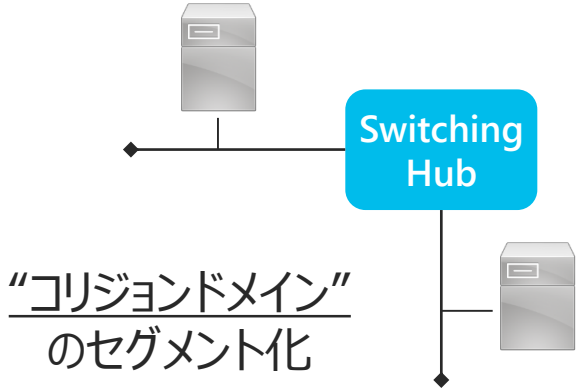
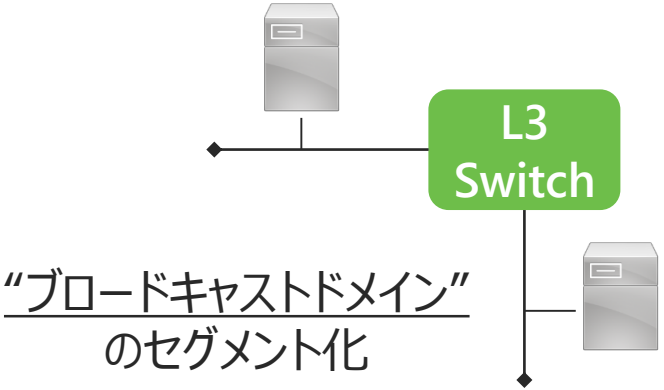
30分でわかるマイクロセグメンテーション

～導入における障壁と成功へのキーポイント～

セキュリティー事業
テクニカルソリューションアーキテクト
満江　貴之
June 4th 2020

“マイクロセグメンテーション”って何？ ~昔話~

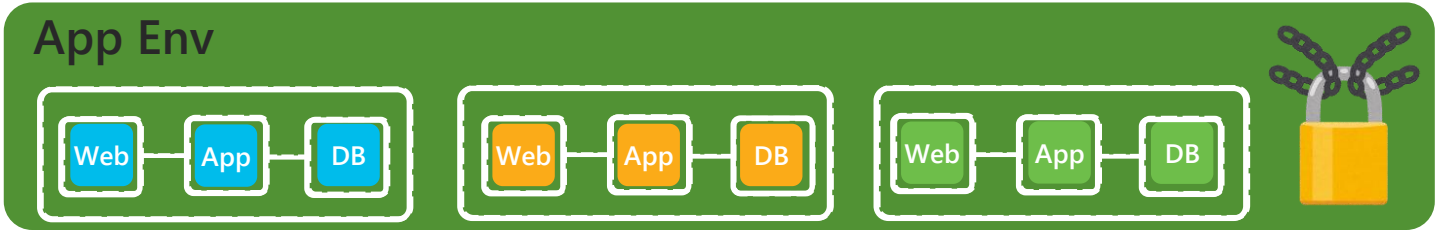




パフォーマンスの向上

障害時の影響範囲低減

“マイクロセグメンテーション”って何？ ~現在~



- アプリケーションを構成する最小の単位(セグメント)まで論理的に分割
- セグメント間の通信内容を必要最低限で定義(ホワイトリストポリシーの策定)
- ホワイトリストを執行して不要な通信を排除(ホワイトリストポリシーの執行)

アプリケーションワークロードの
“保護”(セキュリティ向上)

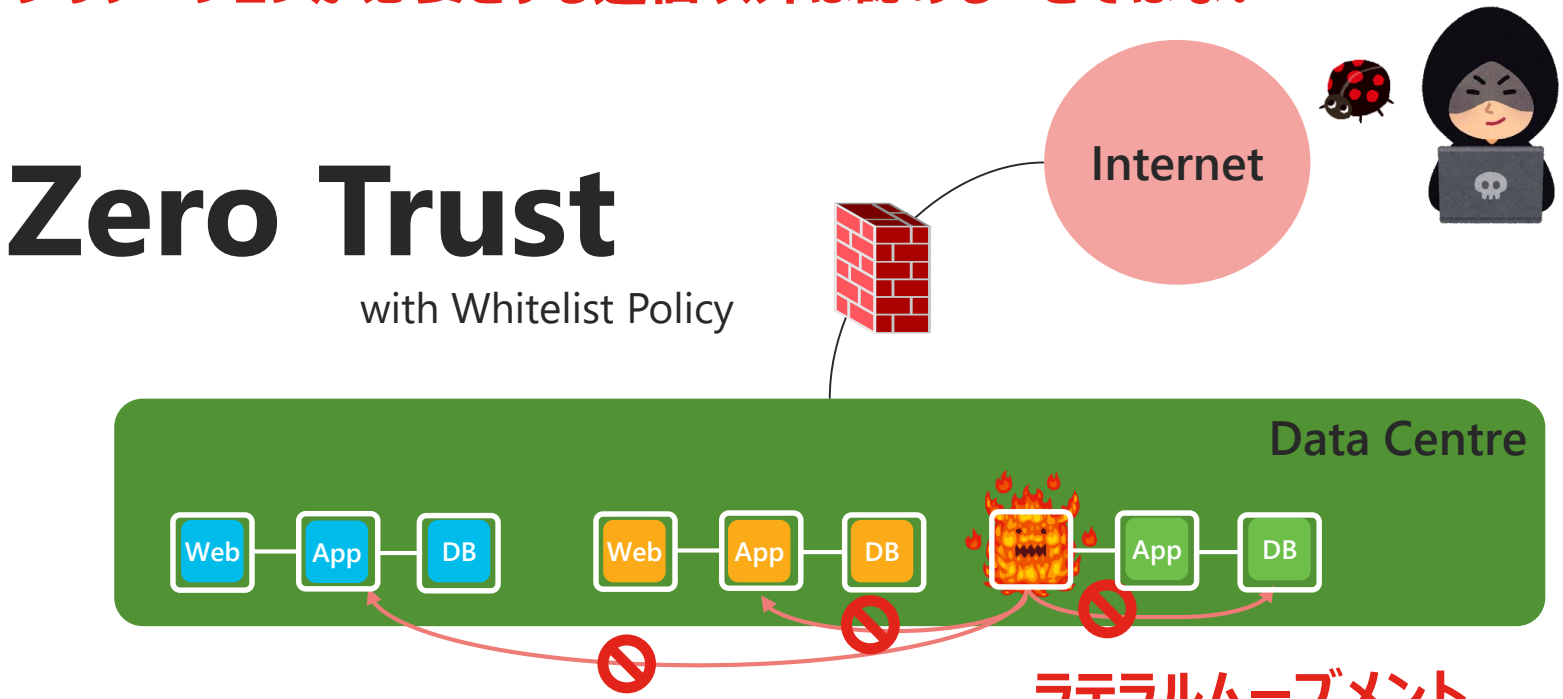
目的は？？？

ラテラルムーブメント

を防ぎたい

ラテラルムーブメントを防ぐには？

アプリケーションが必要とする通信以外は認めるべきではない



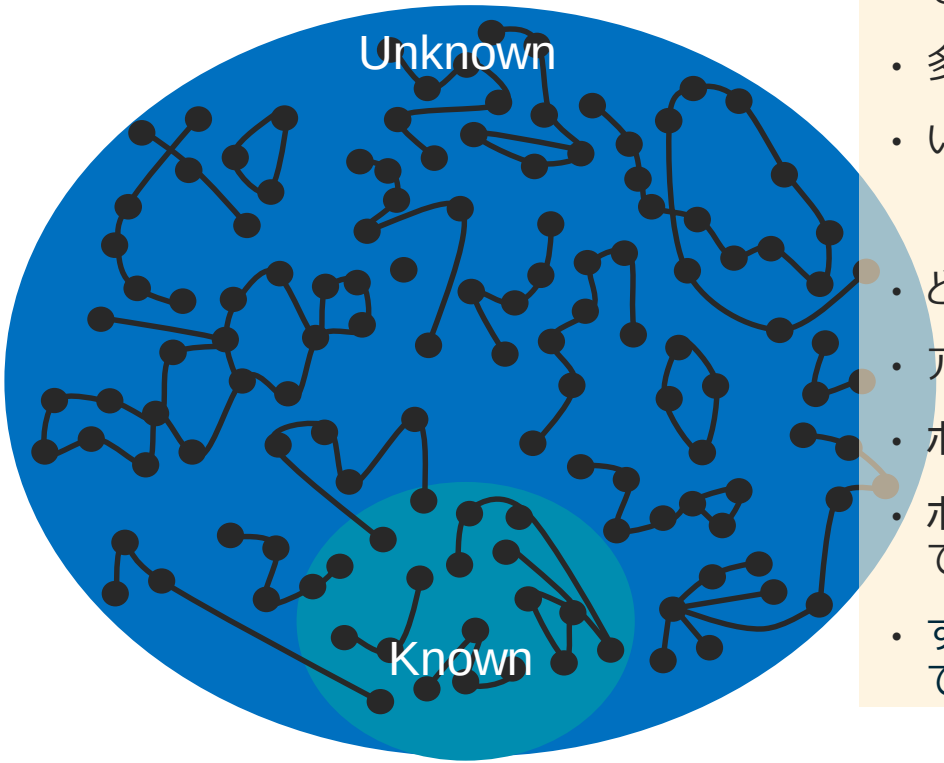
言うは易く行うは難いマイクロセグメンテーション

Firewallや従来の手法で実現するのが非常に難しい

- ホワイトリストポリシーの作成(発見)が困難
- ポリシーの維持と管理の難しさ
- 今やアプリケーションはどこでも動く・・

そもそも正しいポリシーを作成できますか？

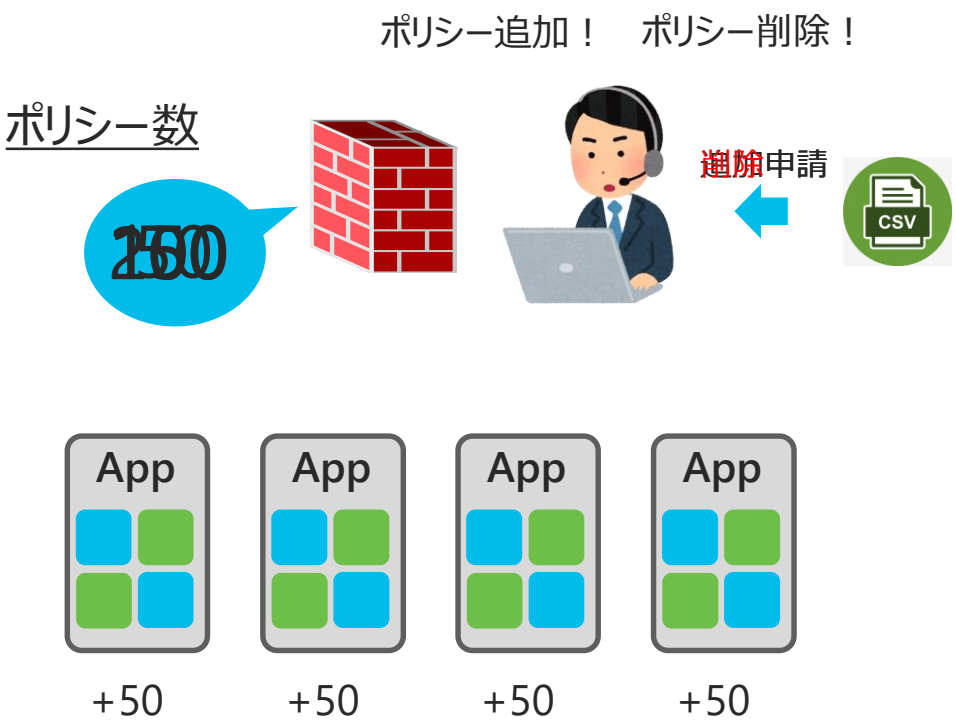
従来のオンプレミスDCの視点



- そもそも現状が理解できていない
- 多数のアプリケーション
- いろんな担当者の要件をどうまとめるか

  NW・基盤・セキュリティ管理ポリシー、アプリ通信要件
- どの組織がどの範囲を面倒みるべき？
- アプリ毎に異なるポリシーとその粒度
- ホワイト ＆ ブラックリスト 両方必要
- ポリシー単位をIPサブネットやSDNのグループで一意に表現できない
- すべての要件をNWチームに集約、IPアドレスをFWにまとめて記載し続ける？（非常にアナログな手法）

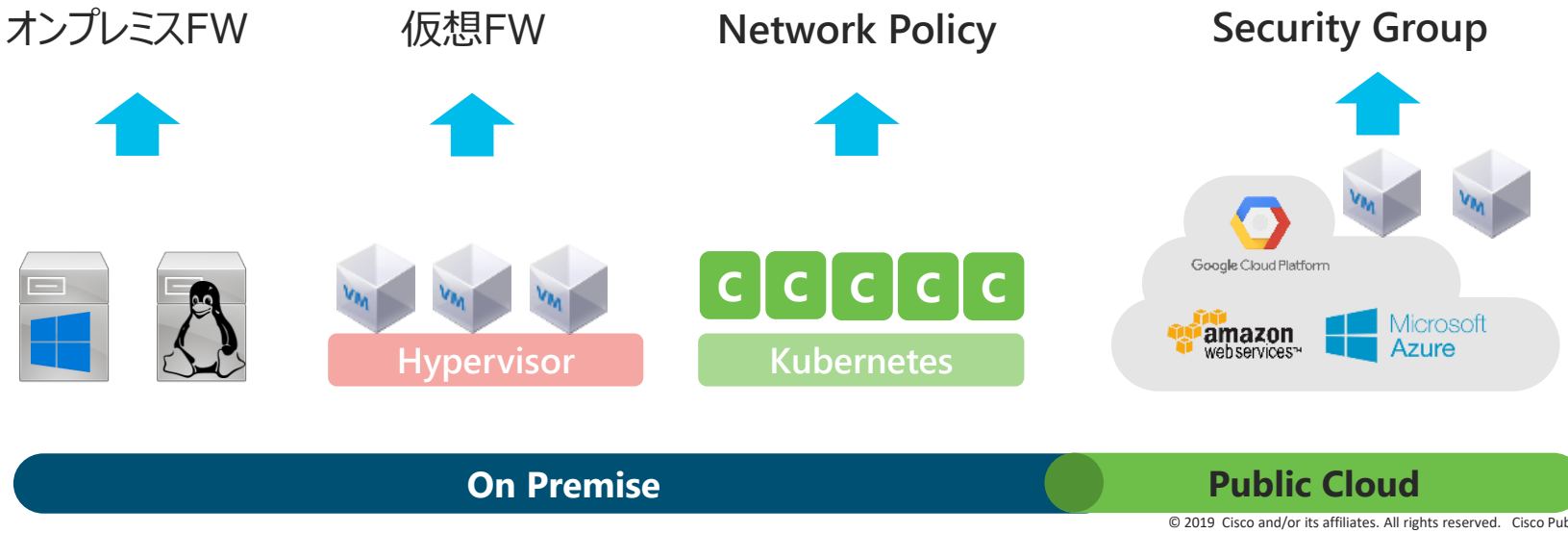
ポリシーの維持と管理の難しさ



- クラウドやコンテナがAppのメインプラットフォームとなった環境では1日に10や20のApp deployは当たり前。
- コンテナは秒でApp deployが完了。Firewallは秒でポリシー追加可能？
- 膨大な数のポリシーの中で頻繁に追加・削除を繰り返す。ポリシーの正当性を誰が保証？
- ネットワークの設計、構成を常に意識しなければならない。

Application.. Anywhere Any Platform

- マルチロケーション(オンプレ、クラウド)で複雑に連携
- マルチプラットフォーム(ベアメタル、VM、コンテナ)で動作
- ロケーションやプラットフォーム毎に異なるポリシーコントロール手法が必要



マイクロセグメンテーション実現への必須３ヶ条

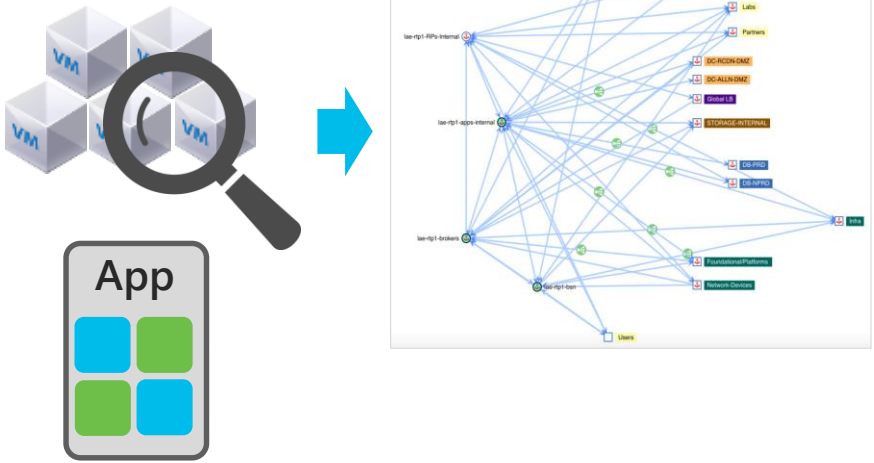
1. 可視化と分析

2. エージェントによるホストベースFW

3. 場所・プラットフォームを選ばない単一のポリシーマネージャー

事実をベースにアプリケーション依存関係を理解

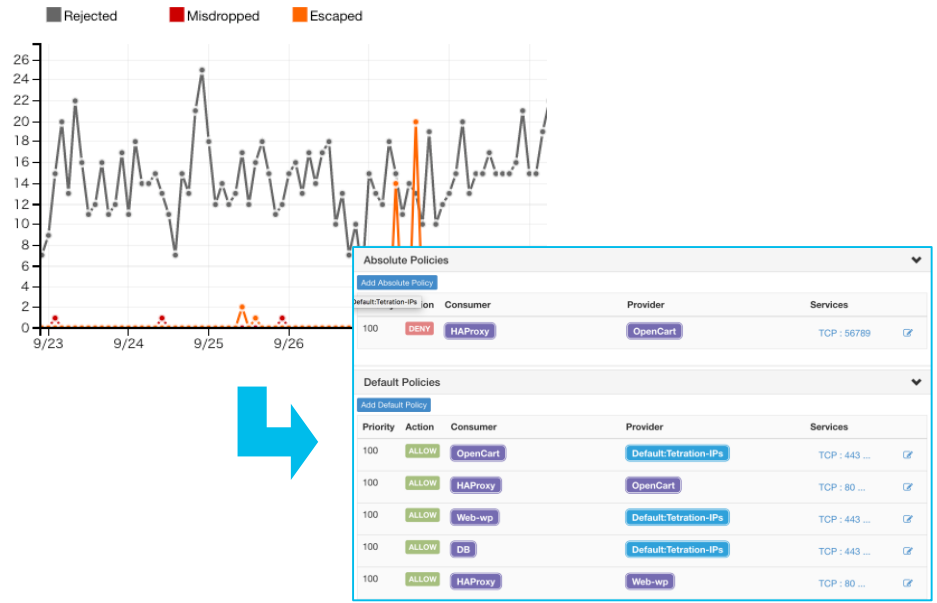
アプリケーションを正しく理解



- アプリケーションワークロードを任意の階層構造で管理できるインベントリ管理フレームワーク。
- マシンラーニング等の技術による同類項判別、セグメンテーションの提示。
- 実際に発生した通信事実に基づいたアプリケーション依存関係の可視化、トポロジー描画。

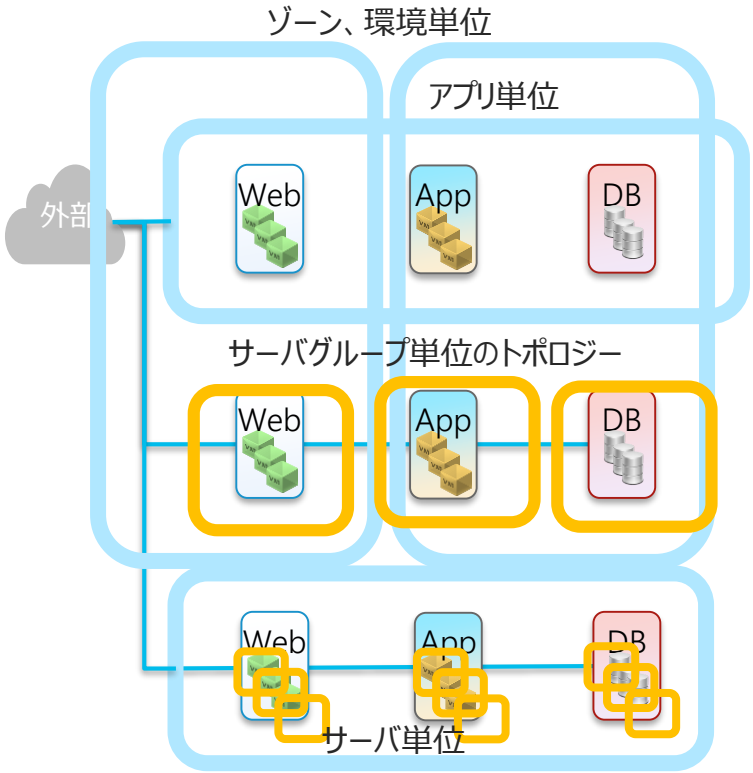
分析によるポリシーの精緻化

あるべきポリシーへのアプローチ



- 現状のポリシーと実際に発生しているフローを対比してポリシーの正確性を客観的に分析。
- ポリシーの変更が実際に発生しているフローにどう影響するかのシミュレーション。
- 分析やシミュレーションから得られたフィードバックを実際のポリシーに反映。

セグメンテーションの粒度と最適なポリシー実行箇所



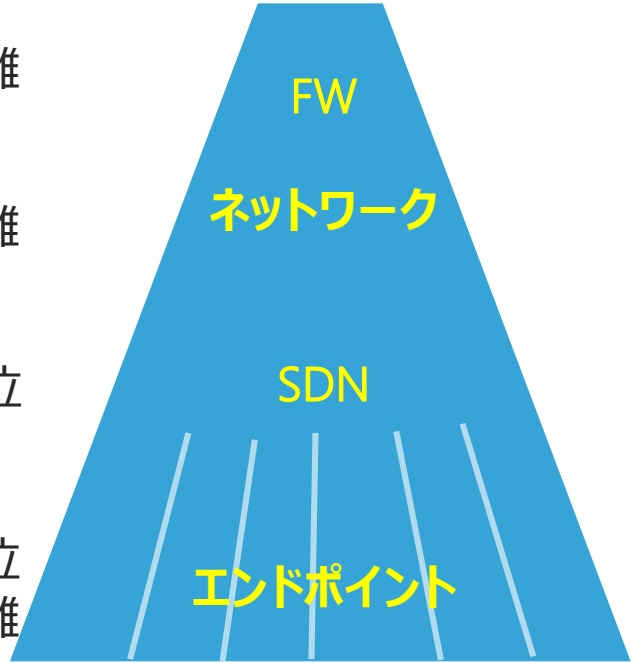
セグメンテーションの適用箇所

ゾーン、環境分離

アプリ分離

サーバグループ単位

サーバ単位
個別サーバ隔離



本当の意味でのマイクロセグメンテーションには

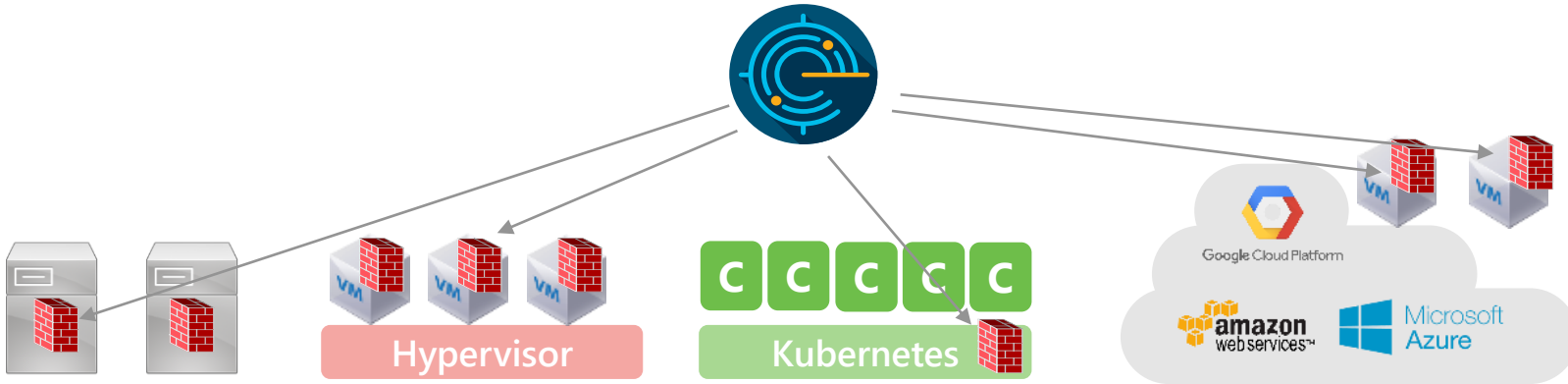
よりアプリケーションに近い場所でポリシー制御する

On Premise　　Public Cloud

ホスト常駐タイプのエージェントでポリシーを実行

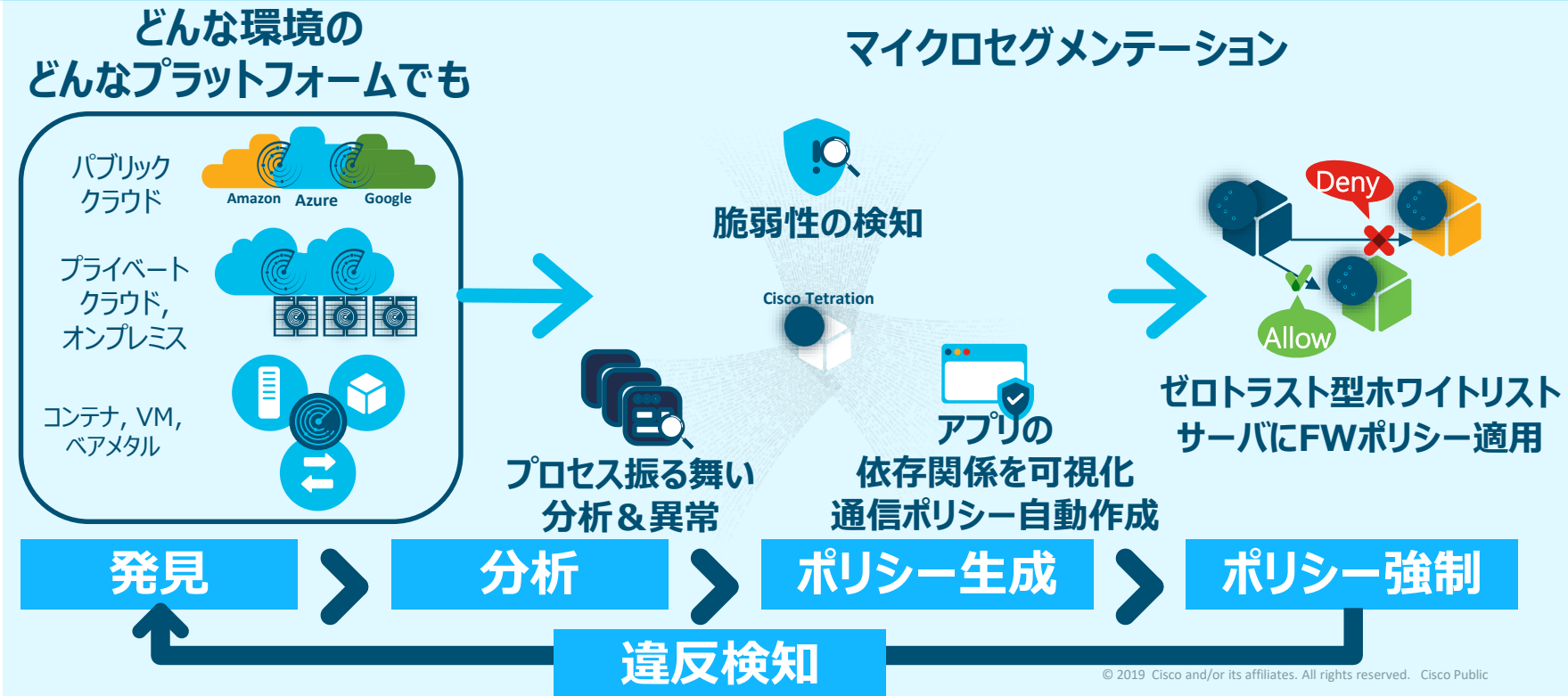
プラットフォームの制約を受けないポリシー管理

シンプルなUIで簡単に使えるポリシーマネージャー



Tetration

マルチクラウド環境を一元的に可視化、ポリシー制御




CISCO