proofpoint.

ソリューション概要

Commercial Proofpoint Threat Protection

メールボックスの数が2,500以下の企業を
今日の「人」を中心とした脅威から保護する

主なメリット

- さまざまなメール脅威を迅速に検知してブロック
- 継続的なAIと脅威インテリジェンスを用いて新しい脅威をさらに高精度に阻止
- 人的リスクや脅威リスクに関する知見を提供
- 従業員をサポートし、行動変容を推進
- メールアカウントやクラウドアカウントの侵害を特定し修復
- メール認証でブランドを保護

メールはサイバーセキュリティ脅威にとって最上位の攻撃経路です。また最近では、従業員を標的にする、マルウェア、フィッシング、ソーシャル エンジニアリング スキームが数多くあります。2024 Verizon Data Breach Investigations Report（2024年Verizonデータ侵害調査レポート）によれば、すべてのデータ侵害の68%には人的要素が関わっています[1]。Proofpoint Threat Protection は、従業員を昨今の高度な脅威から保護する「人」を中心としたセキュリティ アプローチを提供します。

サイバー犯罪は成長ビジネス

Statistaは、世界中のサイバー犯罪による年間損失額は、2029年までに15兆6300億ドルにのぼると予想しています[2]。攻撃者は、重要な個人情報や企業情報を盗み、IDを盗み、攻撃を仕掛けて、メールによる金融詐欺を目論んでいます。また、メールは現代のビジネスの要であるため、従業員にとって最大の攻撃経路となっています。

フィッシング、BEC（ビジネスメール詐欺）、サプライヤー詐欺、ランサムウェアといったマルウェアはすべてメールから始まります。そのため、これらの最新脅威から従業員を保護することは、洗練された組織であっても気の遠くなるような作業です。ぜひ、プルーフポイントにお任せください。

「人」を中心としたセキュリティでさらに多くの脅威を阻止

プルーフポイントは、99.99%の検知精度で最新のさまざまなサイバー脅威を検知します。Proofpoint Nexusは、メールによってもたらされる脅威を継続的に分析します。脅威インテリジェンス、機械学習、振る舞いAI分析や大規模言語モデル（LLM）を用いた意味解析を組み合わせ、攻撃を効果的に特定し、軽減します。

1. Verizon、Data Breach Investigations Report（データ侵害調査レポート）、2024年
2. Statista、Estimated Cost of Cybercrime Worldwide（世界中のサイバー犯罪の推計損失額）、2018-2029、2024年7月

85%

従業員を脅威から保護するためにプルーフポイントを利用しているFortune 100企業の割合

出典: プルーフポイント、2024年

プルーフポイントは、調査が必要な脅威の数を抑え、組織が修復作業を効率化し、インシデント レスポンスにかかる時間を短縮できるようサポートします。配信後の悪意のあるメールの削除を自動化することで、セキュリティチームやITチームのワークロードを低減します。プルーフポイントのユーザーフレンドリーな内蔵レポーティングツールを使って、従業員がメッセージを報告することもできます。プルーフポイントは、自動化され、パーソナライズされたセキュリティ トレーニングにより、ユーザー行動におけるポジティブな変化を推進します。管理者は、プルーフポイントのグローバルなThreat Research Teamによって厳選された実際のフィッシングのシミュレーションを用いて、従業員の知識を確認し、プログラムの成果を測定することができます。

従業員への攻撃は、なりすましやATO(アカウント乗っ取り)が主流になっています。メールアカウントやクラウドアカウントの侵害に対し、プルーフポイントは、AIベースの検知や自動修復手順を用いて、ATO脅威対応を迅速に行います。プルーフポイントは、組織が行うメール認証の手順を簡素化することで、企業のブランドをなりすましの悪用から守ります。専門的なDMARCガイダンスとホスティングサービスを組み合わせ、組織に偽装してメールを送信する類似ドメインを動的に特定します。これらのツールは、従業員を包括的に保護しながらシームレスなユーザー エクスペリエンスを提供します。しかし、メールだけが、防御が必要なアクセスポイントではありません。

プルーフポイントは、メールの枠を超えて、チャットツール、コラボレーション アプリ、ソーシャルメディアのアプリケーションで配布された悪意のあるURLからも保護することでフィッシング保護を拡大します。リアルタイムのURLレピュテーションの調査と分析を提供します。また、クリック時においても悪意のあるURLをブロックします。このようにして、プルーフポイントは、ユーザーを高度なフィッシング攻撃からいつでもどこでも保護します。

Proofpoint Threat Protection は、従業員と組織の保護を向上させる包括的なソリューションです。脅威リスクを低減し、セキュリティチームやITチームによる運用上の成果を向上させます。SEG (セキュア メール ゲートウェイ)またはAPIベースのMicrosoft 365デプロイ オプションといった、組織に最も合ったデプロイ方法を柔軟に選べます。組織が必要とするものが「設定すれば後の作業は不要」のクイックソリューション、またはより包括的な保護であれ、プルーフポイントはニーズに応えます。組織の成長に合わせて、Proofpoint Threat Protectionも拡大し、押し寄せるサイバー脅威に対抗することができます。

Commercial Proofpoint Threat Protectionのパッケージ、ユースケース、説明

メールボックスの数が2,500以下の企業向け

パッケージ	ユースケース	概要
Proofpoint CEP (Core Email Protection)	以下の機能を必要とする組織に最適 • フィッシング、BEC、マルウェア、ランサムウェア、悪意のあるQRコード、URLなどのメール脅威を阻止 • スパム、グレーメール、その他の不要なメッセージを削減 • 自動abuseメールボックス管理により効率向上 • 従業員がどのように攻撃を受けているかについての理解を深める	Proofpoint CEPは、脅威の99.99%を阻止する、AIを活用した完全なソリューションです。高精度の検知と自動化された修復ワークフローにより、リスクを低減し、セキュリティチームの負担を減らします。Proofpoint CEPは、Microsoft 365向けのセキュア メール ゲートウェイ（SEG）またはAPIベースのソリューションが選べるなど、あらゆる組織のセキュリティ要件に対応できる柔軟性を備えています。
Proofpoint Advanced Threat Protection	以下の機能を必要とする組織に最適 • 脅威対策を向上 • ユーザーによる危険な行動を改めさせ、セキュリティ意識向上の文化を育成 • アカウント乗っ取り対策と修復によりアイデンティティを保護 • メッセージングやコラボレーションのアプリケーションにおいて従業員をフィッシング脅威から保護	Proofpoint CEPを基盤として、ユーザーによる危険な行動を改めさせ、さまざまなコミュニケーション チャネルやデジタル アイデンティティを保護します。内蔵のフィッシング シミュレーション、文化や知識のアセスメント、数千のセキュリティ トレーニング モジュール（40言語以上に対応）を用いて、脅威を認識し、対抗できるようユーザーを指導します。フィッシング保護を拡大し、メッセージング、コラボレーション、ソーシャルメディアのアプリケーション経由で配布された悪意のあるURLから保護します。また、侵害されたアカウントを検知し、攻撃者のアクセスをブロックすることでこれを修復します。 *Proofpoint CEPを含む
Commercial Proofpoint Prime Threat Protection	以下の機能を必要とする組織に最適 • 最も包括的な保護を活用 • メールによるブランド悪用やなりすまし脅威から保護 • メール認証（DMARC）を用いた確実なメッセージ配信 • 専門的ガイダンスにより複雑なDMARCプロトコルの実行を簡素化	SPF、DKIM、DMARCなどのメール認証プロトコルを実装することで、企業のブランドをなりすまし脅威やドメインなりすましから保護します。プルーフポイントのコンサルタントがプロセスの各ステップをガイドするため、簡単にDMARCを導入することができます。また、組織のドメインを使って送信されるメール（委託先サードパーティが送ったものも含む）や類似ドメインを可視化できます。 多重防御で従業員を保護します。この包括的なパッケージには、従業員を標的にした脅威から保護するために必要なあらゆる制御が含まれています。他社のソリューションでCommercial Proofpoint Prime Threat Protectionのような機能を実現しようとすれば、さまざまなアドオンの購入が必要となります（メールボックス オートメーション、セキュリティ意識向上プログラム、生産性ツールなど）。 *Proofpoint CEP、Proofpoint Advanced Threat Protectionを含む

Commercial Proofpoint Threat Protectionのパッケージの比較

	機能	PROOFPOINT CEP	PROOFPOINT ADVANCED THREAT PROTECTION	COMMERCIAL PROOFPOINT PRIME THREAT PROTECTION
構成	オンプレミス、ハイブリッドまたはクラウド ホスティング	✓	✓	✓
	柔軟なデプロイオプション	SEGまたはAPI	SEGまたはAPI	SEGまたはAPI
BEC	Proofpoint Nexus LMによる振る舞いAI機能	✓	✓	✓
	Proofpoint Nexus RGによるリレーションシップ グラフ	✓	✓	✓
フィッシング、ランサムウェア、マルウェア	Proofpoint Nexus TIが提供する脅威インテリジェンスとレピュテーション	✓	✓	✓
	Proofpoint Nexus LMによる振る舞いAI機能	✓	✓	✓
	URLの書き換えとサンドボックス	✓	✓	✓
	添付ファイル サンドボックス	✓	✓	✓
	書き換えられたメールクリックのWeb分離	VAP (Very Attacked People) が対象	VAP (Very Attacked People) が対象	VAP (Very Attacked People) が対象
	メール警告バナー	✓	✓	✓
メールの報告と修復	自動mSOAR	✓	✓	✓
	自動abuseメールボックス	✓	✓	✓
	ユーザーによるメール報告	✓	✓	✓
脅威とユーザーのダッシュボード	VAP含む脅威インサイト	✓	✓	✓
	人的リスクダッシュボード	✓	✓	✓
メールハイジーンと構成	スパム対策、ウイルス対策、グレーメール	✓	✓	✓
	エグゼクティブ/VIP設定	✓	✓	✓
	カスタマイズポリシー	✓	✓	✓
メッセージング&コラボレーションアプリにフィッシング保護を提供	リアルタイムで悪意のあるURLをブロック		✓	✓
	マルチチャネルのフィッシング脅威の可視化		✓	✓
セキュリティ意識向上	リスクベースの教育を自動化		✓	✓
	脅威に基づいたコンテンツ		✓	✓
	実際に行われているフィッシングを用いたシミュレーション		✓	✓

Commercial Proofpoint Threat Protectionのパッケージの比較（続き）

	機能	PROOFPOINT CEP	PROOFPOINT ADVANCED THREAT PROTECTION	COMMERCIAL PROOFPOINT PRIME THREAT PROTECTION
ATO	侵害されたアカウントを高精度で検知		✓	✓
	アクセスの前後における調査タイムライン		✓	✓
	攻撃者を自動的に排除し、アカウントの変更を復元		✓	✓
メール認証	メール認証によりドメインなりすましを防止し、確実に配信			✓
	DMARCの実装支援と追加のホスティングサービス			✓
	組織と信頼できるパートナーの類似ドメインの検知			✓
	リスクスコアによりベンダーまたはサプライヤーを自動的に特定			✓