AKAMAI ソリューション概要

複数の手法を駆使した侵害検知の注目点：セグメンテーションポリシーを使用したデータセンターの侵害検知

データセンターに対するセキュリティ侵害がその勢いを弱める兆候は見られません。今こそセキュリティチームは、アプリケーションが相互に通信し、ミッションクリティカルな機能を実行するデータセンターの中心部の保護に本腰を入れなければなりません。複数の仮想化環境にデータセンター資産を分散する組織が増えているため、境界防御はもはや十分ではありません。セキュリティ管理者には、境界防御の侵害に成功した攻撃から水平方向（East ／ West）の内部トラフィックを保護する、効率的な手段が必要です。

限界に達しているファイアウォール型の防御

ファイアウォールは従来、データセンターから送受信される通信のセキュリティを確保するために使用されてきました。しかし、ファイアウォールをデータセンターの中心に配置するのは問題があります。ファイアウォールは膨大な量の水平方向（East ／ West）のトラフィックに対応できず、パフォーマンス上のボトルネックとなります。サーバーレベルでファイアウォールによる防御を使用すると、ホストのコンピューティングリソースを大量に消費します。この負担がすでに非常に大きくなっています。また、データセンター内に存在するさまざまなタイプやブランドのオペレーティングシステムに対応するため、複数のソリューションを展開する必要があり、管理が困難になります。

最近まで、L7 のプロセスレベルでのセキュリティポリシーの実装も課題でした。これは、環境内で通信するすべてのアプリケーションとプロセスの可視性を備えている必要があるためです。さらに、アプリケーションとデータセンター内でプロセスがどのように連携するべきかを総合的に理解する必要があります。こうした知見がないままプロセスレベルのセキュリティポリシーを実装することにはリスクがあり、何らかのミスが入り込む可能性が高くなります。

データセンターの重要な資産を保護すると同時に、セキュリティ侵害の検知と対応の能力を向上させるためには、セキュリティチームには以下を実行できる手段が必要です。

- データセンターで実行されているすべてのアプリケーションとプロセスをリアルタイムで可視化する
- 重要なプロセスを妨げることなく、きめ細かなセキュリティポリシーを実装する
- セキュリティ侵害を示している可能性のある不正な通信を検知する

攻撃は最大の防御：Akamai Guardicore Segmentation によるポリシーベースの検知

セキュリティチームは、ポリシーベースの検知により、脅威を迅速に検知および確認し、封じ込めて、損害を防止し、損失を最小限に抑えることができます。これらのきめ細かなセキュリティ制御により、侵入者がアプリケーションやプロセスに悪意のあるアクセスを取得できないようにすると同時に、侵入者の存在を管理者に警告することができます。

Akamai Guardicore Segmentation のセグメンテーションポリシー機能により、セキュリティ担当者は次のことが可能になります。

- データセンター内のすべてのアプリケーションとアクティビティの包括的なビジュアルマップを生成し、すべてのワークロードを可視化し、アプリケーションレイヤーの通信を完全に理解できるようにする

複数の検知方法により迅速に侵害を検知

動的ディセプション

リダイレクトのアーキテクチャと、実稼働環境と同等の環境を動的に生成する機能により、データセンターのパフォーマンスに影響を与えることなく、攻撃者をおびき寄せ、その手口を見極めることができます。

ポリシーベースの検知

レイヤー 4 のネットワークのレベル、およびレイヤー 7 のプロセスのレベルでのセキュリティポリシーにより、不正な通信やコンプライアンス違反のトラフィックをただちに認識できます。

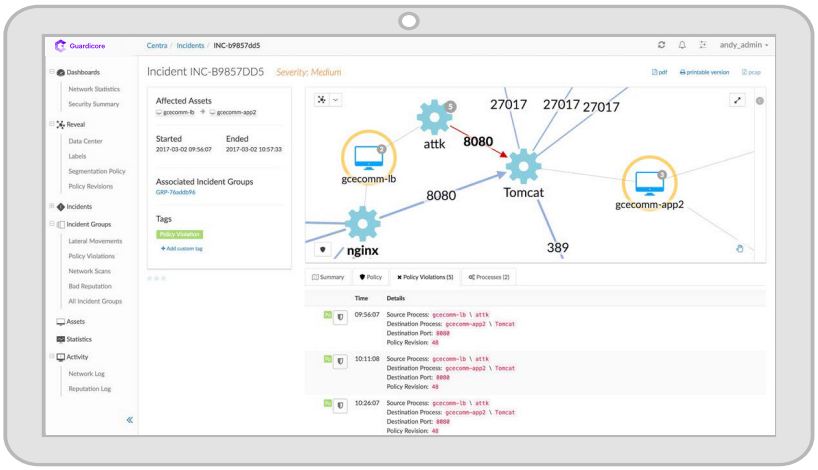
レピュテーション分析

トラフィックフロー内の疑わしいドメイン名、IP アドレス、ファイルハッシュを検知し、包括的なセキュリティ侵害検知を提供します。

Akamai

- アプリケーションをグループにフィルタリングして整理し、共通のセキュリティポリシー（特定のワークフローやビジネス機能に関連するすべてのアプリケーションなど）を設定する目的でラベルを付ける
- アプリケーション間の許可された通信を管理するルールを定義および作成する
- これらのルールをテストして調整し、正常な許可トラフィックを中断しないようにする

非準拠のトラフィック、不正な通信、またはその他のポリシー違反が発生すると、侵入者が存在する可能性を示すアラートが自動的にトリガーされます。これにより、調査プロセスが開始され、脅威を確認して封じ込めます。



Akamai Guardicore Segmentation は、通信が許可されている 2 台のホスト間で、許可されたポートを使用して通信を試みる不正なプロセスに関するセグメンテーションポリシー違反を認識し、アラートを生成することにより、潜在的なセキュリティ侵害を検知します。

複数の検知方法で攻撃者を追い込む

ポリシーベースの検知は、Akamai のソリューションがリアルタイムでのセキュリティ侵害の検知と対応を強化するために使用するいくつかの方法の 1 つにすぎません。相互に連携するこれらの補完的な方法には、次のものも含まれます。

- **動的ディセプション**：実際のデータセンターのサーバー、IP アドレス、オペレーティングシステム、およびサービスをおとりとして使用します。疑わしい活動の初期の兆候を積極的に探索し、そのような兆候を見つけるとその活動に介入して封じ込めのための領域にリダイレクトし、脅威の確認と調査を実施します。
- **レピュテーション分析**：Akamai の脅威センサーとインテリジェンスフィードのグローバルネットワークを利用して、脅威に関連するマイナスの評価を持つプロセスや疑わしい IP アドレス、ドメイン名、ファイルハッシュを特定します。

これらの 3 つの方法を同時に活用することで、強力なセキュリティの網が敷かれ、データセンターに対して試みられる実質的にあらゆるセキュリティ侵害を捉え、緩和し、封じ込めて、詳細な調査を行うことができます。

Akamai Guardicore Segmentation の包括的なセキュリティ侵害検知機能の詳細については、akamai.com/guardicore をご覧ください。

 | サポート | 公開日：2023 年 6 月