CLOUDFLARE

RESUMO DA SOLUÇÃO

Cloudflare for Unified Risk Posture

Aplicação de postura de risco automatizada e dinâmica em mais áreas de sua superfície de ataque em expansão.

Problema: muita superfície de ataque

Complexidade crescente para gerenciar riscos

Está se tornando cada vez mais complexo e ineficiente para as empresas acompanhar e mitigar os riscos cada vez mais diversos em sua superfície de ataque em expansão. As equipes de segurança hoje lutam com:

- **Muitas ferramentas isoladas** com visibilidade e interoperabilidade limitadas para avaliar riscos de forma holística
- **Muitos sinais de risco** que levam à sobrecarga de informações, dificultando a priorização dos riscos
- **Muito esforço manual** para análise de riscos, o que demanda tempo, recursos e experiência

Solução: unificar controles de postura de risco

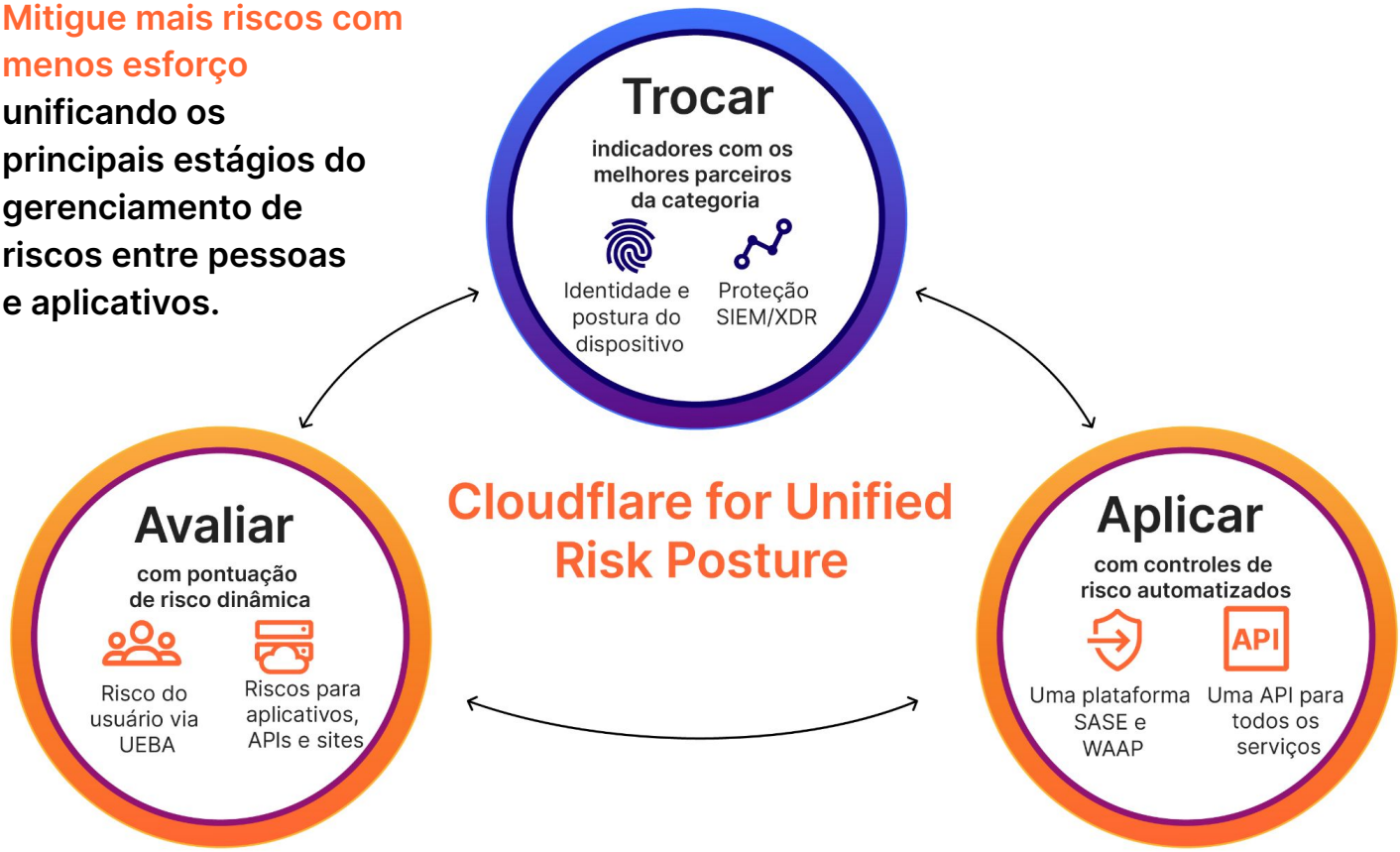
Uma plataforma para se adaptar aos riscos em evolução

Convirja as funcionalidades de segurança SASE e WAAP na rede global da Cloudflare para gerenciar riscos entre seus funcionários e aplicativos. Simplifique o gerenciamento de riscos realizando três tarefas principais em uma plataforma:

- **Avalie o risco entre pessoas e aplicativos** com modelos dinâmicos de pontuação de risco próprios
- **Troque indicadores com as melhores ferramentas** nas plataformas IDP, XDR, SIEM e plataforma de proteção de endpoints
- **Aplique controles de risco automatizados em escala** em qualquer local e ambiente de TI

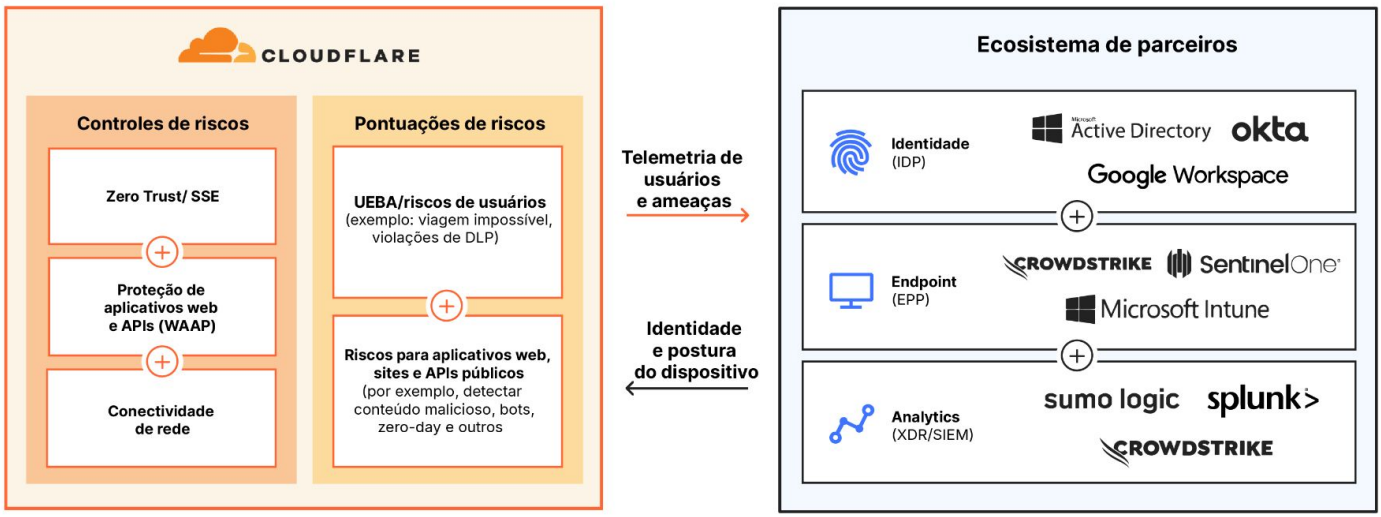
Mitigue mais riscos com menos esforço

unificando os principais estágios do gerenciamento de riscos entre pessoas e aplicativos.



Avalie riscos e troque dados com parceiros

A Cloudflare avalia o risco empresarial aproveitando modelos dinâmicos de pontuação de risco próprios e trocando indicadores de risco com os melhores parceiros de tecnologia.



Pontuação dinâmica de risco primário

Avalie o risco entre pessoas e aplicativos com modelos apoiados por IA e aprendizado de máquina.

Pontuação de risco de usuários (ou UEBA)

Detecte riscos com base no comportamento dos usuários, uma abordagem conhecida como análise de entidades e comportamento de usuários (UEBA). A Cloudflare classifica os usuários como de alto/médio/baixo risco após observar atividades suspeitas ou anômalas, como viagens impossíveis ou violações da política de DLP.

Riscos de aplicativos

Crie políticas para proteger aplicativos, APIs e sites com base em modelos que identificam conteúdo malicioso, scripts de navegador maliciosos, bots e ameaças zero-day.

Esses modelos de risco se aplicam a qualquer infraestrutura pública ou interna protegida pela Cloudflare. Isso significa que você pode aplicar proteções contra explorações de vulnerabilidades de aplicativos, DDoS e bots na frente de aplicativos internos, como servidores Jira e Confluence auto-hospedados.

Troca com parceiros

Integrações únicas com a API unificada da Cloudflare ajudam você a fazer mais com suas ferramentas existentes.

Ingerir indicadores de risco

A Cloudflare ingere pontuações de risco de parceiros de plataforma de proteção de endpoints (EPP) e provedores de identidade (IDP). Com essas integrações, você pode impor verificações de identidade e postura do dispositivo para qualquer solicitação de acesso a qualquer destino, de acordo com as práticas recomendadas de Zero Trust. Integre vários provedores ao mesmo tempo para aplicar políticas diferentes em contextos diferentes.

Compartilhar telemetria

Envie logs da Cloudflare para plataformas estendidas de detecção e resposta (XDR) e informações de segurança e gerenciamento de eventos (SIEM) para mais análise e etapas adicionais de mitigação de riscos.

Aplique controles de risco automatizados em escala

Uma plataforma para aplicar proteções com base em pontuações de risco próprias e de terceiros, alimentada exclusivamente por uma rede em nuvem global inteligente e programável.

Simplifique o gerenciamento de riscos
Consolide fornecedores para reduzir a complexidade e os riscos empresariais.

Veja mais, proteja mais
Obtenha inteligência automatizada e dinâmica sobre riscos e contra ameaças a partir de nossa enorme rede global.

Escale em todos os lugares
Proteções resilientes e consistentes em qualquer local do mundo.

Exemplos de casos de uso

Caso de uso: proteger dados confidenciais

Problema: o usuário trata de forma inadequada dados regulamentados (por exemplo, informações de identificação pessoal, saúde, finanças) ou informações proprietárias (por exemplo, código de desenvolvedores).

Solução: evitar vazamentos de dados com controles de prevenção contra perda de dados (DLP).
Sinalizar o usuário como arriscado com base no grande número de violações de DLP e investigar a atividade. Restringir ou isolar o acesso desse usuário a outros ambientes com acesso à rede Zero Trust (ZTNA) ou políticas de isolamento do navegador.

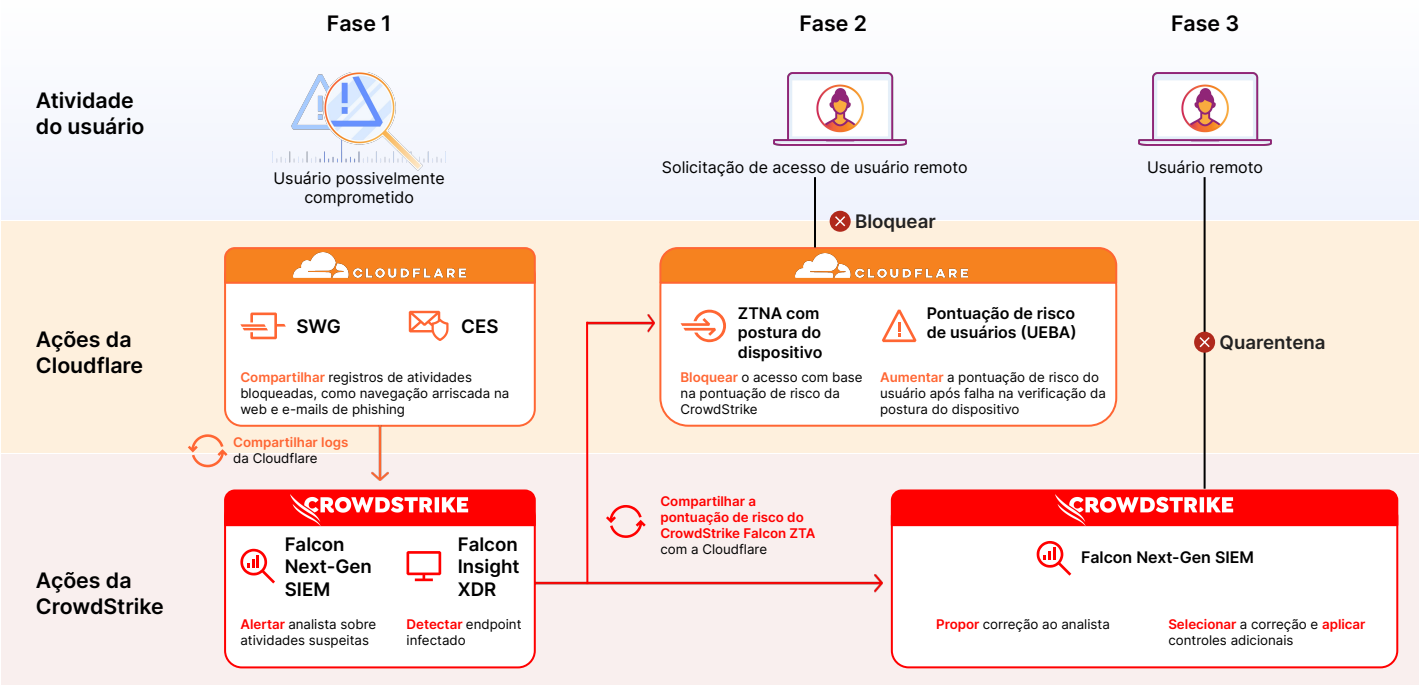
Caso de uso: proteger aplicativos, APIs e sites

Problema: os agentes e bots de ameaças têm como alvo aplicativos, APIs e sites públicos.

Solução: detectar e mitigar conteúdo malicioso, bots e zero-day usando modelos de risco apoiados por ML, como nosso WAF Attack Score ou pontuação de bots. Analisar possíveis configurações incorretas, riscos de vazamento de dados e vulnerabilidades que afetam sua infraestrutura.

Caso de uso: Impor Zero Trust com Cloudflare e CrowdStrike

Abaixo está um exemplo de fluxo de trabalho de como a Cloudflare e a CrowdStrike trabalham em conjunto para aplicar políticas Zero Trust e mitigar riscos emergentes. Juntas, a Cloudflare e a CrowdStrike se complementam trocando dados de atividades e riscos e aplicando políticas e etapas de correção baseadas em riscos.



Fase 1: Investigação automatizada

A Cloudflare e a CrowdStrike ajudam uma organização a detectar que um usuário está comprometido.

Neste exemplo, a Cloudflare bloqueou recentemente a navegação em sites arriscados e e-mails de phishing, servindo como primeira linha de defesa. Esses logs são então enviados para o CrowdStrike Falcon Next-Gen SIEM, que alerta seu analista da organização sobre atividades suspeitas.

Ao mesmo tempo, o CrowdStrike Falcon Insight XDR verifica automaticamente o dispositivo do usuário e detecta que ele está infectado. Como resultado, a pontuação do Falcon ZTA que reflete a saúde do dispositivo é reduzida.

Fase 2: Aplicação de Zero Trust

Esta organização configurou verificações de postura do dispositivo por meio do acesso à rede Zero Trust (ZTNA) da Cloudflare, permitindo o acesso apenas quando a pontuação de risco do Falcon ZTA estiver acima de um limite específico definido por eles.

Nosso ZTNA nega a próxima solicitação do usuário para acessar um aplicativo porque a pontuação do Falcon ZTA fica abaixo desse limite.

Devido a essa falha na verificação da postura do dispositivo, a Cloudflare aumenta a pontuação de risco desse usuário, o que o coloca em um grupo com controles mais restritivos.

Fase 3: Correção

Paralelamente, o Next-Gen SIEM da CrowdStrike continuou a analisar a atividade específica do usuário e os riscos mais amplos em todo o ambiente da organização. Usando modelos de aprendizado de máquina, a CrowdStrike revela os principais riscos e propõe soluções para cada risco ao seu analista.

O analista pode então analisar e selecionar táticas de correção, por exemplo, colocar o dispositivo do usuário em quarentena, para reduzir ainda mais o risco em toda a organização.

Impactos para o cliente

Vantagens	Exemplos de métricas
Reduzir o esforço em SecOps com menos criação manual de políticas e maior agilidade na resposta a incidentes	• Aumentar o número de fluxos de trabalho automatizados • Reduzir o número de cliques para criar políticas • Reduzir o tempo médio de detecção (MTTD) • Reduzir o tempo médio de resposta (MTTR)
Reduzir o risco cibernético com aplicação de postura de risco automatizada e dinâmica em toda a sua superfície de ataque	• Reduzir o número de incidentes críticos • Aumentar o número de ameaças bloqueadas automaticamente

O que eles dizem

"A Cloudflare nos ajuda a mitigar riscos da maneira mais eficaz e com menos esforço e simplifica a forma como fornecemos Zero Trust em toda a minha organização."

Anthony Moisant
SVP, Chief Information Officer
e Chief Security Officer, Indeed

Site de empregos nº 1 do mundo, com mais de 350 milhões de visitantes únicos por mês

"Ter uma solução única da Cloudflare implementada para nos ajudar a gerenciar a complexidade em nossas operações globais tornou nossas vidas muito mais fáceis."

Wilson Tang
Director of Engineering, Platform Core Services,
Delivery Hero

Empresa alemã de pedidos e entrega de alimentos on-line que opera em mais de 70 países

Leia o estudo de caso

Comparações com os concorrentes

Com base em dados de 07 de maio de 2024

	Cloudflare	Zscaler	Netskope	Palo Alto Networks (Prisma Access)
Avaliar o risco com modelos de pontuação de risco próprios				
Modelos de análise de comportamento de usuários e entidades (UEBA) em tempo real /pontuação de risco de usuário	✅	✅	✅	✅
Acesso a e-mail próprio/dados de risco de phishing	✅	❌	❌	❌
Conteúdo malicioso e detecção de zero-day via WAF	✅	❌	❌	❌
Visualização em painel único para todos os riscos apresentados por usuários e aplicativos	Trabalho em andamento na Central de segurança da Cloudflare	✅	Visibilidade avançada de postura via Netskope Cloud Exchange deve ser gerenciada na infraestrutura do cliente	Disponível apenas para riscos de aplicativos e de uso de aplicativos
Trocar sinais de risco com ferramentas de terceiros				
Integrações com os principais provedores de plataforma de proteção de endpoints (EPP) e detecção e resposta estendidas (XDR) (por exemplo CrowdStrike, SentinelOne, Microsoft)	✅	✅	✅	✅
Parcerias com os principais provedores de identidade (IDPs) e logins únicos (SSOs) (por exemplo, Okta, Ping Identity, Microsoft)	✅	✅	✅	✅
Uma API para todos os serviços	✅	❌	Recursos completos da API Netskope disponíveis apenas com intervenção de suporte ao cliente	❌
Configuração única para integrações de terceiros em todos os serviços	✅	❌	❌	❌
Aplicar controles de risco				
Criar políticas baseadas no risco de usuários	✅	✅	✅	✅
Uma interface de gerenciamento para criar todas as políticas de Serviço de segurança de borda (SSE)	✅	❌	✅	✅
Todos os serviços são executados em todos os data centers	✅	❌	✅	✅
Escala de rede	>320 locais >13.000 pontos de peering	70 locais 116 pontos de peering	>70 regiões 183 pontos de peering	119 vias de acesso 47 centros de computação
Automação Terraform	Repositório único para toda a plataforma Cloudflare	19 repositórios	Nenhuma criação de política via Terraform	Requer vários provedores e módulos Terraform

A diferença da Cloudflare

Simplicidade da nossa plataforma unificada

Unifique o gerenciamento de postura de risco em uma plataforma que converge controles de borda de serviço de acesso seguro (SASE) e proteção de aplicativos web e APIs (WAAP).

Interoperabilidade ilimitada entre serviços, para que você possa começar mais rapidamente e simplificar o gerenciamento contínuo de riscos.

Orquestre todos os serviços da Cloudflare com nossa API única para personalização e automação com infraestrutura como ferramentas de código como o Terraform.

Flexibilidade de nossas integrações

Troque dados de risco com as ferramentas plataforma de proteção de endpoints, IDP, XDR e SIEM que você já usa para se adaptar às mudanças de risco em toda a sua organização.

Ao contrário de outros fornecedores, configure integrações apenas uma vez e aproveite esses recursos em toda a plataforma da Cloudflare, para que você possa ampliar os controles em seus ambientes de TI com agilidade.

Escala incomparável da nossa rede global em nuvem

Todos os serviços de segurança estão disponíveis para os clientes executarem em todos os nossos mais de 320 locais de rede.

A inspeção de passagem única e a aplicação de políticas são sempre rápidas, consistentes e resilientes.

Além disso, a visibilidade exclusiva de nossa rede (que faz proxy de 20% da web e observa 3T de consultas de DNS por dia) capacita modelos apoiados por IA/ML para defesa contra riscos emergentes.

Pronto para discutir sua abordagem de gerenciamento de riscos?
Solicite uma consulta

Quer continuar aprendendo mais?
Leia nosso anúncio no blog ou visite nosso site