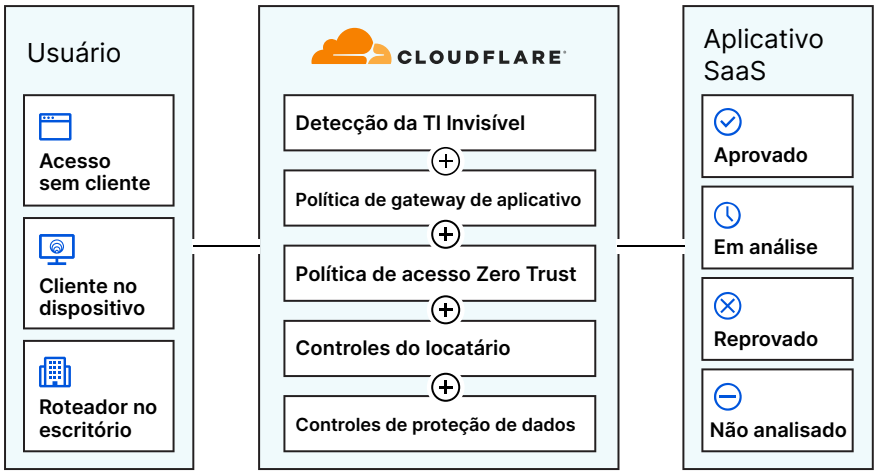
RESUMO DA SOLUÇÃO

# Zero Trust, visibilidade e controle de todos os aplicativos SaaS

Os aplicativos SaaS capacitam suas equipes a fazer mais do que nunca, mas a flexibilidade e a liberdade que proporcionam à sua força de trabalho também apresentam riscos de segurança, desafios de visibilidade e obstáculos de controle de acesso para sua organização.

A Cloudflare oferece as ferramentas de que você precisa para proteger seus dados e sua força de trabalho e, ao mesmo tempo, permite que seus funcionários usem as ferramentas que os ajudam a fazer o trabalho.




## Detecte e controle a TI Invisível

Sem a visibilidade dos aplicativos que seus funcionários usam, você não pode controlar como os dados sensíveis são armazenados, compartilhados ou expostos a terceiros. A Cloudflare ajuda você a descobrir, categorizar e controlar todos os aplicativos aprovados e não aprovados em sua organização, enquanto registra cada conexão e solicitação em um local centralizado.

## Aplique a política de segurança Zero Trust

Os aplicativos SaaS ficam hospedados fora da rede corporativa, limitando a capacidade das suas equipes de segurança de controlar a forma como os usuários acessam e movem dados entre esses aplicativos. A Cloudflare cria uma camada de medidas de segurança Zero Trust na frente de seus aplicativos SaaS para autenticar os usuários legítimos e evitar o acesso de usuários não autorizados ou dispositivos suspeitos aos seus arquivos e dados.

## Aplique controles de proteção de dados e locatários

Quando os funcionários acessam a instância de aplicativos incorreta, podem compartilhar e armazenar seus dados nos locais errados e abrir caminho para possíveis vazamentos de dados e outros riscos de segurança. A Cloudflare ajuda a controlar o compartilhamento e armazenamento de seus dados, estejam eles em trânsito na nossa Rede ou em uso em nosso navegador remoto. Agora, é possível criar e implantar políticas de navegação Zero Trust para proteger os dados que residem em qualquer locatário SaaS e impedir que os funcionários acessem os aplicativos incorretos ou os locatários incorretos de aplicativos aprovados.

## Detecte e controle a TI Invisível

### Avalie os aplicativos usados por seus funcionários

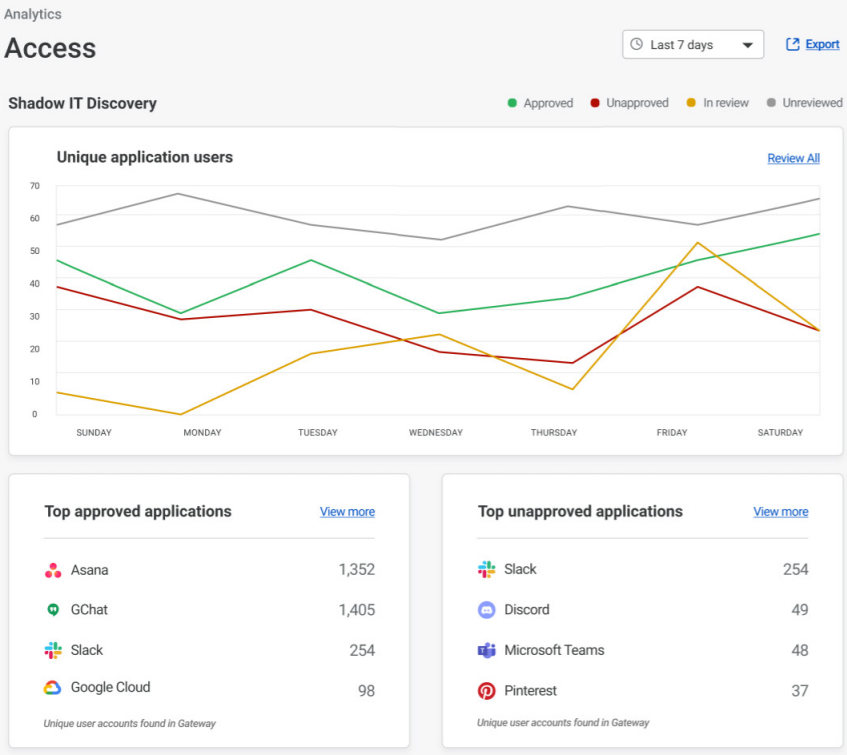
Quando sua equipe de TI não consegue ver os aplicativos usados pelos funcionários, é impossível controlar o que acontece com os dados que ficam dentro desses aplicativos. A Cloudflare agrega e categoriza automaticamente todas as solicitações HTTP em nosso registro de atividades por tipo de aplicativo. Assim, é possível definir o status e acompanhar o uso de aplicativos aprovados e não aprovados em toda a empresa.

### Registre todas as conexões e solicitações

A Cloudflare ajuda a mitigar os riscos gerados para a empresa quando os funcionários acessam aplicativos não aprovados ou usam dispositivos não gerenciados para acessar informações sensíveis. Todas as conexões e solicitações são registradas em um local central, assim você vê quais aplicativos estão sendo usados e o que os usuários estão fazendo dentro deles. Além disso, os administradores podem bloquear e permitir solicitações a aplicativos SaaS evitando que os usuários contornem controles de segurança importantes e ganhem acesso não autorizado a aplicativos, recursos e dados da empresa.

### Principais recursos

- Monitorar automaticamente quais aplicativos já estão protegidos pela Cloudflare
- Reter registros por até seis meses na Rede da Cloudflare
- Enviar registros para um ou mais de seus serviços de armazenamento de registro em nuvem e SIEM



## Aplique a política de acesso Zero Trust aos seus aplicativos SaaS

### Forneça acesso seguro ao SaaS com o proxy de identidade da Cloudflare

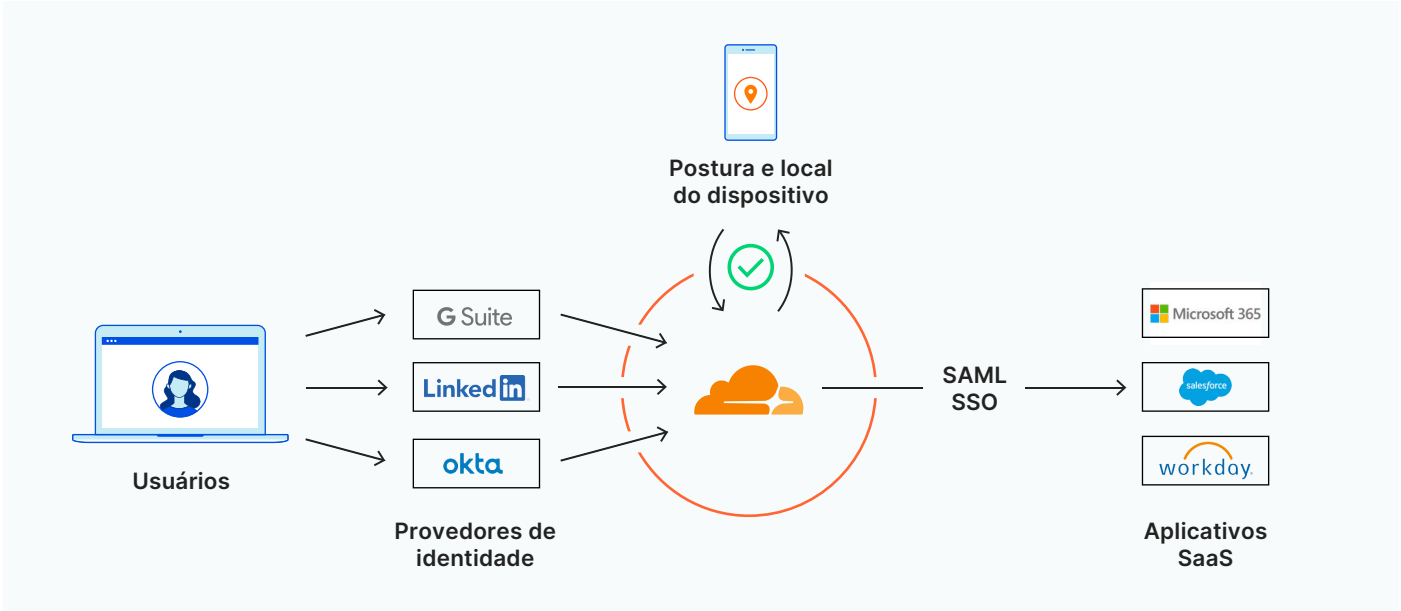
Os aplicativos SaaS são hospedados por terceiros e muitas vezes são gerenciados por unidades de negócios, ou seja, sua equipe de TI tem pouco controle sobre como os usuários acessam esses aplicativos. A Cloudflare fica entre seu provedor de identidade e seus aplicativos SaaS para permitir que você crie e aplique regras Zero Trust com reconhecimento de identidade e orientadas ao contexto no processo de login — tudo isso sem interromper a experiência do usuário final.

### Defina as permissões de aplicativos para os dispositivos dos usuários

Seu departamento de TI precisa de controle granular sobre a maneira como dispositivos gerenciados pela empresa fazem login em aplicativos SaaS. A Cloudflare insere regras Zero Trust no processo de login único de todos os aplicativos compatíveis com a autenticação SAML. Primeiro, os usuários são autenticados no provedor de identidade; em seguida, a Cloudflare compara a solicitação com a postura e o local do dispositivo antes de autorizar o acesso a um aplicativo SaaS -- com gerenciamento de sessão flexível para fazer verificações contínuas. Além disso, os administradores de segurança podem criar políticas específicas para um dispositivo, de modo que os usuários só possam acessar os aplicativos por meio de dispositivos que atendam aos requisitos de segurança pré-estabelecidos, incluindo certificados mTLS.

### Principais recursos

- Integrar vários provedores de identidade ou diversas instâncias do mesmo provedor
- Verificar a identidade do usuário de acordo com as regras do aplicativo (por exemplo, MFA exige chave rígida)
- Verificar a postura do dispositivo de acordo com as regras do aplicativo (por exemplo, política de SWG aplicada, EPP instalada, certificado mTLS, criptografia de disco habilitada) e local
- O portal de inicialização de aplicativos da Cloudflare permite que os usuários vejam e acessem todos os aplicativos SaaS aprovados



## Aplique controles de proteção de dados e locatários a qualquer aplicativo SaaS

### Limite o acesso a instâncias de aplicativos não corporativos

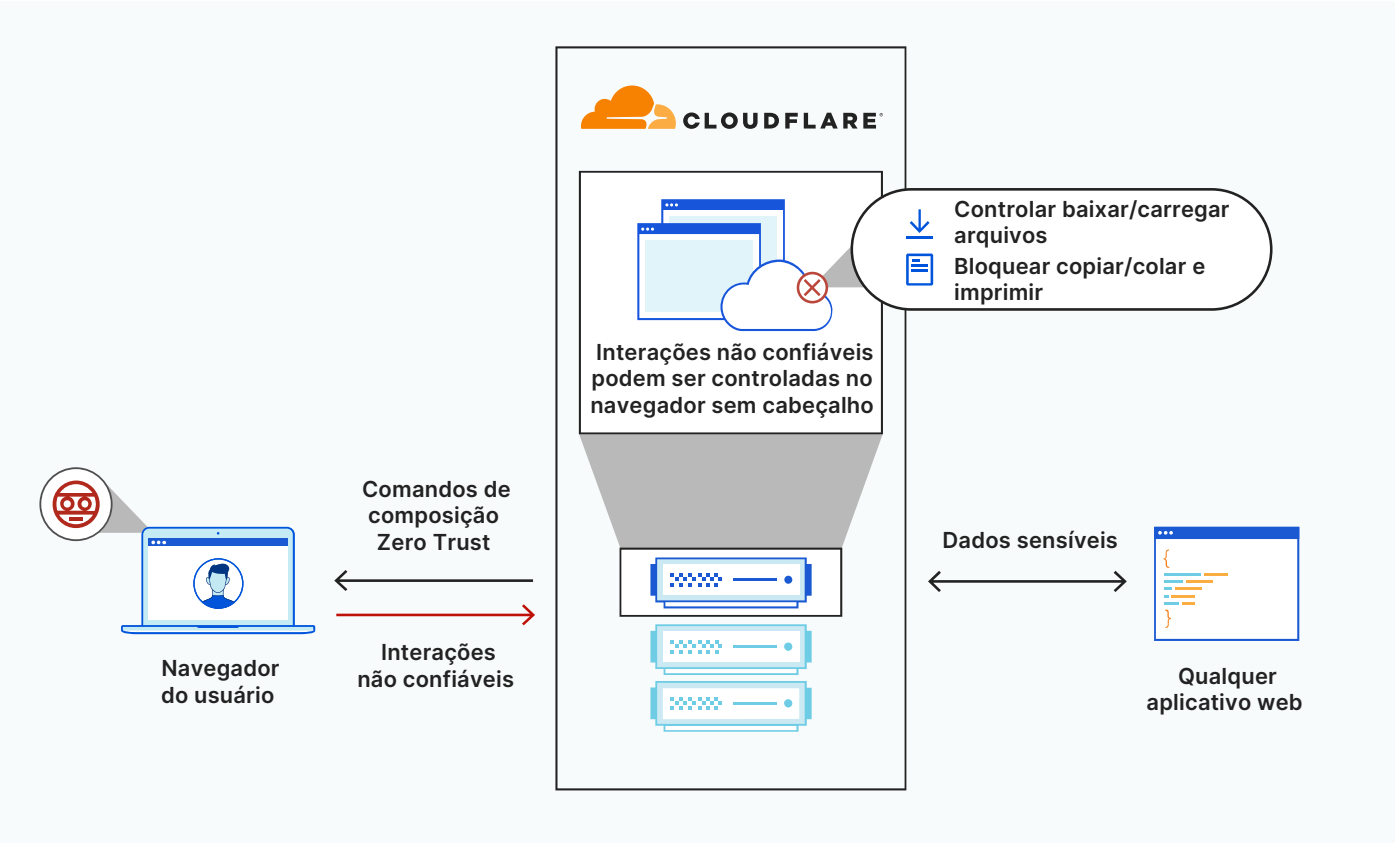
A Cloudflare, permite o controle do locatário por meio de políticas de gateway HTTP, que podem ser configuradas para evitar que os usuários acessem versões para consumidores dos aplicativos. Em vez de aplicar essas políticas usando servidores proxy locais por VPNs corporativas, a Cloudflare filtra e inspeciona todo o tráfego e todas as solicitações em uma vasta Rede global de data centers — para que seus usuários nunca experimentem aumento de latência ou degradação na performance.

### Evite o vazamento de dados corporativos dos locatários

Com a Cloudflare, fica mais fácil criar e implantar políticas de navegação Zero Trust para controlar e proteger os dados que residem em aplicativos web. Todo o código do aplicativo é executado em um navegador sem cabeçalho seguro executado remotamente em nossa enorme Rede global, em vez de dispositivos nos endpoints, de modo que os dados sensíveis são protegidos contra dispositivos comprometidos ou não confiáveis e ameaças de dia zero. Além disso, os administradores controlam a forma como os usuários acessam e compartilham esses dados a fim de minimizar o risco de perda de dados acidental ou outras violações de dados mais graves.

### Principais recursos

- Permitir ou bloquear comportamentos no navegador com base em vários critérios, como aplicativo, tipo de aplicativo, hostname, identidade do usuário e risco de segurança
- Controlar as ações do usuário no navegador: baixar, carregar, copiar e colar, entradas de teclado e funcionalidades de impressão



## A diferença da Cloudflare

### Abrangência da nossa plataforma

A Cloudflare coloca controles de acesso Zero Trust (ZTNA), gateway (SWG) e navegador (RBI) na frente de seus aplicativos SaaS — sua equipe de TI não precisa configurar nem operar um produto CASB dedicado.

### Construídos do zero

Os recursos CASB da Cloudflare funcionam perfeitamente com nossos serviços de ZTNA, SWG e RBI, porque todos foram construídos do zero — o que elimina a necessidade de lidar com produtos pontuais para proteger aplicativos e equipes.

### Painel de controle único

A Cloudflare permite que as organizações definam políticas e gerenciem o acesso e o uso de aplicativos a partir de um único painel — para que você possa monitorar todas as solicitações e permissões em um piscar de olhos.

## A Cloudflare ajuda equipes a monitorar, proteger e controlar aplicativos SaaS por meio de um pacote integrado nativo de recursos de segurança Zero Trust.

Saiba mais agora