AKAMAI ソリューション概要

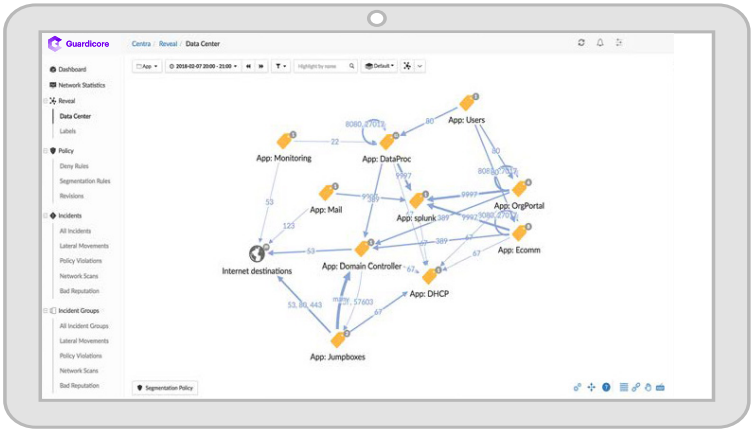
Akamai Guardicore Segmentationを使用したハイブリッド環境での迅速なマイクロセグメンテーション

マイクロセグメンテーションの導入は一筋縄ではいきません。IT 環境におけるアプリケーションフローを検出、理解、制御する過程では、さまざまな紆余曲折があります。しかも、適切な方法で道を進むことができなければ、途中でいくつかの課題に直面する可能性があります。ネットワークに存在する盲点により、アプリケーション、ワークロード、基盤となるプロセスの検出と通信のマッピングが十分にできないことがしばしばあります。柔軟性に乏しいポリシーエンジンを使用すると、大まかなポリシーしか指定できず、アプリケーションのセキュリティが侵害されるリスクが生じます。オペレーティングシステム間でポリシー表現に一貫性がなければ、セキュリティ上のギャップが生じる危険性があります。ポリシー違反に関するデータをセキュリティ侵害検知ツールに統合する作業は複雑で、手作業で行われることも多いため、インシデントの調査と対応が遅れる可能性があります。Akamai Guardicore Segmentation では、3 つのステップで簡単にマイクロセグメンテーションを導入することができます。

ステップ 1：検出と可視化

アプリケーションを自動的に検出して、フローを可視化

Akamai Guardicore Segmentation は、最高レベルの可視性を備えており、展開場所にかかわらず、すべてのアプリケーション、ワークロード、通信フローをプロセスレベルのコンテキストとともに自動的に検出し、可視化します。オンプレミス、クラウド、マルチクラウドなど、資産の展開場所にかかわらず同じレベルの可視性を手にすることができます。この可視化とオーケストレーションメタデータの自動インポートにより、セキュリティチームはすべての資産とアプリケーションのラベル付けとグループ化を迅速かつ簡単に実行し、ポリシー開発を合理化できます。



展開場所にかかわらず重要なアプリケーションをセキュリティ保護

プラットフォームに依存しない

Akamai Guardicore Segmentation では、オンプレミス、クラウド、マルチクラウドなど、場所にかかわらずインフラ全体で資産を可視化し、セキュリティポリシーを適用できます。

迅速なポリシー適用

自動的なルールの提案、柔軟なポリシーエンジン、直感的なユーザーインターフェースにより、ポリシーの作成と適用にかかる時間が短縮されます。

セキュリティ侵害の検知と対応機能の統合

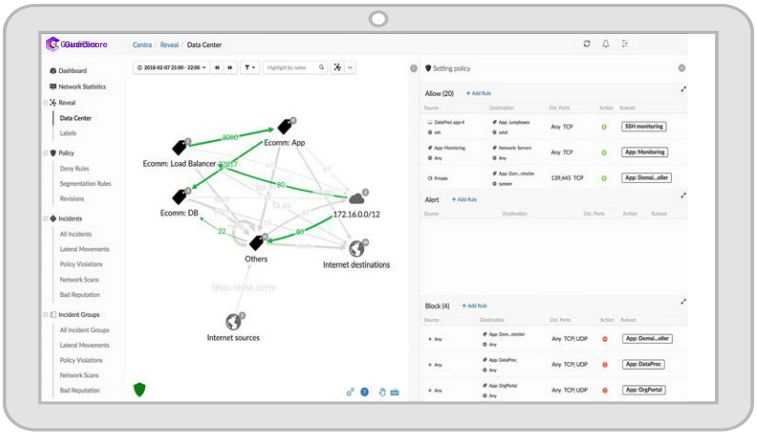
ポリシー違反を可視化し、現在進行中の脅威に迅速に対応して、場所にかかわらず最も重要な資産を保護できます。

Akamai

ステップ 2：構築

ポリシーを迅速に設計、テスト、展開

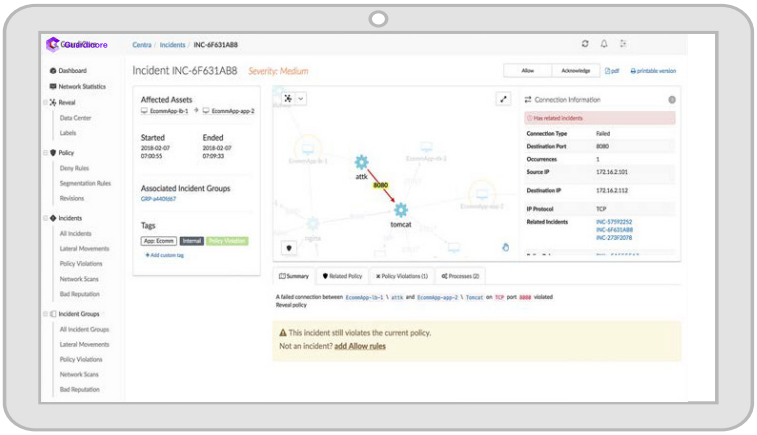
Akamai Guardicore Segmentation は、マイクロセグメンテーションポリシーの開発と管理をシンプル化します。Reveal マップの通信フローを 1 回クリックするだけで、過去に観察された内容に基づき自動的にルールが提案されるため、強力なポリシーを迅速に構築できます。直感的なワークフローと柔軟なポリシーエンジンにより、ポリシーの継続的な改良がサポートされ、コストのかかるエラーが削減されます。



ステップ 3：適用

あらゆる環境で強力なセキュリティを提供

システム全体にわたりネットワークレベルとプロセスレベルで通信ポリシーを適用できる Akamai Guardicore Segmentation で、オペレーティングシステムでポリシー適用に制約がある状況でもセキュリティを維持することができます。また、セキュリティ侵害の検知と対応機能が統合されているので、現在進行中のセキュリティ侵害のコンテキストに沿ってポリシー違反を確認し、攻撃手法を迅速に特定して、修復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。

 | サポート | | 公開日：2023 年 6 月