2020 年 7 月 16 日

関 係 各 位

高 千 穂 交 易 株 式 会 社

高千穂交易、Microsoft 365 専用脅威検知ソリューション『Vade Secure for Microsoft 365』の販売開始

～世界 76 ヵ国、6 億個以上のメールボックスデータを活用した AI エンジンで既存セキュリティを補強～

高千穂交易株式会社(本社:東京都新宿区、代表取締役社長:井出尊信、証券コード 2676)は、Vade Secure（ヴェイド・セキュア）社と、AI（人工知能）搭載の Microsoft 365 専用脅威検知ソリューション『Vade Secure for Microsoft 365』の代理店契約を締結し、その販売を開始しました。

近年、フィッシング、スピアフィッシング、マルウェアといった標的型攻撃*1 の量は増え続けており、その手口もますます巧妙化されております。それらの標的型攻撃はメールを入口として行われ、中でも、Microsoft 365 は、全世界に多くのユーザーが存在することや 1 つのエントリーポイントから OneDrive・SharePoint のような豊富なデータを持つアプリケーションにアクセスできることから、サイバー犯罪者たちにとって最大の標的となっています。そのような背景から、これまで以上にメールへのセキュリティ対策の重要性は高まっています。

今回販売を開始する Vade Secure for Microsoft 365 は Microsoft365 と API ベースの統合により、システム環境を変更することなく容易にソリューションのインストールが可能で、メールフローを変えることなく利用できます。このセキュリティ対策は Microsoft 365 のセキュリティ機能である EOP（Exchange Online Protection）*2 を置き換えるのではなく、新たなセキュリティ層を追加することで機能を強化します。
また、ヴェイド・セキュア社が保護している世界 76 カ国、6 億個以上のメールボックスから収集したデータを基に構築された AI エンジンを備えており、既知の脅威については EOP を利用し、新たな脅威にはこの AI による（最高クラスの）脅威検知機能で防御します。

【提供する主な機能】

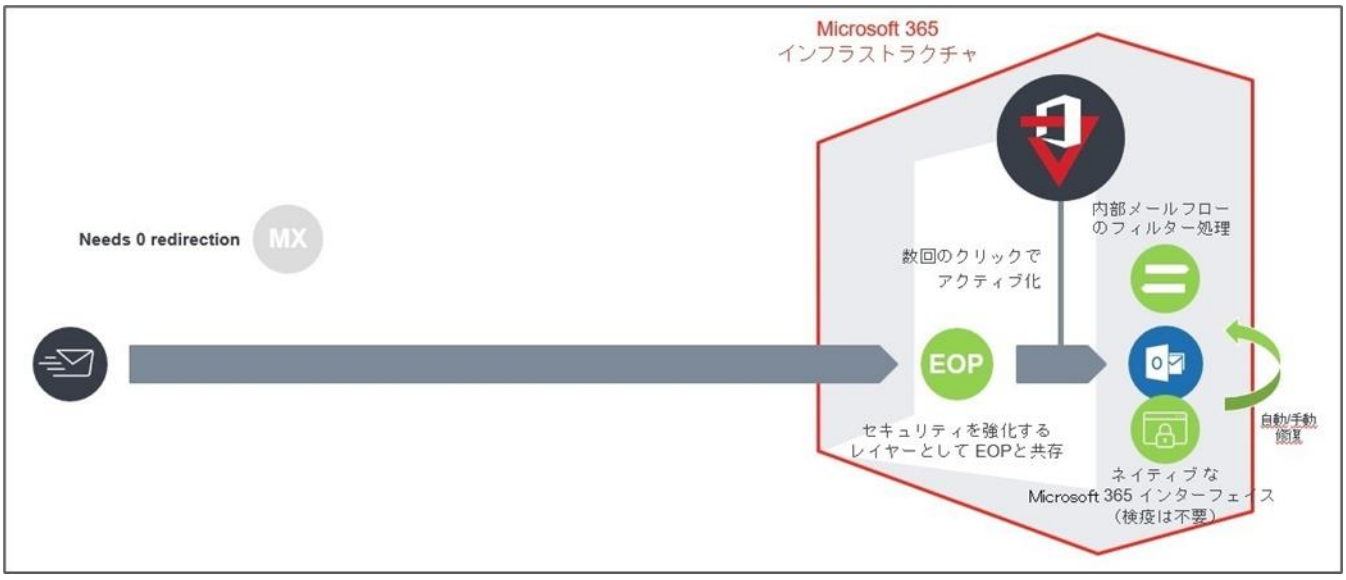
■クリック時のフィッシング対策 :あらゆるリダイレクトを追跡しながらリアルタイムで URL とウェブページを分析し、それらが不正なものでないかどうかを判断します。メール受信時とクリック時の両方でこの分析を行うことで、時限爆弾 URL*3 から保護します。さらに、管理者はユーザーが不正なリンクをクリックすると警告を受信します。

■バナーによるスピアフィッシング対策 :検知が困難なカズンドメイン*4 を使ったなりすまし詐欺などの異常を検知すると、メール内にバナーが表示され、ユーザーに警告します。

■行動に基づいたマルウェア対策：添付ファイルのスキャンだけではなく、AI による機械学習モデルが、メールと添付ファイルの送信元、内容、コンテキストを総合的に分析することで、長時間を要することなく、脅威を検知することができます。
■自動および手動でのメール分類の修復:最初に正規メールとして分類されたものの、後からスパムだとわかったメールに対し、過去 7 日間の受信メールは Microsoft365 の API を利用し、再分類する自動修復機能を持っています。このような脅威受信後の修正を行うことで、リアルタイムのフィッシング検出を強化し、更には AI により継続的な学習を重ねることで、受信ボックスから自動的に脅威を取り除きます。また、管理者は脅威と見なされたメッセージの回復や削除などを手動で修復することが可能です。

【Microsoft 365 ユーザーが導入するメリット】
■短時間で配備完了：Microsoft365 のユーザーは、数回のクリックのみでソリューションの利用が開始できます。従来のメールセキュリティゲートウェイと異なり、MX レコードを変更する必要がないため、これまで通りのメールフローでの利用が可能です。
■Microsoft 365 のセキュリティを補完：AI による（最高クラスの）脅威検知機能で EOP を増強します。
■ネイティブなユーザー体験：使い慣れた Microsoft365 のインターフェースをそのまま使用でき、別の隔離ボックスを確認する必要はありません。
■内部の脅威からの保護：外部からのメール受信時のみではなく、社内メールを含むメールフロー全体をスキャンして、インサイドアタック（社内からの攻撃）からも防御します。

[Vade Secure for Microsoft365 イメージ図]



当社は、この『Vade Secure for Microsoft 365』をこれまでに Microsoft365 やメールセキュリティサービスを販売するパートナー様を通じて、今年度 15,000 ユーザーへの販売を、また、2023 年度末までに 150,000 ユーザーへの販売を目指します。

*1　標的型攻撃：情報の盗み出しなど明確な目的を持ち、企業や団体といった特定の組織のへ行われるサイバー攻撃の一種。

*2　Exchange Online Protection：スパムやマルウェアなどの攻撃から組織を保護するためのクラウドベースのフィルタリングサービス。　詳しくは、右記 Microsoft の WEB サイトをご参照ください。https://www.microsoft.com/ja-jp/

*3　時限爆弾 URL：メール受信時は正当なウェブページの URL が記載されているが、それをクリックすると自動的にフィッシングページの URL へリダイレクトされてしまうフィッシング手法のひとつ。

*4　カズンドメイン：有名な企業や団体、個人などで使用されているドメインに似せて（なりすまし）、正規メールと受信者に信じ込ませる偽装ドメインのこと。

【Vade Secure からのコメント】

「日本は Vade Secure の主要な市場であり、高千穂交易との販売代理店契約は、付加価値サービスとソリューションを追加することでマイクロソフトのセキュリティポートフォリオを強化したい各地域のパートナーに対応するための国際的な開発戦略の一部です」とグローバル・チャネルセールス担当上級副社長のフレデリック・ブラウトは述べています。

当社の AI ベースのソリューションは、パフォーマンス、操作性、インストール、メンテナンスの容易性といった点において、パートナーのニーズに完全に適合しており、高千穂交易が Microsoft 365 ユーザーのためにソリューションを活用し、ビジネスとして成長を続けることを確信しています。

【Vade Secure 社について】

- 2009 年 設立、本社：フランス共和国リール市（世界各地に 6 事業所を持つ）
- 予測的メール防衛の世界的リーダー
- 全世界 76 ヵ国で事業展開し、5,000 社を超える顧客への導入実績
- 93%以上の更新率
- 11 件のアクティブな国際特許
- 全世界で 6 億個のメールボックスを保護
- 1 日当たり 100 億件のメールを分析

Vade Secure 株式会社（日本法人）
住所　東京都港区六本木 7-7-7 TriSeven 8F
設立　2017 年 7 月
代表者　Georges Lotigier
URL　https://www.vadesecure.com/jp/

■このニュースリリースに対するお問い合わせ

高千穂交易株式会社
管理部　総務情報システムチーム　椿、菅野
TEL：　03-3355-1125　/　E-mail：　ktsubaki@takachiho-kk.co.jp