AKAMAI 製品概要

Secure Internet Access Enterprise クラウドベースの DNS ファイアウォール

組織では、ダイレクト・インターネット・アクセス、Software as a Service（SaaS）アプリケーション、クラウドサービス、テレワークというポリシー、Internet of Things（IoT）の普及に伴いアタックサーフェスが大幅に増加しているため、新たなセキュリティの課題に直面しています。マルウェア、ランサムウェア、フィッシング、データ窃取などの高度な標的型脅威から組織とユーザーを守ることが、これまでとは比べものにならないほど難しくなっています。複雑化したセキュリティ制御ポイントや従来のオンプレミスソリューション間のセキュリティギャップは、限られたリソースで管理する必要があります。

Akamai Secure Internet Access Enterprise は、従来のセキュリティソリューションに伴う複雑さと管理のオーバーヘッドをなくし、ユーザーやデバイスがどこからインターネットに接続しても安全な接続を確保できるようにした、クラウドベースのドメイン・ネーム・システム（DNS）ファイアウォールです。Secure Internet Access Enterprise には、インターネットや DNS トラフィックに関する Akamai の比類のないグローバルな知見に基づいた、リアルタイムの脅威インテリジェンスが搭載されています。

Secure Internet Access Enterprise

グローバルな Akamai Connected Cloud および Akamai のキャリアグレードキャッシュ DNS サービス上に構築されている Secure Internet Access Enterprise は、導入や保守に特別なハードウェアを必要とせず、迅速に設定し簡単に展開できるクラウドベースの DNS ファイアウォールです。

Secure Internet Access Enterprise は、リアルタイムの Akamai Cloud Security Intelligence を活用することで、マルウェア、ランサムウェア、フィッシング詐欺、低スループットの DNS ベースのデータ窃取などの標的型脅威を事前に特定してブロックできます。

セキュリティチームは、Akamai のポータルを使うことにより、インターネット接続場所に関係なく全ユーザーに対して一元的に、セキュリティポリシーおよび利用規定（AUP）を数分で作成、展開、実行できます。

ビジネス上のメリット

- クラウドベースの DNS ファイアウォールを使用して、Web セキュリティをクラウドに移行。クラウドベースの DNS は、数分で（ユーザーの作業を中断することなく）設定し、グローバル展開し、迅速にスケーリングできます
- セキュリティ防御を強化。最新かつ独自の脅威インテリジェンスに基づき、マルウェアやランサムウェアのドロップサイト、フィッシングサイト、マルウェアコマンド＆コントロール（C2）サーバーに対するリクエストを事前にブロックし、低スループットの DNS データ窃取を特定します
- シャドー IT や認可されていないアプリケーションの使用を制御。カテゴリーやリスクスコアに基づいてアプリケーションを特定してブロックします
- セキュリティ管理の時間と複雑さを最小限に。誤検知のセキュリティアラートや他のセキュリティ製品からのアラートを減らし、セキュリティポリシーやアップデートをどこからでも数秒で管理し、すべてのロケーションを保護します

Akamai

仕組み

Secure Internet Access Enterprise は、クラウドベースのセキュリティサービスです。数分でアクティブ化でき、パフォーマンスに影響を及ぼすことなく、最適なセキュリティを提供し、複雑さを軽減します。この保護は、キャッシュ DNS トラフィックを Secure Internet Access Enterprise に送信するだけで実現できます。これには、IPsec トンネル、軽量クライアント、Akamai のマネージド型 DNS フォワーダー、既存の DNS リゾルバーの変更など、さまざまな方法を使用します。

リクエストされたすべてのドメインが Akamai のリアルタイム脅威インテリジェンスと照合され、特定された悪性ドメインへのリクエストは自動的にブロックされます。DNS を最初のセキュリティレイヤーとして使用することで、Web 接続の確立前のキルチェーンの初期段階において、脅威を事前にブロックします。さらに、DNS は、あらゆるポートおよびプロトコルにおいて有効であるよう設計されており、標準の Web ポートやプロトコルを使用しないマルウェアからも保護されます。また、ドメインをチェックすることで、ユーザーがアクセスしようとしているコンテンツの種類を判別し、そのコンテンツが組織の利用規定（AUP）に違反していればブロックすることも可能です。

さらに保護を強化するために、危険なドメインはクラウドプロキシに転送して、URL を検査できます。リクエストされた HTTP/S URL は、Akamai のリアルタイム脅威インテリジェンスと照合され、悪性 URL は自動的にブロックされます。

Secure Internet Access Enterprise は、ファイアウォールやセキュリティ情報およびイベント管理（SIEM）ソリューション、外部の脅威インテリジェンスフィードなど、他のセキュリティ製品やレポートツールと簡単に統合できるので、組織はセキュリティスタックのすべてのレイヤーで投資を最大限に活用できます。

さらに、デバイスに軽量の Secure Internet Access Enterprise クライアントを導入すれば、オフネットワークで使用されるラップトップやモバイルデバイスを迅速かつ簡単に保護できます。

Akamai Cloud Security Intelligence

Secure Internet Access Enterprise には、脅威やそれによってエンタープライズが受けるリスクに関するリアルタイムインテリジェンスを提供する Akamai Cloud Security Intelligence が活用されています。

Akamai の脅威インテリジェンスは、お客様のビジネスに影響を及ぼす可能性のある現在の脅威や関連する脅威に対する防御を提供するとともに、セキュリティチームが調査しなければならないフォールスポジティブ（誤検知）アラートの数を最小限に抑えるように設計されています。

この情報は、世界中の Web トラフィックの 30% 近くを管理し、毎日最大 11 兆件の DNS クエリーを配信している Akamai Connected Cloud から常時収集されるデータに基づいて構築されます。Akamai のインテリジェンスは数百もの外部脅威フィードを活用して強化されており、一元化されたデータセットは高度な行動分析技術や機械学習（ML）、独自のアルゴリズムを用いた継続的な分析・更新などに活用されています。新たな脅威が特定されるとただちに Akamai Secure Internet Access Enterprise に情報を追加し、リアルタイム保護を提供します。

Akamai Connected Cloud

Secure Internet Access Enterprise サービスは、クラウドコンピューティング、セキュリティ、コンテンツデリバリーのための世界で最も分散したプラットフォームである Akamai Connected Cloud 上に構築されています。Akamai Connected Cloud は、世界中に分散されており、100% の可用性を保証するサービスレベル契約（SLA）を提供し、エンタープライズの Web セキュリティにとって最適な信頼性を実現します。

ビジネス上のメリット

- VPN を使用せずに、オフネットワークのデバイスに対するリスクを軽減しセキュリティを強化。軽量の Secure Internet Access Enterprise クライアントを使用して、セキュリティポリシーと利用規定（AUP）の両方を適用します
- コンプライアンスや利用規定（AUP）を迅速かつ一元的に適用。問題がある／不適切なドメインおよびコンテンツカテゴリーへのアクセスをブロックします
- Akamai Connected Cloud と Akamai のキャリアグレード DNS プラットフォームで、耐障害性と信頼性が向上します

クラウドベースの管理ポータル

Secure Internet Access Enterprise の設定やその後の管理はすべて、クラウドベースの Akamai Control Center ポータルから実行するため、いつでもどこにいても管理できます。

ポリシー管理も迅速かつ簡単です。変更内容は数分で世界中にプッシュされ、すべての拠点とユーザーを確実に保護できます。リアルタイムの E メール通知と定期的なレポートを設定すれば、重大なポリシーイベントの発生時にセキュリティチームに知らせることができます。これにより、潜在的な脅威を特定し解決する修復手段を講じることができます。リアルタイムダッシュボードには、トラフィック、脅威、AUP イベントの概要が出力されます。これらアクティビティの詳細情報は、個々のダッシュボード要素をドリルダウンすることで確認できます。こうした詳細情報は、セキュリティインシデントの分析や対処方法に関する貴重なリソースとなります。

すべてのポータル機能に、API でアクセスできます。また、データログを SIEM にエクスポートできるため、ご使用の他のセキュリティソリューションやレポーティングツールと Secure Internet Access Enterprise を、簡単かつ効果的に統合できます。

機能

セキュリティ
マルウェア、ランサムウェア、フィッシングの配信ドメインと URL をブロック
マルウェア C2 リクエストをブロック
DNS ベースのデータ窃盗を特定
リスクの高いドメインをプロキシ経由させ、リクエストされた HTTP および HTTPS URL を検査
HTTP および HTTPS URL 検査用にカスタマイズされたドメインリストの作成
新しく発見された脅威の識別とアラートを目的としたお客様のトラフィックログのルックバック分析を実行
許可／拒否のカスタムリストの作成
追加の脅威インテリジェントフィードの統合
エラーページのカスタマイズ
悪性のドメインおよび URL に関するインテリジェンスの獲得を目的とした Akamai 脅威データベースへのクエリー
オフネットワークのデバイス（Windows、macOS、iOS、Android、Chrome）のセキュリティの強化
利用規定（AUP）
グループベースの AUP ポリシーの作成
オンネットワークおよびオフネットワークのユーザーに関する AUP 違反の監視またはブロック
Google、Bing、YouTube に対するセーフサーチの強化

クラウド・アクセス・セキュリティ・ブローカー（インライン）
シャドー IT アプリケーションの特定とブロック
リスクスコアに基づくアプリケーションまたはアプリケーショングループのブロック
SaaS テナントの実行
レポート、監視、管理
IDP と Active Directory の統合
エンタープライズ全体のすべてのアクティビティをカスタマイズ可能なダッシュボードに表示
すべての脅威および AUP イベントの詳細な分析
オンボーディングされたすべてのトラフィックリクエストおよび脅威イベントと AUP イベントの完全なロギングおよび可視化
すべてのログのログ配信：ログは 30 日間保持され API を通じてエクスポート可能
設定、カスタム・セキュリティ・リスト、およびイベントを API で利用可能
SIEM などの他のセキュリティシステムと API を通じて統合
E メールベースのリアルタイムのセキュリティアラート
日次または週次の E メールレポートのスケジュール設定
管理者の委任
Akamai Connected Cloud プラットフォーム
キャッシュ DNS のお客様別専用 IPv4 および IPv6 VIP
可用性 100% の SLA
最適なパフォーマンスを実現する Anycast DNS ルーティング
DNSSEC、DoH および DoT 実施によるセキュリティの強化
エンタープライズ・デバイス・アトリビューション
DNS フォワーダーを使用するインラインアトリビューション
Security Connector を使用するオフラインアトリビューション
ラップトップおよびモバイルデバイス（Windows、macOS、iOS、Android、Chrome）のクライアントベースのアトリビューション

Secure Internet Access Enterprise の詳細や無料トライアルのお申し込みについては、akamai.com をご覧ください。