Cisco Secure Email Threat Defense

目次

最も高度で蔓延する脅威から保護する高度な脅威検出機能

今日の組織は、1 つの困難な課題に直面しています。電子メールは最も重要なビジネス コミュニケーション ツールであると同時に、セキュリティ侵害の主要な攻撃ベクトルでもあります。

ランサムウェアとビジネスメール詐欺（BEC）による損失は驚異的であり、増加し続けています。2023 年、FBI IC3 は 21,489 件のビジネスメール詐欺（BEC）による 29 億ドルの損失の報告を受けました。また、ランサムウェアインシデントの苦情は 2,825 件を超えており、2022 年から 18% 増加しています。

Microsoft 365 のようなクラウドベースの電子メールの採用は増加し続けています。クラウドの電子メールセキュリティは、オンプレミスのアプライアンスに比べてコストがかからず、拡張性が高く、この傾向が SaaS 電子メールセキュリティ市場の成長を促進しています。電子メールは高度な脅威に対して脆弱であるため、Gartner 社は、階層型セキュリティと多様な脅威インテリジェンスを活用してクラウドメールのセキュリティを強化し、クラウドメールボックスを保護することをここ数年間推奨してきました。Cisco Secure Email Threat Defense は、最も脅威媒体になりやすい電子メールから組織を保護します。

製品の概要

Email Threat Defense は、ネイティブの Microsoft 365 セキュリティを強化し、着信、発信、および内部ユーザー間のメッセージを完全に可視化します。

Email Threat Defense を使用すると、次のことが可能になります。

- 脅威の調査と効果を追求する最大のチームの 1 つである Cisco Talos の優れた脅威インテリジェンスを利用して脅威を検出およびブロック
- Secure Endpoint と Secure Malware Analytics を使用して高度な脅威に対処
- インバウンド、アウトバウンド、および内部のメッセージを完全に可視化
- 悪意のあるコンテンツを含むメッセージに高速 API 駆動型修復を活用
- 統合されたダッシュボードを使用して、会話ビューやメッセージトラジェクトリなどの検索、レポート、およびトラッキングを実行
- メールフローを変更せずに 5 分未満で Microsoft 365 のセキュリティを強化
- QR コード、ブランドやユーザーへのなりすましなどの最新の電子メールベースの攻撃を防止

Email Threat Defense – ソリューション コンポーネントと差別化要因

Email Threat Defense は、Cisco Talos の優れた脅威インテリジェンスを活用したクラウドネイティブのソリューションです。API 対応のアーキテクチャにより、対応時間の短縮、内部電子メールを含む包括的な電子メールの可視化、会話ビューによるコンテキスト情報の把握が可能になります。また、Microsoft 365 メールボックスに潜んでいる脅威を自動または手動で修復するツールも利用できます。

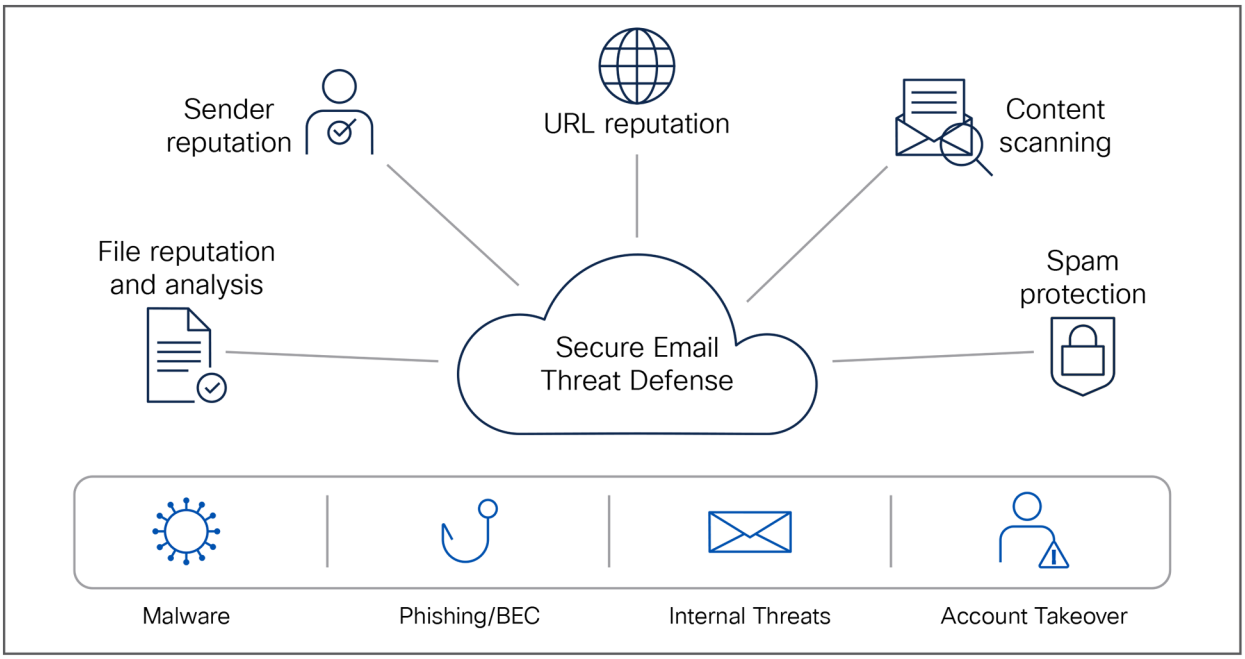

図 1.
Cisco Secure Email Threat Defense ソリューション

高度な脅威防御技術とディテクタ

Cisco Secure Email は、送信者認証と BEC 検出機能を使用してフィッシングに対抗します。機械学習と人工知能エンジンを統合し、ローカルアイデンティティとリレーションシップ モデリングをリアルタイムの行動分析と組み合わせて、アイデンティティ詐欺から保護します。これは、組織内および個人間の信頼できる電子メールの動作をモデル化します。他の重要な機能の中でも、Email Threat Defense には次の利点があります。

- 高度な脅威検出機能を使用して、既知の脅威、新たな脅威、標的型の脅威を発見
- 悪意のある手法を特定し、特定のビジネスリスクのコンテキストを取得
- 危険な脅威を迅速に検索し、リアルタイムで修正
- 検索可能な脅威テレメトリを利用して脅威を分類し、組織のどの部分が攻撃に対して最も脆弱かを把握

Talos：可視性、インテリジェンス、対応

最先端のセキュリティ調査およびインテリジェンスにおける世界最大のプロバイダーである Talos は、効果的で実用的なセキュリティコンテンツとツールを提供し、独自のプロアクティブな包括的アプローチで、正確かつ効果的に多くの脅威を阻止できるようにお客様をサポートします。

Cisco Secure Endpoint と Cisco Secure Malware Analytics

Cisco Secure Endpoint（以前の Cisco AMP）と Cisco Secure Malware Analytics（以前の Threat Grid）は、ファイル レピュテーション スコア、ブロック機能、ファイルサンドボックス環境、ファイルレトロスペクション機能を備え、脅威を継続的に分析します。

お客様は、さらに多くの攻撃をブロックして不審なファイルをトラッキングし、感染範囲を抑えながら迅速に修復できます。Secure Endpoint はシスコのセキュリティデバイス全体で脅威インテリジェンスを共有するため、エンドポイント、ネットワーク、電子メール、クラウド、Web のセキュリティが統合されます。

API 対応アーキテクチャ

Email Threat Defense は Microsoft Graph API を使用して Microsoft 365 と通信し、非常に迅速に脅威を検出して修復できます。このソリューションは RESTful API に対応し、他のセキュリティツールと非常に簡単に統合できる柔軟性を備えています。

統合ユーザーインターフェイス

Email Threat Defense には、レポート、設定、トラッキングに利用できる単一のインターフェイスが用意されています。包括的なカンバセーションビューとメッセージ トラジェクトリ ビューを備え、Microsoft 365 メールボックス内の電子メールトラフィックをすべて可視化できます。そのため、さらに効果的なコンテキスト情報を把握して適切な判断を行うことができます。

Email Threat Defense が選ばれる理由

Email Threat Defense は、シスコの実証済み電子メール セキュリティ テクノロジーを活用して、スパムやランサムウェア、ビジネスメール詐欺、フィッシング攻撃などの電子メールに対する高度な脅威をブロックします。

Microsoft 365 のネイティブセキュリティ機能の強化

Email Threat Defense は、Cisco Talos、Cisco Secure Endpoint、Secure Malware Analytics による業界トップクラスの脅威インテリジェンス（Web、ネットワーク、エンドポイントから収集したさまざまな媒体に関する膨大な脅威インテリジェンスを含む）を活用することで、Microsoft 365 ネイティブの電子メールセキュリティ機能に新たなセキュリティレイヤを加えます。

高度な標的型攻撃から保護する

Email Threat Defense は、メールボックスで送受信される電子メールを継続的に分析することで、フィッシング、ビジネスメール詐欺、アカウント乗っ取り攻撃から保護します。脅威を特定した時期にかかわらず修復可能な、常時オンのセキュリティレイヤです。

Extended Detection and Response（XDR）戦略を強化する

より大規模な XDR 戦略の重要な部分として、Cisco Secure Email は、業界をリードする脅威インテリジェンス、高度な脅威検出機能、および戦略的な脅威保護を通知する重要なテレメトリを使用して、重大な脅威から防御します。多数のサードパーティ統合パートナーおよびより大きな Cisco Secure 製品ポートフォリオとの組み合わせにより、チームが迅速に行動できるようにする可視性、効率性、シンプルさ、およびテレメトリを提供します。

すぐに設定して導入可能

Email Threat Defense はシンプルさを体現しています。保護機能は、メールエクスチェンジャ（MX）レコードを変更することなく、簡単なワンタイム設定でアクティブにできます。そのためメールフローの変更に伴うリスクはなく、メール配信にも遅延が生じません。このソリューションには次の特長があります。

- クイック セットアップ ウィザードを使用して即座に Proof-of-Value（PoV）を実施可能
- Microsoft 365 メールボックスを監査モードでモニターするか、脅威を適用モードで修復
- 5 分未満ですべて設定可能
- Proof of Value（PoV）環境を即座に実稼働環境に変換可能

クラウド ネイティブ ソリューションを活用する

Email Threat Defense は、高可用性、パフォーマンスの最適化、迅速な検出および対応を実現するクラウドネイティブ ソリューションです。真の API 主導型クラウドソリューションとして地域を越えてグローバル規模で迅速に導入でき、需要に基づいてリソースを自動的に拡張可能です。

内部のユーザー間電子メールを始め電子メールを完全に可視化

社内外を問わずメールボックスで送受信されるすべてのメッセージは、同じレベルの精密さで調査する必要があります。そうすることで、組織内の悪意のあるユーザーであれ、侵害された Microsoft 365 メールボックスであれ、内部からの脅威の拡散を最小限に抑えることができます。Email Threat Defense は、メールボックス内のすべてのメッセージ（社内/社外、送信/受信問わず）をスキャンします。管理者は、すべてのメールボックスのメッセージを検索できます。

強力なレポート

Cisco Secure Email Threat Defense は、組織を標的とする最も一般的な攻撃ベクトル、主要な標的ユーザー、ビジネスリスク、および使用されている手法を把握するのに役立つ包括的なレポート機能を提供します。これらのレポート機能が、追加のセキュリティポリシー、エンドユーザートレーニングなどの意思決定を支援します。

Cisco XDR Threat Response ケースブックによる攻撃分析の実行

Email Threat Defense は、Cisco XDR Threat Response ケースブックと統合されており、複数製品での調査や攻撃分析時に一連の調査結果を記録して整理し共有できます。

技術的な詳細情報

展開オプション

- 監査（Audit）
- 監査と施行（Audit with Enforcement）

適用アクション

- ゴミ箱に移動（Move to Trash）
- 迷惑メールに移動（Move to Junk）
- 受信トレイに移動（Move to Inbox）
- 隔離に移動（Move to Quarantine）
- 削除（Delete）
- 動作なし

サポートされている判定

- BEC
- 詐欺
- フィッシング
- Malicious
- スパム
- グレーメール
- ニュートラル

影響力の高い人員リスト

エグゼクティブ リーダーシップ チームのメンバーなどの重要人物は、他のターゲットを侵害することを目的とした、なりすましを受ける危険にさらされています。影響力の高い人員リストは、Cisco Secure Email Threat Defense がなりすまし攻撃から組織を保護するのに役立ちます。

管理者は、最大 100 人のリストを作成して Cisco Talos に送信し、表示名と送信者の電子メールアドレスをさらに精査することができます。個人用に構成された情報からの逸脱は、有害と判定されたメッセージの [判定の詳細（Verdict Details）] パネルで [テクニック（Technique）] として識別されます。

レポート

- 動向レポート
- 影響レポート
  - 以下に関する指標と 12 か月の予測：
    - BEC
    - 詐欺
    - フィッシング
    - Malicious
    - スパムおよびグレイメール（不要なメッセージ）
  - 上位のターゲット：脅威の種類ごとに、最も多くの脅威メッセージを受信したアドレスを示します。
  - 起点ごとの脅威トラフィック（内部、着信、発信、混合）。
  - 侵害された可能性のあるアカウント：ここにリストされている内部アドレスは、組織内から脅威メッセージを送信していることが確認されています。
  - Email Threat Defense による保護：環境内の受信者のメールボックスに提供される Email Threat Defense の保護に関するメトリック。

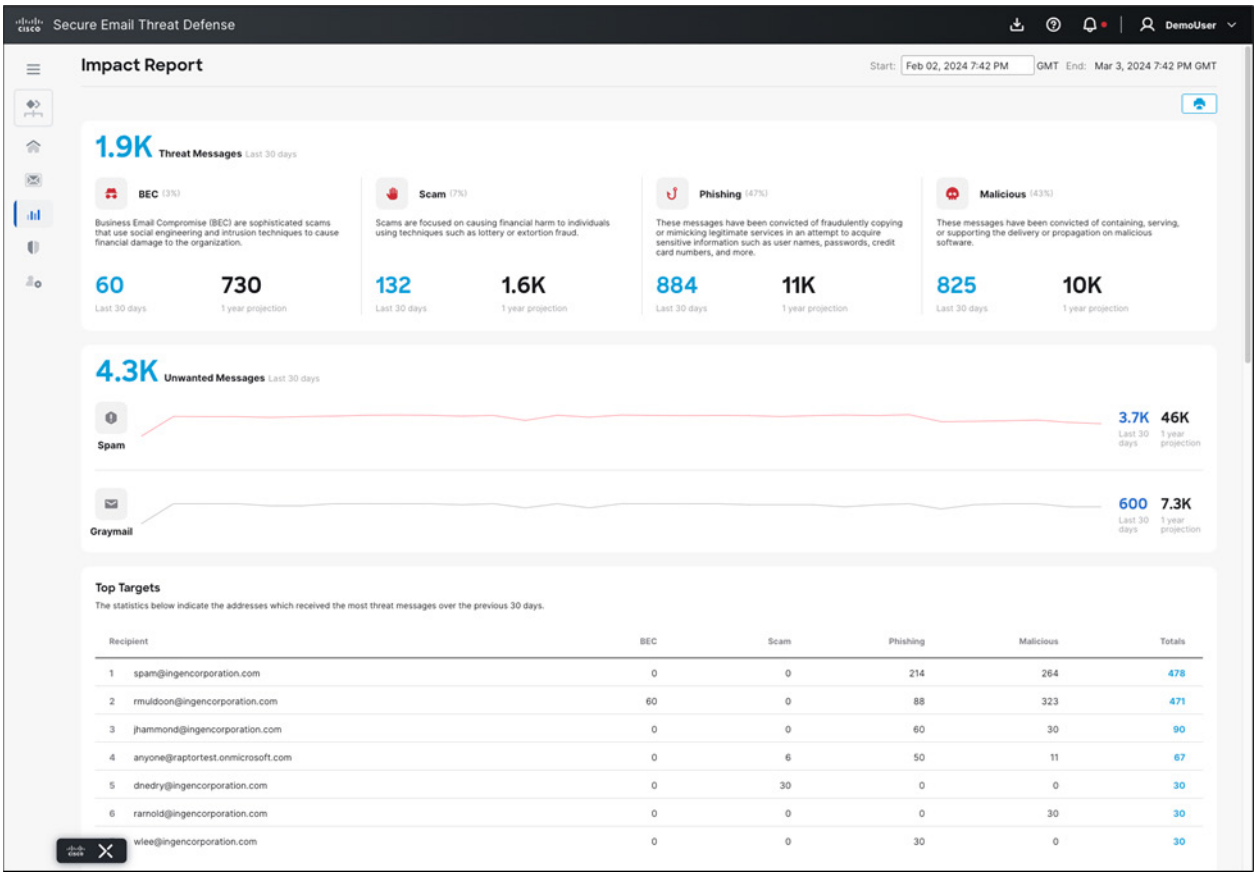

図 2.
影響レポート

ダッシュボード

- スキャンされたメッセージの総数（内部、着信、発信、混合）
- 脅威トラフィック
- スパムトラフィック
- グレイメールトラフィック
- 判定を含むメッセージの詳細、送信者と受信者の詳細、添付ファイル情報、含まれる URL
- 有害判定の詳細（そのメッセージが有害と判定された理由、使用されたディテクタ、見つかった証拠）
- 会話ビュー：電子メールの送信先
- タイムラインビュー：着信、有害判定などから

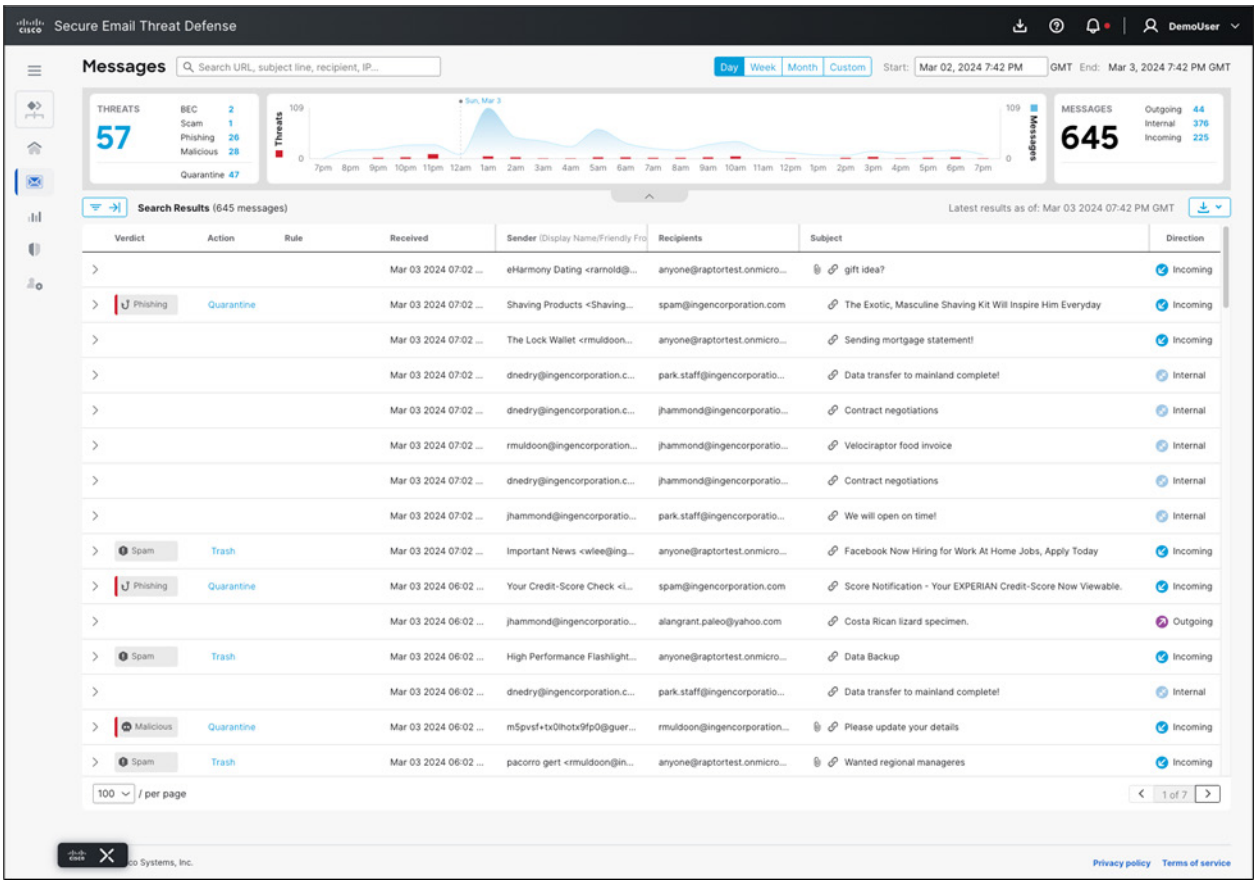

図 3.
メッセージ検索

検索機能

- 送信者
- 受信者
- 件名
- Envelope From アドレス
- 返信先
- SMTP サーバー IP
- SMTP クライアント IP
- X Originating IP
- 組織 BCC
- URL
- 添付ファイル名（Attachment name）
- MS メッセージ ID

メッセージルール

メッセージルールを使用すると、一部のタイプのメッセージを修復またはスキャンしないように指定できます。Email Threat Defense では、次のルールタイプを作成できます。

- 許可リストルール
- 判定のオーバーライドルール
- バイパス分析ルール

メッセージのダウンロード

検索結果のダウンロードで説明したように、[メッセージ（Message）] ページでこのオプションを使用します。特定のフィルタリングされたデータまたは長期間のデータをダウンロードすることができます。現在の検索結果とフィルタ結果にあるメッセージのデータの CSV ファイルを作成します。

ネットワーク管理者および管理者ユーザーは、展開されたメッセージから EML ダウンロード（メッセージのコピー）を要求できます。

REST API

Cisco Secure Email Threat Defense API を使用すると、パートナーとお客様は安全でスケーラブルな方法でプログラムからデータにアクセスして使用することができます。Cisco Secure Email Threat Defense API を使用して独自のレポートとダッシュボードを作成し、クライアントをより適切に管理できます。メッセージ検索 API により、Cisco Secure Email Threat Defense UI で使用可能なメッセージ情報を取得し、API 要求のさまざまなパラメータに基づいてメッセージをフィルタリングできます。

Email Threat Defense ソリューションでは、次の API を使用できます。

- 認証 API
- メッセージ検索 API
- 再分類と修復 API
- ステータス API
- レポート API

詳細については、API ドキュメント https://developer.cisco.com/docs/message-search-api/ を参照してください。

発注とサポートのシンプル化

Email Threat Defense のご注文は簡単です。単一のサブスクリプション SKU を使用して、シート数（1 以上）とサブスクリプション期間（1、3、5 年）を選択するだけです。High-Value Support サービスは最初から含まれています。

CCW の ETD-SEC-SUB トップレベル部品番号を使用して、Cisco Secure Email Threat Defense を注文してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-3274733-01 03/24