proofpoint. x paloalto NETWORKS

# ベスト・オブ・ブリードの脅威情報連携

## 製品

- Proofpoint TAP (Targeted Attack Protection)
- Palo Alto Networks WildFire

## 主なメリット

- 悪意のある添付ファイルを使った高度なメール脅威を検知し阻止
- マルチレイヤーの脅威対策を実現
- ベスト・オブ・ブリードの脅威インテリジェンスを共有

90%以上の脅威はメール経由で届けられます。[1] 企業を標的とする高度な脅威への対処は非常に難しく、リスクを緩和し低減するための包括的ソリューションが必要となっています。プルーフポイントと Palo Alto Networks はパートナーシップを締結しており、メールからネットワーク、そしてクラウドまでを網羅したセキュリティを提供します。

## プルーフポイントと Palo Alto Networks

プルーフポイントを用いれば攻撃者の一歩先を行くことができ、革新的なアプローチで、高度な脅威がユーザーに届く前に検知、分析、そしてブロックできます。プルーフポイントでは、静的解析と動的解析を組み合わせて、常に新しい攻撃パターンを検知し、対応しています。

潜在的な脅威の分析は、以下を検証する複数のアプローチで行われます。

- 振る舞い
- コード
- プロトコル

これにより、一連の攻撃の初期の段階で脅威を検出し、また可能な限り、被害が及ぶ前に対処します。攻撃の中には、マルウェアのインストールや、ユーザーをだまして機密情報を共有させようとすることをもくろむ、悪意のある添付ファイルや URL を含むものが少なくありません。そのため、さまざまな攻撃の分析には、サンドボックスが用いられます。さらにアナリスト支援による分析を活用して、検知精度を向上させ、インテリジェンスを最大限活用します。

Palo Alto Networks のセキュリティ プラットフォームは不審なファイルや URL を WildFire™ に自動ルーティングし、詳細分析を行います。WildFire™ は顧客や脅威インテリジェンスパートナーのグローバルネットワークから取得したサンプルを毎週数百万件検査し、以下について、未知の脅威を探し出します。

- マルウェア
- エクスプロイト
- 悪意のあるドメイン
- アウトバウンドの C&C アクティビティ

1 Verizon「Data Breach Investigations Report (データ漏えい調査レポート)」 2020年7月

WildFire™ は、転送されてきたサンプルを既知のファイルデータベースと照合して、未知のものをサンドボックス内で試験的に実行させて詳細調査を行い、複数の OS/アプリケーションのバージョンに対して静的解析と動的解析をおこないます。そして「悪意がある」と判断された場合は、マルウェア、URL、DNS のシグネチャを自動的に生成し、WildFire™ を利用する全世界の Palo Alto Networks プラットフォームに数分以内に連携します。ユーザーは追加でアクションをする必要がなく、環境内での脅威の拡大をすぐに阻止できます。

Palo Alto Networks とプルーフポイントは戦略的パートナーシップを結んでおり、プラットフォーム間でのインテリジェンス共有が可能です。最新の標的型攻撃にも効果があり、これにより、セキュリティ強化とより幅広い可視性が追加コストなく実現できます。

# 統合の効果

## マルチレイヤーのメール防護

未知の添付ファイルのメールが届くと、Proofpoint TAP (Targeted Attack Protection) はサンドボックス分析をおこない、そのメールが悪意あるものかどうかを判断します。また TAP は同時に Palo Alto Network の WildFire に添付ファイルを送って並行して検査します。いずれかのソリューションが添付ファイルを危険と判断した場合はブロックされ、エンドユーザーにメールが届かないようにします。WildFire™ が添付ファイルを危険だと判断した場合、ファイルハッシュを取得し、Palo Alto Network の Next-Generation Firewall、Advanced Endpoint Protection、Threat Intelligence Cloud に追加します。このように2つのベスト・オブ・ブリードのソリューションを用いて、悪意のある添付ファイルがユーザーに届かないようにすることで、最新の脅威にも対抗できるようになります。このマルチベンダーによる分析で、両社のお客様はより確実な脅威対策を実現できます。

## ソーシャルメディア向けのマルチレイヤー防護

ソーシャルメディアは製品の販売推進や顧客とのコミュニケーションに最適なツールです。しかしソーシャルメディアを多用すれば、それだけ攻撃的なコンテンツやセキュリティ攻撃にさらされる確率も高まります。Proofpoint Digital Risk Protection は、以下のような脅威に対抗するリアルタイムの自動防護で、ソーシャルメディア アカウントを守ります。

- ハッキング
- フィッシング
- 悪質なコンテンツ

ソーシャルメディアに URL を含むメッセージが投稿された場合、サンドボックス分析を行い、また Palo Alto WildFire に送って分析と判定を行います。そして悪意のあるポストがあれば、ポリシーに基づいて Digital Risk Protection がそれらを削除します。

プルーフポイントと Palo Alto Networks は最新の脅威インテリジェンスを活用し、クローズドループの自動プロセスを提供します。これによって標的型攻撃によるデータ漏えいリスクを低減できます。

# 詳細

詳細は **proofpoint.com/jp** でご確認ください。