Akamai

ホワイトペーパー

マイクロセグメンテーション ソリューション選定のための決定版ガイド

今日のアジャイルなビジネス界に最適なソリューションの選定方法

はじめに

今日の IT 環境は複雑さや動的さがさらに増し、マイクロセグメンテーションによる通信フローの分離が不可欠になっています。マイクロセグメンテーションにより、業務においてきめ細かなワークロードベースのセキュリティがもたらされ、比類のないプロセスレベルの可視性が実現します。また、攻撃のリスクが軽減され、IT スタック全体のガバナンスも向上します。

さらに、インフラを完全に把握することで、規制コンプライアンスを実現できる態勢が整い、大きな戦略的価値がもたらされます。これにより、クラウドテクノロジーで安全にイノベーションを起こし、アーキテクチャのあらゆるところに柔軟かつ安全なルールベースのポリシーを組み込むことができるようになります。

マイクロセグメンテーションが普及するにつれ、セキュリティ運用において、ベンダー自体からベンダーが提供するツールやプロセスまで、選択肢も増えていきます。それを詳しく説明していきます。選択する際に考慮すべき重要点とは何で、マイクロセグメンテーションを簡単かつ適切に最大限に活用する上で不可欠なものとは何でしょうか。

このガイドの重点：

- アプリケーションディスカバリーと依存関係マッピングによる可視性
- プラットフォームに依存しないソリューションの確立
- シンプルなポリシー管理とワークフローの設定
- レイヤー 7 の知見を活用したセグメンテーション不足の回避
- 脅威の検知や侵害への対処を盛り込み、セキュリティ体制を強化
- 「100% かゼロか」のマイクロセグメンテーションの落とし穴を回避

アプリケーションディスカバリーと依存関係マッピングによる可視性

マイクロセグメンテーション計画を作成する場合、まず環境を把握する必要があります。これには、利用している環境と、環境内のあらゆる接続や通信をきめ細かく可視化する必要があります。

課題

レガシーファイアウォールや仮想ファイアウォール、または古いマイクロセグメンテーションソリューションでは、プロセスレベルでの可視化が不十分で、コンテキストに応じてデータを確認することができません。詳細なアプリケーションレベルで可視化されないと、アプリケーション、ワークロード、ユーザーのセグメンテーションを特定したりマッピングしたりすることができません。また、認められているふるまいと認められていないふるまいが簡単に見分けられなくなったり、アプリケーションの依存関係を評価できなくなったりし、常に非効率な状態になってしまうでしょう。

さらに、レガシーファイアウォールの機器も複雑で、柔軟性に欠け、高価です。コストも膨大になり、ファイアウォールやハードウェアに対して予めかかる膨大な時間やコストをはじめ、プロジェクト管理、人員、保守にかかるダウンストリームコストにまで及びます。また、実装の時間が長くなることにより、資産の露出が長期化し、まさに現実的なリスクとなります。

従来のネットワークの可視化や手動マッピングも役に立ちません。データ収集や手動マッピングのプロセスでは時間や労力がかかり、求められる詳細レベルに達することはできません。また、今の大規模データセンター環境やハイブリッドクラウド環境では、難易度がさらに上がり、エラーが発生しやすくなっています。さらに、何万ものワークロードや何十万ものアセットがあることを考慮すると、手動マッピングはまさに持続不可能な作業と言えます。

それだけではありません。リアルタイムビューにアクセスできなければ、プロセスレベルの可視化も意味がなくなります。アプリケーションの詳細な静的スナップショットでも、今の環境の動的性質を正確に示すことはできません。

ソリューション

マイクロセグメンテーションソリューションにとって、あらゆる環境およびインフラにおける大規模なアプリケーションの可視化と依存関係マッピングを備えていることは前提条件です。適切なソリューションを使用すれば、マッピングプロセス内でコンテキストが提供されることにより、分析やセグメンテーションがシームレスになり、実装が迅速化し、効率的になります。

アプリケーション内のすべてのコンポーネントのライブマップを使用すると、サービスやポートから通信や基盤のプロセスまで、アーキテクチャの様子をリアルタイムで確認できるようになります。このときに、ソリューションで関連のメタデータをインポートし、資産ラベルを自動生成することができます。

ソリューションで求められるもう 1 つの自動化機能は、リアルタイムのふるまい監視に基づいたセグメンテーションルールを提案し、必要に応じて調整する機能です。このような、きめ細かい可視化と自動化が強力に組み合わさることで、労力のいる作業が軽減されます。また、一部のソリューションでは、事前に作成されたポリシーテンプレートが提供されるため、ランサムウェアの修復など、特定のシナリオに対する個々のルールの作成にかかる時間が短縮されます。セグメンテーションは困難な場合もあるので、セグメンテーションが簡単になるソリューションを探してください。

可視化と自動化の要件：

- リアルタイム、きめ細かいアプリケーション、プロセスレベルのワークロード、ユーザーの可視性
- あらゆる環境やインフラに対する依存関係マッピング
- メタデータに基づいて自動生成された資産ラベル
- リアルタイムのふるまいに基づいて AI が提案するセグメンテーションルール
- 最も一般的なシナリオに基づいて事前に作成されたポリシーテンプレート

プラットフォームに依存しないワークロードマイクロセグメンテーションの確立

マルチクラウド環境やハイブリッド環境を実行している場合、セキュリティ手順はどのプラットフォームからも独立させておくことが重要です。パブリッククラウドとプライベートクラウドのオプションの組み合わせや、SaaS ソリューションを使用するメリットは、ますます増えています。企業では、サーバー、仮想マシン、クラウドテクノロジーの混合使用が増えています。コンテナもその一例です。このようにソリューションが広範になると、セキュリティ対策の責任者や、あらゆる場所のセキュリティ配備を把握するのが困難になる場合があります。

課題

可動性や柔軟性を自動的にスケーリングしたり増強したりできることは、クラウド関連の強力なメリットと言えます。しかし、ネイティブクラウドのセキュリティ制御は限定的です。各クラウドベンダーが独自に提供するネイティブのポイントツールは限定的で、当該のアーキテクチャに特化されるので、個別の問題に対応できない場合があります。一連のクラウドネイティブ・セキュリティ・ツールを管理することに伴い、ポリシーの設定にかかる時間が大幅に増えるという問題が生じることになります。

また、クラウド全体で同時的に発生している事象を把握できなくなります（オンプレミスでの事象は言うまでもありません）。これにより、セキュリティ運用、テキストログ、スナップショットマップにおいてエラーが発生しやくすなり、包括的なセグメンテーションプロジェクトを十分に遂行できなくなります。

動的なポリシー設定は、使用しているクラウドプラットフォームが 1 つしかない場合でも、困難な場合があります。ワークロードがスケールアップまたはスケールダウンしても、セキュリティ制御の更新や修正が適切に行われない場合があります。また、重要なセキュリティ判断の担当者や、アップデートやパッチの担当者を把握するのが困難になる場合があります。アプリケーションレイヤーに可視性がなく、共有セキュリティのモデルを単独使用できないため、盲点が必ず生じてしまうのです。

ソリューション

セキュリティとマイクロセグメンテーションにおいて、プラットフォームに依存しない単一のソリューションを採用することで、レイヤー 7 までの実行を含め、複雑さを大幅に軽減できます。環境にリスクをもたらすことなく、クロスプラットフォームの可能性を活かすことができます。

単一のソリューションを展開して IT スタック全体で機能できるようになると、マイクロセグメンテーションの実装が効率的になるだけではありません。このアプローチにより、複数の異なるセキュリティプロトコルよりもはるかに迅速かつ容易に追跡や管理を行うことができるようになります。また、ゼロトラスト・アーキテクチャやコンプライアンス要件のサポートなど、特定のビジネス目標やセキュリティ要件に適した、ターゲットを絞ったカスタマイズ型の、プラットフォームに依存しないソリューションを提供します。プラットフォームに依存しないソリューションを確立し、ワークロードごとにマイクロセグメンテーションを展開することで、ワークロードがさまざまな動的環境で変化しても、セキュリティプロトコルの整合性や持続性は維持されます。IT セキュリティチームは、複数のポリシーや SLA を管理する必要がなくなります。さらに、問題が発生した場合には、侵害の検知と対応を実施できます。

ソフトウェアベースのセグメンテーションとクラウドネイティブのセキュリティ：選択の基準

- クロスプラットフォームの可視化
- ポリシーの設定にかかる時間の短縮
- セキュリティの強化
- 侵害の検知と対応
- 権限の調整が容易
- きめ細かい制御
- ゼロトラスト・アーキテクチャとコンプライアンスのサポート

シンプルなポリシー管理とワークフローの設定

マイクロセグメンテーションソリューションの成功を左右するのは、ポリシーエンジンです。プロバイダーがシンプルさを維持することが不可欠となります。社内の誰もが、ポリシー設定を把握し、管理できる必要があります。

課題

多くのソリューションには、プロセスの初期段階から完全なセグメンテーション計画の実行まで一貫性のある、シンプルでわかりやすい UI がありません。探しているソリューションが次のものを提供できない場合、注意してください。

- トラフィックへの適用前におけるルールやポリシーのきめ細かな効果。
- 空白ページからマッピングやアプリケーションの依存関係まで、プロセス全体における可視性。これにより、ルール自体を設定したり、アクションのメリットを確認したりすることができるようになります。
- 内蔵型の自動ポリシー提案機能。製品の専門知識を確認したり、プロセスをエンドツーエンドでシームレス化したりすることができます。

ポリシーの作成がどれほど精巧でも、セキュリティを確保できる柔軟性が得られるわけではありません。多くのポイントソリューションが有するルールセットは「許可のみ」で限定的なものです。利用環境に効果的なセキュリティ体制を設定するためには、他のあらゆるルールセットよりも優先される包括的な拒否ルールを適用できる必要があります。これにより、特定のラベルを有するワークロードではインターネットにアクセスできないようにするなど、無許可のアクションを作成することができます。

コンプライアンスや規制評価（PCI、HIPAA、GDPR、PIPEDA など）などの領域で包括的な拒否ルールを適用することで、セキュリティ担当者のワークロードを大幅に簡素化できます。このような「マクロセグメンテーション」ルールを確立すると同時に、同じアプリケーションセグメントのマイクロセグメンテーションで、詳細なポリシーを明示的に作成できる必要もあります。

ソリューション

ソリューションを選択する場合は、セキュリティやビジネスのニーズを満たす柔軟性を備えたソリューションを選択するようにしてください。選択したとおりに環境を確認したり管理したりすることができるようにします。

以下は、マイクロセグメンテーションの選択肢の例です。

- 環境のタイプ（開発、実稼働など）
- 規制の機微性（PCI、HIPAA、GDPR、PIPEDA など）
- アプリケーション（HR、CRM、ドメインコントローラー、課金など）
- 階層や役割（データベース、アプリケーションサーバー、Web サーバーなど）
- プロセス（ホスト、ポートなど）

これが確立されたら、ポリシーエンジンは、変更が発生したときに動的なプロビジョニングや適応を許可する必要があります。ワークフローの自動スケーリングや、サービスの拡張または縮小など、IT 環境は常に変化し、ますます動的になってきています。ポリシーエンジンが適応しないと、マイクロセグメンテーションは実行できません。

ポリシー管理の特徴と機能：

- カスタムコンプライアンスベースのルールを設定できる柔軟性
- ワークフローのスケールアップまたはスケールダウンに応じた動的ラベリング
- ラベルやポリシーを複数のワークロードで共有可能
- セグメンテーションポリシーはブロッキングに転用可能
- ポリシーのブロックが正規のトラフィックに影響しない
- ビジネスクリティカルなプロセスが中断されない
- ポリシーエンジンは、ラテラルムーブメントをプロアクティブに制限できる

お客様の声

Akamai Guardicore Segmentation：
セキュリティの強化、アジリティの向上、コスト削減

ヨーロッパの大手銀行

10,000 個の資産をセグメント化、10 倍の速さ、ダウンタイムはゼロ

> **「[Akamai] は、オンプレミスとクラウド環境全体への厳格なネットワークセグメンテーションの導入をサポートしてくれました。[Akamai を利用すると]、重要なアセットとアプリケーションを効果的に保護することができます」**
>
> **- 情報セキュリティ、バイスプレジデント**

Cogna グループ

2 週間でデータセンターをクラウドに移行

> **「[Akamai のマイクロセグメンテーション] では、認証されたユーザーのみが各サーバーやマシン間の通信チャネルにアクセスできるようにするために、アクセス状況を監視することができます。これは、今日なくてはならないタイプの制御です」**
>
> **- 情報セキュリティマネージャー、Alex Amorim 氏**

The Honey Baked Ham Company

中断することなく、6 週間で 45 個のアプリケーションをセキュリティ保護

> **「[Akamai を利用すると]、実際に誰がどのアプリケーションやサーバーに接続しているのか確認できます。セグメンテーションがより効果的かつ制御しやすくなり、コストも軽減されます。頭を悩ますことはありません」**
>
> **- シニアインフラエンジニア、David E.Stennet 氏**

レイヤー 7 の知見を活用したセグメンテーション不足の回避

適切なソリューションであれば、動的ワークロードを制限しようとするのではなく、単純に最初から安全性を確保するものです。

課題

従来のネットワークセグメンテーションでは、今日の多様なエコシステムに十分に対応できません。旧式のセキュリティ手順では、IT 環境を可能な限りシンプル化することが求められ、未知のリスクを伴う新たな機会は回避が促されます。

ネットワークセグメンテーションでは複雑な環境の管理に重点を置いていますが、マイクロセグメンテーションでは最適なセキュリティを重視します。マイクロセグメンテーションでは、セグメンテーションが可視性や厳格なワークロードに基づくことにより、リスクが常に管理されることになり、セキュリティを損なうことなくアジリティやイノベーションを実現できるようになります。

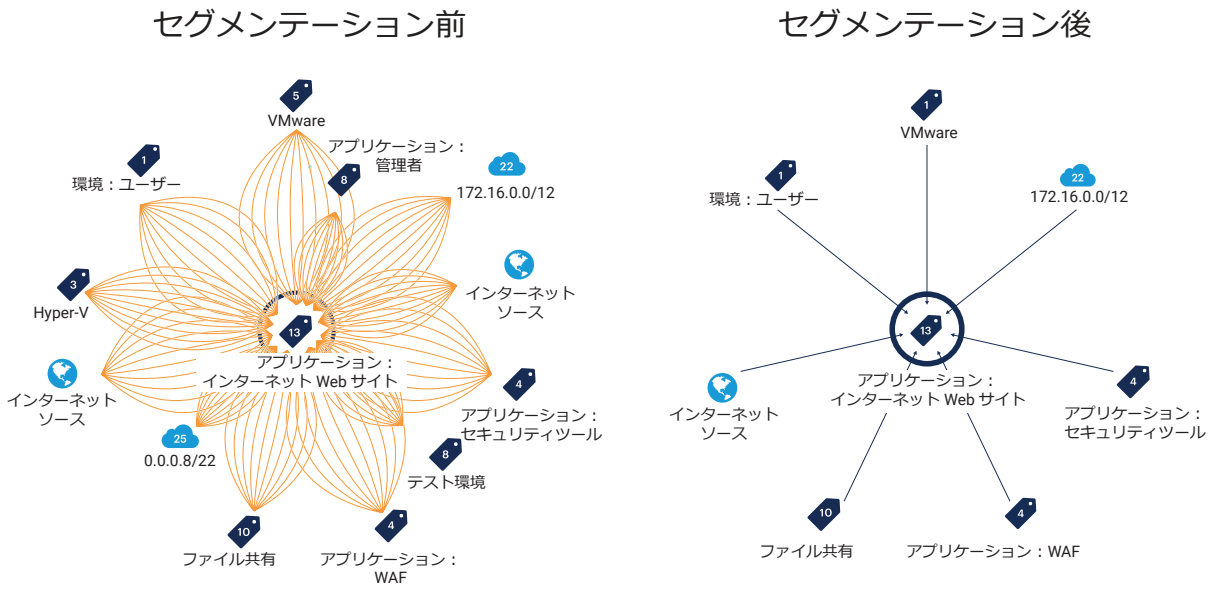
これを実現するためには、業務においてセグメント化が不十分にならないようにする必要があります。つまり、レイヤー 7 までの通信フローを管理することになります。

ポートハイジャックは一般的な脅威となっています。侵害されると、許可されたポートが乗っ取られ、データが流出されることで知られています。レイヤー 4 のアプローチは、トランスポートレイヤーにのみ重点を置いていますが、これでは正面玄関にしか警備員を配備していない銀行と同じです。

これまではそれで十分だったかもしれませんが、攻撃者が境界経由でアクセスしやすくなりつつあります。境界経由でアクセスできると、そこからはどこへでもアクセスできるようになってしまいます。ソリューションによるセグメント化や保護がレイヤー 4 までの場合、アタックサーフェスが制限されません。さまざまなセグメント間で相互作用や通信が行われる中、インフラが動的になるほど、ワークロードが増えるほど、セキュリティにおける脆弱性のリスクがさらに高まります。

ソリューション

マイクロセグメンテーションの強力なアプローチは、境界セキュリティと同様にデータセンターに対しても期待できます。レイヤー 7 のファイアウォール以上の保護が期待できることでしょう。データセンターのアプリケーションレイヤーまでセグメント化や適用を行うことで、オープンポートやプロトコルごとにラテラルムーブメントに対する強力なセキュリティを提供できるようになり、制御不能になる前に攻撃を阻止することができます。また、サーバーやポートだけではなく、すべての OS 上の送信元プロセスと宛先プロセスの両方でトラフィックをブロックまたは許可することができます。



Akamai Guardicore Segmentation、通信を必要最低限に抑えてアタックサーフェスを最大 99% 削減

脅威の検知や侵害への対処を盛り込み、セキュリティ体制を強化

包括的なセキュリティソリューションに含まれる機能としては、マイクロセグメンテーション以上のものである必要があります。たとえば、脅威や侵害が発生したときに記録を取る機能や、大きな損害を被る前にその場で攻撃者を阻止する機能などが挙げられます。

課題

アプリケーションのコンポーネントをセグメント化することで、自動化のメリットが得られます。すなわち、環境への侵害を隔離できるようになります。これにより、脅威が増大したり、ラテラルムーブメントが行われたりする前に、攻撃者を阻止できます。

強力なマイクロセグメンテーションソリューションであれば、これだけにとどまりません。攻撃を最初の時点で阻止する予防策を提供するセキュリティツールと統合することで、さらに多くのことが可能になります。レピュテーション分析を使用すると、侵害を即座に検知できるようになります。脅威対応機能を使用すると、同じセグメント内であっても、リアルタイムで問題を隔離して修正することができます。正規の通信フローに影響を及ぼすこともありません。

ソリューション

適切なマイクロセグメンテーションソリューションは、ある領域への侵害を阻止するだけではありません。その場で侵害を阻止できるだけでなく、組織全体のために水面下でセキュリティ体制を強化できる最高の立場に前もって立てるようになります。

マイクロセグメンテーションソリューションに強力なセキュリティツールを組み込むには、ソリューションが複数の攻撃ベクトルからのデータにアクセスし、ポリシーの違反や異常をリアルタイムで評価できる必要があります。さらに、侵害の試行や成功を検知し、アラートを通知しなければなりません。また、侵害されたアセットを起動ポイントにしてラテラルムーブメントを行うあらゆる試行を積極的にブロックできなければなりません。

無許可の通信やあらゆるタイプの非準拠トラフィックは、速やかに検知できる必要があります。これにより、封じ込めや分析を行って調査プロセスを迅速化し、データを活用して今後の侵害を防止することができるようになります。

侵害の検知機能と分析機能で明らかになること：

- 非準拠トラフィック
- 不正な通信
- 侵害のブロックまたは試行
- 侵害された資産
- ユーザー認証情報
- 攻撃方法
- 侵入者の拡散戦術

「100% かゼロか」のセグメンテーションの落とし穴を回避する

マイクロセグメンテーションへの取り組みは、苦労を重ねながら行うようなものである必要はなく、会社にとって革命的なものである必要もありません。実際には、段階的にゆっくりと進めていくのが最も効果的です。ステップバイステップでサポートしてくれるプロバイダーを見つけてください。

1. **適切な会社なら、可視化から始まる実装計画を作成するはずです。**そのようにすることで、ニーズを明確に把握してから、作成が必要なルールやセグメンテーションのポリシーについて検討できるようになります。この段階で、あらゆるプラットフォームやワークロードにおけるネットワークフローやオーケストレーションの詳細情報など、IT アーキテクチャを詳細に把握できるようになります。それが、オンプレミス、ハイブリッド、クラウドの各環境におけるアプリケーション間の関係性がわかるビジュアルマップです。

2. **次に、重要な資産を特定します。これらは一般的に高リスクまたは高価値のインフラとなります。**ワークフロー作成に固有のシンプルさを取り入れ、レイヤー 7 までの適用など、独自の環境に合わせた柔軟性のあるポリシーを構築します。1 つのポリシーでセキュリティ境界を大幅に縮小できるなど、アプローチのメリットは、まずは個々のアプリケーションのマイクロセグメンテーションで実感できるでしょう。

3. **マイクロセグメント化する領域やアプリケーションが徐々に増えていくと、組織全体にメリットが広がっていくことがわかります。**包括的な一体型ソリューションでは、基本となる侵害検知機能や解決機能を必ず利用してください。

全面的にマイクロセグメンテーションを検討

マイクロセグメンテーションのメリットはシンプルさと簡単さですが、プロセスを始めるのが困難な場合があります。優れた実績を持つ企業の専門知識を活かし、市場で最も優れたツールやサービスも利用して、実装を成功させましょう。

適切なマイクロセグメンテーションソリューションの実装は、可視化やマッピングから始まり、セグメンテーションのワークフローやポリシーの構築を経て、侵害の検知や対応に至る、段階的なプロセスであることを忘れないでください。脅威をリアルタイムで隔離し、検知し、解決するプロセスをコスト効率よくシンプル化して、セキュリティ体制を全面的に強化するなら、今がそのときです。

Akamai Guardicore Segmentation で最も重要なものを保護

その他の詳細については、akamai.com/guardicore をご覧ください。

Akamai は、お客様が生み出すもの全てにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティポスチャの適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 5 月。