AKAMAI ソリューション概要

Deloitte 社、Akamai Guardicore Segmentation を活用してインシデント対応とランサムウェアの緩和サービスを強化

お客様の課題

強固に確立されたセキュリティ製品のカテゴリーは、エンタープライズネットワークに対する最新の脅威に対する保護レベルを確かに向上させます。しかし、悪性のラテラルムーブメント（横方向の移動）から保護することでアタックサーフェスを縮小する包括的な単一ソリューションを提供できるソリューションは、これまでほとんどありませんでした。ラテラルムーブメントが発生する場所とは、オンプレミスのハードウェアとの間の移動、クラウドでホスティングされているワークロード、エンドユーザーのデバイス、コンテナなどがあげられます。さらに、初期のゼロトラスト・セグメンテーションのイニシアチブは、従来、エンタープライズのクライアントが完了するまでに年単位とはいかずとも数か月はかかりました。これは、従来のファイアウォールや EDR などの確立されたセキュリティ製品がバイパスされた場合に、攻撃を阻止することを目指したプロジェクトを実行するための技術的な制約と専門知識を持つ人が限られていることによるものです。

セグメンテーションプロジェクトに取り組む際、エンタープライズのお客様は通常、次のような課題に直面します。

- すべての環境におけるすべての資産、ネットワークフロー、ユーザー、接続を可視化できない
- ハイブリッド・クラウド・インフラ、レガシー・オペレーティング・システム、OT／IoT など、さまざまなテクノロジーやインフラに対するセキュリティ制御が制限されている
- 従来のセグメンテーション手法にありがちなダウンタイムを回避し、事業継続性を確保する必要がある
- ゼロトラストをサポートするイニシアチブを構築、展開、管理するためのセキュリティリソースと人材が不足している

ソリューションの注目点

Akamai Guardicore Segmentation は、最速かつ最もシンプルで直感的な方法によりネットワークにおいてゼロトラストの原則を実現できる、ホストベースのマイクロセグメンテーションソリューションです。Akamai Guardicore Segmentation は、エージェントベースのセンサー、ネットワークベースのデータコレクター、仮想プライベート・クラウド・フローのログを組み合わせてネットワークをマッピングするとともに、レガシーおよび最新のオペレーティングシステム、運用テクノロジー、IoT　デバイスを含めたすべての資産とインフラを一元的に可視化できるように設計されています。これらの機能を活用することで、アタックサーフェスを縮小し、事業継続性を確保し、望ましくない通信を制限するポリシーを簡単に作成し、適用することができます。

主なユースケース

- **水平方向（East/West）のトラフィック管理**
  通信を必要としない環境、アプリケーション、ユーザー、インフラを分離
- **ランサムウェアの緩和**
  AI／ML を使用したポリシーテンプレートを展開し、さまざまなタイプのランサムウェア攻撃で使用されることが知られている攻撃経路をブロック
- **アプリケーションのリングフェンシング**
  ビジネスクリティカルなアプリケーションの特定の依存関係に重点を置き、厳格なセキュリティ制御を作成

- **ユーザーベースのセグメンテーション**
  業務に不可欠ではないアプリケーション、環境、デバイスへのユーザーのアクセスをブロック
- **感染したデバイスの隔離**
  1 台または複数のデバイスが侵入された場合の侵害の拡大を阻止
- **コンプライアンス**
  ネットワーク、デバイス、潜在的な攻撃経路をコンテキストに沿って深く理解し、即座にコンプライアンスを実証できる体制を整備

クライアントのメリット

- サーバー、エンドポイント、クラウド、コンテナ、ユーザーなど、ネットワークおよび接続の全体を1つの画面で可視化することで、可視性の課題を解決
- ゼロトラストポリシーの適用により、ランサムウェア攻撃の成功の可能性を緩和
- 脅威インテリジェンスと包括的な侵害検出およびディセプション機能により、インシデント対応時間を短縮
- リアルタイム機能と履歴機能の両方を使用して、ネットワークフォレンジックとコンプライアンスプロジェクトをシンプル化

Deloitte 社の専門知識

1. **助言**
   インパクトのあるサイバーセキュリティに関する意思決定支援、セキュリティギャップ分析、導入ロードマップ作成における Deloitte 社の経験により、エンタープライズのお客様は、侵害時および将来の計画時に適切な意思決定を行うことができます。
2. **プロフェッショナルサービス**
   完全に管理された導入サービスと、既存のセキュリティ、ITSM、クラウドソリューションへのカスタマイズされた統合を体験できます。
3. **インシデント対応のマネージドサービス**
   Deloitte 社のインシデント対応専門家による迅速で最上級の支援を受け、侵害を阻止し、将来のインシデントを防止します。
4. **ライセンスサブスクリプション**
   Deloitte 社が提供する幅広いライセンスサブスクリプションから選んで購入できます。

お客様事例 - Akamai と Deloitte がお客様のランサムウェアの課題を解決した方法とは

あるお客様企業が、重大なランサムウェアイベントが発生したことで、重要なタイミングですぐに役立つコンサルテーションとソリューションをお求めになっていました。Deloitte　社のインシデント対応およびセキュリティチームの能力を結集し、Akamai Guardicore Segmentation によるネットワーク可視化、侵害フォレンジック、およびアタックサーフェス大幅縮小の継続対策を活用することにより、お困りだったお客様に「勝利のコンビネーション」を提供しました。

背景

あるエンタープライズ組織の事例です。そのお客様は重大なランサムウェアイベントに遭遇してコアビジネス業務が停止し、どのように対応を始めたらよいか苦慮されていました。数千台のサーバーで構成されるデータセンター全体が乗っ取られていたため、セキュリティ侵害を即座に安全な方法で阻止する必要がありました。Deloitte 社の助言を信頼していたそのお客様は、次に何をすべきかを電話して尋ねました。Deloitte チームはすでに Akamai Guardicore Segmentation の提供と展開の準備をしていたため、お客様は攻撃の規模を迅速に把握し、影響を受けた資産とアプリケーションを把握し、関連するアプリケーションの依存関係をすべて確認することができました。

ソリューション

Akamai Guardicore Segmentation は、クライアントの環境全体を個々のプロセスレベルにマッピングすることで、侵入されたインフラからマルウェアが通った可能性のあるすべてのルートを明らかにすることができました。そのため、Deloitte チームは、ネットワークの特定の部分に集中して追加のフォレンジック分析を行うことができました。その結果、お客様は業務を再開し、データセンターへのアクセスが復旧した後、侵害されたデバイスが残存することはありませんでした。

結果

ランサムウェア攻撃が解決され、データセンターがオンラインに戻り、業務を再開した後、このような攻撃が再び発生する可能性を減らすための対策が講じられました。多くのエンタープライズ企業のお客様と同様に、このお客様もレイヤー型セキュリティアプローチを採用し、複数の主要なソリューションを導入して、デバイス、アプリケーション、ユーザーなどを保護しています。しかし、フィッシングメールのような単純なきっかけが攻撃者の侵入口になる可能性があるため、攻撃を阻止するためにはこれらのソリューションでは不十分でした。ネットワーク全体の可視性、アプリケーションの依存関係、およびデータセンターにアクセスできるユーザーに基づいて、お客様は正確なマイクロセグメンテーション制御を導入し、今後ランサムウェア侵害を受ける可能性のあるルートを大幅に削減することができました。

ソリューションの価値を実感し、Deloitte の専門知識に対する信頼を強めたため、このお客様はゼロトラスト・セグメンテーションの提供を継続するためにこのソリューションを維持することを決定し、Deloitte 社に日々の技術管理を依頼されました。

まとめ

Deloitte社は、クライアント向けのゼロトラスト・プロジェクトを実施した経験と深い技術専門知識を備えた、クライアント向け Akamai Guardicore Segmentation の展開と管理の理想的なパートナーです。クライアント企業様は、アタックサーフェスの縮小、ラテラルムーブメントの制御、アプリケーションのリングフェンシング、ランサムウェアの緩和など、あらゆるセキュリティ対策にこの技術をご利用の際には、Deloitte 社をご信頼ください。

Deloitte 社について

Deloitte 社は、Fortune 500® の 90% 近く、および 7,000 社以上の民間企業を含む、世界で最も賞賛されるブランドの多くに、業界をリードする監査、コンサルティング、税務、アドバイザリーのサービスを提供しています。社員は公益のために力を合わせ、今日の市場を牽引し、形成している業界のさまざまな分野で働いています。測定可能で継続的な結果を提供することで、資本市場に対する人々の信頼を強化し、課題を変革と繁栄のチャンスと見なすようにクライアントを促し、より強力な経済とより健全な社会への道を導いています。Deloitte は、クライアントにとって最も重要な市場でクライアントにサービスを提供する最大のグローバルプロフェッショナルサービスネットワークの一員であることを誇りに思っています。175 年以上のサービスの実績を持ち、メンバー企業のネットワークは 150 以上の国と地域に広がっています。約 415,000 人の Deloitte 社員が世界でどのようにつながってインパクトを実現されているかについては、deloitte.com をご覧ください。

お問い合わせ先

Ola Sergatchov
Akamai、Head of Global Strategic Alliances
osergatc@akamai.com

 | サポート | 公開日：2024 年 3 月