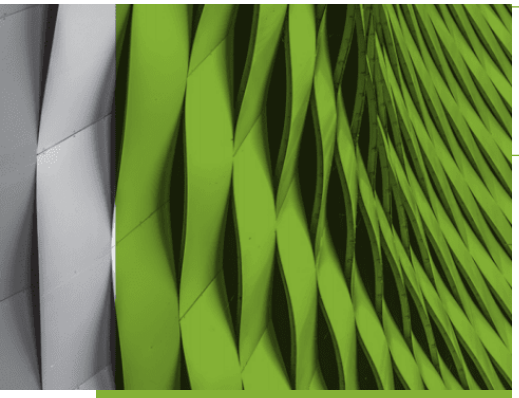

JUNIPER SECINTEL のデータシート

製品概要

Juniper SecIntel は、ネットワーク内のすべての接続ポイントに脅威インテリジェンスを拡張することで、悪意あるトラフィックをブロックし、脅威を検知できるネットワークを提供します。SecIntel を WAN エッジ、有線および無線 LAN 全体（脅威の可視性を高めるため）、ネットワーク内の適用ポイントに展開する事でリスクを軽減できます。

製品説明

Juniper ® Connected Security は、ネットワークやクラウドから侵入する脅威を可視化し、これらの脅威を分析、解読および優先順位付けて、推奨されるアクションをジュニパーのファイアウォール、スイッチ、ルーターにプッシュします。これにより、ネットワークとクラウドの全体像が把握でき、脅威を認識した上で環境を構築することができます。

ジュニパーが考える本当に安全なネットワークには脅威認識が不可欠です。脅威認識ネットワークには、高いネットワークの可視性と、あらゆる接続ポイントにポリシーを適用できる機能の両方が必要です。ジュニパーが特許を取得しているワンクリック自動化機能を含むファイアウォール オーケストレーションは、シンプルな管理オプションの一例です。ポートレベルでトラフィックをブロックするポリシーの自動作成と配布が可能になり、管理者はユーザー、アプリケーション、インフラストラクチャを保護することができます。これこそがセキュリティインテリジェンス（SecIntel）の力なのです。

SecIntel は、ジュニパーデバイスなど、複数のソースからデータを集約したセキュリティ脅威インテリジェンスをフィードし、それを厳選・統合して実用的なインテリジェンスを提供します。これらのフィードは、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のほか、非セキュリティデバイスである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、EX シリーズおよび QFX シリーズスイッチ、さらには企業全体に導入されている Mist 無線ソリューションにも配信されます。これらの脅威インテリジェンスフィードには、Juniper Threat Labs が厳選した脅威情報、Juniper Advanced Threat Prevention（ATP）クラウドベースサービスを介して取得した脅威情報、さらにお客様が自社のソリューションに統合できる業界固有の脅威をカバーするサードパーティーサービスからの脅威データや脅威情報などが含まれます。

被害が出る前にネットワーク上の攻撃をすべて特定して抑え込むことで、ユーザー、アプリケーション、加入者ネットワークを含むインフラストラクチャを侵入から守り、インフラストラクチャを追加することなく接続レイヤーをセキュリティレイヤーに変えることができます。

Juniper Threat Labs は、SecIntel のダイナミックに且つ自動的に脅威インテリジェンスフィードの更新を提供します。ジュニパーのグローバルな専門チームは、センサーやセキュリティの研究者やアナリストで構成され、新たな脅威と侵入技術に関して迅速かつ実用的なインサイトを提供します。さらに Juniper Threat Labs は、その他大勢のセキュリティベンダー、アライアンス、パートナーシップと緊密に連携して、脅威インテリジェンス エコシステムの成長に尽力しています。

NSS Labs が最近行ったデータセンターセキュリティゲートウェイテストの結果、ジュニパーは、悪意ある攻撃の検知・特定で 99% 以上、侵入の検知・特定で 100% という推奨評価を獲得しました。ICSA Labs が四半期ごとに行う高度な脅威への防御評価において、SecIntel を含むジュニパー ATP クラウドは、最新の悪意ある攻撃の検知率がほぼ 100% でした。

SecIntel の脅威フィードは、トラフィックのフィルタリングや自動化されたインシデント 対応のオーケストレーションに使用されます。脅威フィードは、脅威認識ネットワークの重要な構成要素であり、これにより、IT チームはネットワーク リスクを軽減しながら、可視性とセキュリティを向上させることができます。

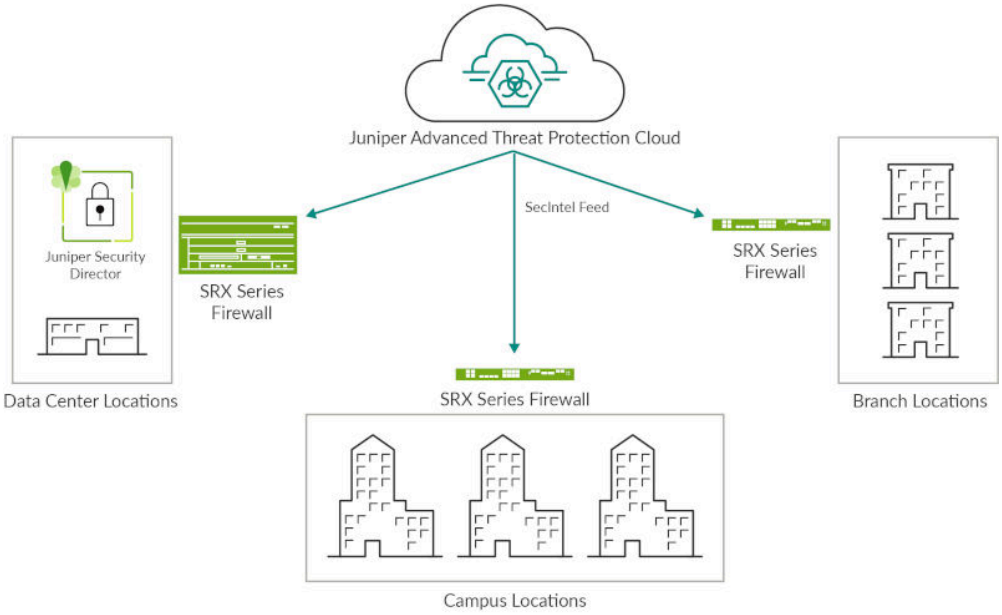

図 1 : SRX シリーズ ファイアウォールでの SecIntel

アーキテクチャと主要コンポーネント

SRX シリーズ ファイアウォールで SecIntel 脅威フィードを使用すれば、ネットワークとアプリケーションの両レイヤーでトラフィック フィルタリングが可能になり、既知の脅威を特定して対処することができます。ATP クラウドが SecIntel を通じて提供する脅威インテリジェンスには、攻撃者の IP、コマンド & コントロール（C&C）、GeoIP、感染したホスト、動的アドレスグループ、グローバル許可リストおよびカスタムされた許可リスト、さらにブロックリストに含まれるファイルハッシュ、ドメイン名、IP アドレス、悪意ある URL、コード署名証明書、署名者組織が含まれています。SRX シリーズ ファイアウォールは設定で、受動的に監視· 警告を行うか、SecIntel を使って検知した脅威を監視· ブロックするか選択することができます（図 1 参照）。

MX シリーズルーターも、SecIntel の脅威フィードに対応しており、ジュニパー ATP クラウドが提供する C&C トラフィックと、カスタムされた許可リストとブロックリストを使って、脅威を識別ブロックすることで、ネットワークセキュリティに追加レイヤーを提供します。この機能がルーターの役割を単純な接続レイヤーから、脅威認識ネットワーク デバイスに進化させます。

脅威認識ネットワークは、能動的に自分のネットワークを防御します。SecIntel 脅威フィードを MX シリーズルーターに取り込むことで、組織はハードウェアを追加せずに、自動化された防御レイヤーを得ることができます。脅威を認識する MX シリーズルーターは、脅威がファイアウォールに到達する前にブロックします。これにより、負荷の高いファイアウォールの演算コストが軽減され、今まではカバーできなかったデータ フローの保護が可能になります。SRX シリーズファイアウォールと同様に、MX シリーズルーターの設定でも、受動的に監視警告を行うか、SecIntel を使って検知した脅威を監視ブロックするか選択することができます（図 2 参照）。

通常、ルーターとファイアウォールはネットワークエッジに配置します。一方で情報セキュリティのベスト プラクティスとしては、危険なポイントの出来るだけ近くでポリシーを適用する必要があります。EX/QFX シリーズスイッチ向け SecIntel は、侵入されたホストがネットワークのどこにあってもホストを特定およびブロック、または隔離して、脅威が横方向に伝搬するのを防ぎます。

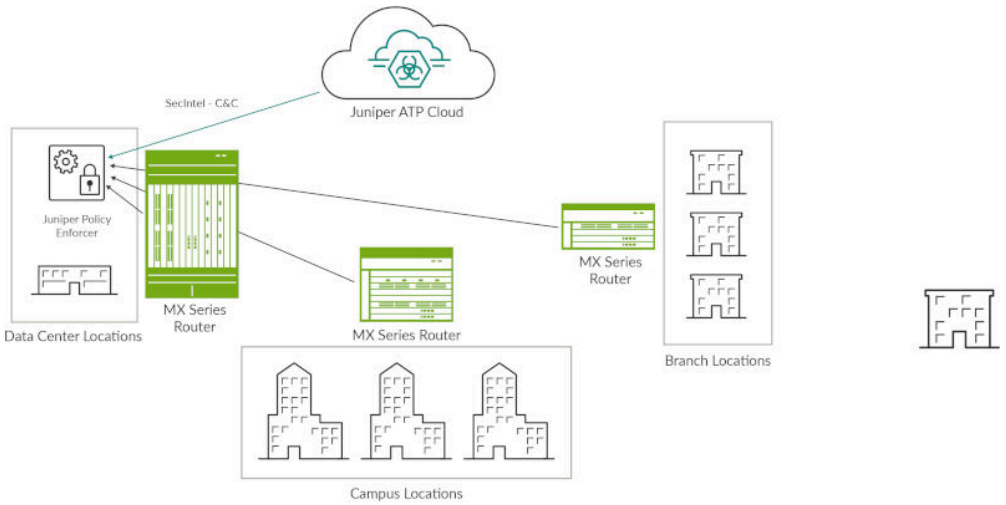

図 2 : MX シリーズルーターでの SecIntel

EX/QFX シリーズのスイッチは、SecIntel が ATP クラウド経由で動的に更新する感染ホストフィードを用いることで、侵入されたホストを素早く特定し、自動的にネットワークから隔離して、ネットワークからのアクセスをブロックします。結果として、ネットワーク上のすべての接続ポイントにポリシーが適用され、脅威認識ネットワークの構築に必要なネットワークの詳細な可視性を得ることができます (図 3 参照) 。

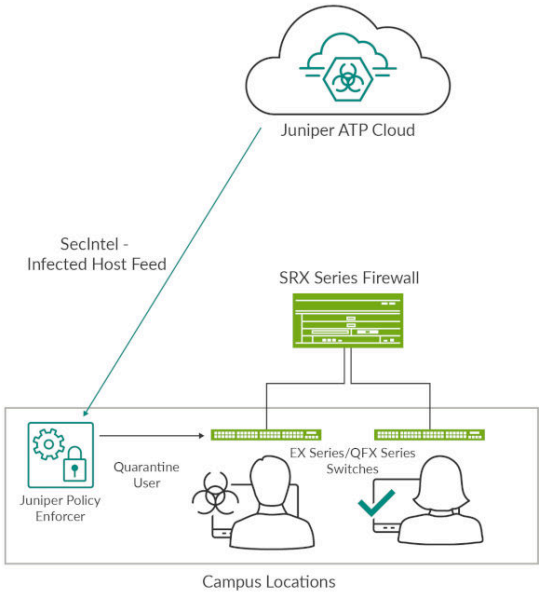

図 3 : EX/QFX シリーズスイッチにおける SecIntel

特長とメリット

特長	説明	メリット
厳選された脅威インテリジェンス	SecIntel は、悪意ある IP、URL、ドメイン、GeoIP など Juniper Threat Labs が提供する厳選された脅威フィードを使用しています。 SecIntel の情報は、Juniper Threat Labs が常に更新し、スクラブと検証を行っています。	常時厳選され、更新された脅威データが提供され、脅威の網羅性は向上し、誤検知を減らすことができます。 最新の脅威データを使えば既知の攻撃による侵入リスクを軽減できるため、セキュリティ チームは未知の脅威に備える時間を確保することができます。
感染したホストのフィード	SecIntel は、感染したホストのフィードとカスタムされた脅威フィードを使用します。 ジュニパー ATP クラウドが提供する脅威フィードには、ネットワーク上で感染が判明している全ホストのリストを含めた感染したホストのフィードが含まれています。	セキュリティ イベントを自動的に検知しイベントの発生を防ぎます。また、発生したイベントを特定し、発生源付近でブロックします。
脅威インテリジェンスのカスタマイズ	脅威フィードをカスタマイズすることで、サードパーティによる業界固有の脅威対策や防御データなど、独自のデータ ソースを追加することができます。	セキュリティ オペレーション チームには、サードパーティが提供する業界固有の脅威インテリジェンスにも追加可能な汎用性の高い入力データが提供されます。
ネットワーク全体で認識した脅威を識別してブロック	SecIntel は、既知の脅威を識別して受動監視するか、ブロックする機能を提供します。この機能は、ネットワーク エッジ、ネットワーク コア全体、有線・無線ネットワークを含むアクセス レイヤーで実行できます。	アドオンとしてではなく、ネットワーク インフラストラクチャ内のネイティブ セキュリティとして、ネットワーク スタックにセキュリティを追加することができます。通常ならセキュリティインテリジェンスに見なされないようなネットワークリソースを、ネットワーク上の識別やポリシー適用ポイントとして活用します。
包括的な脅威ログ機能とオーケストレーション	SecIntel からの脅威ログを、セキュリティ情報およびイベント管理 (SIEM) やジュニパーネットワークス Secure Analytics などのログ管理ツールや Junos Space Security Director Policy Enforcer などのオーケストレーション プラットフォームに送信します。これにより、ネットワークの可視性が向上し、インシデント対応の自動化が可能になります。	追加のデータ ポイントを相互に関連付けて、未知の脅威を発見するだけでなく、それらの脅威に必要な修復を迅速に施すことが可能です。一回の侵入にかかる全体的なコストを削減し、ビジネス内に進行する脅威に対するインサイトを提供できます。

注文情報

Juniper SecIntel ライセンスのご注文や、ソフトウェアライセンス情報へのアクセスをご希望の場合は、購入方法ページ (https://www.juniper.net/jp/ja/how-to-buy/) をご覧ください。

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/

Juniper Networks Driven by Experience