RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

#RSAC

POWER OF OPPORTUNITY

SESSION ID: CSV-W02

# Open Security Controller - Security Orchestration for OpenStack

**Tarun Viswanathan**
Platform Solution Architect
Intel

**Manish Dave**
Platform Architect
Intel

# Notices and Disclaimers



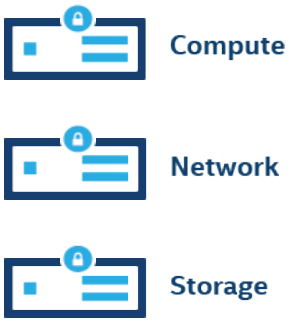
- Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.
- No computer system can be absolutely secure.
- Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.
- Intel, the Intel logo and others are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others.
- 

# SDI—The Application Defines the System

- **The evolution to software-defined infrastructure**

One application per system

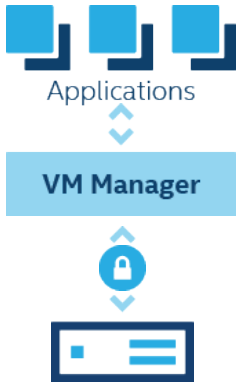
**Static perimeter-focused security hardware appliances**




TRADITIONAL HARDWARE

One application per virtual system

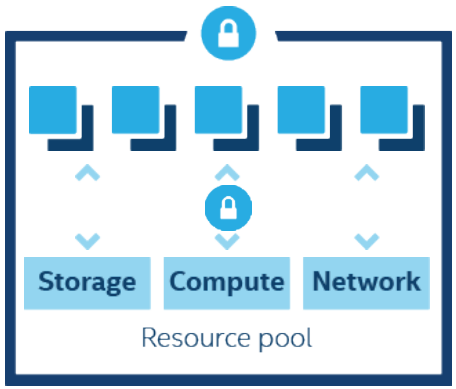
**Partially automated security physical/virtual appliances**




ABSTRACTING THE HARDWARE

Applications **define** the system

**Fully automated software-defined security**

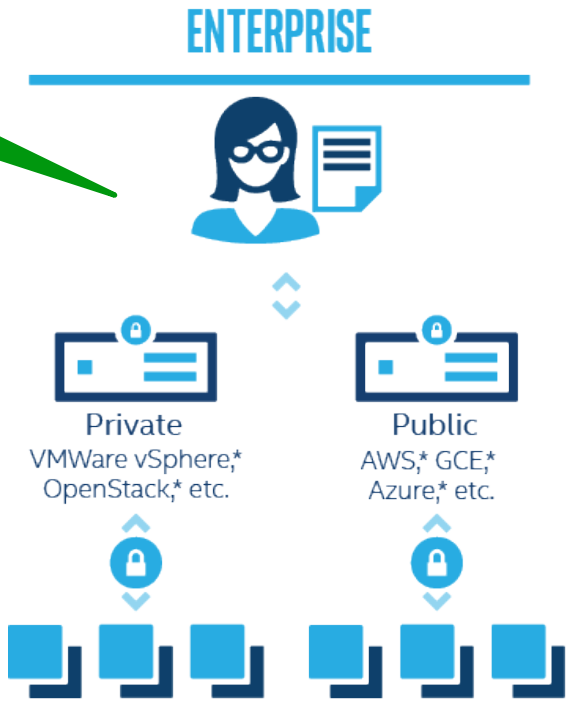



ABSTRACTING THE DATA CENTER

# Enterprise Multi Cloud Security Challenges



How can I provide consistent security across a multi cloud data center environment.




OPEN SECURITY CONTROLLER

Open Security Controller addresses this challenge.

# Open Security Controller Key Design Goals



**Centralized security policy management** for a multi cloud environment.

**Automated provisioning, distribution, and delivery** of security inside data center perimeter

**Dynamic scale-out Security** VNFs

**No Lock-in**
Vendor agnostic open solution

**Policies aligned** with specific application workloads

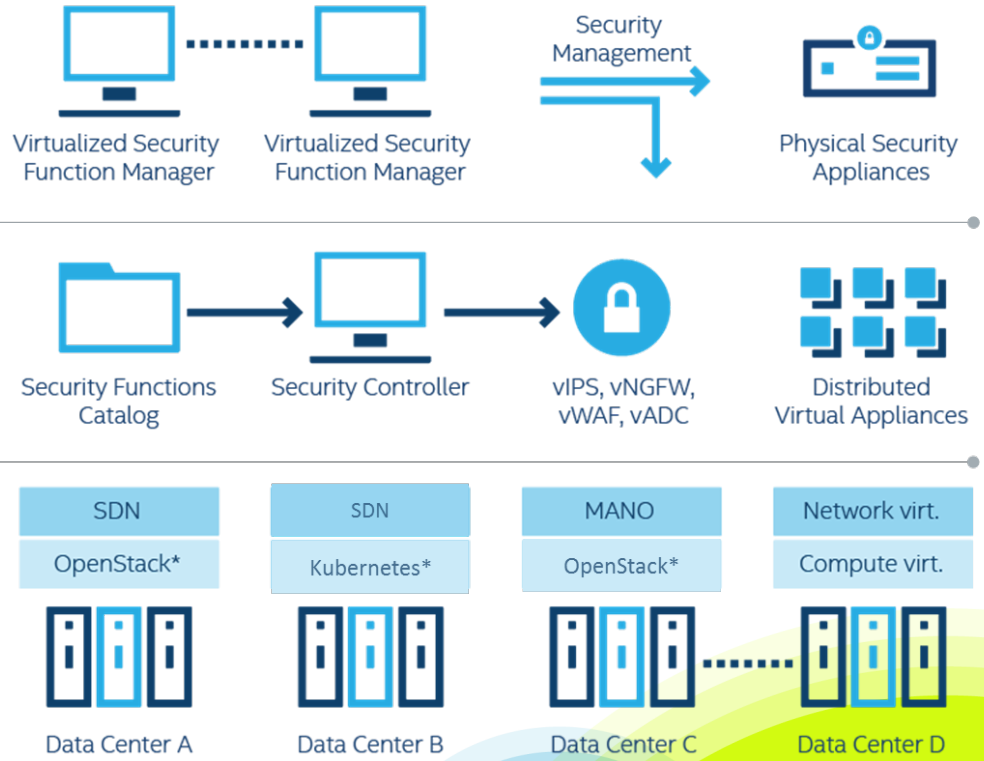
**Separation of duties** to enable use of familiar tools

# Conceptual Architecture



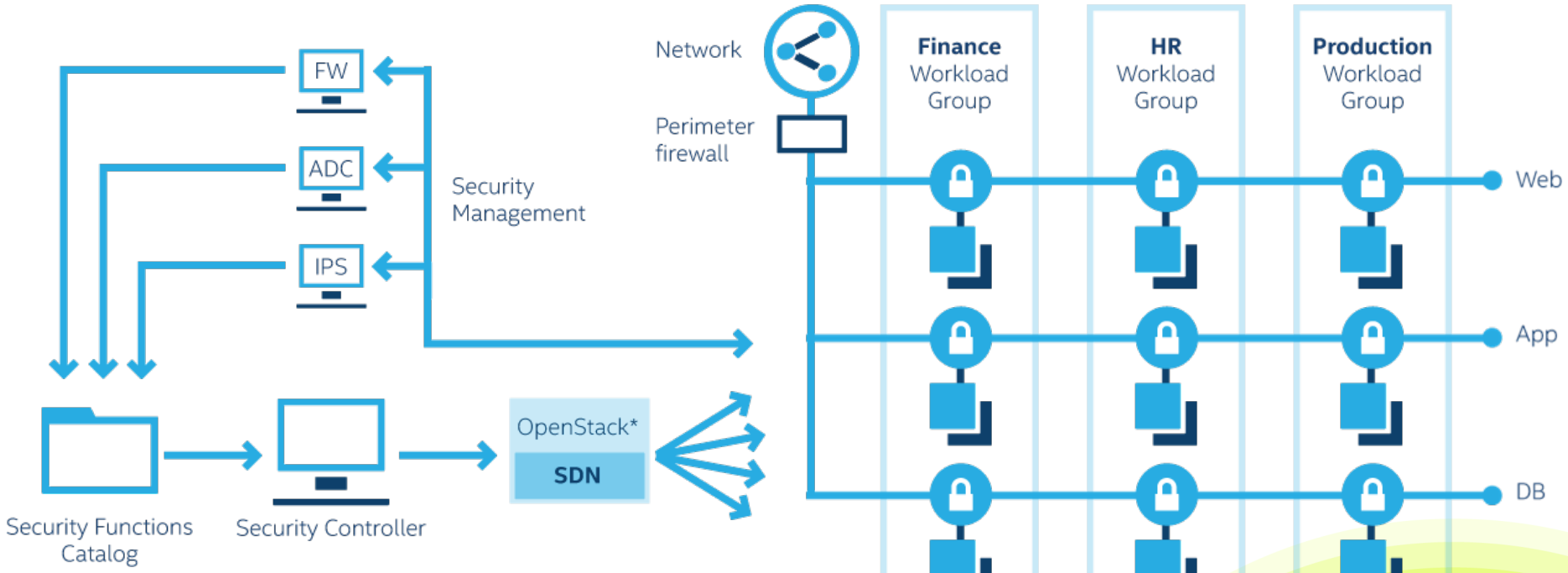
**Orchestrating security policies with network provisioning across *multiple virtual environments***

| | |
|---|---|
| Security Function Manager | Centralized management and separation of duties |
| Security Controller | Security service automation and orchestration |
| Virtualization Infrastructure Management | Abstracts compute, storage, and network |

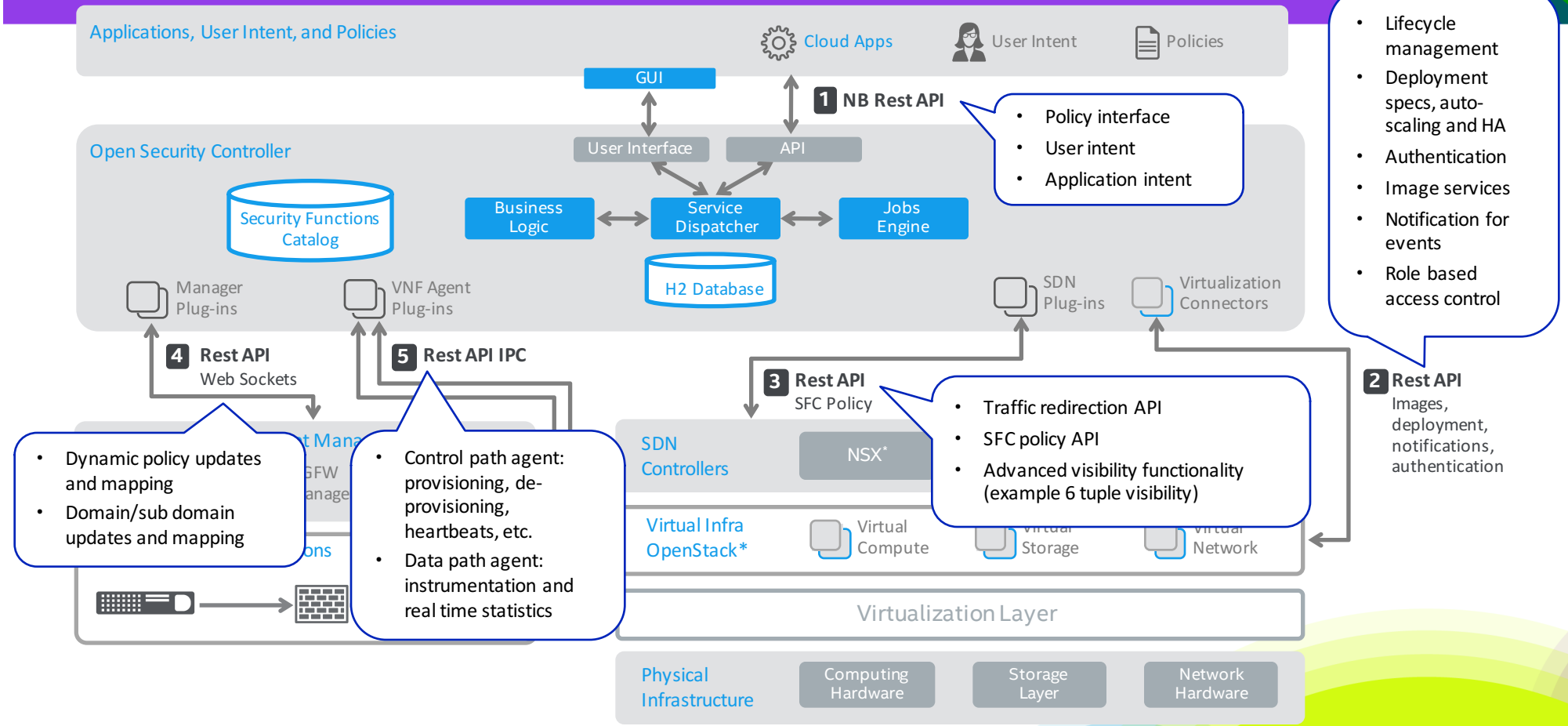


# OpenStack* Micro-Segmentation Use Case

- Advanced threat protection for East-West traffic flows



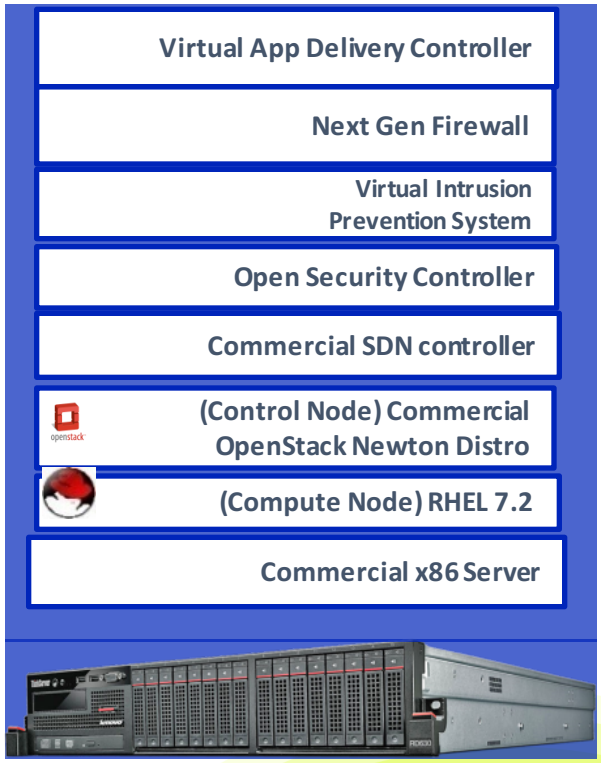
# OSC API Interaction Model



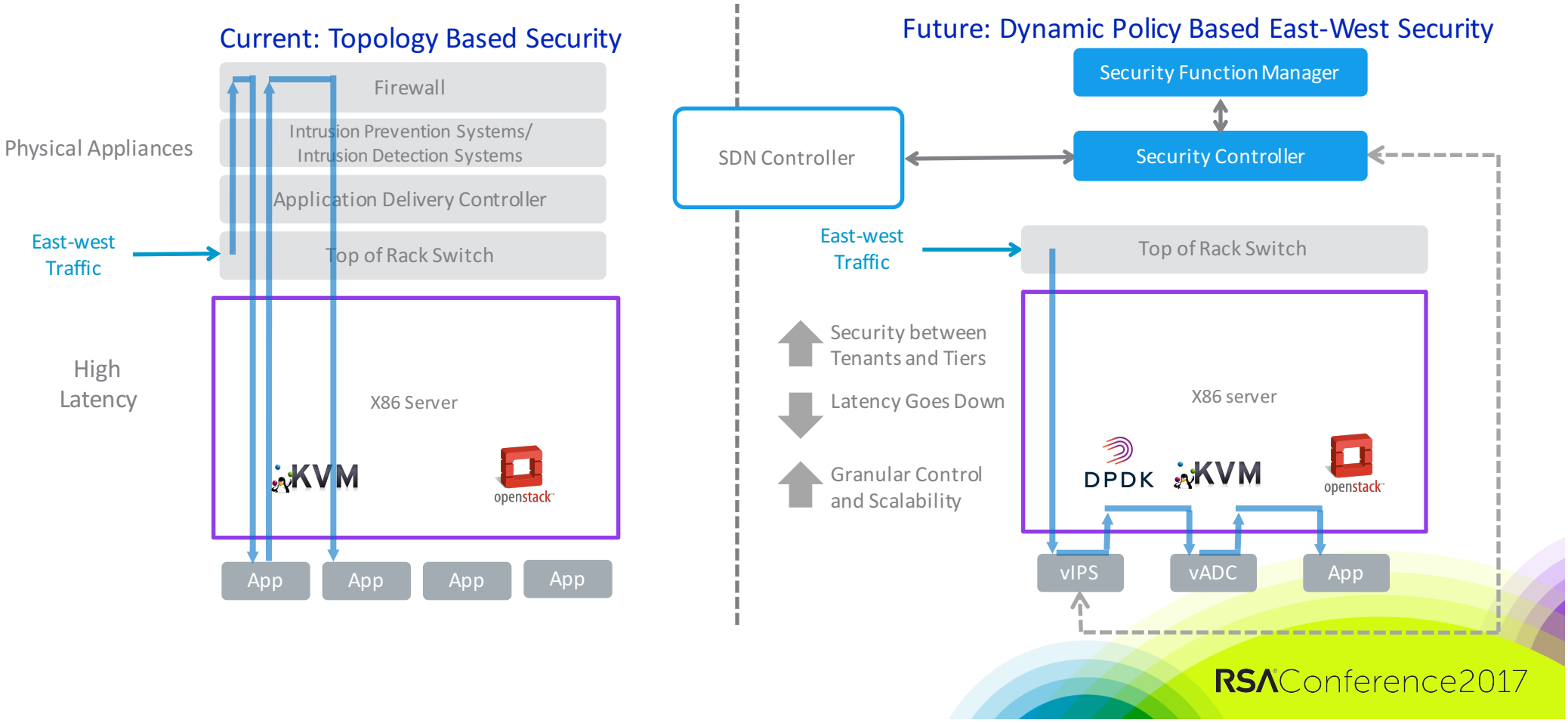
# Customer PoC: Health industry IT services provider



- Customer has to adhere to HIPAA regulatory requirements
- Existing solution was based on DC edge devices.
- Customer wanted to get to a dynamic policy based security solution for East-West traffic inspection.



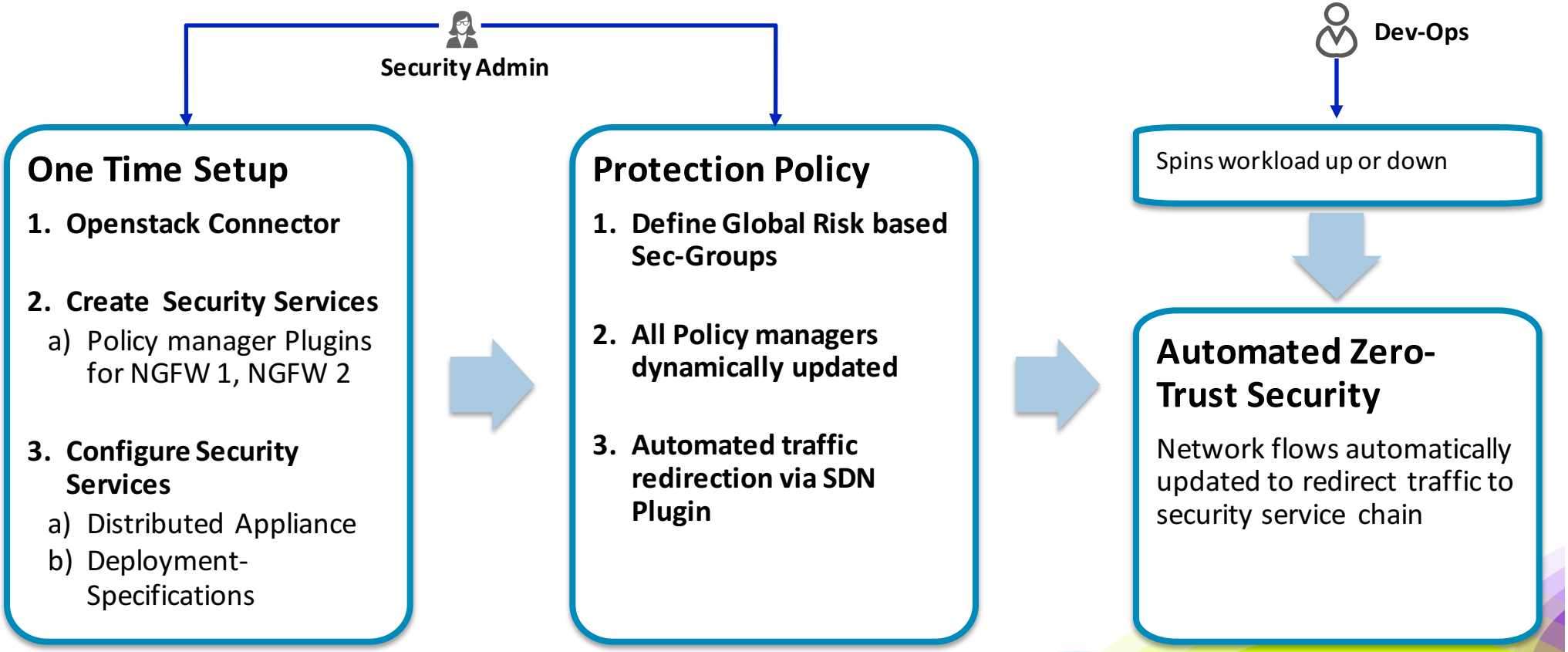
# Customer Deployment Architecture



# Customer PoC: Large financial services provider

- Customer has to adhere to PCI regulatory requirements
- Customer wanted to get to a Risk Based automated security policy management capability for their Openstack environment

# Customer deployment Workflow

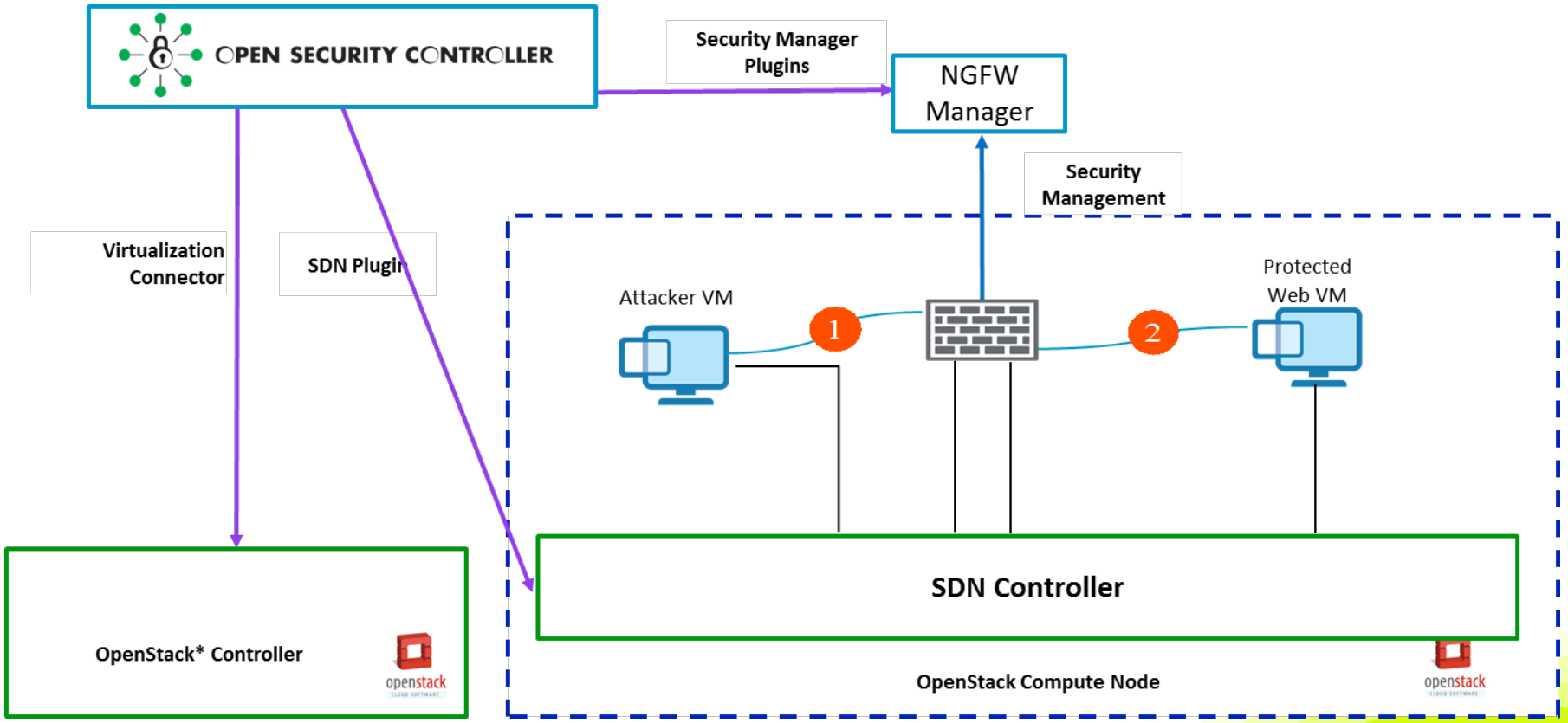


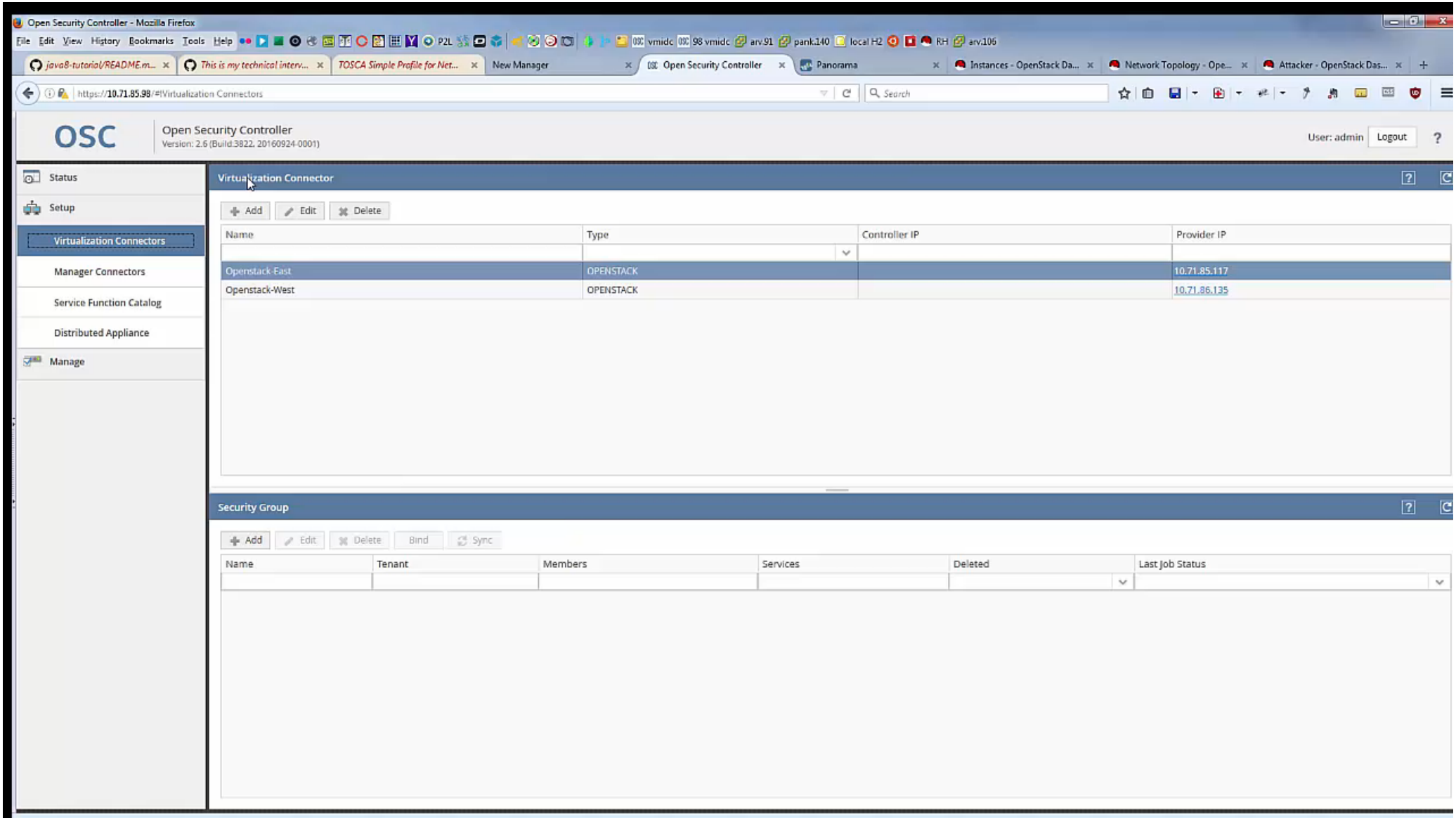
RSAConference2017

# DEMO

## Automated Security Services Orchestration for Openstack

# Demo Topology




Open Security Controller - Mozilla Firefox
https://10.71.85.98/#!Virtualization Connectors
OSC
Open Security Controller
Version: 2.6 (Build:3822, 20160924-0001)
User: admin
Logout
Status
Setup
Virtualization Connectors
Manager Connectors
Service Function Catalog
Distributed Appliance
Manage
Virtualization Connector
Add
Edit
Delete
Name
Type
Controller IP
Provider IP
Openstack-East
OPENSTACK
10.71.85.117
Openstack-West
OPENSTACK
10.71.86.135
Security Group
Add
Edit
Delete
Bind
Sync
Name
Tenant
Members
Services
Deleted
Last Job Status

# Apply: Risk Based Approach



1. Identify workload which needs micro segmentation
2. Identify security controls to mitigate risks (vIPS, vNGFW, vADC)
3. Automate Security Controls orchestration

# Call to Action



- Current Status
  - POC with early adopter customers / Security VNF's
  - Open Security Controller available as Opensource ~ Mid 2017 compatible with few Security VNF and SDN vendors
- Call to Action
  - Contact us to get engaged in the community: Email: manish.dave@intel.com or Tarun@intel.com
  - Additional Information: www.intel.com/osc