Akamai

マイクロセグメンテーションに関する7つの誤解を払拭

規模を拡大する際に小さく考えるのは直感に反するように思われるかもしれませんが、現代のマイクロセグメンテーションソリューションには多くの誤解があります。

ネットワークのダウンタイムが発生するのでは、あるいは、ソフトウェア定義ソリューションの運用が困難になるのではと思っていませんか？もう一度考えてみてください。きめ細かくすることがなぜ重要なのかをご説明します。

誤解 1

使用中の EDR ソリューションでランサムウェア攻撃を十分阻止できる

エンドポイントの検知および応答（EDR）とセグメンテーションはどちらも、ランサムウェア攻撃に対処するためのものですが、キルチェーンの段階と対処法が異なります。EDR ソリューションは、監視対象のデバイスまたはエンドポイントで稼働または実行されているランサムウェアを検知することを目的としています。ランサムウェアが検知されると、EDR はそのプロセスを遮断してデバイスを隔離し、場合によっては発生した暗号化をロールバックします。EDR とセグメンテーションは相補的です。EDR がランサムウェアを検知しなかった場合、セグメンテーションソリューションが、ネットワークをサイロ化されたバケットに分割し、攻撃のラテラルムーブメント（横方向の移動）を制限します。ランサムウェア攻撃を成功させるには、ラテラルムーブメントが不可欠です。セグメンテーションにより、攻撃がエンドポイントを越えて進んでも最終的に障害にぶつかるため、初期感染の被害範囲が制限されます。EDR とセグメンテーションの違いについて詳しくは、こちらをご覧ください。

攻撃者が最初の足がかりを獲得してからネットワーク内でラテラルムーブメント（横方向の移動）を開始するまでの平均時間は

1 時間 42 分

（Microsoft Digital Defense Report 2022）

誤解 2

すでにセグメンテーションを行っている

セグメンテーションは新しい概念ではありませんが、ますます高度になっています。企業は数十年にわたり、VLAN、内部ファイアウォール、ACL、セキュリティグループのパッチワークで、環境をセグメント化してきました。しかし、こうした従来の手法は、最新のハイブリッド・マルチクラウド・インフラの複雑な要求に対応するように進化しておらず、セグメンテーションが不十分のため、防御のギャップや盲点が生じています。

たとえば、従来のファイアウォールはワークフローの依存関係をマッピングしたり評価したりしないため、アプリケーション、ワークロード、またはユーザーに適したセグメンテーションを特定することが困難です。そのため、過度に寛容で広範なセグメンテーションポリシーを実装せざるを得ず、容易に（そしてすぐに）トラブルシューティングの難しい危険な誤設定に陥るおそれがあります。

マイクロセグメンテーションを利用すれば、従来のセグメンテーションツールで可能な範囲をはるかに超えた、レイヤー 7 までのセグメント化と適用が可能になります。

3 年以内に

200 万ドル

のファイアウォールアップグレード費用を削減

（Forrester TEI）

誤解 3

マイクロセグメンテーションは非常に難しく、運用などできない

現代のマイクロセグメンテーションは、エンタープライズ環境に対応する準備がかつてないほど整っています。

Akamai Guardicore Segmentation を利用すれば、データセンターやクラウドから、コンテナベースの資産まで、あらゆる環境でのセグメンテーション、可視化、ポリシー作成、適用に対応する単一のソフトウェアベースソリューションを使用して、運用効率を最大限に高めることができます。導入後、Akamai Guardicore Segmentation は IT インフラ全体の動的なビジュアルマップを作成します。これによりセキュリティチームは、アクティビティを個々のプロセスレベル（リアルタイムと履歴の両方）まで閲覧できます。

さらに、アプリケーションのふるまいに関するこのような詳細な知見を使用し、直感的なビジュアルインターフェースで、きめ細かいマイクロセグメンテーションポリシーを短時間で作成できます。グローバルな拒否ルール、重要なアプリケーションリングフェンシング、大規模な環境を即座にセグメント化する機能により、短期間で価値を実現し、リスクを軽減できます。

従来のセグメンテーション方法は可視性に欠けるため、どこから始めればよいかを把握できません。

SecOps の生産性が

↑95%

向上

（Forrester TEI）

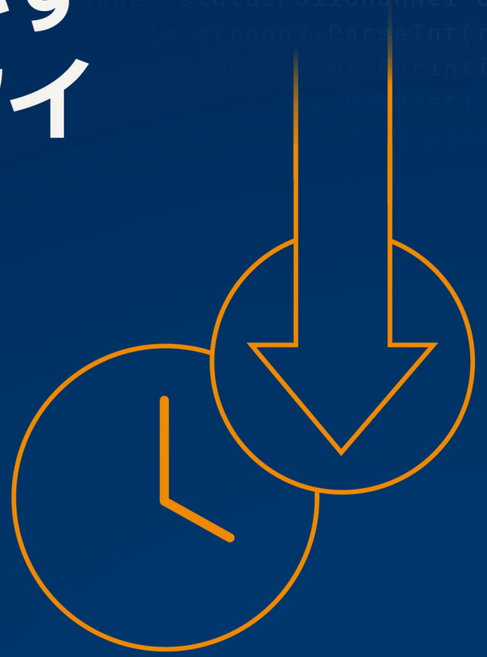
誤解 4

マイクロセグメンテーションを利用すると必ずアプリケーションとネットワークのダウンタイムが発生する

従来のセグメンテーションアプローチでは、サブネット間または VLAN 間でアプリケーションが動かされることが少なくないため、ダウンタイムが発生し、事業継続性が阻害されます。ネットワークエンジニアとファイアウォール管理者は、ダウンタイムのスケジュール、変更管理、またはメンテナンス時間を計画しなければならず、新しいサービスの展開やアプリケーションの更新にかかる時間が増えます。さらに悪いことに、これらの遅延によって、資産への攻撃や脆弱性が生じてリスクが高まるおそれがあります。

一方、ソフトウェア定義セグメンテーションは、基盤となるインフラやオペレーティングシステムとセキュリティを分離するため、ネットワークやアプリケーションに触れることなく、個別にセグメンテーションを実行できます。イベントが発生した場合、影響を受けたマシンを完全に隔離するのではなく、攻撃ベクトルのみをブロックし、ビジネスへの悪影響を抑えます。

また、マイクロセグメンテーションをアラートモードで展開して、ダウンタイムのリスクなしに、稼働中の本番環境でポリシーをテストすることもできます。現代のセグメンテーションソリューションは、セキュリティの向上かビジネスアジリティの向上かの二者択一とは限らないのです。



誤解 5

マイクロセグメンテーションは自社の IoT 環境や OT 環境に対応していない

ゼロトラストポリシーは、ホストベースのセキュリティソフトウェアを実行できない IoT デバイスや OT デバイスに適用できることをご存知ですか？

Akamai のエージェントレスセグメンテーション機能は、エージェントを実行できないデバイス間の防御のギャップを埋めることで、可視性の盲点（エアギャップされたエンドポイントなど）をなくします。このように範囲を拡大することは、ネットワークに接続された（脆弱性のある）多くの IoT デバイスとレガシー OT システムを使用するヘルスケア環境、小売環境、製造環境で特に重要です。エージェントレスのセグメンテーションをネットワークインフラに統合することで、新しいデバイスの自動検出、フィンガープリント、ポリシー適用が可能になり、ゼロトラストの実現に向けた全社的な取り組みを加速させつつリスクを緩和できます。

誤解 6

マイクロセグメンテーションエージェントによってレイテンシーが大幅に増加する

マイクロセグメンテーションに関する大きな誤解の 1 つは、レイテンシーの増加です。

実際には、すべてのトラフィックが特定のファイアウォールチョークポイントを通過するようにするのではなく、分散型でソフトウェアベースのセグメンテーションポリシーを使用することで、ネットワークのボトルネックが解消されます。設計上、Akamai Guardicore エージェントは、Linux、Unix、Windows OS、MacOS で動作するように高度に最適化されており、リソースを大量に消費することはありません。

また、このエージェントはインラインではないため、レイテンシーを増加させるおそれのある、詳細なパケット調査は実行しません。

その代わりに、パケットヘッダーから最小限の情報を取得して、お客様の環境を詳細に把握します。スピードとパフォーマンスを求めているのなら、その両方を手に入れることができます。

誤解 7

マイクロセグメンテーションは、得難いフルタイム従業員を雇用することと同義

CISO は、「より少ないリソースでより多くの成果を出さなければならない」というプレッシャーを感じているため、セキュリティソリューションは、乏しい内部リソースをさらに消費することなく、防御者の負担を軽減する必要があります。

ファイアウォールや VLAN の管理などの従来のセグメンテーション手法では、面倒なマルチステッププロセスが必要です。多くのチームが関与し、スイッチング、ルーティング、ファイアウォールの実装、セキュリティポリシーの作成を個別に担当します。従来のファイアウォールの実装には、平均 14～22 週間かかります。これらすべてによってプロジェクトが長期化し、企業は多大な人件費と運用コストを負担することとなります。

対照的に、Akamai のソフトウェア定義ソリューションの展開にかかる期間は平均 2 週間で、フルタイム従業員 1 人だけでできます。さらに、Akamai のマネージド脅威ハンティングサービス、Akamai Hunt を追加すれば、新たな攻撃、ラテラルムーブメント（横方向の移動）、異常な攻撃動作がないか環境を監視し、時間とリソースを節約できます。

最近では、サイバー人材の雇用は困難であり、つなぎ止めは、ますます困難になっています。今こそ、自社の負担になる防御ではなく、自社のためになる防御を実現するときです。

重要な統計データ

106%

12 か月かからずに最大 106% の ROI を達成

（Forrester TEI）

Akamai の役割

Akamai Guardicore Segmentation は、ソフトウェアベースのマイクロセグメンテーションソリューションです。非常にシンプルで高速かつ直感的な方法で、ゼロトラストの原則を適用できます。このソリューションは、正確なセグメンテーションポリシー、IT 環境内のアクティビティの視覚化、ネットワーク・セキュリティ・アラートによって、ネットワーク内の悪性のラテラルムーブメント（横方向の移動）を防止します。Akamai Guardicore Segmentation は、データセンター、マルチクラウド環境、エンドポイント全体で機能します。インフラセグメンテーションのアプローチよりも短期間で展開でき、ネットワークの可視性と制御性が大幅に向上します。

Akamai Guardicore Segmentation によって、きめ細かい保護、詳細な可視性、セキュリティポリシーの一貫した適用を大規模に実現し、非常に機微な情報を保護する方法をご説明します。