金融サービス業界に見る サイバーセキュリティの緊急課題:
セキュリティから無用な複雑さ、コストを排除

要約

サイバー犯罪者がその最大の標的として狙いを定めているのは、他でもなく世界中に広がる金融機関です。リスクを最小限に抑えるために、金融機関はまずセキュリティの現状を評価し、最も重要なリスクを把握した上で、迅速に改善を施してセキュリティ インフラを最新化し、脅威防御を改善する必要があります。

残念ながら、金融機関においても他の多くの組織と同様、今日のセキュリティ問題に対する応急処置を施すために、長期間にわたり、組織的にネットワークやエンドポイントにセキュリティ製品を継ぎ足してきました。その結果、互いに孤立したセキュリティ ソリューションによるつぎはぎだらけのセキュリティ パッチワーク状態となり、管理は難しく、保守コストは高額で、APTを体系的に識別およびブロックするための統合脅威インテリジェンスをタイムリーに提供できない代物となっています。

パロアルトネットワークスは、金融機関における今日のセキュリティ インフラから複雑さを排除し、膨大なサイバー攻撃やAPTをより効率的にブロックするための支援をします。パロアルトネットワークスのエンタープライズセキュリティ プラットフォームは、セキュリティの最新のアプローチを採用しています。そこに包含されている革新的かつ効率的なテクノロジを活用することで、コンピューティング リソースと人的資源を最適化しながら、すべてのネットワーク トラフィックを監視およびコントロールし、脅威防御を自動化することができます。

サイバー セキュリティへのパロアルトネットワークスの最新アプローチを通じて、運用面での大きなメリットを実現し、全体的なセキュリティを強化することが可能となります。たとえば次のような効果があります。

- 高度な持続型脅威(APT)や内部関係者による侵害まで、サイバー攻撃に関連するビジネス リスクを最小化
- 可視性と制御性能を向上しセキュリティ関連の運用コストを削減
- 今日のグローバル経済における競争力の強化と革新的なテクノロジのセキュアかつタイムリーな導入をサポート
- トランザクションのデジタル化に伴うネットワークの負荷増大に対応したセキュリティ ソリューションの拡張が可能
- 脅威インテリジェンスを一元化し、インシデントへの洞察力を高め、イベントの相関付けによる迅速な対処
- コンプライアンス監査の合理化により、増え続ける業界規制に関するさまざまな要件に対応

ネットワーク、エンドポイント、およびコンピューティング インフラストラクチャを継続的に監視し、サイバー攻撃から保護パロアルトネットワークスのセキュリティ プラットフォームには次のような機能があります。

- ネットワーク上に誰が何をしているかを可視化
- 誰が何にアクセスできるかを制御
- ルールと自動アラートを使用して間断なく監視
- 基本的な大量のセキュリティ タスクを自動化し、セキュリティ チームは危険な脅威に集中

「当社の実運用環境でファイアウォールが極めて効果的な役割を果たし、ネットワーク上でのポリシーのセットアップと実行も容易でわずか1日で完了できたことを受けて、当社のチームも皆パロアルトネットワークスに大いに満足しています。… 当社は日々ネットワーク上を行き来しているデータの機密性を強く認識しています。当社が必要としているのは、顧客の資産を確実に保護すると同時に、事業の効率的な運営を支えるアプリケーションへの高性能なアクセスを確保できるソリューションです。」

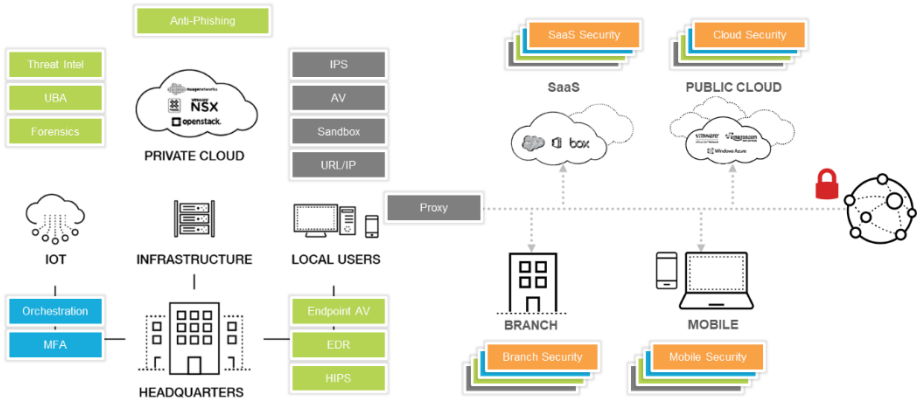
— Raymond James Financial最高情報セキュリティ責任者

セキュリティから無用な複雑さ(およびコスト)を排除

年月を重ねていくと、セキュリティ設計が複雑になっていきます。これは、インターネットの黎明期に設計されたセキュリティ製品を補強するためにさまざまなテクノロジが追加されてきたことが原因です。多くの企業が現在築いている防御体制における共通の課題と弱点は、相互に連携することができないポイント製品が無数にあることです。

サイバーセキュリティ チームの組織がしっかり整っていても、セキュリティ スタッフがバラバラの製品すべてを統合してくれるとは期待できません。サイバー攻撃が衰えることなく増え続けている現在、インシデントを手作業で処理していくことは非常に困難になっているのです。ポイント製品の導入はコストが高く、複雑です。またネットワーク パフォーマンスの低下という高いリスクが伴い、多くの場合、利益よりも害の方が大きくなります。分断化されたアプローチはサイバー攻撃が身を潜めることのできる穴があまりにも多く、手作業で行うステップも非常に多く必要となり、侵害が発生した際の対応能力が遅くなります。

パロアルトネットワークスのソリューションは、ファイアウォール、IPS、IDS、URLフィルタリングをはじめとするさまざまなポイント製品の導入に伴う複雑さを排除します。パロアルトの次世代エンタープライズ セキュリティ プラットフォームは、あらゆるレイヤにおける可視性、そして高度な攻撃のそれぞれのステップの可視性を提供します。そうした機能は一から設計された単一のインライン セキュリティ アプライアンスで実現されており、これを通じて同等のポイント製品のセットを導入および管理した場合の何分の一かのコストで、データのシングルパスに基づいて防御の意思決定を下せるようになります。



パロアルトネットワークスのセキュリティ プラットフォームはあらゆるレイヤにおいて攻撃のステップの可視化を実現

サイバー攻撃とAPT: 事後の検出から事前の脅威予防の対策へ進化する方法

金融機関の場合、投資は高額に上ります。資産を保護するために、多くの金融機関が既に多大なリソースを割り当てています。その結果、攻撃者は金融サービス業界の企業ネットワークに侵入するために迂回した戦術を用いる必要があることを認識しています。

残念ながら、攻撃者は頻繁に標的のネットワークに侵入できるだけでなく、足場を確立することでかなりの期間、セキュリティ製品に検出されないままダメージを与え続けることができます。これは、世間の評判や金銭面、あるいは知的財産の被害に至るまで、多大な損失につながる恐れがあります。今日の高度な攻撃に効果的に対処するには、保護対策にとどまることなく、セキュリティ侵害に対する防御戦略とその予兆の早期検出を強化する必要があります。

パロアルトネットワークスの脅威防御はパロアルトのエンタープライズセキュリティプラットフォームのユニークな機能に基づいて構築されており、さまざまなセキュリティ分野の機能を1つのエンジンにネイティブに統合する次世代ファイアウォールのアーキテクチャと、迂回戦術に関係なく、すべてのポート上のすべてのトラフィックを検査することができます。トラフィックや脅威について大幅に改良されたコンテキスト インテリジェンスを武器に、金融機関のセキュリティ チームは個々のセキュリティ イベントを容易に見通して、アプリケーション、エクスプロイト、マルウェア、URL、DNSクエリ、およびネットワークの異常な動作における相関性を認識することができます。

セキュリティ チームは、パロアルトネットワークスのエンタープライズ セキュリティ プラットフォームから収集したデータを通じて、これまで長時間を要していた日常的なセキュリティ関連のタスクのいくつかを自動化し、詳細なリサーチに多くの時間を費やすことができるようになります。トラフィック、アプリケーション、ユーザー、マルウェアなどに関するより広範な相関情報にすべて1つのエンジンでアクセスできるというメリットにより、セキュリティ管理とレポート作成が合理化されるとともに、セキュリティ インシデントの分析が簡略化され、重要な問題の発見へとより早く到達することができます。

高度な未知の脅威を検出してブロック

APTと未知の脅威に対しては、パロアルトネットワークスはクラウド ベースの仮想環境「仮想サンドボックス」を使用して、悪意がある恐れのあるトラフィックやペイロードの動作を分析します。パロアルトネットワークスのWildFire™サービスは、既存のシグネチャに依存せず、マルウェアの動作を観察し悪意のある実行可能コードの配信を発見します。また、WildFireは、悪意のあるアウトバウンド通信を検査し、次世代ファイアウォールにC2 (コマンド&コントロール)対策シグネチャとDNSベースのコールバック シグネチャを30分以内に配信しC2活動を阻止します。

高度な持続型脅威(APT)は、回避テクニックを駆使してネットワークに侵入し、足場を確立した後、標的の組織内を横方向へと移動します。APTは正当なトラフィックやペイロードを偽装したり、その中に自身を埋め込んだりすることがあるため、従来のセキュリティ ソリューションでは検出が困難になっています。標的となった組織の内部に一旦入ってしまうと、APT はコントローラ/ ハンドラとの通信チャネルを確保することができます。そして情報を盗み、暗号化されたトンネルを経由して外部のC2エンティティからさらなる指令を受けることができます。さらに、悪意のあるコードの更新を受信し、侵害された標的ネットワーク内で再構築することもできます。これによってシグネチャ検出がより困難になるとともに、さらにダメージを与える機能を常駐マルウェアに加えることができます。

また、パロアルトネットワークスの管理インターフェイス「Panorama」やWildFireポータルで統合ログ、分析機能、イベントの監視機能を活用することもできます。これにより、セキュリティ チームは素早い調査により、ネットワークで観測されたイベントを相互に関連付けることができます。

こうした迅速な更新により、特別な操作や分析を行わなくても、マルウェアのさらなる拡散を阻止できるだけでなく、将来の亜種もすべて特定し、増殖を防ぐことができます。

クローズドループ型のアプローチと共有インテリジェンスのメリット

新しい脅威の検出が常に最初のステップですが、WildFireの真価はクローズドループ型のアプローチを通じて自動的にユーザーとネットワークを保護することにあります。新たに発見された脅威に関するインテリジェンスは即座に共有され導入されているパロアルトネットワークスの次世代ファイアウォールに配布されます。

未知の脅威が発見された場合、WildFireはシグネチャを生成し、ネットワークにインラインで導入されている次世代ファイアウォールに更新を送信し、サイバー キルチェーン全体にわたって脅威をブロックします。次に、新たに配布されたシグネチャを直ちに使用して、手作業による操作を一切伴うことなく、発見された脅威に関連する悪意のあるトラフィックをブロックします。これは、アウトバウンドC2トラフィックやDNSベース コールバックなど、インバウンドとアウトバウンドのすべての一般的なマルウェア通信メカニズムをブロックします。パロアルトネットワークスのクローズドループ型のアプローチは、断片化された従来のソリューションで必要となる手作業の多くを排除し、緊急を要するセキュリティ タスクの体系的な自動化をサポートするので、セキュリティ リソースはより積極的なセキュリティ活動に従事することができます。

すべての脅威インテリジェンスがわずか30分で全世界の顧客の基盤と共有されます。パロアルトネットワークスのユーザー コミュニティ全体で、世界中の16,000を超える組織で発見されたマルウェアに関するインテリジェンスを迅速に共有することができるのです。

調査およびインシデント対応時間を短縮

パロアルトネットワークスのエンタープライズ セキュリティ プラットフォームは、脅威インテリジェンスへの即時アクセスと可視性を提供します。管理者は、データの変換や統合を一切行うことなく、統合ログ、分析機能、WildFireイベントの監視機能を活用することができます。セキュリティ チームはネットワーク上で観察されたイベントの調査と相関付けを迅速に行い、タイムリーな調査とインシデント対応に必要なデータ(セキュリティ侵害に関するホスト ベースおよびネットワーク ベースの兆候など)を探して、ログ クエリやカスタム シグネチャを介してそのデータをすぐに使用可能な状態にすることができます。

体系的な事前予防の防御のための重要な推奨事項

1. 現在のネットワーク セグメンテーションを再評価する。最も重要なものがそれにふさわしい扱いを受けているかどうかを確認します。「ゾーン」を使用してネットワークの個々のセグメントを区分し、許可されていないアプリケーションやユーザーから資産を保護するほか、脆弱なシステムやパッチを適用できないシステムのリスクを緩和します。また、ネットワーク全体でマルウェアの横方向の移動を防ぎます。「ゼロ トラスト」アプローチを標準とし、それが何であるか、ネットワーク上のどこにあるかにかかわらず、すべてのトラフィックを検査します。APTの出現で、「信頼しない」ことを前提としたアプローチの採用が極めて重要になっています。

2. ネットワーク上の全アプリケーションについてベースラインビューを確立する。ネットワークの特定のゾーンでトラフィックを生成するアプリケーションの詳細なインベントリを作成します。これは、業務に欠かせない正規のアプリケーションについてIT部門とビジネス部門との間で建設的な意見を交換するのに役立ちます。こうしたベンチマークを検討することで、不正なアプリケーションについてアラートを生成するなど、適切なセキュリティ制御を適用し、正規のアプリケーション(アプリケーションのペイロード、アプリケーションにアクセスする従業員、ユーザー、部門)を継続的に監視して異常を検出できるようになります。

3. ベンチマークを使用してアプリケーションについての重要な意思決定を行う。ネットワーク上の任意のセクションにおける正規のアプリケーションのリストを確認したら、「正規のアプリケーションとして明示的に特定されたいくつかのアプリケーションを除き、すべてをブロックする」など、機密性の高いゾーンにより厳格なセキュリティ制御を徐々に適用できるようになります。アプリケーション、ユーザー、コンテンツを詳細に監視して柔軟性ときめ細かい制御を実現するパロアルトネットワークスならではの機能を活用して、どのアプリケーションやコンテンツをどの部門で利用できるようにするかを選択します。その後、許可されたユーザーのみに、承認されたアプリケーションへのアクセス権を付与します。

4. ユーザー、コンテンツ、およびアプリケーション レベルで継続的に監視する。これはログ分析の手法ではなく、セキュリティチームがセキュリティ侵害の兆候を効果的に特定するために活用できる状況認識、監視、異常検出の手法の1つです。

暗号化された通信に潜む今日の脅威 ― 他のセキュリティ製品が不要な理由

今日のアプリケーション トラフィックの約3分の1はSSLで暗号化されています。そしてセキュリティを強化するためにアプリケーションはデフォルトで暗号化されるようになっているため、その割合はさらに急速に増大しています。暗号化によってAPTから保護されると考えるのは間違いです。多くの悪意のある攻撃は、暗号化されたトラフィックの中に身を隠すことができるからです。残念ながら、暗号化されたトラフィックはセキュリティ製品によって処理されないことが多く、処理をするにはセキュリティ デバイスを追加しなければならないこともあります。パロアルトネットワークスでは、追加デバイスは不要です。暗号化された通信に潜む脅威の通信を監視し、平文による通信でも暗号化された通信でも脅威を検出して防御することができます。

今日のコンピューティング環境: データセンターの統合や仮想化にあたってはセキュリティを最優先する

既存のデータセンター利用の最適化であろうと、あるいは統合プロジェクトの一環であろうと、仮想化とクラウド コンピューティングはすべての現代化イニシアチブの中核です。こうした新しいコンピューティング モデルの真価が効率化、柔軟性の向上、コスト削減にあるとすれば、金融機関はデータセンターの現代化と仮想化の導入における先駆者となってきました。しかしながら、セキュリティは後付けされることが多く、データセンターやインフラの変革に向けた重要な取り組みを遅らせるものと考えられることすらあります。

パロアルトネットワークスは、セキュリティを邪魔者からデータセンター プロジェクトの成功に欠かせない重要な要素へと変えるために、仮想化テクノロジ、製品、およびパートナーシップへの投資を何年も前に開始しました。パロアルトの次世代セキュリティ製品は現在、物理アプライアンスだけでなく、仮想化インフラに対応した仮想化プラットフォームでも利用することができます。パロアルトネットワークスは多数の大手データセンター、エコシステム ベンダとグローバルなパートナーシップを結んでおり、仮想化を可能にするさまざまなテクノロジと細部にわたるシームレスな統合を実現します。

データセンター仮想化の真のメリットを理解する

金融サービス業界のIT部門にとって、データセンターの仮想化の主な目的の1つは、利用可能なコンピューティング能力をアプリケーション、地域、およびイニシアチブ全体で最大限に活用し、規模の経済を実現することです。しかし、仮想化とクラウド コンピューティングの真価は依然として見えづらい状況が続いています。

仮想化データセンターの導入を遅らせる障壁の1つがネットワーク セキュリティです。従来のセキュリティ アプローチは、今日におけるアプリケーションおよびサーバ プロビジョニングのペースに対応できるようには設計されていませんでした。ITチームは仮想サーバをほんの数分で導入することができますが、関連するセキュリティ ポリシーの設定は大量のペーパーワークを伴う手作業で行われており、数か月とまではいかなくても、数週間はかかる可能性があります。

こうした課題に対処するために、パロアルトネットワークスはマネージメント オーケストレーション サービスと直接統合してデータセンターを仮想化します。たとえば、パロアルトネットワークスは、VMwareとパートナーシップを結び、次世代セキュリティをVMwareのNSXネットワーク仮想化プラットフォームと完全に統合しています。この共同ソリューションでは、物理環境と仮想環境間でネットワーク セキュリティを統合することで、software-defined datacenterの潜在能力をフルに発揮することができます。これによって管理が一元化され、新しいサーバやアプリケーションのプロビジョニングに伴ってセキュリティ ポリシーを自動的にプロビジョニングすることができます。

East-Westトラフィックに対する制御と完全な可視性を取り戻す

データセンター仮想化イニシアチブにおけるもう1つの課題は、マルウェアの横方向の移動を可能にする仮想マシン同士の(East-West)トラフィックに対する可視性が欠如している点です。

仮想化サーバ上のリソースを次世代ファイアウォールのVM-Seriesに割り当てると、セキュリティ ポリシーを仮想マシンの行動(追加、移動、および変更)に関連付けや、仮想ワークロードの作成と即座に同期するセキュリティ ポリシーを作成することができます。VM-Seriesは、パロアルトネットワークスの物理セキュリティ アプライアンスと同一のアプリケーション可視性、制御、およびトラフィック検査機能を備えており、既知と未知のあらゆる脅威から仮想環境を保護します。

仮想化サーバに動的に追従するセキュリティ機能を通じて、ITチームはマシン間の(East-West)トラフィックに対する完全な制御を取り戻し、サーバ間における脅威の横方向の移動を防ぐことができます。

高性能のセキュリティ - パフォーマンスとセキュリティをどちらも犠牲にしない

データセンターを保護するには大量のトラフィックを把握する必要があります。複数のセキュリティ層やアドオン製品によって生じる遅延が原因で、ネットワーク運用チームがトラフィック ラインからセキュリティを排除してしまうことがよくあります。

パロアルトネットワークスの革新的なセキュリティ アーキテクチャを導入すれば、すべてのトラフィックをシングルパスで制御し、脅威がないかどうかを検査することができるので、ITチームはセキュリティとパフォーマンスをどちらも犠牲にする必要はありません。次世代セキュリティ アプライアンスのポートフォリオに加わった最新ソリューションにより、最大120 Gbpsの速度でデータセンター環境を保護することができます。

まとめ: データセンター イニシアチブに最適な包括的なセキュリティ ポートフォリオ

パロアルトネットワークスは、物理、仮想、および混合モードの環境を保護し、データセンターのニーズに応じて拡張および進化するセキュリティ アーキテクチャを提供します。パロアルトネットワークスの次世代セキュリティ プラットフォームは、ホスト内通信の検査やセキュリティ ポリシーの追跡から、仮想マシンの作成と移動、オーケストレーション ソフトウェアとの統合に至るまで、仮想化とクラウドの重要な課題に対処します。

パロアルトネットワークスは、データセンター ネットワーク セキュリティについて直面している容認できない妥協を排除します。パロアルトネットワークスのソリューションを導入することで、シンプルで柔軟性に優れた高性能のネットワーク セキュリティ インフラを導入し、ビジネス クリティカルなアプリケーションを安全に運用するとともに、データセンター内で増え続けるトラフィックにも対応することができます。

モビリティ イニシアチブの新しい波を管理する

これまで、スマートフォンの広範な採用は、金融業界における従業員の仕事の柔軟性と生産性の向上に寄与してきました。たとえば多くの組織が、従業員が企業のBlackBerryを使用するよう後押ししました。現在では、AndroidやiOSなどの種々のオペレーティング システムで動作する多くのデバイスが普及し、モバイル テクノロジのユビキタスな導入がより一層広がっています。

今日、使用するデバイスが刷新され多くの金融機関ではBYODモデルへ移行し、BlackBerryは廃棄される方向へ進んでいます。このBYODモデルにより、従業員は自分が選んだデバイスを使用して企業ネットワークに接続できるようになりました。しかしその一方で、従来の企業の境界が完全に破壊され、セキュリティ チームに新たな課題を突き付ける結果となっています。

パロアルトネットワークスのセキュリティ プラットフォームを導入すれば、従業員が企業ネットワークへの接続に使用するモバイル デバイスまで保護を拡大することができます。モバイル デバイスを保護するパロアルトネットワークスのソリューション「GlobalProtect™」は、デバイスの管理、通信の保護、データの制御という3つのステップまたはコンポーネントで構成されています。

GlobalProtect の一部であるMobile Security Manager (MSM) は、モバイル デバイスの設定を管理し、組織全体におけるデバイスの使用状況を監視します。新しいデバイスがビジネス環境に持ち込まれると、MSMはその設定や状態を検証し、マルウェアに既に感染しているデバイスに対して自動的にフラグが付けられます。GlobalProtectはまた、ネットワーク セキュリティ ポリシーの一貫した適用と企業ネットワークへのセキュアな接続(IPsec/SSL VPNトンネル)の確立を保証します。最後に、GlobalProtectゲートウェイには、慎重な扱いを要するアプリケーションやデータへのアクセスを誰に許可するかをきめ細かく制御する機能と、ファイルやデータのフィルタリング機能が備わっており、データの移動を制御することができます。

ネットワーク セグメンテーション: 単なるベスト プラクティスにとどまらない必須のアプローチ (特にコンプライアンスをサポート)

高度に規制されたデータやプロセスを保護および分離するためのベスト プラクティスの1つとして、機密性に応じたゾーンによるネットワーク セグメンテーションが広く認識されています。これは、法規制コンプライアンスをサポートし、監査を必要とするインフラの範囲を縮小することで監査プロセスを簡略化するための最も重要な推奨事項の1つです。

セグメンテーションはまた、世界的に導入する金融機関をリスクの高い地域で開始された攻撃から保護する上で非常に効果的です。ゾーン間のネットワーク トラフィックを正規のアプリケーションだけに限定するなど、厳格な制御を適用することで、グローバルなサイバー攻撃のリスクを大幅に軽減することができます。また、リモート オフィスから本社やデータセンター施設へと向かうマルウェアの横方向の移動を防ぐこともできます。

ネットワーク セグメンテーションは、多層防御を実装するための優れたアプローチでもあります。攻撃が組織の内部から発生するケースがますます増えている現在、どの時点においても企業ネットワーク上には何らかの脅威が存在しているということを組織は前提にしなければなりません。ネットワーク セグメンテーションと体系的な区画化は、脅威の横方向の移動、すなわちネットワークのエッジからコアへと向かう移動を阻止します。

ネットワーク セキュリティに対するパロアルトネットワークスの革新的なアプローチを採用すれば、アプリケーション、ユーザー、コンテンツに基づいてネットワーク上のすべてのトラフィックを識別して分類することができます。このユニークな機能は、ネットワーク セグメンテーションを推進するにあたって重要な差別化要素となります。たとえば、より高レベルの分類では、ビジネス上意義のある基準や属性を使用して、特定のネットワーク ゾーンでトラフィックを許可または拒否するポリシーを体系化することができます。

大規模なセキュリティ: 数千台に及ぶセキュリティ アプライアンスを管理する

大規模なグローバル金融機関に特有の課題の1つは、大規模なセキュリティ製品ポートフォリオの継続的な管理です。グローバルな企業では、数百台あるいは数千台にも及ぶセキュリティ アプライアンスを管理しなければならないことも珍しくありません。すべてのアプライアンスを常に最新の設定に維持すること、セキュリティポリシーが各国の規制も世界的な規制も満たすようにすること、セキュリティ ルールおよびポリシーを増分的に更新しても相互に影響しないようにすることは、決して容易なことではありません。

このような理由から、パロアルトネットワークスはプラットフォームのさまざまな機能の導入と管理を簡略化することを常に製品戦略の中心に据えています。パロアルトネットワークスでは、導入した次世代アプライアンスの管理をさまざまな方法で簡略化することができますが、いくつかの方法を紹介します。

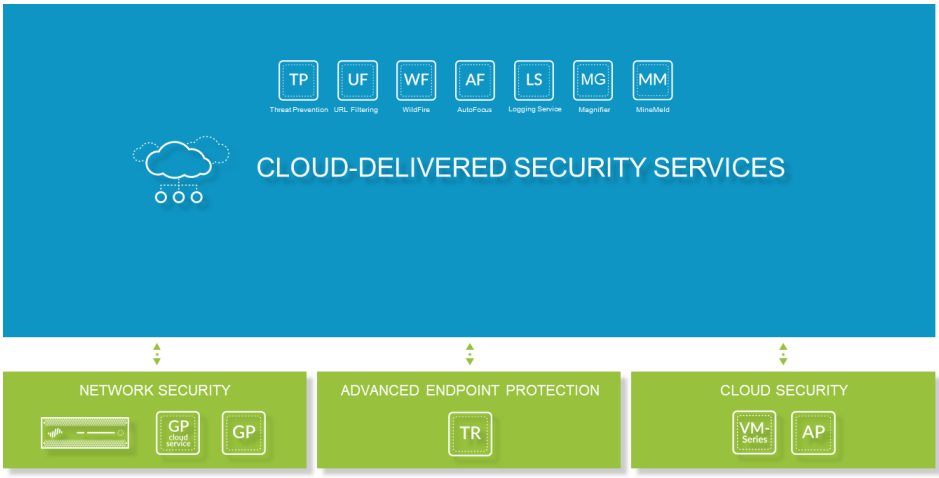
- パロアルトネットワークスのファイアウォールは、ローエンドからハイエンドまで同一の基礎テクノロジに基づいて構築され、それぞれの帯域容量に関係なく、同一の機能を提供します。たとえば、データセンターにはPA-7050を、リモート サイトにはPA-2050をそれぞれ導入して、いずれも同じメリットを得ることができます。
- パロアルトネットワークスの集中管理製品「Panorama」を使用すると、分散しているセキュリティ アプライアンスをすべて中央の1か所から管理できます。たとえば、全トラフィックの表示、デバイス設定のあらゆる側面の管理、グローバル ポリシーのプッシュ、トラフィック パターンやセキュリティ インシデントに関するレポートの生成などを行うことができます。
- 大規模な導入の場合は、管理を階層化することで、ネットワーク インフラと組織に合わせてポートフォリオとテクノロジの導入を構成することができます。
- ポリシーに関しては、多数のお客様が、パロアルトネットワークスへの移行後に、管理する必要があるセキュリティ ポリシーの数を大幅に削減しています。パロアルトネットワークスは、より高レベルの集約により、ポートやIPアドレスではなくアプリケーション、ユーザー、コンテンツに基づいてトラフィックを識別します。そのため、従来のソリューションでは5つのルールが必要になるところを、パロアルトネットワークスのプラットフォームならわずか1つのルールで済みます。

> 「…すべてが非常に容易になりました。従来のファイアウォールでは、情報の発掘に数日を要していましたが今ではボタンを一度クリックするだけです。制御が強化されたほか、IPS機能も大いに成果をあげています。」
> – Head of ICT Exploitation Department、Crédit Agricole Consumer Finance

まとめ: 金融機関におけるサイバーセキュリティ要件にも対処可能なパロアルトネットワークス

パロアルトネットワークスは、金融機関における今日のサイバーセキュリティ要件に対処できる、最も革新的で柔軟性に優れた高度なエンタープライズ セキュリティ プラットフォームを提供しています。パロアルトネットワークスのプラットフォームは、次のような多数のセキュリティ機能を組み合わせて企業ネットワークをより効果的に保護します。

- 次世代セキュリティ ファイアウォール(数年間連続でGartner Groupマジック クアドラントのエンタープライズ ファイアウォール部門で「リーダー」に選出)
- 脅威の検出と防御: わずか30分でシグネチャを作成して脅威を防御するクラウド ベースの脅威サンドボックス分析
- デバイスにインストールする前にマルウェアを阻止する革新的なエンドポイント プロテクション
- 既知の脅威を迅速に検出して防御するIPS
- マルウェア対策
- URLフィルタリング
- ファイルおよびコンテンツ ブロックによる既知の脅威の制御
- 暗号化された通信に潜む脅威の監視および防御
- ネットワークへのゼロデイ脅威のさらなる拡散を防ぐクローズドループ型のアプローチ



パロアルトネットワークスの次世代エンタープライズ セキュリティ プラットフォーム

パロアルトネットワークスをご利用いただいている金融サービス業界のお客様からは、従来のセキュリティ インフラをパロアルトネットワークスの製品に置き換えることで、サイバー攻撃に関連するリスクを最小限に抑えることができた、セキュリティインフラの無用な複雑さを排除することができたというお声を相次いでいただいています。

高度なテクニックを駆使してゼロデイ攻撃を検出し、ネットワークへの拡散を防ぎながら、基本的な大量のマルウェアを自動的にブロックできるパロアルトネットワークスのプラットフォームでチームを強化してください。

事後の検出から事前の脅威予防の対策へ進化: 今すぐ第一歩を踏み出す

既にパロアルトネットワークスを活用して組織の境界を保護している場合でも、あるいは初めてパロアルトネットワークス テクノロジを導入する場合であっても、パロアルトネットワークス プラットフォームを通じてポリシー制御を実装することで、サイバー セキュリティの課題の範囲を狭めて高い効果をあげることができます。また、パロアルトネットワークスのクローズドループ型のアプローチによって、インフラ全体に拡散しないよう攻撃を自動的にブロックすることができます。パロアルトネットワークスのメリットを是非ご自身でお確かめください。

次のようなサービスをご利用いただけます。

- オンライン製品デモ - お客様のニーズに合わせて調整します。
- 製品体感トレーニング - ハンズオン セミナーを通じてパロアルトネットワークスのテクノロジをご紹介します。
- パロアルトネットワークスのアプリケーションの使用および脅威分析レポート - 直ちに対処すべき火急の脆弱性を1週間足らずで明らかにすることができます。

〒102-0094
千代田区紀尾井町4番3号
泉館紀尾井町3F
電話番号: 03-3511-4050
www.paloaltonetworks.jp