ゼロトラストで Fiserv と Fintech を保護

どのようにすれば生産性を維持しながら
サイバー脅威から保護できるか

eBook

MENLO SECURITY

目次

過去10年間で、金融サービス（Fiserv）ほど劇的に変化した業界は他に例が無いでしょう。銀行および金融業での取引は、かつてはほとんどが対面で行われていました。しかし現在、顧客は財務的な処理を日常的にデジタルベースで行っているため、Fiserv企業のユーザーはこれまでのように壁に囲まれた安全な楽園で仕事をするなどということは許されず、Webサイトやクラウド、あるいはSaaSアプリに移行しています。一方でサイバー攻撃者は、金融サービス企業からデータや資産を盗むことができれば高い対価を得られることを知っています。現実に、Ponemon Instituteの最新のサイバー犯罪の年間コストレポート[1]によると、調査したすべての業界の中でサイバー犯罪によるコストが最も高かったのが金融サービスで、180億米ドルを超えて年々上昇しています。

これらの攻撃は、金融サービスとフィンテック企業全体のセキュリティと信頼性に不安を投げかけています。これらの企業が何年にもわたって使用してきたセキュリティツールや戦略は、現代の脅威に立ち向かうには、もはや十分ではありません。ビジネスがより革新的になれば、犯罪者も変化します。今は多くの脅威がネットワーク内に侵入してしまっていますが、従来型のセキュリティツールや手法は境界での受動的なセキュリティに重点を置きすぎているのです。業務に集中して生産性を上げようとしている多くのユーザーにとって、フィッシングやランサムウェア、そしてその他の悪意のあるコードはすべて、引続き脅威となっています。

このeBookでは、FiservとFintechの現在のセキュリティリスクの背後にある要因と、セキュリティリーダーがそれらに効果的に取り組む方法について説明します。

European Systemic Risk Board[2] は、全世界でのサイバー攻撃によるコストを**450億米ドルから6,540億米ドルの間**と見積もっています。欧州中央銀行の総裁は、複数の銀行を標的とした攻撃が金融危機を引き起こす可能性があるという懸念[3] を表明しました。

1 https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
2 https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html
3 https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html

SECTION 1

Fintech における可視性と信頼性の障害

現代の金融機関では、さまざまな要素が組み合わさって、セキュリティとリスクを取り巻く環境を困難なものにしています。

リモートワークにより、攻撃対象がさらに拡大

ユーザーの大部分がリモートに移行した最新の環境は、セキュリティには最悪の状況をもたらしました。ある調査[4] によると、セキュリティ専門家の4分の1近くが、リモートワークに移行した後にサイバーセキュリティインシデントが増加したと述べています。一部では、インシデントの数が2倍になった例もあります。

ユーザーがどこからでも業務を行えるモデルを構築し、それを保護することは、新しいリスクが生まれることも意味しています。セキュリティチームからテレワーカーのシステムに対する可視性は低く、家庭用のWiFi環境やビデオ会議プラットフォームは社内ネットワークよりも安全性が低い可能性があるからです。BYOD（Bring Your Own Device）ポリシーも新しい環境に適応させる必要がありましたが、多くの金融機関では個人用デバイスの保護はセキュリティ戦略に組み込まれていなかったため、移行当初は脆弱なままでした。

マルウェア、スパイウェア、ランサムウェアは、Webサイトとネットワークデバイスが直接接続されていなければ、組織に影響を与えることはできません。しかしほとんどのセキュリティツールは、この状況における根本的な問題に対処できていません。

金融分野での詐欺の急増

Fintechおよび金融サービスでユーザーが行っているのは、基本的にはトランザクション処理であり、それらを止めることはできません。そしてトランザクション処理には、信頼の付与も必要になります。

パンデミック後にデジタル決済と通信への依存が高まりましたが、攻撃者はわずか数週間でその状況を悪用する新しい方法を発見しました。Advisenによると、COVID-19関連のサイバーイベントの25%が金融/保険セクターに向けられたということです。あらゆる種類の金融機関で、景気刺激予算、電信送金、フィッシングに関連した詐欺が増加しましたが、特に決済機関、保険会社、信用組合はハッキングの影響を大きく受けました。

4 https://blog.isc2.org/isc2_blog/2020/04/survey-covid-19-response-sees-nearly-50-of-cybersecurity-workers-reassigned-to-it-tasks.html

SECTION 2

関係する要因：ディスラプターとセキュリティの課題

昨年起きた出来事を振り返ってみると、1つのことが明らかになります。それは、金融、銀行、Fintechの未来はデジタルであり、これらの組織内での業務の進め方も同じだということです。

金融機関はアプリケーションを積極的にクラウドに移行させており、ハイブリッドなクラウドインフラを採用してアプリケーションをリファクタリングし、部門間やパートナーとの間でデータを自由に共有しています。

SaaS[5]の急速な採用が進んでおり、それに伴って多くの問題が発生しています。2017年には、ほとんどの業務をSaaSで運用していた企業は全体の38%に過ぎませんでしたが、今ではほとんどまたはすべての業務でSaaSを利用している組織が主流（68%）となっています。しかしオンラインおよびクラウドベースの情報にアクセスする際に障害があると、速度と生産性に影響を与えることがあります。

また、クラウドやSaaS（Software as a Service）ソリューションへの移行に伴い、セキュリティと規制へのコンプライアンスが懸念事項になります。地域を横断して規制[6]を適用するのは大きな負担となり、特にAPAC内では金融業務が国境を越えて緊密に統合されるために、それが顕著になります。攻撃者はこのような規制間の差異を悪用して、世界経済に影響を与えるようなチャンスを手に入れる可能性があります。

5 https://www.blissfully.com/saas-trends/2020-annual-report/
6 https://www.csis.org/analysis/financial-sector-cybersecurity-requirements-asia-pacific-region

インフラにこれらの新しい要因が重ね合わされることで、組織は新しい脅威に対してより脆弱になります。また、可視性に問題が生じるため、コンプライアンス上の懸念も新たに発生します。そのためチームは、自分たちのアプリケーションやデータ管理が現行の規制要件に適合しているかどうかわからなくなることもあるのです。

しかし、これらの企業が長年にわたって利用してきたセキュリティツールや戦略は、今日のインフラへの要求や増え続ける脅威の状況に対応するにはもはや十分とは言えません。エンドポイント保護や企業向けアンチウイルス、そして侵入検知などの技術は、アプリケーションとデータ、そして顧客やユーザーを完全に保護することができません。これらのツールは事後対応型で、既知のプロフィールに一致する脅威のみをセキュリティチームに通知したり、異常な活動に対して誤ったアラームを発生させてしまいます。

Fintechおよび金融サービスのチームは、最初の段階で攻撃がネットワーク境界に到達するのを防ぐことができるソリューションを必要としています。

国家が支援して組織化した犯罪グループによる攻撃は、金融業務を混乱させるだけでなく[7]、数十億ドル規模の被害をもたらす可能性があります。2016年以来、北朝鮮だけでも38か国：約20億米ドルの損失に関与しています。

7 https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

SECTION 3

Fiserv および Fintech の一般的な攻撃経路

金融分野のユーザーによるWebの利用は、両刃の剣です。Webは調査やニュースのチェック等の際に重要ですが、ユーザーを悪意のあるコードに晒してしまうこともあるからです。ユーザーのWeb使用を保護するためには、管理すべき複数の課題があります。

Webアクセスが増えると、マルウェアリスクが高まる

Fintech組織のユーザーは、固有のリスクを伴うオンラインタスクをいくつも実行する必要があります。安全であると思われる有名なサイトでさえ、実際には危険が潜んでいる可能性があります。組織のセキュリティ戦略が既知の脅威をブロックするためのブラックリストとホワイトリストに依存している場合、ユーザーが業務のために必要なコンテンツにアクセスするのに時間がかかったり妨げられたりするため、生産性に影響を与えてしまいます。

フィッシングがユーザーをトラブルに導く

もう1つの一般的な攻撃経路は、フィッシングです。これは、犯罪者が無防備なユーザーを騙して感染したサイトへのリンクをクリックさせたり、悪意のある添付ファイルをダウンロードさせたりする詐欺メールです。悪意のあるファイルがクラウド内で共有されている場合、SaaSベースのOfficeアプリケーションのユーザーにとっては安全なように見えるかもしれません。しかしほとんどの場合において、ユーザーのデバイスはこれらのファイルに直接アクセスすることができます。そしてそれは、マルウェアをダウンロードしてしまう可能性があることを意味しています。VerizonのData Breach Investigations Report[8] によると、漏えいの25%がフィッシングに由来し、22%が人為的ミスに関係しているということです。

モバイルセキュリティは動くターゲット

スマートフォンやタブレット、そしてノートPCを使って多くの業務が行われているため、現在金融サービスとFintechの最大の関心事はモバイルセキュリティになっています。ほとんどのユーザーは日常的にWebやスマートフォンから企業データにアクセスしており、リモートワークへのトレンドが強まる中でその傾向は強まっています。

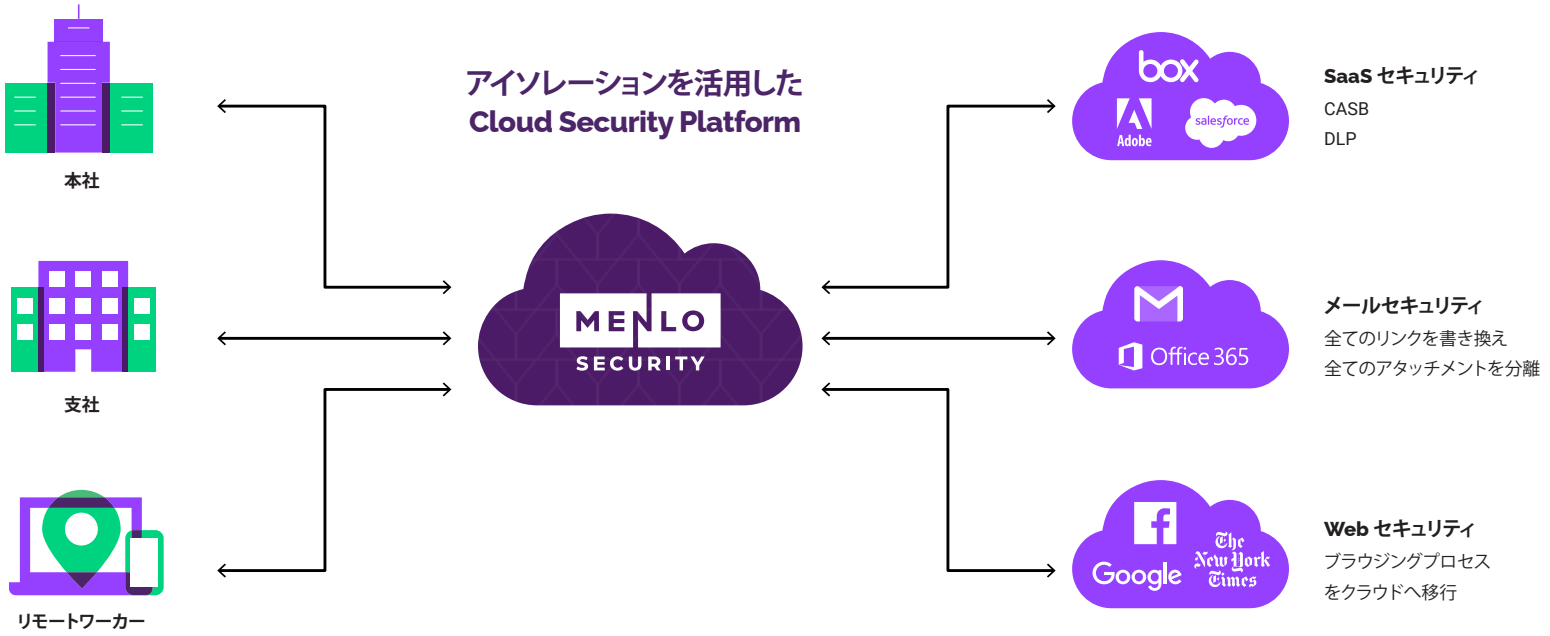
8 https://enterprise.verizon.com/resources/reports/dbir/

SECTION 4

アイソレーションによるゼロトラストの有効化

境界で攻撃を阻止するというセキュリティ戦略は、フィッシングメールを阻止できず、リモートで業務を行っているユーザーをWebでのドライブバイダウンロード攻撃や他の複数の種類のWebベースのエクスプロイトから保護できません。従来の「検知と対応」のアプローチでは、ユーザーや企業が必要とする安全性を提供できないのです。「予防」は攻撃が開始される前にそれを止めることを意味しますが、「検知と対応」はすでに侵入を許してしまっていることを意味しています。

この問題への答えは、悪意のあるコードがネットワーク境界に到達することを防ぐアプローチです。これは、アイソレーションを利用したクラウドセキュリティとSecure Access Service Edge（SASE）ベースのソリューションによって実現できます。



このアプローチにより、組織はSaaSアプリやWebサイトへのアクセスを制限なく許可することができ、生産性を犠牲にせずに済みます。Webサイト、ビデオ、ドキュメントを含むすべてのWebコンテンツをリモートのブラウザーに分離することで、ユーザーとインターネット上の悪意のあるコンテンツの間に仮想的なエアギャップを作り出すことができ、エンドポイントデバイスへのアクセスが効果的に遮断されるため、リスクが軽減されます。組織はセキュリティ体制を維持するために、ユーザーがサイトにアクセスできないようにする必要がありません。

しかしこれを効果的に行うためには、使いやすさとスケーラビリティが重要になります。「デフォルトで分離する」というアプローチにより、ユーザーの生産性に影響を与えることなくマルウェアを排除できます。また、アイソレーション戦略を拡張してSASEの導入展開に必要な大規模なスケーラビリティに対応できるようにすることも重要で、これにより新規の導入展開でもクラウドのセキュリティを確保できます。

リモートワーカーのために

最近急増している、企業のファイアウォールの外側からログインしてくるユーザーには、VPNのようにパフォーマンスに影響を与えたりネイティブのブラウジングエクスペリエンスを低下させたりしない、信頼性の高い安全なインターネットアクセスを提供しなければなりません。業務遂行への要求に応えるためには、ユーザーが接続してくる場所に関係なく、最適で安全なパフォーマンスを提供できるアーキテクチャが必要です。

Isolation Core™ を活用したMenlo Security Secure Web Gatewayは、クラウド内にユビキタスなセキュリティレイヤーを構築し、そこをメール内のリンクや添付ファイルを含むすべてのWebトラフィックが流れるようにします。ここにセキュリティポリシーを適用することで、ユーザーがアクセスしているのがオフィスや自宅、または公共のカフェなのかどうかに関係なく、セキュリティを確実に適用することができます。

クラウドベースのアイソレーションプラットフォームは、エンドポイントへのソフトウェアのインストールを必要とせずに迅速に拡張でき、あらゆる規模の企業に包括的な保護を提供します。このサービスは迅速な導入展開が可能で、エンドユーザーのブラウザーエクスペリエンスを最適化し、誤検知を減らし、セキュリティ制御を強化し、SOCチケットやヘルプデスクへの要求を減らすことで、ITチームとセキュリティチームの負担を軽減します。

メンロ・セキュリティは、Webやダウンロードされたドキュメント、およびメールから、悪意のあるコードに由来する脅威を排除することにより、金融サービスとFintech組織をサイバー攻撃から保護します。メンロ・セキュリティは悪意のある攻撃を防ぐための安全なゼロトラストアプローチを提供するため、エンドユーザーはオンラインで作業している間、セキュリティを気にしなくとも済みます。これにより、セキュリティチームは迅速にイノベーションを起こし、常に移動する顧客の要求に対応できるため、運用上の負担も軽減できます。そして同時に、ユーザーのネイティブWebブラウジングとSaaSアプリのエクスペリエンスを維持します。その結果、ユーザーは重要な業務に集中できます。

アイソレーションにより セキュリティと生産性が向上

メンロ・セキュリティのアイソレーションを活用したプラットフォームは、ユーザーエクスペリエンスに影響を与えることなく、クラウドベースのアプリケーションやWebサイトへの高速で安全なゼロトラストアクセスを実現します。

機能:

- マルウェアとフィッシングから100%保護：マルウェア、ランサムウェア、フィッシング、ゼロデイ攻撃を排除
- オンライン作業を保護：Web、メール、およびSaaS保護のためのマネージドソリューション
- 迅速な導入展開：ハードウェアやソフトウェアを新規に購入または導入する必要が無い、100%クラウドベースのソリューション
- グローバルエラスティッククラウド：世界中のどこからでもユーザーとデバイスを即座に追加できる自動スケーリングアーキテクチャ

メリット:

- リモートワーカー向けに100%マルウェアフリーのWebブラウジングを提供
- Office 365/G Suiteユーザーをランサムウェアやフィッシングから100%保護
- あらゆるデバイスを使うすべてのユーザーに対して一貫したセキュリティ保護を提供
- Webトラフィックをバックホールする必要無く、インターネットへの高速な直接接続を実現

Webベースのサイバー攻撃を排除し、攻撃対象を劇的に減らす方法を学んで下さい

menlosecurity.com/ja-jp/ にアクセスするか、
japan@menlosecurity.com までご連絡ください

MENLO SECURITY