AKAMAI 製品概要

Akamai Guardicore Access
ZTNA とマイクロセグメンテーションの一体化

可視化と制御を単一のコンソールで実行することで、ゼロトラストをシンプル化し、加速させます

組織は、ランサムウェアを阻止し、コンプライアンス要件を満たし、ハイブリッドワークフォースとクラウドインフラのセキュリティを確保するために、ゼロトラスト・セキュリティの導入を迅速に推進しています。ゼロトラスト・ネットワーク・アクセス（ZTNA）とマイクロセグメンテーションは、ゼロトラスト・アーキテクチャへの移行を進めている企業にとって極めて重要なソリューションです。これらを組み合わせることで、アタックサーフェスを減らし、侵害を食い止め、アクセス制御を強化し、ユーザー体験を向上させることができます。

一体化の力

Akamai Guardicore Access は、セグメンテーションと ZTNA を組み合わせたものであり、単一のエージェントで展開され、単一のコンソールで管理されます。この革新的なアプローチにより、ユーザーからワークロード（垂直方向）、エンドポイントからエンドポイントまたはワークロード（水平方向）までの包括的な可視性を確保し、アイデンティティベースのアプリケーションアクセス制御とエンドポイントのセグメンテーションを一気に実現することができます。これらのテクノロジーを組み合わせることで、企業はネットワーク防御を強化し、リスクを緩和し、規制を順守した安全な環境を促進する、堅牢なセキュリティフレームワークのメリットを得られます。

Akamai Guardicore Platform は、業界をリードするマイクロセグメンテーションと ZTNA を組み合わせた初のセキュリティプラットフォームであり、セキュリティチームによるランサムウェアの防止、規制順守、ハイブリッドワークフォースとクラウドインフラの両方の保護を支援します。

これで組織は、あらゆるタイプの資産とインフラで単一のエージェントと単一のコンソールを使用し、セグメンテーションを実行してアタックサーフェスを最小限に抑えながら、どこからでもハイブリッドワークフォースへのアクセスを容易に管理できるようになります。これは史上初めてのことです。

主な機能

エンドツーエンドの可視性
エンドツーエンドの可視性によってネットワークを完全に把握して、マップとログの両方で表示し、エンドユーザーのアクセスパターンに関する知見を提供します。これは、セグメンテーションと ZTNA を 1 つの製品に統合することによって初めて可能になります。エンドポイントからワークロード、プロセスレベルまでの接続パスを確認できます。ほぼリアルタイムの履歴表示によってフォレンジック分析が容易になり、緩和が高速化されます。

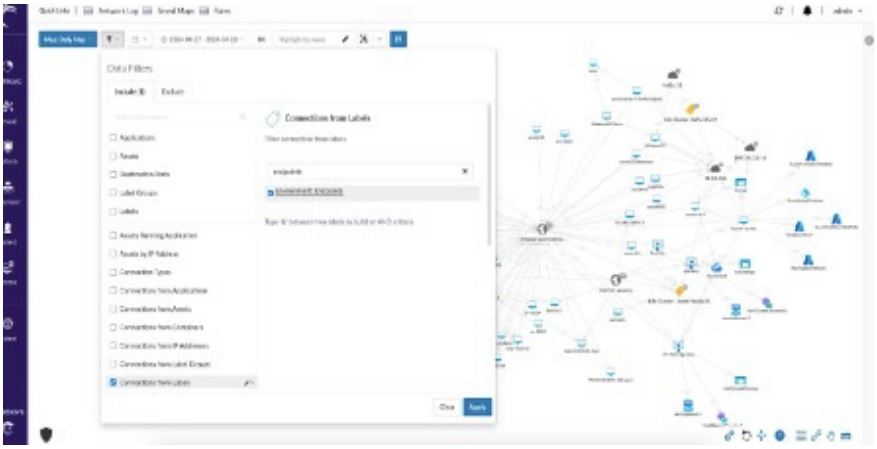
ビジネス上のメリット

単一コンソール、単一エージェント
単一のエージェントと単一のコンソールを使用し、セグメンテーションを実行してアタックサーフェスを最小限に抑えながら、どこからでもハイブリッドワークフォースへのアクセスを容易に管理

幅広い対象範囲
あらゆる場所でアクセス制御を適用し、リモートとオフィス両方で従業員のセキュリティを確保

統一されたポリシー
ゼロトラストを実践する最もシンプルで効果的な手段として、構文やコンソールを変更することなく、水平方向（East／West）のトラフィックと垂直方向（North／South）のアクセスにポリシーを適用

アプリケーション探索
アクセス権限を必要とするアプリケーションを迅速に特定することにより、ポリシーの作成にかかる時間を短縮します。プライベートアプリケーションを簡単に探索して、ユーザーアクセスや頻度などの使用パターンに関する貴重な知見を得ることができます。



アクセス権限を必要とするアプリケーションを簡単に探索

アクセスとセグメンテーションポリシーの同期
アクセス制御とセグメンテーションルールを自動的に同期することで、チーム間の依存関係を減らし、人的ミスの余地を排除します。

主なユースケース

包括的なランサムウェア防御：アイデンティティベースのポリシーやマシンツーマシンのポリシーにより、ランサムウェアやその他のマルウェア攻撃の可能性と影響を低減します。エンドポイントが最小権限でリソースにアクセスするようにすると同時に、きめ細かいアクセス制御を実行します。

- 高価値資産の保護：ユーザーが安全なアクセス制御に基づいて重要な資産にアクセスし、ダイレクト VPN トラフィックをブロックできるようにします
- 特権ユーザーの制限：管理者に安全なアクセスを提供するために、悪用される可能性のある管理ポートへの VPN トラフィックをブロックします

従業員の分散：厳格なアクセス制御を実行し、各デバイスが必要なリソースにのみ接続するようにすることで、あらゆる場所からの業務をサポートします。これにより、アタックサーフェスが最小限に抑えられ、ネットワーク内のラテラルムーブメント（横方向の移動）が減少します。

コンプライアンス：エンドポイント・セグメンテーション・ポリシーを実装することで、企業はエンドポイントを関連する業界標準や規制に準拠させることができます。それにより、コンプライアンス違反に対する罰則のリスクが軽減され、全体的なセキュリティ体制が強化されます。

サードパーティアクセス：業務委託先やパートナーが専用の Akamai ポータルを介してアクセスのルーティングと認証を行うことにより、エージェントをインストールせずに特定のアプリケーションに接続できるようにします。

詳しくは、Akamai ゼロトラスト・セキュリティの Web ページをご覧ください

©2024 Akamai Technologies | サポート | | 公開日：2024 年 10 月