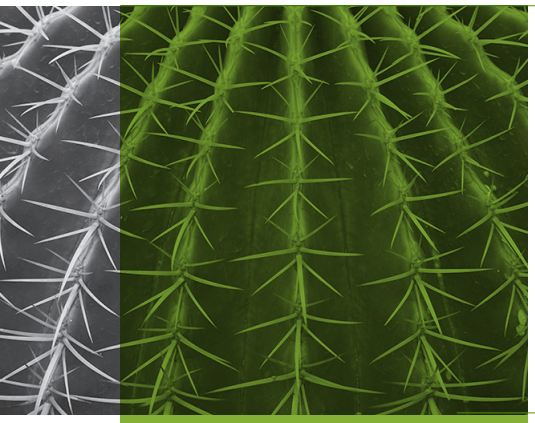

JUNIPER CONNECTED SECURITY ソリューション

ビジネスの継続性を損なわずに脅威の自動修復を実現

課題

ますます巧妙化する、ネットワークを脅かす攻撃に対抗するために、企業は進化し続けることが求められています。しかし、セキュリティを重視する余り、しばしば他の重要なアクティビティが犠牲となり、組織においてネットワークセキュリティとビジネスの継続性が両立しないという課題を引き起こすこともあります。

ソリューション

企業に必要なのは、一元化されたポリシー、分析、および管理を備えたオープンなマルチベンダー エコシステムで、ネットワークとセキュリティ要素を同様に活用して、従来のネットワークをセキュアなネットワークへと変革するという相乗効果をもたらすアプローチを採用することです。

メリット

- エンドポイントからエッジまで、そしてその間の各クラウドで、セキュリティの適用を自動化する
- ネットワーク上に誰がいて何があるかを把握し、すべての接続ポイントにポリシーを適用する
- ネットワーク内でセキュリティ適用ポイントの数を増やし、きめ細かい隔離機能を導入する
- 迅速で自動化された脅威修復機能を実行する
- クラス最高のネットワークを構築する

過去数十年の間に、ネットワーク導入は大きく変化してきました。企業は急速にクラウドに移行し、IoT（モノのインターネット）やブロック チェーンなどの新たな技術を採用していますが、これらはすべてネットワークに大きく依存します。

このような企業では、新しいインフラストラクチャや既存のインフラストラクチャを保護するために、セキュリティへの支出も増加していますが、ブリーチ（抜け穴）も減ることはありません。現在もなお、内部記録や顧客情報が盗まれ、最高の値段を付けた何者かに売却されて、企業の評判に修復不可能な損害を与えています。では、これらの企業は、ネットワーク セキュリティに対するアプローチにおいて不可欠な何かが欠けているのでしょうか？

課題

今日、きわめて効果的なセキュリティの技術やソリューションが多数あります。たとえば、次世代ファイアウォール、サンドボックス、CASB（クラウド アクセス セキュリティ ブローカー）、SIEM（セキュリティ情報およびイベント管理）、エンドポイント保護などが挙げられます。しかし、ネットワークのセキュリティ レベルは、そのネットワークの最も弱いリンクを基準として判断されます。また、すべてのネットワーク構成要素の間で緊密なコラボレーションと同期化が実現されていない限り、大きなセキュリティ ホールが残り、企業は攻撃に対する脆弱性を解決できません。主な利害関係者達は、一般的なセキュリティ製品に対して多額の投資をしても、期待したほどの保護が得られないという現実に直面しています。

一般的なインフラストラクチャとセキュリティ製品を使用している企業における脅威の拡散

それでは、クライアント、エンドポイント、アクセス スイッチ、無線アクセス ポイントを備えた一般的な企業環境について見てみましょう。エンタープライズ環境における境界では、アンチマルウェア サービスに接続された次世代型ファイアウォールが使用され、垂直方向の脅威から保護しています。クライアントの種類やモデルによっては、エンドポイントの防御ソフトウェアを使用できます。IoT、ネットワーク プリンター、新しい種類のエンドポイントでは、この保護を利用できません。

ネットワーク侵害のワークフロー

図 1 は、侵害されたネットワークの図です。これらのブリーチ（抜け穴）は通常、予測可能なパターンをたどります。

1. クライアントが未知のマルウェアのダウンロードを試行します。
2. 境界のファイアウォールでファイルがスキャンされます。
3. ファイアウォールが、そのファイルをアンチマルウェア サービスに分析のために送信すると、アンチマルウェア サービスはそれがマルウェアであることを通知します。

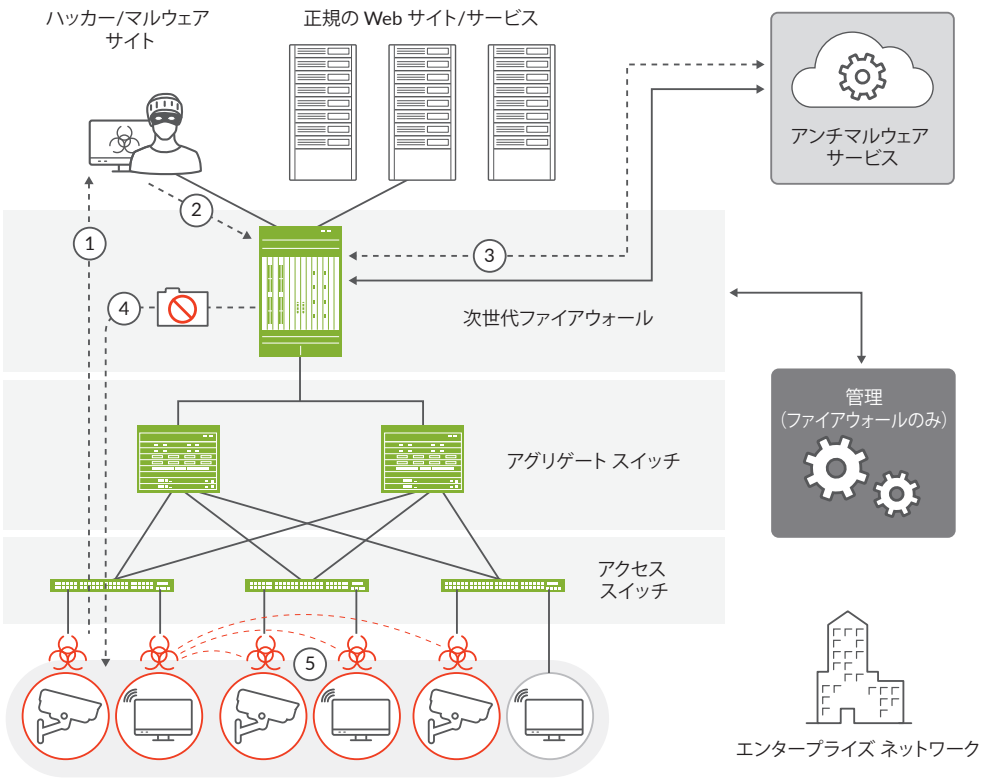

図 1：一般的なインフラストラクチャとセキュリティ製品を使用している企業において侵害されたネットワーク

4. ファイアウォールがそのファイルをブロックし、ダウンロードを阻止します。
5. しかし、もしクライアントがコーポレート ネットワークの外部（「非エンタープライズ」環境）で侵害されていたり、手動による手段で侵害されていたりする場合、ネットワーク内の到達可能なすべてのホストに感染が拡大します（脅威の種類に基づきます）。

結果は、以下のとおりです。

a. クライアントがコーポレート ネットワークの外部から到達されることを単純に阻止するだけでは効果がなく、水平方向への脅威の拡散を防止できません。

b. セキュリティ ソリューションがネットワーク コンポーネントと通信できず、それらを利用できない場合は、可視性が低下し、セキュリティを適用できるポイントの数が制限されます。

c. ロギング サーバー、エンドポイント、およびその他のネットワーク構成要素など、さまざまなナレッジ ソースから異常な動作に関するレポートが提供されても、それらを集約できなければ、セキュリティ戦略における大きな弱点になります。

d. セキュリティ戦略は、ファイアウォールへの依存度が大きいため、ファイアウォール ポリシーの複雑さがセキュリティ チームの大きな負担になります。企業がグローバルに展開している場合は、この問題がさらに拡大します。

ジュニパーネットワークスの Connected Security

Juniper Networks® Connected Security は、ネットワーク全体のすべての接続ポイントにセキュリティを拡大し、他のベンダーの技術とも共存できる方法で、組織によるユーザー、アプリケーション、およびインフラストラクチャの保護を支援します。Juniper Connected Security は、ポリシー、検知、およびポリシーの適用作業と包括的な製品ポートフォリオを組み合わせて、セキュリティを一元化および自動化します。

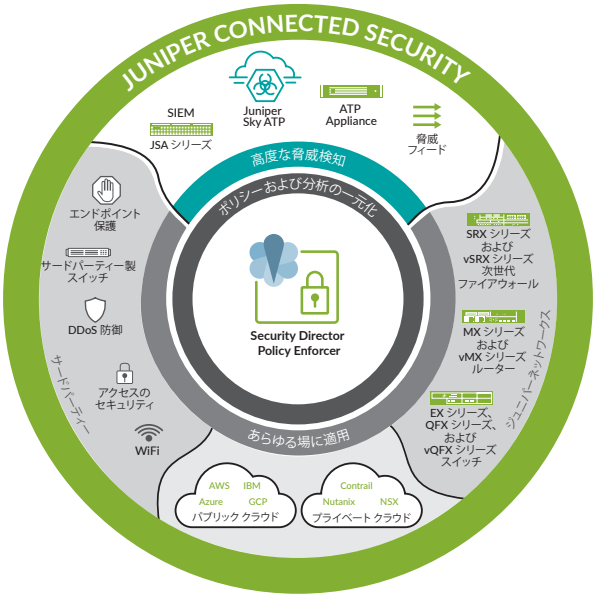

図 2：Connected Security の構成要素

Juniper Connected Security の構成要素

Juniper Connected Security は、以下のコンポーネントで構成されます。

1. 高度な脅威検知エンジン：
   a. Juniper Sky Advanced Threat Prevention（ATP）はクラウドベースのマルウェア検知ソリューションにより、既知および未知の脅威を正確に検知します。
   b. Juniper Networks® Advanced Threat Prevention Appliance は、高度な脅威を検知する、オンプレミスの分析プラットフォームです。
   c. 既知の脅威は、C&C（コマンドおよびコントロール）サーバー、GeoIP、REST API を介したサードパーティー製デバイスなどの多様なソースから得た脅威フィード情報と、社内のログ サーバーから取得した情報を統合して検知します。
   d. 未知の脅威は、Juniper Sky ATP または ATP Appliance がサンドボックス、機械学習、脅威ディセプションなどの技術を使用して特定します。
2. 管理、ポリシー、および分析の一元化：
   a. Juniper Networks Junos® Space Security Director は、単一の管理ポイントによりセキュリティ ポリシーの管理を向上させる、拡張性と即応性に優れたセキュリティ管理アプリケーションです。
   b. Policy Enforcer は、Security Director のコンポーネントです。一元的でインテリジェントなモジュールとして、以下の機能を提供します。
      - マルチベンダーのネットワーク構成要素や次世代型ファイアウォールなどのセキュリティ製品と通信して、セキュリティ ポリシーをグローバルに適用し、分析を行います。
      - 社内の多様なソースから得た脅威インテリジェンスを統合します。
3. あらゆる場へのセキュリティの適用：
   a. あらゆるネットワーク構成要素をポリシー適用ポイントとして活用します。
   b. オープンなマルチベンダー エコシステムを採用し、ジュニパーのソリューション、クラウド、サードパーティー エコシステム全体の脅威を検知してセキュリティを適用します。
   c. 垂直方向または水平方向への脅威の拡散を防止するため、迅速に脅威をブロックまたは隔離する機能を提供します。

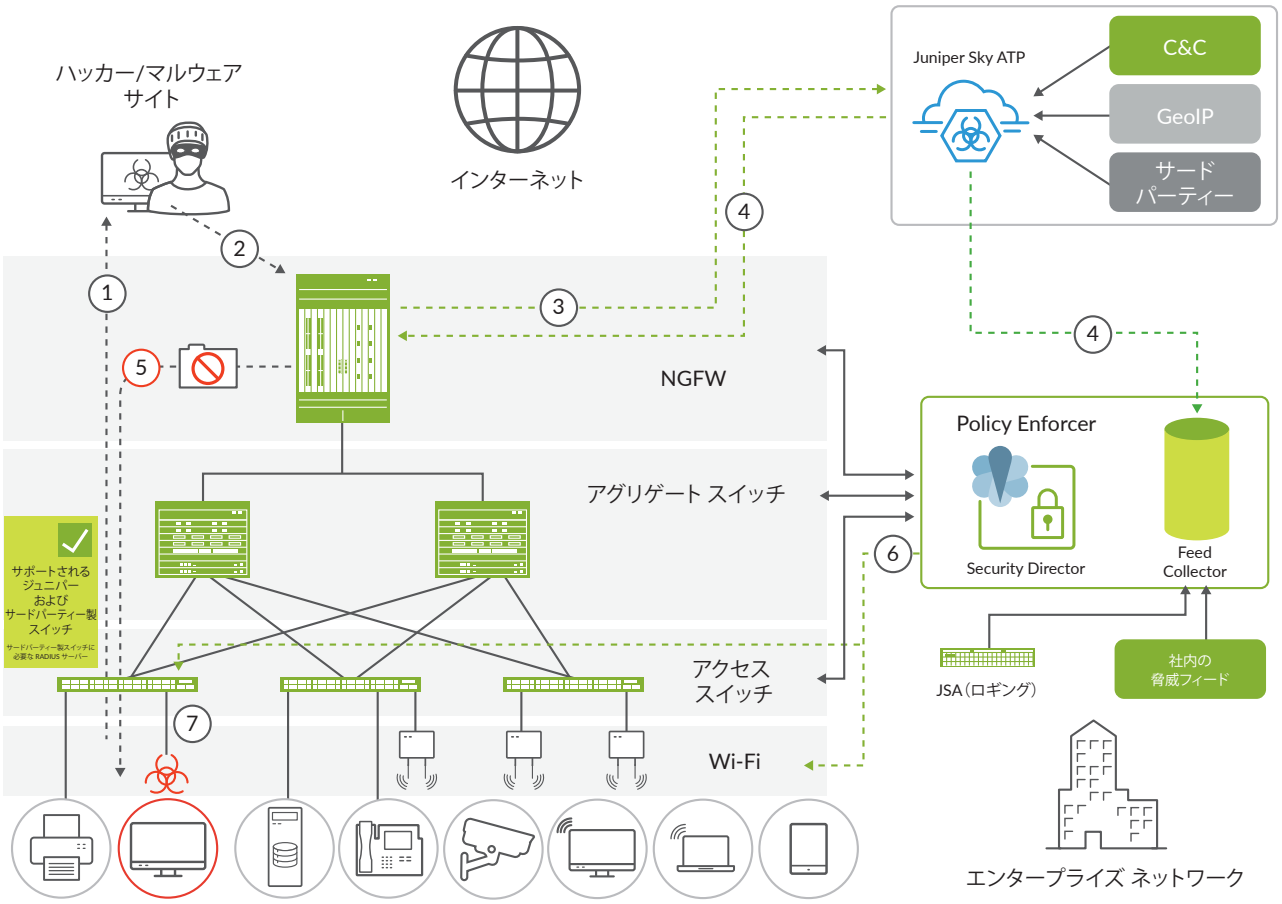

図 3：Juniper Connected Security および Juniper Sky ATP によるセキュアなネットワーク導入

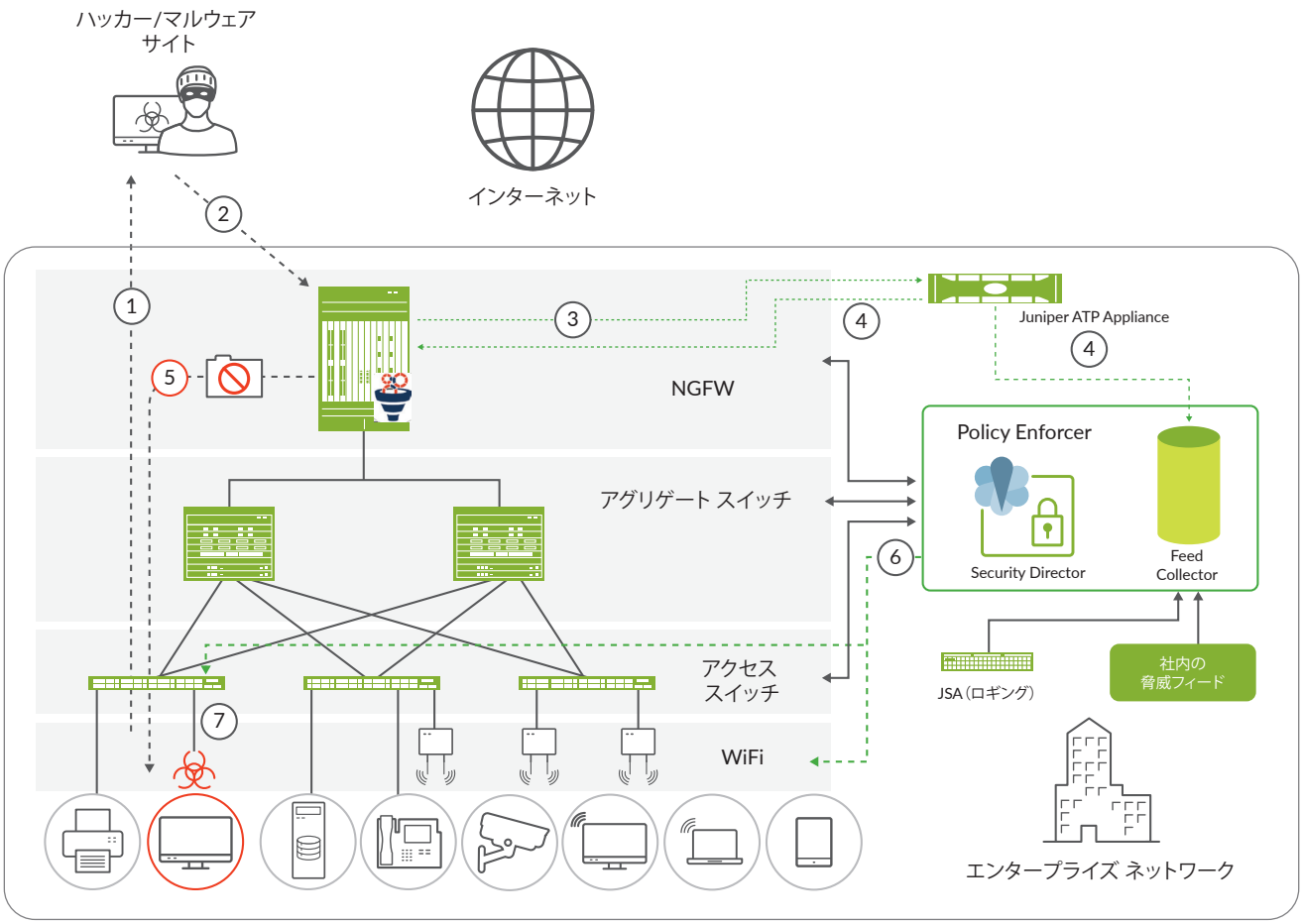

図 4：Juniper Connected Security および JATP Appliance によるセキュアなネットワーク導入

Juniper Connected Security によるセキュアなネットワーク導入

それでは、アンチマルウェア サービスを提供する Juniper Sky ATP、または、Juniper ATP Appliance に接続した境界のファイアウォールとして、ジュニパーネットワークス SRX シリーズ サービス ゲートウェイを導入した Juniper Connected Security ネットワークを見てみましょう。Security Director の Policy Enforcer は、次世代型ファイアウォールを含めた様々なネットワーク構成要素と通信して、セキュリティ ポリシーをグローバルに適用するための、一元的かつインテリジェントなコンポーネントです。

Policy Enforcer の Feed Collector モジュールは、クラウドやオンプレミスのデバイスからロギングとともに受け取った脅威フィードと、社内の脅威フィードを統合します。クライアント/エンドポイントは、エンドポイント防御ソフトウェアが適用されたアクセス スイッチや無線アクセス ポイントに接続されます。IoT デバイス、プリンター、新しい種類のエンドポイントにはこの防御機能はありませんが、Policy Enforcer がアクセス デバイスと通信して情報を共有し、必要に応じてセキュリティを適用します。

Juniper Connected Security は、セキュリティ違反の現状を一変させます。ではここで、ジュニパーネットワークスの保護されたネットワークが攻撃されたときの 2 つのシナリオを見て行きましょう。

ワークフロー 1：マルウェアのダウンロード

1. クライアントが未知のマルウェアのダウンロードを試行します。
2. 境界の SRX シリーズ ファイアウォールによってファイルがスキャンされます。
3. SRX シリーズ ファイアウォールが、そのファイルを Juniper Sky ATP または ATP Appliance に送信します。
4. Juniper Sky ATP または ATP Appliance によって、ファイルがマルウェアであると判断されると、それが SRX シリーズ ファイアウォールと Policy Enforcer に通知されます。
5. SRX シリーズ ファイアウォールが、ファイルのダウンロードをブロックします。
6. さらに詳細な調査が可能になるまで、Policy Enforcer によって、ホストが（スイッチにある）特別な VLAN に隔離されます。また、Policy Enforcer には、クライアントが接続しているスイッチ ポートや Wi-Fi アクセス ポイントを無効にするオプションもあります。
7. これで、ターゲットになったクライアントによるネットワーク内の他のホストへの感染を食い止めることができました。垂直方向と水平方向へのマルウェア拡散が停止しました。Policy Enforcer はクライアントを記憶するため、対象のクライアントが別のスイッチや Wi-Fi アクセス ポイントに移動した場合でも、Policy Enforcer が脅威を認識し、ネットワークからブロックします。

ワークフロー 2：IoT デバイスへの感染

1. ネットワークに接続された IoT デバイスが感染して、制限されたファイルのダウンロードを試行、または重要なインフラストラクチャへの攻撃を開始します。
2. 不正なダウンロード試行が Juniper Secure Analytics（JSA）によってログに記録され、Security Director の Policy Enforcer に通知されます。
3. Policy Enforcer は、影響を受けたスイッチ ポートまたは Wi-Fi アクセス ポートに対して、アクセス コントロール リスト/ネットワーク アクセス コントロール ルールを適用して、ホストを隔離し、迅速に脅威を修復します。

ネットワークに対する攻撃が別の種類のネットワーク セキュリティ環境で発生したのであれば、IoT デバイスがさらに多くの情報へのアクセスを継続できた可能性があります。この場合、従来の次世代型ファイアウォールは単純に IoT デバイスが組織外と通信することを禁止したでしょう。もしこれが、攻撃者がデバイスに物理的にアクセスできる内部からの攻撃であった場合、損害がきわめて大きくなります。

特長とメリット

Juniper Connected Security フレームワークにより、以下のようなメリットが得られます。

- **死角のないセキュリティ：**Juniper Connected Security は、スイッチ、ルーター、Wi-Fi アクセス ポイントだけでなく、ファイアウォール レイヤーに至るまで、ネットワークのあらゆるレイヤーにセキュリティを拡大します。また、オンプレミスの物理的な導入から、プライベート クラウド（VMware NSX や Juniper Contrail など）、パブリック クラウド（Amazon AWS や Microsoft Azure など）まで、様々な導入モデルをサポートする Juniper Connected Security は、妥協のない堅固なセキュリティをお客様に提供します。
- **オープンなマルチベンダー エコシステム：**多くのエンタープライズ環境が、マルチベンダー環境です。リフレッシュ サイクルの間に、既存のインフラストラクチャの入れ替えが必要になる、またはお客様に単一ベンダーを強要するセキュリティ ソリューションは、新しい機能の導入時や、新しいトレンド/技術の採用時に、大きな制限を生み出します。Juniper Connected Security は、オープンなアプローチを採用し、企業が既存のネットワーク機器の大部分を維持しながら、よりセキュアなネットワークへの移行を可能にします。他のネットワークおよびセキュリティ ベンダーとのパートナーシップにより、Juniper Connected Security は真のコラボレーションが可能な包括的アプローチを提供して、ネットワーク セキュリティを実現します。
- **グローバル ポリシーおよびセキュリティ管理：**Policy Enforcer モジュールを含む Junos Space Security Director を使用することで、ローカル展開かグローバル展開かに関わらず、ネットワーク全体に一貫性のあるセキュリティ ポリシーを適用できます。セキュリティ管理者は、システムをきめ細かく可視化して、ネットワーク レイヤーにも仮想環境にもポリシーを適用できるため、セキュリティ体制の最適化に役立ちます。
- **動的で自動化された脅威修復機能：**ネットワーク セキュリティにおいて重要なのは、脅威にすばやく対応できることです。脅威は、Juniper Sky ATP、ATP Appliance、社内フィード、サードパーティーのセンサーによって、休みなく正確に検知されます。Policy Enforcer は、これらの脅威に対して自動的に修復措置を講じ、これとほぼ同時にネットワーク レイヤーで脅威をブロックまたは隔離します。これにより、管理作業の負担が軽減され、ネットワーク拡張時にも、より迅速で、より管理しやすいアプローチを推進します。

概要

Juniper Connected Security は、ネットワークおよびセキュリティの構成要素と一元化された管理および分析を組み合わせて、死角のないセキュリティと真に自動化された脅威の修復機能を提供します。Juniper Connected Security のオープンなマルチベンダー エコシステムのサポートにより、企業はネットワーク内に既に存在するネットワークおよびセキュリティの構成要素を使用し、ビジネスの継続性を確保しつつ、既存の投資を保護できます。

次のステップ

ジュニパーネットワークスのセキュリティ ソリューションの詳細については、www.juniper.net/jp/jp/products-services/security をご覧いただくか、ジュニパーネットワークスの担当者にお問い合わせください。

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、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
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
電話番号：+31.0.207.125.700
FAX：+31.0.207.125.701

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
FAX：03-5333-7401
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