ADVANCED THREAT PREVENTION APPLIANCE

製品概要

Advanced Threat Prevention Appliances は、物理的または仮想的なオンプレミス型デバイスで、高度な脅威検知機能を統合セキュリティ分析と組み合わせて、組織を既知および未知のサイバー攻撃から保護すると同時に、セキュリティ運用チームの生産性を向上させます。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を連携することで、ATP Appliances はウェブ、電子メールと水平方向のトラフィックにおける脅威を検知し、ファイアウォールがインライン導入された場合にこれらの脅威をブロックします。ATP Appliances はまた、既存のセキュリティデバイスからログを取り込むことや、コンテキスト分析を適用して、脅威の状況の統合的な見通しを提供することもできます。

製品説明

ジュニパーネットワークス® Advanced Threat Prevention Appliances は、物理的および仮想的なオンプレミス両方での脅威の検知と緩和ソリューションのニーズに対応します。

JATP400 Advanced Threat Prevention Appliance と JATP700 Advanced Threat Prevention Appliance という、2 つのハードウェアプラットフォームが利用可能で、1 日あたり最大 130,000 のファイル処理をサポートします。VMware vSphere または ESXi で運用されている ATP Appliances の仮想バージョンは、8 または 24 の仮想 CPU コアで 1 日あたり最大 116,000 ファイルを処理することができます。

ジュニパー ATP Appliances は、ジュニパーネットワークス SRX シリーズのサービスゲートウェイや独自の内蔵コレクターを使用して、Web、電子メール、および水平方向のトラフィックを収集しており、複数のファイアウォールソリューションを採用する企業に最適です。収集されたデータは、ATP Appliance のオンプレミスに送られて、ATP Appliance コアでさらに処理されます。ATP Appliance コアは、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、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。ATP Appliance では、Palo Alto Networks、Fortinet、Cisco などのベンダーからサードパーティ ファイアウォールのポリシーを更新するという設定も可能です。JATP Appliances は、ジュニパーネットワークス EX シリーズのイーサネットスイッチ、ジュニパーネットワークス QFX シリーズのスイッチ、またはその他のサードパーティのスイッチと連携して、脅威を分離し、ワンタッチでの脅威緩和を活用して被害を受けたホストを隔離し、水平方向での拡散を制限します。

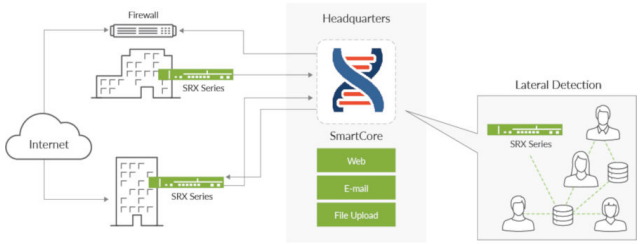

図 1 : Juniper Networks ATP Appliance アーキテクチャ

アーキテクチャと主要コンポーネント

オンプレミス ATP ソリューションでは、インラインの検知とブロックのコレクターとして、SRX シリーズのファイアウォールを使用できます。JATP Appliances は、内蔵コレクターをサードパーティ ファイアウォールで使用することもできます。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 を導入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。外部から隔離された環境の場合、ジュニパー ATP Appliance は、インターネットにアクセ

スできなくてもマルウェアの検知と緩和、さらに相関関係を提供する、プライベートモードでの運用が可能です。

ネットワーク全体で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、JATP400 または JATP700 Appliance にある、SmartCore 検知と分析エンジンに送られます。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。

ATP Appliances は、Active Directory、エンドポイントアンチウィルス、ファイアウォール、安全な Web ゲートウェイ、侵入検知システム、そしてエンドポイント検知とレスポンスツールなど、他のアイデンティティおよびセキュリティソリューションからログを取り込むこともできます。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とイベント管理(SIEM)/syslog サーバーによって転送することができます。

表 1. ジュニパーネットワークス Advanced Threat Prevention Appliance の特徴とメリット

特長	説明	メリット
トラフィックインスペクション	Web、電子メール、水平方向の拡散を含む、複数方向の脅威から保護します。	幅広いプロトコルサポートを提供し、マルウェアとランサムウェアの流通で最も一般的な方法をカバーします
インライン脅威の緩和	SRX シリーズのファイアウォールが導入される場合、インラインブロックを提供します	既知と未知の脅威をブロックする機能を提供します
攻撃分析	サードパーティ セキュリティ ソリューションを含めたネットワーク全体の脅威の状況について、リアルタイムおよび歴史的な見解を提供します	ネットワーク内で相関して発生する脅威アクティビティを可視化し、セキュリティ運用担当者が、優先度の高い脅威を迅速に特定して、対処方法を理解し、アウトブレイクを是正するための隔離を行えるようにします
サードパーティの相互運用性	包括的な API とカスタムメイドのログ取り込みフレームワークが含まれており、サードパーティセキュリティデバイスと容易に統合して、導入済みのセキュリティ製品からの脅威ログ収集とアグリゲーションが可能になります	API を使ったサードパーティ セキュリティデバイスとの統合が容易になり、既存のセキュリティ製品からの脅威ログの収集とアグリゲーションをサポートします
一元管理	MCM (Manager of Central Managers) 機能のマネージャーを含みます	複数のコアを必要とする大規模な導入において、クラスタ化されたコアアプライアンスの、包括的で集中型の一括管理を提供します
柔軟な導入	物理的および仮想的オンプレミスの導入の両方をサポートします	脅威の処理と分析に、高性能な専用ハードウェアを提供します
分散型アーキテクチャ	任意の数のネットワーク拠点に導入可能なコレクターを活用し、本部やクラウドに存在する分析エンジンにすべてのフィードを取り込むことができます。	パブリッククラウドとプライベートクラウドを含むネットワーク全体の、脅威カバレッジが増加します
クラスタリング	拡張可能なアーキテクチャを介して、複数の二次コアのクラスタリングが可能になります	単一以上のアプライアンスが必要な場合、脅威の処理能力を迅速に増加させることができます
認証	SAML と RADIUS を使用したアクセスと認証をサポートします	既存の認証ソリューションと連携します

製品オプション

ATP Appliances は、物理的および仮想的な形式の両方で利用できます。物理的なアプライアンス (1U JATP400 および 2U JATP700) は、オールインワンモード (同じ物理的アプライアンスにインストールされている SmartCore および Fabric Collector) または分散モード (別のアプライアンスにインストールされている SmartCore および Fabric Collector) で導入できます。バーチャルアプライアンスは、分散モードで導入できます。

MacOS のマルウェア検知もサポートされています。お客様は、二次コアとして導入可能な Mac ミニハードウェアを提供する必要があります。MacOS サンドボックス作成の画像は、ATP Appliances のソフトウェアダウンロードページで利用できます。

表 2.ハードウェアアプライアンスパーフォーマンス

製品名	コレクターのパフォーマンス	E-Mail MTA (メッセージ転送エージェント) レシーバー	パフォーマンス (対象物のデトネーション) [1]	ロギング パフォーマンス
JATP400	1.5 Gbps	700,000	最大 50,000 オブジェクト/日	1,500 イベント/秒
JATP700	4 Gbps	200 万	最大 130,000 オブジェクト/日	1,500 イベント/秒

表 3. バーチャルアプライアンス パフォーマンス

製品名	バーチャルメモリ/ディスク	コレクターのパフォーマンス	E-Mail MTA (メッセージ転送エージェント) レシーバー	パフォーマンス (対象物のデトネーション) [1]
バーチャル JATP Appliances ソリューション (8 コア CPU)	32GB/1.5TB	1.5 Gbps	720,000	最大 46,000 オブジェクト/日
バーチャル JATP Appliances ソリューション (24 コア CPU)	96GB/1.5TB	4 Gbps	240 万	最大 116,000 オブジェクト/日

[1] 実際のパフォーマンスに近似するトラフィックミックスに基づいた数。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。

表 4. バーチャルアプライアンスハードウェアの仕様

製品名	ハイパーバイザーサポート	バージョン
バーチャル JATP Appliances	VMware vSphere、ESXi	vSphere (5.5、6.0、6.5) 、ESXi (5.5.1、5.5)

JATP700

JATP400

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	500W 高効率 (94%+) AC-DC 冗長電源；AC 入力：-100～-240V、50～60 Hz、11-4.4 アンプ	920W 高効率 (94%+) AC-DC 冗長電源；AC 入力：-100～-240V、50～60 Hz、11-4.4 アンプ
DC 電源	650W 高効率の冗長電源 DC-to DC 電源供給；DC 入力：650W；-44～-74VDC、20 アンプ	850W/1010W 高効率の冗長電源 DC-to DC 電源供給；DC 入力：850W；-35～-42VDC、30-25 アンプ
ファン	4 x 4 x 5.6 cm (1.6 x 1.6 x 2.2 インチ) 13K-11K RPM カウンター回転ファン、RoHS/REACH	4 x 4 x 5.6 cm (1.6 x 1.6 x 2.2 インチ) 13K-11K RPM カウンター回転ファン、RoHS/REACH
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 情報技術機器の安全性 EN60950-1 UL60950-1 (2nd Edition) IEC60950-1：2005/A2:2013	CAN/CSA-C22.2 No.60950-1 情報技術機器の安全性 EN60950-1 UL60950-1 (2nd Edition) IEC60950-1：2005/A2:2013
電磁波放射基準認定	47CFR パート 15, (FCC) クラス A ICES-003 クラス A EN 55022 クラス A CISPR 22 クラス A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 クラス A CNS13438 クラス A EN 61000-3-3 VCCI クラス A KN22 クラス A EN 61000-3-2 BSMI CNS 13438	47CFR パート 15, (FCC) クラス A ICES-003 クラス A EN 55022 クラス A CISPR 22 クラス A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 クラス A CNS13438 クラス A EN 61000-3-3 VCCI クラス A KN22 クラス 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	8TB (4 x 2TB) 、RAID6	10K SAS の 900GB 2.5 x 8、RAID6
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

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

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands **電話番号：**

+31.0.207.125.700