比較ガイド

Akamai Guardicore Segmentation と従来のマイクロセグメンテーションソリューションの比較

比類のない可視性

自社の環境で何が起きているのかを把握するためには、ワークロード間の通信を可視化することが不可欠です。真に効果的な可視化とは、どのような瞬間にも、各ワークロードが何を行っているのかを詳細なコンテキストで把握できることを意味します。また、迅速かつ効果的にポリシーを作成するためには、資産とルールのグループ化機能とフィルタリング機能も必要です。

Akamai

環境全体を簡単に可視化できる

Akamai Guardicore Segmentation のエージェントは、オペレーティングシステムの新旧に関係なく機能する、ホストベースのファイアウォールです。Windows と Linux のいずれについても、個々のプロセスやサービスレベルまで、ネットワークフローを完全に可視化します。また、MacOS のエンドポイントにも対応しています。

圧倒的に豊富なコンテキスト

可視性については、適切なコンテキストと詳細を伴うことが不可欠です。Akamai Guardicore Segmentation は、フローデータに加えて、プロセス情報、ファイル、パッチレベルなど、重要なコンテキストも収集します。

ラベルの種類も数も無制限

Akamai Guardicore Segmentation は、ラベルの数や種類に制限がないので、さまざまなユースケースに柔軟に対応できます。設定管理データベース（CMDB）などのデータソースにある既存のラベルを変換する手間を省くことができます。

AI を活用したラベリング

アプリケーションの検出とラベリングに AI を活用することにより、信頼できる CMDB がなくても、アプリケーションを特定し、適切なラベルを自動で割り当てることができます。

従来のマイクロセグメンテーション

レガシーシステムへの可視性が不十分

Windows 2002 より前の Microsoft Windows システムは把握できません。これは、従来のマイクロセグメンテーションソリューションのエージェントが、2002 年以降のシステムでのみ使用できる Windows ファイアウォールに依存しているためです。Linux システムについては、エージェントは L4 の可視性のみに対応しています。

最小限のコンテキスト

収集するのはフローとマシンに関する情報のみで、プロセスやファイルなどの重要なコンテキスト詳細が欠落しています。そのため、アプリケーションの依存関係を把握するプロセスに手間も時間もかかります。

柔軟性に欠けるラベリング

従来のソリューションでは、多様な環境要件やビジネスニーズにかかわらず、ラベル階層があらかじめ定義され固定されているため、アプリケーションのラベリングに使用できるラベルが限られています。

CMDB がなければお手上げ

ラベリングが手動で、事前設定されたラベル階層に固定されているため、CMDB を使用していない組織では、ラベリングが非常に複雑になります。

Akamai

業界をリードする保護機能

優れたマイクロセグメンテーションソリューションに求められる主な条件の 1 つは、展開場所やアクセス場所（レガシー、最新、Windows、Linux、オンプレミス、仮想、コンテナなど）を問わず、重要な資産を保護できることです。

Akamai

Windows と Linux の完全サポート

Akamai Guardicore Segmentation のエージェントは、新旧を問わず Windows と Linux のすべてのオペレーティングシステムでサポートされ、基盤となるインフラから完全に切り離されています。

コンテナサポートが包括的

コンテナ化された環境を完全に可視化しながら、コンテナ・ネットワーク・インターフェース（CNI）を使用してポリシーを適用できます。

従来のマイクロセグメンテーション

Windows と Linux のサポートは限定的

ポリシーの適用には、Windows 環境では Windows ファイアウォールを、Linux 環境では iptables を使用します。そのため、一部のレガシー Windows OS については保護されず（または保護に制限があり）、Linux 環境については L7 プロセスレベルのルールがありません。

コンテナサポートが限定的

コンテナ環境ではスケーリングできない、iptables と堂々めぐりのポリシー計算に依存しているため、レイテンシーとダウンタイムが生じます。

シンプルなポリシーをすばやく構築

適切なポリシーエンジンを使用すれば、ポリシー言語の制約なく、可能な限り最小のルールで意図を表現できます。また、自動化とウィザードにより、ポリシーの管理作業を最小限に抑制できます。

Akamai

許可と拒否

許可リストと拒否リストのルールに加えて、これらを組み合わせた中間のルールもサポートしています。これにより、セキュリティチームと IR チームは、あらゆるセキュリティシナリオに迅速に対応できます。最初にすべての正当なフローを許可リストに登録する必要はありません。

多様なユースケースに対応可能なポリシーテンプレート

すぐに使えるテンプレートとポリシー構築ワークフローにより、ランサムウェアの緩和、アプリケーションのリングフェンシング、環境セグメンテーションなど、一般的なシナリオに対応できます。これにより、時間を節約して、人的ミスを削減できます。

豊富なポリシー基準

ポリシー基準には、送信元、宛先、ポート、プロトコル、プロセス、サービス（例：一般的にランサムウェアで使用されるタスクスケジューラ）、ユーザー、完全修飾ドメイン名（FQDN）を含めることができます。

従来のマイクロセグメンテーション

許可リストと制限付き拒否ルールをサポート

従来のセグメンテーションソリューションは、安全性が高い一方で時間のかかる許可リストモデルに忠実に従うため、迅速に阻止する必要のある既知の脅威に自動で対応することはできません。

限定的なテンプレートセット

セグメンテーションテンプレートは、主に Microsoft 環境でサポートされています。リングフェンシングやランサムウェアの緩和、修復など、一般的なセグメンテーションユースケースのテンプレートはサポートされていません。

限定的な基準

Linux OS 向けの L7 プロセスレベルポリシーも、個々の Microsoft Windows サービスに基づくポリシー構築機能もありません。

セキュリティファースト

ランサムウェアなどの複雑なセキュリティ脅威に対抗するためには、包括的なセキュリティアプローチが必要です。セグメンテーションは、米国国立標準技術研究所（NIST）およびホワイトハウスにより、基本的な対策として規定されていますが、これに従うためには、セキュリティと侵害検知の総合的なアプローチを採用して組織のセキュリティを維持する必要があります。

Akamai	従来のマイクロセグメンテーション
ランサムウェアの防止と緩和 Akamai Guardicore Segmentation では、防御から封じ込め、緩和に至るまで、攻撃のキルチェーンのすべてのフェーズに対し、すぐに使用できるテンプレートが用意されています。	**ランサムウェアテンプレートがない** 従来のソリューションは、すぐに使用できるテンプレートを使ってランサムウェア攻撃をブロックする機能が不十分です。
エンドポイントに対するクエリーによる脅威検知とコンプライアンス Osquery ベースのツールである Insight を使用すれば、コンプライアンスとマルウェア検知を目的として、サーバーとエンドポイントに対してリアルタイムでクエリーを実行できます。	**リアルタイム検知ができない** 従来のソリューションでは、データセンター内の悪性アクティビティをリアルタイムで検知できません。
ディセプション機能 Akamai Guardicore Segmentation は、特許取得済みのテクノロジーを活用することで、ブロックされたセッションと失敗したセッションを動的ディセプションエンジンにリダイレクトしたうえで、分析と隔離を行います。	**隔離機能がない** 従来のソリューションにはディセプション機能がなく、脅威の痕跡情報（IoC）に基づいてマシンを検知して隔離する機能もありません。
マネージド型脅威ハンティングサービス Akamai が提供するマネージド型脅威ハンティングサービスにより、自社のセキュリティチームの能力を拡大して、最新の脅威に先んじることができます。	**脅威ハンティングサービスがない** 従来のソリューションでは、ランサムウェアやマルウェアの拡大に直面しても、脅威ハンティングサービスを利用できません。
脅威インテリジェンスファイアウォール 既知の悪質なふるまいを防ぐために、Akamai Guardicore Segmentation は自動ファイアウォールルールを使用し、悪性の IP、ファイル、ハッシュをブロックします。	**脅威フィードがない** 脅威フィードに類する機能がない従来のソリューションでは、既知の悪性 IP や URL とのやりとりを停止できません。

パフォーマンスおよびレイテンシーを最適化した運用

低レイテンシーは、セグメンテーションプロジェクトの成功に不可欠な要素です。つまり、レイテンシーを増大させることなく、ルール、アセットごとのラベルなどのポリシーオブジェクトをポリシーに追加できる機能が必要です。

Akamai

レイテンシー最適化エンジン

Akamai のセグメンテーションエンジンは、大規模シナリオ向けに構築されています。最適化されたフィルタリングメカニズムにより、ポリシーのサイズが変化してもレイテンシーの時間には比較的影響しにくい設計です。

従来のマイクロセグメンテーション

ルールが増えるとレイテンシーも増大

ルールの量が増えサイズが拡大すると、レイテンシーも増大します。Linux の iptables は、エンタープライズ規模の水平方向（East/West）のトラフィック向けに構築されたものではありません。そのため、ポリシーのサイズに応じてレイテンシーが増大します。

Akamai Guardicore Segmentation の詳細、 またはパーソナライズされた製品デモのご依頼については、 akamai.com/guardicore をご覧ください。