

Magic Transit

Cloudflare Magic Transitは、ネットワークインフラストラクチャ、データセンター、パブリッククラウドサービスをDDoS攻撃から保護します

オンプレミス型、クラウド型、ハイブリッド型のネットワークのための分散サービス妨害（DDoS）攻撃対策

迅速で信頼性の高いDDoS攻撃対策

もはや問題は「DDoS攻撃の標的になるかどうか」ではなく、「いつ標的になるか」です。ネットワークインフラストラクチャをDDoS攻撃から保護するには、脅威インテリジェンス、速度、容量を兼ね備える必要があります。帯域幅消費型攻撃は、レガシーソリューションを簡単に圧倒します。他のクラウド型DDoS軽減ソリューションのほとんどは、スクラビングセンターを介してトラフィックをバックホールするため、大幅な遅延増大が起こり、パフォーマンスが低下します。

- ほぼ瞬時の軽減
- DDoS軽減機能を全データセンターで提供
- 数分でできる簡単オンボーディング
- 一元管理



図1：すべてのCloudflareデータセンターでDDoS攻撃対策

業界トップクラスのDDoS攻撃対策

Magic Transitは、Gartner® Peer Insights™「Voice of the Customer」のDDoS軽減ソリューション部門でカスタマーズチョイスに選ばれました。

利点



最新アーキテクチャ

449Tbpsの比類ないネットワーク容量、330の拠点を持つ当社はスクラビングセンターへバックホールしないため、多くのお客様からCloudflare移行後パフォーマンスが向上したと伺っています。



包括的な保護

Cloudflareは、1日あたり平均2340億件のサイバー脅威をブロックしています。脅威インテリジェンスの共有により、複雑で巧妙な新型攻撃に対する防御を強化します。Magic Transitは、たいていの攻撃を3秒以内に軽減する自動保護を提供します。



使いやすさ

独自IPアドレス持ち込み(BYOIP)またはCloudflareのリースIPで、数分でオンボード可能です。「常時オン」の保護を設定したら後はおまかせです。分析、アラート、ログに関する設定はすべて単一のコンソールまたはAPIで行えます。