CONTRAIL SECURITY

NXTWORK 2017
JUNIPER CUSTOMER SUMMIT

Aniket Daptari
Sr. Product Manager
Contrail – Cloud Networking & Security

Scott Sneddon
Senior Director
Cloud and SDN

LEGAL DISCLAIMER

This statement of direction sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

This presentation contains proprietary roadmap information and should not be discussed or shared without a signed non-disclosure agreement (NDA).

JUNIPER NETWORKS

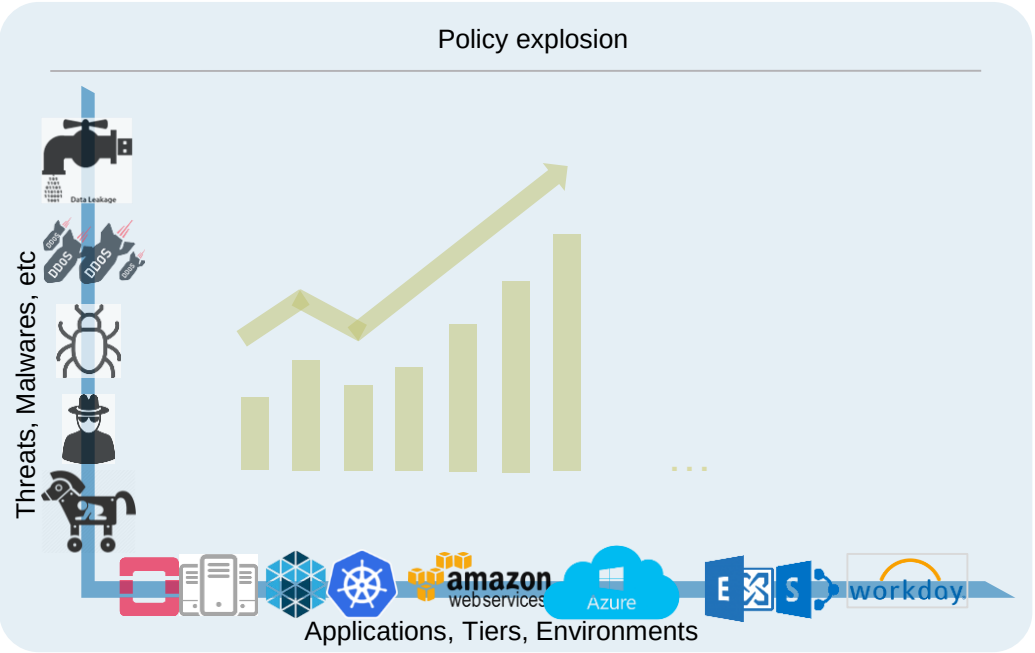
AGENDA

1. PROBLEM STATEMENTS (Why)
2. PRODUCT OVERVIEW (What)
3. POLICY FRAMEWORK (How)

WHY CONTRAIL SECURITY?

Challenges of Traditional Security Paradigm

The Security Scale Challenge



What to protect

1. Applications
2. Number of endpoints
3. Environments – dev, prod, staging, on-prem, public cloud,
4. …

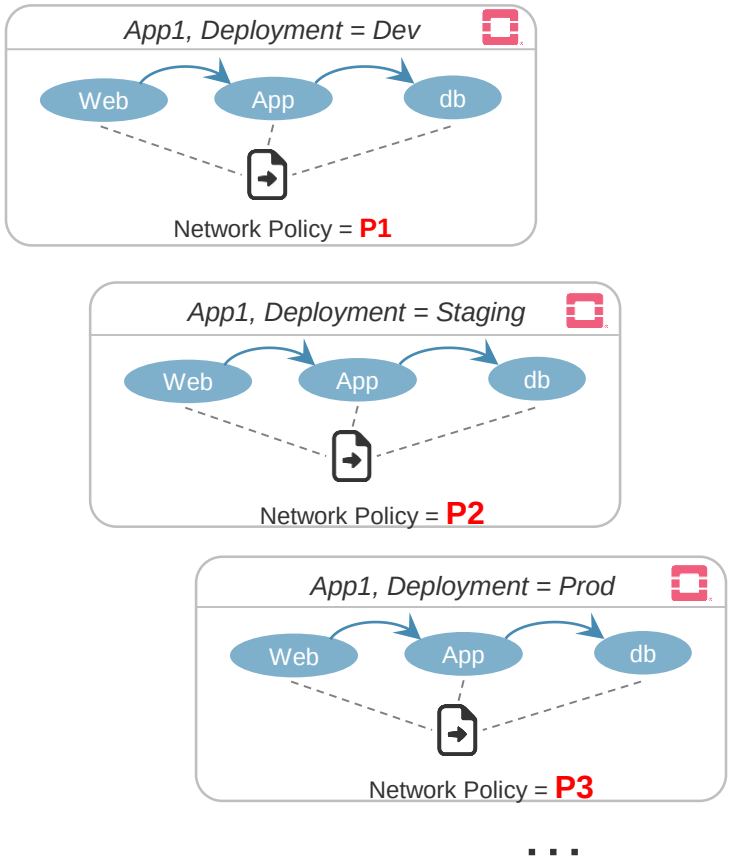
What to protect against:

1. Data leaks
2. DDoS
3. Malware
4. Hacks
5. Viruses
6. Spyware, etc

- Security is Perimeter based – but perimeter is everywhere
- Explosion in # of apps, endpoints, environments on the one hand
- Explosion in # of threats, malware, spyware, hacking, attacks, data leaks on the other hand
- Results in Policy explosion – management complexity and nightmare
- Manual, error prone and non-automated. Does not scale.

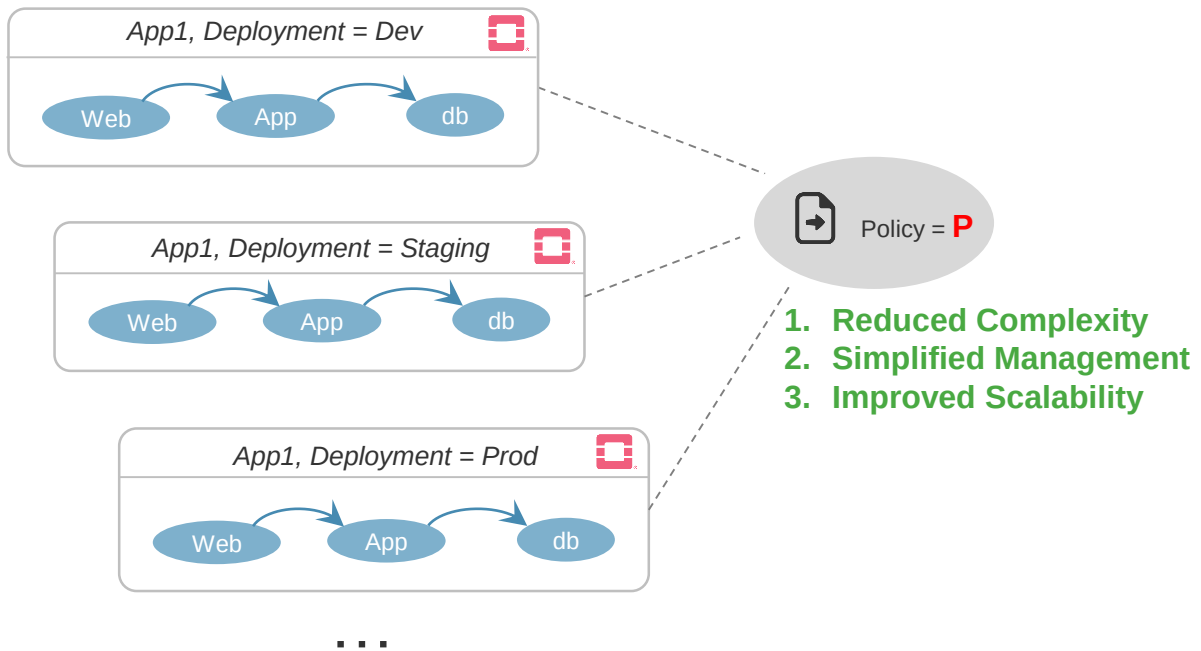
PROBLEM STATEMENT

Current Behavior



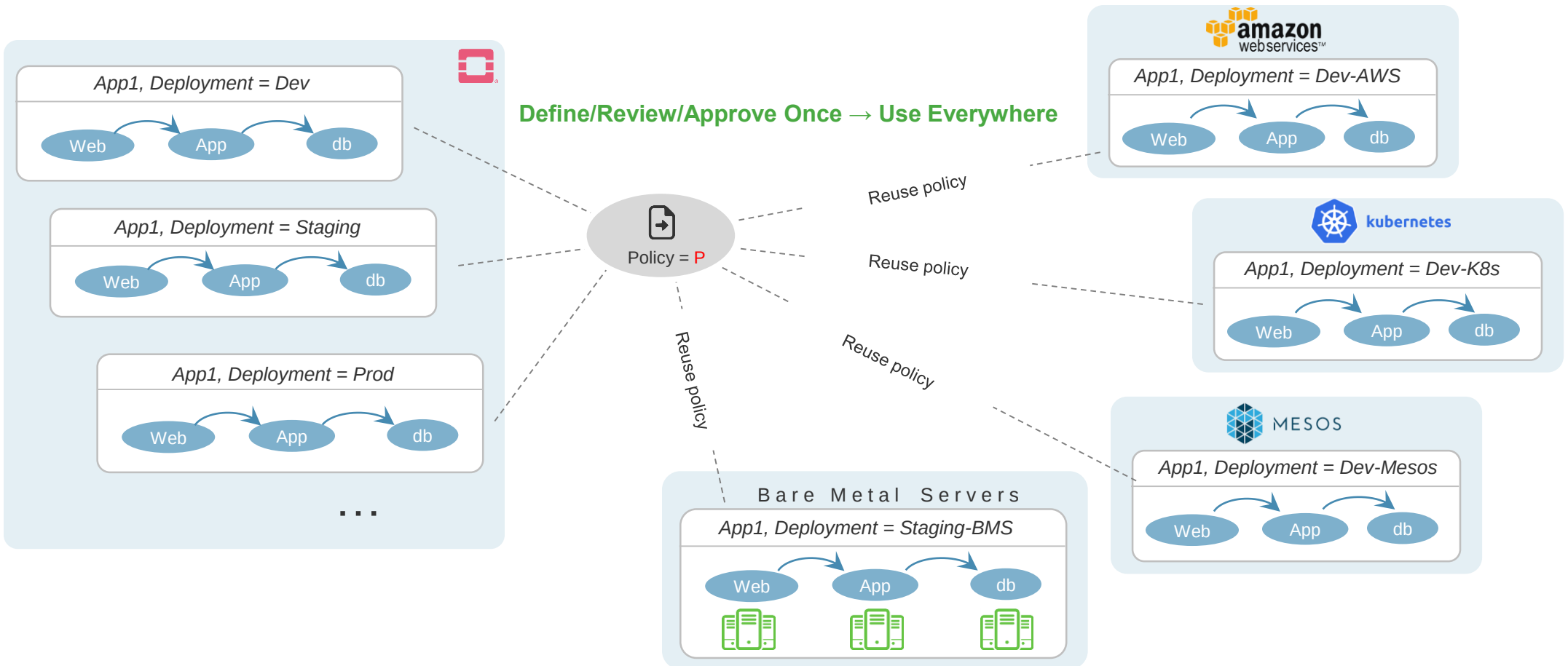
Desired Behavior

Can we use one policy to be applied in all the different deployments ?



PROBLEM STATEMENT

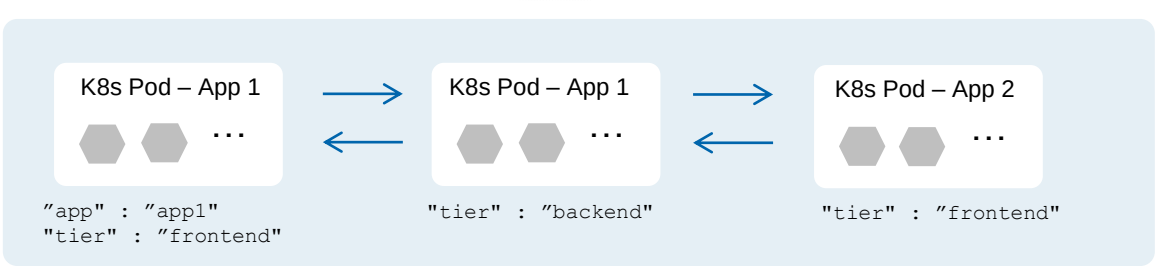
Reuse of policies across multiple clouds and with multiple orchestrators



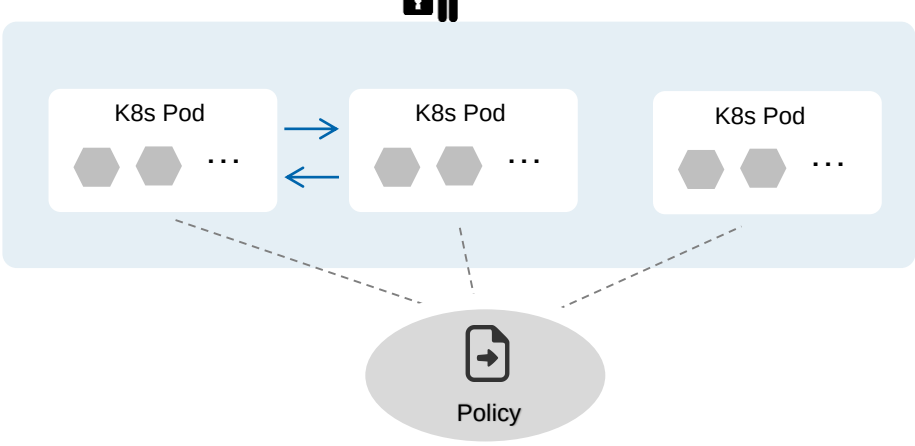
PROBLEM STATEMENT

A Kubernetes application developer creates labels for K8s pods … Can the security admin overlay his policies transparent to the developer – [i.e. use the same (or different) labels to create security policies / boundaries] ?

Kubernetes Application – created by Developer
(uses different labels to imply connectivity characteristics)



CSO / Compliance / Operators puts policies
(using the same or different labels seamless to developer)



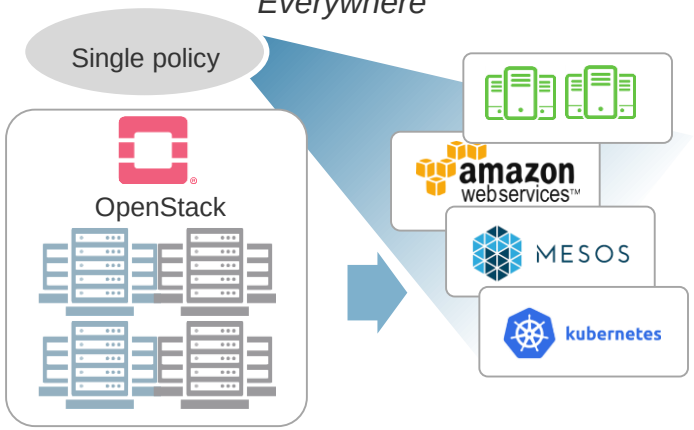
WHAT IS CONTRAIL SECURITY?

CONTRAIL SECURITY KEY CAPABILITIES

Consistent Intent-Driven Policy

Security Admin

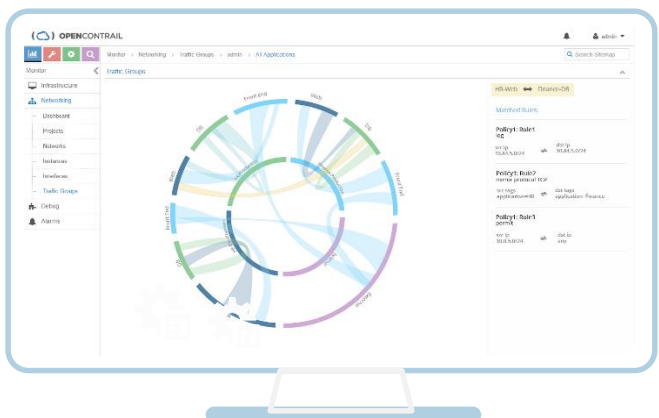
No Policy Rewrite …
Define Once → Enforce Everywhere



- *How to extend the same set of policies to Mesos, AWS, Kubernetes, Bare Metal Servers → without policy rule explosion*

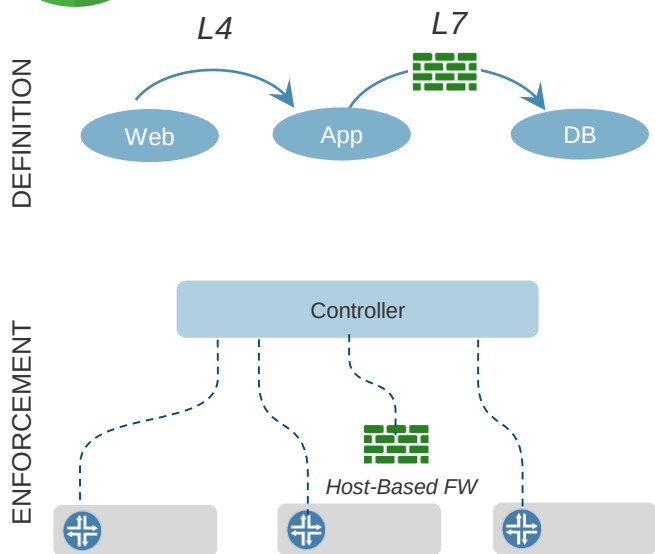
Application Policy Config & Flow Visualization

Discover Inter- and Intra-application traffic flows with/without enforcing policies



- *Offer visualization, analytics, and orchestration for security configurations*
- *Provide reporting, troubleshooting and compliance*

Multiple Enforcement Points

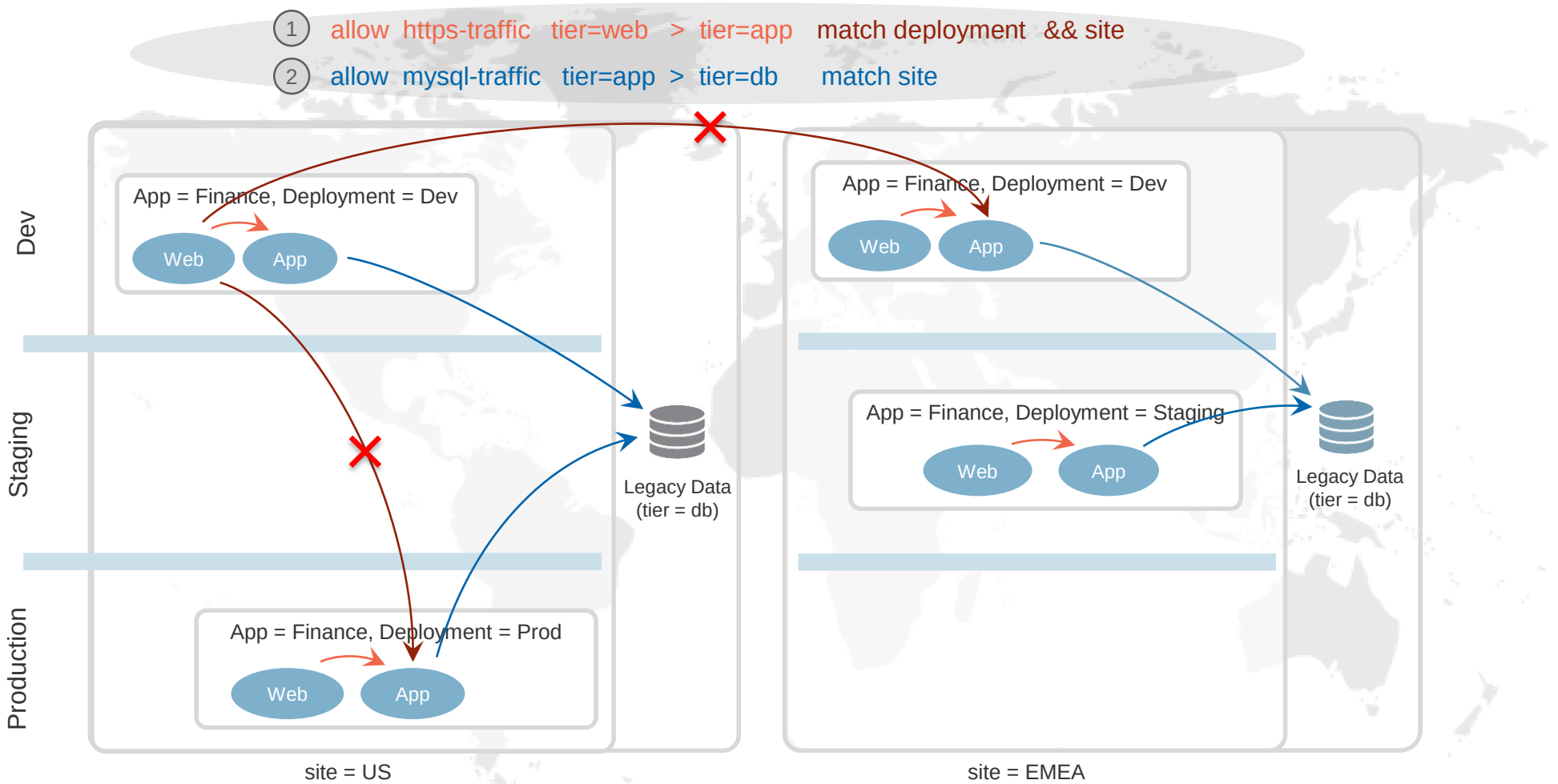


- *L4 Enforcement at the vRouter (Kernel, DPDK, vCenter, Smart NIC)*
- *L7 enforcement at the L7 Firewall*

USE-CASE SCENARIO – POLICY FRAMEWORK

Defn

Enforcement



JUNIPER NETWORKS

TAGS & OTHER POLICY ITEMS

Various ways to tag the workloads

1. Application = HRMS, CRM, …
2. Deployment = Dev, QA, Staging, Production …
3. Site = India, US, EMEA, etc…
4. Tier = Web, App, DB,...

1. Label = anything custom ....
2. Custom Tags

Phase 1 Deliverables

- User
- User Role
- OS
- Software Compliance
- Customer

- Compute Node: e.g. used in affinity / anti-affinity policies for compute
- Rack
- POD
- Cluster
- DC

Roadmap

Address Group

Can be used as an end-point in the policy…

1. Prefixes
2. Static Group of IP Addresses
3. Dynamic Groups with custom labels
4. …

Service Group

List of Protocol & port (e.g. web-service)

1. tcp 80
2. tcp 8080
3. …

Application Policy Group

List of policies → make it an application set … This helps in easy attachment to any application ...

1. Firewall Policy 1
2. Firewall Policy 2
3. …

POLICY – KEY ITEMS TO NOTE

Policy Example: `allow http-traffic tier=web > tier=app match deployment && site`

Tag expression — *Tag expression* — *Tag key expression*

Policy Tags

Objects at different levels can be tagged

Tags / Labels

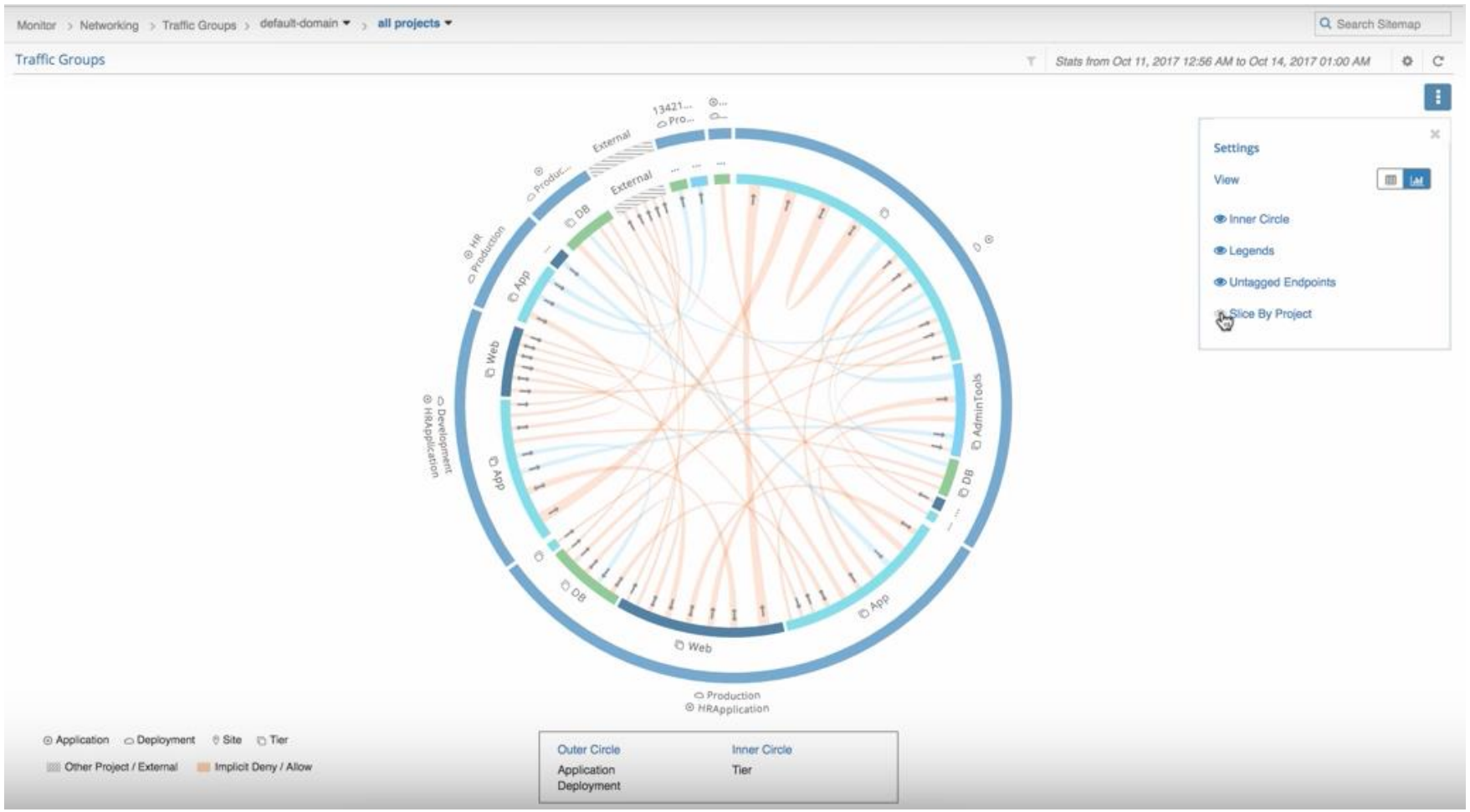
Tags can be defined at different levels

- Global
- Project
- Network
- VM / Container / BMS
- Interface

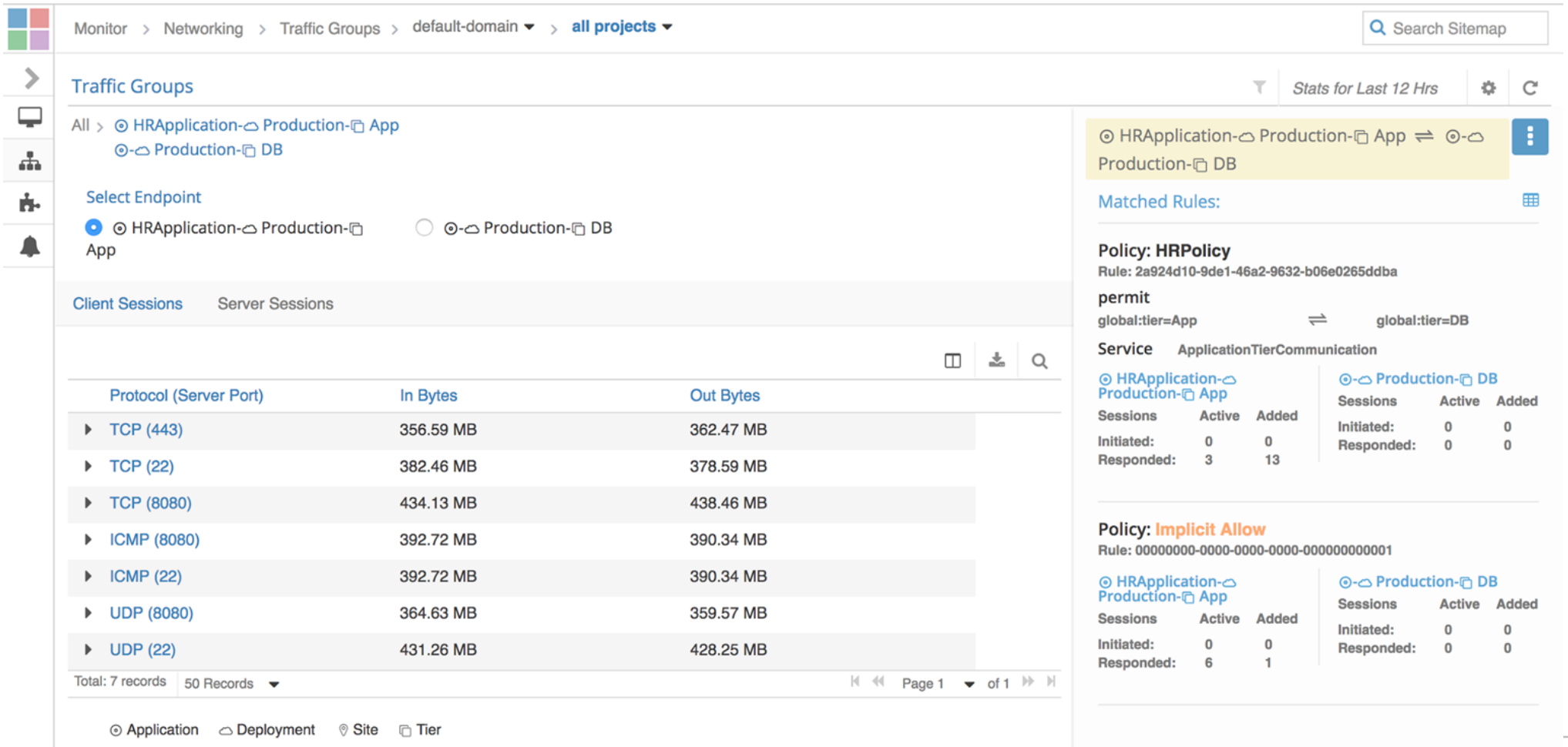
Policy Enforcement

Policies will finally be enforced at the interface level

VISUALIZATION



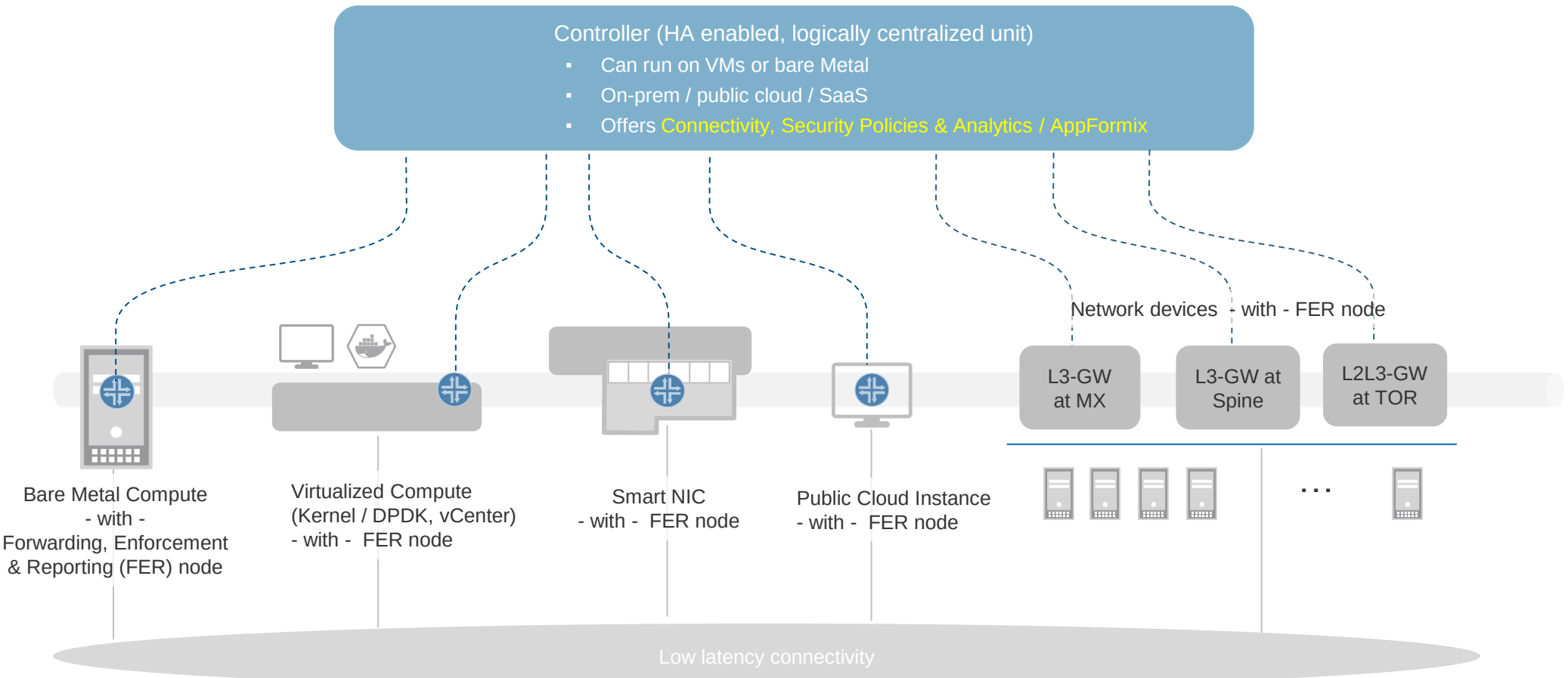
POLICY & FLOW VISUALIZATION



MULTIPLE ENFORCEMENT POINTS

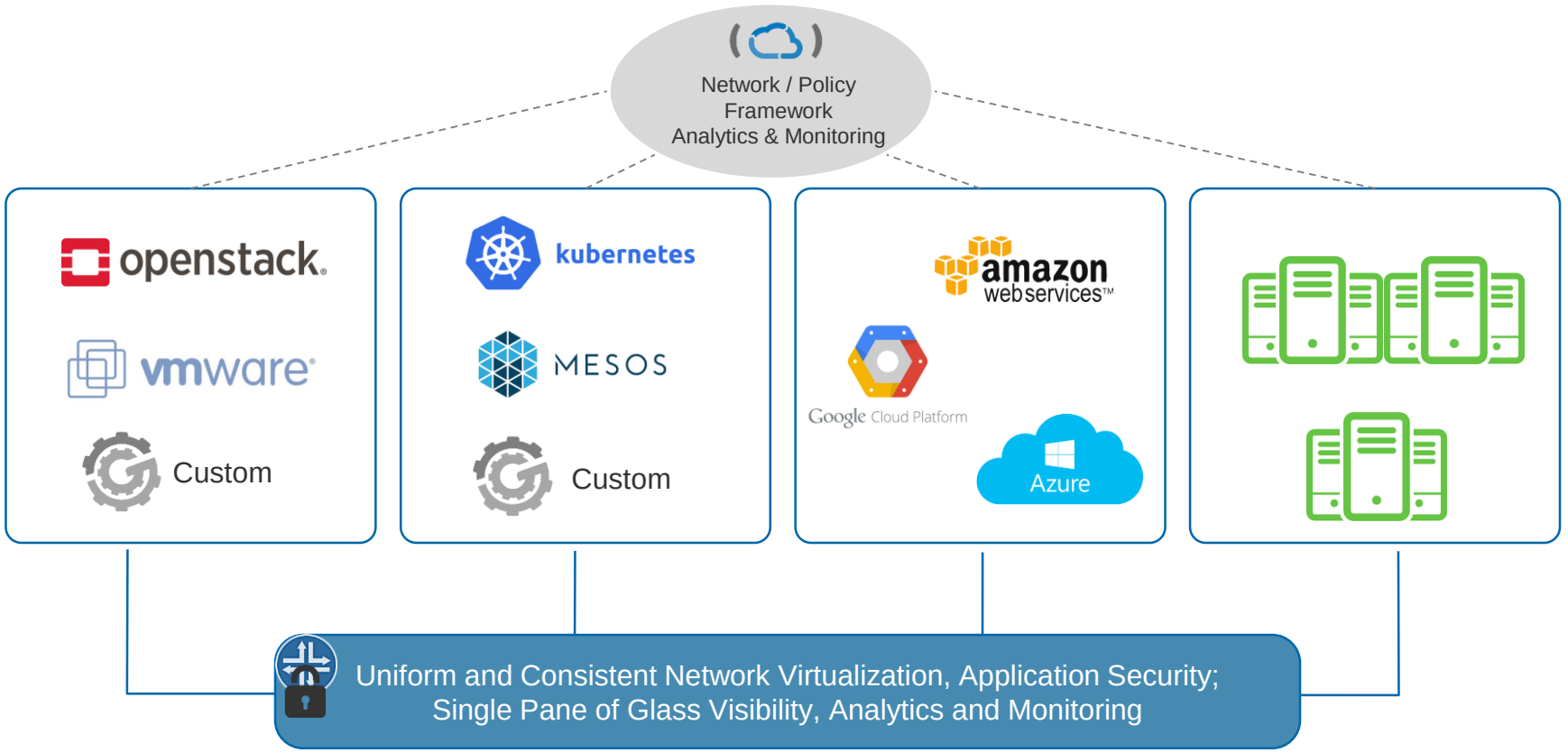
Definition

Enforcement

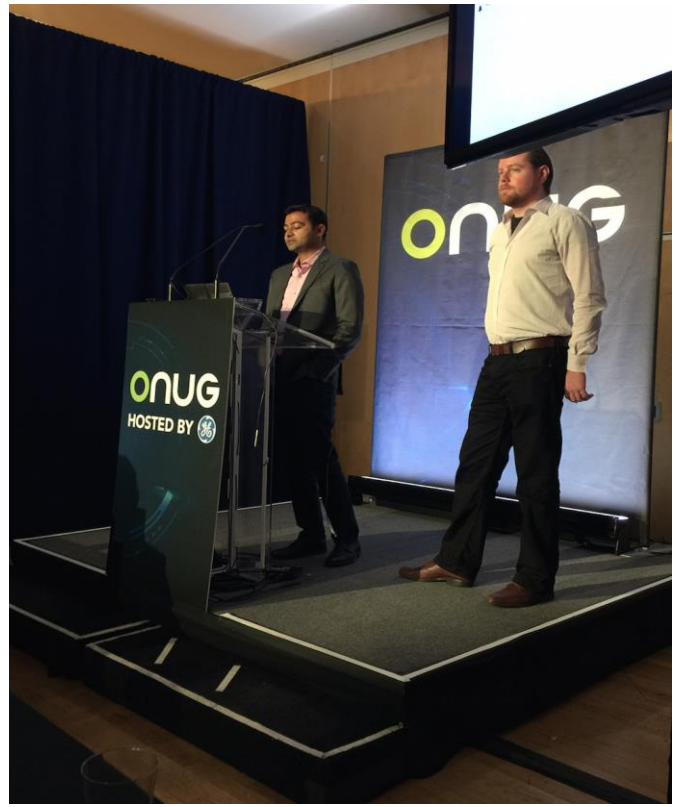


KEY TAKEAWAY

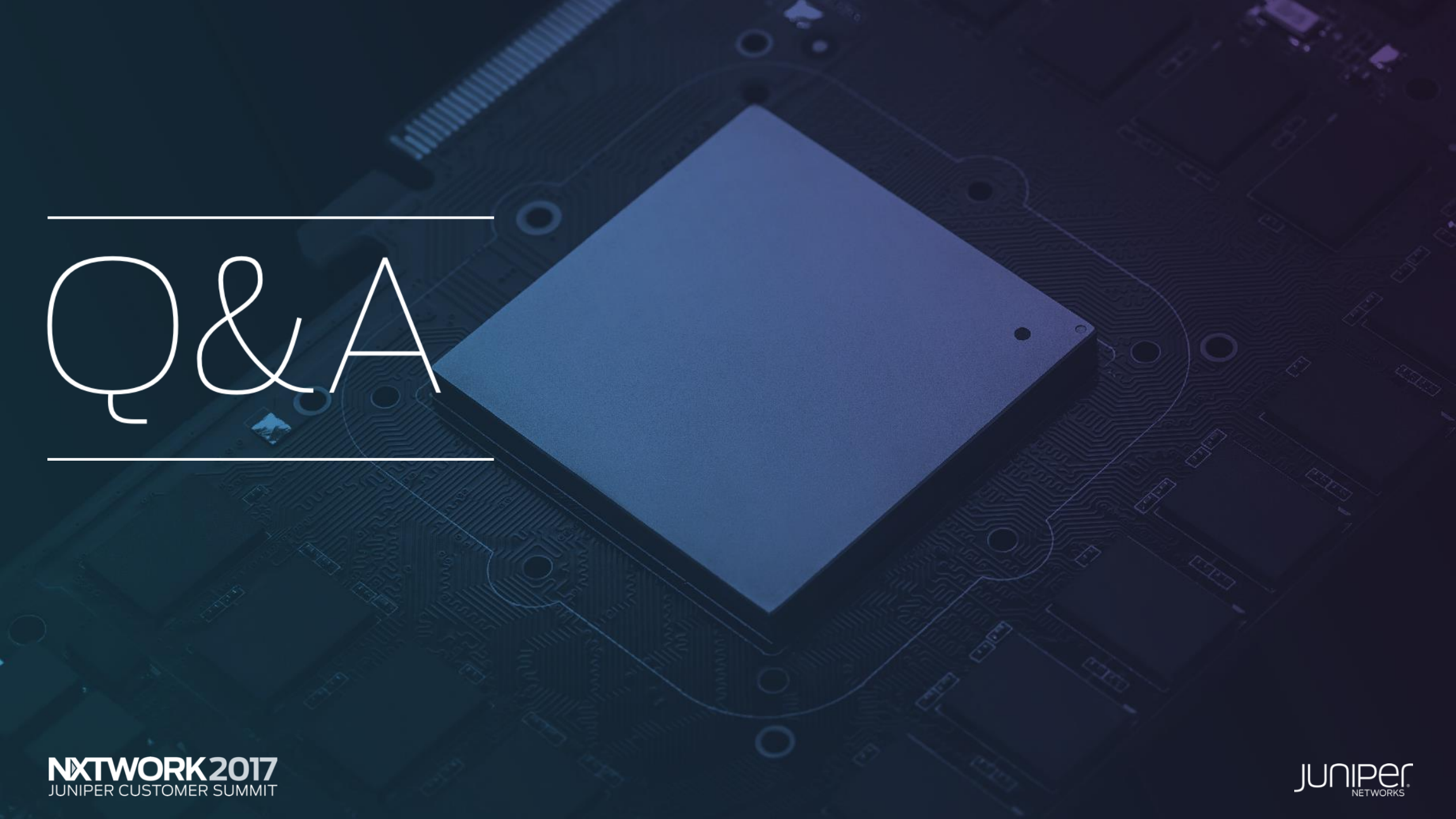
App Discovery, Tag based Policy & Visualization across heterogeneous and distributed environments (ESXi & KVM VMs, K8s / containers, bare-metal servers, Public Cloud, etc.)



RECOGNITION AT 2017 ONUG



Blog: [Contrail Security wins 2017 ONUG Innovation Award!]


Q&A