AKAMAI お客様事例

製造業界の上場企業、Akamai の導入でセキュリティ制御の標準化と時間の節約を実現

安全なグローバルソリューションを必要としていた製造会社

包括的なネットワーク可視性

IT インフラ全体のセグメンテーション

ランサムウェアの脅威への対応

お客様

NYSE に上場し、世界中の市場に参入している大手製造会社。

Manufacturing Company

所在地
米国

業種
製造

ソリューション
Akamai Guardicore Segmentation

主な効果
- ラテラルムーブメントによるランサムウェアの拡散を緩和する
- 詳細に可視化する
- セグメンテーションによってエンドポイントのセキュリティを確保する
- インシデント対応を迅速化する

課題

グローバルなエンタープライズを保護

IT セキュリティグループは、世界中の複数のサイトを管理しています。ほとんどのサイトはオフィスと製造施設の併設です。堅牢なセキュリティ体制を確立するために、チームは組織全体でセキュリティ制御を標準化し、分散した各地域に一貫した保護を提供する必要がありました。

「オープンでフラットなネットワークから、ベストプラクティスのセグメント化アーキテクチャに移行したいと考えていました」と、セグメンテーションプロジェクトを率いるインフラアーキテクトは説明しています。

多くの企業と同様に、この製造会社も当初はファイアウォールに目を向けました。

しかし、ネットワーク全体で複数のインフラベースルールとワークステーションレベルの変更や更新を管理しようとすると、単一のサイトでも膨大な時間がかかることがすぐに判明しました。さらに、可視性は改善されましたが、その効果は特定のゾーンでしか得られず、ネットワークアクティビティとアセット間の依存度をすべて一元管理するのは困難でした。

不正なラテラルムーブメント（横方向の移動）の阻止

ファイアウォールのセグメンテーション制御は厳密ではないため、セキュリティチームのもう 1 つの懸念を払拭できませんでした。つまり、管理されていないピアツーピアの通信です。そのため、この特定の領域に保護と可視性を拡大することが不可欠でした。この問題に対処できないと、パス・ザ・ハッシュ攻撃やランサムウェア、エンドポイント間のラテラルムーブメント（横方向の移動）を利用するその他の脅威に対する脆弱性を放置することになります。

Akamai

ソリューションの選択

扱いにくいファイアウォール制御をいくつか試した後、チームは Akamai Guardicore Segmentation の存在を知り、社内で次世代セグメンテーションのメリットと可能性を検討しました。

新しいソリューションを導入する際は必ず、包括的な調査を実施する必要があるため、複数の代替ソリューションも評価しました。徹底的に検証した結果、Akamai Guardicore Segmentation の導入を決めました。「Akamai のように、すべてを網羅するソリューションは他にはありませんでした。トラフィック監視、柔軟なラベリング、アプリケーションレベルのリッチな可視性を、クライアント上の単一エージェントのフットプリントのみで得ることができます」とインフラアーキテクトは述べています。

> “
>
> マシンにエージェントを 1 つ組み込むだけで、ラテラルムーブメント（横方向の動き）によるエンドポイント攻撃の問題を完全に解決できました。
>
> 製造会社、インフラアーキテクト

Akamai Guardicore Segmentation

プロジェクトの第 1 段階で、同社は Akamai Guardicore Segmentation を約 2,000 台のワークステーションに展開しました。IT セキュリティチームは、ソリューションの導入後すぐに、ネットワークと通信フローの可視性が改善したことを確認できました。

新しい知見とセグメンテーションの効果

「Akamai トラフィックマップのおかげで可視性が 1000% 向上し、PC 間の通信も把握できるようになりました」とインフラアーキテクトは述べています。

各コンピューターのアクティビティにドリルダウンする機能とともに、全体的なアプリケーションレベルのアクティビティも把握できるため、組織は豊富な情報からセキュリティ判断を下すことができます。たとえば、ユーザーが自宅のプリンター用アプリケーションを会社のノートパソコンにインストールすると、そうしたアプリケーションの多くは、サポート対象のデバイスを求めて会社のネットワークを常にスキャンするようになります。Akamai の可視性で得られたこの新たな知見に基づき、チームはこうしたスキャンを停止させることができました。

Akamai Hunt：Akamai Guardicore Segmentation で脅威を検知

ネットワークアクティビティのこの新しい検知機能により、外部からの攻撃も阻止できます。たとえば、プラットフォームの展開直後に、Akamai Hunt サービスは、GoldenSpy と呼ばれるマルウェアの既知の特性を持つファイルと通信するアセットを検知しました。Hunt チームは、検知した脅威を IT セキュリティチームに通知しました。顧客には、感染範囲の分析、想定されるリスク（観測結果を GoldenSpy に関する MITRE の情報と照会）、フォレンジック調査（Insight を活用）を提示し、内部調査と緩和策も提案します。同社は、Akamai ポリシー制御を駆使して、感染したシステムを隔離し、マルウェアが新たなマシンを求めて横方向に移動しようとするのを阻止しました。

標準化と時間の節約

この製造会社は現在、グローバル・ワークステーション・ポリシーを一元管理するなど、ポリシーの策定と一元管理も実践しています。また、ユースケースで必要な場合は、1 回限りの例外を設定する柔軟性も備えています。そのため、Akamai エージェントを導入していれば、場所を問わず一貫してポリシーを適用することができ、設定ミスや遅延のリスクを低減できます。

さらに、組織でのポリシー策定時間も大幅に短縮されました。たとえば、新しいプラットフォームの導入前は、ファイアウォール制御の変更に数日かかっていました。初期ガイドとして Akamai の新しいポリシーテンプレートを使用することで、IT セキュリティチームは、非常に複雑なユースケースでも 1 時間かからずにセキュリティ制御を作成できるようになり、わずか数秒でインストールベース全体に適用できます。

Akamai のさらなる活用

プロジェクトの当初の主眼は、エンドポイントセグメンテーションとアクセスのセキュリティ制御を標準化することでしたが、他のユースケースへの Akamai の適用も計画しています。関係者は、サーバーや、組織の ERP システムといった重要なアプリケーションへの保護の拡大を検討しています。

今後の計画にかかわらず、当初のプロジェクトは会社側で成功だったと評価されています。アタックサーフェスは縮小し、会社のワークステーションに対するリスクも大幅に軽減されています。チームは、エンドポイント間で攻撃が横方向に移動するのを阻止する、組織のセキュリティ体制に自信を深めています。プロジェクトリーダーは次のように説明しています。「マシンにエージェントを 1 つ組み込むだけで、問題を完全に解決できました。ポリシーを一切適用していないワークステーションにも、30 秒以内であらゆるセキュリティ制御を導入できます」

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

> Akamai トラフィックマップのおかげで可視性が 1000% 向上し、PC 間の通信も把握できるようになりました。
>
> 製造会社、インフラアーキテクト