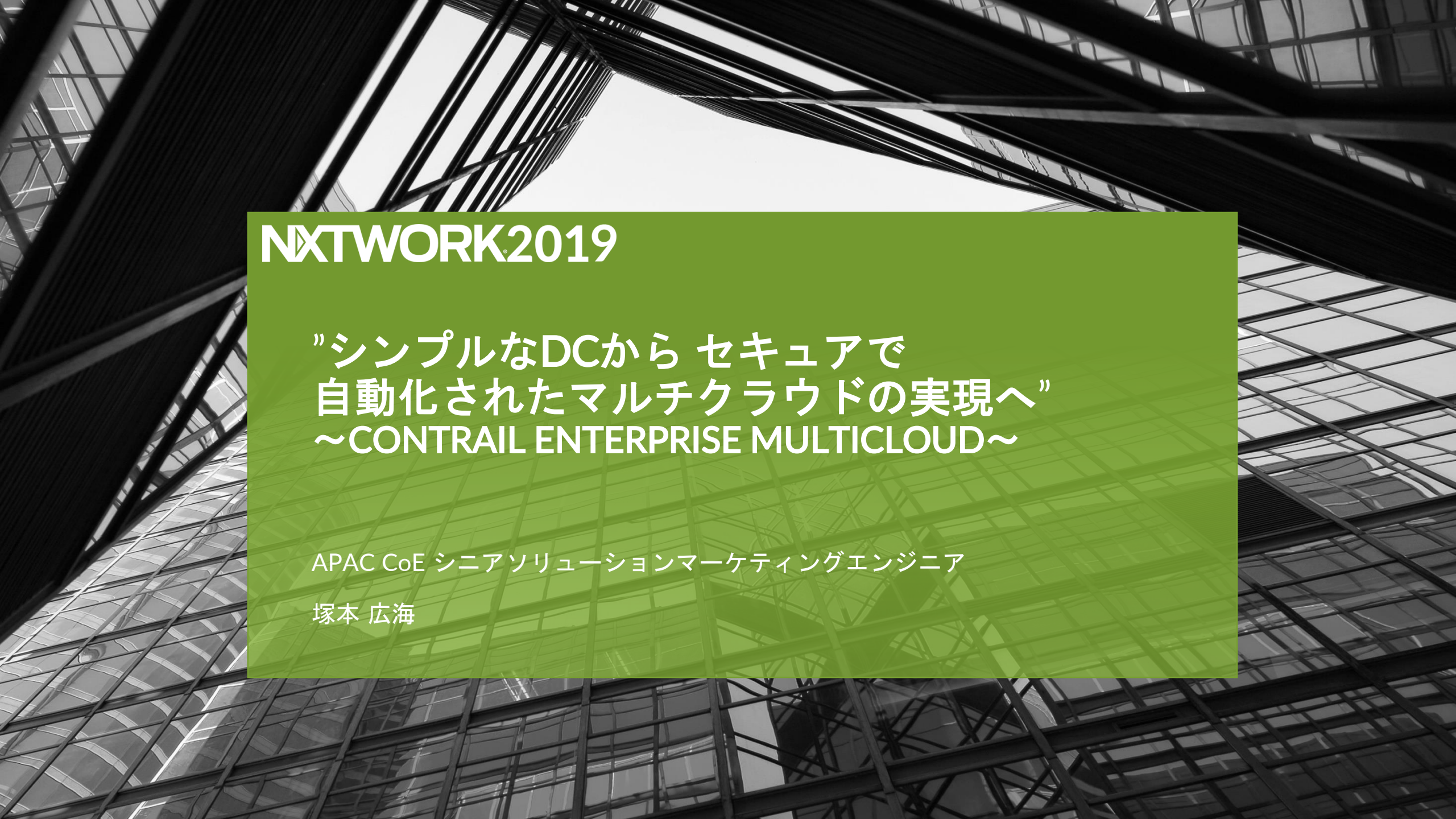


NXTWORK2019

”シンプルなDCから セキュアで 自動化されたマルチクラウドの実現へ” ～CONTRAIL ENTERPRISE MULTICLOUD～

APAC CoE シニアソリューションマーケティングエンジニア

塚本 広海

本日のゴール

JUNIPER DC SDNである
CONTRAIL ENTERPRISE MULTICLOUDの

ケーパビリティ、ユースケースをご紹介し、
最近のクラウドやDCの期待の変化の課題を
どう解決できるのかをご理解いただく。

みなさまの環境でどのユースケースで有効に活用できるか
ご検討いただく。

JUNIPER NETWORKS DISCLAIMER

This plan of record and related information includes information on future releases, future development, and new product introductions. The details provided are based on Juniper's current development efforts and plans. These development efforts and plans are subject to change at Junipers sole discretion. There can be no assurance that Juniper will introduce the future products, features or enhancements described in this presentation and Juniper assumes no responsibility to introduce such products, features or enhancements. Purchasing decisions should not be based on this POR and no purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

AGENDA

- クラウドデータセンタが求める
  インフラ要求の変化とContrailの発展
- Contrail Enterprise Multicloud 活用ケース
  - Contrail Fabric Automation
  - Contrail with Containers
  - Contrail with Public Cloud
- まとめ

ビジネスの変革による新たなインフラ要求

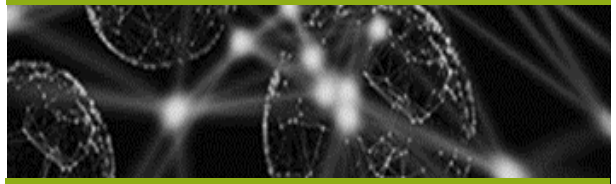
DXビジネス加速

誰もがスタートアップと戦う時代

不確実なビジネスモデルとTRY&ERROR

IT範囲の拡大と新テクノロジーの対応

IT人材不足



アジャイルな開発変化

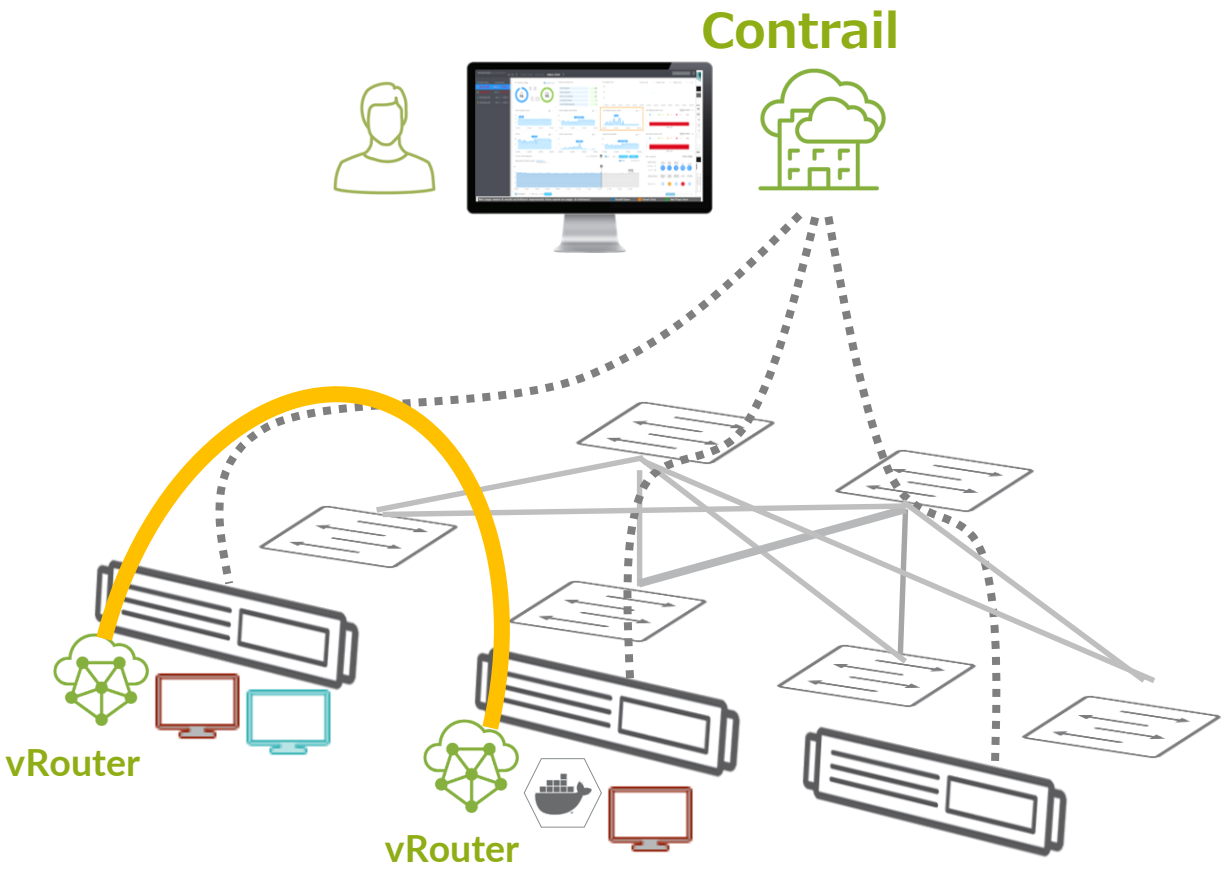
シンプル化

自動化

スケールアウト

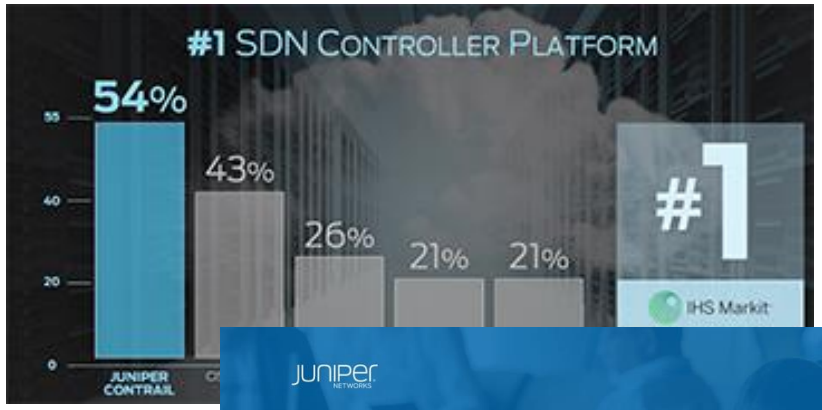
迅速性

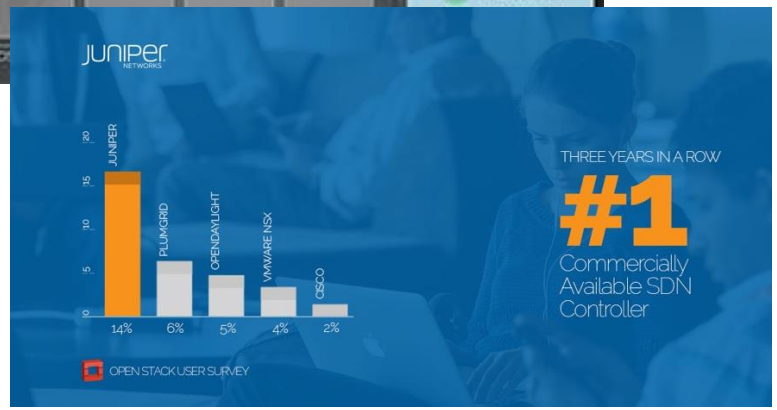
SDNによる抽象化された柔軟な仮想ネットワークの実現



SINCE 2012
CONTRAIL NETWORKING

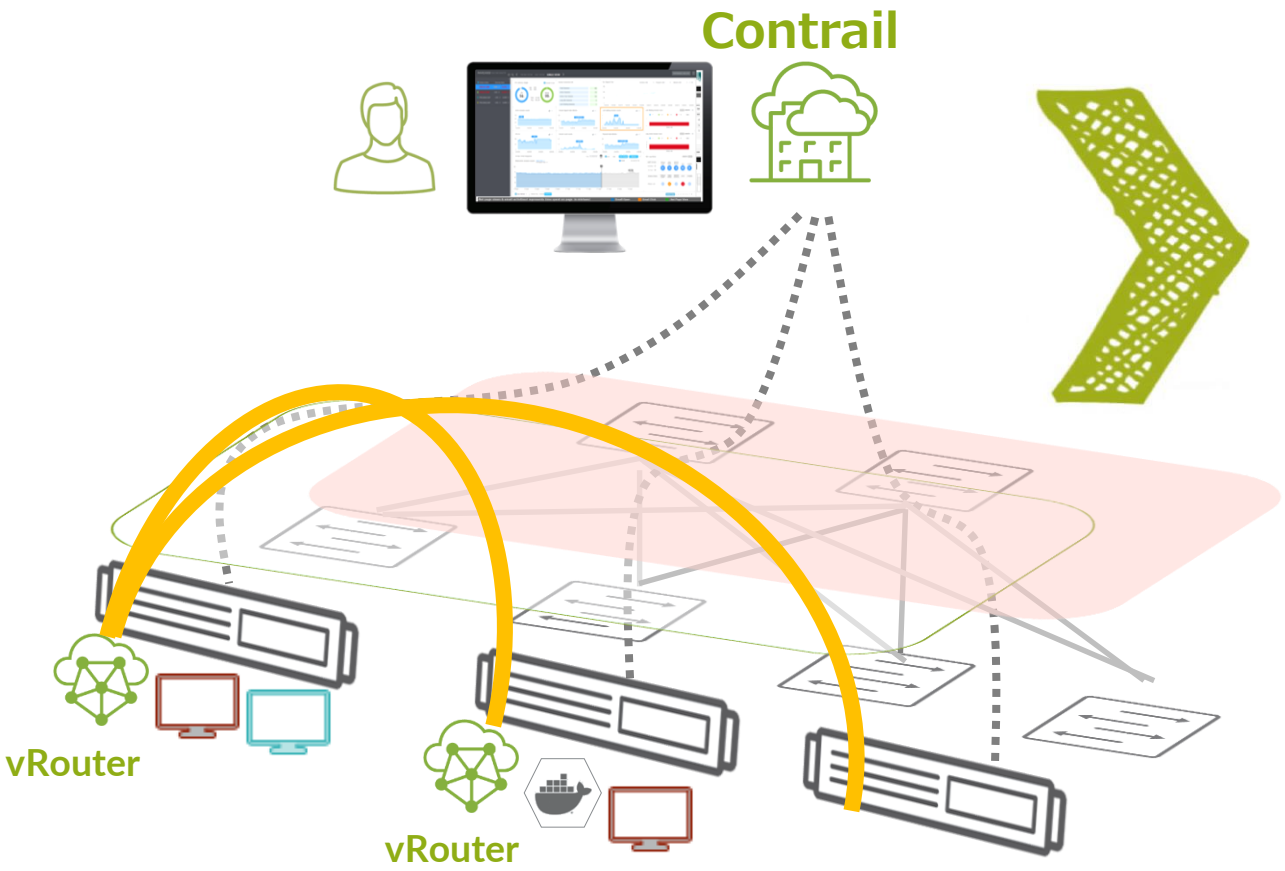
vRouter オーバーレイSDNコントローラ

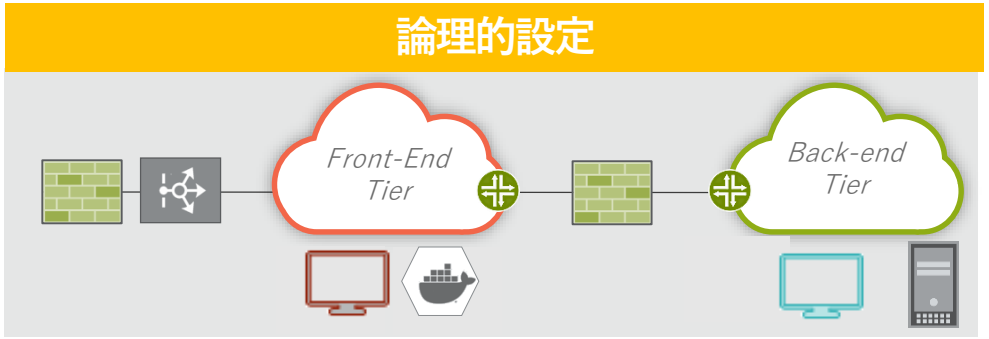




大規模ユーザー(openstack) No.1 SDN Controller

SDNによる抽象化された柔軟な仮想ネットワークの実現





迅速で柔軟なサービス

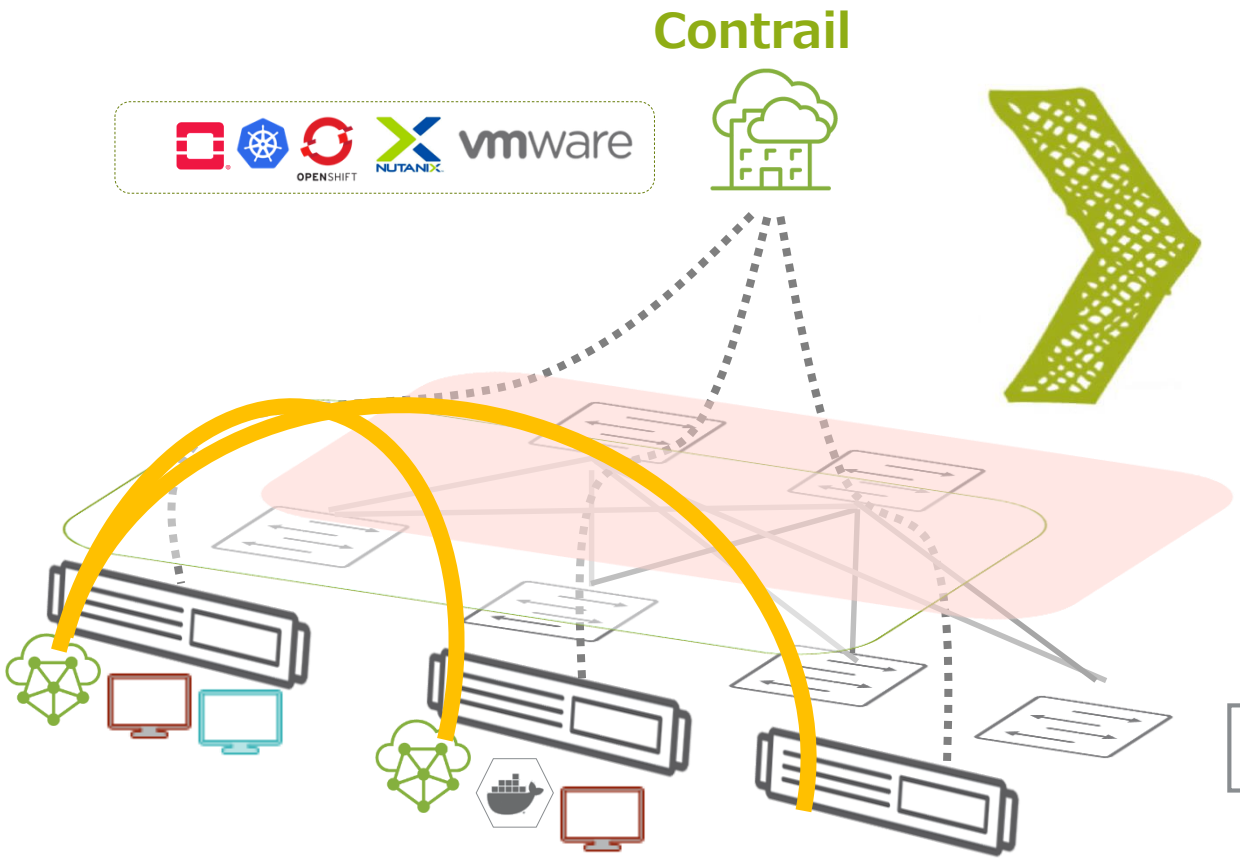
自動化・可視化・マルチテナント

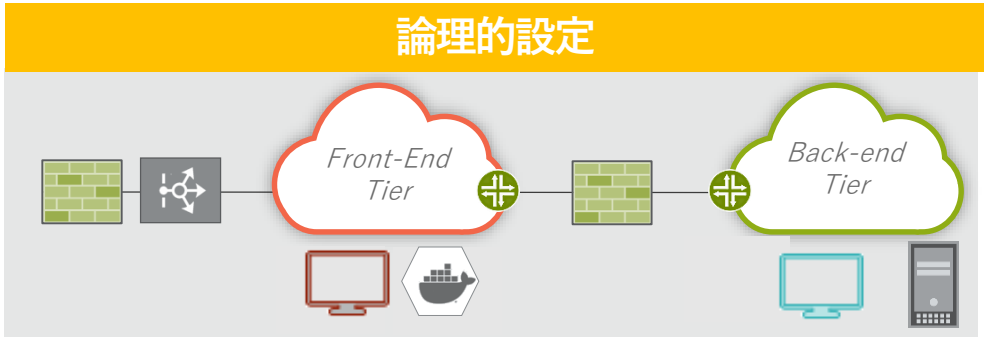
オープン(非ベンダー依存)

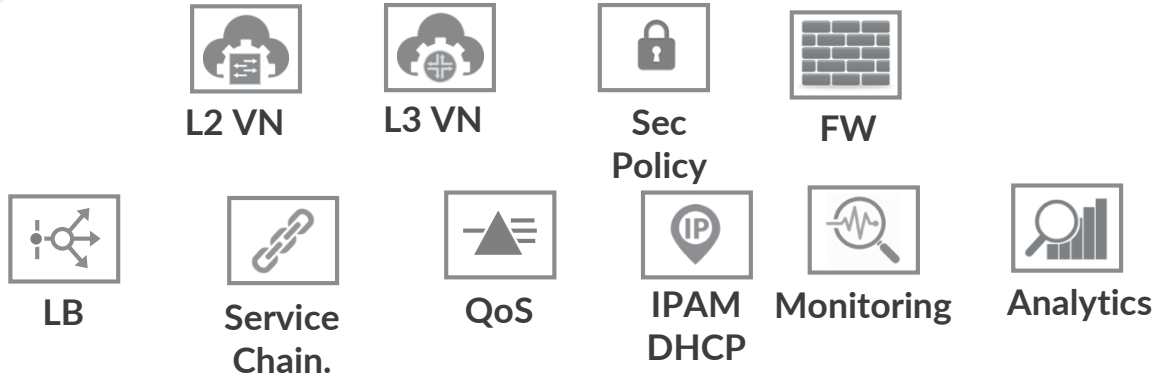
仮想ルーター オーバーレイによる仮想ネットワークの実現

tungstenfabric

SDNによる抽象化された柔軟な仮想ネットワークの実現







仮想ネットワーク上でのネットワークサービスの利用とAPI連携

データセンタクラウドインフラの新たな潮流

Multicloud and Containers

マルチクラウドの利用率

86 %

global enterprise customers

** Source: Forrester*

2022年のコンテナ利用率

75 %

containerized application in production

** Source: Gartner*

パブリック
クラウド

仮想マシン

ベアメタル

コンテナ

インフラの多様な選択肢
- ✓ 機能で選ぶ
- ✓ アーキテクチャで選ぶ
- ✓ コストで選ぶ

etc.

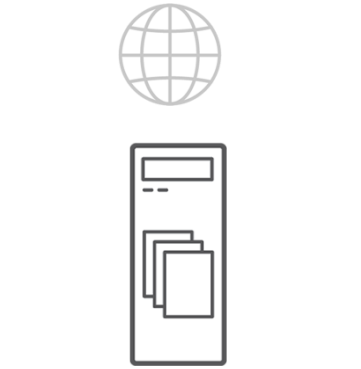
マルチクラウド マルチデータセンタのチャレンジ

それぞれのインフラにそれぞれの異なるツールでそれぞれの管理者

applications

パブリッククラウド

applications



Virtual Machine

applications

Bare-meal

applications

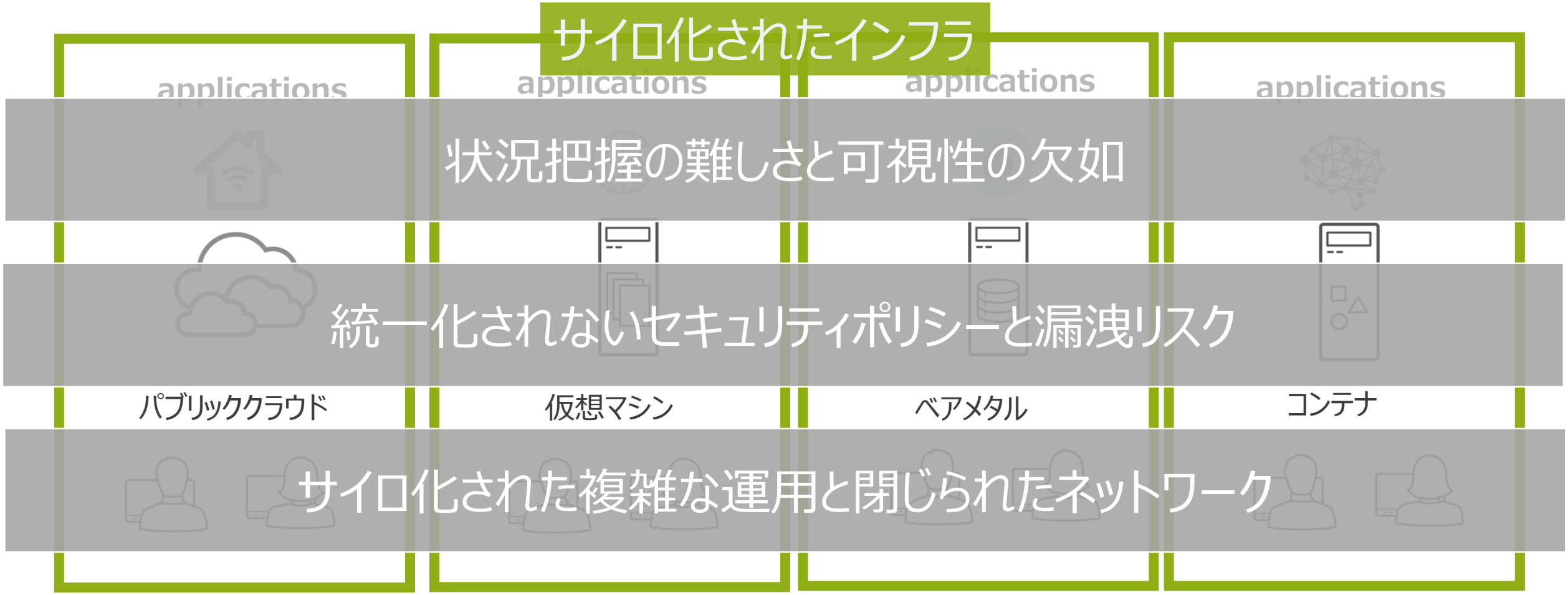
Container

ネットワーク

セキュリティ

マルチクラウド マルチデータセンタのチャレンジ

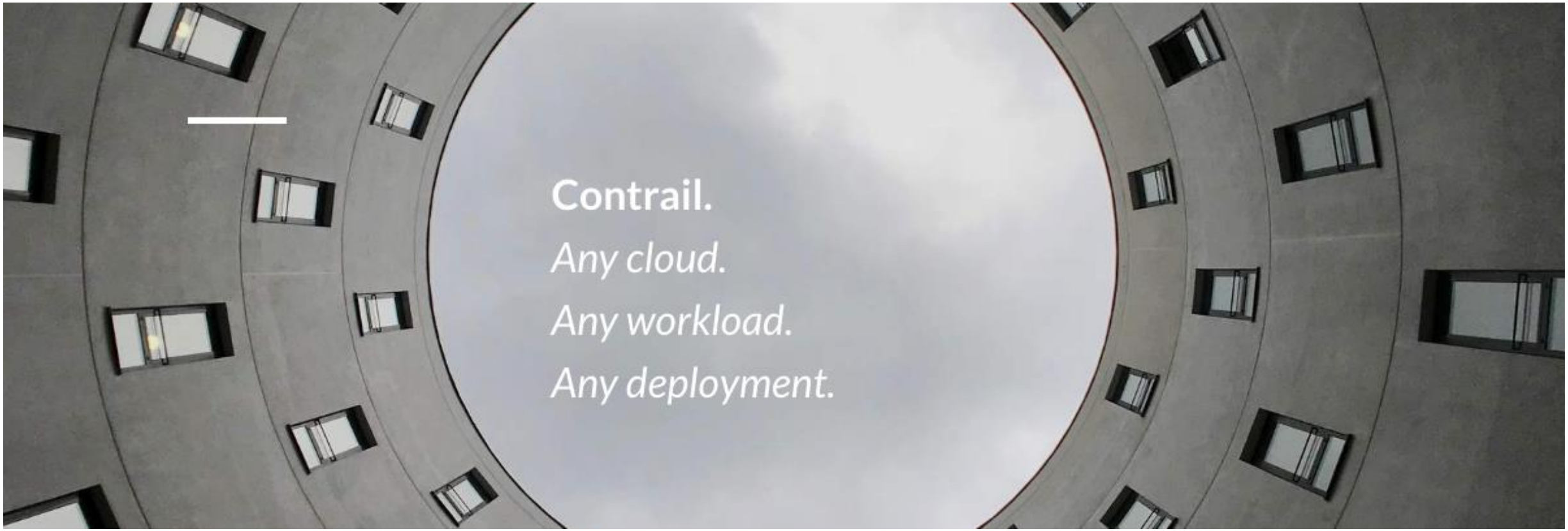
それぞれのインフラにそれぞれの異なるツールでそれぞれの管理者



マルチクラウド　マルチデータセンタのあるべき姿

マルチクラウドの良さを活かし、不必要な複雑さをなくし、オープンなプラットフォーム

共通のプラットフォームにより セキュアで効率的な運用を



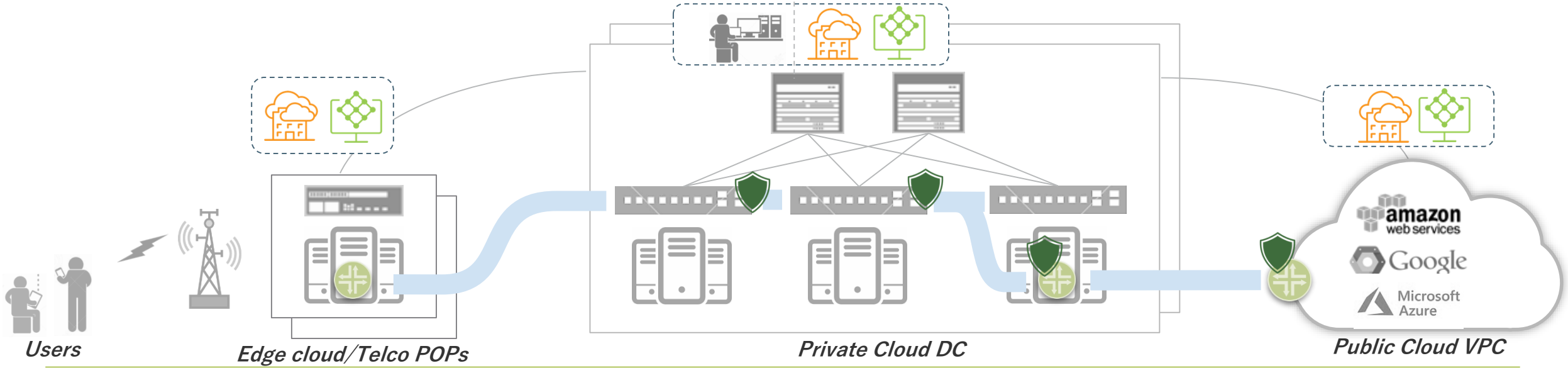
END-TO-END SECURE AUTOMATED MULTICLOUD

CONTRAIL ENTERPRISE MULTICLOUD

クラウド/DCの多様なエンドポイントをシームレスに単一コントローラーで

Contrail Is the Control Point

- Visibility and Analyze
- Secure Workloads
- Automate the Overlay
- Automate the Underlay
- Extend the Multicloud



CONTRAIL ENTERPRISE MULTICLOUD

クラウド/DCの多様なエンドポイントをシームレスに単一コントローラーで

Contrail Enterprise Multicloud

CONTRAIL COMMAND

Appformix： マルチクラウドのリアルタイムモニタリング

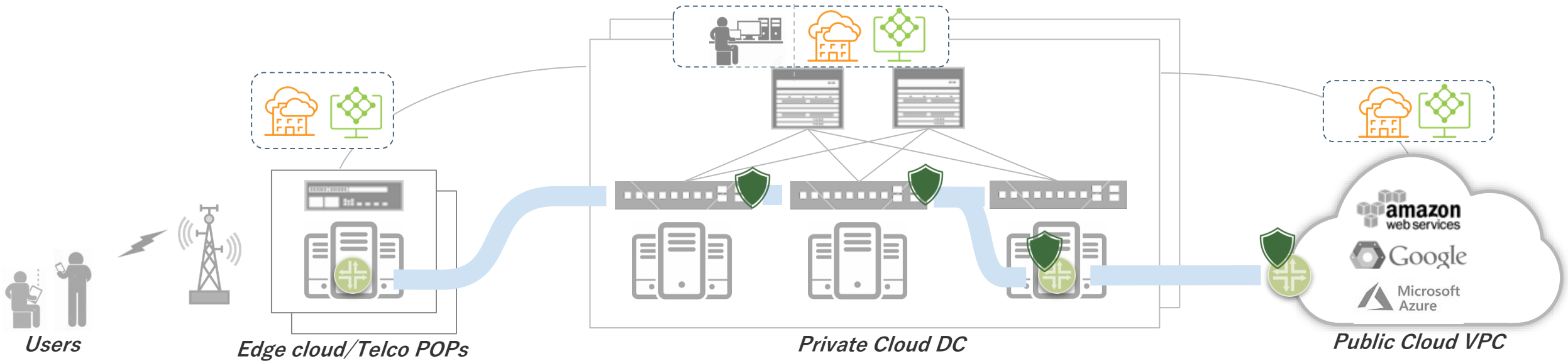
Contrail Security ： 複数クラウドにまたがったセキュリティ―ポリシーオーケストレーション

Contrail Networking

Virtual Networking ： ソフトウェアベースオーバーレイによる仮想ネットワーク

Fabric Automation： CLOS IP Fabricの管理とコネクティビティの拡張

Multi-Cloud Automation ： 仮想ネットワークのマルチデータセンタ & パブリッククラウド拡張



AGENDA

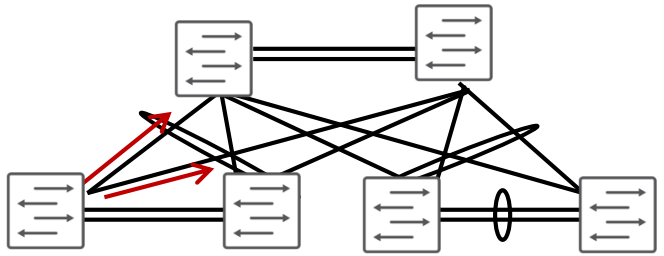
- クラウドデータセンタが求める
  インフラ要求の変化とContrailの発展
- Contrail Enterprise Multicloud(CEM)の
  新たな活用ケース
  - Contrail Fabric Automation
  - Contrail with Containers
  - Contrail with Public Cloud
- まとめ

1 Contrail Fabric Automation

アンダーレイネットワークのシンプル化自動化できてますか？

次世代DC ネットワークアーキテクチャ IP FABRIC

Multi Chassis LAG

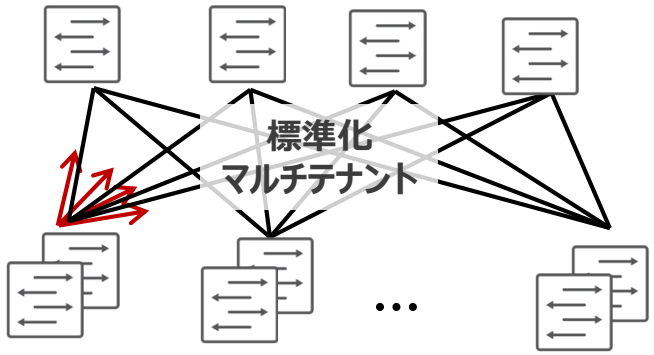


- ブロックポートがなく、アップリンクはデュアルアクティブとなる。ただしSTPの利用も併用することも多い。
- 論理構成を簡略化
- 様々なベンダーが実装済み
- STPに比べ、設計/運用は軽減
- 一台一台の設定は必要

Ethernet Fabric

- マルチパスによる帯域の有効活用
- STPを排除し、かつ、ループを回避
- ネットワーク全体をシンプルな運用管理
- スケールアウトが容易でスモールスタート可能
- ゼロタッチでの容易な追加
- ベンダー同時実装
- 密結合のため障害影響が広がる懸念あり

IP Fabric



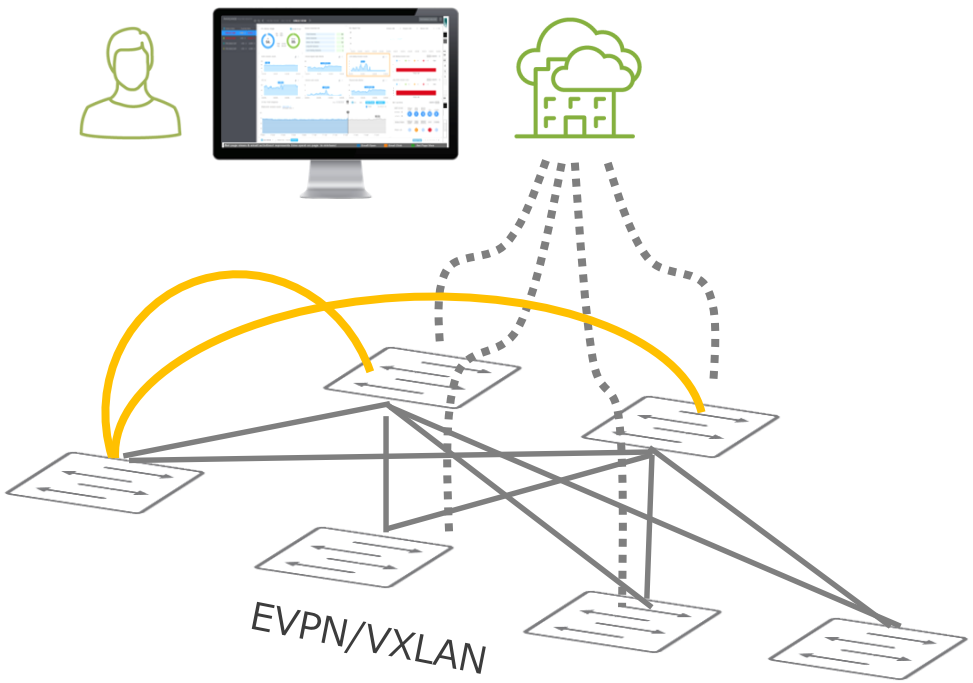
- マルチパスによる帯域の有効活用
- STPを排除し、かつ、ループを回避
- スモールスタート・スケールアウト
- 疎結合による高い冗長性
- マルチテナント環境に最適
- マルチベンダー標準実装
- 一元管理や自動化は組み込まれていない

より柔軟により容易にオープンにネットワークを拡大・管理性を向上

CONTRAILによるシンプル化されたDC ファブリック

IP ファブリック一元管理による抽象化とDCライフサイクルの自動化と可視化

Contrail Enterprise Multicloud



※一部ロードマップ含む

Day 0 : セットアップ - Underlay

- ZTP/ZTRによる容易なデバイス接続
- テンプレートによる初期設定

Day1: 運用 – Overlay

- 仮想ネットワーク(L2)・仮想ルーター(L3)
- セキュリティフィルター
- サービスチェイニング

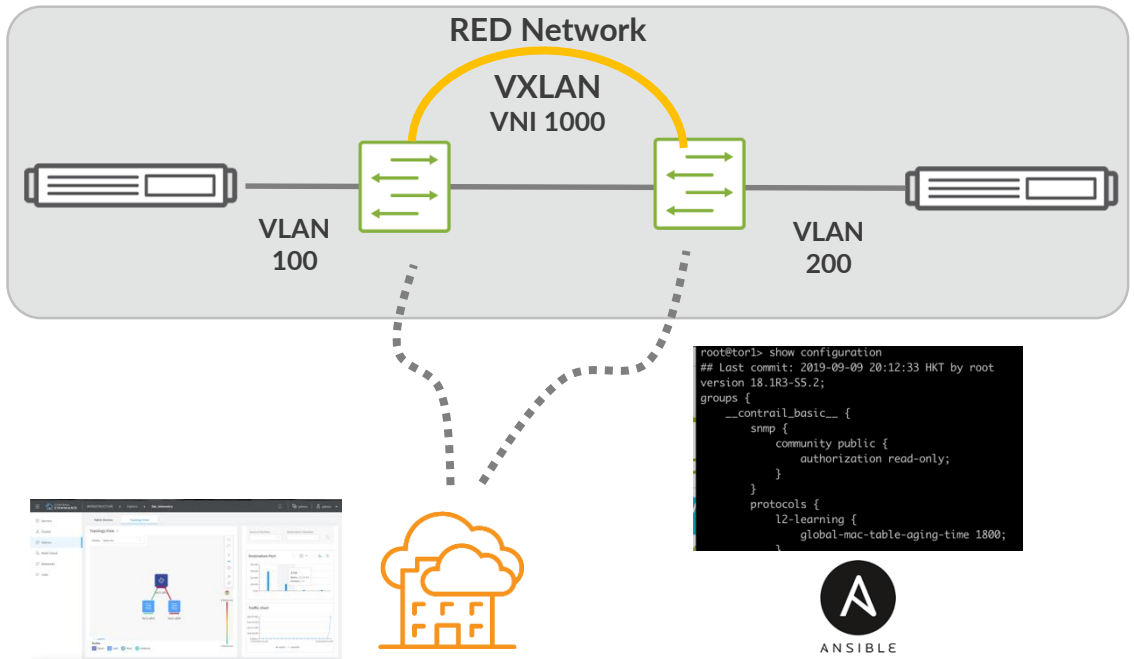
Day2: メンテナンス/トラブルシュート

- ヒットレスアップグレード
- テレメトリ活用 予兆検知
- オーバーレイパス可視化

スケーラブルなデータセンタファブリックが容易に

NETWORK VIRTUALIZATION EVPN/VXLAN

仮想ネットワークにより物理を抽象化



IP Fabric EVPN/VXLAN

- 容易な即時仮想ネットワーク追加
- マルチテナント環境に最適
- スモールスタート・スケールアウト
- 疎結合による高い冗長性
- マルチベンダー標準実装
- マルチパスによる帯域の有効活用
- STPを排除し、かつ、ループを回避

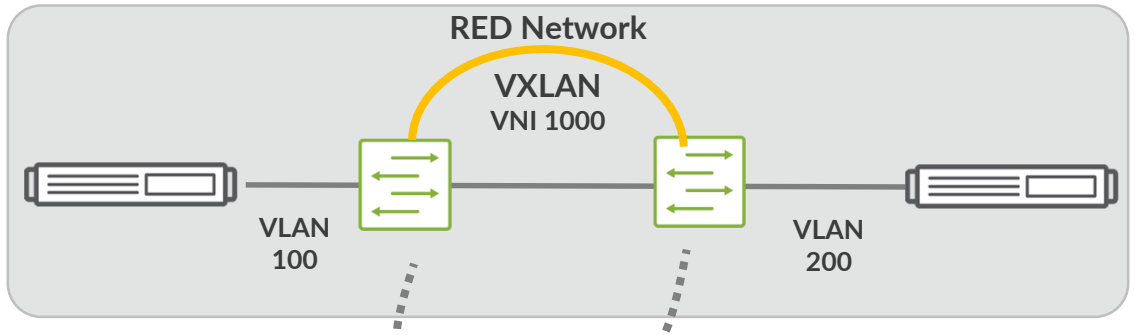
Contrail Fabric with Appformix

- 一元管理 GUIとAPI利用
- Ansibleの自動化によるブラックボックス排除
- テレメトリによるリアルタイムの可視化
- Underlay/Overlayの相関のパスの可視化

スケーラブルなデータセンタファブリックが容易に

NETWORK VIRTUALIZATION EVPN/VXLAN

仮想ネットワークにより物理を抽象化

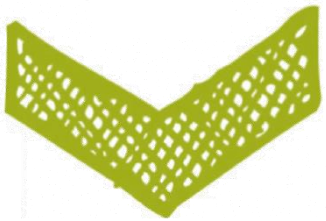


サーバー管理者

vlan/LAG作成依頼

Filter適用依頼

ネットワーク管理者



オーケストレーション連携による
仮想環境に必要なネットワークを自動作成

API連携

人を介さずAPI連携

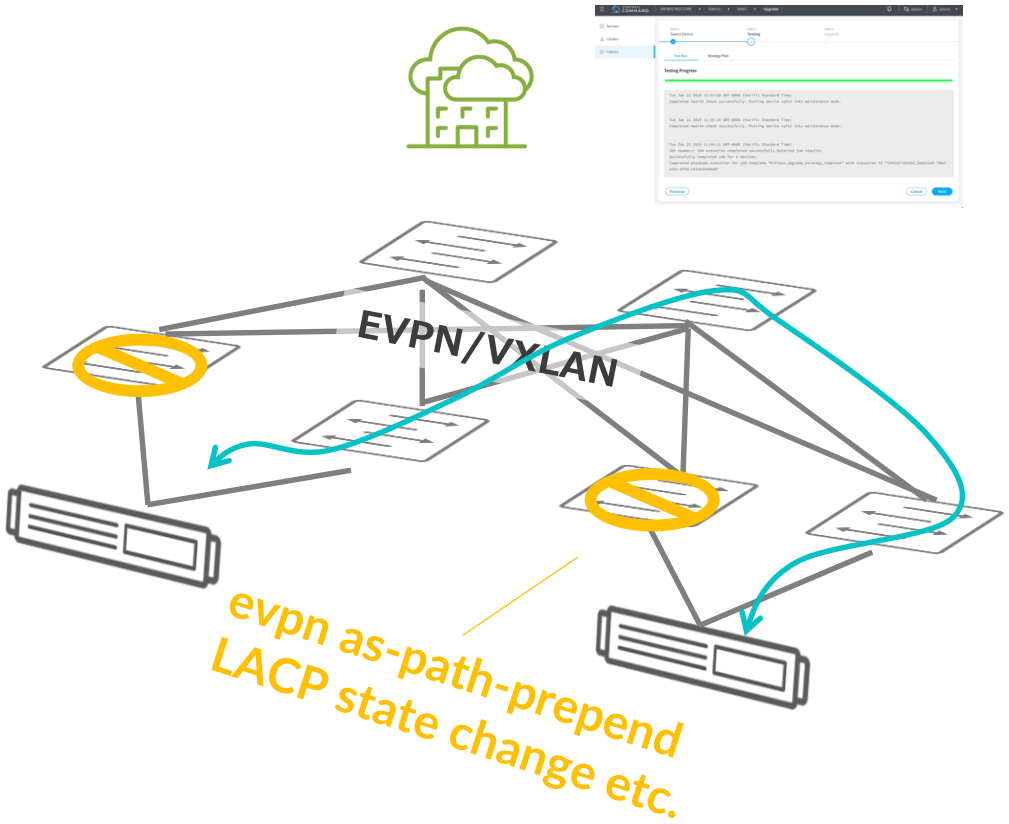
Prism

NUTANIX

※一部ロードマップ含む

メンテナンス: ヒットレスアップグレード & メンテナンスモード

日々の運用だけでなく、メンテンスも容易に



ファブリック全体でパケットロスなくアップグレード

- Hitless DC software upgrade
  - アップグレード前診断
  - メンテナンスモードによるトラフィック迂回
  - アップグレード後診断

トラフィックの明示的な迂回

- Traffic Drain
  - 特定DeviceをMaintenance mode指定
    明示的なトラフィック迂回が可能
  - SFP劣化の交換など

可視化/分析：MONITORING WITH APPFORMIX

マルチクラウド環境のリアルタイムの可視化

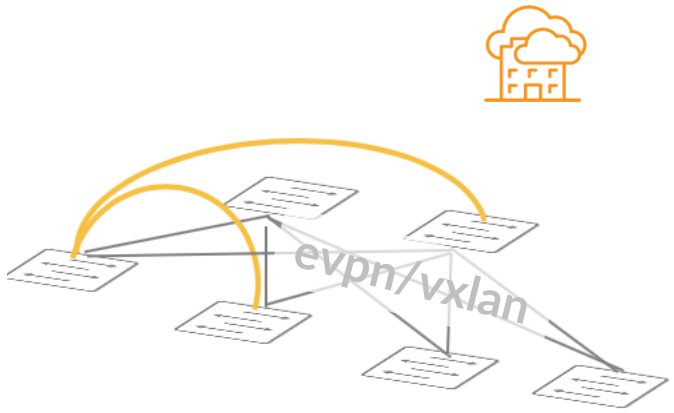
SNMP | Telemetry | flows NEW

- トポロジービュー(物理,論理)
- ヒートマップ
- フローサーチ
- トラフィックパスの可視化
- キャパシティユーセージ
- ダイナミックアラーム(機械学習)

※一部ロードマップ含む

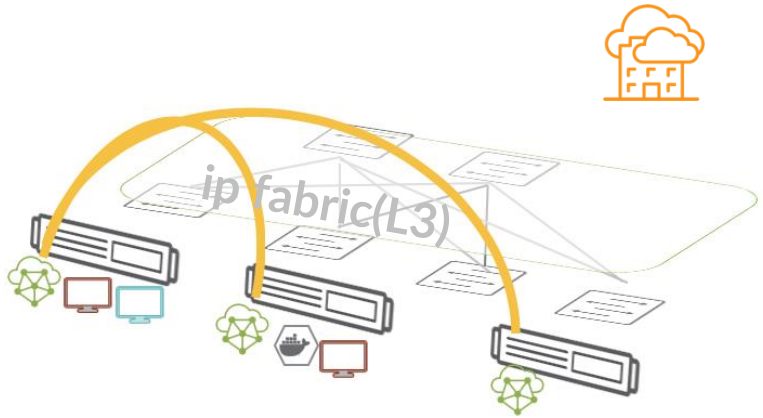
アンダーレイとオーバーレイの柔軟な選択と一元管理

DCファブリック EVPN/VXLANベース



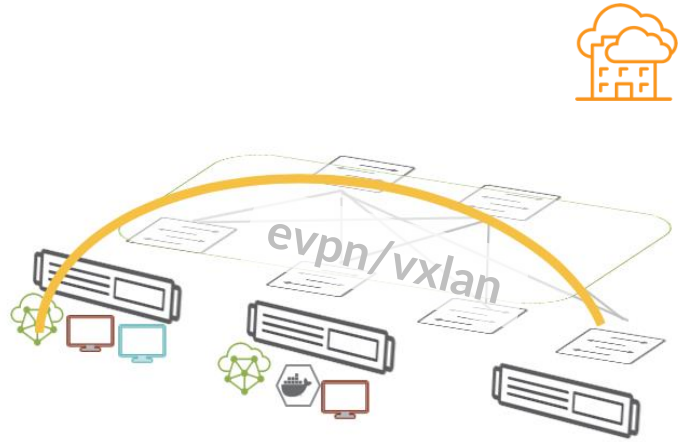
スケーラブルな
ハードウェアベースの
DCファブリック

vRouterオーバーレイと アンダーレイの一元管理



異なる管理が必要だった
オーバーレイとアンダーレイを
一元管理

HYBRID ベアメタルと 仮想化の柔軟な接続



仮想と物理 環境を容易に
同一仮想ネットワーク接続

データセンタのハードウェア環境をシンプル化し更なる拡張も容易

2 Contrail with k8s containers

コンテナを利用するときにネットワークのことも考えてますか？

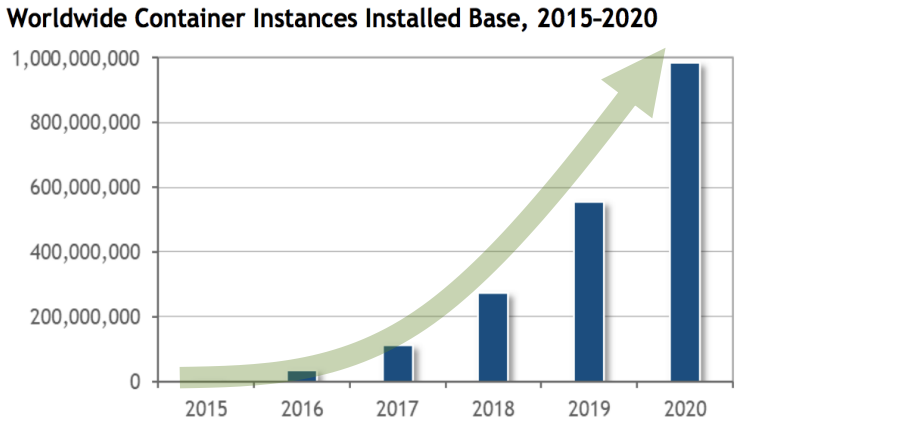
デプロイモデルの変化とコンテナ利用の増加

2022年のコンテナ利用率

75 %

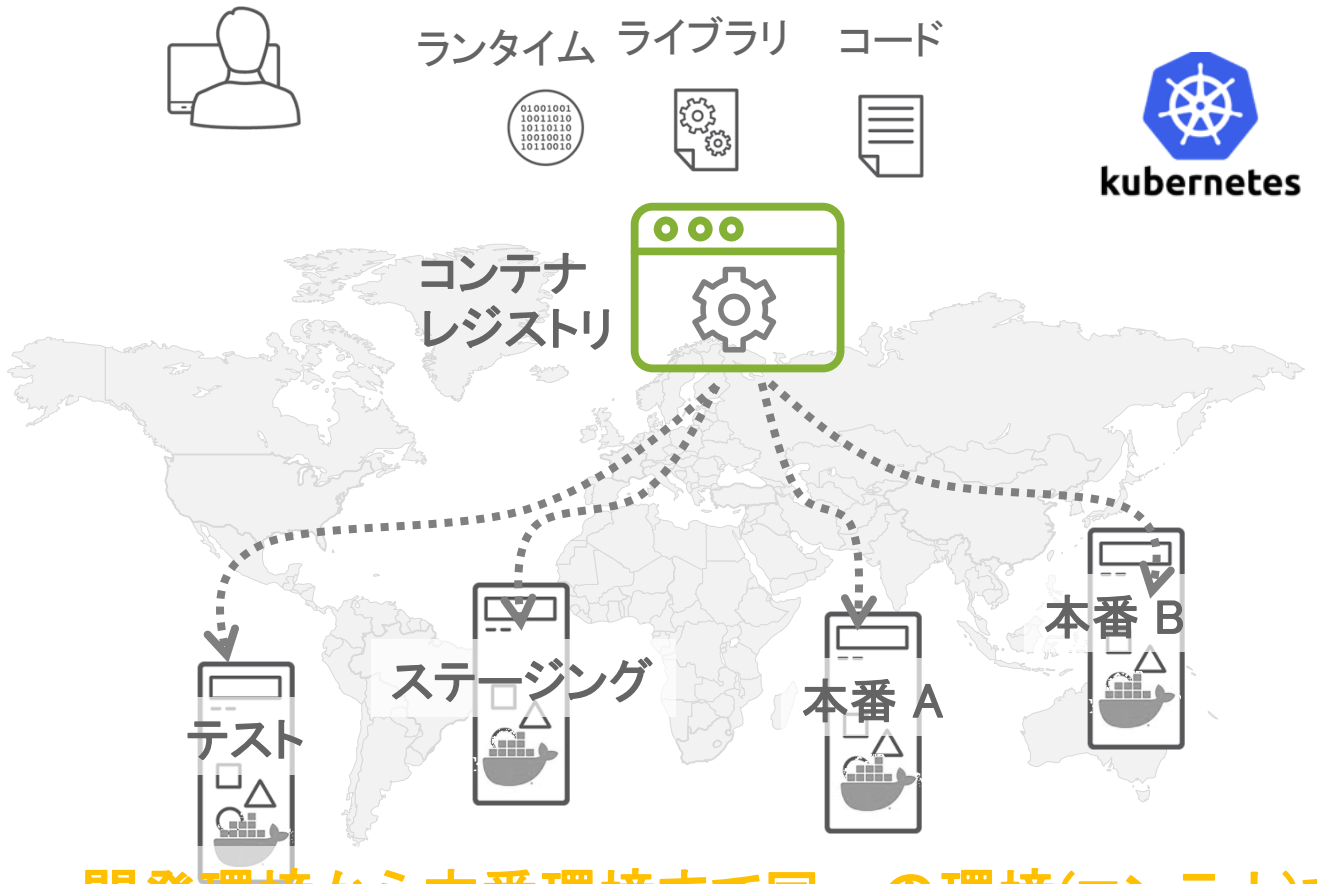
containerized application in production

** Source: Gartner*



Note: See *x86 Software Containers Forecast, 2016-2020* (IDC special study #US42030116, December 2016) for more details.

Source: IDC, 2018



開発環境から本番環境まで同一の環境(コンテナ)で
***即座に* *どこでも* 利用するのが可能に。**

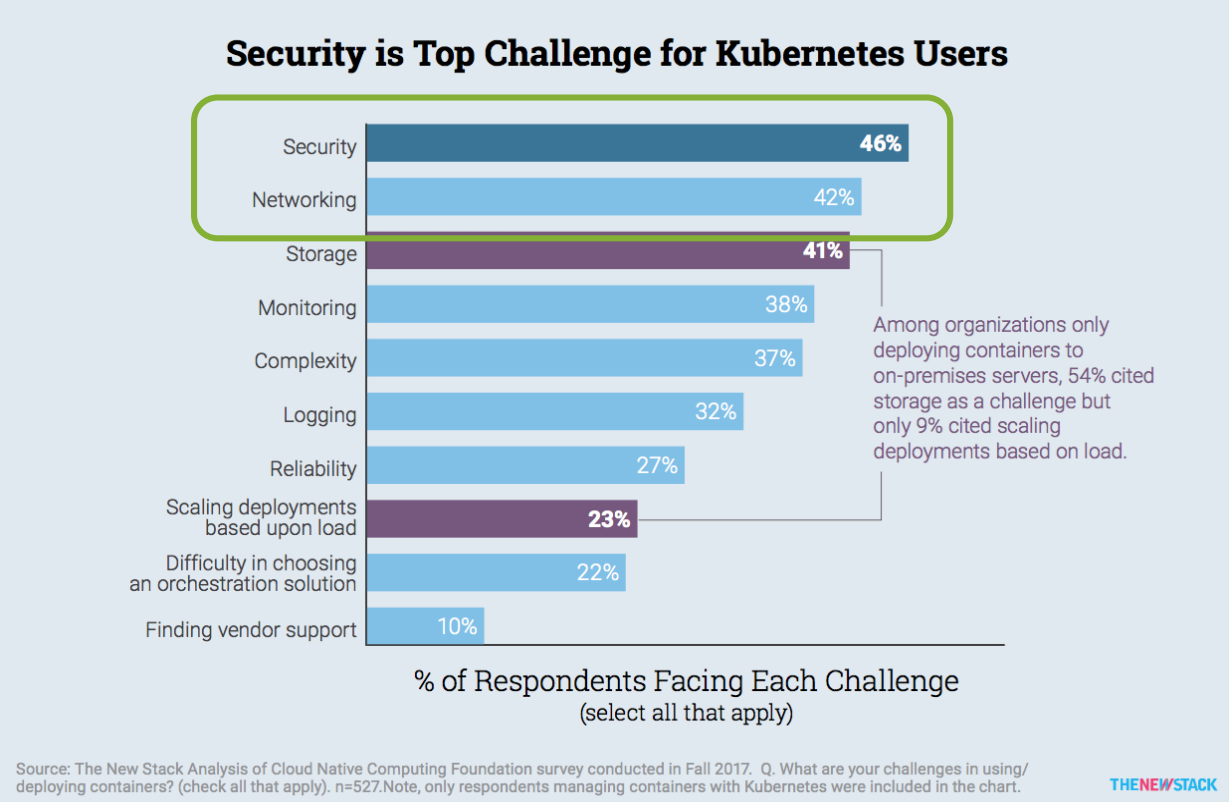
増加するコンテナ/K8S利用 と チャレンジ

メンテンス性向上、耐障害性向上、
スケール向上,、
アジャイル開発(Infrastructure as a Code)

ユースケース

- 自社 開発/保守 アプリケーションのコンテナ化 (CI/CD運用と本番環境)
- クラウドアーキテクチャのリフレッシュ(VM → コンテナ)
- PaaSホスティングでのコンテナ利用
- IoTデバイスのコンテナ利用
- コンテナ エッジコンピューティング

利用しているコンテナの課題は？



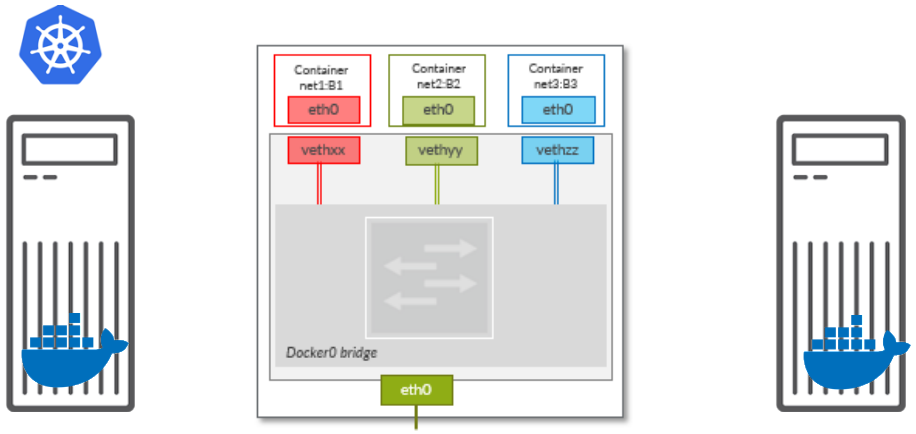
セキュリティとネットワークの検討が重要

商用展開には注意が必要なコンテナネットワーク

小規模POCならよいが、、

デフォルトのDocker/k8s ネットワーク

- フラットなL2ブリッジネットワーク
  ・プロジェクト毎に分割困難
- コンテナ用内部アドレスは自動的に払い出し
- ホスト外との通信はNAT
  ・外部の既存FWでアドレス毎の制御困難
- k8sではSERVICE(LB)で複数ホストにバランス
- ホスト間の通信は考慮が必要



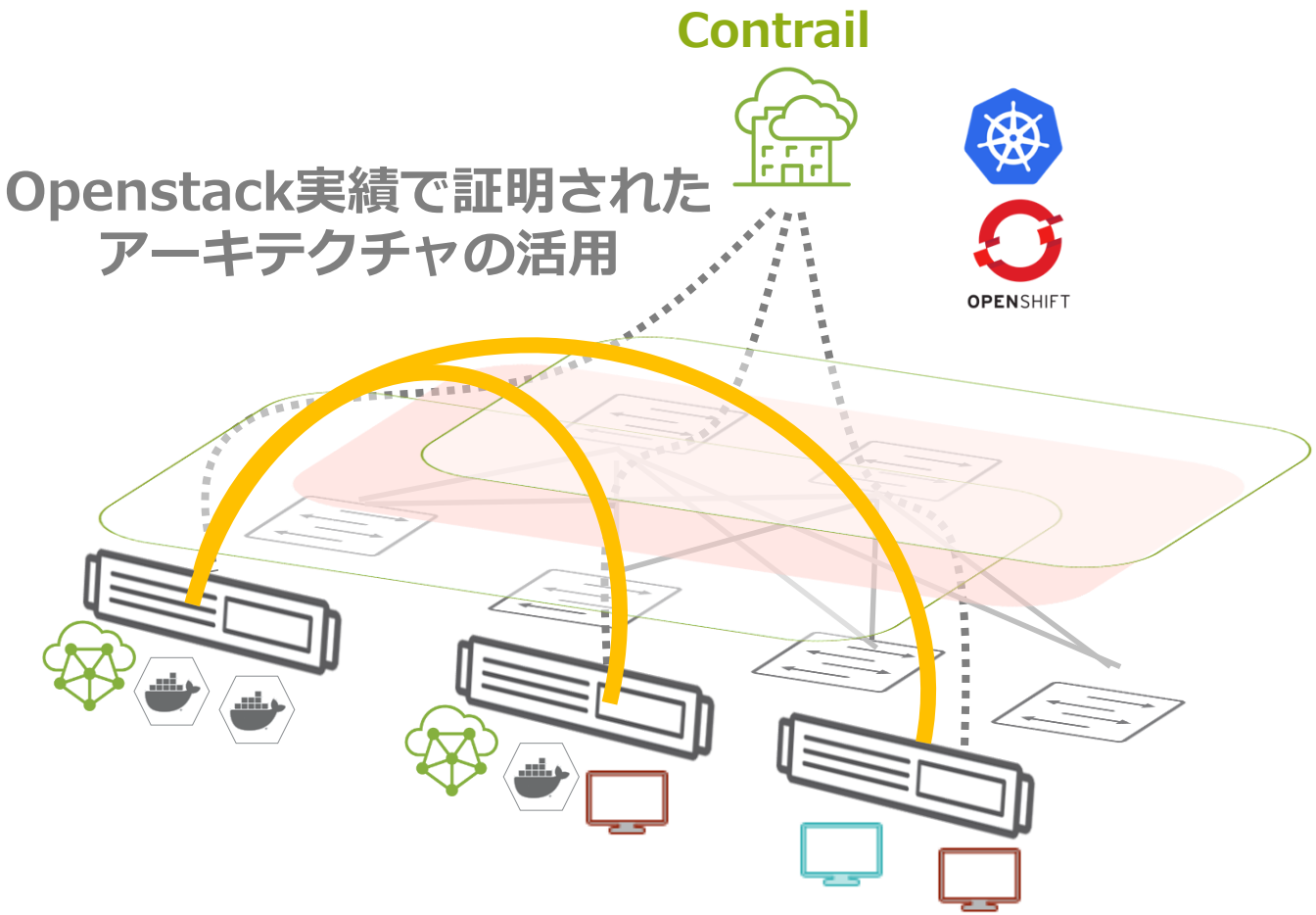
考慮が必要なこと

- ネットワークの接続性/独立性
- IPアドレス管理(IPAM)
- セキュリティポリシー
- 既存環境と接続方法やセキュリティ
- 外部接続方法
- 帯域制限、スケーラビリティ、管理性 etc.

CNI（Container Network Interface）
k8s plugin の利用

kubernetes OPENSHIFT

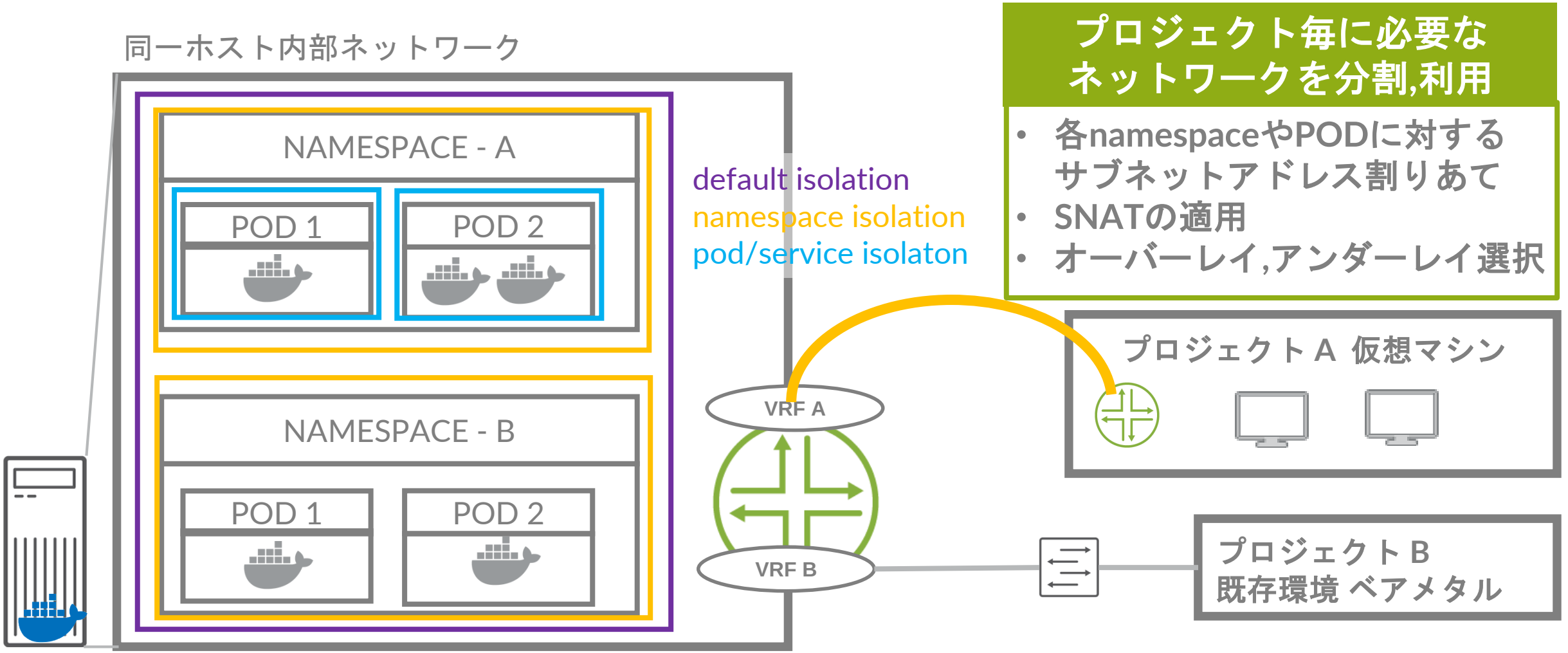
CONTRAIL コンテナ オーケストレーション



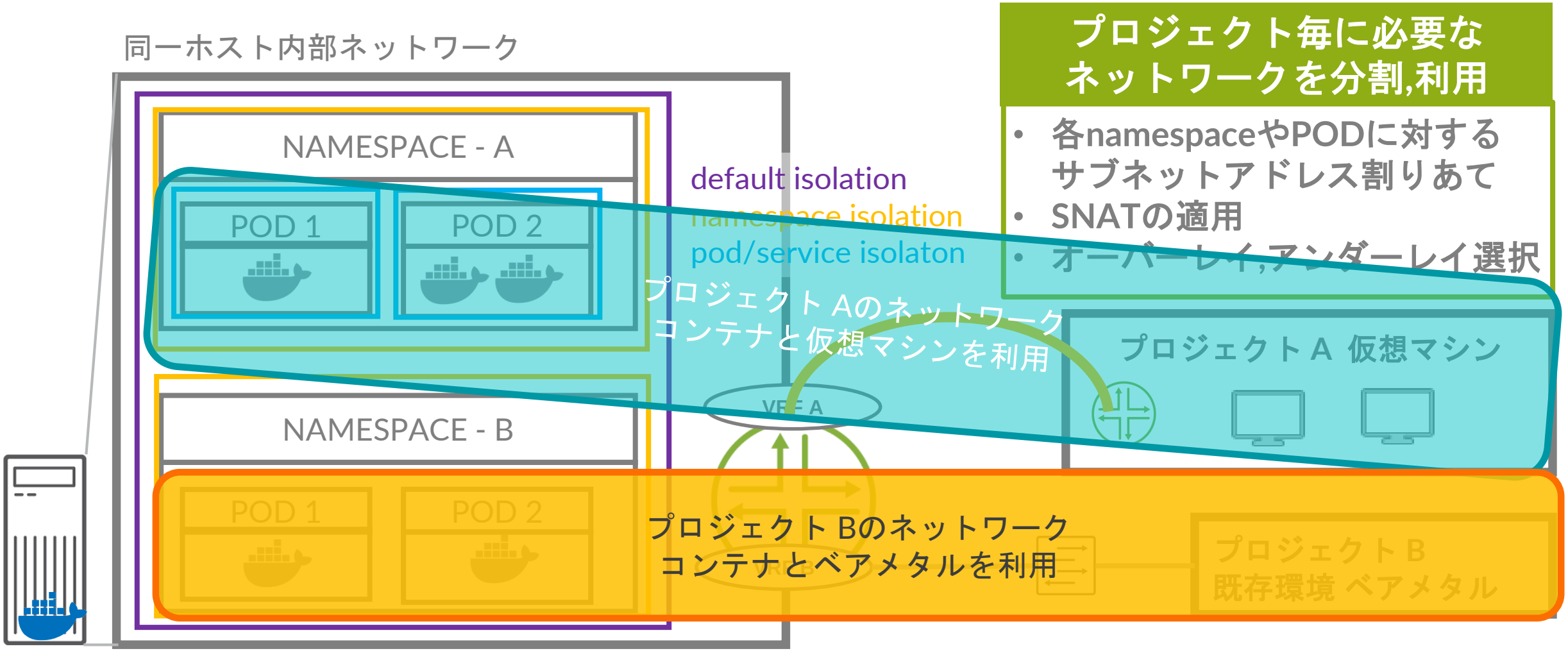
- 柔軟なアイソレーション(L2/L3, テナント)
- vRouterの機能利用
(SNAT, QoS, IPAM, S-Chaining etc.)
- 動的で直感的なセキュリティポリシー
- コンテナと非コンテナ既存の相互接続
- コンテナと非コンテナの仮想NWと一元管理

柔軟性, スケーラビリティ, 管理性の高いコンテナネットワークの実現

柔軟なアイソレーションと 非コンテナ環境との接続



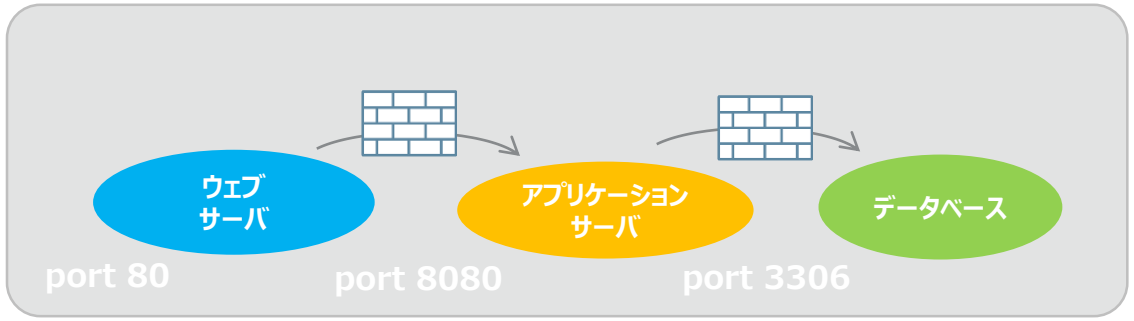
柔軟なアイソレーションと 非コンテナ環境との接続



動的で直感的なセキュリティポリシー　– 分散ファイアウォール

Intent Based Firewall
Contrail Security

セキュリティポリシー テンプレートの事前定義



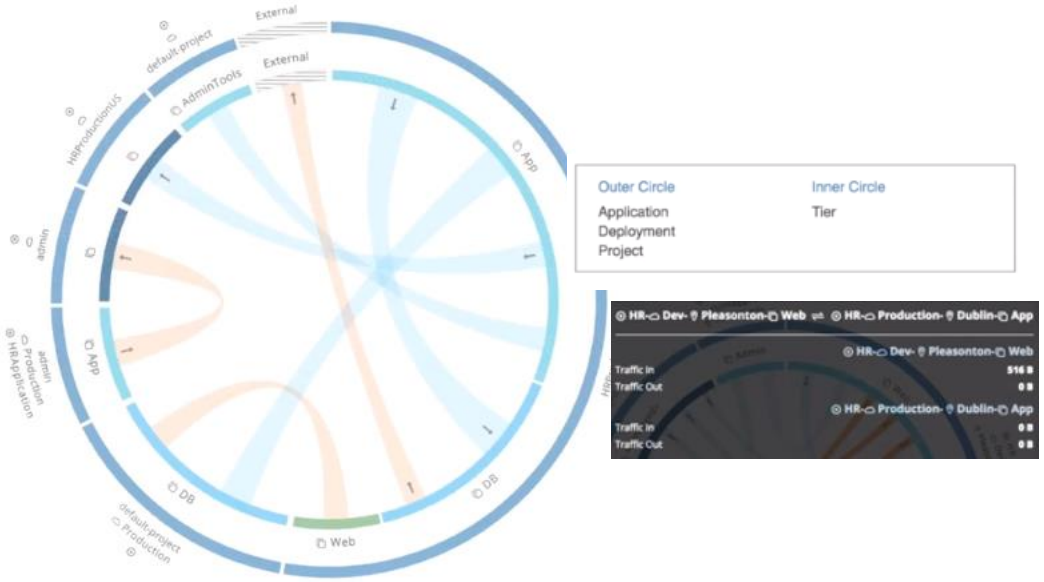
タグベースフィルターでアドレスフィルター管理不要

applicagion:app-1
label:web

applicagion:app-1
label:db

即座にどこでも起動するコンテナに
動的なセキュリテイポリシーの利用

通信トラフィックの可視化



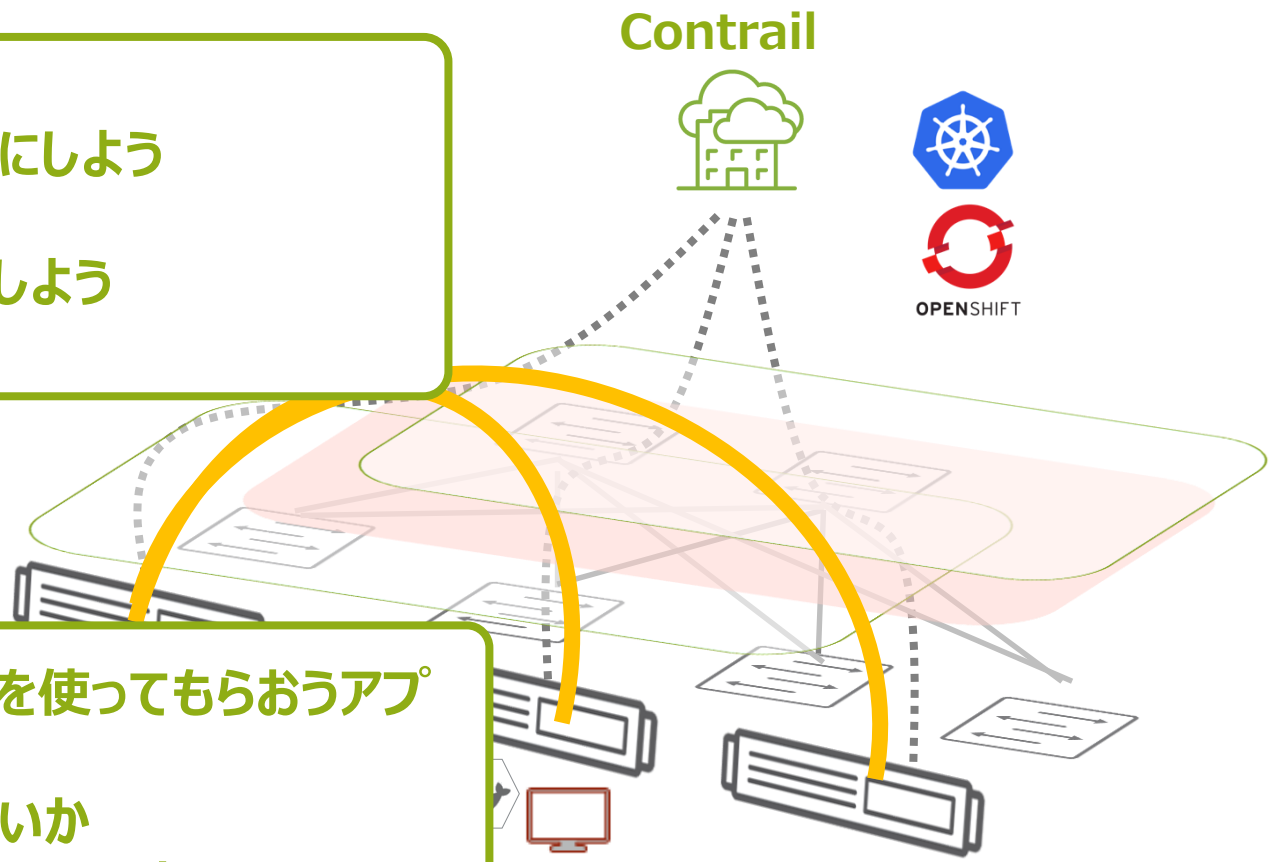
流れているトラフィックを解析しポリシー作成も可能

ユースケース：アプリ開発基盤 既存仮想マシンとの接続も

コンテナの商用導入が可能なネットワークを実現

プロジェクトによって
- サブネット分けてホスト間でもL2接続できるようにしよう
- SNATの変換後のアドレスもわけよう
- 外部の既存FWはこのSNATのアドレスで管理しよう
- DBは既存の仮想マシンを利用

- ウェブアプリAは事前定義のセキュリティポリシーを使ってもらおうアプリエンジニアはラベル指定するだけだし
- ただ、このBのアプリはどういう通信を許可していいかわからないから、まずは動作してもらって可視化してみるか



3 マルチクラウドへの拡張

複数クラウドをすべて個別に管理しますか？

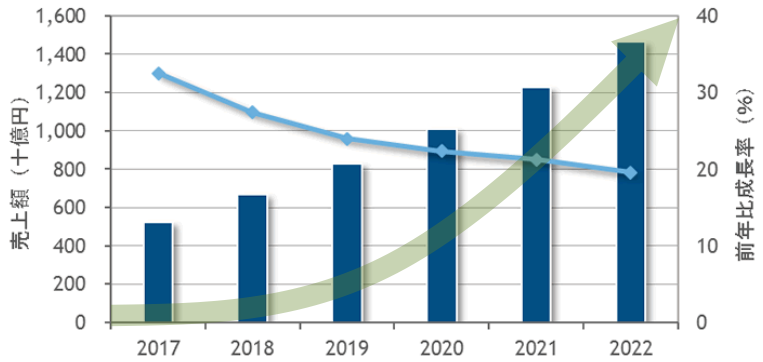
マルチクラウドの期待の増加

マルチクラウドの利用率

86 %

global enterprise customers

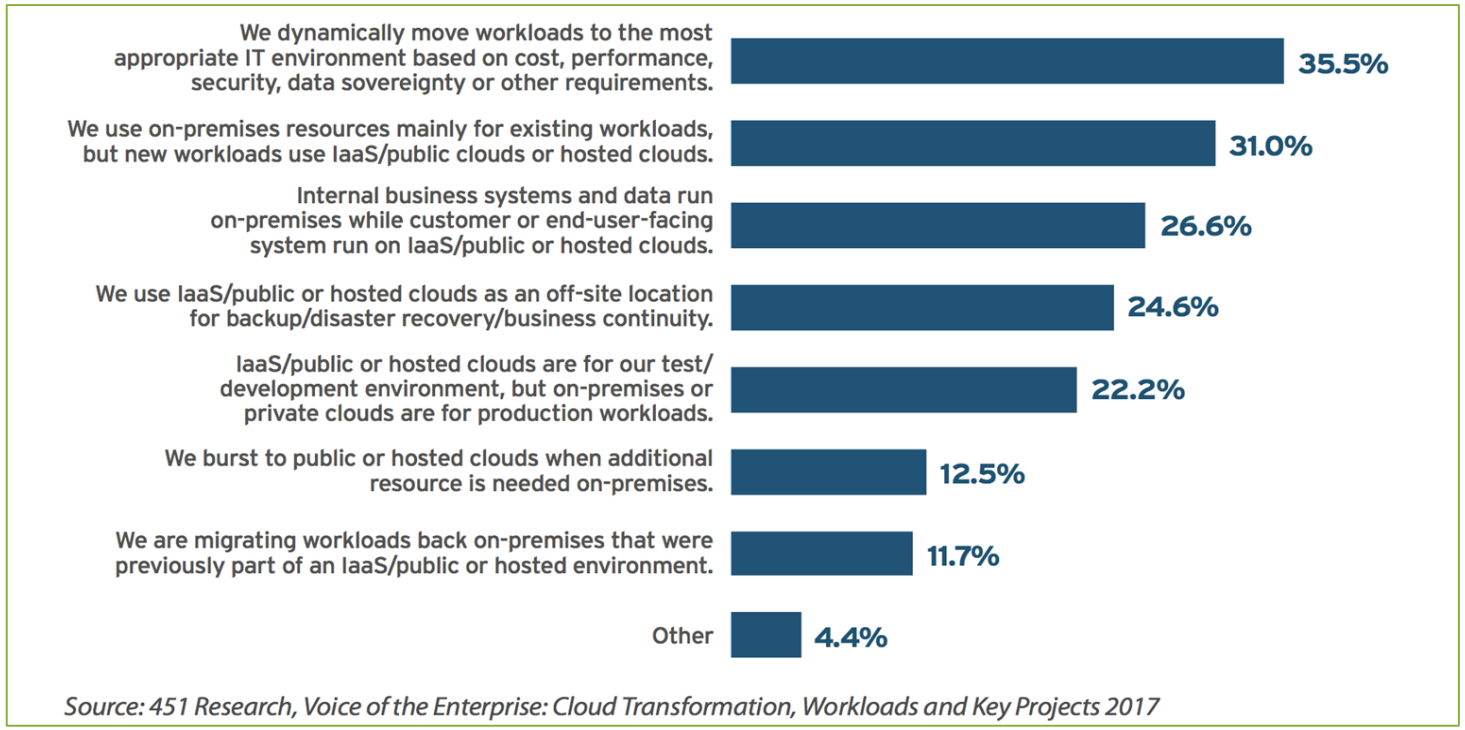
** Source: Forrester*



** Source: IDC Japan、*
国内パブリッククラウドサービス市場予測

デジタルトランスフォーメーション（DX）や
新技術を活用した「生産性の向上」「業務の効率化」を目的として、
パブリッククラウドを利用するユーザー企業は増加

クラウドトランスフォーメーションの期待



クラウドの期待と課題

クラウドは無限の可能性がある

- 利用状況に応じて利用できコストが下がる
- オンデマンドにいつでもすぐに柔軟に利用
- Always onの高い冗長性
- 先進的でイノベーションをリード

広く利用する前に戦略を怠ると

- 自社保有よりコスト増
- サイロの管理となりセキュリティ新たな課題
- 信頼性を考慮をした設計しなければサービス影響
- 最適化や統合が難しく新たな技術ナレッジが必要

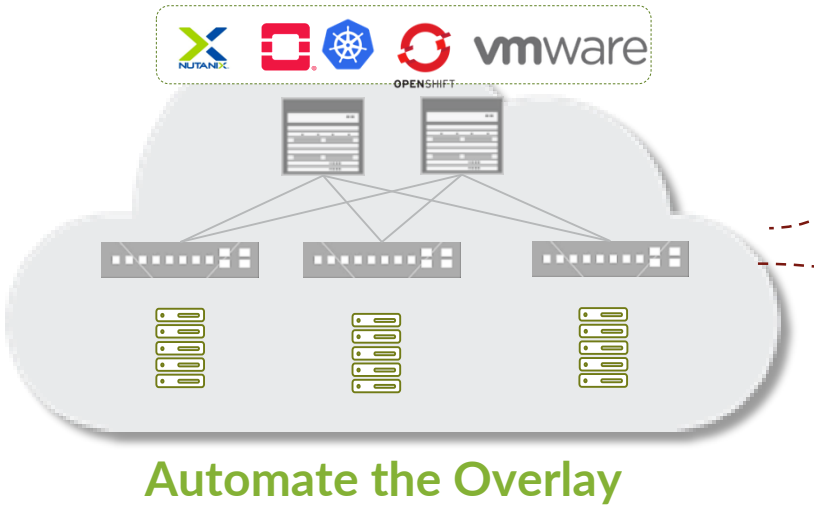
SECURE AUTOMATED MULTICLOUD

CONTRAIL
ENTERPRISE
MULTICLOUD

シームレスな
仮想ネットワーク

直感的な
共有セキュリティ
ポリシー

マルチクラウドの
状況把握



Automate the Underlay

Secure
Workloads

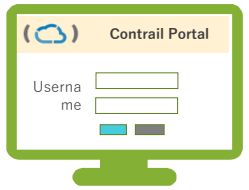
Extend to Multicloud

Automate the Overlay

マルチクラウド環境を個別管理せず一元的に セキュアでシームレスな仮想ネットワーク

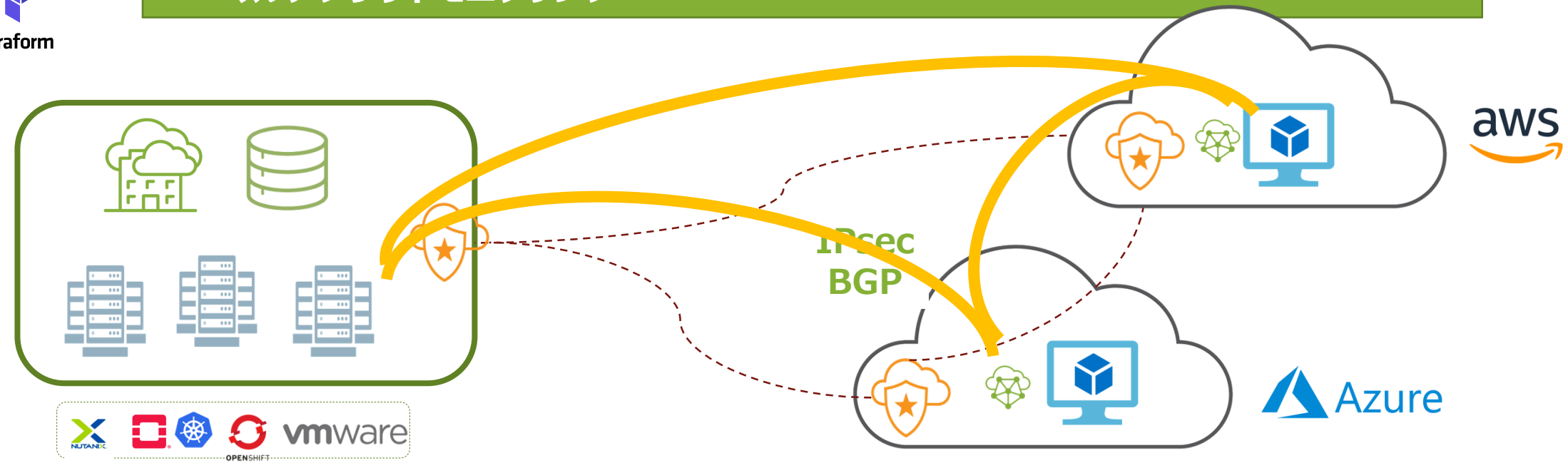
CONTRAILマルチクラウドセキュアコネクション

パブリッククラウドリソースもContrailから一元的に作成及び可視化



- パブリッククラウドのリソース作成
  (VPC, サブネット, インスタンス, セキュリティグループ etc.)
- MultiCloud-GWによるセキュアVPNと経路交換
- インスタンス追加 （k8s ノード等)
- マルチクラウドモニタリング

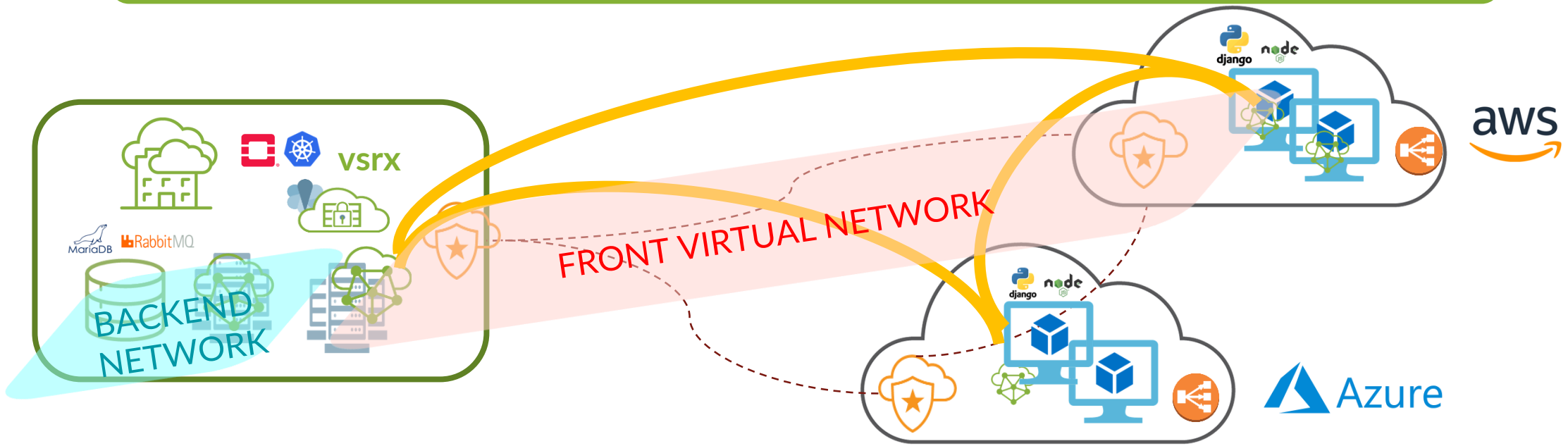
HashiCorp Terraform



某金融DCユースケース：セキュアマルチクラウドアプリ

用途に合わせたワークロードをContrailでシームレスに一元管理

- スケールアウトが必要なフロントエンドはパブリッククラウド上のコンテナでスケールアウト
- DBはオンプレの仮想マシンでよりセキュアに
- フロントとバックエンドの間にはvSRX-FWにチェーニング
- 動的なインテントベースセキュリティフィルター



AGENDA

- クラウドデータセンタが求める
  インフラ要求の変化とContrailの発展
- Contrail Enterprise Multicloud 活用ケース
  - Contrail Fabric Automation
  - Contrail with Containers
  - Contrail with Public Cloud
- まとめ

ROAD TO DATA CENTER TO MULTICLOUD

将来の拡張が可能なプラットフォーム
Contrailで段階的な拡張も可能

将来のための5ステップ

1

レガシー データセンタ

- 3層のデータセンタ
- 境界型セキュリティ

2

シンプル化された データセンタ

- ネットワークの抽象化
- スイッチファブリック
- テレメトリ可視化

- -40% 管理負荷減

3

マルチドメイン プライベートクラウド

- ワークフロー自動
- オーバーレイSDN
- マイクロセグメンテーション

- 70% 展開速度アップ
- ~35% IT管理者によるセルフサービス

4

ハイブリッドクラウド

- 1つのクラウドの拡張
- マルチクラウドポリシー展開
- クラウドDR

- +100x スケーリングスピード
- -38% アプリケーションに対するインフラコストの削減
- -65% 集中化されシンプル化されたセキュリティポリシーによるOPEX削減

5

セキュア & 自動化 マルチクラウド

- マルチクラウドの抽象化
- インテントドリブン
- 統合セキュリティポリシー

- クラウドオーケストレーションにより30%管理負荷減
- アプリケーションライフサイクルの+66% 増加

デジタルトランスフォーメーションに向けた基盤

シンプル化 | **自動化** | **スケールアウト** | **迅速性**

Aopformix Monitoring

Contrail Enterprise Multicloud

Contrail Security

拡張性・耐障害性が証明された No.1 SDNが
マルチクラウド・コンテナ・アンダーレイを管理する唯一のオープン基盤に

まとめ

ケーパビリティ、ユースケース概要はご理解いただけましたか？

アンダーレイからオーバーレイ
さらにはコンテナやパブリッククラウドまで
できるのはContrailだけ！

- ネットワーク単体プロジェクトにも利用可能なファブリックも
  - 他社ファブリックのような独自実装でなく、オープンでブラックボックス排除
- ファブリックからのオーバーレイやパブリッククラウドの拡張も
  - コンテナの相談や評価も増加中


THANK YOU
JUNIPER NETWORKS
Engineering
Simplicity