fastly

プロダクトデータシート

GraphQL インスペクション

GraphQL API に対する優れた可視性と保護

API 開発の進化は、動的アプリケーションの爆発的な増加に大きく貢献しています。組織はリリースサイクルを加速させるより効率的な方法を追求しており、この高速化により、リリースのプロセス (ウォーターフォール型からアジャイル開発への移行など) からアーキテクチャレベルまで、CI/CDのパイプラインが変化しています。

これまで API の作成において REST と SOAP が主に使用されてきましたが、効率が良く、高速で特殊性が高い GraphQL を好んで使用する開発者が急速に増えています。

Fastly 次世代 WAF (Powered by Signal Sciences) は、あらゆる場所でアプリケーションやAPI、マイクロサービスを保護する最先端の統合型セキュリティソリューションです。GraphQLインスペクションの追加により、Fastly 次世代 WAF は使用されているアーキテクチャや仕様にかかわらず API を完全に保護できるようになりました。

API 保護の新たな基準を確立

GraphQL は、無関係なデータを含まず必要な情報だけを呼び出せるという点で REST よりも優れています。また、バックエンドに複数のリクエストを送信する代わりに単一のコールでこれを実行できるため、サーバーへの全体的な負荷を軽減できます。

オープンソースのクエリ言語 GraphQL の採用が広がっているという事実は、開発者が REST ベースの API から、より高速で効率の高い仕様に移行していることを示しています。これにより、開発者とエンドユーザーのエクスペリエンスが改善されますが、その一方で GraphQL は OWASP トップ10の攻撃や GraphQL 特有の脆弱性を悪用する攻撃にさらされています。

Fastly 次世代 WAF は、OWASP トップ10のインジェクション攻撃や DoS 攻撃に加え、その他の脆弱性を悪用した GraphQL API への攻撃をブロックします。GrapQL インスペクションにより、開発チームはアプリケーションのセキュリティリスクを増やすことなく安心して新しいテクノロジーを取り入れることができます。90%のお客様がフルブロックモードで使用している Fastly 次世代 WAF は包括的な API 保護ソリューションを提供し、アプリケーションに不具合を起こしたり、正当なリクエストをブロックすることはありません。

主なメリット

API を狙う攻撃に対する可視性と保護の強化

組織のアプリケーションフットプリントが拡大する中、Fastly 次世代 WAF は、レイヤー7のあらゆるアセットを一貫したフル機能で保護するスケーラブルで包括的なソリューションを提供します。既存の WAF ルールを GraphQL リクエストに適用して攻撃をブロックしたり、GraphQL トラフィックを特定の方法で処理するためにカスタムルールを作成することも可能です。

開発者のニーズに合った保護

開発者は、リリースサイクルをスローダウンさせることなく好きなツールを使ってアプリケーションをデプロイできる必要があります。GraphQA インスペクションにより、開発チームは既存のワークフローにフィットする言語を自由に使って作業できる柔軟性を得ながら API を安全に作成できます。

運用効率の向上

GraphQL インスペクションにより、アプリケーションをリスクにさらすことなく GraphQA がもたらす効率改善のメリットをフルに活かすことができます。

REST は過去20年、API 開発の標準として広く使用されてきましたが、より効率的にコールを実行し、アプリケーションを強化できる方法として GraphQL を採用する組織が急速に増えています。

GraphQL を悪用する攻撃をブロック

Fastly 次世代 WAF の GraphQL インスペクションでは、以下の Fastly 独自のセキュリティアプローチが活用されています。

自動化

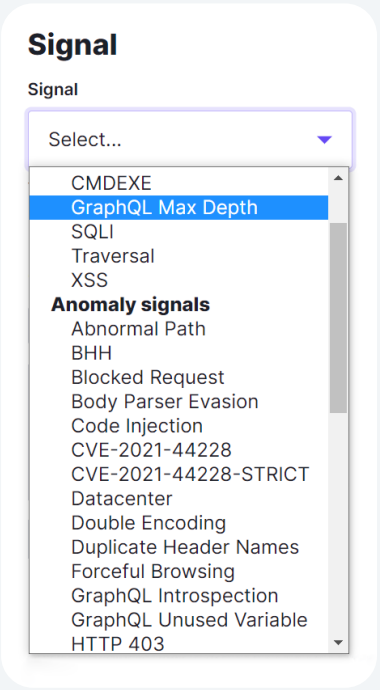
設定不要ですぐに使用できる Fastly ソリューションの一部として GraphQL インスペクションは、GraphQL リクエストを解析し、コンテキストに基づいてリクエストの内容を検査します。追加のセットアップや設定が不要で、OWASP トップ10の攻撃を検出すると自動的にブロックします。

カスタマイズ可能なシグナル

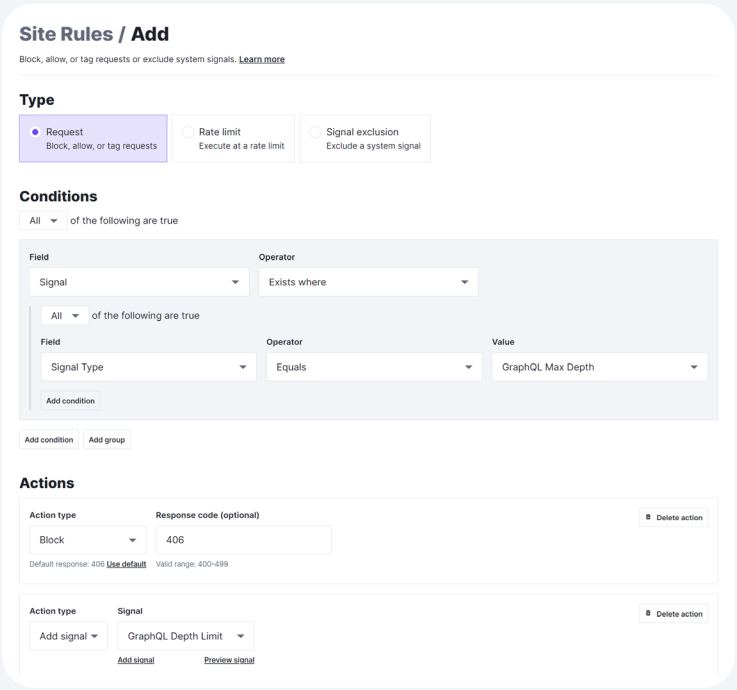
Fastly 次世代 WAF のコンソールのユーザー設定で GraphQL を悪用する攻撃特有のシグナルを選択し、保護対策をカスタマイズできます。選択したシグナルに対してルールを定義し、設定したしきい値に達した場合や特定のイベントが発生した場合にリクエストをルーティングすることができます。これらのシグナルの例については以下をご覧ください。

テンプレートルール

GraphQL IDE のリクエストに対してテンプレート化されたルールを利用できます。コンソールで GraphQL を悪用した攻撃を確認できます。



画像 1



画像 2

1 : GraphQL を悪用する攻撃特有のシグナルも含め、各シグナルについて Corp (コーポレーション) または Site (サイト) に適用するリクエストやレート制限、例外のルールを作成できます。

2 : 悪用や攻撃を避けるため、トラフィックをブロックするよう GraphQL の最大深さのシグナルに対してリクエストルールを作成する例。

シグナルとは？

シグナルはリクエストの内容を示すタブです。シグナルにより、どのタイプの攻撃ペイロードがリクエストに含まれているか、またはリクエストがブロックされたかなど、リクエストの特定の特性を視覚化できます。

一般的な GraphQL 脆弱性と異常シグナルの例

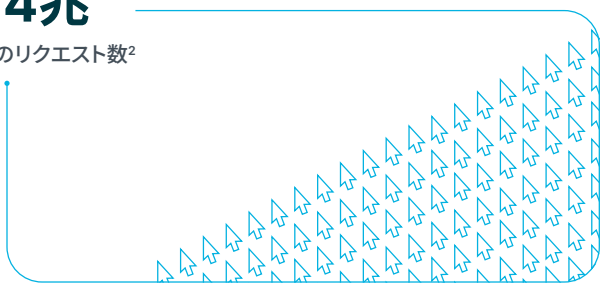
OWASP API セキュリティ脅威トップ10	インジェクション攻撃 • SQL インジェクション • コマンドインジェクション • サーバーサイド • リクエストフォージェリ	DDoS/DoS 攻撃	アクセス制御機能の不具合
GraphQL 特有	最大深さ - サーバーをダウンさせる複雑なクエリ	イントロスペクション - クエリによるパブリックデータの漏えい	未使用の変数 - リクエスト内の攻撃を示唆

90%以上

ブロックモードで Fastly 次世代
WAF を使用しているお客様の割合[1]

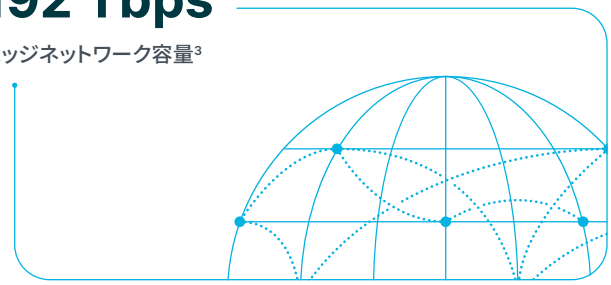
1.4兆

1日のリクエスト数[2]



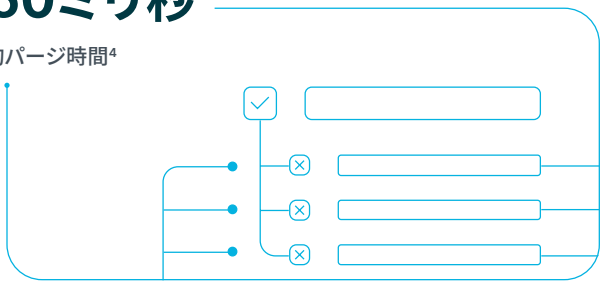
192 Tbps

エッジネットワーク容量[3]



150ミリ秒

平均パージ時間[4]



95% の CSAT[5] (顧客満足度)

ワールドクラスのサポート

Fastly は過去3年連続で95%を超える顧客満足度 (CSAT) を達成し、お客様との関係を大切にしています。Fastly が提供するワールドクラスのサポートには、Fastly エンジニアのチャットによるサポート、詳細な技術ドキュメント、ソリューションパッケージなどが含まれます。プレミアムサービスからセルフサービスまで、**お客様のニーズに合ったサポートサービスをご利用いただけます。**

Fastly サポートの詳細 ->

Fastly を試してみませんか?

戦略的なセキュリティ計画において API の保護が欠かせません。Fastly の次世代 WAF は、主な API のセキュリティカテゴリーと既存および新しい API アーキテクチャ全体に渡って API に対する幅広い種類の脅威から防御できる唯一の Web アプリケーション & API 保護プラットフォームです。

Fastly のセキュリティソリューションについて詳しくは fastly.com/jp/secure をご覧いただくか、または japan@fastly.com までお問い合わせください。

1 : 2021年3月31日現在　2 : 2022年1月31日現在　3 : 2022年1月31日現在　4 : 2020年12月31日現在　5 : 2020年6月30日現在