AKAMAI 製品概要

Secure Internet Access ThreatAvert

重要なネットワークアセットを保護し、加入者に影響を与えるマルウェアを特定

サービスプロバイダーは、ネットワークセキュリティが加入者の満足度に直接影響しブランドの資産価値を高めることを認識しています。ある脅威がどう機能するかはほとんど DNS に依存するため、新たな脅威は重要な DNS インフラを特に標的として開発されてきました。すべてが接続された今の世界では脅威がより動的かつ多様になっているため、プロバイダーはネットワークリソースと加入者をいかに保護するかを見直す必要があります。

Akamai Secure Internet Access ThreatAvert は、リアルタイムで DNS ルックアップを評価して、悪性のアクティビティを検知し、阻止します。Secure Internet Access ThreatAvert は、ネットワークの停止や速度低下を引き起こし、加入者の体験に悪影響を及ぼし、他のネットワーク保護を妨害する脅威を阻止します。対象とする脅威は、以下の通りです。

- 大量のクエリーでリゾルバーに過剰な負荷をかける DNS ベースの DDoS
- 重要な個人データを盗む、または顧客のデバイスを侵害するボットマルウェア
- DNS 内に他のプロトコルを持ち込んでサービスを盗む DNS トンネル

Secure Internet Access ThreatAvert は、Akamai の動的な脅威フィード機能を備えた、優れた CacheServe DNS リゾルバーを活用しています。CacheServe は、信頼性では絶対的な基準です。パフォーマンス最適化とソフトウェア強化に長年投資を続け、DNS トラフィックの急増が発生しても、確実に耐障害性と可用性が保証されます。Akamai の脅威インテリジェンスは、日々 1,000 億もの DNS クエリーや世界中からのライブストリーミングを処理する Akamai Data Science チームが開発しています。

DNS セキュリティは DNS サーバーの責任

DNS クエリーは悪性のアクティビティの主要な指標です。それは、（コマンド＆コントロールサーバー、マルウェアのダウンロード、窃盗サイトなど）悪性リソースのアドレス解決が、たいていの悪性アクティビティを可能にする第一段階だからです。DNS リゾルバーは、プロバイダーネットワークのすべてのクエリーを確認できるため、脅威を標的とするインテリジェンスを埋め込むのに最適の場所です。悪性のアクティビティは、受信したクエリーを動的脅威リストのエントリーと照合すると検出できます。

Secure Internet Access ThreatAvert は、データプレーンのトラフィックにあわせて拡張する専用のパケット処理ソリューションよりも、はるかに低いコストと少ない運用作業量で対応でき、ネットワーク影響も受けにくく、DNS コントロールプレーンの拡張性を実現できます。

ビジネス上のメリット

- 軽量なソリューション、何百万人もの加入者に拡張可能、すべてのデバイスに対応
- 最先端のデータ科学に基づき、脅威カバレッジに関する卓越した専門性と範囲を提供
- 継続的に脅威フィードを更新することで、エクスプロイトの変化に応じて保護を維持
- 読みやすいリアルタイムのレポートで、脅威ステータスを一目で分かるように表示し、詳細情報へのリンクも提供
- 脅威およびテレメトリーデータを効率的に収集し、スケーラブルに管理

軽量かつ効率的で、ネットワークトラフィックによるさらなる遅延発生もありません。ネットワークベースであるため、すべてのデバイスに対応し、クライアントとホストにセキュリティソフトウェアをインストール、更新する必要はありません。

脅威カバレッジの優れた正確性、深度、範囲

マルウェア開発者は常に革新を続け、エクスプロイトの投資回収率の最大化に努めています。つまり、ほとんどの脅威は検出を回避するために入念に設計されており、長期間生き残ることができるよう、すばやく変化しています。また、そのアタックサーフェスは IoT（「モノのインターネット」）に接続されている膨大な数の機器にまで拡張されており、攻撃者がその目標の達成に使用する方法はかなり多様化しています。

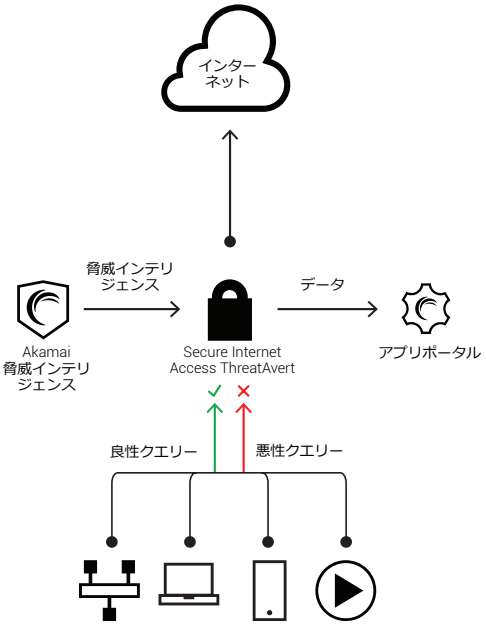
脅威の状況の巧妙さと多様性を認識したうえで、Akamai の Data Science チームは、ライブストリームの DNS クエリーを分析する主要なシステムを開発、実装、統合してきました。プロセスには、レピュテーションリスト、ハニーポット、その他サードパーティーのソースからの脅威データが統合されています。以下の投資を通じて、きわめて多様な範囲と深度の脅威のカバレッジ、正確性、アジリティが実現しています。

- 異常な挙動（DNS ベースの DDoS など）を即時に検出し、個別の脅威を関連付け、ボットの新たなドメイン生成アルゴリズムを特定するアルゴリズム（特許申請中）
- 「正当な」DNS クエリーが常に保護されるように、名前を自動的に許可する高度なテクニック
- セキュリティに関する経験を長年蓄積し、マルウェアや DNS データを深く理解する研究スタッフ
- ライブ・データ・ストリームをリアルタイムで処理する世界中のネットワークとデータセンター

精度ポリシーで悪性のトラフィックをブロックし、良性のトラフィックを保護

Akamai 脅威インテリジェンスフィードに精度ポリシーを組み込んで、不要な DNS トラフィックを管理します。広範で詳細な機能セットにより、きめ細かいフィルタリングが可能になり、悪性のクエリーを標的として、正当なクエリーを保護（回答）します。

- 精度ポリシーは受信クエリーまたは送信する回答に適用できます
- フィルターまたはレート制限は、IP、QTYPE、FQDN、その他多くのクエリーパラメーターに基づいて設定できます
- フィルターまたはレート制限では、複数のクエリーパラメーターとともに以下の論理演算子を使用できます：QTYPE AND FQDN、IP AND FQDN など
- フィルターまたはレート制限は、Akamai 脅威インテリジェンスの動的な脅威リスト、またはオペレーターから提供されたリストと照合できます
- ポリシーおよび脅威リストは次のように組み合わせることができます：「BLOCKLIST と合致、かつ ALLOWLIST にない（MATCH against BLOCKLIST and NOT on ALLOWLIST）」など
- drop、synthesize answer （回答を合成）、answer with truncate（省略して回答）、NXD、NOERROR、など複数のポリシーアクションにより、クエリーの処理の方法が決定されます
- より強力にするために、ポリシーを組み合わせてネストすることもできます



Akamai の専門家により加工された大量のデータストリームにより、インターネット全体の悪性のアクティビティの全体像と限定された地域の攻撃情報の、両方を把握することができます。

精度ポリシーを手動で設定すると、プロバイダーネットワークのローカルの問題に対処できます。

スケーラブルなデータ管理、豊富なテレメトリーとレポート機能

Secure Internet Access ThreatAvert は、世界で最大規模のネットワークで実証されたオープンソリューションに基づいたデータ管理アーキテクチャを組み込んでおり、Web の規模とスピードで優れた運用が実現します。ネットワーク全体の Secure Internet Access ThreatAvert システムからのライブ・ストリーミング・データを集計し、レポート（以下の説明を参照）やその他のシステム向けに利用します。耐障害性に優れたアーキテクチャが中断なく可用性を提供し、ノンストップの顧客体験を実現します。ビッグデータシステム（Splunk、Hadoop）や専用アプリケーションを利用するためのオプションのコネクターを利用すると、運用、セキュリティ、ビジネスに関する知見をさらに引き出すことができます。

Secure Internet Access ThreatAvert のレポート機能では、ブロックされた DNS クエリー、節約されたピーク DNS 帯域幅、ネットワーク内の上位マルウェア、感染した加入者、脅威インテリジェンスの最新情報を、Executive Dashboard 画面に一元表示するため、セキュリティ対策を即座に評価することができます。Security Dashboard を追加すれば、DDoS およびマルウェアの詳細をグラフで表示させることができます。マルウェアおよび感染したクライアントの詳細に関する一連のレイヤーについて、1 クリックで情報を入手できます。それぞれの運用要件にあわせて、カスタムのダッシュボードおよびレポートを数分で作成して、ユーザー定義の形式でセキュリティデータを表示することもできます。タグベースのレポートを活用して、運用スタッフは自社の Secure Internet Access ThreatAvert トポロジーを独自の要件に応じて設定できます。