fastly

Powered by Signal Sciences

プロダクトデータシート

Fastly 次世代 WAF

アーキテクチャとデプロイの概要

環境を問わない Web アプリと API の統合セキュリティソリューション

Fastly は、コンテナ、オンプレミス、クラウド、エッジなど、あらゆる環境でアプリと API を保護する、WAF 市場で最も柔軟性の高い統合型ソリューションを提供します。パフォーマンスを犠牲にしたり、管理のために専用スタッフを追加する必要がなく、包括的な保護を実現できます。Fastly (旧 Signal Sciences) の次世代 WAF はすぐに使用可能な上、有効性が高いため、90%以上のお客様がフルブロックモードで使用しています。

Fastly 次世代 WAF は最先端のアプリが必要とするプロアクティブな保護を提供し、既存の DevOps とセキュリティのツールチェーンに統合することで、卓越した可視性を実現します。この柔軟なアーキテクチャにより、開発、運用、セキュリティの各チームは Web アプリケーションや API への攻撃が発生した際に、その場所や方法についてインサイトが得られるため、アプリケーションのセキュリティ戦略をさらに進化させることができます。

このデータシートでは、高度なパフォーマンスを発揮する Fastly 次世代 WAF の特許取得済みアーキテクチャについて詳しくご説明します。また、幅広いデプロイオプションについてもご紹介します。このデータシートは、以下のセクションによって構成されています。

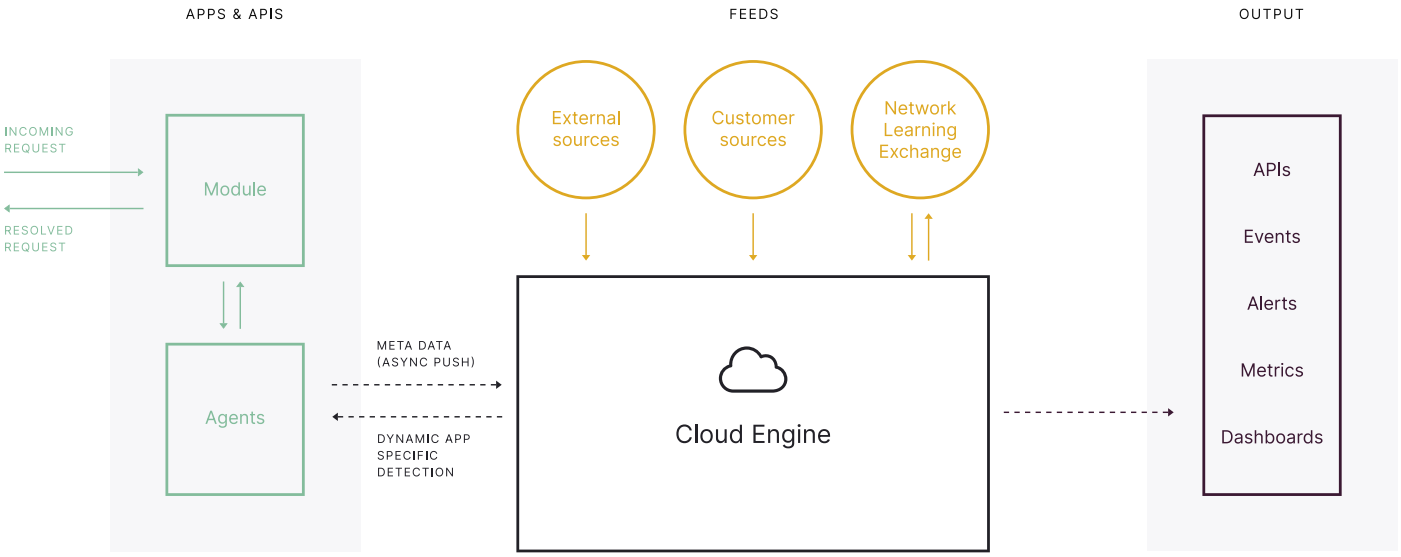
- **アーキテクチャの概要**
- **デプロイオプション**
- **DevOps とセキュリティのツールチェーンとの統合**

Gartner peerinsights customers' choice 2021™

現在は Fastly の一部である Signal Sciences は、Gartner Peer Insights の Web アプリケーションおよび API 保護 (WAAP)部門で「カスタマーズチョイス」に4年連続で選出された唯一のベンダーです。2022年1月31日[1] 現在、267件のレビューに基づく総合評価が**5段階中4.9ポイント**と、市場で**最も高い評価**を得ている WAAP ソリューションのひとつです。

1： Gartner Peer Insights の内容は、同プラットフォーム上に記載されたベンダーを利用した個々のエンドユーザーの体験に基づいた意見をまとめたものであり、事実の記述として解釈されるべきではなく、Gartner やその関連会社の見解を表すものでもありません。Gartnerは、ここに掲載されたいかなるベンダー、製品、またはサービスを推奨することはなく、このコンテンツに関して、商品性または特定の目的への適合性の保証を含め、正確性または完全性について、明示または黙示を問わず、いかなる保証も行いません。GARTNER PEER INSIGHTS のロゴは、Gartner, Inc. およびその関連会社における商標およびサービスマークであり、同社の許可を得て使用しています。All rights reserved.

アーキテクチャの概要



Fastly 次世代 WAF は、3つの主要コンポーネントで構成されるハイブリット SaaS (Software as a Service) です。Signal Sciences が開発した特許取得済みのアプローチにより優れたスケーラビリティを実現し、大量のリクエストを受信するアプリケーションや API でも、パフォーマンスに影響を与えることなく効果的に保護します。

エージェント

お客様の既存のインフラストラクチャにデプロイされた軽量のエージェントが、リクエストに対する検出と判断を迅速かつ正確に実行します。

モジュール

エージェントと連動して高いパフォーマンスと信頼性を確保する、オプションでありながら強力なコンポーネントです。

Cloud Engine

外部および独自のソースから収集したインテリジェンスを使用してエージェントを非同期で強化し、アプリケーション固有の動的な検出を可能にするクラウドホスティング型の分析バックエンドです。

エージェント

エージェントは小さなデーモンプロセスで構成されています。ローカル環境で正確な検出と判断を高速に実行し、極めて高い負荷にも対応できるよう設計されています。エージェントは処理した悪意のあるリクエストに関するメタデータも収集し、それを Cloud Engine と共有します。Fastly 次世代 WAF は、最大規模の Web サイトを保護しており、本番環境で何万ものエージェントが何兆件ものリクエストを処理していますが、アプリや API のパフォーマンスに影響を与えることはありません。エージェントは、攻撃がアプリケーションや API に到達する前にブロックするだけでなく、受信したリクエストやサーバーのレスポンス、アプリケーションの動作異常なども可視化することができます。

モジュール

モジュールは、ほぼすべての Web サーバー（NGINX、Apache、IIS など）やアプリケーション言語 (.NET、Java、Python、PHP、.nodeJS など) で実行可能です。たった数百行のコードで構成されていますが、信頼性と極限のパフォーマンスの実現に役立ちます。モジュールの唯一の役割は、エージェントにリクエストを送り、エージェントから受け取った判断を実行することであり、アプリケーションへのリクエストを許可したり、リクエストをログまたはブロックします (コンソールで設定されたモードによります)。

Cloud Engine

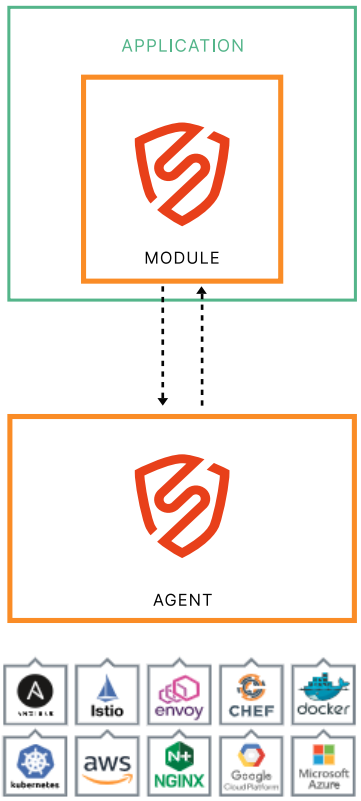
Cloud Engine は、顧客ベース全体から何千ものソフトウェアエージェントを通じて匿名化された攻撃データとテレメトリを収集し、分析します。エージェントは Cloud Engine が提供するデータをローカルで利用することで、より優れた検出と、より効果的なブロックの判断を行うことができます。エージェントの判断は、NLX (Network Learning Exchange) によって強化されています。NLX は管理コンソール内で既知の悪質な IP ソースを共有し、アプリケーションや API が脅威に晒される前に疑わしいユーザーに関するアラートを発信します。その他のフィードには悪質な IP の外部リストとお客様のカスタム IP リストが含まれており、これらはすべて、さらなるリクエストコンテキストとしてエージェントの判断の強化に活用されます。この可視性とコンテキストは、Fastly の API に加え、お客様がすでに使用している DevOps ツール (Slack、PagerDuty、Jira など) や、セキュリティツール (Splunk、Elastic、Palo Alto Networks の Cortex XSOAR など) とのネイティブ統合を通じて共有されます。またアプリケーションフットプリント全体のメトリクスとイベントレポートも、単一管理コンソールのダッシュボードで簡単に確認することができます。

デプロイオプション

データセンター、クラウド、コンテナ、サーバーレス環境向けのネイティブデプロイオプション

デプロイオプション1：クラウド & コンテナネイティブ

ご利用の Web サーバー、API ゲートウェイ、またはアプリレベルで、Fastly 次世代 WAF のエージェントとモジュールのペアを数分でインストールできます。Fastly WAF のエージェントはインフラ環境に依存しないため、開発言語やフレームワーク、依存関係を気にすることなく、必要な場所にデプロイ可能な柔軟性を備えています。



Kubernetes やサービスメッシュへのデプロイ

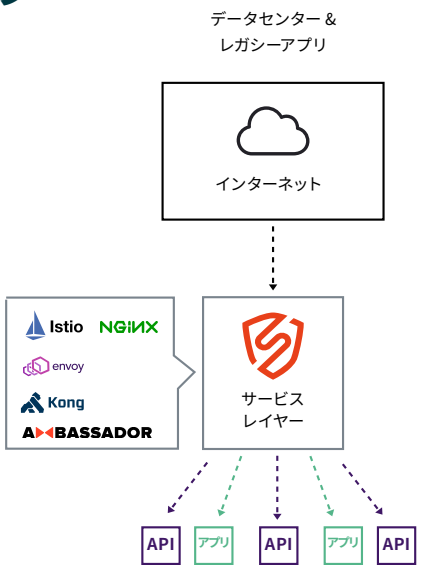
Kubernetes などの新しいアプリツールやフレームワークの登場で、企業は DevOps に特化した環境へ急速に移行しています。企業がかつてないスピードでコードをリリースする中、Fastly はお客様のコンテナ戦略に最適な、柔軟性の高い複数のデプロイオプションを提供し、これらは Kubernetes に Fastly 次世代 WAF をインストールできる 3 つの「レイヤー」と、4 つのデプロイ方法で構成されています。さらに、Envoy Proxy や Istio などのサービスメッシュとのネイティブ統合により、縦方向(クライアントとサーバー間)と横方向 (サービス間) の両方のリクエストに対する可視性が得られます。

インストール方法	レイヤー1：イングレスコントローラー	レイヤー2：ミッドティアサービス	レイヤー3：アプリケーション層
エージェント + モジュール (同一アプリコンテナ内)	✓	✓	✓
エージェント + モジュール (異なるコンテナ内)	✓	✓	✓
リバースプロキシモードのエージェント (アプリと同一のコンテナ内)	✓	✓	✓
リバースプロキシモードのエージェント (サイドカーコンテナ内)	✓	✓	✓

Fastly WAF との完全な統合が可能なデプロイ先： kubernetes docker envoy Istio

デプロイオプション2：データセンター & レガシーアプリケーション

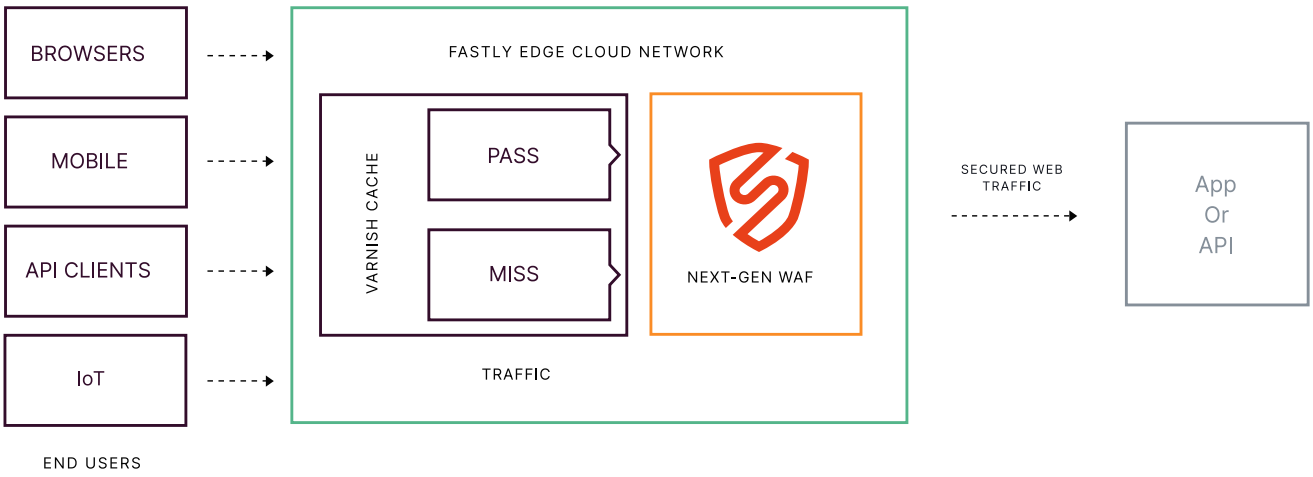
レガシーアプリケーションやデータセンターにデプロイされているアプリケーションの保護を必要とする場合、2つのデプロイオプションがあります。1つは、Web リクエストがアプリや API エンドポイントに到達する前にトラフィックを検査できるように Fastly 次世代 WAF をインストールする方法です。もう1つは、リバースプロキシモードでエージェントをインストールする方法です。例えば、ロードバランサー（HAProxy、NGINX）や API ゲートウェイ（Ambassador、Kong、Cloudentity）に Fastly WAF のモジュールをインストールすることが可能です。ロードバランサーや API ゲートウェイへのインストールが難しい場合は、Fastly WAF のエージェントをリバースプロキシモードでデプロイできます。いずれのデプロイオプションでもフル機能へのアクセスが可能で、他のデプロイオプションと同じレベルの可視性と実用的なインサイト、およびアラート機能をご利用いただけます。



デプロイオプション3：エッジへのデプロイ

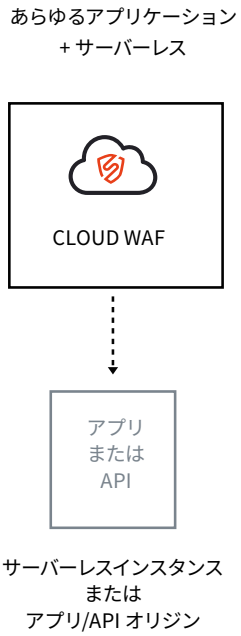
Fastly 次世代 WAF を[Fastly のエッジクラウドネットワーク]で使用し、Fastly 配信サービスの一環としてセキュリティ対策を強化することができます。エッジクラウドへのデプロイオプションでは、Fastly のキャッシュレイヤーである Varnish にシームレスに統合できます。

これにより、ユーザーにより近い場所での保護と脅威への迅速な対応が可能になり、不正な攻撃トラフィックからオリジンシステムを守ると同時に、最高レベルのパフォーマンスを維持できます。エッジへのデプロイは、既存のインフラストラクチャにソフトウェアをインストールできないお客様や、Fastly のグローバルなコンテンツ配信ネットワーク (CDN) のパフォーマンス上のメリットを活用したいとお考えのお客様に最適です。このデプロイオプションでは、レイヤー3、およびレイヤー4での常時オンの DDoS 対策と TLS 管理を含む追加機能もご利用可能です。



デプロイオプション4： Cloud WAF

Cloud WAF を使用すると、インフラストラクチャにソフトウェアをインストールすることなく、迅速かつ簡単に Web アプリケーションや API、マイクロサービス、サーバーレスアプリケーションを保護できます。デプロイ後に、DNS に簡単な変更を加えてアプリケーションのトラフィックを Cloud WAF に向けるだけで、Fastly 次世代 WAF がアプリケーションを保護し、セキュリティに関する可視性を提供します。すべての Web リクエストは Fastly WAF のクラウド実行レイヤーにリダイレクトされ、不正なリクエストが検出・ブロックされます。すべての正常なトラフィックは、お客様のアプリケーションのオリジンサーバーに転送されます。Cloud WAF は CDN レイヤーの上流に変更を加えることなく、簡単に管理できる WAF をお求めのお客様に最適です。



データプライバシーを重視するセキュリティ対策

大手のファイナンスサービス企業やヘルスケア企業、その他の厳格なデータ保護規則の要件への準拠を必要とする企業の多くが、データ保護を重視して構築された強力なアーキテクチャを採用した Fastly 次世代 WAF を利用しています。機密性の高いデータはすべてお客様の環境の内部で処理され、攻撃または異常なリクエストとしてマークされたリクエストに関しては、サニタイズまたは編集された部分のみが Fastly WAF の Cloud Engine に送信されます。

リクエストにおいて潜在的な攻撃または異常が特定されると、カスタマイズ可能な編集設定がローカルで適用されます。その後エージェントによって、攻撃ペイロードを含むリクエストの編集済みの各パラメーターと、クライアント IP やユーザーエージェント、URI など、リクエストに含まれる機密性がなく無害な情報のみが送信されます。バックエンドでは、レスポンスコードやサイズ、時間など、レスポンスのメタデータのみが収集されます。お客様は、必要に応じて編集ポリシーやフィールドを自由にカスタマイズできます。さらに、Fastly はバックエンドにリクエストを送信する前に一般的な種類の機密データ（パスワード、キー、GUID、あらゆる種類の PII と PHI）に自動的に編集を施し、機密性の高い情報を保護します。

Betterment

「導入後すぐに効果を発揮し、自動的にスケールアップするだけでなく、アプリケーションを保護しながら優れた可視性も提供してくれます」

Anson Gomes 氏
Betterment
Lead Security Engineer

DevOps とセキュリティのツールチェーンに統合

アプリケーションと API を効果的に保護するためには、開発、運用、セキュリティの各チームが、すでに使用しているツールを通じて、同じベースラインのセキュリティデータを得られるようにすることが重要です。Fastly は業界トップクラスのツールやプラットフォームと連携し、お客様の DevOps とセキュリティのツールチェーンにリアルタイムでアラートを送信します。お客様のチームは、Fastlyが提供する本番環境のセキュリティに関するテレメトリを既存のツールやワークフロー内で簡単に利用して、さらに詳細な調査や分析を行うことができます。

導入後、すぐにこれらのツールに容易に統合できるため、最先端の開発モデルやアーキテクチャへの移行を後押しします。またワンクリック統合には、最も一般的な開発・運用アラートエンジン、ChatOps、プロジェクト管理、インシデント追跡システムなどの機能が含まれます。

統合可能なテクノロジー & プラットフォーム

Platform integrations & partners

Run the Fastly Next-Gen WAF anywhere

WEB SERVERS

NGINX
Microsoft IIS
APACHE SOFTWARE FOUNDATION
Apache Tomcat

IAAS

Google Cloud
Microsoft Azure
aws

PAAS

Microsoft Azure
HEROKU
Red Hat
IBM Cloud
VMware Tanzu

CONTAINERS

kubernetes
docker
OPENSHIFT
Istio
envoy
MESOS

CONFIG MANAGEMENT

CHEF Progress
Red Hat Ansible
puppet
SALTSTACK
Terraform

Feed integrations & partners

Send and receive data from the Fastly Next-Gen WAF

DEVOPS TOOLCHAIN

Jira Software
DATADOG
PivotalTracker
VictorOps
slack
PagerDuty
Opsgenie
Microsoft Teams

SOC/SIEM

splunk>
McAfee
elastic
NETWITNESS
ELK Stack
ArcSight
Radar
LogRhythm
sumo logic
CISCO
CORTEX XSOAR BY PALO ALTO NETWORKS

Fastly を試してみませんか？

パフォーマンスに影響を与えることなく、効果的なセキュリティ対策を実現できます。

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

お問い合わせ