



Application Centric Infrastructure

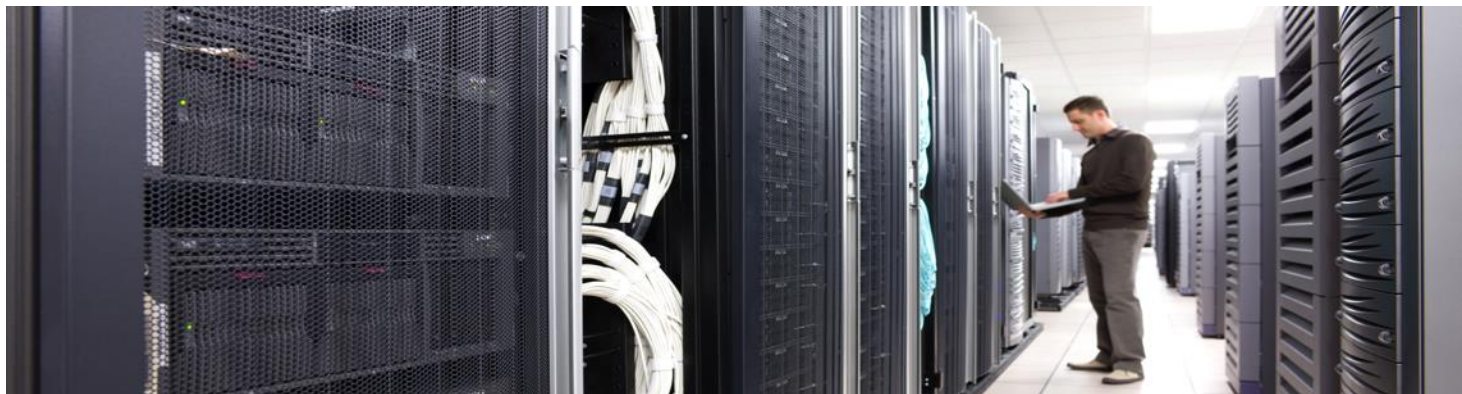
*How to address security and compliance in the next generation data center
using software defined networking concepts*

Alexander Stoklasa
Consulting Systems Engineer

27 März 2014

Today's Challenges





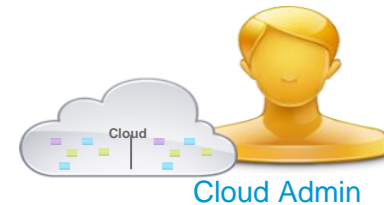
“Through 2018, more than 95% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws.”

Greg Young, Gartner Inc

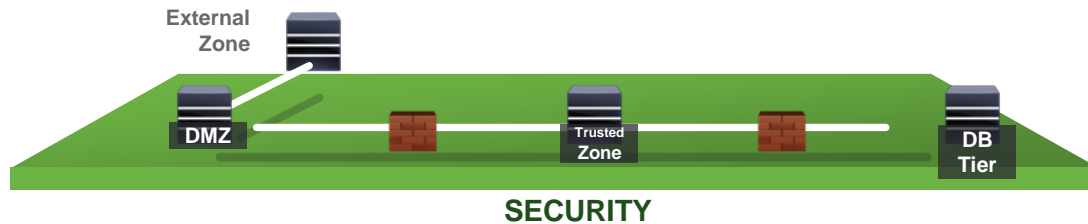
Today's Challenges cont'd



Application Admin



Cloud Admin



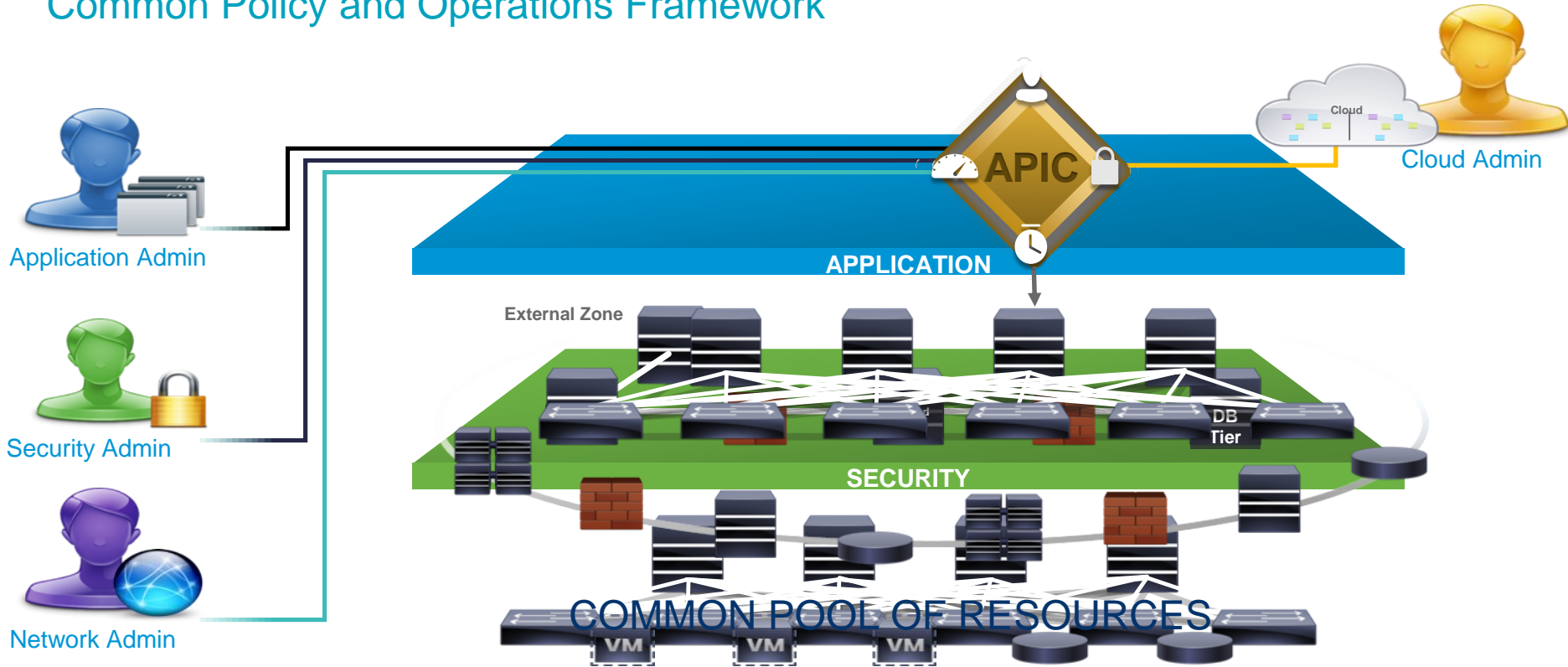
Security Admin



Network Admin

Application Centric Infrastructure Goal

Common Policy and Operations Framework



Infrastructure Innovation – beyond SDN

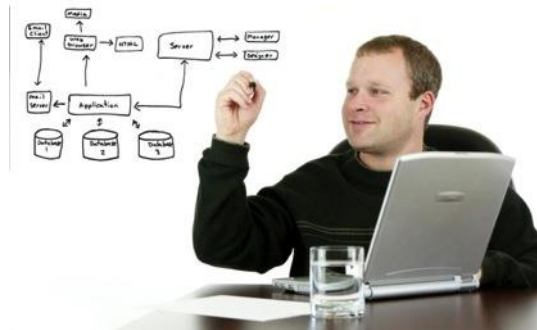


Believe!

Policy and the Network

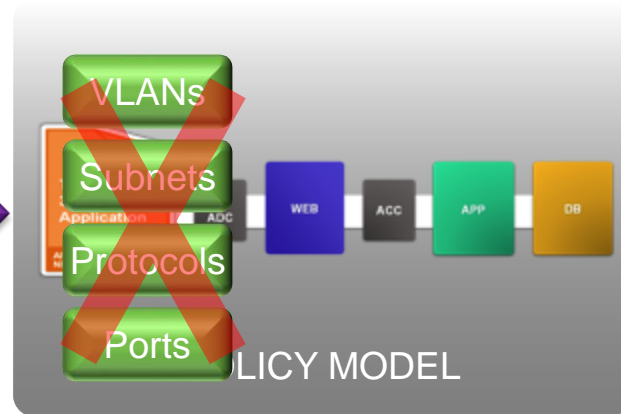


Developers



Application Tiers

Provider / Consumer Relationships



ACI policy model:

Definition of an Endpoint in ACI

- Device connected to network directly or indirectly
- Can be physical or virtual port (VM port group)
- VLAN ID
- VXLAN (VNID)
- IP address/ IP Prefix
- DNS name *
- Layer 4 ports *



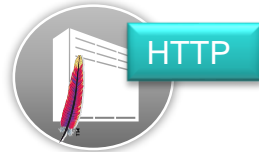
Server



Virtual Machine



Storage



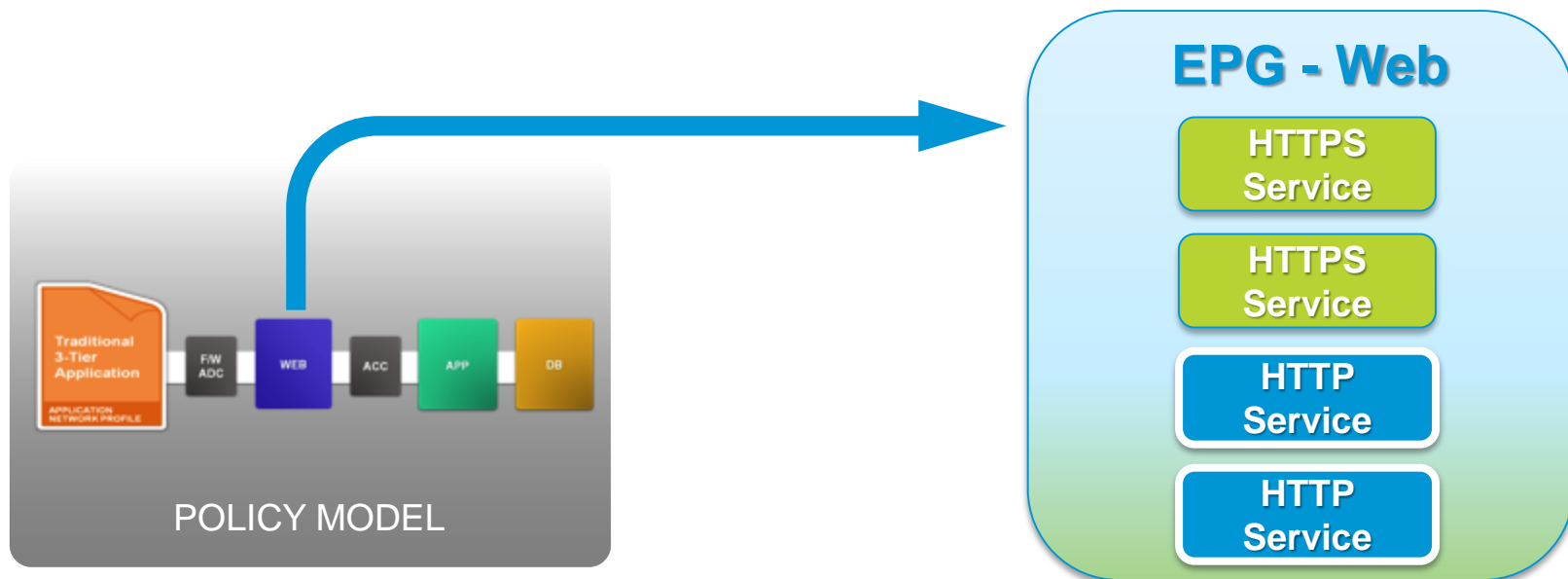
Daemon/Service

*) Future

ACI policy model

End-Point Group (EPG)

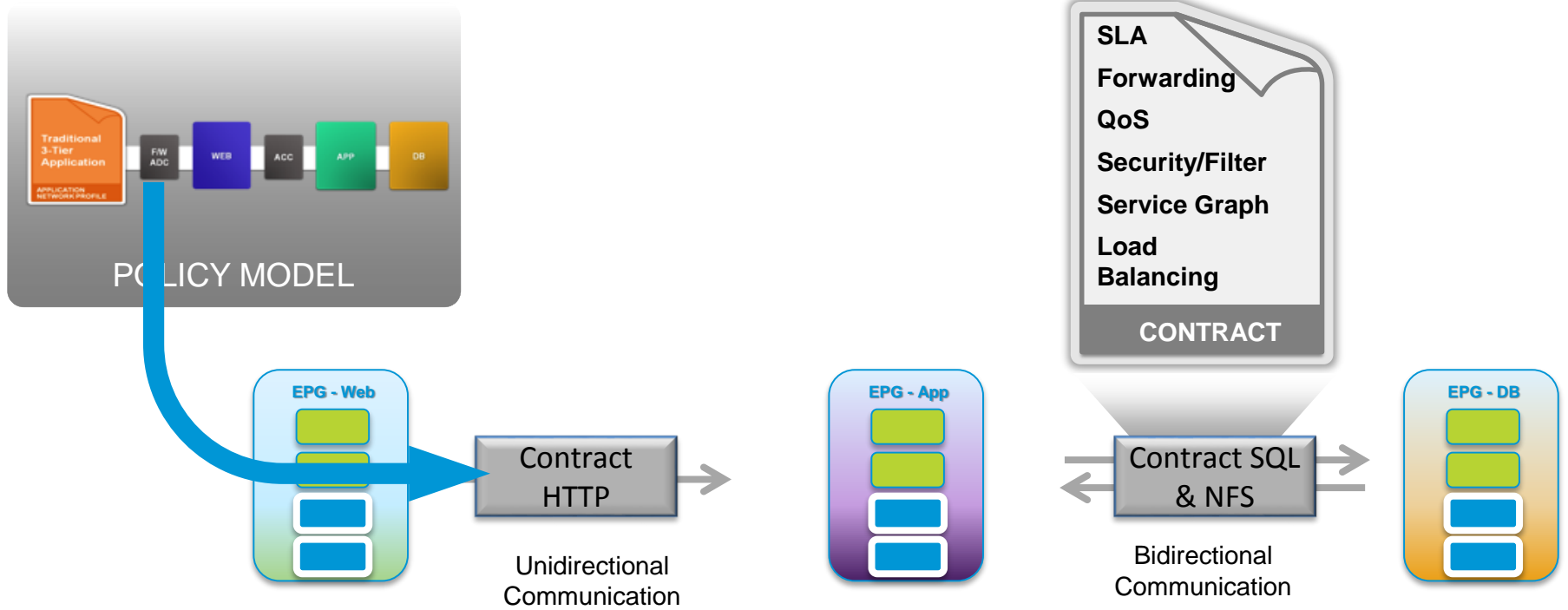
EPGs are a **grouping of end-points** representing **application or application components independent** of other network constructs such as Vlans.



ACI policy model

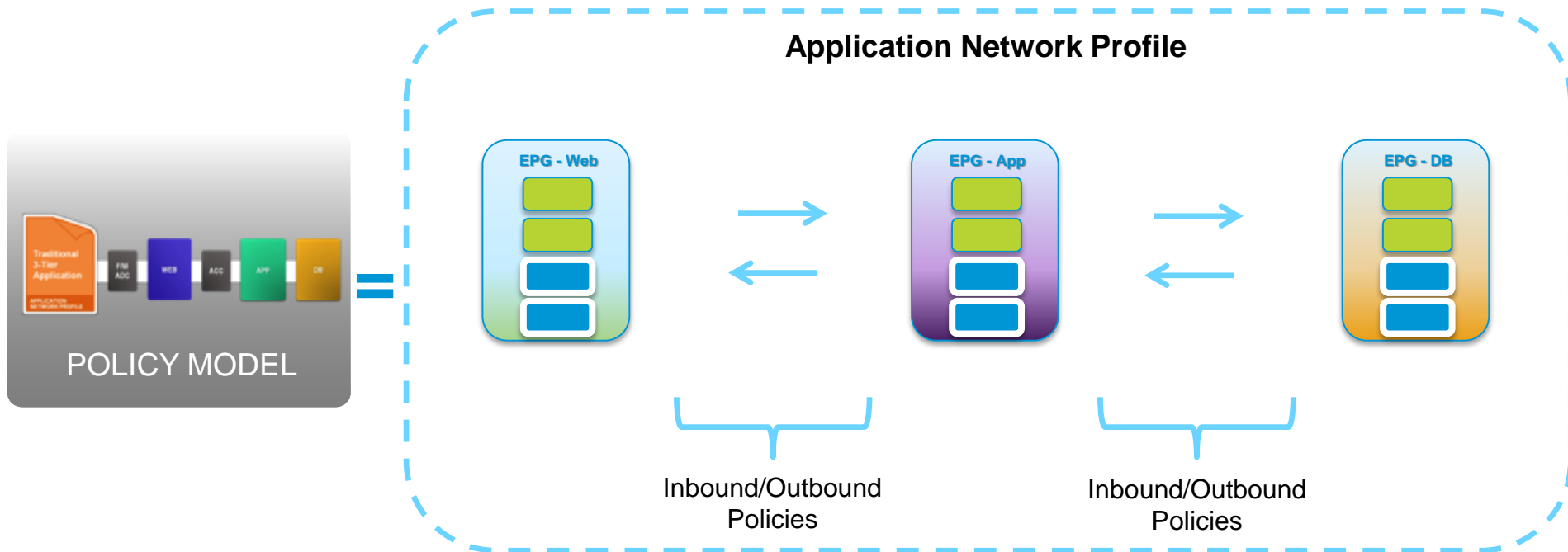
Contracts

Contracts define the way in which EPGs interact.



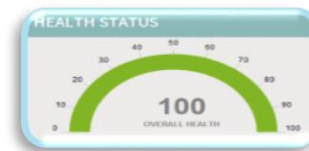
Application Network Profiles (ANP)

Application Network profiles are a group of EPGs **and** the policies/contracts that define the communication between them.

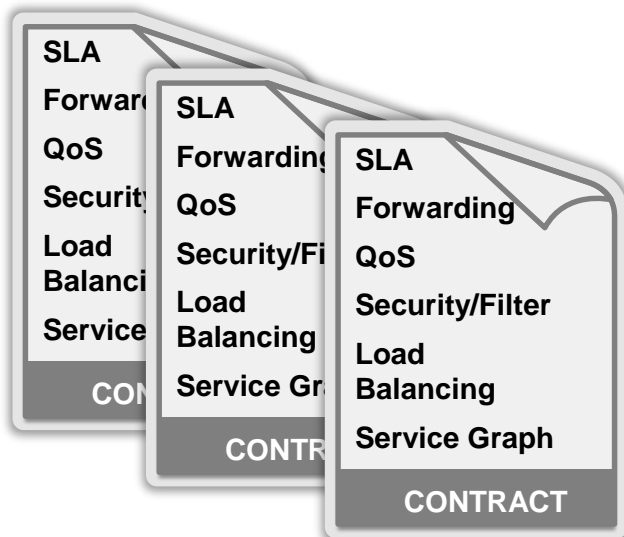
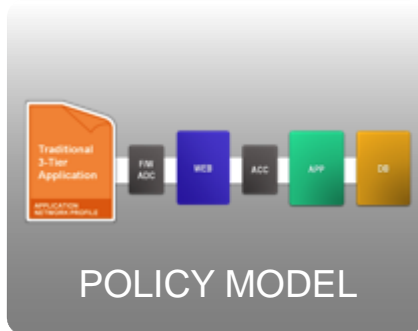


Application Network Profiles (ANP)

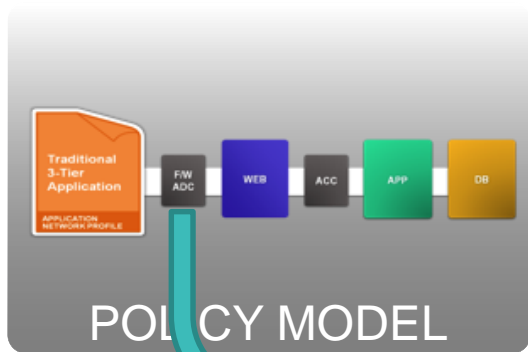
Visualization of Application-Health



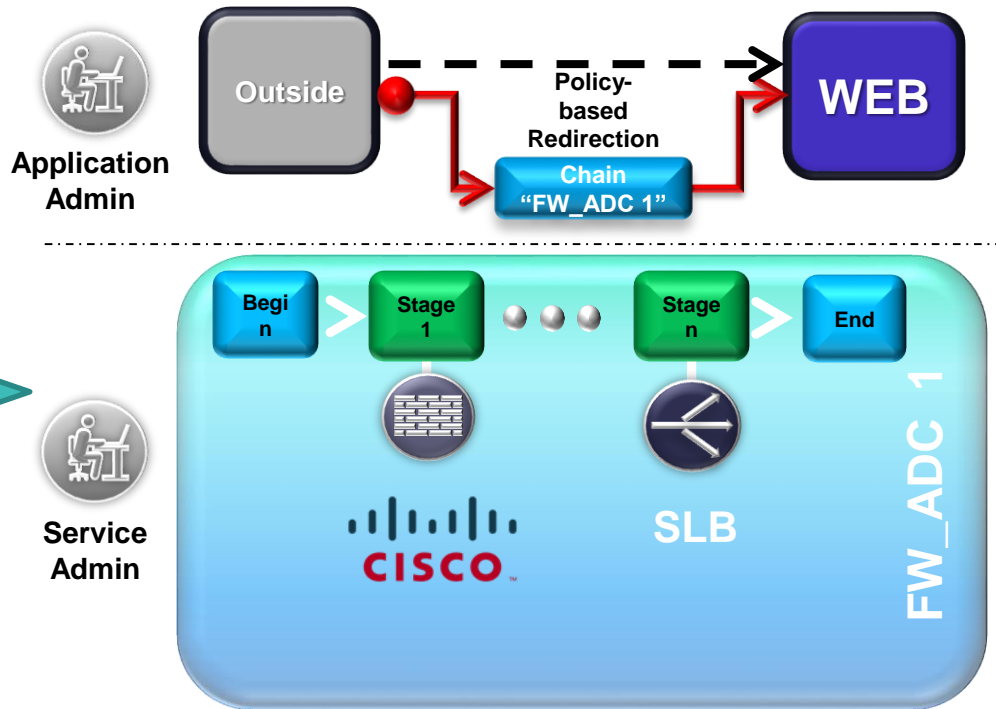
Application 1 Telemetry



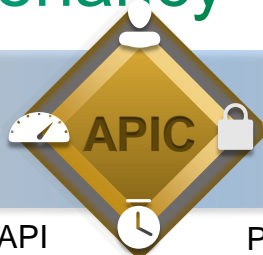
ACI service redirection policy



- Automated and scalable L4-L7 service insertion
- Packet match on a redirection rule sends the packet into a services graph.
- Service Graph can be one or more service nodes pre-defined in a series.



ACI Security with multitenancy



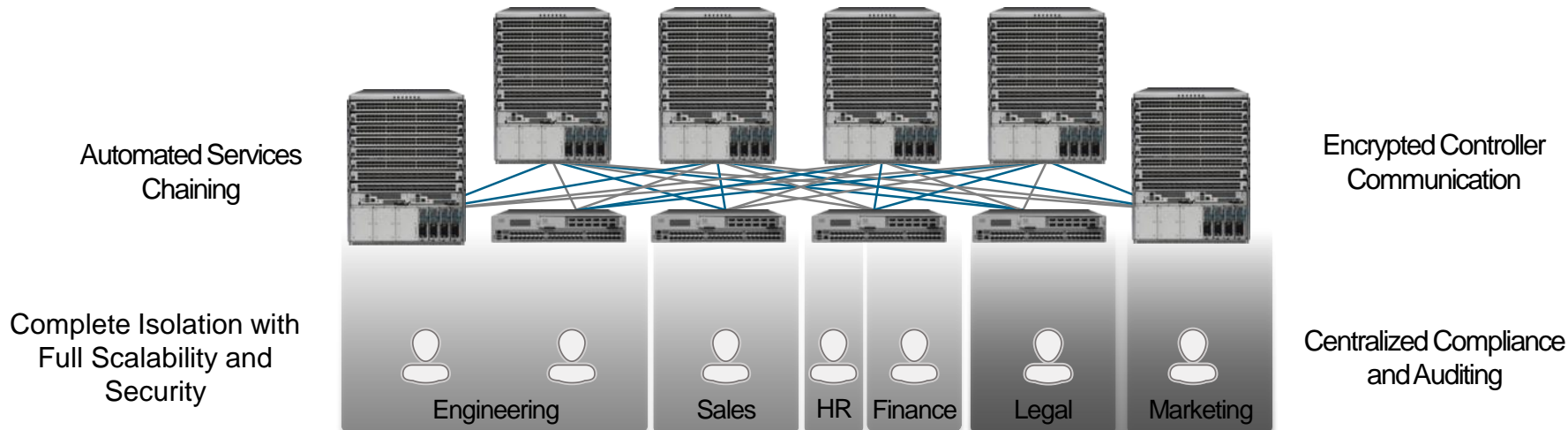
Policy Engine



Advanced Role Based Access Control

Import / Export Policy via API
(Support for External Policy Engines)

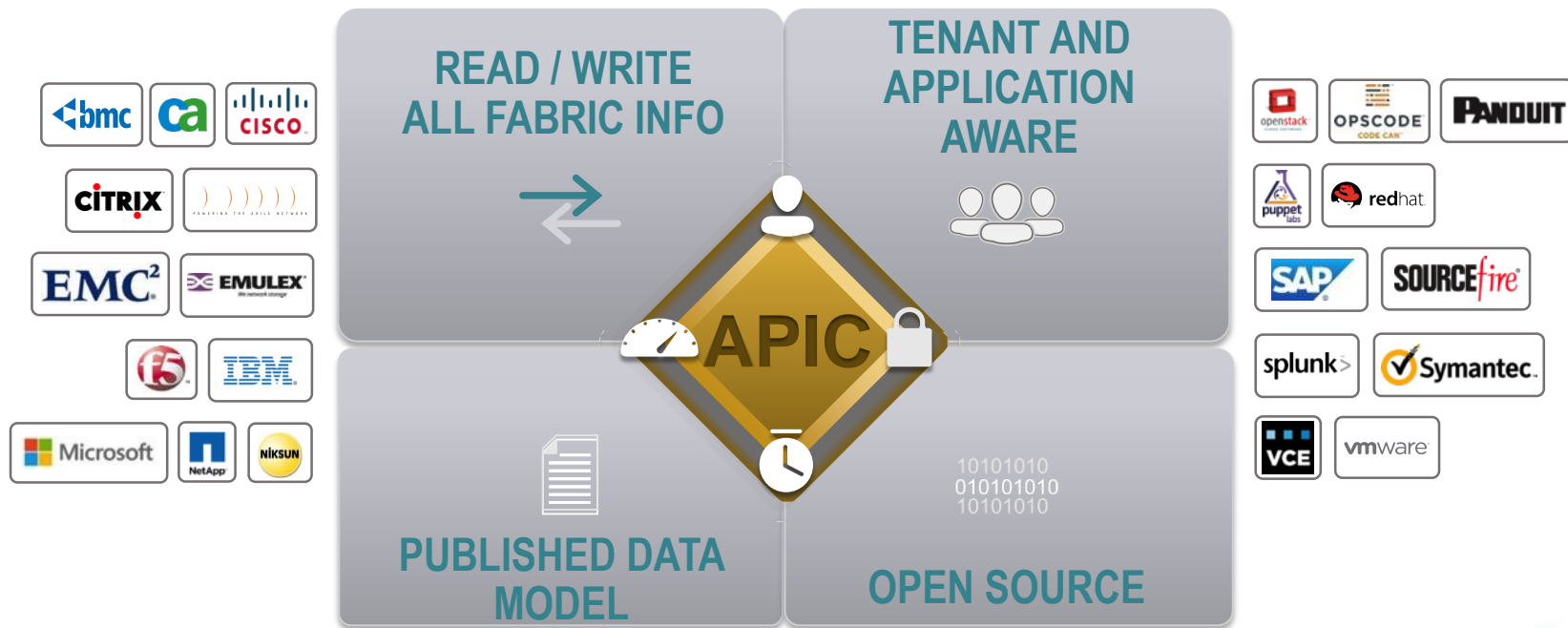
Policy Separated from Network Forwarding



ENABLING A DYNAMIC ENTERPRISE WITHOUT COMPROMISE

OPEN ECOSYSTEM, OPEN APIS

Comprehensive access to underlying information model



Industry Standard Compliant



FlexPod Certified

Key Takeaways

- **Policy-driven infrastructure and service management through contracts**
- **True network abstraction without compromising visibility & security**
- **Application Level Visibility**
- **Consistent model for physical, virtual and cloud**
- **Open and strong ECO System**



Thank you.

