Building YOURcloud:

The U.S. Government's First Secure Hybrid Community Cloud

Travis Howerton
&
Anil Karmel

U.S. DEPARTMEN
ENERG

DOE IT Modernization Strategy

TRANSFORM

Consolidate and Connect Enterprise Networks and Services to Create the DOE "Cloud of Clouds"

Establish Architecture, Policy and Standards that Embrace Platform and Device Diversity and Enable Timely Insertion of Disruptive Technologies

Streamline, Simplify and Reduce the Cost of IT Solutions and Acquisition

Develop a Corporate Data and Information Management Strategy

Align IT Governance with DOE's Integrated Management System

PROTECT

Establish JC3 Full Operational Capability for Information Sharing, Shared Analytics, Reporting and Collaborative Incident Response

Strengthen Cybersecurity Risk Management, Including Understanding and Managing our IT Supply Chain

Improve Cybersecurity Training and Awareness

ADVANCE

Establish and Advance the Cyber Sciences Laboratory

Engage the Best of Government, Industry, Academia and Innovators

TRANSFORM

Consolidate and Connect Enterprise Networks and Services to Create the DOE "Cloud of Clouds"

Establish Architecture, Policy and Standards that Embrace Platform and Device Diversity and Enable Timely Insertion of Disruptive Technologies

Streamline, Simplify and Reduce the Cost of IT Solutions and Acquisition

Develop a Corporate Data and Information Management Strategy

Align IT Governance with DOE's Integrated Management System

PROTECT

Establish JC3 Full Operational Capability for Information Sharing, Shared Analytics, Reporting and Collaborative Incident Response

Strengthen Cybersecurity Risk Management, Including Understanding and Managing our IT Supply Chain

Improve Cybersecurity Training and Awareness

TRANSFORM

Consolidate and Connect Enterprise Networks and Services to Create the DOE "Cloud of Clouds"

Establish Architecture, Policy and Standards that Embrace Platform and Device Diversity and Enable Timely Insertion of Disruptive Technologies

Streamline, Simplify and Reduce the Cost of IT Solutions and Acquisition

Develop a Corporate Data and Information Management Strategy

Align IT Governance with DOE's Integrated Management System

PROTECT

Establish JC3 Full Operational Capability for Information Sharing, Shared Analytics, Reporting and Collaborative Incident Response

Strengthen Cybersecurity Risk Management, Including Understanding and Managing our IT Supply Chain

Improve Cybersecurity Training and Awareness

ADVANCE

Establish and Advance the Cyber Sciences Laboratory

Engage the Best of Government, Industry, Academia and Innovators

PROTECT

Establish JC3 Full Operational Capability for Information Sharing, Shared Analytics, Reporting and Collaborative Incident Response

Strengthen Cybersecurity Risk Management, Including Understanding and Managing our IT Supply Chain

Improve Cybersecurity Training and Awareness

ADVANCE

Establish and Advance the Cyber Sciences Laboratory

Engage the Best of Government, Industry, Academia and Innovators

TRANSFORM

Consolidate and Connect Enterprise Networks and Services to Create the DOE "Cloud of Clouds"

Establish Architecture, Policy and Standards that Embrace Platform and Device Diversity and Enable Timely Insertion of Disruptive Technologies

Streamline, Simplify and Reduce the Cost of IT Solutions and Acquisition

Develop a Corporate Data and Information Management Strategy

Align IT Governance with DOE's Integrated Management System

PROTECT

Establish JC3 Full Operational Capability for Information Sharing, Shared Analytics, Reporting and Collaborative Incident Response

Strengthen Cybersecurity Risk Management, Including Understanding and Managing our IT Supply Chain

Improve Cybersecurity Training and Awareness

RIGHT PATH

Delivering revolutionary business transformation within a government agency requires navigating a complex maze

RightPath takes a lean and agile approach that provides integrated and effective technology solutions to business problems

People, Processes, + Technology

ONE Voice powered by YOUR cloud

Immersive Collaboration
+ Social Networking tools

Virtual Servers and Desktops hosted in
your Secure Hybrid, Community Cloud

ONE NNSA

ONE VOICE

YOURcloud

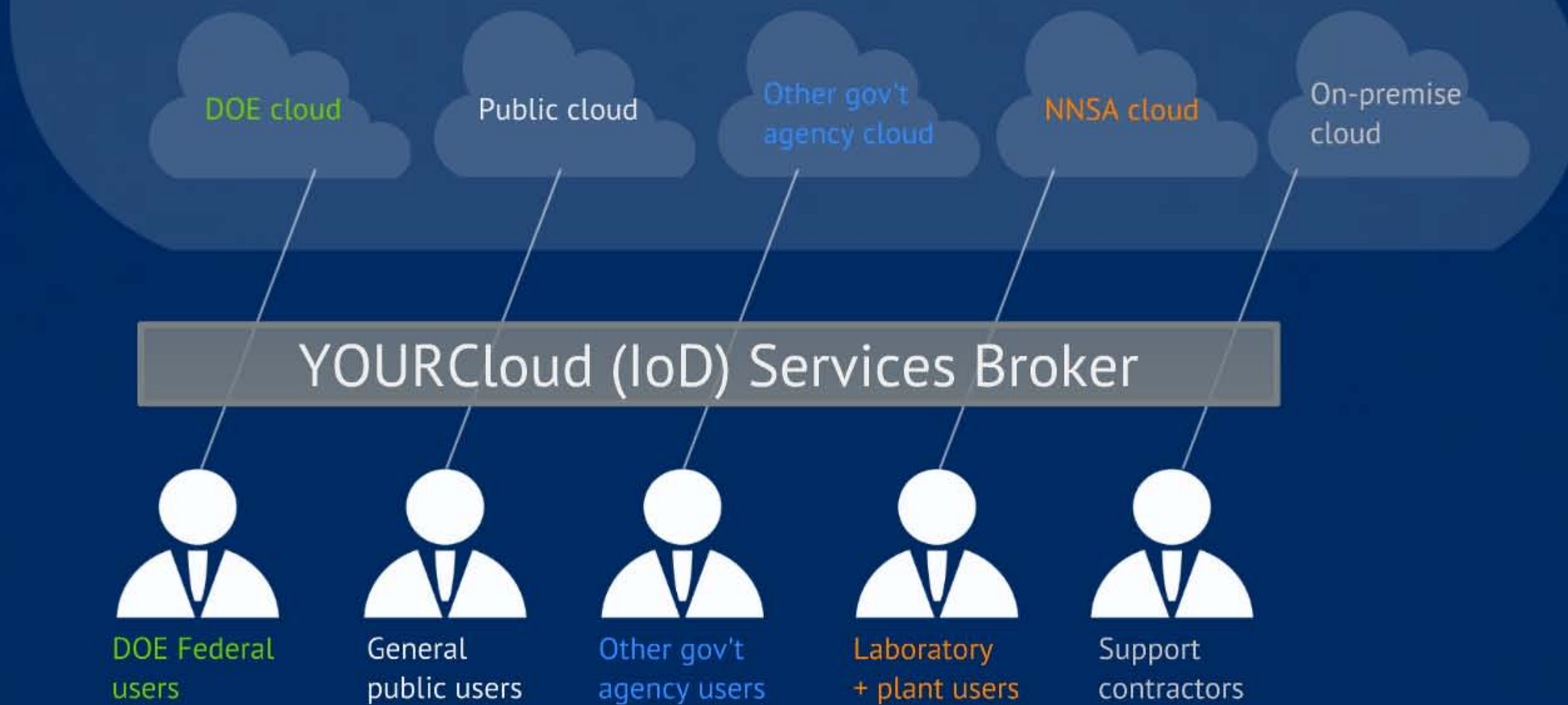
ONE NNSA

YOURcloud


YOURcloud
Private
DOE
Cloud of clouds
Public


YOURcloud
LLNL
NNSS
SNL/ABQ Complex
LANL
Pantex
KCP
Y-12
HQ
SRS

A Cloud of Clouds approach brokering any organization, through any device, to any service respectful of site autonomy, powered by the innovation of the National Labs



Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources

NIST

National Institute of Standards and Technology

Technology Administration, U.S. Department of Commerce

A recent study
conducted by MeriTalk found that
1/3 of the organization surveyed

have plans to
move some mission
critical apps to the cloud
in the next year

& up 44% of their mission critical apps in the next five years

http://www.meritalk.com/missioncriticalcloud

DOE IaaS Business Use Cases

Rapid deployment of servers to scientists

Security controls based on data sensitivity

Calculating energy savings

Disaster recovery

Capital expenditure reduction

DOE SaaS Business Use Cases

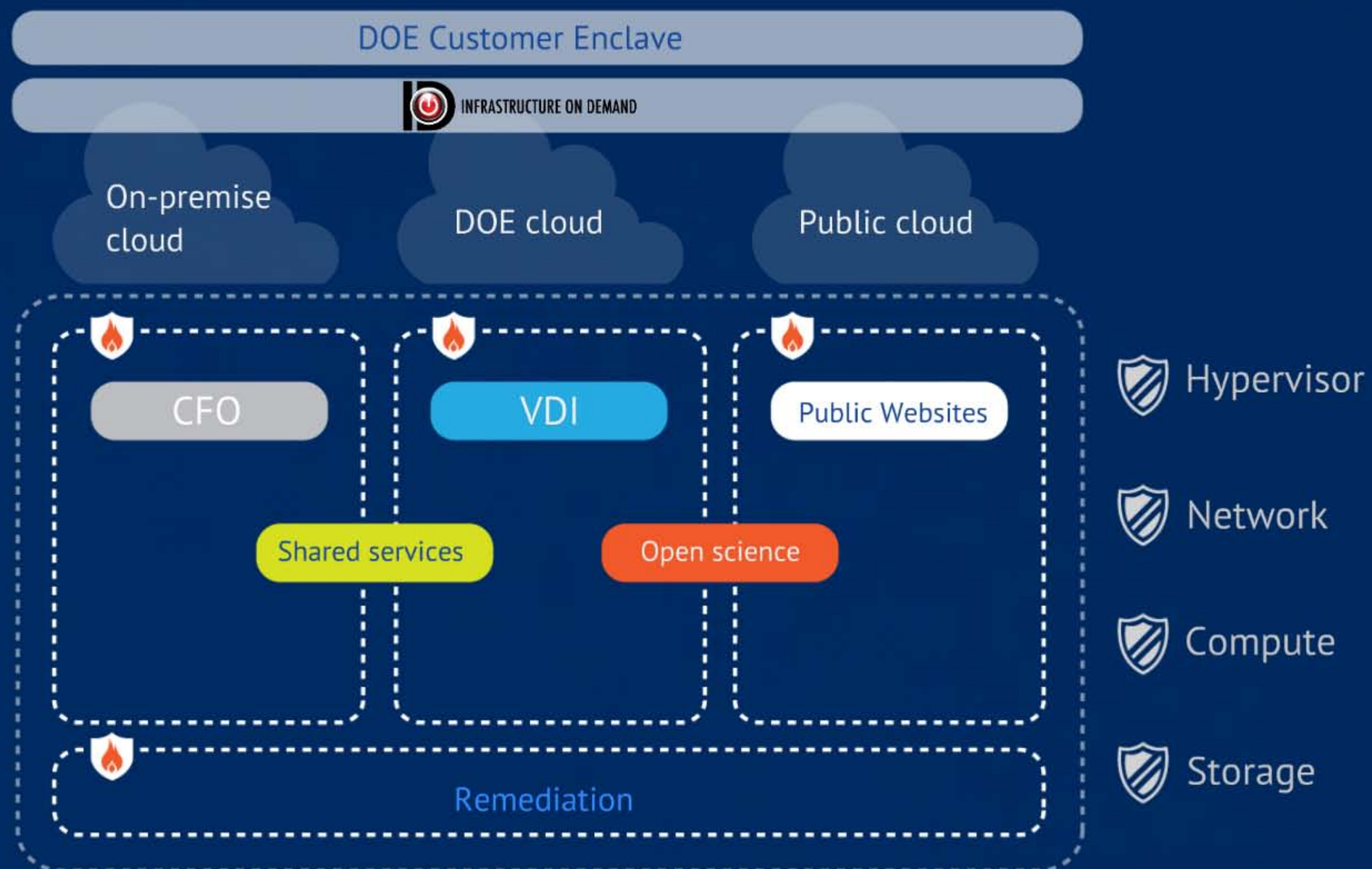
Social computing

Web conferencing

Instant messaging

Enterprise mobility

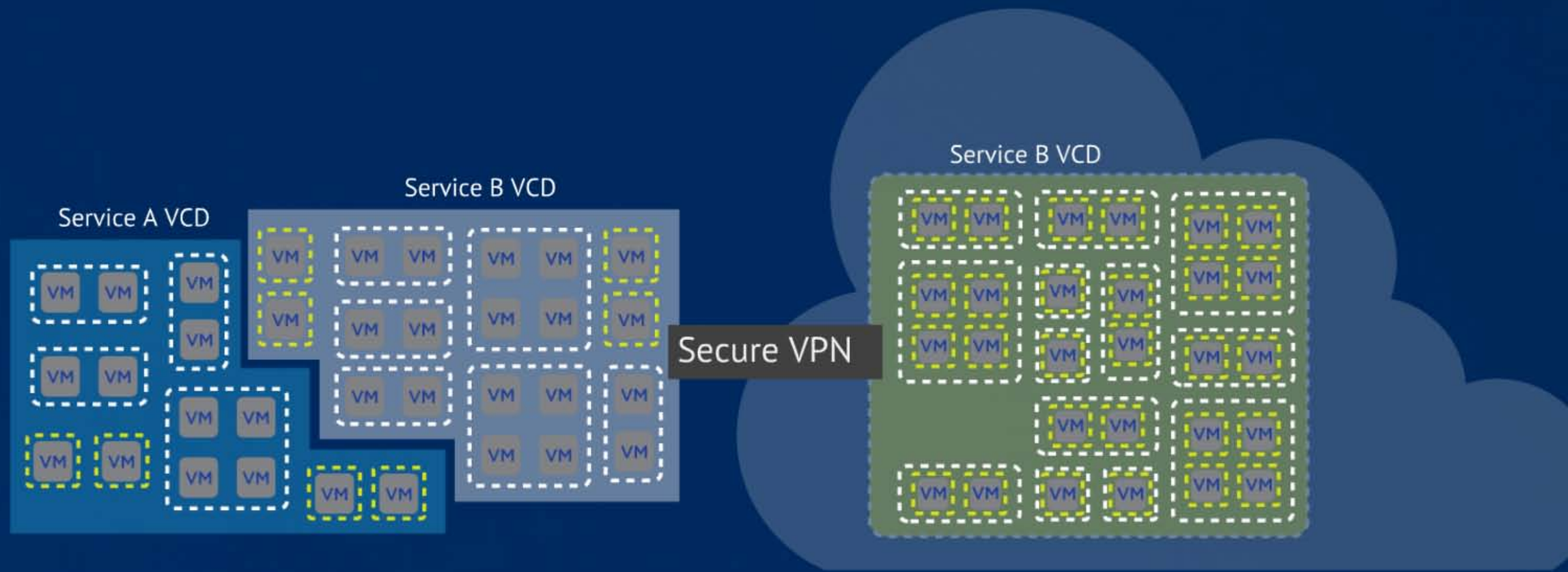
YOURcloud Service Broker Enclaves



Network Journey

Traditional Networking		Software Defined Networking
Complex	→	Simple
Rigid	→	Adaptive
Labor Intensive	→	Change Aware

Secure Hybrid Cloud Computing



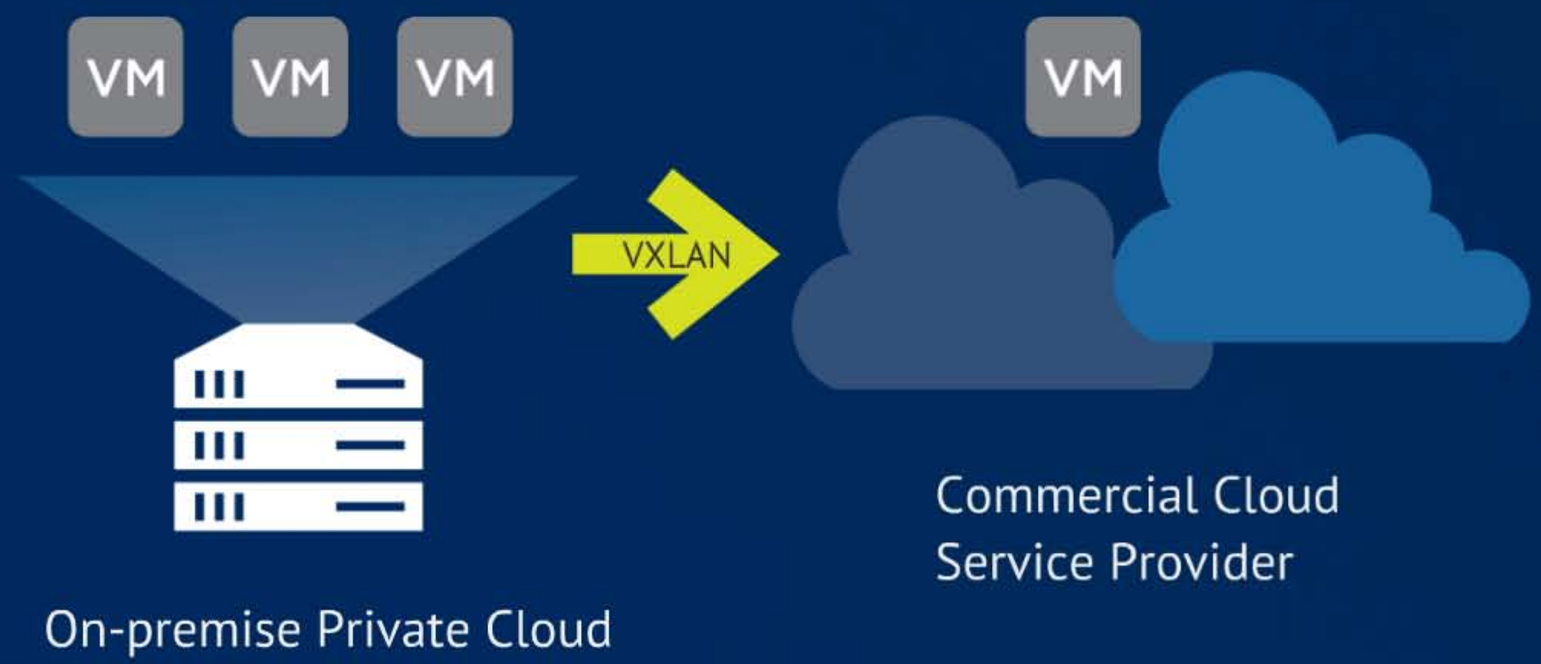
On-premise Private Cloud

Commercial Cloud
Service Provider

Cross Cloud Management Makes Hybrid Cloud Real

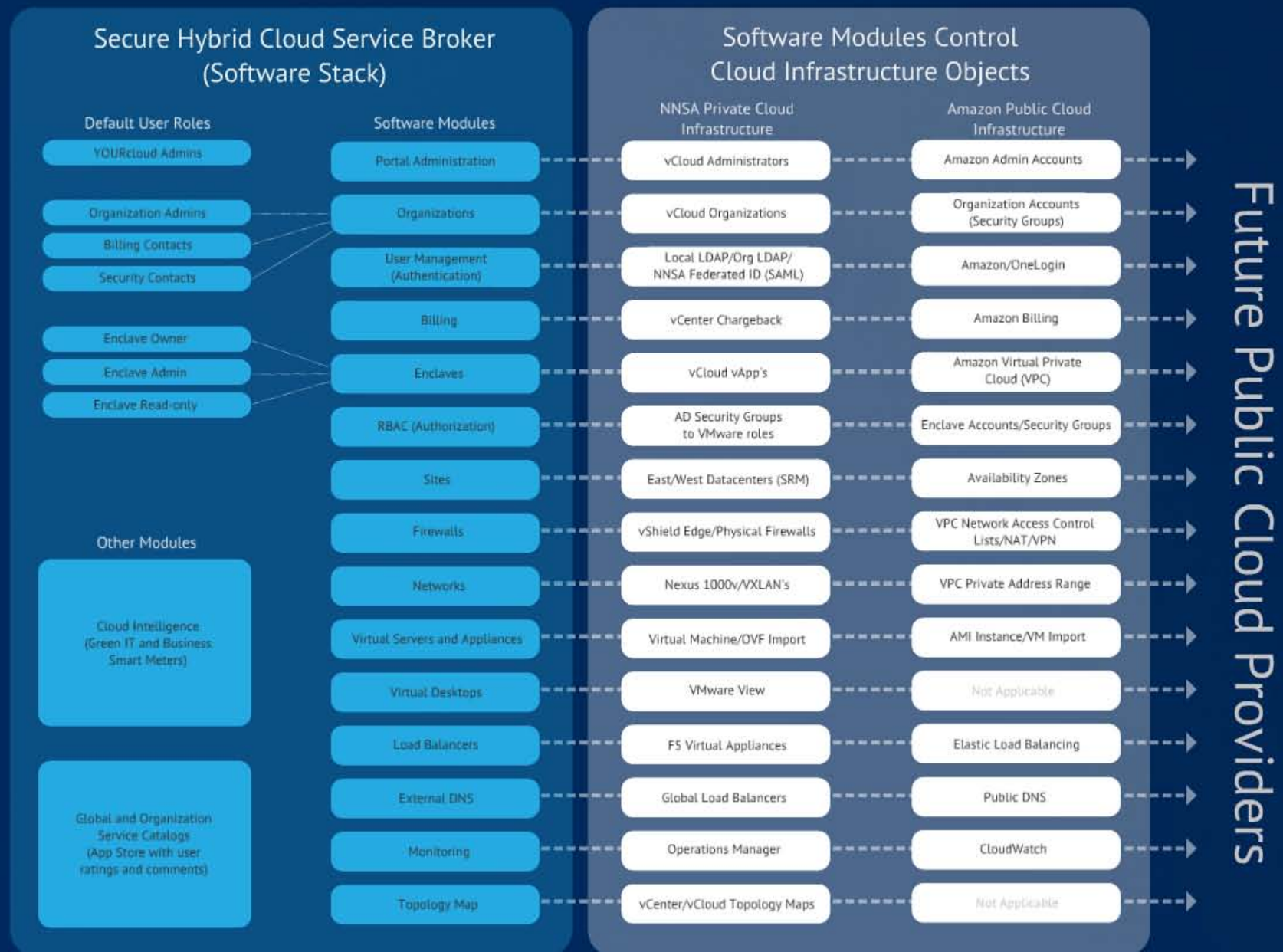
- Visualize resources across hybrid clouds
- Copy and operate resources across clouds
- Deliver enterprise level security

Elastic Compute

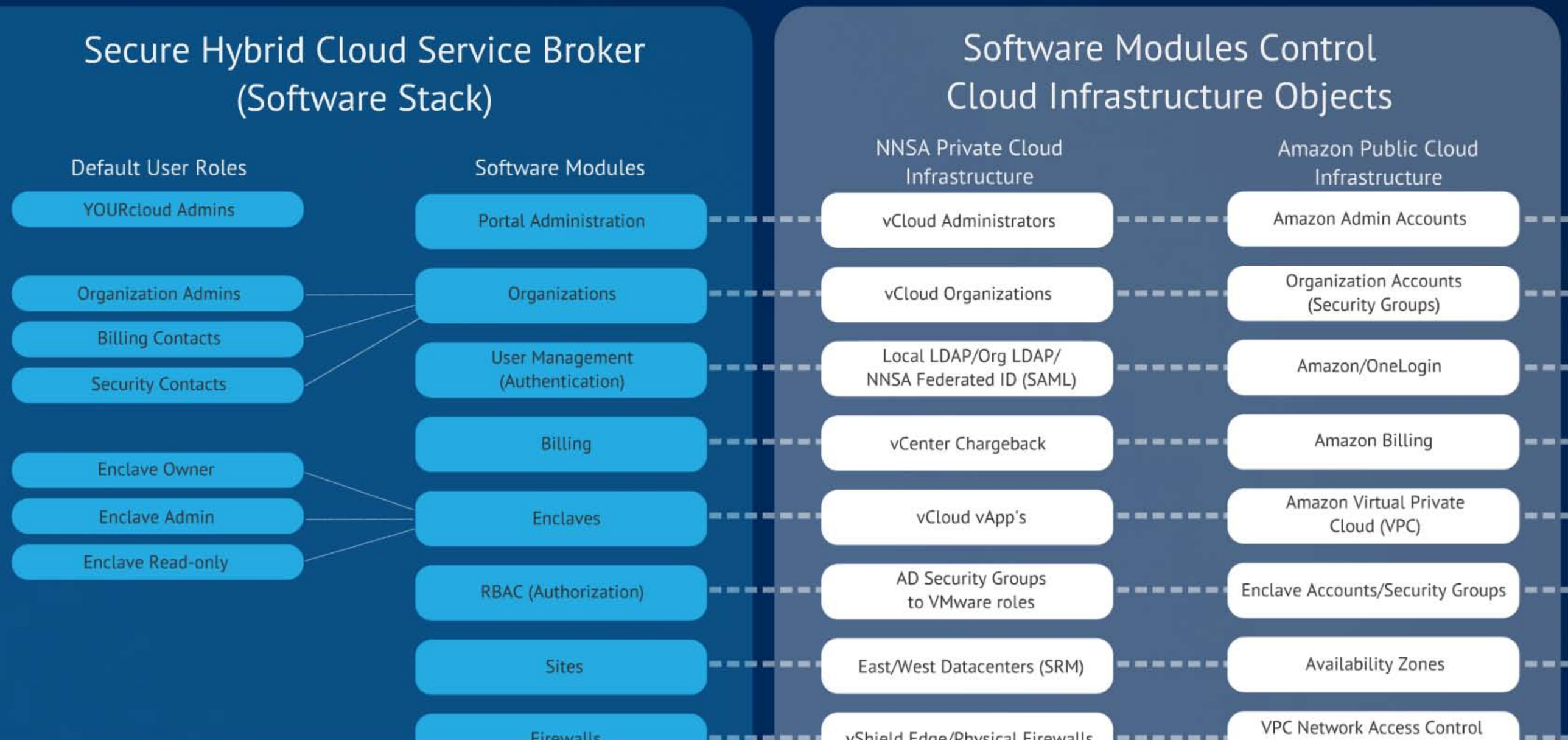


Management Framework

YOURcloud Service Broker Modules

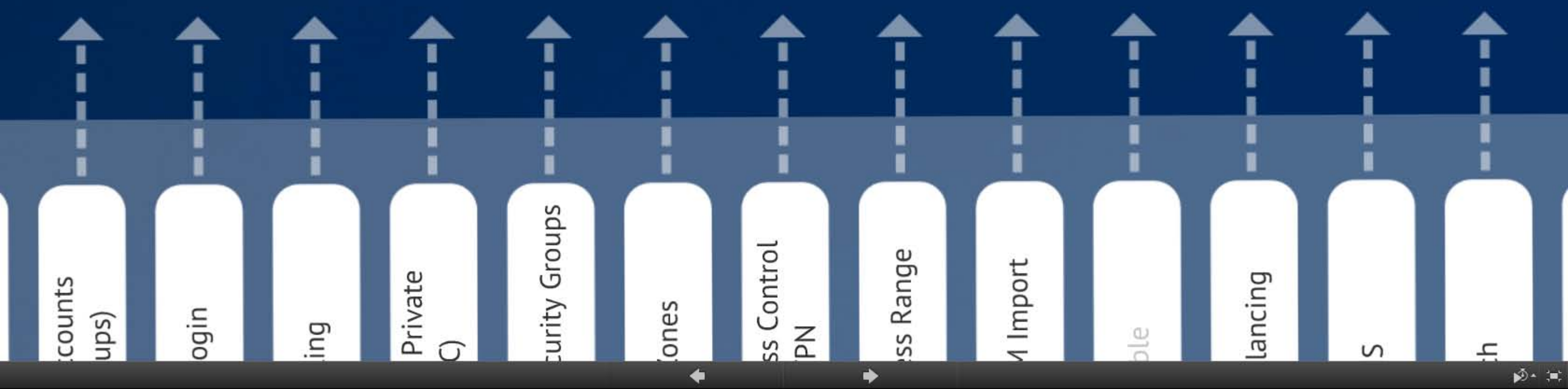


YOURcloud Service Broker Modules




Enclave Admin
Enclave Read-only
Enclaves
vCloud vApp's
Amazon Virtual Private Cloud (VPC)
RBAC (Authorization)
AD Security Groups to VMware roles
Enclave Accounts/Security Groups
Sites
East/West Datacenters (SRM)
Availability Zones
Firewalls
vShield Edge/Physical Firewalls
VPC Network Access Control Lists/NAT/VPN
Networks
Nexus 1000v/VXLAN's
VPC Private Address Range
Virtual Servers and Appliances
Virtual Machine/OVF Import
AMI Instance/VM Import
Virtual Desktops
VMware View
Not Applicable
Load Balancers
F5 Virtual Appliances
Elastic Load Balancing
External DNS
Global Load Balancers
Public DNS
Monitoring
Operations Manager
CloudWatch
Topology Map
vCenter/vCloud Topology Maps
Not Applicable
Other Modules
Cloud Intelligence (Green IT and Business Smart Meters)
Global and Organization Service Catalogs (App Store with user ratings and comments)

Future Public Cloud Providers

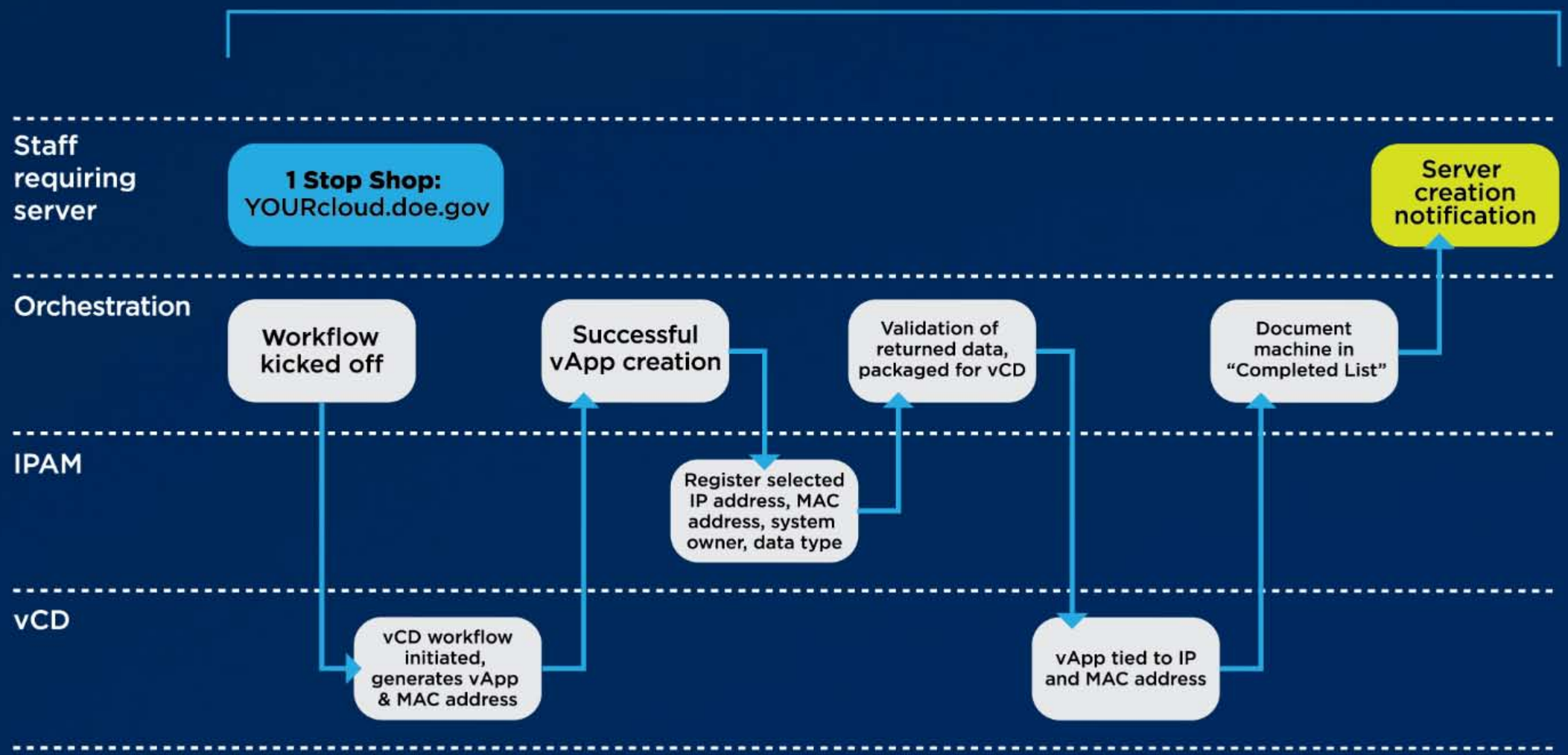


Secure Hybrid Community Cloud

LANL's Infrastructure on Demand is the first Infrastructure-as-a-Service secure hybrid cloud to automatically request and provision virtual servers.

Insfrastructure on Demand

30 minute setup



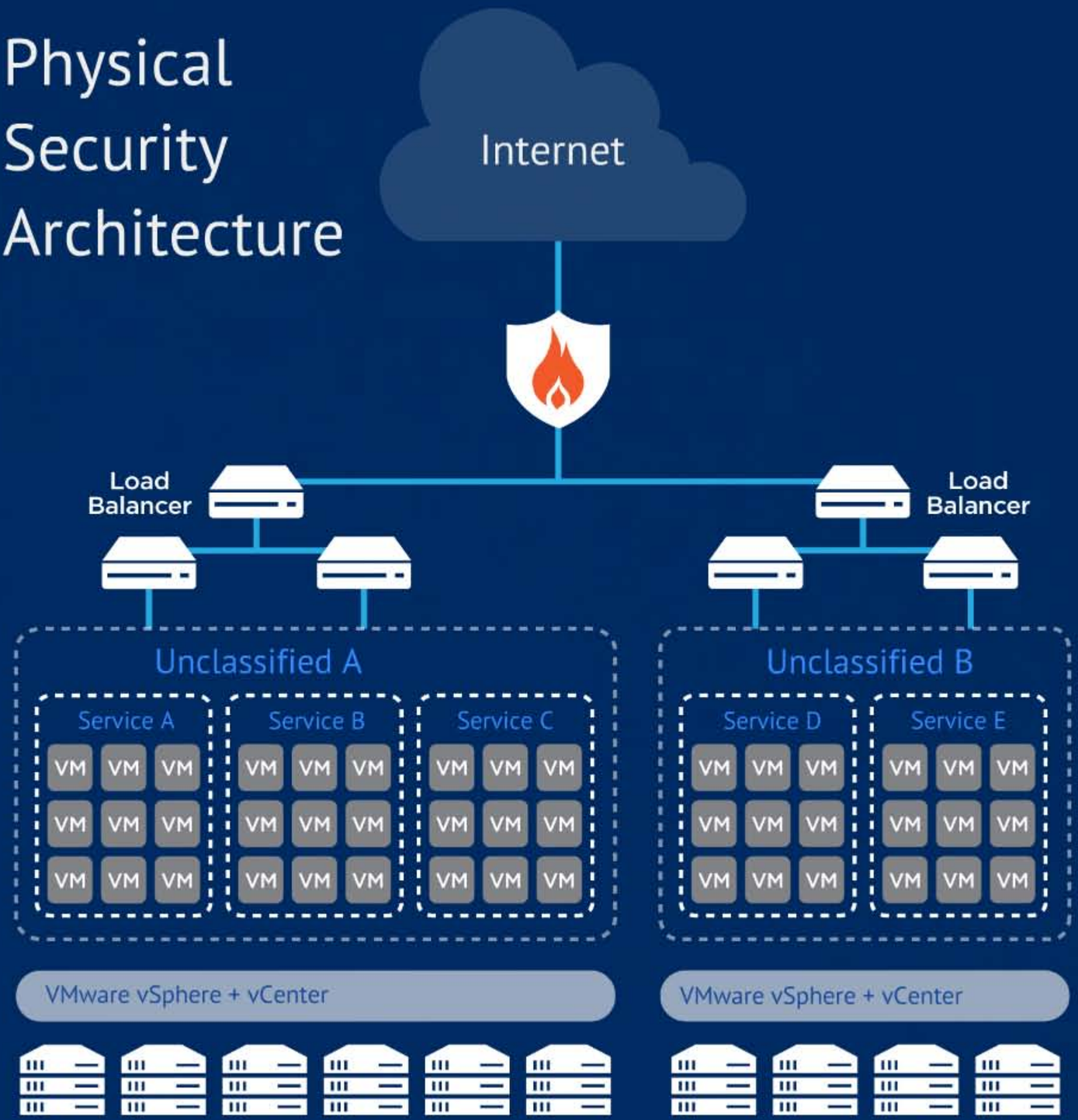
Security Journey

Security remains the number one concern IT professionals have when moving applications to the cloud environment

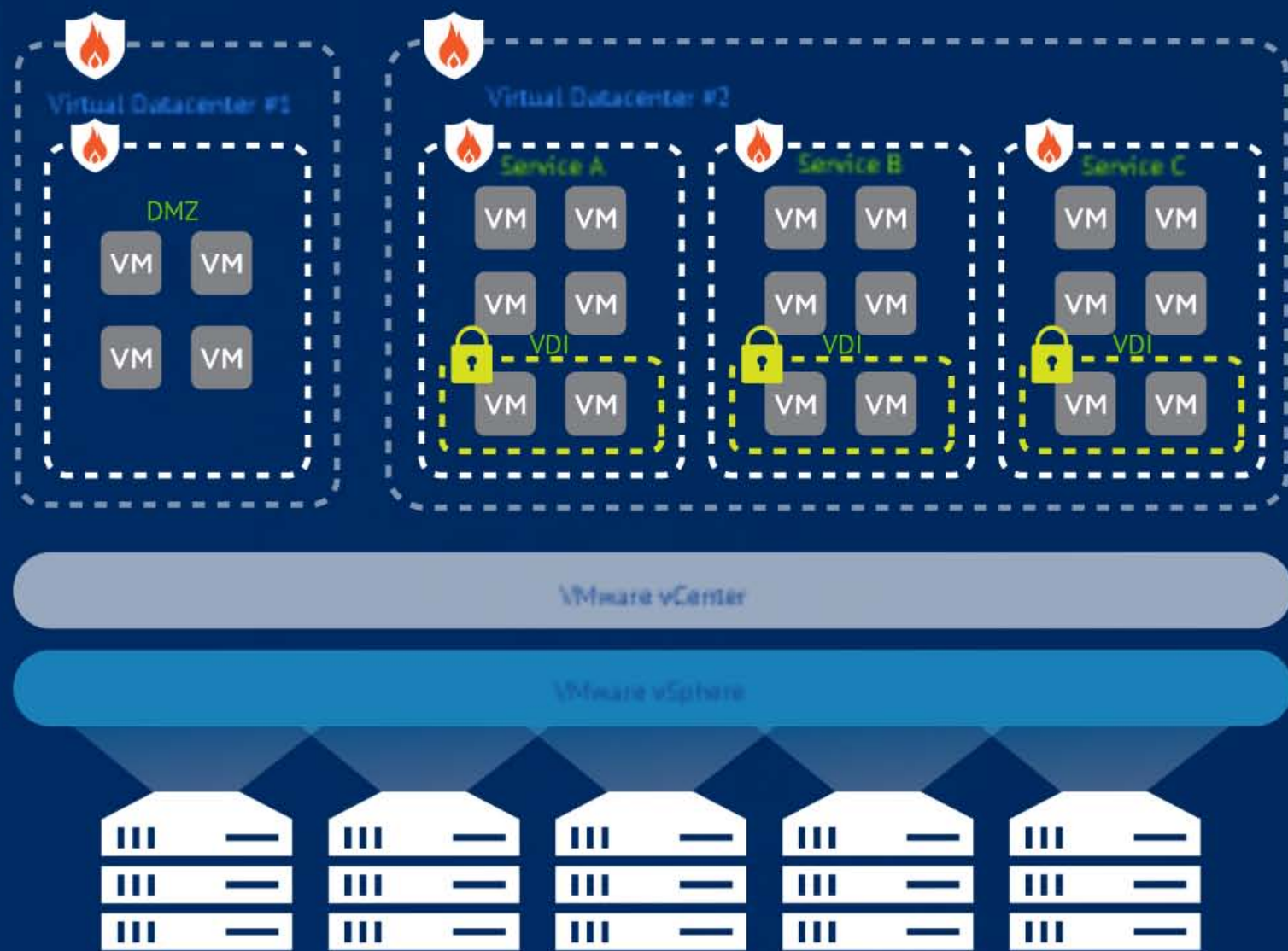
http://www.meritalk.com/missioncriticalcloud

Traditional Security		Virtualized Security
Complex	→	Simple
Rigid	→	Adaptive
Labor Intensive Compliance	→	Automatic Compliance

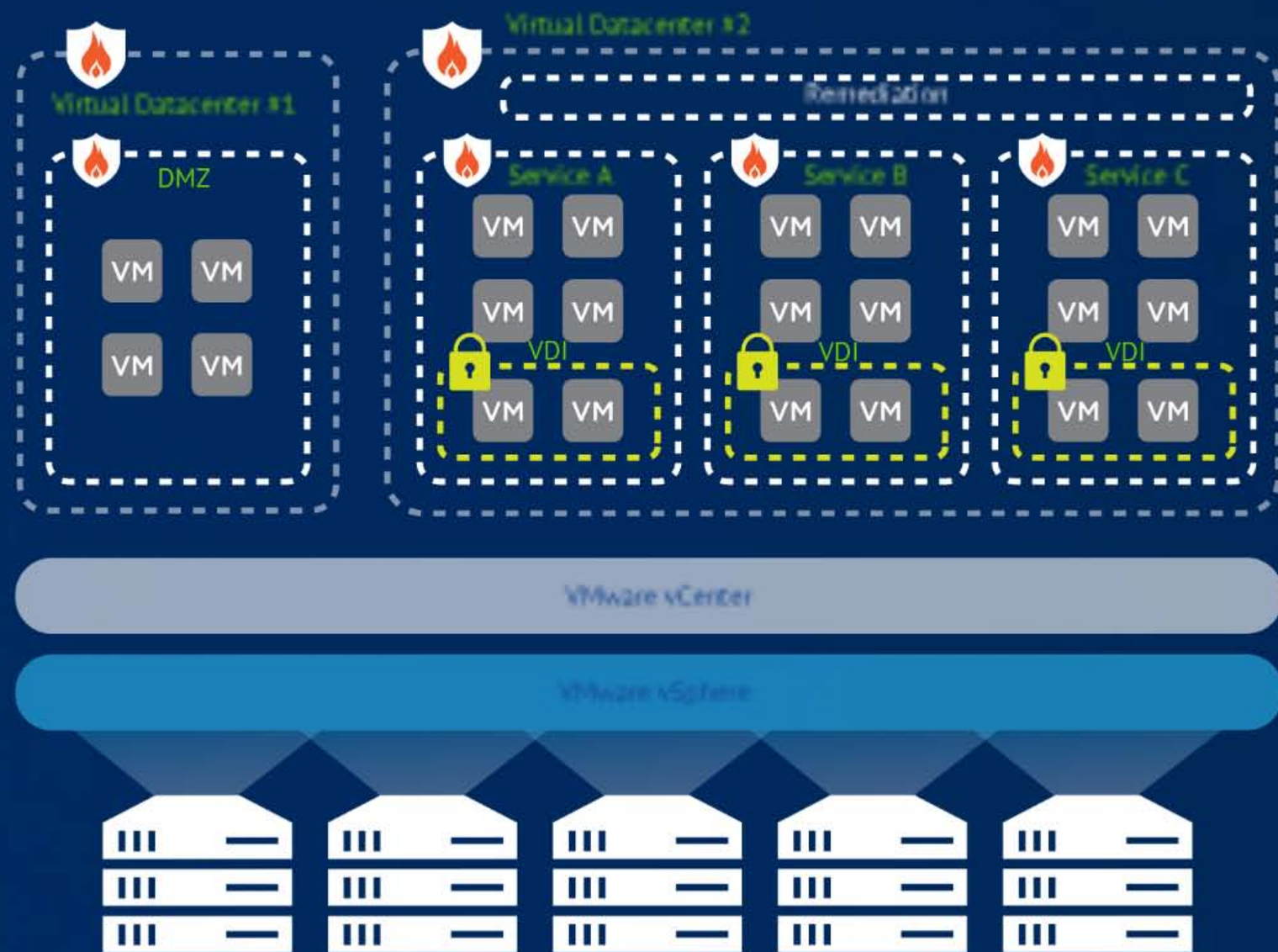
Physical Security Architecture



Cloud Security:
Protect the VDI Clients



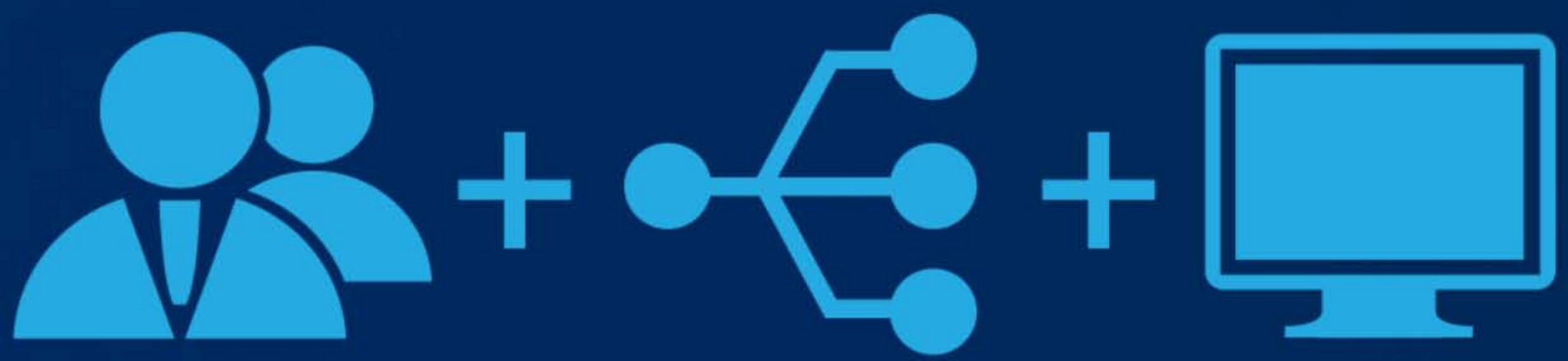
Cloud Security:
Quarantine Compromised Virtual Machines



How do we address this?

EDUCATION

People, Processes, + Technology



Organization Registration

Organization registration is a critical function of the service broker because it identifies the organizations top level contacts and ensures that unnecessary organization overlap is not occurring.

Technical Contacts

- Selecting Providers
- Creating Enclaves
- Granting Permissions
- Managing configurations

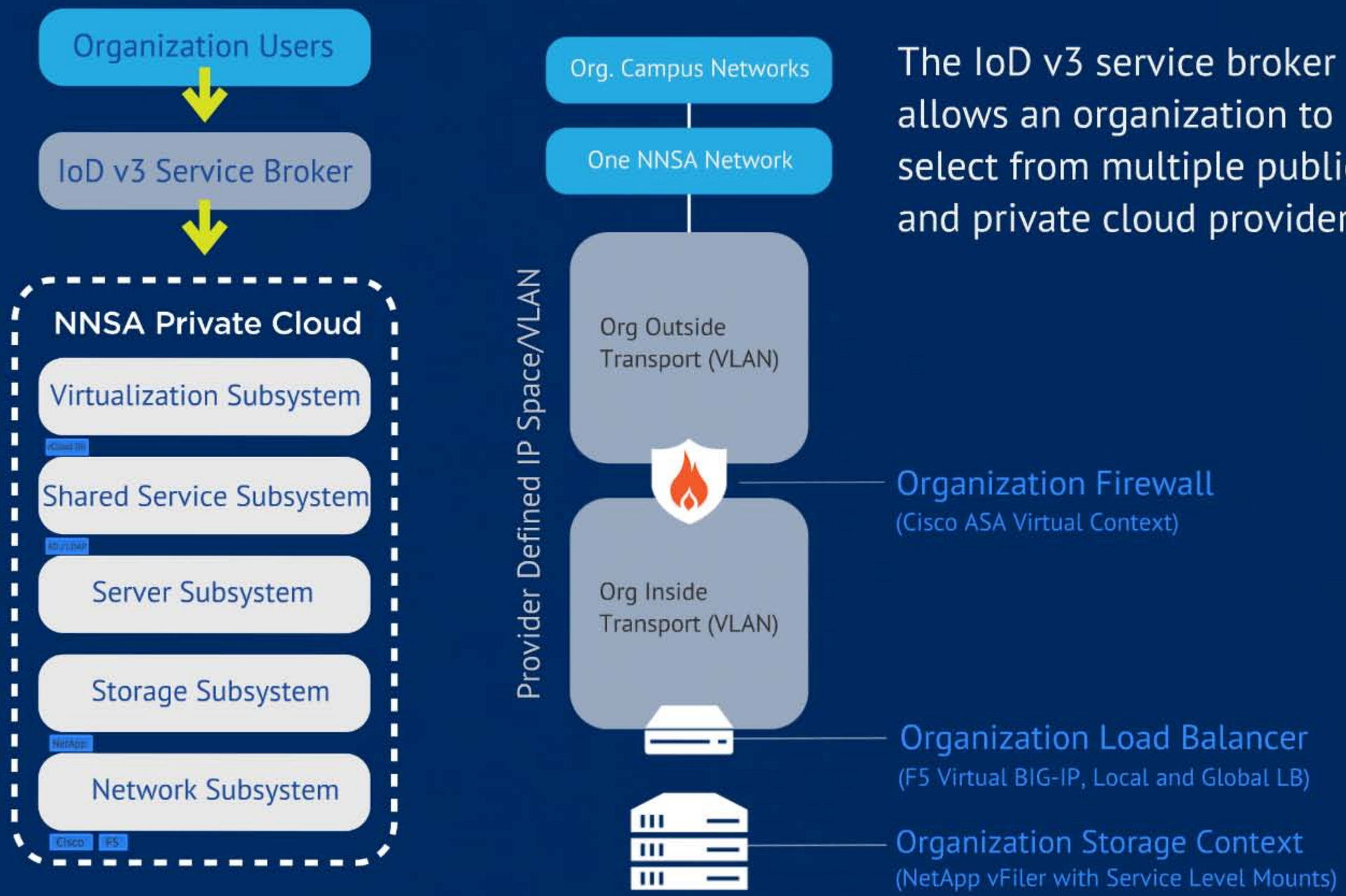
Security Contacts

- Receives Notifications
- Org Firewall Control
- Security functions outside of the system

Billing Contacts

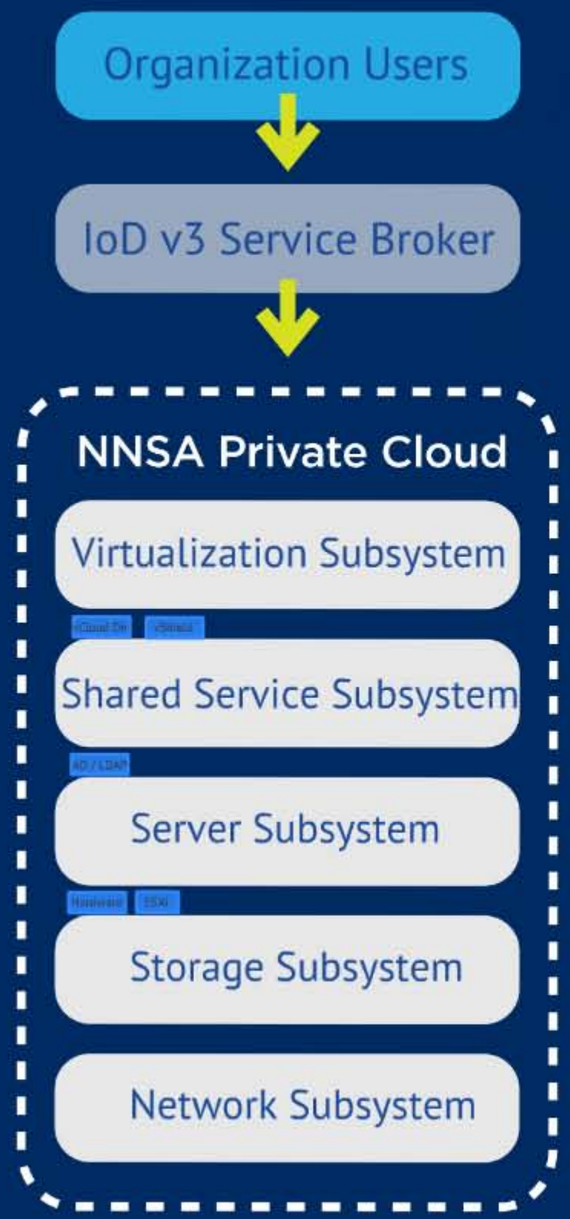
- Receives Notifications
- Billing Statement Controls
- Billing functions outside of the system

Provider Selection

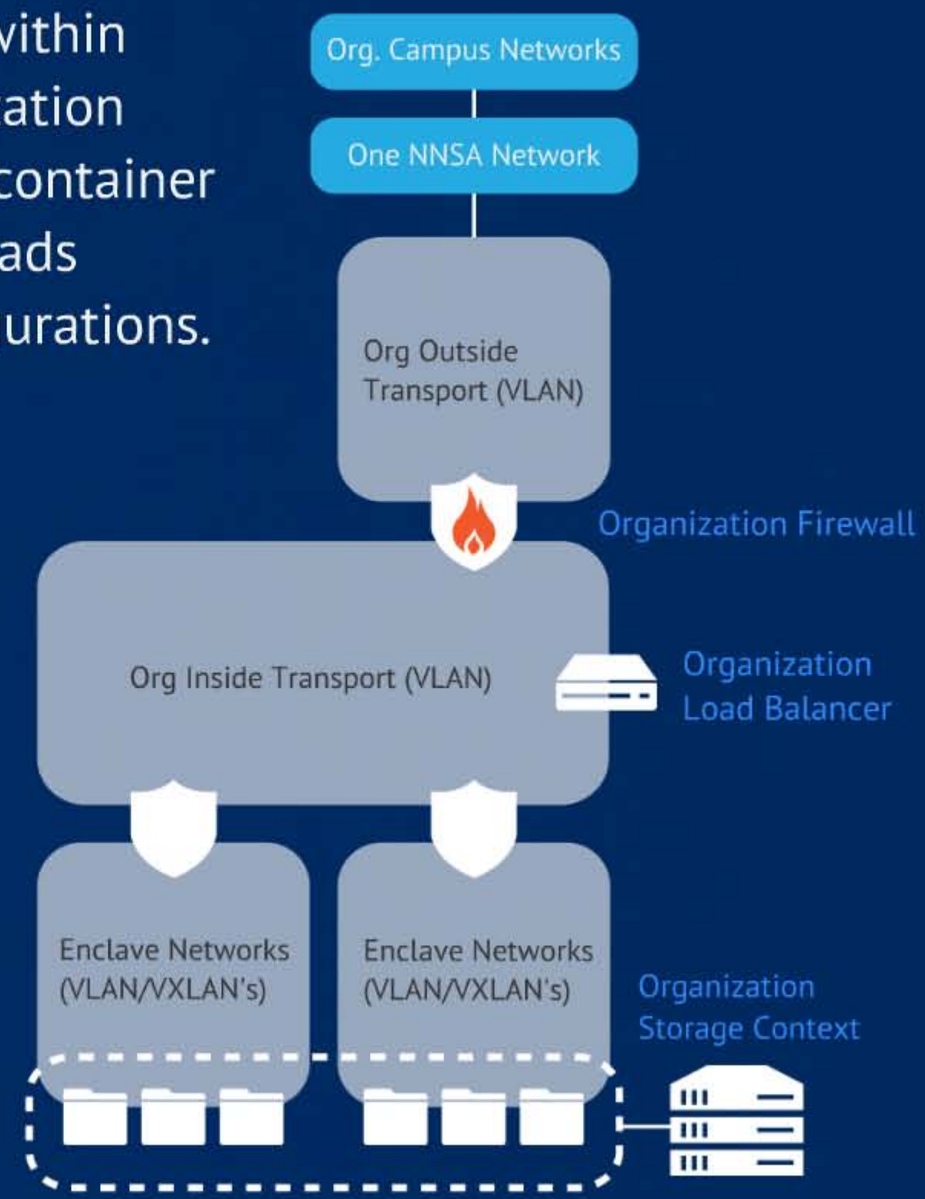


The IoD v3 service broker allows an organization to select from multiple public and private cloud providers.

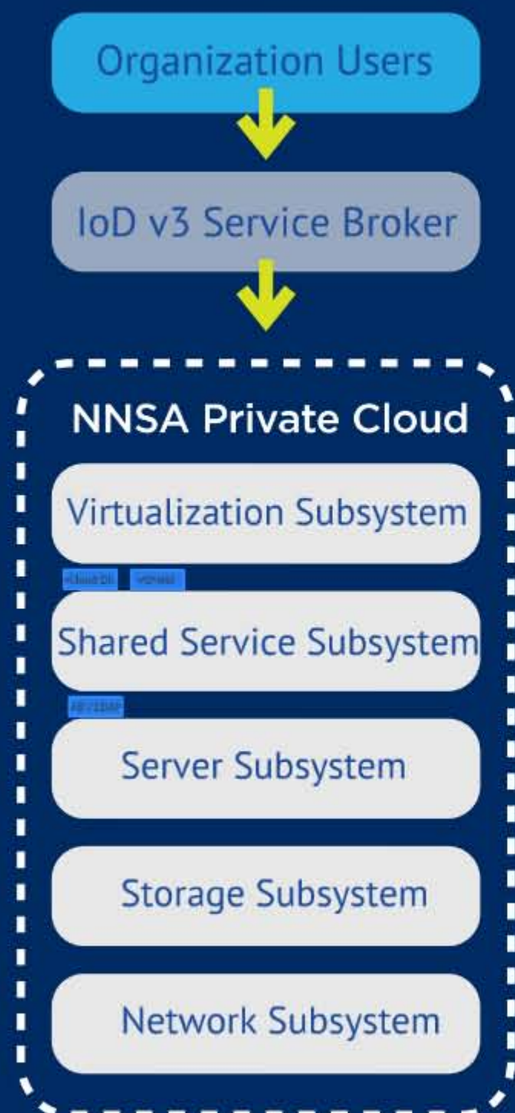
Enclave Creation



Enclaves within an organization provide a container for workloads and configurations.



Enclave RBAC



After an Enclave is created, Role Based Access Control (RBAC) is established by assigning permissions to the organization's technical staff.

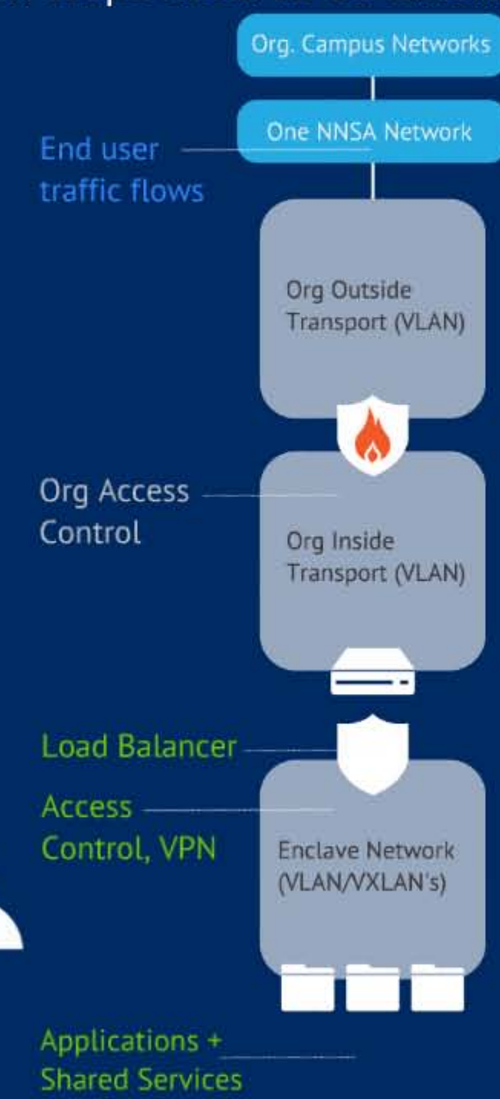
Enclave Management

Once an Enclave has been established and applications are ready to be presented to end users, several configuration steps need to be taken.

End Users

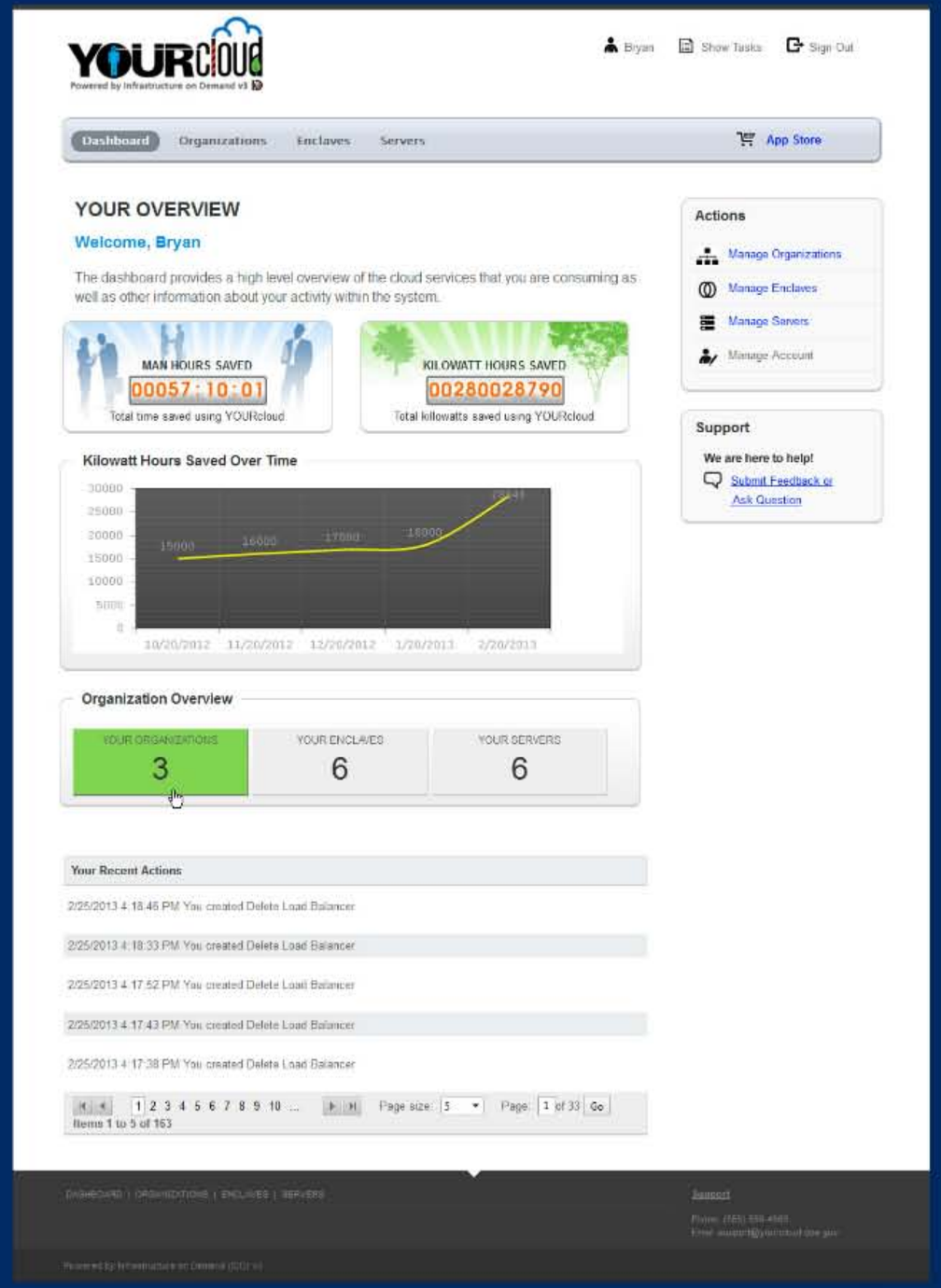
Technical + Security Contacts

Enclave Administrators



What should end users see?

Splash Screen



Enclave Management

YOURCloud
Powered by Infrastructure on Demand v3

Bryan | Show Tasks | Sign Out

Dashboard | Organizations | Enclaves | Servers | App Store

Dashboard > Enclave List > Enclave Management (flash)

FLASH

This page provides an overview of the Enclave's current configuration. Use the links listed below in the actions menu to manage resources within this Enclave.

General Information

Organization Name:	DOE
Provider Name:	Amazon Web Services
Location Name:	US West (N. California)
Service Level:	Gold
Owned By:	James Archuleta

Enclave Overview

NUMBER OF NETWORKS	NUMBER OF SERVERS	NUMBER OF USERS
0	0	2

Actions

- Change Owner
- Manage Networks
- Manage Servers
- Manage Load Balancers
- Manage Firewall
- Manage Users
- Enclave Topology

Support

We're here to help!
Submit Feedback or Ask Question

DASHBOARD | ORGANIZATIONS | ENCLAVES | SERVERS

Support

Create Load Balancer

YOURcloud
Powered by Infrastructure on Demand v3

Bryan | Show Tasks | Sign Out

Dashboard | Organizations | Enclaves | Servers | App Store

Dashboard > Enclave List > Enclave Management (flash) > Load Balancer > Load Balancer Create

CREATE LOAD BALANCER

Use this form to create a new load balancer. Scroll over the tool tips if you need more direction for a specific input field.

Basic Information

Load Balancer Name:

Load Balancer Description:

Servers

Virtual Servers:

Initial Rule

Load Balancer Protocol: TCP

Load Balancer Port:

Server Protocol: TCP

Server Port:

Actions

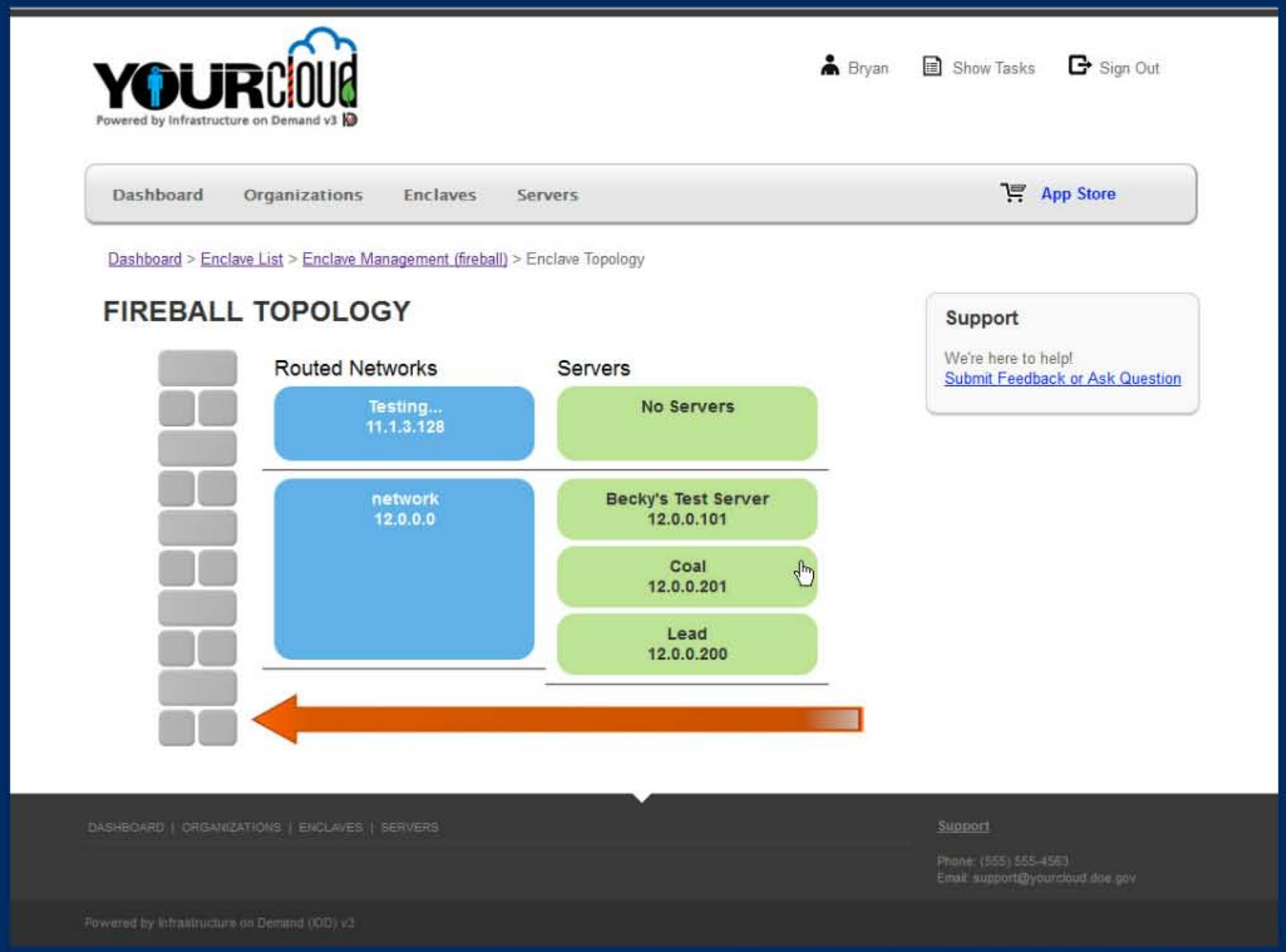
Submit

Cancel

Support

We're here to help!
Submit Feedback or Ask Question

Firewall Topology



Business

Cost Savings

Federal
7% annu

gs

Federal CIOs and IT managers report an average 7% annual savings after moving to the cloud

e

$5.5 billion saved

How to get to the cloud

- Leverage managed cloud service providers with strong SLAs
- Focus on mission or security requirements
- Ensure strong competition to drive down pricing
- Understand billing/charge-back prior to start dates
- Involve security from the beginning

- Dynamic Cost Calculator
- Chargeback / Showback
- Green and Business IT Smart Meters
- Enterprise Application Store
- 30 Minute Set Up

Technical

- Unified Management across private, h
public clouds
- Broker Concept – cloud computing m
agency
- Advanced Orchestration – no touch
- Comprehensive Management
  - Networks and Firewalls
  - Load Balancers
  - DNS
- Workload Management

- Unified Management across private, hybrid and public clouds
- Broker Concept – cloud computing meets travel agency
- Advanced Orchestration – no touch
- Comprehensive Management
    - Networks and Firewalls
    - Load Balancers
    - DNS
- Workload Management

Security

- Software Defined Security
  - Network
  - Storage
  - Compute
- Adaptive Security
  - VDI
  - Remediation Enclave
- Interactive Intelligence
  - Business
  - Social
  - Cyber

eam

- Software Defined Security
  - Network
  - Storage
  - Compute
- Adaptive Security
  - VDI
  - Remediation Enclave
- Interactive Intelligence
  - Business
  - Social
  - Cyber

Virtual Workforce

Cloud • Big Data

Mobility • Social •

What's Next?

Insource Security, Outsource Compute

- Transparent Data Encryption
- Secure Workload Portability
- Automated Risk Analysis
- Moving Target Security
- Software Defined Security

Rapid Results

Begin with the end goal in mind.

Low Risk

Focus on real business solutions.

Low Cost

Take a lean, agile approach to technology.

Mobility
Cloud
Social
Big Data

Building YOURcloud:

The U.S. Government's First Secure Hybrid Community Cloud

Travis Howerton
&
Anil Karmel

NNSA National Nuclear Security Administration

U.S. DEPARTMENT OF ENERGY