Signal Sciences
Now part of fastly

ホワイトペーパー

Web 攻撃指標の特定

クレデンシャルスタッフィング、API の悪用、SQL インジェクション、ビジネスロジックの悪用 : セキュリティチームが注目すべき、4種類の高リスクの攻撃を特定

Signal Sciences
Now part of fastly

Web 攻撃指標の特定

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を保護する堅牢なセキュリティソリューションを提供するため、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、大規模にアプリケーションを保護できるようになりました。ユーザーのエクスペリエンスを強化する最先端の次世代セキュリティ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。

目次

背景

Webアプリケーションやクラウドベースのアプリケーションが攻撃対象として選ばれるのは、ごく単純に、これらの攻撃が成功する可能性が高いためです。Verizonは『2020 Data Breach Investigations Report』 (2020年度データ侵害調査レポート)の中で、Webアプリケーションへの攻撃を利用して不正侵入に成功したケースが多く、脅威ベクトルの上位に位置していると指摘しています。[1]

顕著なWeb 攻撃タイプ

Signal Sciences は、Web セキュリティチームが重点的に対応すべき高リスクの攻撃タイプとして以下の4つを挙げています。

1. **クレデンシャルスタッフィング：** 10件の侵害のうちおよそ3件で、盗まれた認証情報が利用されています。

2. **API の悪用：** API ファーストの開発が普及するにつれ、攻撃者が API をターゲットにするケースが増えています。

3. **SQL インジェクション：**インターネットスキャンの約3分の2がバックエンドデータベースを攻撃しています。

4. **ビジネスロジック ：** アプリケーションの設計上の欠陥を検出し、ビジネスロジックを攻撃します。

これらの攻撃を防ぐためには、攻撃の兆候を理解し、自社のビジネスを標的とする脅威についてのインサイトを得る必要があります。しかし攻撃の指標は必ずしも明確ではなく、他の正当なトラフィックに紛れ込んだ「ロー＆スロー」攻撃の検出は容易ではありません。

可視性を得るための最初のステップは、アプリケーションの予想トラフィックのベースラインを把握することです。ベースラインのトラフィックパターンを理解することで攻撃を検出しやすくなり、より適切に対応できるようになります。さらに、悪意があると思われるトラフィックはどれか、またその理由についても可視化する必要があります。リクエストを攻撃として分類する理由が分からないシステムでは、防御力を高めることはできません。

> セキュリティ侵害の80%以上を占める Web アプリケーションは最大の攻撃対象[2]

1

攻撃タイプ：その1

クレデンシャルスタッフィング

企業がビジネス推進のために多くのアプリケーションを導入するなか、多くの場合、ビジネスデータやユーザーデータへのアクセスは、シンプルなユーザー名とパスワードの組み合わせによって保護されています。これでは、クレデンシャルスタッフィングが昨年最も成功した攻撃手法であるのも不思議ではありません。Verizonによると、セキュリティ侵害の29%が盗んだ認証情報を使用して機密データにアクセスしており、これはフィッシングに次いで多い数です。

攻撃者はこれらの認証情報を利用して、アカウントの乗っ取り、プライベートな IoTデバイスへのアクセス、アカウント回復用メールアドレスへのアクセスによる連鎖的な攻撃などを行います。

> Verizon によると、セキュリティ侵害の29%が盗んだ認証情報を使用して機密データにアクセスしており、これはフィッシングに次いで多い数です。

実例

2019年2月、ハッカーが保存された認証情報を利用してNestデバイスをコントロールしようとしている脅威について、Googleは顧客にメールで警告しました。その一例では、ハッカーがある家族の Nest デバイスをコントロールし、乳児に話しかけたり、室温を上昇させたりしました。[3,4]

2件の大規模な認証情報漏えいが公表されて以来、認証情報を利用したアカウント乗っ取り攻撃が全般的に増加しています。2019年1月、あるセキュリティ研究者が、7億7,300万件の固有のメールアドレスと2,100万件の固有のパスワードを含むデータベース（コレクション #1と呼ばれる）をオンライン上で発見しました。コレクション #2-5と呼ばれる2つ目のダンプには、250億件以上のメールとパスワードの記録がありました。[5]

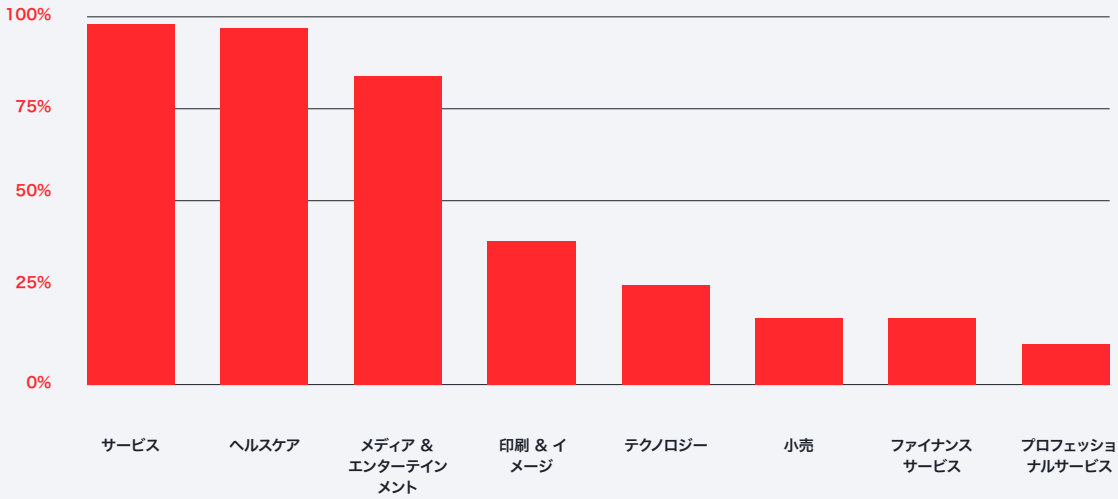
これらのデータベースと他の2つのデータベースを合わせると、漏えいされたユーザー記録の数は260億件以上に上ります。[6]

DEVOPS文化を促進するプロアクティブなフィードバックの作成

最近の企業は、新機能のロールアウト、コードへのパッチ適用、攻撃のブロックを可能な限り短時間で行うことを重視しています。また、アプリケーションの開発やデプロイ、管理に DevOpsプロセスを使用している場合、問題や修正をトラックするために、コミュニケーションチャネルにアラート機能を統合する必要があります。DevOpsサイクルにリアルタイムのフィードバックを提供するアプリケーションセキュリティおよびパフォーマンス管理ツールを使用することで、アプリケーションのセキュリティ侵害が起きてから対処するのではなく、セキュリティ問題にリアルタイムで対処できるようになります。

Signal Sciences
Now part of fastly

業界別のアカウント乗っ取り試行



このグラフは、2019年7月にアカウント乗っ取りの試みが一定のしきい値に達した、攻撃指標となるカスタマーイベントの割合を表しています。

2019年7月、Signal Sciences が観測した1兆件以上のプロダクションリクエストを標的とした Webレイヤー攻撃の中で、クレデンシャルスタッフィングは最も頻度の高い攻撃手法でした。クレデンシャルスタッフィング試行の分析を上のグラフで業種別に見てみましょう。サービス、ヘルスケア、メディア & エンターテイメントなどの業種が攻撃対象の上位となっています。

攻撃の指標

クレデンシャルスタッフィングは、アカウント乗っ取り攻撃の主な手口であるため、攻撃の兆候は辞書攻撃やブルートフォース攻撃のパスワード推測とは異なります。頻繁に多数の IP アドレスに分散して送信されるため、単一の送信元から大量の認証情報が送信されることはありません。攻撃の指標には以下が挙げられます。

- 地理的に多様なエリア、特にユーザーの通常のエリア外からのログイン試行
- 全ユーザーにおける、ログイン失敗の回数増加
- 疑わしい IP アドレスからのログイン成功

対策

完全にアクセスをブロックするのではなく、ログインの試行が正規のユーザーによるものかを確認する方法があります。アプリケーションは、二要素認証などセキュリティチェックを追加してリクエストに対応する必要があります。また、セキュリティチームとオペレーションチームが、ログイン試行やメールアドレスまたはパスワードのリセットリクエストなど、主要な認証作業に関するリクエストの量をモニタリングするのも有効です。そして、想定されるしきい値を超えたリクエストを一時的にブロックします。特定のタイプの認証イベントを可視化できるセキュリティツールは、認証情報の不正使用検出に不可欠です。

Signal Sciences
Now part of fastly

2

攻撃タイプ：その2

API の悪用

ネイティブのモバイルアプリケーションやシングルページのWebアプリケーションの急激な普及により、データへのアクセスがAPIを介して行われるようになりました。アプリケーションがクラウドインフラにデプロイされ、特定の開発チームや DevOps チームによって管理されるようになり、RESTful API やマイクロサービスが急増しています。

一方、APIの普及により、APIに対する攻撃も急激に増加しています。インジェクション攻撃は、OWASPトップ10のソフトウェアリスクで最上位に位置付けられている攻撃タイプです。ブルートフォース攻撃では、検出した重要な API サービスにリクエストを大量に送信し、重要なリソースにアクセスできないようにしてアプリケーションを機能できない状態にします。より巧妙な手口で正当に見えるリクエストを送信してデータを盗み出し、自らの目的にAPIを利用しようとする攻撃者もいます。

実例

2017年、セキュリティ研究者の Dylan Houlihan 氏は、カフェチェーン店 Panera Bread の Web サイトに、顧客データへのアクセスを可能にする安全でない API を発見しました。この API では顧客記録に連番を付けていたため、ボットがサイトから700万件以上の顧客情報をスクレイピングできる状態でした。場合によっては、3,700万件以上の顧客情報が流出した可能性もあります。[7]

企業が新規顧客獲得のために無料トライアルを提供する場合にも、同様の問題が起こりかねません。これにより、試用版ソフトウェアをインストールした攻撃者がそれを使用して重要なAPIにアクセスし、サーバーに侵入することが可能になると考えられます。無料トライアルは、販売プロセスをスピードアップさせる一方で、インフラが悪用されるリスクを伴います。解決策としては、全ての顧客を制限するのではなく、試用版ソフトウェアをインストールした顧客をより積極的にブロックするなどの方法が考えられます。

イスラエルの国営航空会社をはじめとする140社の航空会社が使用している Amadeus予約システムでは、攻撃者は予約識別子を列挙することで、顧客データやフライト情報を取得することができました。[8]攻撃者は、ユーザーアカウントや消費者特典などのリソースの識別子が推測可能な API を探します。API のセキュリティが不足していたり、認証メカニズムが正常に機能していない場合、システムが悪用される可能性が高まります。

攻撃の指標

SQLインジェクションと同様、API への攻撃は一見すると正当なリクエストのように見えますが、奇妙なパターンが含まれていたり、期限切れの認証情報が使用されていたり、正規のトラフィックよりはるかに頻繁に発生します。API 攻撃の指標には以下が挙げられます。

- 異常な量の API リクエスト
- 無効な API リクエスト、不適切な Cookie、信頼できないデバイスからの接続試行
- 適切な認証を受けていない API リクエスト、疑わしい地理的位置からの API リクエスト、または保護されたデータへのアクセスを試みる API リクエスト

対策

企業としては、顧客がクラウドベースのアプリケーションにアクセスできなくなるのを避けるため、初期の緩和策として、攻撃が発生している可能性があることをまず顧客に警告します。不審なIPアドレスや攻撃クラスターを調査し、攻撃のパターンを把握することで、より広範な対策を取ることが可能になります。最終的には、攻撃パターンや IP アドレスに基づいて API へのアクセスをブロックするルールを作成し、今後の攻撃を抑制することができます。

3

攻撃タイプ：その3

SQLインジェクション

Web サイトの大半は、バックエンドの SQL データベースに接続しています。これらのデータベースを攻撃することで、データベースに保存されている全ての顧客情報へのアクセスが可能になることが少なくありません。SQLインジェクション (SQLi) が依然として攻撃者の間で人気が高いのも不思議ではありません。実際、インターネットスキャンの約3分の2がバックエンドデータベースをターゲットにしています。[9]

SQL データベースは至る所に存在し、貴重な情報を含んでいるため、攻撃者は Web サイトを通じて SQL データベースにアクセスしようとします。攻撃者は SQL インジェクション攻撃によって、商品の機密データ (在庫情報など) を発見したり、ユーザーのデータ (住所、電話番号、クレジットカード情報など) を収集したり、ユーザー名やパスワードを盗んだりします。

実例

2019年3月、人気の eコマースアプリケーションは、プラットフォームの脆弱性により、攻撃者がバックエンドのデータベースにアクセスできることを報告しました。[10]犯罪者たちは、16時間以内にこの脆弱性を狙って攻撃を開始し、ネット店舗ソフトウェアのセキュリティ侵害に成功しました。その多くは利用者の決済カード情報を盗むマルウェアを植え付けるという手口でした。

当時、Signal Sciences の eコマース企業のお客様が、一連の異常な SQL リクエストを検出しました。これらのリクエストは、複数の中国の IP アドレスから送信され、Web サイトのさまざまなパスをターゲットにしていました。Signal Sciences は、SQLi 攻撃がブロックされたことをお客様に通知しました。このお客様はリクエストの内容を調査し、バックエンドの WordPress データベースに対する新しい攻撃のドキュメントを発見しました。

SQL インジェクション攻撃は、あらゆる業界で頻発しています。

2019年7月に観測された攻撃のテレメトリ分析については、付録のチャートをご覧ください。

WEB アプリケーションのブロック機能の改善

従来の Web アプリケーションファイアウォール (WAF) では、アプリケーションのブロックに問題がありました。WAF が適切に調整されるまで、誤検知によって実際のビジネスチャンスを逃す可能性があるためです。Web セキュリティテクノロジーは、企業が収入の損失を心配することなく、デフォルトで攻撃をブロックできるものでなければなりません。精度が高ければ高いほど、あまり一般的ではない攻撃に集中することが可能になります。

攻撃の指標

単純なパターンマッチングでも SQL インジェクションを検出することは可能ですが、誤検知が発生しやすく、新しい攻撃を見逃してしまう可能性もあります。攻撃を自動ブロックするには、以下を検出できる精度の高い検出機能が必要です。

- 通常の SQL リクエストのしきい値を超える攻撃
- SQL サーバーによる405レスポンス (許可されていないメソッド)
- パターンマッチングによる一般的な攻撃の検出、または攻撃コードの検索

対策

リクエストのしきい値超過をベースに攻撃をブロックすることが不可欠です。攻撃のパターンに応じてインシデントを精査し、特定のグループが自社のデータアセットを狙っているのかを判断できることが重要です。

Signal Sciences
Now part of fastly

4

攻撃タイプ：その4

ビジネスロジック

多くの場合、攻撃者はアプリの仕組みを理解し、設計の特定部分を悪用して目的を達成しようとします。このようなビジネスロジック攻撃では、公開されている機能を利用して情報を盗んだり、アカウントにアクセスしたり、サービスを中断させることができます。

例えば、セッションのステートを維持するためにサーバーに送信されるパラメータをリバースエンジニアリングすることで、攻撃者は昇格した権限を得ることが可能です。ユーザープロファイルに応じて割引を行うeコマースサイトでは、攻撃者はプロファイルを変更することで、割引を利用できるようになります。また、コンサート会場の座席を5分間確保するアプリを操作して、攻撃者は大量のチケットを予約することができます。

実例

あるセキュリティ研究者は、企業ドメインを持つ人なら誰でもチームチャットに参加できる機能を利用して、ある企業のヘルプデスクのチケットシステムを悪用しました。ヘルプデスクシステムの中には、チケットごとに企業ドメインを使用した固有のメールアドレスを使用して対応するものがあるため、研究者は企業にチケットを提出した後、そのメールアドレスを使用して、複数のエンタープライズレベルのお客様のメッセージングアカウントにサインインしました。[11]

また別のケースでは、チケットの引き換えコードを発行するオンラインチケット会社が攻撃されました。攻撃者は、有効なチケット引き換えコードを発見しようとする自動スクリプトを使用して、API の乱用を試みました。

攻撃の指標

ビジネスロジックの悪用は、アプリケーションの有効な機能を利用するため検出が困難です。企業はアプリケーションの悪用指標を追跡し、以下のような潜在的リスクを伴うリクエストをチェックできるアプリケーションコントロール機能を導入する必要があります。

- アプリケーションリソースの使用、あるいはパフォーマンスに関する問題
- 異常な API コールやサービス使用

対策

攻撃を検出した場合、対策を講じてアプリケーションをアップデートするまでの間、特定のルールを用いて悪用をブロックすることが可能です。最高レベルのセキュリティツールでは、アプリケーションから抽出されるシグナルに基づいてルールを定義することができます。これらのシグナルには、ユーザーとのインタラクションやユーザーエージェント、リクエストパラメータ、Cookie、その他攻撃者に関連するデータなどの外部データが含まれます。これらのルールを使用することで、企業は攻撃に対する可視性を高め、自動化されたアクションを定義することが可能になります。

WEB 保護に最適なツールの選択

アプリケーションやクラウドインフラへの攻撃を可視化するには、柔軟にデプロイ可能で、通常では検出が困難な攻撃をキャッチできるツールが必要です。また、エンジニアはバグの修正やアプリケーションの改善に役立つ実行可能なデータを必要としています。最良の Web セキュリティツールは、パフォーマンスや潜在的な攻撃に関するデータを意思決定者に提供すると同時に、問題に仮想パッチを適用してアプリケーションを保護します。

Signal Sciences
Now part of fastly

可視性の向上でWebアプリケーションのセキュリティを強化

攻撃を阻止するためには、まずどのアプリケーションが攻撃を受けているかを認識する必要があります。攻撃を効果的に検出するには、アプリケーションに何が起きているのかを可視化することが重要です。正規表現パターンのみを使用して異常なアクティビティや悪意のあるアクティビティを検出しようとする製品では、見落としが多くなります。攻撃者は効果的な攻撃方法が見つかるまで手法を変えるため、ルールベースのシステムでは攻撃の兆候を検出できないことがよくあります。

対応が早く、自動保護機能を備え、ルール調整が最小限で済むシステムが必要です。Signal Sciences の Web アプリケーションおよび API 保護プラットフォームは、広範な攻撃動作を可視化することが可能です。Signal Sciences のソリューションを使用することで、Web アプリケーションの問題を診断し、実行可能なインテリジェンスをリアルタイムで得ることができます。

アプリケーションの周囲に重要なセキュリティレイヤーを配置することで、Web アプリケーション、API、マイクロサービスが提供する貴重なデータを保護します。チューニングなしですぐに使用可能な保護ソリューションを提供するだけでなく、特定の攻撃への対応を自動化するカスタムルールを容易に作成できます。

真の可視性を実感

私たちは、世界の大手企業のアプリケーションや API、マイクロサービスを保護しています。包括的な Web アプリケーションおよび API 保護プラットフォームを使用することで、スピードを犠牲にすることなくセキュリティを向上させ、サイトの信頼性を維持すると同時に、総保有コストを最小限に抑えることが可能になります。

> 企業に必要なのは、対応が早く、自動保護機能を提供し、ルール調整が最小限で済むシステムです。

Signal Sciences
Now part of fastly

Appendix：業種別上位攻撃シグナル

Signal Sciences は、当社独自のアプローチによる広範な攻撃や異常シグナルの可視性を活用して、業種別に上位の攻撃シグナルを分析しました。当社の顧客ベースでは、多くの業種において、アカウント乗っ取り試行の検出とブロックが必要不可欠であることが分かります。データは、2019年7月中に観測された攻撃全体に占める割合を示しています。

ファイナンスサービス

1. 検索ボット偽装
2. アカウント乗っ取り試行
3. 強制ブラウジング
4. SQL インジェクション
5. コードインジェクション

メディア & エンターテインメント

1. アカウント乗っ取り試行
2. SQL インジェクション
3. クロスサイトスクリプティング
4. トラバーサル攻撃
5. 攻撃ツール

印刷 & イメージ

1. アカウント乗っ取り試行
2. 検索ボット偽装
3. クロスサイトスクリプティング
4. SQL インジェクション

プロフェッショナルサービス

1. アカウント乗っ取り試行
2. SQL インジェクション
3. ボット偽装
4. 攻撃ツール
5. クロスサイトスクリプティング

小売

1. アカウント乗っ取り試行
2. プライベートファイル
3. SQL インジェクション
4. クロスサイトスクリプティング
5. コマンド実行

テクノロジー

1. アカウント乗っ取り試行
2. クロスサイトスクリプティング
3. 攻撃ツール
4. SQL インジェクション
5. バックドア

Signal Sciences
Now part of fastly

エンドノート

1. "2020 Data Breach Investigations Report". Verizon Enterprise Solutions. https://enterprise.verizon. com/resources/reports/dbir/ (2020年7月アクセス).
2. "2019 Data Breach Investigations Report". Verizon Enterprise Solutions. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (2019年7月17日アクセス).
3. "Google Warns Nest Users to Update Security". Popular Mechanics. https://www.popularmechanics.com/technology/security/a26214078/google-nest-hack-warning/ (2019年7月17日アクセス).
4. "Hacker talks to baby through Nest security cam, jacks...". NakedSecurity. https://nakedsecurity.sophos.com/2019/02/01/hacker-talks-to-baby-through-nest-security-cam-jacks-up-thermostat/ (2019年7月17日アクセス).
5. "Hackers Are Passing Around a Megaleak of 2.2 Billion Records". WIRED. https://www.wired.com/story/collection-leak-usernames-passwords-billions/ (2019年7月17日アクセス).
6. "Security firm identifies hacker behind Collection 1 leak, as...". ZDNet. https://www.zdnet.com/article/security-firm-identifies-hacker-behind-collection-1-leak-as-collection-2-5-become-public/ (2019年7月17日アクセス).
7. "Panerabread.com Leaks Millions of Customer Records". Krebson. https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/ (2019年7月17日アクセス).
8. "Over 140 International Airlines Affected by Major Security Breach". https://www.bleepingcomputer.com/news/security/over-140-international-airlines-affected-by-major-security-breach/ (2019年7月17日アクセス).
9. "SQL Injection Attacks Represent Two-Third of All Web App...". https://www.darkreading.com/attacks-breaches/sql-injection-attacks-represent-twothird-of-allweb-app-attacks/d/d-id/1334960(2019年7月17日アクセス).
10. "Two hacking groups responsible for huge spike in hacked...". ZDNet. https://www.zdnet.com/article/two-hacking-groups-responsible-for-huge-spike-in-hacked-magento-stores/ (2019年7月17日アクセス).
11. "This hacker gained access to hundreds of companies through their...". https://thenextweb.com/security/2017/09/21/ticket-trick-see-hackers-gain-unauthorized-access-slack-teams-exploiting-issue-trackers/ (2019年7月17日アクセス).

寄稿者

Zane Lackey、Global Head of Security Product Strategy 兼 Signal Sciences 共同創設者

Jack Zarris、Principal Sales Engineer

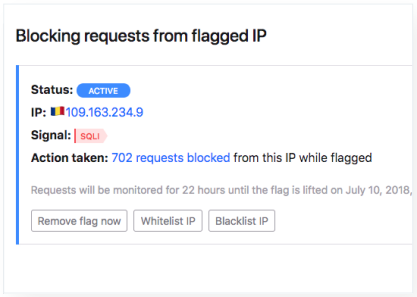
Orlando Barrera、Senior Solution Architect

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 ー 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。

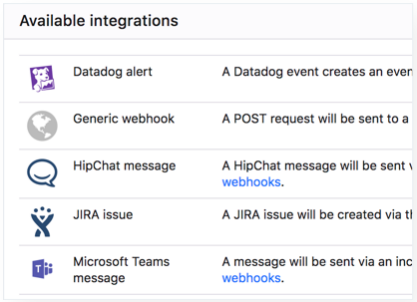
信頼性の高い自動ブロック機能

- Webサーバーまたはアプリケーションコードで直接実行可能
- フェイルオープンアーキテクチャでサイトの高速パフォーマンスを維持
- 独自のSmartParse 検出技術により、チューニングやメンテナンスが不要



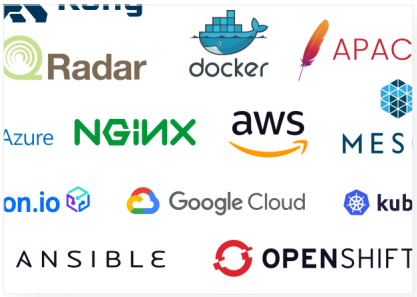
DevOps を意識したソリューション

- 運用チームによる簡単なデプロイ
- メトリクス、パフォーマンス、トレンドを可視化してチーム間で共有
- ツールチェーンへの統合による迅速なアクセスとコラボレーション



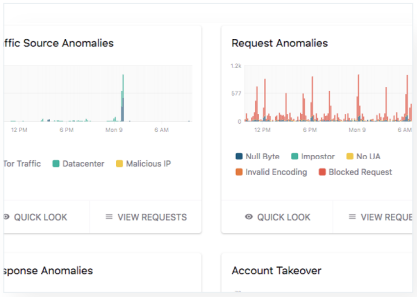
すべてのプラットフォームを単一の UI で

- コンテナ、オンプレミス、クラウドなど、あらゆる場所を保護
- フットプリント全体を確認できる一元化されたビュー
- 社内外のサービスの保護とモニタリング



あらゆる脅威から保護

- 一般的な OWASP Top 10 の攻撃を即時ブロック
- PCI 要件6.6への準拠などのコンプライアンス対応
- アカウント乗っ取り、悪意のあるボット、アプリケーションのサービス拒否などをブロック



Signal Sciences
Now part of fastly