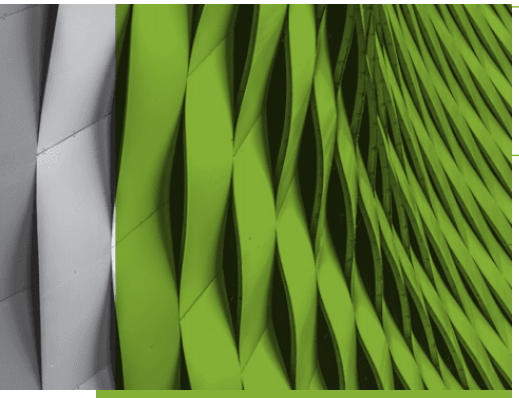

SECURITY DIRECTOR データシート

製品概要

Juniper Security Director は、中央管理された Web ベースのインターフェイスを通して広範なセキュリティポリシー管理を提供し、最新および従来の脅威ベクトルに対してポリシーを適用し、物理、仮想およびコンテナ化されたファイアウォールをオンプレミスおよび複数のクラウドで同時に保護します。アプリケーションのパフォーマンスを詳細に視覚化し、リスクを低減して、ユーザーが迅速に問題を診断し解決できるようにします。

大規模な拡張、詳細なポリシー管理、ネットワーク全体へのポリシーの適用を可能にする Security Director は、オンプレミス、クラウド内、およびサービスとして、ネットワーク全体の可視性とポリシーの管理を提供します。管理者は、ゼロタッチプロビジョニングや設定を含む、ファイアウォールや次世代ファイアウォールサービスのセキュリティポリシーのライフサイクルのあらゆる段階を迅速に管理できます。また、ネットワーク全体のリスク要因に関するインサイトを取得でき、これらはすべてシングルユーザーインターフェイスから行うことができます。

製品説明

ネットワークセキュリティ管理とは、管理者がファイアウォール構成を管理し、個々の展開、ポリシー、トラフィックの全体にわたる可視化を提供し、ネットワークトラフィック全体の脅威分析からインサイトを得る方法です。

管理ソリューションが十分でなく、粒度や可視化のレベルに制限のある場合は運用の足かせになります。直感的なウィザード、時間を節約できるオーケストレーションツール、多彩なインサイトを反映させるダッシュボードがあれば従来運用の足かせから解放されます。Juniper Security Director は、物理、仮想、およびコンテナ化されたすべてのファイアウォールにセキュリティポリシー管理を提供します。直感的な、一元管理された Web ベースのインターフェイスを通じて、Security Director はパブリッククラウドとプライベートクラウドの両方におけるジュニパー SRX シリーズファイアウォールの展開に対して可視性、インテリジェンス、自動化、および効果的なセキュリティを提供することで、管理コストとエラーを削減します。

Security Director Cloud

Security Director Cloud は、現在のセキュリティ展開を SASE ロールアウトにブリッジするセキュアアクセスサービスエッジ（SASE）へのポータルとなります。Security Director Cloud は、オンプレミス、クラウド、サービスなど、あらゆる場所でセキュリティ管理を可能にし、ユーザー、デバイス、アプリケーションの場所を選ばない統合ポリシー管理を実現します。ポリシーは一度作成すれば、どこにでも適用できます。企業は Security Director Cloud を使用してネットワーク全体の可視性と展開のポリシーを管理すると同時に、SASE アーキテクチャに安全に移行することができます。

Security Director Cloud を利用することでシームレスかつ安全に、それぞれの企業のビジネスに最適なペースで SASE アーキテクチャに移行することができます。Security Director とオンプレミスおよび個々のファイアウォールとの双方向の同期により、クラウドへのシームレスな移行をサポートする一貫した管理エクスペリエンスを提供します。統一されたポリシー管理により、ユーザー、デバイス、アプリケーションに応じた一貫したセキュリティポリシーを提供します。

図 1：Security Director クラウドアーキテクチャ

Security Director のダッシュボードには、カスタマイズ可能で情報に富んだウィジェットを提供し、セキュリティデバイスの状態を一目で分かるように視覚的に直感的に表示することができます。パレットを使用して、SRX シリーズのファイアウォール環境のカスタムビューを作成するための、ファイアウォール、脅威、侵入防御システム（IPS）、

アプリケーション、スループット、およびデバイスに関連する情報間を容易に移動できます。

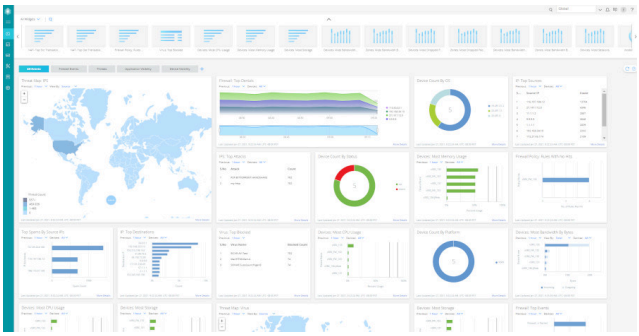

図 2 ：Security Director ダッシュボード

ダッシュボードを通じて、特定の時間に SRX シリーズのどのデバイスが最も多くのアラームを生成したか、または最も多くの CPU サイクルや RAM を消費したかを迅速に判断できます。

ウィジェットをよく調べることにより、管理者は、さまざまなイベントの並べ替えや検索を行って、ブロック回数の多いウィルス、多く使用された送り先、多く使用されたソース、そしてネットワークが安全であることを確認するためのその他の詳細などの詳細情報を容易に入手できます。

Security Director は、アプリケーション、ユーザー、IP 環境を管理するための革新的なソリューションです。ネットワーク管理者は、アプリケーションとユーザーがネットワークにどのような影響を及ぼすかを確認する、帯域幅の使用レベルを監視する、または作成したセッションの数を決定するという、3 つの異なるビューを選択できます。どのアプリケーションのリスクが最も高いかなど、詳細情報も表示できます。トップトーカーの特定および修復が容易です。また、異なるタイムフレームを比較して、通常の場合に使用率がピークとなる時刻を判断することもできます。

ほとんどのセキュリティ管理ソリューションでは、管理者は管理したいアプリケーションまたはユーザーを見つけるために、レポートを実行するか、いくつかのタブを開く必要があります。次に、必要なファイアウォールのルールを手動で作成し、それらのルールの設定場所を判断して、それらが既存のルールと矛盾して新しい多くの問題を発生させることがないようにしないといけません。このタスクは非常に面倒で、時間がかかり、ミスを犯しやすいプロセスです。

Security Director は非常にユーザーフレンドリーで、ユーザーは答えを見つけるために複数のレポートを実行したり、複数のタブを開いてデータを分析する必要はありません。その代わりに、Security Director は、レポートを詳しく調べなくても一目で重要な回答を迅速に見つけることができる機能を管理者に提供します。

Security Director が提供する実用的なインテリジェンスを使用して、管理者はアプリケーション可視性またはユーザー可視性から 1 つ以上のアプリケーションまたはユーザーのグループを選択した後で、単に「ブロック」を選択することができます。Security Director は、必要な 1 つまたは複数のルールを自動的に作成し、ルールのベース内で最適な場所にそれらを展開し、異常を回避して、アプリケーションおよびユーザーの環境の管理から推測を取り除くことができます。

Security Director は、脅威の緩和に関する実用的なインテリジェンスも提供します。例えば、脅威マップには地域ごとに検出された IPS イベントの数が表示され、脅威アクティビティが即ちに意識できるようになり、修復する手段がワンクリックで提供されます。

Juniper Secure Edge

Juniper® Secure Edge は、Juniper Security Director Cloud が管理するシングルスタックのソフトウェアアーキテクチャで FWaaS（サービスとしてのファイアウォール）を提供し、どこにいても従業員の安全を確保できるようにします。ユーザーは、必要なアプリケーションやリソースに高速、高い信頼性、安全にアクセスでき、ユーザーに優れたエクスペリエンスを約束します。IT セキュリティチームは、既存の投資を活用しながら、ネットワーク全体をシームレスに可視化することができ、自社のペースでクラウド提供型アーキテクチャに移行することができます。

Juniper Secure Edge は、ユーザー、デバイス、アプリケーションに沿ったセキュリティーポリシーと、ルールセットのコピーも作り直しも必要としないセキュリティアプリケーションを使用して、可視性またはセキュリティーの適用を中断せずに、クラウドが実現するアプリケーション管理、侵入防御、コンテンツおよび Web フィルタリング、および効果的な脅威防御の展開を容易にします。

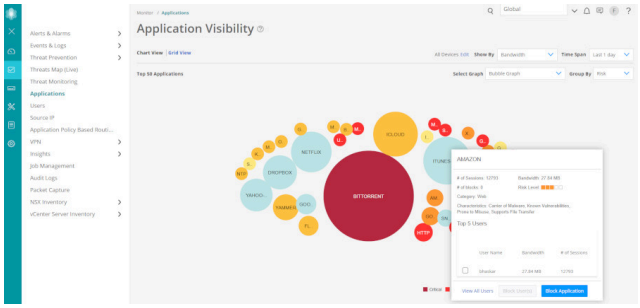

図 3 ：アプリケーション可視性ダッシュボード

Security Director Insights

Security Director Insights は、セキュリティ スタック全体にわたる脅威イベントの関連付けとスコアリングにより、エンドツーエンドの可視化を拡大します。MITRE 攻撃フレームワークにマッピングされたタイムライン ビューが表示されるので、管理者は最も優先度の高い脅威に集中できます。 他ベンダー製品からの検知を含む脅威検知情報を関連付けることでネットワーク全体の可視性を統一し、ワンタッチでミティゲーションを行うことで防御までのギャップを大幅に圧縮することができます。

Security Director Insights は、Security Director に組み込まれたオーケストレーションである Policy Enforcer を使用して、企業がネットワーク全体での脅威の修復とマイクロセグメンテーションポリシーを自動化できるようにします。

図 4 ：Security Director Insights ダッシュボード

Security Director Insights は電子メール、エンドポイント、サーバー、クラウドワークロード、およびネットワークという複数のセキュリティーレイヤー全体でデータの収集と自動的な関連付けを行いますので、脅威はより迅速に検出され、セキュリティ チームは調査時間と応答時間を改善できます。将来の攻撃を防ぐために、ミティゲーションルールも使用されます。

Security Director Insights の導入で、お客様は以下のことが可能になります。

- ネットワークのさまざまな部分で、複数のセキュリティソリューションからのセキュリティイベントを相関させ、優先順位をつけるために使用することで、いつ、どこで攻撃が起こっているかを理解することができます。
- 脅威とインシデントのスコアリングをカスタマイズして、セキュリティチームがビジネスに最も損害を与える可能性のある攻撃に対応し、その被害を軽減できるようにします。
- ジュニパーの SRX シリーズファイアウォール、EX および QFX シリーズスイッチ、Mist AI ドリブンの有線および無線アクセスポイントなど、ネットワーク上のあらゆるアクティブな脅威をワンクリックで軽減します。

お客様は、Security Director Insights を使用して、クライアントからワークロードまで、ネットワーク全体の攻撃指標を、環境内のどのベンダー製品が検知したかに関係なく追跡することができます。

Policy Enforcer

Policy Enforcer は、単純化されたユーザーのインテントベースの脅威管理ポリシーの変更と配信を行うツールを提供します。更新されたポリシーを、ジュニパーネットワークス EX シリーズイーサネットスイッチ、MX ルーター、QFX シリーズスイッチ、およびジュニパーの物理、仮想、およびコンテナ化された SRX シリーズファイアウォールに展開することができます。

Security Director は、セキュリティポリシーの自動適用とポリシーオーケストレーションを提供し、更新されたセキュリティポリシーをジュニパーの SRX ファイアウォール、EX シリーズスイッチ、QFX シリーズスイッチ、MX シリーズルーター、サードパーティ製ネットワーク機器に展開することが可能です。このソフトウェアは、ネットワーク全体における脅威の修復とマイクロセグメンテーションのポリシーを自動化できます。

Security Director 内の直感的なユーザーインターフェイスは、ネットワークの要素、適用グループ、脅威管理サービス、およびプロファイルの定義を管理および変更する柔軟性を管理者に提供します。

Security Director は、Policy Enforcer を使用して、ジュニパー Advanced Threat Prevention (ATP) が識別した脅威に基づいてポリシーを自動的に更新します。更新されたポリシーは、Policy Enforcer を通じて、ファイアウォール、スイッチ、無線ソリューションなどの実施ポイントに配信され、リアルタイムにネットワークを保護します。

ファイアウォール ポリシー分析

ファイアウォールポリシー分析では、シャドーまたは余分なファイアウォールルールを表示するレポートをスケジュールすることで、ネットワークの異常を可視化することができます。ファイアウォールポリシー分析では、報告されたすべての問題を修正するための推奨事項を作成し、自動化を使用してルール ベースを最適化します。

ファイアウォールポリシー分析により、毎月または四半期ごとに異常レポートを実行する必要がなくなり、すべての問題を手動で修正する必要がなくなります。レポートは一度実行すれば、Security Director が適応します。

表 1. Security Director の機能とメリット

特長	説明	メリット
Secure Edge	すべてサービスとして配信される、アプリケーション制御、IPS、アンチマルウェア、Web プロキシとフィルタリング、高度な脅威保護を備えたシングルスタックソフトウェアアーキテクチャで FWaaS を提供します。	管理者は、ユーザーがどこにいても、一貫したセキュリティポリシーでリモートワークのセキュリティをシームレスに確保することができます。
Security Director Insights	電子メール、エンドポイント、サーバー、クラウドワークロード、およびネットワークという複数のセキュリティーレイヤー全体でデータの収集と自動的な関連付けを行いますので、脅威はより迅速に検出され、セキュリティチームは調査時間と応答時間を改善できます。ミティゲーションルールを使用して将来の攻撃を防止します。	• ネットワークのさまざまな部分で、複数のセキュリティソリューションからのセキュリティイベントを相関させ、優先順位をつけるために使用することで、いつ、どこで攻撃が起こっているかを理解することができます。 • 脅威とインシデントのスコアリングをカスタマイズして、セキュリティチームがビジネスに最も損害を与える可能性のある攻撃に対応し、その被害を軽減できるようにします。 • SRX シリーズのファイアウォール、EX および QFX シリーズスイッチ、Mist AI ドリブンの有線および無線アクセスポイントに加えてワンクリック式のサードパーティソリューション上で、ネットワーク全体のアクティブな脅威を緩和します。
Policy Enforcer	ユーザーのインテントに基づいたシステムによってセキュリティポリシーを作成し、一元管理します。複数のソースからの脅威情報を評価しながら、ネットワーク全体にほぼリアルタイムでポリシーを動的に適用します。Advanced Threat Prevention Cloud、SecIntel、オンプレミスのカスタム脅威インテリジェンスソリューションからの脅威フィードを集約し、許可リストとブロックリストをサポートしながら、ファイアウォールとアクセススイッチで脅威管理ポリシーを適用します。	• 古いルールを削除することにより侵害のリスクを削減し、ネットワーク脅威条件に基づいて自動的に適用を更新します。 • 感染したホストの隔離と追跡によって保護の体勢を改善します。 • セキュリティ担当者が、面倒なポリシールールを作成するのではなく、セキュリティの最大化に集中できるようにします。
ファイアウォールポリシー分析	シャドーまたは冗長なファイアウォールルールを表示するレポートをスケジュールする機能を提供し、報告されたすべての問題を修正するためのアクションを推奨します。	管理者は、効果のないルールや不要なルールを迅速に特定し、効率的なファイアウォールルールベースを維持することができます。
ファイアウォールルール設置のガイドライン	新しいルールを作成した時点で、既存のファイアウォールルールベースを分析して、最適な位置とアプリケーションを推奨します。	シャドーイングルールを大幅に削減
メタデータ ベースのポリシー	管理者は、オブジェクトメタデータに基づいたユーザーインテントファイアウォールポリシーを作成することができます。	ポリシー作成とメンテナンスワークフローを簡素化します。この機能により、ユーザーのインテントに沿ったポリシーの読み取りが可能になるほか、ファイアウォールのトラブルシューティングが効率化されます。
ダイナミックポリシーアクション	セキュリティ管理者が、ファイアウォール、ログ作成、IPS、URL フィルタリング、アンチウィルスなどの異なるアクションを条件に応じて開始することが可能です。	異なる条件下で組織のセキュリティ体勢を調整するために必要な時間を短縮し、脅威修復のワークフローを効率化します。
ファイアウォールポリシーのヒットカウント	各ファイアウォールのヒット数をメーターとフィルターで表示し、どのルールが最もヒットしなかったかを表示します。また、Security Director も、ライフタイムヒットカウントを維持できます。	管理者は、各ファイアウォールルールの有効性を評価し、使用されていないルールを迅速に特定することができ、その結果、ファイアウォール環境がより良く管理されるようになります。
ライブ脅威マップ	脅威がほぼリアルタイムで発信されている場所が表示され、それらを停止するアクションを実行できます。	ネットワーク関連の脅威について、ほぼリアルタイムのインサイトを提供します。特定の国に行くトラフィックまたは特定の国から来るトラフィックを、ワンクリックでブロックできます。
セキュリティアシュアランス	正確な適用や、一貫したセキュリティおよびコンプライアンスのために、ファイアウォール、ルーター、スイッチなどの全体にわたるセキュリティポリシーを自動化します。	セキュリティルールが常に正しく配置され、インテントした効果を発揮することを保証します。
革新的な適用の可視性および管理	アプリケーションが最も多くの帯域幅を使用するか、最も多くのセッションを行うか、または最もリスクが多いかを、簡単かつ直感的に確認する方法を提供します。どのユーザーが生産性の低いアプリケーションにアクセスしているか、どれほどの時間アクセスしているかを把握することができます。トップトーカーがわかりやすい方法で表示されます。マウスをクリックするだけでアプリケーション、IP アドレス、ユーザーをブロックします。	ネットワーク上でより高い可視性、適用、制御、保護を提供します。
簡素化された脅威管理	グローバルマップを介して、脅威の発信元の場所と送信先の場所を報告します。国のブロックは、マウスオーバーするだけで簡単に行えます。	ネットワーク関連の脅威を効果的に管理する上で必要となるインサイトを提供します。特定の国に行くトラフィックまたは特定の国から来るトラフィックを、ワンクリックでブロックできます。
スナップショットサポート	ユーザーが設定バージョンをスナップショット、比較、ロールバックできるようにします。	設定変更を簡素化し、設定エラーからの切り戻しが可能になります。
ポリシー ライフサイクル管理	セキュリティポリシーのライフサイクルの作成、導入、監視、修復、保守を含めて、すべての段階の管理を行う機能を提供します。	• Security Director 管理コンソールで、ステートフル、ファイアウォール、AppFW、URL フィルタリング、アンチウィルス、IPS、VPN、NAT を一元管理できるようにします。 • 単一のインターフェイス内で共通のポリシータスクを統一することで、管理を容易にします。 • 複数のデバイス全体に、ポリシーを再利用することで、エラーを削減します。
ドラグ アンドドロップ	ファイアウォール、IPS、NAT のルールを新しい場所にドラッグすることで並べ替えられるようにします。	ファイアウォール、IPS、NAT オブジェクトを、1 つのセルから別のセルに、またはポリシーテーブルの一番下にあるパレットからドラッグすることで、追加またはコピーすることができます。
VPN 自動プロビジョニングとインポート	Security Director に、使用する VPN トポロジーと、そのトポロジー内で参加したいデバイスを指示すれば、Security Director がトンネルを自動的にプロビジョニングします。ジュニパー VPN 環境が既に存在する場合、Security Director は、VPN をインポートして、容易かつ効果的な管理方法を提供することができます。	既存 SRX シリーズのファイアウォール VPN の管理が容易になります。

特長	説明	メリット
ポリシーとオブジェクトへのロールベースのアクセス	デバイス、ポリシー、オブジェクトをドメイン内に設定し、ユーザーに読み書きのパーミッションを割り当てます。	ポリシーとオブジェクトの管理責任をセグメント化する方法をお客様に提供します。
自動化のための REST API	自動化ツールと組み合わせて使用する RESTful API を提供します。	物理、仮想、またはコンテナ化された SRX シリーズのファイアウォールの設定と管理を自動化します。
Junos Space Log Director のアプリケーションによるログ作成と報告	統合された口グ作成とレポートが有効になります。	セキュリティディレクターとの緊密な連携： • ルールとイベントを同じウィンドウで表示 • 管理者は、ログからそれに対応するルールへ、またその逆へと、ビューを簡単にシフトできます。 Security Director ポリシーとオブジェクトへの直接アクセス： • 役割ベースのアクセス制御（RBAC） • アグリゲーションとフィルタリングのためのイベントビューア • カスタマイズ可能なグラフを備えたダッシュボード • 電子メールで生成され自動送信されたレポート • SRX シリーズのヘルスモニタリングのしきい値に基づき、自動的にメールアラートを生成します。 - CPU 使用率 - メモリ使用率 - VPN 監視 セキュリティ情報およびイベント管理（SIEM）へのシステムログ転送

注文情報

ジュニパー Security Director の注文およびソフトウェア ライセンス情報へのアクセスに関しては、https://www.juniper.net/jp/ja/how-to-buy/form.html の購入方法のページを参照してください。

分析のためにクラウドにアップロードされたファイルは、その後、プライバシを保証するため破棄されます。ジュニパーネットワークスのプライバシー ポリシーについては、https://www.juniper.net/jp/ja/privacy-policy.html をご確認ください。

ジュニパーネットワークスのサービスとサポート

ジュニパーネットワークスは、ネットワークの高速化、拡張、最適化を実現する高度なパフォーマンスサービスに対応するリーダーです。当社のサービスをご利用いただくと、コストを削減し、リスクを最小限に抑えながら、業務効率を最大限に高めることが可能となり、早期にネットワーク投資の価値を高めることができます。ジュニパーネットワークスは、必要なレベルのパフォーマンス、信頼性、および可用性を維持するようにネットワークを最適化することで、オペレーショナルエクセレンスを確保します。詳細については、https://www.juniper.net/jp/ja/products.html 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/