Akamai

ホワイトペーパー

包括的なセグメンテーションで AWS のワークロードを保護 — よりシンプルで迅速なセキュリティ

セキュリティ面の懸念からクラウドの導入をためらう必要はありません。1 つのソリューションで、AWS における可視性、ラテラルムーブメントの防止、セキュリティ侵害の検知と対応を実現できます。

世界中のエンタープライズ組織の 60% 以上が、クラウド導入をためらう主な理由にセキュリティを挙げています。インフラのコストやメンテナンスが不要で、無制限とも言えるリソースやコンピューティング能力を利用してスケーラビリティと弾力性を向上でき、機械学習や AI などの最新のイノベーションを活用してパフォーマンスの向上や分析の強化を実現できるなど、重要なワークロードを AWS に移行するメリットは明らかです。しかし、多くのエンタープライズ組織がセキュリティ上の懸念から、クラウドの導入をためらっています。

AWS におけるセキュリティの課題

まったく新しい環境を検討する場合、セキュリティを最初から再確認する必要があることは意外ではありません。クラウドをこれまで利用していなかった場合や、別のベンダーから移行する、新しいハイブリッドソリューションを選択した場合、既存のエコシステムに AWS を追加する場合が考えられます。いずれにしても、クラウドを導入する場合は、クラウドというインフラがもたらす固有の課題に対応するため、クラウド独自のツールセットが必要となります。すべてのクラウドベンダーに共通する要因もありますが、Azure、Google Cloud Platform（GCP）、AWS に固有の要因もあります。AWS テクノロジーを含むクラウドまたはハイブリッドクラウドを使用している企業の主な懸念事項を以下に示します。

責任分担についての理解：ワークロードを AWS に移行する際には、多くの責任を負うことを認識する必要があります。顧客データ、アプリケーション、プラットフォームを保護する必要があります。Gartner は、2025 年にかけてクラウドにおけるセキュリティインシデントの 99% がクラウド利用者側の落ち度が原因で発生すると予測していますが、その根拠としているのが責任分担モデルに対する理解不足です。

可視性の欠如：把握できないものは制御できません。クラウドでは、可視性がはるかに複雑になります。特に、水平方向（East ／ West）と垂直方向（North ／ South）に移動するネットワークトラフィックの保護と可視化にあたっては複雑さが顕著です。フローを見るだけでは不十分です。重要な資産が複数の AWS アカウント、コンテナ、またはネットワーク・セキュリティ・グループに分散して存在していることがあります。このような資産がどこに存在しているかを含め、資産に関するあらゆる情報を的確に把握しなければ、フローや相互依存関係を正確に理解できない可能性があります。

ポリシー作成の制御が限定的：オンプレミスでレイヤー 7 のレベルでの知見を獲得できている企業であれば、ワークロードをクラウドに移行したとたんにレイヤー 4 レベルでの可視性しか得られない状態に逆戻りし、今まで手にしていた詳細な知見やきめ細かな制御機能を失うのは望ましくないでしょう。Amazon のセキュリティグループでは、レイヤー 4 までのトラフィックの制御がサポートされています。しかし、基盤となるインフラにかかわらずレイヤー 7 のレベルでの可視性と制御を手にできれば、ポートと IP にのみ頼る場合と比べてはるかに有用な知見を手にし、確実な制御を実施できます。多くの場合ポートと IP のみに頼っていたのではセキュリティ侵害の検知やトラブルシューティングを行うことができません。

コンテナのセキュリティ：AWS では、Amazon セキュリティグループを使用してコンテナのセキュリティポリシーを適用しますが、このポリシーはクラスターのレベルでしか適用できず、個々のポッドのレベルでは適用されません。通信の内容を完全に把握するためには、物理的なインフラ上で実行されているオーバーレイネットワークのコンテキストを認識し、ポッドレベルまで詳細にドリルダウンできるソリューションが必要です。VM とコンテナの両方を含むネットワークポリシーを作成する場合は設定や管理がさらに複雑になり、多くの場合、セキュリティ制御の仕組みを 2 種類用意しなければなりません。

オールインワンのセキュリティプラットフォームでこれらの問題に対処

Amazon には、Amazon セキュリティグループなどの組み込みのツールが用意されており、これらを使用することでインフラをクラウドに移行する際に生じるいくつかの課題に対処できます。AWS を利用する組織には、グループを使用して権限を割り当て、認証情報を定期的にローテーションし、IAM グループを利用して簡素化を図るなど、AWS IAM（アイデンティティアクセス管理）を最大限に活用することをお勧めしています。しかし、パブリッククラウドがさまざまな形で利用されるようになっている現在、特にレガシーインフラからマルチクラウド、コンテナテクノロジーまで、あらゆるテクノロジーを駆使するハイブリッド環境においては、このようなツールだけでは単なる足掛かりにしかなりません。ハイブリッド環境においても、盲点を取り除き、他のセキュリティスタックとシームレスに連携できるテクノロジーで AWS の機能を補完できる、高度なセキュリティソリューションが必要です。Akamai Guardicore Segmentation の特長は次のとおりです。

AWS インスタンスの完全な可視性

IT インフラの複雑性が高まるにつれて、自動的に深いレベルの可視性を実現できる仕組みがますます重要となります。手動による移動、追加、変更、削除は、信頼性が低くギャップやエラーが発生しやすいだけでなく、速度が低下するため、クラウド導入の妨げとなります。一方、自動化により優れた可視性を手にすることができれば、あらゆるアプリケーションやフローを検出して、個々のプロセスのレベルに至るまでインスタンスの可視化を実現できます。

Akamai Guardicore Segmentation には、オーケストレーションデータを取得する強力な AWS API が含まれており、ラベリングやアプリケーションマッピングに使用できる貴重なコンテキストを手にできるとともに、EC2 タグを自動的に取得して EC2 インスタンスを可視化することができます。インフラのベースライン測定を通して、アプリケーション相互

でどのように通信が行われ、どこに依存関係が存在し、スムーズでアジャイルな運用のためにはどのようにポリシーを作成すればよいかをしっかりと把握するのに必要な詳細情報を手にすることができます。ユーザーは、クラウドベンダーや環境ごとに個別のセキュリティソリューションを用意するのではなく、ネイティブクラウド情報と AWS 固有のデータをすべて同じダッシュボードに表示できます。Akamai のソリューションはあらゆるプラットフォーム、インフラ、クラウドをカバーできるため、環境全体をくまなく可視化できます。

セグメンテーションと適用 - ワークロードに沿って機能する単一のポリシー

すべての環境をカバーするこの「単一画面」ビューを手にしたら、セキュリティポリシーの設計と展開の作業に取り掛かることができます。アプリケーション認識型ポリシーを使用すると、Amazon セキュリティグループで実現できるレイヤー 4 のレベルにとどまらず、レイヤー 7 でのきめ細かなセキュリティを実現できます。ラテラルムーブメントを制限するためにオンプレミスで次世代ファイアウォールの使用を試みる組織もありますが、このようなファイアウォールでは水平方向（East ／ West）のトラフィックのおおまかなセグメンテーションしかサポートされません。この方法では、ファイアウォールを通じてトラフィックを再ルーティングするためにインフラおよびネットワークの大規模な変更が必要となるため、セグメンテーションによるきめ細かな制御のソリューションとして使用するのは非常に困難です。オンプレミスでは実現できたとしても、このレベルの制御をクラウドでも行うのは至難の業と言えます。そこで登場するのが、基盤となるネットワークインフラの変更を一切必要としない、動的なワークロードのためのポリシーを備えたレイヤー 7 のマイクロセグメンテーションです。ポリシーはワークロード自体に沿って機能するため、手作業でインフラなどを変更する必要がありません。そのため組織のアジリティを高め、変化の速い DevOps 環境へも問題なく対応することができます。ハイブリッド環境の管理がシンプル化され、1 つのマイクロセグメンテーションポリシーで、一貫性のある単一のポリシー表現を使用して、地域、VPC、コンテナ、VM、オンプレミスなどにルールを適用できます。提供される高い可視性をもとに、セグメンテーションポリシーをわずか数分で定義して適用できます。ポリシー作成プロセスは、パブリッククラウド上でクラス最高のセキュリティプロトコルを提供する自動ポリシー推奨によっても強化されます。

AWS クラウドでのセキュリティ侵害の検知とインシデント対応

Akamai Guardicore Segmentation のようなフルサービスソリューションを選択すると、セグメンテーションや可視性以外の面でも AWS セキュリティを強化できます。ポリシー違反の検知は、セキュリティ侵害検知の重要な部分であり、アプリケーションレベルの詳細情報を使用して、潜在的なサイバー脅威にリアルタイムで対応できます。ハイブリッドクラウド環境で悪性の活動を即座に警告できるように、以下のような複数のセキュリティ侵害検知方法が提供されています。

- **レピュテーション分析：**ドメイン名や IP アドレスからファイルハッシュやコマンドラインまで、フロー内の疑わしい情報を自動的に検知します。
- **動的ディセプション：**攻撃者の知識を必要とせずに、高インタラクションのハニーポット環境に攻撃者を誘導し、攻撃者の行動から安全に学ぶことができます
- **インシデント対応を迅速化するツール：**AWS との統合により、ポリシー違反やセキュリティインシデントを AWS Security Hub にリアルタイムで送信できます。
- **カスタム脅威ハンティング：**Akamai Hunt サービスを利用すると、Akamai Guardicore Segmentation のインフラと Akamai の大規模なグローバル脅威インテリジェンスを活用し、ハイブリッドクラウド環境の非常に発見しにくい脅威をも阻止することができます。

すべてを統合することで、AWS などのセキュリティを強化

クラウドに移行したからといって、必ずしもオンプレミスよりも低いセキュリティ、可視性、制御で妥協する必要はありません。Akamai Guardicore Segmentation を使用すると、インフラ全体の AWS インスタンスを完全に可視化できます。この基本的なマップを使用することで、ポリシーの作成がシームレスになり、AWS セキュリティグループが強化され、手動サポートを必要とせずにきめ細かな制御が可能になります。セキュリティ侵害検知とインシデント対応も加わって、AWS クラウド上のすべてをカバーするエンドツーエンドのプラットフォームを手にすることができます。

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