AKAMAI ソリューション概要

ハイブリッドクラウド環境のセグメンテーション

クラウドインフラのセグメンテーションで攻撃を封じ込める

アプリケーションやワークロードのクラウド移行が進んでいますが、それに伴い、セキュリティチームやクラウドチームは新たな課題に直面しています。その 1 つが、セグメンテーションとゼロトラストの原則をクラウド環境のアプリケーションやワークロードへと拡張することです。Akamai Guardicore Segmentation を使用すれば、エージェントをインストールしなくても、アタックサーフェスを縮小し、パブリッククラウド環境内のアプリケーションやワークロードに対する攻撃を封じ込めることができます。これは、アプリケーションの自動探索、クラウドフローの包括的な可視化、詳細なセグメンテーションポリシー、ネットワーク・セキュリティ・アラートを通じて実現され、これらの機能すべてを 1 画面で確認、制御できます。

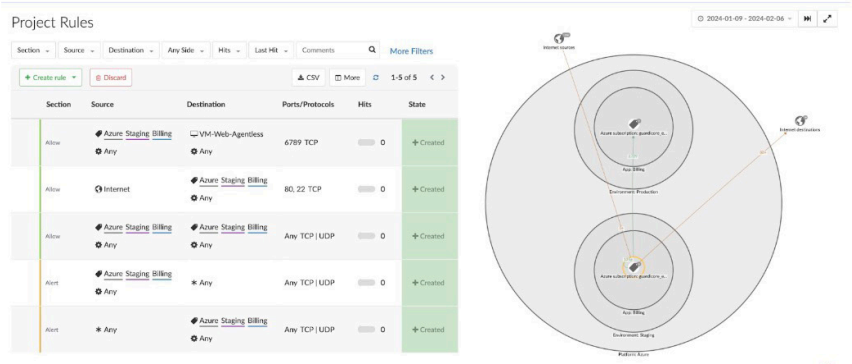
クラウド特有の課題

今では多くの組織が、重要なシステムの管理や、貴重なデータの保存をクラウドに依存するようになりました。

IBM の「2023 年データ侵害のコストに関する調査レポート」によると、データ侵害の 82% は、クラウド（パブリック、プライベート、またはその両方の環境）に保存されているデータに関連して発生しています。攻撃者は、複数のクラウドプラットフォームへのアクセス権を入手する可能性が高いため、データ侵害の 39% は複数の環境に分散し、そのコストは平均コストを上回る 475 万米ドルに上っています。

クラウド固有の動的な特性により、クラウドのワークロードは、オンプレミスのリソースよりも外部の脅威にさらされやすいといえます。そのため、セキュリティチームは、いくつか特有の課題に対処しなければなりません。

- **低い可視性** — クラウドプロバイダーの可視性は、異なるワークロード間のフローの生ログデータに基づいています。クラウド環境内のさまざまなワークロードとアプリケーションの関係を明確に理解できないと、効果的なセキュリティポリシーを作成することはほとんど不可能になります。
- **単一ポリシーの欠如** — ネイティブのクラウド・セキュリティ・ツールのみを使用してハイブリッドクラウド環境全体に適用できるような一貫したポリシーを作成することは、非常に複雑かつ困難です。 クラウドインスタンスはそれぞれオブジェクトとルールが異なるため、独自のポリシーを有し、その結果、クラウド内のポリシーは断片化しがちです。
- **統一的なガバナンスの欠如** — クラウドではセキュリティが常に優先されるとは限りません。アプリケーションのオーナーは、セキュリティを考慮せずにワークロードをスピンアップすることがあるため、セキュリティチームとの間に認識の相違が生じます。



ポリシーの自動提案を使用した *Azure* アプリケーションのリングフェンス

ビジネス上のメリット

単一のインターフェースでクラウドフローを可視化
動的なネットワーク依存関係マップを使用して、クラウドのワークロードとアプリケーションのやりとりを詳細に把握し、セキュリティ制御を簡単に適用できます。

一貫したセグメンテーションポリシーの適用
ハイブリッドクラウド環境全体で矛盾なく機能する単一のセグメンテーションソリューションを展開することで、ベンダー固有のソリューションによるセキュリティのサイロ化を回避できます。

セキュリティ侵害の阻止
クラウド環境内のあらゆる変更にセキュリティポリシーを適応させることができます。手動更新による負担を軽減できます。

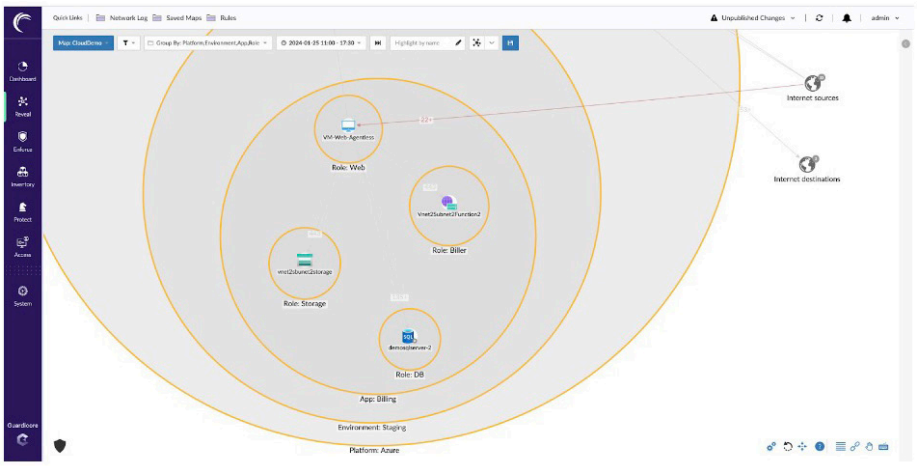
Akamai

クラウドセキュリティの脅威を防御

Akamai Guardicore Segmentation は、業界をリードするセグメンテーション機能をクラウドのアプリケーションとワークロードにまで拡張します。セグメンテーションをクラウドの資産まで拡張すれば、不正な接続が自動的に阻止されます。これにより、ラテラルムーブメント（横方向の移動）を制限し、侵害やランサムウェアインシデントによる損害を軽減することができます。

主な機能

- **エージェントレスかつクラウドネイティブの包括的な可視性と適用機能：**管理者は真のネットワークフローに関するほぼリアルタイムのインタラクティブマップを通じて、クラウドのワークロードが可視化されるため、アプリケーションの依存関係を把握できます。また、クラウドネットワークのセキュリティガバナンスにおいて、DevOps チームと SecOps チームを統合できます。
- **複数の適用ポイントを活用するハイブリッド適用エンジン：**ネットワークポリシーの意図を定義すれば、残りの処理は Akamai Guardicore Segmentation のポリシーエンジンが実行します。データセンター全体で使用されるエージェントベースおよびエージェントレスの適用ポイントが動的に決定されます。
- **レピュテーション分析と脅威インテリジェンスファイアウォール機能の統合：**セキュリティ侵害時の検知およびインシデント対応時間を短縮できるように設計されています。
- **スケーラブルかつ安全なソリューション：**データがクラウド環境から出ることはありません。また、ソリューションアーキテクチャはクラウド環境内で自動的に拡張されます。



1 **つのマップでオンプレミス環境とハイブリッドクラウド環境を可視化**

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

 | サポート | 公開日：2024 年 2 月