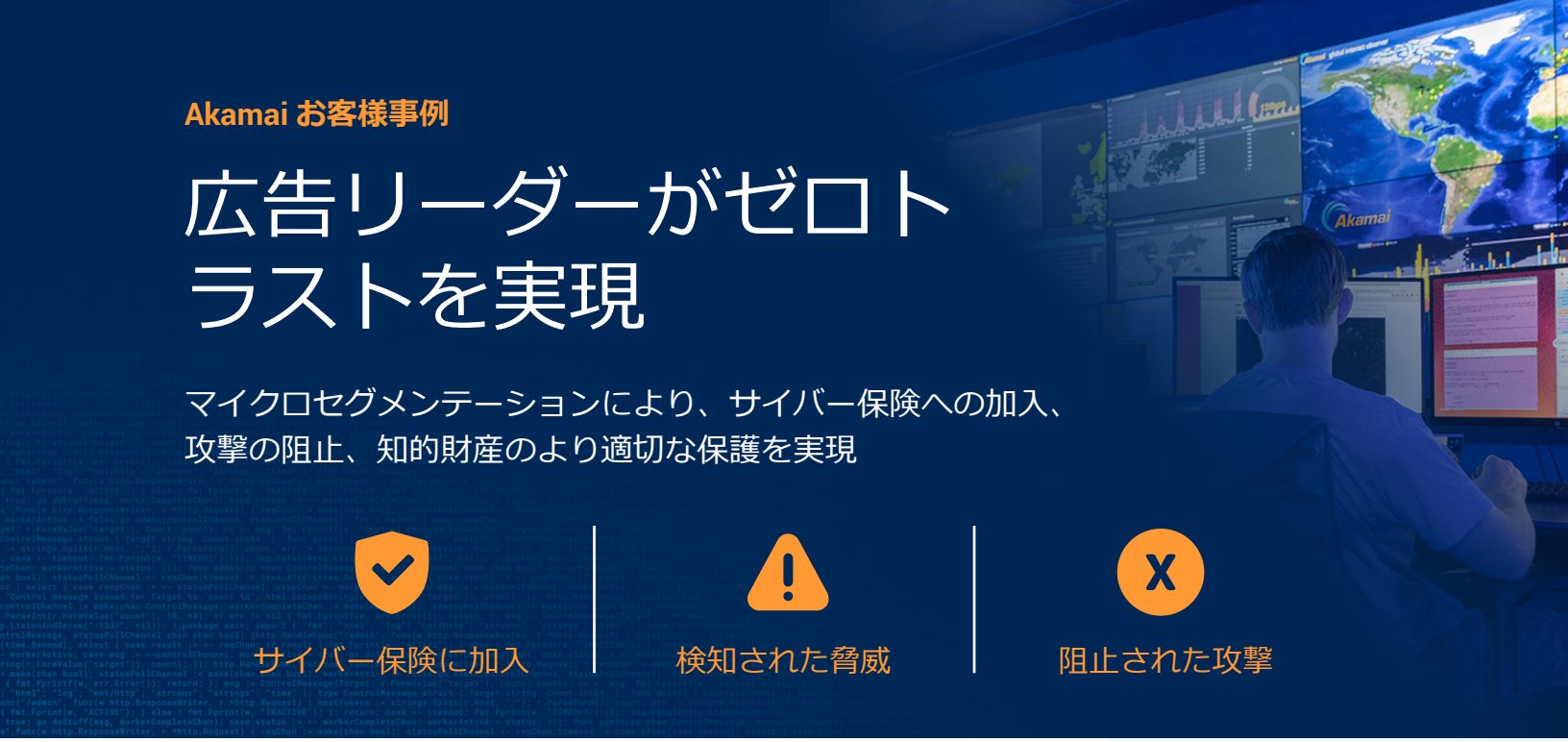
Akamai お客様事例

広告リーダーがゼロトラストを実現

マイクロセグメンテーションにより、サイバー保険への加入、攻撃の阻止、知的財産のより適切な保護を実現



サイバー保険に加入

検知された脅威

阻止された攻撃

ブランドとテレビ視聴者をつなぐ

コネクテッド TV 広告のグローバルリーダーは、断片化されたストリーミング視聴者へのリーチ率を改善することで、ブランドが広告の費用対効果を最大化できるよう支援しています。同社はサイバー保険に加入したいと考え、Akamai Guardicore Segmentation を導入し、セキュリティ対策を強化しました。

サイバー保険への加入

イノベーターである同社は、当然ながら知的財産（IP）を保護しています。現代の多くの企業と同様に、ボットやハッカーが内部のサーバーやアプリに侵入した場合、同社の IP が漏洩する可能性がありました。

潜在的な侵害による経済的影響を緩和するため、親会社にサイバー保険への加入を求められました。サイバー攻撃の増加に伴い、保険会社は保険加入を認める前に、企業のセキュリティ対策を精査しています。この点を念頭に、同社は内部にセグメンテーションを導入することを決断しました。

Advertising Leader

所在地

米国

業種

メディアおよびエンターテインメント

ソリューション

Akamai Guardicore Segmentation

Akamai

内部セグメンテーション制御の展開

同社が解決策として見出したのが、マイクロセグメンテーションにソフトウェアベースのアプローチを提供する Akamai Guardicore Segmentation です。デジタル環境全体でラテラルムーブメント（横方向の移動）を阻止するように設計されている Akamai Guardicore Segmentation は、同社の IP 保護における重要な要素となります。マイクロセグメンテーションにより、同社は IP を含むサーバーとアプリケーション、そしてそれらのワークロードがインフラの他の部分から完全に分離されるようにすることができます。

Akamai Guardicore Segmentation を使用して重要な資産をリングフェンシングし、ラテラルムーブメントを制限することで、攻撃者が IT 環境全体を簡単に移動できないようにすることができます。物理環境と仮想環境の両方における移動をきめ細かく可視化することで、攻撃者をその場で阻止します。

ランサムウェア攻撃の検知と防止

同社は Akamai Guardicore Segmentation が最適な選択肢であることを確認するために、概念実証（PoC）を実施しました。PoC 中、この Akamai ソリューションは多くの攻撃者に加え、ランサムウェアのインシデントも検知しました。

Akamai Guardicore Segmentation が環境を保護する能力を目の当たりにした同社は、適切なソリューションを見つけたことを確信しました。今後、Linux、ベアメタル、クラウドが混在する 3,000 台以上のサーバーと、約 1,500 のコンテナ（Docker と Kubernetes）をセグメント化する計画です。

 | 公開日：2024 年 11 月