ADVANCED THREAT PREVENTION データシート

製品概要

Juniper Advanced Threat Prevention（ATP）は、クラウドベースのサービスまたは仮想化されたオンプレミスソリューションで、完全で高度なマルウェア検出と対策を提供します。SRX シリーズファイアウォールと統合することで、Juniper ATP から、静的および動的分析と機械学習による識別を活用した脅威インテリジェンスとマルウェア分析機能が得られるようになり、ユーザー、アプリケーション、インフラストラクチャを保護できます。

製品説明

ジュニパーネットワークスの SRX シリーズファイアウォールに Juniper Networks® Advanced Threat Prevention（ATP）を追加することで、既知および未知の脅威を特定してブロックすることができます。Juniper ATP は、機械学習を使用してファイルとネットワークトラフィックを分析し、悪意のある行動の兆候を探すことで、既知および未知のサイバーセキュリティ脅威を見つけてブロックします。ATP は、暗号化されたトラフィックに隠れているボットネットや C&C サーバーを含む、ゼロデイマルウェアの脅威や悪意のある接続を発見することができます。ジュニパーの厳選されたセキュリティインテリジェンスフィードである SecIntel を使用することで、ATP がすべてのネットワーク接続ポイントに保護メカニズムを適用し、これらの脅威を未然に防ぎます。

Advanced Threat Prevention Cloud

ATP クラウドは、SRX シリーズファイアウォールのアドオンライセンスとして導入できます。静的および動的分析と機械学習を組み合わせて、Web からダウンロードされたり電子メールで送信される未知の脅威を迅速に特定します。ファイルの判断とリスクスコアを SRX シリーズのファイアウォールに返すため、ネットワークレベルでのブロッキングが可能です。

さらに、ATP クラウドは、ファイルの分析、Juniper Threat Labs による調査、高い評価を得ているサードパーティの脅威フィードから収集された、悪意のあるドメイン、URL および IP アドレスで構成された SecIntel セキュリティインテリジェンスを提供します。これらのフィードは、SRX シリーズのファイアウォールとジュニパーネットワークスの MX シリーズユニバーサルルーティングプラットフォームに配信され、コマンドアンドコントロール通信を自動的にブロックすることができるため、企業への攻撃を成功させることがさらに困難になります。

ATP クラウドは、ネットワーク上の DNS トラフィックに関する重要なインサイトも提供します。コマンドと制御に DNS を活用する攻撃や、データの配信や漏洩を目的とした攻撃を緩和するための情報を提供します。ATP クラウドは、DNS 生成アルゴリズム（DGA）と DNS トンネリング脅威からも保護します。IoT の普及によるセキュリティ上の懸念に対処するために、ATP クラウドはネットワーク上の IoT デバイスを特定して分類することができます。この情報をもとに、セキュリティ運用チームはネットワーク全体でポリシーを適用するためのフィードを ATP クラウドで管理し、大規模な IoT 攻撃面が表面化するリスクを低減することができます。

ATP Cloud には、コンフィグ/ライセンス/レポートを管理する独自のポータルが含まれます。

Advanced Threat Prevention Appliance

ATP Appliance はオンプレミス導入に対応しており、Juniper ATP の仮想化バージョンとして利用できます。VMware vSphere または ESXi で実行され、8 または 24 個のバーチャル CPU コアを使用して導入することができ、1 日あたり最大 116,000 個のオブジェクトをデトネーションできます。

Juniper ATP Appliance は、SRX シリーズのファイアウォールや独自のビルトイン型コレクターを使用して Web、電子メール、水平方向のトラフィックから収集するため、複数のファイアウォールソリューションを採用している企業に最適です。収集されたデータは、オンプレミスにある ATP Appliance に送信され、ATP Appliance コアでさらに処理されます。この ATP Appliance コアが、既知および未知の脅威を特定し、攻撃キルチェーンの検知をマッピングすることで、環境内の脅威の進捗状況について、詳細で包括的な分析を提供します。

いったん脅威が検知されると、Juniper ATP Appliance は、ファイアウォールポリシーの更新を SRX シリーズのファイアウォールに送信します。Juniper ATP Appliance は、サードパーティファイアウォールベンダーのポリシーを更新するように設定することもできます。

また、Juniper ATP ソリューションは、ジュニパーやサードパーティのスイッチと連携して脅威を隔離し、ワンタッチで侵害されたホストを隔離して、感染の水平方向の拡散を制限します。Juniper ATP が検出に基づいて感染ホストのリストを作成します。ジュニパーネットワークスの Policy Enforcer と連携することで、ジュニパーネットワークス EX シリーズおよび QFX シリーズスイッチ、ForeScout などの NAC ベンダーと統合し、ネットワーク上の侵害されたホストをブロックまたは隔離します。

アーキテクチャと主要コンポーネント

Advanced Threat Prevention Cloud

Juniper ATP は、ジュニパーの次世代 SRX シリーズのファイアウォールを活用して、トラフィックのルーティングと可視化を実現しながら、同時に脅威、構成、レポートのクラウド管理を提供します。

Juniper ATP Cloud は、Web ベースの脅威または電子メールで配信された脅威を特定します。SRX シリーズのファイアウォールに備わる SSL 暗号化解除機能を使用することで、暗号化されたセッションに送信されたあらゆるマルウェアを容易に特定することもできます。Juniper ATP Cloud は SMTP および IMAP 電子メールプロトコルに対応しており、悪意のある添付ファイルがないか電子メールを検査し、エンドユーザーに脅威を与える可能性のある電子メールを隔離することができます。

Juniper ATP Cloud は、パブリッククラウドインフラストラクチャを活用して、柔軟で拡張性の高いファイル分析と脅威特定を提供します。SRX シリーズファイアウォールとクラウド間のすべての通信は安全で、両側から暗号化接続することで実現しています。分析のためにクラウドにアップロードされたファイルは、その後、プライバシを保証するため破棄されます。Juniper ATP Cloud プライバシポリシーと、より広範なジュニパーネットワークスのプライバシポリシーに関する詳細な説明については、www.juniper.net/jp/ja/privacy-policy/をご覧ください。

Juniper ATP Cloud は、グローバルで利用できます。北米 (米国とカナダ) 、EMEA、APAC のデータセンターから配信されています。この広範囲にわたる可用性により、これらの地域のお客様は、クラウドベースの脅威防御とインテリジェンスサービスからメリットを享受しながら、同時にお客様のデータのローカライゼーションやデータプライバシーの懸念に対応することができます。送信されたデータはその地域で処理され、その地域の境界を超えることはありません。お客様は、データの所在位置をより細かく管理することができ、規制やプライバシーに関する要件を満たすことができます。

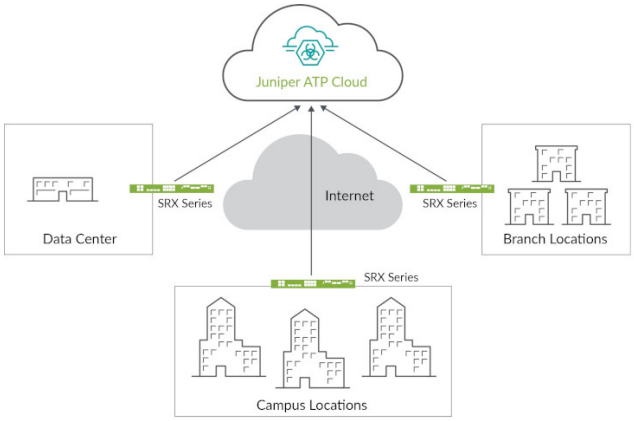

図 1 : Juniper Advanced Threat Prevention クラウドアーキテクチャ

特長とメリット

特長	説明
マルウェア分析	マルウェア分析は、Web からダウンロードされたファイルや電子メールを介して配信されたファイルの静的および動的分析から、悪意のあるコンテンツを特定し、そのファイルが悪意のあるペイロードをインストールするために、コマンドアンドコントロール (C&C) サーバーに接触しようとしているかを検出します。脅威が検出されなかった場合、ファイルはダウンロードされるか、受信者へと配信されます。マルウェアやグレーウェアが検知された場合、SRX シリーズのファイアウォールなら、ダウンロードをブロックしたり、電子メールの配信を阻止したりすることができます。ジュニパー ATP では、Windows バージョン 7 および 10、Mac、Linux、Android 用のファイルと実行可能ファイルを分析することができます。カスタムの企業向け Windows イメージを作成している場合は、JATP アプライアンスにアップロードすることができます。
暗号化トラフィックのインサイト (ETI)	暗号化されたトラフィックのインサイトにより、TLS/SSL による完全な暗号化解除の負荷をかけることなく暗号化トラフィックの脅威を可視化することができます。SRX シリーズのファイアウォールでは、使用された証明書、ネゴシエートされた暗号スイート、接続の動作など、SSL/TLS 接続についての関連データを収集します。 Juniper ATP Cloud がこの情報を処理し、ネットワーク動作分析と機械学習に基づいて接続が無害なものか悪意のあるものかを判定します。悪意があると判明された暗号化トラフィックについては、SRX シリーズのファイアウォール上で設定されたポリシーを使用して、これらの脅威をブロックすることができます。
SecIntel	SecIntel は、精選されたセキュリティインテリジェンスを、既知の攻撃で使用されていた悪意のあるドメイン、URL、IP アドレスが含まれる脅威フィードという形式で提供します。また SecIntel では、お客様はインラインブロック向けに、独自の脅威インテリジェンスをフィードして配信することもできます。この情報は、SRX シリーズのファイアウォールや、ケースによっては MX シリーズユニバーサルルーティングプラットフォームや EX シリーズおよび QFX シリーズスイッチにも提供され、既知の脅威を特定してブロックします。
適応型脅威プロファイリング	企業は、ATP クラウドの適応型脅威プロファイリングを使用して、ネットワークを攻撃している人や現在攻撃している対象に基づいて、セキュリティインテリジェンス脅威フィードを自動的に作成し、新しい脅威の継続的な攻撃に対抗することができます。適応型脅威プロファイリングでは、ジュニパーセキュリティサービスを利用してエンドポイントの動作を分類し、複数の実施ポイントでさらなる検査やブロックに使用できるカスタム脅威インテリジェンスフィードを構築します。リアルタイムで攻撃に対応できる能力を企業に提供します。
攻撃分析	分析ビューは何が起きているのかを把握する手段を提供します。セキュリティ運用担当者は、ネットワーク内で発生している相関性のある脅威アクティビティを確認し、優先度の高い脅威を迅速に特定して対応方法を理解したり、発生した問題を修復するために隔離することができます。
DNS セキュリティ	ジュニパーネットワークスは、増え続ける DNS を活用した攻撃に対応する Advanced Threat Prevention を提供します。DNS を悪用した C&C 通信、データ漏洩、フィッシング攻撃、およびさまざまな技術を使用して DNS を悪用するランサムウェア攻撃から保護することができます。ATP は、DGA や DNS トンネリング技術を利用した攻撃から脅威を防御します。
IoT 脅威防止	ATP クラウドは、IoT デバイスを特定して分類する簡単な方法を提供するため、お客様はネットワーク上の IoT 攻撃対象領域を制御することができます。セキュリティデバイスから、トラフィックのフローを含む ATP クラウド IoT デバイス情報が提供され、提供されるメタデータを使用して脅威フィードを作成し、ネットワーク内の IoT トラフィック全体にセキュリティポリシーを適用することができます。
脅威の防御と緩和	物理または仮想 SRX シリーズのファイアウォールに沿って悪意の拡散をブロックするか、サードパーティファイアウォールを使用してネットワークタップを介して検出してログに記録します。脅威の横方向への拡散を防ぐために、ジュニパー ATP は既存のネットワークアクセスコントロール (NAC) ソリューションと統合し、感染が修復されるまで感染したホストを隔離するか、ネットワークからドロップします。ジュニパーの SecIntel 脅威フィードは、SRX シリーズのファイアウォール、MX シリーズのルーター、ジュニパー無線アクセスポイント、EX シリーズおよび QFX シリーズスイッチに定期的に更新される実用的なインテリジェンスを提供します。
自動化	セキュリティ運用担当者がホストやエンドポイントを識別する際の手作業の負荷を軽減するために、ジュニパー ATP は、IP アドレスとメディアアクセス制御 (MAC) アドレスの両方をもとにマシンやホストを識別することができます。防御機能を自動化するために、ジュニパー ATP はサードパーティのファイアウォール、スイッチ、無線技術と統合して、脅威が取り除かれるまでユーザーをブロックしたり、ホストを隔離したりすることができます。この機能は、SRX シリーズのファイアウォール、MX シリーズのルーター、EX シリーズおよび QFX シリーズのスイッチに適用されます。自動化により、各デバイスで個別のポリシーを選択するのではなく、異なるシステム全体にポリシーを設定して定義することができます。

Advanced Threat Prevention Appliance

オンプレミスの Juniper ATP Appliance は、SRX シリーズのファイアウォールをコレクターとして使用してインライン検出とブロックを行うか、サードパーティ製ファイアウォールで内蔵されているコレクターを使用することができます。MSSP (Managed Security Service Provider) 環境の場合、マルチテナントをサポートするためにコレクターとコアを分けて ATP Appliance を展開することもできます。お客様の各拠点にコレクターを設置し、コアまたはコアのクラスターが、すべてのトラフィックを分析します。

ネットワーク全体から収集されたファイルと関連する実行可能ファイルは、さらなる分析のために、ATP 仮想アプライアンスにある SmartCore 検知および分析エンジンに送られます。Juniper ATP Appliance は、外部から隔離された環境向けにプライベートモードで実行でき、インターネットアクセスが利用できない場合でもマルウェア検出、攻撃の緩和、さらには関連付けを提供します。

SRX シリーズのファイアウォールは、SmartCore エンジンによって検知された脅威をブロックできます。包括的な攻撃分析を行うために、Juniper ATP Appliance は、アクティブディレクトリ、エンドポイントアンチウィルス、ファイアウォール、セキュア Web ゲートウェイ (SWG)、侵入検知システム、エンドポイント検出および応答ツールなどの、他の特定製品およびセキュリティ製品から得られる検出ログも取り込みます。ログは、サードパーティデバイスから直接取り込むか、既存のセキュリティ情報やイベント管理 (SIEM) /システムロギングサーバーから転送されます。

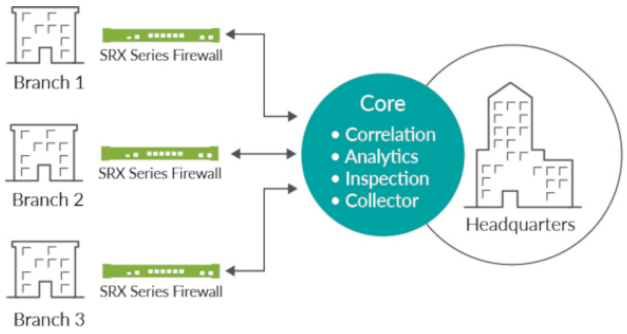

図 2 : Juniper Advanced Threat Prevention のオンプレミスアーキテクチャ

Security Director Cloud

Security Director Cloud が、単一の UI から提供されるシンプルかつシームレスなジュニパーの管理エクスペリエンスを提供し、お客様の現在の導入と将来のアーキテクチャ展開を結び付けます。

ジュニパーの Connected Security 戦略は管理を中心としたもので、ネットワーク上のあらゆる接続ポイントを保護してユーザー、アプリケーション、インフラストラクチャを保護します。

企業はオンプレミス、クラウドベース、クラウド型、ハイブリッドなど、あらゆる環境全体にわたる一貫したセキュリティポリシーでアーキテクチャを保護し、エッジからデータセンター、アプリケーションやマイクロサービスにいたるまでのネットワークのすべての部分に対してゼロトラストを拡大することができます。Security Director Cloud を使用すると、企業は単一の UI から途切れることのない可視性、ポリシー構成、管理、集合的な脅威インテリジェンスを確認できます。

Juniper Security Director Cloud を使用することで、企業はポリシーを一度だけ作成して、あらゆる場所に適用することができます。統一されたポリシー管理により、場所を問わず、すべてのユーザー、アプリケーション、デバイスにシームレスなセキュリティが確保されます。ジュニパーは、お客様が移行のどの段階にいるのであれ要件を満たして、既存の投資を活用できるようにサポートし、Security Director Cloud で移行を自動化することで、お客様のビジネスに最適なペースで、希望するアーキテクチャに移行できるようにします。

注文情報

Juniper Advanced Threat Prevention

ライセンスオプション	MX シリーズルーター	EX/QFX シリーズスイッチ	SRX シリーズファイアウォール	Juniper ATP Cloud	Juniper ATP Appliance
ATP および SecIntel 機能の導入	クラウド	N/A	クラウド	クラウド	オンプレミス ATP バーチャルアプライアンス
SecIntel フィード	○—MX240、MX480、MX960（C&C、カスタムホワイトリスト、ブロックリストのみ）	×。感染したホストフィードに基づく実施ポイント	○	○	○
動的分析	×	×	×	○	○
適応型脅威プロファイリング	×	×	○	○	×
暗号化されたトラフィックのインサイト[1]	×	×	×	○	×
ファイアウォール/コレクター	N/A	N/A	SRX シリーズ ファイアウォール	SRX シリーズ ファイアウォール	SRX シリーズのファイアウォールまたは J ATP バーチャルアプライアンス
脅威分析	×	×	×	○	○[2]
サードパーティ脅威検出ログインの取り込み	×	×	×	×	○[2]
Policy Enforcer が必要です	○	○	×	×	×
ライセンスタイプ	S-MX（モデル）-CSECINTEL	N/A	プレミアム 1、2、または 3	SRX プレミアム 1、2、または 3 が必要です	スタンダード 1 または 2、アドバンスド 1 または 2
ライセンスの有効期間	サブスクリプション：1、3、5 年間	N/A	サブスクリプション：1、3、5 年間	サブスクリプション：1、3、5 年間	サブスクリプション：1、3、5 年間

[1] Encrypted Traffic Insights（暗号化されたトラフィックのインサイト）には、Junos OS 20.2 以降が必要です

[2] これらのオプションは、ATP Appliance でアドバンスド 1 またはアドバンスド 2 ライセンスをご購入された場合にのみご利用いただけます

ジュニパーネットワークスについて

ジュニパーネットワークスは、ネットワーク運用を劇的に簡素化し、エンドユーザーに最上のエクスペリエンスを提供することに注力しています。業界をリードするインサイト、自動化、セキュリティ、AI を提供する当社のソリューションは、ビジネスで真の成果をもたらします。つながりを強めることにより、人々の絆がより深まり、幸福、持続可能性、平等という世界最大の課題を解決できるとジュニパーは確信しています。

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号： 888.JUNIPER (888.586.4737)
または +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
日本, 東京本社
ジュニパーネットワークス株式会社
〒 163-1445 東京都新宿区西新宿 3-20-2
東京オペラシティタワー 45 階
電話番号： 03-5333-7400
FAX：03-5333-7401
www.juniper.net/jp/ja/