana líder de mercado nesta categoria.

A Asana ajuda equipes como a sua a planejar, organizar e realizar o trabalho para que possam avançar mais rapidamente e alcançar resultados comerciais. Mais de 75.000 organizações pagantes e milhões de clientes em 190 países usam a Asana para proporcionar clareza e alinhamento ao garantir que todos os membros das equipes saibam o que deve ser feito, quem são os responsáveis e quais são os prazos. Já foram criadas mais de 1 bilhão de tarefas na Asana.

Os clientes confiam seus dados à Asana para poderem se dedicar se dedicar ao trabalho que realmente importa para seus negócios. É por esse motivo que não estamos focados apenas na criação de uma solução de gerenciamento colaborativo de trabalho que seja fácil de usar, preocupamo-nos também com a segurança dos dados de nossos clientes.

Na Asana, promovemos a conscientização da segurança em todos os funcionários por meio da cultura da empresa. Esta cultura de confiança e transparência define o tom da conscientização e atitude geral e da importância de proteger os ativos de informação de nossos clientes. Esta conscientização é reafirmada em nossos valores e padrões comportamentais por meio de declarações da política, códigos de conduta, missão compartilhada e declarações de valor comunicadas por nossa equipe executiva, que também toma medidas para criar um ambiente que incentive as pessoas a assumir e atribuir a plena responsabilidade.

Ressaltamos os seguintes princípios na elaboração e implementação do nosso programa e práticas de segurança:

- Segurança física e ambiental para proteger nossos aplicativos para Web e dispositivos móveis contra acessos não autorizados
- Manutenção da disponibilidade de nossos aplicativos
- Confidencialidade para proteger os dados dos clientes
- Integridade para manter a precisão e consistência dos dados ao longo do seu ciclo de vida

Neste relatório técnico, abordaremos a segurança e a privacidade desde as perspectivas de: infraestrutura, produto, operações, conformidade e certificações.

Embora a maior parte deste relatório técnico possa ser aplicada a qualquer tipo de plano Asana, ele foi elaborado levando em consideração os planos Asana pagos: Premium, Business e Enterprise.[2] Serão assinalados os recursos que não estiverem disponíveis para todos os planos.

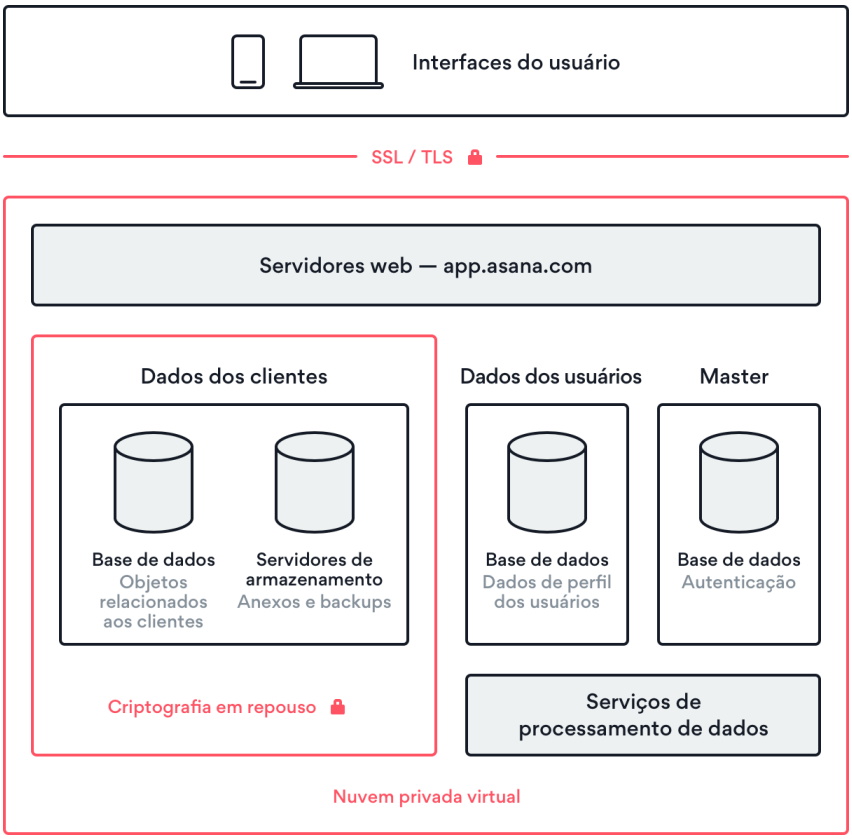
[2] Para obter mais informações sobre os planos Asana, acesse asana.com/pt/pricing.

Infraestrutura

A Asana utiliza serviços de computação em nuvem, principalmente da Amazon Web Services (AWS), como componentes essenciais da plataforma Asana.

A AWS gerencia a segurança e a conformidade da infraestrutura de computação em nuvem, e a Asana gerencia a segurança e a conformidade do software e dos dados confidenciais armazenados na infraestrutura de computação em nuvem. Consulte o Modelo de Responsabilidade Compartilhada da AWS.[3]

A Asana usa o Virtual Private Cloud da Amazon, e a sua arquitetura de rede foi projetada para ser segura, dimensionável e facilmente gerenciada mediante o uso dos serviços de rede e dos componentes essenciais fornecidos pela AWS. O serviço *Elastic Compute Cloud* (EC2) da Amazon opera a maior parte da plataforma Asana e oferece uma maneira confiável, dimensionável e segura para processar os dados dos clientes. Veja a seguir um diagrama simplificado da infraestrutura da Asana.



Nossa infraestrutura de produção é bloqueada, de modo que apenas nossos computadores de balanceamento de carga tenham permissão para receber o tráfego externo da Web. Cada host recebe uma função, e são usados grupos de segurança para determinar o tráfego esperado entre essas funções.

[3] https://aws.amazon.com/pt/compliance/shared-responsibility-model/

* A criptografia aplica-se apenas aos clientes do plano Enterprise.

Servidores Web

O Amazon CloudFront é um serviço rápido de rede de entrega de conteúdo (CDN), usado para disponibilizar os ativos estáticos da Asana de maneira dimensionável, com baixa latência e velocidades de transferência elevadas.

Bases de dados

As bases de dados consistem no Relational Database Service (RDS) da Amazon e executam uma base de dados MYSQL gerenciada.

Master

Armazena senhas criptografadas (bcrypt com hashes e salts criptográficos) e informações de autenticação dos distintos usuários.

Dados dos clientes

Armazenam todas as informações enviadas pelos clientes à Asana, incluindo equipes, projetos e tarefas.

Dados dos usuários

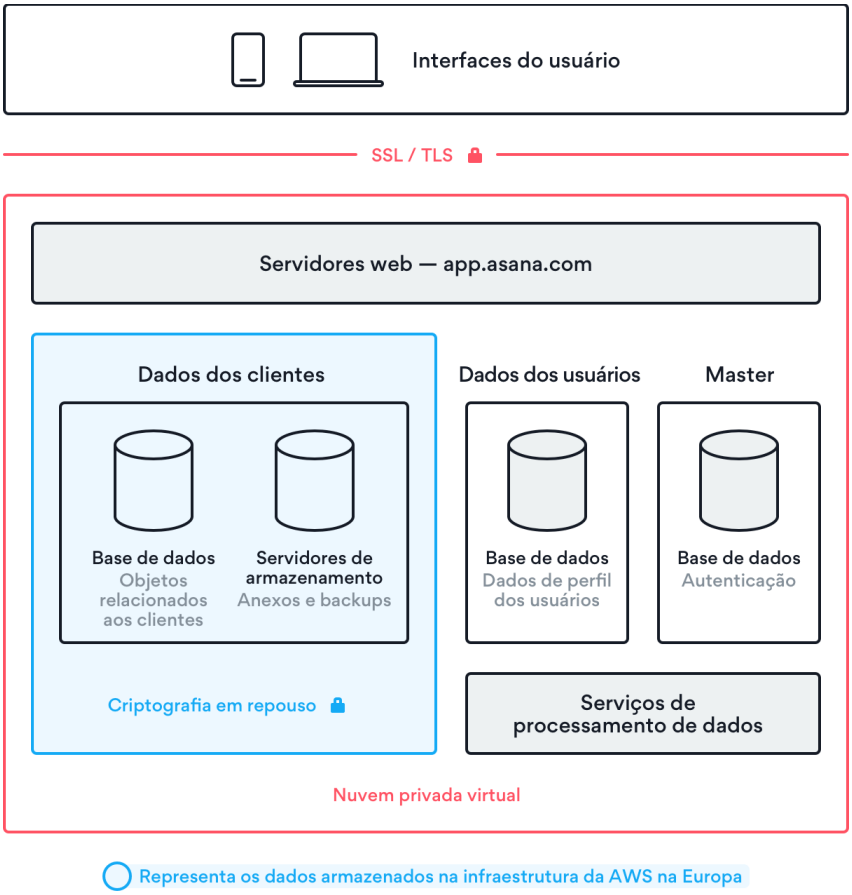
Armazenam as informações relacionadas a perfis de usuários, como nome e endereço de e-mail.

Armazenamento de arquivos

Os servidores de armazenamento consistem no Simple Storage Server (S3) da Amazon. Eles armazenam anexos e backups de bases de dados. Os anexos são quaisquer arquivos enviados a tarefas na Asana a partir de um computador. Os anexos provenientes das plataformas de colaboração de conteúdo hospedadas na nuvem são criados como links que levam a essas plataformas, mas não são mantidos nos servidores de armazenamento da Asana.

Infraestrutura Europeia

A Asana oferece centros de dados europeus para os clientes do plano Asana Enterprise que necessitam que os seus dados permaneçam na Europa. Os dados dos clientes serão armazenados na região da AWS Alemanha (Frankfurt), com backups armazenados na região da AWS Dublin (Irlanda). As instalações
da AWS são usadas tanto para as infraestruturas da UE quanto dos EUA. Todos os dados dos clientes de uma organização serão mantidos nos EUA ou na UE, a depender da preferência dos clientes.
Veja a seguir um diagrama simplificado da infraestrutura da Asana para os clientes que usam a infraestrutura europeia.



Segurança de dados

Criptografia em trânsito

As conexões com o app.asana.com são codificadas com criptografia de 128 bits e oferecem suporte ao protocolo TLS 1.2 e versões superiores. As conexões são codificadas e autenticadas com AES_128_GCM e usam ECDHE_RSA como o mecanismo de troca de chaves. A Asana oferece suporte a forward secrecy e AES-GCM e proíbe conexões inseguras que usem os protocolos RC4 ou SSL 3.0 e versões anteriores. Logins e transferências de dados confidenciais são realizados apenas sob o protocolo TLS/SSL.

Criptografia em repouso

Para os clientes do plano Enterprise, a Asana garante a criptografia em repouso com chaves secretas (AES-256 bits) para os dados dos clientes.

Multilocação

A infraestrutura é compartilhada entre instâncias do cliente, portanto, a Asana é um aplicativo web multilocatário. A autenticação de contas, a separação lógica de campos da base de dados e os controles de gerenciamento de sessões são implementados de maneira a limitar o acesso dos clientes aos dados relacionados com a organização correspondente.

Escalabilidade e confiabilidade

A Asana usa a Amazon Web Services, que garante a escalabilidade ou capacidade de expansão do serviço. A base de dados é replicada de maneira sincronizada para que possamos nos recuperar rapidamente de uma falha na base de dados. Como precaução adicional, são capturados instantâneos regulares da base de dados que são transferidos com segurança para um centro de dados separado, para que possamos restaurá-los em outro local conforme for necessário, mesmo ao ocorrer uma falha regional na Amazon.

Grau de disponibilidade do sistema

O funcionamento do serviço para nossos clientes do plano Enterprise é garantido durante 99,9% do tempo.

Página de Confiança

A confiança deve ser conquistada, e nós acreditamos que ela começa quando ofereceremos transparência sobre o status e o desempenho do nosso sistema. A página de Confiança da Asana compartilha a disponibilidade do nosso aplicativo Web, dos aplicativos para dispositivos móveis e da API nas últimas 12 horas, semana, mês e ano. Acesse trust.asana.com.

Backups

São capturados instantâneos da base de dados diariamente. Os backups contam com a mesma proteção das bases de dados em produção. Garantimos o armazenamento de backups inter-regionais para os clientes do plano Enterprise.

Recursos de segurança do produto

A Asana fornece aos usuários e administradores os recursos necessários para proteger seus dados. Esses recursos proporcionam controle administrativo abrangente e visibilidade quanto aos dados dos clientes. A disponibilidade dos recursos a seguir varia conforme o plano Asana. Veja os planos em asana.com/pricing.

Administradores

Os administradores podem gerenciar as equipes para adicionar e remover membros e convidados à medida que ingressam e deixam a empresa ou o fluxo de trabalho. Eles também podem usar a nossa API de administrador para gerenciar exportações de domínios, configurações, permissões, aplicativos de terceiros e configurações de equipes e usuários.

Provisionamento e desprovisionamento de usuários

A Asana permite que os usuários e administradores controlem quem tem acesso aos seus dados.

- Os usuários e administradores podem convidar membros e adicionar convidados (membros externos) às suas organizações e equipes.
- Os administradores podem remover qualquer membro ou convidado no Painel do administrador.

Além disso, os clientes do plano Enterprise podem integrar a Asana com o seu fornecedor de identidade em nuvem por meio do padrão do sistema para gerenciamento de identidade entre domínios (SCIM, System for Cross-domain Identity Management), para adicionar e remover usuários conjuntamente com o restante de suas soluções SaaS.

Segurança do login

Os administradores da Asana podem determinar o mecanismo usado por seus usuários para fazer login em suas contas Asana. Há três opções diferentes: credenciais Asana, SSO do Google ou Single Sign-On via SAML 2.0.

Proteções de senhas

Quando os usuários têm permissão para fazer login em suas contas usando as credenciais Asana, os administradores podem especificar a força necessária para as senhas. Exigir senhas “fortes” obrigará os usuários a utilizar, no mínimo, 8 caracteres que contenham três dos seguintes elementos: letra minúscula, letra maiúscula, números e caracteres especiais.

Os administradores também podem impor uma redefinição de senha para todos os usuários da organização.

SSO do Google

Os administradores podem exigir que os usuários da organização façam login na Asana usando a sua conta do G Suite (Google).

Single Sign-On via SAML

Os administradores de um plano Enterprise podem configurar um fornecedor de identidade próprio e requerer que os usuários façam login na Asana com as credenciais da conta do fornecedor de identidade na nuvem. Isso é configurado por meio do padrão de autenticação SAML.

Permissões de acesso

Os administradores e usuários podem convidar outras pessoas para ter acesso a seus dados. Os usuários podem ser convidados para participar de uma organização com privilégios distintos. Os convites são feitos por elemento (tarefa, projeto, equipe ou organização) com diferentes tipos de acesso. As permissões para os usuários são definidas no âmbito do elemento e não do usuário, ou seja: um usuário pode ter acesso somente para comentar em alguns conteúdos, outros podem estar "disponíveis mediante solicitação", pode ter acesso pleno a determinados elementos enquanto outros permanecem completamente ocultos. É possível compreender a fundo os detalhes de cada elemento e tipo de permissão em nosso Guia Asana: asana.com/guide.

Elementos da Asana

Tarefas

As tarefas na Asana podem ser privadas, públicas, estar contidas em um projeto privado ou em um projeto público.

Projetos

Tarefa:	Acessível para:
Tarefa privada	Colaboradores da tarefa
Tarefa pública	Todos os membros da organização
Tarefa em um projeto privado	Colaboradores da tarefa e membros do projeto
Tarefa em um projeto público	Colaboradores da tarefa, membros do projeto e membros da equipe
Subtarefa	Colaboradores da tarefa e pessoas com acesso à tarefa principal

Os projetos na Asana podem ser privados ou públicos. Se alguém tem acesso a um projeto, significa que essa pessoa pode acessar todas as tarefas e conversas contidas nesse projeto. Os usuários podem ser adicionados a um projeto com acesso para editar ou somente comentar.

Projeto:	Acessível para:
Projeto privado	Membros do projeto
Projeto público	Membros da equipe e do projeto
Projeto público em uma equipe pública	Membros da organização, da equipe e do projeto

Equipes

As equipes na Asana podem ser ocultas, públicas ou de associação por solicitação. Se alguém pertence a uma equipe, significa que essa pessoa pode acessar todas as conversas e projetos públicos contidos nessa equipe.

Equipe:	Acessível para:	Podem participar:
Oculta	Membros da equipe	Não
Pública para a organização	Membros da equipe e da organização	Sim
Associação por solicitação	Membros da equipe	Sujeito a aprovação

Organizações

As organizações na Asana são o elemento de nível mais elevado, que contém em si as equipes, projetos e tarefas.

Usuários

Os usuários da Asana têm contas individuais que são vinculadas ao seu endereço de e-mail e cujo acesso aos diferentes elementos de dados é determinado como mencionamos anteriormente. Por padrão, as contas dos usuários obtêm acesso automático a uma organização de acordo com o seu domínio de e-mail.

Membros com acesso completo

A associação à organização é feita com base no domínio do endereço de e-mail. Para se tornar membro de uma organização, é necessário ter um endereço de e-mail com um domínio aprovado pela sua organização.

O membro de uma organização pode:

- Criar novas equipes
- Ver a lista completa das equipes às quais pode pedir para participar dentro da organização

- Ver nomes e endereços de e-mail de outros membros e convidados da organização
- Acessar projetos e tarefas que foram definidos como públicos para a organização

Convidados

É possível colaborar com clientes, terceirizados, ou qualquer outra pessoa que não tenha um endereço de e-mail com um domínio aprovado pela sua organização. Essas pessoas passam a ser convidados da organização. Os convidados têm acesso limitado à organização e podem ver apenas o que é explicitamente compartilhado com eles.

Um convidado da organização só pode participar de equipes se receber convites específicos. Os convidados não podem criar novas equipes ou ver e pedir para participar de qualquer outra equipe.

Membros com acesso a projetos específicos

Cada equipe tem seus próprios membros e projetos. Os membros que não têm acesso a todos os projetos na sua equipe aparecem na aba Membros das configurações da equipe como membros com acesso a projetos específicos.

Membros com acesso a projetos específicos podem ver os projetos e tarefas a que foram adicionados, mas não têm acesso a conversas ou a outros projetos da equipe.

Gerenciamento de convidados

Os administradores do plano Enterprise podem determinar quem tem permissão para convidar membros externos (convidados). Os administradores têm as três opções abaixo ao decidir quem pode adicionar convidados à organização:

- Administradores
- Administradores e membros da organização
- Todos (isso inclui os membros e convidados da organização)

Aplicativos permitidos

Os administradores do plano Enterprise podem determinar quais integrações de terceiros podem ser utilizadas pelos usuários com suas contas Asana, e podem também bloquear as integrações indesejadas. Acesse asana.com/apps para saber quais aplicativos de terceiros estão disponíveis.

Controle de dados

Os clientes podem exportar ou excluir dados da Asana de maneira fácil e seletiva e automatizar exportações de domínios completos usando a nossa API.

Segurança do aplicativo

O serviço da Asana consiste em um software como serviço on-line. Os usuários podem acessar seus dados por meio de um navegador da Internet, aplicativo para dispositivos móveis (Android e iOS) ou API (Interface de Programação de Aplicativos, na sigla em inglês).

Os serviços e elementos que compõem a Asana são escritos principalmente em JavaScript, TypeScript, Python e Scala, com base na estrutura de aplicação React. A Asana foi desenvolvida de acordo com as boas práticas de segurança definidas pela Fundação OWASP e com uma abordagem de "segurança por design" em todos os momentos. Portanto, foram implementados mecanismos abrangentes para evitar riscos à segurança, incluindo, entre outros, os tópicos a seguir:

- Injeção
- Falhas de autenticação
- Exposição de dados sensíveis
- Entidades externas XML (XXE)
- Controle de acesso ineficiente
- Má configuração de segurança
- Cross-Site Scripting (XSS)
- Desserialização insegura
- Utilização de componentes com vulnerabilidades conhecidas
- Registro e monitoramento insuficientes
- Cross-Site Request Forgery (CSRF)
- Redirecionamentos e encaminhamentos não validados

São realizadas auditorias anuais na Asana quanto aos dez riscos de segurança mais críticos em aplicativos Web, segundo a OWASP.

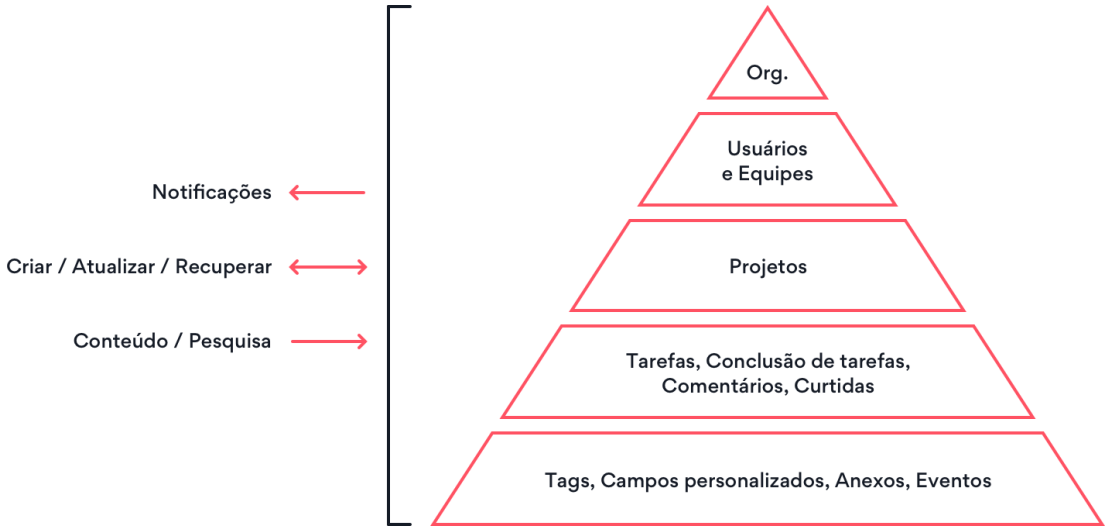
Plataforma Asana

Integrações

A Asana permite que os usuários acessem suas contas por meio de uma API (Interface de Programação de Aplicativos). A API da Asana consiste em uma interface RESTful, que lhe possibilita atualizar e acessar de forma programática muitos de seus dados na plataforma, bem como reagir automaticamente quando ocorrem alterações. Fornece URLs previsíveis para acessar os recursos e usa as funcionalidades HTTP incorporadas para receber comandos e retornar respostas. Isso facilita a comunicação com a Asana a partir de uma ampla variedade de ambientes, que abrangem desde utilitários da linha de comando a plugins de navegadores e aplicações nativas. Os clientes podem usar essas APIs para criar soluções personalizadas ou para fazer a integração com outros softwares. A Asana oferece suporte para OAuth 2.0 ou Token de Acesso Pessoal como métodos de autenticação com a API.

Para saber mais sobre a API da Asana, acesse asana.com/developers.

A ilustração a seguir apresenta um resumo das ações que podem ser executadas e dos elementos com os quais é possível trabalhar.



Por padrão, qualquer software ou script terá as mesmas permissões que o usuário que o está executando. Portanto, os dados disponíveis limitam-se aos dados aos quais o usuário tem acesso. Quando é necessário acesso adicional, os clientes do plano Enterprise podem usar as contas de serviço, abordadas a seguir.

Contas de serviço

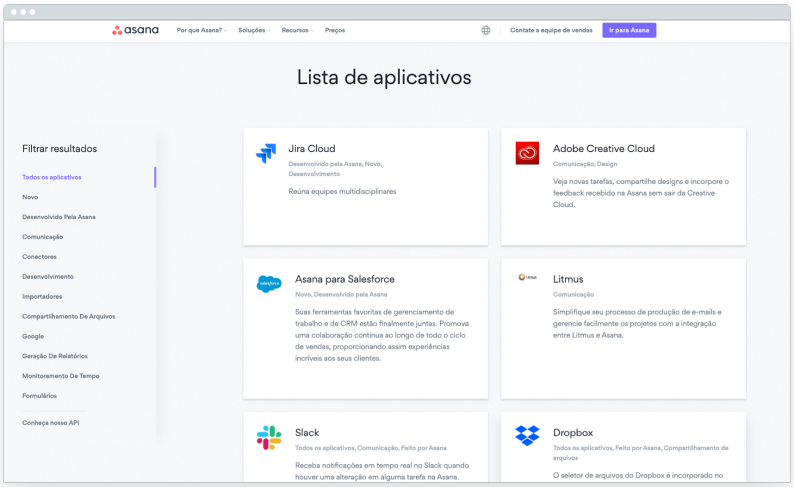
Os clientes do plano Asana Enterprise podem usar as contas de serviço para acessar todos os seus conteúdos. Por exemplo, as contas de serviço podem ser usadas para realizar uma exportação completa dos dados da organização ou para monitorar as atividades das equipes.

Aplicações de terceiros

A API da Asana permite o uso pelos clientes de centenas de integrações prontas para aprimorar ou complementar a sua experiência na Asana. A Asana integra-se a diversas ferramentas do Google e da Microsoft para agilizar os fluxos de trabalho dos clientes e aumentar a produtividade. É possível também integrar ferramentas externas de outros fornecedores para:

- Sincronização de mensagens entre os aplicativos
- Automatização do fluxo de trabalho
- Extensões da plataforma
- Desenvolvimento de software
- Importações de dados
- Compartilhamento de arquivos
- Relatórios
- Monitoramento de tempo
- Recebimento de dados

Um diretório contendo os aplicativos de terceiros pode ser visto em asana.com/apps.



Segurança operacional

Segurança das informações da Asana

A Asana mantém um programa formal de gerenciamento de segurança da informação com uma equipe de segurança dedicada, que presta contas ao diretor de segurança da informação na Asana (CISO, na sigla em ingês). Essa organização é responsável por implementar controles de segurança e monitorar a Asana quanto a atividades maliciosas.

Informações confidenciais

A Asana trata todos os dados dos clientes como confidenciais, independentemente da classificação. Essa política restringe o acesso a informações confidenciais aos funcionários que devem ter acesso a esse tipo de informação para o desempenho do seu trabalho, e apenas nos casos em que o acesso a tais informações se fizer necessário para prestar um serviço específico aos clientes. Nessas condições, os funcionários são orientados a acessar somente o mínimo de informações confidenciais necessárias para o desempenho de sua tarefa.

Recursos humanos

Todos os funcionários ou terceirizados da Asana devem assinar um contrato de confidencialidade e propriedade de invenções. Além disso, são submetidos a um treinamento formal de conscientização sobre segurança no ato da contratação e anualmente nos anos subsequentes.

Todos os nossos engenheiros assinam um contrato de política de acesso a dados e são submetidos a uma verificação de antecedentes antes de serem contratados pela Asana. Além disso, dispomos de gateways para os pontos de entrada aos dados dos clientes: todos os acessos a dados são registrados e armazenados indefinidamente.

A Asana possui uma política disciplinar e de sanções por violações à política.

Revisões e política de acesso dos usuários

Trimestralmente, a direção revisa o acesso dos usuários aos sistemas com abrangência relevante para verificar a adequação constante e revogar os acessos que já não forem necessários. Após o desligamento dos funcionários, o seu acesso é também removido.

Segurança física

Escritórios da Asana

Nossos escritórios são protegidos por acessos com cartões-chave registrados. Além disso, todos os escritórios dispõem de sistemas de alarme contra invasão. Os visitantes devem fazer registro na recepção. Todos os funcionários devem informar atividades suspeitas, acessos não autorizados a instalações ou incidentes de roubo/perda de objetos.

Segurança dos centros de dados

A Asana conta com os controles físicos e ambientais de excelência da AWS.[4]

Segurança da rede

Monitoramos a disponibilidade da nossa rede de escritórios e os dispositivos contidos nela. Coletamos num local central os registros produzidos por dispositivos de rede, como firewalls, servidores DNS, servidores DHCP e roteadores. Os registros de rede são armazenados para o dispositivo de segurança (firewall), os pontos de acesso sem fio e os comutadores.

Segurança da Tecnologia da Informação

Todos os computadores portáteis e estações de trabalho são protegidos com criptografia de disco completo e são provisionados a partir de uma imagem administrada de forma centralizada. Aplicamos diligentemente as atualizações aos dispositivos dos funcionários e monitoramos malwares nas estações de trabalho. Também podemos aplicar patches críticos de segurança e apagar qualquer máquina remotamente por meio do gerenciador de dispositivos. Sempre que possível, utilizamos a autenticação em duas etapas para proteger ainda mais o acesso à nossa infraestrutura corporativa. A Asana realiza verificações de segurança periodicamente.

Gestão de riscos e vulnerabilidades

A Asana mantém um processo contínuo de gestão de riscos que visa identificar as vulnerabilidades nos sistemas da Asana e avaliar ameaças novas e emergentes às operações da empresa de forma proativa.

Há também um processo de verificação de vulnerabilidades para sistemas externos e internos no ambiente de produção. A equipe de segurança da Asana realiza verificações ao menos trimestralmente e corrige as vulnerabilidades com base na classificação. As verificações de vulnerabilidade também são realizadas após qualquer alteração significativa no ambiente de produção, conforme determinado pelo diretor de segurança.

Testes de penetração

Trabalhamos em colaboração com profissionais de segurança terceirizados para testar o nosso código quanto a exploradores de vulnerabilidades comuns e usamos ferramentas de verificação de rede em nossos servidores de produção. O teste de penetração é realizado anualmente. As vulnerabilidades confirmadas são corrigidas e testadas novamente.

Recompensas por vulnerabilidades

Mantemos um programa de recompensas externo[5] no qual concordamos em remunerar os pesquisadores de segurança que descobrirem vulnerabilidades.

---

[4] http://aws.amazon.com/compliance/data-center/controls

[5] http://asana.com/bounty

Ciclo de desenvolvimento de software

A Asana usa o sistema de controle de revisões Git. As modificações feitas à base de códigos da Asana são submetidas a um conjunto de testes automatizados e passam então por uma etapa de análise e verificação manual. Quando as modificações de código são aprovadas pelo sistema automatizado de teste, são inicialmente aplicadas a um servidor de ensaio, no qual os colaboradores da Asana podem testar as mudanças antes de eventualmente implementá-las nos servidores de produção e nossa base de dados de clientes. Também está em funcionamento uma verificação de segurança específica para modificações e recursos particularmente sensíveis. Os engenheiros da Asana podem ainda eleger atualizações críticas para serem implementadas imediatamente nos servidores de produção.

Além de haver uma lista onde são publicadas todas as modificações feitas aos controles de acesso, temos um conjunto de testes automatizados para verificar se as regras de controles de acesso estão escritas corretamente e se são aplicadas conforme esperado.

Resposta a incidentes

A Asana mantém um Plano de Respostas a Incidentes elaborado para estabelecer uma resposta sensata e consistente a incidentes de segurança e a episódios suspeitos de segurança que envolvam destruição acidental ou ilegal, perda, roubo, alteração, divulgação não autorizada ou acesso a dados proprietários ou pessoais transmitidos, armazenados ou processados pela Asana. Tais procedimentos de resposta a incidentes especificam como a Segurança da Asana deve fazer as triagens, investigar, corrigir e gerar relatórios sobre os incidentes de segurança. A Asana tem contrato firmado com empresas terceirizadas de análises forenses digitais e respostas a incidentes em caso de violação dos dados.

Recuperação após desastres e continuidade do negócio

A Asana preparou um plano de continuidade do negócio para interrupções prolongadas no serviço causadas por desastres imprevisíveis ou inevitáveis, com o objetivo de restaurar os serviços tanto quanto possível dentro de um prazo razoável. A Asana documentou um conjunto de políticas e procedimentos de recuperação após desastres para possibilitar a recuperação ou continuidade da infraestrutura e dos sistemas de tecnologia vitais após um desastre.

O principal centro de dados da Asana está hospedado numa AWS localizado nos EUA (Virgínia) ou na Alemanha (Frankfurt), para os dados que se encontram nos EUA ou na UE, respectivamente, e conta com redundância[6] na mesma região da AWS. Caso ocorra a perda de um único centro de dados da AWS, os procedimentos de recuperação empregam os nós disponíveis em outro centro de dados. Como plano de contingência no evento de grandes catástrofes, há um local de recuperação de desastres localizado em um centro de dados da AWS nos EUA (Ohio) e na Irlanda (Dublin), para os dados que se encontram nos EUA ou na UE, respectivamente.

[6] Múltiplas zonas de disponibilidade por meio de implantações Multi-AZ do Amazon RDS.

Retenção e remoção de dados

Retenção de dados

Suas informações serão mantidas pelo período que for necessário para cumprir as finalidades descritas em nossa Política de privacidade. Os dados dos domínios de clientes do plano Enterprise poderão ser excluídos mediante solicitação.

Remoção de dados

Mediante solicitação do representante autorizado de um cliente, é possível fazer a exportação ou exclusão de domínio de seus dados. Além disso, a Asana pode concordar em preservar a confidencialidade de quaisquer dados armazenados, e somente processará ativamente tais dados de clientes após a data da solicitação em cumprimento às leis a que está sujeita.

Monitoramento

A Asana usa o Amazon CloudWatch em conjunto com scripts personalizados que extraem dados importantes dos registros e os enviam para seus serviços de monitoramento. A Asana monitora a capacidade de utilização da infraestrutura física e computacional tanto internamente quanto para os clientes, para assegurar que a entrega dos serviços corresponda aos acordos de nível de serviço. Dispomos de verificações de segurança automatizadas em nossa rede e aplicativos. Um script de monitoramento é executado semanalmente para confirmar se as alterações ao código foram revisadas corretamente.

Determinados registros de aplicativos e máquinas são retidos de modo indeterminado e mantidos normalmente no armazenamento de longo prazo no S3. Os registros de máquina mais detalhados são armazenados somente na máquina que os gerou e costumam ser mantidos por duas semanas.

Gestão de subcontratantes e fornecedores

A Asana toma medidas razoáveis para selecionar e manter somente fornecedores de serviços terceirizados que respeitarão e implementarão as medidas de segurança conforme determinadas em nossas políticas. Antes de implementar um software ou poder usar um fornecedor de softwares na Asana, a equipe de TI da Asana revisa cuidadosamente os protocolos de segurança, as políticas de retenção de dados, as políticas de privacidade e o histórico de segurança dos fornecedores. A equipe de TI pode rejeitar o uso de qualquer software ou fornecedor de softwares caso não demonstre ter a capacidade de proteger adequadamente os dados e usuários finais da Asana. As reavaliações de fornecedores são realizadas anualmente.

Os subcontratantes atuais podem ser consultados na nossa página de Termos.[7]

[7] http://asana.com/terms#subprocessors

Privacidade, certificações e conformidade

Política de privacidade

Você pode consultar a Política de privacidade da Asana na nossa página de Termos.[8] Ela inclui:

- Que tipo de usuário eu sou e quais termos de privacidade se aplicam a mim?
- Termos de privacidade para assinantes
- Termos de privacidade para usuários de planos gratuitos
- Termos de privacidade para visitantes do site
- Termos de privacidade adicionais para todos os usuários
- Informações de contato da Asana

Certificações e conformidade legal

A Asana foi avaliada quanto a diversas normativas de privacidade e segurança e obteve as certificações a seguir:

Estrutura do Escudo de Proteção da Privacidade

A Asana é certificada de acordo com as Estruturas do Escudo de Proteção da Privacidade da UE-EUA e da Suíça-EUA[9] com relação à coleta, uso e retenção de informações pessoais dos países-membros da União Europeia e da Suíça, respectivamente.

Controles do serviço e da organização (SOC 2)

A Asana concluiu com sucesso sua auditoria SOC 2 (Tipo II) para os controles que foram implementados em relação à segurança, à disponibilidade e à confidencialidade. A obtenção da certificação SOC 2 (Tipo II) significa que foram estabelecidos processos e práticas sobre esses três princípios de controle que foram validados por um terceirizado independente.

[8] http://asana.com/terms#privacy-policy

[9] https://www.privacyshield.gov/participant?id=a2zt0000000TNLRAA4&contact=true

RGPD

O Regulamento Geral de Proteção dos Dados (RGPD) é uma lei europeia que estabelece proteções aos dados pessoais dos residentes da UE, em vigor desde 25 de maio de 2018. De acordo com o RGPD, as organizações que coletam, mantêm, utilizam ou processam os dados pessoais dos residentes da UE (independentemente da localização da organização) devem implementar determinadas garantias de privacidade e segurança para esses dados. A Asana definiu um programa abrangente de conformidade com o RGPD e está comprometida em estabelecer parcerias com seus clientes e fornecedores para reforçar a conformidade com o RGPD. Algumas das medidas significativas adotadas pela Asana para alinhar suas práticas ao RGPD incluem:

- Revisões de nossas políticas e contratos com nossos parceiros, fornecedores e usuários
- Melhorias aos nossos procedimentos e práticas de segurança
- Revisões e mapeamentos rigorosos dos dados que coletamos, usamos e compartilhamos
- Elaboração de uma documentação interna mais robusta sobre privacidade e segurança
- Capacitação de funcionários sobre os requisitos do RGPD e boas práticas gerais para privacidade e segurança
- Avaliação e elaboração minuciosas de um processo de resposta e de uma política dos direitos dos titulares dos dados. Fornecemos a seguir detalhes adicionais sobre as principais áreas do programa de conformidade com o RGPD da Asana e como os clientes podem usufruir da Asana para apoiar suas próprias iniciativas de conformidade com esse regulamento.

Adendo de Processamento de Dados

De acordo com o RGPD, os "controladores de dados" (ou seja, as entidades que estabelecem as finalidades e meios para processamento de dados) devem celebrar um acordo com as entidades que processarem dados em seu nome (denominadas "processadores de dados"). A Asana oferece aos clientes que atuam como controladores de dados pessoais na UE a opção de celebrar um contrato robusto de processamento de dados sob o qual a Asana se compromete a processar e proteger os dados pessoais de acordo com os requisitos estipulados no RGPD. Isso inclui o compromisso da Asana de processar os dados pessoais conforme as instruções do controlador de dados. Consulte o Adendo de Processamento de Dados na nossa página de Termos.[10]

Aplicação da lei

A Asana segue as Diretrizes de solicitação de dados para a aplicação da lei descritas na nossa página de Termos.[11]

[10] http://asana.com/terms#data-processing

[11] http://asana.com/terms#law-enforcement-guidelines

Conclusão

Usamos a Asana diariamente para manter a nossa equipe organizada, conectada e focada nos resultados. Garantir que a nossa plataforma permaneça segura é fundamental para proteger nossos próprios dados e as informações de nossos clientes. Essa é a nossa maior prioridade.

Empenhamo-nos para sermos líderes no gerenciamento colaborativo do trabalho ao tornar a Asana fácil de usar e manter a segurança dos dados em primeiro lugar. Para obter mais informações sobre as ofertas dos planos pagos da Asana, entre em contato com a nossa equipe de vendas pelo endereço sales@asana.com.

Quer reportar uma questão de segurança? Envie um e-mail para security@asana.com.