SASE で実現する ゼロトラストでセキュアな 次世代テレワーク環境

つながるだけじゃない！
次世代型のリモートアクセスとは？

笠掛 利彰

ヴイエムウェア株式会社

ネットワーク&セキュリティ技術本部
シニア スペシャリストエンジニア

vmware®

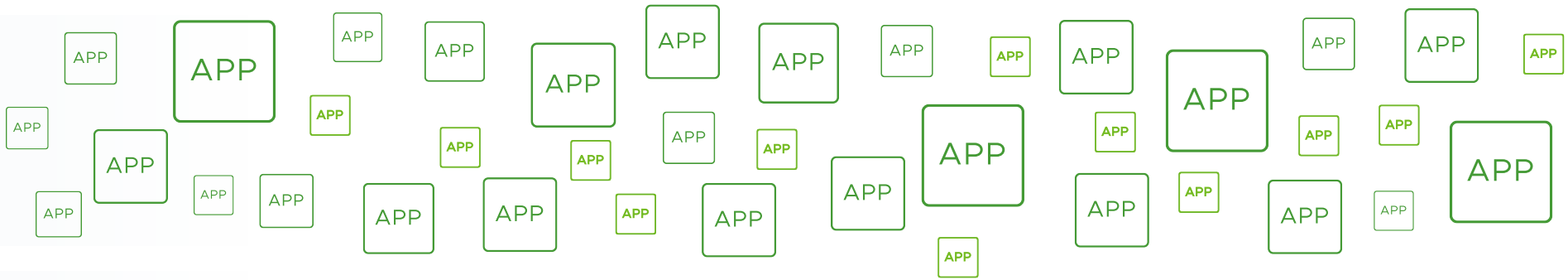
免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

企業システムの分散化が進む世界

分散化した
業務環境

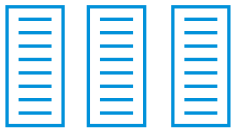
分散した
アプリケーション



分散したクラウドと
インフラストラクチャー

データセンター

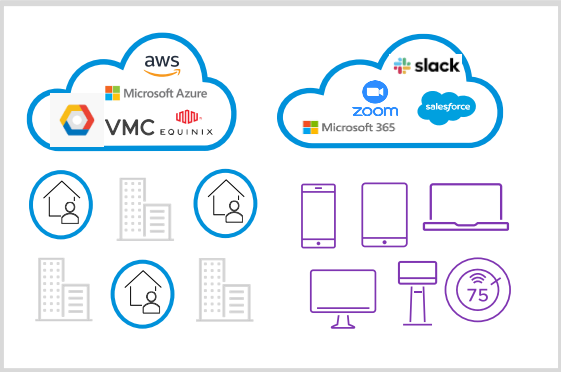
ニア エッジ



ファー エッジ

時間とともに複雑化する多様なマルチクラウド環境

分散した業務環境へのネットワーク・セキュリティ懸念

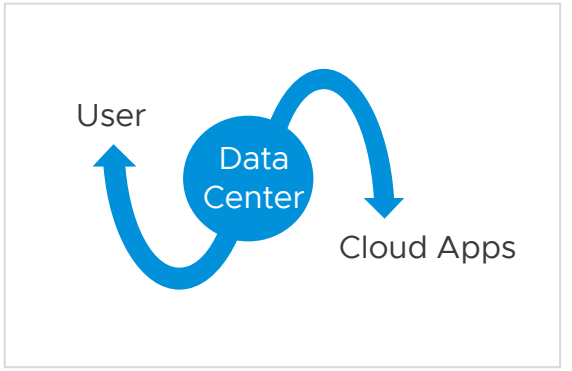


アタックサーフェイスの拡大

インターネット・アプリケーション、BYoD、テレワークによる侵害へのエントリーポイントの増加

オンプレセキュリティ機器のスケーラビリティ

堅牢性、耐障害性、可用性に優れたデザインが必要とされるが、スケールの限界にぶつかる



劣悪なユーザー体感

セキュリティを強化するためにデータセンター経由でトラフィックをルーティングする事によるユーザー体感の低下

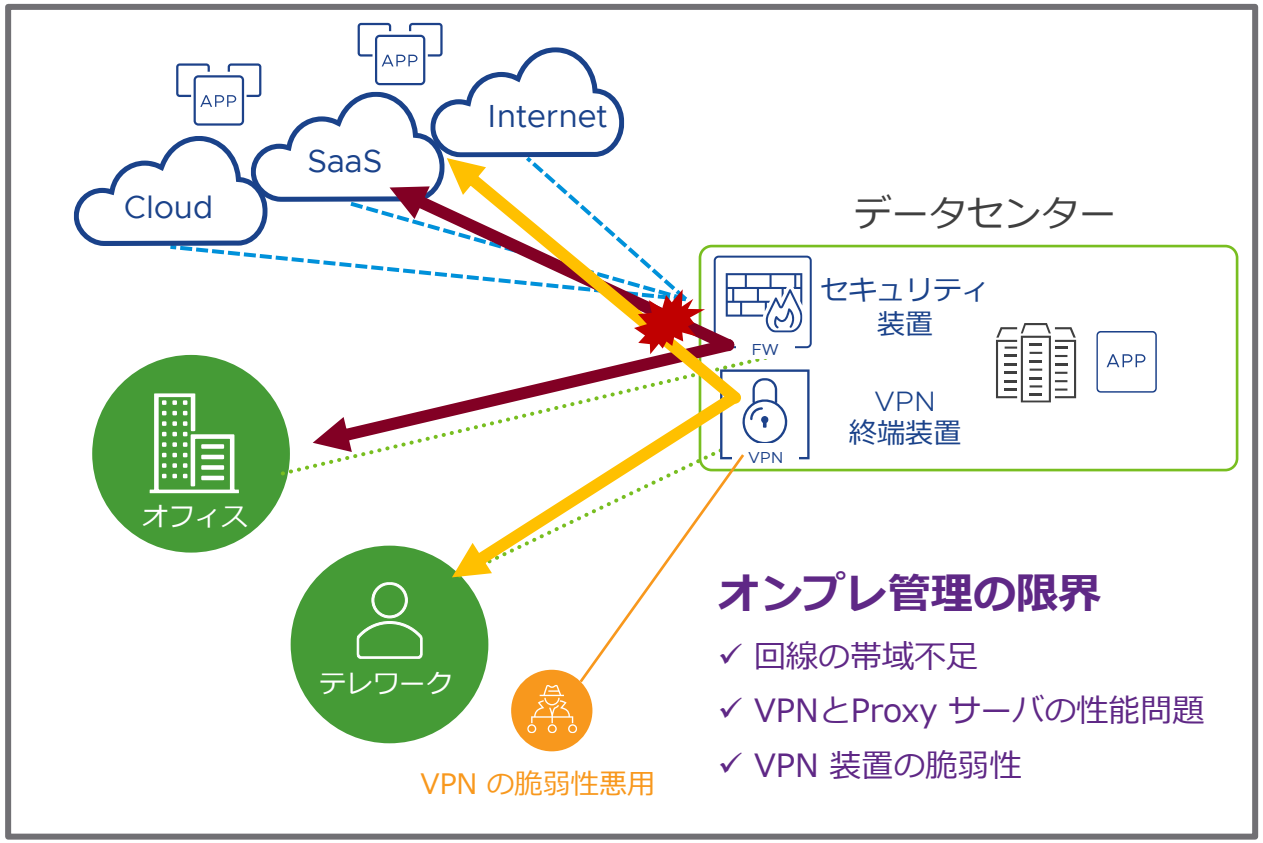
俊敏性の欠如

脅威の変化への対応の遅れ

システムのクラウド化に伴う課題

オンプレミス管理の限界と、多様化した働き方への追従の限界

従来ネットワーク設計の課題



クラウド利用に未対応なネットワーク構成

- DC 経由のバックホール接続が必要
- 企業 WAN 閉域網や DC での回線帯域不足

データセンターにおける各種装置スケール

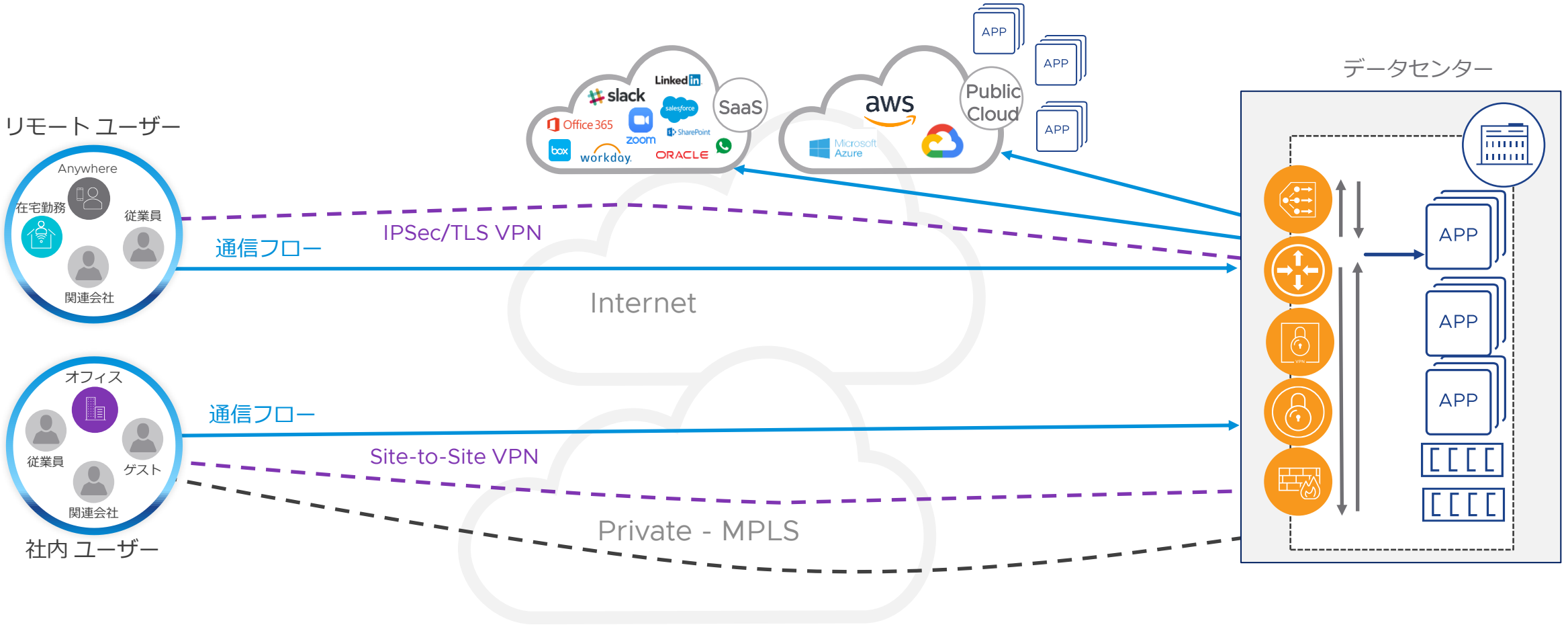
- Proxy/セキュリティ装置の性能不足
- VPN 装置の性能・拡張性の欠如

オンプレ環境のセキュリティ対策

- オンプレ VPN 装置の脆弱性による脅威
- 多様なデバイスの管理・運用の継続

従来のアプローチ：データセンターへのバックホール接続

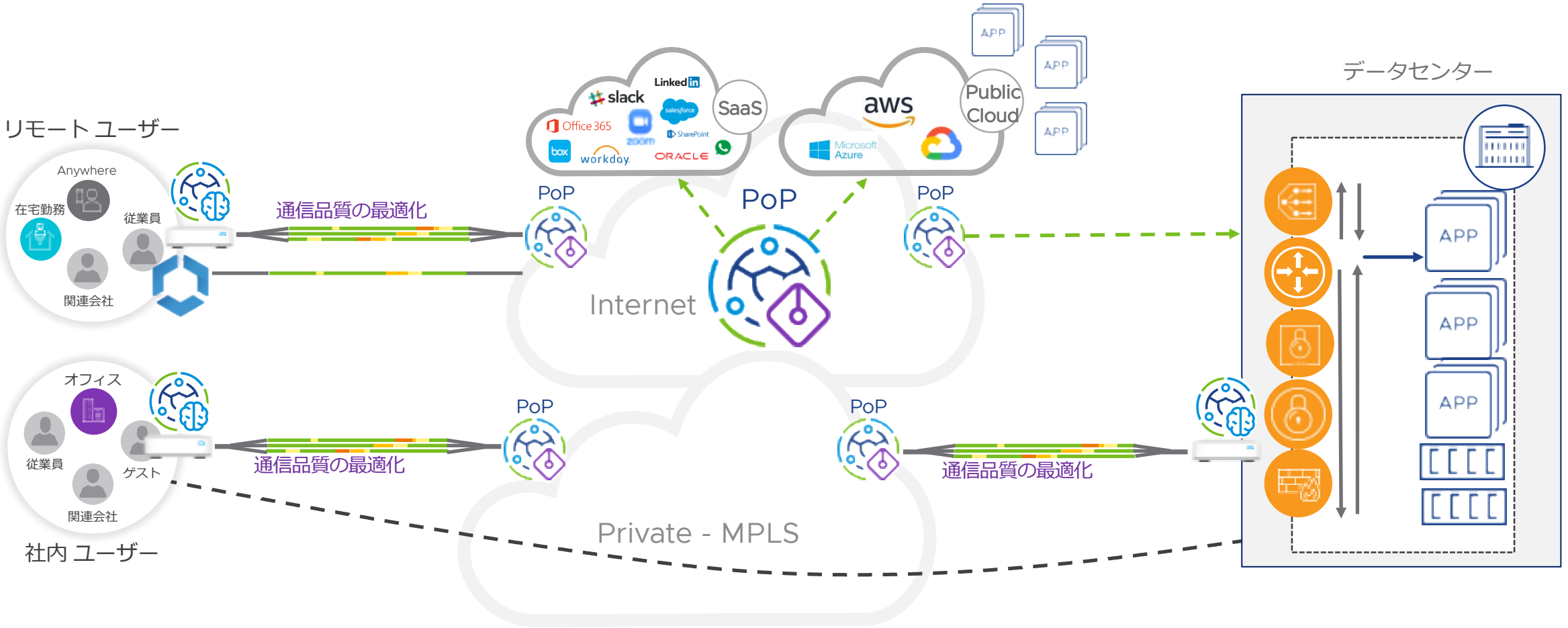
DC 中心のネットワーク・セキュリティ構成はクラウド時代には複雑で不十分



高遅延 • 高オペレーションコスト • 複雑性 • 俊敏性の欠如

マルチクラウドを実現する Secure Access Service Edge アーキテクチャ

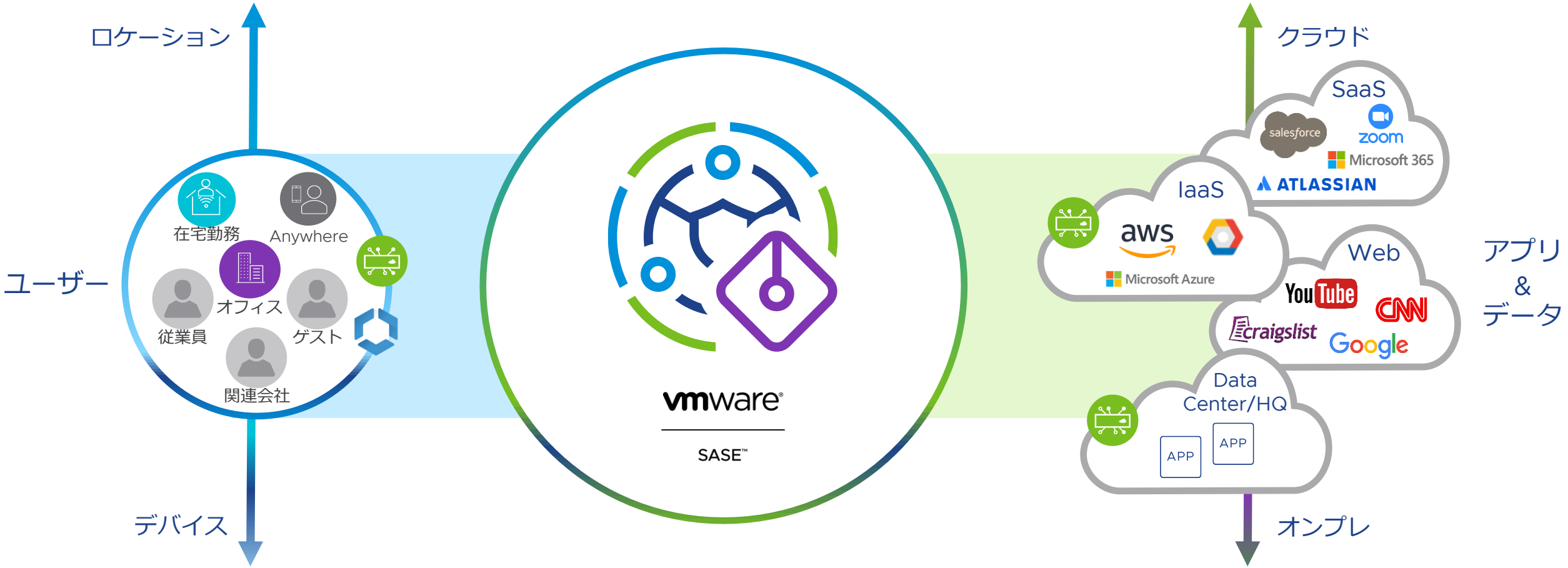
ユーザー中心のアプローチでアプリのモダナイゼーションを加速



アプリパフォーマンスの改善 • Opex の低減 • クラウド対応なスケール • 容易なオペレーション

VMware SASE

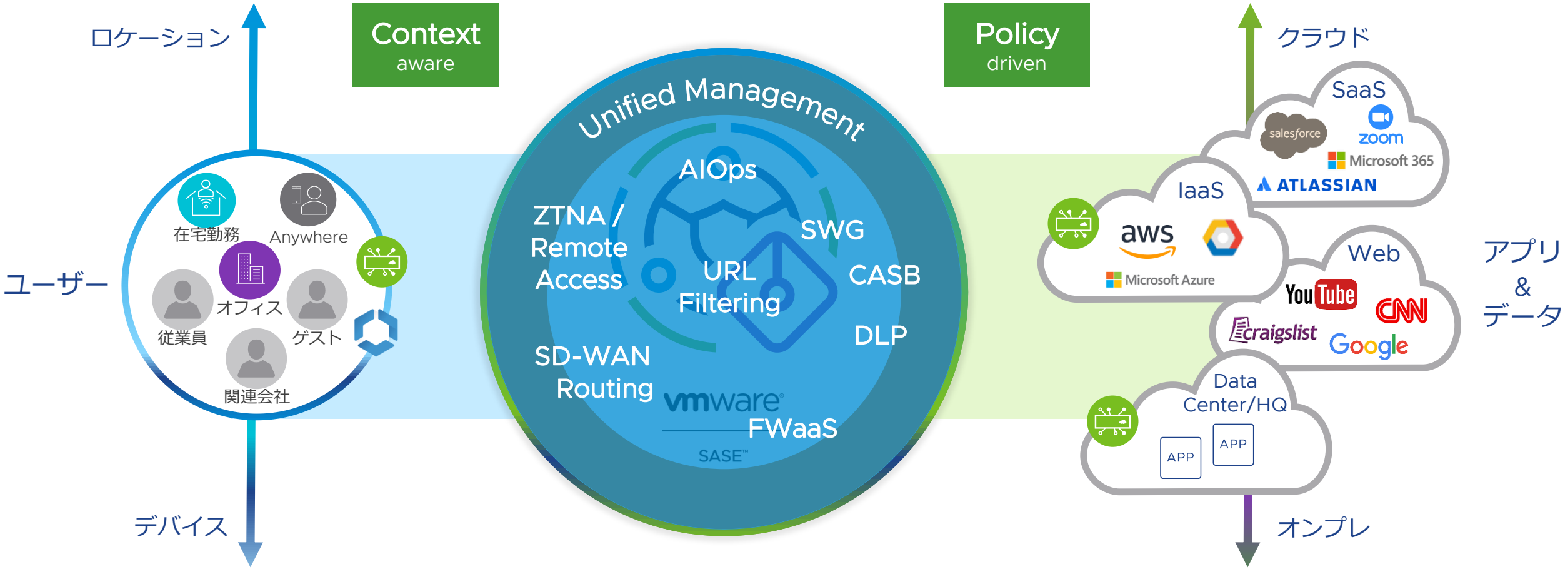
分散した業務環境におけるネットワークとセキュリティ要件に対応する統一的なアプローチ



ネットワーク・セキュリティ・分析・エッジコンピューティングなど複数のクラウドサービスを連携

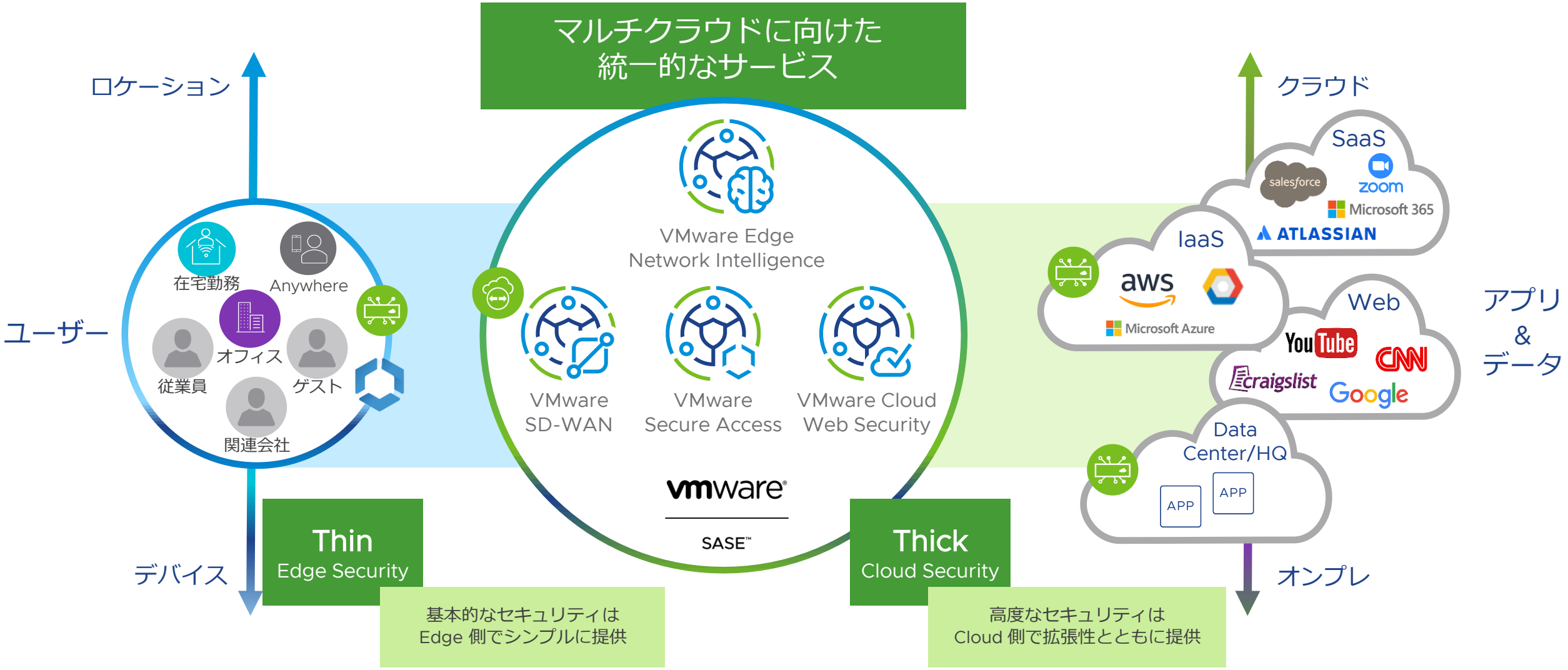
VMware SASE で包括的に提供される機能

分散した業務環境におけるネットワークとセキュリティ要件に対応



VMware SASE が管理と拡張性をサービスとして提供

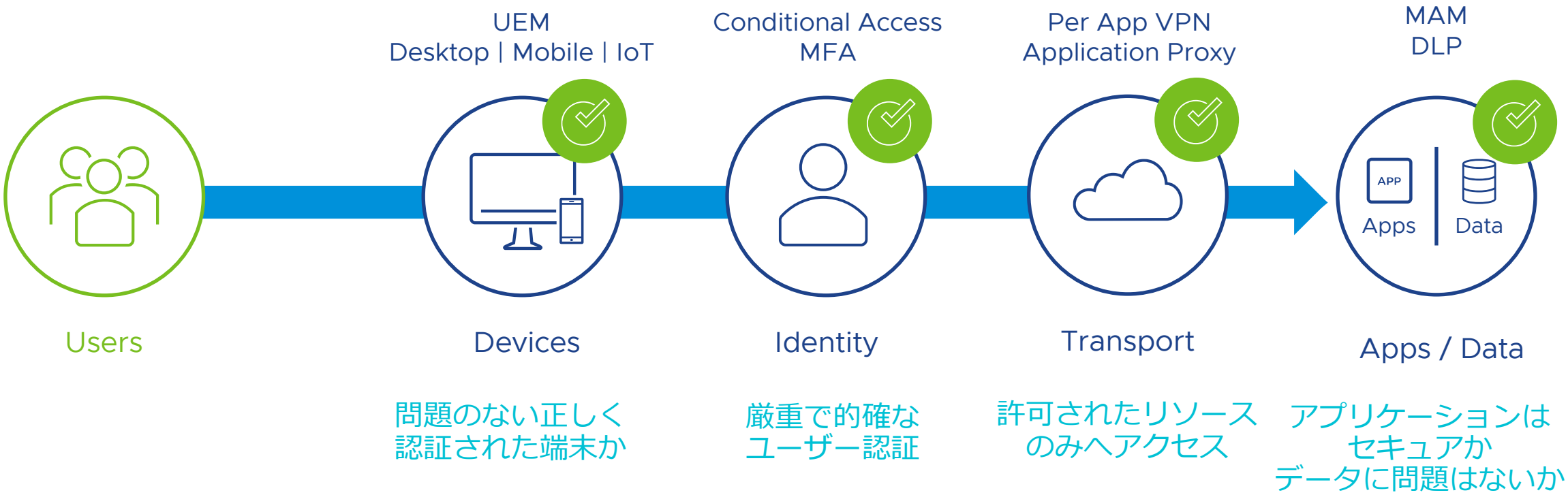
Pay as you Grow モデルのネットワークとセキュリティ



クラウドで実現する ZTNA ソリューション

VMware Secure Access

なぜ Zero Trust Network Access が必要なのか



テレワーク・モバイルユーザーのための VMware Secure Access

レガシー VPN vs. Zero Trust Network Access (ZTNA)

オンプレ DC で VPN 終端

ネットワーク単位での
アクセスポリシー適用

すべてのアプリへのアクセス

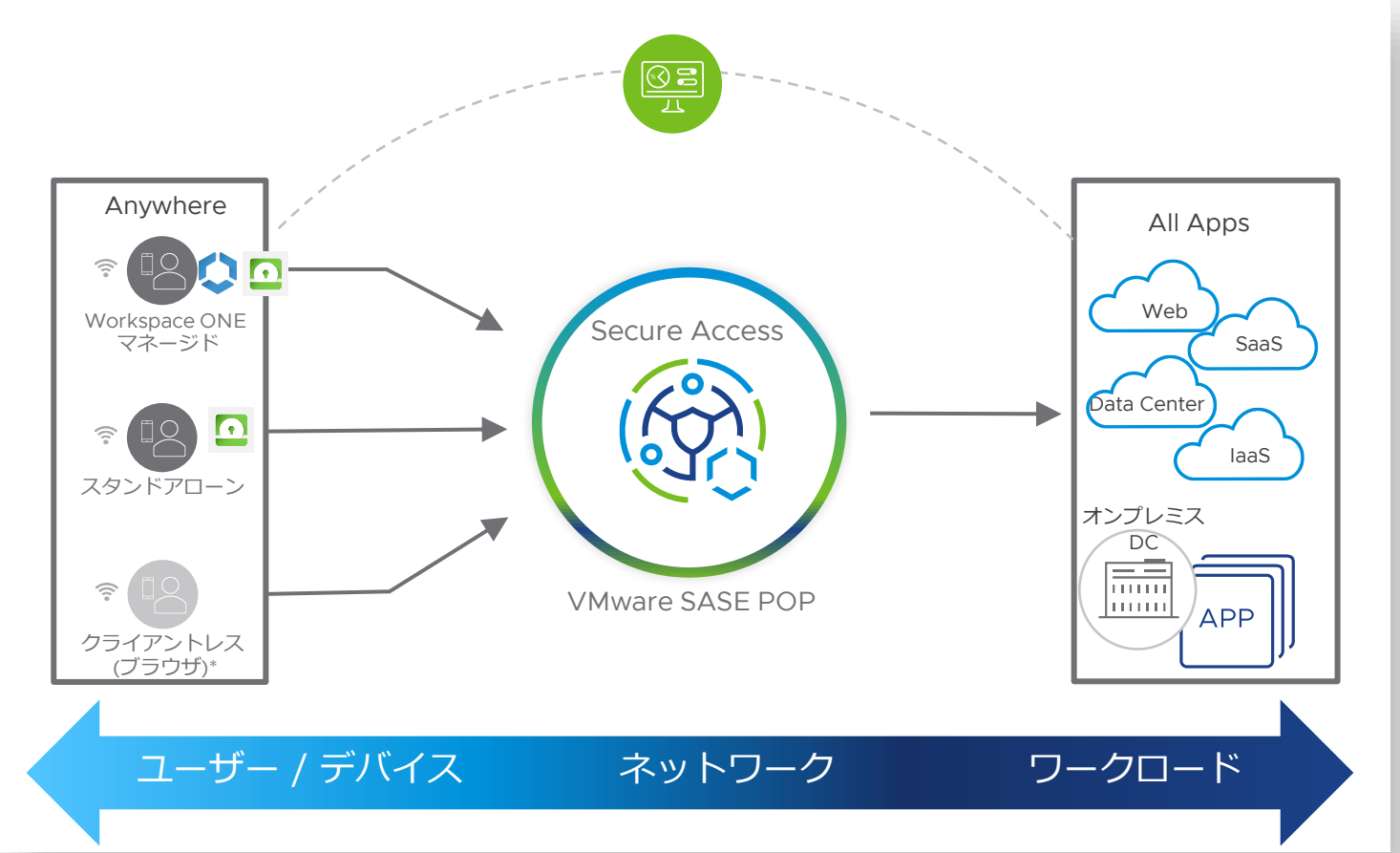
クラウド ネイティブ:
クラウドでの VPN 終端によりスケールとクラウドアプリの最適な体感を提供

ユーザー単位の制御：
ユーザー情報、端末状態、ユーザーの振る舞いに基づくポリシーの適用

詳細なアプリケーションアクセスポリシー：
ユーザーの要件に応じたアプリアクセスの提供

VMware Secure Access

セキュリティコンテキストに応じた Zero Trust Network Access で統一的なリモートアクセスを提供



1

One Fabric, One Policy

VMware SD-WAN と SASE と VMware Secure Access を組み合わせることで既存 VPN ソリューションへの課題解決と、統一的な管理を提供

2

Zero Trust Access

ユーザーID、デバイスタイプ、OS、パッチ適応状況、脱獄・Root 奪取の状況、等によるリスクプロファイルをふまえ、継続的な認証認可管理と状況に応じた動的なアクセスを提供

3

すべてのワークロードに

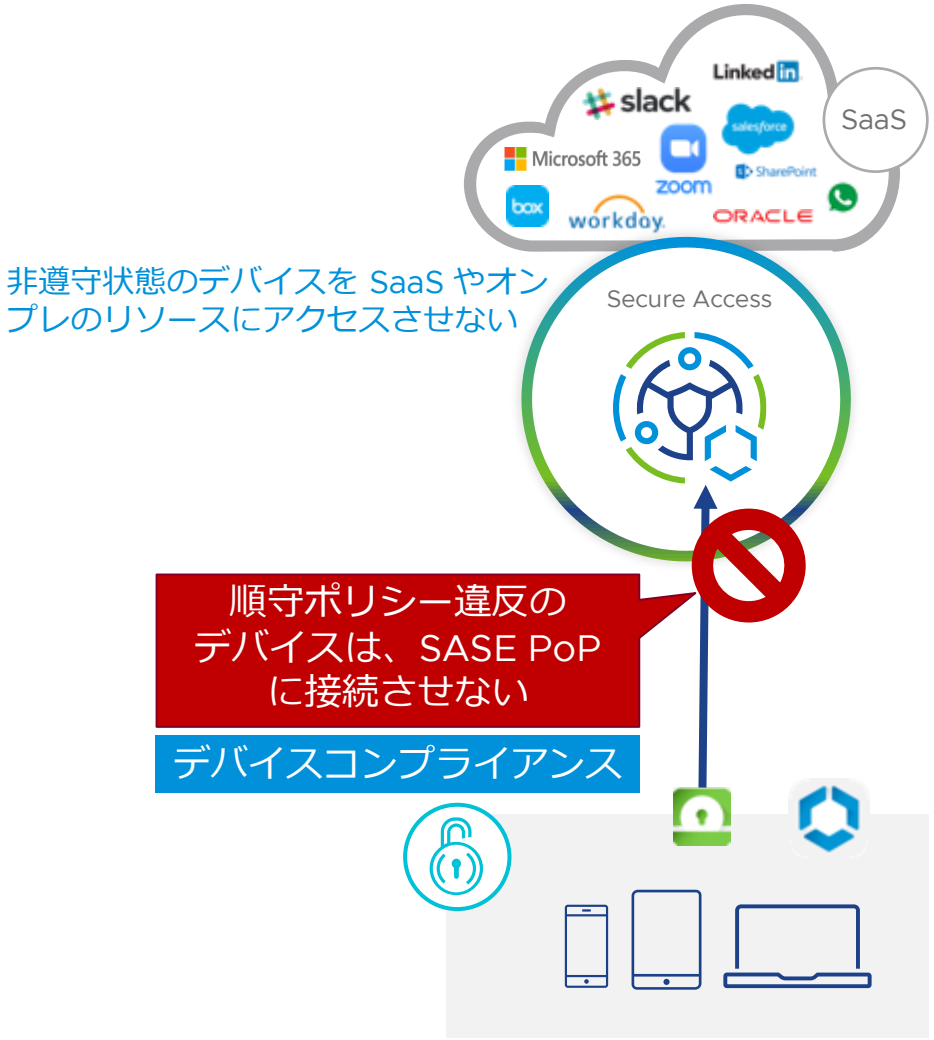
データセンター、SaaS、インターネットへのアクセスをユーザー、デバイス、エンタープライズデータに対する保護と共に提供

多量で様々な端末種別のデバイス展開に対しても VMware Workspace ONE® が容易で統一的な管理を実現

* ロードマップ

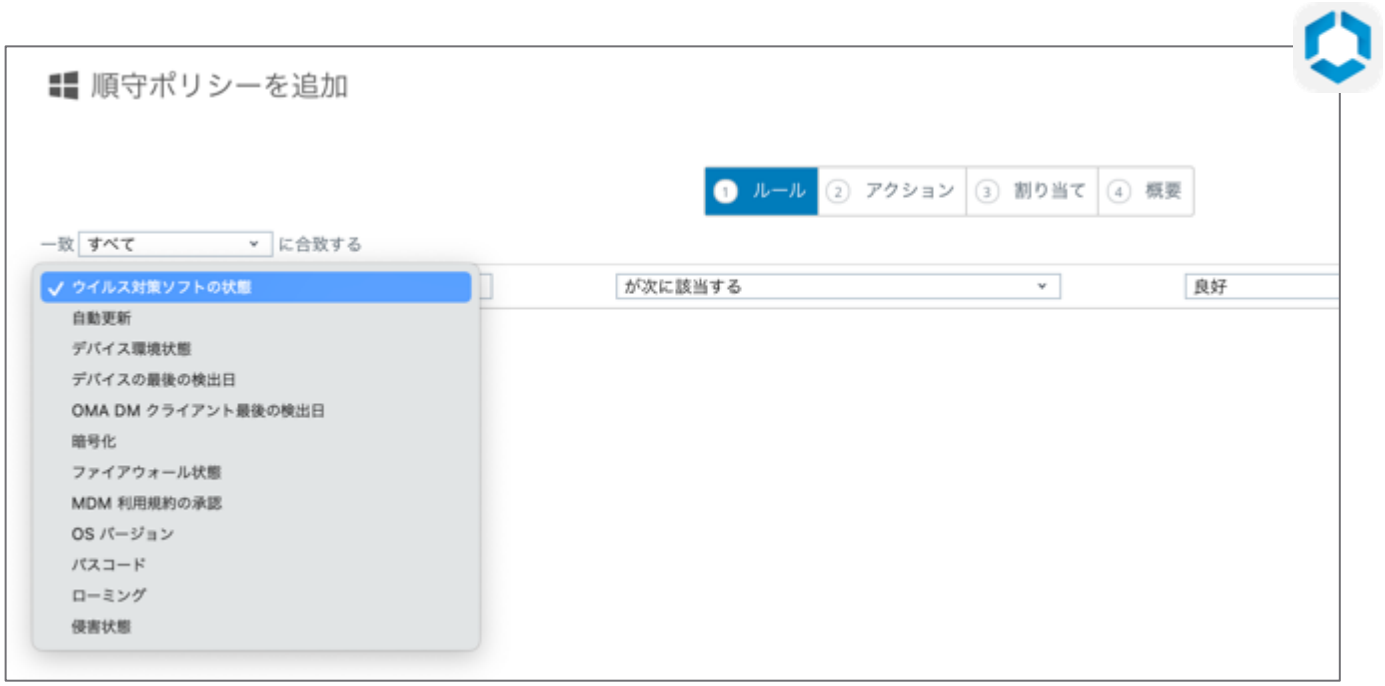
デバイスコンプライアンスに基づくアクセス制御

VMware Workspace ONE® によるデバイス、ユーザ確認

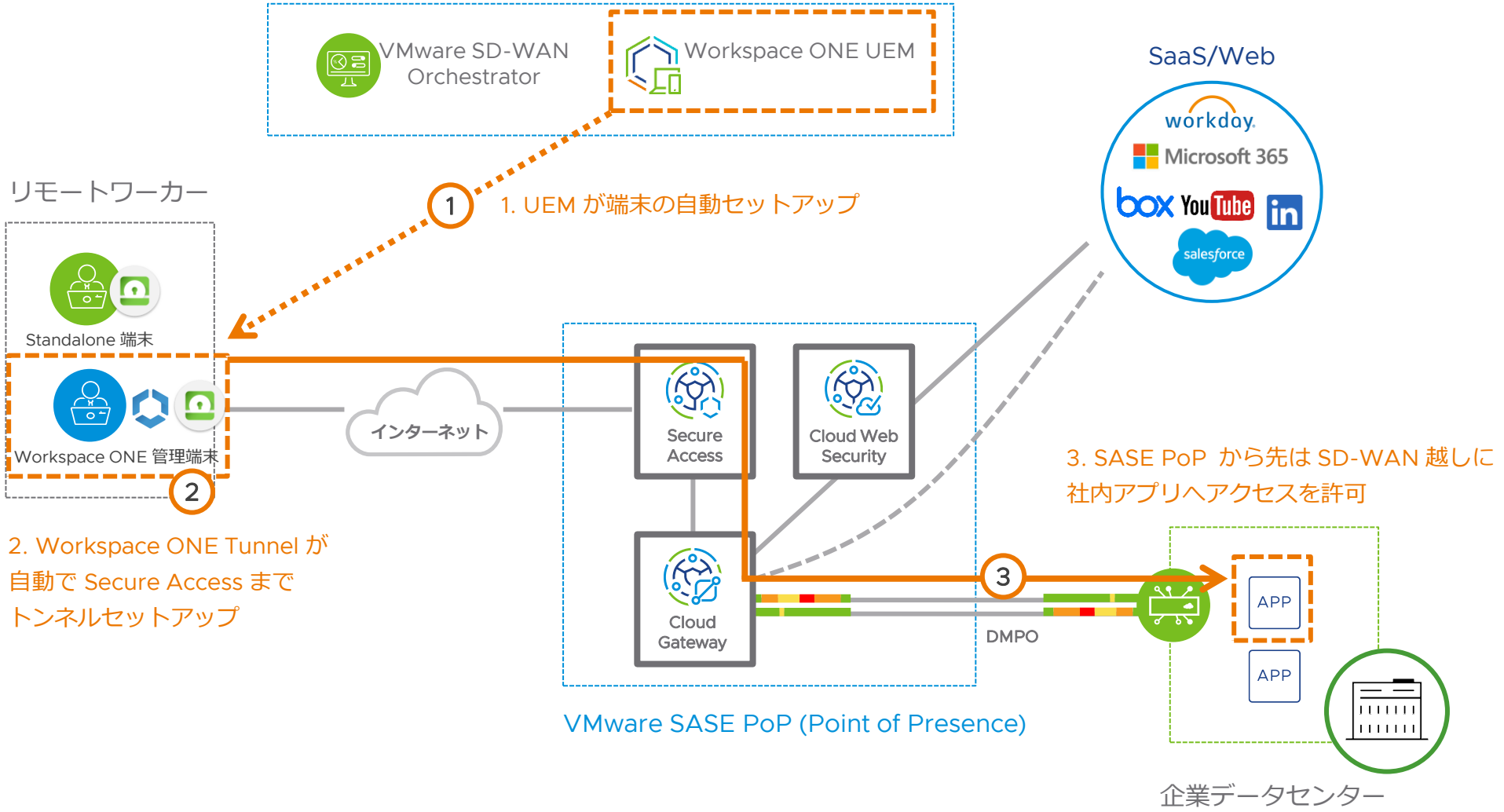


デバイスの多層チェックによるセキュアな接続を実現

- Workspace ONE で管理されたデバイス
- 認証されたユーザーのみ
- 指定アプリからのみ
- 指定 URL のみ
- デバイスコンプライアンス



デモ: Secure Access による社内アプリへの接続



次世代テレワーク環境を提供する WAN ソリューション

VMware SD-WAN

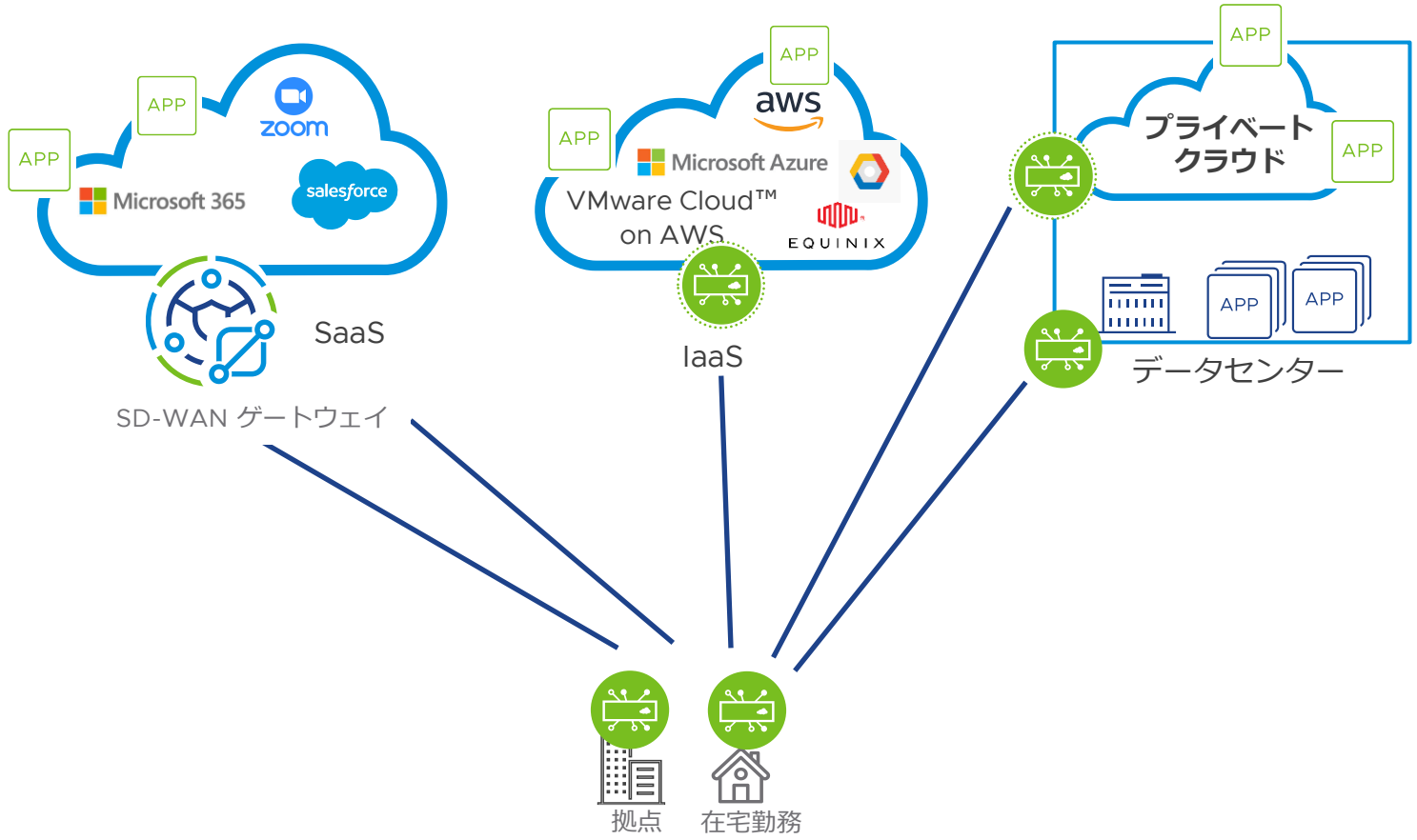
VMware SD-WAN

エンタープライズの ハイブリッド/マルチクラウド戦略を最適なパフォーマンスと共にサポート

SaaS アプリへの容易な接続

クラウド・データセンターへの
接続最適化を自動化とともに提供

オンプレミスのエンタープライ
ズアプリケーションへの接続

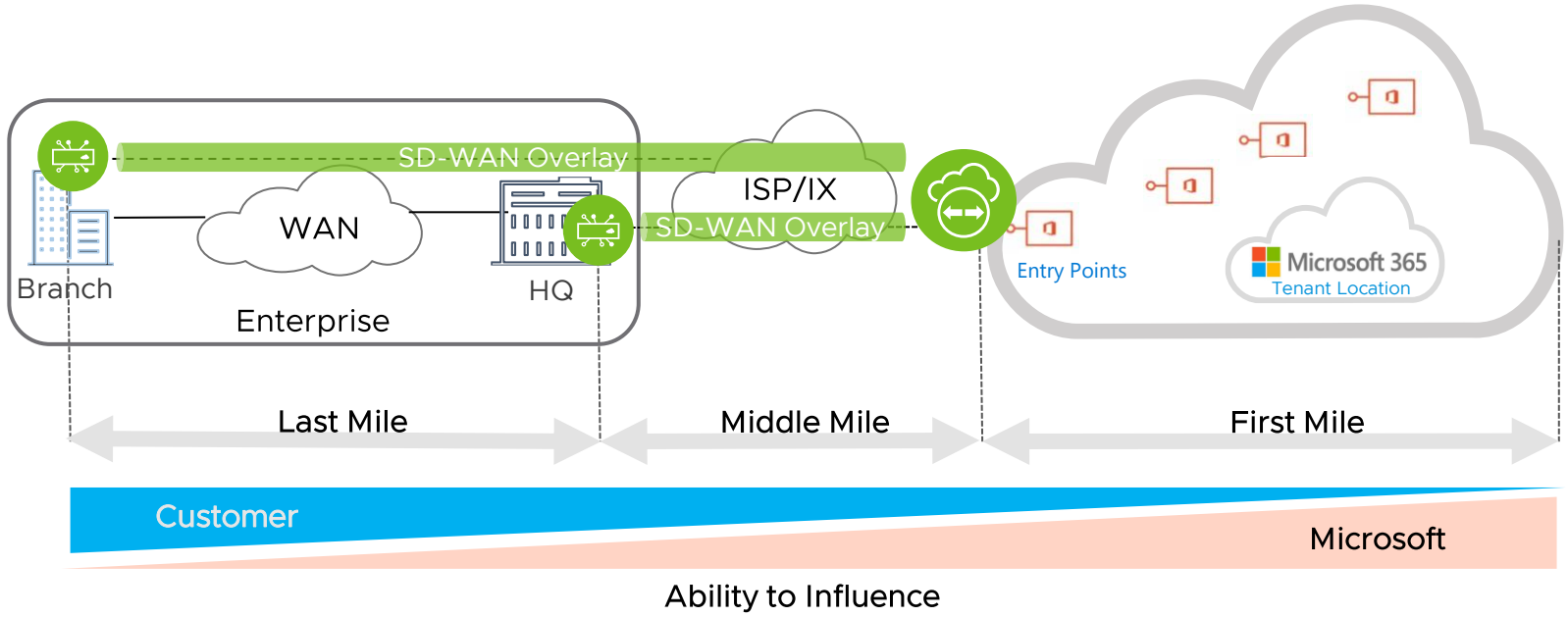


あらゆるクラウドへの最適なパフォーマンスでの接続を容易に制御

なぜクラウドサービス接続に Network as a Service が必要なのか

ベストな SaaS アプリケーションパフォーマンスを得るためのボトルネック

- SaaS アプリ利用体感にとってアクセスネットワークは非常に重要
  例：Microsoft 社は First Mile の多くの最適化を実施している
- Last Mile, Middle Mile についてはユーザーの選択するアクセス方法に依存した接続クオリティとなる
  例：クラウドベンダー専用線ソリューション（高品質、高価） >> SD-WAN >> ブロードバンド接続（Best Effort、安価）



Dynamic Multi-Path Optimization による回線品質補正

インターネット越しでもアプリケーションパフォーマンスを保障

継続的にリンクをモニタリング

- インターネット回線品質の見える化
- 自動化と最適化を実現

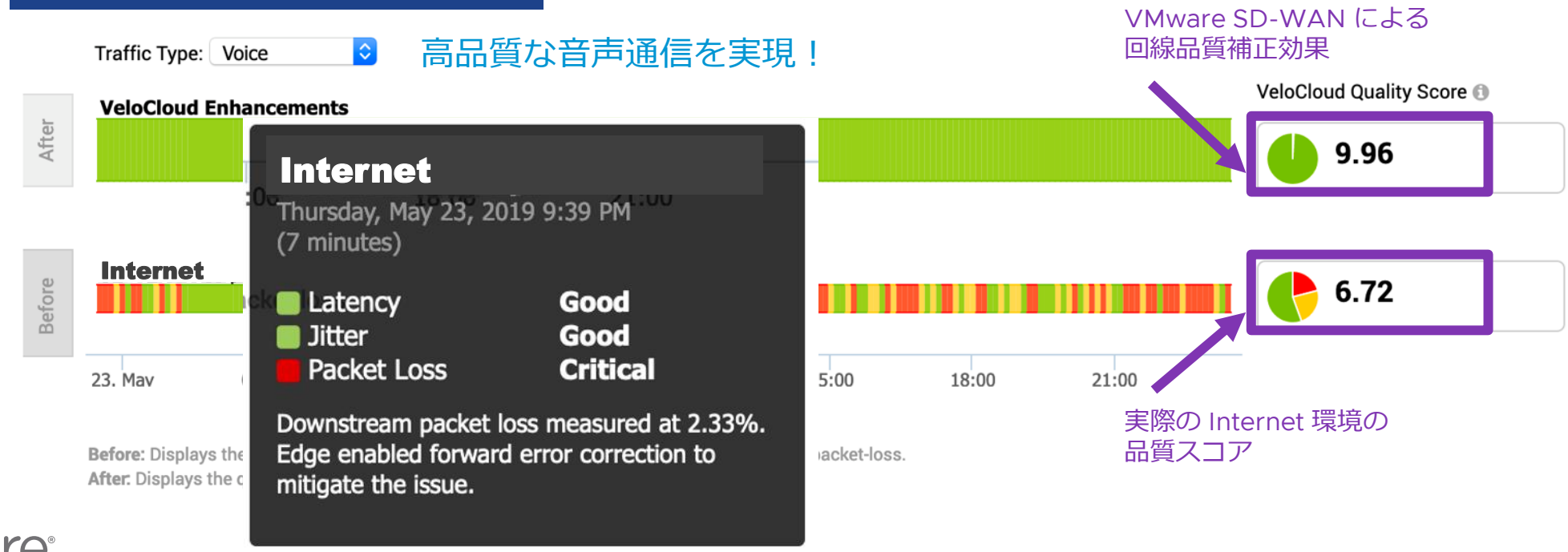
動的なパケット単位での制御

- セッション切断無しでサブセカンドの切り替り
- 一つのフローでも複数リンク帯域を統合し転送

オンデマンド品質改善

- 品質劣化を保護
- 1 回線での利用可能な帯域を最大化

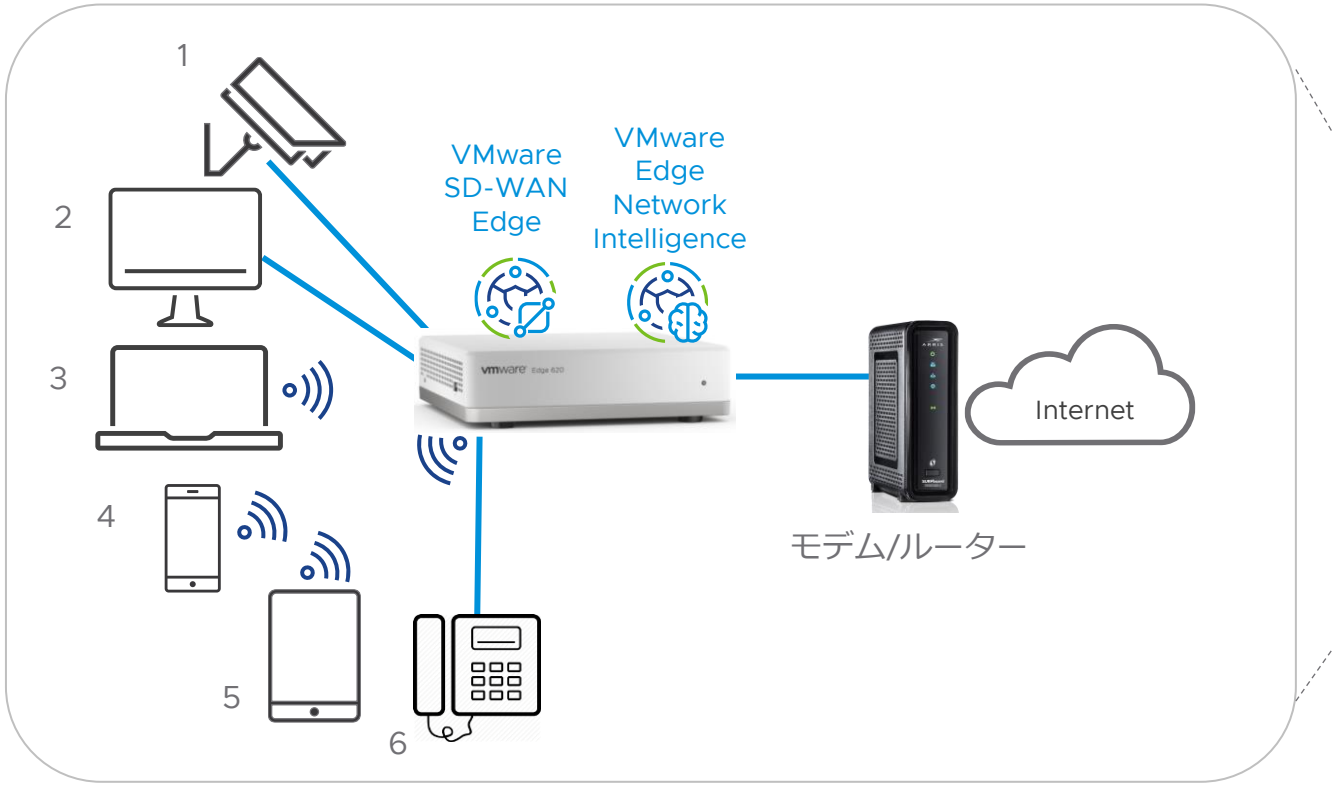
東京都千代田区のインターネット環境の例



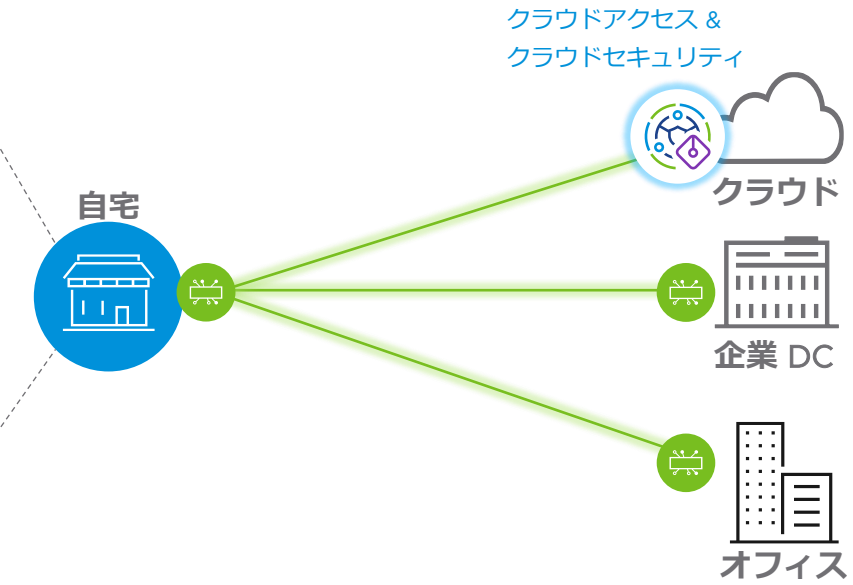
在宅業務環境への SD-WAN Edge 導入とユースケース

低価格デバイス＆WFH ライセンス – ホームルーターの置き換え可能

- ✓ ゼロタッチ導入 & IT部門よりクラウドからの管理 が可能
- ✓ 自宅 WAN 回線をソフトウェアによりビジネスクオリティへ拡張
- ✓ 同時 6 デバイス接続/ 1 ビジネスユーザー、最大 1 Gbps をサポート(1
- ✓ 私用・家族利用のデバイスも論理的に分離可能(2



企業ネットワーク や **クラウド** へ
セキュアで最適化された接続を提供！



- ❖ SD-WAN セキュアトンネル自動構成
- ❖ WAN 回線品質の最適化
- ❖ WAN 環境の見える化
- ❖ ユーザーアプリ体感の可視化とトラシューアシスト

1) 同時 3 デバイス接続/ 1 ビジネスユーザー、スループット最大 350 Mbpsまでのサブスクリプションもございます。
2) 接続デバイス単位で企業ネットワークなどへのアクセス可否を制御可能です。

ビデオ会議における VMware SD-WAN の効果

2 % パケットロスが発生している WAN リンク環境での検証

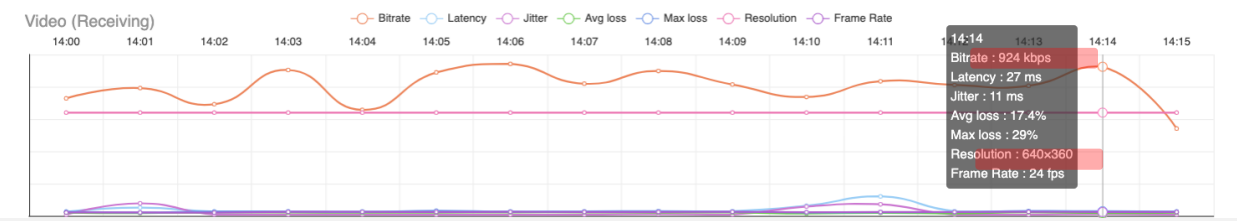
VMware SD-WAN なし

VMware SD-WAN あり

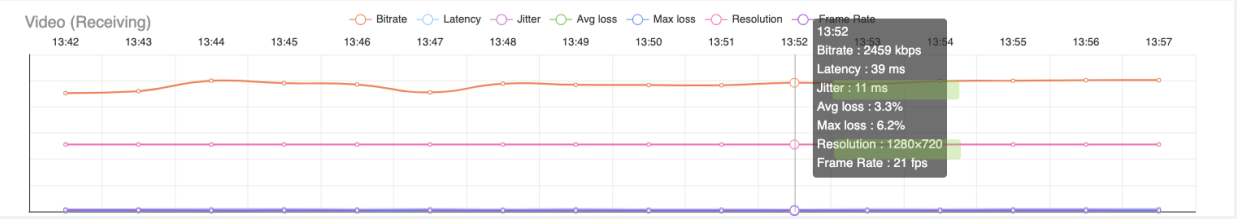
ビジネスクリティカルなアプリパフォーマンスを最適化

Zoom と Microsoft 365 の品質改善テスト結果

Non-SD-WAN Client with 20% Packet Loss on WAN



SD-WAN Client with 20% Packet Loss on WAN



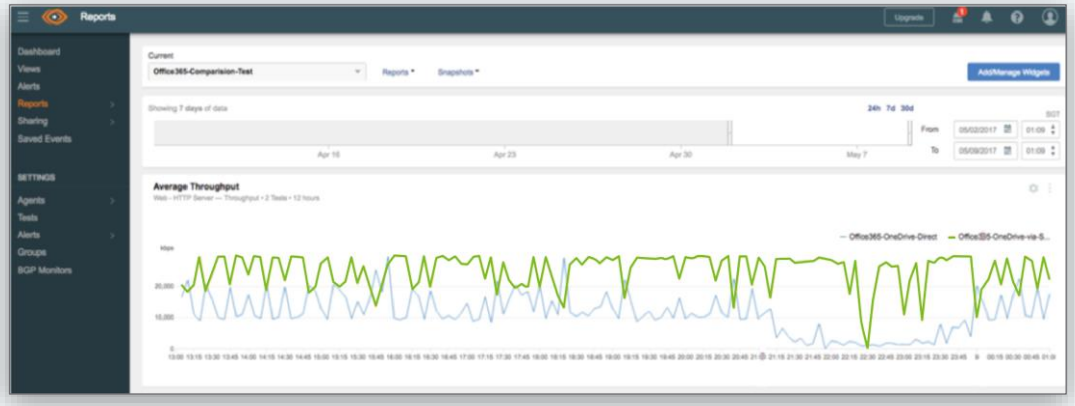
- 定常的な回線モニタリング、動的なパス制御、品質補正機能が用いられ、安定した接続を提供
- 360p HD video となる通信状況で、SD-WAN 適用により 720p HD video クオリティを実現
- 最寄りの Gateway を経由し、最寄りの Zoom テナントへアクセス
- アプリ名で通信を識別し、ワンクリックで Zoom の要件を満たす通信制御が可能

結果

VMware SD-WAN の使用で 10倍 高い平均スループットを実現

検証状況

Microsoft 365 を 1本の WAN リンク越し (ブラウンアウト状況) にタイの拠点からシンガポールの VMware SD-WAN ゲートウェイ経由で通信



（Zoom ホワイトペーパー）https://vmware-juku.jp/resource/form_224/

VMware SASE が実現する クラウド提供のセキュリティ

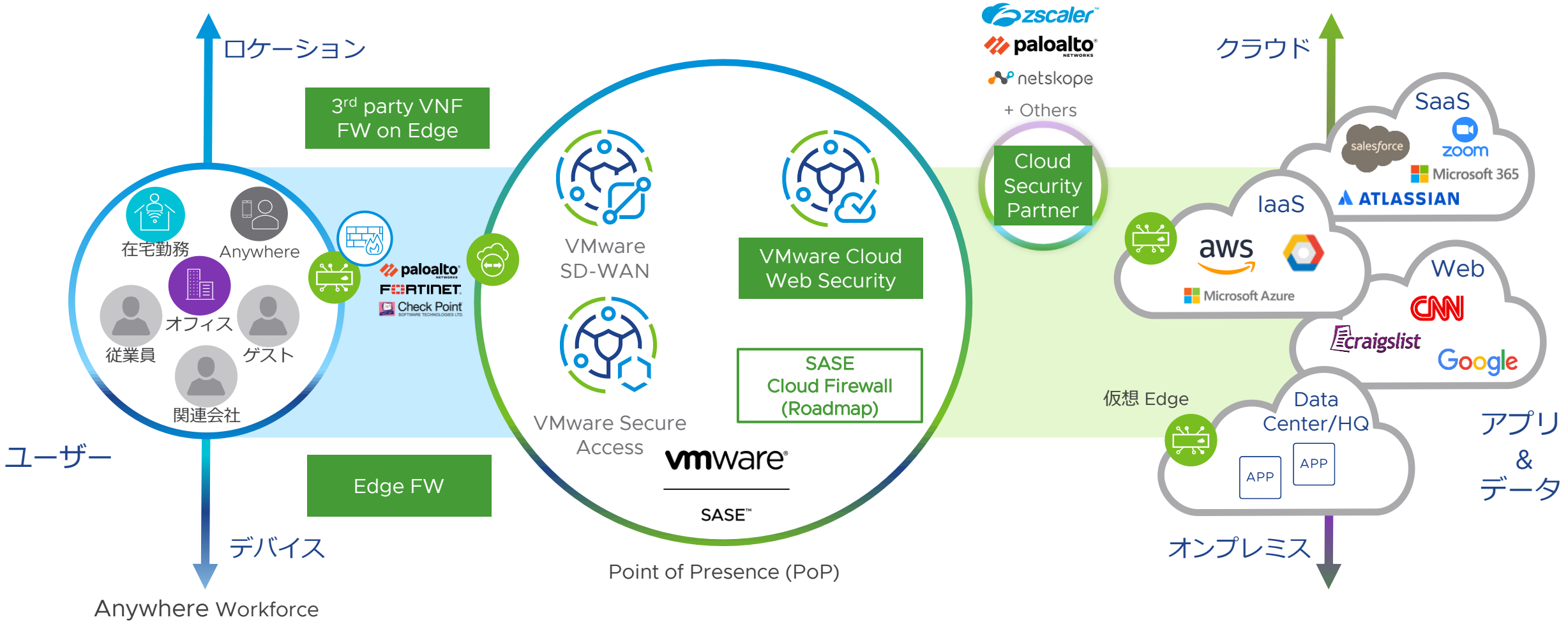
VMware Cloud Web Security &

SASE Cloud Firewall &

Cloud Security Partner

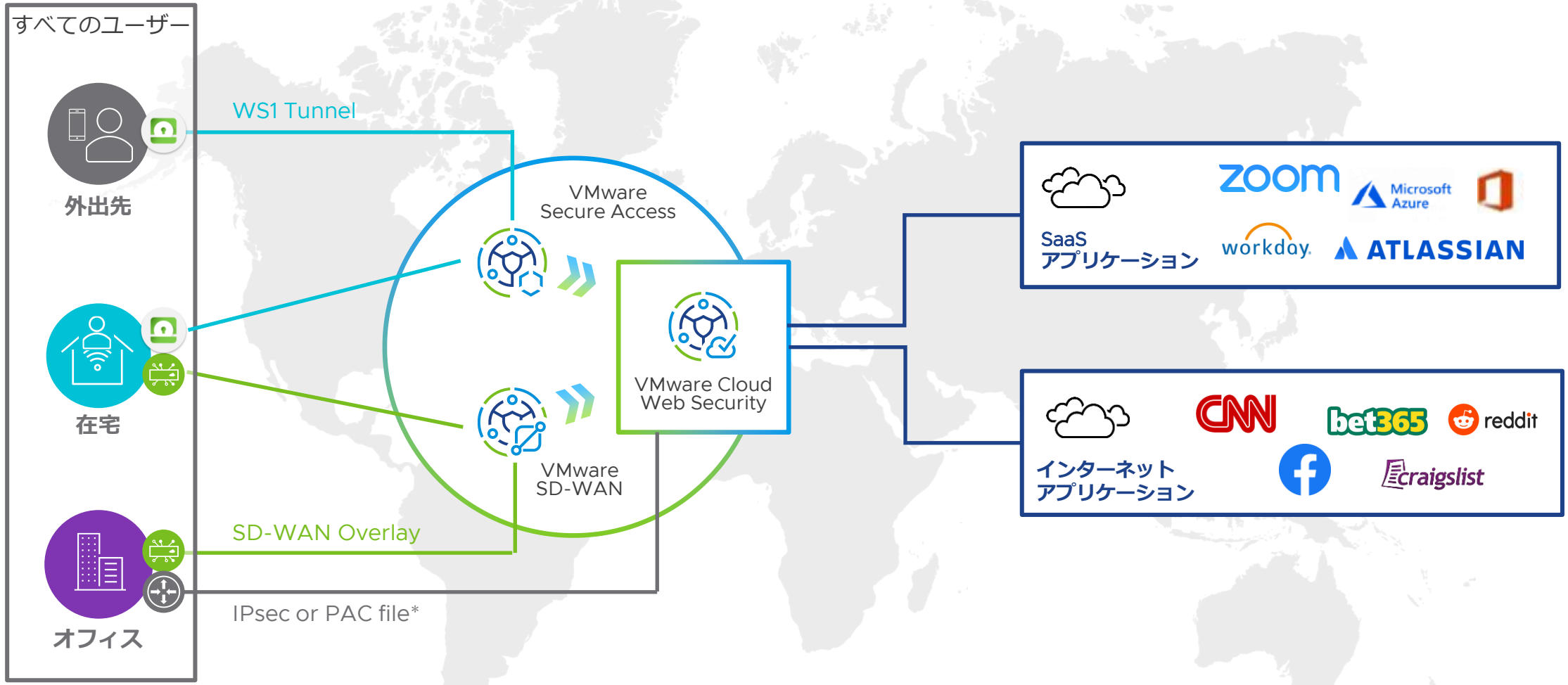
VMware SASE が提供する様々なセキュリティサービス

分散業務環境のための包括的なセキュリティとパフォーマンス



あらゆる場所からのアクセスに適用可能な Cloud Web Security

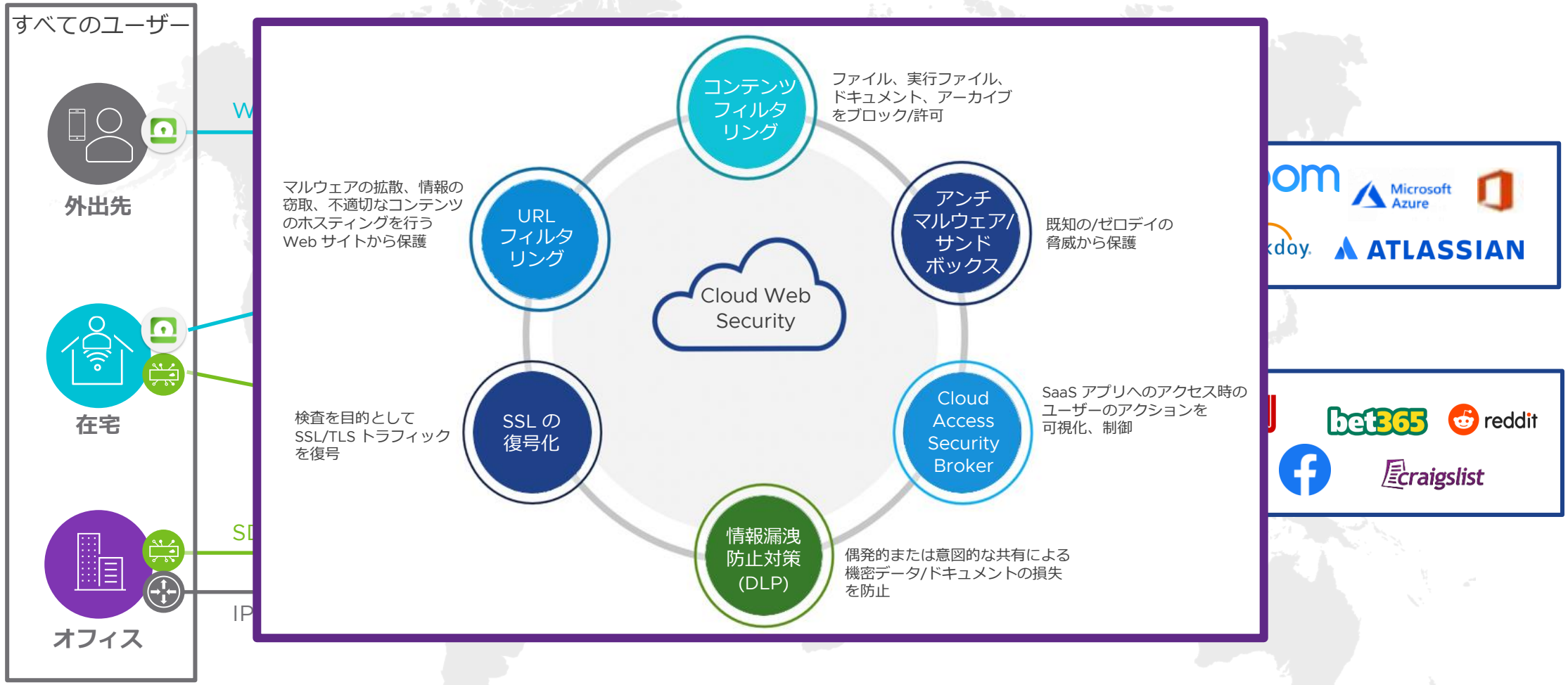
SaaS やインターネット・アプリケーションへのセキュリティ、可視性、制御、コンプライアンス



*Roadmap (H2CY22)

あらゆる場所からのアクセスに適用可能な Cloud Web Security

SaaS やインターネット・アプリケーションへのセキュリティ、可視性、制御、コンプライアンス

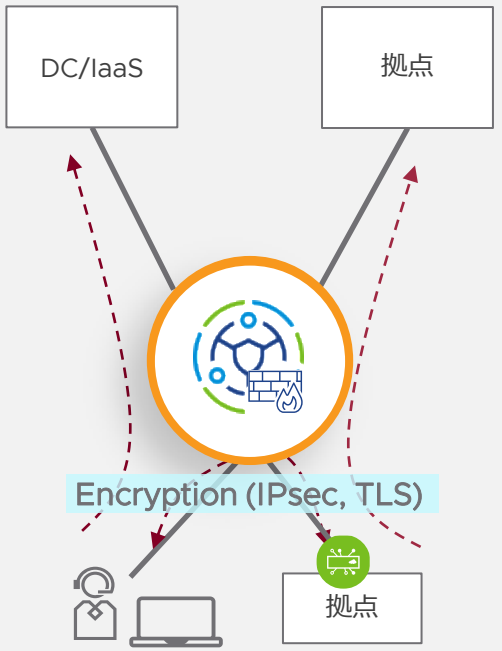


*Roadmap (H2CY22)

SASE Cloud Firewall – 機能とユースケース

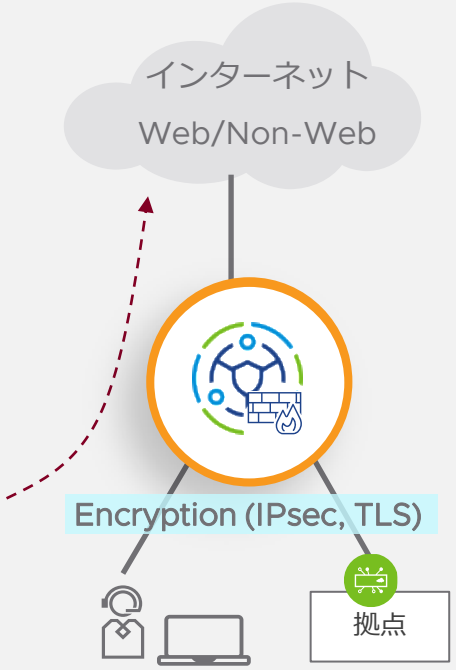
拠点とリモートユーザーのセキュリティをさらに拡張するクラウドサービス

プライベートアクセス



リモートワーカー / 拠点

インターネットアクセス



リモートワーカー / 拠点

概要

- Next Gen Firewall (NGFW) をサービスとして提供
- VCO による一元管理
- 他 SASE サービスとの同時利用 (SD-WAN, SA, CWS)

セキュリティ サービス

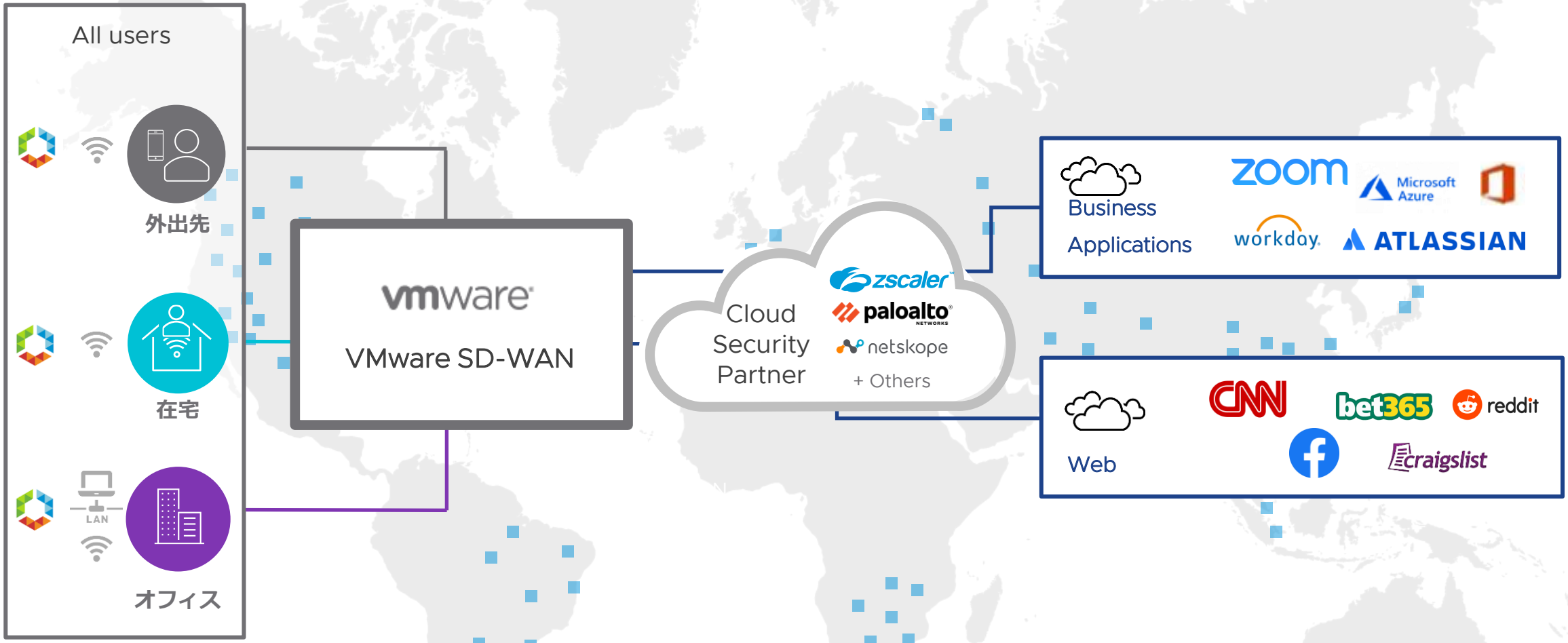
- L4-L7 ファイアウォール
- SSL/TLS 復号化
- IDS/IPS
- URL フィルタリング
- アンチマルウェア
- サンドボックス
- アプリ ID
- ユーザー ID

対象通信種別

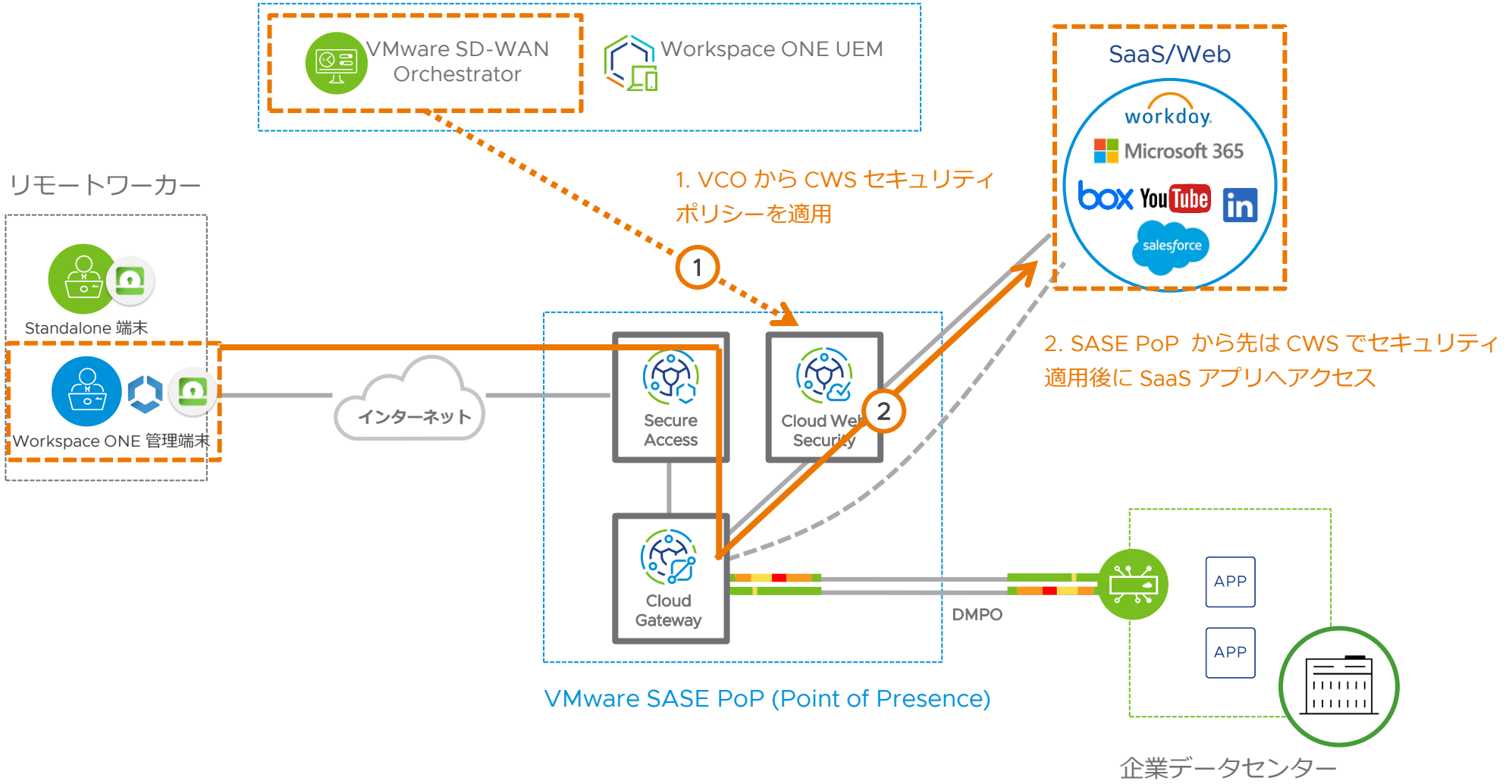
- 企業内部（プライベート）通信 (拠点/DC/IaaS)
- インターネット向け 標準ポート以外の Web 通信
- インターネット向け Web 以外の通信 (全ポート)

VMware SD-WAN + Cloud Security Partner 連携

SD-WAN と Cloud Security でユーザーとその通信をすべてのレイヤーで保護



デモ: Secure Access 端末の Cloud Web Security による保護



Anywhere Workspace ソリューション

多様な
従業員体験の管理

ワークスペースの
自動化

分散化された
エッジの保護

VMware Carbon Black

クラウドネイティブ |
エンドポイントの保護

VMware Workspace ONE

統合エンドポイント管理および
仮想アプリ/デスクトップの提供

VMware SASE

ゼロトラスト セキュリティと
ネットワーク パフォーマンスの管理

IT、ネットワーク、セキュリティを網羅する統合テクノロジー

まとめ：VMware SASE が選ばれるポイント

シンプルに解決する、新時代のクラウドスケールで安全な業務環境を実現

VMware Secure Access

リモートアクセス VPN をクラウド提供

さらに
従来の VPN に代わる
「ゼロトラストネットワークアクセス」
（ZTNA）を提供

WS1 Managed client

リモートワーカー

SaaS/IaaS/Web

workday.
Microsoft 365
aws
salesforce

クラウド
業務系通信

Cloud Security Partner

zscaler
paloalto NETWORKS
netskope

Network Security

リージョン毎の SASE POP 上で提供される
Web のみならず様々な通信パターンに適用可能で豊富な
クラウド・セキュリティ機能
また
ユーザーの利用シーンに合わせて柔軟に選択可能な
セキュリティ パートナー連携
によるマルチベンダー対応

VMware SASE

必要機能を包括的に提供

SASE実現に必要な機能を全て提供し、
ネットワークとセキュリティインフラを一括してサポート
さらにこれらの全ての機能を
一元的に管理運用することが可能に

単一のクラウドサービス

柔軟性、俊敏性、拡張性

VMware
SASE PoP ™

業務系通信

DMPO

DMPO

VMware SD-WAN

DC・オフィス・在宅勤務などの
分散する企業 WAN 環境を
統合的にセキュアに接続
さらに
最寄りの PoP との DMPO 接続による
ハイパフォーマンスなクラウドアクセス
を実現しビジネスの加速に貢献

オフィス・拠点

在宅勤務

SD-WAN Edge

企業データセンター

APP

SD-WAN Edge

Thank You