# Juniper Sky Advanced Threat Prevention

製品概要

Sky Advanced Threat Prevention は、マルウェアから徹底して防御する高度なクラウドベース サービスです。SRX シリーズ サービス ゲートウェイおよび Spotlight Secure 脅威インテリジェンス プラットフォームと統合された Sky Advanced Threat Prevention は、絶え間なく変化を続ける脅威環境に適応できるダイナミックなアンチマルウェア ソリューションです。

## 製品説明

マルウェアが進化してより高機能になるにつれて、従来のアンチマルウェア製品ではこれらのタイプの攻撃を効果的に防御することがますます難しくなります。ジュニパーネットワークス Sky Advanced Threat Prevention は、ネットワークの侵入トラフィックと退出トラフィックを監視して、マルウェアおよび他のセキュリティー侵害の兆候を探すことにより、高機能な「ゼロデイ攻撃」や未知の脅威に対して、高度なアンチマルウェア保護を実現します。Sky Advanced Threat Prevention がクラウドからテクノロジに関する情報を入手して行う漸進的な判定では、各種の潜在的攻撃のリスク レベルを評価し、脅威から高精度で保護します。クラウドで安全にホスティングされた Sky Advanced Threat Prevention は、ジュニパーネットワークス SRX シリーズ サービス ゲートウェイと統合して、ディープ インスペクション、インライン マルウェア ブロッキング、アクショナブル レポーティングを行います。

Sky Advanced Threat Prevention の識別テクノロジでは、様々な技法を使用して脅威をすばやく見つけ出し、迫り来る攻撃を防御します。既知のファイルを見つけ出すキャッシュ迅速検索から、サンドボックス環境でマルウェアを騙してアクティブ化させて自己特定させるユニークな偽装技法を用いた動的解析まで、様々な防御方法が適用されています。マシン ラーニング アルゴリズムにより Sky Advanced Threat Prevention は、絶え間なく変化する脅威環境で新型マルウェアに適応して、見つけ出すことができます。

巨大なデータセットの複数の属性と振る舞いを考慮に入れる進化技術により、Sky Advanced Threat Prevention はゼロデイ攻撃を見つけ出して、攻撃者がネットワークに潜入する前に脅威を除去することもできます。マルウェアのシグネチャは、いったん識別されると検索キャッシュに記録されるので、その後に発生する同様の攻撃をすぐにくい止めることができます。

## アーキテクチャと主要コンポーネント

Sky Advanced Threat Prevention はすべての管理、構築、通知において、ジュニパーの最新の SRX シリーズ ファイアウォール プラットフォームとクラウドベースのサービス コンポーネントを活用しています。

Sky Advanced Threat Prevention の漸進的パイプライン解析エンジンは、既知の脅威のデータベースに対するキャッシュ検索を、スタートしてから 2 秒以内で完了します。疑わしいファイルは、マルウェアを積極的に見つけ出そうとする一連のディープ インスペクション ステップを経なければなりません。複数のアンチウィルス エンジンによる処理と静的解析が連動して脅威を見つけ出そうとします。あるファイルが解析によりマルウェアであると特定されると、そのシグネチャがキャッシュに追加されるので、脅威がその後繰り返されてもすぐに見つかります。

最後に、動的解析がサンドボックス環境で適用されて、そこで脅威は「デトネーション（爆発）」が観測されます。マルウェア反応を引き出して自己識別するためにユニークな偽装技法が採用されています。脅威はもっと広範な解析段階でそっと通り過ぎようとしても見つかり、記録、報告されるので、セキュリティー担当者が簡単に攻撃を防御できます。感染したホストは自動的に隔離されて、外部ネットワークへアクセスできなくなります。

Your ideas.Connected.™

## 特長とメリット

検出とポリシー適用で SRX シリーズ ファイアウォールと統合することで、Sky Advanced Threat Prevention は既知のマルウェアや高度なゼロデイ攻撃の脅威に対して動的な自動保護メカニズムを作動させるので、瞬時の脅威対応が可能になります。

特長や機能を以下に示します。

- 感染したファイルが抽出されてクラウドへ送られ、ディープ インスペクションと解析が行われます。Sky Advanced Threat Prevention は、クラウドからテクノロジに関する情報を入手し、既知の脅威を迅速に見つけ出す高速メソッドからファイルを詳しく検査する高度なアプローチまであらゆる手段を最大限に活用して、より高度で回避的なマルウェアを探します。
- マルウェアを迅速に見つけ出して（高速判定）、その情報を瞬時に SRX シリーズ ファイアウォールに伝えて、悪意のあるトラフィックをブロックします。
- 高度化したマルウェアを徹底解析してファイル実行中の振る舞いを、制御された動的環境の中で観測する—サンドボックス技法では、動的解析と「デトネーション」を使用します。
- Web ベース ポータルを介した製品ライセンス、製品構成、詳細レポート作成などのサービス管理充実した内容のレポートと分析から、お客様のネットワークにどんな脅威が侵入しているか、組織内のどのホストが感染しているかをしっかり把握できます。
- Spotlight Secure 脅威インテリジェンス プラットフォームと緊密に連携しているので、感染したホスト情報を SRX シリーズ ゲートウェイに転送して、お客様が指定した措置を直ちに取ることができます。コマンド アンド コントロール（C&C）サーバーのリストを SRX シリーズ ファイアウォールに提供することで、感染した内部システムがこれらのデバイスと通信できなくなります。
- 内部ホストが感染したサーバーと通信しようとすると、SRX シリーズ ファイアウォールを介して警報を発して、Sky Advanced Threat Prevention サービスに警告するので、組織は社内でのさまざまな「感染の兆候」に関する豊富なデータを得ることができます。
- 分析機能を介してデータを分析して関連付けることにより、管理者やセキュリティー担当者は感染したシステムを特定して、この情報を SRX シリーズ ゲートウェイへ送って、感染したシステムを隔離できます。

## 製品のオプション

Sky Advanced Threat Prevention のライセンスには、無料バージョンとプレミアム サービスの 2 種類があります。無料バージョンの Sky Advanced Threat Prevention では基本ファイル タイプ（.exe のみ）を分析でき、アンチウィルス解析、統計解析、疑わしいファイルの動的解析および詳細情報通知など Sky Advanced Threat Prevention アンチマルウェア技術の全機能がついています。

プレミアム サービスではサポートされるファイル形式が無料バージョンよりも多く（.exe、pdf、MS Office スイート ファイルの .doc、.ppt、.xls など）、さらに詳細なレポート機能と、静的解析と動的解析を含むすべての Sky Advanced Threat Prevention アンチマルウェア識別スタックが搭載されています。詳細レポート機能が強化されているので、Sky Advanced Threat Prevention の高度な識別技法で見つかった感染ホストをセキュリティー担当者が容易に防御できます。プレミアム バージョンも感染したホストを隔離して、C&C サーバーとの通信をブロックします。

## 仕様

Sky Advanced Threat Prevention には、最新バージョンの ジュニパーネットワークス Junos® オペレーティング システム（15.1）で動作する SRX シリーズ ファイアウォールが必要です。ジュニパーネットワークス SRX1500 サービス ゲートウェイ プラットフォームにはサポートがリリース時に含まれています。vSRX および他のすべての SRX シリーズ プラットフォームでは将来のリリースでサポートが予定されています。

## 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、ネットワークイノベーション事業に従事しています。デバイスからデータセンターまで、消費者からクラウドプロバイダまで、ジュニパーネットワークスはネットワークの使い勝手や経済性を向上させるソフトウェア、シリコン技術やシステムを提供しています。ジュニパーネットワークスは、世界中のお客様とパートナー企業のために尽力しています。詳しい情報は、www.juniper.net/jp/ をご覧ください。

**米国本社**
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話：888.JUNIPER（888.586.4737）
または +1.408.745.2000
FAX：+1.408.745.2100
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：+31.0.207.125.700
FAX：+31.0.207.125.701

ジュニパーネットワークスのソリューションの購入については、03-5333-7400 にお電話いただくか、認定リセラーにお問い合わせください。



1000549-001-JP　2015 年 12 月