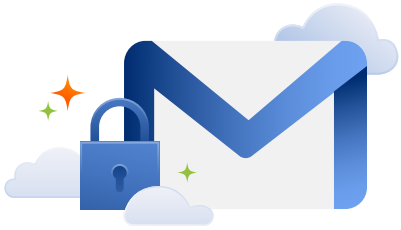
Advanced Email Security

Acronis Cyber Protect Cloud の拡張オプション

スパムメールがエンドユーザーに到達する前にメール由来の脅威を検出することによりお客様のセキュリティリスクを回避

スパム、フィッシング、ビジネスメール詐欺（BEC）、マルウェア、APT（高度な標的型永続的脅威）、ゼロデイ攻撃など、エンドユーザーのMicrosoft 365、Google Workspace、またはOpen-Xchangeメールボックスに悪意のあるメールが到達する前にブロックします。次世代型クラウドベースのPerception Pointによるメールセキュリティソリューションを活用します。



フィッシングとスプーフィングを防止

強力な脅威インテリジェンス、シグネチャベースの検出、URL評価チェック、独自の画像認識アルゴリズム、機械学習、DMARCのレコードチェックによりお客様のメールに由来のリスクを最小限に抑えます。

高度な回避手法を捕捉

添付、またはメールに埋め込まれた添付ファイルやURLを再帰的に展開し、動的および静的検出エンジンにより個別に分析することにより、隠れた悪意あるコンテンツを検出します。

APTとゼロデイ攻撃を防止

マルウェアが活動する前にエクスプロイトをブロックし、数秒以内に明確な判定を提供するPerception Pointの独自のCPUレベルのテクノロジーで従来の防御を回避しようとする高度な脅威を防止します。

クラウドメールセキュリティによりサイバープロテクションをさらに強化

新たな提案と収益源の確保	お客様のメール由来の攻撃による脅威から保護	限られたリソースで、効率的にサービスを統合・合理化
• メールセキュリティによりサービスメニューを拡大/強化 • 実装に必要な時間に悩むことなく、サービスのアップグレードを計画。Advanced Email Securityはスイッチを入れるだけで利用可能	• お客様メールによるコミュニケーションのリスクを最小限に抑え、エンドユーザーのMicrosoft 365、Google Workspace、Open-Xchangeのメールボックスに悪意を持ったメールが到達する前に脅威を阻止 • スパム、フィッシング、ビジネスメール詐欺（BEC）、スプーフィング、マルウェア、悪意あるURL、ゼロデイ攻撃、APT（高度な標的型永続的脅威）を防止	• メールセキュリティ、バックアップ、ディザスタリカバリ、次世代のマルウェア対策、サイバープロテクション管理をすべて統合する単一ソリューションによる管理で、サービス提供に必要なリソースを軽減 • ソリューションの統合によりコスト削減

- 事業計画の向上と新たな利益と収益源の確保
- サブスクリプションによる提供

- 全てのトラフィックをカバーし、あらゆる規模のコンテンツをくまなく分析
- 所要時間7～20分のサンドボックスソリューションと比較して、誤検知をほぼゼロに抑えながら、平均3秒以内に明確な判定を提供
- 第三者評価機関のSE Labsで認められた業界をリードするテクノロジー上にサービスを構築

- メールセキュリティのデプロイメントにかかる煩雑な作業を排除し、デプロイメント時間を数分に短縮
- アラートとインシデントにより、メールセキュリティの可視性を向上
- サイバーアナリストやメールセキュリティエキスパートが、貴社のメールセキュリティサービスデリバリとセキュリティチームの生産性を向上

お客様の高リスクのコミュニケーションチャネルを今までにない優れた検出テクノロジーで保護

スパムフィルタ

複数の市場をリードするテクノロジーの統合データを活用しながら、スパム防止や評価ベースのフィルタで悪意あるコミュニケーションをブロックします。

回避防止 *独自機能

30秒以内に複数のエンジンにより動的にチェックされる小規模なユニット（ファイルやURL）にコンテンツを再帰的に展開することにより、隠れた悪意あるコンテンツを検出します。20分以上かかる従来のサンドボックスソリューションに比べ、はるかに高速です。

脅威インテリジェンス

6つの市場をリードするソースの統合脅威インテリジェンスと、悪意のあるURLやファイルをスキャンするPerception Point独自のエンジンにより新興の脅威を先回りします。

静的シグネチャベースの分析

高度に複雑なシグネチャを特定できる、Perception Pointによる独自のツールで強化された、最高レベルのシグネチャベースのアンチウイルスエンジンにより、既知の脅威を特定します。

アンチフィッシングエンジン *独自機能

URLの適正を検証するためにPerception Pointの高度な画像認識テクノロジーと組み合わせて、4つの業界をリードするURL評価エンジンに基づいて悪意あるURLを検出します。

スプーフィング防止

IP評価、SPF、DKIM、DMARCレコードチェックを使用し、機械学習アルゴリズムにより、スプーフィング、類似のドメイン、表示名偽装といったペイロードレス攻撃を今までにない高い精度で防止します。

次世代の動的検出 *独自機能

Perception Point独自のCPUレベルの分析によりAPTやゼロデイ攻撃といった高度な攻撃を阻止します。ランタイム時の通常の実行フローからの逸脱を特定することにより、エクスプロイト段階で攻撃を検出し、ブロックすることができます。

X-rayインサイト

各メールのフォレンジックデータと共に組織全体の脅威状況の包括的ビュー、脅威のプロアクティブなインサイト、サービスデリバリチームがフォレンジックを必要とするファイルまたはURLの分析を活用します。

インシデント対応サービス

自社のサービスデリバリチームの延長として機能するサイバーアナリストに直接アクセスできます。継続的なレポートと、誤検知の処理、必要に応じて修正および解放などのサポートにより、すべてのカスタマートラフィックを監視し、悪意あるコンテンツを分析します。

レポート機能

インシデント対応チームからの週次、月次、特定目的でのレポートに加え、アクセスと管理が容易なデータセットを提供して、お客様に価値を提示します。

エンドユーザー向けの特定目的でのメール分析

エンドユーザーは、危険な操作をしてしまう前に、疑わしいメールについてPerception Pointのメールセキュリティエキスパートに直接相談できます。

エンドユーザーのコンテキストベースのヘルプ

ポリシーとルールに基づいてカスタマイズ可能なバナーでメールのフラグを作成し、エンドユーザーに追加のコンテキストベースの情報を提供することにより、セキュリティ意識を向上させます。

ACRONIS CYBER PROTECT CLOUDの拡張オプション

Advanced Email Securityは、サイバーセキュリティ、データ保護、エンドポイント保護の管理を、サービスプロバイダー向けに設計された1つの統合ソリューションに集約した、Acronis Cyber Protect Cloudの高度なプロテクションパックの1つです。各アドバンスドパックにより、サービスプロバイダーは、あらゆるワークロードに最適なレベルのサイバープロテクションを確保しながら、お客様のニーズに応える強化機能でサービスを拡張できます。

今すぐ試用

Acronis

詳細情報はこちらをご覧ください：
www.acronis.com