Signal Sciences
Now part of fastly

プロダクトブリーフ

今日のソフトウェア駆動型の世界は、DevOpsとクラウドの力によって支えられています。そのような中、拡大するインフラを横断して、新しいアプリケーションやサービスを今まで以上に早くリリースする必要性が増しています。この拡大し、変化し続けるフットプリントを保護するためには、統一したアプローチが必要です。

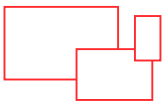
Fastly + Signal Sciences：セキュリティランドスケープの変革に向けて

Fastly はWebアプリケーションと API に対するより堅牢なセキュリティを提供するため、2020年後半、Signal Sciences を買収しました。両社が力を合わせることで、アプリケーションのデプロイの方法や場所にかかわらず、規模に応じてアプリケーションを保護できるようになりました。最先端の次世代ソリューションについて詳しくは、Fastly のセキュリティエキスパートまでお問い合わせください。

アプリケーション、API、マイクロサービスのための次世代セキュリティ

Signal Sciences は、高度な Web レイヤー攻撃から保護し、DevOps ツールと容易に連携することで、チームが必要とするセキュリティデータを随時共有できます。つまり、速度を犠牲にすることなく保護を強化し、信頼性を維持するために、エンジニアリング、セキュリティ、運用の各業務を統合することが可能なのです。

Signal Sciences は、柔軟性に優れたデプロイオプション、OWASP Top 10 を含むさまざまな攻撃からの保護と可視性、そして既存のツールとの高い連携性を備えています。さらに、どのようなインフラにも簡単にインストール可能で、ルールのチューニングも必要なく、タイムトゥバリュー (TtV) の短縮を実現できます。

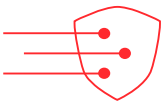


柔軟性に優れたデプロイ

オンプレミスやクラウドなど、あらゆる環境でWebサーバー、アプリケーション、PaaS、ゲートウェイにソフトウェアをインストールできます。

高度な攻撃からの保護

OWASP Top 10攻撃、悪質なボット、アカウント乗っ取り、DoS攻撃、アプリケーションの悪用や誤用など、さまざまな攻撃をブロックすることができます。



DevOps ツールとの容易な統合

運用チームやエンジニアリングチームが既に使用しているツールを通じて、アラートやデータにアクセスできます。

現在は Fastly の一部として統一されたSignal Sciences は、Gartner Peer Insights Customers' Choice の Web アプリケーションファイアウォール (WAF) 部門に3年連続で選出された唯一のベンダーであり、2021年1月31日現在、総合評価が5点満点中4.9と、市場で最も高い評価を得ている WAF ソリューションの1つです。

主なメリット

- 90 %以上のユーザーがフルブロッキングモードを使用
- 7万5,000以上のアプリのデプロイを保護
- 100以上のクラウドネイティブとデータセンタープラットフォームにデプロイ可能

可視化

セルフサービスでアクセス可能な実用的なセキュリティデータ

イベント発生の際、ネイティブツールを介してエンジニアと運用チームに通知が送られるため、迅速な対応が可能です。Fastlyのセキュリティソリューションは、頻繁に変更を行うアジャイルなチームのために設計されています。直感的なダッシュボードとワークフローが統合されているので、チーム間で関連データとセキュリティのインサイトを共有し、現在のセキュリティ状況を把握できます。

セキュリティ

手作業に頼らない、効率的な保護

お客様の90%が、本番環境における幅広い攻撃の種類 (OWASP Top 10、アプリケーション　DoS、ボット、アプリケーションの悪用や誤用など)に対するブロックを利用しています。ログを手作業で探し回ったり、誤検知を回避するために正規表現ルールを調整する必要はありません。直感的なルールビルダーのインターフェースを使用し、Webアプリケーションや API トランザクションを定義し、モニタリング、アクションを実行できます。

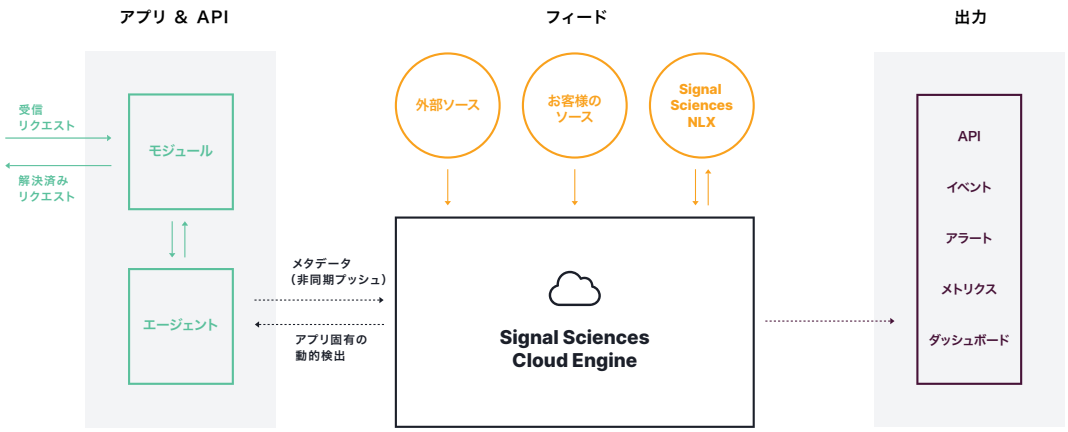
スケーラビリティ

従来のWAFやRASPとは違う、環境を選ばないソリューション

サーバーからコード、コンテナに至るまで、アプリケーションが稼働するあらゆる場所をモニタリングできるため、脆弱性を迅速に発見し、修復することができます。Fastly の次世代 WAF とランタイムアプリケーション自己保護 (RASP) は、どのようなアーキテクチャ上でも動作します。また総保有コストを最小限に抑え、シグネチャの管理も必要ないほか、パフォーマンスにほとんど影響を与えません。

特許取得済みのアプローチ

Web サーバーとアプリケーション全体で軽量なソフトウェアモジュールとエージェントを使用し、セキュリティ状況に関する情報を収集します。さらに、Signal Sciences Cloud Engine によるセルフサービスのダッシュボード、インテリジェントアラート、強力なレポート機能を使用することで、リアルタイムイベントの詳細を確認できます。



柔軟性に優れたデプロイオプションを利用することで、開発、セキュリティ、運用のニーズに合わせてスタック内のさまざまなポイントに Web 保護テクノロジーをインストールできます。すべてのオプションにおいてフル機能が装備され、Signal Sciences Cloud Engine と非同期に接続することができます。また、さまざまなチームが管理する大規模で複雑なアプリケーション内で、異なるデプロイタイプを併せて利用することも可能です。

多くの従来型 WAF では、必要な可視性を得るために複数のツールにログインする必要がありました。Signal Sciences の単一管理コンソールは、実用的な情報と主要なメトリクスを一元化されたインターフェースに迅速に表示します。

従来の WAF との違い

	従来型の WAF	Signal Sciences の次世代 WAF
デプロイモード	91%のユーザーがログモードかモニターモードで運用、もしくは誤検知を理由にWAFを完全に停止[1]	90%以上のユーザーがフルブロッキングモードを使用
アーキテクチャの互換性	物理または仮想アプライアンス クラウドでの使用には不向き CDN 異なる CDN WAF 製品間で統一管理ができない	Webサーバー、アプリケーションサーバー、PaaS、ネイティブクラウド、ハイブリッドクラウド、マルチクラウド、オンプレミス、サーバーレス、コンテナなど、アプリケーションデプロイ全体を単一のアーキテクチャおよびUI で管理
攻撃の種類	OWASP Top 10 のみ	OWASP Top 10、DoS攻撃、ブルートフォース/ATO攻撃、アプリの悪用や誤用、悪質なボット
DevOps のサポート	セキュリティ以外での使用やアクセスはほとんど行われず、ツールチェーンの統合も不十分	Slack、Jira、Pagerduty、Splunk、その他多数のツールを通じて、アラートの全詳細をDevOpsやセキュリティチームに提供

[1] Fastly の委託により Enterprise Strategy Group が実施した調査結果 (2021年6月発表)

Signal Sciences について (現在は Fastly に統合)

Web アプリケーションの安全性を高める―私たちはこのミッションを胸に掲げ、セキュリティ、運用、エンジニアリングチームにとって実際に役立つ Web 保護ソリューションを提供します。
詳しくは signalsciences.com をご覧ください。