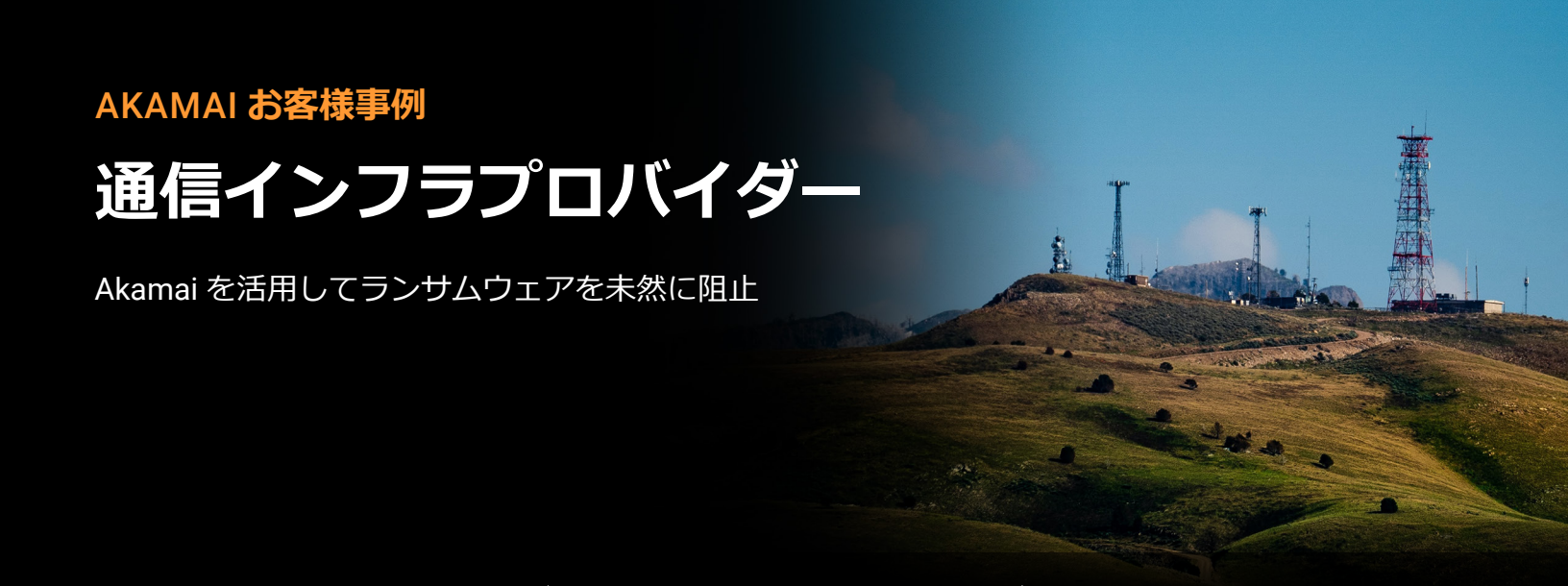
AKAMAI お客様事例

通信インフラプロバイダー

Akamai を活用してランサムウェアを未然に阻止



100 万ドルの損失を未然に阻止

潜在的なシャドー IT の防止

水平方向（East/West）のトラフィックの可視化

お客様

急速に変化する現代において、米国を拠点とするこの通信インフラプロバイダーは企業や住民の常時接続を確保する役割を担っています。中でも、顧客が日常生活で利用する携帯電話基地局や光ファイバーの広範なネットワークを維持しています。

課題

エンドポイントの可視性と制御における制約

6,000 台以上のラップトップが組織全体に展開されているため、IT セキュリティチームはそれらが IT 環境全体に及ぼすリスクについて懸念を深めていました。さらに、一部のパワーユーザーによるシャドー IT の問題も継続しており、対処する必要もありました。

以前からエンドユーザー・コンピューティング・チームがいくつかのセキュリティ対策を実施していましたが、限界がありました。マルウェアの伝播を効果的に阻止するために、ユーザーによるシステムへのアクセスを細かく制御したり、ピアツーピア通信を制限したりすることもできませんでした（特に後者は組織で大きな懸念となっていました）。

こうしたギャップに対処するために、関係者は、可視性と詳細なセグメンテーション制御を従業員のデバイスに拡張できるソリューションを導入することで、ビジネスのセキュリティ体制を改善したいと考えていました。これには、承認されていないラテラルムーブメント（横方向の移動）を観察し、防止する効果も期待されていました。

ソリューションの選択

セキュリティ関係者は、数回にわたって Akamai Guardicore Segmentation の検討を重ねており、サイバーセキュリティに関する複数のユースケースへの適用に関心を持っていました。同社は、きめ細かな可視性と分かりやすいポリシー作成プロセスに大きな可能性を感じ、段階的にアプローチしていくことに決めました。

通信インフラプロバイダー

所在地
米国

業種
通信インフラ

ソリューション
Akamai Guardicore Segmentation

主な効果
- ランサムウェアの防止
- シャドー IT の停止
- 水平方向（East/West）のトラフィックの可視化

Akamai のソフトウェア定義のセグメンテーションポリシーは基盤インフラに縛られていないため、同社はいくつものセキュリティ対策プロジェクトに対処することも可能でした。しかし、従業員のラップトップの危険性が高いと認識し、Akamai エージェントをエンドポイントに導入することを優先しました。

Akamai Guardicore Segmentation

プロジェクトの開始後、Akamai の合理化された Windows エージェントが組織のコンピュータに迅速に導入されました。拡張されたプロセスレベルの可視性により、ユーザーアクセスとラップトップアクティビティが可視化されました。

IT セキュリティチームは、こうしたエンドポイントのセキュリティ制御を一元的に作成・管理することができました。この作業はすべて、正確な環境データに基づいています。その後、ログイン試行の失敗など、特定の Microsoft Remote Desktop Protocol（RDP）アクティビティに関するアラートを含む、複数のポリシーも迅速に設定することができました。

きめ細かい可視性を実現

開後まもなく、異常な RDP 関連アクティビティを報告するように設定されたポリシーが、おびただしい数のアラートを発信したことがありました。ログインに失敗するケースが相次いだため、攻撃者が総当たり攻撃を試みていることがすぐに判明しました。

IT セキュリティチームが状況をつぶさに監視したところ、その攻撃者は攻撃を続けていたため、Akamai エージェントを使用してすべてのエンドポイントで RDP をコールしてブロックすることにしました。わずか数回のクリックで、RDP を無効にする新しいセグメンテーションポリシーを作成・適用し、エンドポイントが 1 つでも侵害される前に攻撃者を阻止したのです。

ランサムウェアの活動を阻止

セキュリティチームは、事後検証プロセスにおいて、あらゆる指標が既知の主要なランサムウェア攻撃者の存在を示していることにすぐに気づきました。

その攻撃キャンペーンが成功していたら、攻撃者はいつもの手口で、アクセスできたものを暗号化し、身代金要求を試みたと思われます。同社の組織規模と現在の傾向を考えると、攻撃者の身代金要求額は 100 万ドルに達していたかもしれません。もし、ERP システムなど、ビジネスに不可欠な資産が侵害されていたら、さらに大きな混乱とダウンタイムが発生していた可能性があります。

しかし、迅速に対応したセキュリティチームと Akamai のおかげで、攻撃未遂による組織への影響はありませんでした。

シャドー IT の停止

Guardicore のプラットフォームは、外部からの脅威を食い止めるだけでなく、社内における課題にも効果を発揮しました。Akamai の導入前はエンドポイントの可視性が限られていたため、一部のユーザーは正式なプロセスを簡単に回避し、組織のポリシーに反して勝手に行動していました。エンドポイントに対する新たな知見とセキュリティ制御の実施能力が得られたことで、IT セキュリティ部門はシャドー IT を抑制することに成功しました。また、DevOps 組織のメンバーが公式な承認ルートを通さずに新しいリソースを立ち上げようとすることも防止できました。

Akamai による保護の拡大

この通信インフラプロバイダーにとって、エンドポイントの保護は始まりにすぎません。同社はさらに新機能追加の検討、データセンターへの Akamai の展開、Citrix 環境のセキュリティ確保、外部ベンダーのサードパーティーアクセス制御の適用を予定しています。

同社は、このプラットフォームの柔軟性により、将来に M&A 戦略やデジタルトランスフォーメーション構想が展開された場合でも、巧妙な脅威に対する保護をあらゆる環境に拡大できるという安心感を得ることができました。

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