ADVANCED THREAT PREVENTION APPLIANCE

製品概要

Juniper Networks Advanced Threat Prevention Appliance は、高度な脅威検知、統合型のセキュリティ分析、ワンタッチの脅威防御を組み合わせて、サイバー攻撃から組織を保護し、セキュリティ チームの生産性を向上させる分散ソフトウェア プラットフォームです。ATP Appliance は、Web、電子メール、および拡散トラフィックの脅威を検知します。さらに、セキュリティ デバイスからログを取り込み、コンテキスト分析を適用して、環境内のすべての脅威を包括的に表示できます。

製品説明

世界中の組織がセキュリティと生産性の課題に毎日直面しています。一般的に、署名ベースの検知に依存する従来のセキュリティ デバイスでは、このようなデバイスを認識できないため、多くの場合、マルウェアは検出されません。この問題に加えて、セキュリティ チームが多くのアラートに圧倒されるため、多くの場合、重大なインシデントを認識して対処することができなくなります。

Juniper Networks® Advanced Threat Prevention Appliance は、Web、電子メール、およびネットワーク全体を移動する拡散トラフィックを継続的かつ段階的に検出および分析します。高度な機械学習と行動分析技術を使用して、複数の攻撃ベクトルから情報を収集し、高度な脅威をわずか 15 秒で特定します。このような脅威は、ネットワーク内の他のセキュリティ ツールから収集されたデータと組み合わされ、分析と関連付けを行い、感染したホストに関連するすべてのマルウェア イベントを包括的な 1 つのタイムラインに表示できます。脅威が特定されると、「ワンタッチ」ポリシー アップデートがインライン ツールにプッシュされ、高度な攻撃の繰り返しから保護されます。

ATP Appliance の検知コンポーネントは、ネットワーク トラフィックを監視し、キル チェーンの途中で脅威を特定し、フィッシング、悪用、マルウェアのダウンロード、コマンドとコントロールの通信、および内部の脅威を検知します。マルチステージの脅威分析プロセスは、静的解析、ペイロード、機械学習、動作、およびマルウェア評価分析を含み、ジュニパーのグローバル セキュリティ サービスを活用して、変化の激しい脅威に対して継続的に対応します。このサービスは、セキュリティ研究者、データ科学者、倫理的ハッカーのチームによって生成された最新の脅威検知と緩和情報を提供するクラウド ベースのサービスです。

ATP Appliance の脅威分析コンポーネントは、Active Directory、エンドポイントのアンチウィルス、ファイアウォール、セキュア Web ゲートウェイ、侵入検知システム、エンドポイントの検出および応答ツールなどのさまざまなソースの集合から収集したアイデンティティと脅威のアクティビティを包括的に可視化します。分析コンポーネントは、これらのソースからのデータを認識し、高度な悪意の特徴を特定し、イベントを相互に関連付けることで、脅威のキル チェーンを完全に可視化します。セキュリティ アナリストは、ホストやユーザーの展開時にイベントがどのように発生したかを表す包括的なホストとユーザーのタイムラインを受け取ります。このタイムラインでは、マルウェア インシデントのトリアージと調査に取り組んでいる Tier 1 および Tier 2 のセキュリティ アナリストの生産性を向上させることができます。

ATP Appliance は、脅威を緩和するために他のセキュリティ デバイスと統合することができ、ユーザーは、REST API を使用して Google および Office 365 で電子メールを自動的に検疫できます。悪意のある IP アドレスがファイアウォール デバイスにプッシュ送信され、感染したエンドポイントと C&C（コマンドおよびコントロール）サーバーの間の通信がブロックされます。ネットワーク アクセス コントロール デバイスとの統合により、感染したホストを分離できます。ATP Appliance のオープン API アーキテクチャでは、Cisco、Palo Alto Networks、Fortinet、Bluecoat、Check Point、Carbon Black、Bradford など、多数のサードパーティー セキュリティ ベンダーと統合することもできます。

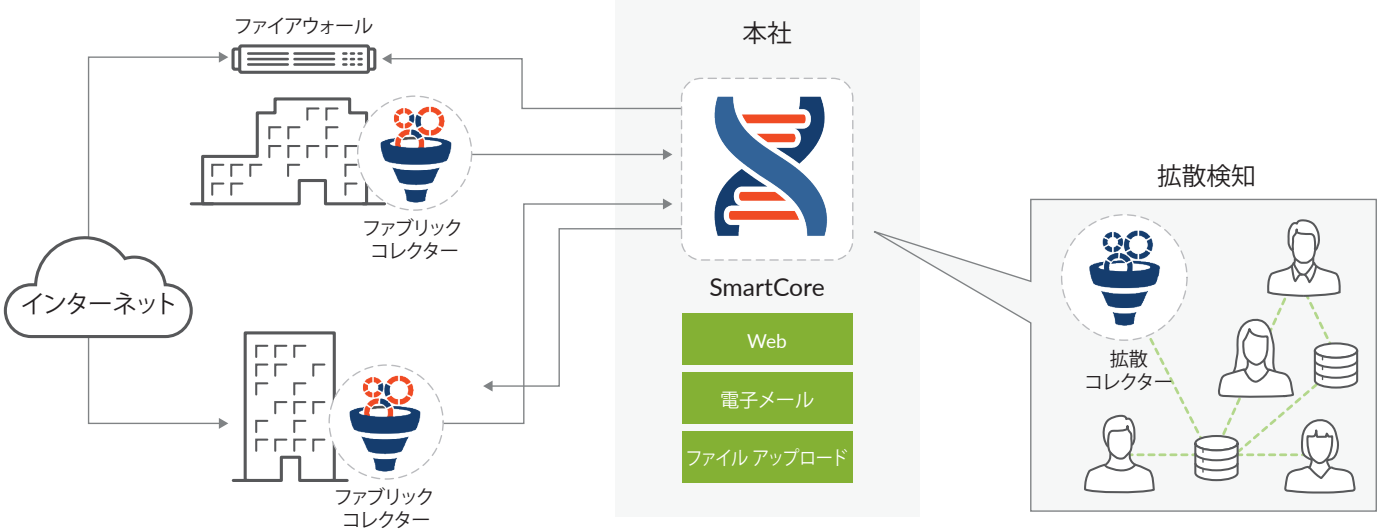

図 1：Juniper Networks ATP Appliance アーキテクチャ

アーキテクチャと主要コンポーネント

ATP Appliance のアーキテクチャは、遠隔地を含むネットワーク内の重要なポイントに配備されたコレクターで構成されています。これらのコレクターは、センサーと同じように機能し、Web、電子メール、および拡散トラフィックに関する情報を取得します。ファブリック全体で収集されたデータおよび関連する実行可能ファイルは、SmartCore 分析エンジンに提供されます。この分析エンジンは、ジュニパーネットワークス SRX シリーズ サービス ゲートウェイと完全に統合されています。SRX シリーズ ファイアウォールがコレクターとして導入されている場合、ソリューションはインライン脅威防止モードで動作できます。ATP Appliance は、ネイティブ コレクターからのトラフィックとともに、Active Directory、エンドポイントのアンチウィルス、ファイアウォール、セキュア Web ゲートウェイ、侵入検知システム、エンドポイントの検出および応答ツールなどの他のアイデンティティおよびセキュリティ製品からのログも取り込みます。ログは、サードパーティー製デバイスから直接取り込むことも、既存の SIEM/syslog サーバーから転送することもできます。

SmartCore 分析エンジンは、さまざまなソースから収集したデータを使用して、次のマルチステージの脅威分析プロセスを実行します。

- **静的解析**：継続的に更新されるルールとシグネチャを適用して、インライン デバイスを回避していた可能性のある既知の脅威を検出します。
- **ペイロード分析**：インテリジェントなサンドボックス アレイを活用して、Windows、OSX、または Android のエンドポイント デバイスを対象にした不審な Web やファイルのコンテンツをデトネーションすることで、マルウェアの動作を深く理解します。
- **機械学習と行動分析**：特許出願中の技術を採用して、長期のマルチコンポーネント攻撃などの最新の脅威の動作を特定し、以前に知られていなかった脅威を迅速に検知します。
- **マルウェア評価分析**：分析結果と同様の既知の脅威とを比較して、新たに検知された脅威が既存の問題の変種であるかまったく新しいものであるかを判断します。
- **優先度の設定、リスク分析、関連づけ**：脅威の重大度、ネットワーク内のターゲット資産、エンドポイント環境、およびキル チェーンにおける脅威の進行に基づいて、脅威に優先度が設定されます。たとえば、深刻度の高い Mac での Windows マルウェアの感染は、中程度の深刻度の保護されたサーバーでのマルウェアの感染よりも低いリスク スコアが与えられます。ATP Appliance およびその他のセキュリティ デバイスからのすべてのマルウェア イベントは、エンドポイントのホスト名と時刻に基づいて関連付けられた後でホストのタイムラインにプロットされるため、セキュリティ チームは脅威のリスクと、迅速に対処する必要があるかどうかを評価できます。たとえば、ATP Appliance によって検知されてもアンチウィルス ソリューションによって検出されなかった脅威は、より高いリスク スコアが与えられます。これにより、セキュリティ チームは過去に戻って、感染したホストで発生した悪意のあるイベントをすべて確認できます。

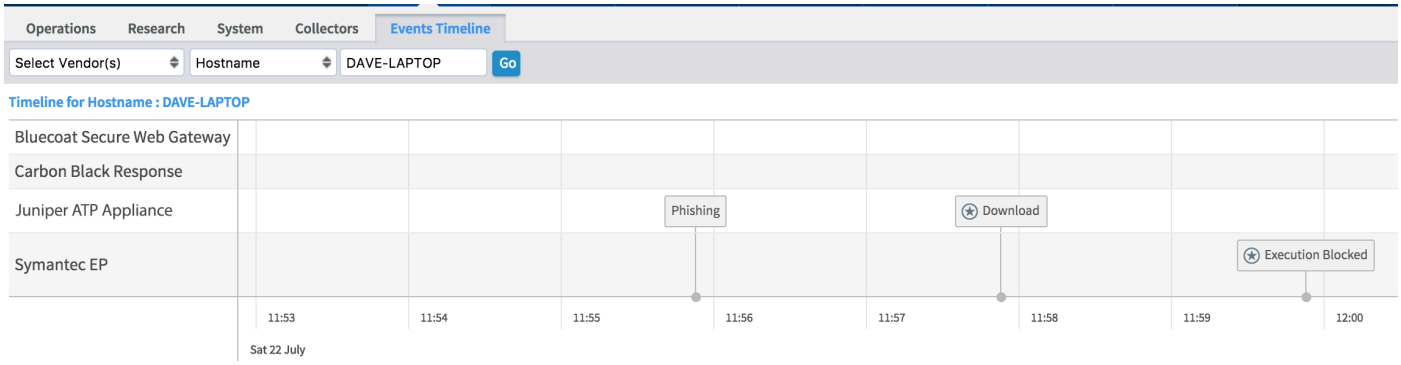

図 2：ATP Appliance イベントのタイムライン

特長とメリット

ATP Appliance には、次の特長とメリットがあります。

- Web、電子メール、拡散など、さまざまな経路のトラフィックを検査します。
- Web UI を通じて不審なファイルをアップロードして処理します。
- Windows 7 および OSX 10.10 オペレーティング システムをサポートします。
- SRX300、SRX4000、SRX5000 の各シリーズ、および SRX550M と SRX1500 に完全に統合されています。Junos 18.1 は、SRX シリーズ統合でサポートされる最小リリースです。
- インライン モードで SRX シリーズ ファイアウォールで使用した場合、インライン ブロック モードで動作します。
- 実行可能ファイル、DLL、Mach-o、Dmg、PDF、Office、Flash、ISO、ELF、RTF、APK、Silverlight、Archive、JAR をはじめとした多様なファイル タイプを分析します。
- exploit 検知、ペイロード分析、C&C（コマンドおよびコントロール）検知、YARA ルール、SNORT ルールなど、検知手法を採用しています。
- サードパーティー製のセキュリティ デバイスと簡単に統合できる、包括的で文書化された API を提供します。
- ジュニパーネットワークス、Palo Alto Networks、Checkpoint、Cisco、Fortinet、Bluecoat の各ソリューションと連係し、悪意のある IP アドレスと URL を自動的にブロックします。
- Office 365 と Gmail の電子メールを自動的に隔離します。
- Carbon Black Protect and Response（エンドポイント ソリューション）と連係し、エンドポイント上で実行されるバイナリのアップロードを可能にします。
- 拡張性に優れたアーキテクチャを通じて複数のセカンダリ コアをクラスタリングできるため、処理能力が向上します。
- MCM（Manager of Central Managers）機能を搭載し、複数のコアを必要とする大規模な導入環境で一元的な管理を可能にします。
- SAML および RADIUS を使用したアクセスと認証をサポートします。
- キル チェーンの各段階でのイベントを関連づけ、脅威の進行状況とリスクを監視します。
- マルウェア活動の可視化とマルウェアのグループ化によって、インシデント対応チームはマルウェアの動作に関する認識を深めることができます。
- 脅威の重大度、脅威の進行状況、資産の価値、その他のコンテキスト データから計算したリスクに基づき、脅威の優先度を設定します。
- ホストをタイムラインで表示し、ホストで発生したマルウェア イベントに関するすべてのコンテキストを取得できます。

製品オプション

ATP Appliance には、物理/仮想の両方の筐体が用意されています。物理アプライアンス（1U JATP400 と 2U JATP700）はオールインワン モード（SmartCore とファブリック コレクターが同じ物理アプライアンスにインストールされます）または分散モード（SmartCore とファブリック コレクターが別のアプライアンスにインストールされます）で導入できます。仮想アプライアンスは、分散モードでのみ導入可能です。MacOS のマルウェア検知もサポートされています。お客様は、セカンダリ コアとして導入できる Mac ミニ ハードウェアを提供する必要があります。MacOS サンドボックス イメージは JATP ソフトウェア ダウンロード ページにあります。

物理

オールインワン

製品番号	パフォーマンス（オブジェクトのデトネーション）[1]	パフォーマンス
JATP400	最大 25,000 オブジェクト/日	1 Gbps
JATP700	最大 61,000 オブジェクト/日	2.5 Gbps

SmartCore

製品番号	パフォーマンス（オブジェクトのデトネーション）[1]	ロギング パフォーマンス
JATP400	最大 50,000 オブジェクト/日	1500 イベント/秒
JATP700	最大 130,000 オブジェクト/日	1500 イベント/秒

[1] 数値は、トラフィックの組み合わせを基にして現実のパフォーマンスを近似しています。実際の数値は、トラフィックの組み合わせ、繰り返しのオブジェクト、ユーザー環境に固有のその他の要因によって異なる場合があります。

コレクター

製品番号	パフォーマンス
JATP400	1.5 Gbps
JATP700	4 Gbps

電子メール MTA レシーバー

製品番号	1 日あたりの最大電子メール数
JATP400	70 万
JATP700	200 万

仮想

サポートされるハイパーバイザー

製品番号	バージョン
VMware vSphere ESXi	5.5, 6.0

Virtual SmartCore

製品番号	パフォーマンス（オブジェクトのデトネーション）	仮想 CPU	仮想メモリ	仮想ディスク
vSC-8	最大 46,000 オブジェクト/日[1]	8	32 GB	1.5 TB
vSC-24	最大 116,000 オブジェクト/日[1]	24	96 GB	1.5 TB

仮想コレクター

製品番号	パフォーマンス	仮想 CPU	仮想メモリ	仮想ディスク
FC-v500M	500 Mbps	4	16 GB	512 GB
FC-v1G	1 Gbps	8	32 GB	512 GB
FC-v2.5G	2.5 Gbps	24	64 GB	512 GB

仮想電子メール MTA レシーバー

製品番号	1 日あたりの最大電子メール数	vCPU 数	仮想メモリ
vMTA-M	72 万	8	16 GB
vMTA-L	140 万	16	16 GB
vMTA-XL	240 万	24	32 GB

JATP700

JATP400

JATP700 仕様

仕様	JATP400	JATP700
重量	13.79 kg（30.4 ポンド）	19 kg（42 ポンド）
外形寸法（幅 x 高さ x 奥行き）	43.7 x 4.3 x 65 cm（17.2 x 1.7 x 25.6 インチ）	43.7 x 8.9 x 63 cm（17.2 x 3.5 x 24.8 インチ）
フォーム ファクター	1 U（ラック マウント型）	2 U（ラック マウント型）
A/C 電源	500 W 高効率（94%+）AC-DC 冗長電源 AC 入力：-100 ～ 240 V、50 ～ 60 Hz、11 ～ 4.4 A	920 W 高効率（94%+）AC-DC 冗長電源 AC 入力：-100 ～ 240 V、50 ～ 60 Hz、11 ～ 4.4 A
DC 電源	650 W 高効率冗長 DC-DC 電源、DC 入力：650 W、 -44 Vdc ～ -74 Vdc、20 A	850 W/1010 W 高効率冗長 DC-DC 電源、DC 入力：850 W： -35 Vdc ～ -42 Vdc、30-25 A
ファン	40 x 40 x 56 mm 13K-11K RPM ファン x 5	8 cm 7 K RPM、4 ピン PWM ファン x 3
動作時温度	10°～ 40° C（50°～ 104° F）	10°～ 40° C（50°～ 104° F）
保管時温度	-40 ～ 70° C（-40 ～ 158° F）	-40 ～ 70° C（-40 ～ 158° F）
相対湿度（動作時）	8 ～ 90%（結露しないこと）	8 ～ 90%（結露しないこと）
相対湿度（保管時）	5 ～ 95%（結露しないこと）	5 ～ 95%（結露しないこと）
高度（動作時）	最大 1,981 m（6,500 フィート）	最大 1,981 m（6,500 フィート）
高度（保管時）	最大 10,668 m（35,000 フィート）	最大 10,668 m（35,000 フィート）
安全規格	CAN/CSA-C22.2 No. 60950-1 Safety of Information Technology Equipment EN 60950-1 UL 60950-1（2nd Edition） IEC 60950-1: 2005/A2:2013	CAN/CSA-C22.2 No. 60950-1 Safety of Information Technology Equipment EN 60950-1 UL 60950-1（2nd Edition） IEC 60950-1: 2005/A2:2013

仕様	JATP400	JATP700
電磁波放射基準認定	47CFR Part 15（FCC）Class A ICES-003 Class A EN 55022 Class A CISPR 22 Class A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 Class A CNS13438 Class A EN 61000-3-3 VCCI Class A KN22 Class A EN 61000-3-2 BSMI CNS 13438	47CFR Part 15（FCC）Class A ICES-003 Class A EN 55022 Class A CISPR 22 Class A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 Class A CNS13438 Class A EN 61000-3-3 VCCI Class A KN22 Class A EN 61000-3-2 BSMI CNS 13438
NEBS	×	×
RoHS	○	○
CPU	10 コア	10 コア x 2
メモリ	32 GB	128 GB
ストレージ	8 TB（2 TB x 4）、RAID 6	900 GB 2.5 インチ 10K SAS x 8、RAID 6
トラフィック ポート	SFP+ 10 GbE x 2、RJ-45 GbE x 4	SFP+ 10 GbE x 2、RJ-45 GbE x 4

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、世界をつなぐ製品、ソリューション、サービスを通じて、ネットワークを簡素化します。エンジニアリングのイノベーションにより、クラウド時代のネットワークの制約や複雑さを解消し、お客様およびパートナーの皆様が日々直面している困難な課題を解決します。ジュニパーネットワークスは、世界に変革をもたらす知識の共有や人類の進歩のリソースとなるのはネットワークであると考えています。私たちは、ビジネス ニーズにあわせた、拡張性の高い、自動化されたセキュアなネットワークを提供するための革新的な方法の創造に取り組んでいます。

米国本社
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

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.0.207.125.700

日本
ジュニパーネットワークス株式会社
東京本社
〒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
西日本事務所
〒530-0001 大阪府大阪市北区梅田2-2-2
ヒルトンプラザウエストオフィスタワー 18階
www.juniper.net/jp/jp

JUNIPER NETWORKS | Engineering Simplicity