



## SMXがメールセキュリティ、アーカイブ、プラットフォームソリューションおよびサービスにVADE SECUREを統合

Vade Secureと提携したことで、フィッシングのキャッチ率が向上し、SMXの製品ラインが発展しました。

### SMXについて

SMXは、ニュージーランドの企業、政府機関、組織向けのメールセキュリティを提供する、現地で経営されている最大のプロバイダーです。ニュージーランド全体だけでも1000社以上の顧客を抱え、100万のメールボックスを保護しているSMXは、クラウドメールフィルタリング、コンプライアンス、ソフトウェアのアーカイブ、マネージドサービス、メールセキュリティ、通信会社のホスティングサービスを提供しています。

### 課題

SMXは、ニュージーランド最大の通信会社を自社の顧客専用のメールマネージメントプラットフォームに移行させることに成功しました。しかしながら、プラットフォームに組み込まれていた最初のメールセキュリティ製品は、スパムのフィルタリングには十分でしたが、当時急激に増加していたフィッシングメールのような動的な脅威の新しい波に対処するのに苦戦していました。

特にニュージーランドを拠点としたフィッシング攻撃は激化しつつありました。「私たちがニュージーランドで分かったことは、大量の脅威を目にしたのは概して私たちが初めてだということです」と、SMXの製品マネージャーであるジェイミー・キャラガン氏は言いました。「私たちは、フィッシングが世界展開する前の試験的なプラットフォームのようなものです」

人口およそ500万人のニュージーランドは、スーパーマーケットから通信事業プロバイダーまで、消費者が信頼を寄せる小規模ながら確立したブランドグループがあります。それらの信頼あるブランドを装った利益中心型のフィッシングメールは、メール通知やその他の定期購読に登録している消費者に対して標的型でパーソナライズされた攻撃をしかけるようになりました。

ますます洗練されていくフィッシングメールに対処するためには、現行のソリューションを絶えず適応させていかなければなりません。「私たちは、膨大な時間をベンダーとの協力で当て、この問題に対処するために数えきれないほどの業務時間を費やしました」とキャラガン氏は言いました。キャラガン氏によれば、それは持続可能なことではなく、別のレベルの分析が必要であることが明らかになったそうです。SMXは、第2のさらに最新型のソリューションを実装する必要があると判断しました。

### ソリューション

この問題を解決するために、SMXは新しいメールセキュリティフィルターを探し始めました。評価基準の中で、現代的かつ自動化されたメールセキュリティアプローチを採用することが最重要基準になりました。「私たちが、新種のエンジンを求めています」と、キャラガン氏は言いました。「つまり、私たちが保護し、異なる方法で新しい脅威を見張るソリューションです」

SMXが求めていなかったのは、Fingerprintベースの検出機能によってメール脅威を阻止する従来型のソリューションです。キャラガン氏によれば、それ

### SMXがVADE SECUREを選んだ理由

- ✓ キャッチ率の向上
- ✓ エンジンを微調整する機能
- ✓ パーソナライズされたサポートとアカウントサービス
- ✓ きめ細かなレポート

らのレガシーソリューションでは、新しい脅威が出現してから最終的にエンジンがそれに追いつくまでに遅れが生じるということです。「私たちはその時間差を縮めなくてはなりませんでした」

Vade SecureのコンテンツフィルタリングSDKは、人工知能とヒューリスティックベースの行動分析を活用して、フィッシング、マルウェア、スパイフィッシングを含む動的なメール脅威を阻止します。コンテンツフィルタリングSDKはローカル分析とグローバル分析を組み合わせ、メールの送信元、内容、背景を調べて動的なメール脅威を阻止し、グレーメールを分類します。ヒューリスティック分析と人工知能によって、メールとウェブページの10以上の要素を計算し、安全性と分類について判断を下します。

その他複数のソリューションを評価した後で、SMXはVade SecureをPOC中にモニタリングモードで作動させることにしました。モニタリングモードは、メールトラフィックを分析しますが、メールに対してアクションを起こさないため、SMXの顧客やユーザーへのリスクを限定します。

## 結果

POCの期間中、SMXはフィッシング検出機能で直ちに結果が現れたのを確認しました。「Vade Secureは問題を解決しました」とキャラガン氏は言いました。「しかし、誤検出もありました」この問題を解決するために、SMXはVadeと密接に協力して、フィルターが顧客のメール環境やその地域のニュアンスに適応するように調節しました。

「私たちはVadeと協力して、エンジンをニュージーランドの状況に合わせて微調整しました」とキャラガン氏は言いました。例えば、その地域特有の言葉やキーワードがエンジンを訓練するために使われました。「Vadeは非常に優れた方法でプラットフォームをプロファイリングし、経験したことから学習し、迷惑メールを検出しながら正規のメールを拒絶しないように最適なバランスを見出します」

キャッチ率が増加したという報告だけでなく、自社の顧客からのエスカレーションとサポートが大 要求 幅に減少したことがSMXから報告されました。キャラガン氏によれば、全体として、エスカレーションとサポート要求が減少したことで、費用 削減の効果を得るとともに、風評被害のリスクが減少しました。

SMXは階層化されたメールセキュリティアプローチを採っているため、Vadeをその他のソリューションに重ねることで顧客により包括的な保護を提供できるようになりました。「私たちは、Vade Secureだけでなく他のベンダーからも脅威インジケータを取得し、3つか4つのレイヤーを組み合わせお客様を保護しています」

プロジェクトが成功したのを受けて、SMXは、ニュージーランドとオーストリア中に存在する通信事業者の顧客のためのマルチテナントビジネスプラットフォームと独自のSMXのマルチテナントプラットフォームにVade Secureのコンテンツフィルターを統合しました。「それらのプラットフォームで、私たちはすでに2つのエンジンを使用していました。Vade Secureの最新の検出機能の価値を確認したことで、私たちは、そのうちの1つのエンジンをVade Secureに置き換えました。それはキャッチ率の低さに基づいた非常に簡単な決断でした」

「Vadeのおかげで、私たちは脅威検出におけるバイナリの意思決定から発展することができ、当社の製品全体を発展させることができました。さらにVadeは、カスタマイズされた線形アプローチの開発をサポートしてくれました。つまり、Vade Secureを使うことで当社の製品が進化しました。」

SMXはVadeと密接に連携して、SMXのビジネス顧客に適するようにフィルターを調整しました。特に金融サービスの顧客は、金融取引関連のメールトラフィックが非常に多いため、警告が発せられて誤検出を招きます。「正規のメールを阻止することに関しては、彼らは非常に敏感です。私たちは、お客様とVade Secureの両者と密に連携して誤検出の解決に取り組みました」とキャラガン氏は言いました。「物事をより寛大にして、お客様に対するSMXのビジネスプロフィールを微調整するために複数のルールをオンにしたりオフにしたりしました」

SMXは、最終的にその他複数のSMX製品やサービスにVade Secureを統合しました。それらには、隔離、URL分析、ビジネスがデータ損失を防止してコンプライアンスポリシーを実行できるようにするインジケータや条件をフィードするSMXの高度なルールを基本とするエンジンなどが含まれます。

「Vadeのおかげで、私たちは脅威検出におけるバイナリの意思決定から発展することができ、当社の製品全体を発展させることができました。さらにVadeは、カスタマイズされた線形アプローチの開発をサポートしてくれました。つまり、Vade Secureを使うことで当社の製品が進化しました。」

さらに、SMXはVadeの レポート 機能を自社の製品に統合しました。キャラガン氏によれば、この機能は高度な詳細を提供し、メール分類に関するよりきめ細かな情報（結果と判断）を提供するというものです。「私たちは、お客様が直面する脅威の種類と彼らのリスクプロフィールをお客様に提示できます。SMXがお客様に提供できる価値を伝えることは重要であり、Vade Secureによって提供される情報がそれに役立っています」

人とテクノロジーを組み合わせることで、プロジェクトは最終的に成功しました。これは、メールセキュリティとアカウントサービスの両方に対する パーソナライズ されたアプローチです。

「ニュージーランドを拠点とするフィッシング攻撃のキャッチ率—それは当時、競合他社が提供できないものでした。しかも、Vade Secure の提供しているサポートとアカウントサービスは非常に優れています。また、非常に高いレベルで パーソナライズ された レポート を提供されています。他のベンダーからこのレベルの報告を受けることは絶対にありません」

ジェイミー・キャラガン、SMX 製品マネージャー