Proofpoint プロダクト

Proofpoint は、 組織にとっての最大の資産であり、 同時にセキュリティリスクでもある「人」 を可視化し、 保護するために、 人を標的にする脅威を防御し、 ユーザーが作成しアクセスする情報を保護し、 そしてユーザー自身を保護するための、 最も効果的なツールを提供しています。

Proofpoint のサイバーセキュリティ及びコンプライアンスソリューションは、 メール、 ソーシャルメディア、 Web、 ネットワークおよび Microsoft Office 365 や Google G Suite 等のクラウドプラットフォームに対応しています。 また、 業界を代表するセキュリティプロバイダーとの戦略的技術統合も行っています。 これによりユーザー、 データ、 ブランドをより安全に保護することができます。

メール保護

メール経由の脅威への対策を行い、 メール利用の継続性を確保し、 メール送受信ポリシーを適用します。

Email Protection

Proofpoint Email Protection は、 マルウェアおよび非マルウェア （詐欺メールやビジネスメール詐欺（BEC）など）による脅威を含む、望ましくない悪意のあるメールからユーザーを守ります。 あらゆる規模の組織について、 詳細なビジビリティを提供し、 業務の継続をサポートします。 ポリシーを設定し、 受信メールと送信メールをあらゆる面でコントロールすることで、 IT/ セキュリティチームは、 エンドユーザーをメール脅威から保護し、 障害時にもメールの継続利用を可能にします。

Email Fraud Defense (EFD)

Proofpoint Email Fraud Defense (EFD) は、 詐欺メール攻撃がユーザーのメールボックスに届かないよう阻止し、 従業員、 顧客、 ビジネスパートナーをさまざまなメール詐欺から守ります。 このソリューションを用いると、 どのような攻撃手法が使われていても、 また誰を標的にしたものであっても、 単一のポータルから正規メールの承認、 詐欺メールのブロック、 脅威の確認ができるようになります。 EFD はメール認証、 機械学習、 ポリシーを活用し、 さらに DMARC 認証を適用することで、 攻撃者が高度な詐欺攻撃に用いるあらゆる詐欺手法を阻止します。

Threat Response Auto-Pull (TRAP)

Proofpoint Threat Response Auto-Pull (TRAP) は、 オーケストレーションと自動化機能を用いてユーザーのメールボックスに届いてしまった悪意のあるメールを取り除きます。 これは Threat Response のエントリーレベルのバージョンで、 TRAP からのアラートに基づいて悪意あるメールを識別して除去します。 そしてその後はビジネスロジックを用いて、 その他の受信者グループでもこれらのメールを見つけて除去します。 TRAP はまた、 隔離の試み・成功及び失敗の状況、 そしてどのユーザーが最も標的にされたかについてのレポートを生成しますので、 セキュリティチームの作業負荷を減らすことができます。

Internal Mail Defense

Proofpoint Internal Mail Defense は組織の内部メールを保護し、 また侵害されたアカウントを検出するためのマルチレイヤーの強固な防御策で、 すべての内部メールをスキャンして、 スパムや悪意のある添付ファイル、 そして不正な URL を検出します。 内部から送信されたメールに危険を示すフラグが立った場合は、 自動的にそのメールを除去し、 隔離します。 また、 悪意のある URL を送信したアカウントが可視化されるため、 セキュリティチームは迅速に侵害アカウントを見つけて対応できます。

スモールビジネス向け Essentials

Email Protection をスモールビジネスのニーズに適合させたものが 、 Proofpoint Essentials です。 これにはスパムフィルタリング、 フィッシング検出、 マルチレイヤーアンチウイルス、 URL ダイナミックサンドボックス、 強固なフィルタリングルールエンジン、 メール継続性、 ポリシーを用いた暗号化、 メールアーカイブ、 ソーシャルメディアアカウント保護などが含まれます。 さらに、シンプルで直感的なユーザーインターフェースを使って管理できるため、 小規模なセキュリティチームでも簡単に運用できます。

高度な脅威対策

脅威の検出、 調査、 対応を、 より迅速、 正確に、 そして自信をもって行えます。

Targeted Attack Protection (TAP)

Proofpoint Targeted Attack Protection (TAP) は、 メールやクラウドアプリ （Microsoft Office 365 や Google G Suite など） 経由で悪意のある添付ファイルや URL を送って組織内の「人」 を攻撃する高度な脅威を検出、緩和、ブロックします。 TAP は組織内の Very Attacked People (VAP) を明らかにし、どのデバイス上でも、埋め込まれた URL を書き換えてユーザーを守り、 悪意のあるリンクのクリックを追跡します。

Email Isolation

Proofpoint Email Isolation を用いれば、 ユーザーが会社のデバイスを使って個人の Web メールへアクセスすることによるセキュリティ上の問題を回避できます。 これは TAP と統合して VAP を守る追加レイヤーとして機能し、 未知もしくは危険な Web サイトからユーザーを守ります。 このクラウドサービスは、 マルウェアや悪意のあるコンテンツがユーザーやデバイスに到達しないよう防ぐため、 企業データやネットワークから Web コンテンツを分離してセキュリティを向上させると同時に、 リスク管理や運用コスト管理を容易にします。

Browser Isolation

Proofpoint Browser Isolation は Proofpoint Email Isolation の機能を拡張し、 すべてのエンドユーザー （VAP を含む） の Web ブラウジングを保護します。 Browser Isolation の導入、 管理、 サポートは非常に簡単で、 安全で匿名性の高い Webブラウジングサービスを提供します。これによりユーザーが Web メールなどのサイトにアクセスする際のプライバシーを守ることができ、 リスクを低減できます。

Threat Response

Proofpoint Threat Response はセキュリティの高度化を目指して努力しているセキュリティオペレーションチームにとって、最適なソリューションです。 ネットワークの脅威を可視化し、豊富なアラートを提供し、 自動的にフォレンジックの収集と比較を行います。 これにより、 インシデント対応時に手作業や推測による対応が不要になり、 問題を迅速かつ効率的に解決できます。 また、 従来のインシデント対応プロセス関連ツールとは異なり、 自動的にマルウェア感染を確認し、 過去の感染のエビデンスをチェックし、 内部及び外部コンテキストやインテリジェンスを追加してセキュリティアラートを強化します。

Emerging Threats Intelligence

Proofpoint Emerging Threats Intelligence (ET) は脅威研究者にとっては必須のツールで、 世界有数のマルウェアエクスチェンジからの、 100% 検証済みの脅威インテリジェンスを提供しています。 これを用いれば、 脅威の出所と作者について詳細な履歴を確認でき、 また他のセキュリティツールともシームレスに統合できます。 ドメインや IP アドレスを報告するだけの他のインテリジェンスソースとは異なり、Proofpoint のインテリジェンスには 10 年分の履歴、 不正の証拠、 40 以上の脅威カテゴリー、 および関連する IP/ ドメイン / サンプルが含まれています。

Emerging Threats Pro Ruleset

Proofpoint Emerging Threats (ET) Pro Ruleset は最新の正確なルールセットで、 既存のネットワーク セキュリティ アプライアンス (次世代ファイアウォールやネットワーク IDS/IPS など) に適用して脅威を検出し、 阻止します。 ET Pro Ruleset は毎日 SNORT 及び Suricata フォーマットでアップデートされ、 40 種類以上のカテゴリー （ネットワーク動作、マルウェアコマンドおよびコントロール、 DoS 攻撃、 ボットネット、 エクスプロイト、 脆弱性、 SCADA ネットワークプロトコル、 エクスプロイトキットアクティビティなど） を網羅しています。 この、 日々のアップデートと自動化されたサンドボックス環境により、 すべての脅威を完全に評価することができます。

Premium Threat Information Service (PTIS)

Proofpoint Premium Threat Information Service (PTIS) は、常に変化する脅威ランドスケープの詳細な状況を提供して、 セキュリティに関連する意志決定を支援します。 PTIS には、 業界最先端の脅威研究者への直接アクセス、 月次のカスタム脅威レポート、 急増する脅威に関する詳細な警告 (アナリストログブックへのアクセス) という 3 つのコンポーネントが含まれます。 これにより、 ただでさえ不足しているセキュリティアナリストの手作業による対応を減らすことができ、 アナリストは最も重要度の高い問題に集中することができます。

セキュリティ意識向上トレーニング

エンドユーザーがフィッシングやその他のサイバー攻撃への最後の砦となれるよう、 脅威を識別し報告する方法を教育します。

Anti-Phishing Suite

Proofpoint Anti-Phishing Suite は、 ユーザーがどれだけ攻撃に騙されやすいかを識別して、 フィッシング攻撃の被害とマルウェア感染を最大 90% 低減します。 ユーザーが ThreatSim フィッシング攻撃シミュレーションに騙された場合は、 安全確保のためのアドバイスである 「Teachable Moment」 が表示されます。 攻撃シミュレーションに騙されたユーザーを自動的にフィッシング対策トレーニングモジュール （8 種類） の 1 つに登録することができ、 あるいは別途個別に登録することもできます。 また、 このパッケージには PhishAlarm® メール報告ボタンと PhishAlarm Analyzer メール分析ツールが付属しています。 これらのツールは Closed Loop Email Analysis and Response (CLEAR) ソリューションの一部で、 フィッシング攻撃の報告を効率化し、 対応を自動化します。

エンタープライズセキュリティ意識向上トレーニング

Proofpoint Security Awareness Training Enterprise パッケージには、 Anti-Phishing Suite のすべてと、 ThreatSim USB、 CyberStrength® ナレッジアセスメント、 トレーニングモジュールすべて、 そしてセキュリティ意識向上のための資料すべて（動画を含む）が含まれます。 このパッケージは、最も効果的で包括的なセキュリティ意識向上トレーニングプログラムを必要としているお客様に最適なパッケージです。 リスクの識別、 行動の変化、 危険の回避に役立つツールで、より影響力の強い、 人を中心としたリスク低減戦略を実行できるようになります。

クラウドアプリのセキュリティ

クラウドアプリに存在する脅威、 データ漏洩、 コンプライアンスのリスクから人とデータを守ります。

Cloud Account Defense (CAD)

Proofpoint Cloud Account Defense (CAD) は、 Office 365 や G Suite 上でのアカウント侵害や悪意のあるファイルからの保護を、 自動で提供します。 アカウント侵害は通常、 フィッシング、 クレデンシャルを盗むマルウェア、 または総当たり攻撃 （クレデンシャルスタッフィング等） がきっかけとなって発生します。 侵害されたアカウントは、 社内から、 または社外から次の攻撃 （BEC やフィッシングなど） を仕掛けるために利用されます。 CAD は、 機密データや信用されているアカウントが侵害された場合の迅速な検出、 調査、 防御をサポートするために、 人を狙う脅威の検出、 脅威アクティビティとの相関関係、 豊富な脅威インテリジェンスを使った詳細なフォレンジック、 自動レスポンスのための柔軟なポリシーを提供します。

Cloud App Security Broker

Proofpoint Cloud App Security Broker (PCASB) は、 クラウドアカウントの侵害、 機密情報の行き過ぎた共有、 クラウドのコンプライアンスリスクから組織を保護します。 PCASB はアプリのアクセスおよびデータの取り扱いについて、 人を中心とした詳細な視点を提供しています。 このソリューションは侵害されたアカウントの検知、 アクセス管理、 情報漏洩対策 (DLP)、 サードパーティアプリのコントロールおよび分析を組み合わせて、 Microsoft Office 365 や Google G Suite、 Box などの保護を強化するものです。 この強力な分析機能を用いると、 組織にとって最も重要なリスク要因をもとにして、 サードパーティアプリやユーザーに適切なレベルのアクセス権を割り当てられるようになります。

情報保護

メール、 クラウドアプリケーション、 オンプレミスでのファイル共有、 及び SharePoint 内のデータを特定し、 追跡、保護します。

Email Data Loss Prevention (DLP)

Proofpoint Email DLP は、 メール送信における従業員の不注意による機密情報やプライベートな情報の漏洩を防ぎます。 送信するコンテンツの重要性や保護の必要性をユーザーに判断させるのではなく （こういった対策は作業負荷と時間を増やす原因となります）、 ソリューションを用いてメール通信ポリシーを集中的に自動管理することで、 ユーザーはいつも通りに仕事をできます。 きめ細かく調整された 80 以上のポリシーに基づいて機密情報を含むメールを自動的に発見、 分類、ブロックするため、 データ漏洩のリスクを減らすことができます。

Email Encryption

Proofpoint Email Encryption はポリシーベースの暗号化を使用して、 メールや添付ファイルの安全なコミュニケーションを自動的かつシームレスに行えるようにします。 従来のメール暗号化サービスは、 ユーザーにとっては操作が面倒でした。 しかし Email Encryption を使えば、 送受信メールの暗号化はバックグラウンドで処理されるので、 ユーザーが手作業で暗号化する必要はなくなります。 これにより、 機密メールを確実に保護しながら、 関連会社、 ビジネスパートナー、 そしてエンドユーザーはコンピューターやモバイルデバイスからメールにシームレスにアクセスできるようになります。

Data Discover

Proofpoint Data Discover は、ファイル共有、データストア、SharePoint サイト上の機密データを特定し、 監視、 保護します。 コンテンツ分析を自動化して、組織のオンプレミスネットワーク上の情報を追跡し、 不正な漏洩のリスクに晒されている機密情報 （PII や PHI を含む） を自動的に識別します。 そして、 これらを検疫、 複製または削除して、 リアルタイムにリスクを緩和します。

Meta

Proofpoint Meta は次世代の安全なエンタープライズアプリケーションへのアクセスを実現します。Meta はデータセンターやクラウド上の企業リソースについて、 従業員やコントラクター、 そしてパートナーに、 ゼロトラストのアイデンティティベースのアクセスを可能にする、 人を中心としたソリューションです。

ObserveIT Insider Threat Management

Proofpoint は ObserveIT を 2019 年 11 月に買収しました。 Insider Threat Management は内部脅威のリスクを識別し緩和する、 軽量なエンドポイントソリューションです。 このソリューションは、 従業員、 特権ユーザー、 及び第三者などのユーザーの悪意や不注意からデータを守るための検出機能と保護機能を提供します。Insider Threat Managementを使えば、ユーザーの行動監視、 リアルタイムの教育、 そしてリアルタイムの攻撃阻止でセキュリティインシデントのリスクの大幅削減が可能です。 通常は数日かかる調査を数分で完了し、 さらにレスポンスタイムの改善やコンプライアンスの簡潔化に必要なセキュリティインシデントのプレイバックを提供します。

デジタルリスク保護

ソーシャルメディア、 Web ドメインおよびダーク Web の脅威からブランドと顧客を保護します。

Digital Risk Protection

Proofpoint Digital Risk Protection は、 Web ドメイン、 ソーシャルメディア、およびディープ Web におけるデジタルセキュリティリスクからブランドと顧客を守ります。 これには、 会社のドメインを悪用したブランド詐欺を阻止し、 フィッシングやアカウント乗っ取り、 スパム被害にあわないよう、 ソーシャルメディアアカウントを保護し監視する機能が含まれています。 またディープ Web 及びダーク Web で、 高度な脅威、 クレデンシャルの漏洩、 物理的攻撃のロケーション、 そして類似の重要イベントを監視することもできます。 機械学習を用いることで、 計画中の脅威、 差し迫った脅威、 そして現在発生している脅威に先んじることが可能になります。

アーカイブとコンプライアンス

すべてのコミュニケーションプラットフォーム上でのデータの保持、 ディスカバリ、 そして監視を通してコンプライアンスを確保します。

Enterprise Archive

Proofpoint Enterprise Archive はクラウドインテリジェンスと機械学習を活用して、 重要なビジネス情報をわかりやすい形で検出し、 保持します。 このソリューションは法的なディスカバリ、 規制へのコンプライアンス、 コストと複雑さの低減という、 3 つの基本的な課題に対応しています。 IT チームがインハウスでアーカイブを管理する必要はありません。 スケーラブルなクラウドアーキテクチャ、 確実な検索パフォーマンス、 非常に高い顧客満足度、 業界最高の洗練された暗号化で、 法的及びコンプライアンス上のコントロールを可能にします。

Enterprise Collaboration Archive

Proofpoint Enterprise Collaboration Archive はポリシーに沿って Salesforce Chatter、 Jive、 Skype for Business、 LinkedIn、 Twitter やその他のプラットフォームのソーシャルコンテンツを収集します。 そしてこれらはコンプライアンスのためのアーカイブや監視プラットフォーム上にあるその他の重要なデータ資産と同じように管理され、 レビューされます。 これにより法令順守が容易になります。 また、 コンプライアンス上の重要なタスクを自動化および効率化する高度な機能も提供しています。

Intelligent Supervision

Proofpoint Intelligent Supervision は、 FINRA、 SEC、 IIROC などの複雑で厳しい規制の順守を効率化する、 金融機関向けソリューションです。 Enterprise Archive と統合されており、 また機械学習を活用して、 規制に対応するためのキャプチャ、 レビュー、 レポートを簡単に、 効率的、 効果的に実行します。 これを用いると、メール、インスタントメッセージ、 コラボレーションツール、 通話、 SMS、 そしてソーシャルメディアを完全に可視化できるようになります。

eDiscovery Analytics

Proofpoint eDiscovery Analytics は、 法務部門向けの直感的な e-Discovery ワークフローです。 機械学習、 リアルタイムの検索結果、 そして早い段階での訴訟分析でさらなる知見を得られます。 これによりプロアクティブな訴訟準備が可能になり、 リスクをコントロールして低減させることができるようになります。

Social Media Compliance

Proofpoint はソーシャルメディアに関するコンプライアンスとマーケティング活動の間のギャップを埋めて、 ユーザーが最新のソーシャルメディア規制を順守できるよう、 サポートします。 Digital Risk Protection は主要なアーカイブソリューションと統合して、将来の検索や e-Discovery に使用するソーシャルメディアコンテンツを収集し分類します。 これらにより、 監査にかかる時間と費用を節約できます。

詳細は **proofpoint.com** でご確認ください。

---

proofpoint について

Proofpoint, Inc. （NASDAQ:PFPT） は、サイバーセキュリティの主導的企業であり、組織の最大の資産であり同時に最大のリスクでもある 「人」 を守ります。 Proofpoint は、クラウドベースの統合ソリューションによって、 世界中の企業が標的型脅威を阻止し、 データを守り、 ユーザーがサイバー攻撃に対してより大きな耐性を持てるように支援します。 また、 Fortune 1000 の過半数を超える企業を含むあらゆる規模のトップ企業が、 メールやクラウド、 ソーシャルメディア、 Web 関連の最も重要なセキュリティリスクおよびコンプライアンスリスクを低減させるために、 Proofpoint を利用しています。 詳細は **www.proofpoint.com** でご確認ください。

proofpoint.