金融サービスの規制コンプライアンス

5 つの主要なビジネス目標

目次

金融サービスのコンプライアンス機能の向上は、顧客体験の向上、生産性の向上、回復力のある成長につながります。

急速に変化する金融サービスの世界では、コンプライアンスを維持し、業務の耐障害性を維持することが重要です。この e ブックは、コンプライアンスのシンプル化、生産性の向上、顧客体験の向上、セキュリティコストの効率的な管理、耐障害性と信頼性の構築を実現するための構造化されたアプローチを提供します。コンプライアンスだけではセキュリティ全体を確保できませんが、監査に失敗すると業務の中断や財務上の重大な影響が生じる可能性があるため、経営陣にとって依然として最優先事項です。

セキュリティチームにとって、コンプライアンス評価は常に時間と人的資源を大量に消費する活動です。境界のないデジタル環境へのシフトとテレワークの台頭が、既に存在していた課題に追加されただけです。金融機関は、Payment Card Industry Data Security Standard（PCI DSS）、Digital Operational Resilience Act（デジタルオペレーションレジリエンス法、DORA）、Society for Worldwide Interbank Financial Telecommunication（国際銀行間通信協会、SWIFT）システムなどの基準を満たすために、環境を隔離し、規制対象資産をリングフェンスする必要があります。この e ブックは、金融機関がこれらの複雑さを克服し、次の **5 つの主要なビジネス目標**を達成するのに役立つ知見と戦略を提供します。

1. コンプライアンスのシンプル化
2. 生産性の向上
3. 顧客サービスの向上
4. セキュリティとコンプライアンスのコストを効率的に管理する
5. 耐障害性と信頼性を築く

金融サービスにおける Akamai

現在、大手銀行や資本市場、保険会社、フィンテック企業が Akamai に委託し、クラウドをパフォーマンスや脅威の見通しがきかない混沌とした環境から、セキュアで、信頼性の高いコスト効果の高いビジネス環境へと変革しています。

当社のクライアントには、次のような企業があります。

証券会社のトップ **20** 社すべて

銀行のトップ **20** 行中 **17** 行

フィンテック企業のトップ **10** 社中 **7** 社

1 コンプライアンスのシンプル化

マイクロセグメンテーションソリューションは、ネットワークを小規模な境界に分割し、個々のワークロードを分離することで、コンプライアンス環境の範囲を狭め、規制監査を合理化し、機微な情報へのアクセスを制限すると同時に、ネットワークトラフィックとデータフローを比類ないほど可視化することができます。

コンプライアンス環境の範囲を狭める

コンプライアンス関連のデータをセグメント化して他の IT 資産から分離できれば、コンプライアンス作業の範囲を大幅に縮小し、コストと複雑さを軽減できます。金融機関は、ネットワークの特定のセグメントにコンプライアンス活動を集中させることができるため、プロセスの効率化と人的資源にかかる負担の軽減が実現します。

コンプライアンスへの取り組みと監査プロセスの合理化

マイクロセグメンテーションは、コンプライアンス環境の範囲を縮小し、コンプライアンスの実証を容易にすることで、監査要求とプロセスを遵守する作業をシンプル化します。この合理化されたアプローチにより、時間を節約できるだけでなく、規制要件を満たす精度も向上します。

保護された API

最新の連邦金融機関審査会（FFIEC）情報テクノロジー検査ハンドブックに概説されているように、堅牢な API セキュリティ対策の実装は、金融機関が API を保護し、機微な情報を保護し、攻撃から防御するのに役立ちます。これは、厳格な API セキュリティ規制の遵守を維持するために不可欠です。

2

生産性の向上

統合セキュリティ管理

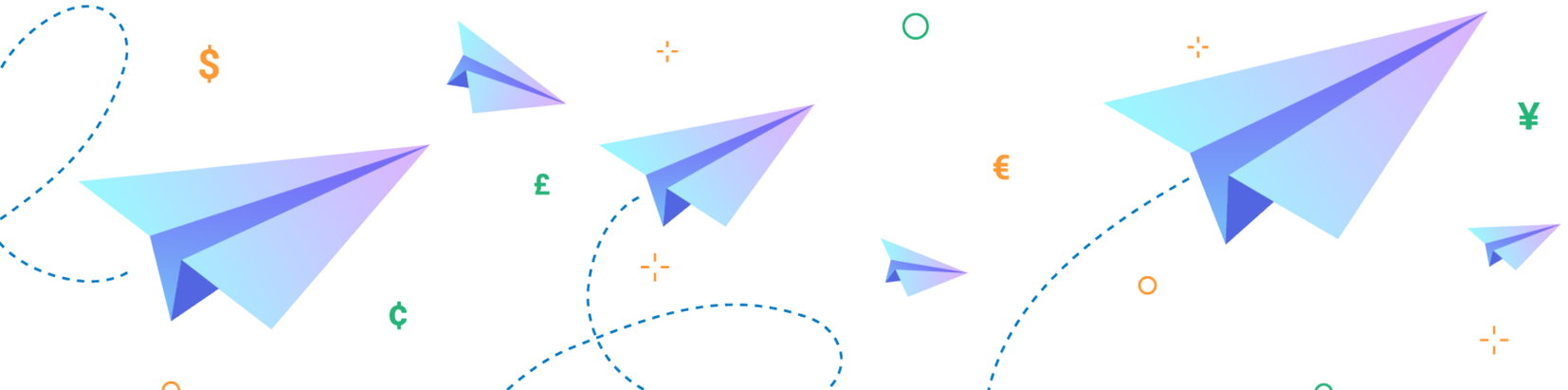
Akamai の統合プラットフォームを使用してセキュリティ管理を統合することで、複数のセキュリティソリューションの管理にかかる時間を短縮し、運用効率を向上させることができます。このアプローチにより、セキュリティチームは、運用に関する目先の問題ではなく、戦略的イニシアチブに集中することができます。

プロアクティブな脅威ハンティング

プロアクティブな脅威ハンティングにより、業務に影響が出る前に脅威を特定して無効化し、事業継続性を向上させることで生産性を高めることができます。Akamai の高度な脅威検知および緩和機能により、リソースの効率的な割り当てが可能になります。

高度な API 保護

人工知能（AI）と機械学習（ML）を活用したランタイム保護機能を使用することで、金融機関は高度な API 攻撃をリアルタイムで検知してブロックできるため、高度な攻撃者を阻止し、全体的な生産性を向上させることができます。



3

顧客サポートの向上

シームレスなユーザーアクセス

Akamai のエッジ・セキュリティ・ソリューションを使用することで、シームレスで安全な顧客体験を実現し、ユーザーの場所に関係なく、ユーザーデータを保護し、高いパフォーマンスを維持します。分散型サービス妨害（DDoS）からの保護と負荷分散によりサービスの可用性が向上するため、継続的なサービスが確保されます。これは、顧客の信頼と満足度を維持するために不可欠です。

パーソナライズされたセキュリティポリシー

個々のユーザーのふるまいやニーズに合わせてパーソナライズされたセキュリティポリシーを実装することで、堅牢なセキュリティを維持しながら全体的な顧客体験を向上させることができます。Akamai のソリューションは、金融機関が安全でパーソナライズされた体験を顧客に提供できるようにします。

リアルタイム API 監視

リアルタイム分析を使用して API のふるまいを監査することにより、金融機関は脅威を迅速に検知して対応し、機微な情報を保護し、スムーズで安全な顧客体験を実現できます。

4

セキュリティとコンプライアンスのコストを効率的に管理する

スケーラブルなセキュリティソリューション

Akamai のスケーラブルなセキュリティソリューションは、お客様のビジネスニーズに合わせて成長し、多額の設備投資を必要とせずにコスト効率の高い保護を提供します。このスケーラビリティにより、金融機関はセキュリティコストとコンプライアンスコストを効率的に管理できます。

運用コストの削減

Akamai のクラウドベースのサービスを利用することで運用コストを削減でき、高額なオンプレミスインフラを維持する必要がなくなります。Akamai の包括的なリスク管理フレームワークは、リスクを効率的に特定、評価、緩和するため、セキュリティ侵害による潜在的な財務損失を削減できます。

コンプライアンス監査のシンプル化

コンプライアンス環境の範囲を縮小し、コンプライアンスの実証を容易にすることにより、Akamai のマイクロセグメンテーションソリューションは、監査プロセスをシンプル化し、時間を節約し、コンプライアンス管理の全体的なコストを削減します。

また、今日の金融機関が必要としているアジリティを提供し、インターフェースの迅速な調整、可視化の最適化、ビジネスルールの調整、新しい情報の統合を可能にします。その結果、ケース管理のニーズに合わせて、より完全で適応性の高いソリューションが実現します。

5

耐障害性と信頼性を築く

業務の耐障害性の向上

常に進化する脅威の状況に対処するためには、金融機関にとって、高度なデジタル運用の耐障害性の実現が非常に重要です。Akamai のソリューションは、金融機関によるサイバーセキュリティインシデントの防止、対応、復旧を支援し、継続的な運用を保証し、お客様の信頼を高めます。

堅牢なセキュリティ対策

世界中の規制当局が、堅牢なサイバーセキュリティ対策の必要性を強調しています。Akamai の包括的なセキュリティポートフォリオは、これらの規制要件に適合し、運用の耐障害性を維持し、高度な脅威から保護するために必要なツールを提供します。

信頼性と安定性

Akamai のセキュリティソリューションは、現在の脅威から保護するだけでなく、信頼性と安定性の基盤を構築します。業務の中核にセキュリティを組み込むことで、金融機関は長期的な耐障害性を確保し、顧客の信頼を維持することができます。

> 重要なのは、セキュリティ上の弱点を理解して、それを管理することです。環境の可視化は、リスクを特定するうえで非常に有用です。レッドチームのアクティビティを監視することで、一般的な攻撃ベクトルをブロックするためのポリシーを速やかに作成できました。
>
> **– 登録証券ブローカーディーラーの CISO**

グローバルな銀行が 2 週間で SWIFT コンプライアンスを達成

外部の規制当局が、Akamai クライアントであるグローバルな銀行に、重要なアプリケーションをすべてリングフェンスし、金融機関間で送金するための安全なプロセスである SWIFT の要件を満たすことを求めました。通常、このようなアプリケーションでは、ベアメタルサーバーや仮想サーバーなど、さまざまな場所に 100 台以上のサーバーを導入する必要があります。平均すると、この規模の銀行では、このプロセスの計画と実行には 8～12 か月を要します。なぜなら、複数の拠点にまたがるセグメントに対してバーチャル・ローカル・エリア・ネットワーク（VLAN）を構築する必要があるためです。SWIFT アプリケーションの依存関係を決定し、ルールセットが正しいことを確認することは、タイムラインをさらに長くすることになります。

一方、このプロジェクトでは、新しいファイアウォール機器の購入も必要になります。また、SWIFT アプリケーションは銀行業務にとって不可欠であるため、ダウンタイムは許されません。全体として、セグメンテーションプロジェクトには多くの人々の多大な努力が必要であると予想されていました。

しかし、Akamai を活用したことで、たった 1 人のセキュリティエンジニアが約 2 週間でプロセス全体を完了することができました。ネットワークの変更も不要で、銀行はアプリケーションの変更やダウンタイムも回避できました。

時間の節約
226–351 日

FTE の削減
FTE を 4 人以下に

確実に
ダウンタイムなし
かつ可視性を向上

時間を節約し、可視性を向上

ある金融機関は、ベアメタル、VMware、OpenStack インフラで構成される複雑な環境内で、SWIFT アプリケーションをリングフェンスする必要がありました。従来のセグメンテーション手法では難しいことが分かり、完了するためには 8～12 か月の期間と 5 人以上のフルタイム従業員（FTE）が必要でした。ダウンタイムの問題も増え、アプリケーションや依存関係の可視性も失われていました。Akamai Guardicore Segmentation を導入したことで、SWIFT アプリケーションのマッピング作業はわずか数時間で完了し、自動的に提案されたセグメンテーションポリシーを適用して微調整することができました。新しいハードウェアやファイアウォールも必要ありませんでした。全体のプロセスは 2 週間で完了し、必要なフルタイム従業員は 1 人だけでした。

結論

Akamai は、金融機関が規制コンプライアンスとサイバーセキュリティの複雑な状況に対応できるよう、包括的なソリューションを提供しています。金融機関は、マイクロセグメンテーションなどの高度なテクノロジーを活用することで、コンプライアンスのシンプル化、生産性の向上、顧客体験の向上、セキュリティコストとコンプライアンスコストの効率的な管理、耐障害性と信頼性の構築を実現できます。Akamai は確かな実績と革新的なソリューションを有しており、セキュリティ体制の強化とコンプライアンスの確保を目指す金融機関にとって、理想的なパートナーとなります。

金融サービス向けソリューションの詳細をご覧ください

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と可視性を活用して、お客様と当社が提携し、脅威を防止、検知、緩和することで、お客様はブランドの信頼を構築し、ビジョンを実現することができます。

 | サポート | | 公開日：2024 年 9 月