Akamai

ホワイトペーパー

ファイアウォールの再考

ソフトウェアベースのセグメンテーションの経済的なメリットを示す魅力的な事例

エグゼクティブサマリー

内部ネットワークのセグメンテーションを行うのに、ネットワークおよびセキュリティチームはなぜいまだにレガシーファイアウォールを使用しているのでしょうか。ポリシーで保護されたアプリケーションやセグメントが急増し、物理ファイアウォールアプライアンスでは、今日の動的なハイブリッドクラウド環境のセキュリティ上の課題に対応するには複雑すぎて柔軟性に乏しく、非効率的であることがわかってきました。また、チームが考えているよりも大きなコストがかかります。ファイアウォールとハードウェアの膨大な設備投資コストに加えて、プロジェクト管理、人件費、メンテナンスなどのコストが下流で多く発生するほか、導入に時間がかかるために資産がリスクにさらされる時間が長くなり、そのリスク自体も無視できないものとなります。今日のエンタープライズ組織がアジャイルな DevOps、迅速なアプリケーション展開、クラウドのメリットを享受するためには、セグメンテーションによって重要な資産を保護するためのより優れた方法が必要となります。その方法が、ソフトウェアベースのセグメンテーションです。ソフトウェアベースのセグメンテーションは従来の方法よりも、簡単かつ迅速、効果的に展開でき、このホワイトペーパーで示すように、はるかに低い総所有コストで最適なセキュリティを実現します。

はじめに

現在、ネットワークおよび個々の資産をよりきめ細かくセグメント化する方法が求められていますが、その背景には 3 つの大きな流れが存在しています。1 つ目として、アジャイルな DevOps やその他の迅速なデリバリーモデルでは、本番環境へのアプリケーションの短時間での展開が重視されています。これには必然的に、より正確なポリシーを使用して、より安全なゾーンを作成する必要があります。2 つ目は、組織がクラウドへと移行し、ハイブリッド IT インフラを導入するようになり、アプリケーションが異なる環境間で移行されることが増え、ネットワーク全体でセグメントの垣根を超えたトラフィックが増加しています。3 つ目として、アジャイル開発によるアプリケーションの急増により、ハッカーが標的とするアタックサーフェスがますます広くなっています。

セグメンテーションのためのファイアウォール：時代遅れの方法

このような状況を考えると、セグメンテーションのために VLAN とファイアウォールのみに依存する方法を続けていくことはできません。純粋に技術的な観点から見ると、アプリケーションの開発速度に合わせて複数の VLAN とファイアウォールを設置して構成する作業は、複雑で手間がかかります。また、人手がかかるため、多数のチームメンバーが優先度の高いセキュリティプロジェクトに従事できなくなります。展開までの時間もまた問題で、長い時間にわたって資産がリスクにさらされ、脆弱性を狙った攻撃を受ける危険性が高まります。そして何よりも、追加のトラフィックをサポートするためのファイアウォールや新規ハードウェアの設備投資コストのみならず、設備の継続的な管理、変更、メンテナンスに関連するコストもかかるため、導入のコストが非常に高くなります。

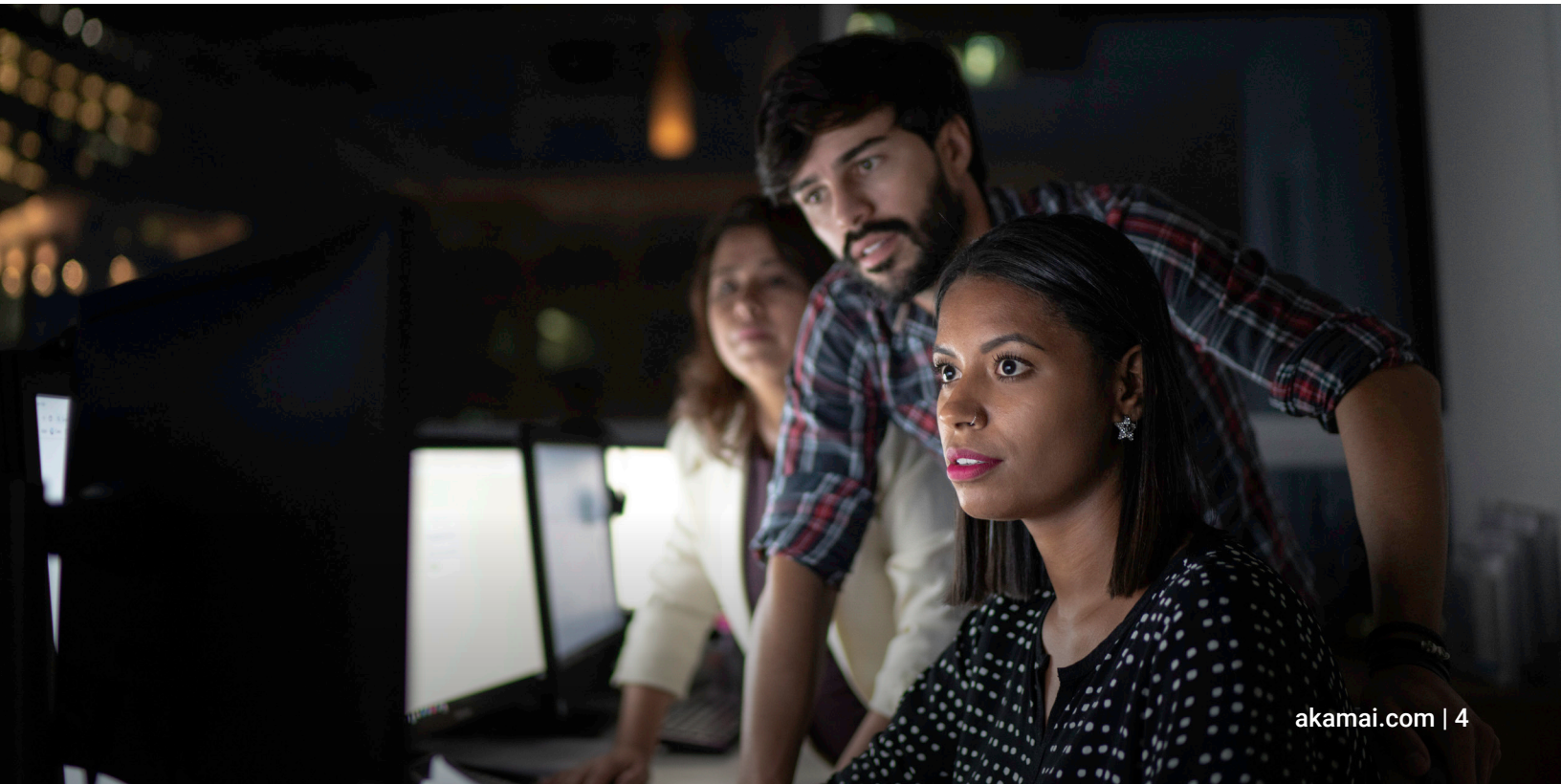
簡単に言えば、従来のネットワークセグメンテーションのアプローチは限界に達しています。特に、動的なクラウドおよびハイブリッド環境の活用を組織が模索するなか、内部のファイアウォールのみでセキュリティを確保しようとすると、アジリティの足かせとなるとともに、ポリシーの作成や適用のスピードが低下し、運用を安全にスケーリングすることが困難となります。従来のファイアウォールに代わる、先進的かつ効率的で、コストが低く、効果が高いセグメンテーションの必要性がかつてないほど高まっています。そこで登場するのがソフトウェアベースのセグメンテーションです。

> 従来のファイアウォールに代わる、先進的かつ効率的で、コストが低く、効果が高いセグメンテーションの必要性がかつてないほど高まっています。

現状の課題 - コストのかかるファイアウォール管理

ソフトウェアベースのセグメンテーションの利点を掘り下げる前に、現状と比較してみましょう。エンタープライズ組織の成長に伴い、アプリケーションの数や関連するデータトラフィックの量も増加し、追加のネットワークセグメントやより複雑なセキュリティポリシーの需要が高まります。ファイアウォールで保護された VLAN に頼っている場合、新しい VLAN を展開するたびに、セグメント間トラフィックが流れるすべてのスイッチ・トランク・ポートにこれを追加する必要があります。新しい VLAN ごとに IP サブネットワークを作成する必要があります。ファイアウォールにサブインターフェースも作成する必要があります。その後、ファイアウォールポリシーを作成する必要があります。これらの変更には通常、承認やメンテナンス期間が必要で、ダウンタイムの可能性もあるため、ネットワークが中断するリスクが増大します。

VLAN とファイアウォールの追加には、複数ステップから成る手間のかかるプロセスが伴い、スイッチング、ルーティング、ファイアウォールの実装、ESXi サーバー、セキュリティポリシーの作成をそれぞれ担当する 5 つものチームの連携を要します。このすべての要素が合わさって導入期間が長くなり、組織が長期間リスクにさらされることとなり、ソフトウェア、ハードウェア、人件費のコストが増大します。さらに、エンジニアの観点からは、これはリスクが高い割にはメリットの少ない作業です。わずかな成果を得るために多くの労力が必要とされ、他の優先度の高いリスク管理活動に時間とリソースを割くことができなくなります。残念ながら、ファイアウォールで保護された VLAN 環境内の変更管理プロセスのうち、自動化になじむステップはほとんどありません。



解決策 - 3 つの簡単なステップで導入できるソフトウェアベースのセグメンテーション

従来の境界ファイアウォールテクノロジーは、より正確で帯域幅に制約のあるきめ細かな内部セグメンテーションの要求を意図したものではありませんでした。今日の動的な環境においてはより安全で厳格なネットワークセグメントが求められますが、そのようなニーズを満たし、より短時間で導入でき、効果が高くコストを抑えることのできる代替手法として、ソフトウェアベースのセグメンテーションが近年登場しました。ソフトウェアベースのセグメンテーションの実装の中心にあるのが、「分散ファイアウォール」の概念で、従来のネットワーク・ファイアウォール・アプライアンスよりもはるかにアジャイルで管理しやすいものです。

> ソフトウェアベースのセグメンテーションは、従来のファイアウォールの方法と比較して **10 倍から 20 倍の速度**で展開でき、必要なスタッフが少人数で、ダウンタイムや中断が生じることもほとんどありません。

ソフトウェアベースのセグメンテーションソリューションの業界をリードする一例が、Akamai Guardicore Segmentation です。時間とコストがかかり、複雑な VLAN ファイアウォール導入プロセスとは異なり、Akamai のソフトウェアベースのセグメンテーションソリューションは次の 3 つの簡単なステップだけで導入できます。

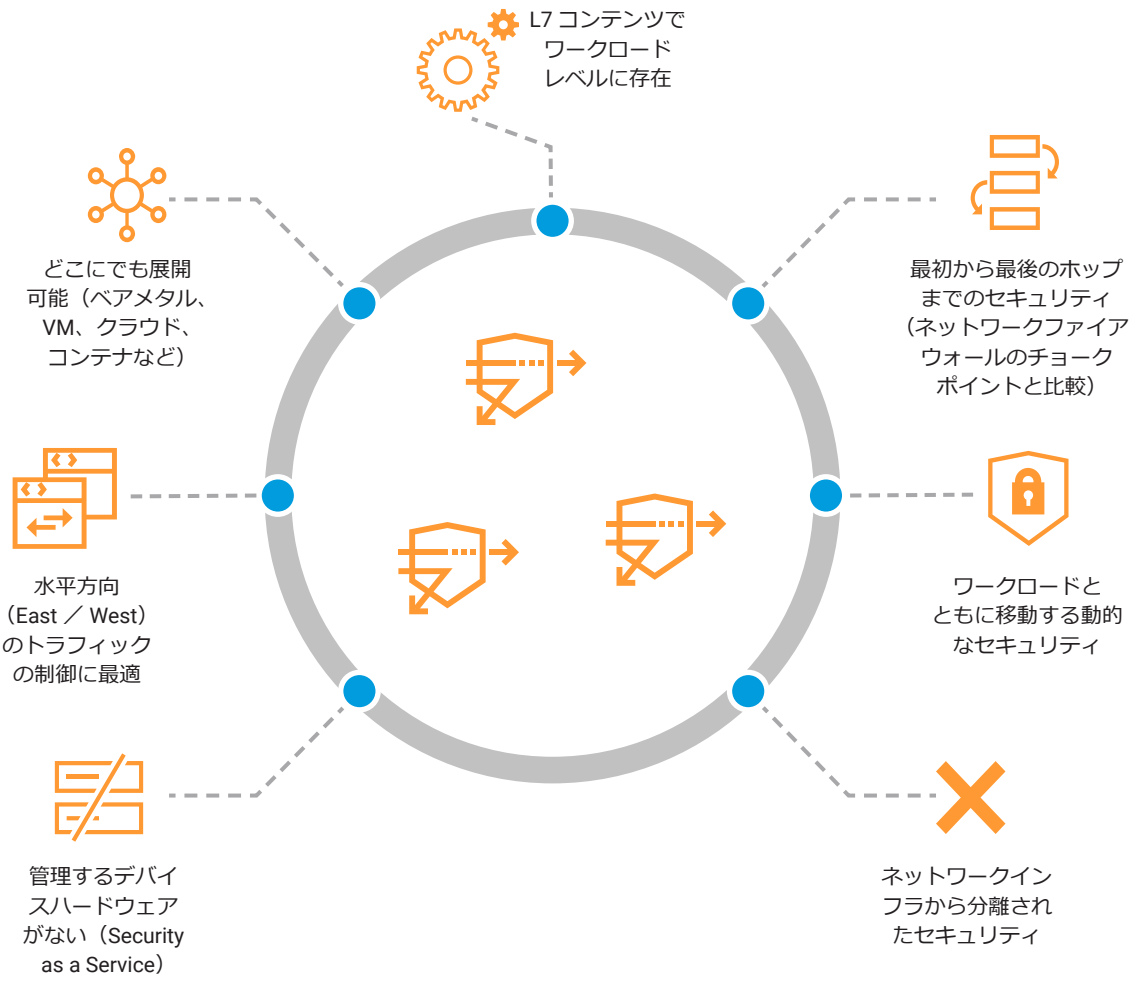
1. **資産の特定とラベル付け：**従来のファイアウォールプロセスで発生する主な障害は、セキュリティ保護が必要な資産の可視性が欠如していることです。Akamai Guardicore Segmentation には、組織のインフラ全体で実行されているすべてのアプリケーションとその依存関係をオペレーターが特定してラベル付けできる可視化機能が含まれています。

2. **ラベルごとの表示およびグループ化：**コンテキストに応じて可視化できる機能により、オペレーターはラベルに基づいてアプリケーションを論理的なグループに整理して、それらの間の依存関係をマッピングできます。Akamai のラベリングプロセスは非常に柔軟で、使い慣れた用語を使用して、ユーザー固有のビジネスコンテキストに基づいてアプリケーションをグループ化できます。

3. **ポリシーの作成：**その後オペレーターは、実際に観察されたフローに基づいて、どのアプリケーション間で通信を許可するかを決定するきめ細かなセキュリティポリシーを作成できます。一般的なユースケース向けに事前に構築されたポリシーテンプレートにより、プロセスがさらにシンプル化されます。これで、アプリケーションとワークフローが環境内のどこにあっても、相互から効果的にセグメント化できます。

ソフトウェアベースのセグメンテーションは、従来のファイアウォールの方法と比較して 10 倍から 20 倍の速度で展開でき、必要なスタッフが少人数で、ダウンタイムや中断が生じることもほとんどありません。さらに、可視化とセグメンテーションのプロセスを開始した後は、ネットワークのさらなる分割やラベルに基づくさまざまなポリシーの追加、プロセスの自動化、セキュリティインシデントへの対応、ビジネス要件や規制要件に応じた俊敏な変更を行うことも簡単になります。

分散ファイアウォールの利点



ケーススタディ：大手食品加工業者がセグメンテーションにより 85% のコスト削減

米国の大手豚肉食品加工業者では、2 か所に展開された 45 のアプリケーションのセグメント化を行う必要がありました。アプリケーションあたり平均 5 台のサーバーが使用されていました。同社の目標は、サービスの中断を最小限に抑えながらフラットなネットワークを排除し、可能な限り迅速にポリシーを導入することでした。

代替案を検討した結果、同社は Akamai のソフトウェアベースのセグメンテーションソリューションを選択しました。導入がスピーディーでシンプルなことに加えて、主要ファイアウォールサプライヤーの製品で VLAN を保護する場合と比較して、3 年間で 90 万ドル以上（85%）のコストを削減できるという分析結果が導入の決定打となりました。具体的には以下のとおりです。

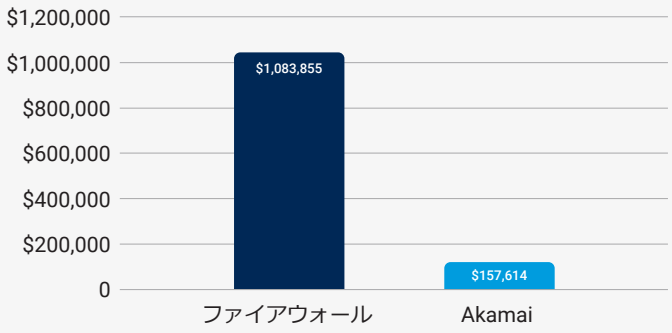
- Akamai Guardicore Segmentation のライセンス費用は、VLAN ファイアウォール実装のハードウェアコストより 55% 低い
- 人件費を 1 週間に 2,000 ドルと仮定すると、はるかに長い期間がかかる VLAN プロジェクトよりも Akamai のほうが最大で 93% 低い

さらに、Akamai は迅速なポリシー導入というお客様のニーズに応え、一切の中断なくわずか 6 週間で 45 のアプリケーションを保護しました。

ファイアウォール TCO*
$1,083,855

Akamai TCO*
$157,614
-$926,241

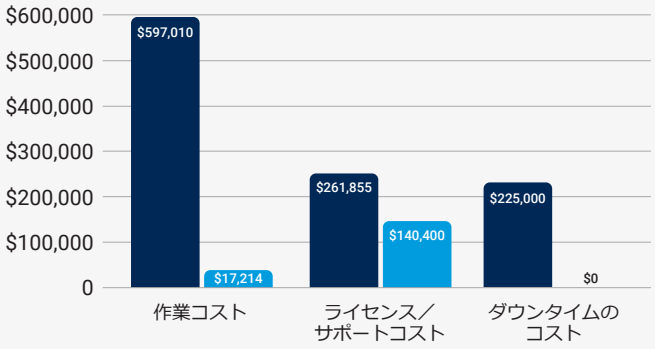
* 3 年間のコスト



Akamai の作業コスト *
$17,214
-$579,796

Akamai のライセンス／サポートコスト *
$140,400
-$121,455

Akamai のダウンタイムコスト *
$0
-$255,000



もたらされる効果

ソフトウェアベースのセグメンテーションには、従来のファイアウォール方式に対して 3 つの主なメリットがあります。

より効果的なリスク低減：ソフトウェアベースのセグメンテーションにより、アプリケーションを非常にきめ細かく、迅速にセグメント化できるため、アタックサーフェスを大幅に減らすことができます。ネットワーク資産へのアクセスを試みるすべてのユーザー、デバイス、アプリケーションに対して厳格な認証を要求するゼロトラストの原則を利用したソフトウェアベースのセグメンテーションでは、データセンターまたはネットワーク環境内における脅威のラテラルムーブメント（横方向の移動）を阻止できます。これにより、データ漏えいの影響がさらに緩和され、攻撃者によって境界の防御が破られたとしても、プロセスが乗っ取られることがなくなります。また、重要で機密性の高いアプリケーションを一般的なネットワークトラフィックから分離することを求める規制へのコンプライアンスを、より迅速に実現できます。

最適なセキュリティ体制を実現するまでの速度：簡単に言うと、ソフトウェアベースのセグメンテーションにより、セキュリティを強化するとともに、アジャイルな DevOps アプリケーションの展開ペースに合わせて、セキュリティチームがより迅速に本番環境のすべてのアプリケーションを適切に保護できるようになります。また、長期間に及ぶセグメンテーションプロジェクトに縛られる技術的リソースや人的リソースを抑えられます。チームは他の重要なイニシアチブに集中できます。

総所有コストの大幅な削減：これは実質的な利益であり、おそらくビジネスの観点から最大の利点です。ソフトウェアベースのセグメンテーションは、ファイアウォールアプライアンスや追加ハードウェアを購入するよりも、ソフトウェアソリューションの設備投資（CapEx）を大幅に削減できます。また、継続的なメンテナンスと管理のための人件費とリソースの節約という形で、時間の経過とともに運用コスト（OpEx）が大幅に削減されます。

これらの基準だけをとっても、10 のアプリケーションセグメントについてソフトウェアベースのセグメンテーションとファイアウォールソリューションを比較対照した結果、Akamai のアプローチは合計で 85% のコスト削減につながることがわかりました。これはおよそ 100 万ドルに相当します。

展開後最初の 1 週間で大幅なコスト削減が期待できますが、総所有コスト（TCO）には当然ながら、設備投資における購入価格や、継続的にかかる経費以外のコストも含まれます。全体としてのコストを正確に計算するのは簡単ではありませんが、ソフトウェアベースのセグメンテーションでは、ダウンタイムとサービスの中断がほとんど発生しないため、大きなコスト削減となります。さらに、エンタープライズ組織は、データ漏えいによる財務上の損失やコンプライアンス違反に伴う罰金も回避できます。また、セキュリティ侵害による評判の低下やビジネス損失のリスクを大幅に低減することができます。IT チームとリソースを、ファイアウォールの変更管理から、より生産的なプロジェクトに割り当て直すことができます。これらのコスト要因はすべて、ソフトウェアベースのセグメンテーションソリューションを選択したお客様にとって、TCO の削減と収益の向上に貢献します。

ケーススタディ：コンプライアンス制裁に直面した大手グローバル銀行が Akamai Guardicore Segmentation を導入

ヨーロッパのある大手金融機関では、監査によって同行のフラットネットワークが抱えるセキュリティ上のリスクが明らかとなり、より厳格なセグメンテーションを求める多数の新たな規制が導入されたことをきっかけに、VLAN とファイアウォールルールを使用したセグメンテーションプロジェクトを開始することにしました。このプロジェクトには膨大な時間がかかり、複数の関係者とチームの関与が不可欠でした。これにより、実稼働環境でダウンタイムが発生し、ポリシーが不明瞭になりました。その結果、非常に高額な導入コストに加えて、コンプライアンス違反により罰金まで科されることになりました。

IT チームは速やかに代替ソリューションを検討し、Akamai がセキュリティ運用にもたらす自動化のレベルに感銘を受けました。同行は、複数の地域と IT インフラタイプにわたり Akamai Guardicore Segmentation を展開しました。このプロジェクトは 3 か月未満で完了し、従来のセグメンテーション方法を使用した場合にかかると見積もられていた期間と比較して 10 倍のスピードで終わらせることができました。同行は、セキュリティ体制をアップグレードできただけでなく、10,000 件以上の資産のコンプライアンス要件も満たすことができました。迅速に展開することができたため、コストと内部リソースを大幅に削減するとともに、リスクの軽減を加速させることができました。

大手グローバル銀行

プロジェクトの目標：

開発／本番／ UAT の分離

プロジェクトの範囲：

1. 本番環境と非本番環境の間のトラフィックを制限する
2. アプリリングフェンシングの準備

従来のセグメンテーション

- 進行速度が非常に遅い
- 監査の失敗、罰金、本番環境のエラー
- アプリケーションのダウンタイムによる本番環境の停止

時間：2 年（ファイアウォール／ VLAN を使用）

Akamai による効果

- 非準拠の 10,000 件の資産をセグメント化
- アプリケーションのダウンタイムがゼロ
- 10 倍の導入速度
- DevOps による手作業の削減

時間：6 か月 **スタッフ：**アーキテクト 3 人

結論：総合的な評価

ファイアウォールは廃れていません。確かに、ネットワーク境界の保護において役割を果たしています。しかし、今日の動的な環境においては、境界は決まった形を持たない概念になっています。セキュリティとアジリティの間で必要なバランスを取るには、L4 のネットワークのレベルだけでなく、L7 のアプリケーションレベル（具体的には個々のプロセスのレベル）でデジタル資産を保護できる必要があります。この目的にはファイアウォールは不適切なだけでなく、実際には進行の妨げになります。ファイアウォールを使用してきめ細かなセグメンテーションを実現しようとすると、人的リソース、技術的リソース、そして金銭的リソースを浪費することになります。

ソフトウェアベースのセグメンテーションを使用すると、ファイアウォールを使用した従来のアプローチと比べて、著しく低減された TCO でセキュリティのリスクを飛躍的に抑え、価値創出までの時間を全体的に大幅に短縮できることが示されています。これにより、高い ROI を迅速に達成できます。これは未来的なビジョンではありません。ソフトウェアベースのセグメンテーションが登場し、今、さまざまな分野の組織にこのようなメリットをもたらしています。

IT の進化に関する考察

これまでのテクノロジーを振り返ると、継続的な改善、簡素化、コスト削減の繰り返しであることがわかります。セグメンテーションも例外ではありません。

ストレージの例を考えると、わずか 20 年でフロッピーディスクからフラッシュドライブ、Network Attached Storage（NAS）、最終的にはクラウドストレージへと進化しています。コンピューティングランタイムの場合は、サーバーから仮想マシン、クラウドコンピューティングからコンテナ、そして最終的にサーバーレスコンピューティングへと進化しました。いずれの場合も、主な推進要因はコストの削減と柔軟性の向上でした。もちろん、それを可能にしたのは技術の急速な進歩です。

物理ファイアウォールアプライアンスから、ネットワークから抽象化されたソフトウェアベースの分散ファイアウォールへのセグメンテーションの進化も、これと似ています。また、根底にある推進要因も、コストの削減と柔軟性の向上（それによる展開スピードの向上）と同じものです、それと同時に、ゼロトラストをサポートするよりきめ細かなアプローチによるセキュリティポリシーの効果が着実に向上します。

ネットワークチームとセキュリティチームが、他のテクノロジーセクターで明らかになっているように、セグメンテーションによるセキュリティ保護の新しいモデルを採用するときが来ました。セグメンテーションに物理ファイアウォールを使う方法は、フロッピーディスクと同じ運命をたどることになるでしょう。

ソリューションの活用例をご覧になりたい場合は
今すぐデモをご依頼ください：akamai.com/guardicore

Akamai は、お客様が生み出すものすべ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、セキュリティ体制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。