Building YOURcloud:

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

Travis Howerton
&
Anil Karmel

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

YOURCLOUD

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

DOE cloud

Public cloud

Other gov't agency cloud

NNSA cloud

On-premise cloud

YOURCloud (IoD) Services Broker

DOE Federal users

General public users

Other gov't agency users

Laboratory + plant users

Support contractors

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

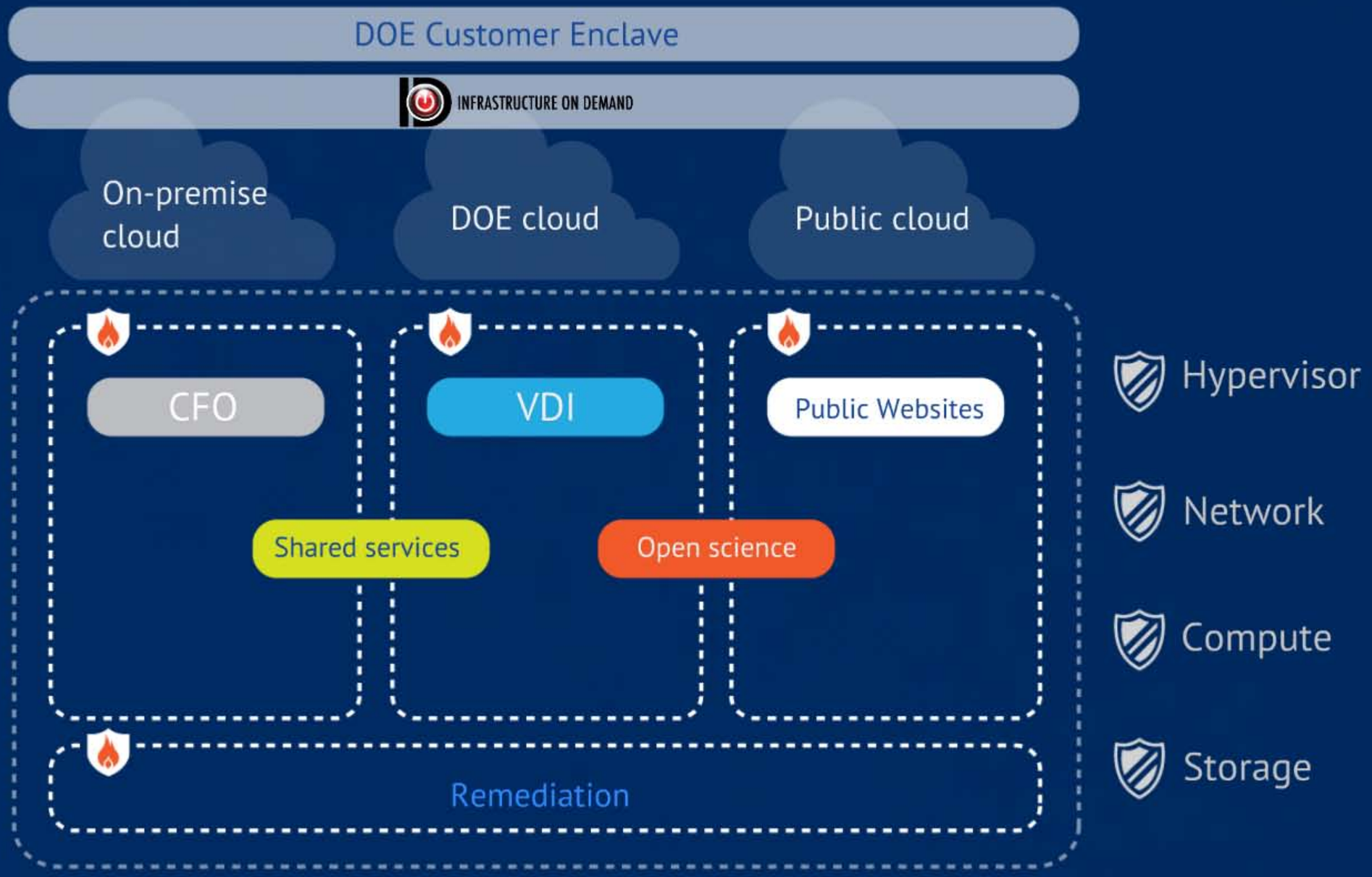
Social computing

Web conferencing

Instant messaging

Enterprise mobility

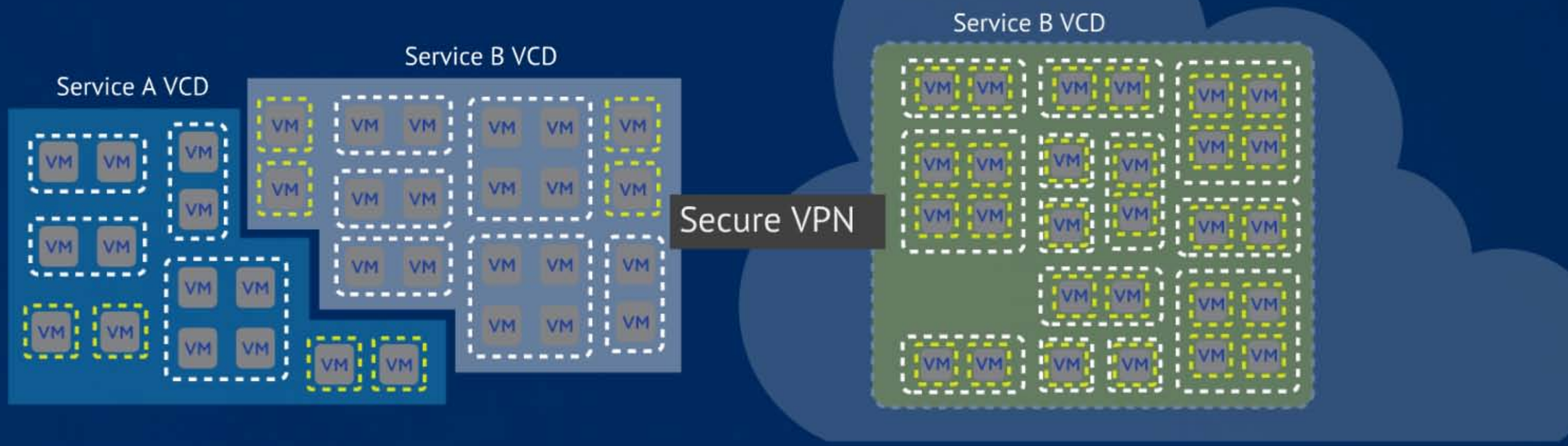
YOURcloud Service Broker Enclaves



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

INFRASTRUCTURE ON DEMAND

192.168.10.1

VM VM VM

192.168.10.1

VM

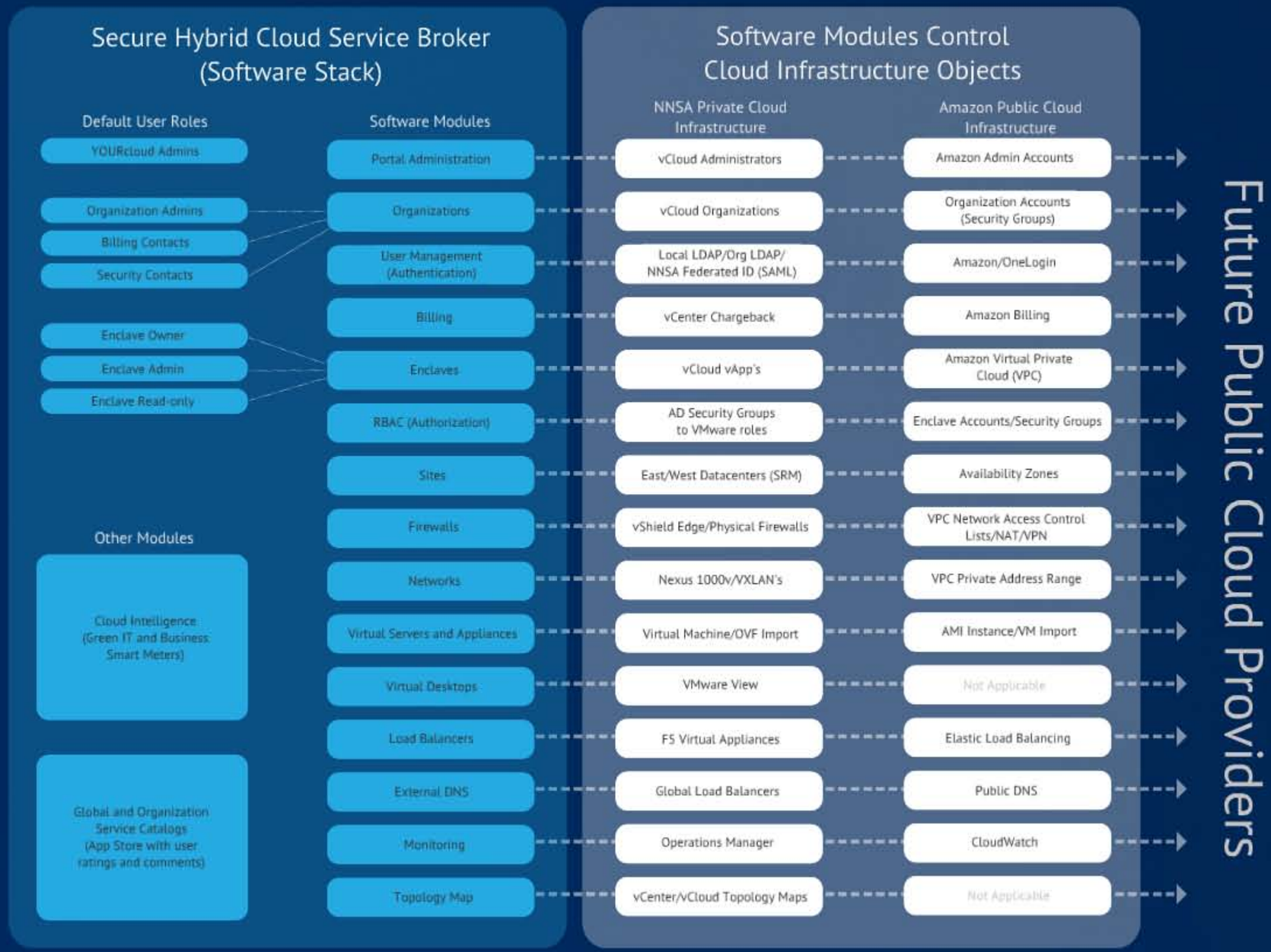
VXLAN

On-premise Private Cloud

Commercial Cloud
Service Provider

Management Framework

YOURcloud Service Broker Modules



YOURcloud Service Broker Modules

Secure Hybrid Cloud Service Broker (Software Stack)

Default User Roles	Software Modules
YOURcloud Admins	Portal Administration
Organization Admins, Billing Contacts, Security Contacts	Organizations
	User Management (Authentication)
	Billing
Enclave Owner, Enclave Admin, Enclave Read-only	Enclaves
	RBAC (Authorization)
	Sites
	Firewalls

Software Modules Control Cloud Infrastructure Objects

NNSA Private Cloud Infrastructure	Amazon Public Cloud Infrastructure
vCloud Administrators	Amazon Admin Accounts
vCloud Organizations	Organization Accounts (Security Groups)
Local LDAP/Org LDAP/ NNSA Federated ID (SAML)	Amazon/OneLogin
vCenter Chargeback	Amazon Billing
vCloud vApp's	Amazon Virtual Private Cloud (VPC)
AD Security Groups to VMware roles	Enclave Accounts/Security Groups
East/West Datacenters (SRM)	Availability Zones
vShield Edge/Physical Firewalls	VPC Network Access Control

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

Other Modules

Cloud Intelligence (Green IT and Business Smart Meters)

Load Balancers

F5 Virtual Appliances

Elastic Load Balancing

Global and Organization Service Catalogs (App Store with user ratings and comments)

External DNS

Global Load Balancers

Public DNS

Monitoring

Operations Manager

CloudWatch

Topology Map

vCenter/vCloud Topology Maps

Not Applicable

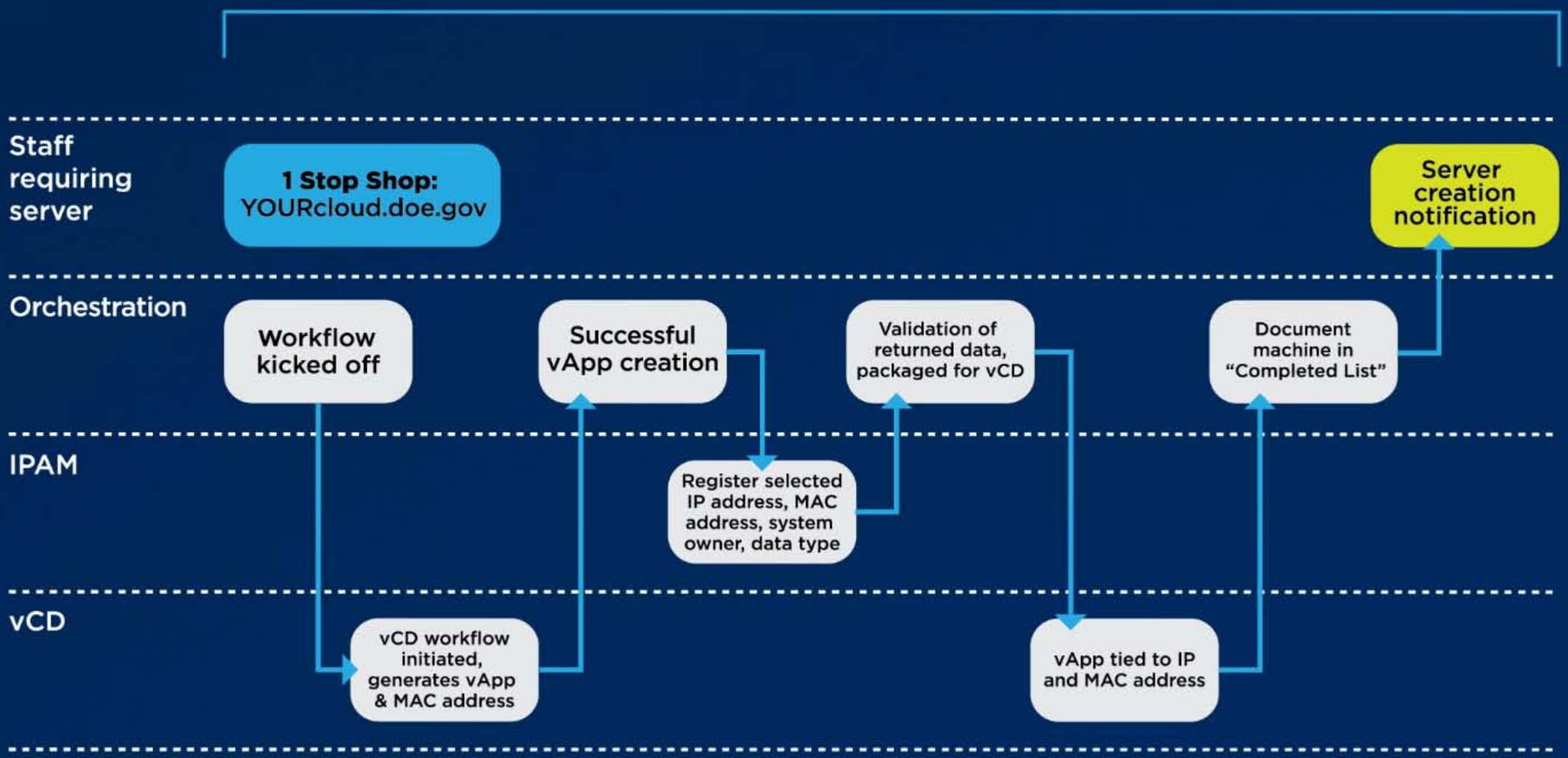
Future Public Cloud Providers

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



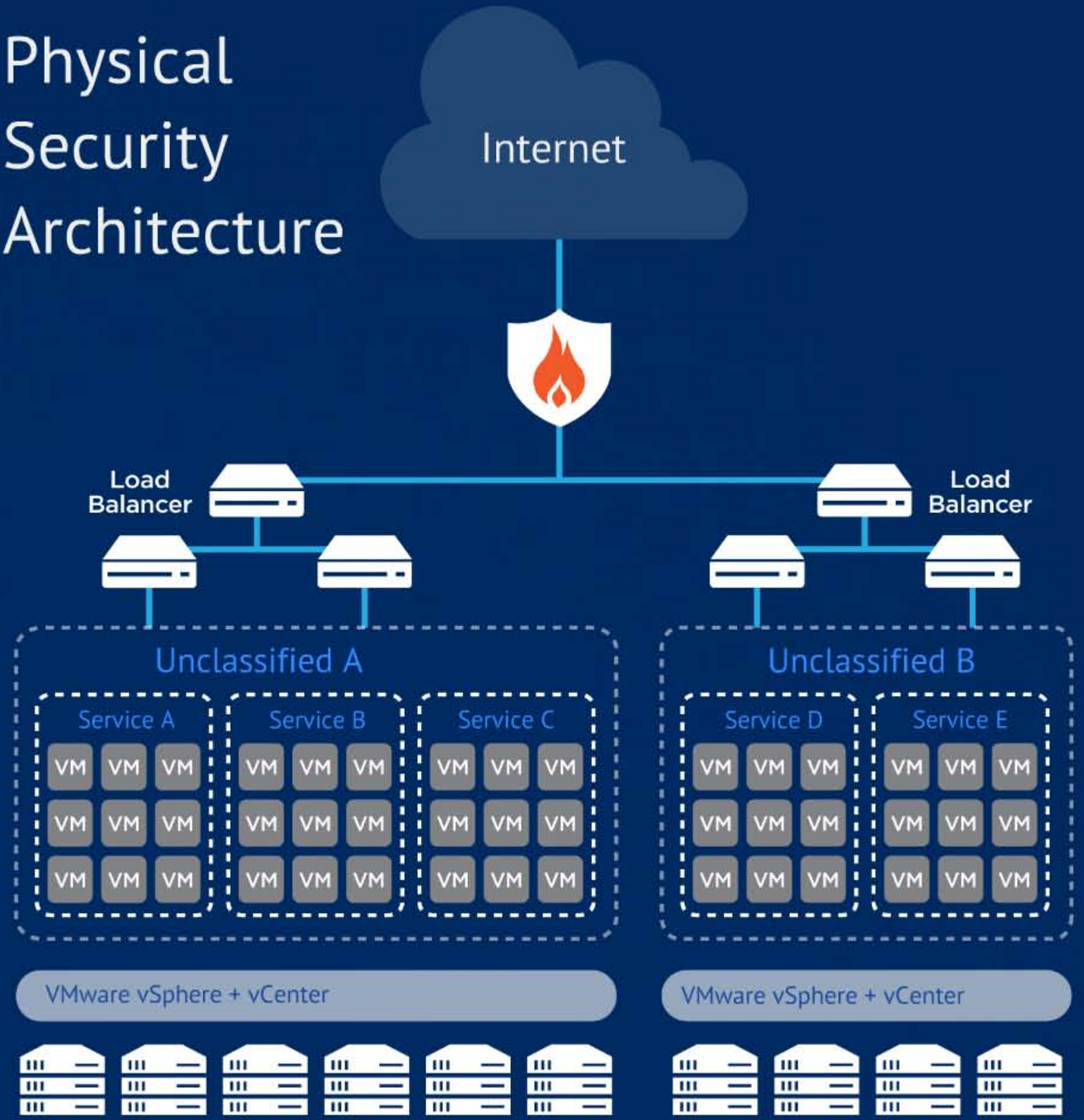
Security Journey

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

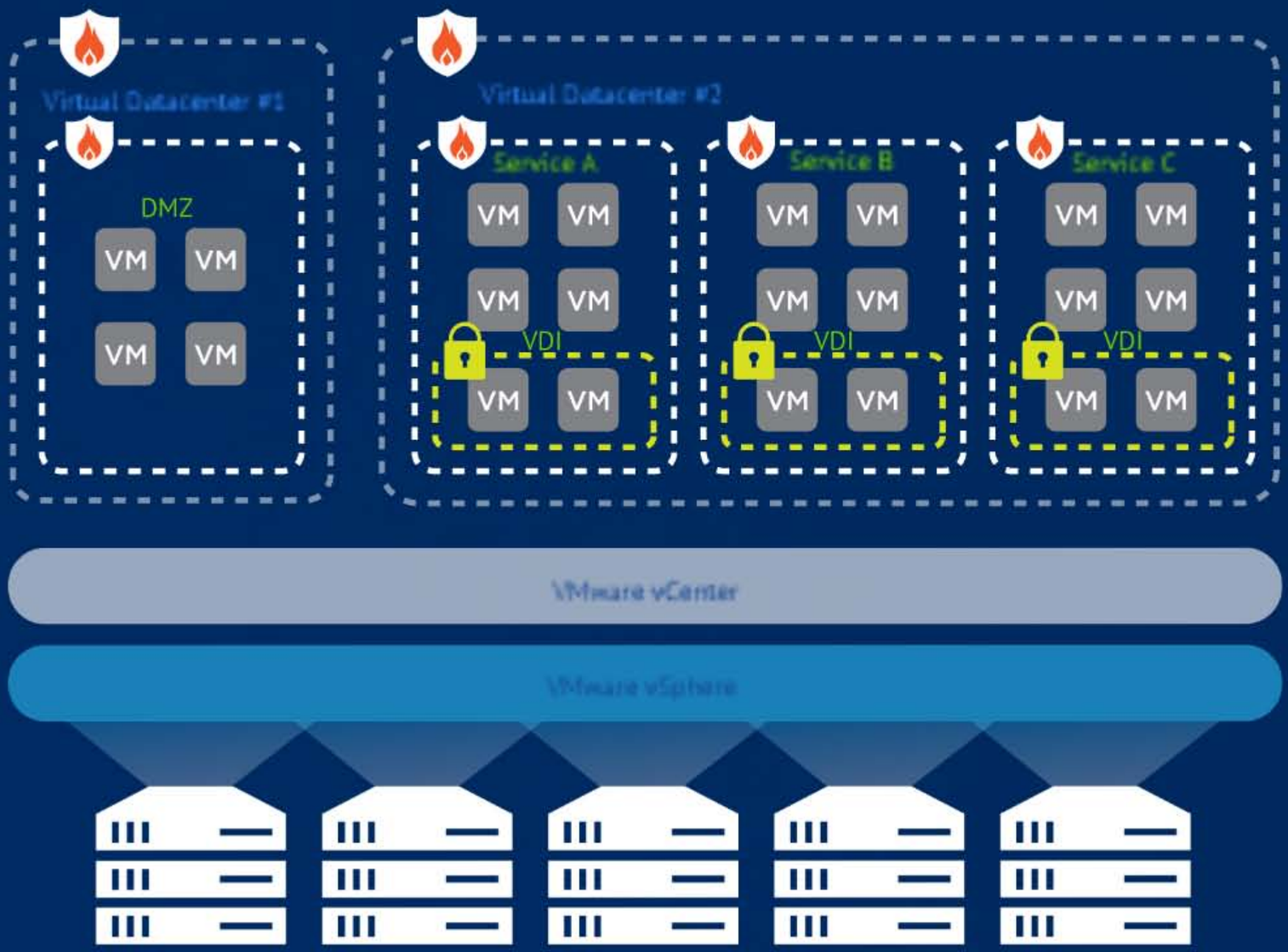
http://www.meritalk.com/missioncriticalcloud

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

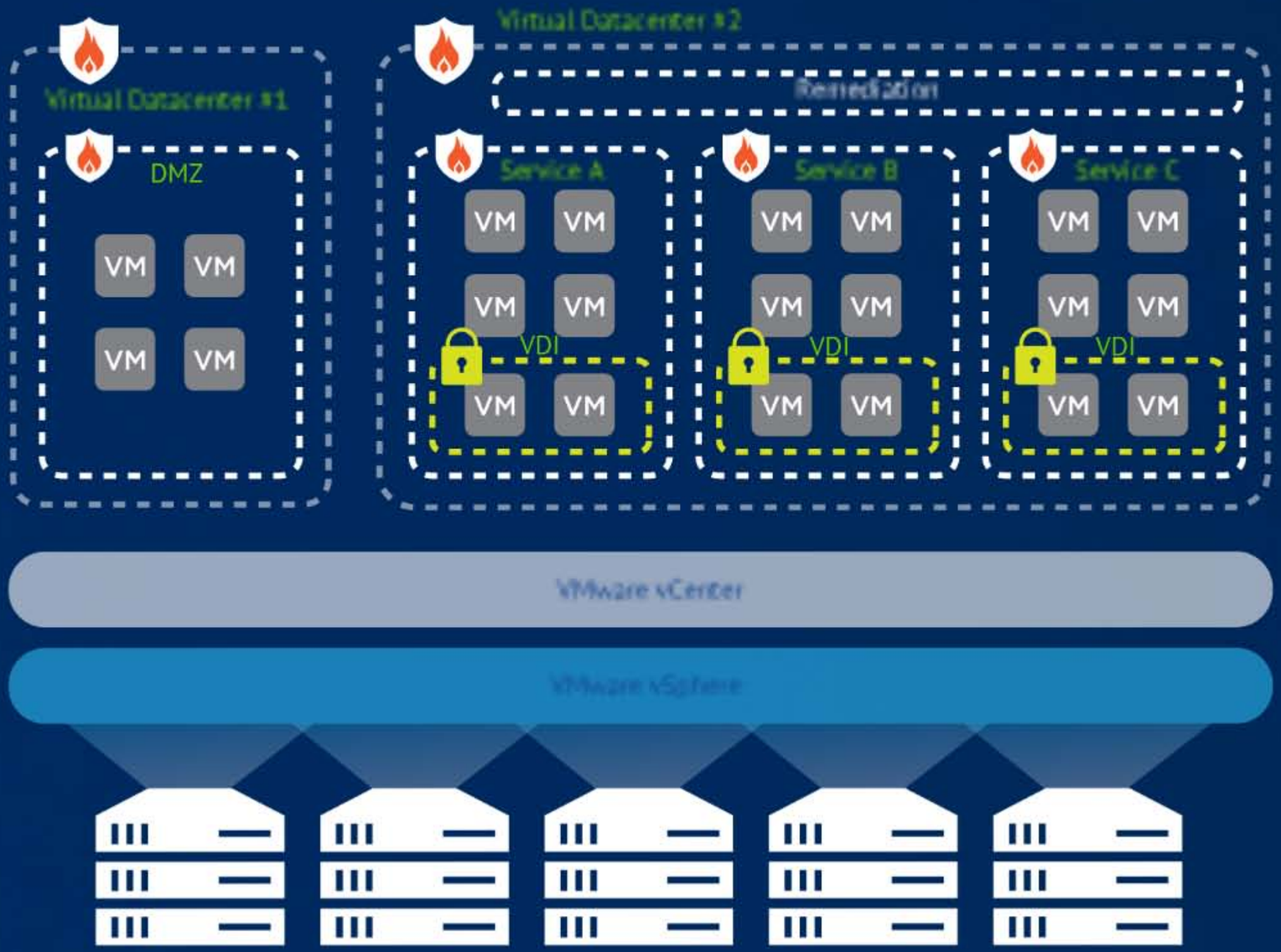
Physical Security Architecture



Cloud Security:
Protect the VDI Clients



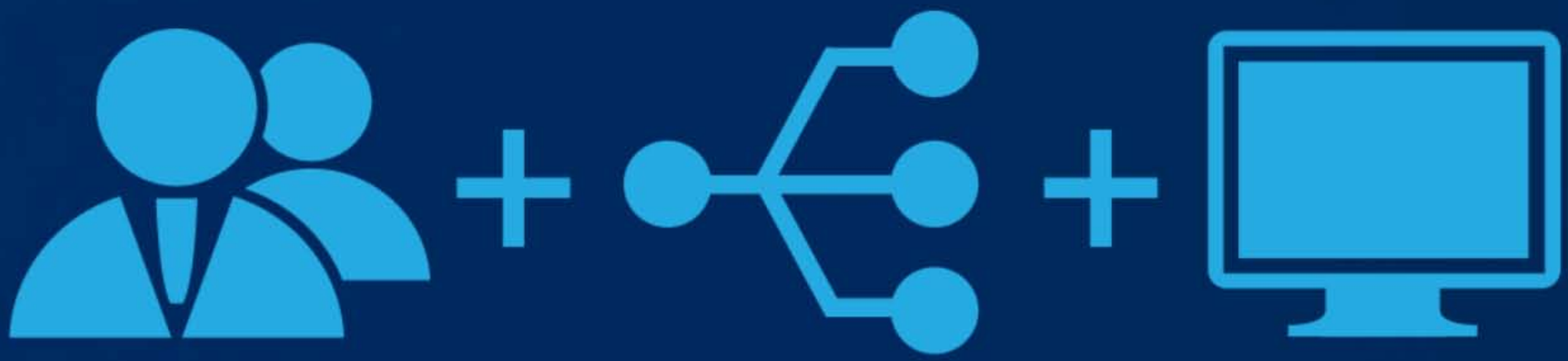
Cloud Security:
Quarantine Compromised Virtual Machines



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

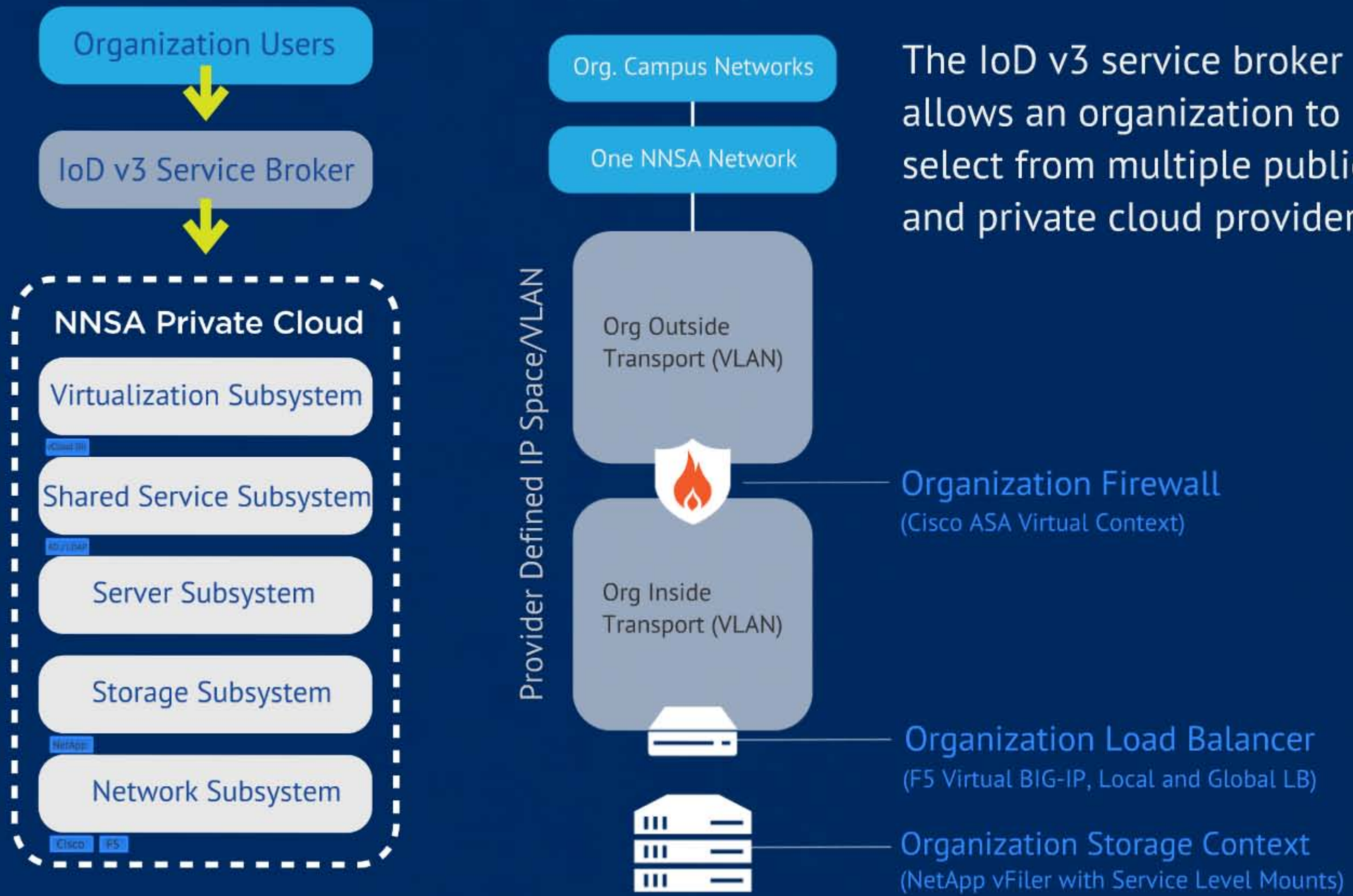
Security Contacts

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

Billing Contacts

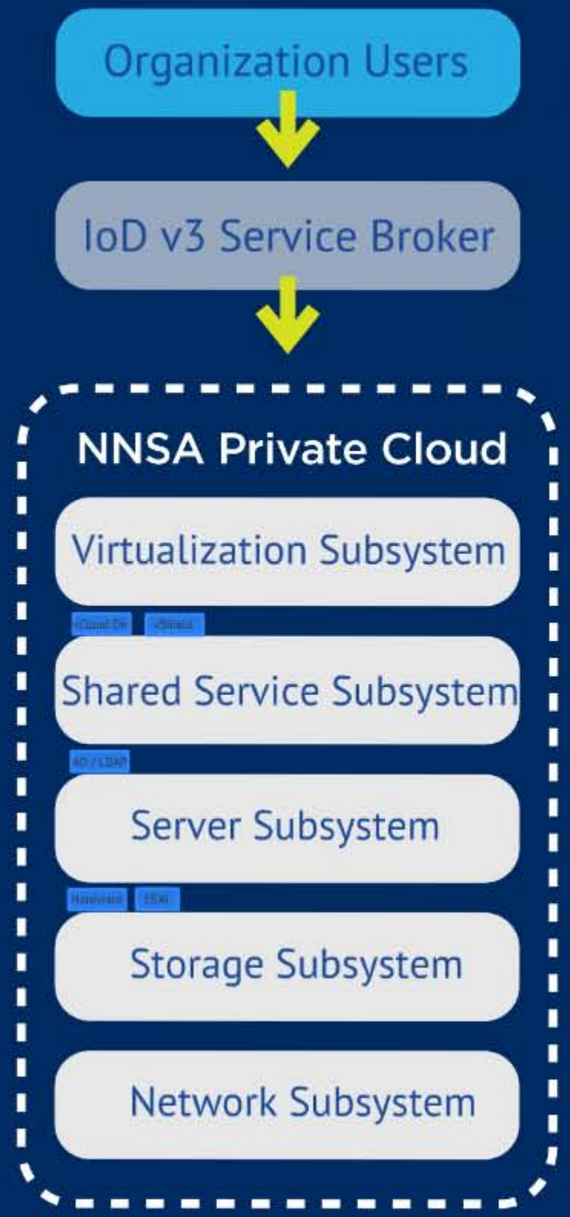
- Receives Notifications
- Billing Statement Controls
- Billing functions outside of the system

Provider Selection

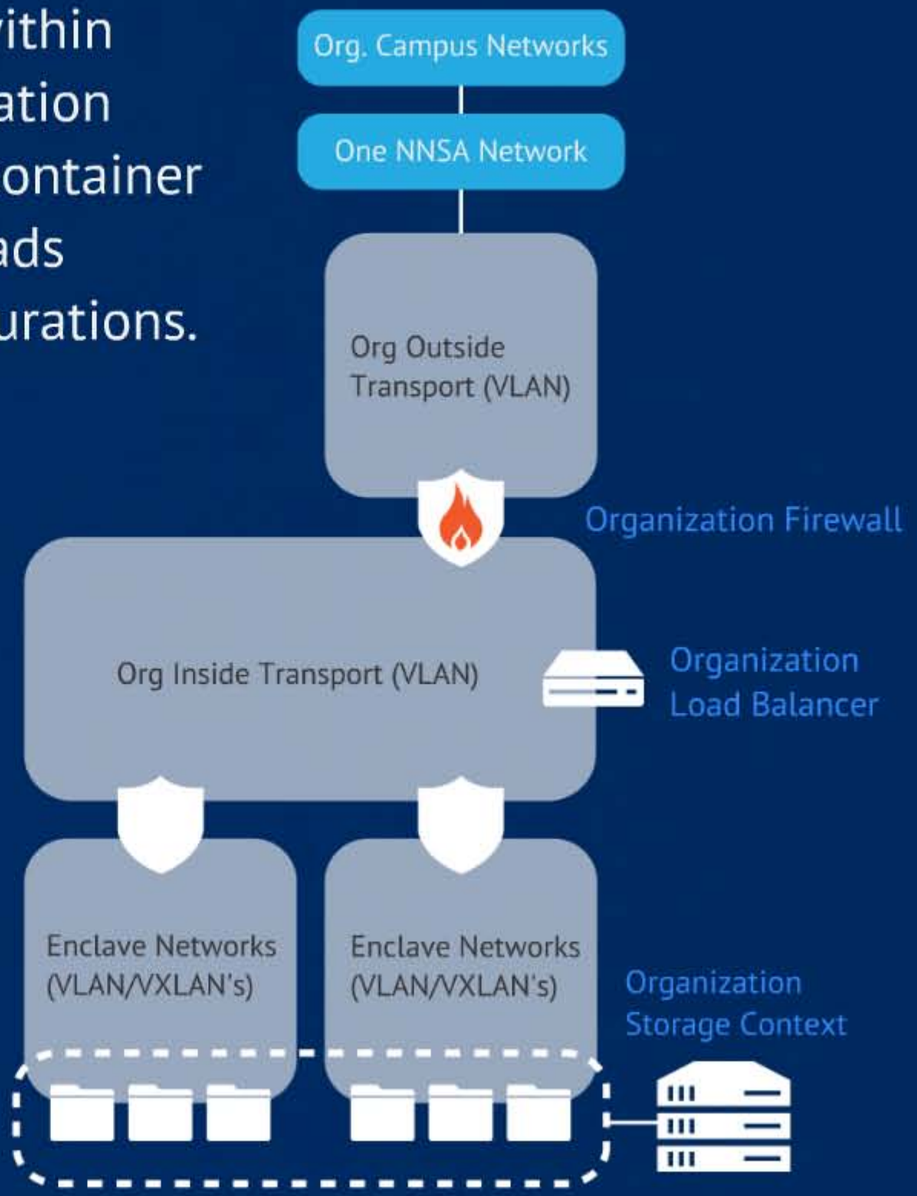


The IoD v3 service broker allows an organization to select from multiple public and private cloud providers.

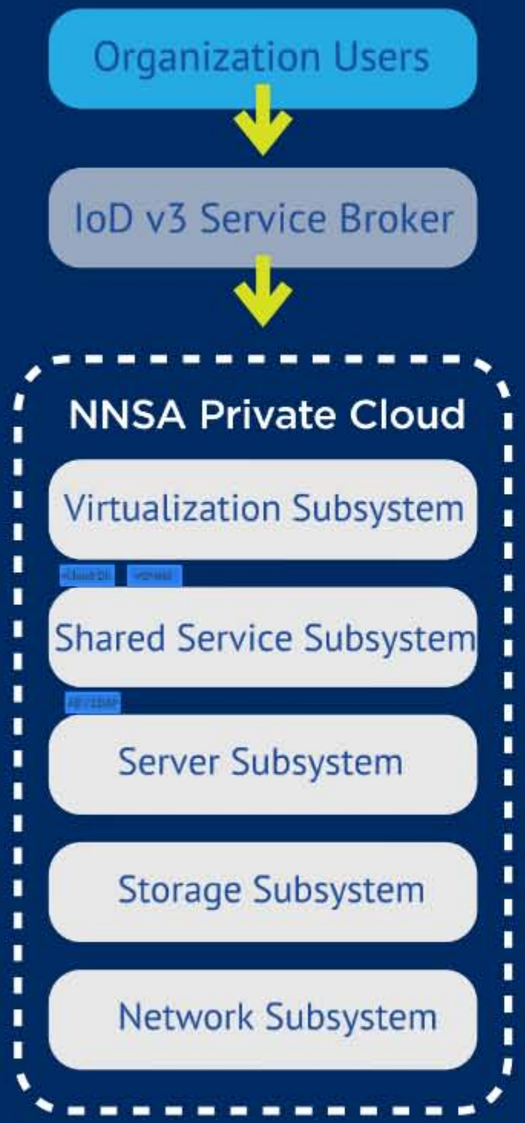
Enclave Creation



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.

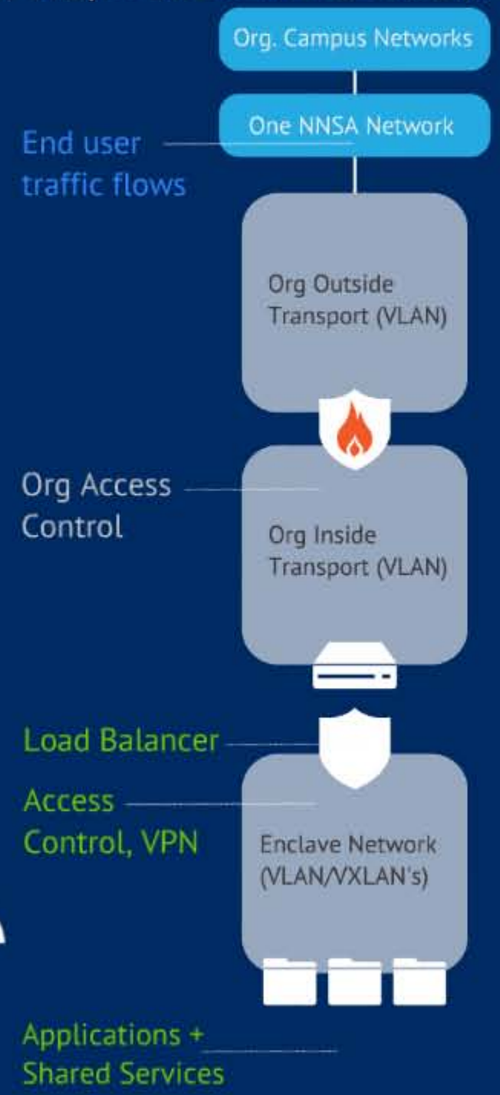
Enclave Management

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

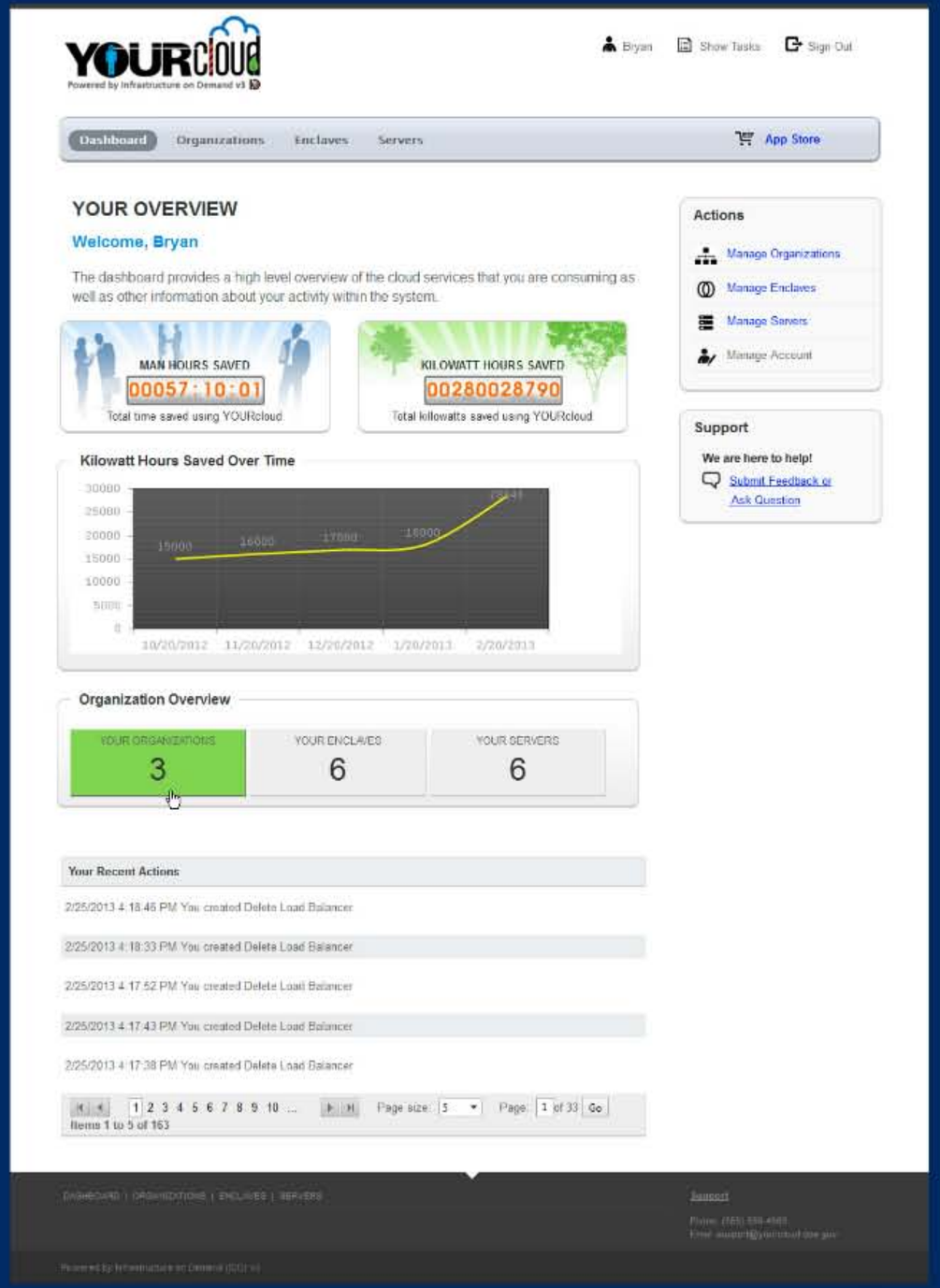
Technical + Security Contacts

Enclave Administrators

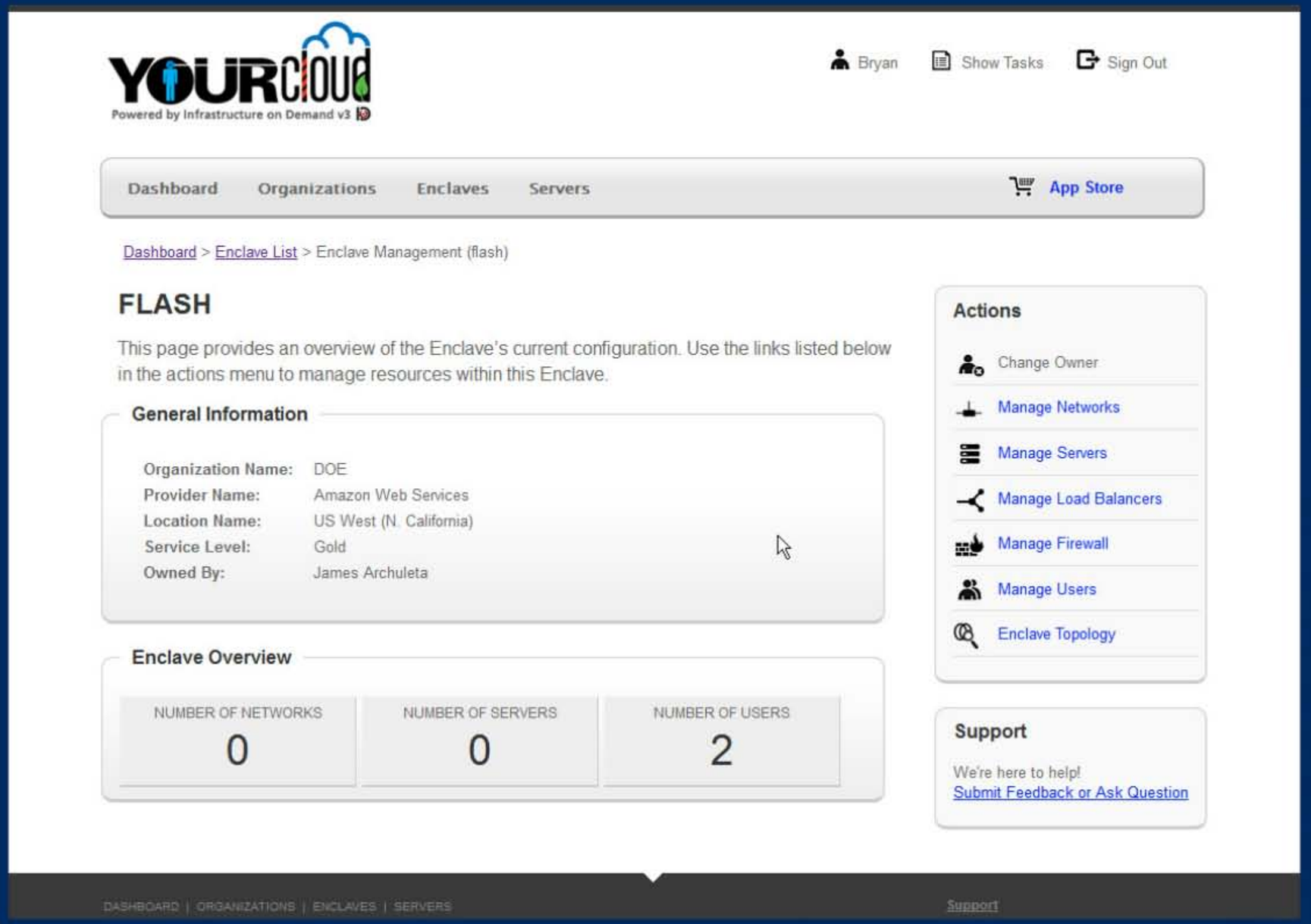


What should end users see?

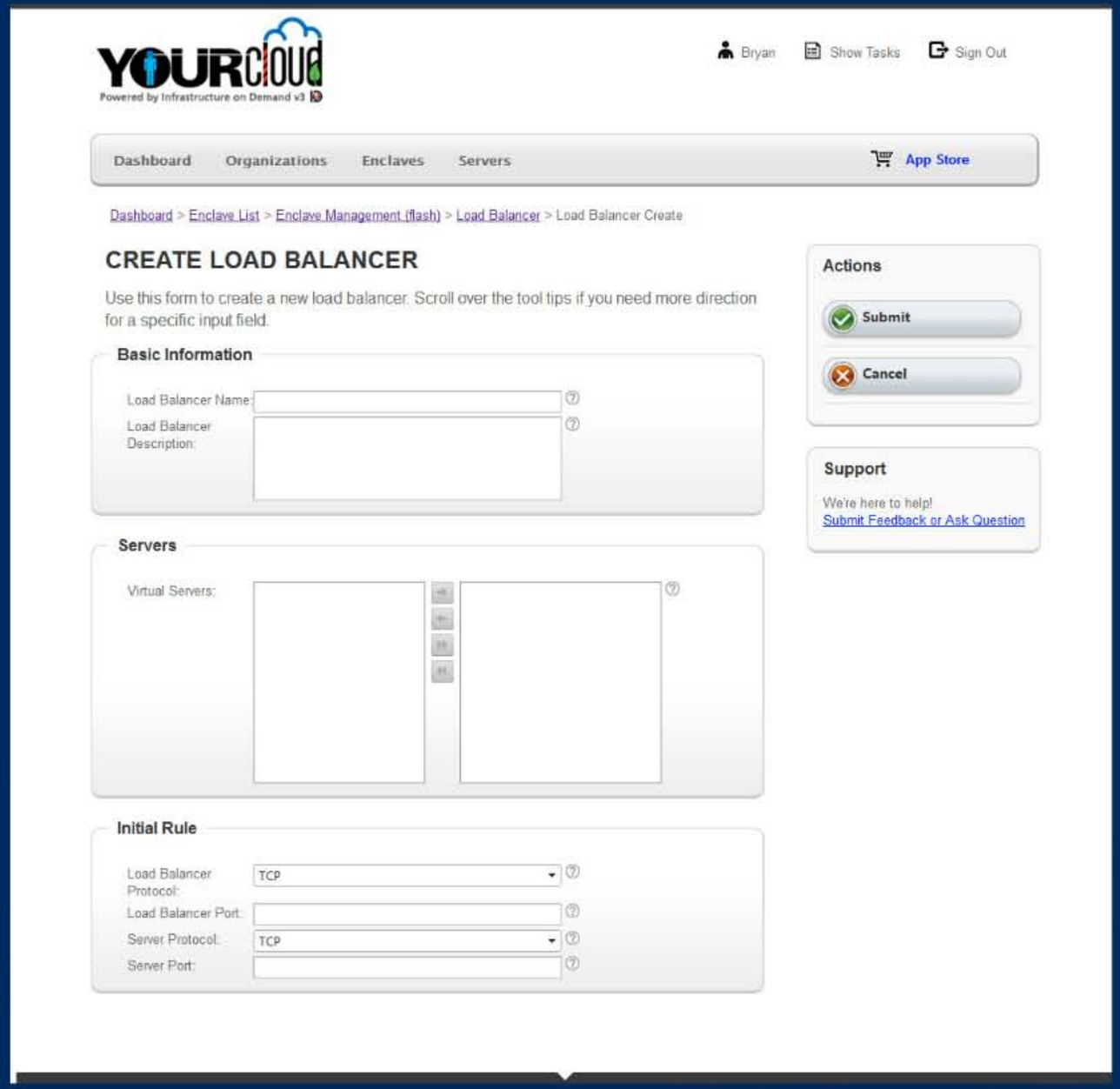
Splash Screen



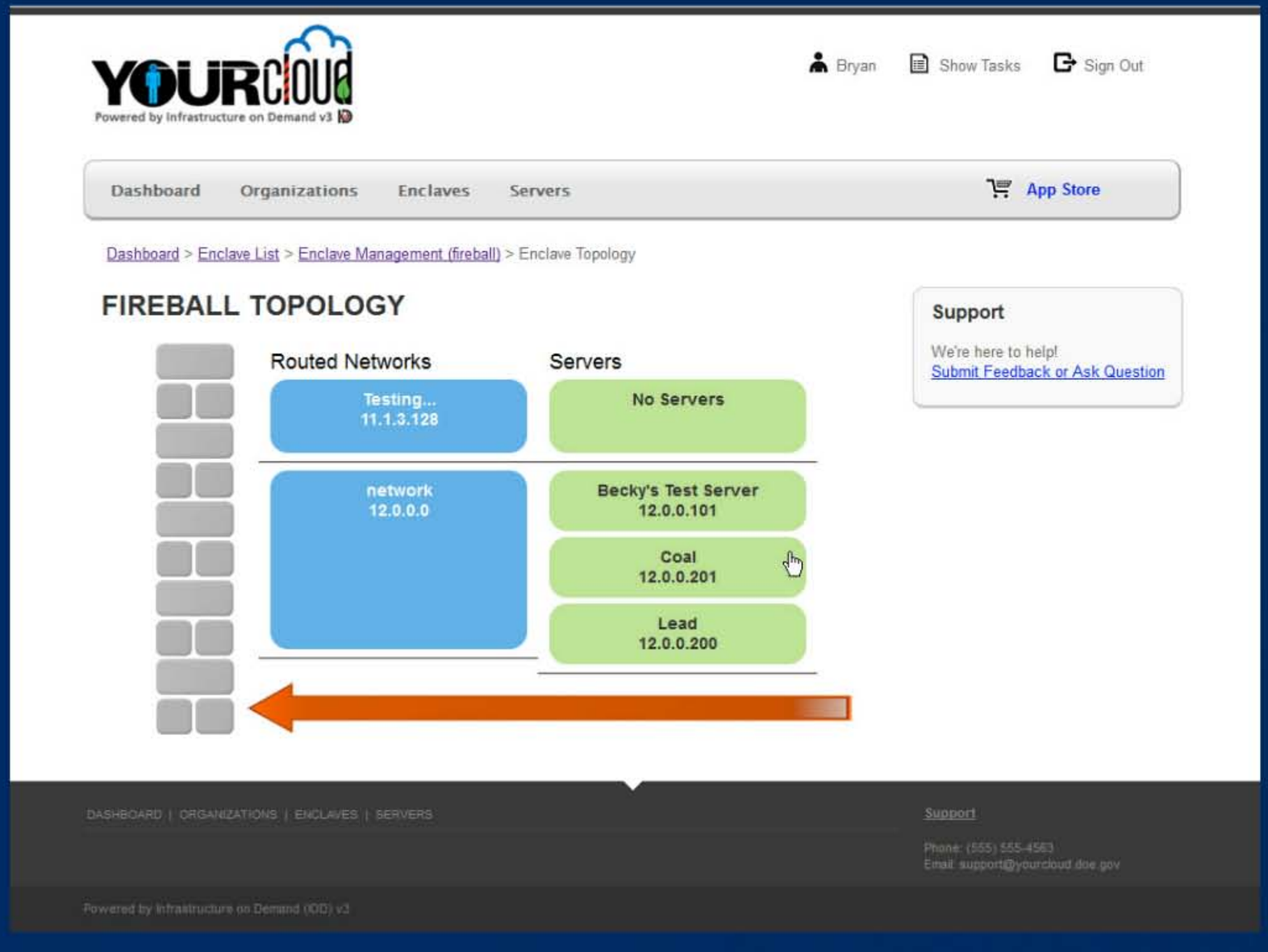
Enclave Management



Create Load Balancer



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

.gif

- 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