

# Building YOURcloud:

---

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

Travis Howerton  
&  
Anil Karmel



U.S. DEPARTMENT OF  
**ENERGY**

# 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

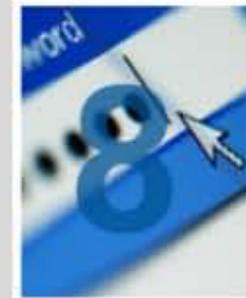
# PROTECT



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

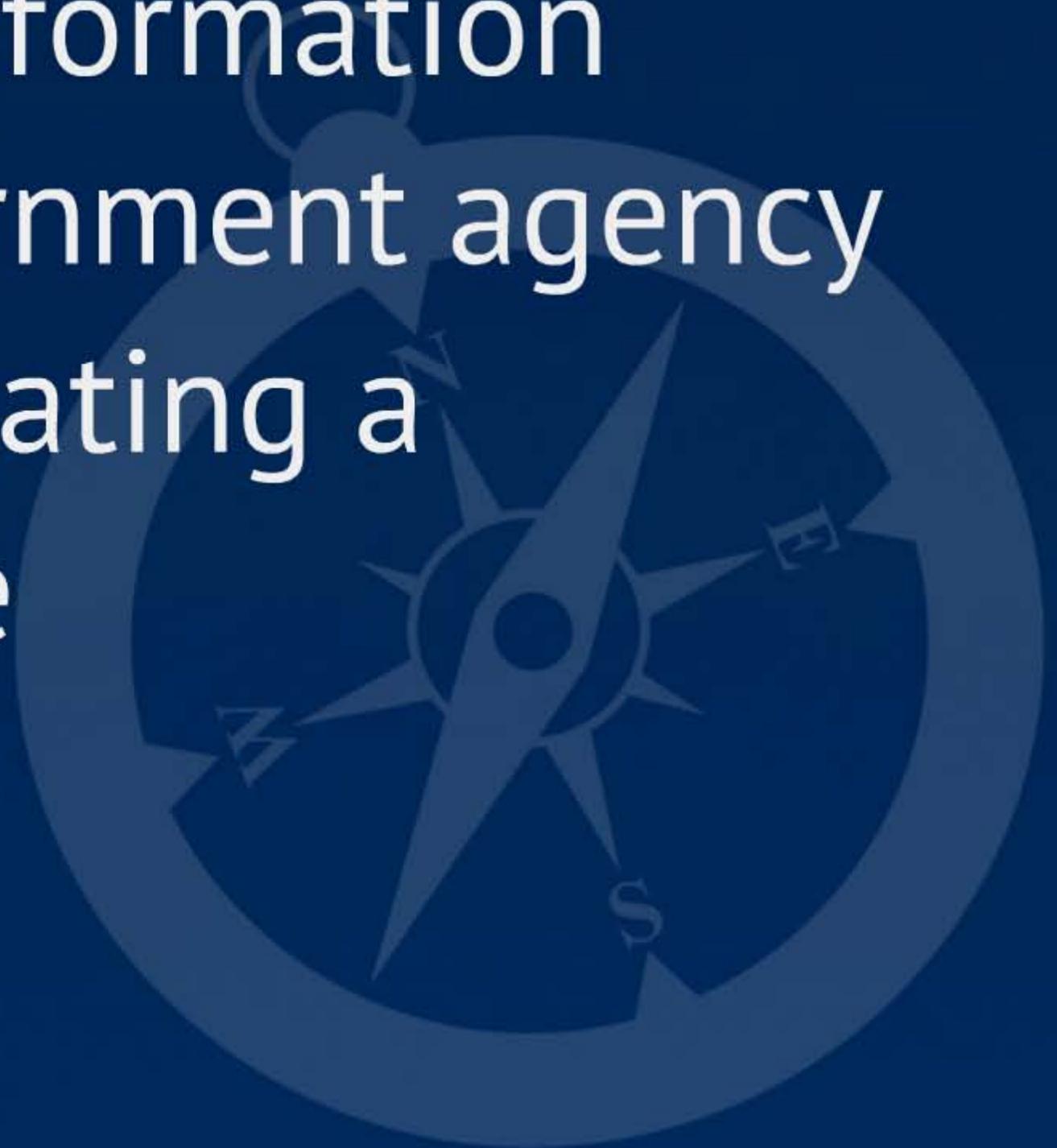


Improve Cybersecurity Training and Awareness



**RIGHT** **PATH**

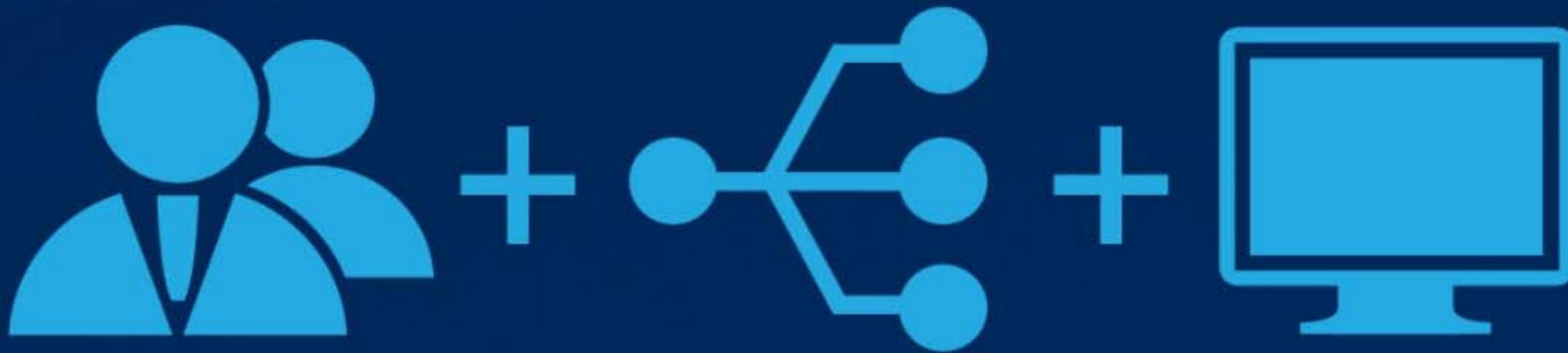
Delivering revolutionary  
business transformation  
within a government agency  
requires navigating a  
complex maze



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



People, Processes,  
+ Technology





Immersive Collaboration  
+ Social Networking tools

powered by



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





YOURcloud

The logo features the text 'YOURcloud' in a white, bold, sans-serif font. The letter 'O' in 'YOU' contains a blue silhouette of a person. The letter 'C' in 'cloud' is filled with red and white diagonal stripes. Above the letters 'C', 'l', 'o', and 'u' is a blue outline of a cloud. The letter 'd' at the end of the word contains a green leaf icon.



ONE NNSA

The logo consists of a white circle on the left containing a blue molecular structure of interconnected nodes. A blue line extends from the top of this circle, runs horizontally to the right, and then drops vertically to the top of the letter 'N' in 'NNSA'. The word 'ONE' is in white, and 'NNSA' is in blue.

YOURcloud

The logo features the text 'YOURcloud' in a white, bold, sans-serif font against a dark blue background. The letter 'O' in 'YOU' contains a blue silhouette of a person. The 'c' in 'cloud' is filled with a red and white diagonal striped pattern. Above the 'cloud' part of the text is a blue outline of a cloud. The letter 'd' in 'cloud' contains a green leaf icon. At the bottom of the image, there is a white curved shape that resembles a horizon line.

Private

DOE  
Cloud of clouds

Public



LLNL

NNSS

SNL/ABQ  
Complex

LANL

Pantex

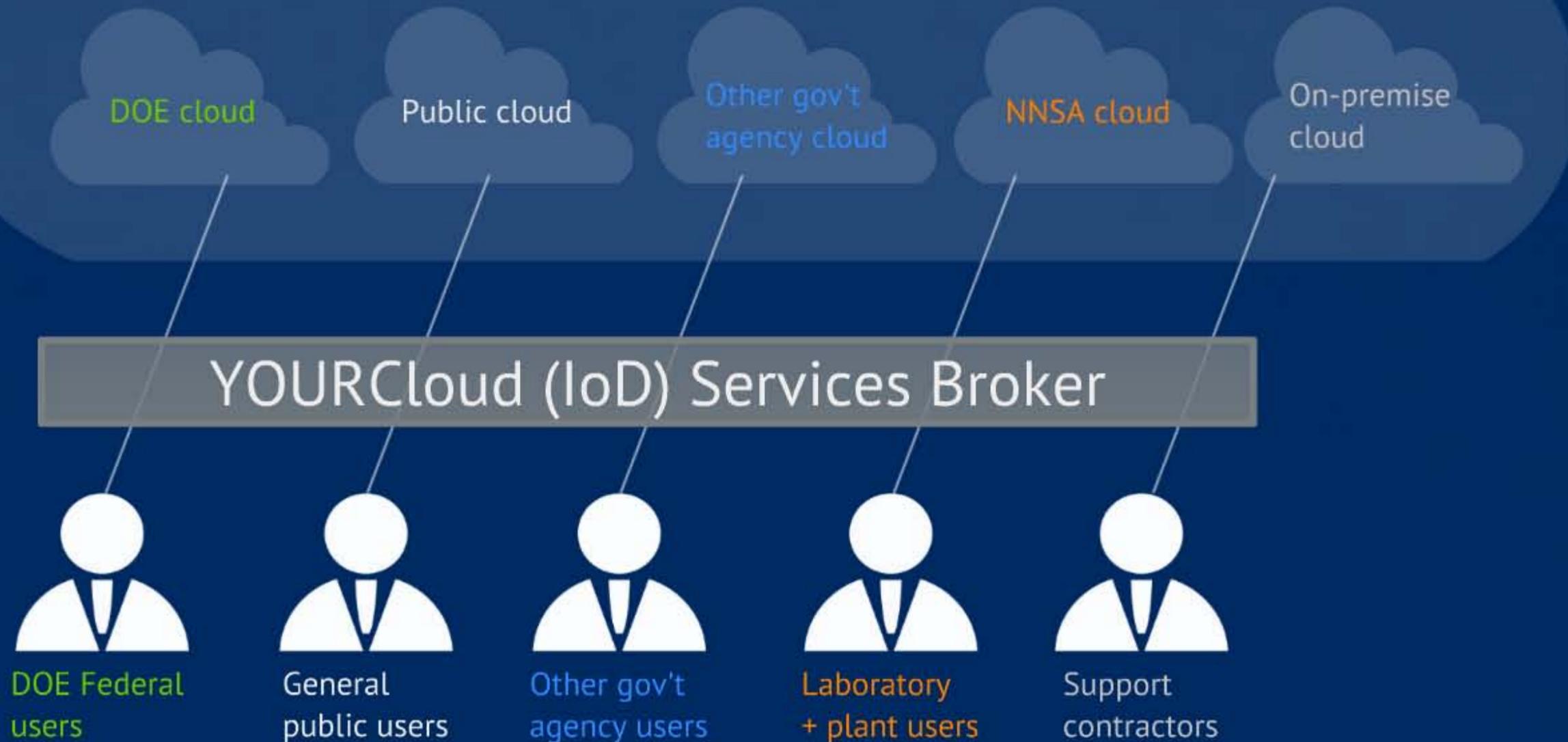
KCP

Y-12

SRS

HQ

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

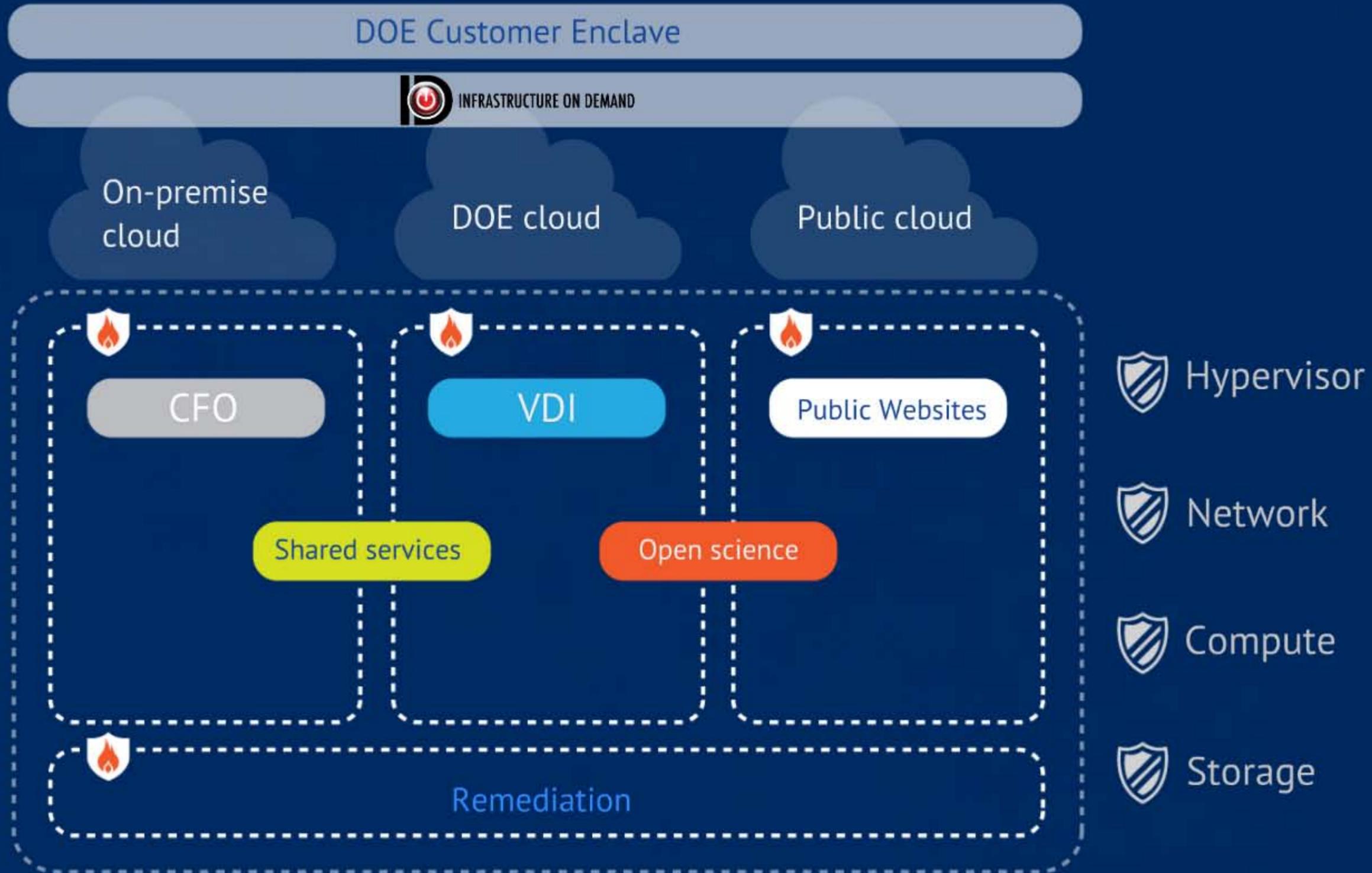


Instant  
messaging



Enterprise  
mobility

# YOURcloud Service Broker Enclaves



# Network Journey



## Traditional Networking

## Software Defined Networking

Complex



Simple

Rigid



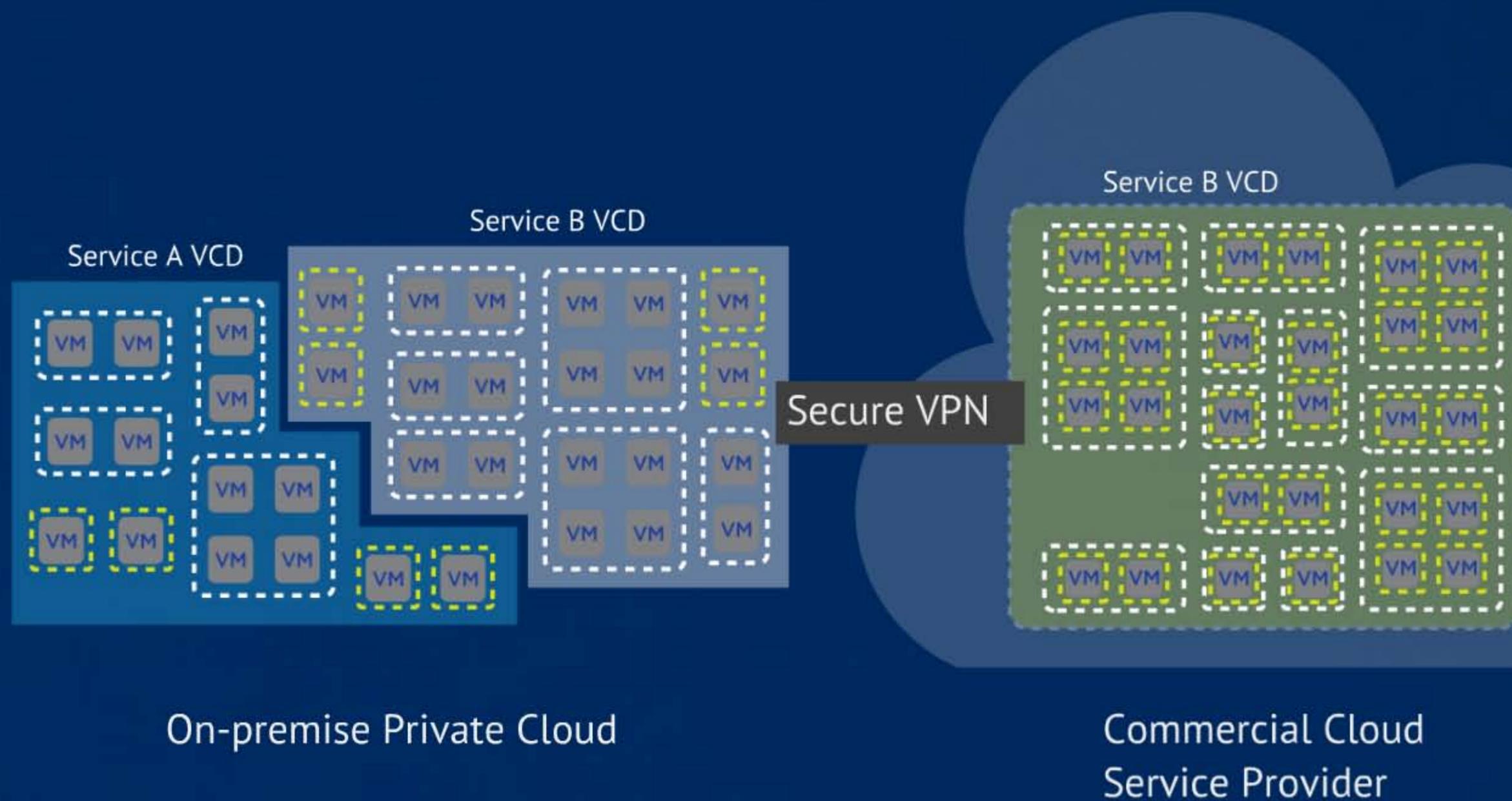
Adaptive

Labor Intensive



Change Aware

# Secure Hybrid Cloud Computing



# Cross Cloud Management Makes Hybrid Cloud Real

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



# Elastic Compute



192.168.10.1



On-premise Private Cloud



192.168.10.1

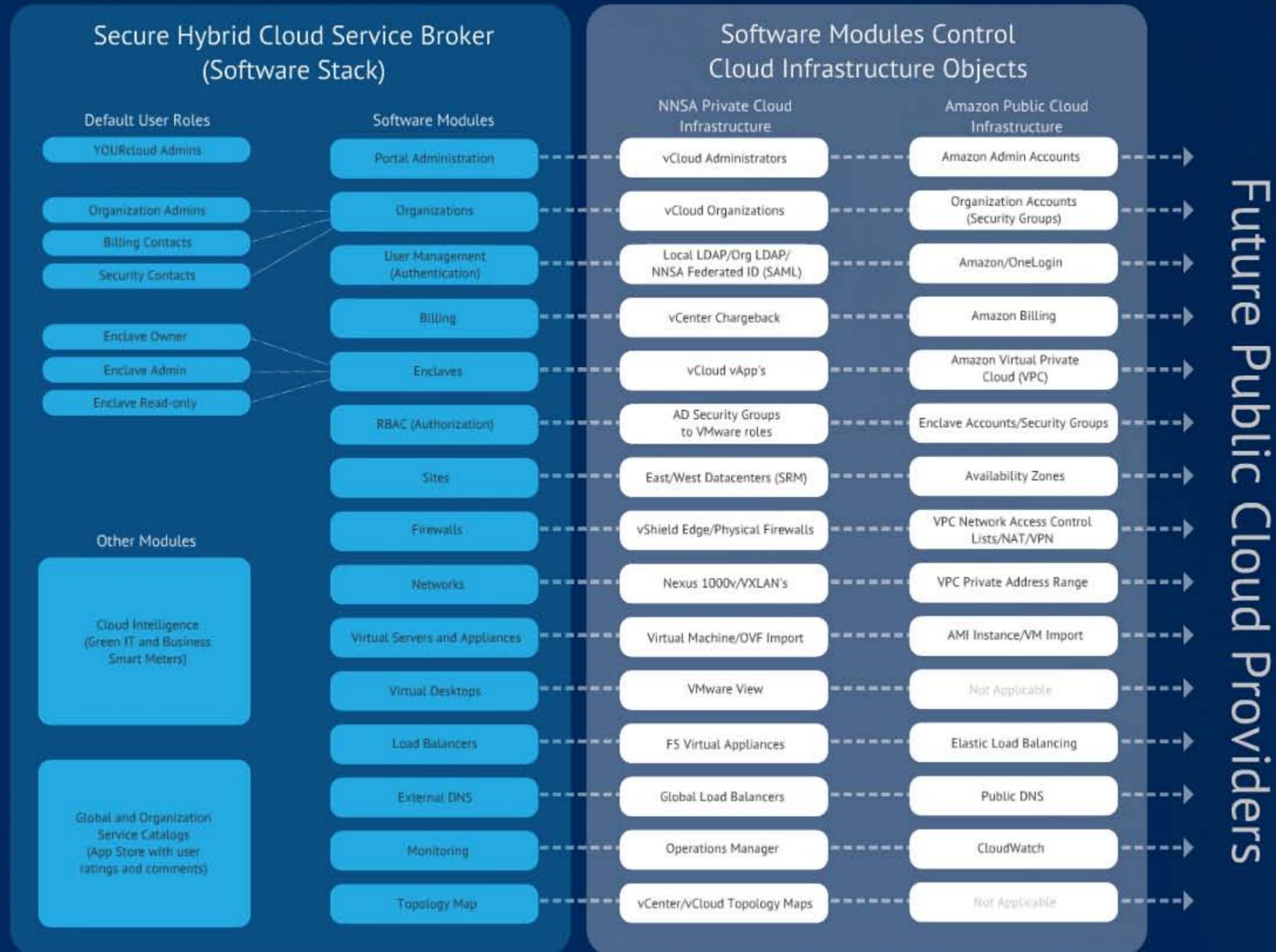


Commercial Cloud  
Service Provider

# Management Framework



# YOURcloud Service Broker Modules



# YOURcloud Service Broker Modules

## Secure Hybrid Cloud Service Broker (Software Stack)

### Default User Roles

YOURcloud Admins

Organization Admins

Billing Contacts

Security Contacts

Enclave Owner

Enclave Admin

Enclave Read-only

### Software Modules

Portal Administration

Organizations

User Management  
(Authentication)

Billing

Enclaves

RBAC (Authorization)

Sites

Firewalls

## Software Modules Control Cloud Infrastructure Objects

### NNSA Private Cloud Infrastructure

vCloud Administrators

vCloud Organizations

Local LDAP/Org LDAP/  
NNSA Federated ID (SAML)

vCenter Chargeback

vCloud vApp's

AD Security Groups  
to VMware roles

East/West Datacenters (SRM)

vShield Edge/Physical Firewalls

### Amazon Public Cloud Infrastructure

Amazon Admin Accounts

Organization Accounts  
(Security Groups)

Amazon/OneLogin

Amazon Billing

Amazon Virtual Private  
Cloud (VPC)

Enclave Accounts/Security Groups

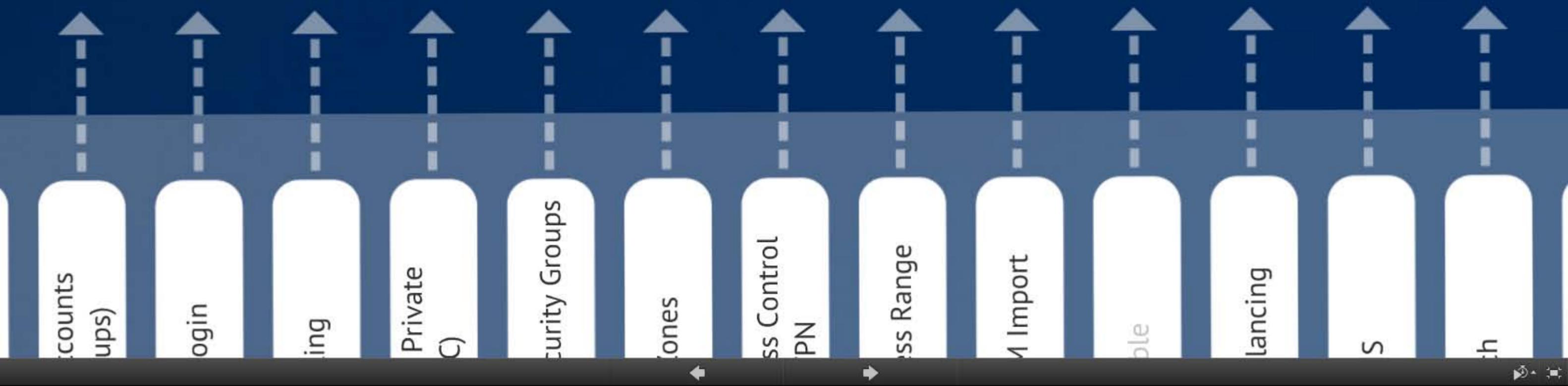
Availability Zones

VPC Network Access Control





# 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.

## AWARDS

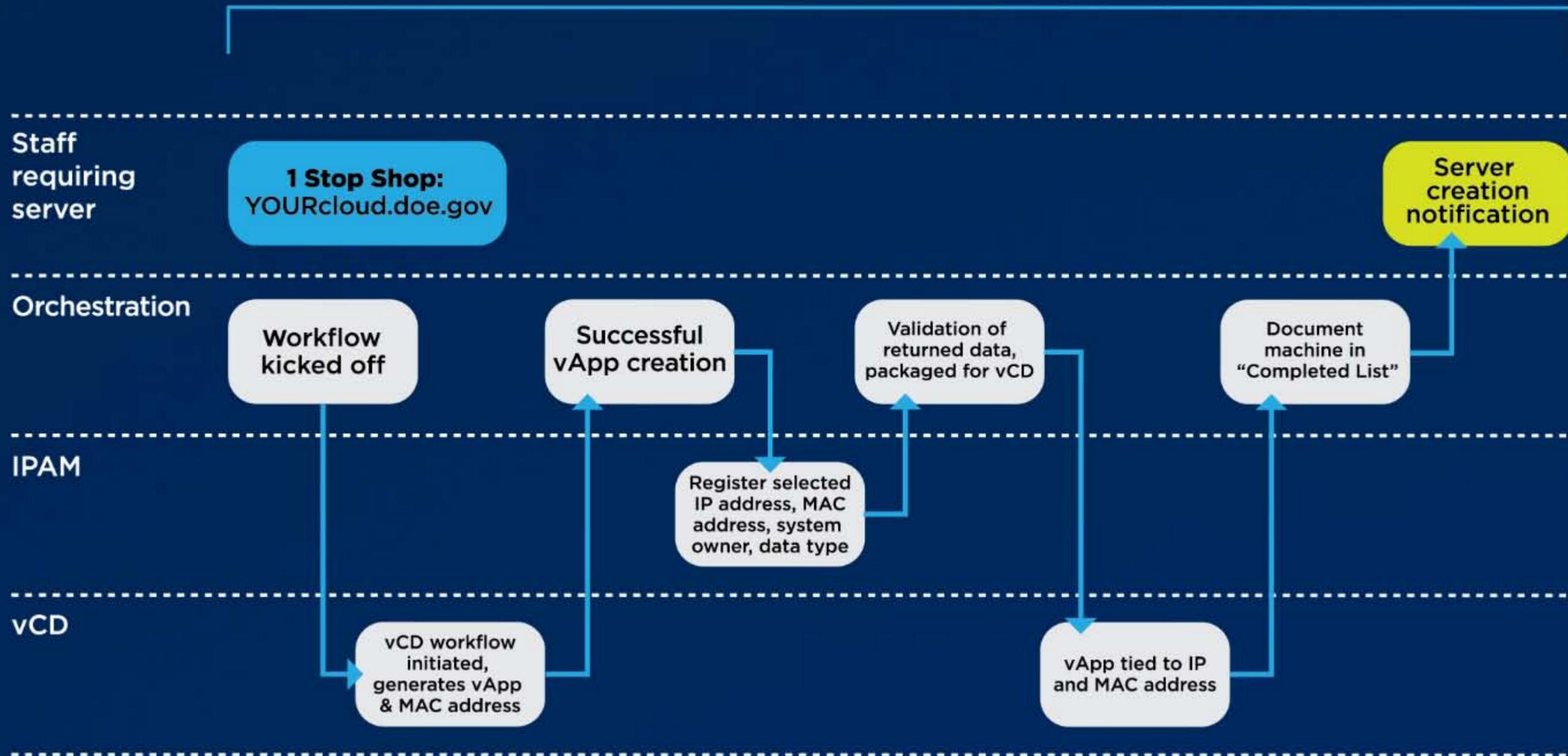
SANS National  
Cybersecurity Innovators  
Award: Cloud Security

InformationWeek 500  
Top IT Government  
Innovators

# Infrastructure 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



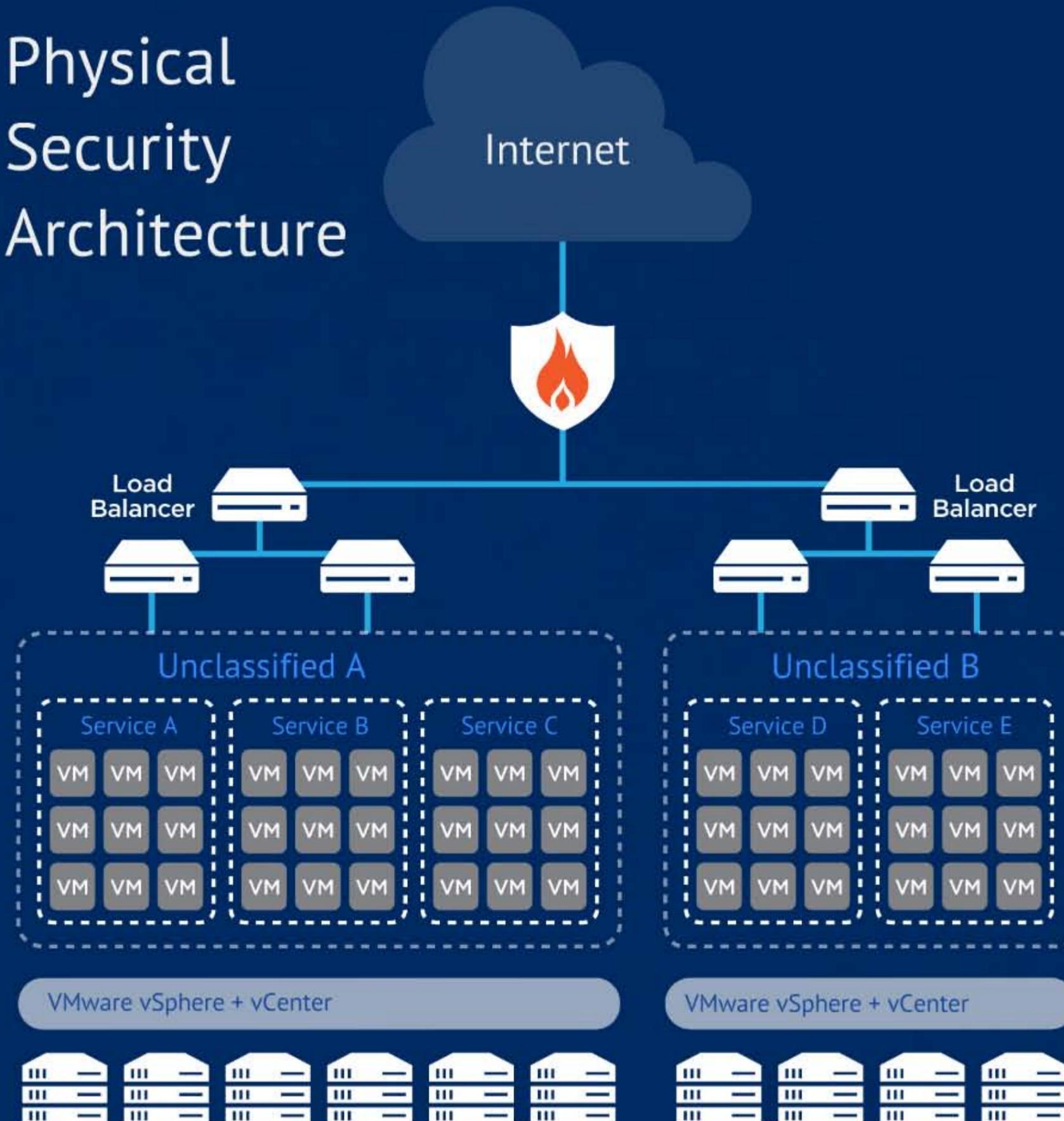
Adaptive

Labor Intensive  
Compliance

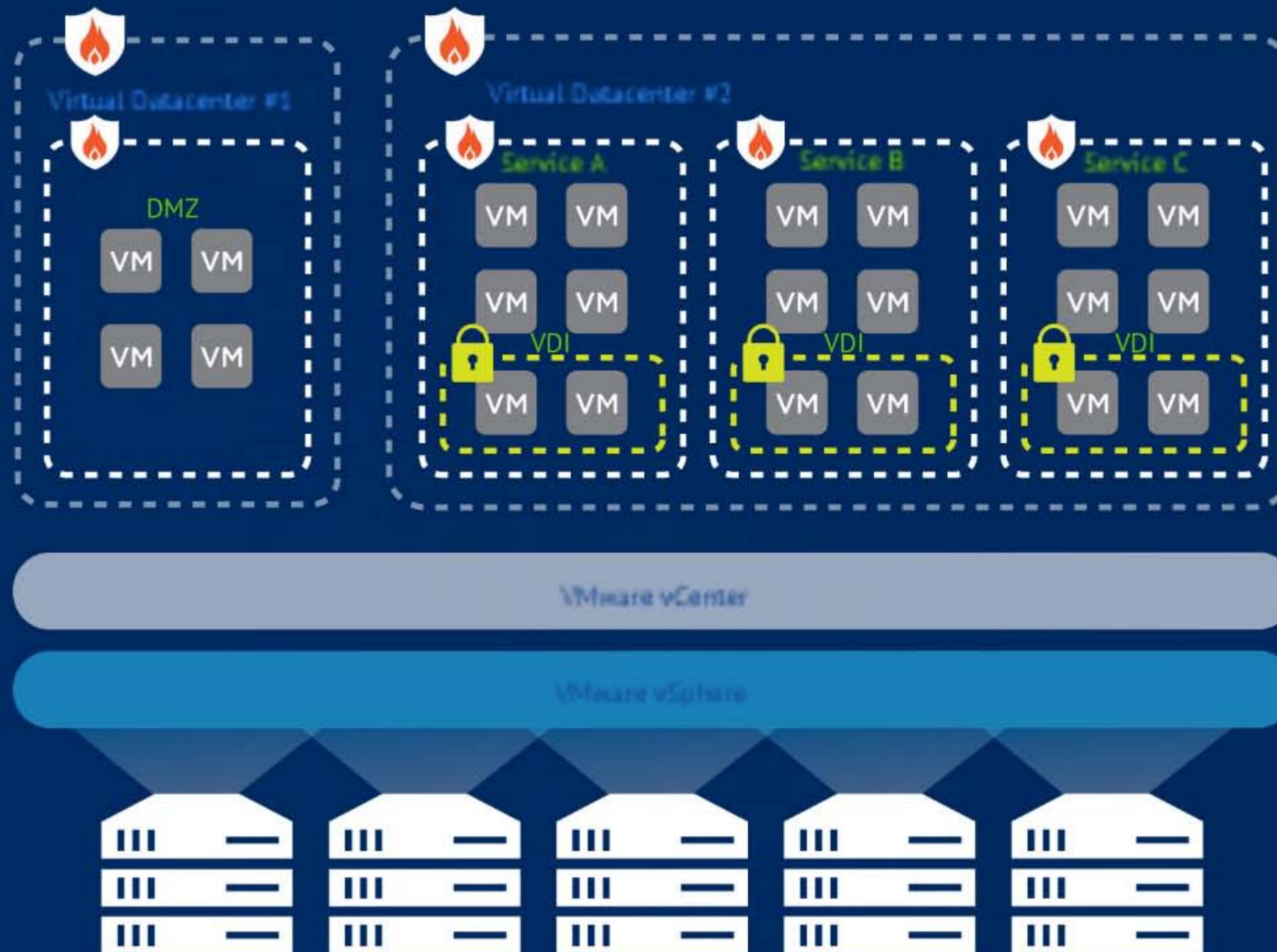


Automatic  
Compliance

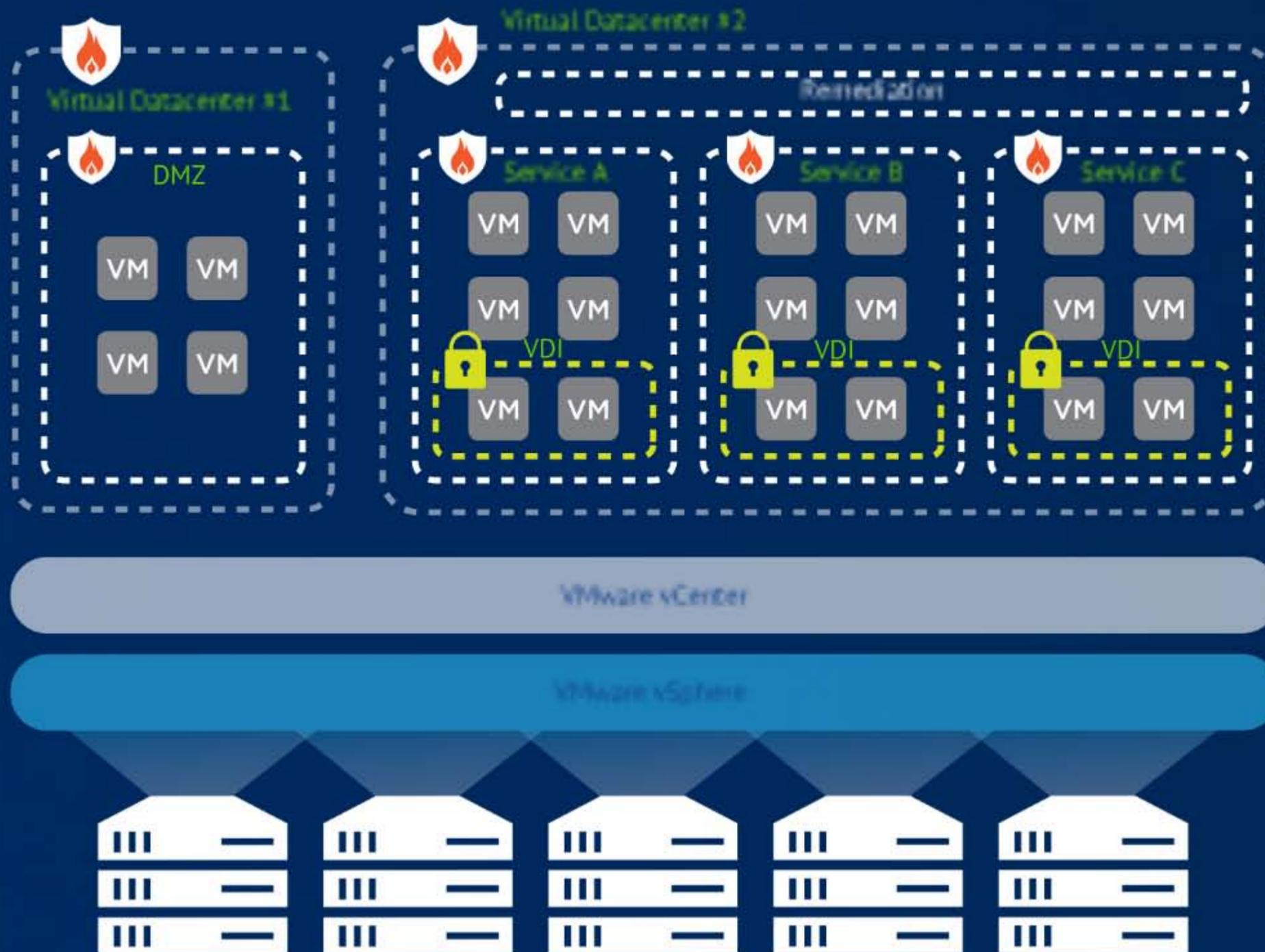
# Physical Security Architecture



# Cloud Security: Protect the VDI Clients



# Cloud Security: Quarantine Compromised Virtual Machines

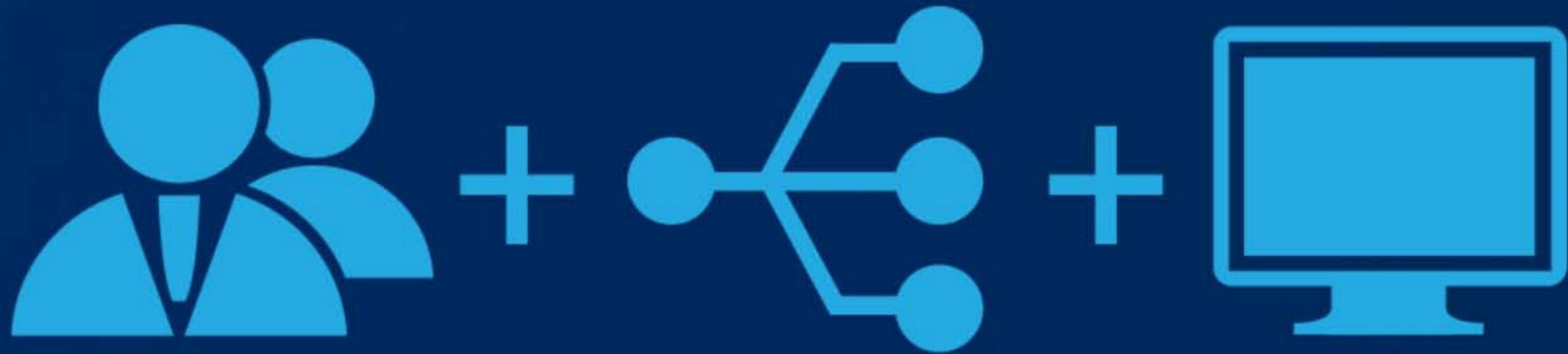


How do we address this?

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

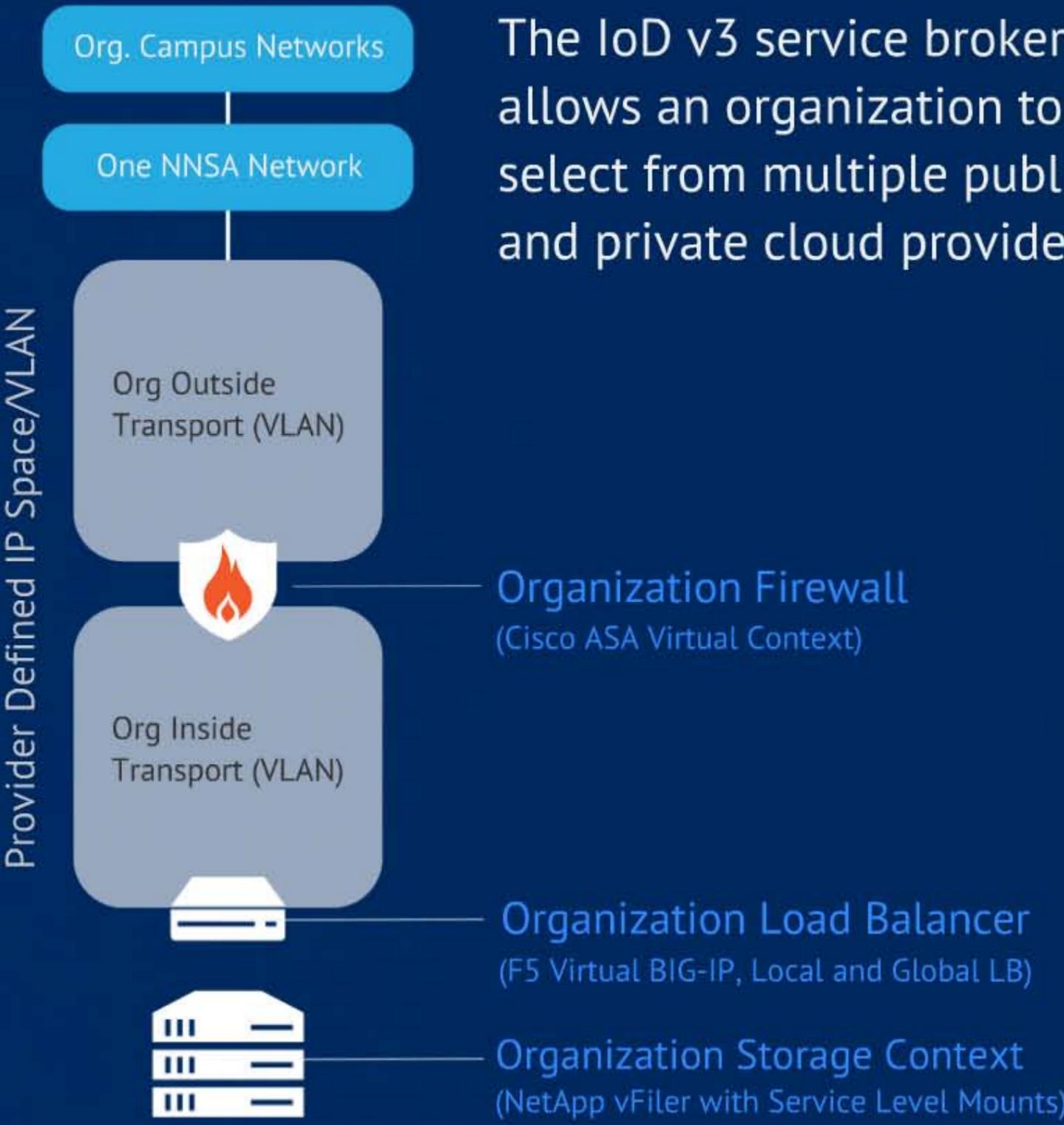
- Receives Notifications
- Org Firewall Control
- Security functions outside of the system



## Billing Contacts

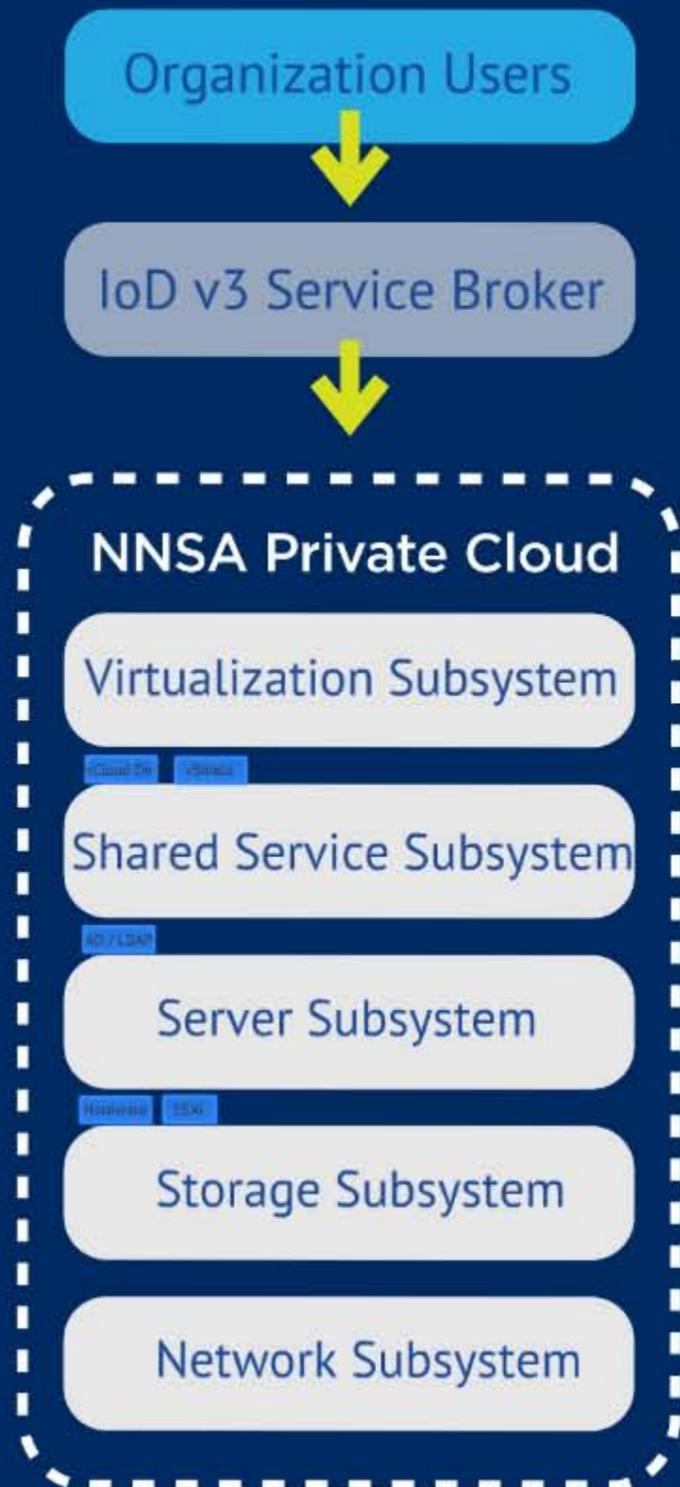
- Receives Notifications
- Billing Statement Controls
- Billing functions outside of the system

# Provider Selection

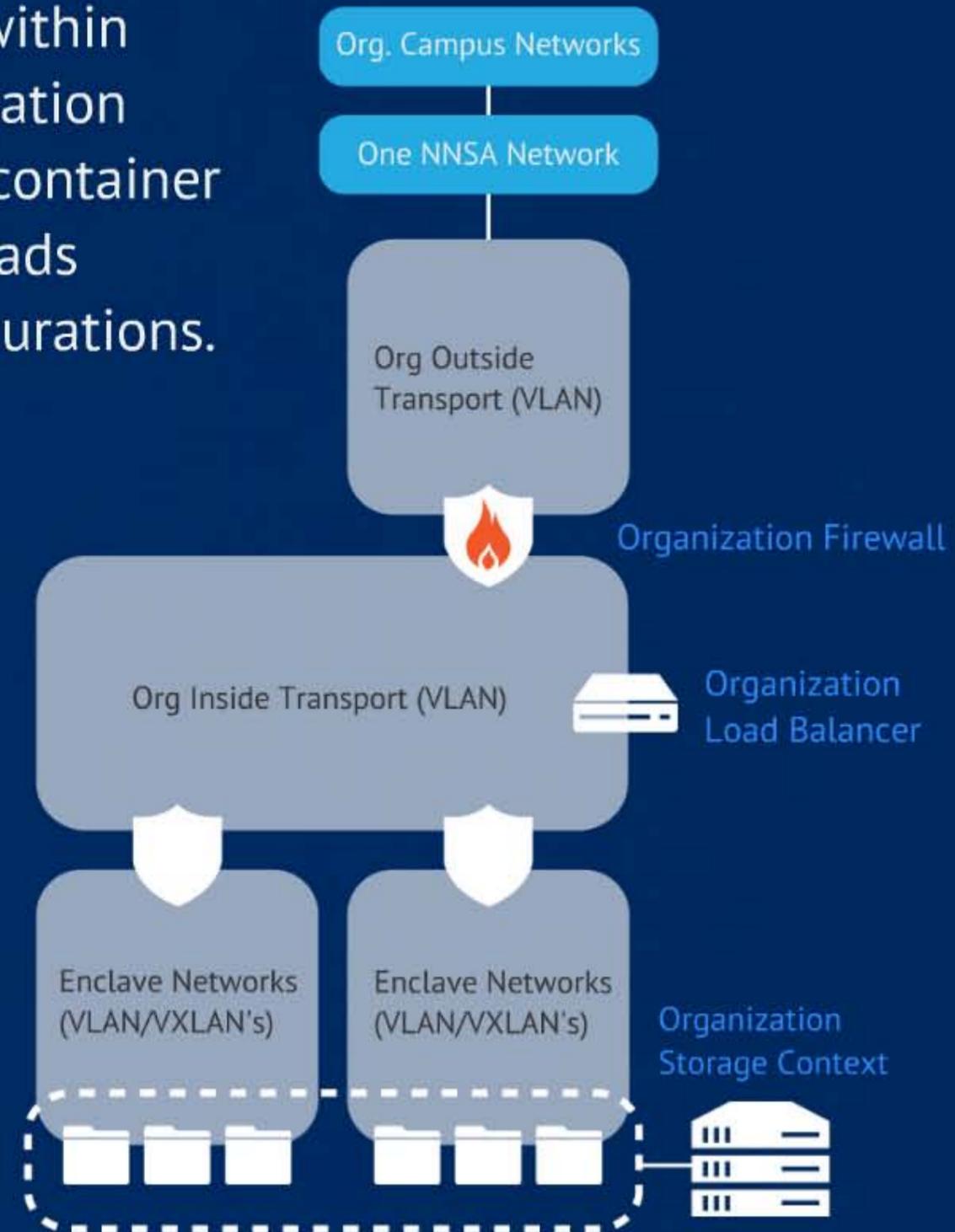


The IoD v3 service broker allows an organization to select from multiple public and private cloud providers.

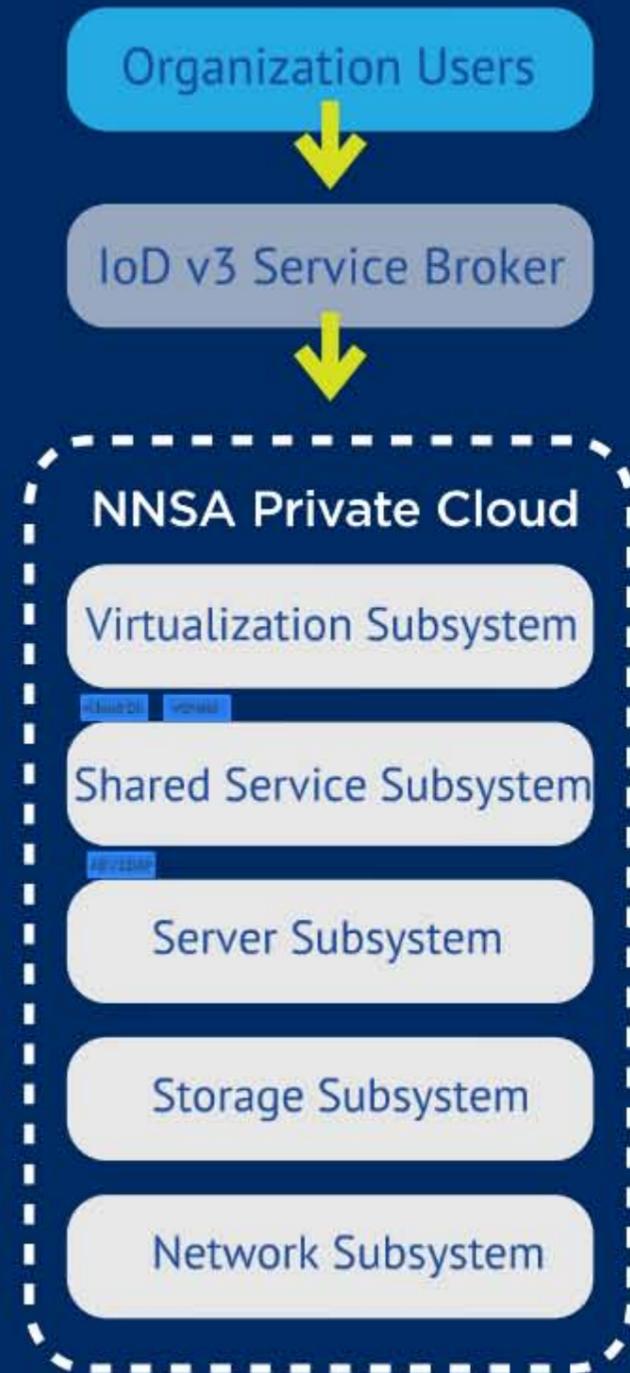
# Enclave Creation



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



# Enclave RBAC



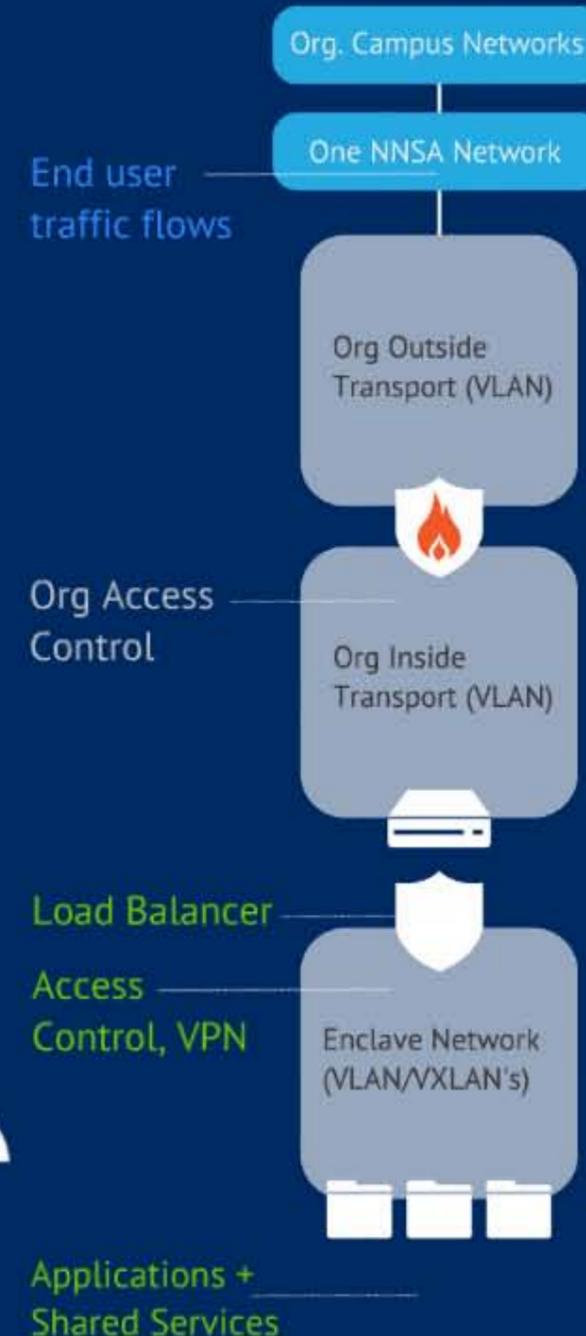
After an Enclave is created, Role Based Access Control (RBAC) is established by assigning permissions to the organization's technical staff.



# 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.



What should end users see?

# Splash Screen

The screenshot shows the 'YOURcloud' dashboard splash screen. At the top left is the logo 'YOURcloud' with the tagline 'Powered by Infrastructure on Demand v3'. The top right shows the user 'Bryan', 'Show Tasks', and 'Sign Out' options. A navigation bar contains 'Dashboard', 'Organizations', 'Enclaves', 'Servers', and 'App Store'. The main content area is titled 'YOUR OVERVIEW' and includes a welcome message for 'Bryan', a brief description of the dashboard, and two summary cards: 'MAN HOURS SAVED' (00057:10:01) and 'KILOWATT HOURS SAVED' (00280028790). Below these is a line graph titled 'Kilowatt Hours Saved Over Time' showing an upward trend from 15,000 in October 2012 to 28,790 in February 2013. An 'Organization Overview' section shows 3 organizations, 6 enclaves, and 6 servers. A 'Your Recent Actions' list shows five entries of 'You created Delete Load Balancer' from February 25, 2013. A pagination bar at the bottom indicates 'Page size: 5', 'Page: 1 of 33', and 'Go'.

**YOURcloud**  
Powered by Infrastructure on Demand v3

Bryan Show Tasks Sign Out

Dashboard Organizations Enclaves Servers App Store

### YOUR OVERVIEW

Welcome, Bryan

The dashboard provides a high level overview of the cloud services that you are consuming as well as other information about your activity within the system.

**MAN HOURS SAVED**  
00057:10:01  
Total time saved using YOURcloud.

**KILOWATT HOURS SAVED**  
00280028790  
Total kilowatts saved using YOURcloud.

#### Kilowatt Hours Saved Over Time

Date	Kilowatt Hours Saved
10/20/2012	15000
11/20/2012	16000
12/20/2012	17000
1/20/2013	18000
2/20/2013	28790

#### Organization Overview

Category	Count
YOUR ORGANIZATIONS	3
YOUR ENCLAVES	6
YOUR SERVERS	6

#### Your Recent Actions

- 2/25/2013 4:18:45 PM You created Delete Load Balancer
- 2/25/2013 4:18:33 PM You created Delete Load Balancer
- 2/25/2013 4:17:52 PM You created Delete Load Balancer
- 2/25/2013 4:17:43 PM You created Delete Load Balancer
- 2/25/2013 4:17:38 PM You created Delete Load Balancer

Page size: 5 Page: 1 of 33 Go

Items 1 to 5 of 163

Dashboard Organizations Enclaves Servers Support

Phone: (753) 538-4565  
Email: support@yourcloud.com

Powered by Infrastructure on Demand (v3)

# 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



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:  ⓘ

Load Balancer Port:  ⓘ

Server Protocol:  ⓘ

Server Port:  ⓘ

### Actions

### Support

We're here to help!  
[Submit Feedback or Ask Question](#)

# Firewall Topology

The screenshot displays the YOURcloud interface for Firewall Topology. The header includes the YOURcloud logo (Powered by Infrastructure on Demand v3) and user navigation options: Bryan, Show Tasks, and Sign Out. A navigation bar contains Dashboard, Organizations, Enclaves, Servers, and an App Store link. The breadcrumb trail is Dashboard > Enclave List > Enclave Management (fireball) > Enclave Topology.

## FIREBALL TOPOLOGY

	Routed Networks	Servers
	Testing... 11.1.3.128	No Servers
	network 12.0.0.0	Becky's Test Server 12.0.0.101
		Coal 12.0.0.201
		Lead 12.0.0.200

A large orange arrow points from the Servers column back to the Routed Networks column, indicating a return path or relationship.

**Support**  
We're here to help!  
[Submit Feedback or Ask Question](#)

**Footer:**  
DASHBOARD | ORGANIZATIONS | ENCLAVES | SERVERS  
Support  
Phone: (555) 555-4563  
Email: support@yourcloud.doe.gov  
Powered by Infrastructure on Demand (IOD) v3

Business

# Cost Savings

Federal

7% annu

gs

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

\$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, hybrid, and public clouds
- Broker Concept – cloud computing marketplace 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

## • 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

