ビジネス上のメリット

- **スタンドアロン IPS のコストと管理作業を排除します。** Snort などの強力な IPS の機能を弊社の NGFW と統合して活用し、単一のセキュリティ ポリシー ルール ベースを確保します。
- **攻撃を可視化し、お客様の組織を確実に保護します。** ポート、プロトコル、暗号化の区別を問わず、すべてのトラフィックを検査して脅威を探します。
- **脆弱性とパッチの管理に必要なリソースを削減します。** 既知のマルウェア、脆弱性エクスプロイト、C2 を自動的にブロックします。
- パフォーマンスを犠牲にすることなく、防御管理による**すべての脅威の検出および制御の適用機能を活用します。**

Threat Prevention

従来の侵入防御機能は進化していない

組織は、利益や、イデオロギー / ハクティビズム、さらには組織への不満など、さまざまな動機を持つ攻撃者が仕掛ける集中砲火に直面しています。今日の攻撃者には十分な資金と設備があります。攻撃者は回避戦術を使って標的とするネットワークに足場を築き、大量の高度な攻撃を開始します。攻撃者は、標的を絞り込み、巧妙な計画に基づいて組織を侵害し、横方向に移動して貴重なデータを抽出するという方法を使います。一連の操作は、従来の個別防御機能にまったく検出されることなく実行されます。

さらに悪いことに、従来の侵入防御 / 侵入検知システム (IPS/IDS) は、脅威ランドスケープの進化前に使っていた防御戦略にいまだに頼っています。トラフィックの検査は一部のポートでのみ行われます。防御スタックへの単一機能デバイスの追加によって一部の問題が軽減される可能性はありますが、その反面、パフォーマンスが低下します。また全体的な可視性は確保されません。さらに、多くの場合、基礎部分は対応範囲に含まれず、セキュリティ チームが責任を負うことになりますが、チームでは脆弱性の特定やパッチ適用を行うための適切な設備が整っておらず、データの侵害を自信をもって防ぐことができません。2019 年の Ponemon の調査によると、回答者の 67% が、すべての脆弱性を軽減して侵害を防ぐには時間とリソースが足りないと感じています。[1]

包括的な防御によって、エクスプロイト、マルウェア、およびコマンド アンド コントロールからネットワークを保護

パロアルトネットワークスの Threat Prevention サービスは、複数の防御層を提供し、攻撃の各フェーズで脅威に対処することによって、ネットワークを保護します。Threat Prevention は、従来の IPS 機能に加えて、独自の機能を備えています。この機能は、事前定義済みの限られたポート セットに基づいてシグネチャを呼び出すのではなく、あらゆるポートで脅威を検出してブロックします。

弊社の全世界のお客様のコミュニティは、グローバルな集合的脅威インテリジェンスを共有しており、脅威を最初の検出後すぐに阻止することによって、高度な攻撃の成功率を大幅に低下させています。エクスプロイト、マルウェア、悪意のある URL、コマンド アンド コントロール (C2)、スパイウェアなどを阻止するための Threat Prevention の日次更新には、弊社の他のクラウド提供セキュリティ サブスクリプションのデータが活用されます。Threat Prevention はすべての Palo Alto Networks NGFW に不可欠であり、パロアルトネットワークスの他のサブスクリプション (未知のファイルベースの脅威に対処する WildFire® マルウェア防御サービス、Web 経由の攻撃に対処する URL Filtering、ドメイン ネーム サービスを使用した攻撃に対処する DNS セキュリティ、非管理対象デバイスの可視性とコンテキストを提供する IoT セキュリティなど) と組み合わせることによって、新たな未知の脅威に対する防御の速度をほぼリアルタイムにまで高めることができます。

主な機能

アプリケーションを利用可能にしながら、脅威を阻止

アプリケーションは企業の業務運営に不可欠です。そのため、企業では、ユーザーが暗号化チャネルを使用して、非標準ポート (多くの場合、ステートフル インスペクション ファイアウォールを迂回するために使用) とポートホッピングによってネットワークに入れるようにすることで、アプリケーションへのユーザーのアクセスを容易化し、常時アクセスを保証しています。

残念なことに、高度な脅威はこの動作を悪用して、検出されることなくネットワークに不正侵入します。こうした脅威は、アプリケーション内にトンネルを作り、暗号化されたトラフィック内に隠れ、無防備な標的を餌食にしてネットワーク内に足場を築き、悪意のあるアクティビティを実行します。

弊社は、複数の防御層を提供し、攻撃の各フェーズで脅威に対処することによって、こうした脅威からお客様のネットワークを保護します。Threat Prevention は、従来の IPS 機能に加えて、事前定義済みの限られたポート セットに基づいてシグネチャを呼び出すのではなく、あらゆるポートで脅威を検出してブロックする機能を備えています。Threat Prevention エンジンは、弊社の機械学習を活用した NGFW 上で User-ID™ および App-ID™ テクノロジを使ってすべてのポートのすべてのトラフィックにコンテキストを追加することによって、どのような回避手法を使った脅威でも決して見失いません。

ますます多くのエンタープライズ トラフィックが、TLS/SSL で暗号化され、内容が判別しにくくなっており、攻撃者はこの可視性の欠如を悪用して攻撃を開始し、より多くのリスクをビジネスにもたらしています。弊社の機械学習を活用した NGFW はネイティブの復号化機能を提供し、Threat Prevention は、ポリシーを通じて、TLS/SSL トラフィックを選択的に復号化して検査する機能を提供しているため、セキュリティとパフォーマンスのバランスを適切に取ることができます。[2]

各フェーズで脅威を排除

ここ数年、単一目的の防御ツールが攻撃者に迂回されたことが原因で発生した侵害は数えきれません。Threat Prevention サブスクリプションでは、包括的な保護を保証するために、弊社の機械学習を活用した NGFW との緊密な統合により、以下に示す複数の防御メカニズムを組み合わせて適用します。

- **ヒューリスティックベースの分析**：ポート スキャン、ホスト スイープ、denial-of-service (サービス拒否 - DoS) 攻撃などの異常なパケットおよびトラフィック パターンを検出します。
- **設定が容易なカスタムの脆弱性シグネチャ**：ネットワークの固有のニーズに合わせて侵入防御機能を調整でき、Snort や Suricata® などの広く使用されているオープン ソース フォーマットからルールをインポートすることも可能です。
- **その他の攻撃防御機能**：無効なパケットや不正な形式のパケットのブロック、IP デフラグメント、TCP 再構築などの機能が、回避および隠蔽手法に対して防御します。

パロアルトネットワークスでは、ネイティブに統合された防御テクノロジ群を採用し、脅威が 1 つのテクノロジを逃れても別のテクノロジによって捕捉できるようにしています。効果的な防御の秘訣は、情報の共有、および検査対象のトラフィックと特定 / ブロック対象の脅威の両方に関するコンテキストの提供を目的として構築されたセキュリティ機能を使用することです。

すべての脅威に対するスキャンをシングル パスで実行

Threat Prevention エンジンは、トラフィックの検査および分類と、マルウェアと脆弱性エクスプロイトの両方の検出およびブロックをシングル パスで実行する、業界初のエンジンです。従来の脅威防御テクノロジでは、それぞれ個別に管理する必要がある複数のスキャン エンジンと複数のルール ベースが必要なため、大幅な遅延と管理オーバーヘッドが発生し、またスループット パフォーマンスが劇的に低下します。弊社では、すべての脅威に対して統一されたシグネチャ形式を使用し、単一の統合スキャンですべての分析を実行して、従来のソリューションに共通する冗長プロセスを排除することによって、処理を迅速化しています。

Threat Prevention テクノロジは、各パケットがプラットフォームを通過するときにパケットを精査し、パケット ヘッダー内とペイロード内の両方のバイト シーケンスを綿密にチェックします。この分析から、使用アプリ

1. 「Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture」、Ponemon Institute、2019 年 2 月、https://www.balbix.com/app/uploads/Ponemon-Survey-Vuln-Management-.pdf
2. パロアルトネットワークスの特定のネットワーク ファイアウォールに対して有効にした Threat Prevention のスループットについては、paloaltonetworks.com/resources/datasheets/product-summary-specsheet をご覧ください。

ケーション、送信元と送信先、プロトコルが RFC に準拠しているかどうか、ペイロードにエクスプロイトや悪意のあるコードが含まれていないかどうかなど、パケットについての重要な詳細を特定することができます。個々のパケットの分析だけでなく、複数のパケットの到着順序およびシーケンスによって提供されるコンテキストの分析も行い、回避手法を捕捉して阻止します。これらすべての処理が 1 回のスキャンで実行されるため、ネットワーク トラフィックの速度は望ましい速度を維持します。

侵入防御機能を活用

脅威ベースの防御機能によって、ネットワーク層とアプリケーション層の両方でエクスプロイトの試みと回避手法 (ポート スキャン、バッファ オーバーフロー、リモート コード実行、プロトコル フラグメンテーション、隠匿など) が検出され、ブロックされます。シグネチャ マッチングと異常検出に基づく防御が適用され、プロトコルのデコードと分析が行われます。そして、分析から得られた情報に基づいてアラートが送信され、悪意のあるトラフィック パターンがブロックされます。ステートフル パターン マッチングにより、複数のパケットにわたる攻撃が検出されます。この検出では、パケットの到着順序とシーケンスが考慮され、許可するすべてのトラフィックについて、それが善意のものであり、回避手法が使われていないことが確認されます。弊社の侵入防御テクノロジには次の機能があります。

- **プロトコル デコーダベースの分析**：プロトコルに対してステートフルなデコードを実行し、その後、ネットワークとアプリケーションのエクスプロイトを検出するシグネチャをインテリジェントに適用します。
- **プロトコル異常ベースの防御**：長すぎる URI や FTP ログインなど、RFC 非準拠のプロトコルの使用を検出します。
- **設定が容易なカスタムの脆弱性シグネチャ**：ネットワーク固有のニーズに合わせて侵入防御機能を調整できます。

1 つの脆弱性に対してエクスプロイトの方法は複数あるため、弊社では、脆弱性自体に基づいて侵入防御シグネチャを構築することによって、さまざまなエクスプロイトに対してより徹底した防御を行えるようにしています。1 つのシグネチャによって、システムまたはアプリケーションの既知の 1 つの脆弱性に対する複数のエクスプロイト試行を阻止することができます。

カスタムのシグネチャで新たな脅威に対処

Threat Prevention では、Snort および Suricata ルールの変換の柔軟なサポートも提供しているため、新たに検出された脆弱性に対して迅速に防御できます。このサポートと継続的なカスタム シグネチャ開発によって、スタンドアロン IPS または IDS ソリューションの必要性が完全に排除されるとともに、IPS の主要ユース ケースの 1 つとその根底にある目標に対処できます。つまり、未確認または新たな脆弱性に対して、確認済みの更新を組織のソフトウェアおよびアプリケーションのすべてに導入できるようになるまでの暫定的な対策として、この脆弱性に対応したシグネチャを適用することができます。変換のサポートによって、Snort や Suricata のルールの変換、サニタイズ、アップロード、管理を自動的に実行できるため、従来のシグネチャベースの IPS テクノロジで必要となる時間と労力を削減しながら、インテリジェンスのフィードを活用できます。公開された API を活用して、新たな Snort ルールの対応範囲を環境全体に適用するプロセスを自動化できます。

マルウェア防御

インラインのマルウェア防御では、ハッシュではなくペイロードに基づくシグネチャを使用して、マルウェアが標的のホストに到達する前にブロックされます。この防御では、既知のマルウェアだけでなく、まだ Web に出回っていないものも含む将来の亜種も検出対象に含まれます。弊社のストリームベースのスキャン エンジンは、大幅な遅延を伴うことなくお客様のネットワークを保護します。プロキシベースのスキャン エンジンに頼るネットワーク アンチウイルス製品では、こうした遅延が重大な欠点となっています。ストリームベースのスキャンでは、ファイルの最初のパケットの受信時に直ちにトラフィックが検査されるため、脅威が排除されるだけでなく、従来のスタンドアロン ソリューションに関連するパフォーマンスの問題が解消されます。アンチマルウェアの主要機能には以下のものがあります。

- 圧縮ファイルや Web コンテンツ内にひそむマルウェアに対する**インラインのストリームベースの検出と防御**
- Office/Microsoft 365™ドキュメントや PDF などの一般的なファイル タイプ**内の隠れたペイロードに対する防御**
- **WildFire からの更新**による、ゼロデイ マルウェアに対する確実な防御

パロアルトネットワークスが収集した何十億ものサンプルから、あらゆるタイプのマルウェアのシグネチャが直接生成されます。これらのサンプルには、WildFire や、弊社の Unit 42 脅威リサーチ チーム、および世界中のサードパーティのリサーチおよびテクノロジ パートナーに送信された未知のマルウェアなどが含まれます。

ペイロードベースのシグネチャとハッシュベースのシグネチャ

ペイロードに基づくシグネチャでは、ファイルの本文のパターンが検出されます。今後作成されるこのファイルの変種でファイルの内容が若干変更されていても、このパターンを使って、変種を特定することができます。そのため、従来の方法では新たな未知のファイルとして扱われるポリモーフィック型マルウェアを直ちに特定し、ブロックすることが可能です。

ハッシュに基づくシグネチャでは、個々のファイル固有の固定されたエンコーディングに対してマッチングが行われます。ファイルのハッシュ値は容易に変更されるため、ハッシュベースのシグネチャは、ポリモーフィック型マルウェアや、同一ファイルの亜種の検出には効果がありません。

WildFire との統合

ゼロデイ マルウェアと C2 攻撃に対する防御を、業界最先端の分析および防御エンジンである WildFire サービスで拡張することによって、高度な回避性を備えたゼロデイ マルウェアやエクスプロイトに対処できます。クラウドベースのこのサービスでは、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、ベア メタル分析を組み合わせた独自の

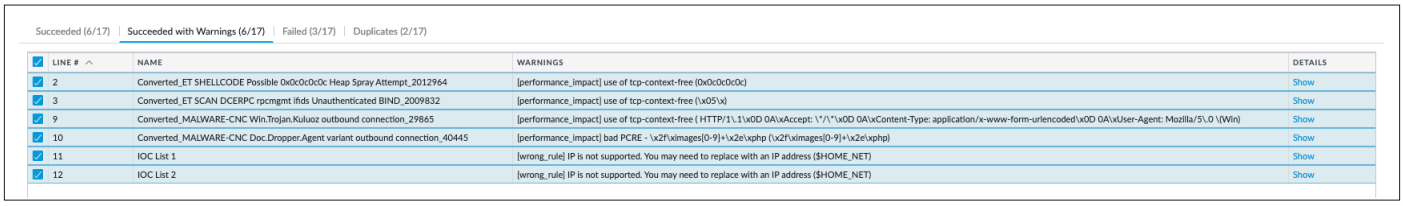

図 1: PAN-OS® での Snort のサポート

多手法アプローチを採用しており、回避性がきわめて高い脅威でも検出し、阻止することが可能です。脅威が特定されると、Threat Prevention は、フォーム ファクタを問わず機械学習を活用したすべての NGFW に、リアルタイムで判定を適用し、企業環境全体で脅威の増殖を即座に阻止します。

コマンド アンド コントロールに対する防御

ネットワークへのあらゆる脅威の侵入を防止する特効薬というものはありません。最初の感染後、攻撃者は C2 チャネル経由でホスト マシンと通信し、ここから追加のマルウェアを引き出し、さらなる指令を発行してデータを盗みます。弊社の C2 防御では、このような不正な通信チャネルに焦点を定め、悪意のあるドメインに対するアウトバウンド要求や、感染したデバイスにインストールされた既知の C2 ツールキットからのアウトバウンド要求をブロックすることによって通信を遮断します。

パロアルトネットワークスは、URL とドメインに基づく C2 シグネチャの標準的な自動化を超える機能を提供しています。弊社では、WildFire で観測された悪意のあるトラフィックに基づいて、リサーチャーグレードの C2 シグネチャをマシンの速度とスケールで自動生成し、配信しています。このシグネチャはペイロードに基づいているため、C2 ホストが未知のものでも、また急速に変化していても、C2 トラフィックを検出できます。さらに、DNS セキュリティ サブスクリプションによって、C2 防御全体を拡張することもできます。このサブスクリプションでは、DNS トンネリング戦術を使って C2 チャネルを隠そうとする攻撃者の試みを打破できます。

攻撃対象領域の縮小

Threat Prevention と、パロアルトネットワークスのクラウド提供セキュリティ サブスクリプションの追加機能は、機械学習を活用した NGFW に組み込まれている防御を重視した機能とシームレスに連携することによって、お客様の組織の攻撃対象領域を大幅に縮小し、関連するビジネスリスクを軽減します。このセクションでは、補完的なテクノロジの例をいくつか紹介します。

SSL 復号化

エンタープライズ ネットワーク トラフィックの大半は、暗号化されています。これらのトラフィックを復号化し、スキャンして、脅威が含まれていないか調べないことには、ネットワークの防御上、大きな抜け穴ができてしまいます。弊社のプラットフォームに組み込まれた SSL 復号化サービスでは、インバウンドとアウトバウンドの SSL トラフィックを選択的に復号化することができます。復号化後、すべてのトラフィックが完全に検査されます。安全であることが確認されると、トラフィックは再び暗号化され、通過を許可されて宛先に送られます。

ファイル ブロック

実行可能ファイルは、スピア フィッシング攻撃で使用される悪意のあるファイルの中で大きな割合を占めており、従業員の不注意は主要セキュリティ リスクの 1 つと見なされています。これは、多くの従業員が安全なファイルと危険なファイルを見分けられない可能性があるためです。実行可能ファイルなど、マルウェアの仕込みに使われることが判明している危険なファイル タイプのネットワークへの侵入を阻止することによって、マルウェア感染の発生リスクを抑えてください。ファイル ブロック機能を User-ID と組み合わせることで、ユーザーの業務内容に基づいて不要なファイルなブロックできます。すべてのユーザーがそれぞれ必要とするファイルにアクセスできるようにしながら、組織の要件に基づいて、リスクへの暴露を詳細に制御することが可能です。また、すべての許可ファイルを WildFire に送信して分析し、ゼロデイ マルウェアが含まれていないか調べることによって、攻撃の機会をさらに減らすことができます。

ドライブバイ ダウンロード防御

無防備なユーザーがお気に入りの Web サイトにアクセスしただけで、知らぬ間にマルウェアがダウンロードされてしまうことがあります。サイトの所有者も、自分のサイトが侵害されていることに気づいていない場合があります。弊社の Threat Prevention テクノロジは、潜在的に危険なダウンロードを特定し、ユーザーに警告を送信して、そのダウンロードがユーザー自身が意図し承認したものであることを確認します。Threat Prevention 内で、検出されたこのような「フィッシング キット」ランディング ページや Web シェル ファイル (Web サーバのリモート管理を可能にして他の内部システムを標的とすることを狙ったもの) はスパイウェア シグネチャとしてパッケージ化され、配信されます。この防御機能を URL Filtering およびファイル ブロックのポリシーと関連付けることによって、これらの機能を拡張して新たなドメインや急速に変化するドメインからの攻撃を阻止できます。

脅威を容易かつ正確に軽減

DNS Sinkhole

ファイアウォールがローカル DNS サーバよりもインターネット側にある通常の導入環境では、脅威ログには、実際に感染したホストではなくローカル DNS リゾルバがトラフィックの送信元として示されます。その結果、ファイアウォールからは、感染したクライアントの DNS クエリ (DNS クエリの発信元) が見えません。Threat Prevention 内の DNS Sinkhole 機能は、この可視性の問題を解決してデータの漏えいを防ぎ、被害を受けたクライアントを正確に特定します。悪意のあるドメインや IP アドレスに対するアウトバウンド要求が、ネットワークの内部 IP アドレスのいずれかにリダイレクトされるように、シンクホールを設定できます。この設定によって、このような要求はネットワークから出られなくなり、C2 通信が効果的にブロックされます。

自動相関オブジェクト

弊社の Threat Prevention テクノロジとログは、パロアルトネットワークスのファイアウォールと Panorama のアラート機能への強力な追加機能である自動相関エンジンにデータを供給します。このエンジンは関連性のある一連の脅威イベント (Threat Prevention ログ内のイベントなど) を相関させます。これらのイベントが組み合わされることで、ネットワーク上で攻撃が行われている可能性があることが示されます。ネットワーク上の侵害されたホストなどのリスク領域が特定されるため、対応が可能なアラートの短いリストに集中して取り組み、リスクを評価し、対応措置を実行してネットワーク リソースの悪用を防止できます。相関オブジェクトでは、Unit 42 の脅威リサーチに加えて、WildFire の未知の脅威分析と User-ID が活用され、トラフィックの異常やセキュリティ侵害の兆候 (IOC) の相関付けが行われます。この機能を通じて、ネットワーク上の感染デバイスを迅速かつ正確に特定できます。

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。Threat Prevention 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。

- **WildFire®**: 業界をリードするクラウドベースの分析により、多くの場合数秒で、未知のマルウェアを自動的に検出し、阻止することによって、ファイルの安全性を保証します。
- **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 C2 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。

運用上のメリット

Threat Prevention サブスクリプションによって、以下のことが可能です。

- **すべてのデータ、アプリケーション、およびユーザーに対する包括的なセキュリティの確保**。すべてのトラフィックをスキャンするとともに、アプリケーションおよびユーザーに関する完全なコンテキストを提供します。
- **セキュリティの自動化による手作業の削減**。新たな脅威に対応した自動更新を取得します。
- **Snort シグネチャの導入**。Snort および Suricata のルールの変換、サニタイズ、アップロード、管理を自動化して、新たな脅威を検出し、インテリジェンスを活用します。
- **ポリシーベースの詳細な制御による、ネットワークのセキュリティの維持**。悪意のあるコンテンツを単にブロックするだけではなく、特定のファイル タイプを制御して、組織全体のリスクを軽減します。
- **C2 リスクの遮断**。マシンのスケールと速度で C2 シグネチャを自動生成します。

表 1: PA-Series での Threat Prevention のスループット

モデル	脅威スループット
PA-200	50 Mbps
PA-500	100 Mbps
PA-2020	200 Mbps
PA-2050	500 Mbps
PA-3020	1 Gbps
PA-3050	2 Gbps
PA-3060	2 Gbps
PA-5020	2 Gbps
PA-5050	5 Gbps
PA-5060	10 Gbps
PA-7050	100 Gbps
PA-7080	180 Gbps

表 2: プライバシーとライセンスの概要

Threat Prevention サブスクリプションでのプライバシー	
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。
ライセンスと要件	
要件	Threat Prevention サブスクリプションをご利用になるには、PAN-OS を実行する Palo Alto Networks Next-Generation Firewall が必要です。
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、エクスプロイト、マルウェア、スパイウェア、C2、URL などを含むネットワーク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。
Threat Prevention ライセンス	Threat Prevention 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。

〒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

threat-prevention-ds-061220