Akamai

ホワイトペーパー

現代の法律事務所におけるセキュリティ確保

重要なアプリケーションとクライアントデータの保護

はじめに

法律の専門家は、機微な情報を日々取り扱っています。そのため、多くの法律事務所が高度なセキュリティ制御に投資し、ゼロトラストの IT システム／プロセスを設計することで、重要なアプリケーションのセキュリティを確保し、エンドユーザーによるアクセスを制御しています。

ゼロトラスト・アプローチでは、最小権限の原則に基づいて、許可されたユーザー、システム、アプリケーションに、それぞれの役割に必要なアクセス権のみを確実に付与すると同時に、ラテラルムーブメント（横方向の移動）、ランサムウェア、不正アクセスから保護します。このゼロトラスト・アプローチを実装するための非常に柔軟で安全な方法が、マイクロセグメンテーションです。

ゼロトラスト・アプローチがなぜ重要なのかを理解するために、過去の出来事を振り返ってみましょう。

大きな注目を集めたセキュリティ侵害：法曹界への警鐘

米国連邦当局はかねてより、大量の企業データを保有する大手法律事務所はサイバー犯罪者にとって格好の標的になると警告してきました。FBI は、大手法律事務所がサイバー犯罪組織の標的となっていることを 2009 年から警告し続けています。2011 年には、大手法律事務所 200 社を招いて、法曹界を標的とする巧妙なサイバー攻撃の増加について話し合っています。

> **このゼロトラスト・アプローチを実装するための非常に柔軟で安全な方法が、マイクロセグメンテーションです。**

Law.com によると、2014 年以降、14 の州にある 100 社以上の法律事務所がデータ漏えいを報告しています。アメリカ法曹協会が作成した『2022 Legal Technology Survey Report』（法曹界におけるテクノロジーの使用に関する年次調査）によると、1/4 以上の法律事務所（規模を問わず）でセキュリティ侵害が発生していました。これらのセキュリティ侵害により、ランサムウェアを原因とするダウンタイムから、インターネットでのクライアントデータの漏えいに関する長期に及ぶ訴訟など、さまざまな影響が生じています。

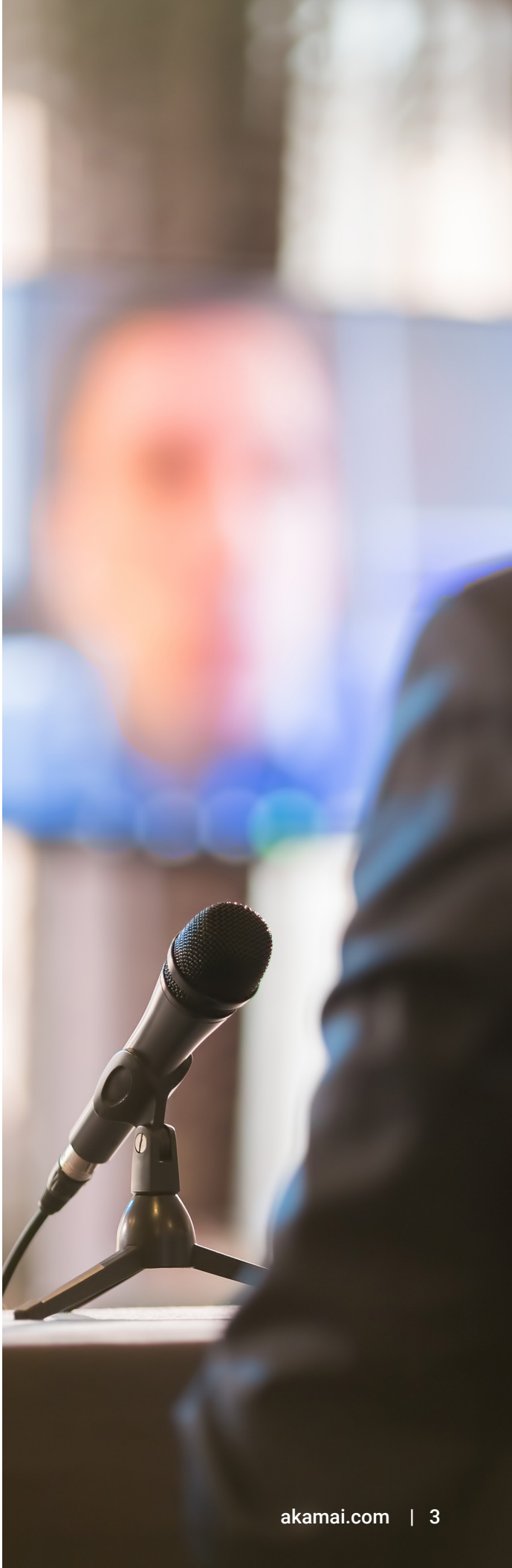
2015 年には、Cisco が毎年発表する、ハッカーの標的になりやすい業界のランキングに法曹界が初めて入りました。その結果、多くの金融機関が、取引を行う法律事務所に対して、サイバーセキュリティ対策の定期監査を要求するようになりました。

特に、国際的法律事務所の Mossack Fonseca & Co と DLA Piper で発生した 2 件の大規模セキュリティ侵害は、法曹業界および金融業界全体に警鐘を鳴らす結果となりました。オフショア法律事務所の Mossack Fonseca & Co で、1,100 万件以上のドキュメント、40 年以上分の記録が漏えいしました（漏えいした文書は「パナマ文書」と呼ばれています）。この事件により、グローバル企業や影響力を持つ世界のリーダーのタックスヘイブンやオフショア口座が漏えいし、深刻な事態を招く結果となりました。このデータ漏えい事件が引き金となり、同法律事務所は 2018 年に廃業しました。法律事務所には、保有する情報を保護するためにあらゆる合理的努力を払う、倫理的責任および受託者責任があります。「パナマ文書」データ漏えい事件は、法律事務所によるクライアントの機微な情報の漏えいとしては最大規模のものであり、この事件を契機に法曹業界では、サイバーセキュリティに対するアプローチが変化しています。しかし、法律事務所がセキュリティ対策を改めて強化しているにもかかわらず、攻撃の手が緩む気配はありません。

> **1/4 以上の法律事務所でセキュリティ侵害が発生している。**
>
> **— アメリカ法曹協会『Legal Technology Survey Report 2022』**

Mossack Fonseca & Co のデータ漏えいとほぼ同時期に、40 か国超で事業を展開する大手法律事務所の DLA Piper も NotPetya マルウェア攻撃の餌食となりました。この攻撃により、同事務所は数週間の業務中断、数百万ドルのビジネス損失、回復コスト、評判の失墜などの被害を受けています。

最近では、Grubman Shire Meiselas & Sacks がランサムウェア攻撃を受けて、レディー・ガガ、レブロン・ジェームズ、マドンナなどの著名人クライアントに関する 756 ギガバイト分のデータが漏えいしています。同法律事務所が身代金の支払いに消極的だったため、攻撃者はレディー・ガガの情報を漏えいさせて、その他のクライアントに関する詳細データを競売にかけました。

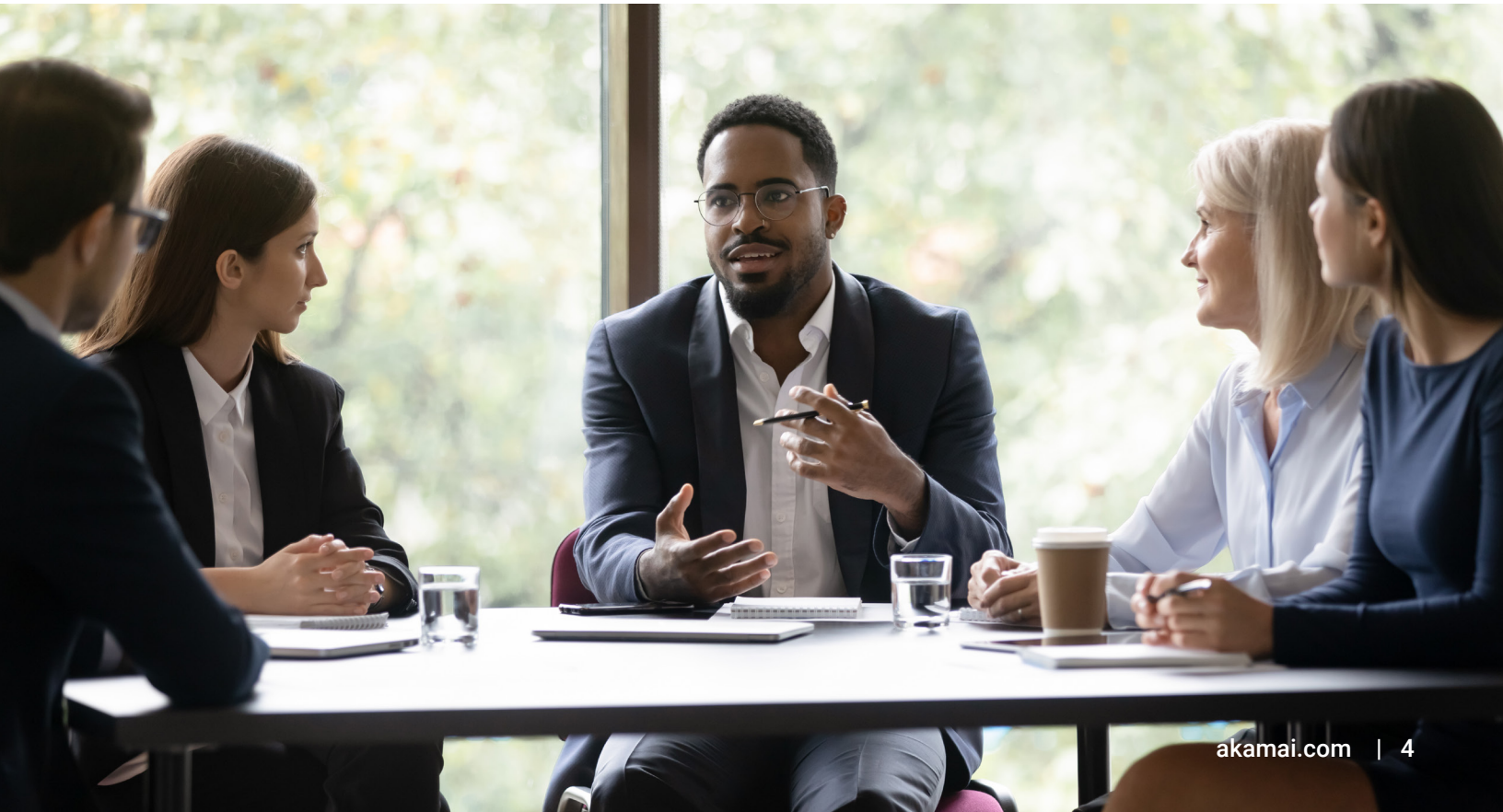


現代の法律事務所には現代のサイバーセキュリティソリューションが必要

上記のデータ漏えいの多くは、フィッシング、マルウェア、ランサムウェアなどの高度な持続型脅威（APT）攻撃を通じて、クライアントの機微な情報、合併資料、知的財産、財務情報を盗むものでした。サイバー犯罪は金銭的利益が大きいため、攻撃ツールやプロのチームに多額の投資を行う犯罪組織が攻撃者を支援するケースも増えています。

> **IT 環境を適切にセグメント化していない法律事務所は、データ漏えいが発生しても保険金の支払いを拒否される可能性があります。**

また、クライアントが法律事務所を選択する際には、サイバーセキュリティが重要な判断基準となっています。最新のセキュリティ制御を導入していない法律事務所は、セキュリティ体制を強化し、クライアントデータ保護を重視する姿勢を示している法律事務所にビジネスを奪われる可能性が高くなります。また、現在では多くのサイバー保険会社が、機微な情報やアプリケーションを何らかの形でセグメント化することを求めています。IT 環境を適切にセグメント化していない法律事務所は、データ漏えいが発生しても保険金の支払いを拒否される可能性があります。

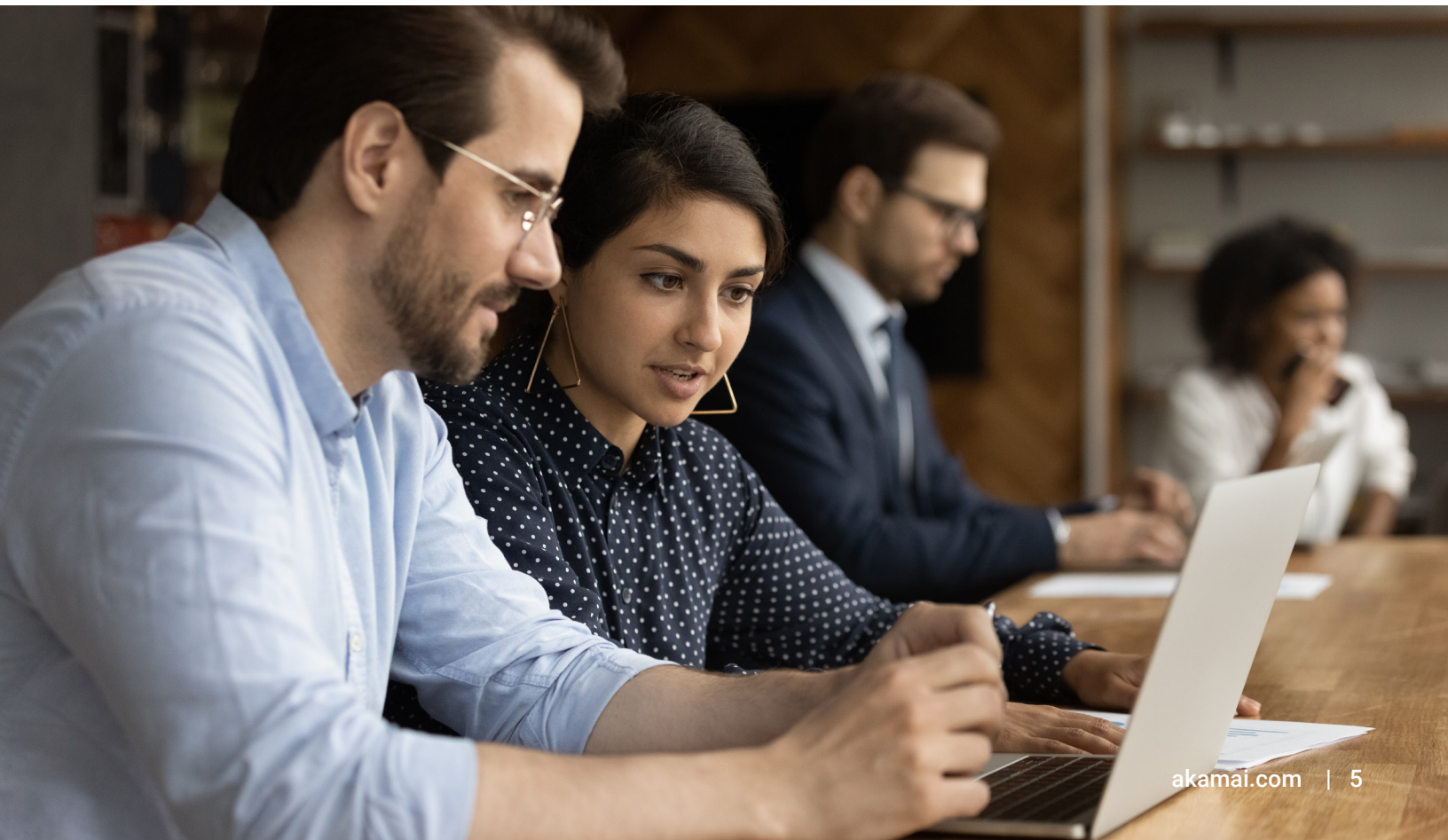


必要なのは、重要アプリケーションの保護

現在の法律事務所は、以前とは異なり、機微な情報の安全な保管場所ではなくなっています。サイバー犯罪者は法律事務所を格好の標的として認識しています。法律事務所には、企業の機微な情報や専有データが保管されているためです。

実際、サイバー犯罪者の多くは、法律事務所のクライアントを攻撃するよりも、法律事務所を攻撃するほうが簡単だと考えています。そのため、特定の企業のデータを盗もうとする攻撃者は、その企業ではなく、その企業の法律事務所から盗もうとします。法律事務所には、機微な情報が豊富に保管されており、セキュリティ制御が不十分であることが少なくないため、攻撃者にとっては魅力的な標的となっています。

攻撃者は、法律事務所のビジネスクリティカルなアプリケーション、特に文書管理システム（DMS）や電子メールに保存されている情報に強い関心を持っています。IT セキュリティの観点から見ると、法律事務所の最も重要なビジネスアプリケーションは、DMS アプリケーションと電子メールアプリケーションです。このようなアプリケーションには、クライアントの機微な情報の多くが保管されています。また、これらのアプリケーションはオンプレミスのデータセンターにあるとは限りません。



DMS アプリケーションは、ファイルとフォルダの一元管理、バージョン管理、電子メール管理、文書編集、インデックス作成と検索、権限管理など、幅広い機能を備えています。このアプリケーションは通常、仮想サーバーとベアメタルサーバーを組み合わせた異種混在 IT 環境に展開されており、セキュリティレベルの異なる複数のシステムと統合して使用します。この統合により、DMS は法律事務所にとってより便利なソリューションとなる一方、セキュリティが低下し、アタックサーフェスが大幅に増大するおそれもあります。

また、エンドポイントのモバイル化と動的化が進んだ結果、従来のセキュリティソリューションでエンドポイントを保護するのは困難となっています。多くの組織と同様、法律事務所は境界を防御するセキュリティツールに主に投資してきたためです。もはや、このようなソリューションでは法律事務所の重要アプリケーションは保護できません。加えて、多くの法律事務所には、攻撃者のラテラルムーブメント（横方向の移動）を検知または阻止するための制御機能がありません。そのため、感染したエンドポイントからネットワークに侵入したら、機微な情報を格納するシステムにそのままアクセスできてしまいます。

こうした課題を解決するため、法律事務所の多くが、固有のニーズや変化するニーズに対応できる、新世代のサイバーセキュリティソリューションを導入し始めています。ソフトウェアベースのセグメンテーション（マイクロセグメンテーション）により、ネットワーク内の通信をより詳細に制御し、許可されたユーザーとシステムのみが重要アプリケーションと通信できるゼロトラスト・アプローチを通じて、重要なアプリケーションとデータを保護できます。これにより、ネットワーク全体で攻撃者のラテラルムーブメントを阻止して、アタックサーフェスを縮小できます。

新型コロナウイルス感染症により、セキュリティの確保はさらに困難になっている：

- 多くの法律事務所がテレワークに移行した
- その結果、従業員は企業のオフィスではなく、安全性の低い自宅からネットワークに接続するようになった
- VPN ソリューションと VDI ソリューションの使用が増加したことで、セキュリティポリシーを実装したり、許可されたユーザーにネットワークトラフィックを関連付けたりすることがさらに困難になった

Akamai は次の 4 つの方法を通じて法律事務所によるクライアントデータの保護を支援

完全な可視性

ワークロードを包括的に可視化することで、機微な情報を格納するアプリケーションへのオープンな接続をすべて把握できます。

ユーザーアクセス制御

ポリシーを実装して、オンプレミスやクラウドにあるアプリケーションとデータに対するアクセスを制御できます。

ソフトウェアベースのセグメンテーション

DMS や電子メールなどの重要アプリケーションを迅速かつ柔軟にマイクロセグメント化することで、セキュリティ侵害が発生した場合の影響を制限できます。

脅威検知および防止

動的なセグメンテーション機能とディセプション機能により、進行中のセキュリティ侵害を検知して封じ込め、クライアントデータを保護できます。

Akamai Guardicore Segmentation による包括的保護

Akamai Guardicore Segmentation は、ビジネスクリティカルなアプリケーションを保護するための、業界で最も包括的なマイクロセグメンテーションソリューションです。セグメンテーションポリシーを速やかに実装して、継続的なメンテナンスをシンプル化し、ラテラルムーブメントを伴う脅威を効果的に緩和できます。

> **多くの法律事務所が、マイクロセグメンテーションなどのソリューションを活用して、ネットワーク内の通信をより詳細に制御し、承認を受けたユーザーとシステムのみが重要アプリケーションと通信できるよう許可することで、クライアントデータの保護を強化しています。**

Akamai ソリューションにより、データセンター内のすべてのアプリケーションとその他の資産（およびその依存関係）を視覚的に把握できます。セキュリティ担当者は、ネットワークレベル／プロセスレベルのセキュリティポリシーを迅速かつ直感的に作成および適用し、重要なアプリケーションと資産を分離およびセグメント化できます。ソフトウェア定義セグメンテーションは基盤となるインフラから独立しているため、オンプレミスシステム（レガシーシステムと最新システムの両方）、VM、コンテナ、クラウド、デバイスにまたがるワークロードを一貫して保護できます。

データセンターでのアプリケーションの配置先を問わず、個々のアプリケーションまたは論理的にグループ化されたアプリケーションに関するポリシーを作成できます。これらのポリシーにより、相互に通信できるアプリケーションと通信できないアプリケーションを規定して、真のゼロトラスト・アプローチを実現できます。さらに、セキュリティ侵害の検知と対応機能が統合されていることも Akamai Guardicore Segmentation ならではの特長の 1 つです。この統合により、複数の専用ツールを管理する煩わしさが軽減されます。ニューヨーク州金融サービス局（DFS）の規制や PCI DSS などの業界規制を遵守したり、法律事務所を監査する有名企業の要求を満たしたりするためには、セキュリティ侵害の検知と対応機能は必須です。

Akamai Guardicore Segmentation：重要アプリケーションを包括的に保護

クライアントデータを保護：複雑化と相互接続がますます進む環境において、ゼロトラスト・フレームワークの基盤を構築し、ネットワークセキュリティに関する対策とベストプラクティスを実施します。

重要アプリケーションを IT インフラから分離：リングフェンシングポリシーを使用して、DMS や電子メールアプリケーションなどの重要資産をセグメント化することで、法律事務所内外からの脅威を緩和します。

安全かつ迅速にクラウドに移行:クラウドに移行する前に、ワークロードをマッピングし、すべての重要アプリケーション（およびその依存関係）のインベントリを作成します。このマッピングを基盤として、リングフェンシングポリシーにより、移行プロセス全体を通してワークロードのセキュリティを一貫して確保できます。このアプローチにより、同じセキュリティ制御を維持しながら、ワークロードを迅速かつ安全にクラウドに移行できます。

セキュリティ侵害を効率的に緩和して、事業継続性を確保：水平方向（East/West）のトラフィックに対する詳細な可視性と、異常なふるまいを通知するセキュリティ侵害指標を使用して、ランサムウェアなどの脅威がビジネスの中断を招く前に攻撃者を阻止します。

ラテラルムーブメントを制限してリスクを緩和：内部に境界を設定して、ビジネスクリティカルなアプリケーションとシステムをリングフェンシングすることで、アタックサーフェスを縮小します。これにより、攻撃のラテラルムーブメントを効果的に阻止できるため、万が一セキュリティ侵害が発生しても損害を制限できます。

結論

Akamai Guardicore Segmentation により、法律事務所は、攻撃に利用される可能性のあるオープンな接続を可視化して把握できます。さらに、マイクロセグメンテーションにより、そのような接続のセキュリティを確保できます。

Akamai は、ハイブリッド IT 環境（仮想マシン、ベアメタルマシン、オンプレミス、IaaS、PaaS）にある重要アプリケーションを保護するための包括的なセキュリティソリューションを提供しています。アプリケーションの依存関係とフローを可視化して、きめ細かいセグメンテーションポリシーを適用できるだけでなく、セキュリティ侵害の検知と対応機能も統合されています。データの損失や業務の中断を防止するためには、こうした機能が不可欠です。

Akamai Guardicore Segmentation を使用することで、法律事務所は自社の環境をより詳細に把握して、重要アプリケーションのセキュリティを確保し、セキュリティ侵害が発生した場合の影響と対応時間を大幅に削減できます。さらに、このソリューションに含まれる、ソフトウェアベースのセグメンテーション機能は、従来型ファイアウォールなどの多くのセグメンテーションソリューションと比べて、コスト効率、柔軟性、有効性に大幅に優れ、より短時間で対応できます。Akamai Guardicore Segmentation は業界をリードするセキュリティソリューションであり、現代の法律事務所がセキュリティ上の課題を解決するための機能を豊富に備えています。

クライアントの貴重なデータを保護する方法をご紹介します。
詳細については、akamai.com/guardicore をご覧ください。

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティポスチャの適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 7 月。