Akamai

ホワイトペーパー

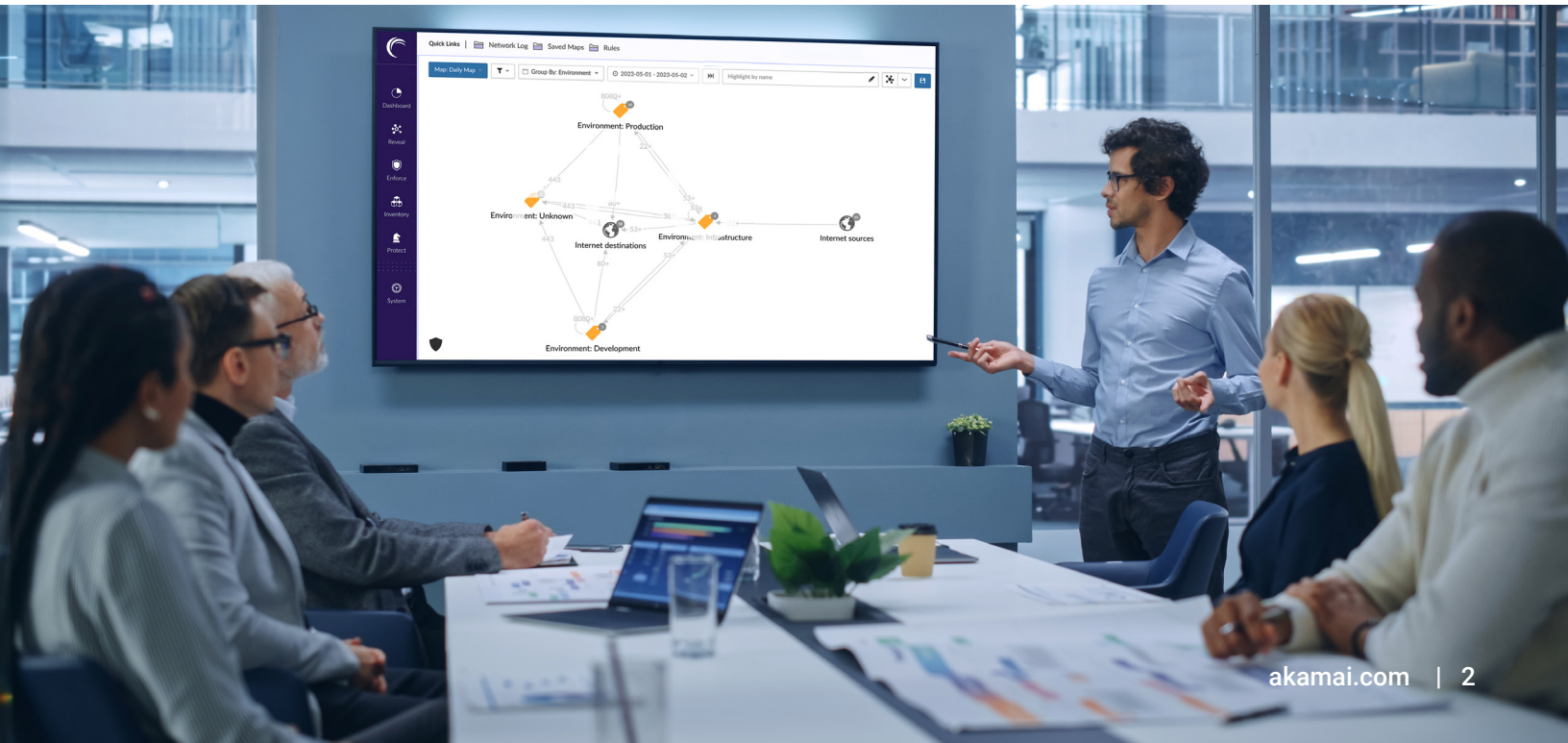
データセンター事業者向けのソフトウェア定義セグメンテーション

マルチテナントデータセンター事業者にとって、コンピューティング環境のセグメンテーションは、単に重要であるだけでなく、必要不可欠な運用モデルです。まず、自社のインフラをクライアントの環境から切り離し、特定のリソースを共有しながら、その他のリソースへのアクセスを防止する必要があります。次に、偶然か意図的かを問わず、各顧客環境での「二次汚染」を防止する必要があります。そのためには、ある顧客の環境でセキュリティ侵害やマルウェア感染が発生した場合に、それが他の顧客の環境に広がるのを防がなければなりません。最後に、所有する運用アプリケーションを適切に分離して、セキュリティ侵害の影響を制限する必要があります。データセンタープロバイダーの運用ネットワークに目を向けると、効率的にセグメンテーションを導入すれば、セキュリティ体制を大幅に強化しコストを削減できるシナリオが、3 つあります。

1. **運用ネットワークの分離**：運用ネットワーク（DCIM、BMS など）をエンタープライズネットワーク（請求システムなどのプロバイダーの社内システム）および顧客ネットワークから分離します。

2. **運用ネットワーク内でのラテラルムーブメント（横方向の移動）リスクの抑制**：運用ネットワーク内にはパッチを適用しにくいシステムが多数あるため、適切にセグメント化しなければリスクが生じます。

3. **顧客向けネットワーク間の効率的かつ安全な接続の確立**：カスタムポータルが配置されている DMZ などは、運用ネットワークからのデータ（例：電源ステータスを読み取るため）やエンタープライズネットワークからのデータ（例：請求情報を読み取るため）に安全にアクセスできる必要があります。



このような接続は現在、非常に複雑で、実装に時間がかかり、効率性の低いネットワーク構成、VLAN、中間ネットワークなどを通じて処理されています。複雑なネットワーク設定が不要のソフトウェア定義ソリューションを導入することで、コストを大幅に削減するとともに、より厳密かつ堅牢に接続を制御することもできます。

さらに、顧客は（ホスト型またはオンプレミス）アプリケーションに強力なセグメンテーションを実装し、それを維持することに苦労しています。そこで、データセンター事業者は、セグメンテーションに関する専門知識、ツール、運用モデルを活用して、顧客にマネージドサービスを提供することで、セグメンテーション業務を中心とする非常に魅力的な収益源を創出できます。さらに、適切な方法、ツール、プロセスを通じて、セキュリティポリシーを顧客の環境に拡張することで、データセンター事業者は非ホスト型アプリケーションに対するアクセスと可視性を獲得できます。これにより、ホスト型データセンターへの安全な移行を促進できるため、中核事業にもつながります。

Equifax：最悪のシナリオ

環境のセグメンテーションをまったく実施していなかったり、不十分だったりした場合の「最悪のシナリオ」とはどのようなものでしょうか？その最たる例は、大きなニュースにもなった、2017 年に Equifax で発生したセキュリティ侵害事件です。このセキュリティ侵害により、米国の 1 億 4,300 万人の個人情報が漏えいしました。米国会計検査院（GAO）の調査によると、攻撃者はまず、Apache Struts Web フレームワークの脆弱性（CVE-2017-5638）を悪用して、大手信用情報会社 Equifax の顧客紛争解決ポータルに侵入しました。侵入後、攻撃者は 76 日間にわたって同社のシステム内を自由に動き回りました。攻撃者が自由にラテラルムーブメントを行えたのは、Equifax がセグメンテーションを実施しておらず、攻撃者は簡単にデータベースにアクセスでき、アタックサーフェスがほぼ無制限にあったためだと GAO は報告しています。

問題は、どうすればこのようなセグメンテーションを最も効果的、効率的、経済的に達成できるかです。データセンター事業者はこれまで、従来型のファイアウォールや VLAN を使用して、マルチテナント／マルチユーザーアーキテクチャ内の環境を分離してきました。しかし、このような方法でセグメンテーションを実施および維持するのは非常に大変で、多くの手作業を必要とし、時間とコストがかかります。さらに、ファイアウォールや VLAN は完璧とはほど遠く、大きなアタックサーフェスが残るおそれもあります。データセンターを防御するのに境界防御ソリューションでは不十分です。データセンターには、さまざまな仮想マシン、ハイパーバイザー、コンテナ、クラウドコンポーネントがあり、ワークロードのスピンアップ／スピンダウンが自動的かつ動的に行われているためです。また、VLAN を使用したセグメンテーションではアプリケーションのダウンタイムが発生しますが、重要な運用管理においてはこのようなダウンタイムは許されません。

以上のような理由から、共有環境を提供する事業者は、最新のソフトウェア定義セグメンテーション手法（マイクロセグメンテーションなど）に注目しています。テクノロジーの進歩により、マイクロセグメンテーションはあらゆるタイプの企業にとって有効な選択肢となっているだけでなく、ゼロトラスト・セキュリティ・モデルを実現するための最適な選択肢となっています。また、適切なツールと周到な計画さえあれば、マイクロセグメンテーションは前述の手法（VLAN など）よりも迅速かつ容易に実装でき、管理と保守も容易に行えます。実際、最近実施されたテストによると、マイクロセグメンテーションは従来のファイアウォールと比較して、1/30 の時間で導入できます。さらに、ソフトウェア定義セグメンテーションには、ネットワークの変更が不要で、アプリケーションのダウンタイムが発生しないというメリットもあります。このような時間短縮と効率化は、導入ライフサイクル全体における大幅なコスト削減につながります。

従来の手法の落とし穴

ソフトウェア定義セグメンテーションやマイクロセグメンテーションのメリットを理解するためには、オンプレミスとクラウドで使用される標準的な手法の欠点や制限に注目して、比較するのが有効です。標準的な手法とは、物理ファイアウォール、仮想ファイアウォール、ネットワーク設定（VLANなど）を組み合わせたものです。一般に、これらの手法は多大なリソースと労力を必要とします。セキュリティポリシーの作成に手間がかかります。追加や変更を手動で行う必要があるため、運用効率が低下し、脆弱性のリスクが上昇します。

特に、内部ファイアウォールは入手するのに高コストが発生し、セットアップが複雑です。また、従来の手法は通常のトラフィックフローの妨げとなり、パターンに変更をもたらし、回りくどい「ヘアピン」を発生させるため、システムパフォーマンスの低下につながります。ファイアウォールはデータセンターのセグメンテーションには不向きだという考えが業界では一般的となっており、使用すべきでないと断言するデータセンタープロバイダーもいます。

稼働中の本番環境にセグメンテーションを導入する際の最大の課題の 1 つは、従来の手法ではアプリケーションのダウンタイムが発生することです。ダウンタイムはコストにつながります。ダウンタイムは通常、限られた時間内でのみ許されるか、または一切許されません。

もう 1 つの課題は、内部セグメンテーションを実施するためには、水平方向（East/West）のアプリケーションの依存関係を十分に把握しなければならないことです。しかし、ほとんどの組織はこのような依存関係を把握していません。アプリケーションの依存関係を容易にマッピングする方法がなければ、ブラウンフィールド環境の分離は非常に困難かつ高リスクです。

ソフトウェア定義セグメンテーションが有効な理由

運用効率とセキュリティ体制の向上：ソフトウェア定義セグメンテーションなら、従来の手法に内在する非効率性を克服できるだけでなく、マルチユーザー環境のセキュリティを強化できます。ソフトウェア定義セグメンテーションでは、その名が示すとおり、インフラを変更することなく、ネットワークをセグメント化できます。ハイブリッドデータセンターでのアプリケーションの配置先を問わず、個々のアプリケーションまたは論理的にグループ化されたアプリケーションに関するセキュリティポリシーを作成できます。これらのポリシーにより、相互に通信できるアプリケーションと通信できないアプリケーションを規定して、真のゼロトラストを実現できます。

手動での変更もダウンタイムもなし：ソフトウェア定義セグメンテーションでは、ネットワークの変更や VLAN の作成は一切不要のため、運用コストを大幅に削減できます。また、新しい VLAN に移行する場合はアプリケーションのダウンタイムや変更が発生しますが、これらも一切発生しません。これは非常に重要です。ダウンタイムが高コストにつながったり、ダウンタイムが一切許されないアプリケーションを保護するためには、ソフトウェア定義セグメンテーションが唯一の選択肢です。

広範な可視性：水平方向（East/West）のトラフィックセグメンテーションの課題を解決することを念頭に構築された高度なソフトウェア定義セグメンテーションソリューションには、可視化ツールが統合されています。このツールにより、セグメントの境界やアプリケーションの依存関係を把握できます。これにより、プロセスを効率化して、ポリシー作成時の運用ミスを回避できます。

ポリシーと制御の自動化：ソフトウェア定義セグメンテーションではポリシーを動的に適用することもできます。ワークロードをスピンアップ／スピンダウンすると、自動的に適切なポリシーに割り当てられます。移動、追加、変更を手動で行う必要がないため、リソースを大幅に節約できます。

インフラに依存しない：ソフトウェア定義セグメンテーションの主なメリットは、インフラに依存しないことです。1 つのツール、1 つの画面、1 つのワークフローを通じて、あらゆるインフラ（ベアメタル、仮想、PaaS、クラウド、コンテナなど）を可視化およびセグメント化できます。これにより、運用上の自由度が大幅に高まり、基盤となるインフラにかかわらず、何の制約もなくセキュリティ基準を達成できます。

収益の増加、関係の維持：ソフトウェア定義セグメンテーションによってデータセンター事業者に大きな機会がもたらされる点が最も重要です。内部セグメンテーションを実施して管理するだけでなく、トレーニング、ツール、プロセスを活用して、要望の高いマネージドサービスを顧客に提供できます。1 つのツール、1 つの画面を通じて、ホスト型アプリケーションだけでなく、顧客の環境やクラウドにあるアプリケーションのセグメンテーションも管理できます。これにより、収益が増加するだけでなく、データセンター事業者の重要度が増すことになるため、より長期的な関係を維持して、利益率を高めることができます。

Akamai を選ぶ理由

上記のメリットを実現するためには、いくつかの必須条件を満たすソフトウェア定義セグメンテーションソリューションが必要です。コンピューティング環境で実行中のすべてのアプリケーションをプロセスレベルで詳細に可視化し、アプリケーション間のすべてのデータフローをマッピングする機能を備えている必要があります。ソフトウェア定義セグメンテーションを効率的に導入および管理するためには、資産に適切なラベルを柔軟に付けてポリシーを作成し、ワークロードの自動拡張に応じてラベルを自動修正できなければなりません。また、プラットフォームやインフラに依存しないソリューションが必要です。各環境のアプリケーションに対して、一貫してポリシーを適用できるソリューションも求められます。そして、ポリシーの作成、管理、適用を自動的またはシンプルに行えるソリューションが必要です。

これらの条件すべてを満たしているのは、Akamai Guardicore Segmentation だけです。ソフトウェア定義セグメンテーションは Akamai の中核となる機能です。Akamai Guardicore Segmentation により、ベアメタル、仮想マシン、パブリッククラウド、コンテナ、IoT デバイスなど、環境内のすべての資産とその依存関係をかつてないレベルで視覚化できます。この詳細な可視性により、アプリケーションのマイクロセグメンテーションに関するセキュリティポリシーを特定、グループ化、作成するためのプロセスを大幅に高速化できます。

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