CLOUDFLARE®

Proteção de aplicativos na nuvem

Defesa em camadas, fácil de implantar e ágil contra DDoS, comprometimento dos dados e bots mal-intencionados

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Proteção de aplicativos na nuvem

Defesa em camadas, fácil de implantar e ágil contra DDoS, comprometimento dos dados e bots mal-intencionados

As empresas estão enfrentando cada vez mais pressão para fortalecer a própria postura de segurança. As três forças que estão contribuindo com a pressão são:

- Os invasores estão mais fortes, mais sofisticados e bastante motivados
- A área de superfície dos ataques aumenta devido à maior exposição de APIs públicas pelos aplicativos, maior adoção de SaaS e a integração com mais aplicativos de terceiros
- Aumento do exame minucioso público e governamental de dados, privacidade e segurança

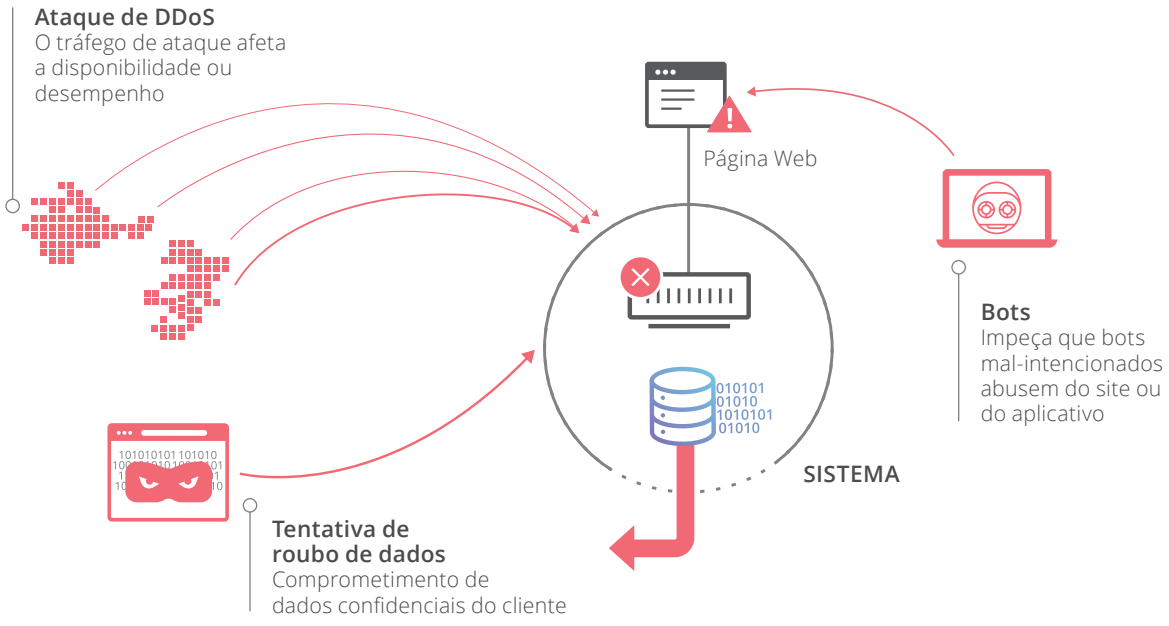
Os invasores estão aumentando a frequência e o volume de ataques DDoS (Negação de serviço distribuído). Aproveitando os botnets e os milhões de dispositivos IoT (Internet das Coisas) online, eles conseguem desferir ataques volumétricos altamente distribuídos com maior facilidade e impacto.

Além de enviar volumes superiores, os invasores estão mudando o foco da camada de rede para a camada de aplicativo. Os ataques na camada de aplicativo, ou "Camada 7", são mais difíceis de detectar, normalmente exigem menos recursos para derrubar um site ou aplicativo e interrompem operações.

Os invasores são capazes de monetizar as tentativas de derrubar sites ou roubar dados confidenciais, por exemplo, sequestrando sites. Como resultado, devido ao pagamento do resgate pelas empresas-alvo, os invasores estão mais motivados, organizados e difusos.

Com uma exposição maior, as empresas precisam fortalecer as defesas contra três problemas e riscos principais:

- Um ataque DDoS contra aplicativos, sites e APIs que prejudica a disponibilidade ou o desempenho, resultando na diminuição da receita, no aumento dos custos operacionais e na degradação da marca
- Comprometimento de dados confidenciais do cliente e da empresa, como PII (informações de identificação pessoal) ou propriedade intelectual, resultando na perda de clientes e da confiança deles
- Bots mal-intencionados abusam dos aplicativos do cliente por meio do recorte de conteúdo, tomada de controle da conta e check-outs fraudulentos



Embora os custos em dólar de um DDoS, uma violação de dados ou bots mal-intencionados variem de acordo com o tamanho da empresa ou setor, a gravidade do impacto comercial está crescendo em todos os negócios.

De acordo com um relatório da IDC de 2015, o custo médio do tempo de inatividade da infraestrutura é de US$ 100 mil por hora.[1]

Um comprometimento de dados poderia ser o vazamento de informações do usuário ou a extrusão de dados confidenciais do cliente, como cartões de crédito e senhas do repositório de dados de um aplicativo. O custo médio global da violação de dados por registro roubado ou perdido foi de US$ 141 em 2017, e o custo médio total de uma violação de dados foi de US$ 3,62 milhões.[2] Graças ao exame mais minucioso dos governos e da mídia, as empresas estão enfrentando repercussões maiores até mesmo pelo menor comprometimento dos dados, não só por meio de multas, mas pela perda da confiança do público.

Além de assumir o controle da conta de um usuário, os bots mal-intencionados também podem conduzir check-outs fraudulentos e recortes de conteúdo. A fraude de check-out de um bot que compra repetida e automaticamente estoques em ofertas limitadas pode prejudicar a marca de uma loja, desencorajar futuros clientes, resultando em menos vendas futuras, e pode até mesmo prejudicar a relação com os fornecedores. O recorte de conteúdo, principalmente para empresas conduzidas por anúncios, pode reduzir diretamente a receita por meio da redução nos rankings de SEO, redução do custo por mil impressões (CPMs) ou perda de anunciantes.

A vantagem

Para combater tanto o aumento da exposição quanto os impactos comerciais cada vez maiores, as empresas precisam resolver os problemas estratégicos específicos, mas também encontrar uma vantagem sobre os vilões em um cenário de ameaças sempre em evolução.

As três diferenças fundamentais são **escala, desempenho e facilidade de uso**.

A escala é importante

A Cloudflare tem a vantagem da capacidade de variação de tamanho e tráfego de rede para análise dos dados. Por proteger mais de 6 milhões de sites de clientes, a Cloudflare tem muitas informações sobre ameaças globais emergentes. Como resultado, as proteções contra DDoS e o Firewall de Aplicativo Web da Cloudflare defendem de forma proativa os clientes contra ataques que causam tempo de inatividade e perda de receita.

Projetada para permitir a escala, a rede da Cloudflare proporciona velocidade e resiliência. Para fornecer todos os seus serviços em mais de 300 bilhões de solicitações por dia, os serviços em execução em cada servidor, em todos os data centers, como DNS, Criptografia e WAF, podem processar cargas imensas de tráfego com baixa latência e alta confiabilidade.

À medida que o tamanho dos ataques de DDoS aumenta, o tamanho e a resiliência da rede beneficia os clientes. A escala da Cloudflare de seus mais de 116 data centers, combinada com a rede Anycast, permite que a Cloudflare resista até mesmo aos ataques com maior distribuição.

Aumente o desempenho e proteja os aplicativos

Tradicionalmente, era comum os clientes sacrificarem a segurança em detrimento do desempenho. Com frequência, as soluções de TLS e WAF prejudicavam o desempenho de um site. Por exemplo, TLS, um protocolo para criptografia de conexões, pode introduzir até quatro viagens de ida e volta para iniciar uma única sessão segura. Essas viagens adicionais de ida e volta podem aumentar a latência. De forma semelhante, como um WAF inspeciona cada solicitação em linha, ele introduz mais atrasos.

[1] IDC, DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified, Stephen Elliot, março de 2015

[2] Ponemon Institute, 2017 Cost of Data Breach Study, junho de 2017

A Cloudflare acaba com a necessidade de sacrificar o desempenho em prol da segurança. Em vez de diminuir o desempenho, os recursos de segurança da Cloudflare podem aumentar o desempenho do aplicativo devido aos serviços de segurança de baixa latência integrados à aceleração do tráfego. O suporte para TLS 1.3 e a continuidade da sessão global podem reduzir o número de viagens de ida e volta, e o HTTP/2, que permite downloads multiplexados, acelera o tempo de carregamento das páginas. Como os serviços de segurança da Cloudflare são integrados aos serviços de aceleração de tráfego, como cache e roteamento inteligente, os aplicativos podem experimentar um desempenho superior em comparação com a execução insegura sem a Cloudflare.

O cache aproxima o conteúdo estático dos visitantes do site. Isso não apenas reduz a carga nos servidores de origem, mas também acelera a resposta do aplicativo. O roteamento inteligente determina o caminho mais rápido da Cloudflare até a origem, acelerando o conteúdo dinâmico e estático.

Escala

Criado desde o início com a resiliência em mente

Facilidade de uso

Interface do usuários e API intuitivas para configuração e administração ágil

Velocidade

Segurança de alto desempenho integrada à aceleração de tráfego

A facilidade de uso aprimora a postura de segurança

Facilitar o uso de uma solução de segurança para usuários e administradores não se resume apenas a uma interface bonita; isso também contribui com o aprimoramento da postura de segurança de uma empresa. Uma pesquisa da Gartner sugere que, até 2020, 99% das violações de firewall serão causadas por simples configurações incorretas de firewall, e não por falhas.[3]

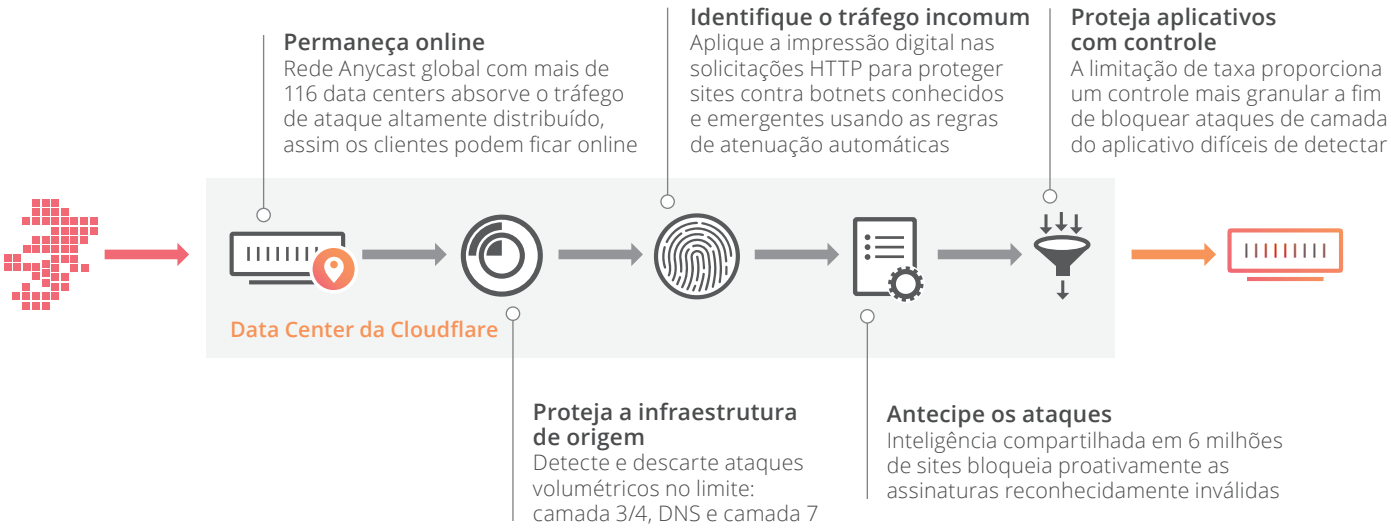
Uma boa experiência do usuário (UX) reduz os riscos à segurança causados por configurações incorretas e melhora a agilidade em um cenário de ameaças em constante evolução. A configuração da Cloudflare pode demorar menos de 5 minutos. Essa facilidade de uso permite que as empresas escalem o gerenciamento de políticas de segurança para mais funcionários sem experiência com segurança, reduzam o tempo de alteração e implantação de novas políticas e melhorem os ajustes pontuais na postura de segurança de aplicativos complexos.

A Cloudflare aplica essas vantagens para proteger os clientes contra três desafios principais: Ataques de DDoS que podem prejudicar o desempenho e a disponibilidade de seus aplicativos, comprometimento dos dados do cliente por ataques multivetor e bots mal-intencionados que abusam de seus sites.

Proteja seus aplicativos contra DDoS

Um ataque de DDoS envia grandes volumes de tráfego em uma tentativa de derrubar um site ou serviço. Ao sobrecarregar os servidores de origem, esse tráfego mal-intencionado torna o aplicativo-alvo lento ou não disponível para usuários finais. A Cloudflare permite uma defesa em várias camadas.

[3] Gartner, Inc., One Brand of Firewall Is a Best Practice for Most Enterprises, Adam Hils e Rajpreet Kaur, 5 de junho de 2017



Rede Anycast global

A rede Anycast de mais de 116 data centers aumenta a área de superfície na qual a Cloudflare pode dispersar ataques de DDoS. Com a Anycast, várias máquinas compartilham o mesmo endereço IP. Quando uma solicitação é enviada a um endereço IP de Anycast, os roteadores a direcionam para a máquina mais próxima na rede. Isso reduz os ataques altamente distribuídos de botnets, já que uma parte do tráfego de DDoS é absorvida por cada um dos nossos data centers, em vez de ficar concentrada em um único ponto.

Atenuações inteligentes e automatizadas no limite

Como a Cloudflare tem visibilidade em seus 6 milhões de sites, o serviço de proteção contra DDoS pode desenvolver heurística com base em ataques em um site para proteger muitos outros.

Atenuações automatizadas por fluxos de rede de impressão digital e tráfego de ataque HTTP identificam e interrompem proativamente o tráfego de ataque antes de prejudicar o site dos clientes.

Ao descartar esses ataques de alto volume no limite da rede, os servidores de origem do cliente permanecem protegidos e online.

Pilha integrada de DNS, rede e proteções de Camada 7

Como cada servidor de borda tem uma pilha integrada de serviços de segurança, como DNS, firewall, limitação de taxa e WAF, a Cloudflare pode fornecer uma proteção distribuída, mas também uma defesa em camadas contra tipos diferentes de ataques de DDoS, particularmente DNS, rede e DDoS em camada de aplicativo.

O serviço de DNS distribuído da Cloudflare pode aguentar ataques direcionados contra servidores de nome de domínio. Ataques de rede, como Camada 3 e 4, não são apenas bloqueados automaticamente, mas podem ser configurados por clientes a fim de bloquear as fontes inválidas por IP, país de origem ou ASN por meio de um Firewall de IP. As configurações de segurança podem aproveitar a visibilidade da Cloudflare sobre a reputação de qualquer endereço IP em seus 6 milhões de sites, a fim de bloquear proativamente o tráfego inválido identificado.

> Adoramos a paz de espírito de sabermos que podemos configurar o Cloudflare e confiar que não seremos afetados por qualquer tipo de ataque de DDoS mal-intencionado.

BUYCRAFT | LEE MCNEIL, CTO

Atenuações configuráveis com base em taxas

Embora as soluções de DDoS da Cloudflare protejam automaticamente os clientes contra ataques volumétricos de rede e de aplicativo, alguns clientes precisam de controles configuráveis para se proteger contra tráfegos de volumes inferiores, mas ainda assim mal-intencionados.

A capacidade de personalizar os limites de taxa de solicitação, o URI de destino e os atributos da solicitação, como o método e o código da resposta, proporciona aos clientes a flexibilidade de ajuste da defesa com base no perfil do aplicativo e do tráfego.

Reduza os riscos de comprometimento dos dados por meio da defesa em camadas

Normalmente, os invasores usam vários vetores de ataque ao tentar comprometer os dados do cliente. Para se protegerem, as empresas precisam de uma defesa em camadas.

ATAQUES	SOLUÇÕES CLOUDFLARE
1. Injeção de cargas mal-intencionadas por meio de formulários e APIs	**Bloqueie os principais ataques OWASP e ataques emergentes no nível do aplicativo por meio do WAF**
2. Consulta de dados confidenciais não criptografados inseridos pelos clientes	**Criptografia por meio de SSL/TLS bloqueia a espionagem**
3. Entrada por força bruta em páginas de login	**Proteção de login por meio da limitação de taxa**
4. Os invasores tentam forjar as respostas de DNS a fim de interceptar as credenciais do cliente	**DNS e DNSSEC resilientes impedem respostas forjadas**

Reduza a falsificação por meio de DNS seguro

O envenenamento de cache ou "falsificação" engana os visitantes desavisados do site fazendo-os inserir dados confidenciais, como números de cartão de crédito, em um site atacado. Esse tipo de ataque ocorre quando um invasor envenena o cache de um servidor de nome DNS com registros incorretos. Até que a entrada do cache expire, esse servidor de nomes retornará os registros de DNS falsos. Em vez de serem direcionados ao site correto, os visitantes são encaminhados ao site de um invasor, permitindo que o vilão roube dados confidenciais.

O DNSSEC verifica os registros DNS usando assinaturas criptográficas. Ao verificar a assinatura associada a um registro, os solucionadores de DNS podem verificar se as informações solicitadas são provenientes de seu servidor de nome autoritativo, e não de um invasor man-in-the-middle.

Reduza a falsificação por meio da criptografia

Os invasores podem interceptar ou "bisbilhotar" as sessões do cliente a fim de roubar dados confidenciais do cliente, incluindo credenciais como senhas ou números de cartão de crédito. No caso de um ataque "man-in-the-middle", o navegador pensa que está falando com servidor em um canal criptografado, e o servidor pensa que está falando com o navegador, mas ambos estão falando com o invasor, que está bem no meio dos dois. Todo tráfego passa por esse man-in-the-middle, que consegue ler e modificar quaisquer dados.

Criptografia/encerramento rápido, facilidade no gerenciamento do certificado e suporte dos padrões de segurança mais recentes permitem que os clientes protejam a transmissão dos dados do usuário.

Bloqueie cargas mal-intencionadas por meio de WAF escalonável e atualizado automaticamente

Os invasores exploram vulnerabilidades do aplicativo enviando cargas mal-intencionadas que podem extrair dados confidenciais do banco de dados, do navegador do usuário ou por meio da injeção de malware, que pode comprometer os sistemas visados.

Um WAF (Firewall de Aplicativo Web) examina o tráfego da Web em busca de tráfego suspeito e depois filtra automaticamente as solicitações ilegítimas com base em conjuntos de regras aplicadas mediante sua solicitação. Ele analisa solicitações HTTP baseadas em GET e POST e aplica um conjunto de regras, como o conjunto de regras básicas ModSecurity, cobrindo as 10 principais vulnerabilidades OWASP a fim de determinar qual tráfego bloquear, desafiar ou deixar passar. Ele pode bloquear spam de comentários, ataques de script entre sites e injeções de SQL.

O WAF da Cloudflare atualiza as regras com base em ameaças identificadas de 6 milhões de clientes e pode proteger os clientes sem prejudicar o desempenho do aplicativo graças à sua inspeção de baixa latência e integração com a aceleração de tráfego.

Redução das tomadas de controle de contas por meio da proteção de login

Os invasores podem desferir "ataques de dicionário" automatizando os logins com credenciais despejadas a fim de acessar uma página protegida com login usando "força bruta". A Cloudflare permite que os usuários personalizem as regras de limitação de taxa a fim de identificar e bloquear esses ataques difíceis de detectar no limite.

Proteja por meio do monitoramento e pontuação

Ao monitorar um site em busca de vulnerabilidades, pontuar a maturidade da segurança de uma empresa e integrar em seu processo de implantação, os aplicativos de terceiros da Cloudflare fornecem uma camada adicional de proteção proativa.

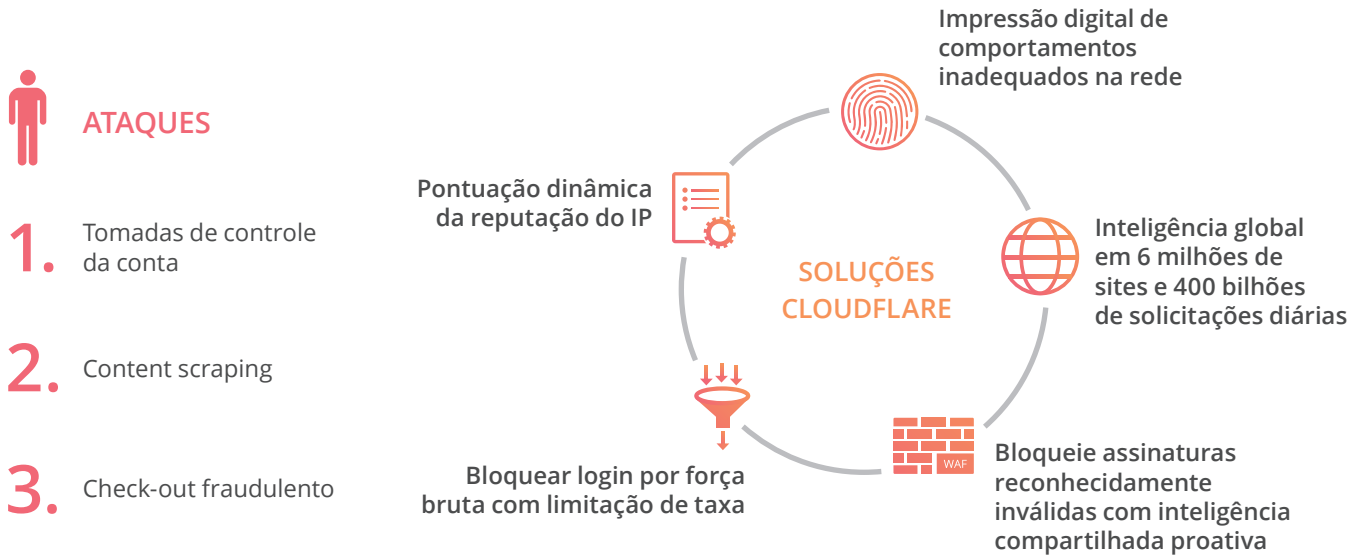
> Os recursos de segurança da Cloudflare tiraram dos ombros de nossos desenvolvedores a preocupação em manter o site online e permitiram que se concentrassem em outros aprimoramentos de site.

Gazeta Esportiva | DAVID VERZOLLA
Chefe de tecnologia

Impeça bots abusivos

Três formas de bots abusivos estão crescendo em frequência, sofisticação e impacto no cliente. Como resultado, uma solução de prevenção contra bot precisa de elementos diferentes para resolver os possíveis perfis de ataque diferentes.

Os ataques mais comuns são tomadas de controle da conta, recorte de conteúdo e check-out fraudulento. Todos os três podem usar "estilos" de bot diferentes, cada um deles pode ser detectado e atenuado com abordagens diferentes.



Detecção e atenuação com base na taxa

Como alguns bots são automatizados e precisam acessar o site com uma taxa alta a fim de alcançar seus objetivos, a automação com base em taxa pode detectar e atenuar esses ataques. Por exemplo, logins de força bruta têm uma taxa superior de logins com falha de um único endereço IP em comparação com um usuário normal. Limites com base em taxa podem detectar esses tipos de tentativa de tomada de controle de conta. De forma parecida, os recortadores de conteúdo que acessam páginas que não podem ser mais encontradas (erros 404) os gerarão a uma taxa superior em comparação com um usuário normal.

Bloqueio com base em assinaturas reconhecidamente inválidas

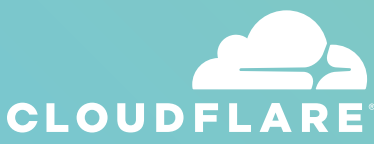
Com 6 milhões de sites protegidos na Cloudflare, as assinaturas reconhecidamente inválidas de bots abusivos podem ser detectadas em um site e, depois, bloqueadas em todos os outros.

Conclusão

Para permanecerem seguras e "sempre ligadas" em um cenário de ameaças em constante evolução, as empresas precisam de desempenho, segurança inteligente em escala e defesas em camadas a fim de se proteger contra ataques de negação de serviço, roubo de dados e bots mal-intencionados.

Como os humanos sempre farão parte da equação, políticas de segurança fáceis de usar, implantar, configurar e ajustar afetarão a postura de segurança geral, reduzindo a digitação acidental e permitindo que mais funcionários reajam às alterações sem riscos ou atritos desnecessários.

A segurança de nuvem da Cloudflare defende contra a crescente sofisticação de ataques de DDoS, tentativas de comprometimento de dados por vilões e bots mal-intencionados.



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com