Barracuda
Your business, secured.

Google Workspaceの標準メールセキュリティに保護レイヤーを追加すべき5つの理由

Google Workspaceは、メール保護のための強固な基盤を備えており、大量のスパムやフィッシング、既知のマルウェアを効果的にブロックします。 しかし、現代の攻撃は極めて巧妙になっています。より目立たず、標的を絞り込み、人間の信頼を悪用するよう設計されており、技術的な脆弱性ではなく心理的な隙を突いてきます。 また、セキュリティの適用範囲は設定やライセンス階層によって異なるため、運用者側では監視が行き届きにくい「盲点」が生まれやすく、攻撃者に迅速に悪用される可能性があります。

本稿では、Google Workspaceの標準メールセキュリティに存在する5つの重要なギャップと、Barracuda Email Protectionが多層的で目的特化型の防御機能でそれらのギャップを解消し、今日の高度な攻撃から組織を保護する方法を紹介します。

37% フィッシングや認証情報の窃取から始まったアカウント乗っ取りの割合

84% メールで配信される情報窃取型マルウェアの前年比増加率

出典：BM X-Force脅威インテリジェンス・インデックス2025

01 | なりすましの検出機能は認証が中心であり、攻撃の意図を判断できない

Googleの制約

Google Workspaceは、送信者の偽装やなりすましを検出する際、送信者認証の検証に大きく依存しています。このアプローチは明らかな攻撃の検出には有効ですが、メッセージのコンテキストや挙動パターン、さらには悪意ある意図までを十分に考慮して判断することはできません。高度ななりすまし攻撃の多くは、正しく認証されたドメインや侵害された取引先アカウント、巧妙に似せたアイデンティティを利用しており、技術的な検証を容易にすり抜けます。

Barracudaにできること

Bararcudaは、認証だけでなく意図まで分析します。 Barracuda Email Protectionは、送信者のアイデンティティ、過去のコミュニケーション履歴、文体、関係性の文脈、挙動の異常などを総合的に評価し、そのメールが受信者にとって、その時点で自然であるかどうかを判断します。この高度な分析により、見た目には問題のないメールであっても、CEO詐欺や取引先のなりすましなどのソーシャルエンジニアリング攻撃を検出することが可能になります。

02 | 配信後の脅威対応は時間がかかる手動の作業となる

Googleの制約

Google Workspaceには、フィッシングメールが初期の防御をすり抜けた場合に調査および対応するための機能がありますが、その対応の多くは手作業になります。管理者は、多くの場合、ログ検索やスクリプト、あるいはユーザーからの報告されたメッセージを頼りに脅威を特定し、メールボックスから削除しなければなりません。これらのプロセスは、特に大規模な環境では、時間、経験、連携を必要とします。 対応している間にも、悪意のあるメールは受信トレイに残り続けるため、ユーザーのリンククリック、機密情報の返信、社内転送などのリスクが高まります。

Barracudaにできること

Barracuda は、メールがユーザーの受信トレイに配信された後も脅威を検出できる、配信後の保護機能を提供します。 AIによる分析に加え、コミュニティで蓄積された脅威インテリジェンスやユーザーから報告されたメール情報を活用し、影響を受けたメールボックスから悪意のあるメッセージを自動的に削除します。この自動修復により、脅威の滞留時間を短縮し、ユーザーへのリスクを最小化するとともに、手作業による対応に依存することなく、セキュリティチームの迅速な対応を支援します。

03 | アカウント侵害後の可視性が制限される

Googleの制約

Google Workspaceは不正なログインを効果的に防止しますが、攻撃者が有効な認証情報を用いてログインした場合、ログイン後の活動は正当なものに見えてしまうことが多くあります。受信トレイルールの作成、メール転送、データアクセスなどのログイン後の動作は、悪意ある兆候として継続的に評価されるわけではありません。認証後の挙動を監視しなければ、侵害されたアカウントは信頼されているユーザーになりすまして悪用され、ラテラルムーブメントが行われ、データが秘密裡に外部に持ち出される恐れがあります。

Barracudaにできること

Barracudaは、ログイン後の受信トレイの挙動を監視し、アカウント乗っ取りの兆候を特定します。Barracudaは異常な送信パターン、不審な転送ルール、リスクの高い設定変更などを分析し、侵害されたアカウントを早期に可視化します。この早期検知により、攻撃者が信頼を悪用したり、権限を拡大したり、被害を拡大させる前に、セキュリティチームが迅速に対応できるようになります。

04 | マルウェアを利用しないフィッシングが悪用するのは、アイデンティティではなく人の心理

Googleの制約

最近のフィッシング攻撃の多くは、特定の信頼された人物へのなりすましに依存していません。その代わりに、短くもっともらしく、一見すると日常的で無害に見えるメッセージを用いて、人間の心理的な隙を巧みに突いてきます。こうしたメールには、悪意のあるリンクや添付ファイルが含まれていない場合も多く、一見正規に見えながら実際には無関係なドメインや、一般的な無料Webメールアカウントから送信されることもあります。

Google Workspaceの標準フィルタでは、これらのメールは認証を通過し、侵害を示す明確な技術的な兆候がないため、検知されない場合があります。こうしたメールは、日常的で自然なやり取りに溶け込むよう設計されており、簡単な質問や、さりげない再連絡、単純な依頼を装うケースが多く見られます。その結果、送信者を明確に信頼していない場合でも、ユーザーが応答してしまうリスクが高まります。

Barracudaにできること

Barracudaは、送信者のなりすましではなく、メッセージの挙動に着目し、AIを活用した分析を行います。メッセージのトーン、送信タイミング、会話の流れ、ドメインの類似性、メッセージの意図などを総合的に分析し、ソーシャルエンジニアリングの兆候となる不審なパターンを特定します。Barracudaはこのアプローチにより、アイデンティティの悪用にとどまらず、ユーザーをだまして特定の行動を取らせることを目的としたメールも阻止します。

05 | Google Workspaceのエディションによってセキュリティ機能が異なる

Googleの制約

Google Workspaceの高度なセキュリティ機能は、ライセンス階層や設定によって大きく異なります。高度な調査機能、自動修復、詳細な脅威分析といった機能は、利用しているエディションによっては提供されていなかったり、手動での有効化が必要になったりする場合があります。こうしたばらつきにより、ユーザーや部門ごとに保護レベルに差が生じ、一部の受信ボックスが他よりも脆弱な状態になる可能性があります。攻撃者はこのようなセキュリティレベルのばらつきを悪用し、防御が最も手薄なユーザーを侵入口として狙います。

Barracudaにできること

Barracudaは、Google Workspaceのエディションに依存せず、あらゆるユーザーに一貫して適用できるメール保護レイヤーを追加します。高度な検知、挙動分析、自動対応、可視化といった機能を、Google Workspaceの標準制御の外部で拡張することで、ライセンスによるギャップを埋め、攻撃者に狙われやすい弱点を最小化します。

多層防御のメール保護機能でギャップを解消

Google Workspaceはメールセキュリティの基盤を提供しますが、それだけでは現代のあらゆる攻撃、特に人を標的とした攻撃を十分に防ぐことはできません。Barracudaは、Google Workspaceの標準的な保護機能を補完・強化し、なりすまし、ソーシャルエンジニアリング型フィッシング、アカウント乗っ取り、そして侵害後に受信トレイ内で展開される攻撃など、特に見逃されやすい脅威に焦点を当てて対策を提供します。

Google WorkspaceとBarracudaを組み合わせることで、真の多層防御を実現できます。 Google Workspaceが既知の脅威や一般的な攻撃を大規模にブロックする一方で、Barracudaは高度なインテリジェンス、挙動のコンテキスト、自動対応機能を提供し、信頼を悪用する巧妙な攻撃の検知と阻止を可能にします。その結果、ユーザー体験や既存環境に影響を与えることなく、Google Workspaceをそのまま活用しながら、より広範なカバレッジ、迅速な対応、そして強固なセキュリティを実現します。

Barracuda
Your business, secured.

3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772（米国およびカナダ）• barracuda.com バラクーダネットワークスおよびバラクーダネットワークスのロゴは、米国におけるBarracuda Networks, Inc.の登録商標です。その他のすべての名称は、それぞれの所有者に帰属します。