WildFire

高度な回避性を備えたマルウェアがもたらすリスクを排除

数秒が命取り : 従来のマルウェア分析とサンドボックスが失敗した理由

今日の攻撃者は、クラウドスケールの正規のインフラストラクチャだけでなく機械学習にも容易にアクセスでき、これらを通じて回避型の悪意のあるファイルをエンド ユーザーにすばやく配信することができます。今日のマルウェアは増殖し続け、5 分ごとに 1,000 個の新たな脅威を生み出しており、その 5 分後には最大 10,000 個の亜種が発生しています。サイロ化したセキュリティ ツールでは、こうしたマルウェアには対応しきれません。

ビジネス上のメリット

新たな脅威の最初の被害者を発生させません。機械学習を活用した次世代ファイアウォール (NGFW) 上で、新たなインライン防御ステップが、生産性に影響を及ぼすことなく、一般的なファイル タイプ内に潜む未知の脅威を阻止します。

滞在時間がもたらすリスクを排除します。ネットワーク、エンドポイント、およびクラウド全体での組織的な防御策の自動配信を通じて、脅威への対応に要する時間を数時間や数分から数秒に短縮します。

対応を要するイベントとセキュリティ操作の作業負荷を削減します。機械学習を活用した NGFW 上のインライン防御機能が、最初の脅威を阻止することで、調査および封じ込めが必要となる検出イベントの数を減少させます。

クラウドベースのアーキテクチャによって、総所有コストを削減します。アプライアンスベースのサンドボックスの導入、管理、パッチ適用、および保守コストを排除します。

追加コストなしで無制限の分析能力が得られます。弊社のサブスクリプション モデルは、容量ベースの追加料金なしで、お客様が必要とする処理能力と拡張性を提供します。

手動による統合は不要です。生成されたインテリジェンスはすべて、自動でパロアルトネットワークスのエコシステムに還元され再運用されるため、手動のツールも統合も不要です。

データ侵害をもたらすゼロデイ攻撃や advanced persistent threat (APT 攻撃 - APT) を受けた組織は、以下のリスクに直面する可能性があります。

- **評判リスク**—政府および業界の報告要件により、マスコミや新聞雑誌で広く報道されます。失われた情報の量と種類によっては、いっそう大きく取り上げられます。
- **規制リスク**—統治機関から制裁を受けるとともに、標的となった情報資産によっては (個人を特定できる情報 [PII]、アカウント情報、企業または顧客の知的資産など)、コンプライアンスおよび評価要件が増加します。
- **財務リスク**—購入者の信頼の低下、ランサムウェア、規制の増加に関連する収益の損失 (ダウンタイム、売上減少、コンプライアンス要件の増加、データ取得コストなど) が発生する可能性があります。
- **法的リスク**—顧客データの損失と、規制 (HIPAA、GDPR、米国の州法 [CCPA や、NYDFS サイバーセキュリティ規制など]、オーストラリアのデータ プライシー規制など) の遵守をめぐって、民間からの異議申し立てによる法的責任やデュー デリジェンスの問題が問われます。

回避型攻撃に関連するリスクを軽減するために、組織はネットワーク サンドボックス ソリューションを使用したマルウェア分析に頼っています。残念なことに、こうした従来のソリューションはいずれもユーザーの生産性に影響するうえ、判定が下るまでに時間がかかり、分析のためにファイルを保持してワークフローを中断させたり、サンプルのスキャン中、一部のコンテンツの流れを遅らせたり、コンテンツを変更して多くのファイルを読み取り不能にしたりします。さらに、こうしたソリューションにはもう 1 つ致命的な欠陥があります。新たな脅威に対する防御は、組織内で最初の被害者 (第 1 号) が特定された (つまり、侵害が発生した) 後で初めて可能になることです。

拡張性がきわめて高いクラウド分析を活用した即時防御

パロアルトネットワークスの WildFire® マルウェア防御サービスでは、パフォーマンスを考慮したセキュリティの妥協は不要です。このサービスにより、組織はついに防御第一の対策を採用することができます。業界最先端のクラウドベースのマルウェア分析および防御エンジンである WildFire は、未知のあらゆるファイルを分析して悪意のあるコンテンツがないか調べ、防御策を記録的な速さで配信することによって、最初の被害者の発生リスク、およびその後のあらゆる脅威のリスクを軽減します。

オフラインによる (つまり遅延のある) 未知のマルウェア分析だけに頼った従来のソリューションとは異なり、WildFire の分析およびインテリジェンスは、ローカルのファイアウォール レベルで動作する機械学習モデルに直接送られ、このモデルを通じて新たな脅威の最大 95% がインラインで阻止されます。その他に対しては、WildFire は革新的な多手法アプローチを使って、機械学習を活用したすべての NGFW にシグネチャを数秒で配信します。

生産性に影響することなく防御機能を提供できるマルウェア分析エンジンは、WildFire をおいて他にありません。ダイナミックおよびスタティック分析、革新的な機械学習手法、再帰的な分析、カスタム構築の画期的な分析環境を組み合わせた WildFire では、巧妙性、回避性がきわめて高い脅威でも分析、特定し、防御することができます。分析後の自動化された処理で WildFire はその威力を発揮します。WildFire は、エッジで、データセンターで、さらにクラウドから、また Software as a Service (SaaS) アプリケーション内で、そしてエンドポイント上で、迅速で一貫した防御を適用します。

主な機能

インラインの機械学習によるファイアウォール レベルでの未知の脅威に対する防御

WildFire は、クラウドで継続的に磨きがかけられている脅威モデルを活用するとともに、インラインの機械学習ベースのエンジンを備えています。このエンジンは、機械学習を活用した弊社のハードウェアおよびバーチャルの NGFW 内で提供されます。シグネチャを使わないこの革新的な機能は、Portable Executable (PE) ファイルや、PowerShell® 由来のファイルレス攻撃などの一般的なファイル タイプをインラインで完全に阻止します。クラウド分析は不要で、コンテンツが損なわれることはなく、ユーザーの生産性が失われることもありません。未知のファイルが既存のシグネチャに一致した場合でも、機械学習を活用した NGFW によって分類された場合でも、WildFire は常に完全分析を実行します。この分析から、有益なインテリジェンスとデータが抽出され、セキュリティ アナリストにコンテキストが提供されるとともに、機械学習モデルのトレーニングの更新が生成されます。またインテリジェンスが他のサブスクリプションと共有され、その他の攻撃ベクトルに対する防御に役立てられます。

グローバルな防御策を WildFire のエコシステム全体に数秒で配信

インラインの機械学習を活用した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は、WildFire はクラウドベースの強力な分析を適用して、ネットワーク、クラウド、エンドポイント、または WildFire 対応センサーの導入場所のすべてに防御策を配信します。PAN-OS® の新機能と連携して動作することで、WildFire は、ほとんどの新たな脅威の最初の分析後、

数秒以内に防護策を生成し、グローバルに配信します。回避に対抗できるシグネチャのクラウドスケールのこの革新的な配信により、攻撃者が悪意のあるコンテンツを展開する機会が封じられます。

ハッシュではなくシグネチャを使用

WildFire は、ハッシュではなくコンテンツのシグネチャを使って防御するため、1 つのシグネチャでより多くのマルウェアを特定することができます。したがって、1 対 1 の割合を必要とする主にハッシュ ベースのシステムに比べて、WildFire では同じリソースでより多くの攻撃が防がれます。1 つの WildFire シグネチャで、1 つのマルウェアの最大数百万のポリモーフィック型亜種に対する防御ができます。

すべてのトラフィックで悪意のある動作を一掃

WildFire は、潜在的な悪意のある動作を含むファイルを特定し、以下に示す高度な機能と平行して脅威インテリジェンス、分析、相関付けを適用することにより、ファイルのアクションに基づいて判定を下します。

- **悪意のある動作の完全な可視性：**ポートや暗号化の区別にかかわらず、Web トラフィック、電子メール プロトコル (SMTP、IMAP、POP など)、ファイル共有プロトコル (SMB、FTP など) を含む、数百ものアプリケーションのすべてのトラフィックで脅威を特定します。
- **不審なネットワークのトラフィック分析：**バックドアの構築、次の段階のマルウェアのダウンロード、評判の良くないドメインへのアクセス、ネットワークの偵察など、不審なファイルによるあらゆるネットワーク アクティビティを監視します。
- **ファイルレス攻撃 / スクリプトの検出：**ネットワークを通過しようとする、JScript や PowerShell などの潜在的に悪意のあるスクリプトを特定し、そのスクリプトを分析および実行するために WildFire に転送します。

WildFire の強力な検出および分析機能は、パロアルトネットワークスのポートフォリオの製品群だけでなく、さまざまな電子メールおよびクラウド プラットフォームで主要パートナー ソリューション内の多数の製品とシームレスに統合されます。

複数の手法を使用した回避対抗型アプローチにより、新たな脅威を発見

WildFire では、未知の脅威をクラウド分析環境で検出するための従来のサンドボックス アプローチを越えて、以下に示す複数の手法を組み合わせています。

- **ダイナミック分析：**回避に対抗できる専用のバーチャル環境でファイルを実行して動作を観察し、数百もの動作特性に基づいて未知のマルウェアを検出することができます。
- **機械学習：**各ファイルから何千もの固有の特徴を抽出し、予測機械学習モデルのトレーニングを行って、スタティック分析やダイナミック分析だけでは特定不可能な新たなマルウェアを特定できるようにします。
- **スタティック分析：**マルウェアを効果的に検出し、マルウェア亜種を即時に特定することによって、ダイナミック分析を補完します。さらに、スタティック分析では、ダイナミック アンパック処理を活用して、パッキング ツール セットの使用により検出を逃れようとする脅威を分析します。

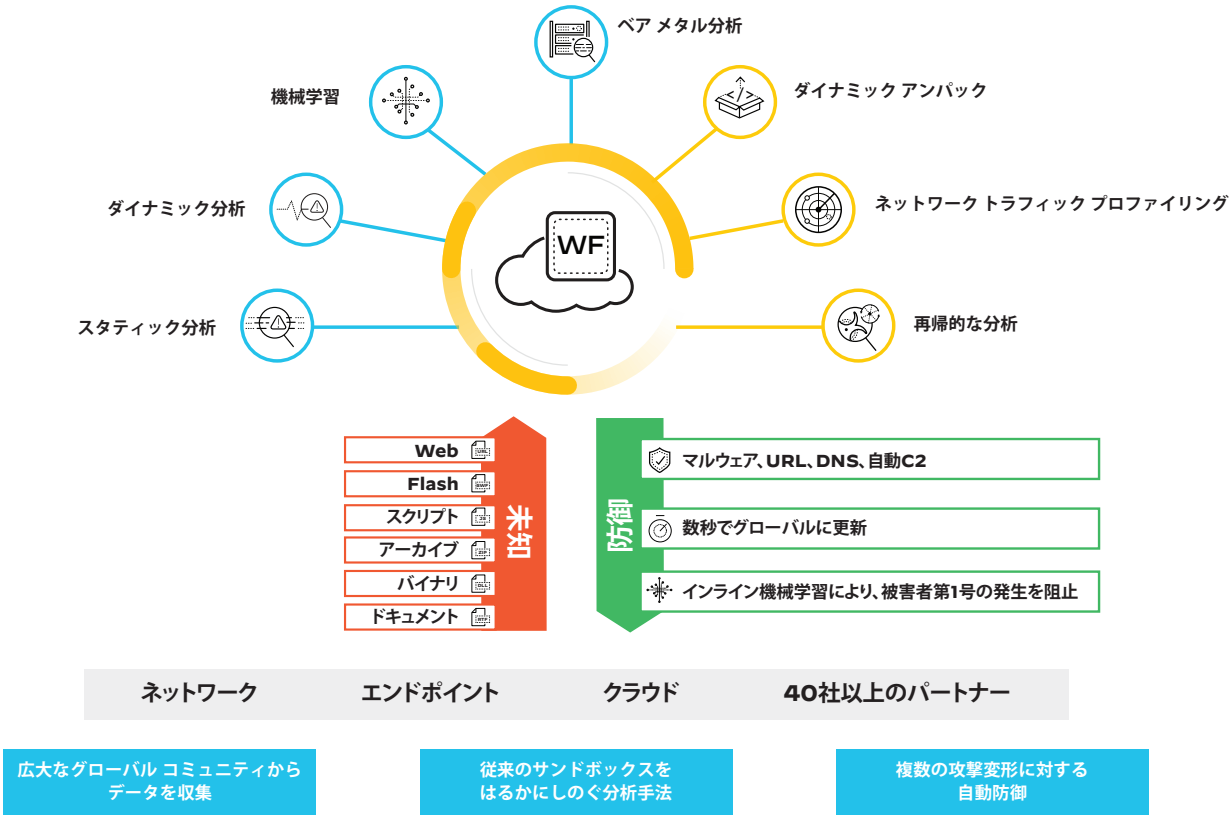

図 1: WildFire: マルウェア分析のグローバルな中枢部

- **ベア メタル分析：**回避型の脅威を実際のハードウェア環境で実行することによって、攻撃者のアンチ VM 分析手法の展開能力を完全に排除します。
- **カスタム構築のハイパーバイザ：**攻撃者がアクセスできるオープン ソース プロジェクトや専有ソフトウェアに依存しない、堅牢な専有ハイパーバイザによって、攻撃者の回避手法を阻止します。

これらの独自の手法の組み合わせによって、WildFire は、きわめて効率的に、誤検知ほぼゼロの精度で、未知のマルウェアを分析し、阻止することができます。

複雑な多段階攻撃を阻止

攻撃者は、既存の分析手法を逃れるためにマルウェアを継続的に進化させており、攻撃を異なる複数の要素と段階に分割し、複数の同時配信ベクトルを使用し、評判の良いクラウド サービスを悪用することによって、検出を回避しようとします。こうした戦略に対しては、単一段階、単一ベクトルの従来のマルウェア分析は役に立ちません。

WildFire のクラウド スケールを高度なファイル分析および URL クロールと組み合わせた Multi-Vector Recursive Analysis（マルチベクトル再帰分析 - MVRA）は、攻撃者が仕掛ける多段階、マルチホップの巧妙な攻撃を阻止する、独自の包括的なソリューションを提供します。他のソリューションとは異なり、WildFire では、ファイル分析の観点から複数の攻撃段階を追跡することができ、ある段階で実行が失敗しても追跡可能です。このワークフローでは、Web とファイルの両方の攻撃ベクトルに対して分析が統合されるため、独自の視点から複数の段階によるキャンペーンの全体像をつかむことができます。攻撃者が、無害な URL や評判の良いドキュメント共有サイトを使った複数の段階の背後に、悪意のあるコンテンツを隠すことは、もはや不可能です。

運用上のメリット

- **セキュリティ制御の自動的な再プログラミングによって、未知の脅威をブロック：**35,000 を超えるサブスクライバ間で共有されるリアルタイムのインテリジェンスによって、ネットワーク、エンドポイント、クラウド全体で自動的に脅威情報が更新され、脅威が阻止されます。
- **分析された脅威についての詳細なコンテキストを取得：**さまざまなオペレーティング システム環境およびアプリケーション バージョンにわたって、WildFire に送られる悪意のあるすべてのファイルについての詳細なレポートを取得します。
- **既存のセキュリティ ツールとのシームレスな統合：**SIEM、TIP、チケット、SOAR、または XDR ツールとのオープン API 統合を活用して、セキュリティ侵害の兆候（IOC）を処理します。
- **実用的な脅威インテリジェンスを活用：**AutoFocus ™コンテキスト脅威インテリジェンスと組み合わせて、攻撃者とその意図について理解し、キャンペーンを追跡することによって、次に行う措置の妥当性を確認できます。

安全性と拡張性に優れたクラウドベースのアーキテクチャで導入

WildFire のクラウドベースのアーキテクチャでは、ネットワーク、エンドポイント、クラウド全体での未知の脅威の大規模な分析と防御をサポートしています。ファイルは、スケールとスピードを提供する WildFire のグローバル クラウドに送信されます。パロアルトネットワークスのお客様は、どのお客様でも（機械学習を活用したハードウェアおよびバーチャルの NGFW、パブリック クラウド サービス、Prisma™ SaaS、Cortex XDR™ エージェントのお客様など）、すばやくサービスを有効にすることができます。WildFire のインフラストラクチャは、パロアルトネットワークスが、セキュリティと守秘義務に関する業界標準のベスト プラクティスに従い、SOC 2 コンプライアンスの定期監査を実施することによって直接管理します。詳細については、「WildFire プライバシー データシート」を参照してください。

お客様がデータの主権とプライバシーの問題により適切に対処できるようにするため、弊社では、各地域で分散 WildFire クラウドを管理することによって、お客様がデータの場所を制御しやすいようにしています。各地域の分散クラウドでは、WildFire パブリック クラウドと同じ検出および防御機能を提供しているため、お客様は地域のデータ プライバシーの問題に対処できるよう送信先を調整することができます。

ログ、レポート、フォレンジックを統合

WildFire のユーザーは、悪意のあるイベントに関する統合されたログ、分析、および可視化機能を、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、AutoFocus、Cortex XDR、Cortex™ XSOAR、または WildFire ポータルから使用できるため、チームでのネットワークで観測されたイベントの調査と相関付けが迅速化されます。この情報に基づいて、セキュリティ チームは、どのアプリケーションを使用しているかにかかわらず、タイムリーな調査とインシデント対応に必要なデータをすばやく見つけてアクションを実行できます。

パロアルトネットワークスのセキュリティ サブスクリプションの威力

今日、サイバー攻撃は、増加しているだけでなく、巧妙化しており、ネットワーク セキュリティ デバイスやツールを回避する高度な手法が使われています。そのため、組織では、セキュリティ チームの作業負荷を増やすことなく、またビジネスの生産性を妨げることなく、ネットワークを保護することが困難になっています。業界初の機械学習を活用した NGFW プラットフォームとシームレスに統合された、弊社のクラウド提供セキュリティ サブスクリプションは、インテリジェンスを調整し、あらゆる攻撃ベクトルに対する防御を可能にすることによって、クラス最高の機能を実現するとともに、個々のネットワーク セキュリティ ツールの対象範囲に含まれない隙間を排除します。市場をリードする機能を、単一プラットフォームでの一貫した操作により駆使して、きわめて高度な回避型脅威からお客様の組織を保護してください。WildFire または以下に示す弊社の各セキュリティ サブスクリプションのメリットをご活用ください。

- **Threat Prevention：**従来の侵入防御システム（IPS）ソリューションの範囲を越えて、シングル パスですべてのトラフィックにわたって既知のあらゆる脅威を自動的に阻止します。
- **URL Filtering：**既知および未知の悪意のある Web サイトへのユーザーのアクセスを未然に防ぐことによって、インターネットを安全に利用できるようにします。
- **DNS セキュリティ：**DNS を利用してコマンド アンド コントロールやデータの窃盗を行う攻撃を遮断します。お客様のインフラストラクチャを変更する必要はありません。
- **IoT セキュリティ：**業界初のターンキー IoT（モノのインターネット）セキュリティ ソリューションによって、お客様の組織全体の IoT および OT デバイスを保護します。
- **エンドポイント向け GlobalProtect™ネットワーク セキュリティ：**機械学習を活用した NGFW の機能をリモート ユーザーにまで拡張して、お客様の環境内のあらゆる場所で一貫したセキュリティを実現します。

表 1: 機能とライセンスの概要	
WildFire サブスクリプションでアクティベートされる機能	
高度な分析、防御、および回避対抗手法	**スタティック分析**—メモリ分析、機械学習、およびファイルの異常、悪意のあるパターン、既知の悪意のあるコードの分析を組み合わせます。 **インラインの機械学習ベースの防御 (ファイアウォール上)**—未知の悪意のある実行ファイルと PowerShell 攻撃をブロックします。 **ダイナミック分析**—カスタム ハイパーバイザ、動作スコアリング、ネットワーク プロファイリング、複数バージョンの分析を含みます。 **MVRA**—高度なファイル分析と URL クロールの組み合わせによって、多段階のマルチホップ攻撃を阻止します。 **ベア メタル分析**—バーチャル環境もハイパーバイザも使用しない、実際のハードウェア上での完全なダイナミック分析を可能にします。
OS サポート	macOS、Android、Windows XP/7/10
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
1 日あたりのファイル分析量	柔軟
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たな / 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、正確性と安全性がテストされます。
未知のマルウェアに対する防御の更新	• 数秒。接続された次世代ファイアウォールに遅延ゼロのシグネチャが配信されます。*
地域のクラウドの場所	• 北米 (2: グローバルおよび地域)、アムステルダム、シンガポール、日本。
主な統合	• パロアルトネットワークスとの統合 (クラウド提供のすべてのセキュリティ サブスクリプション、AutoFocus、Cortex XDR、Prisma SaaS などとの統合)。 • テクノロジ パートナーとの統合。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。
管理およびレポート	パロアルトネットワークス Panorama および WebUI、API
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て、複数のオペレーティングシステム環境にわたって 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 サンプルを使用して、ダイナミック分析セッションの完全な PCAP によるリバース エンジニアリングを実行します。 • オープン API を通じて、セキュリティ情報およびイベント管理 (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。
信頼とプライバシー	• パロアルトネットワークスでは、プライバシーとセキュリティの厳格な制御により、機密情報や個人の識別が可能な情報への不正アクセスを防止しており、セキュリティと守秘義務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、弊社のプライバシー データシートをご覧ください。

表 1: 機能とライセンスの概要 (続き)	
ライセンスと要件	
要件	パロアルトネットワークス WildFire サブスクリプションを使用するには、以下のものが必要です • PAN-OS を実行する Palo Alto Networks Next-Generation Firewall • パロアルトネットワークス Threat Prevention ライセンス
WildFire のフル ライセンス	WildFire は、Palo Alto Networks Next-Generation Firewall の統合されたクラウドベースのサブスクリプションとして提供されるスタンドアロン ライセンスを必要とします。また、パルアルトネットワークス サブスクリプション ELA、VM-Series ELA、または Prisma Access の一部としてもご利用可能です。
推奨環境	任意の場所に導入された Palo Alto Networks Next-Generation Firewall。内部ソースと外部ソースのどちらからも、ファイルベースの脅威がネットワークに持ち込まれる可能性があるためです。
WildFire の基本ライセンス	WildFire の基本機能は Palo Alto Networks Next-Generation Firewall の一部として組み込まれていますが、この場合、一連の機能に制限があり、次の操作のみ可能です。 • 圧縮および暗号化されたコンテンツ (Windows XP/7 のみ) など、EXE および DLL ファイル タイプの、WildFire 分析への転送 • アンチウイルスまたは Threat Prevention の更新による WildFire シグネチャの取得 • アクティブな Threat Prevention サブスクリプションがある場合、24 ～ 48 時間ごとの自動更新 (インラインの機械学習ベースの防御と遅延ゼロのシグネチャのサポートはありません)

* PAN-OS 10.0 が必要です。

〒 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
www.paloaltonetworks.jp

wildfire-ds-061220