SECURE EDGEデータシート

データシートのダウンロード

製品概要

労働環境の分散化が進むにつれて、ネットワークエッジセキュリティを保護するの方法は変化しており、新たなクラウドベースのアーキテクチャへと移行しています。多くの選択肢がある中で、企業は既存の投資を活用しながら、セキュアに、自分のペースでシームレスにクラウド型アーキテクチャに移行できる柔軟性を必要としています。

Juniper Secure Edgeは、フルスタックのセキュアサービスエッジ（SSE）機能を提供します。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るのであれセキュリティを提供します。ジュニパーのAIドリブンSD-WANと組み合わせて活用することで、Juniper Secure Edgeは最高の組み合わせのSASEソリューションとなります。シームレスかつセキュアなエンドユーザーエクスペリエンスを提供して、既存のアーキテクチャを活用しながら、SASEフットプリントの拡大にも対応できるようになります。

製品説明

Juniper® Secure Edgeは、FWaaS（Firewall as a Service）、SWG（Secure Web Gateway）、CASB（Cloud Access Security Broker）、データ損失防御（DLP）、Advanced Threat Preventionなどを含めた、フルスタックのセキュアサービスエッジ（SSE）機能を提供します。従業員がどこにいるのであれ、企業が従業員の安全を確保できるようになります。ユーザーは、必要なアプリケーションやリソースに、高い信頼性を持って素早く安全にアクセスすることができるため、優れたエクスペリエンスが確保できます。ITセキュリティチームは、既存の投資を活用しながら、ネットワーク全体をシームレスに可視化することができ、お客様のビジネスに最適なペースでSASEへの移行をサポートします。

Secure Edgeの機能はすべてSecurity Director Cloudで管理されています。Security Director Cloudは、Secure Edge, クラウド、オンプレミスのセキュリティのすべてをシングルユーザーインターフェイス（UI）で管理することができます。ジュニパー独自のAIドリブンSD-WANソリューションと組み合わせることで、今現在どの過程にいるのかに関わらず、SASEアーキテクチャを適用するためのコスト効率がよく信頼性の高い方法が得られます。

アーキテクチャと主要コンポーネント

企業はJuniper Secure Edgeでリモートワーカーをサポートできます。Juniper Secure Edgeは、ユーザーや端末に応じた一貫したセキュリティポリシーを適用でき、ルールのコピーや再作成を繰り返さずに、オフィスでも自宅でも外出先でも、ユーザーが必要とするアプリケーションやリソースへ安全にアクセスすることが可能です。

Juniper Secure Edgeは、リモートユーザーがどこにいてもサポートします。リモートデバイスにPACファイルをインストールすることで、ユーザーを最も近いSecure EdgeのポイントオブプレゼンスPoP）にルーティングさせることが可能です。

同様に、ジュニパーのAIドリブンSD-WANが導入されているキャンパスや支社/拠点にいるユーザーも、各々のサイトの最も近いSecure EdgeのPoPに接続することができます。さらに、セキュリティサービスを最も近いクラウドにオフロードすることも可能です。この過程では、セッションスマートルーティング、アプリコントロール、AppQoS、Mist AIのインサイト、異常検知、自動化されたトラブルシューティングなど、ジュニパー独自の複数の技術からメリットを得ることができます。

これらのサービスとジュニパーのフルスタックSASEを組み合わせることで、企業はオフィス、キャンパス、移動中を問わず、アプリケーションを保護し、ユーザーに一貫性のあるセキュアなアクセスを提供できるようになります。

Juniper Secure Edgeは、スタート点がオンプレミスであるかクラウドであるかに関わらず、どこからでも組織を取り込めるAIを活用したシームレスなSASEエクスペリエンスを形成し、共通のネットワーキングおよびセキュリティポリシーフレームワークを作り出します。ネットワークエクスペリエンスを最適化するジュニパーのSecure Edgeは、AIを活用してセキュリティ実務者のエクスペリエンスを向上させ、リスクの低減とエンドユーザーのエクスペリエンス向上を同時に実現します。

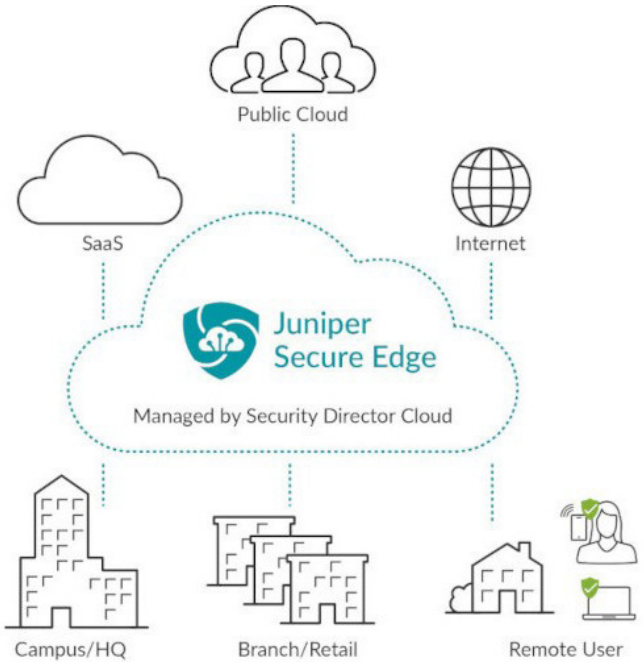

図 1：Secure Edgeは、トラフィックの検査や脅威防御のために集中管理された場所にトラフィックを戻す必要なく、あらゆる場所にいるユーザーをユーザーが必要とするアプリケーションリソースに直接、安全に接続します。

特長とメリット

Firewall-as-a-Service (FWaaS)

FWaaSがアプリケーションを特定し、脆弱性やマルウェアのトラフィックを99.5%以上検知をします。

ジュニパーのFWaaSは、次世代ファイアウォール（NGFW）の全機能をジュニパーのマネージドクラウド経由でサービスとして提供されます。パブリッククラウドのポイントオブプレゼンスを利用することで、ユーザーがどこにいても、あるいは「ネットワーク上」にいるかどうかに関わらず、アプリケーションへの迅速なアクセスを確保します。この独自のアーキテクチャにより、Secure Edgeは超低レイテンシが特徴のトラフィックの検査と管理を可能にします。

Secure Web Gateway (SWG)

SWGは、ポリシー違反や悪意のある通信を防止して、Webアクセスを保護します。

ジュニパーのSWGは、詳細なURLベースのポリシーを通したWebトラフィックの制御、コンテンツのインスペクション、選択的なSSL復号化、暗号化されたトラフィックのインサイトを提供することで、たとえ復号化が不可能な場合であってもWebベースの攻撃から保護します。SWGはコンプライアンス違反のウエブサイトへのアクセスを制御し、許可されたWebトラフィックに流れるマルウェアを除去します。これを実現するために、SWGにはURLフィルタリング、侵入防御、SSLインスペクション、HTTPS通信のふるまい検知、機械学習に基づくマルウェア検知機能を実装しています。

Cloud Access Security Broker (CASB)

CASBは、SaaSアプリケーションを可視化し、きめ細かな制御を提供することで、許可されたアクセス、脅威の防御、コンプライアンスを保証します。

ジュニパーのCASBは、不正または不注意によるアクセス、マルウェアの感染と拡散、情報漏洩等のリスクからSaaSアプリケーションを保護します。これにより企業は、キャンパスや支社/拠点でのユースケースを想定したオンプレミス型、リモートワークを想定したクラウド型、あるいはハイブリッド型のいずれの形式でも既存環境を活用して開始することができます。

データ損失防御（DLP）

DLPは、データ取引を分類して監視し、ビジネスのコンプライアンス要件とデータ保護規則が遵守されることを確認します。

ジュニパーのDLPがファイルを読み取り、クレジットカード番号、社会保障番号、住所などのコンテンツを分類し、特定のタイプのデータが含まれるファイルとしてタグ付けします。そのデータが、企業のDLPポリシーによって消費されます。このポリシーは必要不可欠なもので、企業はドキュメントに対する粒度の細かい制御を追加する際に、HIPAAやPIIなどのタグを追加することができます。ユーザーが企業からデータを削除しようとすると、ジュニパーのDLPはその行動を阻止します。

Advanced Threat Prevention

脅威の状況が進化し、セキュリティリスクが加速する中で、脅威を特定してブロックするために、ネットワークエッジにある単一のデバイスに頼ることはもはやできません。その代わりに、セキュリティアナリストが未知の脅威の探索に集中できるようにし、組織のリスクをさらに低減するために、脅威認識ネットワークが必要です。

Advanced Threat Preventionは、暗号化通信を復号化できない場合でも、ボットネットやコマンド&コントロール（C2）を含むゼロデイ マルウェアや悪意のある通信を検出します。これにより、ファイルの隔離やアクセス権限の制御などのきめ細かい仕組みを実施します。

ジュニパーのAdvanced Threat Preventionの一環であるJuniper SecIntelは、ネットワーク上のすべての接続ポイントに脅威インテリジェンスを提供し、悪意のあるトラフィックをブロックして、脅威を認識するネットワークを構築します。SecIntelを脅威の可視性を高める有線および無線LANのWANエッジや、エンフォースメントポイントに展開する事でリスクを軽減できます。

セキュアなユーザーアクセス

オフィスや自宅にいる、または移動中のリモートワークの従業員に、効率的に仕事をするために必要なアプリケーションやリソースへの迅速かつセキュアなユーザーアクセスを提供します。セキュリティポリシーはIDに基づいており、どこからでもユーザーを追跡します。

ユーザー追跡（Follow-the-user）ポリシーが粒度の細かいリスクベースの制御でサードパーティの請負業者に自動アクセスを提供し、サードパーティのアクセスを攻撃ベクトルとして封鎖します。Secure Edgeのポリシーは、サードパーティがリソースにアクセスする際に追加の検証を要求し、終了予定日に基づいてアクセスが自動的に取り消されるように構成できます。コントラクターやサードパーティは契約満了後にアクセスできなくなります。

ユーザーは、複数の認証ポータルの間をジャンプしたり、データセンターへのバックホールトラフィックに煩わされることなく、企業のリソースにシームレスかつセキュアにアクセスできます。

管理者は、ユーザーが自宅から機密性の高いリソースにアクセスしているのであれ、オフィスからインターネットを閲覧しているのであれ、一貫したセキュリティポリシーの適用を確保することでリスクレベルを管理することができます。

シングルポリシーのフレームワーク

Secure Edgeは、SRXシリーズファイアウォールと同じポリシーフレームワークを使用します。これにより管理者は、SRXシリーズファイアウォール用に作成したポリシーを、最も近い場所にあるSecure Edgeポイントオブプレゼンスにルーティングするリモートユーザーや支社/拠点に対して、簡単に適用することができます。

管理者は、手作業でポリシーを再度作成したり、各ルールの配置場所を判断する必要がありません。Secure Edgeはこれらすべてを自動的に行うため、ユーザー、デバイス、アプリケーションのセキュリティルールをエッジ全体からデータセンター内まで一貫して適用することが非常に簡単になり、ポリシーギャップが減り人的エラーも排除され、ネットワーク全体がより安全になります。

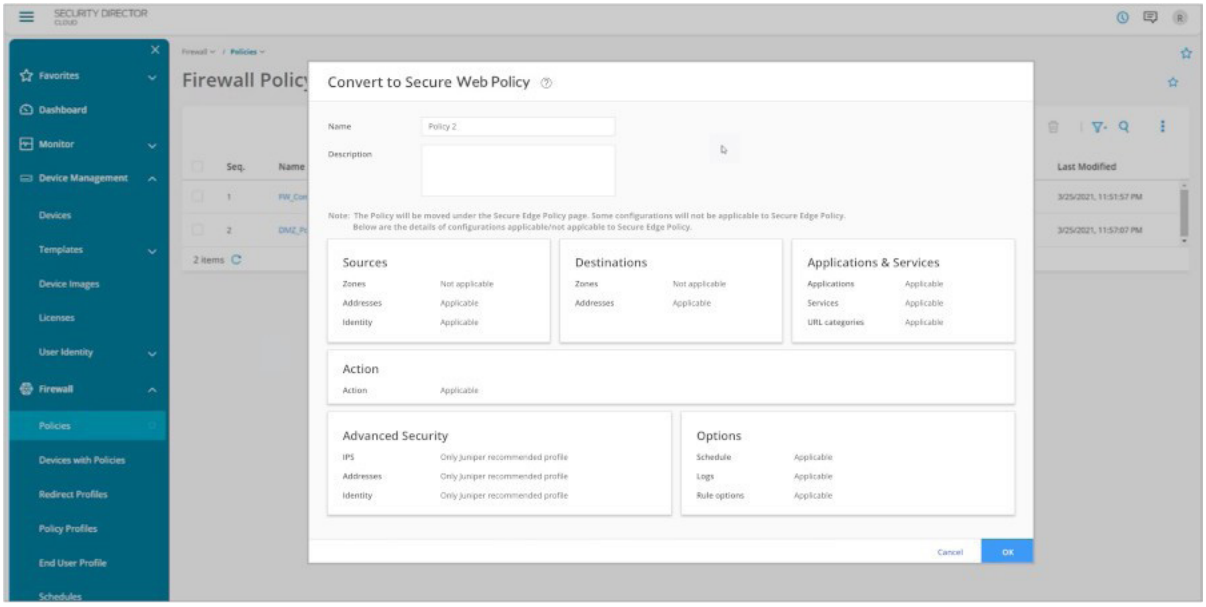

図2：単一のポリシーフレームワークと組み合わせた統合管理により、物理または仮想ファイアウォール用に作成したセキュリティポリシーを、Secure Edgeがこれらと同じポリシーをサービスとして提供するサイトにも簡単に、自動で適用することができます。

既存の投資を活用する

クラウドベースのセキュリティアーキテクチャへと移行するからと言って、既存のIT投資を放棄することにはなりません。Secure Edgeにより、組織は社内のペースでのセキュアアクセスサービスエッジ（SASE）アーキテクチャへの移行が可能となり、管理者はオンプレミスとクラウド型セキュリティとの間で個別の管理プラットフォームを切り替える必要がなくなります。導入、構成、管理のすべてが、SRXシリーズファイアウォールのすべてを管理する管理プラットフォームであるSecurity Director Cloudを通じて行われます。

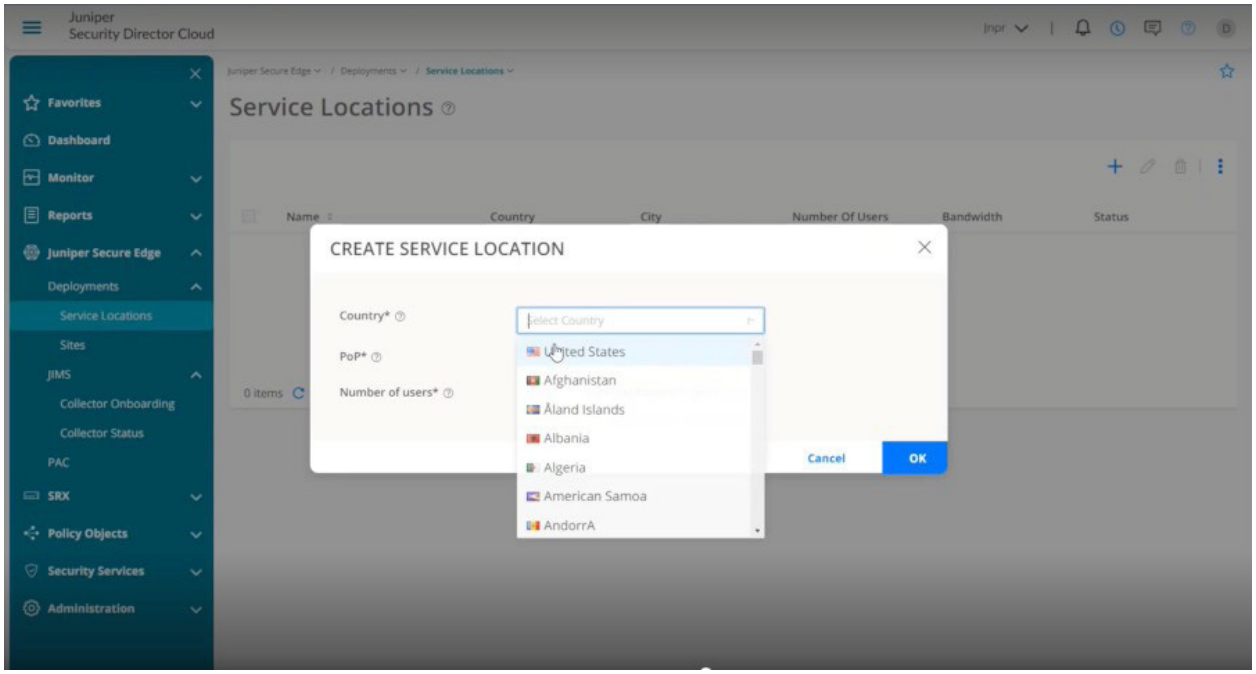

図3：簡単に使用できるWebインターフェイスを通じて、どこからでもサイトの導入と構成、ユーザー認証、ポリシーを容易に管理できます。

さらに、既存のIDソリューションを使用し続けたい場合は、それらを置き換える必要がありません。Secure EdgeはMicrosoft Azure Active DirectoryやOktaなどのすべての主要IDプロバイダーに対応しています。SAML（Security Association Markup Language）2.0をサポートしており、一般的なルーティングカプセル化（GRE）またはIPsecをサポートするルーターを介して機能します。

セキュリティ保証

従来のファイアウォールポリシーであるか、またはサービスとして提供するポリシーであるかに関わらず、ルールは適切に配置して、必要な時に効果を発揮できるようにすることが重要です。しかし、ルールはすぐに膨れ上がり、ルールが古くなったりシャドウ化したりすることで効果が失われることがあります。また、ルールが重複している場合、管理者は確実に変更を行うために、何百、時には何千ものルールを選別しなければならず、何時間にもわたる作業が必要になります。

Secure EdgeはSecurity Director Cloudを介して管理されるため、重複したルールやシャドウルールが有効化される前に特定されます。ルールのヒット数がハイライト表示されるため、管理者はすぐに変更を行い、新しいポリシーと既存のポリシーをインテント（意図）されたユーザーに対して適時に適用することができます。

実証済みのセキュリティ効果

クラウド型のFWaaS、SWG、CASB、DLP、Advanced Threat Preventionが使いやすいというだけでは十分ではありません。トラフィックやユーザーアクセスを制御し、脅威を検査するセキュリティサービスも効果的でなければなりません。Secure Edgeがサービスとして提供する脅威防御機能は、物理、仮想およびコンテナ型のSRXシリーズファイアウォールで提供される脅威防御機能と同じものです。これらの機能には、侵入検知、アンチマルウェア、Juniper Advanced Threat Prevention Cloudによる高度な脅威検知などがあり、複数のサードパーティのテストにより、サーバー側およびクライアント側の搾取に対しては98.9%、マルウェアに対しては100%の効果があることが証明されています。

クラス最高のSSEを提供

Juniper Secure Edgeは、クラス最高のSSEをフルスタックのSASEソリューションの一部として提供し、SASE移行のどの段階にいるのかに関わらず、企業がSASEアーキテクチャに移行できるようにサポートします。

ジュニパーは、クラウドのパワーを活用してネットワークとセキュリティの両方のエクスペリエンスの最適化を図るフルスタックのWANエッジとSSEを提供します。

ダイナミックなポリシーをユーザー、ユーザーグループ、デバイス、デバイスグループ等を中心にして作成することができるので、地理やネットワーク上の場所に関係なく、アクセスや脅威の保護に関するルールを一貫した形で適用することができます。管理者は、ルールセットの複製や再作成を行う必要がないため、業務効率の向上と組織内のゼロトラスト構想の推進に貢献します。

表1：Secure Edgeの機能とメリット

特長	メリット
アプリケーションの可視化と制御	Software as a Service (SaaS) アプリケーションを含む、アプリケーションアクセスの即時認識と管理の円滑化：ポート、プロトコルまたは暗号化の方法に関係なく、アプリケーション名、サービスの説明、内在リスクのレベル。
セキュアWebゲートウェイ	SSL/TLSプロキシおよび検査を装備したセキュアWebゲートウェイ機能により、ユーザーがどこにいてもWeb由来の脅威からWebトラフィックを保護し、インターネットへの直接アクセスをユーザーに提供します。
Cloud Access Security Broker（CASB）	CASBは、SaaSアプリケーションを可視化し、粒度の細かい制御を提供することで、許可されたアクセス、脅威の防御、コンプライアンスを保証します。不正または不注意によるアクセス、マルウェアの配信と分散、データの漏洩からSaaSアプリケーションを保護します。
URLフィルタリング	アプリケーションやセキュリティポリシーに統合できるWebトラフィックのカテゴリー化を提供することで、マルウェアのダウンロードがきっかけとなりWebから発生する脅威、フィッシングサイト、悪用キットなどのWeb由来の脅威からユーザーを自動的に保護します。また、Secure EdgeのURLフィルタリングは、Webアクセスを管理したり望ましくない閲覧行為を防止することで、組織のコンプライアンス維持をサポートします。
コンテンツ フィルタリング	有害な悪意のあるコンテンツが含まれていないか、電子メール、Webページ、ファイルを検査します。管理者は、許可、制限またはブロックするコンテンツをセキュリティポリシー内で詳細に管理することができます。
SaaSセキュリティ	データ、使用状況、コンプライアンス、脅威の防御とアクセスを含むSaaSアプリケーションの可視化と制御を提供し、ユーザーの動作を監視および制御し、許可されていないアプリケーションの使用、または「シャドーIT」に生じる潜在的なリスクを最小限に抑えます。
情報漏洩対策	ネットワーク、ユーザー、サービス間を移動する機密データや、SaaSアプリケーション内に保存されている機密データを監視し、保護します。規制されているデータが移動したり保管されるあらゆる場所で、コンプライアンス要件に従って、情報漏洩を防ぎます。 構造化および非構造化データ、データ分類、EDM（Exact Data Match）、光学式文字認識（OCR）をサポートします。
ユーザーID	Azure ADやOktaなどのIDサービスと統合して、個々のユーザーまたはユーザーグループに基づいてポリシーやアプリケーションの使用を定義します。IPアドレスの代わりにユーザーレベルでアプリケーションの使用に関する可視性を提供し、ネットワークを通過するアプリケーションのトラフィックへのインサイトを提供します。
ダイナミックユーザーセグメンテーション	ユーザー追跡（follow-the-user）ポリシーにより、攻撃ベクトルとなるサードパーティからのアクセスを制限するのに役立ちます。社内ネットワーク内外のユーザーの居場所に関わらず、ユーザーに適用するポリシーを作成して、従業員やサードパーティのコントラクターに対する自動アクセス管理を提供します。
侵入検出および防止サービス（IDS/IPS）	ネットワークやアプリケーションの悪用を軽減し、複数の第三者機関によるテストで効果が証明されたシグネチャでさまざまな攻撃から保護します。ジュニパーの侵入検出および防止（IDP）は最近検知された脆弱性を標的とする新しい悪用を常時監視し、最新のサイバー攻撃に対するネットワークの保護を最新の状態に維持して、攻撃者がネットワーク内に足がかりを得る前に突破した段階で攻撃者を撃退します。
アンチマルウェア	Cyber Threat Allianceなどの脅威情報共有団体の調査情報により強化され常に更新されるグローバル脅威データベースを使用して、エッジを保護します。Secure Edgeはインライン検査とブロッキングにより、既知のマルウェアがエンドポイントにインストールされるのを防ぎ、マルウェアへの感染による悪意のあるアウトバウンド（C2）通信をブロックします。
ドメイン名システム（DNS）フィルタリング	リスクが高いことで知られるドメイン（通常は攻撃キャンペーンに関連するドメインや不要なコンテンツを含むドメイン）を特定し、ドメインとそれに関連するIPアドレスとの通信をブロックします。
DNSセキュリティ	トンネリング、C2通信、ドメイン生成アルゴリズムなどの脅威に対するDNSクエリを分析し、不正侵入の試みを特定して、さらなる感染を防ぎます。攻撃者がセキュリティ制御を回避するために利用するDNS悪用の兆候を特定します。
脅威からの高度な保護機能	最新の脅威保護に対応したジュニパーのグローバル脅威インテリジェンスハブであるJuniper ATP Cloudを利用して、ゼロデイマルウェアを迅速に検知・抑制して、リアルタイムの脅威情報を取得してネットワーク上の全ポイントに配信することにより、脅威に対するレスポンスタイムを改善します。Juniper ATP Cloudは複数のサードパーティのテストにより新規のマルウェアやコモディティマルウェアに対して効果的であることが証明されています。
暗号化されたトラフィックのインサイト	完全なTLS/SSL暗号化解読の負担なく、暗号化のために失われた脅威の可視化を再現します。Secure Edgeは関連するSSL/TLSの接続データを収集します（これには、使用された証明書、ネゴーシエイトされた暗号スイート、接続の動作が含まれます）。ネットワークの動作分析や機械学習を使用してこの情報を処理して、接続が無害か有害かを判断します。悪意のあるトラフィックを切断し、トラック中のボットネットなどの脅威に対して防御します。
適応型脅威プロファイリング（Adaptive Threat Profiling）	既存のインフラストラクチャを利用して、ネットワーク上で発生するリアルタイムのイベントに基づくセキュリティインテリジェンスフィードを作成します。これらのフィードは企業毎に固有で、セキュリティポリシーに基づいて構成し、脅威を検知してインフラストラクチャをリアルタイムで更新して潜在的な攻撃をブロックするためにネットワーク上のその他の実施ポイントで利用することができます。
侵入されたホストの隔離	侵入されたデバイスを特定し、手動または自動で隔離リストに追加して、それらのデバイスによる機密データへのアクセスをブロックし、水平方向へのマルウェアの拡大を防ぎます。
エージェントレスオンランプ	エージェントレス機能によるセキュリティポリシーによりユーザーを保護します。ユーザーはシングルサインオン（SSO）でログインすることにより、アプリケーションや必要なデータに安全にアクセスできます。

特長	メリット
SaaS セキュリティ動態管理（SSPM）	明確に定義されたセキュリティガイドラインに照らし合わせてSaaS環境を自動評価し、複数のアプリケーションを管理する際の運用の複雑さを軽減し、設定ミスによるデータ損失を防ぎ、マルチクラウド環境でのコンプライアンスを確保します。CIS基盤ベンチマーク、SOC 2、PCI、NIST 800-53、もしくはHIPAAなどの共通規格やベストプラクティスに基づいたコンプライアンスライブラリを使用します。 お客様のSaaSアプリケーションに接続されるサードパーティアプリケーションの可視化と洞察を提供します。
クラウドデータディスカバリー	DLPテンプレートを使用して、クラウドアプリケーションのデータを定期的または特定の目的で評価し、セキュリティの状況や、外部への共有状況を検知し、PCI、HIPAA、GDPR、GLBAなどの多くのグローバル規格への対応をします。

製品オプション

Secure Edgeは、ユーザー数に基づくサブスクリプションライセンスとして購入可能。期間が1年間および3年間のライセンスは、スタンダード層とアドバンス層の両方でご利用いただけます。

特長	Standard	Advanced
TLS/SSLインスペクション	○	○
セキュアWebゲートウェイ	○	○
URLフィルタリング	○	○
コンテンツフィルタリング	○	○
アプリケーション可視性	○	○
ユーザーの認識とセグメンテーション	○	○
Standard threat prevention（脅威情報フィード、DNSフィルタリング、マルウェア防御、侵入されたホストの隔離）	○	○
Advanced Threat Prevention（DNSセキュリティ、ゼロデイマルウェア防御、暗号化トラフィックのインサイト、適応型脅威プロファイリング）	×	○
侵入検出および防止サービス（IDS/IPS）	×	○
アウトオブバンドCASB-DLP-SSPM	アドオン	アドオン

WAN Assuranceへのアドオン

お客様は、アクティブなWAN Assurance（SD-WAN）またはSecure Edgeライセンスにアウトオブバンドcasb-dlpを追加できます。

Out-of-band CASB-DLP*	Standard	Advanced
CASB	○	○
DLP	○	○
SaaSセキュリティ動態管理（SSPM）	X	○
追加クラウドデータディスカバリー（TBあたり）	アドオン	アドオン

*アウトオフバンドCASB-DLPライセンスは、Juniper Secure EdgeもしくはJuniper WAN Assurance/SD-WANのアクティブベースライセンスに関連付ける必要があります。

仕様

	Standard	Advanced
トラフィック転送	保護アクセス認証（PAC）、GRE、IPsec	PAC、GRE、IPsec
認証	Security Assertion Markup Language（SAML）、Lightweight Directory Access Protocol（LDAP）、Juniper Identity Management Service（JIMS）	SAML、LDAP、JIMS

Juniper Security Director Cloud

Security Director Cloudは、フォームファクターに関わりなく、すべてのセキュリティポリシーに対応したジュニパーのクラウドベースの集中管理プラットフォームです。Security Director Cloudを利用することで、企業はオンプレミス、クラウド内、クラウドからなど、あらゆる場所でセキュリティを管理することができ、ユーザー、デバイス、およびアプリケーションがどこに存在しようとも、統合されたポリシー管理が得られます。ポリシーは一度作成すれば、どこへでも適用できます。

Security Directorクラウドでは、一元化されたインターフェイスを通じて、広範にわたるセキュリティポリシー管理と制御をすることができます。オンプレミスの物理的、仮想的およびコンテナ化されたファイヤーウォール上と複数のクラウドで同時にポリシーを実施し、さらにSecure Edge FWaaS、SWG、CASB、DLPおよびAdvanced Threatポリシーに対するポリシーも実施します。管理者は、ゼロタッチプロビジョニング、構成、ルールの配置、効果など、セキュリティポリシーライフサイクルの全ての段階を簡単に管理しながら、ネットワーク全体のリスク元に関するインサイトも得られます。

企業はSecurity DirectorクラウドとSecurity Directorのオンプレミスインスタンスを同時に使用して、SASEアーキテクチャに安全に移行することができます。

注文情報

Juniper Secure Edgeのご注文とソフトウェアのライセンス情報については、ご購入方法のページ（https://www.juniper.net/jp/ja/how-to-buy/form.html）をご覧ください。

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、製品Webポータル https://www.juniper.net/jp/ja/privacy-policy.html をご覧ください。

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。

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
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：+31.207.125.700

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
https://www.juniper.net/jp/jp/

JUNIPER NETWORKS | Driven by Experience™