APAC Cohesion
Juniper Secure Edge
いつでも どこでも ユーザーを安全に守る

Tech Roundup Q4-2022

ジュニパーネットワークス株式会社

JUNIPER NETWORKS | Driven by Experience™

あらゆる接続ポイントにセキュリティを拡張し、ユーザー、アプリケーション、インフラを保護します

脅威を認識するネットワークの力

Gartner Peer Insights Customers' Choice 2022

上位 10 社のうち 9 社

グローバルサービスプロバイダーがジュニパーを利用してモバイル加入者ネットワークの接続とセキュリティ確保を実現

ネットワーク・セキュリティ・チームの節約

20 %

ジュニパーのセキュリティ・ソリューションの導入により、20 %の時間短縮を実現

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

canalys CYBERSECURITY CHAMPION 2021

THE CHANNEL CO. CRN SECURITY 100 2021

Juniper Networks AA Enterprise Firewall February 2021 Cyber Ratings

cyber secured AWARDS 2020

JUNIPER NETWORKS SRX5400 JUNOS 18.2X30.1 DATA CENTER SECURITY GATEWAY NSS LABS RECOMMENDED NOVEMBER 2019

AIセキュリティ機械学習

2022年 ガートナー・ピアインサイト「顧客の声」。ネットワーク・ファイアウォールGARTNER PEER INSIGHTS CUSTOMERS' CHOICEバッジは、Gartner, Inc.および/またはその関連会社の商標およびサービスマークであり、許可を得てここに使用されています。

Juniper Secure Edge

JUNIPER NETWORKS | Driven by Experience™

Agenda

- SASE の概要
- JSE 展開の詳細
- CASB と DLP
- ロードマップ
- リソース

デジタルの世界は変化している

進化するアーキテクチャの回復力とスケーラビリティ

現在 1 つの組織は平均して
2.6 のパブリッククラウドと 2.7 の
プライベートクラウドを使用しています。

どこからでもすべてにアクセス

労働者の 75% が
週に2~3日以上
自宅で仕事をすることになります。

サイバー攻撃の成功率が急増

企業の 63% が侵害され
ゼロデイエクスプロイトの使用は
2021 年に2倍以上になりました。

ネットワークは高度に分散されより複雑になっています

IT エグゼクティブの 75% は
自社のネットワークが複雑すぎて
「懸念される」リスクがあると述べています。

Juniper Connected Security

クライアントからワークロードまで、どこでも、どんな場所でも

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**
すべての接続ポイントを安全に保護

SASE の概要

JUNIPER NETWORKS

Juniper SASE

AI-driven SD-WAN + Juniper Secure Edge

AI-driven SD-WAN

Marvis Virtual Assistant

- フルスタックのブランチオペレーション
- 先進の AI & ML
- セッションスマート・ネットワーキング
- ゼロトラスト
- セグメンテーション

+

Juniper Secure Edge

- FWaaS
- SWG
- CASB
- DLP
- ATP

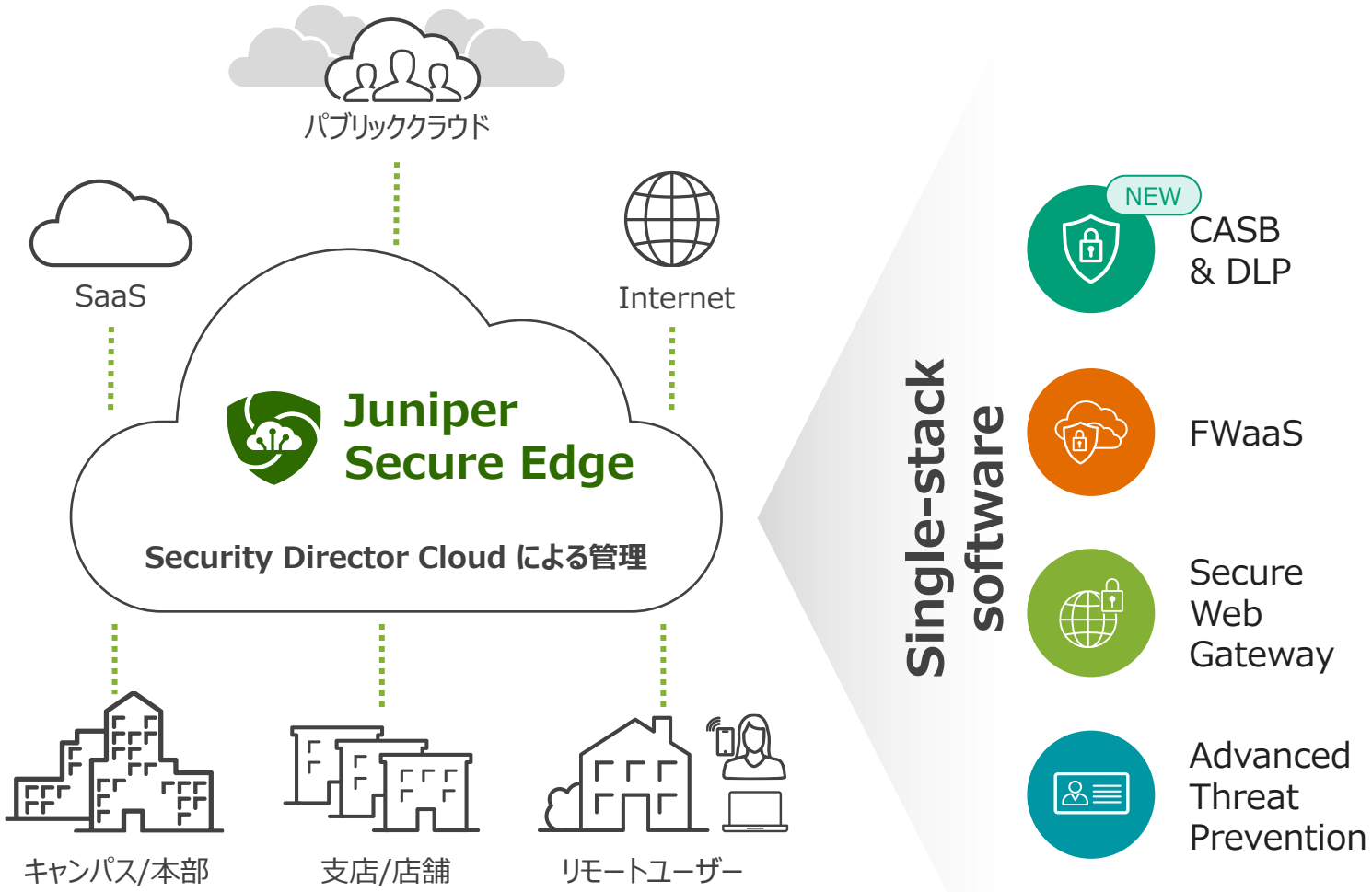
- アプリケーションコントロール
- アイデンティティとアクセスコントロール
- 侵入防止
- アンチマルウェア
- スレット インテリジェンス
- セキュアなウェブアクセス

Secure the Edge

あらゆる場所で
ユーザーとデバイスを
つなぎ、保護する

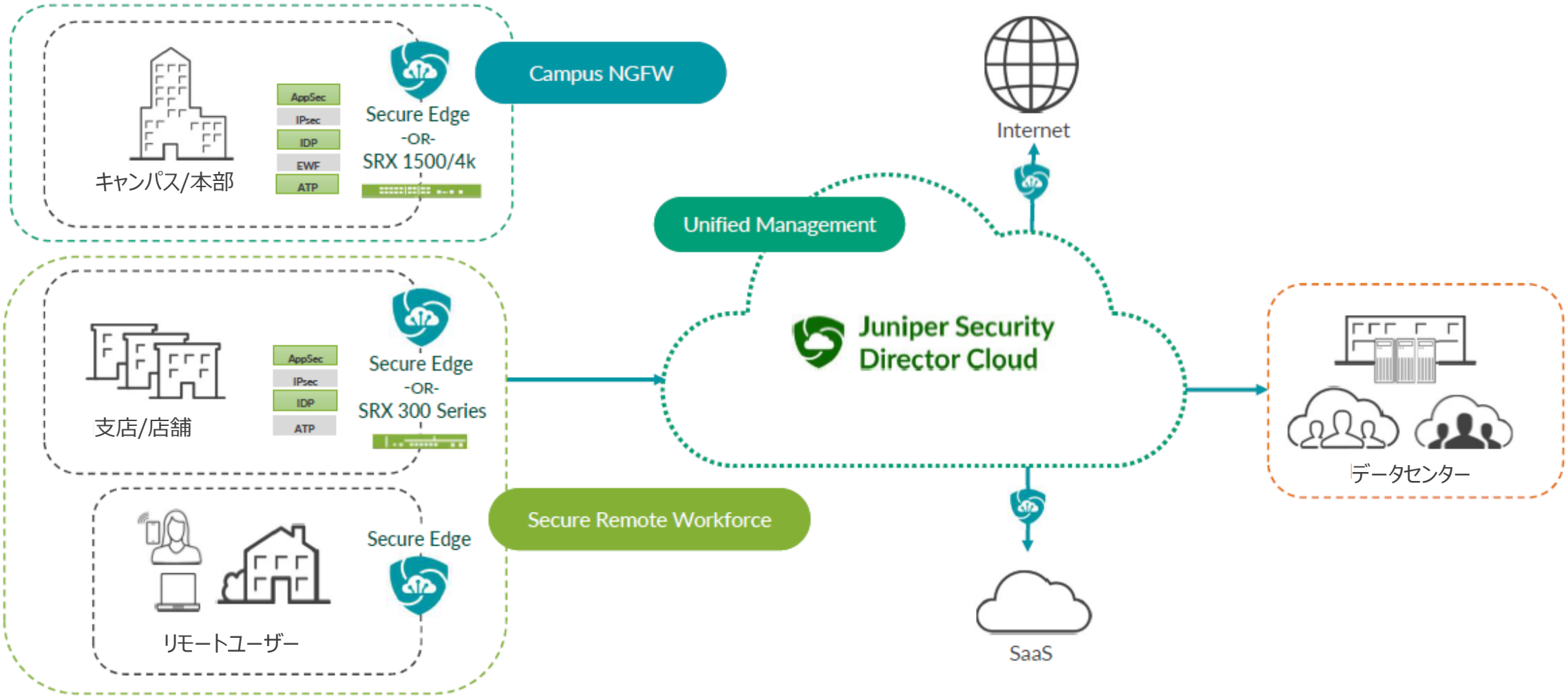
"ジュニパーは優れた
ファイアウォールセキュリティを
提供し、 ウイルスや不審な
攻撃、脅威から ネットワークと
資産を保護します。
また、ファイアウォールは
小規模なネットワークから
大規模なネットワークまで
パフォーマンスに影響を
与えることなく対応することができます。"

- ガートナー・ピアインサイト 2021年6月号
サービス機関のセキュリティ管理者



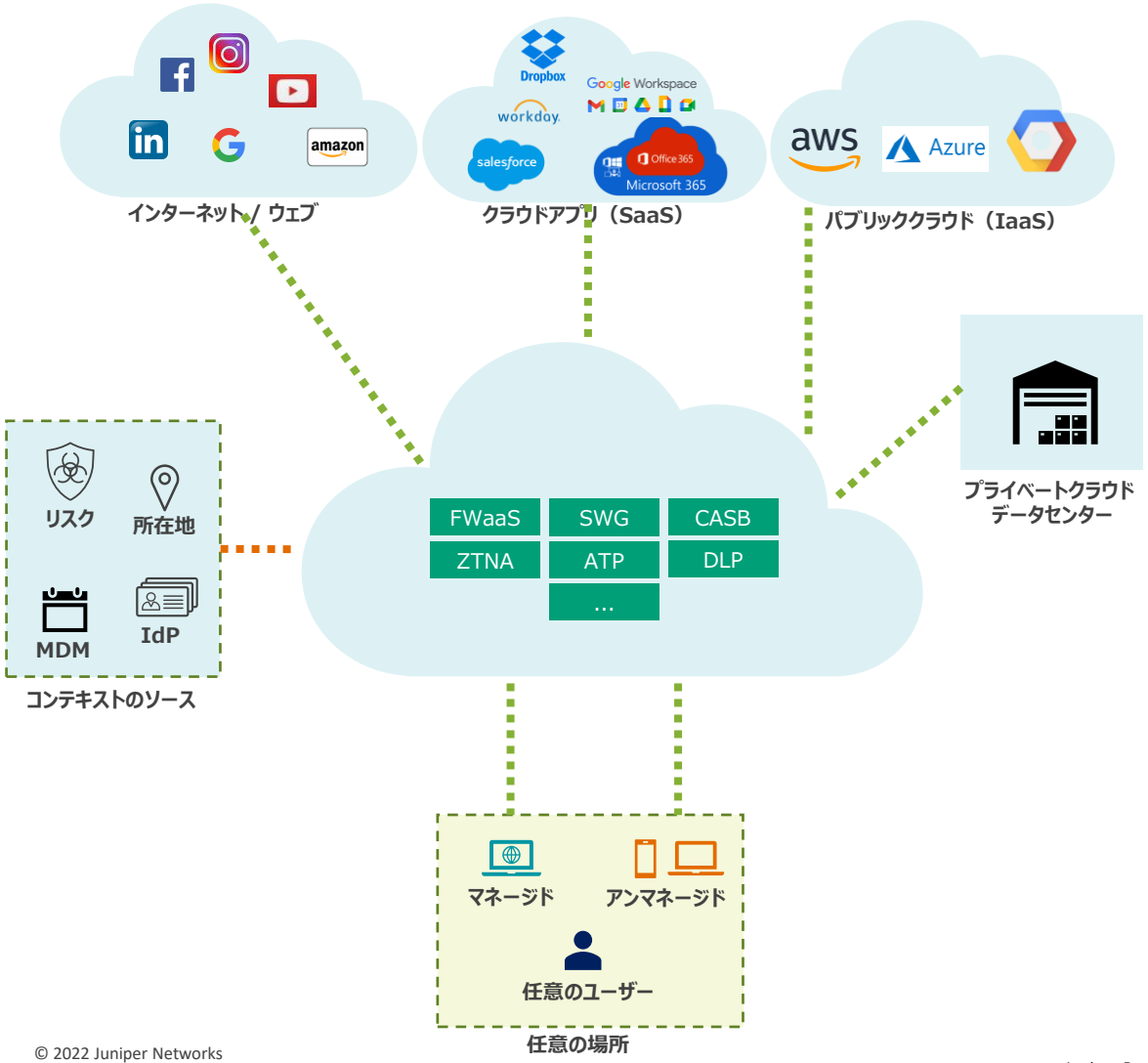
ブランチセキュリティからセキュア（エンタープライズ）エッジへ

あらゆる場所でユーザーとデバイスをつなぎ、保護する



SSE の主な使用例

クラウドで実現するセキュリティ



視認性

- 企業資産（ユーザー、デバイス、アプリ、ネットワーク、クラウド）に関わる利用状況の把握
  - 許可された使用、許可されたものとされていないもの（シャドーIT）
  - 機密データ、異常値など

アクセス制御

- コンテキストを考慮した**アクセス制御**と**アクティビティ制御**を**リアルタイムに実行**します。
  - 許可、拒否
  - コーチ／警告、隔離、暗号化、など。

脅威の防止

- 脅威の発見と防止
- 外部情報（EDR/XDR、SOARなど）に基づくポリシーの適用

データ保護

- 企業のアプリ/デバイス/データベースとの間でやり取りされる機密データを検出し、保護する
  - 動いているデータ

お客様とのパートナーシップ

JSE は目的に応じて提供可能です

セキュア SD-WAN/SASE に興味がある

運用、デプロイメント、ポリシーが容易で
購入プロセスも簡単です

ファイアウォール,セキュリティに興味がある

SD-WAN ベンダーを既に選定している、もしくは
現状、SD-WAN に興味はないが、セキュリティベンダーが
SASE（または SSE）戦略を持っていることを期待している

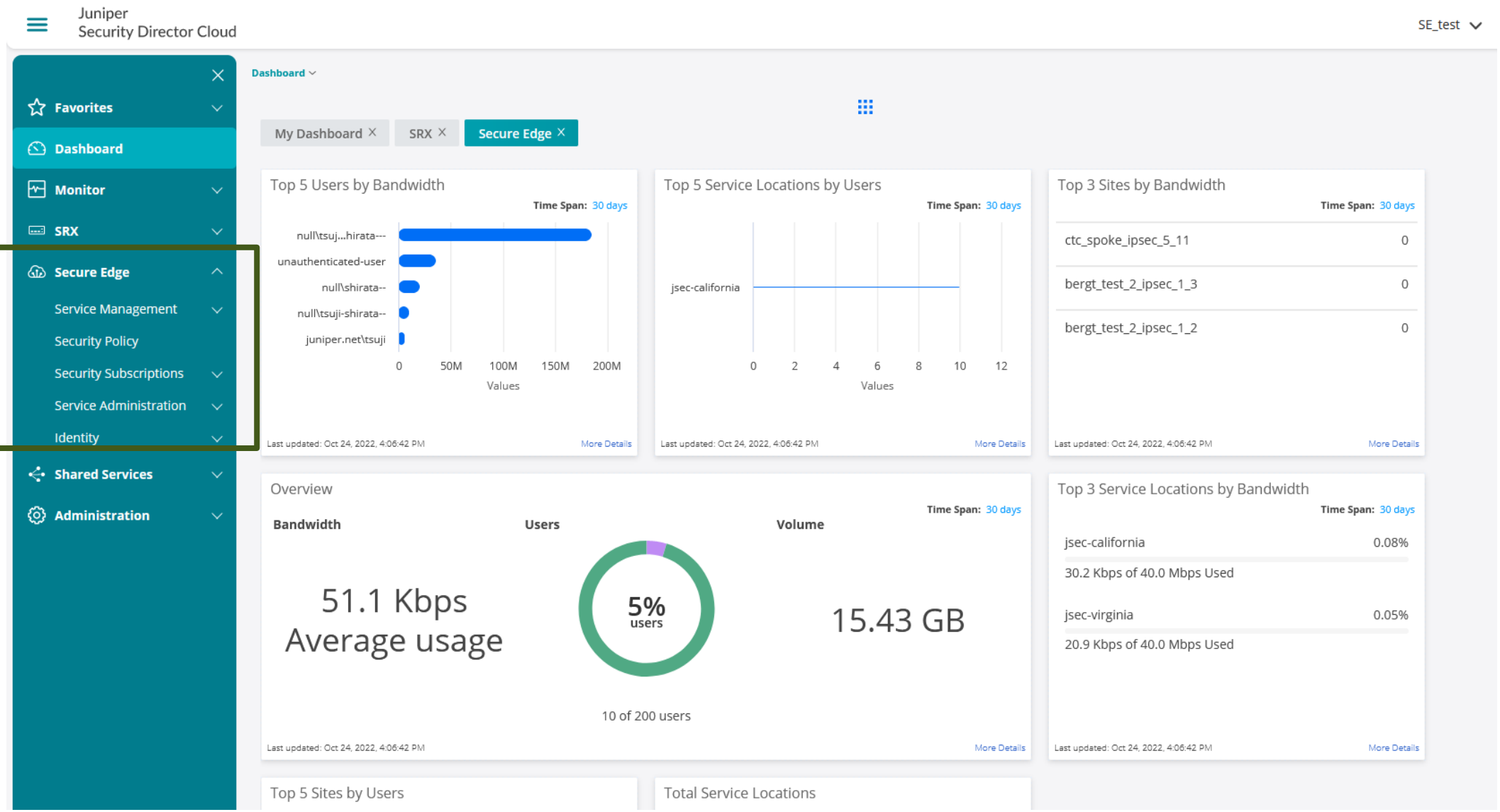
SD-WAN に興味がある

セキュリティベンダーを既に選定している、もしくは統合の
準備が整っているものの、1年以内にチャンスがあり、
SD-WAN ベンダーがSASE（または SSE）戦略を
持っていることを期待している

JSE 展開の詳細

JUNIPER NETWORKS

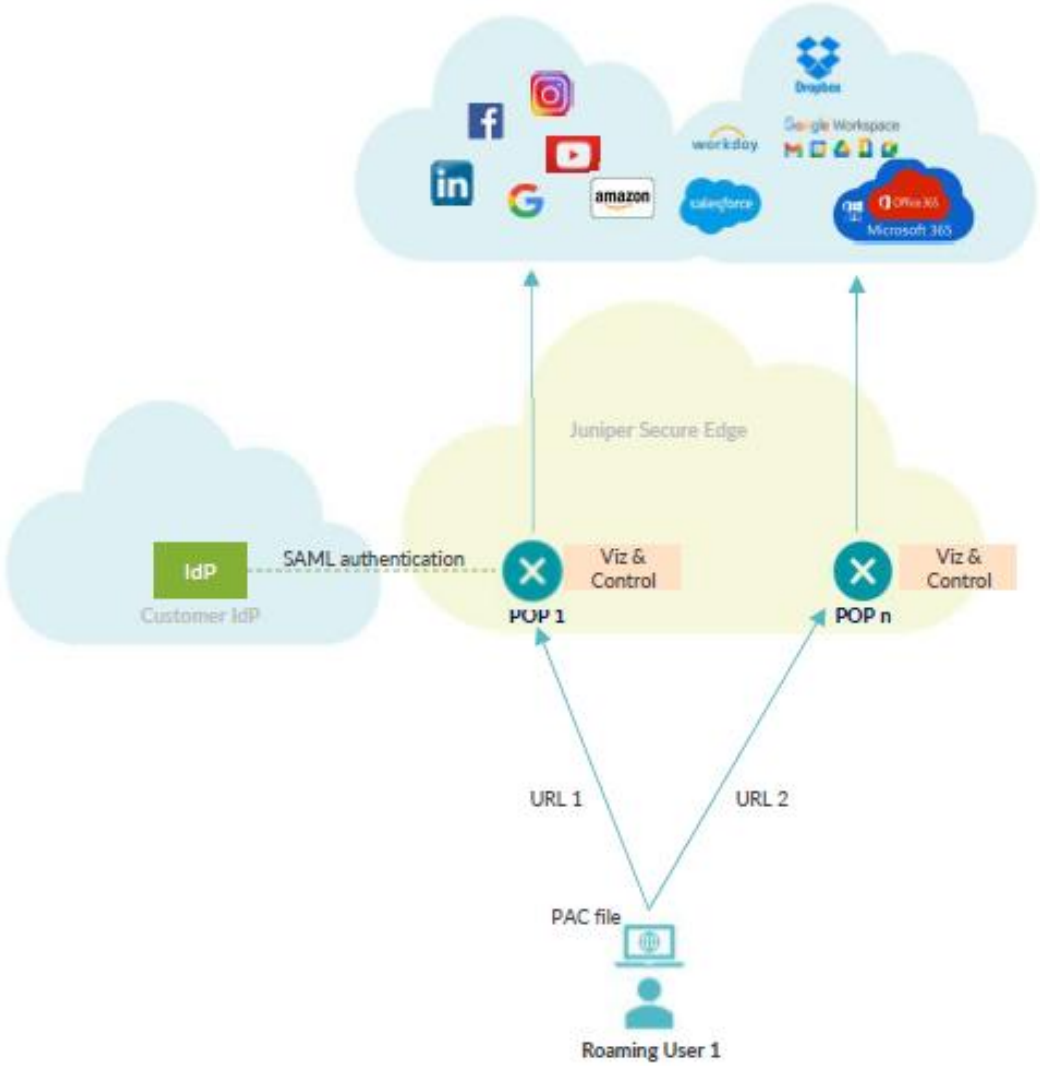
Security Director Cloud の ユーザーインタフェース



サービス拠点（POP）

- POPS - 合計 4 つの POP が利用可能で、今後さらに追加される予定です
- 2 つの POP を用意し、最小限のサービスを選択している
- ユーザー
  - ユーザー数で POP あたりのデータプレーンインスタンス数が決まる
  - 現在、1,000 ユーザーあたり 1 インスタンスを展開 - デバイスは考慮されない
  - (1 ユーザー 5 デバイス = 1 ユーザー）
- 帯域幅
  - 帯域幅は、UI では次のように表されます
    - "プロビジョニング" - 想定されるユーザー数に基づいています
    - "送信" - 管理者の参照および会計処理のために使用されます
  - トンネル最大負荷 300 Mbps

ローミングユーザーによる Web/SaaS アクセス

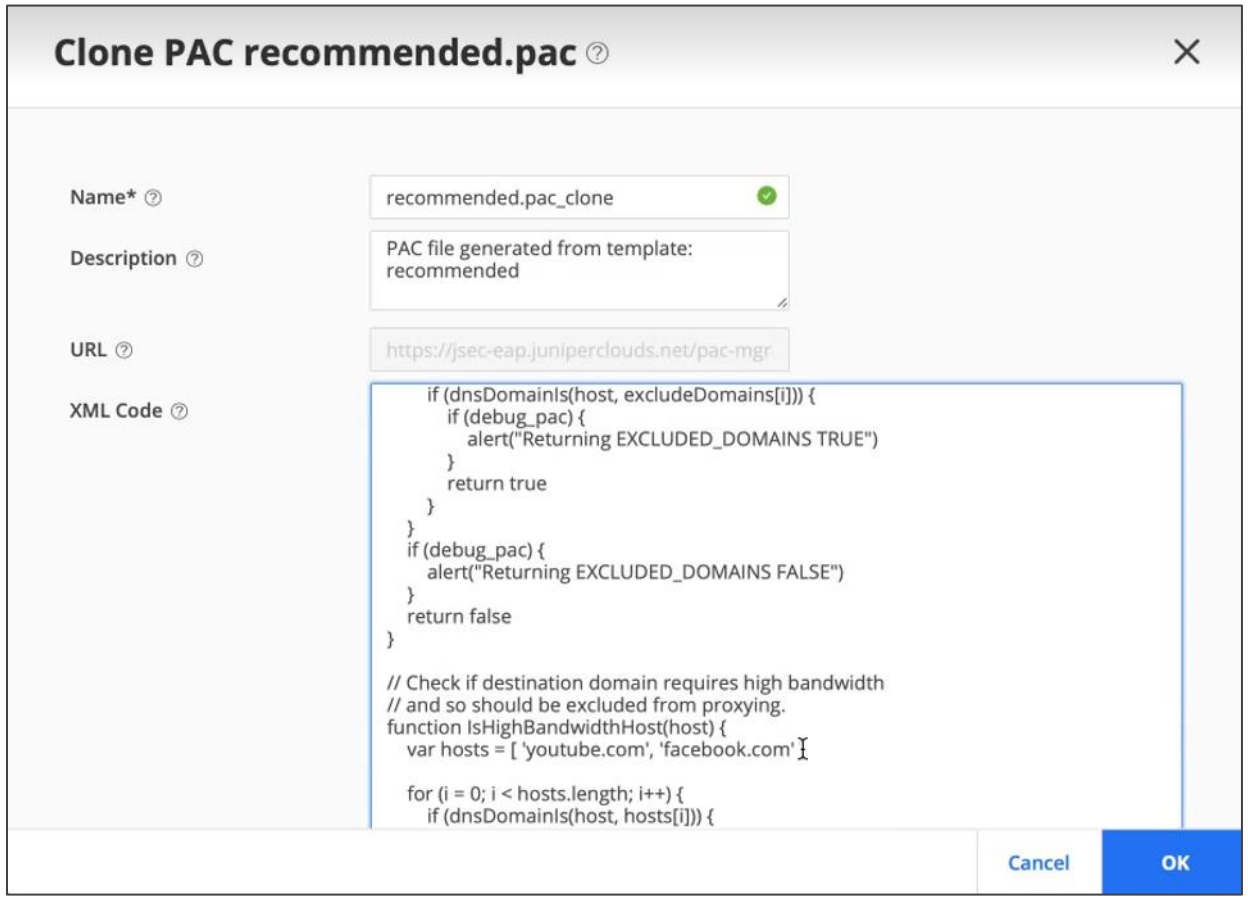


エンドユーザーとエンドポイント	管理対象デバイスのローミングユーザー
トラフィックリダイレクション	HTTP/S で「最寄りの」POP へ
認証	SAML（ IdP 統合）、LDAP、ローカルデータベースによるユーザー認証
コンテキストを考慮したエンフォースメント	**Web/SaaS のトラフィック**に対して、アイデンティティとアプリケーションを意識した可視化と制御
継続的な許可	ATP クラウドによる高度な脅威防御

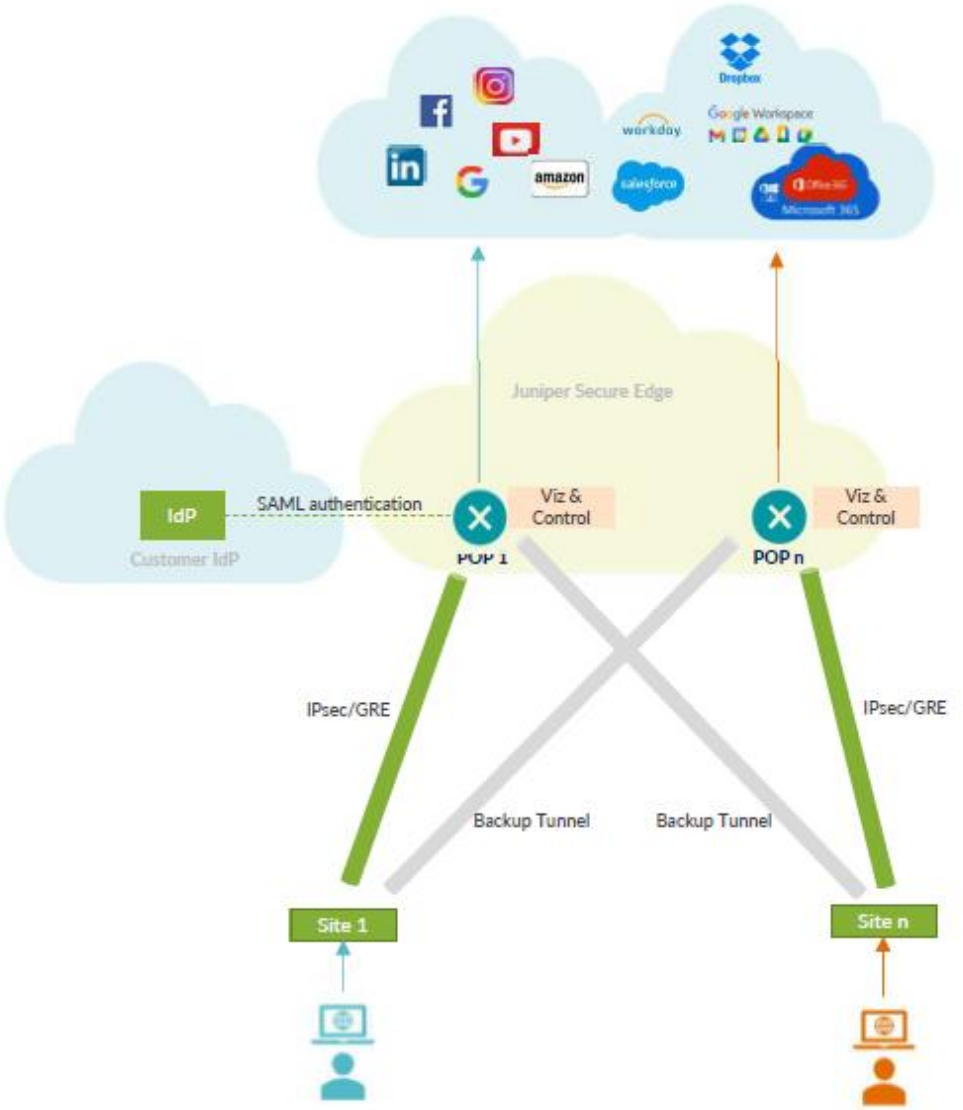
ローミングユーザー - PAC (Proxy Auto Configuration)

PAC とは？

- ユースケース認証されたユーザーのみで管理される
  Windows、MacOS、iOS、またはAndroid クライアント
  - 対応ブラウザ Chrome、Firefox、Microsoft Edge
    （Safari 対応予定）
- ブラウザトラフィック（HTTP/S）にのみ適用され
  すべてのトラフィックはプロキシされます（Explicit Proxy）
  - エンドポイント証明書が必要
- 推奨 PAC ファイルはあらかじめ定義されています
- 推奨 PAC ファイルはクローン化し
  独自のユースケースに 合わせることができる
- DNS
  - AWS で利用されている Route 53 は
    「最も近い」POP の位置の IP アドレスを返します



オンプレミスユーザーによる Web とインターネットへのアクセス



エンドユーザーとエンドポイント	あらゆるオンプレミスユーザー（従業員、契約社員、ゲスト）、 あらゆるデバイス（管理下、非管理下）
トラフィック リダイレクション	検査のために、すべてのトラフィックを Secure Edge にルーティングする可能性がある
認証	JIMS 経由のユーザー認証（クラウド Idp を追加予定）
コンテキストを 考慮した エンフォースメント	アイデンティティとアプリケーションを意識した、 **すべてのトラフィックの可視化と制御**
継続的な許可	ATP クラウドによる高度な脅威防御

サイト - オンプレミスブランチユースケース

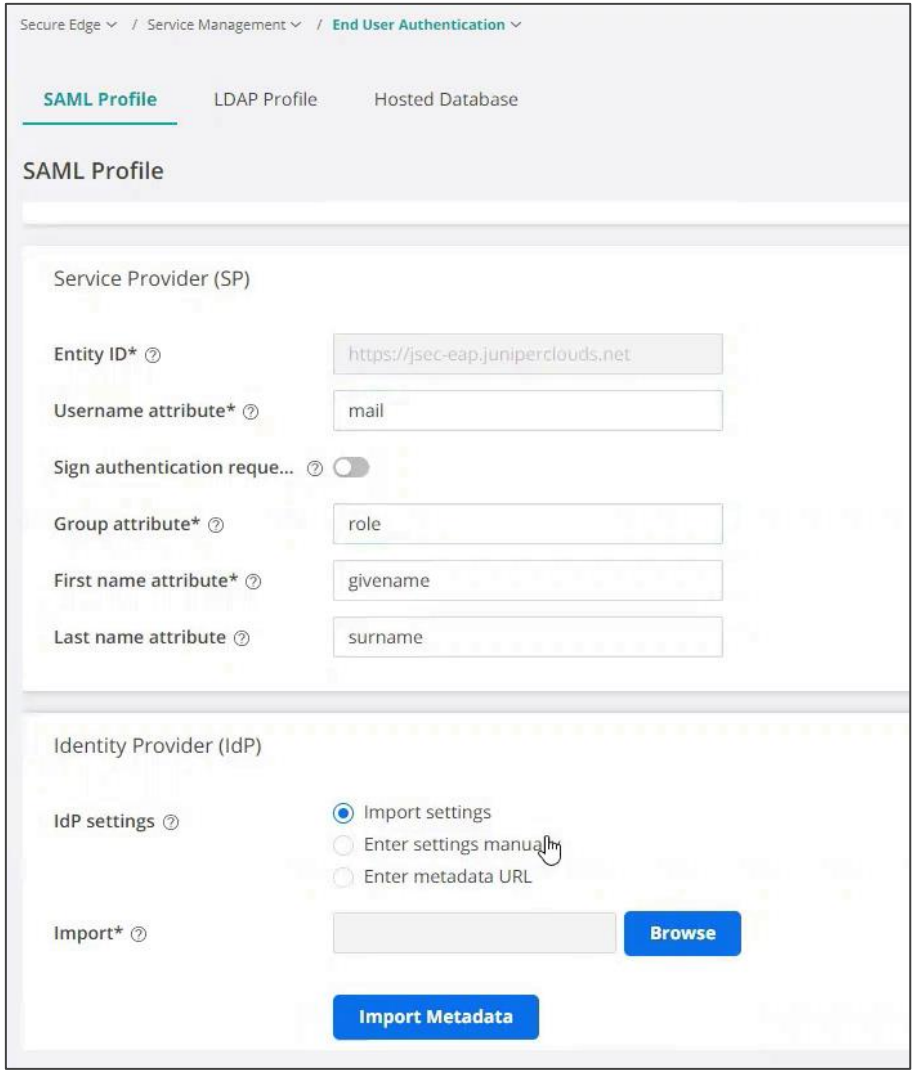
- ユースケース：すべてのユーザー（認証済み、未認証）、デバイス、ネットワークトラフィック
- ユーザー数を選択することでプロビジョニングされる帯域幅が決定されます
  - その際、トンネル構成も決定されます
- トラフィックフォワーディング
  - CPE で NAT しないこと
    ソース IP はユーザーを特定するために重要です（UserFW のマッピングのため）
  - 認証は、JIMS Collector との連携によるユーザーと IP のマッピングに基づきます
    （オンプレミスの Active Directory の場合）
  - プライマリとバックアップの 2 つのトンネルを設定（ECMP は必要ありません）
  - 2 種類のトンネリングオプション
    - IPSec 優先
    - GRE は暗号化されていない、ネイティブのヘルスモニタリング機能なし、GRE キープアライブサポートなし

プロキシ

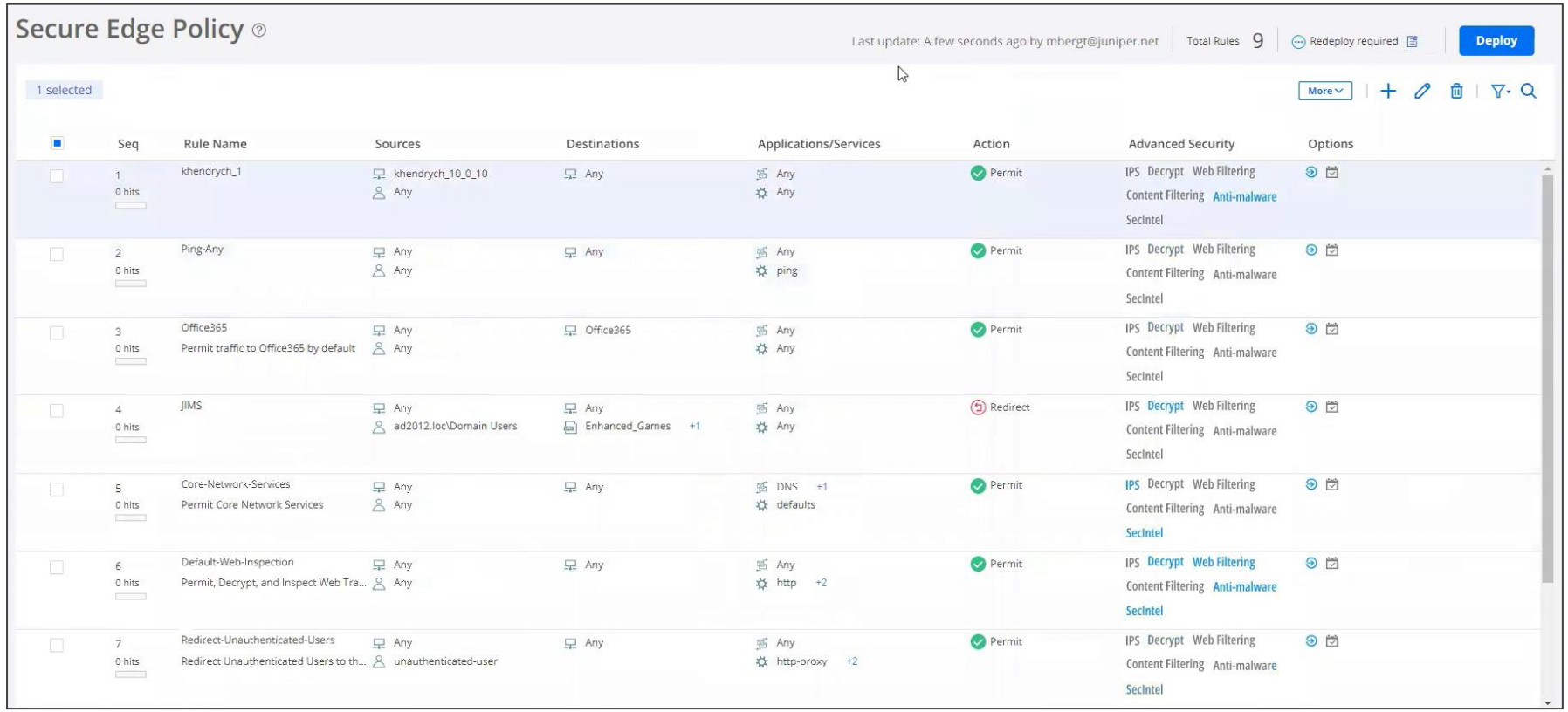
- TLS 1.3/1.2 対応
- エンドポイント SSL 証明書はローミングで使用する場合に必要であり、オンプレミスブランチでトラフィックを復号化する場合に必要です
- ローミングユーザー
  - Explicit Proxy - すべてのトラフィックがプロキシされます。
  - ユーザーと IP のマッピングはドメイン(ユーザー) Cookie に基づく
- オンプレミスユーザー - Transparent Proxy - ポリシー設定によりプロキシ動作を決定します
  - 標準的な UserFW ベースのポリシーを適用 - ポリシーで復号化が有効で、SOURCE の 設定によって制御されている場合にのみ復号化する
  - ユーザーと IP のマッピングは、IP ベース

認証とユーザー識別

- ユーザーの認証と識別のためのオプション
- ローミングユーザー
  - SAML: GA には Okta with MFA と AzureAD が含まれる予定です
  - LDAP
  - ホスティングデータベース
- オンプレミスユーザー
  - Juniper Identification Management Service Collector
  - IdP サービスは将来的に対応予定
- グループ情報に対応
  - 以下より抽出:
    - JIMS の Active Directory
    - SAML アサーションによる認証サービス



セキュリティポリシー
対応する NGFW の機能



- ✓ IDP
- ✓ ウェブフィルタリング
- ✓ コンテンツフィルタリング
- ✓ SecIntel
- ✓ アンチマルウェア

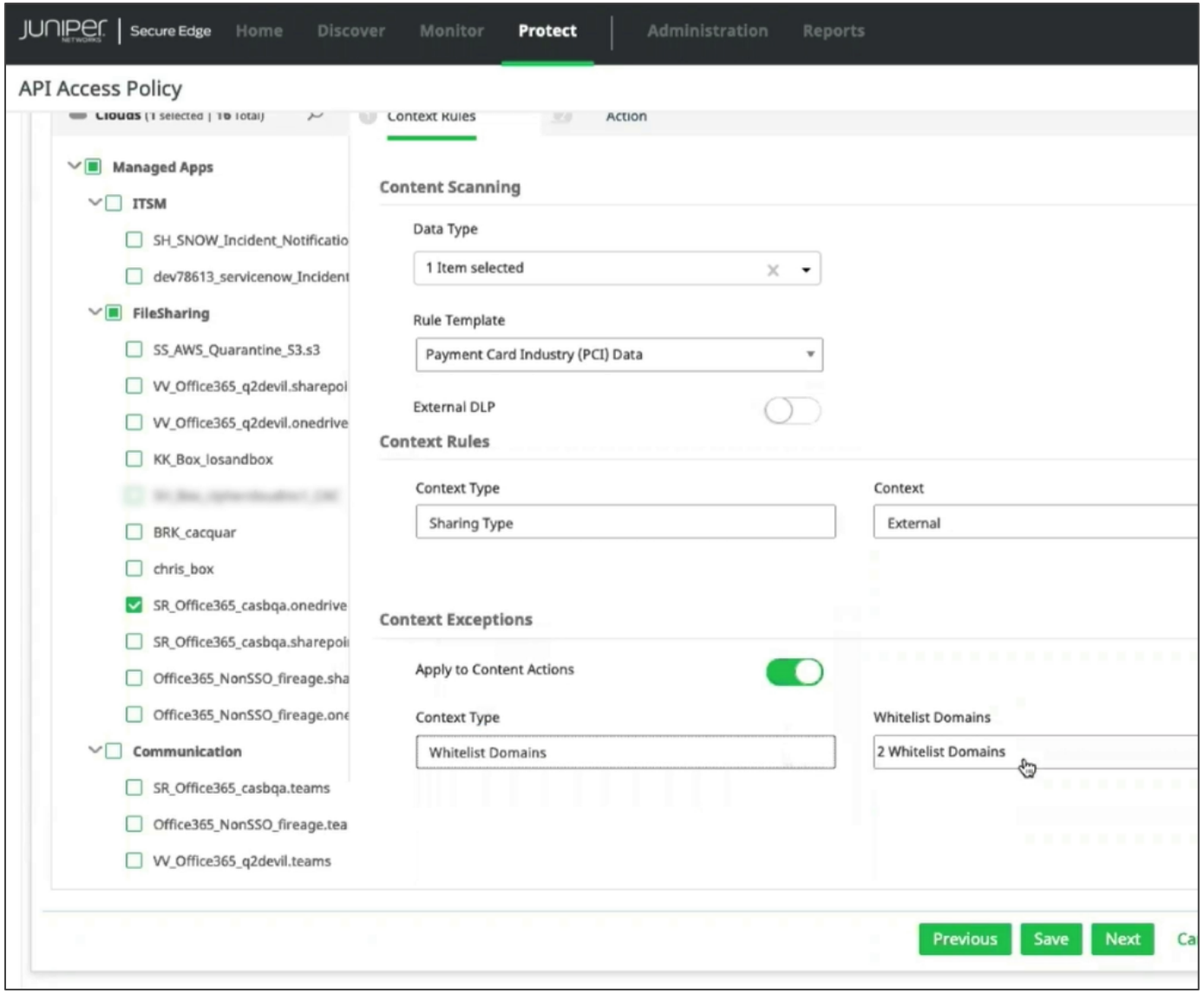
クラウドアクセスセキュリティブローカー(CASB)
データロスプレベンション(DLP)

- 高度な分類とデータ損失防止（DLP）で
  ビジネスクリティカルなデータを保護します
- 暗号化と権限管理で外部と共有するデータを
  安全に管理
- ユーザーとエンティティの行動分析（UEBA）による
  インサイダー脅威の検出
- クラウドインフラとアプリケーションのセキュリティ管理

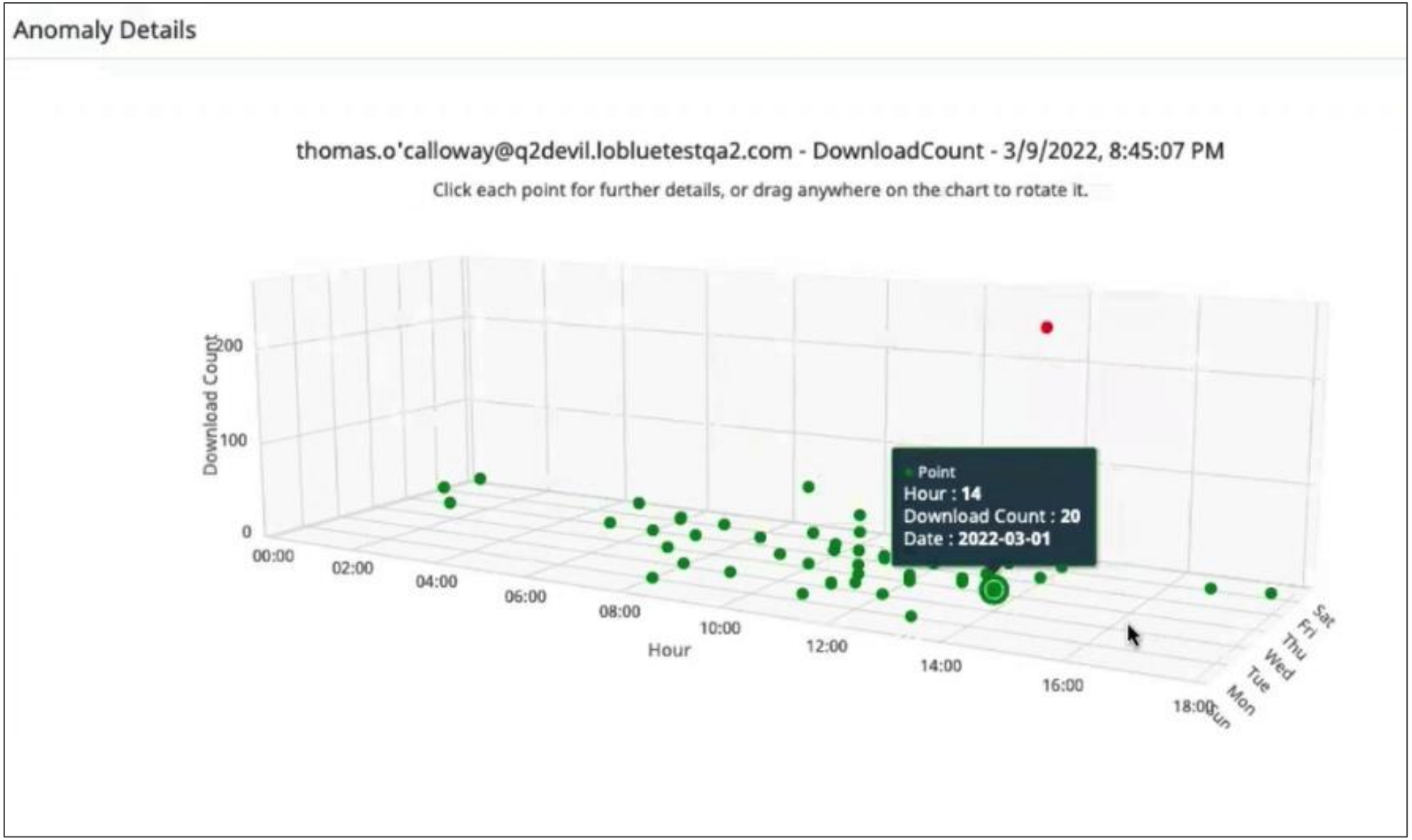
アクセスポリシー

管理者が指定可能:

- ✓ データ型（PCI、PII）
- ✓ アクション（ダウンロード、アップロード、共有）
- ✓ ホワイトリストドメイン
- ✓ ブロックリスト入りドメイン
- ✓ ポリシー(許可、拒否、MFA)



ユーザー行動データの異常の発見



Secure Edge ロードマップ

コア SSE

- FWaaS
- SWG
- 高度な脅威からの保護
  - 脅威のフィード
  - サンドボックス化
  - 暗号化されたトラフィックインサイト
- DNS セキュリティ
- IDS/IPS
- アウトオブバンド CASB & DLP
- SSPM

- Security Director Cloud による一元管理・ポリシー

サービス拡充

- インライン CASB & DLP
- エンドポイントクライアント
- リモートアクセス as a Service

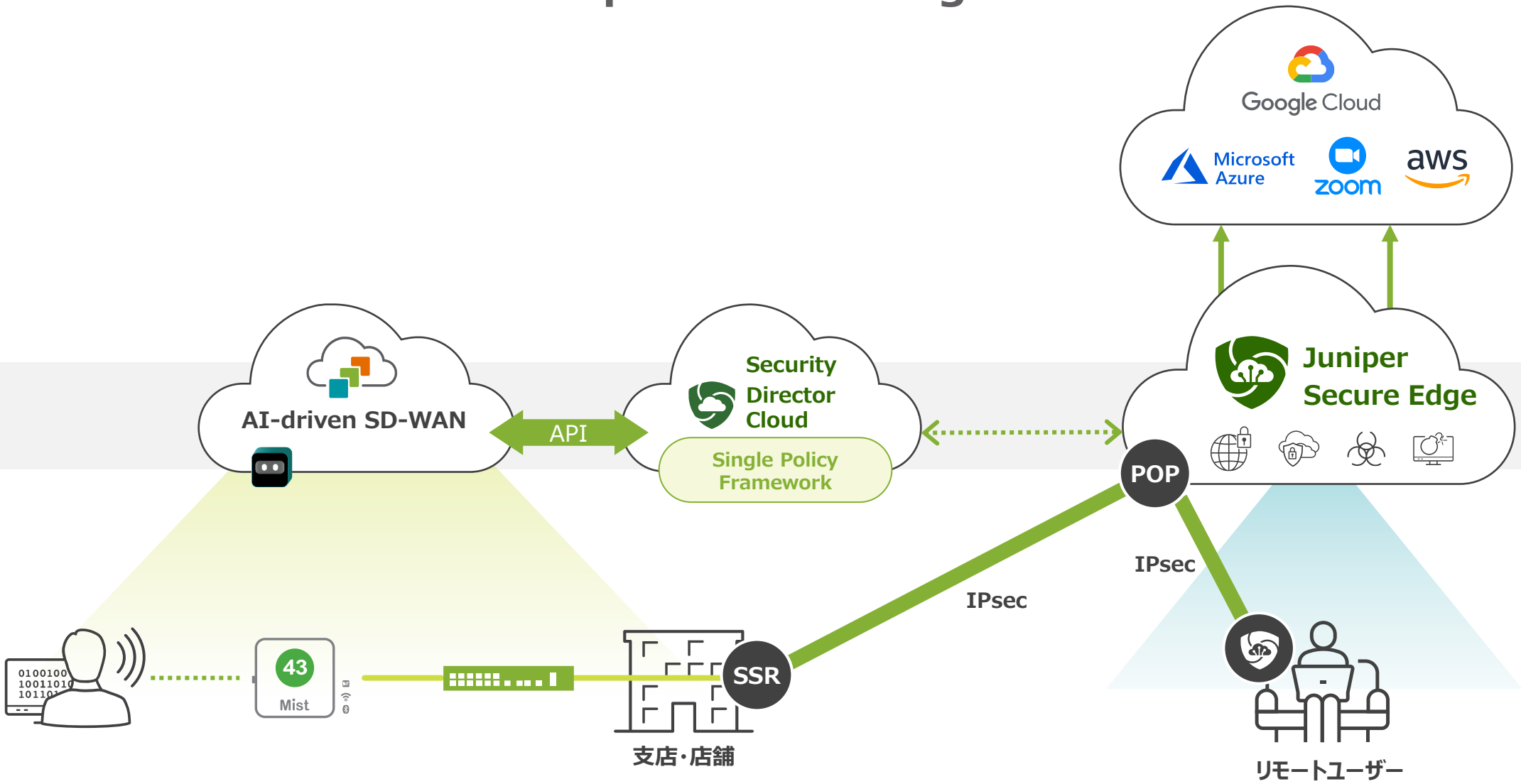
- グローバルクラウドフットプリントの拡大
  - EMEA、アジア太平洋地域

エッジから DC までのゼロトラスト

- ゼロトラストネットワークアクセス
  - エージェントベース
  - エージェントレス
- リモートブラウザの隔離

ジュニパーの SASE が活躍

AI-deiven SD-WAN + Juniper Secure Edge



Juniper Secure Edge のライセンシング

従量制

- ユーザー数に応じた SKU
- SKU tier bundles - 買いやすく、使いやすい
  - 標準: FWaaS ＋セキュア Web アクセス
  - アドバンスド: 標準機能すべて＋ IPS＆ATP クラウド
- Security Director Cloud のライセンスを含む
- サポート含む
- クラウドサービス拠点（POP）2 ヶ所含む
- サブスクリプション期間 1 年、3 年

アドオンの柔軟性

- サービス拠点（POP）追加
- ログストレージの充実

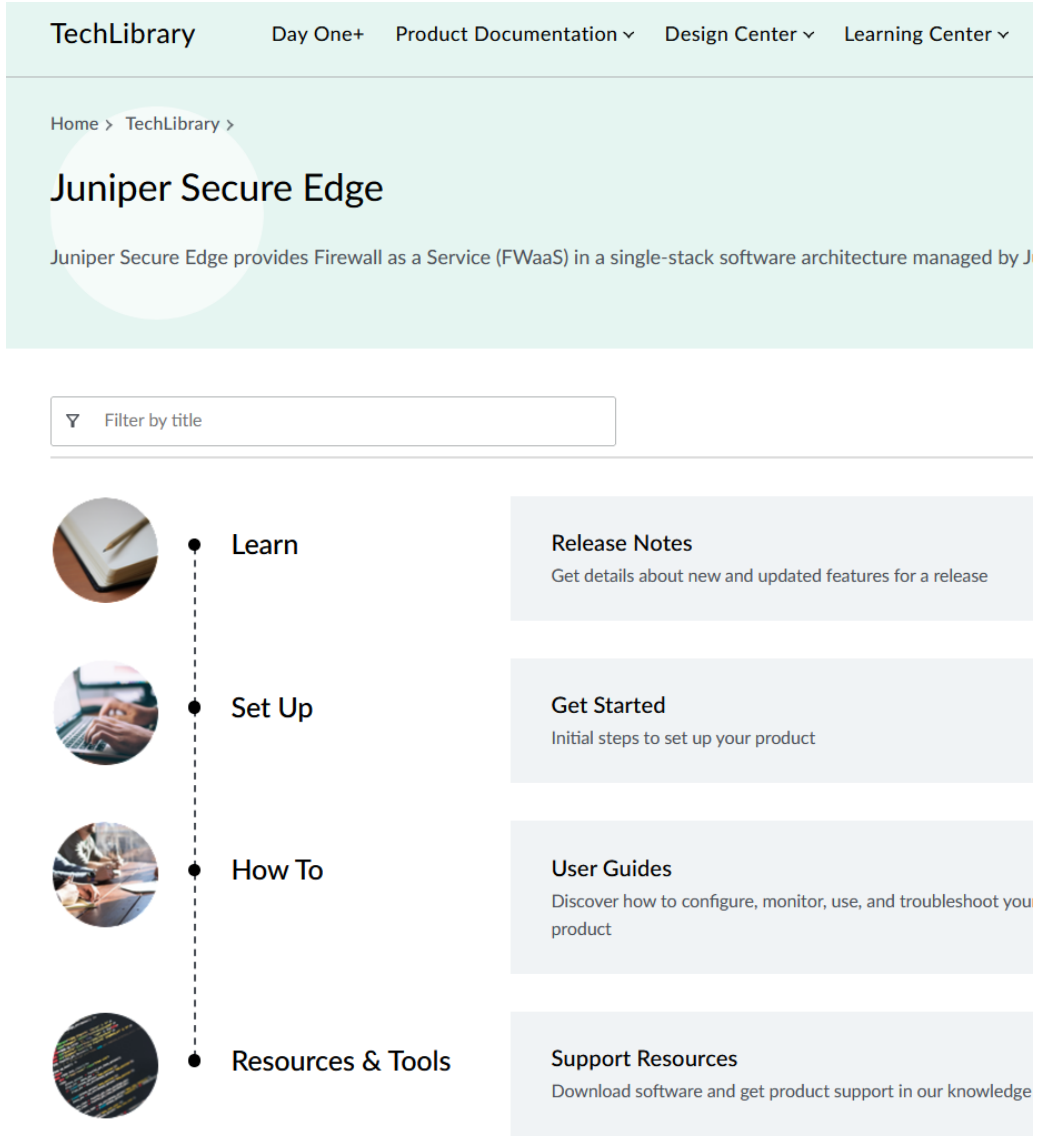
	S-JSEC-S1-Cx-x	S-JSEC-A1-Cx-x
機能	**Standard**	**Advanced**
セキュアなウェブアクセス (TLS プロキシおよびインスペクション)	X	X
URLフィルタリング	X	X
コンテンツフィルタリング	X	X
アイデンティティ／ユーザー FW	X	X
アプリケーションコントロール	X	X
脅威のフィード	X	X
アンチマルウェア	X	X
DNS フィルタリング	X	X
DNS セキュリティ		X
IPS		X
マルウェアのサンドボックス化		X
暗号化された トラフィックインサイト		X
帯域外 CASB-DLP	アドオン	アドオン

パートナー向けセキュリティ関連資料

Partner Center のセキュリティページ

https://partners.juniper.net/partnercenter/solutions/security/

Seure Edge のためのリソース



- Secure Edge のデータシート
- Juniper Secure Edge Tech Library
- Juniper Secure Edge: getting started guide
- Security Director Cloud ドキュメント
- デモ動画 Juniper Secure Edge のデモ CASB と DLP : https://www.youtube.com/watch?v=QRpNIJDZZUk
- 動画で見る Juniper Secure Edge でリモートワーカーを保護する https://www.youtube.com/watch?v=zYBTL8kKBxw

Juniper Secure Edge

お客様の成果

- いつでも、どこでも、ユーザーを保護
- 既存投資の活用
- ネットワーク全体のセキュリティを容易に確保
- クライアントからワークロードまでゼロトラストポリシーを実施
- 自分のペースでシームレスかつ安全にクラウド提供型アーキテクチャに移行することが可能

THANK YOU

JUNIPER NETWORKS | Driven by Experience™