Akamai お客様事例

米国のヘルスケア企業が 1 日に 4,000 件以上のサイバー攻撃を阻止

ネットワークエンジニアチームは、マイクロセグメンテーションによるレイヤー 7 の可視化とスマートポリシーを使用して、サイバーリスクを軽減

ランサムウェアを阻止 | 可視性の向上 | ポリシーの改善

患者と適切なヘルスケアを繋げる

ますます巧妙化するサイバー攻撃に先手を打ちながら、同時に患者の命に直結するネットワークを守る必要があることを想像してみてください。これは、ある中規模ヘルスケア企業にとっての課題でした。同社のネットワークエンジニアリングチームは、拡大するランサムウェアの脅威と可視性の向上の必要性に直面していました。Akamai Guardicore Segmentation を導入し、企業のセキュリティポスチャの強化を実現しました。

ゼロトラスト・アーキテクチャの拡張

この組織は、ゼロトラストの原則に基づいて IT 環境を強化しながら、HIPAA および SOC 2 認証要件に適合するという、大胆なビジョンを持っています。それは大きな賭けだったため、ネットワークエンジニアリングチームは次のような目標を掲げました。

- セキュリティインシデントの発生時でも、重要なアプリケーションのオンライン状態を維持する
- ランサムウェアの拡散を抑制することで、攻撃の影響を軽減する
- 従来のファイアウォールをはるかに超えた詳細なネットワーク可視性を獲得する

同組織は、既存の IT インフラのリッピングや置き換えを必要としない、コスト効率に優れた、スケーラブルなマイクロセグメンテーションソリューションを必要としていました。さらに、少数精鋭のチームでも管理ができるほどシンプルであると同時に、企業とともに成長できるスケーラビリティも必要でした。

あるネットワークエンジニアはこのように説明しました。「ランサムウェアはヘルスケアを標的としています。こうした脅威を早期に特定し速やかに排除することでより効果的に対処できます」。

Healthcare Company

所在地

米国

業種

ヘルスケア & 生命科学

ソリューション

Akamai Guardicore Segmentation

Akamai

組織に合ったマイクロセグメンテーションソリューションの探求

コンテナ化のアプローチを早期に断念し、同社はマイクロセグメンテーションソリューションの可能性を検討しました。「次世代ファイアウォールと同じ機能、つまりアプリケーションレイヤーでの可視性を求めていました」と、ネットワークエンジニアは説明します。

多くのソリューションを評価する中で、Akamai Guardicore Segmentation に出会いました。同社は Akamai のエンジニアが提供した実践的なサポートと分かりやすいデモを受けて、契約を結びました。ソリューションには次の項目が全て含まれていました。

- **深い可視性：**レイヤー 7 の検査とネットワーク全体に関する知見
- **導入の容易さ：**ハードウェアを追加しないソフトウェアベースのエージェント
- **回復力：**コアネットワークに単一障害点なし
- **柔軟性：**多様なオペレーティングシステムのサポート

IT インフラおよび情報セキュリティ担当 Vice President は、Akamai Guardicore Segmentation の導入によって、少数精鋭のチームに大きなメリットがもたらされていると言います。「導入を開始してすぐに、可視性と制御の面でメリットを感じられました。

複数の水平方向（East-West）ファイアウォールを購入して管理する必要がなくなり、コストを大幅に削減し、ファイアウォールでは不可能なレベルの可視性を得ることができます」と、IT インフラ担当マネージャーは付け加えました。

ランサムウェアを即座に停止

導入後間もなく、見事な成果が現れました。アプリケーションのリングフェンシングを改善し、すぐに使用できる Akamai Guardicore Segmentation のランサムウェア防止ポリシーを適用することで、初日から 4,000 件のサイバー攻撃を無効化したのです。このソリューションには、組織固有のニーズに合わせて調整されたポリシーも備わっています。

「中間的なポリシーには、アラートモードを使用して、ダウンタイムを発生させることなくインシデントにフラグを立てることにしました。中断することなくポリシーを改めることができる点が、非常に優れています」と、あるネットワークエンジニアは語りました。

> Akamai Guardicore Segmentation は、ランサムウェアの懸念に対処する以上のことを可能にしました。サイバーセキュリティへのアプローチを強化してくれたのです。
>
> **– ネットワークエンジニア**

> 「ゼロトラストへの道のりは非常に困難です。Akamai Guardicore Segmentation は、コストと複雑さの課題を減らしながら、私たちが迅速に導入するのをサポートしてくれました」
>
> **—IT インフラおよび情報セキュリティ担当 Vice President**

他に類を見ないレイヤー 7 の知見を得る

IT インフラ担当マネージャーによると、Akamai Guardicore Segmentation は、さまざまなアプリケーション間のトラフィックフローに関する貴重な視点を提供しています。このソリューションによって、チームは大量の貴重なデータを活用できるようになりました。チームは、レイヤー 4 ログを超えて、ユーザー ID、コマンドライン入力、サービス相関に至るまで、詳細な情報まで検査することができます。

「当社のネットワークチームは、トラフィックフローを調べて問題をトラブルシューティングし、インシデントをくまなく調査するために必要な情報をセキュリティチームに提供できます」と、ネットワークエンジニアは述べています。

この可視性は、予期しないポリシー違反が発生したときに役立ちました。ある新入社員が、家庭用ルーターで保護された LAN ポートを経由せず、PC を通信事業者の顧客構内設備（CPE）に直接接続したのです。CPE が PC にパブリック IP を割り当て、インターネットのパブリックスキャンを受けやすくなったため、これは全く問題ではありませんでした。

同社のネットワークエンジニアは次のように説明します。「Akamai Guardicore Segmentation は問題を即座に検知するため、PC を隔離し、エスカレーションする前に状況に対処することができました。さらに、将来的に類似のインシデントが起こるのを防ぐためのポリシーを作成する上で、非常に参考になりました」。

ラベリングをスマート化してポリシーを改善

直感的なラベル付けとポリシー作成により、ネットワークエンジニアリングチームはトラフィックを容易にマッピングし、セキュリティルールを適用できました。ネットワークエンジニアはこのように述べています。「私たちは、環境に最適なものを決定できました。この機能は、期待以上の成果を上げ、効率的なポリシー作成の助けになりました」。

たとえば、チームはプリントサーバーへのアクセスを制限し、信頼済みのゾーンのみを許可しました。これにより、組織全体のセキュリティポスチャが向上します。エンジニアはこう続けます。「これにより、すぐさま成果を出せるようになりました」。

可視性の向上で自信を高める

思いがけないメリットもありました。内部トラフィックフローとアプリケーションのふるまいを明確に把握できるようになったのです。この新たな可視性により、アプリケーション所有者とのコラボレーションが向上し、メンテナンスウィンドウが合理化されました。たとえば、チームには、アプリケーション所有者のトラフィックがブロックされているかどうかを示す権限が与えられます。

「これまでは、トラブルシューティングと将来への備えが問題でした。今では、カットオーバー中に、古いサーバーから新しいサーバーにトラフィックがいつ移行したか、自信を持って確認できるようになりました。これにより、レガシーシステムを確実に撤去することができました」と、ネットワークエンジニアは述べています。

同組織の IT インフラおよび情報セキュリティ担当 Vice President は次のように結びました。「Akamai Guardicore Segmentation はすでに大きな効果を与えており、セキュリティ対策において不可欠な製品となっています。この展開を組織全体に拡大していくことを楽しみにしています」。

| 公開日：2025 年 2 月