組み合わせれば、強力になる:
2つの技術を統合し、先進的脅威に対抗

主な特徴

- **両社の技術を統合し、ネットワーク、エンドポイント、メール、ソーシャルメディアプラットフォームを横断した検知と保護を提供**
- **異なる攻撃手法に対し、統合した脅威インテリジェンスを提供**
- **統合ソリューションを簡単に、追加コスト無しで導入**

パロアルトネットワークスとプルーフポイントが脅威検知機能で提携し、現代の洗練された攻撃に対抗

洗練されたサイバーセキュリティ上の脅威は新しい形態をとり、複数の攻撃手法を使った新しい方法で企業を狙っています。Proofpoint と Palo Alto Networks は、両社の技術を統合してお客様の従業員とデータを狙う脅威から保護し、脅威に関するインテリジェンスを提供するためにパートナーシップを結びました。

両社が持つクラス最高のセキュリティソリューションと、ネットワーク・エンドポイント・クラウド・メール・ソーシャルメディアプラットフォームを横断した脅威インテリジェンスの組合せでなければ実現できない、高度な保護技術を提供します。

ソリューションを構成するコンポーネント

Palo Alto Networks WildFire

新たな脅威が検出されると、Palo Alto Networks の次世代セキュリティプラットフォームが自動的に疑わしいファイルや URL を WildFire に送り、より詳細な解析を行います。WildFire は世界中のお客様、及び脅威インテリジェンスパートナーから送られてくるサンプルを毎週数百万個も検査しており、未知のマルウェア・エクスプロイト・悪意のあるドメイン・アウトバウンドのコマンド＆コントロール行動などについての新しい形態を探し出します。

WildFire は送られてきたサンプルを過去のデータベースと突き合わせ、マッチしないファイルをさらなる調査にかけます。この調査は複数の OS とアプリケーションのバージョンを使った静的な解析及び動的な解析により行われます。WildFire は悪意のある行動を探し、行動解析と判定のレポートを出力します。「悪意がある」と判定した場合、自動的にマルウェア・URL・DNS 用のシグネチャを生成し、即座に WildFire のサブスクリプションを契約している世界中の Palo Alto Networks プラットフォームに配信します。これにより、脅威が広がる前に封じ込めることができます。ユーザーは何もする必要はありません。WildFire の解析レポートからの IoC (Indicators of compromise) 情報は NGFW 及びテクノロジーパートナーと共有され、感染したホストを特定し、第 2 のダウンロードを防止します。

この閉ループの自動化されたプロセスにより、組織はネットワーク、エンドポイント及びクラウドが最新の脅威インテリジェンスによって確実に守られることになります。

Proofpoint Targeted Attack Protection

Proofpoint Targeted Attack Protection (TAP) により、組織は悪意のある添付ファイルやメールに含まれる URL を使って標的を狙う既知または未知の先進的脅威を検知し、防御し、それらに対応することができるようになります。現代の主要な脅威はポリモーフィックマルウェア、兵器化ドキュメント及びアカウント情報を狙ったフィッシング攻撃であり、電子メールは組織内の人々に到達するために有効なため、攻撃者が最も好む攻撃経路です。TAP は洗練された解析技術を採用し、Proofpoint の安全なメールゲートウェイとシームレスに統合されており、コスト効率が良く簡単に使え、クラウドベースのクラス最高のメールセキュリティを提供します。

Proofpoint SocialPatrol

Proofpoint SocialPatrol は、Facebook、Instagram、Twitter、LinkedIn、Google+、YouTube などの主要なソーシャルネットワークなどの上で企業、顧客及びブランドを守るための先進的な保護を提供します。企業は多くのリソースをソーシャルメディアマーケティングに投入していますが、ハッカーが狙うのもまたお金です。一般的な企業は平均して 178 個のソーシャルメディアアカウントを持っており、セキュリティの管理やコンプライアンス違反を防ぐのは非常に大変です。

SocialPatrol は特許申請済みの技術を使って、ハッカーが企業のソーシャルメディアアカウントをロックしてブランド価値を毀損したり、マルウェアやフィッシング攻撃を阻止してセキュリティインシデントを防止したり、不適切なコンテンツを削除してコンプライアンスの遵守や容認できる利用を促したり、接続したアプリケーションをコントロールして未承認のコンテンツが流れ出るのを防止したりします。

Palo Alto Networks + Proofpoint

今回のパートナーシップにより、両社の脅威に関するナレッジをリアルタイムで統合し、両社のお客様によりよいビジビリティと現代の先進的脅威と効果的に戦うための同期された保護機能を提供することができます。両社のお客様はPalo Alto Networks WildFire と Proofpoint TAP 及び/または Proofpoint SocialPatrol を、API キーベースのアクティベーションを使って数分で統合できます。

Proofpoint TAP と Palo Alto Networks の主要なセキュリティプラットフォームである WildFire を統合したことにより、潜在的なマリシャス添付ファイルが解析の為に両社に送られ、Proofpoint のメールゲートウェイと Palo Alto Networks の次世代セキュリティプラットフォームを連携させた自動保護が可能になり、ネットワーク・クラウド・エンドポイントを保護できます。TAP がメールの添付ファイルを未知のレピュテーションとして検査する場合、ファイルは Proofpoint TAP のサンドボックスと Palo Alto Networks WildFire の両方に送られて解析されます。双方のソリューションが脅威インテリジェンスを生成し、判定を返します。もしどちらかのソリューションがファイルを怪しいと判定した場合、TAP はあらかじめ決められたポリシーに従ってメッセージを阻止するか追跡し、即座に保護と通知を行い、一方で WildFire は自動的に新しい保護データを生成して世界中に配信し、脅威の拡散を防ぎます。WildFire の脅威インテリジェンスレポートは TAP ダッシュボードから直接見ることができ、組織の中の複数のコントロールポイントを横断した攻撃の統合されたビューをセキュリティチームに提供します。

Wildfire と SocialPatrol の統合では、SocialPatrol が監視しているソーシャルメディアアカウントにポストされたリンクを WildFire のサンドボックスで解析できます。悪意のあるリンクには Proofpoint SocialPatrol に設定されたお客様のポリシーが適用され、悪意のあるコンテンツを自動で削除するか、管理者にアクションを起こすよう通知します。この統合により、お客様は WildFire クラウドから提供される脅威インテリジェンスにより、ソーシャルメディアプラットフォーム上の既知もしくは未知の URL 脅威から保護されます。

Palo Alto Networks と Proofpoint の間で共有された脅威インテリジェンスと連係した保護により、次に同じ脅威が現われた際 (攻撃経路に関係なく) にはそれを簡単に検知し、迅速に阻止することができます。