NS154

ネットワーク仮想化 最新アップデート
～ NSX-T Data Center 2.5 & vRealize Network Insight 5.0 ～

ヴイエムウェア株式会社
パートナー SE 本部
第一パートナー SE 部
ソリューションエンジニア　千田　霞

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。

Agenda

VMware NSX ポートフォリオ

ネットワークの仮想化を実現する VMware NSX Data Center

ネットワーク仮想化 最新アップデート

- NSX-T Data Center 2.5 アップデート
- vRealize Network Insight 5.0 アップデート

VMware NSX ポートフォリオ

Virtual Cloud Network のプラットフォーム

ネットワークとセキュリティの管理と自動化

クラウドベースの管理　ワークフローの自動化　ブループリント / テンプレート　洞察 / 検出　可視化

VMware vRealize® Network Insight™
エンドツーエンドのネットワークの可視化

VMware vRealize® Automation™
エンドツーエンドのワークロードの自動化

ネットワークとセキュリティの仮想化

セキュリティ　統合　拡張性　自動化　柔軟性

VMware NSX® Data Center
すべてのワークロードにネットワークとセキュリティを提供

VMware NSX® Cloud
クラウドネイティブのネットワークサービス

VMware SD-WAN by VeloCloud®
クラウドネイティブなWAN接続サービス

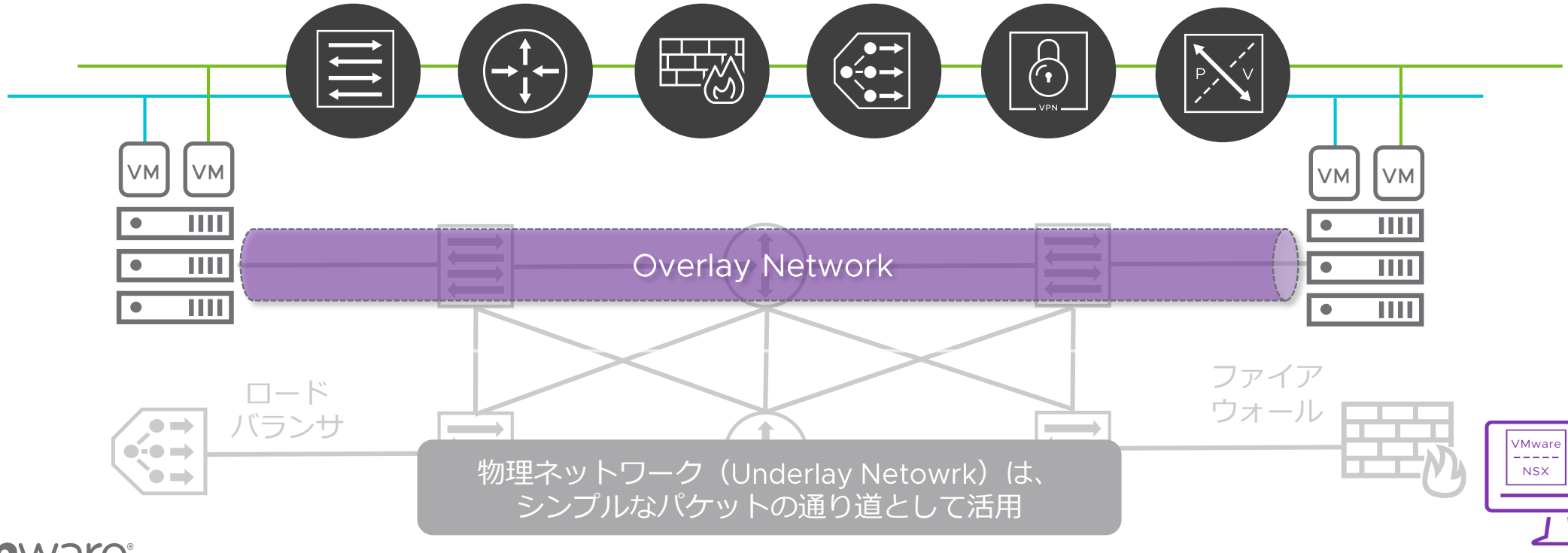
VMware NSX® Hybrid Connect™
データセンターとクラウドのワークロードの移行

VMware AppDefense™
最新のアプリケーションセキュリティ

NSX Advanced Load Balancer
ロードバランスとアプリケーションサービス

ネットワークの仮想化を実現する VMware NSX Data Center

エッジ（サーバ・ハイパーバイザー）側でインテリジェントな機能を実装し、
トンネリングすることで物理ネットワークから分離（オーバーレイネットワーキング）
その上で仮想のネットワークサービスを提供し、ソフトウェアで集中制御する事を実現
物理ネットワークはメーカーを問わず、従来の環境をそのまま利用することも可能



NSX Data Center のラインナップ

2 種類の NSX Data Center

- ソフトウェアベースのネットワーク仮想化
- ソフトウェアベースのオーバーレイ
- 分散ルーティング
- 分散ファイアウォール
- アドバンスド ネットワークサービス
- API による自動化
- Guest Introspection
- Service Insertion

VMware NSX Data Center for vSphere

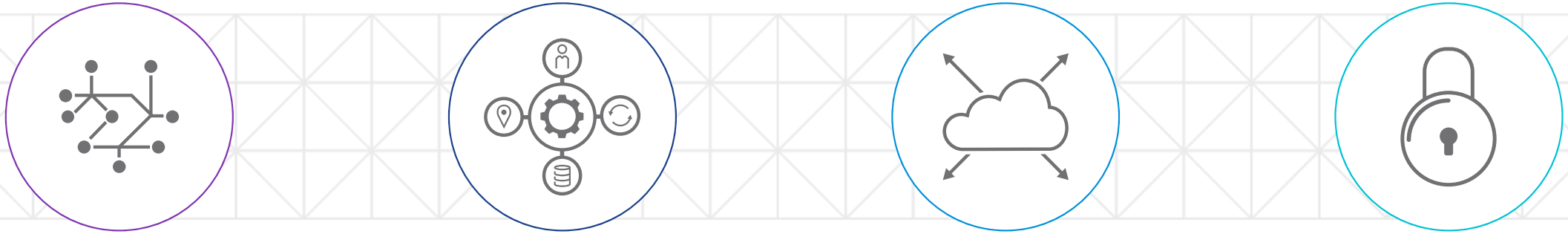
VMware ソリューション郡との密な連携
より高度なセキュリティサービス
パートナーソリューションとの連携・統合

VMware NSX-T Data Center

マルチプラットフォーム – ESXi, KVM
コンテナ環境などの新しいアプリケーションへ対応
（ K8s / PKS / OpenShift ）
パブリッククラウドへの対応（ AWS / Azure ）
ベアメタルサーバーのサポート
より高いパフォーマンスとスケーラビリティ

NSX-T：マルチクラウド時代に向けたネットワークとセキュリティ

仮想マシン、コンテナ、物理サーバ、パブリッククラウドなど様々なプラットフォームに対応

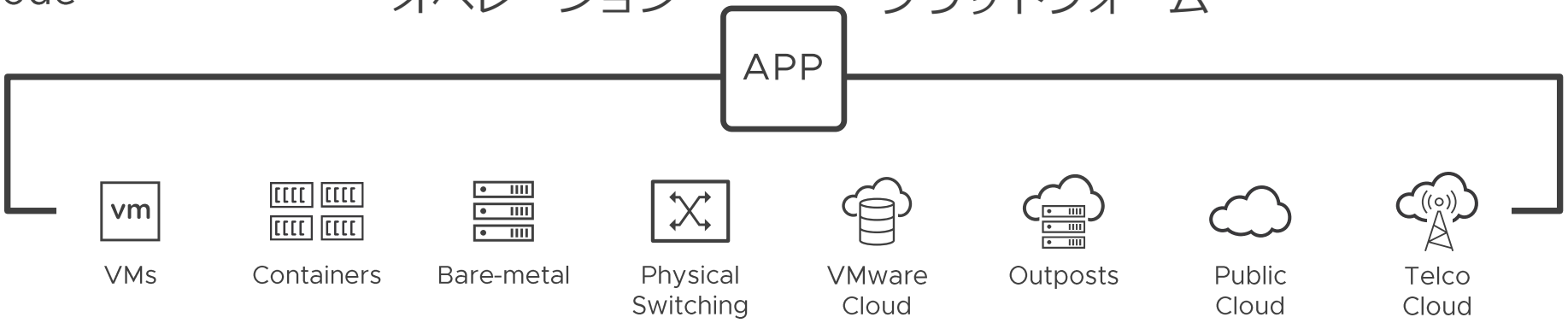


Infrastructure as Code

シンプルで一貫性のあるオペレーション

クラウドスケールプラットフォーム

内包されたセキュリティ



NSX-T Data Center 2.5

最新バージョンのアップデート情報

NSX-T 2.5 アップデート内容

新たな分析と可視化機能、マルチクラウドとセキュリティの向上

分析と可視化

NSX Intelligence による VM およびコンテナのフローベース分析と可視化

クラウド

NSX Cloud に新ポリシーモードを追加

セキュリティ拡張

レイヤー7 , サービス挿入, VPN の機能拡張

運用の簡素化

ファイアウォール操作の簡素化
キャパシティ監視ダッシュボード

コンプライアンス強化

FIPS 140-2

NSX-T 2.5 アップデート内容

新たな分析と可視化機能、マルチクラウドとセキュリティの向上

分析と可視化

NSX Intelligence による VM およびコンテナのフローベース分析と可視化

クラウド

NSX Cloud に新ポリシーモードを追加

セキュリティ拡張

レイヤー7 , サービス挿入, VPN の機能拡張

運用の簡素化

ファイアウォール操作の簡素化
キャパシティ監視ダッシュボード

コンプライアンス強化

FIPS 140-2

NSX Intelligence による分散アナリティクス

全てのパケットレベルを詳細分析し、アプリケーショントポロジーレベルで可視化
マシンラーニングにより、L7FW ポリシーの提案、シュミレーション、自動適用を実現

NSX Intelligence
プラットフォームアプリケーション

モデルと分析を
すべてのホストにプッシュ

NSX Intelligence v1.0

セキュリティとネットワーク分析の進化

v1.0 ”Foundation” リリース

Basic

通信とトポロジーの可視化

Static

プロセス / Flow / パケットを分析し、マイクロセグメンテーションを計画

Dynamic

ネットワーク動作の異常分析、脅威検出

Behavioral

様々な脅威フィードを使用した脅威分析と追求

Predictive

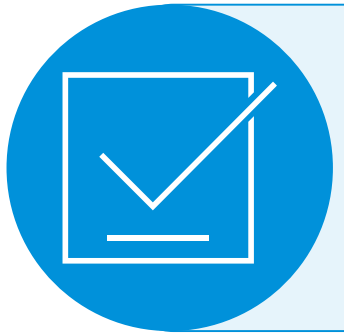
動作と脅威フィードに基づく影響分析と脆弱性マッピング

NSX Intelligence の主要なユースケース

v1.0 リリース

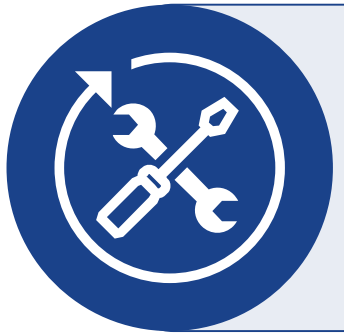
大規模なマイクロセグメンテーション / ファイアウォールの自動化

- ポリシーの管理と実施のためのリポジトリ
- 自動化されたファイアウォールポリシーの推奨
- トポロジーの可視化に更新を伴う継続的でインタラクティブなワークフロー提供



ポリシーコンプライアンスの実証と維持

- すべてのワークロードからのすべてのフローの完全記録
- 誤った構成、ポリシー例外、ワークロードまたはセキュリティスコープ間の非準拠フローを強調表示、および相関フローとポリシー
- 継続的分析



セキュリティインシデントのトラブルシューティングを簡素化

- セキュリティチーム向けの包括的なトラフィックの可視性
- アプリケーションマップと完全なワークロードインベントリを組み合わせたドリルダウンのトポロジーの可視化
- サンプリングなしで、すべてのフローのレイヤー7 分析

NSX-T 2.5 アップデート内容

新たな分析と可視化機能、マルチクラウドとセキュリティの向上

分析と可視化

NSX Intelligence による VM およびコンテナのフローベース分析と可視化

クラウド

NSX Cloud に新ポリシーモードを追加

セキュリティ拡張

レイヤー7 ,
サービス挿入,
VPN の機能拡張

運用の簡素化

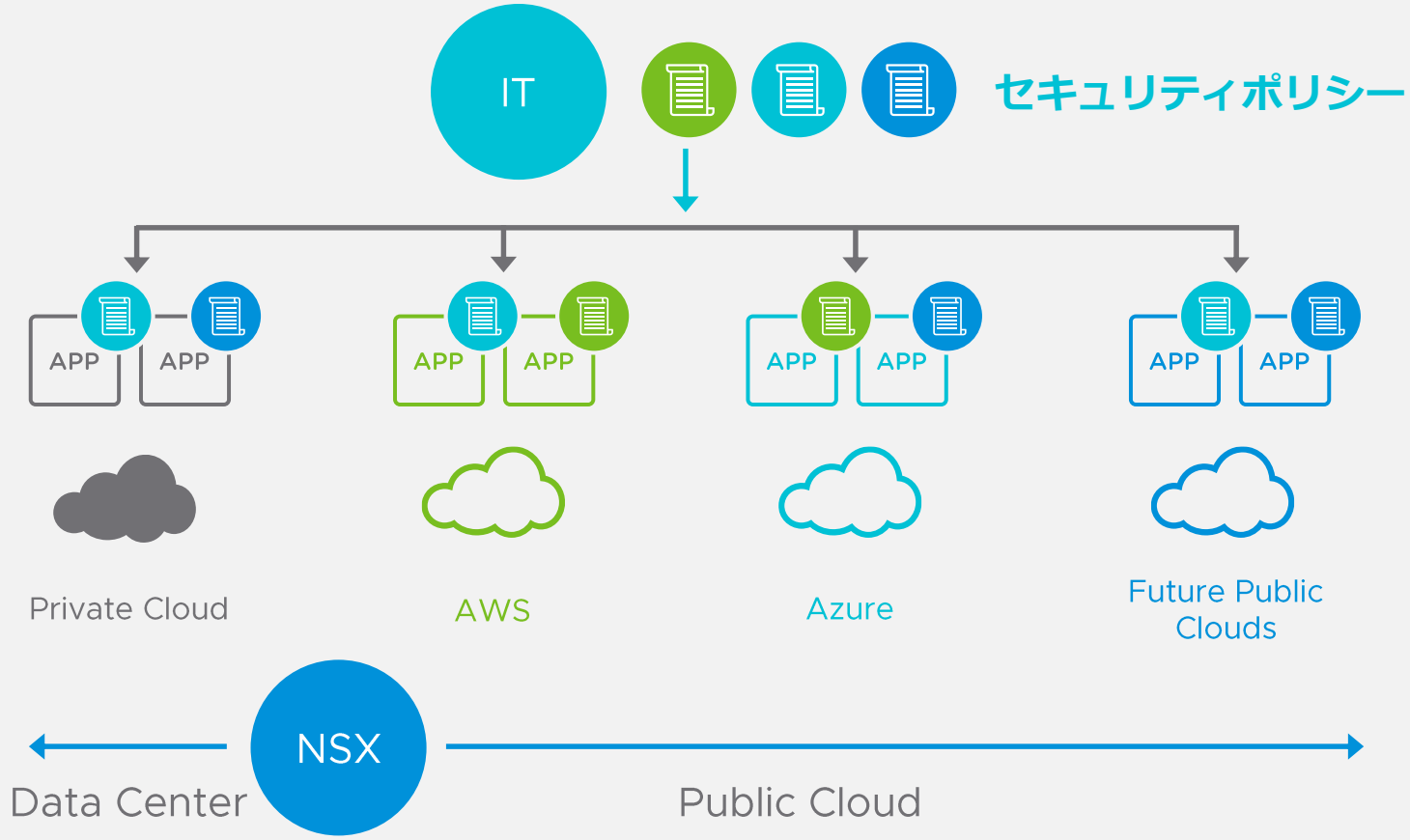
ファイアウォール操作の簡素化
キャパシティ監視ダッシュボード

コンプライアンス強化

FIPS 140-2

NSX Cloud : パブリッククラウドのネットワークサービス

NSX-T Data Center のセキュリティポリシーをパブリッククラウドまで拡大



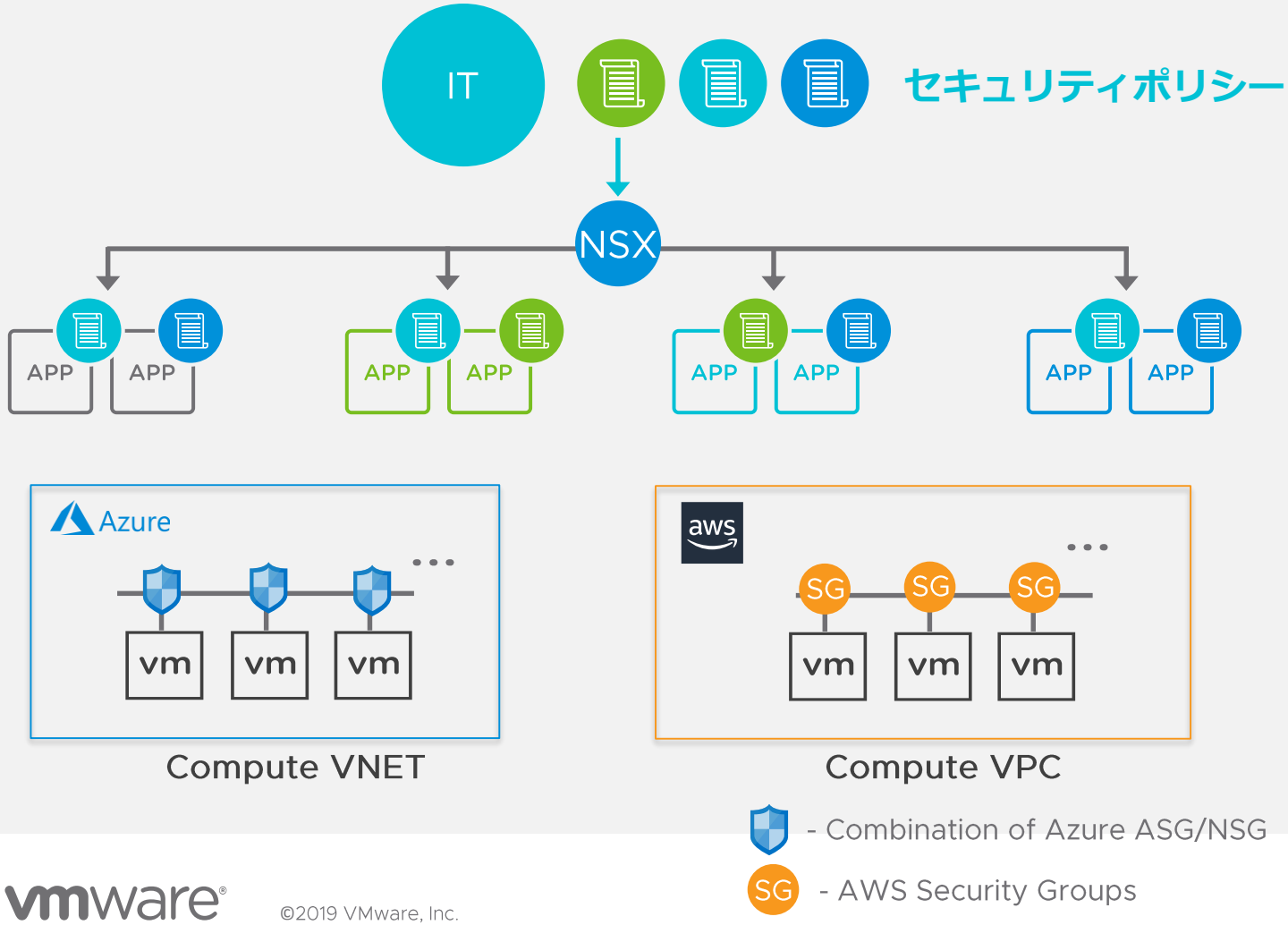
- 一つのセキュリティポリシー
  - 一度の定義でどこでも適用

L4 セキュリティとマイクロセグメンテーション

- 豊富な抽象化セット
- ポリシーをアプリケーションワークロードに細かく適用
- 動的なセキュリティグループ

NSX Cloud の新たなセキュリティポリシーモード

エージェントレスの Native Cloud 強制モード



機能

NSX で定義したセキュリティポリシーを、ネイティブクラウドのセキュリティポリシーに変換し、VM へ適用*

*可能な限り最高の範囲

メリット

ネイティブクラウドの VM に NSX Tools のインストールが不要

すべてのオペレーティングシステムをサポート

NSX Cloud の強制モード

柔軟な 2 つのクラウドポリシー強制をサポート

Native Cloud 強制モード (New)

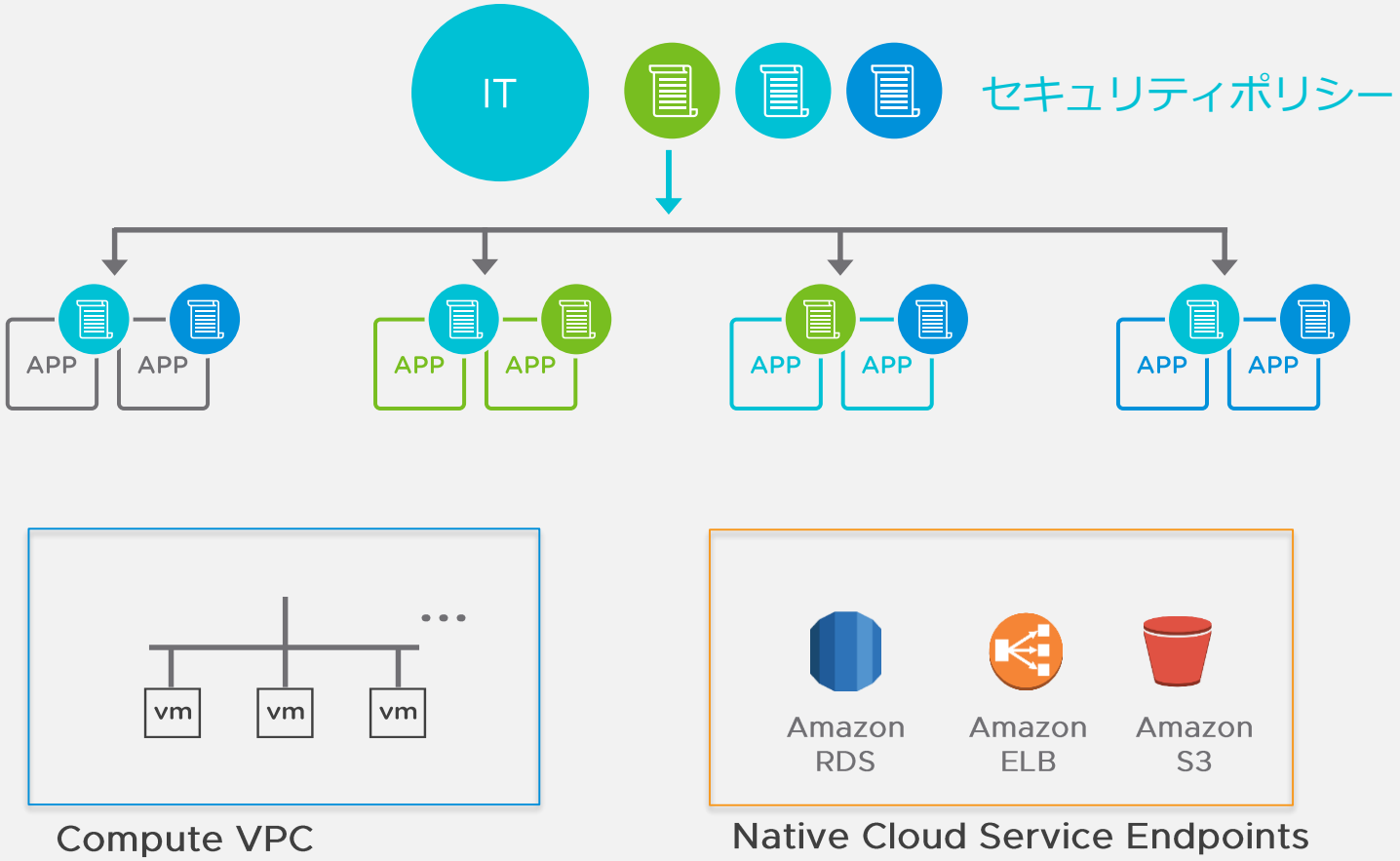
- NSX ポリシーをネイティブのクラウド固有のセキュリティポリシーに変換することにより、**一般的なポリシーフレームワーク**を提供
- エージェントレス（ NSX Tools 不要 ）
- クラウドプロバイダーのポリシーによる制限あり

NSX 強制モード

- NSX Tools 内で NSX ポリシーが実施される**一貫したポリシーフレームワーク**を提供
- NSX Tools のインストールが必須
- クラウドプロバイダーのポリシーによる制限なし

サービス検索と制御

単一のセキュリティポリシーによってクラウドサービスへのアクセスを制御



機能

S3、ELB、RDS などのクラウドネイティブサービスエンドポイントを VPC / VNET 内で自動的に検出して保護

メリット

NSX Cloud からネイティブクラウドサービスの可視化とセキュリティを制御

NSX-T 2.5 アップデート内容

新たな分析と可視化機能、マルチクラウドとセキュリティの向上

分析と可視化

NSX Intelligence による VM およびコンテナのフローベース分析と可視化

クラウド

NSX Cloud に新ポリシーモードを追加

セキュリティ拡張

レイヤー7 ,
サービス挿入,
VPN の機能拡張

運用の簡素化

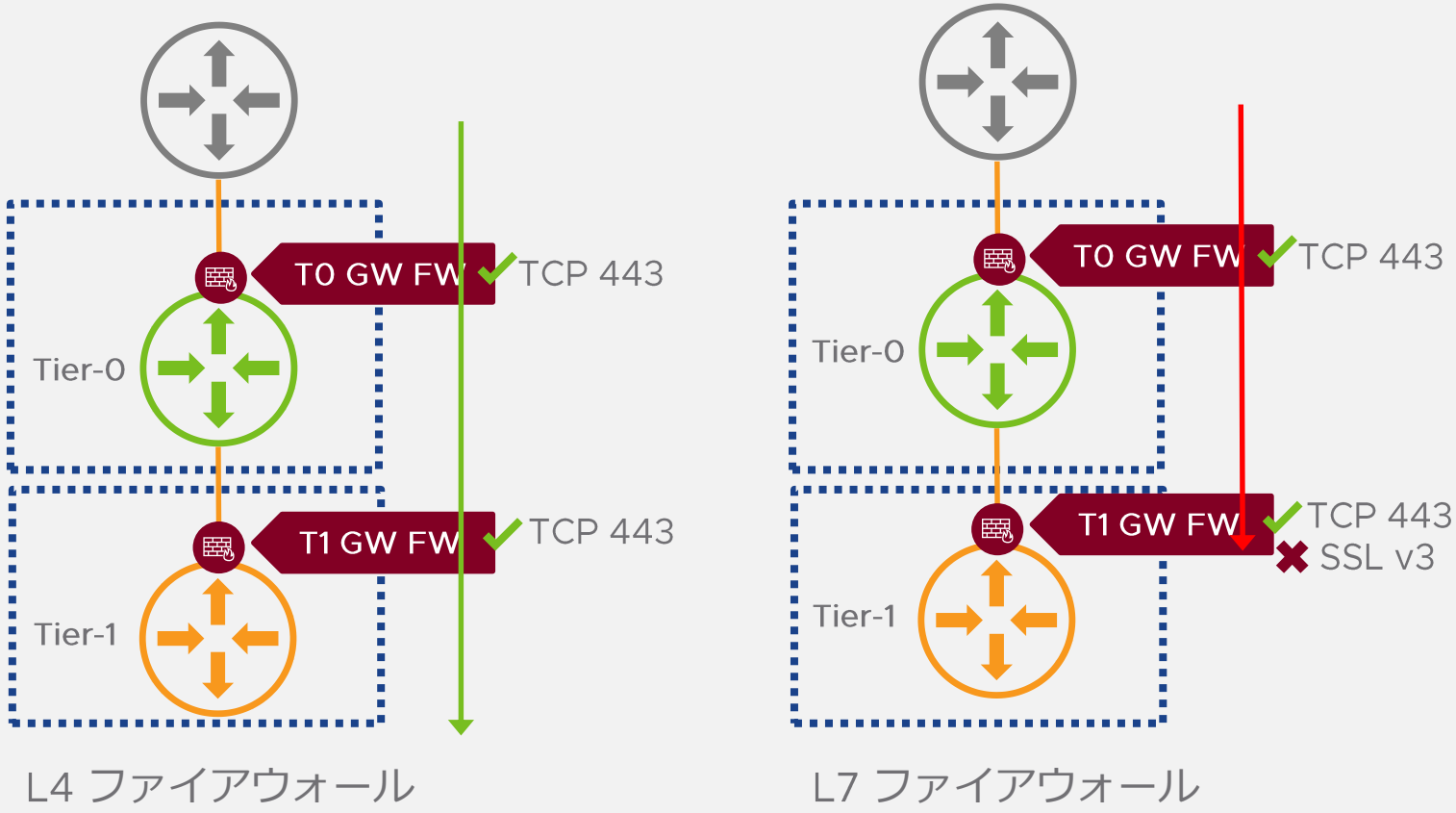
ファイアウォール操作の簡素化
キャパシティ監視ダッシュボード

コンプライアンス強化

FIPS 140-2

NSX-T セキュリティの向上

ゲートウェイファイアウォールのレイヤー 7 App-ID サポート



機能

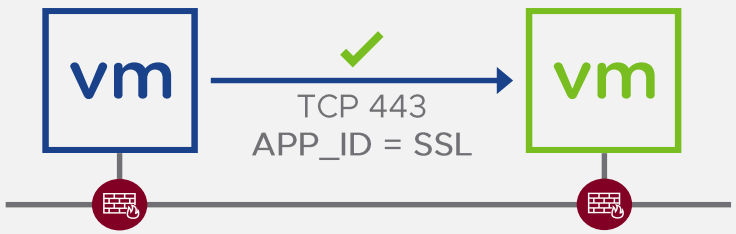
Tier-1 ゲートウェイでポートに依存しないレイヤー L7 ファイアウォール（ App-ID ）をサポート

- 以前は L2 – L4 のみ
- コンテキストプロファイル経由でルールを使用
- Tier-0 ゲートウェイでは未サポート
- バージョン / 暗号化スイートサポート

NSX-T セキュリティの向上

KVM の分散ファイアウォールでのレイヤー 7 App-ID サポート

L4 ファイアウォール



L7 ファイアウォール

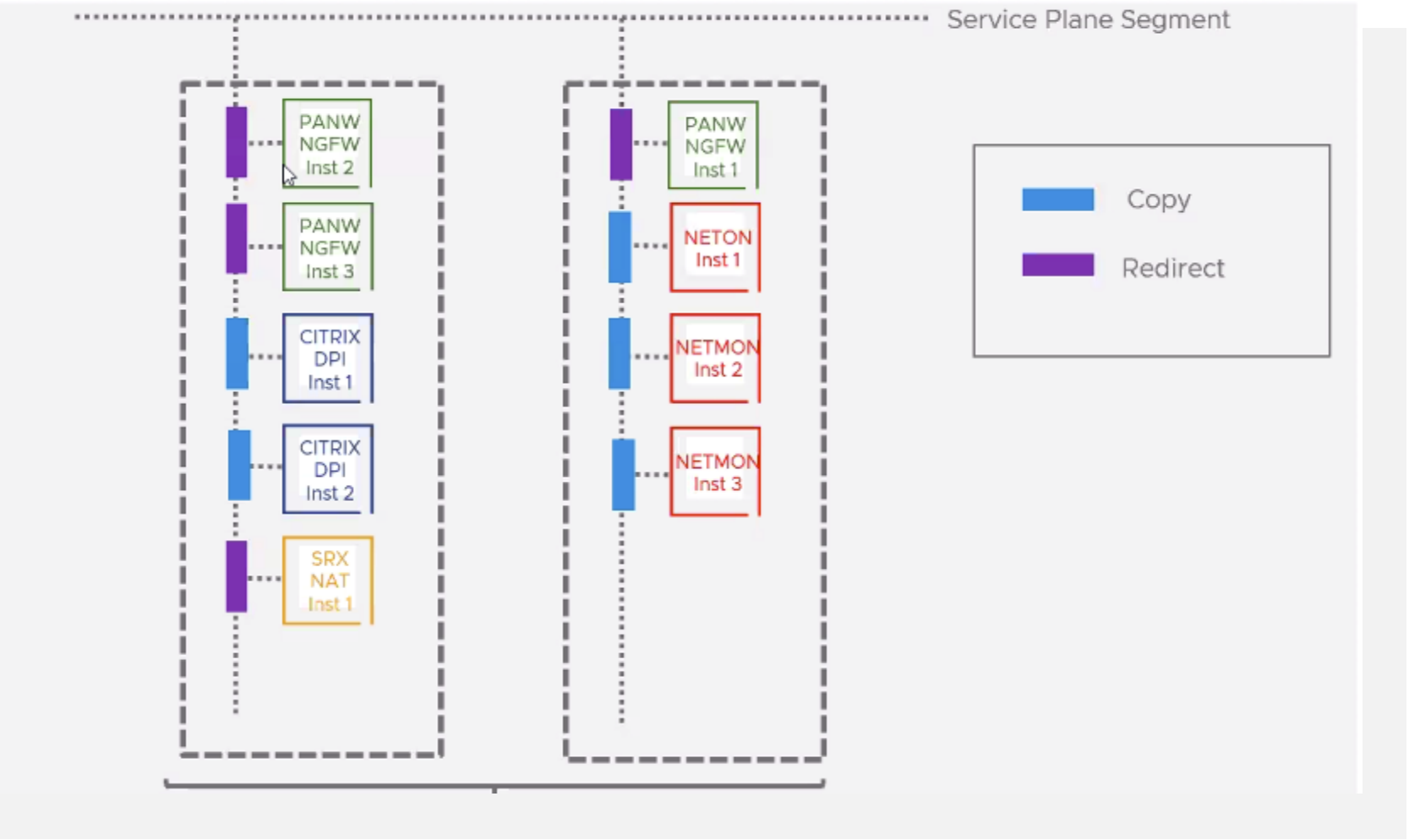
機能

East – West（ VM 間 ）通信でポートに依存しないレイヤー L7 ファイアウォール（ App-ID ）をサポート

- 以前の ESXi のみから機能拡張
- コンテキストプロファイル経由でルールを使用
- バージョン / 暗号化スイートは KVM では未サポート

パートナーインテグレーション

East – West サービス挿入 : パートナー仮想マシン（ SVM ）へのパケットコピーサポート



機能

リダイレクトに加えて SVM への
パケットのコピーをサポート

リダイレクトまたはコピーは、
サービス登録時にベンダーによって
定義

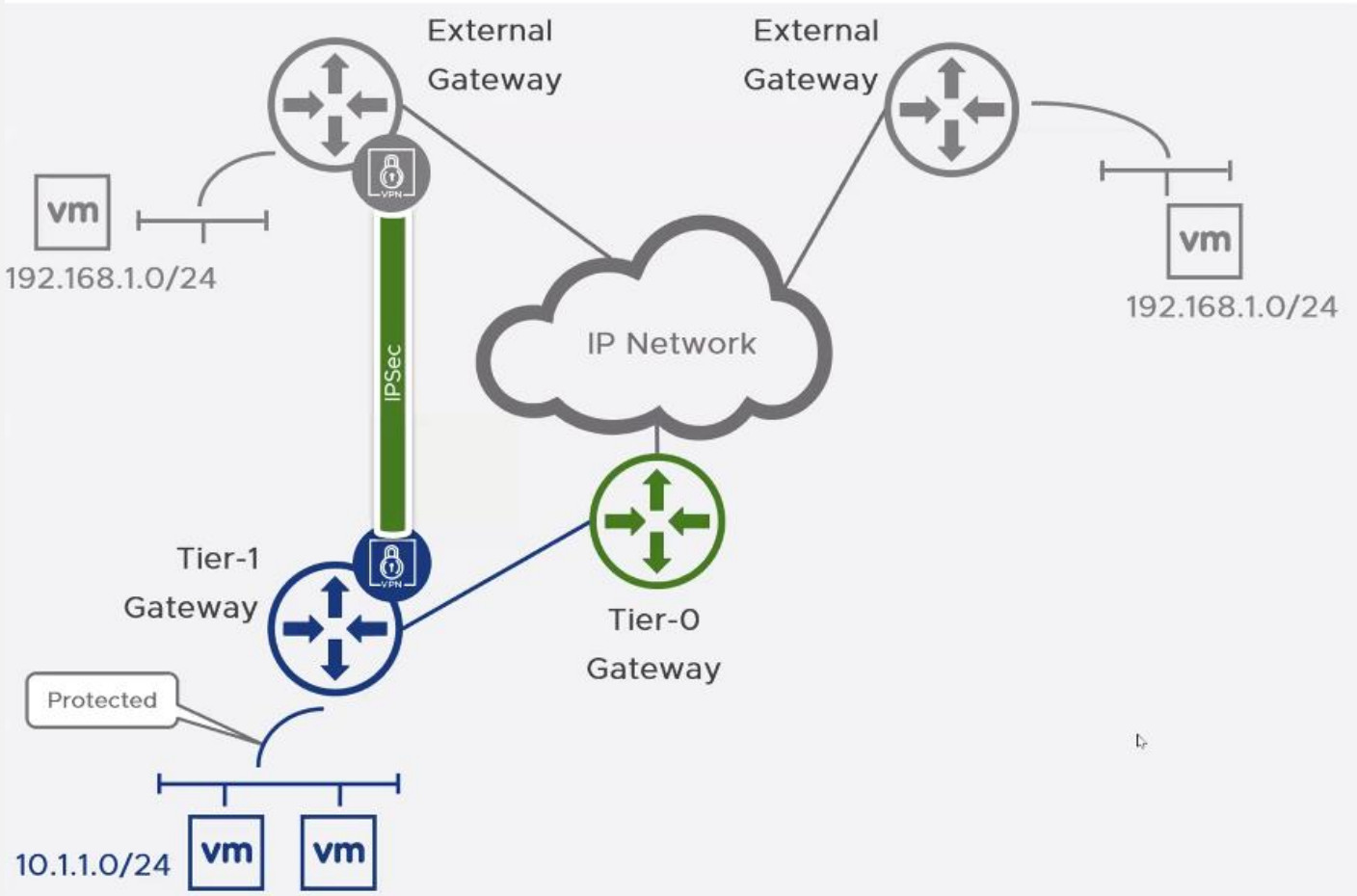
メリット

セキュリティ分析やネットワーク
モニタリングソリューションを
有効化

- インスペクション
- モニタリング
- 統計収集

マルチテナント用の VPN 拡張

Tier-1 ゲートウェイで IPSec VPN が利用可能に



機能

Tier-1 ゲートウェイ上の IPSec VPN をサポート

- 以前は Tier-0 ゲートウェイのみ
- ポリシーベースとルートベースの両方をサポート

メリット

より柔軟な IPsec VPN トポロジーの構成が可能に

- マルチテナント
- テナントで管理される VPN

NSX-T 2.5 アップデート内容

新たな分析と可視化機能、マルチクラウドとセキュリティの向上

分析と可視化

NSX Intelligence による VM およびコンテナのフローベース分析と可視化

クラウド

NSX Cloud に新ポリシーモードを追加

セキュリティ拡張

レイヤー7 , サービス挿入, VPN の機能拡張

運用の簡素化

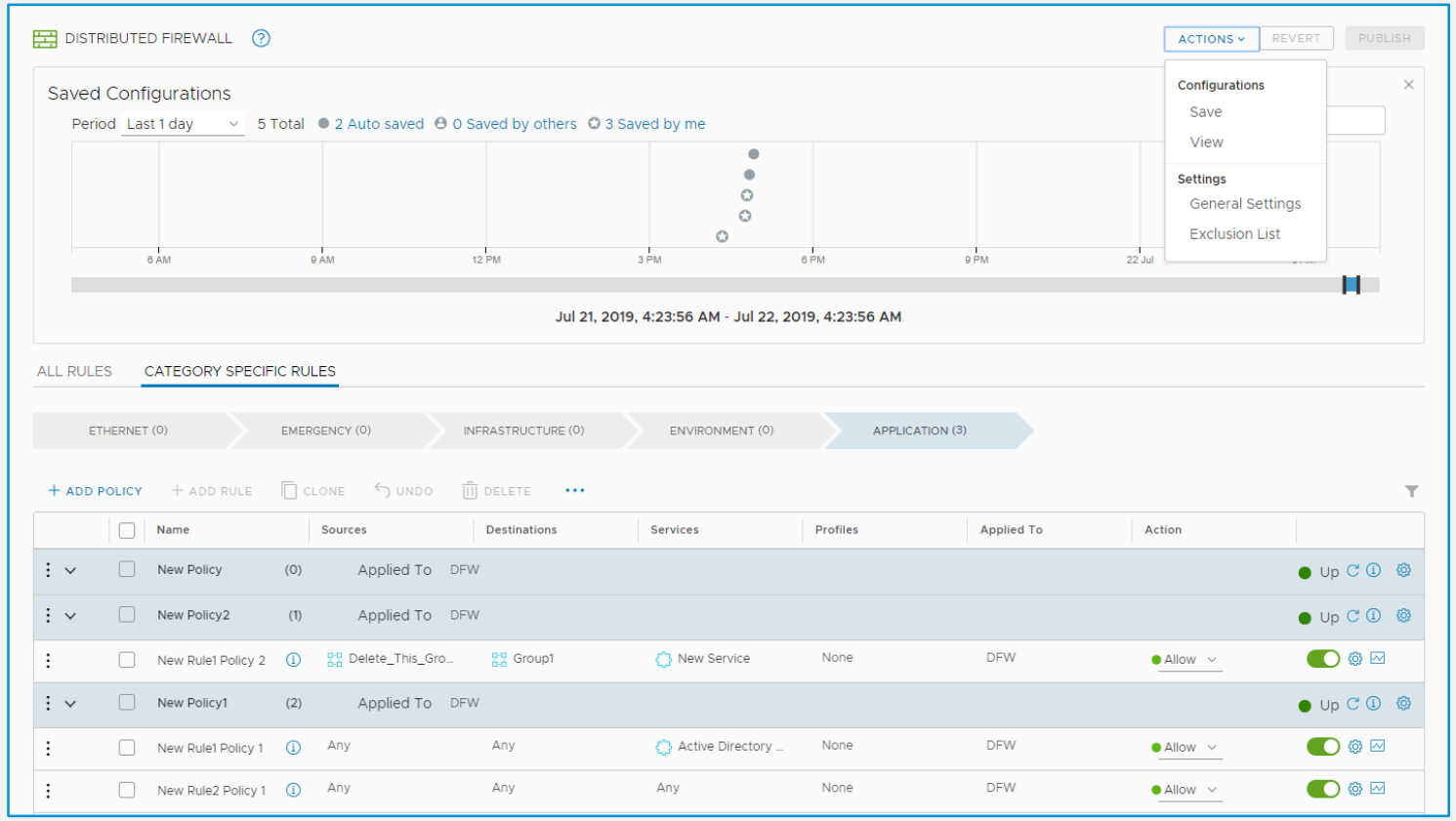
ファイアウォール操作の簡素化
キャパシティ監視ダッシュボード

コンプライアンス強化

FIPS 140-2

運用の簡素化

ファイアウォールの運用性が向上



機能

- 構成自動保存
- マルチユーザー ロッキング & ドラフティング
- 自動ドラフトの有効化 / 無効化
- ロールバックの拡張

メリット

より柔軟な IPsec VPN トポロジーの構成が可能に

- マルチテナント
- テナントで管理される VPN

NSX-T 2.5 アップデート内容

新たな分析と可視化機能、マルチクラウドとセキュリティの向上

分析と可視化

NSX Intelligence による VM およびコンテナのフローベース分析と可視化

クラウド

NSX Cloud に新ポリシーモードを追加

セキュリティ拡張

レイヤー7 ,
サービス挿入,
VPN の機能拡張

運用の簡素化

ファイアウォール操作の簡素化
キャパシティ監視ダッシュボード

コンプライアンス強化

FIPS 140-2

コンプライアンスの強化

FIPS においては UI / API を使用したコンプライアンスステータスレポートの生成が可能に

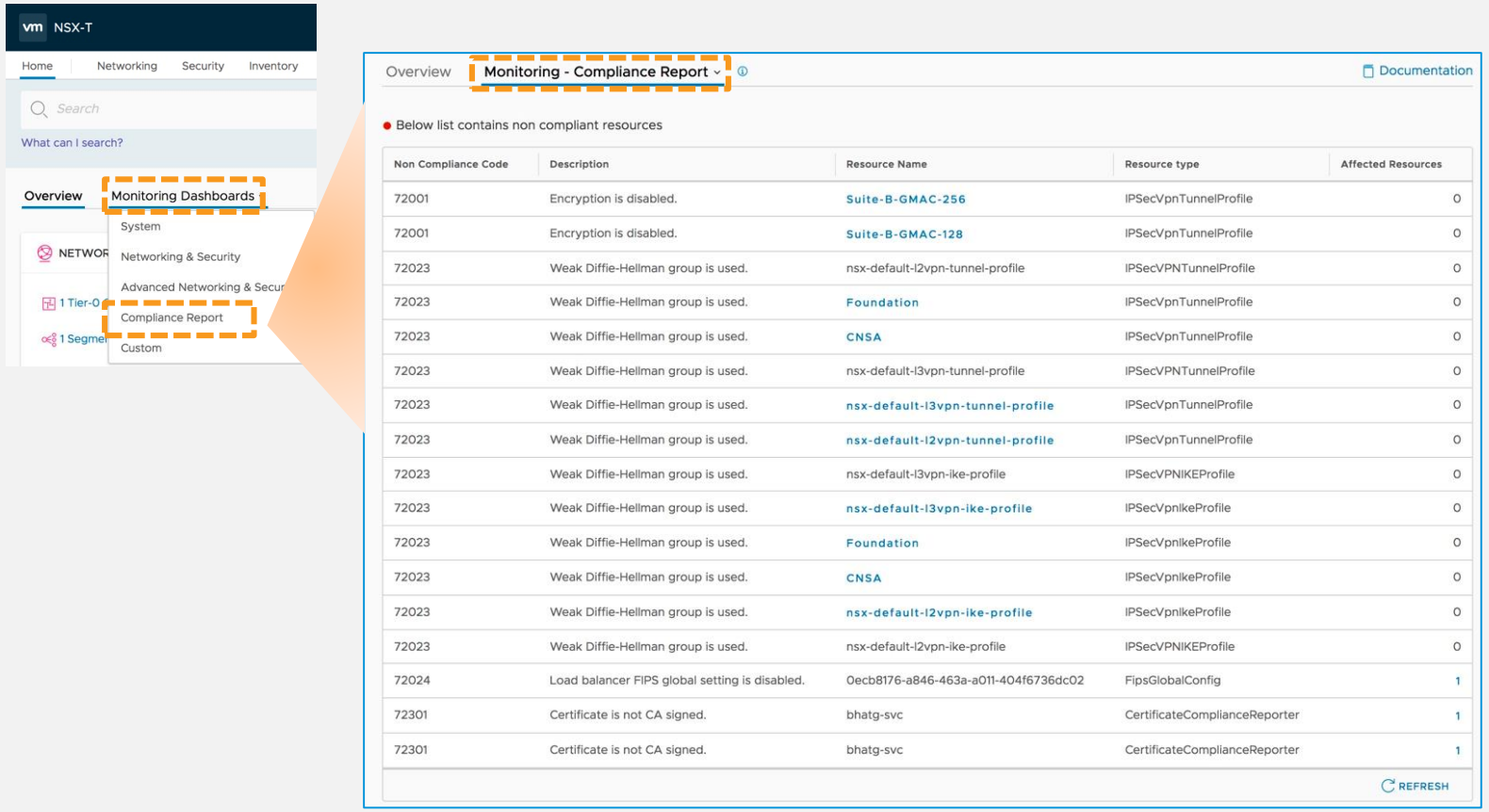
NSX-T 2.5 で認定

評価保証レベル(EAL) 4

ステータス：“評価中”

FIPS コンプライアンス
ステータス & レポート

Compliance Status Report API: GET https://<nsx-t-mgr>/policy/api/v1/compliance/status



機能

NSX-T は FIPS 140-2 対応

- Uses FIPS 140-2 validated cryptographic modules

UI / API を使用してコンプライアンスステータスレポート生成

デフォルトでは FIPS non-compliance モードで LB ルールが稼働、API を使って有効化

メリット

特別な連邦政府に厳格なコンプライアンスチェックを顧客に提供

プラットフォームのセキュリティ保証を提供

vRealize Network Insight 5.0

最新バージョンのアップデート情報

vRealize Network Insight と vRealize Network Insight Cloud

データセンターからクラウド、ブランチまで、
アプリのセキュリティとネットワーク接続の検出、最適化、トラブルシューティング

ネットワーク

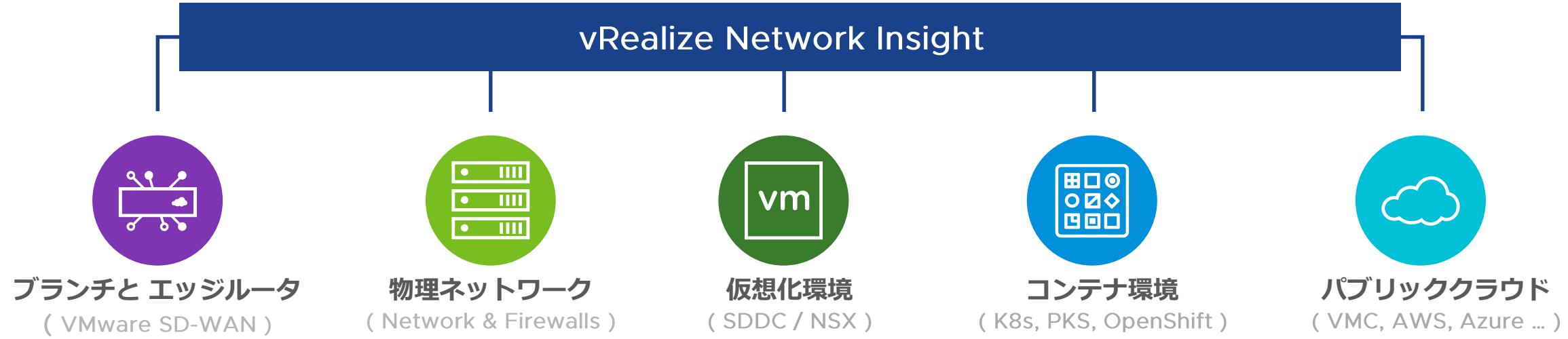
- エンドツーエンドのトラブルシューティング、トラフィック、通信経路の分析
- アプリケーション遅延とネットワークパフォーマンス

セキュリティ

- トラフィック可視化とアプリケーションのモデリング
- 運用、変更 / 監査、コンプライアンス

アプリケーション

検出、キュレーション、運用

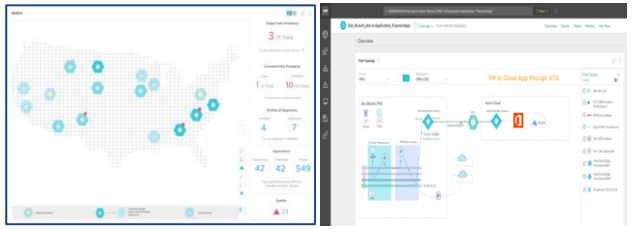


NSX Intelligence と vRNI / vRNI Cloud それぞれの役割

組み合わせることで包括的なエンドツーエンドセキュリティを提供

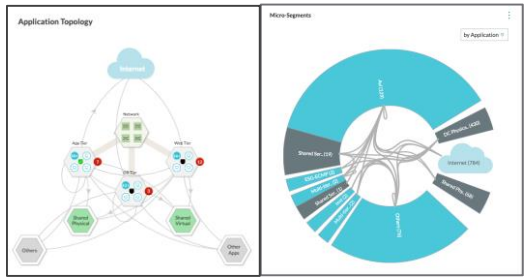
vRealize Network Insight ユースケース

アプリのセキュリティとネットワーク接続の検出、最適化、トラブルシューティング



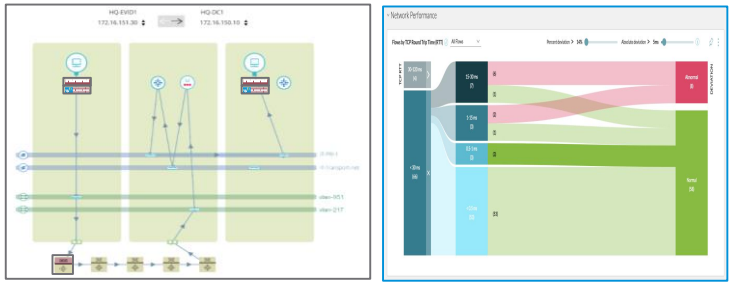
ネットワーク可視化を促進

- ハイブリッドクラウドと SD-WAN の可視化: NSX, VMC, AWS, Azure, VeloCloud
- オーバーレイネットワークとアンダーレイネットワーク間の接続の検出
- ハイブリッドクラウド全体のトラフィックとアプリを分析



セキュリティとクラウドの移行計画

- アプリ（ VM、コンテナ ）の検出、トラフィックパターンの特定
- セキュリティ計画：ファイアウォールポリシー、マイクロセグメンテーション推奨
- ハイブリッドアプリケーション（ VM、コンテナ、クラウド間）のセキュリティのトラブルシューティング

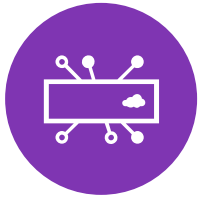


物理と仮想ネットワークの最適化とトラブルシューティング

- アプリケーション接続の問題である MTTR を削減
- ネットワークのボトルネックを排除して、アプリケーションのパフォーマンスを最適化
- 大規模な NSX 環境の管理・運用

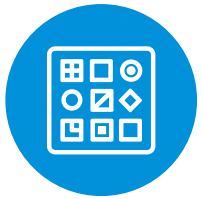
VMware vRealize Network Insight 5.0 アップデート概要

What's New?



VMware SD-WAN by VeloCloud

- データセンターからクラウド、ブランチの可視化
  - ダッシュボード、サイト、アプリおよびフロー分析
  - 通信経路を可視化とホットスポットの検出



Kubernetes

- Kubernetes ネットワークパストレース
- ワークロード間の接続問題に対する
  トラブルシューティング

Azure パブリッククラウド

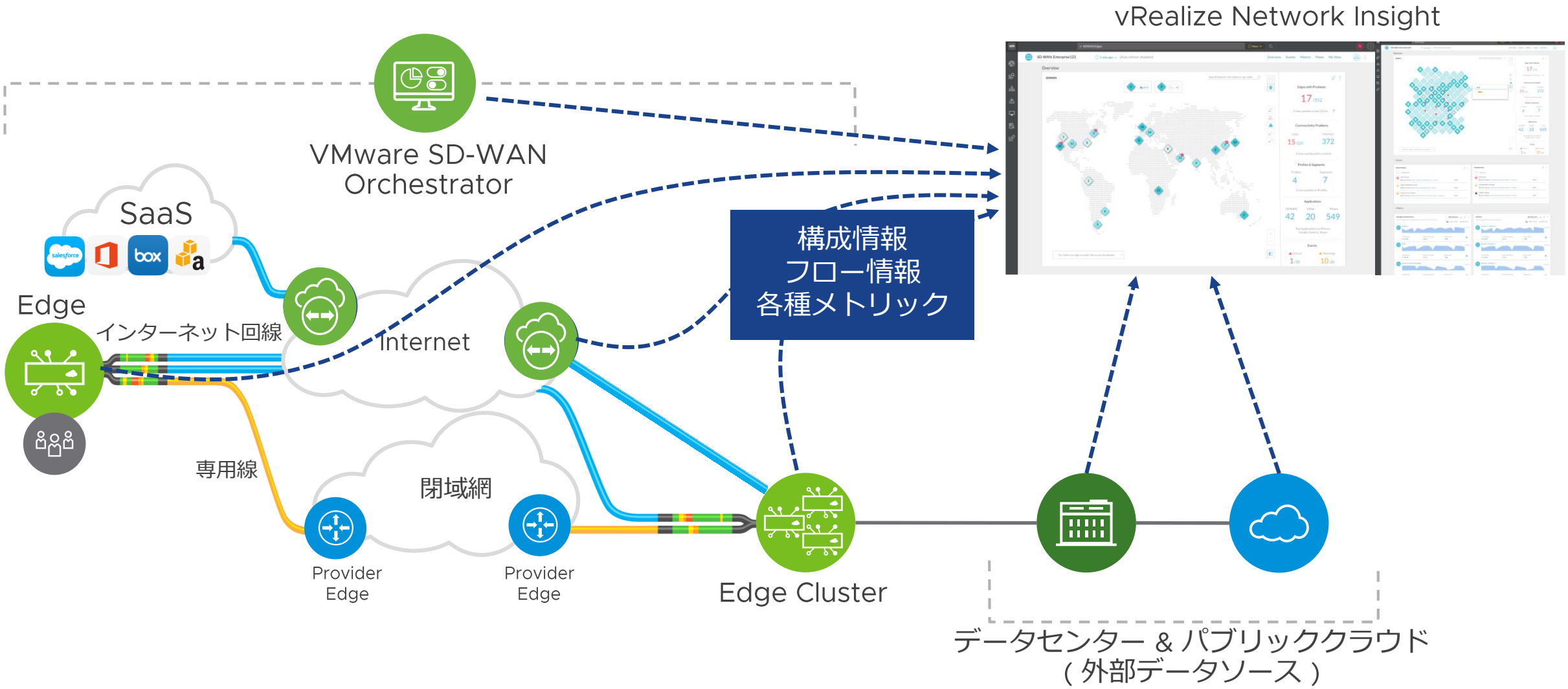
- 可視化/分析の範囲をパブリッククラウドまで
  - ダッシュボード、セキュリティプランナー、
    フロー分析
  - プロアクティブなネットワークトラフィック分析
    （外れ値、しきい値、トップトーカー）

ストリーミングテレメトリ

- ネットワークに流れる Streaming Telemetry
  を直接収集が可能に

VMware SD-WAN の可視化とトラブルシュート

データセンターからクラウド、ブランチまで



VMware SD-WAN の可視化とトラブルシュート

データセンターからクラウド、ブランチまで

アプリケーション可用性

- 健全性
- ダッシュボードの提供:
  - アプリケーション(レイヤー7 検出)
  - サイト、エッジ(ハブ)、ゲートウェイ

フロー分析とセキュリティ計画

- 体感品質
- セグメンテーション可視化
- 利用アプリケーション
- 通信量の多いエッジ
- 回線の品質低下

キャパシティ管理

- 全体利用状況
- 回線のしきい値
- Link Thresholds
- 使用状況に基づくアラート

すべての通信経路の可視化

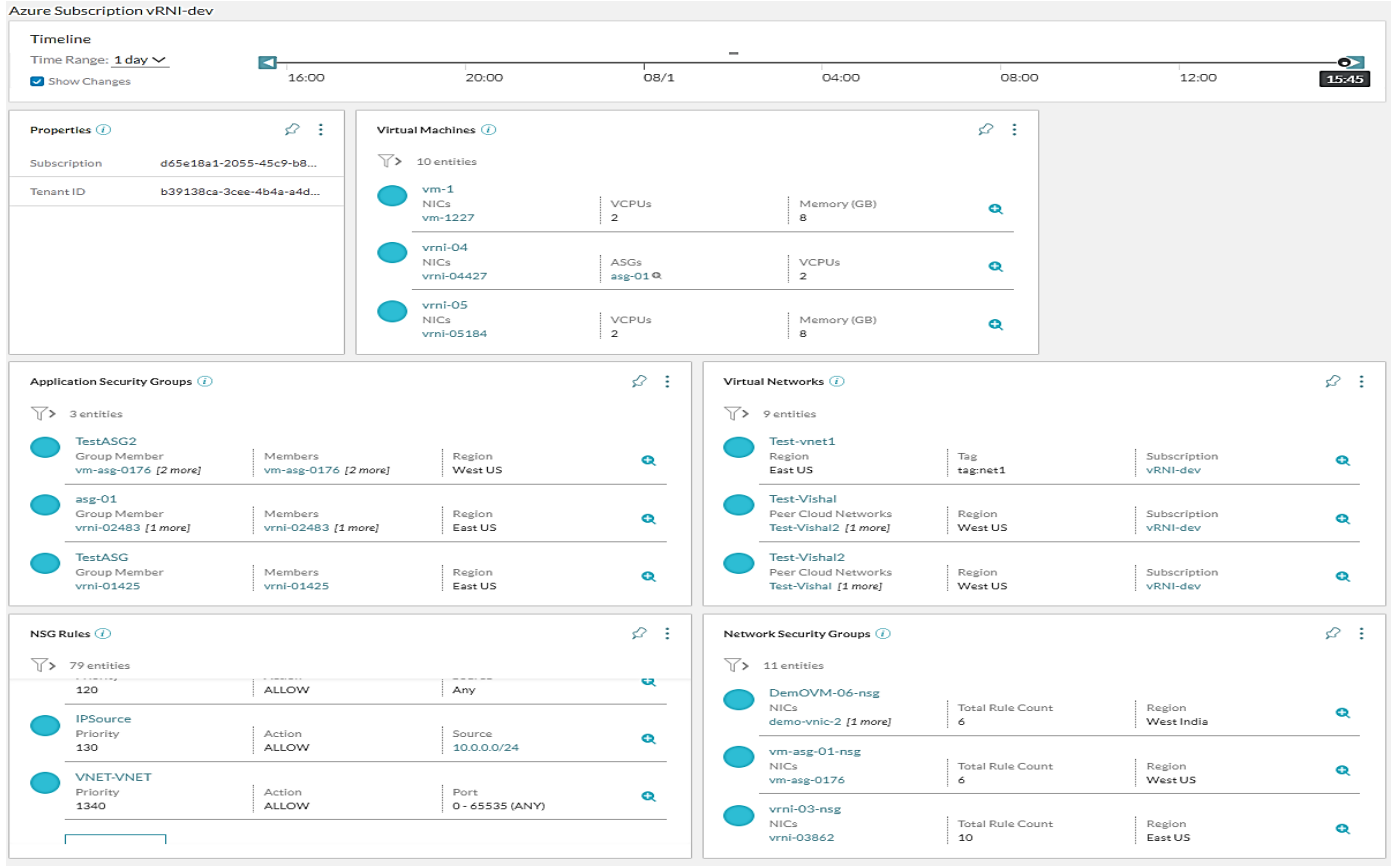
- Edge からデータセンター、クラウドまでのトポロジーをプロット
- すべてのネットワークコンポーネントを可視化し、潜在的な問題を特定

Microsoft Azure
パブリッククラウドの可視性も強化

- パブリッククラウドでは
  AWS , VMware Cloud on AWS に加えて
  新たに **Microsoft Azure** をサポート

- 含まれる機能:
  - ダッシュボード（サブスクリプション / Vnet, NSG, ASG, VM, サブネットなど)
  - アプリケーション依存関係のマッピング
  - アプリケーションセキュリティ計画
  - フロー分析（ Internet, Intranet と ハイブリッド VNET ）
  - ネットワークフローの分析（エレファントフロー, トップトーカー, しきい値, 外れ値)

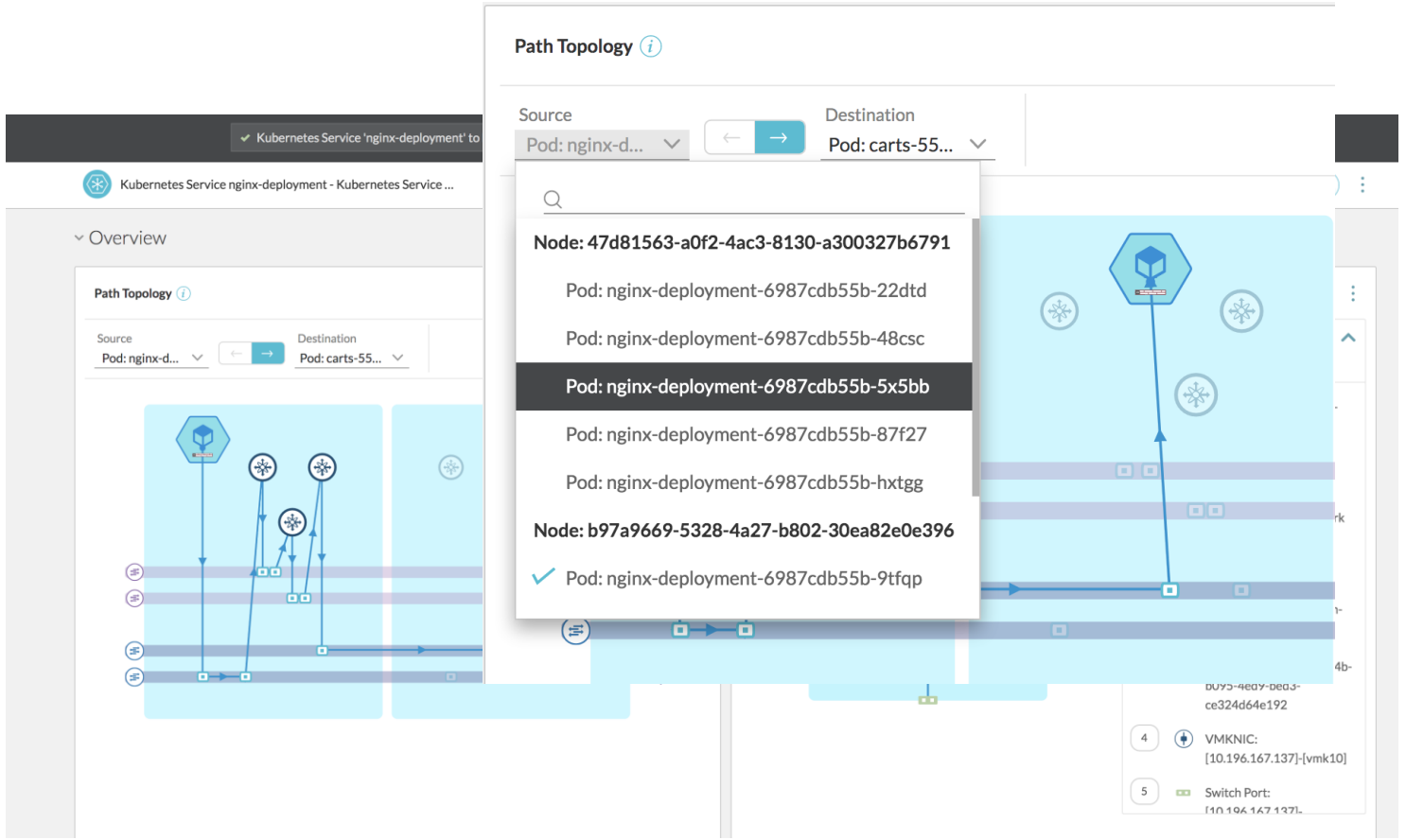
Microsoft Azure



Kubernetes
コンテナネットワークの可視化にも対応

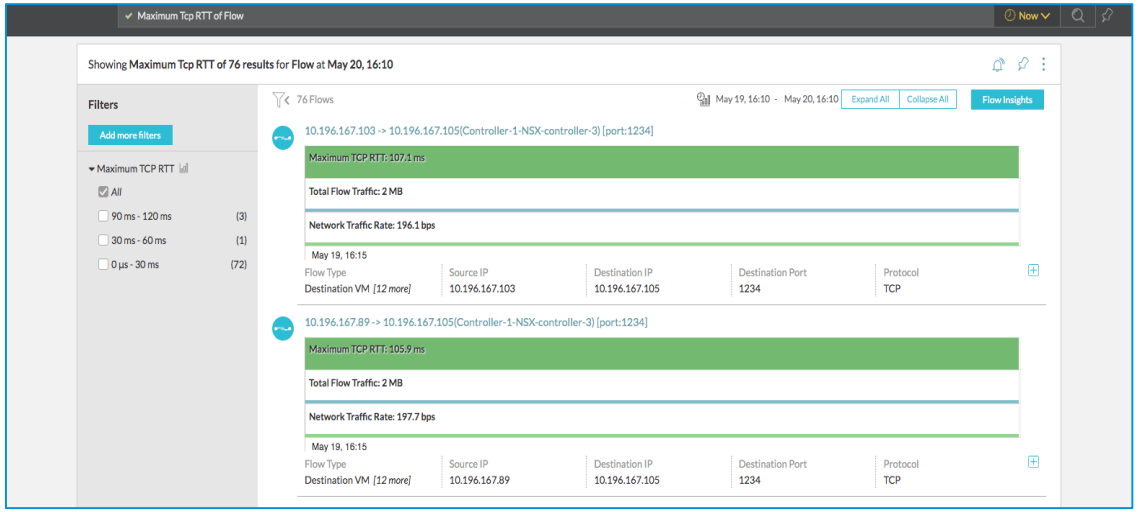
- 新たに Kubernetes 環境に対応

- 含まれる機能 :
  - Kubernetes ポッドとサービス間のネットワーク経路
  - NSX のコンポーネント
  - ネットワーク経路の問題を強調表示

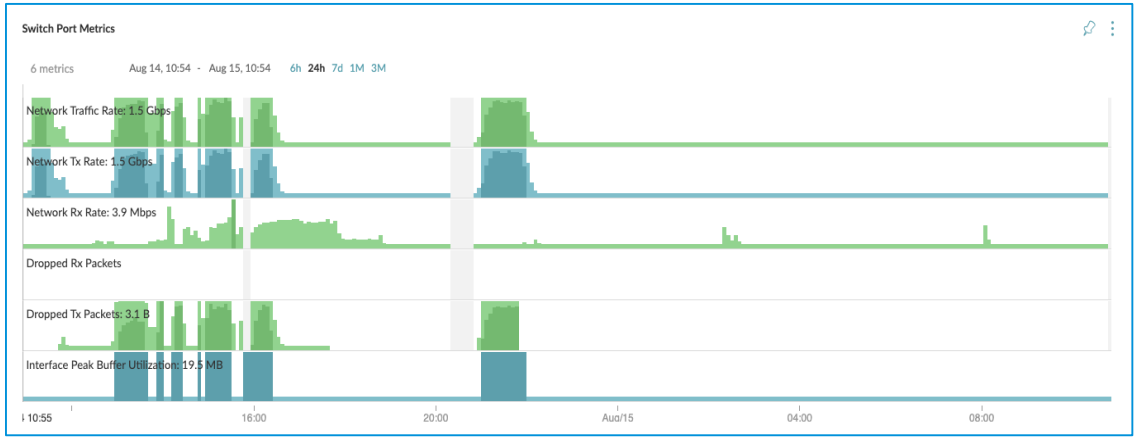


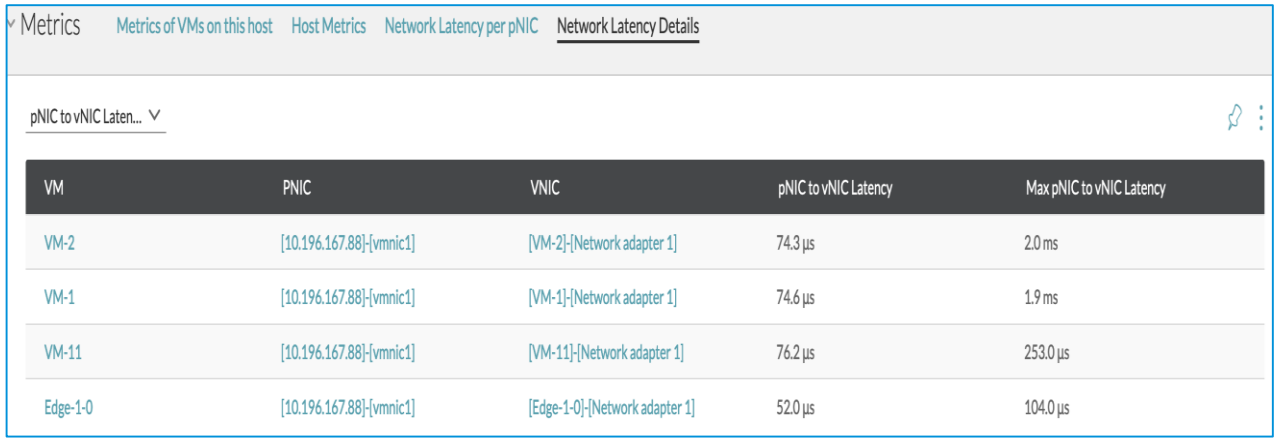
Day2 運用 : ストリーミングテレメトリ

フローのラウンドトリップタイム（ RTT ）: NSX のメトリック、異常フロー検出



レイテンシメトリック : NSX がレポートする vNIC と pNIC のレイテンシを vRNI が集約し分析





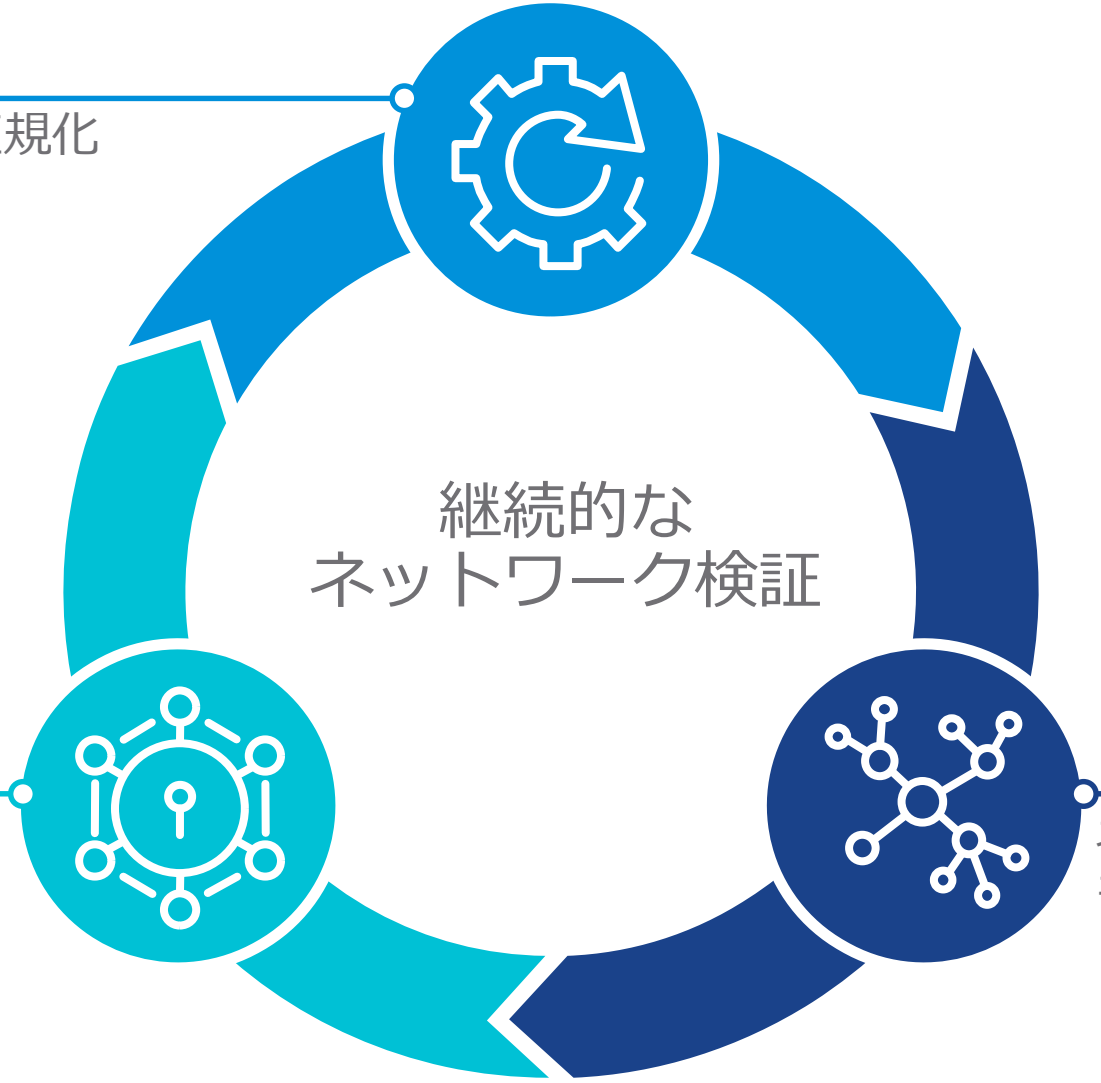
VM	PNIC	VNIC	pNIC to vNIC Latency	Max pNIC to vNIC Latency
VM-2	[10.196.167.88]-[vmnic1]	[VM-2]-[Network adapter 1]	74.3 µs	2.0 ms
VM-1	[10.196.167.88]-[vmnic1]	[VM-1]-[Network adapter 1]	74.6 µs	1.9 ms
VM-11	[10.196.167.88]-[vmnic1]	[VM-11]-[Network adapter 1]	76.2 µs	253.0 µs
Edge-1-0	[10.196.167.88]-[vmnic1]	[Edge-1-0]-[Network adapter 1]	52.0 µs	104.0 µs

Veriflow 統合による vRealize Network Insight の今後

継続的なネットワークのモデリングと検証

Step 1

ネットワーク状態の収集と正規化



Step 2

ネットワーク全体の挙動を
モデル化し予測、仮設を立てる

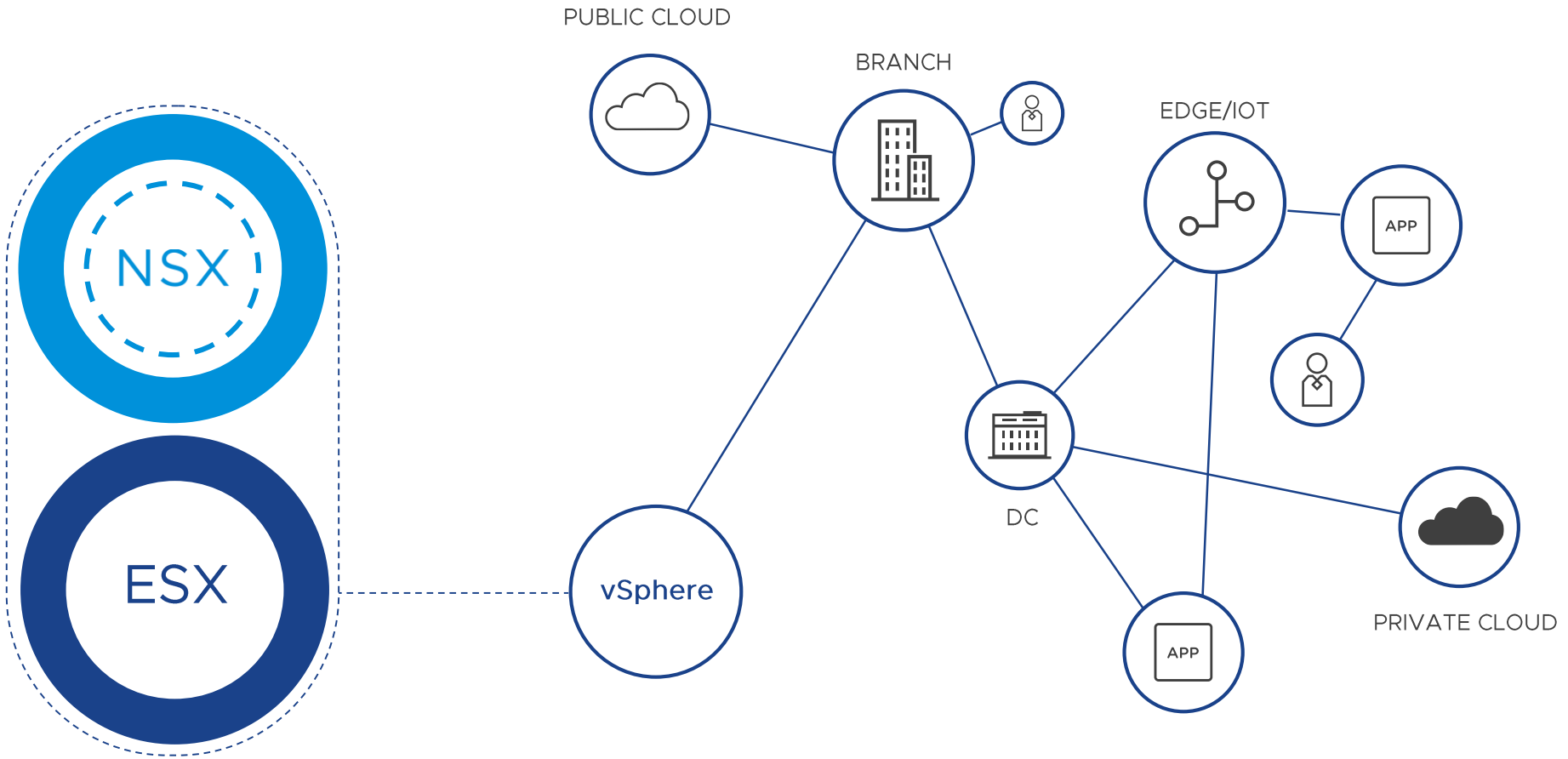
Step 3

回復力とセキュリティの
検証と分析

本セッションのまとめ

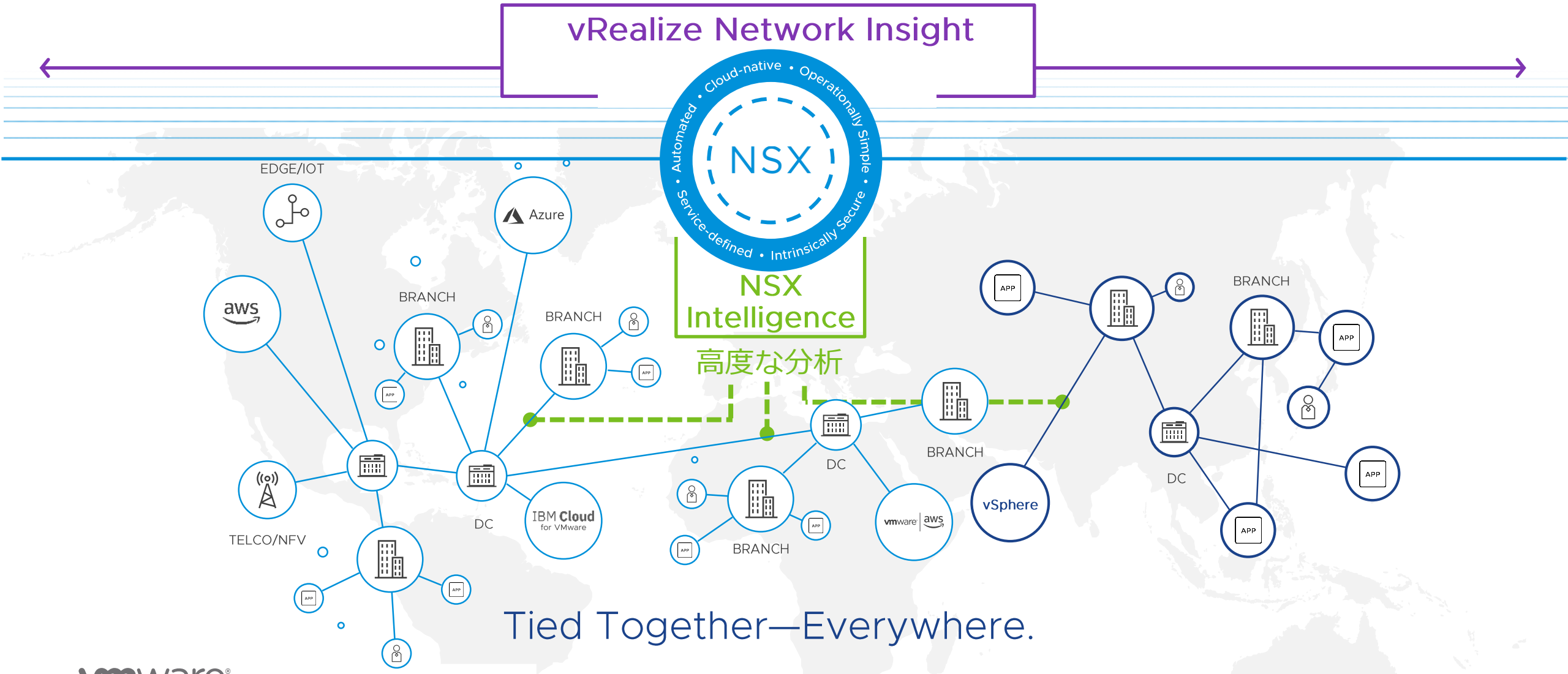
NSX の進化

すべてのプラットフォームとワークロードにネットワークとセキュリティを提供



Virtual Cloud Network と vRealize Network Insight

エンドツーエンドの可視化



Tied Together—Everywhere.

ご清聴、ありがとうございました

vmware®