Cisco Cloud Mailbox Defense

Microsoft Office 365 の補足的なクラウド電子メール保護

目次

クラウドへのメールボックスの移行

電子メールインフラストラクチャのオンプレミスからクラウドへの移行が進み、2021 年までに公共および民間の組織の 70% がクラウド電子メールサービスを使用するようになることが予測されています（**Gartner 社、Market Guide for Email Security、2019**）。Microsoft 365 は、広く普及しているオフィススイートです。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推奨しています。Cisco Cloud Mailbox は、Microsoft 365 向けの統合電子メールセキュリティであり、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
Cisco Cloud Mailbox は、ネイティブの Microsoft 365 セキュリティを強化し、着信、発信、および内部ユーザ間のメッセージを完全に可視化します。 Cisco Cloud Mailbox 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

クラウドベースの電子メールのセキュリティ上の課題

セキュリティ管理者は、メールボックスをクラウドに移行する際にセキュリティリスクが増加することに注意する必要があります。

ネイティブのクラウドメールセキュリティではリスクが高い可能性がある

組織の電子メールデータがすべてクラウドでホストされるため、エンタープライズレベルの革新的なセキュリティと多様な脅威インテリジェンスによってセキュリティ防御を強化するのは当然です。

変化の激しい未知の脅威

変化の激しい未知の脅威は見逃され、クラウドメールボックスに残り続ける可能性があります。電子メールから発生した脅威が組織内に拡散されないようにするには、高速の自動検出/修復ツールが必要です。

プラットフォーム全体をターゲットにした攻撃

クラウドメールを広く導入することで、組織は新たな脅威媒体を開放することになります。クラウドメールボックスをターゲットとして乗っ取り、そこから組織全体を攻撃する傾向がますます強まっています。クラウド メール プラットフォームは、最も偽装されやすいドメインの 1 つです。ログイン情報がフィッシングされるとオフィススイート全体にまで攻撃対象が拡大し、インサイダー攻撃やスピアフィッシング攻撃が開始される可能性もあります。

進化した脅威による高度な攻撃

ランサムウェア、ビジネスメール詐欺（BEC）、スピアフィッシングなどの標的型フィッシング攻撃を始めとした高度な脅威は、クラウド メール プラットフォームのネイティブセキュリティ防御を突破する可能性があります。

境界セキュリティでは電子メールトラフィックを完全には可視化できない

クラウド メール プラットフォームは、オフィススイート内で発生する脅威の影響を受けやすくなっています。ログイン情報がフィッシングされると、アカウントが乗っ取られて内部の通信へのアクセスが可能になり、内部でのフィッシング攻撃やビジネスメール詐欺の足がかりが築かれます。

境界セキュリティでは内部の脅威は認識されないため、各クラウドメールボックスで送受信されるすべてのメールをスキャンすることが重要です。メールボックスを継続的に分析することが、内部の脅威から保護するための鍵です。

Cloud Mailbox：ソリューションのコンポーネントと差別化要因

Cisco Cloud Mailbox は、シスコ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。

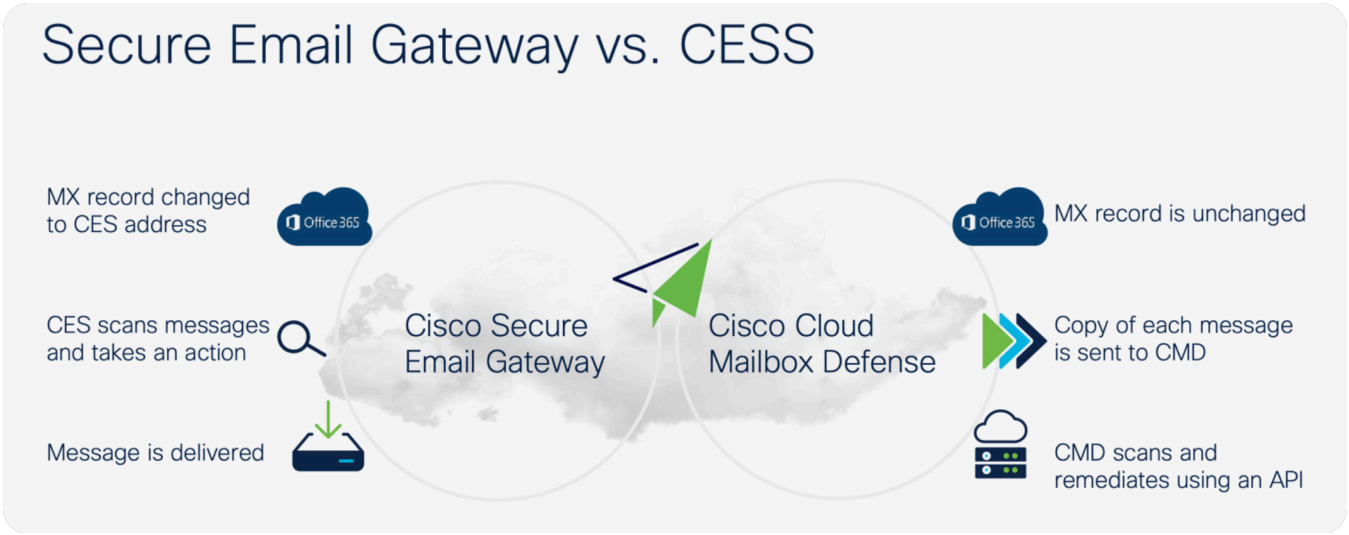

図 1.
Cisco Talos：可視性、インテリジェンス、対応

グローバル規模での非常に高い可視性とテレメトリにより、Talos はより多くのスパム、悪意のある添付ファイル/URL、フィッシングを阻止できます。

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（以前の Cisco AMP）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

Cisco Cloud Mailbox 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。

統合ユーザインターフェイス

Cisco Cloud Mailbox 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。包括的な会話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。

クラウドネイティブ

Cisco Cloud Mailbox のスキャンエンジンは Microsoft Azure 内で実行されるため、電子メールメッセージが Azure のリージョン外に出ることはありません。スキャンエンジンは、Cloud Mailbox プラットフォームでポリシーの適用、検索、修復、レポート作成を実施するにあたり、電子メールのメタデータと判定結果のみを生成して送信します。

Cisco Cloud Mailbox が選ばれる理由

Cisco Cloud Mailbox は、シスコの実証済み電子メールセキュリティの技術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することで、Microsoft 365 の電子メールセキュリティでは不十分な点を強化します。

Microsoft 365 のネイティブセキュリティ機能の強化

Cisco Cloud Mailbox は、Cisco Talos、AMP、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

Cisco Cloud Mailbox 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。

すぐに設定して導入可能

Cisco Cloud Mailbox はシンプルです。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 ソリューションの活用

Cisco Cloud Mailbox 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 駆動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。Cisco Cloud Mailbox は、メールボックス内のすべてのメッセージを（インバウンド、アウトバウンド、内部を問わず）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。

Cisco SecureX の脅威対応ケースブックによる脅威分析の実行

Cisco Cloud Mailbox は、Cisco SecureX の脅威対応ケースブックとあらかじめ統合されており、複数製品での調査や脅威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。

データの保護とプライバシーの向上

Cisco Cloud Mailbox のセキュリティエンジンは、Microsoft Azure クラウド内で実行されます。Cisco Cloud Mailbox プラットフォームでレポートを作成したり、ポリシーベースのアクションを実施したりするために送信されるのは、電子メールのメタデータと判定結果のみです。そのため電子メールメッセージが Microsoft 365 Azure のリージョン外に出ることは決してないため、データプライバシーが向上します。

発注とサポートのシンプル化

Cisco Cloud Mailbox の発注は簡単です。単一のサブスクリプション SKU を使用して、シート数（25 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。

この資料の記載内容は 2021 年 3 月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-743547-03JA 21.03