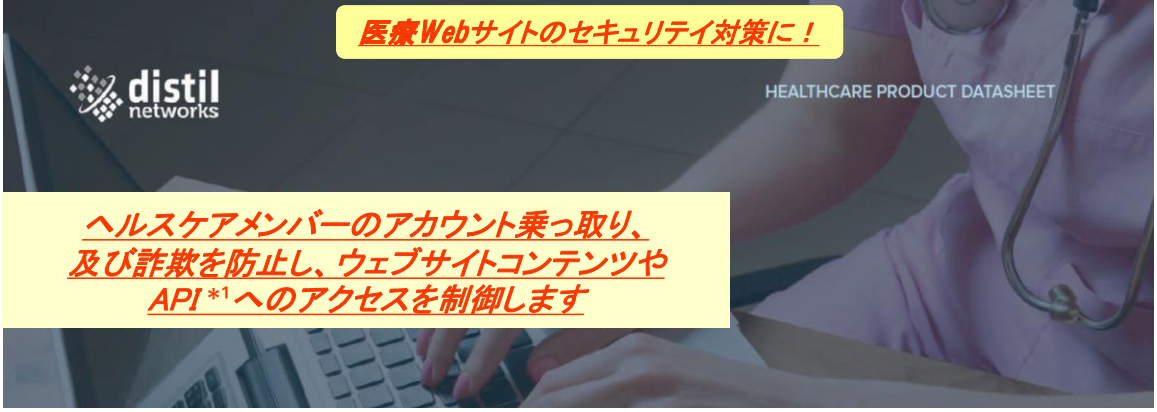


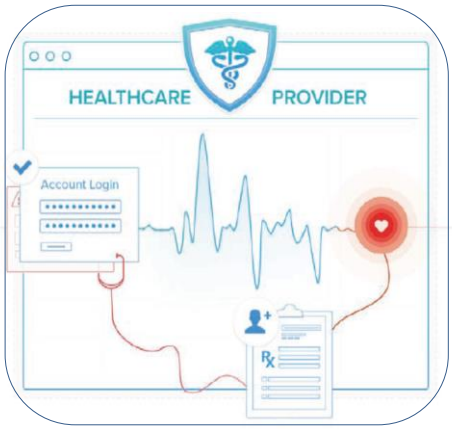
distil networks

● ヘルスケア向けアプリケーション

ダークウェブ上での医療記録の価値は、$500もの高額になることがあります。サイバー犯罪者は、悪いボット(OWASPが「自動化された脅威(Automated Threats)」と呼ぶもの)を使用して、ログイン画面を攻撃し、患者記録を盗み、アカウント詐欺を行います。
ヘルスケアデータの侵害は、個人情報の盗難だけでなく、医療費請求詐欺や保険金詐欺をもたらします。

Distil Networks(アメリカ)は、オンラインアプリケーションと、PHI*2、アプリケーションパフォーマンス及び独自のコンテンツを含むデータとを保護します。Distilは、ヘルスケアデータを保護し、世界のセキュリティ基準に対するコンプライアンスを維持する重要性を理解しています。

1) アカウント乗っ取りや詐欺を防止する
2) 情報収集サイトが独自の価格設定やコンテンツを盗むのを阻止する
3) 情報収集サイトが見込み客や顧客を引き抜くのを防止する
4) 無許可の脆弱性スキャナーをブロックする
5) ペイメントカード詐欺、保険金詐欺、恐喝のリスクを低減する
6) ウェブトラフィックを特定・規制できることを規制機関 に示す



*1 API (Application Programming Interface)とは、広義の意味ではソフトウェアコンポーネントが互いにやりとりするのに使用するインタフェースの仕様である。API には、サブルーチン、データ構造、オブジェクトクラス、変数などの仕様が含まれる。(ウィキペディア)

*2 PHI (Protected Health Information: 保護されるべき医療情報)
参照)HIPAA(HIPAA(Health Insurance Portability and Accountability Act of 1996;
医療保険の携行性と責任に関する法律)によりみなされる医療情報。

Distil Networksは、OWASP Automated Threat Handbookに含まれるあらゆるBOT問題を防止し、従来のWebスクレイパーをブロックするだけの単純なプラグインなどでは防げないWebスクレイピング、Webサイトや APIを攻撃、悪用、誤用するAPB(Advanced Persistent Bot)などからオンラインアプリケーションを他に類を見ない精度で防御します。

世界最高精度(99．9%)の“不正BOT検出”ソリューション！

今日のサイバーセキュリティ環境は、ハッカー、いかがわしい競合他社、詐欺師の不正行為を行う精巧なBOT(自動化プログラム)であふれています。自動化された脅威や悪いBOTは、アカウント認証情報、ペイメントカード保有者情報の悪用、脆弱性のスキャン、コンテンツ・スクレイピング、広告詐欺、アプリケーションサービス拒否を引き起こすなどを含む多くの方法で、日・夜企業を攻撃しています。

Distil Networksは、悪意のあるWebサイトのトラフィックを常時監視、唯一正確な方法で「不正BOT検出と軽減」を可能にする世界的リーダーです。
ユーザに影響を与えずに不正BOTの99.9%をブロックし、Webスクラップ、データマイニング、アカウントハイジャック、迷惑メール対策、詐欺行為などから保護しながら、ユーザ資産を業界トップの精度で防御・保護します。

Gartner

2年連続でGartnerのOnline Fraud Detection Market Guideに記載される唯一のボット対策ソリューション！

・悪いBOTを排除することによって、Webサイト・セキュリティを強化。
・悪用、誤用、開発者の誤りからAPIをセキュリティ保護。
・正確なウェブ分析と非常に速いロード時間を保証。
・人によるトラフィック、良いBOTのトラフィック、悪いBOTのトラフィックに対する完全な可視性と制御を実現。

SC MAGAZINE

SC 2017 Trust AwardのBest Fraud Prevention Solution部門で受賞
世界で最も成功しているウェブサイトによって信頼されています

Doctor.com　Neiman Marcus　StubHub　B&H　yelp　Sabre

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

ウェブアプリケーション、モバイル、API向けの唯一のプロアクティブで正確なボット軽減ソリューション

● Distil Networksを採用する理由

正確な保護

ファイアウォール、WAF、IDSシステムはこれまで、今日のボットやボットネットを防止し、その量、種類、精巧化を管理するように設計されたことがありませんでした。Distilの相違点は、使いやすさと正確さです。Distilの自己最適化保護は、正規のユーザに影響を与えることなく、悪意のあるボットの99.9%をブロックします。

ユーザ独自の設定を迅速に微調整し、どのようにボットを管理し、サービスを使用するかを完全に制御することができます。

● インラインのHi-Def（ハイデフ）デバイスフィンガープリンティング

各クライアント要求からの情報の200を超える属性を解析します。Hi-Defフィンガープリントは、ボットがランダムなIPアドレスから再接続しようとしたり、匿名プロキシの後ろに隠れようとしたりする場合でも、ボットに張り付きます。

● 既知の違反者データベース

世界最大の既知の違反者データベースからの悪いボットのHi-Defフィンガープリントのリアルタイム更新は、Distilが保護する全てのサイトの集合的なインテリジェンスに基づいています。

更に、サードパーティの詐欺、スパム、マルウェア及びプロキシのリストから得たリアルタイムの脅威インテリジェンスを収集し、それらは全て顧客をリアルタイムで保護するために更新・使用されます。

Distil Networksの「HI-Def（ハイデフ）」フィンガープリント

● 挙動モデル化と機械学習

機械学習アルゴリズムは、サイトの独自のトラフィックパターンに固有の挙動の異常を突き止めます。又、Distilは、多数の動的な分類の相関に基づいて、ボットをプロアクティブに予測します。これは、IPレート制限などの静的ルールに依存するウェブアプリケーションファイアウォールに固有のリアクティブなアプローチとは全く対照的です。

● チャレンジとブラウザ確認

Distilは、ブラウザが完全に自称通りのものであることを確認し、チャレンジと詳細な取り調べを通じて、ブラウザがボットではなく人間によって使用されていることを確認します。SeleniumやPhantomJSのようなブラウザ自動化ツールでも、Distilの検出を逃れることはできません。

● デバイスベースのレート制限

レート制限は、IPアドレスではなく、DistilのHi-Defフィンガープリントに基づいています。予測解析は、1分毎のページ数、セッション毎のページ数、セッション長などのレート制限を上下させたときにトラフィックがどの程度影響を受けるかを示します。

● 汎用アクセスコントロールリスト

Distilの汎用アクセスコントロールリストを使用することによって、ホワイトリストとブラックリストを作成する時間を節約します。ポリシーを迅速に作成し、そのポリシーを特定のドメイン、URL/パス、APIに適用するか、又はアカウント全体にわたって適用します。

● APIセキュリティ

DistilのAPIセキュリティは、APIクライアントを追跡し、許容できる使用を監視して、APIのハイジャック、スクレイピング、悪用に対する自動シールドとして機能します。APIセキュリティは、開発者のミスや統合上のバグに対する保険でもあります。

● Distilのアナリストマネージドサービス

Distilのプロフェッショナルサービスソリューションは、ユーザの代わりにDistil実装の微調整とボット軽減プログラムの管理を行うセキュリティアナリストの専門チームを提供します。これには、リアルタイムの脅威の検出と対応、事後インシデントレポートが含まれており、敵の一歩先を行っていることを保証します。

柔軟な導入オプション

Distil Networksは、柔軟な導入オプションを提供し、現在および将来の統合を妨げない任意のタイプのウェブ環境に導入することを可能にします。

Distilプライベートクラウド

・AWS上での単一テナントのクラウド導入
・Distilによって完全に構成・管理されます

オンプレミスインフラ

・Distilハードウェア、仮想化アプライアンスまたはベアメタルアプライアンス上に容易に導入します
・CDN、ロードバランサ、その他のネットワークインフラとシームレスに統合します
・Distilまでのハートビートを介して、新規の悪いボットのhi-defフィンガープリントを自動的に取得します
・既知の違反者クラウド

● Distil Networksについて

ボットの検出及び軽減のグローバルリーダーであるDistil Networksは、悪いボット、API悪用、詐欺からウェブアプリケーションを保護する、唯一の簡単で正確な方法です。Distilを用いれば、正規のユーザに影響を及ぼすことなく、悪意のあるトラフィックの99.9%を自動的にブロックします。

Distilのウェブセキュリティは、ウェブスクレイピング、ブルートフォース 攻撃、競争上のデータマイニング、アカウント乗っ取り、オンライン詐欺、不正な脆弱性スキャン、スパム、中間者攻撃（MITM）、デジタル広告詐欺、ダウンタイムからウェブサイトを防御します。

DistilのAPIセキュリティは、ウェブブラウザ、モバイルアプリケーション、及びIoT接続デバイスにサービスするAPIを含む、全てのタイプのAPIを保護します。開発者の誤り、統合によるバグ、自動化されたスクレイピング、ウェブ及びモバイルのハイジャックからAPIを防御します。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp