Advanced WildFire

高度な回避能力を備えたマルウェアを インライン AI による保護で阻止

現代の脅威アクターは、ターゲットとする組織に対して、機会とアクセス性という 2 つの点で有利な立場にあります。ハイブリッド ワークの普及、クラウド移行の加速、IoT や SaaS アプリケーションの急成長に伴い、アタック サーフェスは拡大しています。これは、組織に侵入できる方法を探している脅威アクターにとって、絶好の機会が生まれることを意味します。さらに、サービスとしてのランサムウェアや自動化を利用できるようになったことで、高度なマルウェア キャンペーンを展開するための技術的ハードルが下がりました。つまり怠惰で技術レベルが低い脅威アクターでも、さまざまなツールに容易にアクセスして、攻撃の量、重大度、範囲を拡大することが可能になったのです。

クラウドを活用したインライン ML とインライン静的分析でファイル分析を超える

パロアルトネットワークスの Advanced WildFire® は、特許取得済みの機械学習検知エンジンを使用して高度な回避能力を備えた脅威から組織を保護し、ネットワーク、クラウド、顧客アプリケーションのエンドポイントにわたる自動保護を可能にする、業界最大のクラウドベース マルウェア防御エンジンです。

Advanced WildFire で分析されるサンプルには、以下の分析エンジンが複合的に適用されます。

- **軽量なインライン機械学習モデル**：次世代ファイアウォール上の機械学習モデルが既知のマルウェアと未知のマルウェア亜種をリアルタイムに防ぎます。
- **クラウドを活用したインライン ML と静的分析**：ゼロデイ マルウェアを検出して阻止し、ゼロ号被害者攻撃に対する防御を行います。
- **静的分析**：ファイルの特性を調査するとともに、パッキング ツール セットを用いて検出回避を試みる脅威を動的アンパックを用いて分析します。
- **クラウドベースの機械学習モデル**：静的分析や動的分析を行わないと抽出できない何千種類もの固有の特徴を抽出します。
- **動的分析**：回避技術への対策を施した専用の仮想環境でファイルをデトネーションして観察します。これにより、従来検出できなかったマルウェアの検出が可能になります。
- **インテリジェント リアルタイム メモリ分析**：メモリ内の悪意のあるアクティビティのスナップショットを作成し、リアルタイム分析を実行して悪意ある動作を検知することで、これまで検出できなかった高度な回避能力を持つマルウェアを見つけ出します。

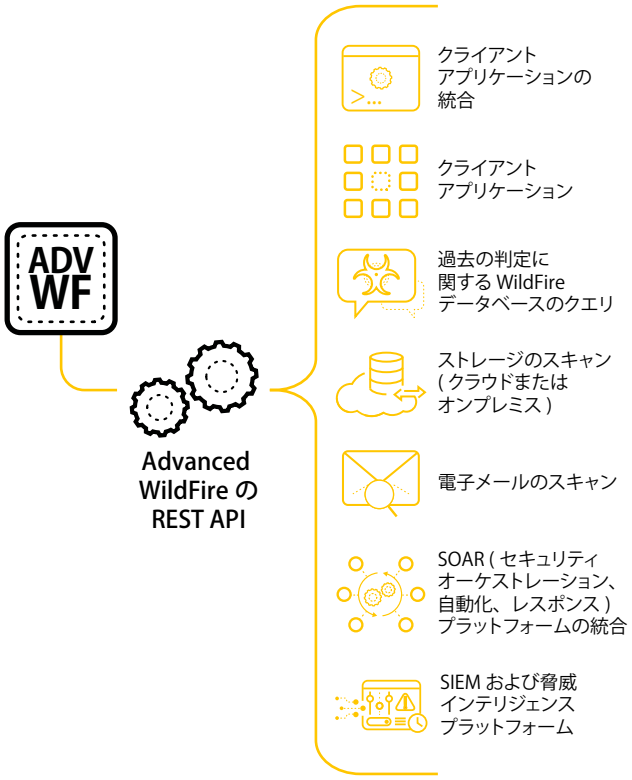


図 1: Advanced WildFire の REST API

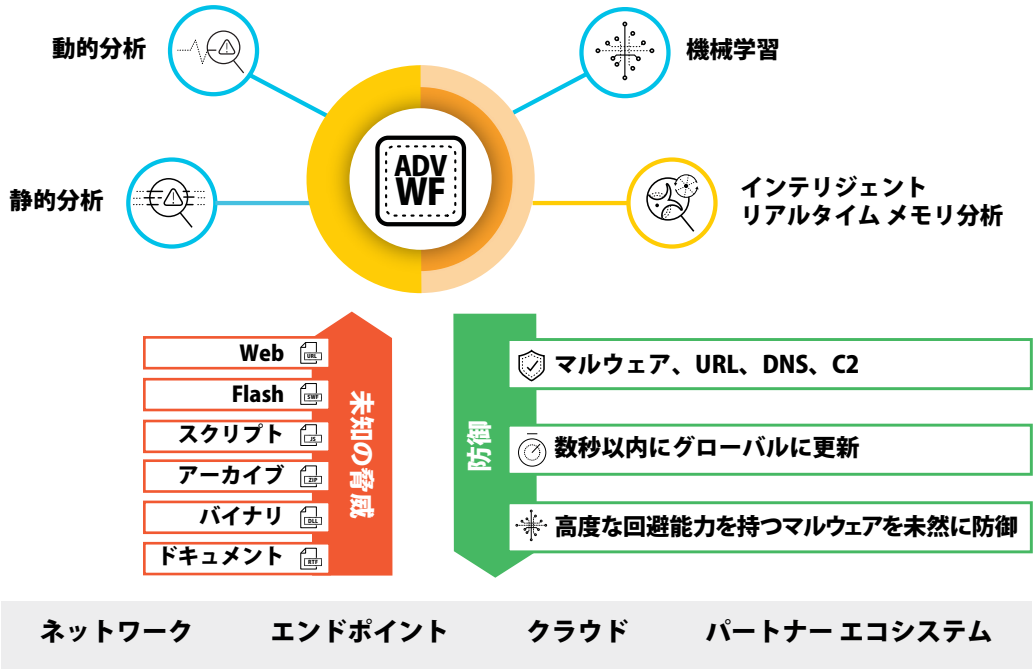
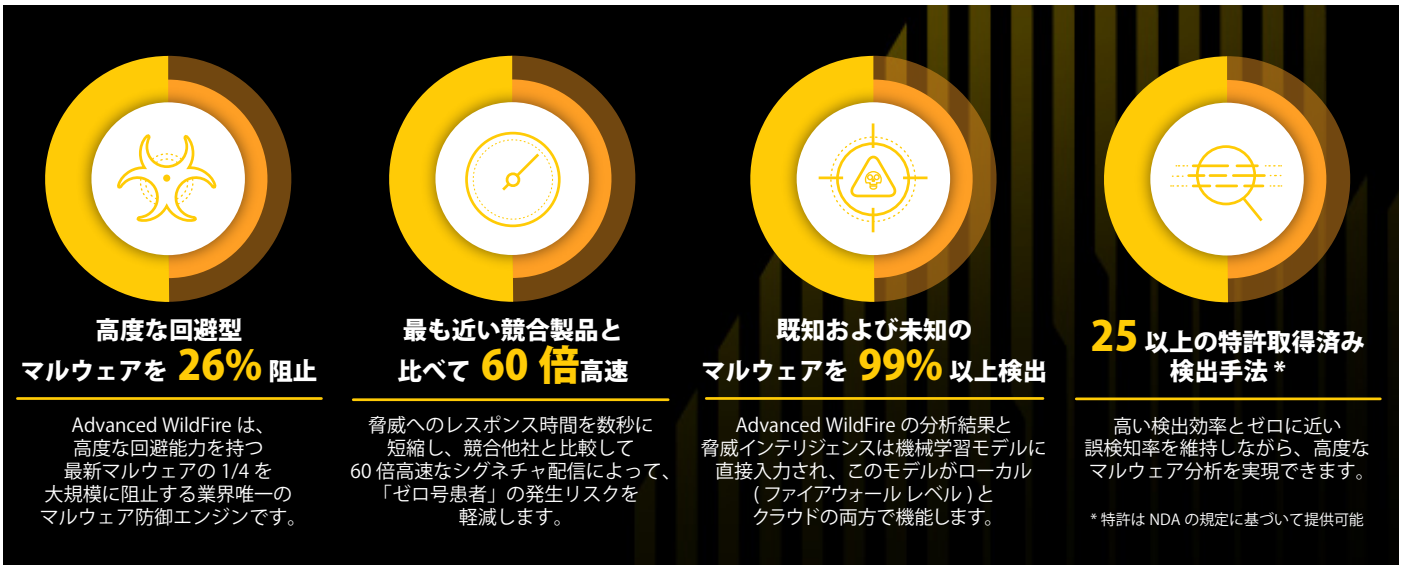


図 2: 組織全体を保護する統合セキュリティ

分析時は、Advanced WildFire の強力な自動防御機能が役立ちます。迅速で一貫性のある防御策が、エッジ、データセンター、クラウド、Software-as-a-Service (SaaS) アプリ、エンドポイントに適用されます。Advanced WildFire では、従来のサンドボックス手法を超え、高度な回避能力を備えた未知のマルウェアをクラウド環境において未然に防御することができます。



主なメリット

Advanced WildFire ソリューションには以下のメリットがあります。

- 「無制限の」シグネチャ リポジトリを活用して、既知のあらゆる AV シグネチャにアクセスできます。
- コンプライアンス要件を満たしながら包括的な保護を実現します。
- SOC が対処すべきイベントとワークロードを削減します。
- パロアルトネットワークスのプラットフォームとネイティブに統合します。
- ML ベースのエンジンを活用しながら悪意のあるファイル タイプをインラインでブロックします。

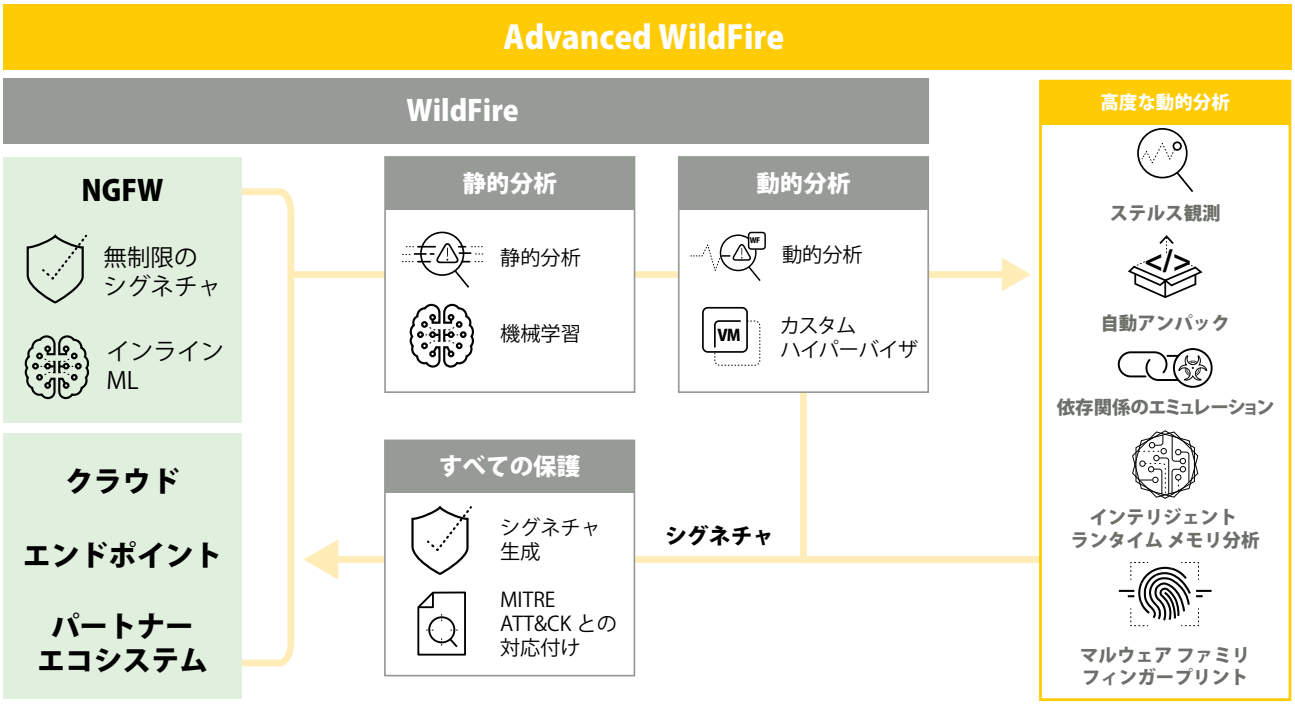


図 3: Advanced WildFire の検出エンジン

製品機能

悪意のある動作を検出

Advanced WildFire は、脅威インテリジェンス、分析、相関付けを適用することで、悪意のある動作を含む可能性のあるファイルを特定し、ファイルのアクションに基づいた判定を下します。これには以下に示す高度な機能が使用されています。

- **悪意ある動作を完全に可視化**：数百種類のアプリケーションに関連したすべてのトラフィックから脅威を特定します。例として、Web トラフィックや電子メール プロトコル (SMTP、IMAP、POP など) に対応します。
- **疑わしいネットワーク トラフィックの分析**：バックドアの作成、多段式マルウェアのダウンロードなど、疑わしいファイルから生じたすべてのネットワーク アクティビティを評価します。
- **ファイルレス攻撃/スクリプト検出**：有害性が疑われる JScript や PowerShell などのスクリプトをネットワーク通過時に特定し、Advanced WildFire に転送して分析と実行を行います。

インライン機械学習でファイアウォール レベルで脅威を阻止

Advanced WildFire は、クラウドで継続的にトレーニングされる脅威モデルを基盤としており、パロアルトネットワークスのハードウェアと仮想 ML を活用した NGFW でデプロイされる、インライン機械学習ベースのエンジンが組み込まれています。この斬新なシグネチャレスの機能は、一般的なファイル タイプに潜む危険なコンテンツ (Portable Executable ファイルや、PowerShell を起源とするファイルレス攻撃など) を完全にインラインで防御します。その際、クラウド分析は必要なく、コンテンツが被害を受けることも、ユーザーの生産性が低下することもありません。

高度な回避能力を持つマルウェアを未然に防御

以下に示す主な機能が、最新のマルウェアが持つさまざまな回避技法を無効化します。

- **ステルス観測**：マルウェアは環境をチェックし、その環境がサンドボックス環境だと判断した場合はデトネーションを保留します。分析コンポーネントがゲスト仮想マシン (VM) の外部に存在する、カスタムハードニングされたハイパーバイザを使用します。
- **自動アンパック**：Advanced WildFire は、分析時にファイルの内容を完全に可視化し、パックされたペイロードのシグネチャを生成します。
- **依存関係のエミュレーション**：新しい依存関係エミュレーション機能により、マルウェア実行に必要なすべての外部依存関係をサンドボックス環境に再現して、悪意のある行動を分析エンジンで観察できるようになります。
- **インテリジェント ランタイム メモリ分析**：インテリジェント ランタイム メモリ分析をサポートする検知用インフラストラクチャでは、悪意ある動作が確認された時点でメモリ内の重要ポイントでスナップショットを作成することができます。
- **マルウェア ファミリ フィンガープリント**：特許取得済みのマルウェア ファミリ フィンガープリント検出機能を使用して新しい脅威と既知のマルウェア ファミリを関連付けることで、回避能力を備えたマルウェアに対する防御策を大規模に生成できます。

Advanced WildFire エコシステム全体にわたるグローバルな防御を数秒で

Advanced WildFire は、インライン機械学習による防御では阻止できない高度にカスタマイズされた脅威に対して、強固なクラウドベース分析を実行した上で、ネットワーク、クラウド、エンドポイント全体に防御手段を展開します。さらに、Advanced WildFire 対応センサーを導入することで、ほとんどの新たな脅威に対し、初期段階での分析後数秒以内に、グローバルな防御策を提供します。

ハッシュではなくシグネチャを使用

Advanced WildFire は防御にハッシュではなくコンテンツのシグネチャを使用することで、1 つのシグネチャでより多くのマルウェアを特定し、1 つのマルウェアのポリモーフィック型亜種を最大で数百万件防御します。

コンプライアンスに準拠した安全なクラウドベース アーキテクチャへの展開

ファイルは、高速性と拡張性を備えた Advanced WildFire のグローバル クラウドに送信されます。ハードウェアのユーザーや仮想 ML を活用した NGFW、パブリック クラウド製品、次世代 CASB、Cortex XDR® エージェントなど、弊社のお客様はサービスを即座に有効に利用できます。さらに、パロアルトネットワークスは、セキュリティと機密性に関する業界標準のベストプラクティスに従って Advanced WildFire のインフラストラクチャを直接管理し、SOC 2 のコンプライアンス監査を定期的に受けています。詳細については、Advanced WildFire プライバシー データシートおよび認証に関する Web ページをご覧ください。

既存のセキュリティ ツールおよびカスタム アプリケーションとのシームレスな統合

急速なクラウド移行とデジタル変革に伴い表面化したセキュリティ課題の特徴は、次世代ファイアウォールや従来の制御ポイントの外部で、迅速かつ効果的なオンデマンド マルウェア分析が必要とされる点です。お客様は Advanced WildFire の業界最先端のマルウェア分析機能を活用し、既存の SOAR ツールとの統合、カスタム アプリケーション (ビジネス - 顧客間の Web ポータルなど) の保護、クラウド移行前のファイル共有およびストレージの場所での悪意のあるコンテンツのスキャンなどを行うことができます。さらに、NGFW に対する Advanced WildFire サブスクリプションは、固定数のサブミッションとクエリに対して API アクセスを開放します。

スタンドアロンの WildFire API

スタンドアロンの WildFire API サブスクリプションでは、組織固有の要件に基づいて、WildFire クラウド脅威データベースに対して有害性が疑われるコンテンツに関する情報を問い合わせ、ファイルを送信して WildFire の高度な脅威分析機能を使用した分析を行うことができます。

ログ、レポート、フォレンジックの統合

Advanced WildFire のユーザーは、PAN-OS® 管理インターフェイス、Panorama® ネットワーク セキュリティ管理、Strata™ Cloud Manager、Cortex XDR、または Cortex XSOAR® を通じて、悪意のあるイベントに関する統合ログや分析情報を入手し、可視化された現状を把握できます。このためチームは、ネットワークで観測されたイベントを迅速に調査し、関連付けることができます。

表 1: 機能およびライセンスの概要

	NGFW に適用される Advanced WildFire サブスクリプションでアクティベートされる機能
ファイルのサポート	PE ファイル (EXE、DLL、その他)、Microsoft Office の全ファイル タイプ、Mac OS X ファイル、Linux (ELF) ファイル、Android パッケージ キット (APK) ファイル、Adobe Flash および PDF ファイル、アーカイブ (RAR および 7-Zip) ファイル、スクリプト (BAT、JS、VBS、PS1、シェル スクリプト、および HTA) ファイル、電子メール メッセージ内のリンクの分析、および暗号化 (TLS/SSL) ファイル。
プロトコルのサポート	SMTP、POP3、SMB、FTP、IMAP、HTTP、HTTPS。暗号化バージョンはさらに前述のプロトコルもサポート。
1日あたりのファイル分析量	ユニーク ファイル数で 1 日 8,000 万以上を分析。
シグネチャ タイプ	• Web トラフィック (HTTP/HTTPS)、電子メール プロトコル (SMTP、IMAP、POP)、および FTP トラフィックで検出された新規/ゼロデイ マルウェアに基づきます。 • サンプルのマルウェア ペイロードで生成され、精度と安全性についてテストされます。
未知のマルウェアに対する防御の更新	数秒で、接続された NGFW に遅延ゼロのシグネチャを配信します。*
地域のクラウドの場所	オーストラリア、カナダ、ドイツ、インド、日本、オランダ (EU 地域クラウド)、シンガポール (APAC 地域クラウド)、英国、米国 (グローバル クラウドおよび米国政府クラウド)。地域クラウド。
WildFire APIキー	NGFW 上の Advanced WildFire サブスクリプションは Advanced WildFire API へのアクセスを含み、Advanced WildFire を別のアプリケーションに統合できます。この API には、ファイルの送信とハッシュ クエリの 1 日単位の制限があります。
統合	• パロアルトネットワークスとの統合。クラウドで提供されるすべてのセキュリティ サブスクリプション、Cortex XDR、Cortex XSOAR、Prisma Access、Prisma Cloud、SaaS Security が含まれます。 • テクノロジ パートナーとの統合。Advanced WildFire API を使用して、サードパーティ サービスで判定を行います。
管理とレポート	パロアルトネットワークスの Panorama および WebUI、API、AIOps。

表 1: 機能およびライセンスの概要 (続き)		
	NGFW に適用される Advanced WildFire サブスクリプションでアクティベートされる機能	
フォレンジック	• ホストベースとネットワークベースの両方のアクティビティを含め、複数のオペレーティング システム環境にわたって Advanced WildFire に送信された悪意のあるすべてのファイルを詳細に分析します。 • 元のマルウェア サンプルにアクセスし、ダイナミック分析セッションの完全な PCAP により、リバース エンジニアリングを実行します。 • オープン API により、セキュリティ情報イベント管理 (SIEM) システムなどのサードパーティ セキュリティ ツールと統合します。	
信用とプライバシー	パロアルトネットワークスは機密情報または個人を特定できる情報への不正アクセスを防ぐため、厳格なプライバシー管理とセキュリティ管理を実施しています。セキュリティと機密性に関する業界標準のベストプラクティスを適用しています。詳細については、プライバシー データシートを参照してください。	
	Advanced WildFire の機能	**PAN-OS のバージョン要件**
要件†	WildFire クラウドベース ファイル分析	任意のサポート対象 PAN-OS
	Advanced WildFire クラウドベース ファイル分析	任意のサポート対象 PAN-OS
	NGFW インライン機械学習 (PE、ELF、PS1、PS2、Office)	10.1 以上
	Advanced WildFire リアルタイム シグネチャ配信	10.1 以上
	Advanced WildFire インライン ゼロデイ防御	11.1
推奨環境	内部と外部の両方のソースとして、任意の場所に導入された Palo Alto Networks Next-Generation Firewalls は、ファイルベースの脅威をネットワーク内に持ち込む可能性があります。	

* PAN-OS 10.1 が必要。

† PAN-OS のバージョンに関係なく Advanced WildFire を購入頂けますが、追加機能の利用はアップグレード後となります。Advanced WildFire サブスクリプションに含まれる各種機能を利用するには、本書に示す PAN-OS のバージョン要件を満たす必要があります。

〒 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-wildfire_032624