Vade Secure
Predictive Email Defense

Vade Secure for Microsoft 365

Microsoft 365のためのネイティブなAPIを搭載とする予測的メール防衛

Microsoft 365のセキュリティ機能（EOPなど）は、スパムや既知の脅威の大半を捕獲できますが、組織には未知のダイナミックな脅威から防御するための追加の保護が必要です。その理由から、Microsoft 365のクライアントのうち50%が2020年までにサードパーティソリューションのサポートを受けることになるとGartnerは予測しています。

Vade Secure for Microsoft 365を使って、高度なフィッシング、スピアフィッシング、マルウェア攻撃からユーザーとビジネスを保護しましょう。ネイティブなAPI統合によってMicrosoft 365内に配置されるVade Secureは、AIを基本とした予測的メール防衛を活用してMicrosoft 365のレピュテーションおよびシグネチャベースの防衛を強化します。しかも、そのためにユーザーが行動を変える必要はありません。

未知の標的型の攻撃を検出する人工知能

Vade Secure for Microsoft 365 は、ヒューリスティックルールと複数のAIテクノロジーを活用した行動フィルターエンジンにより、最初のメールで攻撃を阻止します。Vade Secureは、リアルタイムでURLや添付ファイルを含むメール全体の行動分析を実行しながら、世界中で保護されている 10億 のメールボックスから寄せられるデータやユーザーからのフィードバックレポートを活用して、フィルターエンジンを継続的に微調整して高い精度率を保ちます。

多面的なフィッシング対策-あらゆるリダイレクトを追跡し、最終ページが不正なものかどうかを判断して、リアルタイムでメールとURLの多層的な行動分析を実行します。マシンラーニングモデルがメールとURLの47種の特徴を分析して悪意のある行動を調べる一方で、Computer Visionアルゴリズムは、変更されたロゴ、QR Codeおよびフィッシング攻撃でよく使われるその他の画像をスキャンします。

バナーベースのスピアフィッシング対策-Natural Language Processingアルゴリズムが不審なテキストを解釈すると同時に、異常検出機能が従業員一人一人についての正常なコミュニケーションパターンを確立する匿名のプロファイルを構築します。ユーザーのなりすまし攻撃や財務的な要請などの異常が検出されると、カスタマイズ可能なバナーが表示されてユーザーに警告します。

行動に基づいたマルウェア対策-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します。添付ファイルのスキャンだけでなく、このソリューションは、サンドボックス技術よりもずっと早くマルウェアを検出できるため、ユーザーに対するレイテンシーが発生しません。

インサイダー脅威対策-Microsoft 365にネイティブに統合するため、社内のメールトラフィックをスキャンして、不正アクセスされたアカウントを使ったインサイダー攻撃を予防します。

配信後の脅威に対する機能と性能

忙しい管理者のために作られた、ユーザーによって強化されるAIベースのテクノロジー

Auto-Remediate-配信後の脅威の自動化されたremediationによって、脅威の検出機能を強化します。Vadeが保護している 10億 のメールボックスから得たリアルタイムの世界的な脅威情報を活用しながら、Auto-Remediateは絶えずメールをスキャンし、新たな脅威が検出された場合は、ユーザーの受信ボックスから自動的にメッセージを削除します。管理者が手動でワンクリックでメッセージを回復することもできます。

Vade Threat Coach™ -ユーザーがフィッシングメールを開いたり、フィッシングリンクをクリックしてしまった時に、軌道修正のための自動化された適応型のトレーニングを配信します。フィッシングメール内のなりすましブランドに適応したゲーム化されたフィッシングトレーニングを用いたVade Threat Coach は、ベストプラクティスを強化する補完的で臨機応変な学習コンテンツを提供することで、構造的なトレーニングのギャップを埋めます。

ログと報告-ダッシュボード、報告、リアルタイムのログを表示して、検出されて回復された脅威の最新情報の概要を提供します。管理者は、メールトラフィックを監視して、現在進行中のイベントをベースにしたメール脅威を特定したり、誤って分類されたメールをワンクリックで修正したりできます。

統合されたフィードバックループ-Microsoft Outlookの「迷惑メール」および「フィッシング」ボタンを使って、ユーザーがVade SecureのSOCにメール脅威を直接報告できます。Vade Secureのフィードバックループは、ユーザーのフィードバックをフィルターと自動回復機能の有効性を継続的に強化するために使われる極めて重要な脅威インテリジェンスに変えます。

ネイティブなMICROSOFT 365のユーザー体験を提供する、完全にAPIベースのソリューション

MXレコードの変更が必要で、メールフローを中断させてしまうメールセキュリティゲートウェイ（SEG）とは異なり、Vade Secure for Microsoft 365は、Microsoft APIとネイティブに統合するため Microsoft 365の内部に配置されます。

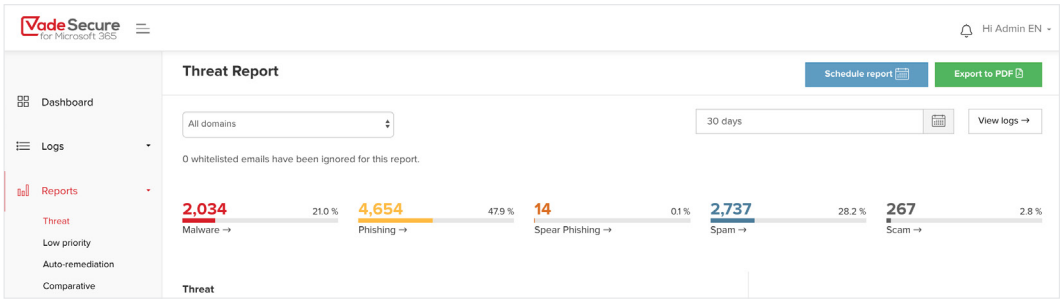
この構造的なアプローチは、管理者とエンドユーザーに数々の利点をもたらします：

MXレコードの変更不要 – 数回クリックするだけで起動します。MXレコードを変更する必要はありません。

EOPと層を成す-Microsoftが見逃してしまう脅威をキャッチする補完的な技術でEOPを強化します。付加価値レポートEOPのキャッチ率にVadeのキャッチ率を加えて数値化します。

複雑なルールも設定もなし：簡潔な脅威ベースのポリシーを設定し、Exchange Onlineの設定をシームレスに取り込んで重複を回避します。

UXの変更不要、外部隔離なし-ユーザーは、ユーザー体験を変更したり、外部隔離を管理したりせずに引き続きMicrosoft Outlookで作業を続けられます。Vadeは、Outlookのフォルダー内で定義されたポリシーに基づいてメールをフィルタリングします。



Vade Secureについて

- 世界中で10億個以上のメールボックスを保護
- 1,400 世界中のパートナー
- 95%以上の更新率
- 11件のアクティブな国際特許
- 昨年20億件のメッセージがフィルタリングされました

お問い合わせ先

Vade Secure株式会社
sales.japan@vadesecure.com