

CUSTOMER STORY

デジタル・ペイメントのイノベーターが 数百万ユーザーのオンライン取引のセキュリティを守る

FireEyeポートフォリオが国内のバンキング・システムのインフラをサポート

概要

業界



ソリューション

- FireEyeネットワーク・セキュリティ
- FireEyeエンドポイント・セキュリティ
- FireEye Eメール・セキュリティ
- FireEye File Protect
- Mandiant Threat Intelligence

利点

- 複数の攻撃経路にわたって、シームレスで統合された保護
- 自動化されたリアルタイムのインテリジェンスをソリューション間で共有
- 質の高い検知、封じ込め、緩和策によりチーム効果を向上
- 構造化データと非構造化データの監視を最適化

企業紹介

この電子決済オペレーター企業は、国内のバンキング・システム全体の標準を規定し、インフラを提供することを目指しています。



これまで現金中心だった経済において、ある電子決済システム企業が、国全体における電子決済の普及とアクセス性に革命をもたらしました。

この企業は、国内のデビット・クレジットカードとモバイル・アプリを含む技術革新により、ユーザーがさまざまな決済システムにアクセスして異なるシステム間で送金を行えるような、ファイナンシャル・インクルージョンの経済を構築しようと取り組んでいます。この企業の最高情報セキュリティ責任者 (CISO) はこう語っています。「当社がスタートしたときのビジョンは、国内のあらゆる人に向けて、世界レベルの電子決済システムへのアクセスを提供することでした」

最優先事項はセキュリティ

このビジョンを達成するためには、決済システム・オペレーターのサービスを利用する何百万人もの消費者のデジタル個人情報を収集する必要があります。CISOとしてミッション・クリティカルな任務の中心は、この情報のセキュリティを確保することです。この国では厳しい金融規制が施行されており、組織には、管理する大量の個人情報の完全性を維持する厳しい責任が課されています。

さらに、この国では、多くの金融機関が自社インフラのセキュリティの規範とするために、この決済システム・オペレーターに注目しています。すなわち、この企業は世界トップレベルのセキュリティ体制を築いて、模範を示す必要があるのです。

「対等なプレーヤーとして、またこの国の金融エコシステムをサポートする原動力として、他の金融機関が進化する脅威を常に把握できるように支援し、この国の環境全体を守っていくことが、当社にとって非常に重要です」と、CISOは語ります。

この企業はさらに、国内および世界の手形交換所兼カード決済システムのプロバイダーの役目も果たしているため、広範かつ複雑で標的にされやすい環境を保護する必要があります。CISOは次のように語ります。「セキュリティは、経営部門から取締役会に至るまで、組織全体のコア・バリューに深く組み込まれています。当社にとって、侵害の影響を被るということは全く受け入れられるものではありません。しかしながら、経営部門では今後攻撃を受ける可能性は避けられないことを認識しています。そのため、インシデントを速やかに軽減するための備えが優先事項となります」

「FireEyeのおかげで、脅威の発見と回避にほぼリアルタイムで対処できるようになっています。以前は数日間かかっていた作業が、わずか数分にまで短縮されています」

— 最高情報セキュリティ責任者、電子決済オペレーター企業

総合的なプロバイダー1社から得られる均一な保護

この決済システム・オペレーター企業の最優先事項のひとつは、非構造化データに由来する脅威に対する防御の改善でした。「犯罪者たちは、非構造化データを扱うアプリの脆弱性を悪用してアプローチし、境界の防御をかいくぐって攻撃を仕掛けてきます」と、CISOは説明します。この企業ではさらに、シグネチャベースの防御を補強するために、その広範な環境にわたってシグネチャレスの脅威を検知、阻止するためのテクノロジーを使用しています。

この企業が無数の攻撃経路のセキュリティを確保するソリューションを探すにあたっては、相互運用性が重要な基準でした。CISOはこう語ります。「当社のデータを均一に保護し、脅威トレンド全体にわたって防御を強化してくれるような、包括的なプロバイダーを探していました」

最初から、CISOはFireEyeをと考えていました。彼は前職で、主要なソリューションについての厳しい評価を実施したことがあり、その企業で最終的に最も望ましいセキュリティ・プロバイダーに選ばれたのがFireEyeでした。彼はこう語ります。「FireEyeに関する以前の経験から、今回も自信を持ってFireEyeソリューションの導入を検討しました」

FireEyeの基盤の上に構築

FireEyeネットワーク・セキュリティとFireEyeエンドポイント・セキュリティはこの決済システム・オペレーター企業にすでに導入されており、他の脅威経路に対する潜在的な脆弱性に対処するため、追加のFireEyeソリューションが導入されました。企業のデータ・リポジトリの保護を強化するため、FireEyeエンドポイント・セキュリティのフットプリントを拡大して、同社のサーバーだけでなくエンド・ユーザーも含めるようにしました。

あらゆる主要な攻撃経路にわたって防御を強化するために、CISOはさらにFireEye Eメール・セキュリティとFireEye File Protectも追加しました。提携銀行は、主に非構造化データからなる大量の文書を、この決済システム・オペレーターのインフラに日常的にロードしています。FireEye File Protectはこれらのファイルやコンテンツ・リポジトリを解析し、次世代ファイアウォールや侵害保護システムをすり抜けたマルウェアや、正当な手段を装いネットワークに入り込んだマルウェアの検知と隔離を行います。

Mandiant Threat Intelligenceを含めたことで、外部の具体的な情報が定期的に提供され、防御体制に組み込まれます。

シームレスな統合による複数の攻撃経路の保護

FireEyeのソリューションのセットが、セキュリティ・チームに積極的に知見を提供する一方で、Mandiant Threat Intelligenceからの情報供給によって、世界中の攻撃の最前線に出現している、これまで知られていなかったシグネチャでは検知できない脅威を特定する方法がわかります。あるソリューションがこの決済システム・オペレーターの環境内で脅威を検知すると、他のFireEyeソリューションにアラートが伝達され、攻撃の封じ込めや阻止が行われます。

CISOは力強く語ります。「FireEyeソリューションの相互運用ネットワークによって、総合的に統合されたプラットフォームを形成し、あらゆる攻撃経路に対処できます。Mandiant Threat Intelligenceから得た情報により、世界的な脅威トレンドに対する可視性が得られ、フォレンジック分析が必要な状況になった場合はすぐに対処できます」

発見と回避が数日から数分に短縮

FireEyeソリューションの包括的な統合により、企業のセキュリティ・オペレーター、アナリスト、調査担当者がインシデントの調査や原因の究明、脅威の排除にかかる時間が劇的に短縮されました。「FireEyeのおかげで、脅威の発見と回避にほぼリアルタイムで対処できるようになっています」

「以前は数日間かかっていた作業が、わずか数分にまで短縮されています。FireEyeテクノロジーを活用して、人員リソースの時間を最適化できるようになりました」と、CISOは語ります。

FireEye: ビジョンを提供

FireEyeへの投資における最も特記すべき点について、CISOの立場から次のように語っています。「CISOは複数のセキュリティ・テクノロジー企業と常にやり取りしています。FireEyeは、ミッションを常に完遂するという点で群を抜いています。FireEyeのCEOのビジョンはFireEyeのソリューションやサービスの隅々に至るまで効果的かつ正確に浸透しており、私たちはその成果を享受しているのです」

「CISOである私にとって、FireEyeとの対話は他に代えがたい貴重なものです。当社独自の環境と課題が組織全体でうまく共有されているからです。」

そのため、営業部門と話すときでも、テクニカル・サポートと協力するときでも、そのときの自分のニーズに合った情報を提供できます。これほど詳細で透明性を備えた情報を有する組織を、私は他に知りません。個人的にFireEyeをぜひおすすめします」

FireEyeの詳細については、www.FireEye.jp をご覧ください。

ファイア・アイ株式会社

〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。お客様は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をする上で課題となっていた複雑性や負担を解消します。

