ファイアウォールの概要

Palo Alto Networks Next-Generation Firewall

アプリケーションの使い方やユーザーの行動、そして複雑なネットワーク インフラストラクチャの根本的な変化が進んでいる現在、それらに起因した新たな脅威として、従来のポートベースのネットワーク セキュリティに対する脆弱性が顕在化しています。ユーザーである組織のメンバーは多様なデバイスを利用して、数多くのアプリケーションを使用したいと考えていますが、ビジネス リスクやセキュリティ リスクに対する考慮がなされることはほとんどありません。一方でそれを管理する側にとっては、データセンターの拡張、ネットワークのセグメント化、仮想化、モビリティ イニシアチブを推進する上で、従来のセキュリティ メカニズムを巧みに回避する、より巧妙になった新たな高度な脅威からネットワークを保護しなければならない上に、アプリケーションやデータへのアクセスに対する許可のあり方についても再考を迫られています。

ネットワーク セキュリティの考え方には、歴史的に 2 つの選択肢がありました。ネットワーク セキュリティを優先してすべてをブロックするか、あるいはビジネスを優先してすべてを許可するか、です。どちらを選択するにせよ、そこには妥協の余地はほとんどありませんでした。Palo Alto Networks® Next-Generation Security Platform は、サイバーセキュリティの脅威を阻止しながらアクセスを許可することで、ユーザーが必要とするアプリケーションの安全な運用を実現することができます。

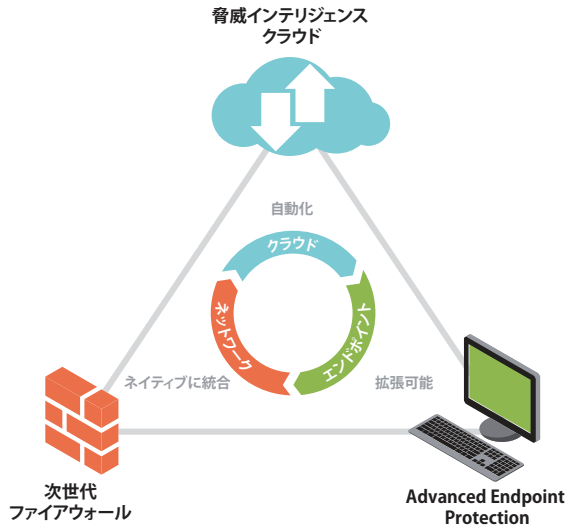

図 1: Palo Alto Networks Next-Generation Security Platform

この次世代セキュリティ プラットフォームの中核を担っているのが、現在の非常に巧妙な脅威にも対処できるように一から設計されたパロアルトネットワークスの次世代ファイアウォールです。次世代ファイアウォールは、場所やデバイスの種類に関係なく、アプリケーション、脅威、およびコンテンツを含むすべてのトラフィックを検査し、安全なトラフィックをユーザーに導きます。アプリケーション、コンテンツ、およびユーザー (いずれも事業活動に欠かせない要素) はエンタープライズ セキュリティ ポリシーの設定に不可欠な要素になっています。その結果、重要なビジネス イニシアチブに合わせてセキュリティを導入することができます。弊社の次世代セキュリティ プラットフォームを使用すると、インシデントに対する応答時間を短縮し、未知の脅威を検出し、セキュリティ ネットワークの導入を合理化できます。

- すべてのトラフィックの分類、ビジネス ユース ケースの特定、およびポリシーの割り当てにより、Software as a Service (SaaS) などの関連するアプリケーションへのアクセスを許可および保護することで、アプリケーション、ユーザー、およびコンテンツを安全に有効化。
- 好ましくないアプリケーションを排除することで、潜在的な脅威を阻止。また、標的を絞ったセキュリティ ポリシーを適用することで既知の脆弱性を利用したエクスプロイト、ウイルス、スパイウェア、ボットネット、および未知のマルウェア (APT) をブロック。
- アプリケーションの検証、データの分離、不正なアプリケーションの制御、および高速な脅威防御によるデータセンターの保護。
- 可視性と制御能力を高めてパブリックおよびプライベート クラウド コンピューティング環境を保護。また、仮想マシンの管理と同様にハードウェアに依存することなく、セキュリティ ポリシーを実行およびメンテナンス。

- 場所に関係なくユーザーやデバイスに次世代セキュリティ プラットフォームを拡張することにより、安全なモバイル コンピューティングを導入。
- 組織の構造に合わせるために、直観的な管理機能を使用してデバイス、ネットワーク、ポリシー管理を合理化。

次世代セキュリティ プラットフォームは、組織が求める一般的な広範にわたるセキュリティ要件に対処するのに非常に効果的です。ネットワーク セキュリティに対するグローバルな脅威インテリジェンスとエンドポイントの防御をバランスよく組み合わせることで、全体的なセキュリティ体制を強化し、またセキュリティ インシデントへの応答時間を短縮しながら、ビジネス イニシアチブをサポートすることができます。

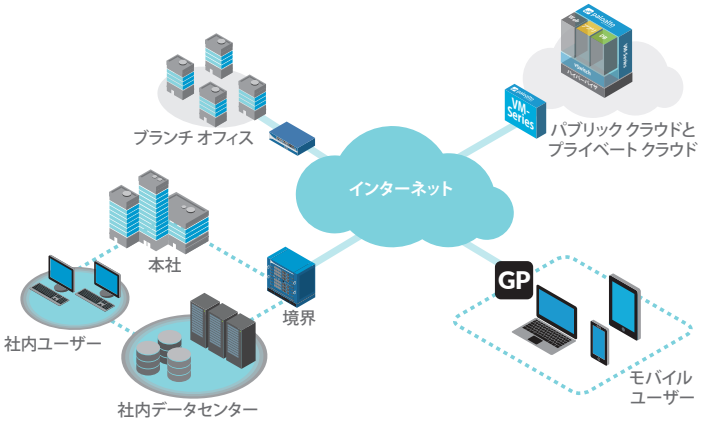

図 1: 全社にわたって安全な使用許可ポリシーを展開

セキュリティを活用してビジネスをパワーアップ

パロアルトネットワークスの次世代セキュリティ プラットフォームの導入により、アプリケーション、ユーザー、およびコンテンツを意識したポリシーを展開してビジネスをより強力に推進することが可能になります。パロアルトネットワークス セキュリティ プラットフォームに特有のデザインであるポジティブ制御モデルを通じて、特定のアプリケーションまたは機能を有効にし、それ以外は (明示的または暗黙的に) すべてブロックすることができます。次世代ファイアウォールは、すべてのポート間のすべてのトラフィックに対してフルスタックのシングル パス インスペクションを実行します。これにより、セキュリティ ポリシーを決定するための基準として、アプリケーション、関連するコンテンツ、およびユーザー ID の完全なコンテキストを提供します。

- 常時、全ポートの全トラフィックを分類。現在、アプリケーションとその関連コンテンツは、さまざまなテクニックを用いてポート ベース ファイアウォールを容易に迂回することができます。パロアルトネットワークスの次世代セキュリティ プラットフォームでは、トラフィック ストリームに対して複数の分類メカニズムを適用し、正規のアプリケーション、脅威、マルウェアを識別します。使用されているポート、暗号化 (SSL または SSH) の分類、または回避テクニックが何であっても、すべてのトラフィックが分類されます。未確認のアプリケーション (一般にはトラフィックの中で小さな割合であるものの、潜在的なリスクは高い) も自動的に分類され、体系的に管理されます。
- 脅威の及ぶ範囲を小さくしてサイバー攻撃を防止。トラフィックの完全な分類が終了したら、特定のアプリケーションを許可してそれ以外はすべて拒否することにより、ネットワーク脅威フットプリントを削減することができます。組織的なサイバー攻撃には、既知のマルウェア サイトをブロックし、脆弱性エクスプロイト、ウイルス、スパイウェア、および悪意のある DNS クエリを阻止することで防御することができます。バーチャル サンドボックス環境でファイルを実行し、悪意ある動作を直接監視することで、カスタムまたは未知のマルウェアを分析し識別します。新しいマルウェアが発見されると、感染ファイルと関連するマルウェア トラフィックのシグネチャが自動的に生成され配信されます。
- アプリケーション トラフィックとユーザーやデバイスに関連した脅威をマッピング。セキュリティ体制を強化し、インシデントへの応答時間を短縮するためには、アプリケーションの使用状況をユーザーやデバイスの種類にマッピングする

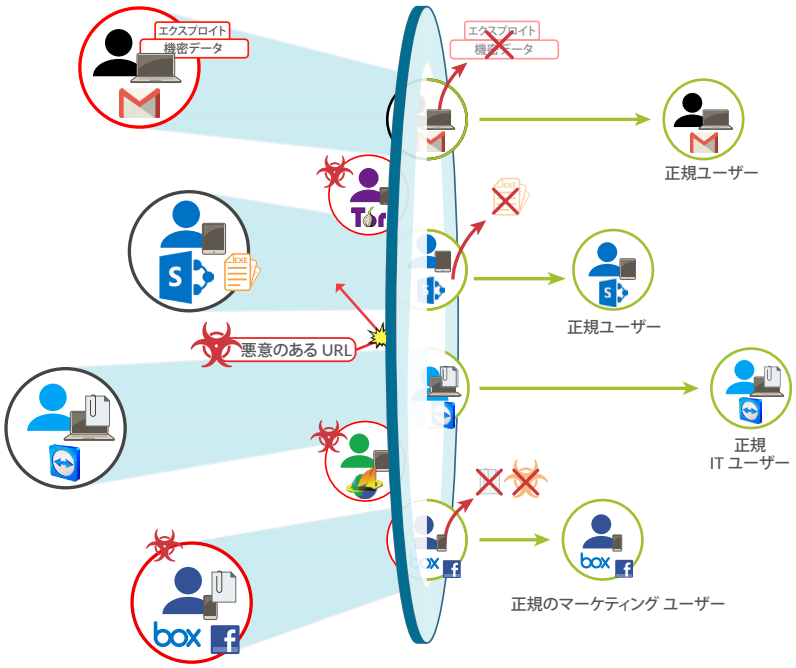

図 2: アプリケーション、コンテンツ、ユーザー、デバイス – すべて制御

図 3: アプリケーション アクティビティを明確でわかりやすい形式で表示。
フィルタの追加および削除で、アプリケーション、機能、利用者の詳細情報を把握できます。

とともに、そのコンテキストをセキュリティ ポリシーに適用できるようにすることが極めて重要になります。エンタープライズ ユーザー リポジトリの幅広い統合を通じて、アプリケーションにアクセスする Microsoft® Windows®、Mac® OS X®、Linux®、Android®、または iOS ユーザーおよびデバイスの ID が提供されます。ユーザーとデバイスの両方に対する卓越した可視性と制御機能が装備されているため、ユーザーがどこにいても、また使用しているデバイスの種類が何であっても、ネットワーク上を行き来する任意のアプリケーションの使用を安全に許可することができます。

使用されている特定のアプリケーション、それを経由して侵入される恐れのあるコンテンツや脅威、そして関連するユーザーやデバイス — それら全体のコンテキストを確立することで、ポリシー管理の効率アップ、セキュリティ体制の強化、およびインシデントの迅速な調査が可能になります。

完全なコンテキストの確立によって実現するより緊密なセキュリティ ポリシー

セキュリティのベスト プラクティスでは、ポリシーについての意思決定、ネットワーク活動についてのレポート機能、およびフォレンジック キャパシティがコンテキストに基づいていることが要求されます。使用中のアプリケーション、アクセスされた Web サイト、関連するペイロード、そしてユーザー — それら全体の関係性を意味するコンテキストは、すべてのネットワークを保護するための貴重なデータ ポイントとなります。どのアプリケーションが自社のインターネット ゲートウェイを通過しているのか、どれがデータセンター内で動作してどれがクラウド環境で動作しているのか、あるいはリモート ユーザーが使用しているのはどれかを正確に把握した上で、特定のポリシーをそれらのアプリケーションに適用して、組織的な脅威防御を運用することができます。IP アドレスだけでなくユーザー単位で動きを把握することで、関係性に新たな要素が増え、ポリシーの割り当てをよりきめ細かく行うことが可能になります。

極めてインタラクティブな可視化とログ フィルタリング機能を装備した充実したツール セットにより、アプリケーション アクティビティ、関連するコンテンツや脅威、ユーザーの身元、およびデバイスの種類に関するコンテキストを明らかにすることができます。これらのデータ ポイントはそれぞれネットワークの各部分を描画できますが、完全なコンテキストがそろった場合は潜在的なセキュリティ リスクの完全なビューが表示され、より多くの情報に基づいて意思決定を下すことが可能になります。すべてのトラフィックは絶え間なく分類されます。その状態の変化に応じて分析用として変更がログ記録されます。また、グラフィカル サマリーは動的に更新され、簡単に使用できる Web ベースのインターフェイスにより情報を表示することができます。

- インターネット ゲートウェイにおいて、新しいアプリケーションや未知のアプリケーションを調査し、アプリケーション、その動作特性、およびそれを使用しているユーザーの身元についての説明を迅速に表示できます。URL カテゴリ、脅威、およびデータ パターンへの可視性をさらに高めることで、ゲートウェイを通過するネットワーク トラフィックの全体像が一段と鮮明になります。
- WildFire™により未知のマルウェアについて分析された結果はすべて記録され、使用されたアプリケーション、ユーザー、ファイルの種類、標的の OS、観察された悪意のある活動などの詳細情報に完全にアクセスできます。
- データセンター内において、使用されているすべてのアプリケーションを検証し、許可されているユーザー以外にそれらのアプリケーションが使用されていないことを確認します。データセンターへの可視性を高めることで、アプリケーションの設定の誤りや、SSH や RDP の使用に問題がないことを確認することができます。
- 脅威分析、フォレンジック、捕捉のワークフローは、AutoFocus™脅威インテリジェンス サービスによって加速され、デバイスから PAN-OS® に固有のコンテキストに関する脅威データを直接提供します。
- パブリックおよびプライベート クラウド環境において、次世代セキュリティ プラットフォームでポリシーの施行とアプリケーションの保護を実行しつつ、仮想サーバの作成と移動にタイムリーに対応します。
- あらゆる導入シナリオにおいても、分析と体系的な管理を目的として未知のアプリケーション (どのネットワークにおいても一般的に小さな割合) をカテゴライズすることができます。

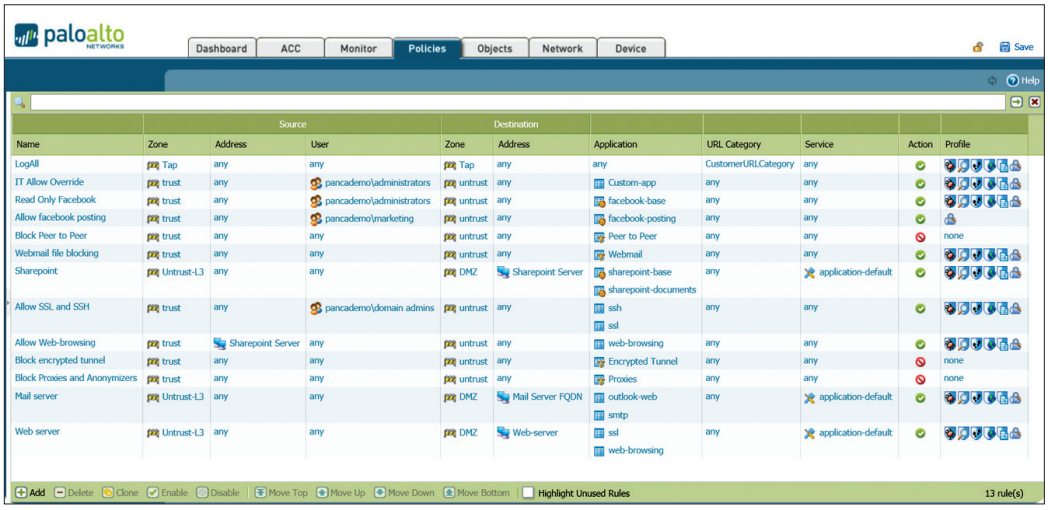

図 4: 統合ポリシー エディタにより、アプリケーション、ユーザー、およびコンテンツを制御するポリシーの迅速な作成と導入を実現

多くの場合、どのアプリケーションが使用されているか、またそれが誰によって、どれくらい頻繁に使用されているかを完全には把握できないことがあります。ネットワーク トラフィックがビジネスにどう関係しているのか、そうした側面を完全に把握できるようにすることが、より多くの情報に基づくセキュリティ ポリシー制御を実現するための最初のステップとなります。

アプリケーションの安全な使用許可を通じてリスクを緩和

従来、リスクを軽減させるプロセスとはネットワーク サービスへのアクセスを制限することにほかならず、ビジネスを妨げる恐れがありました。現在では、リスクの軽減とは、従来の「すべて拒否する」アプローチと「すべて許可する」アプローチの間で適切なバランスをとるビジネス中心のアプローチを用いたアプリケーションの安全な使用許可を意味します。

- アプリケーション グループと SSL 暗号解読を用いて Web メールとインスタント メッセージングを少数の特定のアプリケーションに限定します。そしてそれらのアプリケーションに対してあらゆる脅威がないか検査し、未知の疑わしいファイル (EXE、DLL、ZIP ファイル、PDF ドキュメント、Office ドキュメント、Java®、および Android® APK) を WildFire にアップロードし、分析およびシグネチャ作成を行います。
- 業務関連の Web サイトへのトラフィックは許可およびスキャニングし、業務に無関係な Web サイトへのアクセスはブロックすることで、全ユーザーに対する Web サーフィンをコントロールします。また、カスタマイズされたブロックされたページを通じて、疑わしいサイトにアクセスしようとすると「指導」が行われます。
- 全ユーザーに対してすべてのピアツーピア ファイル転送アプリケーションを、ダイナミック アプリケーション フィルタを用いて明確にブロックします。
- 組織内での SaaS アプリケーションの使用状況を把握し、各アプリケーションに対する細やかなアクセス制御と使用制御を設定し、これらのアプリケーションを通じたマルウェアの配信を防ぎます。
- インターネット ゲートウェイ ポリシーと threat prevention の各種機能を GlobalProtect™モバイル セキュリティ サービスによってリモート ユーザーまで拡大することにより、モバイル デバイスまでカバーします。

データセンターではコンテキストを用いて、データセンター アプリケーションが標準ポート上で実行されていることの確認や、不正なアプリケーションの検出、ユーザーの検証、データの分離、脅威からのビジネスクリティカルなデータの保護を実行します。例を以下に示します。

- セキュリティ ゾーンを使用して、Oracle® ベースのクレジット カード番号リポジトリを分離します。これにより、Oracle トラフィックを標準ポート間に制限すると同時に、インバウンドの脅威がないかどうかトラフィックを検査したり、財務部門だけにアクセスを限定することができます。
- IT 部門だけがデータセンター内で使用するためのリモート管理アプリケーション グループ (たとえば SSH、RDP、Telnet) を作成します。
- 仮想データセンターにおいて、SharePoint® 仮想マシンの設置、撤去、または仮想環境内での移動を行った場合に、ダイナミック オブジェクトを用いてセキュリティ ポリシーを自動生成します。

許可されたアプリケーションとコンテンツを保護

脅威防御およびコンテンツ スキャン ポリシーを適用する場合、アプリケーションとユーザーのコンテキストがセキュリティ ポリシーの不可欠な構成要素となります。脅威防御ポリシーに含まれる完全なコンテキストを通じて、ポート ホッピングやトンネリングなどの回避戦術を無効にすることができます。アプリケーションを厳選して許可することで脅威の対象領域を縮小し、続いて脅威防御およびコンテンツ スキャン ポリシーをそのトラフィックに適用します。

ポリシーで利用可能な脅威防御およびコンテンツ スキャン要素として次の機能があります。

- **IPS およびネットワーク アンチウイルス / アンチスパイウェアを用いて既知の脅威を阻止。**統一されたシグネチャ フォーマットとストリーム ベースのスキャン エンジンを用いたシングル パス インスペクションによって、幅広い既知の脅威に対する防御を実現します。侵入防御システム (IPS) は、ネットワークおよびアプリケーション レイヤーの脆弱性エクスプロイト、バッファ オーバーフロー、DoS 攻撃、およびポート スキャンを防止する機能を備えています。アンチウイルス / アンチスパイウェアは、既知の PDF ウイルスはもちろん、圧縮ファイルや Web トラフィック (HTTP/HTTPS 圧縮) に潜む数百万のマルウェアの亜種をブロックします。SSL で暗号化されたトラフィックの場合、ポートとは無関係に、ポリシー ベースの暗号解読を選択的に適用してから、脅威がないかどうかトラフィックを検査することができます。

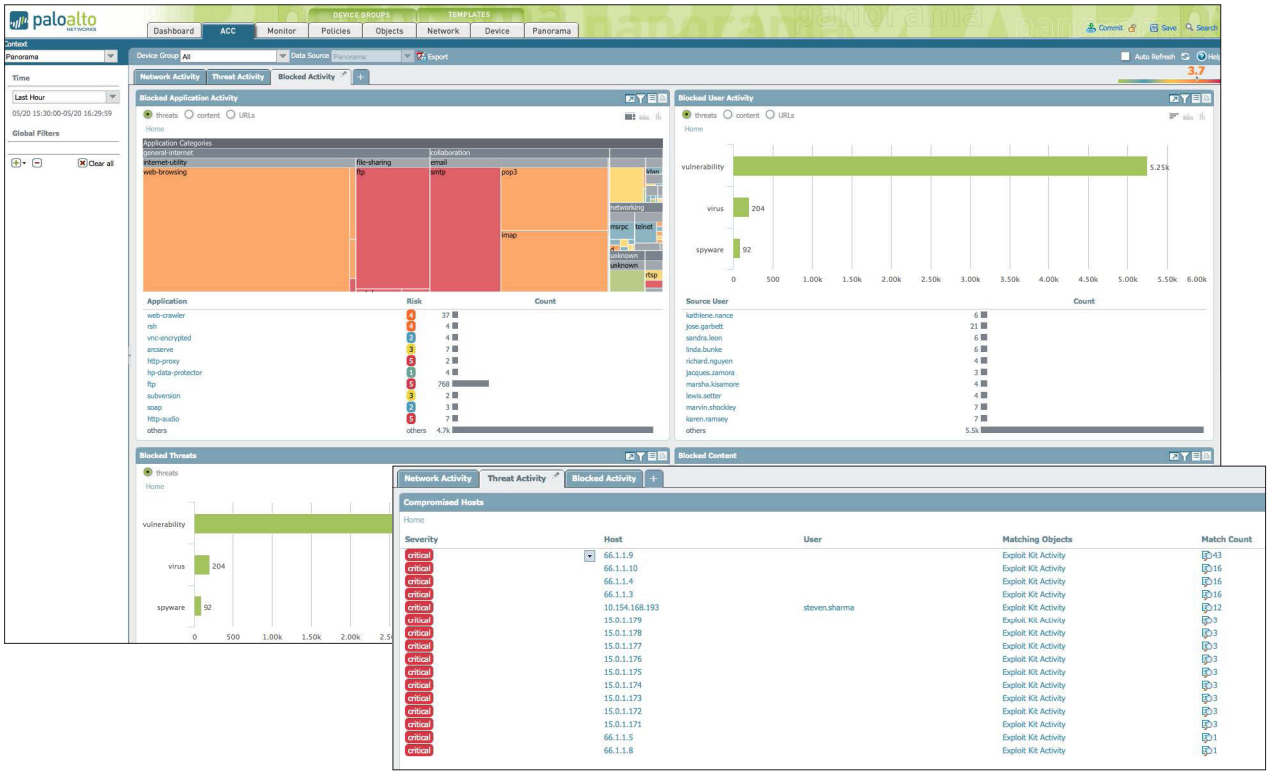

図 5: コンテンツと脅威の可視化 – URL、脅威、およびファイル / データ転送アクティビティに加え、侵入されたホストをカスタマイズ性に優れた明確でわかりやすい形式で表示。フィルタを追加および削除して、個々のエレメントの詳細情報を把握できます

- **WildFire で未知または標的型マルウェアをブロック。**WildFire によって、複数のオペレーティング システムやアプリケーション バージョンにわたってファイル内に潜む未知または標的型のマルウェア (たとえば APT 攻撃) を識別および分析することができます。WildFire は、クラウドまたは WF-500 アプライアンスの仮想サンドボックス環境において未知のファイルを観察および実行する機能を提供します。WildFire は 420 を超える悪意のある動作を監視し、マルウェアが発見されるとわずか 5 分で自動的にシグネチャを開発してユーザーに配信します。WildFire では次のような主要なすべての種類のファイルがサポートされます。PE ファイル、Microsoft Office (.doc、.xls、および .ppt)、PDF、Java アプレット (jar および class)、Android アプリケーション パッケージ (APK)。また、WildFire はメールに含まれるリンクを分析してスピアフィッシング攻撃を阻止します。
- **ボットに感染したホストを特定し、マルウェアによるネットワーク活動を阻止。**多くの場合、未知のトラフィックを含め、全ポートにわたりすべてのアプリケーションを関係性に基づいて分類をすることで、ネットワークにおける異常や脅威を明らかにすることができます。コマンド & コントロール App-ID™、ボットネットの振る舞いレポート、DNS Sinkhole、およびパッシブ DNS により、未知のトラフィック、疑わしい DNS、および URL クエリを感染したホストと迅速に関連付けます。グローバル インテリジェンスを適用し、悪意のあるドメインに対するシンクホール DNS クエリを捕捉します。
- **ファイルとデータの不正な転送を制限。**データ フィルタリング機能により、管理者はポリシーを実装して、許可されていないファイルやデータの転送に伴うリスクを軽減することができます。ファイルの拡張子だけを見て判断するのではなくファイルの中身を調べることで、ファイル転送をコントロールし、転送操作が許可されているかを判断することができます。ドライブバイ ダウンロード攻撃でよく見受けられる実行ファイルをブロックできるため、目に見えないマルウェアの拡散からネットワークを保護することが可能です。データ フィルタリング機能を通じて、機密データ パターン (クレジットカード番号や社会保障番号、またはカスタム パターン) のフローを検出してコントロールすることもできます。
- **Web サーフィンを制御。**完全に統合されたカスタマイズ可能な URL フィルタリング エンジンによって、管理者はきめ細かい Web ブラウジング ポリシーを適用でき、アプリケーションの可視性と制御ポリシーを補完し、法令や規制、および生産性に伴うあらゆるリスクから企業を保護します。
- **アプリケーション アクセスに対するデバイス ベース ポリシー。**GlobalProtect を使用すると、特定のアプリケーションやネットワーク リソースにアクセスできるデバイスの制御ポリシーを設定することができます。たとえば、ノート PC から、データセンターへのアクセスを許可する前に、企業のセキュリティ ポリシーに準拠していることを確認してください。機密データにアクセスする前に、モバイル デバイスが最新の状態にあるか、企業の所有物であるか、そしてパッチが完全に適用されているかどうかを確認します。
- **侵入されたホストを自動的に確認。**自動相関エンジンは、ネットワーク全体について事前に定義したセキュリティ侵害の兆候がないか探り、兆候に一致したものを関連付け、侵入されたホストを自動的に検出して明らかにします。そのため、手動でデータ マイニングを行う必要はありません。

ネットワーク セキュリティ管理

次世代セキュリティ プラットフォームは、コマンドライン インターフェイス (CLI) を介して、または、全機能装備のブラウザベースのインターフェイスを介して個別に管理することができます。大規模導入環境の場合、Panorama™を用いることで、ハードウェア ファイアウォールとバーチャル アプライアンス

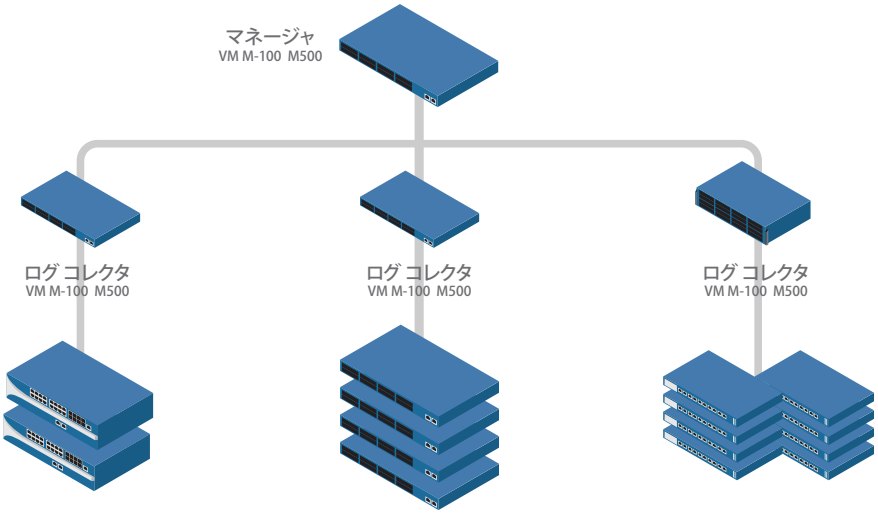

図 6: Panorama は、専用アプライアンスで導入することも、あるいは分散型で導入し拡張性を最大化することも可能

ファイアウォールのすべてに対して可視性、ポリシー編集、レポート作成、ログ記録の各機能をグローバルに提供することができます。Panorama は、1 台のアプライアンスとまったく同じレベルのコンテキスト制御をグローバルな導入環境に提供します。

ロールベースの管理をプレルールおよびポストルールと組み合わせることにより、柔軟なローカル ポリシー編集やデバイス設定の必要性と一元的な管理とのバランスを適切に取ることが可能となります。デバイスの Web インターフェイスと Panorama インターフェイスのいずれを使用しても、ルック & フィールはまったく同じであるため、一方から他方に切り換えた場合でもとまどうことはありません。管理者は標準のインターフェイスを用いて、同期の問題を心配することなくポリシーの変更を行うことができます。SNMP などの標準ベースのツールや REST ベースの API が追加サポートされているため、サードパーティ製の管理ツールと統合することもできます。

レポートとログ記録

セキュリティのベスト プラクティスとは、継続的な管理と事後対応の措置の両立を意味し、セキュリティ インシデントの調査と分析、そして日々のレポート生成も含まれます。

- **レポート :** 特定の要件に合わせて、事前定義済みレポートをそのまま使用することも、カスタマイズすることも、1 つのレポートにまとめることもできます。レポートはすべて CSV 形式または PDF 形式にエクスポートすることができ、スケジュールどおりに実行したり、電子メールで送信することもできます。
- **ログ記録 :** リアルタイムのログ フィルタリングにより、ネットワークを通過するすべてのセッションに対するフォレンジック調査が迅速かつ容易に行えます。フィルタの基準として、アプリケーション、WildFire が検出したマルウェアを含めたコンテンツ、およびユーザーに関する完全なコンテキストを使用することができます。またその結果を、オフラインでのアーカイブや詳細な分析を目的として、CSV ファイルにエクスポートしたり、syslog サーバに送信することもできます。Panorama が収集したログも同様に syslog サーバに送信し、アーカイブや、詳細な分析に役立てることができます。
- **脅威の捕捉 :** AutoFocus サービスの脅威インテリジェンスは、PAN-OS で直接使用できます。それにより、他の特殊なリソースを使用することなく、脅威分析ワークフローと捕捉ワークフローを高速化できます。さらに分析が必要な場合は、ユーザーは、AutoFocus と PAN-OS に対して事前入力されている検索を使用して、この 2 つのシステム間で一括処理を実行できます。

Palo Alto Networks Next-Generation Security Platform に搭載されているレポートやログ機能に加えて、Splunk® for Palo Alto Networks などのサードパーティ製 SIEM ツールとの統合が可能です。これらのツールはレポートやデータの可視化機能を強化するもので、これによって全社規模における多数のシステムにわたるセキュリティ イベントを相関付けることができます。

専用ハードウェアまたは仮想化プラットフォーム

パロアルトネットワークスの次世代ファイアウォールは、企業のブランチ オフィスから高速データセンターまでをカバーする専用ハードウェア プラットフォームと、クラウドベースのコンピューティング イニシアチブをサポートする仮想化フォーム ファクタのどちらの形態でも使用することができます。パロアルトネットワークスは最も広いバリエーションの仮想プラットフォームをサポートし、多様な仮想化データセンターやパブリックおよびプライベート クラウドの要件を満たします。VM-Series ファイアウォール プラットフォームは、VMware® ESXi™、NSX™、Citrix® SDX™、Microsoft Hyper-V®、Amazon® Web Services (AWS)、Microsoft Azure™、および KVM ハイパーバイザで使用できます。パロアルトネットワークス プラットフォームをハードウェアまたは仮想フォーム ファクタのどちらで導入しても、集中管理のために Panorama を使用することができます。

〒 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
www.paloaltonetworks.jp

© 2020 Palo Alto Networks, Inc. パロアルトネットワークスは、パロアルトネットワークスの登録商標です。商標のリストについては、https://www.paloaltonetworks.com/company/trademarks.html をご覧ください。本書に記述されているその他の商標はすべて、各社の商標である場合があります。
pan-next-generation-firewall-overview-ds-050616