CLOUDFLARE®

クラウド内のアプリケーションの保護

DDoS、データ漏えい、悪意のあるボットに対する、簡単にデプロイでき、高速かつスケーラブルな多層防御

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

クラウド内のアプリケーションの保護

DDoS、データ漏えい、悪意のあるボットに対する、簡単にデプロイでき、高速かつスケーラブルな多層防御
企業では、セキュリティに対する取り組みを強化するようにという圧力が日々高まっています。以下の3つの要因が、この圧力に拍車をかけています。

- 攻撃者が、より強力で高度になり、意欲も増している
- アプリケーションの公開API、SaaSの採用、サードパーティアプリケーションとの統合が増えており、攻撃を受ける範囲が拡大している
- データ、プライバシー、セキュリティに対する一般機関または政府機関による調査が増えている

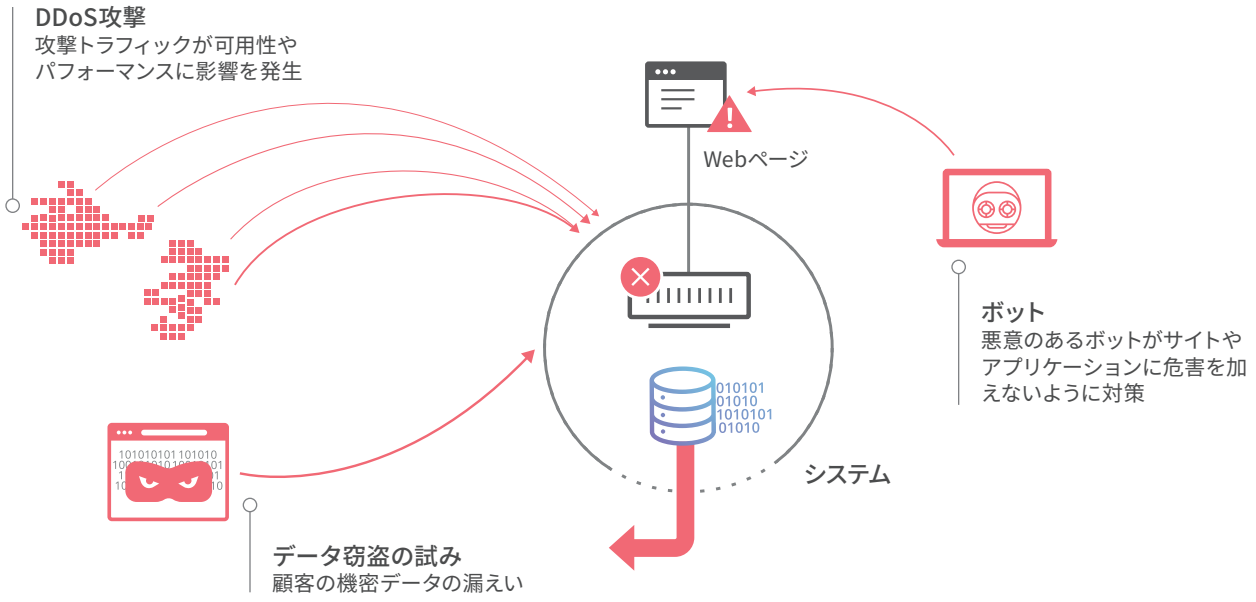
攻撃者は、分散型サービス拒否（DDoS）攻撃の頻度や容量を増加させています。ボットネットとモノのインターネット（IoT）の無数のデバイスをオンラインで活用することで、高度に分散しており影響が大きな帯域幅消費型攻撃を簡単に実行できるようになっています。

また、送信するデータの容量を増やすことに加え、標的をネットワークレイヤーからアプリケーションレイヤーに変えています。アプリケーションレイヤー（「第7層」）への攻撃は検出が難しく、通常、より少ないリソースで、Webサイトやアプリケーションに障害を発生させて運用を中断させることができます。

攻撃者は、サイトに障害を発生させたり機密データを盗んだりした後、サイトを再開するための身代金を要求するなどして、収益を得ることができます。標的の企業から身代金を受け取ることに成功すると、さらに意欲を増して、組織化することになり、被害が拡大します。

攻撃に遭うリスクの増加に伴い、企業は以下の3つの主要な問題およびリスクに対する防御を強化する必要があります。

- アプリケーション、Webサイト、APIに対するDDoS攻撃。可用性やパフォーマンスを低下させ、収益の減少、運用コストの高騰、ブランドイメージの低下を招きます。
- 顧客およびビジネス上の機密データの漏えい（個人を特定できる情報（PII）や知的財産など）。顧客とその信頼を失うことになります。
- 悪意のあるボット。コンテンツスクレイピング、アカウントの乗っ取り、決済詐欺によって顧客のアプリケーションに危害を加えます。



DDoS、データ漏えい、悪意のあるボットで必要になるコストは企業の規模や業種によってさまざまですが、ビジネスへの影響の深刻度はあらゆるビジネスで高まっています。

2015年のIDCレポートによると、インフラストラクチャーのダウンタイムによる平均コストは1時間あたり10万ドルです。[1]

データ漏えいでは、ユーザー情報が漏えいしたり、顧客の機密データ（アプリケーションのデータストアに保存されているクレジットカード番号やパスワードなど）が抜き取られたりする可能性があります。データ漏えいで喪失したり盗難に遭ったりしたレコード1件あたりの平均総コストは2017年で141ドル、データ漏えいの平均合計コストは362万ドルでした。[2]政府とメディアによる調査が強化された結果、企業は、最小限のデータ漏えいの場合でも、財務的ペナルティだけでなく、社会的信頼の喪失による大きな影響を受けるようになりました。

悪意のあるボットは、ユーザーのアカウントを乗っ取ることができるだけではなく、決済詐欺とコンテンツスクレイピングを実行することもできます。供給量が限られた商品を繰り返し自動的に購入するボットによる決済詐欺は、店舗のブランドを傷つけ、見込み顧客の購買意欲を失わせることにより、将来の売上を低下させ、供給者との関係までも悪化させる可能性があります。コンテンツスクレイピングは、特に広告主導のビジネスで、SEOランキングの低下、1000インプレッション当たりのコスト（CPM）の低下、広告主の喪失により、収益を直接減少させる可能性があります。

Cloudflareの長所

攻撃に遭うリスクとビジネスへの影響の両方の増加に対応するには、企業は個別の戦術的な問題に対処する必要があるだけではなく、脅威が絶え間なく進化する状況で攻撃者に対する長所を見つける必要があります。

Cloudflareが他社と異なる3つの重要な特長は、**規模、パフォーマンス、使いやすさです。**

規模の活用

Cloudflareの長所の1つは、データ分析におけるネットワークの規模とトラフィックの多様性です。Cloudflareは、600万社を超える顧客のWebサイトを保護することで、新たに出現したグローバルな脅威についての洞察を得ています。その結果、CloudflareのDDoS保護とWebアプリケーションファイアウォールが、ダウンタイムと収益の損失を引き起こす攻撃から顧客を事前に保護します。

Cloudflareのネットワークは規模を考慮して設計されているため、速度と回復力に優れています。1日あたり3000億件のリクエストに対して必要なすべてのサービスを提供するために、DNS、暗号化、WAFなど、すべてのデータセンターの各サーバーで実行されているサービスが、莫大なトラフィックの負荷を短い待機時間と高い信頼性で処理することができます。

DDoS攻撃の規模が大きくなると、ネットワークの規模と回復力が効果を発揮します。116か所以上のデータセンターで構成されるCloudflareの規模にエニーキャストネットワークを組み合わせることで、Cloudflareは最大級の分散型攻撃にも耐えることができます。

パフォーマンスとアプリケーションの保護の両立

顧客はこれまで、セキュリティのためにパフォーマンスを犠牲にする必要がありました。TLSとWAFのソリューションは、多くの場合、サイトのパフォーマンスを低下させます。たとえば、TLS（暗号化接続プロトコル）は、セキュアなセッションを1つ開始するためだけに、最大4回のラウンドトリップを実行します。このようなラウンドトリップの増加が待機時間を長くする可能性があります。同様に、WAFは各リクエストをインラインで検査するため、遅延時間が長くなります。

[1] IDC、『DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified』、Stephen Elliot、2015年3月
[2] Ponemon Institute、『2017 Cost of Data Breach Study』、2017年6月

Cloudflareを使用すると、セキュリティのためにパフォーマンスを犠牲にする必要がなくなります。Cloudflareのセキュリティ機能は、トラフィック高速化と統合された待機時間の短いセキュリティサービスであるため、パフォーマンスを低下させるのではなく、アプリケーションパフォーマンスを向上させることができます。TLS 1.3のサポートとグローバルなセッション再開により、ラウンドトリップの回数を減らすことができ、HTTP/2で多重ダウンロードを実行できるため、ページの読み込み時間が短くなります。Cloudflareのセキュリティサービスは、キャッシュやスマートルーティングといったトラフィック高速化サービスと統合されているため、Cloudflareで保護していない状態で実行した場合と比較して、アプリケーションの実行速度が向上します。

キャッシュにより、Webサイトの静的コンテンツを訪問者の近くに配置できます。これにより、配信元サーバーの負荷が削減されるだけでなく、アプリケーションの応答が速くなります。スマートルーティングは、Cloudflareから配信元への最速のパスを決定し、動的コンテンツと静的コンテンツの両方を高速化します。

規模

ゼロからの回復力のために確立

使いやすさ

俊敏性に優れた構成と管理を実現する直観的なUIとAPI

速度

トラフィックの高速化機能と統合された高いパフォーマンスセキュリティ

使いやすさによるセキュリティの取り組みの強化

ユーザーと管理者にとってセキュリティソリューションが使いやすいということは、インタフェースが優れているだけでなく、企業のセキュリティに対する取り組みの強化に貢献していることにもなります。Gartnerの調査は、2020年に発生したファイアウォール侵害の原因の99%が、欠陥ではなくファイアウォールの単純な構成ミスであると指摘しています。[3]

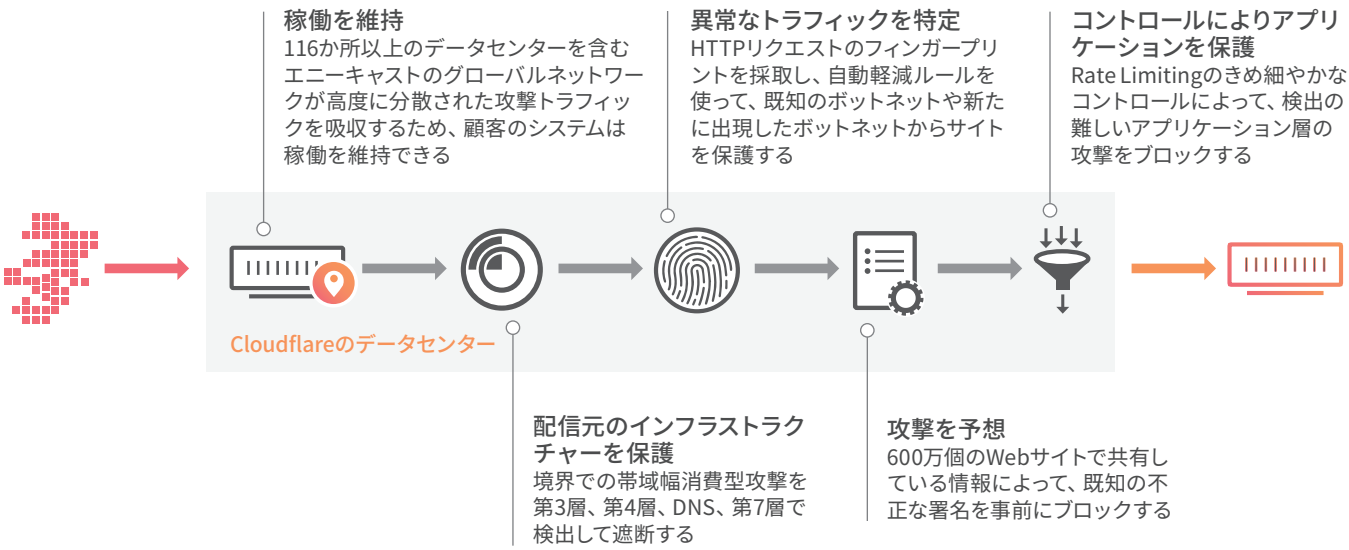
優れたユーザーエクスペリエンス（UX）は、構成ミスによるセキュリティリスクを削減し、脅威が絶え間なく変化する状況での俊敏性を強化します。Cloudflareの設定にかかる時間は5分未満です。この使いやすさのおかげで、企業は、セキュリティの専門家でない従業員の増加に合わせたセキュリティポリシー管理の拡大、新しいポリシーを変更およびデプロイする時間の削減、複雑なアプリケーションでのセキュリティに対する取り組みのタイムリーな調整を実現できます。

Cloudflareでは、このようなメリットを活用して、アプリケーションのパフォーマンスと可用性を低下させる可能性のあるDDoS攻撃、マルチベクトル型攻撃による顧客データの漏えい、Webサイトに危害を加える悪意のあるボットといった、3つの主要な課題から顧客を保護しています。

顧客のアプリケーションのDDoSからの保護

DDoS攻撃は、1回の攻撃で大量のトラフィックを送信して、サイトまたはサービスに障害を発生させます。悪意のあるこのトラフィックでは、配信元のサーバーを過負荷にすることで、標的のアプリケーションの速度を低下させたりエンドユーザーが利用できないようにしたりします。Cloudflareではマルチレイヤー防御を利用できます。

[3]Gartner, Inc.、『One Brand of Firewall Is a Best Practice for Most Enterprises』、Adam HilsおよびRajpreet Kaur、2017年6月5日



グローバルなエニーキャストネットワーク

エニーキャストネットワークには116か所以上のデータセンターがあるため、CloudflareがDDoS攻撃を撃退できる範囲が増加します。エニーキャストを使うと、複数のマシンが同じIPアドレスを共有することになります。エニーキャストのIPアドレスにリクエストを送信すると、ルーターがそのリクエストをネットワーク上の最も近くにあるマシンに振り向けます。これによって、DDoSトラフィックの一部が1つの地点に集中するのではなく各データセンターで吸収されるため、ボットネットによる高度な分散型攻撃が軽減されます。

ネットワークの境界での高度な自動軽減策

Cloudflareは600万個のサイト全体の状況を監視しているため、DDoS保護サービスでは、1つのサイトでの攻撃に基づいて経験則を打ち立てて、他の多くのサイトを保護できます。

自動軽減策では、ネットワークの流れとHTTP攻撃トラフィックのフィンガープリントを採取することにより、顧客のサイトに障害が発生する前に攻撃トラフィックを特定して停止します。

ネットワークの境界でこのような大量の攻撃を遮断することで、顧客の配信元のサーバーは保護され、稼働し続けます。

DNS、ネットワーク、第7層の保護の統合

Cloudflareの各エッジサーバーにはDNS、ファイアウォール、Rate Limiting、WAFといったセキュリティサービスの統合スタックがあるため、さまざまな種類のDDoS攻撃、特にDNS、ネットワーク、アプリケーションレイヤーへのDDoSに対して、分散型の保護だけでなく、多層防御を実装できます。

Cloudflareの分散型DNSサービスでは、ドメインネームサーバーを狙った攻撃に対応できます。第3層や第4層への攻撃といったネットワーク攻撃は自動的にブロックされます。また、顧客がIPファイアウォールを使って、IP、配信元の国、ASNに基づいて不正な配信元をブロックするように構成することもできます。セキュリティの設定では、600万個のWebサイト内のあらゆるIPアドレスの評価を確認できるというCloudflareの特長を活用して、不正であることが特定されているトラフィックを事前にブロックできます。

> Cloudflareを設定した後は、設定したことも忘れ、どのような種類の悪意のあるDDoS攻撃の影響も受けないと信じて、安心していられます。

BUYCRAFT | LEE MCNEIL氏
CTO

構成可能な確率ベースの軽減策
CloudflareのDDoSソリューションはネットワークやアプリケーションに対する帯域幅消費型攻撃から顧客を自動的に保護しますが、顧客によっては、容量が少ないものの悪意のあるトラフィックから自社のシステムを保護するためにコントロールを構成する必要があります。

顧客は、リクエスト率のしきい値、対象のURIとリクエストの属性（手法や応答コードなど）をカスタマイズする機能により、アプリケーションやトラフィックのプロファイルに基づいて柔軟に防御を調整できます。

多層防御によるデータ漏えいのリスクの削減

攻撃者は、顧客のデータを侵害するときに、たいてい複数の攻撃ベクトルを使用します。企業は、自社のシステムを保護するために、多層防御を実装する必要があります。

攻撃		Cloudflareのソリューション
1. フォームやAPIを使って悪意のあるペイロードを挿入する	→	OWASPの上位と新たに出現したアプリケーションレベルの攻撃をWAFでブロックする
2. 顧客が入力した暗号化されていない機密データをのぞき見る	→	SSLやTLSを使った暗号化がスヌーピングをブロックする
3. ログインページに力ずくで入る	→	Rate Limitingを使ってログインを保護する
4. 攻撃者はDNSの応答をねつ造して顧客の資格情報を横取りしようとする	→	回復力のあるDNSとDNSSECが応答のねつ造を予防する

セキュアなDNSを使ったスプーフィングの削減

「スプーフィング」はキャッシュの侵害のことで、疑いを持っていないサイト訪問者を騙して、クレジットカード番号などの機密データを攻撃対象のサイトに入力させます。この種類の攻撃が発生するのは、攻撃者がDNSネームサーバーのキャッシュを不正なレコードで侵害した場合です。キャッシュエントリーの期限が切れるまで、そのネームサーバーは偽のDNSレコードを返します。訪問者は正しいサイトではなく攻撃者のサイトに転送されるため、攻撃者が機密データを窃盗できるようになります。

DNSSECは、暗号による署名を使用して、DNSレコードを検証します。レコードに関連付けられた署名をチェックすることで、DNSリゾルバーは、リクエストされた情報が信頼できるネームサーバーから送信されたものであって、中間者攻撃によるものではないことを確認できます。

暗号化によるスプーフィングの削減

攻撃者は、パスワードやクレジットカード番号といった資格情報が含まれる顧客の機密データを窃盗するために、顧客のセッションに割り込んだり、顧客のセッションを「のぞき見」たりします。「中間者」攻撃の場合、ブラウザーからは暗号化されたチャネルでサーバーに対して通信していると認識しており、サーバーからはブラウザーに対して通信していると認識していますが、どちらも中間に存在する攻撃者に対して通信しています。すべてのトラフィックがこの中間者を経由しており、中間者は任意のデータを読み取って変更することができます。

高速暗号化／終了処理、簡単な証明書管理、最新のセキュリティ標準のサポートにより、顧客はユーザーデータの転送を保護できます。

自動更新されるスケーラブルなWAFを使った、悪意のあるペイロードのブロック

攻撃者は、データベースやユーザーのブラウザーから機密データを抽出できる悪意のあるペイロードを送信することや、標的のシステムを侵害できるマルウェアを挿入することにより、アプリケーションの脆弱性を悪用します。

Webアプリケーションファイアウォール（WAF）は、Webトラフィックを調査して、疑わしいトラフィックを探します。次に、適用する必要のあるルールセットに基づいて、不正なリクエストを自動的に除外します。GETベースとPOSTベースの両方のHTTPリクエストを確認し、OWASPの上位10位の脆弱性が含まれるModSecurityのCore Rule Setといったルールセットを適用して、ブロック、調査、許可を行うトラフィックを判断します。これによって、コメントスパム、クロスサイトスクリプティング攻撃、SQLインジェクションをブロックできます。

CloudflareのWAFは、600万社の顧客から特定した脅威に基づいてルールを更新し、短時間での検査とトラフィック高速化の統合により、アプリケーションのパフォーマンスを損なうことなく顧客を保護することができます。

ログイン保護によるアカウントの乗っ取りの減少

攻撃者は、ダンプされた資格情報でログインを自動化して、ログイン保護されたページに「力ずく」で入ることで、「ディクショナリー攻撃」を実行できます。Cloudflareにより、ユーザーはRate Limitingルールをカスタマイズし、このような検出が難しい攻撃を境界で特定してブロックすることができます。

監視と採点による保護

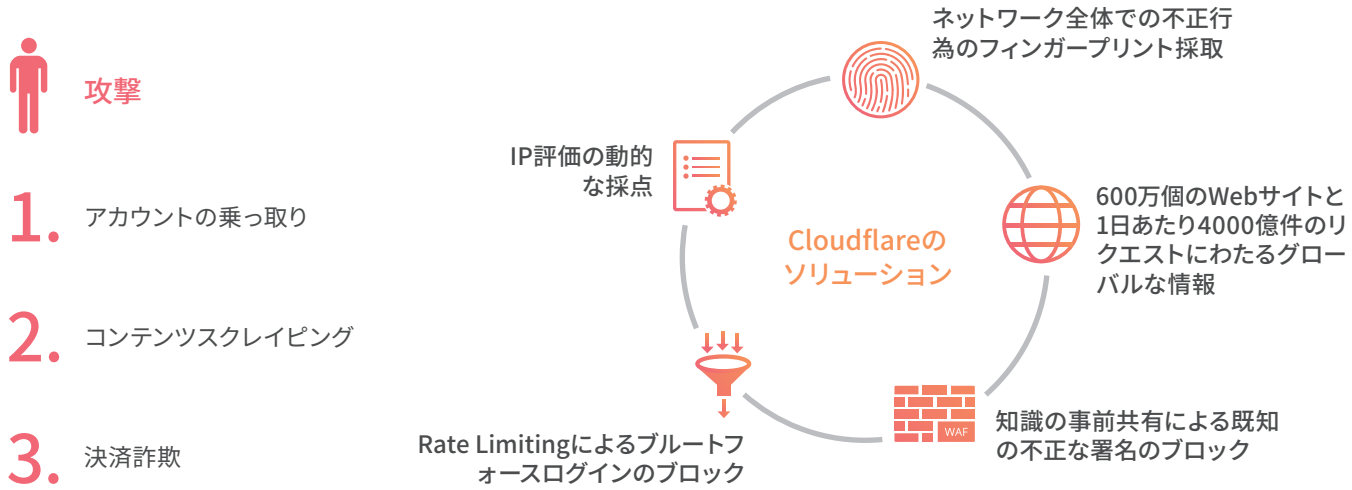
Cloudflareのサードパーティアプリを使うと、Webサイトを監視して脆弱性を探し、企業のセキュリティの成熟度を採点し、開発プロセスに統合することで、事前の保護を強化できます。

> Cloudflareのセキュリティ機能により、開発者は、サイトを常に稼働させておくことについて心配しなくてもよくなり、サイトに関するその他の改善に注意を集中できるようになります。
>
> Gazeta Esportiva | DAVID VERZOLLA氏
> テクノロジー部門責任者

迷惑ボットへの対策

高度で顧客への影響が大きい3つの形式の迷惑ボットが、頻繁に使用されるようになってきています。その結果、ボット対策ソリューションでは、使用される可能性のある攻撃プロファイルに対処するために、異なる要素が必要になります。

特によくある攻撃が、アカウントの乗っ取り、コンテンツスクレイピング、決済詐欺です。この3つにはすべて異なるボット「形式」が使用されており、それぞれ別の方法で検出して軽減する必要があります。



確率ベースの検出と軽減

一部のボットは自動化され、目標を達成するために高い確率でサイトにヒットする必要があります。確率ベースの自動化を使用すると、このような攻撃を検出して軽減することができます。たとえば、ブルートフォースログインでは、単一のIPアドレスからのログインの失敗率が通常のユーザーよりも高くなります。確率ベースのしきい値では、このような種類のアカウント乗っ取り攻撃を検出できます。同様に、コンテンツスクレイパーは、見つけられなくなったページ（404エラー）のエラーを通常のユーザーよりも高い確率で生成します。

既知の不正な署名に基づくブロック

Cloudflareでは600万個のWebサイトを保護しているため、迷惑ボットの既知の不正な署名を1つのサイトで検出してから、他のすべてのサイトでブロックすることができます。

まとめ

脅威が常に進化する状況において、企業が自社のシステムをセキュアで「稼働中」の状態に維持するには、パフォーマンス、大規模で高度なセキュリティ、多層防御を実装して、サービス拒否、データの窃盗、悪意のあるボットから保護する必要があります。

システムにはそれを使う人が常に関係するため、セキュリティポリシーのデプロイ、構成、調整を実行しやすいと、「ケアレスミス」を削減し、より多くの従業員がリスクや不要なプレッシャーを受けずに変化に反応できるようになり、セキュリティに対する取り組み全体に良い影響を及ぼします。

攻撃者と悪意のあるボットによるデータ漏えいを目的としたDDoS攻撃が高度になっていく中で、Cloudflareのクラウドセキュリティは顧客のシステムを安全に保護しています。

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