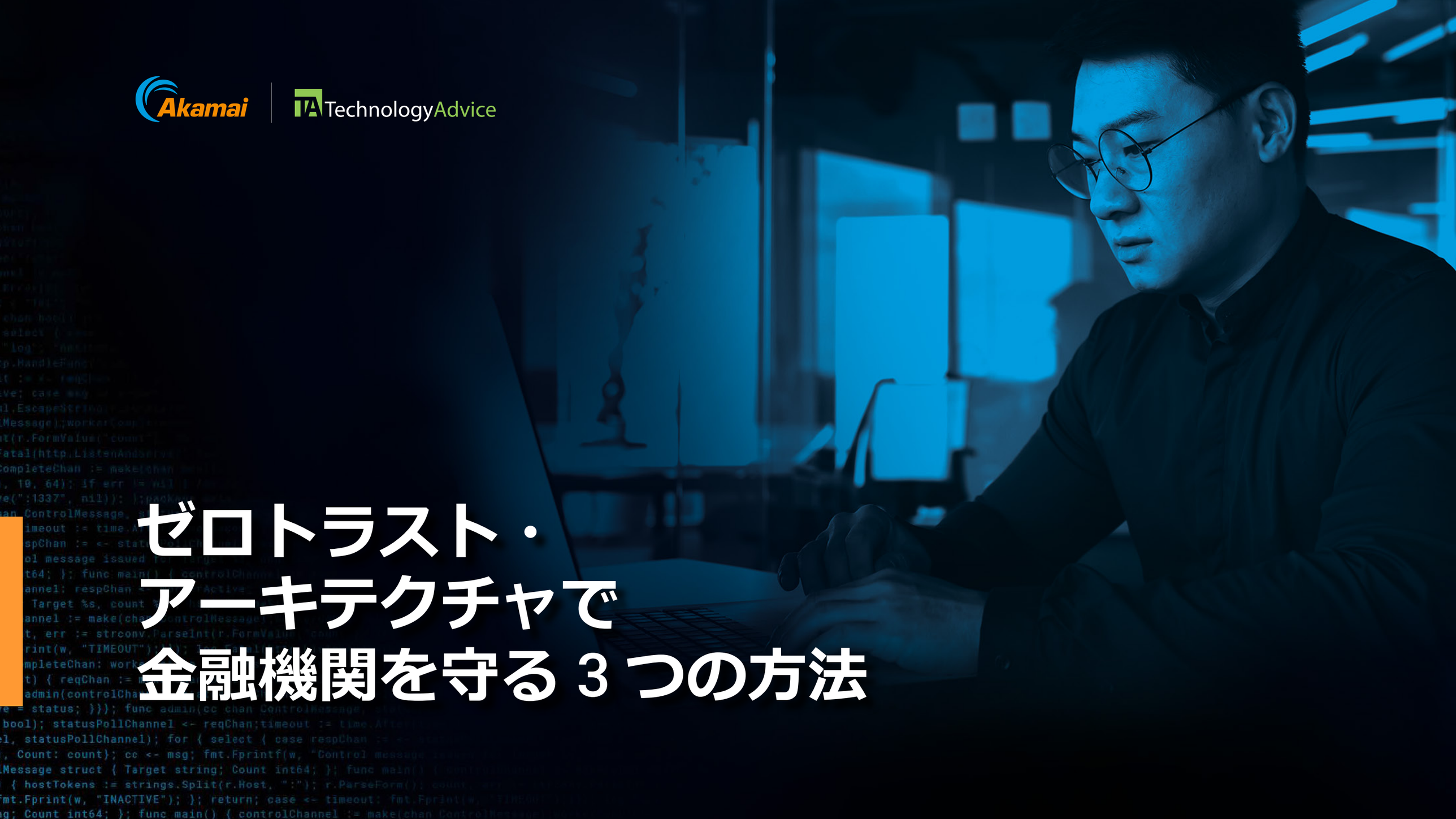
Akamai | TechnologyAdvice



ゼロトラスト・アーキテクチャで金融機関を守る 3 つの方法

金融機関は今も攻撃者の主な標的となっています。2022 年と 2023 年の第 2 四半期を比較したところ、Web アプリケーション攻撃および API 攻撃が **65% 増加**していました。サイバー脅威が進化するなか、このような執拗な攻撃が続けば、リソースが枯渇するだけでなく、重要な中核事業に注力できなくなります。

従来のファイアウォールやエンドポイントソリューションは暗黙の信頼を特徴としています。つまり、パスワードとユーザー名の組み合わせによる最初のスクリーニングを通過したエンドポイント、デバイス、ユーザーは暗黙で信頼されます。稀に多要素認証（MFA）で強化されているものもありますが一般的とはいえません。多くの場合、ネットワーク内のアプリケーション、API、システムサービスは、基本的なエンドポイントのマルウェア監視以外にセキュリティスクリーニングを受けることなく稼働しています。増え続けるランサムウェアの脅威に対抗し、厳しい規制を遵守し、クラウド移行に伴う課題を克服するために、金融機関はゼロトラストを採用し始めています。

ゼロトラストは暗黙的な信頼を排除し、すべてのアプリケーション、ユーザー、デバイスに対するアクセス許可を、リクエストと許可のコンテキストに基づいて継続的に確認します。攻撃者がデバイスや認証情報を侵害してネットワークにアクセスできたとしても、アクセス可能な範囲が狭く限定されるため、損害を大幅に軽減できます。

では、ゼロトラスト・フレームワークは具体的にどのような方法で金融機関を守るのでしょうか。

絶え間なく変化する規制を遵守する

金融機関は多様な規制へのコンプライアンスを証明するために多大なリソースを必要とします。たとえば、すでに確立され普及している Payment Card Industry Data Security Standard（PCI DSS）のほか、2025 年 1 月には Digital Operational Resilience Act（DORA）が全面的に適用される見込みです。規制はわかりにくく、矛盾しがちで、頻繁に変更されます。そのため定期的な監査は複雑になり、時間もコストもかかりますが、金融機関は投資せざるを得ません。監査を通過しなければ、収益損失や、規制違反による制裁、罰金、罰則の適用につながる可能性があり、評判が低下したり、法的責任を問われるケースもあります。

コンプライアンスに関するレポートには、規制対象データを扱うシステムについての明瞭かつ正確な説明に加え、それらのシステムが適切に保護されているとの証明が記載される必要があります。しかし、大手の金融機関では、IT 環境の規模、細かさ、複雑さにより、アセットやアクセスの追跡は非常に困難です。

古いファイアウォールやエンドポイント防御機能で追跡、防御できるのは、主に従来のユーザーやアセットです。このような従来のアプローチでネットワークセグメンテーションに取り組むと、運用のスケーリングが問題となり、ポリシーの作成と適用が妨げられ、アジリティが制限されます。

金融機関は、将来の戦略にも対応できるテクノロジーで、レガシー環境の課題を克服しなければなりません。そのためには、水平方向（East-West）のトラフィックに対するきめ細かい可視性や、マルチクラウド環境とコンテナ環境にセグメンテーションポリシーを適用できるような機能が必要となります。複数の地域や、コンテナテクノロジーなど、多種の IT インフラを管理する必要性が増している今、金融機関に必要なのは、ポリシーの柔軟性や、DevOps の統合、自動化に対応でき、かつシンプルで合理的な方法でマイクロセグメンテーションに移行することです。

すべてのリソースを定期的に識別し、追跡して、セキュリティを確保できなければ、規制対象データへのアクセスを完全に制御し保護することは不可能です。データ、ユーザー、アプリケーション、またはデバイスの監視が見過ごされたり不適切であったりすれば、サイバー攻撃を受けるリスクが増し、コンプライアンスの監査に不合格となる可能性も高まります。

ゼロトラスト・アーキテクチャは、デフォルトではアクセスを拒否するので、すべての接続に対し、「認証済みのユーザーが認証済みのデバイスを使用し、リクエストされたデータへのアクセスが許可されている」というコンテキストに基づいて許可を付与する必要があります。ゼロトラストではデフォルトでは最小限のアクセス権が適用されるため、忘れられていたり未知であるレガシー接続は中断されます。Akamai のソリューションを使用すれば、古い支社や買収した企業のレガシーテクノロジー環境に悪性デバイスやレガシーユーザー（人、API、またはアプリケーション）、忘れ去られたデータソースがあっても、それらをすばやく特定できます。

Akamai のゼロトラスト・アーキテクチャはユーザーの所在地に関係なく適用されますが、アクセスに関する判断のプロセスには所在地のコンテキストを含めることができます。セキュリティチームは、総合的な制御力とレポート作成機能を得ることで、ローカルネットワーク、データセンター、またはクラウド内のリソースへのアクセスをすばやく分析し、完全に管理することができます。

規制により、重要なアプリケーションの保護や水平方向のトラフィックのセキュリティ確保に対する圧力が強まるなか、金融機関は環境を可視化して把握する機能の強化に力を入れています。ゼロトラストの原則を適用すれば、金融機関は非遵守のアセットをシームレスに識別、セグメント化し、アプリケーションチームに自律的にセグメンテーションポリシーを管理させることができます。これにより、ワークフローが効率化し、レポートプロセスもシンプルになります。

コンテキストリッチな可視性によって横方向のトラフィックを完全に把握できれば、ビジネスクリティカルなアプリケーションのマッピングとリングフェンシングが容易になります。インフラやアプリケーションを変更する必要はありません。この機能を活用することで、金融機関はサードパーティのアクセスを制限し、全体的なセキュリティを強化することができます。

可視性は、クラウドへのセキュアで合理的な移行に役立ちます。また、DevOps のサイクルにセグメンテーションを統合すれば、インフラを大きく変更せず、すぐにポリシーを更新できます。つまり、古い VLAN 方式から脱却できるのです。さらに、Akamai を使用すれば、複数のインフラ全体でのコンプライアンスポリシーの統一的な作成、適用、レポート生成が可能となり、しかもこれらの手順がシンプルになります。これを可能にしているのは、高度な可視性、アプリケーション依存関係のマッピング、セグメンテーションポリシーの自動化、DevOps ポリシーの自動化、変更管理のシームレスな統合です。

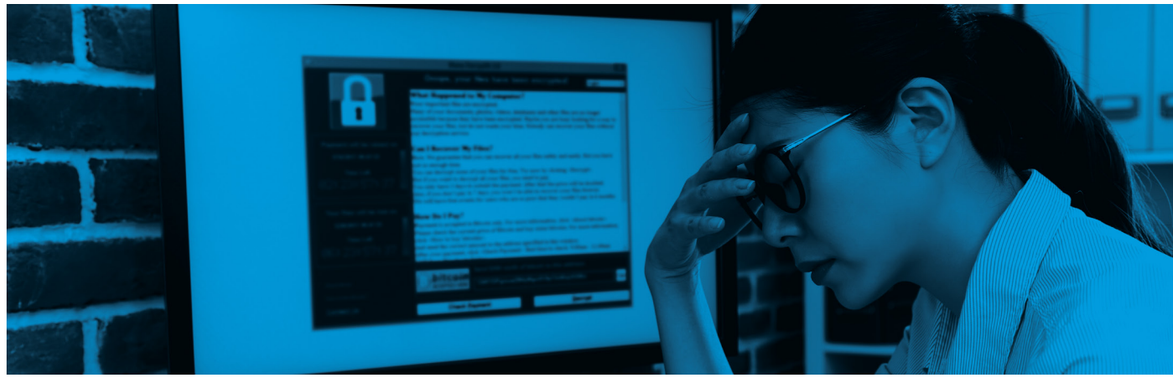
ランサムウェアの拡散を防ぐ

支店からグローバルな金融機関に至るまで、ランサムウェア攻撃はニュースを賑わし、世界中の頭痛の種となっています。事実、Cybersecurity Ventures 社の **2022 年ランサムウェア市場レポート**によると、「2031 年までには企業、消費者、またはデバイスへのランサムウェア攻撃が 2 秒ごとに発生すると予測されています」。

金融サービス機関は頻繁な M&A を通じて事業を拡大しますが、こうした統合によって全社的なテクノロジーエコシステムへの可視性が失われ、攻撃者が悪用できるバックドアが開いたままになりがちです。ランサムウェアの攻撃者は、バックドアの悪用やフィッシング攻撃によって、認証情報を盗み出したり、エンドポイントの防御を回避する未知のマルウェアをエンドポイントに投下したりします。

ユーザーに必要以上のアクセスを許可するようなポリシーや、パスワード中心の認証では、攻撃者はファイアウォールを迂回し、エンドポイントの検知を回避して、トラフィック、ユーザー、接続デバイスを暗黙的に信用する無制限のネットワークアクセス権を取得する可能性があります。ランサムウェアの攻撃者は、CL0P のように、グループを構成している場合が多く、感染した資産を悪用してラテラルムーブメント（横方向の移動）を実行しながら、他の脆弱な資産を探索してさらに悪用します。**MOVEit の SQL インジェクション脆弱性**のようなゼロデイ脆弱性があると、攻撃者は自動化スクリプトを使用してすばやくアクセス権を取得し、攻撃を拡散して、システムの暗号化、データ窃取、身代金要求を行います。

Akamai のゼロトラスト・ソリューションは、重要なシステムを特定、隔離し、これらのシステムを宛先または送信元とするネットワークアクセスを制限する機能を金融機関に提供します。このアプローチでは、ランサムウェア攻撃の可能性や影響だけでなく、攻撃からの回復に要する期間も最小限に抑えることができます。Akamai はまず、攻撃の開始を阻止するために、悪性のドメインや IP アドレスを追跡、監視して、適切な隔離ブロックを実装します。



その後は、ネットワークトラフィックに対するほぼリアルタイムの可視性を活用して、プロセスレベルおよびサービスレベルで細かくトラフィックを観測し制御します。これらから得た詳細な知見は、セキュリティ・オペレーション・センターやネットワーク・オペレーション・センターの担当チームが直面している脅威を正確に特定し、狙いを定めるために役立ちます。

たとえ攻撃が成功したとしても、Akamai Guardicore Segmentation が提供するマイクロセグメンテーションによって、影響範囲を狭く限定することができます。認証情報や許可はアクセス要求のたびに確認され、Akamai Enterprise Application Access が保護するアプリケーションへの接続は拒否されます。

さらに、ユーザーに不要なアプリケーション、サーバー、その他のリソースは見つからないように自動的に非表示にすることで、ラテラルムーブメントや攻撃者へのアクセス権の拡張を防ぎます。最後に、Akamai Hunt の異常検知機能により、通常と異なるふるまいがあれば、フラグを立てて、セキュリティチームに警告します。これは、データの抽出や暗号化が行われる前に攻撃を特定するために役立ちます。

デジタルトランスフォーメーションを合理化する

アジリティ、スケーラビリティ、モダナイゼーションに対応するため、多くの金融機関がクラウドへのアプリケーション移行に取り組んでいます。しかし、こうした移行によって新たな課題も生じています。

まず、検知できない未知のリソースや接続は移行できません。また、クラウドへの移行によってアタックサーフェスが拡大するだけでなく、マルチクラウドやローカルのハイブリッドクラウドの統合によって、アプリケーションが壊れ、確立されていたセキュリティレイヤーにギャップが生じることも少なくありません。さらに、ソフトウェア展開インフラ（コンテナ、仮想マシンなど）の自動展開が高速であるため、レガシーソリューションではセキュリティ確保や監視の効果が低下します。

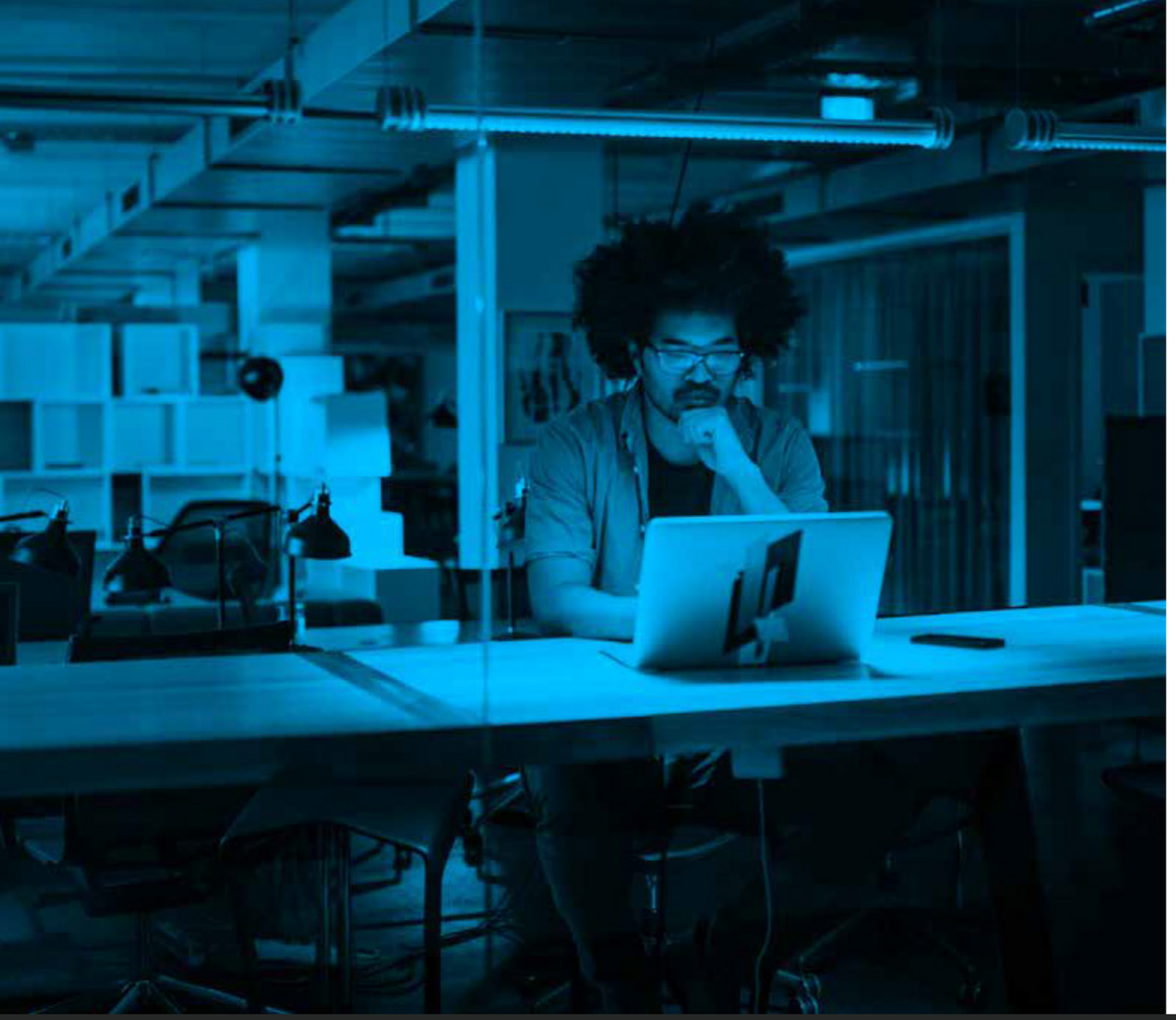
ゼロトラスト・ソリューションを利用すれば、金融機関はクラウドベースのアプリケーションを簡単に展開し、防御を強化しながら運用のオーバーヘッドを軽減できます。Akamai のゼロトラスト・ソリューションは、すべてのデータフローを追跡して潜在的なアタックサーフェスをすばやく特定し、ビジネスを中断させることなくポリシーを適用します。

特定後は、セキュリティチームとオペレーションチームは Akamai の一元管理機能を利用し、アプリケーションをセグメント化してセキュリティを確保するとともに、データフローを監視できます。Akamai はきめ細かい制御機能を提供すると同時に、運用コストと複雑さを軽減します。金融機関のセキュリティチームとオペレーションチームは、統一的にポリシーを適用することで、インフラのモダナイゼーションを迅速かつアジャイルに進めることができます。ただし、これを達成するためには、最小権限のゼロトラスト・セグメンテーションによる堅牢なセキュリティが必要です。強力な防御によって、進化する脅威に対抗できるようにすることが重要なのです。

金融機関にとってゼロトラストは無視できない要件

レガシーテクノロジーを狙った攻撃は、大規模なデータ漏えいにつながる可能性があります。そうなれば、膨大な経済的損失が生じ、顧客やパートナーの信頼も失うことになります。攻撃がますます高度になり、高速化している今、テクニカルエコシステム全体を可視化できない金融機関は、開いているバックドアを見逃す可能性があります。

Akamai は、ネットワークへの広範かつ高度な可視性に加え、ユーザーアクセスのインテリジェントな制限や、継続的な脅威ハンティングの機能を提供します。また、異常があればセキュリティを再確認できるように警告します。**金融機関**のニーズに対応する **Akamai のゼロトラスト・ポートフォリオ**については、こちらから詳細をご覧ください。



Akamai が提供する デジタル金融向けの セキュリティをご覧ください

詳細はこちら

TechnologyAdvice | Akamai

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、セキュリティ体制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 のクラウドコンピューティング、セキュリティ、コンテンツ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、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。