Advanced Threat Prevention

ゼロデイ脅威とエクスプロイトをリアルタイムに阻止

近年のネットワーク防御における主要な課題の 1 つは、高度な回避技術を用い、自動化された攻撃の増加と関係します。高度なツール セットに加えて、サービスとして入手できるハッカー向け製品や、広く公開されている一般的なレッド チーム ツールの亜種を利用することで、秘密裏に進行する攻撃のスピードと成功率が大幅に増加しています。さらに、悪意ある攻撃者が脆弱性、アタックサーフェス、その他の未知の侵入経路を特定するための難易度もコストも下がり続けています。つまり今では非常に手軽にサイバー脅威を実行できるのです。

刷新され強化された侵入防御システム (IPS)

パロアルトネットワークスの Advanced Threat Prevention は、業界初の侵入防御システム (IPS) であり、ゼロデイ C2 攻撃と未知のエクスプロイトを完全にインラインで阻止します。従来の IPS 機能を超えて、既知と未知の脅威を阻止する業界最高水準の防御機能を提供します。Advanced Threat Prevention は、VM–Series や Prisma® Access などのハードウェア / ソフトウェア ファイアウォールで利用できる、高度なクラウド提供型セキュリティ サービス スイートの一部です。

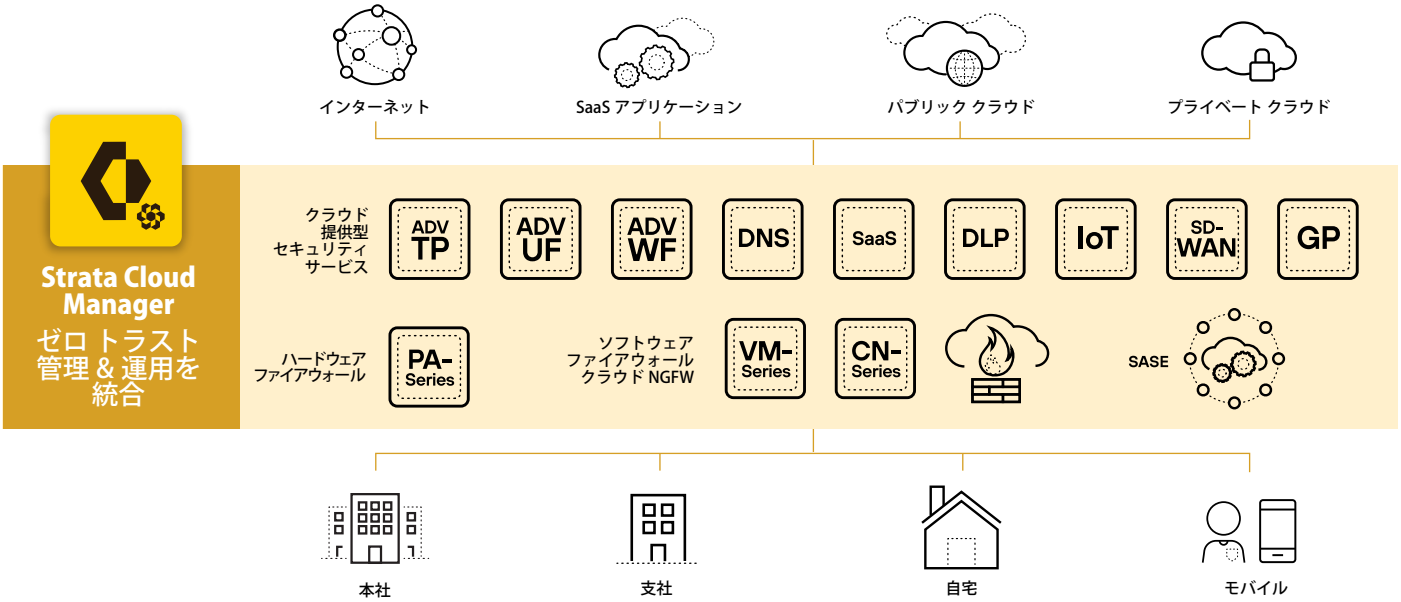

図 1: パロアルトネットワークスのクラウド提供型セキュリティ サービス

主要なメリット

- 敵対的ツールからのゼロデイ攻撃や既知の攻撃に対するインライン防御。
- 既知と未知の脆弱性に対するエクスプロイトに対するインライン防御。
- Web ベースの脅威に対する、ML を活用した、業界最高水準のリアルタイム検出。
- 攻撃を包括的に可視化し、すべてのネットワーク トラフィックを検査して脅威を検出。
- Unit 42® や Advanced WildFire® による業界屈指の脅威インテリジェンスを活用。

製品機能

業界をリードする Advanced Threat Prevention

Advanced Threat Prevention は、ネットワーク レイヤーとアプリケーション レイヤーでエクスプロイトや回避戦術を検出し、阻止します。シグネチャ マッチング、機械学習、インライン ディープ ラーニング モデルを含むさまざまな検出方法が採用され、確認された脅威の特性に応じて防御が実施されます。この機能は、パロアルトネットワークスのすべての次世代ファイアウォール (NGFW) と Prisma Access で利用できます。

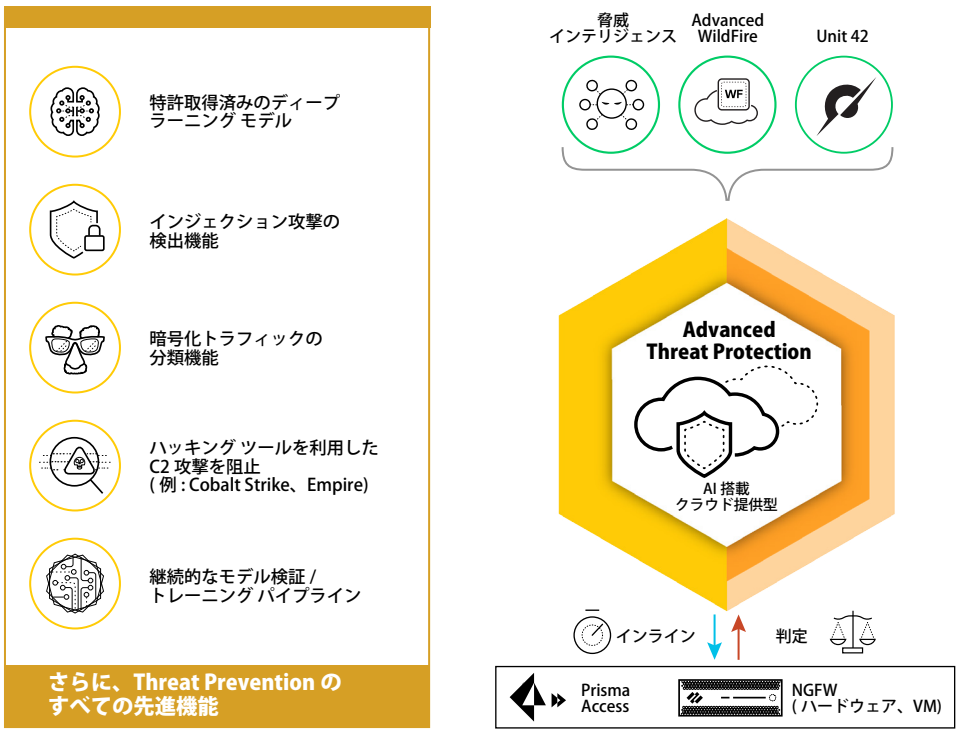

図 2: パロアルトネットワークスの Advanced Threat Prevention

コマンド & コントロール (C2) の検出

Advanced Threat Prevention は、特許取得済みのインライン ディープ ラーニング モデルを使用して、Cobalt Strike や Empire などの主要なレッド チーム ツールから送られる、回避能力を備えた未知の C2 トラフィックを阻止します。これらのモデルは新たに出現する攻撃を防ぐため、クラウド内で絶えず更新されています。Advanced Threat Prevention は、未知の Web ベースの攻撃も阻止します。シグネチャベース検出との組み合わせによって、敵対的攻撃に対する強固な防御を実現します。

エクスプロイト防御

Advanced Threat Prevention は、最新のトレーニング データセットによって定期的にアップデートされるクラウドベースの機械学習モデルを使用することで、未知のコマンド インジェクション /SQL インジェクション エクスプロイトを阻止します。ここには、数千もの既知の脆弱性に対するシグネチャベースの防御や、トップ ベンダーの「重大」および「高」の CVE に対する業界屈指のレスポンス時間なども含まれます。

マルウェア防御

Advanced Threat Prevention は、インラインのシグネチャベースの検出によってネットワーク レイヤーでマルウェア攻撃をブロックします。Advanced WildFire との組み合わせによって、既知と未知の亜種がターゲット ホストに到達する前に阻止します。

主なマルウェア対策機能には以下のようなものがあります。

- よく使用されるファイル タイプに隠蔽されたマルウェアからの保護。
- 圧縮ファイルや Web コンテンツに埋め込まれたマルウェアに対する防御。
- 弊社の Unit 42 脅威リサーチ チームによる高精度なデータセットとインテリジェンス。
- パロアルトネットワークスが収集した数十億のサンプルから生成されたシグネチャ。

96%
の Web ベース Cobalt Strike C2 攻撃を阻止可能。
さらに、回避能力に優れた C2 トラフィックの検知率を **48%** 向上。*
*パロアルトネットワークスのテストに基づく結果。

99%
Empire を悪用した C2 攻撃を阻止。
さらに、ATP は Empire を悪用した未知の C2 攻撃を従来のソリューションより **43%** 多く阻止。*
*パロアルトネットワークスのテストに基づく結果。

90%
のインジェクション攻撃 (SQLi など) を阻止可能。
さらに、ゼロデイ インジェクション攻撃の検知率を **60%** 向上。*
*パロアルトネットワークスのテストに基づく結果。

中核的な侵入防御サービス

上記に加えて、弊社の中核的な侵入防御テクノロジは以下を提供します。

- カスタム シグネチャの Snort および Suricata ルールとの互換性。
- ソフトウェアの脆弱性とコマンド & コントロール攻撃に合わせたシグネチャ。
- ヒューリスティックベースの分析、プロトコル デコーダを用いた分析、プロトコル異常ベースの防御、設定が容易なカスタム脆弱性シグネチャ。
- マルウェアと脆弱性エクスプロイトをシングル パスで検出およびブロックしながら、トラフィックを検査して分類。
- 厳選された IP アドレス ブロック リスト。

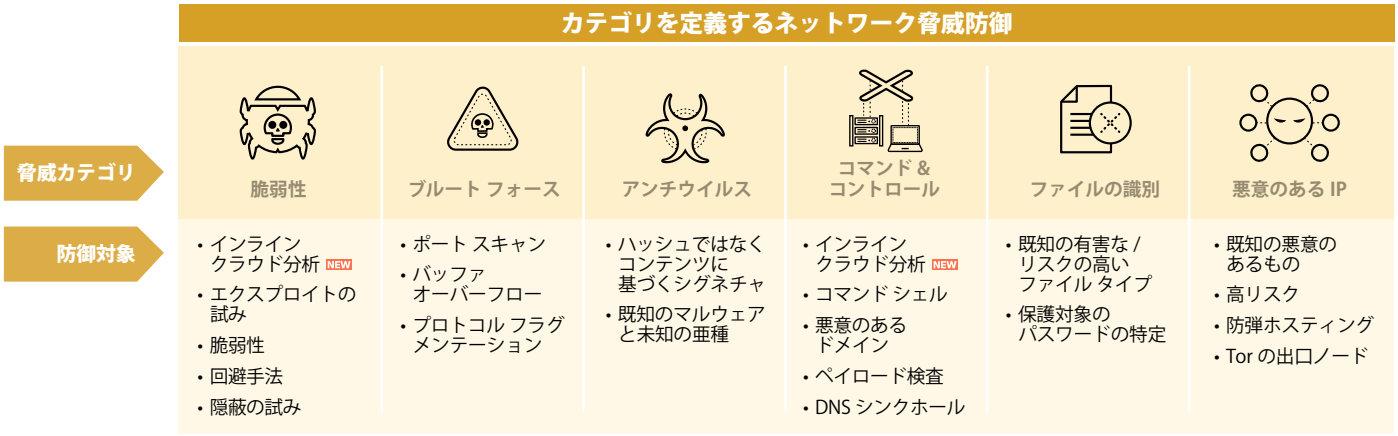

図 3: Advanced Threat Prevention の機能

〒 100-0011
東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
wwwpaloaltonetworks.jp

strata_ds_advanced-threat-prevention_022824