

CUSTOMER STORY

ハイブリッド統合プラットフォーム・サプライヤーがセキュリティ運用を再生

AxwayがFireEyeのソリューションとサービスでセキュリティ態勢を強化



概要

業界



ソリューション

- FireEye Helix
- Mandiant Managed Defense

利点

- 製品に依存しない統合によって従来のセキュリティ・コンポーネントを継続利用
- 一元化したインテリジェンス・フィードにより、さらなる調査が必要なアラートの特定を簡略化
- マネージド・サービスへの戦略優先アプローチにより、全体的なセキュリティ態勢を改善
- ソリューションの一貫したアップデートにより、進化するサイバー攻撃への防御も万全

企業紹介

Axwayは2001年に設立されたソフトウェア・パブリッシャーです。デジタル・トランスフォーメーションの大手企業として、分散データの移動、統合、安全な公開を通じて、顧客のインフラの最新化をサポートしています。Axwayは、世界100か国以上で11,000を超える顧客のデータに関する困難な問題を解決しています。



多くの企業が、成功への道として、カスタマー・エクスペリエンスとそれに関連して求められるデータ・セキュリティとプライバシーに注目しています。Axwayは、このような企業が責任を持ってデータの管理に取り組めるように、インフラ・ソリューションを提供しています。企業が最高のカスタマー・エクスペリエンスを提供するためにあらゆる場所から集められたデータを安全に集積し、個人やシステム、ビジネスと顧客のエコシステムをつなぐソリューションです。

Axway SoftwareでITセキュリティ・マネージャーを務めるマイケル・クリステンセン (Michael Christensen) 氏は、同社のインフラが定められたセキュリティ・ポリシーに準拠しており、セキュリティ・オペレーション・センター (SOC) が内外の脅威に効果的に対処していることを保証する責任を負っています。

拡大し続けるサイバー攻撃に関する動向と、年々増大するサイバー・セキュリティの知識量に対抗するため、Axwayではセキュリティ態勢を強化するために今あるリソースを最適化したいと考えました。クリステンセン氏は自社のSOCを強化するために増員を検討しましたが、そのコストを考慮した結果、増員の代わりにMDRサービスを探すことにしました。

クリステンセン氏は次のように語っています。「当社の目標は、頼りになるセキュリティ・プロバイダーを見つけることでした。データを評価して実際の問題が発生しているアラートを特定、理解するためには、優れた脅威インテリジェンスと知識豊富な専門家が欠かせません。それなしには、どのソリューションも、実際に役に立っているとは言い切れません」

セキュリティ戦略重視のセキュリティ・プロバイダーを探す

選択肢を絞り込むために、クリステンセン氏は、単に運用サポートだけでなく、セキュリティ戦略を重視したプロバイダーに注目しました。その結果選ばれたのがFireEyeでした。「FireEyeは、セキュリティ環境についての深い理解をもたらすこと、また当社のインフラに起こり得るイベントに対して、単に対応するだけでなく、予防するための手段を見つけることに対し、熱意とパワーを持っているとわかっていました」と、クリステンセン氏は感慨を込めて語ります。

「FireEyeのサービスを導入することで、当社の企業としての態勢を見直し、FireEyeのソリューションとサービスを支えている世界レベルの専門知識に沿った考え方に変える機会が得られました」

— **マイケル・クリステンセン氏**, Axway Software, ITセキュリティ・マネージャー

従来のツールで最前線で得られた脅威インテリジェンスを活用

クリステンセン氏は、FireEye Helixを導入してすぐに得られたメリットとして、Amazon Web Services (AWS) のクラウド・プラットフォームですべてが提供されるので、簡単に使いやすかったという点を挙げています。「SIEMタイプの製品は数多く見てきましたが、FireEye Helixは他とは大きく異なっています。最初のセットアップは、それまで経験したどのソリューションよりもずっとシンプルで、必要な情報を見つけるためのインターフェイスの操作も簡単でした」

クリステンセン氏は、新機能の定期的な更新と継続的な進化こそ、FireEye Helixが優れたプラットフォームである証だと言います。スケーラブルなストレージ (S3)、コンピューティング (EC2)、コンテナ管理 (Fargate) の構成要素としてAWSサービスを使用することで、Axwayではクラウド配信と同じ速さで製品のアップデートを受け取ることができ、ダウンタイムが短縮され、全体的な所有コストが削減されました。

クリステンセン氏は、FireEyeのソリューションだけでなく、他社の製品も統合できるという、FireEye Helixの柔軟性についても評価しています。「現実問題として、当社はすでに一部のツールに投資しており、これを簡単に無駄にしてしまうわけにはいきません。FireEye Helixのすばらしい点は、既存のツールと簡単に統合できることです。これまでに確立した情報ソースも引き続き利用できるのです。FireEyeのソリューションにいつでも切り替えることもできます」

FireEye Helixによって、クリステンセン氏は、全社にわたって配備された複数のソリューションから収集される脅威インテリジェンスを一元管理できます。Eメール、ネットワーク、エンドポイントなどの重要な攻撃経路を網羅する包括的な視野を手に入れたことにより、不審な活動を速やかに分離し、直ちにMandiant Managed Defenseによる調査に回すことができます。

最近の例を挙げると、ある社員が不注意により、フィッシング攻撃を受けました。Helixがこの脅威を迅速に特定して封じ込め、ITセキュリティ部門がMandiant Managed Defenseチームと協力して対処した結果、インシデントの影響を最小限に抑えることができました。

「すばらしかったのは、Mandiant Managed Defenseチームがその後2週間にわたってこのインシデントに取り組んでくれたことです。その結果、攻撃を受けてから24時間の全容が明らかになり、他には被害がなかったことを確認できました。Mandiant Managed Defenseチームは当社のチームと毎日話し合い、当社が正しい情報を得ていること、今後の防御方法を理解していることを確認してくれました」と、クリステンセン氏は語ります。

インシデント対応への注力と侵害の被害拡大の回避が、Mandiant Managed Defenseと他のサービスとの大きな違いだとクリステンセン氏は強調します。「Mandiant Managed Defenseチームのおかげで、当社が直面する脅威に関する具体的な情報と、潜在的な脆弱性への対処方法に関する知見を得ることができました。当社の環境を大きな視点で理解し、どのように守ればいいのかを知ることができたのです」

セキュリティのトップ企業との提携

AxwayとFireEyeとのこれまでの経験を振り返って、クリステンセン氏は次のようにまとめています。「FireEyeはセキュリティのトップ企業です。FireEyeのサービスを導入することで、当社の企業としての態勢を見直し、FireEyeのソリューションとサービスを支えている世界レベルの専門知識に沿った考え方に変える機会が得られました。FireEyeとの間に築かれた関係は、当社のセキュリティ態勢全体を改善する原動力となっています」

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

©2019 FireEye, Inc. All rights reserved.
FireEyeはFireEye, Inc.の登録商標です。その他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。F-EXT-CS-JA-JP-0000230-01

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の課題となっていた複雑性や負担を解消します。

