Trend Vision One – Email and Collaboration Security™

メール攻撃に対する防御・検知・対応の一元的な管理を実現

攻撃者はメールからの初期侵入を成功させるために攻撃手法を日々巧妙化させています。フィッシングはメール攻撃の中でも多く悪用されており、Microsoft 365を利用している500社のうち92%の企業がメールに加えコラボレーションツールにまで拡大した最新の攻撃手法による被害を受けています。

ビジネスメール詐欺（BEC）、ランサムウェア、フィッシング、ソーシャルエンジニアリング、マルウェアからユーザを保護する必要があります。しかし、既知の脅威を防御する従来のメールセキュリティ対策では、限られた範囲の攻撃のみしか把握できず、攻撃の全体像を把握することはできません。

システム管理者にとっての死角

世界各国で企業はコラボレーションツールを活用し、生産性を高めています。このようなコミュニケーション手段の変化に対して、十分なセキュリティ対策ができておらず、リスクに晒されている可能性があります。

巧妙化する攻撃を防ぐ技術や、不審メールへの適切な対応や報告について従業員を教育するトレーニングがなければ、攻撃被害に遭うリスクの軽減は難しいでしょう。

Trend Vision One – Email and Collaboration Security

Trend Vision One - Email and Collaboration Securityは、統合サイバーセキュリティプラットフォームを活用することで、巧妙化する攻撃への防御から復旧までを実現し、メールやコラボレーションツール対策の進化をより加速させます。

API連携・インライン・ゲートウェイ保護と管理の一元化

- API連携によるクラウドメールおよびコラボレーションツールの保護：受信、送信、内部メールおよびファイル、チャットメッセージにおける脅威をAPI経由でリアルタイム検査し、メールおよびコラボレーションツール（Microsoft 365、Google Workspace、Box、Dropbox）を保護します。
- ゲートウェイでのメール保護：送受信メールにおける脅威のリアルタイム検査およびメール暗号化による機密情報漏えいの防止、脅威を含むメールやなりすましメールから保護します。
- Trend Vision One - XDR for Email：メールをはじめ複数レイヤーから連携されたデータの相関分析により、攻撃の全体像を可視化します。XDR for Emailでは、連携されたEmail Sensorを介して収集されたメールアクティビティデータを活用します。
- Trend Vision One - Attack Surface Risk Management (ASRM)：継続的なリスク評価と対応の優先度付けによるリスク軽減を行います。

主なベネフィット:

- アカウント乗っ取りに対する保護
- フィッシングやビジネスメール詐欺（BEC）に対するメールおよびコラボレーションツールのリアルタイム保護
- API + インライン + ゲートウェイによるマルチレイヤーでのセキュリティ対策
- 一元管理によるサイロ化の解消と可視性の向上
- メールおよびコラボレーションツール全体のセキュリティポスチャの改善
- メールおよびコラボレーションツール保護の最適化、従業員のセキュリティ維持、アナリストエクスペリエンスの統一

Trend Vision One - Email and Collaboration Security 概要

主な特徴:

メール・コラボレーションツールの保護

API連携によるクラウドメールおよびコラボレーションツール保護により、BEC、アカウント乗っ取り、フィッシングに対する高度な脅威対策およびデータ保護を実現。クラウド上でのファイル共有およびコラボレーションツール（Microsoft 365、Google Workspace、Box、Dropbox）のコンプライアンスを強化。

AI・機械学習などの高度な機能による攻撃防御

ゲートウェイでのメール保護により、既知および未知の脅威、そして巧妙化しているフィッシング等の攻撃を防御。不審メールの文体分析*やメール暗号化にも対応。

*ご利用の場合、別途API連携が必要です。

「何を」「誰が」「どこで」の可視化

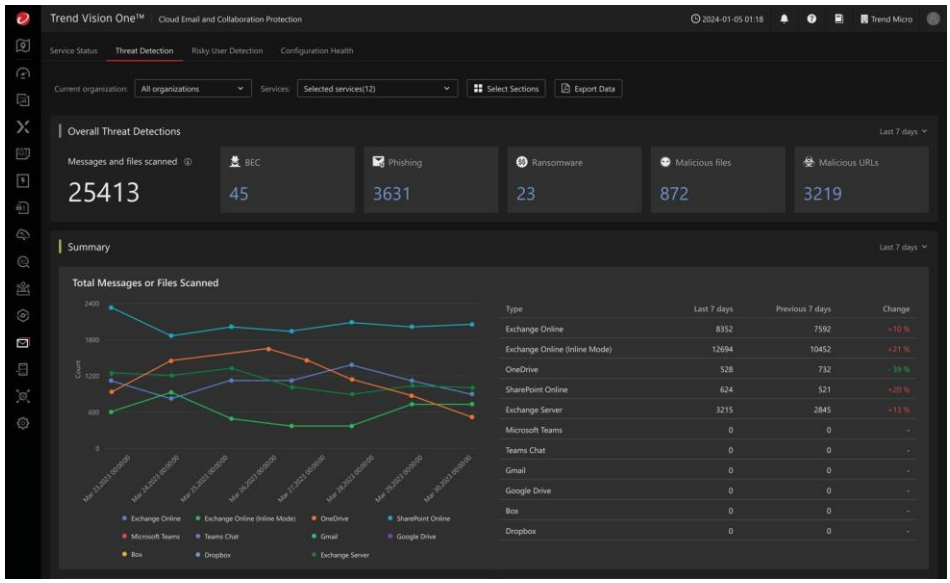
XDR for Emailの高度な分析によるクラウドメールのセキュリティ運用（SecOps）を向上。メールアクティビティデータを活用し、1カ所に集約された他レイヤーのデータも含めたクロスレイヤーでの検知、対応（XDR）を実現。

最新脅威・脆弱性・リスクの分析

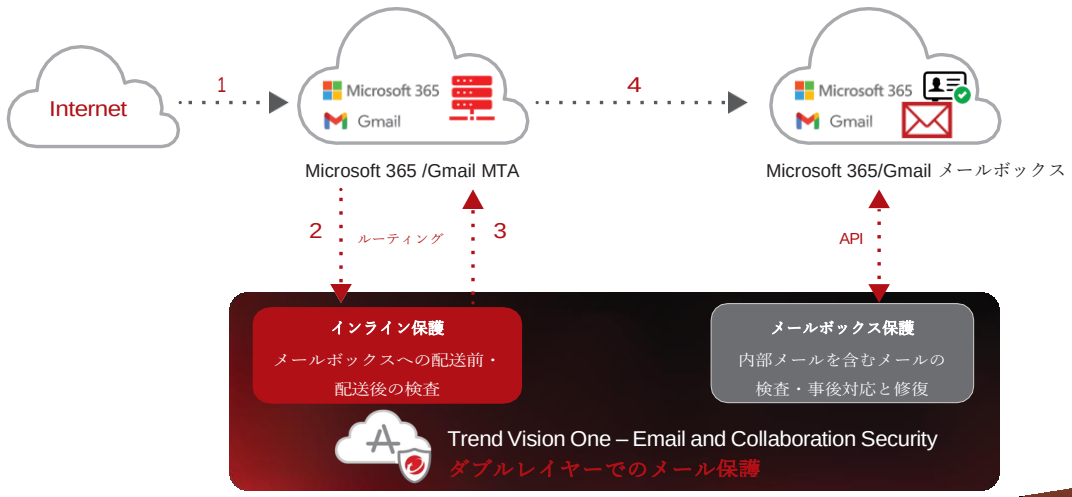
ASRMにより、ビジネスエグゼクティブおよび運用担当者向けにリスク状態を一元的に可視化。継続的なアイデンティティベースのリスク評価と対応の優先度付け、標的になっているリスクが高い従業員や高リスクのイベントが発生している従業員へ対する推奨対応を実現。

統合サイバーセキュリティプラットフォームTrend Vision One – Email and Collaboration Security:

Microsoft365・Google Workspace Gmailに対するインラインおよびAPI連携でのメール保護



ソリューション・アーキテクチャ:



機能一覧:

	CLOUD EMAIL AND COLLABORATION PROTECTION	CLOUD EMAIL GATEWAY PROTECTION
アーキテクチャ	API連携・インライン	ゲートウェイ
アンチウイルス・アンチスパム・Webレピュテーション・高度な脅威対策	√	√
情報漏えい対策	√	√
エンドユーザメール隔離	√	√
IPレピュテーション	√	√
ドメインの真正性確認		√
不達メール継続管理		√
メール暗号化		√
DMARC監視		√
サンドボックス解析（ファイル・URL）	√	√
ビジネスメール詐欺（BEC）対策	√	√
ライティングスタイル分析	√	√
QRコードの検査	√	√
パスワード解析	√	√
不審オブジェクト連携	√	√
レトロスキャン（過去数日間のメールの自動再検索）	√	
MIP（Microsoft Purview Information Protection）との連携	√	
コラボレーションツール対策 (Microsoft 365, Google Workspace, Box, Dropbox)	√	
手動検索（任意期間のメールの事後検索）	√	
APIリクエストによる対応	√	
エンドユーザによるフィードバック機能	√	
標的型攻撃リスクのあるユーザの可視化	√	
アカウント乗っ取りリスクのあるユーザの可視化	√	
	XDR FOR EMAIL	
ログの連携・参照・検索	√	
メールおよびクロスレイヤーでのXDRアラート検知	√	
メールへの事後対応	√	
Observed Attack Techniques: MITRE Att&ck マッピング	√	
テレメトリデータの収集	√	
不審オブジェクト設定による自動スイーピング	√	
	ASRM	
ビジネスエグゼクティブ向けダッシュボード	√	
リスクの可視化	√	
運用担当者向けダッシュボード	√	

Trend Vision Oneでのメールセキュリティ対策の強化 – XDR(Extended Detection and Response)：

メールに加え、エンドポイント、サーバ、クラウドワークロード、アイデンティティ、ネットワーク、IoTなどのあらゆるレイヤーに対するXDRを実現します。

攻撃に対するより広い可視性、より深い分析

XDR は、攻撃起点からネットワーク全体への攻撃の横展開まで、複数のセキュリティレイヤーにわたる詳細なアクティビティデータを収集し、相関分析することで、攻撃起点の特定および調査分析を可能にし、SOC チームの可視性を向上させます。

攻撃フェーズの迅速な深堀り

メール攻撃を分析することにより、攻撃の詳細情報を迅速に確認することができるようになります。攻撃の詳細情報には、関連アセット、スコア、影響範囲、不審なリンク、ユーザの詳細、攻撃フェーズ、初期アクセス、重大度レベルなどが含まれます。

XDR for Emailとともに実現する対応の優先度付け

フィッシング攻撃の範囲とその深刻度を把握することで、どの脅威が早急な対応を必要としているかを判断し、また攻撃の連鎖を断ち切るために対応の自動化を設定することができます。（例：複数のユーザにまたがるメールの隔離や、メール、エンドポイント、サーバ、クラウドにまたがるIPアドレスのブロックなど）

幅広い統合エコシステム

オープンAPIとサードパーティシステムのポートフォリオ拡大とともに、Trend Vision Oneはインフラストラクチャから有意義なデータを取得し、XDRの能力をさらに充実させることで、エコシステムとセキュリティ運用ワークフローに適合します。

統合サイバーセキュリティプラットフォームTrend Vision One – XDR・ASRM

Trend Vision Oneでのメールセキュリティ対策の強化 – Attack Surface Risk Management (ASRM)：

トレンドマイクロは、サイバーリスクの把握、対応の優先度付け、リスク軽減のために、アタックサーフェス（攻撃対象領域）のリスク管理につながる継続的なリスク可視化と分析を支援します。

未知および未管理のサイバー資産の可視化

アタックサーフェスは日々拡大し、防御は困難になりつつあります。Attack surface discovery機能では、既知および未知のアセットを継続的に特定し、攻撃への露出度とセキュリティ設定状態を通知します。

サイバーリスクの低減

アタックサーフェスのリスクに関する詳細な分析により、自社全体のリスク軽減および修復する適切な予防策を適用することができます。防御の強化、脆弱性の低減、侵害の回避をするための推奨対応と対応の自動化を実現します。

サイバーリスクの動的分析・評価

自社全体の継続的なリスク評価には、動的なリスク分析に基づくスコアリングが含まれます。リスク分析とは、脆弱性への対応状態や既存のセキュリティ設定状態、自社で確認されている脅威や攻撃フェーズについての分析を指します。

XDR for Emailとの統合

XDR によって収集されたデータは、アタックサーフェスにおける脅威活動に関する有益なインサイトを提供し、どのように対応されているかのスナップショットを提供します。アイデンティティのリスク分析結果を提示し、軽減につながる推奨方法に基づく対応を実現します。