Cloudflare Area 1メールセキュリティ

フィッシング、ビジネスメール詐欺（BEC）、メールサプライチェーン攻撃から
ユーザーを守るには先手必勝です。

フィッシングは、企業が直面する頻度が最も高く、被害が高額に及ぶサイバー脅威のひとつです。

Cloudflare Area 1はクラウドネイティブのメールセキュリティプラットフォームで、攻撃がユーザーの受信箱に到達する前に、攻撃を検出して阻止します。つまり、既存の防御をすり抜けるスピアフィッシング、BEC、その他の高度な脅威に対し、より効果的な保護を実現できます。

Area 1は、MicrosoftやGoogleの環境とワークフローに深いレベルで統合し、クラウドメールプロバイダーが提供するビルトインのセキュリティを強化します。

Area 1は、Zero Trustサービスの一部です。

標的を絞ったフィッシングの脅威を阻止

Area 1は大規模なキャンペーンから、準備に数か月を要するような高度に狙いを定めたメールサプライチェーンを巻き込む攻撃まで、フィッシング攻撃を幅広く防御します。

フィッシング

Verizon 2021 DBIRはフィッシングについて最も一般的な不正行為と言及します。Area 1は、大規模なWebクローリング、小規模なパターン分析、強化された検出機能などを活用し、フィッシング攻撃がユーザーの受信箱に到達する数日前に阻止します。

BECとソーシャルエンジニアリングを使った脅威

攻撃者が他人になりすます、あるいは、信頼されている人や組織に予め侵入しておくことで、金銭やデータを盗み出そうとするのが、BEC（ビジネスメール詐欺）です。Area 1ではメール通信の内容と背景を分析し、本来なら見つけ出すのが不可能な脅威を阻止します。

メールサプライチェーン攻撃

攻撃者はベンダーのメールを悪用してメールのパターンを観察します。その後、既存のスレッドを傍受し、請求詐欺を仕掛けるのです。Area 1はメールのスレッド、メッセージのセンチメント、ソーシャルグラフなどを分析し、これらの高度な攻撃を阻止します。

脅迫やランサムウェアのメール

ガートナー社の調査によれば、ランサムウェア攻撃の40%がメールから始まっています。Area 1はランサムウェアの送信するメールがエンドユーザーに到達する前に先回りして防御し、悪意のあるメッセージが検出された場合にはそれが広がる前に除去します。

従来のメールゲートウェイより一枚上手

先手を打つ

攻撃サイクルの初期段階でフィッシングを止めるため、早期に攻撃者のインフラストラクチャと攻撃メカニズムを特定します。

内容と背景を重視

BEC、ベンダーメール詐欺、その他のペイロードを持たない脅威を捕らえる高度な検知テクニック（言語分析、コンピュータビジョン、ソーシャルグラフなど）を活用します。

包括的に守る

メール攻撃のあらゆるタイプ（URL、ペイロード、BEC）、ベクトル（メール、Web、ネットワーク）、チャンネル（外部、内部、信頼できるパートナー）をカバーします。

途切れない防御

メールがユーザーの受信箱に到着する前、転送中、到着した後と、複数の脅威防御層で多層防御態勢をとります。

メリット

ネイティブのメールセキュリティを強化

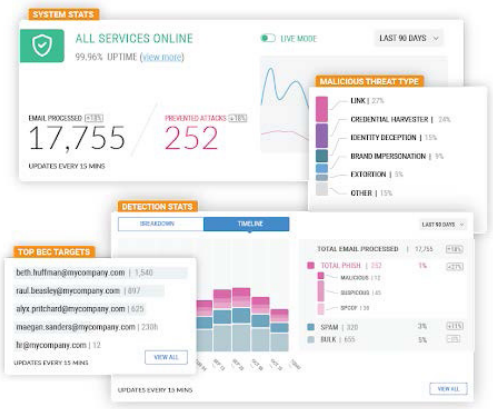
ビルトインのセキュリティレイヤーをかわして侵入する高度なフィッシング攻撃とBEC攻撃を阻止します。クラウド型メール環境と深く統合する特性を生かし、メールの生産性に影響を与えることはほぼありません。

クラウド優先アーキテクチャを採用

最新のスケーラブルなアーキテクチャを優先し、従来のメールゲートウェイにありがちな手間のかかる作業や柔軟性のなさを回避します。メールに元々備わっていたセキュリティ機能と同様の働きをするセキュリティレイヤーへの支出を減らします。

SOCチームの時間を削減

ハードウェア、エージェント、アプライアンスを必要とせず、数分でデプロイ。ポリシーの作成や調整に費やした時間を開放。SIEMやSOARの統合で、SOCの調査を迅速化します。



フィッシングリスク評価を依頼

Area 1を現在お使いの本番環境メールトラフィックで実際に作動させ、既存のセキュリティコントロールを通過するメール攻撃がどのようなものか、リアルタイムでご覧いただけます。

評価には、ハードウェアやソフトウェアのインストールは一切必要なく、メールのフローに影響を及ぼすこともありません。

本番環境でのデモは[こちら]よりお申し込みください。