CLOUDFLARE

VISÃO GERAL DO PRODUTO

Isolamento do navegador remoto (RBI)

Isolar os usuários contra ameaças on-line e proteger dados em aplicativos com controles de navegador integrados.

Proteger a linha de frente do trabalho moderno

Hoje, o navegador é fundamental para os negócios diários, apresentando riscos como alvo de invasores e como ambiente de vazamento de dados. No entanto, os controles por meio do isolamento do navegador remoto tradicional ou de infraestrutura de desktop virtual (VDI) levaram, historicamente, a experiências do usuário frustrantes, implantações complexas e altos custos.

O Isolamento do navegador da Cloudflare simplifica a proteção de dados e contra ameaças e, ao mesmo tempo, preserva uma experiência de navegação nativa. Ao executar todo o código da web em nossa rede global em nuvem (em vez de localmente nos dispositivos), as organizações podem eliminar riscos comuns:

- **Isolar a navegação na web** para proteger os usuários contra ameaças cibernéticas, incluindo dia zero
- **Isolar aplicativos** para funcionários, terceiros e dispositivos não gerenciados para bloquear dados em uso
- **Isolar ferramentas de IA** para restringir o compartilhamento excessivo de informações proprietárias

Isolamento na arquitetura SSE da Cloudflare

O Isolamento do navegador da Cloudflare foi desenvolvido desde o início em nossa rede para funcionar nativamente com nossos outros serviços de Serviços de segurança de borda (SSE) combináveis.

Os controles de isolamento funcionam junto com ZTNA, SWG, DLP, segurança de e-mail e muito mais para reduzir o risco em ambientes web, SaaS, e-mail e aplicativos privados.

Por que a Cloudflare?

Simples de configurar e escalar

Para dispositivos gerenciados, implante com um cliente de dispositivo. Para prestadores de serviços e dispositivos não gerenciados, simplifique o isolamento de destinos específicos por meio de links.

Compatível em qualquer página web com qualquer navegador.

UX rápida e consistente globalmente

Nosso Isolamento do navegador remoto foi projetado para ser executado em mais de 300 locais em nossa rede global, de modo que as sessões isoladas sejam realizadas perto dos usuários finais onde quer que estejam.

Mantenha os usuários seguros e produtivos com navegação responsiva.

Arquitetado para Zero Trust

Aplique uma abordagem de “nunca confiar” à navegação na internet, para que nenhum conteúdo da web seja confiável por padrão.

Unifique a visibilidade e os controles nos serviços SSE, incluindo isolamento do navegador remoto, em uma única rede e plano de controle com a Cloudflare.

Caso de uso: isolar a navegação na web para se defender contra ameaças

Neutralize malware, ransomware, ameaças de dia zero e muito mais, executando todo o conteúdo da web na rede da Cloudflare, longe dos dispositivos dos usuários.

Mitigue ameaças de phishing impedindo a entrada do usuário em sites arriscados. Minimize os riscos de links desconhecidos em e-mails, SMS, mensagens instantâneas, LinkedIn, redes sociais e aplicativos de colaboração em nuvem.

Isolar toda a navegação na web

LUANA SAVINGS BANK

Serviços financeiros
Ler o estudo de caso

- **Nenhum dispositivo infectado por malware** proveniente de navegação na internet desde a primeira adoção do isolamento do navegador remoto
- **Doze horas economizadas mensalmente** para dois funcionários ao eliminar o tempo de investigação de infecções por malware

Comece a usar

Etapas prioritárias

- **Implantar cliente de dispositivo** por meio de registro gerenciado ou automático
- **Configurar filtragem de DNS e inspeções HTTP** como camadas iniciais de defesa contra ameaças
- **Isolar o navegador** para domínios de risco ou usuários prioritários

Expandir controles

- **Implantar a segurança de e-mail em nuvem** para proteger caixas de entrada contra phishing e isolar links suspeitos.

Caso de uso: isolar o acesso ao aplicativo para proteger os dados, com/sem um cliente de dispositivo

Controle como os usuários interagem com os dados (por exemplo, restringir copiar/colar, fazer upload/download, entradas de teclado, impressão) isolando o acesso a aplicativos específicos, incluindo ferramentas de IA.

A implantação sem cliente em sites e aplicativos específicos ajuda a reduzir os riscos de exposição de dados apresentados por prestadores de serviços, terceiros e dispositivos não gerenciados.

APPLIED

Tecnologia para seguros
Ler o estudo de caso

Isolar ferramentas de IA disponíveis publicamente para evitar que os usuários copiem e colem informações confidenciais em LLMs.

OpenAI Bard

Comece a usar

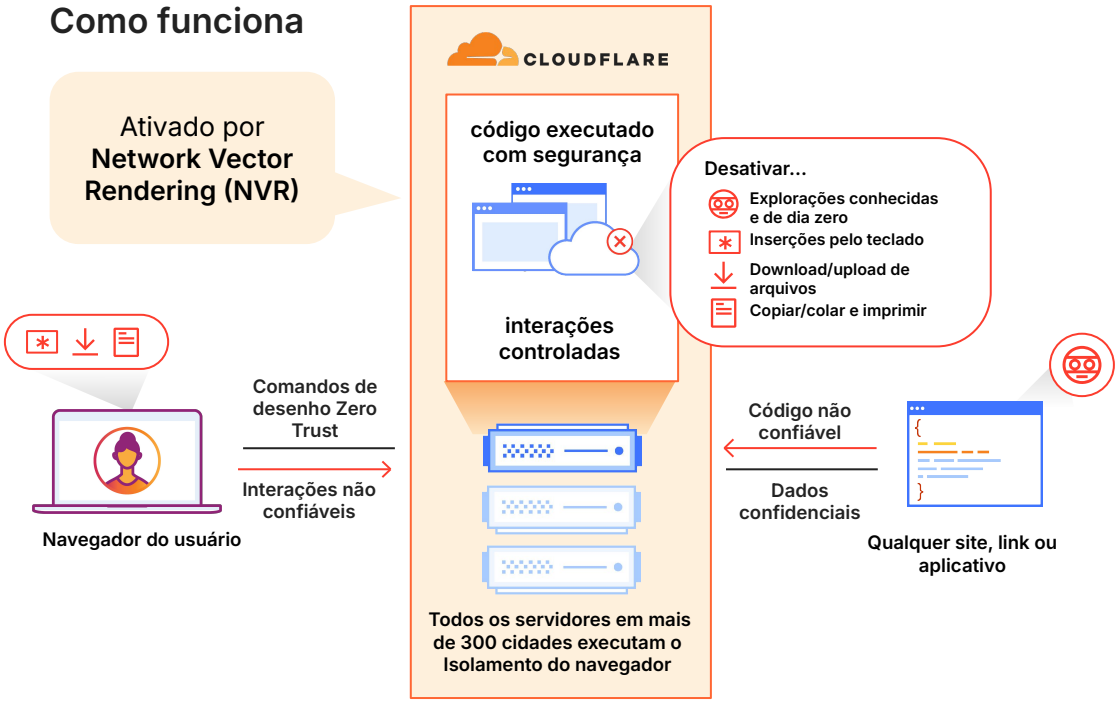
Etapas prioritárias

- **Isolar destinos por meio de um URL com prefixo ou isolar aplicativos auto-hospedados por domínio**, sem necessidade de um cliente de dispositivo
- **Implantar cliente de dispositivo (se necessário)** para visibilidade e controles HTTP mais granulares
- **Definir controles de dados em uso**: bloquear copiar/colar, fazer upload/download, entradas de teclado ou impressão

Expandir controles

- **Bloquear a movimentação de dados confidenciais** com verificações e políticas de prevenção contra perda de dados (DLP).

Como funciona



Experiência do usuário ultra rápida com o NVR

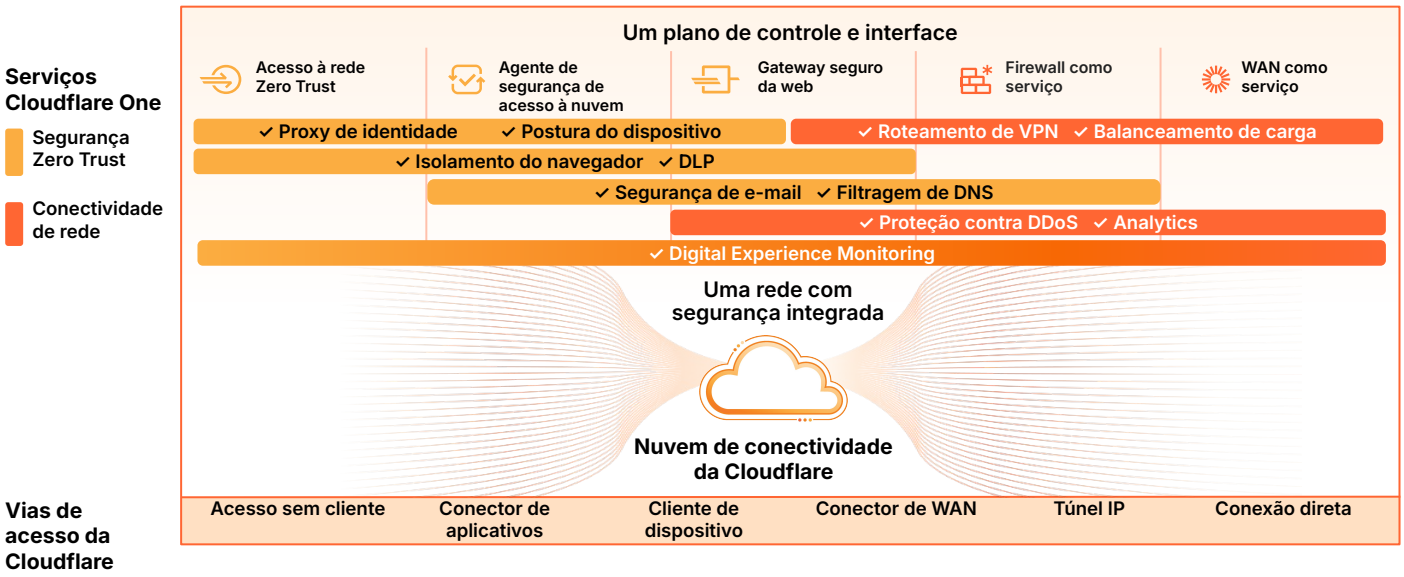
- Transmitir comandos de desenho seguro para o dispositivo.
- Eliminar a latência de métodos tradicionais de isolamento do navegador remoto, como pixel-pushing ou reconstrução de modelo de objeto de documento.

Exemplos de recursos

Políticas	
Isolar por identidade, ameaça à segurança ou conteúdo	Isolar sites com base em identidade, ameaças à segurança ou conteúdo. Cobertura abrangente de riscos de segurança (por exemplo, ransomware, phishing, domínios de DGA), categorias de conteúdo (por exemplo, entretenimento) e aplicativos (por exemplo, inteligência artificial, redes sociais).
Controles do navegador para dados em uso	Definir políticas para restringir entradas do teclado, impressão e fazer upload/download. Bloquear totalmente copiar e/ou colar, permitir copiar e/ou colar apenas em um navegador isolado para evitar a movimentação de dados para áreas de transferência locais. Exportar logs que rastreiam essas ações dos usuários.
Funcionalidade SWG completa	Controlar o tráfego com base na origem, no destino, em domínios, em métodos HTTP, em URLs e em outros critérios. A inspeção HTTP1/2/3 permite verificações de AV e DLP, postura do dispositivo, locatários e muito mais. Inspeção ilimitada de TLS 1.3 ativada por padrão. As chaves TLS são armazenadas com criptografia pós-quântica segura.
Políticas de DLP para dados em trânsito	Analisar o tráfego HTTP em busca de dados confidenciais (por exemplo, financeiros, de saúde, código-fonte) e bloquear com políticas de prevenção contra perda de dados (DLP). Aplicar em navegadores isolados com ou sem um cliente de dispositivo.
Vias de acesso	
Vias de acesso baseadas em identidade	Aplicar políticas de HTTP baseadas em identidade ao tráfego que faz proxy por meio de nosso cliente de dispositivo ou a aplicativos protegidos por nosso serviço Acesso à rede Zero Trust (ZTNA).
Não identidade	Aplicar políticas de HTTP sem identidade ao tráfego encaminhado para um endpoint de proxy com arquivos de configuração automática de proxy (PAC) ou por meio de um túnel GRE/IPsec.
Isolamento da web sem cliente	Renderizar páginas web em um navegador remoto quando os usuários acessam um URL com prefixo: https://<your-team-name>.cloudflareaccess.com/browser/<URL>.
Serviços extensíveis	
Isolamento de link de e-mail	Em combinação com o Cloudflare Email Security, reescreva links suspeitos/desconhecidos em e-mails para abrir em um navegador isolado, protegendo os usuários contra ameaças de phishing e malware.
Extensão de navegador	O Isolamento do navegador da Cloudflare é compatível com a execução de extensões web Chromium nativas. Estender as ferramentas que exigem acesso ao modelo de objeto de documento (como gerenciadores de senhas e bloqueadores de anúncios) para páginas isoladas. A extensão sincroniza cookies entre o navegador local e remoto, para que os usuários possam acessar perfeitamente aplicativos isolados e não isolados sem precisar se autenticar novamente.

Modernizar a segurança com a plataforma SSE/SASE da Cloudflare

O Isolamento do navegador da Cloudflare é um serviço combinável dentro do Cloudflare One, nossa plataforma SSE/SASE. As organizações normalmente implantam o isolamento do navegador remoto junto com ZTNA, SWG e outros recursos para aumentar a segurança da web e do e-mail ou para impor controles de dados granulares em ambientes web, SaaS e de aplicativos privados.



Uma plataforma unificada

- **Acesso seguro** ao verificar e segmentar qualquer usuário para qualquer recurso
- **Defesa contra ameaças** ao cobrir todos os canais com IA/ML e inteligência contra ameaças alimentadas por rede
- **Proteção de dados** ao aumentar a visibilidade e o controle dos dados em trânsito, em repouso e em uso

Uma rede programável

- **Mais eficaz** ao simplificar a conectividade e o gerenciamento de políticas
- **Mais produtiva** ao garantir UX rápida, confiável e consistente em todos os lugares
- **Mais ágil** ao inovar rapidamente para atender aos seus requisitos de segurança em constante evolução

Quer experimentar a navegação isolada com a Cloudflare?

Experimente agora. Não requer instalação

Ou quer modernizar a segurança do seu navegador?

Solicite um workshop