ENTERPRISE DEFENDER
エッジでのゼロトラスト・セキュリティ

防御可能なネットワークの境界というものはすでに存在しません。少なくとも認識できる形では、もはや存在しなくなりました。20 年前は有効だったセキュリティやアクセス方法を現在の環境で利用することは、最善な場合でも不完全であり、最悪の場合は非常に危険です。これは単なる理論ではありません。ここ 5 年間で見られたデータ侵害の件数や規模において明確に証明されており、その大部分は境界内部で信頼が悪用された結果起きています。今こそ、ゼロトラスト・セキュリティを導入すべきときです。その前提は、企業ネットワークの信頼性は元から存在せず、セキュリティやアクセスについては識別情報やデバイス、ユーザーの状況に基づいて動的に決定されます。

ENTERPRISE DEFENDER

Akamai Intelligent Edge Platform 上に構築された Enterprise Defender は、適応型のアプリケーションアクセス、セキュリティ、高速化にマルウェア防御を組み合わせ、エッジで簡単に利用できるセキュリティサービスを提供します。Enterprise Defender により、組織はハードウェアや機器を使用せずにゼロトラスト・セキュリティの状態に移行することができます。Enterprise Defender に登録するだけで、リスクや複雑さを軽減できると同時に、ユーザー体験を向上させることができます。

仕組み

Enterprise Defender は、Akamai の Intelligent Edge Platform を利用して、すべてのエンタープライズアプリケーションとエンタープライズユーザーのセキュリティを確保します。これにより、パフォーマンスを低下させることなく最適なセキュリティを提供し、複雑さを軽減することが可能になります。また、管理対象のアプリケーションへの安全なアクセスを提供するとともに、ユーザーが管理対象外のアプリケーションにアクセスする際のリスクを緩和することができます。

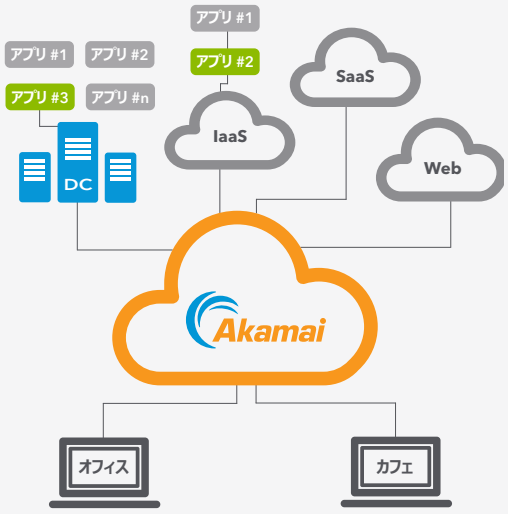
Enterprise Defender には次のような機能があります。これらは、1 ユーザーあたり 1 か月ごとの登録サービスで手軽に利用できます。

マルウェア防止：マルウェア、ランサムウェア、フィッシング、DNS データ窃盗、高度なゼロデイ攻撃など、標的型脅威を事前に特定およびブロックして、緩和します。Akamai はセキュア・インターネット・ゲートウェイ（SIG）を提供します。これによってセキュリティチームは、ユーザーやデバイスがインターネットや管理対象外のアプリケーションに安全に接続できるようにすることが可能になります。従来型のセキュリティ対策のような複雑さはありません。

安全なアプリケーションアクセス：許可されたユーザーやデバイスのみが、企業ネットワーク全体ではなく、必要な社内アプリケーションにアクセスできるようにします。アプリケーションがインターネットや公衆回線から隠されるため、アプリケーションに直接アクセスすることは誰にもできません。Enterprise Defender では、データパスの保護、シングルサインオン、ID、アプリケーションアクセス、管理の可視化と制御が 1 つのサービスに統合されています。

Web Application Firewall（WAF）：極めて大規模で巧妙な DDoS 攻撃およびウェブアプリケーション攻撃から、重要なウェブアプリケーションを幅広く保護します。WAF にはウェブサイト用の堅牢なセキュリティ保護が組み込まれており、組織が常に進化するセキュリティの脅威に対応できるように、業界最高の脅威研究チームによって更新されます。

アプリケーションの高速化：Akamai を利用することで、組織はコストパフォーマンスに配慮しながら、高速で確実、かつ安全なアプリケーションを提供できます。これによってエンタープライズ組織は、インターネット経由でのビジネスアプリケーション配信に伴う課題を克服できます。なぜなら、Akamai Intelligent Edge Platform のなかにアプリケーション配信機能を置くことにより、ユーザー、クラウド、オンプレミスのワークロードに極めて近い場所に配置することが、世界中どこであろうと可能になるからです。



エッジでのアプリケーションのアクセス／高速化／セキュリティの制御

ユーザーを企業ネットワークに入れない

エンタープライズアプリケーションのシングルサインオンと多要素認証

あらゆる場所で悪意のあるドメイン、URL、コンテンツへのアクセスをブロック

ENTERPRISE DEFENDER

ビジネス上のメリット

- **マルウェアの伝播とラテラルムーブメント（横方向の移動）を阻止**
  従来の境界ベースのネットワークでは、セグメント化が欠如し、ネットワークの可視性が乏しいため、マルウェアが深く浸透することがよくあります。Enterprise Defender では、特定のアプリケーションに対するよりきめ細かいアクセスルールと脅威の事前防御を組み合わせることで、マルウェアが伝播しにくく、また攻撃者が他のワークロードへのアクセス権を取得することが難しくなります。

- **複雑さの軽減と運用の合理化**
  Enterprise Defender などのクラウドベースのセキュリティにより、管理費と維持費の高い仮想機器やハードウェア機器を、エッジでのシンプルなセキュリティサービスに置き換えることができます。

- **セキュリティの CapEx と OpEx を両方削減**
  セキュリティの強化はたいていコスト増につながりますが、Enterprise Defender ならご心配は無用です。むしろ、CISO やセキュリティチームは、強化されたセキュリティとクラウドによる簡素化によって、複数の異なるセキュリティ制御を統合し、管理コストを削減することができます。

- **可視性が向上し、セキュリティ侵害の検出にかかる時間が短縮**
  セキュリティ侵害に関連する記事には、「〇 か月間、攻撃者は検出されなかった」、「攻撃者はいったん境界を越えると、ネットワークを自由に動き回ることができた」などの記述がよく見られます。Enterprise Defender では、よりきめ細かいアプリケーション・アクセス・ロギングと DNS ベースのセキュリティ制御を組み合わせることで、可視性が向上し、セキュリティ侵害の検出にかかる時間を短縮できます。

- **社内データの窃盗を阻止**
  データが攻撃者の手に渡ることを許せば、ビジネスに深刻な影響が生じる可能性があります。その影響は、個人データに十分な配慮をしなかったことによる罰金の場合もあれば、知的財産や戦略計画が盗まれたことによる収益損失の場合もあります。Enterprise Defender では、「最小権限」ベースの適応型アクセス制御と DNS ベースの可視性およびセキュリティによって、社内データの窃盗を阻止します。

- **デジタルビジネス変革を実現**
  IT ／セキュリティチームはデジタル変革のパートナーとなることが可能です。境界ベースのセキュリティでは、チームはいつも「おびえている管理人」と言われていました。新しいクラウドサービスや、パートナーまたは顧客モデルをサポートするために、いったん会社の境界内へのアクセスを許可すると、会社のネットワーク全体へのドアを開き、そこへのアクセスを許可することになるからです。これも Enterprise Defender ならご心配は無用です。アクセス権は ID やセキュリティコンテキストに基づいて限られた数のアプリケーションにしか付与されず、ネットワーク全体へのアクセス権が付与されることはありません。さらに、悪意のあるドメイン、URL、コンテンツへのアクセスをブロックすることで、ユーザーがオフィスでも地元の喫茶店でも「どこにいても働ける」今日の企業文化を実現できます。