

JUNIPERSECURITY DIRECTOR

製品概要

Juniper Security Directorは、一元化されたWebベースのインターフェイスを通じて、広範なセキュリティポリシーの管理と制御を提供します。新たな脅威ベクトルと従来の脅威ベクトルに対してポリシーを適用し、オンプレミスと複数のクラウドにわたって物理ファイアウォール、仮想ファイアウォール、コンテナ化されたファイアウォールを同時に保護します。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、迅速に問題を診断し解決できます。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構成など、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ライフサイクルのすべてのフェーズを迅速に管理できます。また、単一のユーザーインターフェイスからネットワーク全体のリスク源に関するインサイトも得られます。

製品説明

ネットワークセキュリティ管理で、管理者はファイアウォールアーキテクチャを管理できます。個々の展開、ポリシー、トラフィック全体を可視化し、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が得られます。

管理ソリューションが不十分で、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、すべての物理、仮想、コンテナ化されたファイアウォールのセキュリティポリシーを管理します。Security Directorは、直感的で一元化されたWebベースのインターフェイスを通じて、パブリッククラウドとプライベートクラウドの両方でジュニパー® SRXシリーズファイアウォールの展開全体で可視性、インテリジェンス、自動化、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クラウド

Security Director Cloudは、単一のUIで提供されるHPEのシンプルでシームレスな管理エクスペリエンスであり、お客様の現在の展開と将来のアーキテクチャの展開を結び付けます。管理は、コネクテッドセキュリティ戦略の中心にあり、組織がネットワーク上のあらゆる接続ポイントを保護し、ユーザー、データ、インフラストラクチャを保護するのに役立ちます。

組織は、オンプレミス、クラウドベース、クラウド配信、ハイブリッド、そしてゼロトラストをネットワークエッジからデータセンター、アプリケーション、マイクロサービスまで。Security Director Cloudにより、組織は中断のない可視性、ポリシー構成、管理、脅威インテリジェンスの集合を一元的に実現できます。

ジュニパーは、お客様が移行のどの段階にいるのであれ、その要件を満たして、既存の投資を活用できるようにサポートします。Security Director Cloudで移行を自動化することで、お客様のビジネスに最適なペースで、希望するアーキテクチャに移行できます。

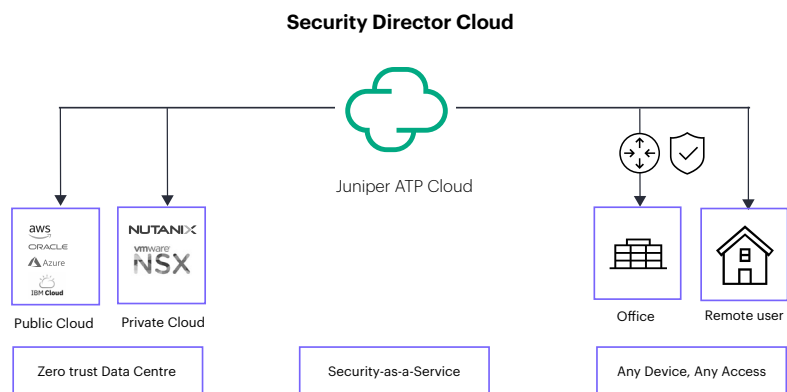


図1. Security Directorクラウドアーキテクチャ

Juniperセキュアエッジ

Juniper® Secure Edgeは、必要な高速、高信頼性、セキュアなアクセスにより、あらゆる場所で従業員を保護します。FWaaS、SWG、DLP付きCASB、ZTNA、高度な脅威保護などのフルスタックSSE機能を提供し、Web、SaaS、オンプレミスアプリケーションへのアクセスを保護し、ユーザーがどこにいても従うセキュリティを提供します。HPEは、お客様の現状に応え、お客様が望むところに連れて行きます。そのために、銀行や運用チームを壊すことなく、ゼロトラストイニシアチブをクラウド配信アーキテクチャに拡張します。

Security Director Cloudによって管理されるJuniper Secure Edgeでは、単一のポリシーフレームワークを採用しており、セキュリティポリシーを一度作成すれば、ユーザー、デバイス、データがどこにいても同じポリシーを適用することができます。

お客様はクラウド配信セキュリティを採用する際に、最初から始める必要はありません。3回のクリックで完了するウィザードで、既存のキャンパスエッジポリシーを活用して、SSEポリシーへと簡単に交換することができます。導入モデルに関係なく、単一のポリシーフレームワークを使用するため、Secure Edgeでは、従来の導入からクラウド配信モデルへと、わずか数回のクリックで既存のセキュリティポリシーを適用することができ、誤設定やリスクを軽減することができます。

リモートユーザー、キャンパスおよびブランチロケーション、プライベートクラウド、パブリッククラウド、ハイブリッドクラウドデータセンターのいずれを保護する場合でも、HPEは、すべてのアーキテクチャにわたって一元的な管理と中断のない可視性を提供します。これにより、運用チームは、現在の投資をSASEを含む将来のアーキテクチャの目標に簡単かつ効果的に結びつけることができます。お客様は、場所を問わず、オンプレミス、クラウド、クラウドからセキュリティを管理できます。ユーザー、デバイス、データを追跡するセキュリティポリシーはすべて単一のUIから利用できます。

ユーザーには、必要なデータやリソースへの高速で、信頼性の高いセキュアなアクセスを提供することで、優れたユーザーエクスペリエンスを確保できます。ITセキュリティチームは、既存の投資を活用しながら、ネットワーク全体のシームレスな可視化を実現し、独自のペースでクラウド配信アーキテクチャーを実現

Juniper Secure Edgeからあらゆる場所のユーザー、デバイス、データに一貫したセキュリティポリシーが提供され、ルールセットをコピーしたり再作成したりする必要がありません。クラウド配信のアプリケーション制御、侵入防止、コンテンツとWebフィルタリング、効果的な脅威防止を簡単に展開でき、可視性やセキュリティの適用を損ねることはありません。

HPEは、過去4年間にわたり、市場で最も効果的なセキュリティテクノロジーとして複数のサードパーティテストによって一貫して検証されており、すべてのユースケースで100%のセキュリティ有効性を実現しています。

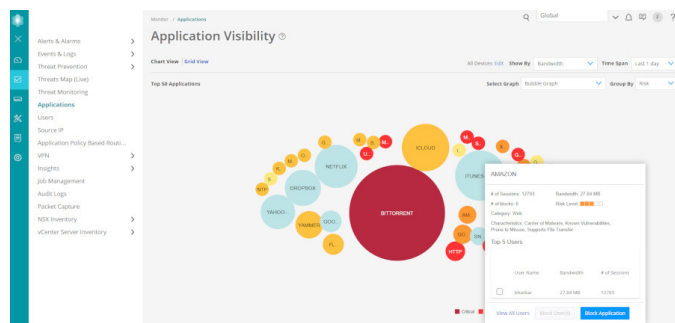


図3. アプリケーション可視化ダッシュボード

Security Directorのインサイト

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性を拡大します。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専念できます。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、ワンタッチで緩和して、防御におけるギャップに迅速に対応することができます。

Security Director Insightsにより、組織はセキュリティでネットワーク全体の脅威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、ネットワークという複数のセキュリティレイヤー全体でデータを収集し、自動的に関連付けします。より迅速に脅威を検出できるため、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、優先順位をつけることで、いつ、どこで攻撃が起きているかを把握
- セキュリティチームがビジネスに最大の損害をもたらす可能性のある攻撃に対応し、軽減できるように、カスタム脅威およびインシデントスコアリングを使用します。

— Juniper SRXシリーズファイアウォールで、ネットワーク全体のアクティブな脅威をクリック1回で緩和

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。

Security DirectorのPolicy Enforcerには、ユーザーのインテントベースの単純化された脅威管理ポリシーを変更し、配信するツールが用意されています。

Security Directorは、ポリシーの適用とオーケストレーションを自動化できるため、更新されたセキュリティポリシーをJuniper SRXシリーズファイアウォールに展開できます。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を使用し、ネットワークの要素、適用グループ、脅威管理サービス、プロファイルの定義を管理および変更できます。

Security Directorは、Policy Enforcerを使用して、Juniper® Advanced Threat Prevention (ATP) が特定した脅威に基づいてポリシーを自動的に更新します。さらに、SecIntelフィードとPolicy Enforcer統合も利用可能です。更新したポリシーは、Policy Enforcerを通じて、ファイアウォール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。

表1. Security Directorの機能とメリット

項目	説明	メリット
セキュアエッジ	FWaaS、SWG、DLP付きCASB、ZTNA、高度な脅威保護などのフルスタックセキュリティサービスエッジ (SSE) 機能を提供し、Web、SaaS、オンプレミスアプリケーションへのアクセスを保護し、どこにいてもユーザーを追跡するセキュリティを提供します。	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カーのセキュリティをシームレスに確保できます。
Security Directorのインサイト	メール、エンドポイント、サーバー、クラウドワークロード、ネットワークなど、複数のセキュリティレイヤーにわたってデータを収集して自動的に関連付けるため、脅威を迅速に検出し、セキュリティチームが調査と応答時間を短縮できます。緩和ルールで将来の攻撃を防止	<ul style="list-style-type: none">— 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、優先順位をつけることで、いつ、どこで攻撃が起こっているかを把握— 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、ビジネスに最も損害を与えるおそれのある攻撃にセキュリティチームが対応し、その被害を軽減— アクティブな脅威をMarvis® AI Assistantを搭載したSRXシリーズファイアウォール、スイッチ、有線および無線アクセスポイント、およびサードパーティソリューション上のネットワークをワンクリックで

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してすべての問題を手動で修正する必要がなくなります。レポートを一度実行すれば、Security Directorが適応します。

Security Director

Security Directorは、SaaS Security Director Cloudのサービスに加えて、オンプレミスのサービスとしても利用可能です。

オンプレミスバージョンはSecurity Director Cloudをベースとしているため、同じ外観と操作性で同じ豊富な機能、監視、分析などを提供します。

Security Directorの詳細については、以下をご覧ください。[Juniper Security Directorのドキュメント](#)

表1. Security Directorの機能とメリット

項目	説明	メリット
ポリシー エンサー	ユーザーインテントベースのシステムを通じてセキュリティポリシーを作成および一元管理し、ネットワーク全体でほぼリアルタイムでポリシーを動的に実行しながら、複数のソースからの脅威インテリジェンスを評価します。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の各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	<ul style="list-style-type: none"> 古いルールを削除することで侵害のリスクを軽減し、ネットワーク脅威条件に基づいて自動的に適用を更新 感染したホストの隔離と追跡により、保護体制を改善 セキュリティ担当者は、面倒なポリシールールの作成ではなく、セキュリティの大幅向上に専念
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	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
ファイアウォールルール設置のガイドライン	ルールを新規作成した時点で、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	シャドーインクルールを大幅に削減
メタデータベースのポリシー	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可能	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
ダイナミックポリシーアクション	セキュリティ管理者は、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可能	さまざまな状況下で組織のセキュリティポスチャを調整するのに必要な時間を短縮し、脅威修復ワークフローを合理化
ファイアウォールポリシーのヒットカウント	ファイアウォールごと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。Security Directorも、ライフタイムヒットカウントを維持	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の管理が改善
ライブ脅威マップ	脅威が発信されている場所がほぼリアルタイムで表示され、それらを阻止するアクションを実行可能	ほぼリアルタイムでネットワーク関連の脅威です特定の国向けの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可能
Security Assurance	ファイアウォール、ルーターを含むネットワーク全体のセキュリティポリシーを自動化し、正確な実施、一貫したセキュリティ、コンプライアンスを実現	常にセキュリティルールを適切に配置して、意図した有効性を達成
革新的な適用の可視性および管理	どの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	ネットワークの可視性、適用、制御、保護を向上
脅威の管理を簡素化	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。マウスカーソルを合わせるだけなので国のブロックは簡単	管理に必要なインサイトを提供ネットワーク関連の脅威を効果的に検出できます 特定の国向けの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可能
スナップショットサポート	設定のバージョンをスナップショット、比較、ロールバック可能	設定の変更が簡素化され、設定ミスからの回復が可能

表1. Security Directorの機能とメリット

項目	説明	メリット
ポリシーライフサイクル管理	作成、展開、監視、修復、メンテナンスなど、セキュリティポリシーライフサイクルのすべてのフェーズを管理する機能を提供	<ul style="list-style-type: none"> Security Directorの管理コンソール1つで、ステートフルファイアウォール、AppFW、URLフィルタリング、アンチウイルス、IPS、VPN、NATを一元管理 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、管理を簡素化 複数のデバイスでポリシーを再利用することでミスを削減
ドラッグアンドドロップ	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だけで並べ替え可能	ファイアウォール、IPS、NATのオブジェクトを、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、追加またはコピーが可能
VPN自動プロビジョニングとインポート	Security DirectorにどのVPNトポロジーを使用するか、どのデバイスをトポロジーに参加させるかを伝えるだけで、Security Directorがトンネルを自動プロビジョニングします。既存のHPE Juniper Networking VPN環境がある場合、Security DirectorはVPNをインポートして、簡単かつ効果的に管理できます。	既存のSRXシリーズファイアウォールVPNの管理が容易
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、ユーザーに読み取り/書き込みの権限を付与	ポリシーとオブジェクトごとに管理責任のセグメント化が可能
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を用意	物理、仮想、またはコンテナ化されたSRXシリーズファイアウォールの構成と管理を自動化
アプリケーションのロギングとレポート作成	ロギングとレポート作成が可能	<ul style="list-style-type: none"> ルールとイベントを同じウィンドウに表示する ログからそれに対応するルールへ、またその逆へと、ビューを簡単に切り替え可能 <p>Security Directorのポリシーとオブジェクトへの直接アクセス:</p> <ul style="list-style-type: none"> ロールベースのアクセス制御 (RBAC) イベント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ー カスタマイズ可能なグラフを備えたダッシュボード レポートが生成され、電子メールで自動的に送信される SRXシリーズの正常性監視のしきい値に基づいてメールアラートを自動生成 <ul style="list-style-type: none"> CPU利用率 メモリ使用率 VPN監視 <p>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</p>

注文情報

Juniper Security Directorを注文し、ソフトウェアライセンス情報にアクセスするには、www.juniper.net/us/en/how-to-buy/form.html。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、プライバシーを保護するため破棄されます。HPE Juniper Networkingのプライバシーポリシーは、www.juniper.net/us/en/privacy-policy.html

免責事項: 本データシートは、機械翻訳を使用してご提供しております。人間翻訳者による確認もしくは検証が行われていないため、言語表現に誤表現、また不正確な内容が含まれている可能性があります。あらかじめご了承ください。正確な情報の確認につきましては、英語版のデータシートをご参照ください。

HPEについて

HPEは、重要なエンタープライズテクノロジーのリーダーであり、AI、クラウド、ネットワーキングの力を結集して、組織がより多くの成果を達成できるよう支援しています。可能性のパイオニアとして、ジュニパーのイノベーションと専門知識は、人々の生活と働き方を前進させます。さまざまな業界のお客様に、運用パフォーマンスを最適化し、データを予測に変換し、その影響を最大化していただけるようサポートします。HPEで、最も大胆な野心を解き放ちましょう。詳細については、HPE.com。

HPE.comにアクセス

[今すぐチャット](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. 本書の内容は、将来予告なく変更されることがあります。ヒューレット・パカード エンタープライズ製品およびサービスに対する保証については、すべて当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、省略に対しては責任を負いかねますのでご了承ください。

a00150843JPN

HEWLETT PACKARD ENTERPRISE

hpe.com

