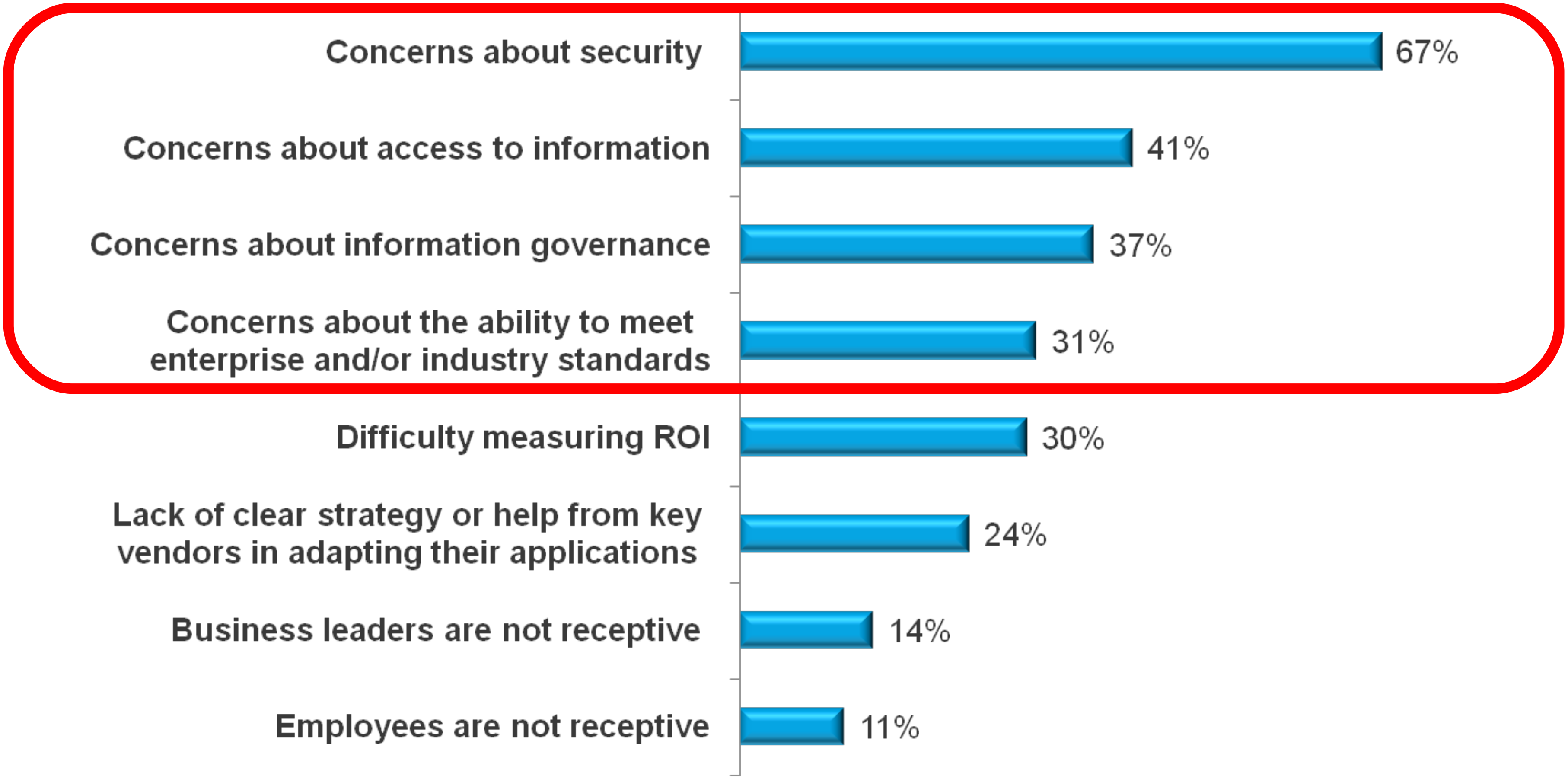
Securing your Cloud

Matt Northam, VMware

In partnership with

Security and Compliance are Key Concerns for CIOs Moving to Cloud

Q. What are the top challenges or barriers to implementing a cloud computing strategy?

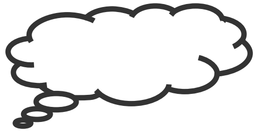


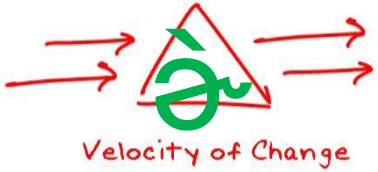
Top 4 Concerns are on Security and Compliance

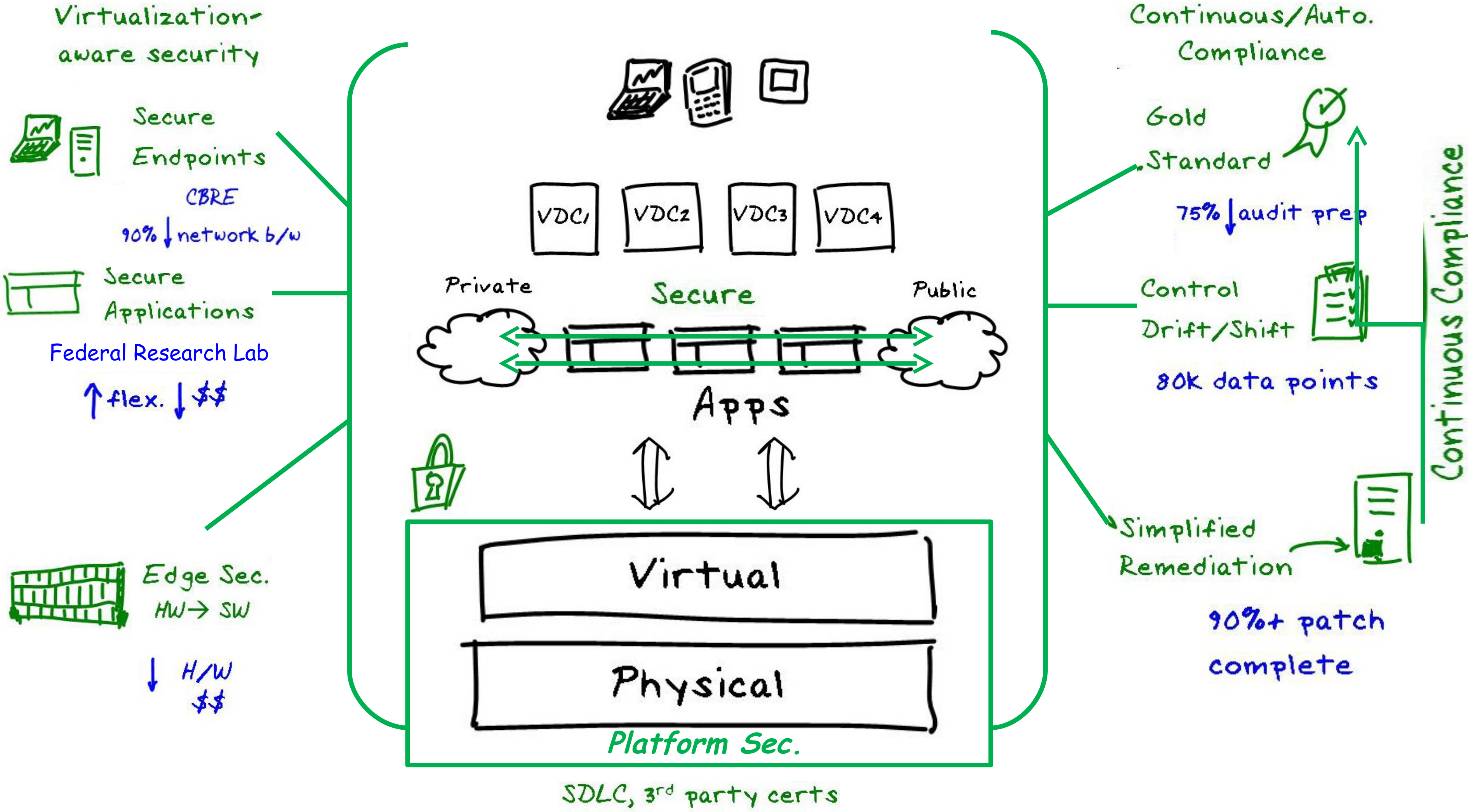
Source: 2010 IDG Enterprise Cloud-based Computing Research, November 2010

IT Security & Compl. in VI & Endpoints

Viz & Control
à
Devices
Apps/Data
Infra
Journey



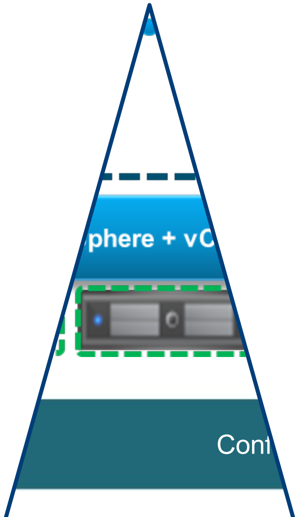




ices

vShield

Elastic
Logical
Efficient
Automated
Programmable
Security as a Service



Shield Edge

- Secure the edge of the virtual datacenter
- Security and Edge networking services gateway

App & Data Security

- vApp and VDI micro-segmentation
- Discover and report regulated data in the Datacenter and Cloud

hield Endpoint

- Efficient offload of anti-virus and file integrity monitoring
- Dramatically improved server VM and VDI consolidation

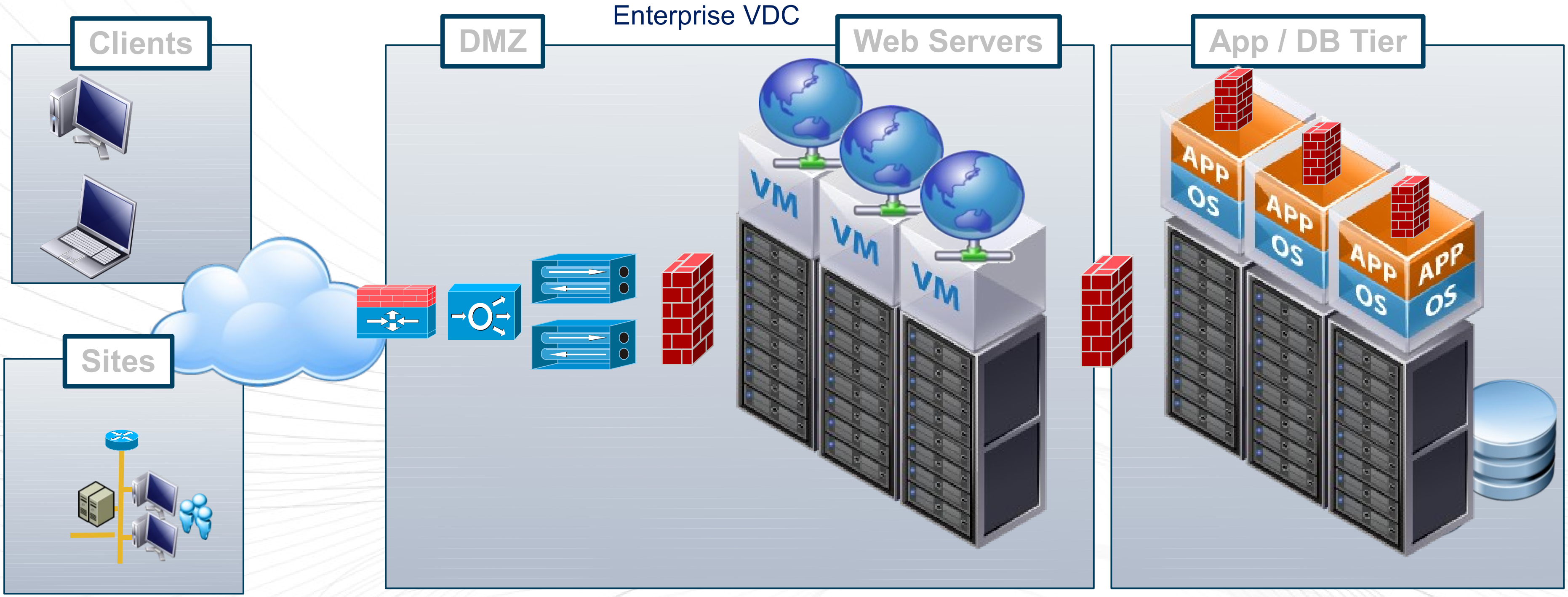
FICO
Building a Secure Private Cloud

This presentation is provided for the recipient only and cannot be reproduced or shared without Fair Isaac Corporation's express consent.

Background

- FICO (NYSE:FICO) is the leader in Decision Management, transforming business by making every decision count. We use predictive analytics to help businesses automate, improve and connect decisions across organizational silos and customer lifecycles.
  - 2,200 Employees around the Globe
  - 4 Data Center Locations
    - 2 US
    - 2 UK
  - 2,300 VMs
    - 1500 server VMs
    - 800 desktop VMs
    - <12 months P2V / virtualize additional 300 servers

FICO – Legacy Environment



Perimeter/DMZ

- Threat Mitigation
- Perimeter security products w/ FW/ VPN/ IPS
- Hardware Sprawl, Expensive

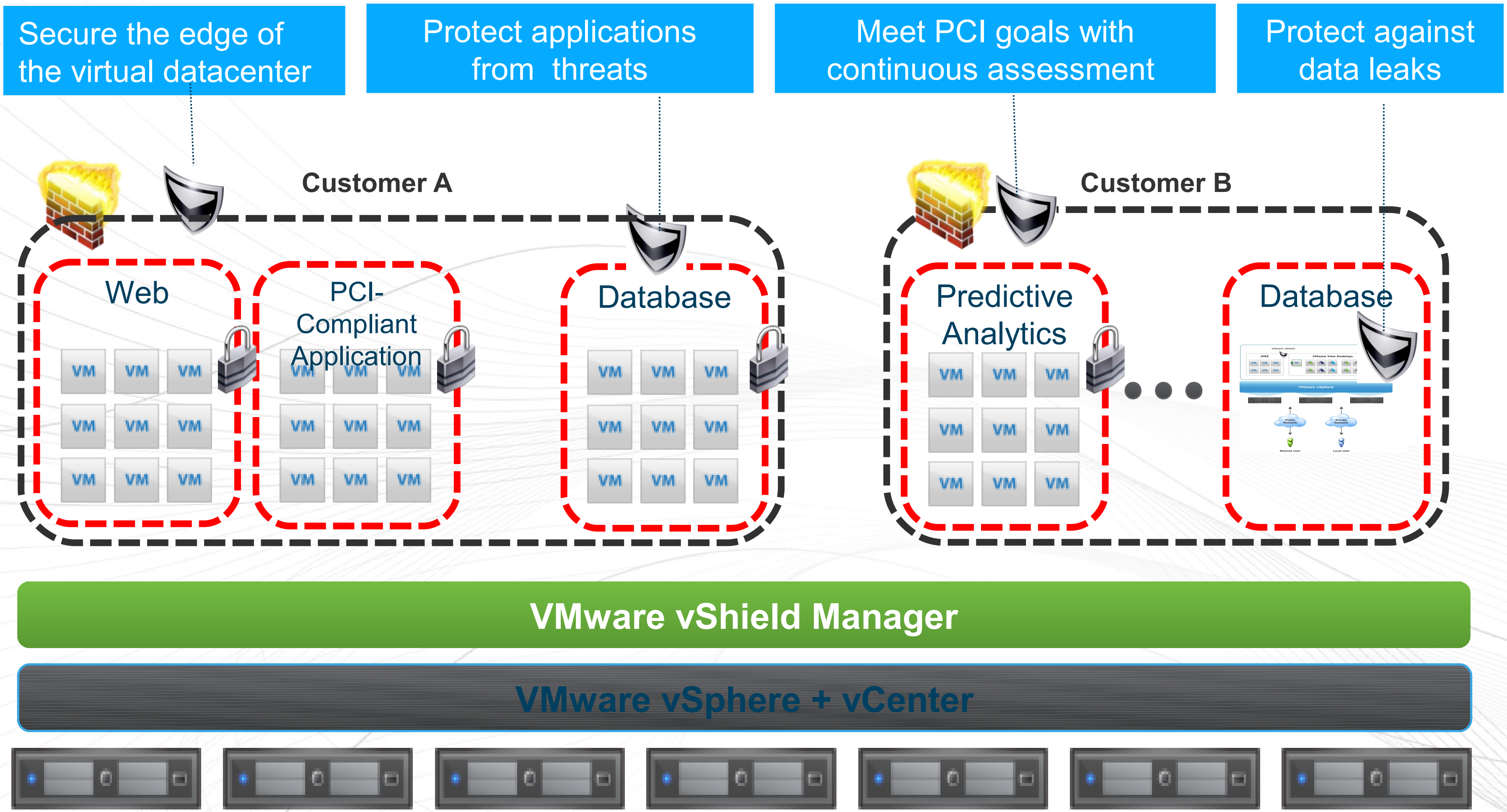
Interior security

- Segmentation of applications and Server
- VLAN or subnet based policies
- VLAN Sprawl, Complex

Endpoint security

- Protecting the Endpoint
- AV, HIPS agent based security
- Agent Sprawl, Cumbersome

FICO – Foundation for Trusted Private Cloud



Secure the edge of the virtual datacenter

Protect applications from threats

Meet PCI goals with continuous assessment

Protect against data leaks

Customer A

Web

PCI-Compliant Application

Database

Customer B

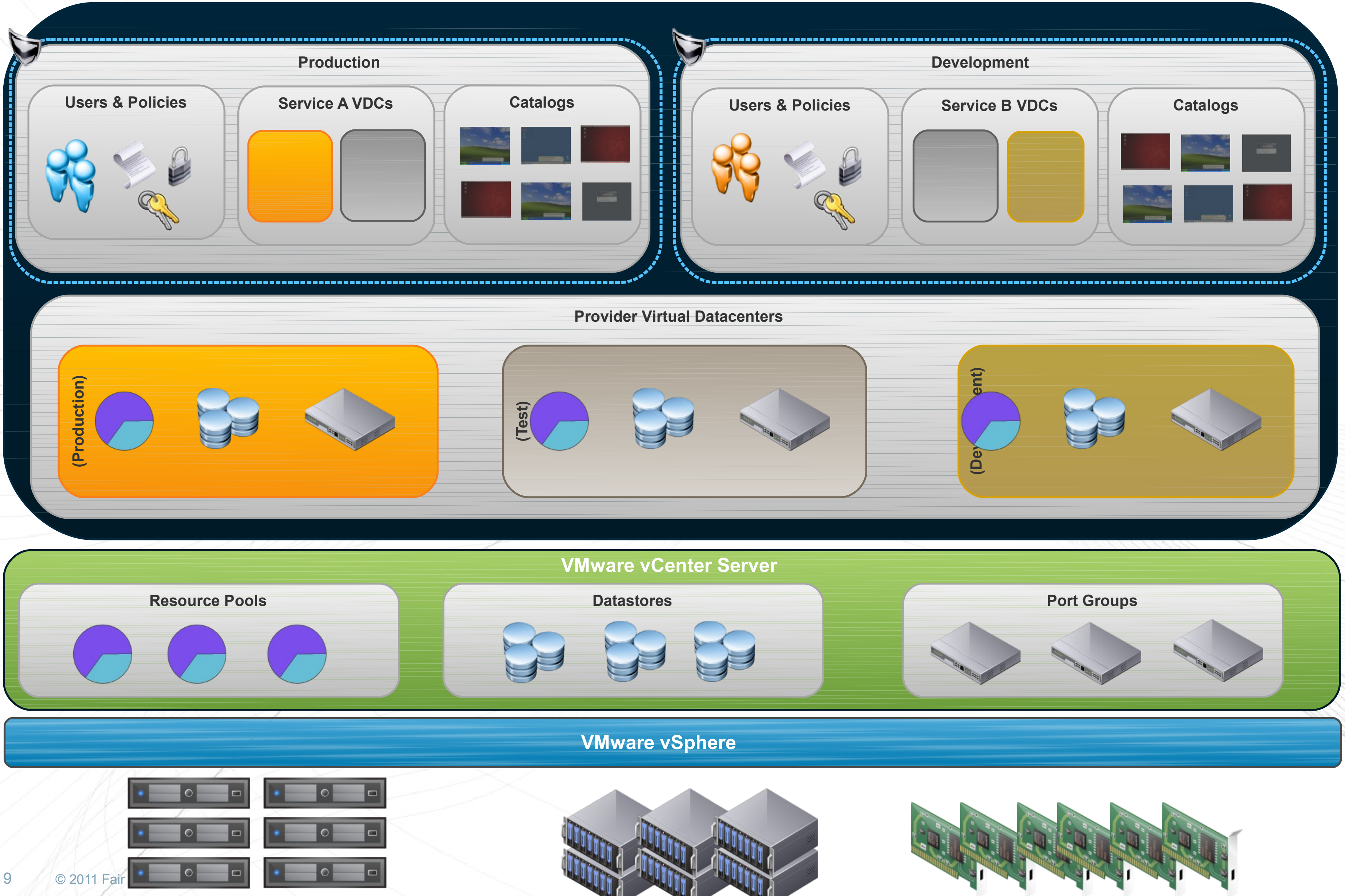
Predictive Analytics

Database

VMware vShield Manager

VMware vSphere + vCenter

FICO Cloud Architecture



Production

Users & Policies

Service A VDCs

Catalogs

Development

Users & Policies

Service B VDCs

Catalogs

Provider Virtual Datacenters

(Production)

(Test)

(De ent)

VMware vCenter Server

Resource Pools

Datastores

Port Groups

VMware vSphere

Building a Secure Hybrid Cloud: LANL's Infrastructure on Demand

Anil Karmel

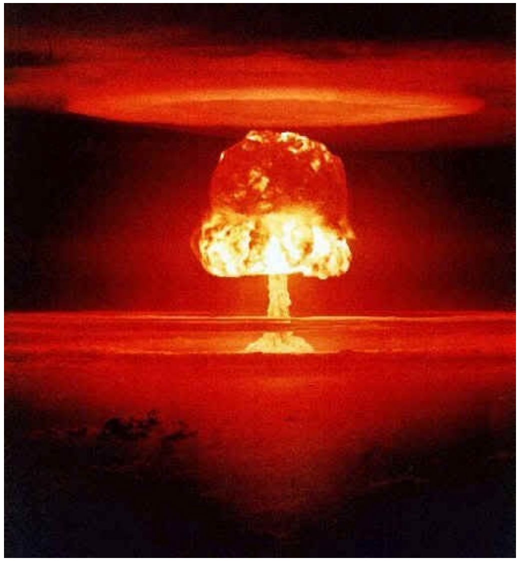
Solutions Architect

Network & Infrastructure Engineering
Production Systems

Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA

Background
Los Alamos National Laboratory

- LANL applies its expertise in defense science and technology to the broad spectrum of DOE requirements from basic research to ensuring the safety and reliability of the U.S. nuclear weapons stockpile

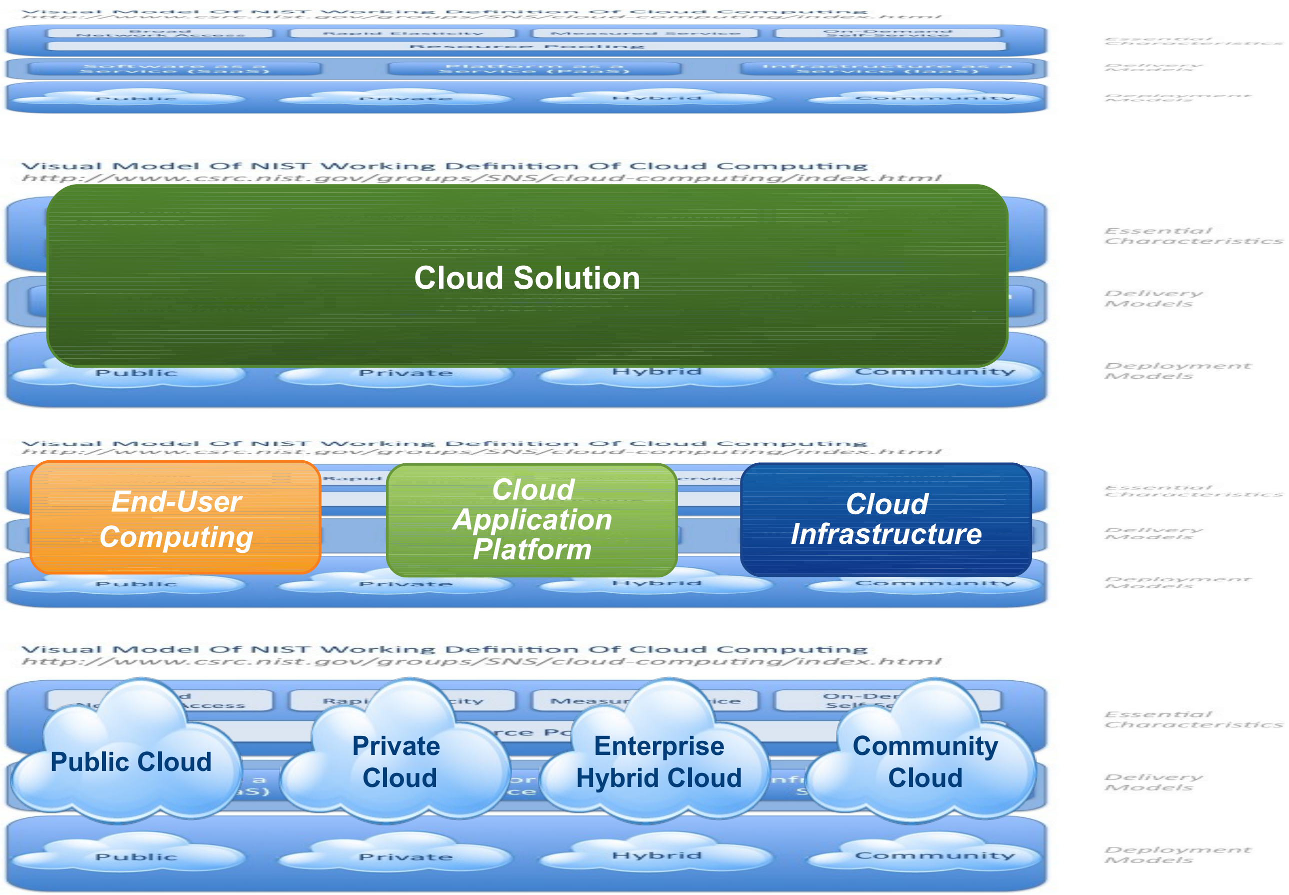


Background
Los Alamos National Laboratory

- Located in northern New Mexico
- Elevation – 7500 feet
- 42 square mile campus
- 10,000 employees
- Unclassified Protected Network Stats
  - ~ 20,000 devices
    - ~ 14,000 Windows Systems
    - ~ 3,000 Apple Systems
    - ~ 1,500 *Nix Systems

Cloud Requires Elasticity, On-demand Access, and Resource Pooling

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

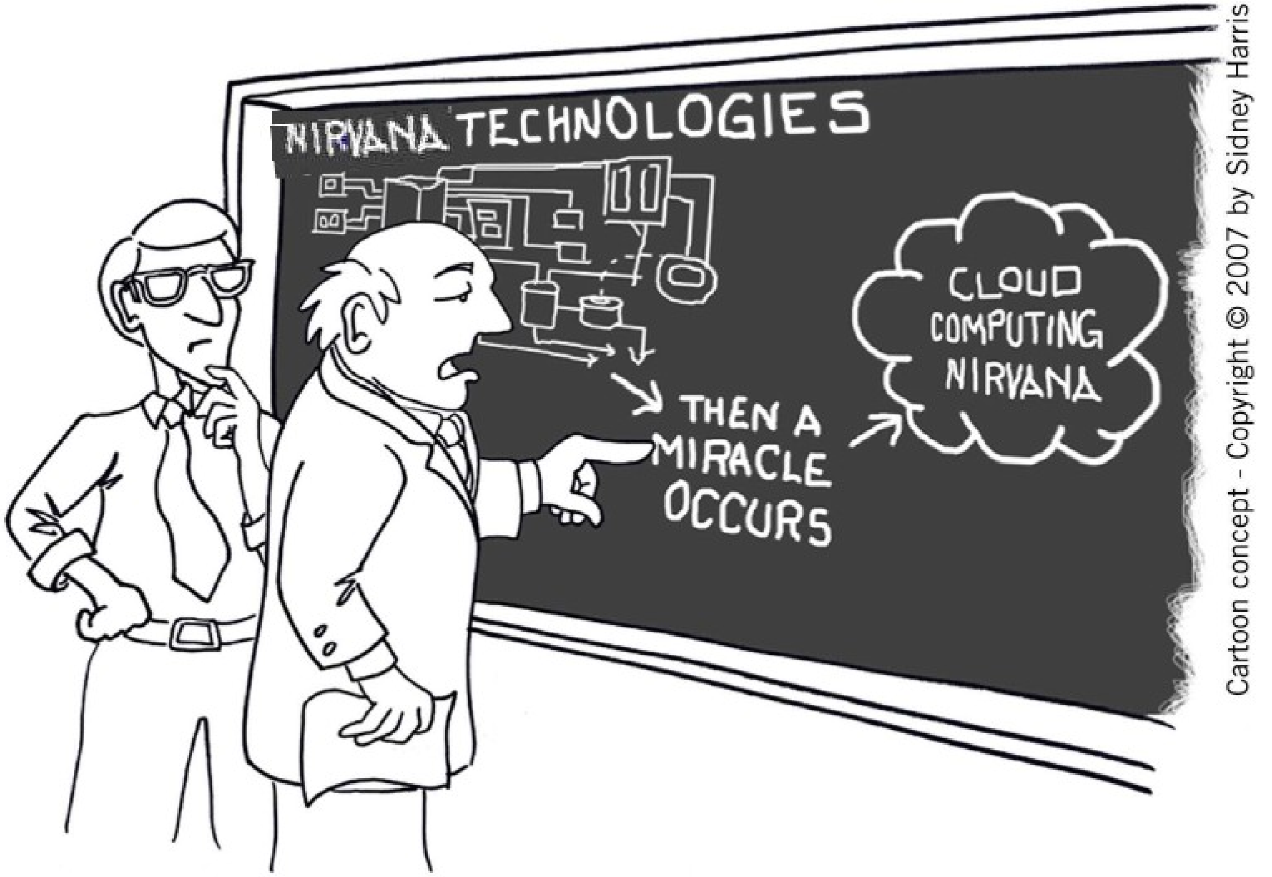


Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services).

Private Cloud
LANL Infrastructure on Demand (IoD)

- LANL's Infrastructure on Demand
  - DOE first Infrastructure-as-a-Service (IaaS) private cloud
  - Self-service web portal to automatically request and provision virtual servers
  - Green IT savings dynamically computed and displayed on website
  - Includes LifeCycle Management and Chargeback
  - OS Support
    - Microsoft Windows
    - Red Hat Enterprise Linux
    - Sun Solaris

How Did We Do It?



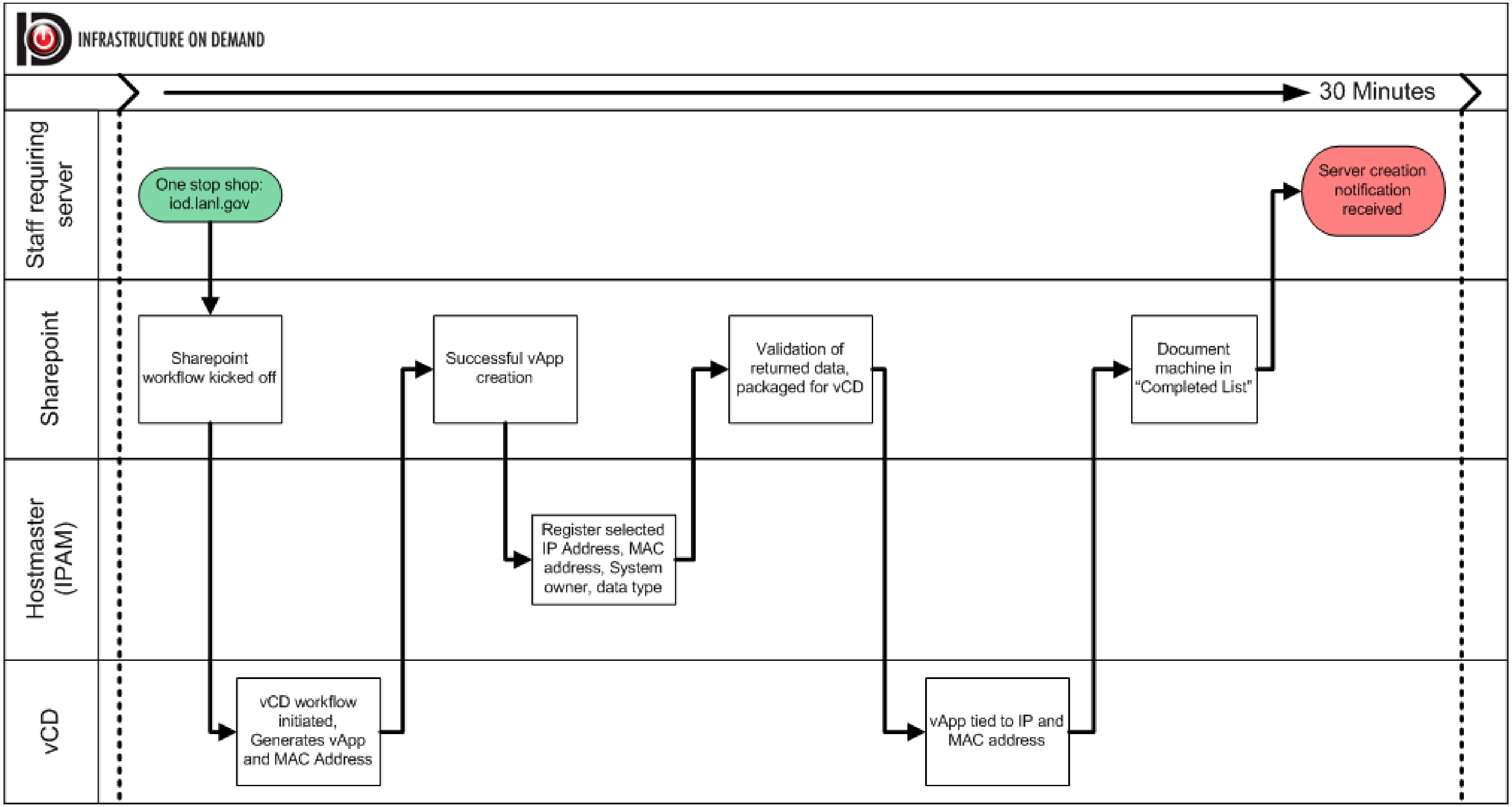
Cartoon concept - Copyright © 2007 by Sidney Harris

"I think you should be more explicit here in step two."

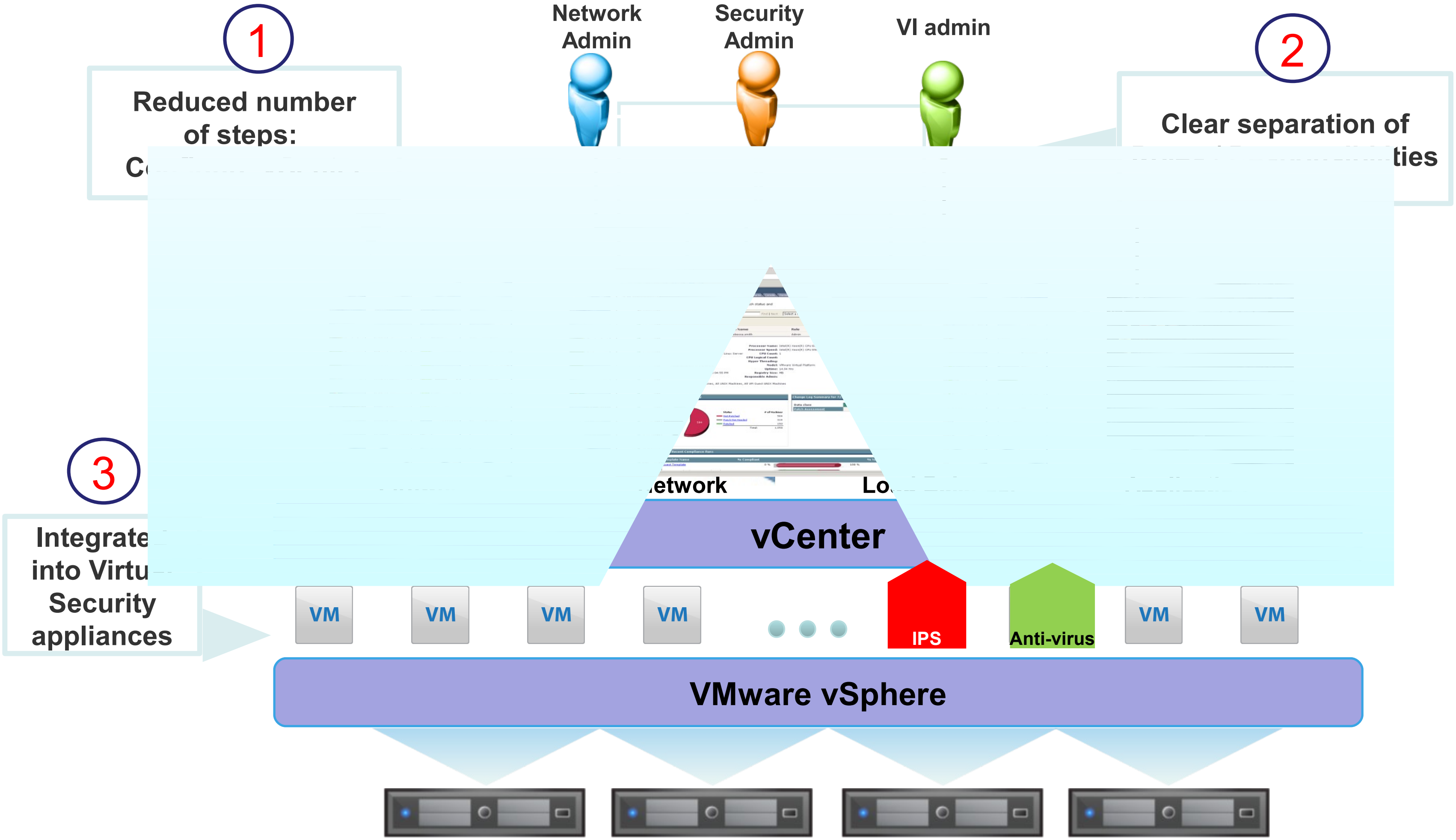
Private Cloud
LANL Infrastructure on Demand (IoD)

- Key Components
  - Web Portal
    - Front End displaying information regarding the service and form to request a system
  - Microsoft SharePoint
    - Workflow Engine including Lifecycle Management
    - Integration Point for internal systems including Chargeback and Hostmaster Registration System
  - VMware vCloud Director
    - Web Based User Interface to consume cloud resources
    - Enables the Private Cloud
  - VMware vShield Application / Edge
    - Virtual Appliance to implement, manage and maintain security policy
    - Security in the Private Cloud

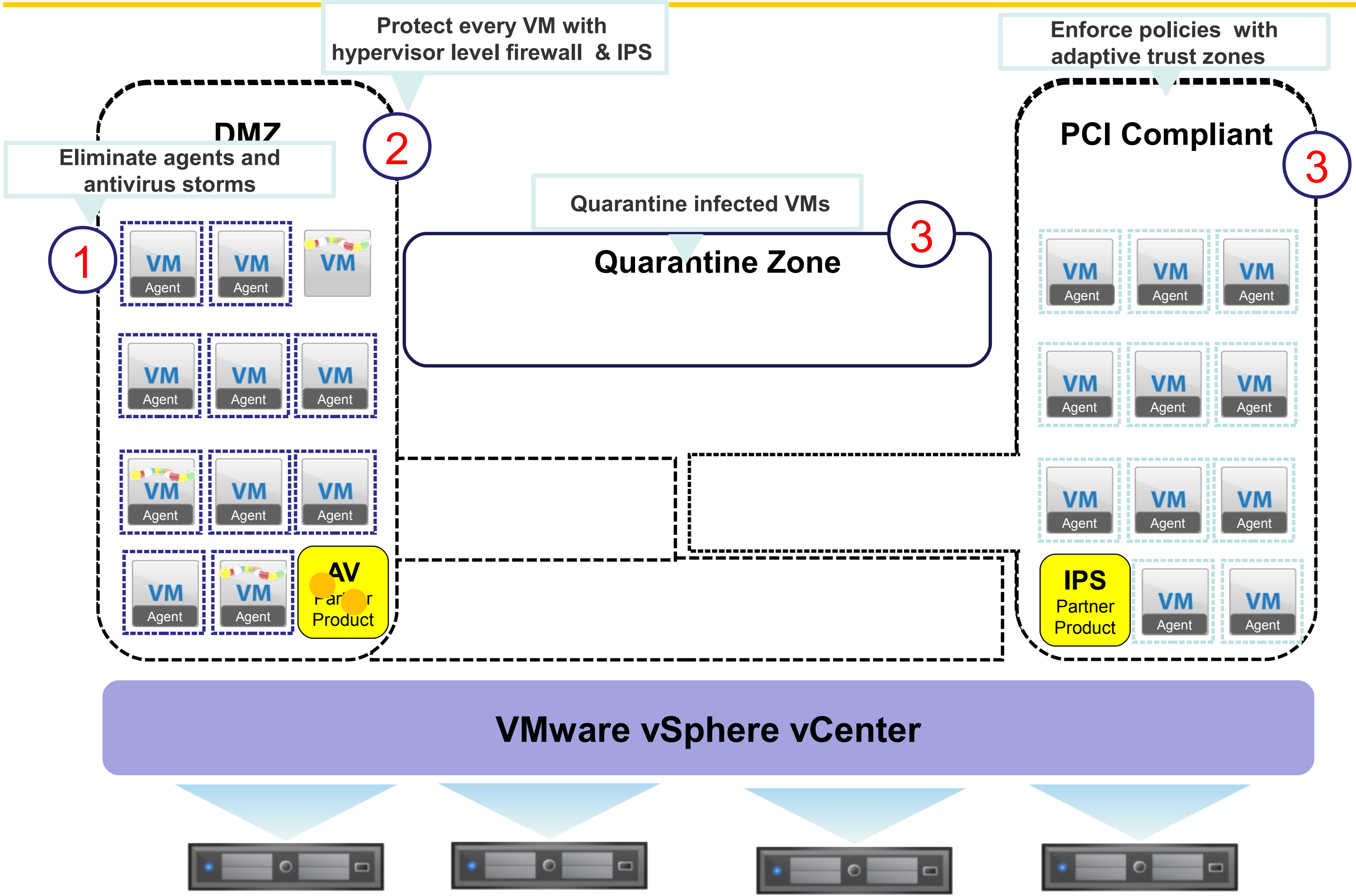
Private Cloud
LANL Infrastructure on Demand (IoD)


INFRASTRUCTURE ON DEMAND
30 Minutes
Staff requiring server
Sharepoint
Hostmaster (IPAM)
vCD
One stop shop: iod.lanl.gov
Sharepoint workflow kicked off
vCD workflow initiated, Generates vApp and MAC Address
Successful vApp creation
Register selected IP Address, MAC address, System owner, data type
Validation of returned data, packaged for vCD
vApp tied to IP and MAC address
Document machine in "Completed List"
Server creation notification received

1. Requirement – Disruptively Simple Architecture



2. Requirement – Adaptive Security



Protect every VM with hypervisor level firewall & IPS

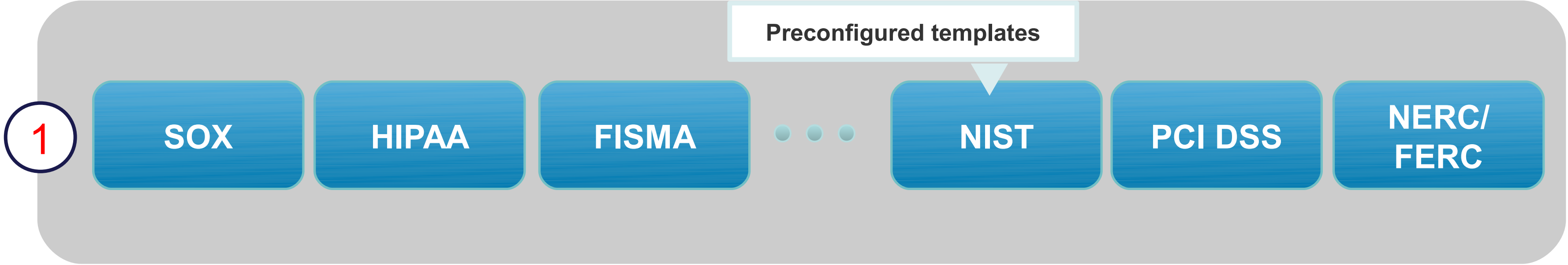
Enforce policies with adaptive trust zones

Eliminate agents and antivirus storms

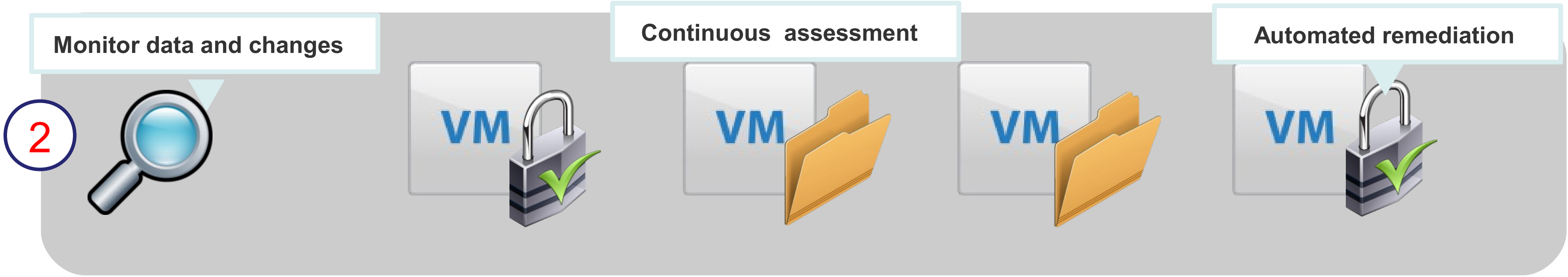
Quarantine infected VMs

3. Requirement – Continuous Compliance

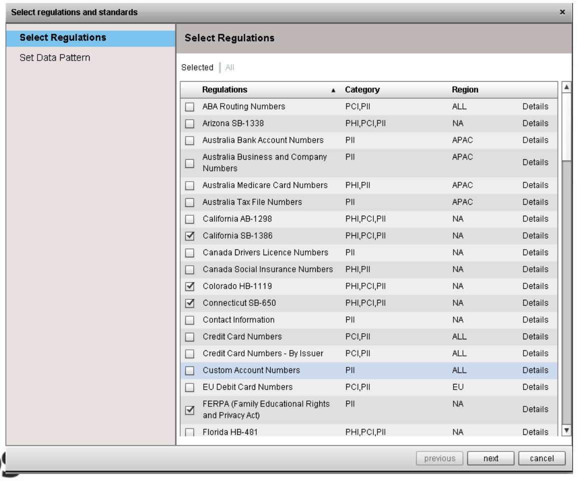
1



2



3



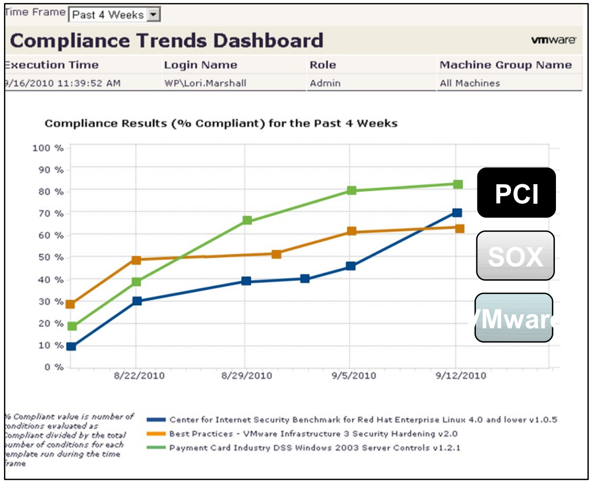
Select regulations and standards

- **Select Regulations**
- Set Data Pattern

Select Regulations

Selected | All

	Regulations	Category	Region	
□	ABA Routing Numbers	PCI,PII	ALL	Details
□	Arizona SB-1338	PHI,PCI,PII	NA	Details
□	Australia Bank Account Numbers	PII	APAC	Details
□	Australia Business and Company Numbers	PII	APAC	Details
□	Australia Medicare Card Numbers	PHI,PII	APAC	Details
□	Australia Tax File Numbers	PII	APAC	Details
□	California AB-1298	PHI,PCI,PII	NA	Details
☑	California SB-1386	PHI,PCI,PII	NA	Details
□	Canada Drivers Licence Numbers	PII	NA	Details
□	Canada Social Insurance Numbers	PHI,PII	NA	Details
☑	Colorado HB-1119	PHI,PCI,PII	NA	Details
☑	Connecticut SB-650	PHI,PCI,PII	NA	Details
□	Contact Information	PII	NA	Details
□	Credit Card Numbers	PCI,PII	ALL	Details
□	Credit Card Numbers - By Issuer	PCI,PII	ALL	Details
□	Custom Account Numbers	PII	ALL	Details
□	EU Debit Card Numbers	PCI,PII	EU	Details
☑	FERPA (Family Educational Rights and Privacy Act)	PII	NA	Details
□	Florida HB-481	PHI,PCI,PII	NA	Details



Time Frame: Past 4 Weeks

Compliance Trends Dashboard

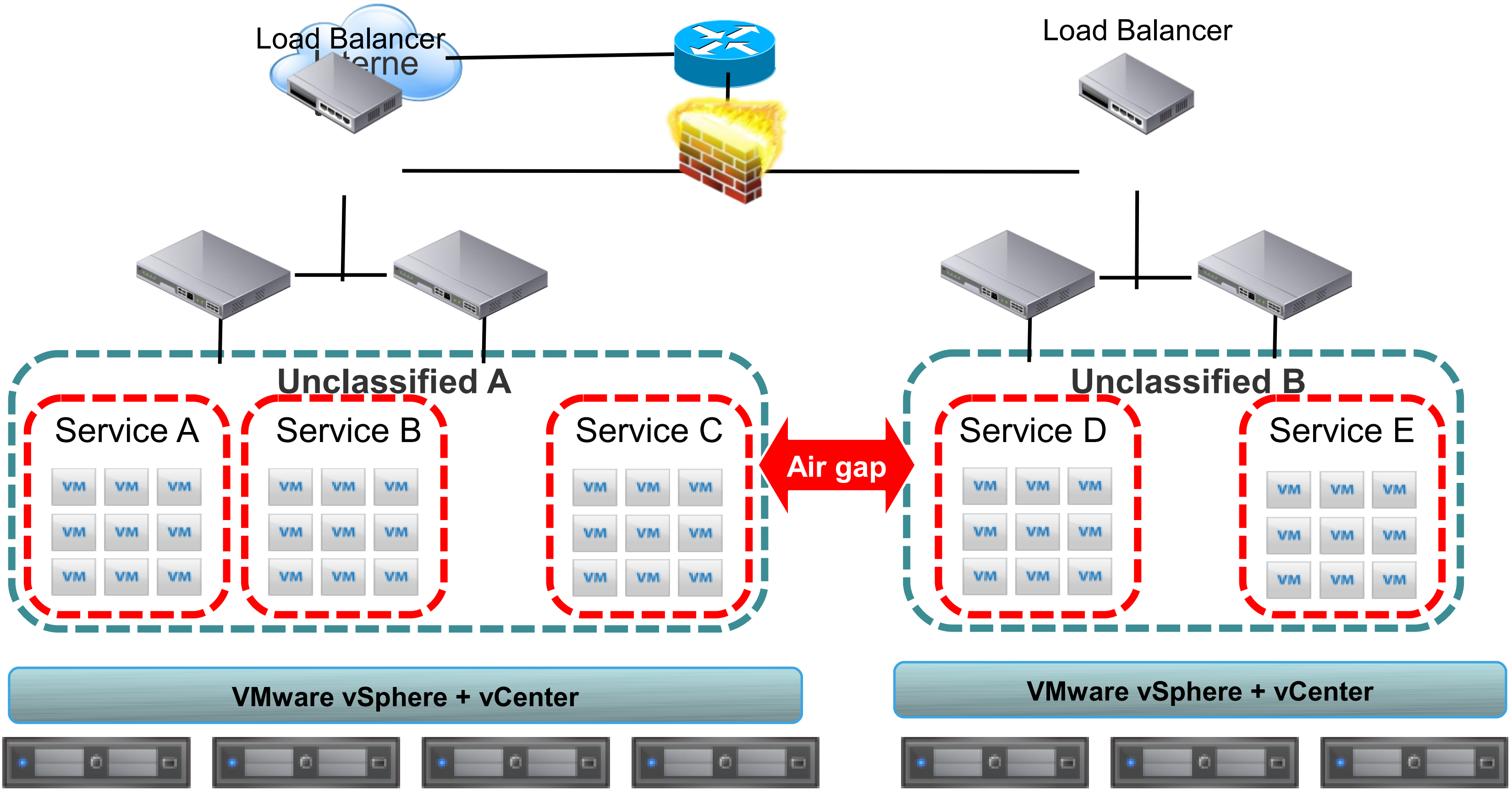
Execution Time	Login Name	Role	Machine Group Name
9/16/2010 11:39:52 AM	WP\Lori.Marshall	Admin	All Machines

Compliance Results (% Compliant) for the Past 4 Weeks

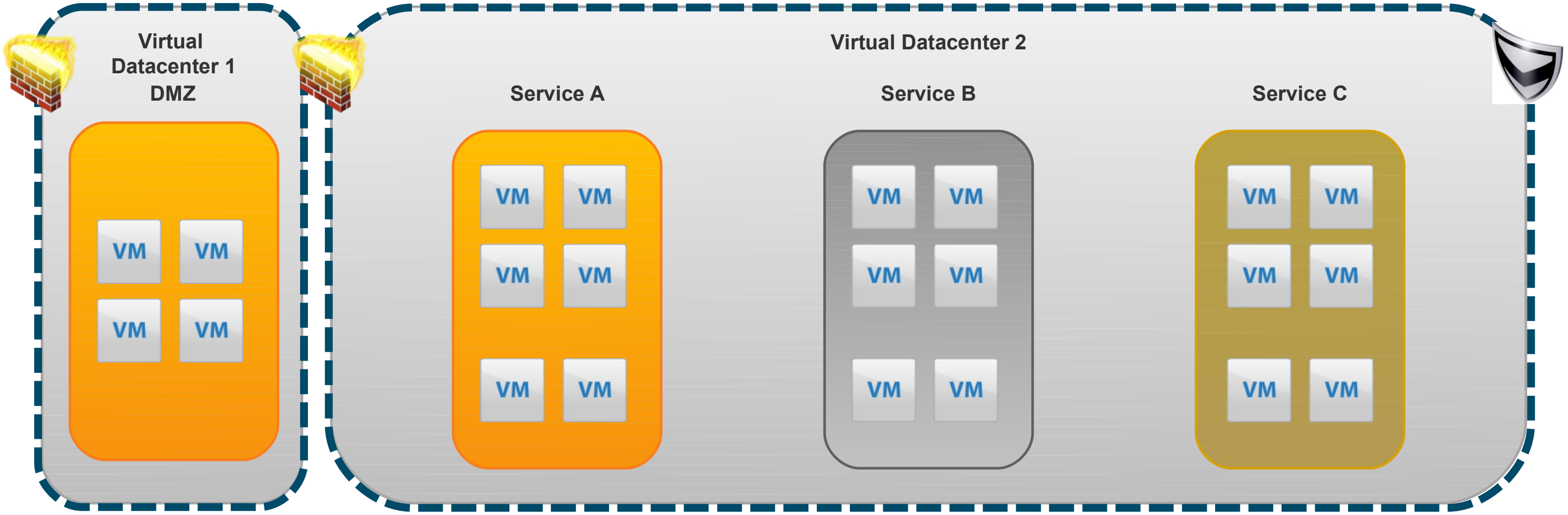
% Compliant value is number of conditions evaluated as Compliant divided by the total number of conditions for each template run during the time frame

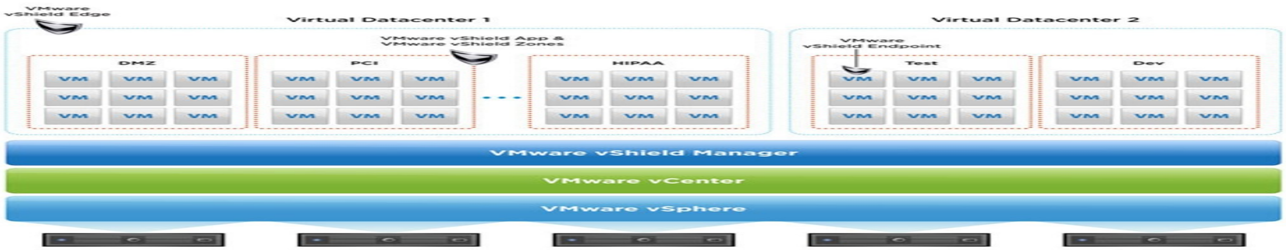
- 🟦 Center for Internet Security Benchmark for Red Hat Enterprise Linux 4.0 and lower v1.0.5
- 🟧 Best Practices - VMware Infrastructure 3 Security Hardening v2.0
- 🟩 Payment Card Industry DSS Windows 2003 Server Controls v1.2.1

Physical Security Architecture
Hardware Appliances and VLANs

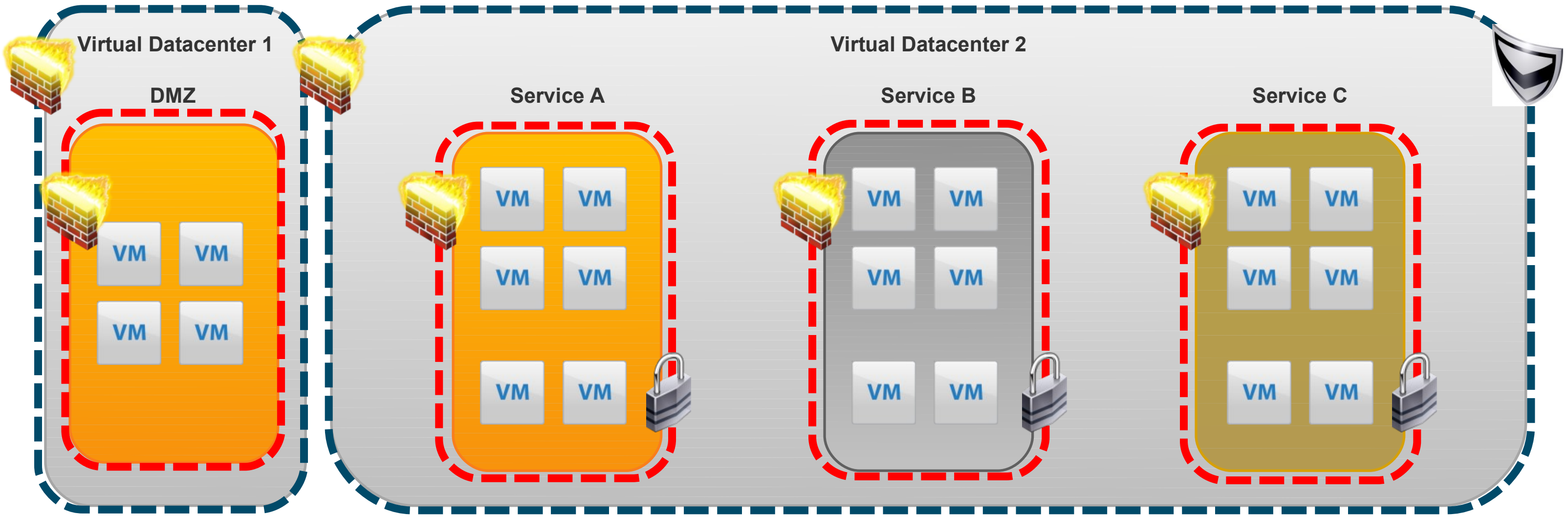


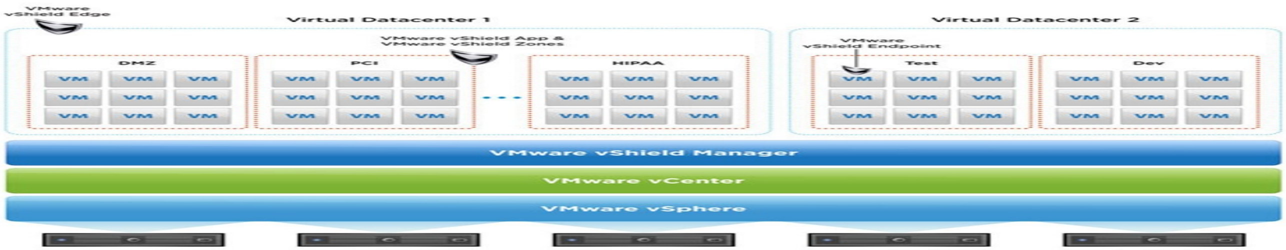
2. Secure the Perimeter



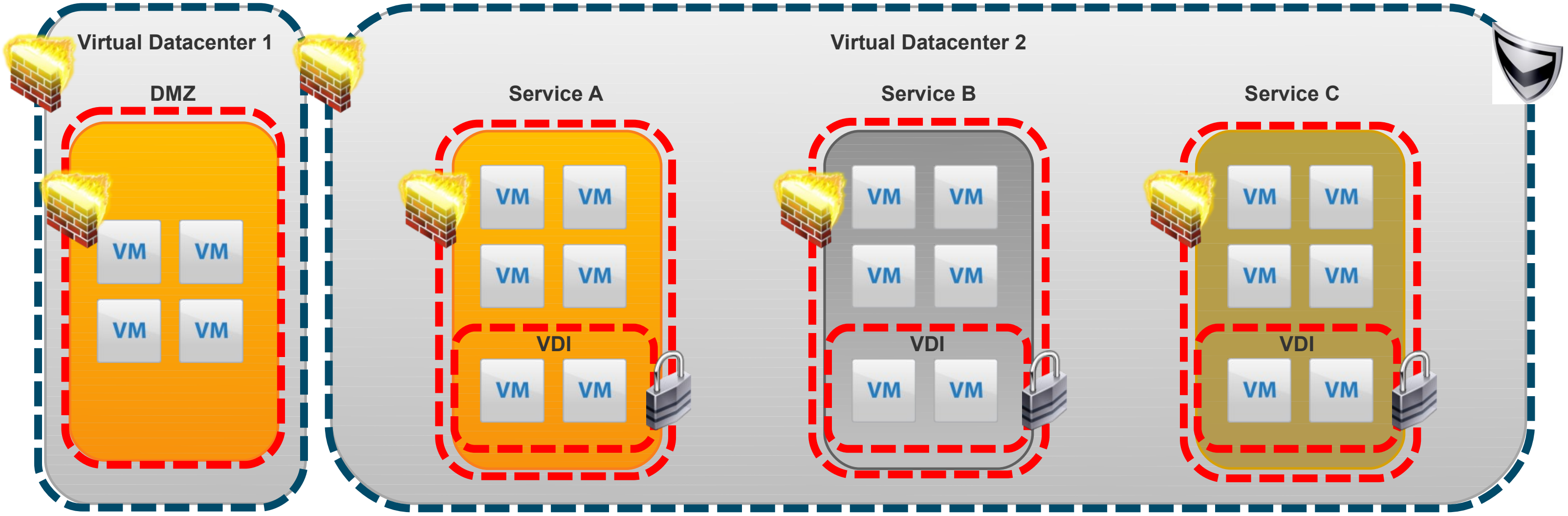


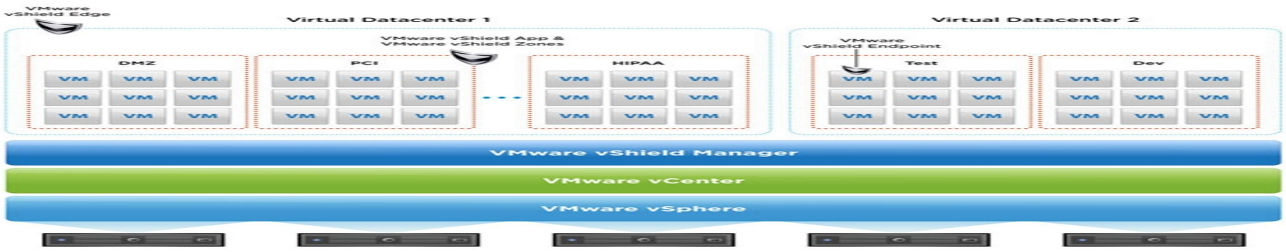
3. Protect the Applications



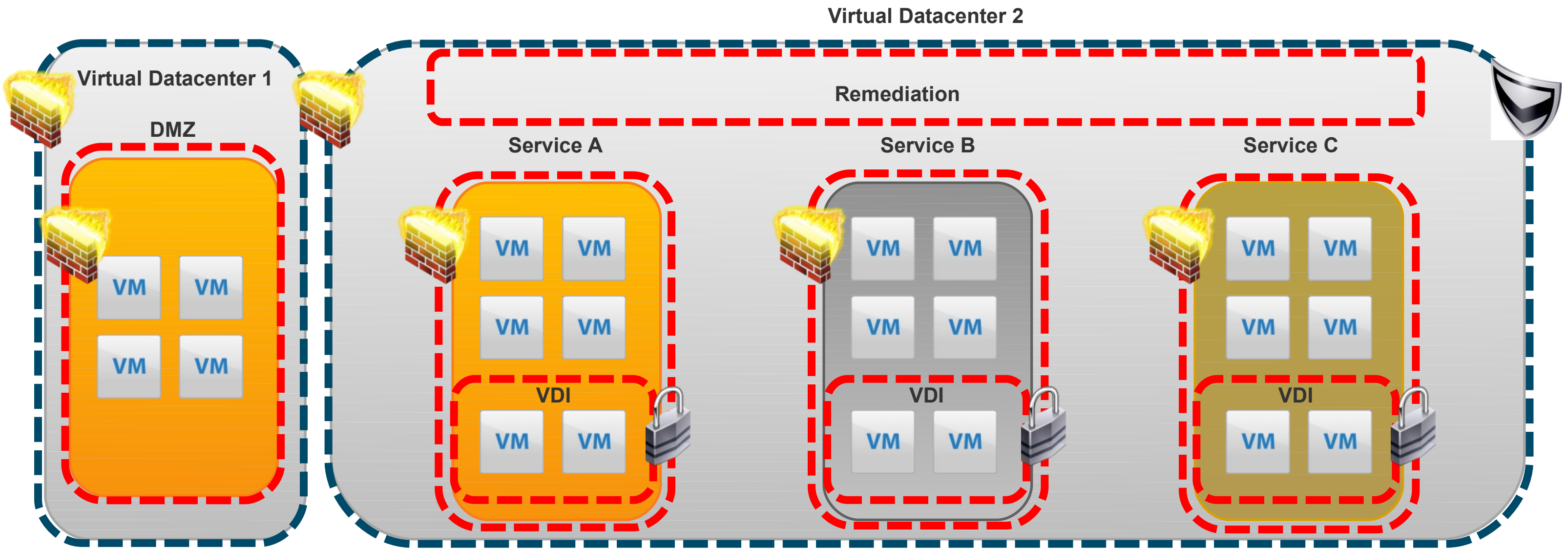


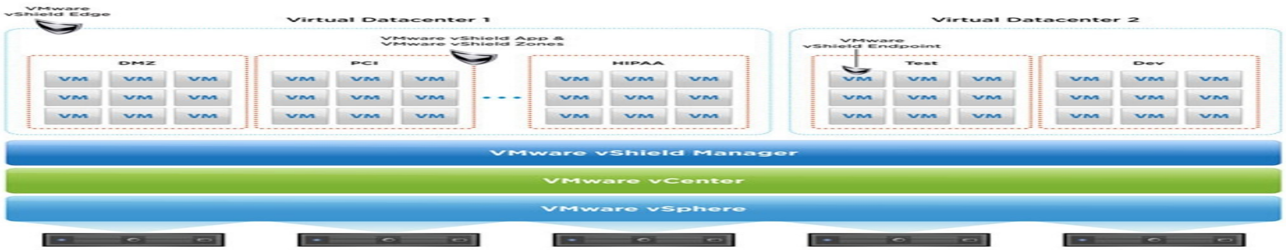
4. Protect the VDI Clients



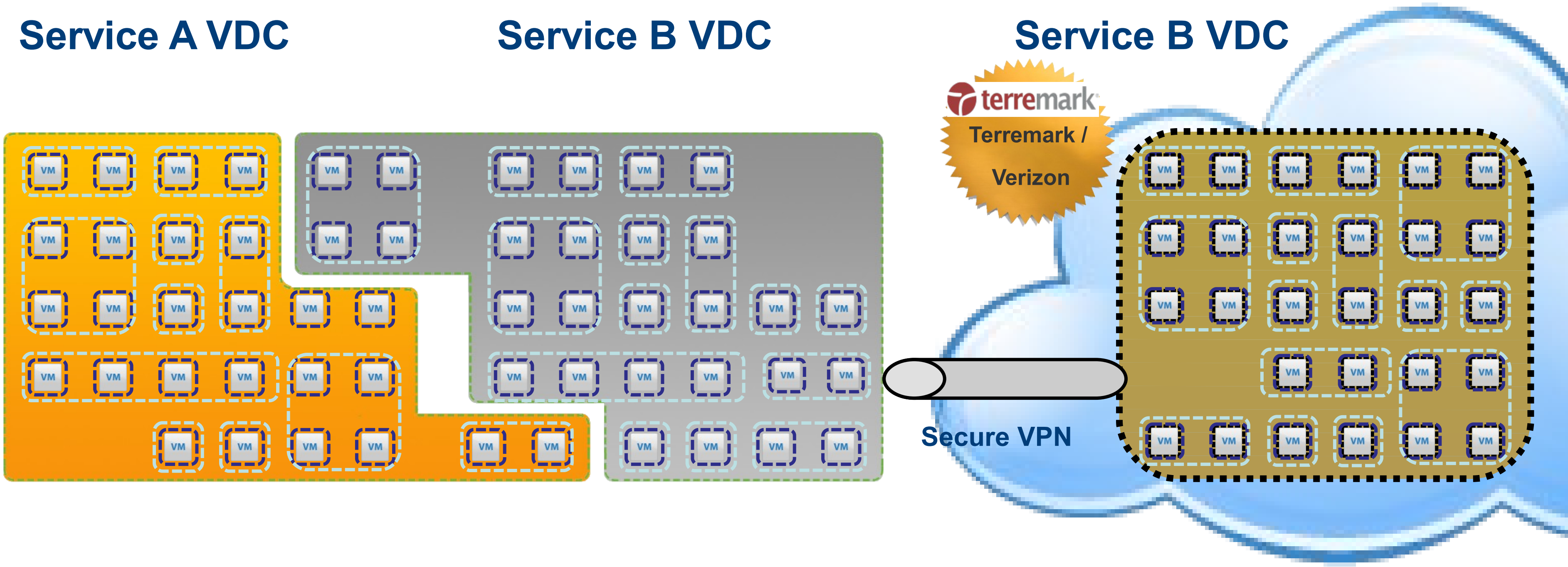


5. Quarantine Compromised Virtual Machines





6. Secure Hybrid Cloud Computing



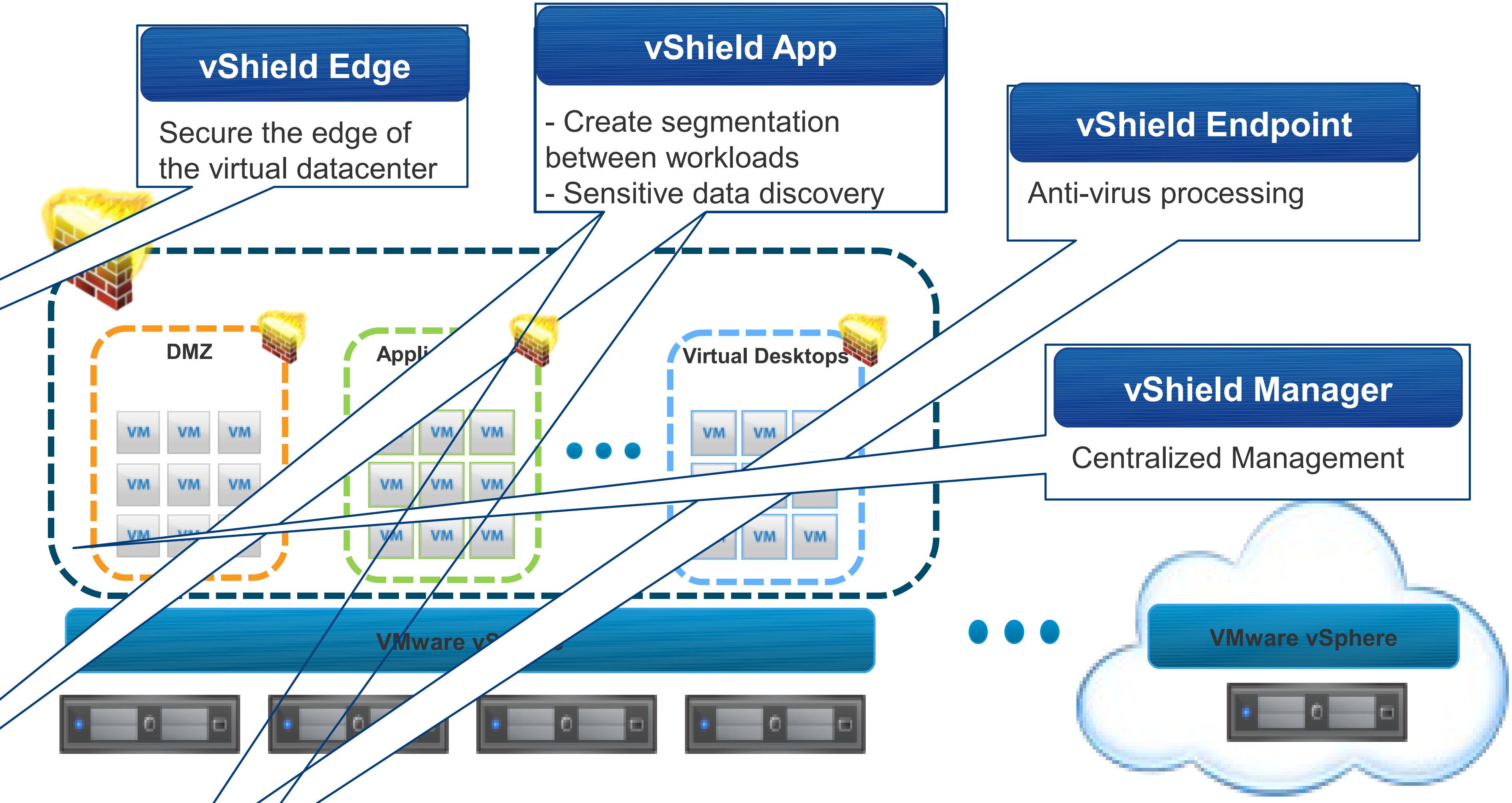
Secure Private Cloud

Cloud Datacenter

vShield Product Overview

vShield Product Family

Securing the Private Cloud End to End: from the Edge to the Endpoint



vShield Edge

Secure the edge of the virtual datacenter

vShield App

- Create segmentation between workloads
- Sensitive data discovery

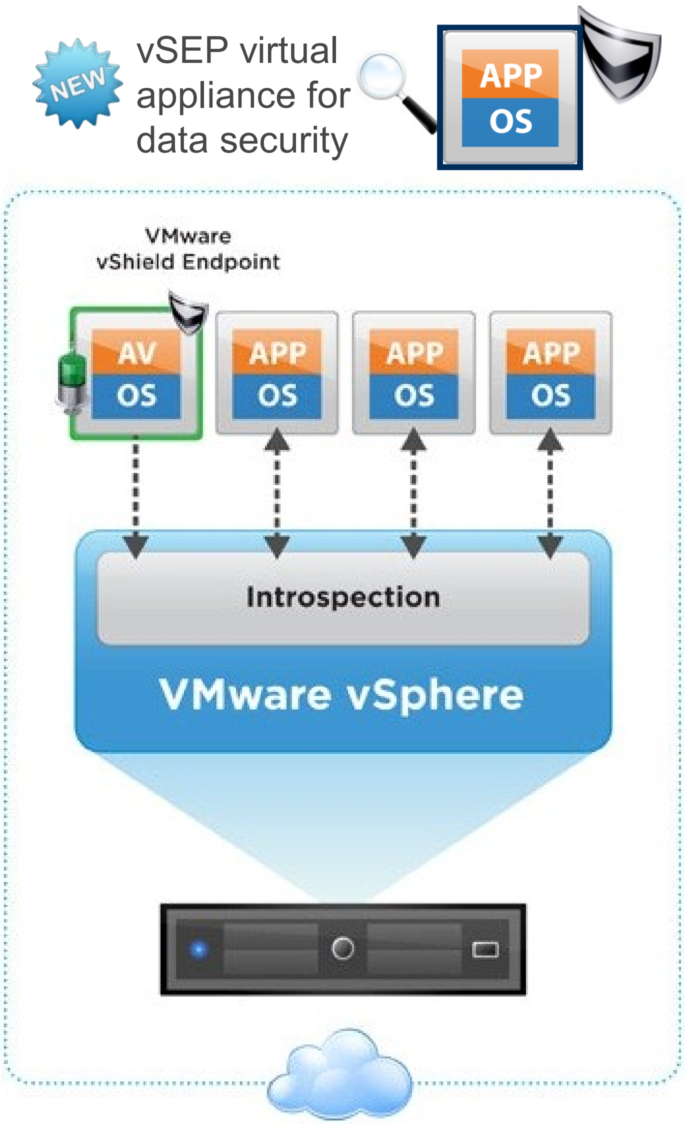
vShield Endpoint

Anti-virus processing

vShield Manager

Centralized Management

EPSEC 2.0 Enables Anti-virus and Data Security Solutions



- **What's the same**
  - vShield Endpoint Virtual Appliance (vSEP-VA)
  - Thin Agent
  - vShield Endpoint ESX hypervisor module
- **New Features to support data security**
  - Support for two or more vSEP-VAs (allows anti-virus and data security to run on the same host)
  - A vSEP-VA for data security, provided by vShield
- **End user packaging**
  - vShield App with Data Security (confirmed)
  - vShield Data Security (planning stages)
  - Both require vShield Endpoint

Disclaimer

- **This presentation may contain product features that are currently under development.**
- **This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.**
- **Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.**
- **Technical feasibility and market demand will affect final delivery.**
- **Pricing and packaging for any new technologies or features discussed or presented have not been determined.**

IMPORTANT

Do not leave behind the PPT version of this presentation in electronic or printed form.

Leave-behinds can only be in PDF format for approved customers.

The information on the roadmap is intended to outline our general product direction and it should not be relied on in making a purchasing decision. It is for informational purposes only and may not be incorporated into any contract.

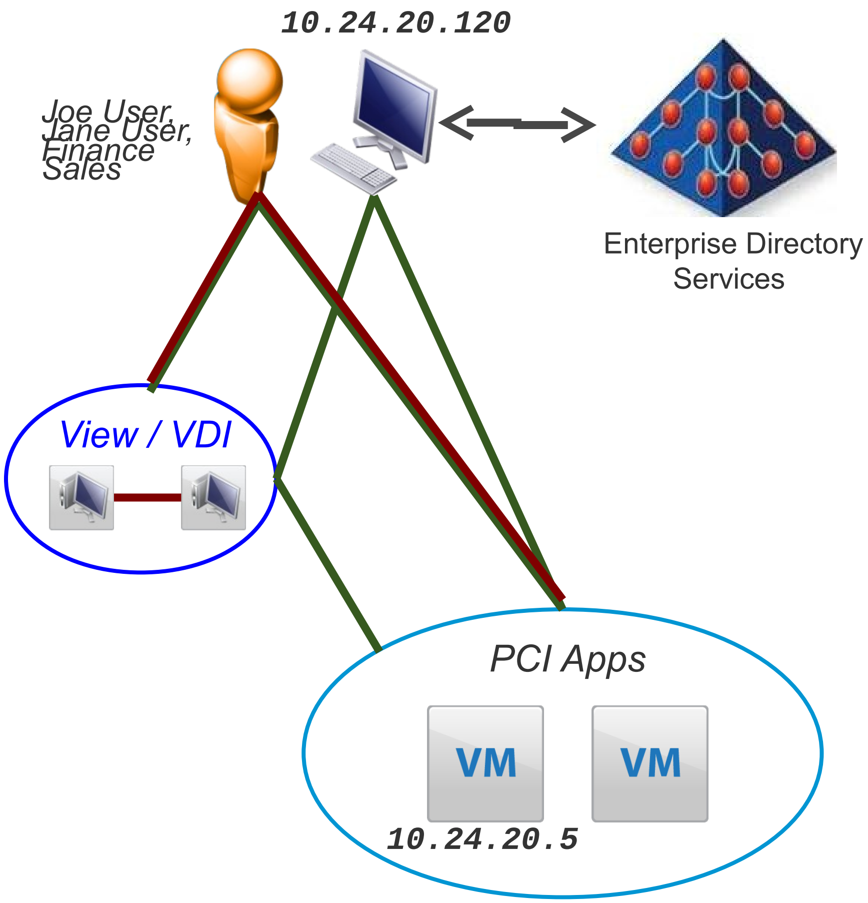
Where we’re headed

Edge, App, Endpoint, Data, Platform Security

New World: Security & Compliance for the Hybrid Cloud

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA
ADMINISTRATIVE SIMPLIFICATION: PRIVACY SECURITY TRANSACTIONS

vShield Identity Services for vShield App



"Sales User DENY PCI Apps"

First, logical containers

- IP address ✳ shows what system
- vShield App enables creation of logical security groups (zones)
- Firewall rules secure these groups

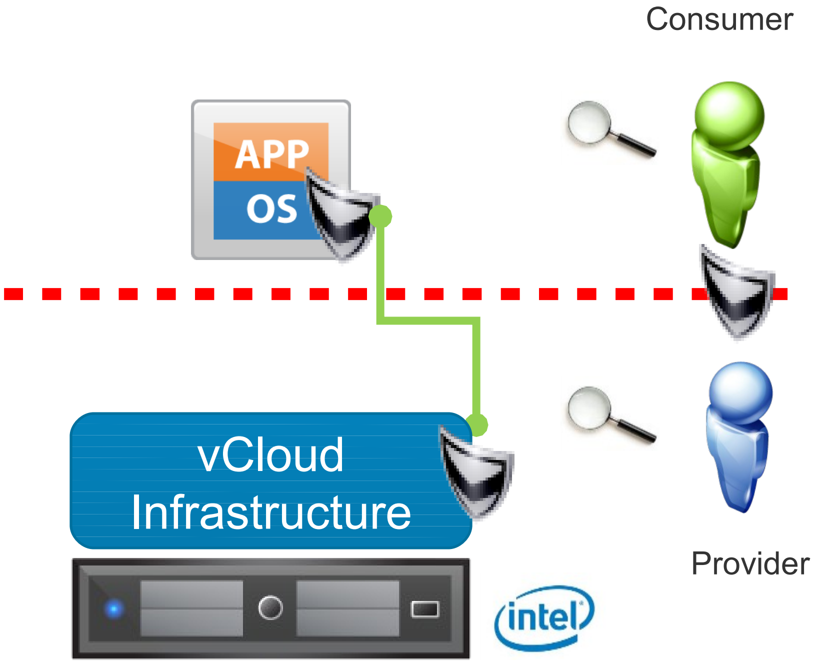
Now, identity context

- See the who - physical and virtual source IP transforms to groups and users
- Firewall leverages identity context

Unprecedented agility

- Language matches business policy

Secure The Cloud Platform and Isolate the Provider



Trusted Platform

- Trusted boot with Intel TPM
- Deploy workloads and store data only in trusted infrastructure

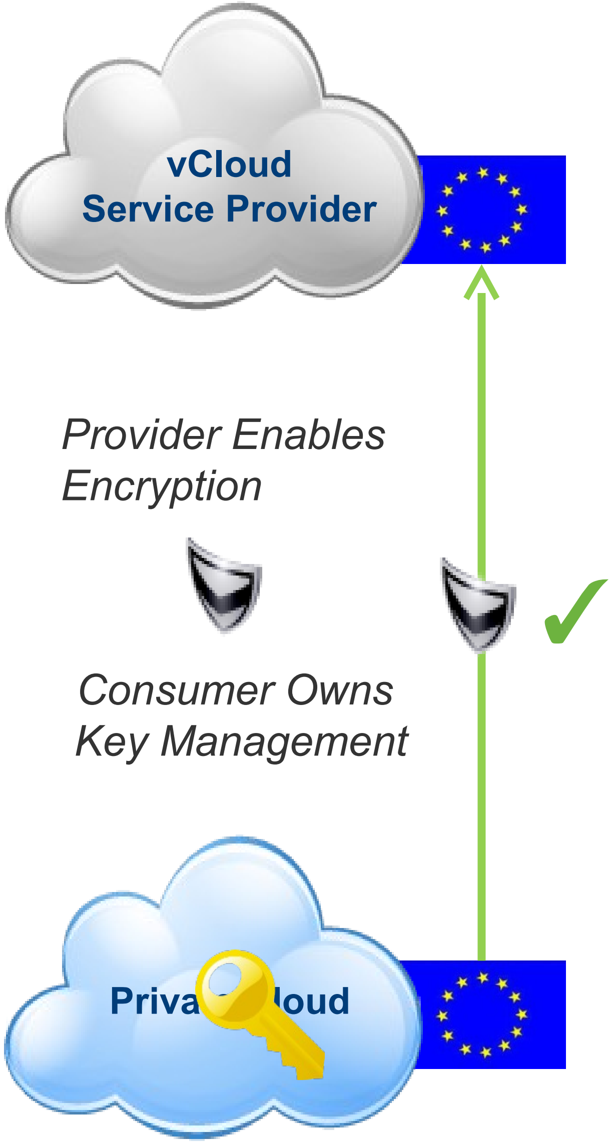
Admin Separation of Duties

- Across Functional Areas
- Between provider and consumer

User Activity Monitoring

- Of privileged users in Cloud Infrastructure

Secure and Isolate Data in the Hybrid Cloud



Confidentiality

- Encrypt application, user data
- At rest, in motion, in use
- Within and across clouds

Simplified key management

- Consumer owns their keys
- Provider requests keys
- Interoperability is mandatory

Geo Location

- Enforce geo location policy for data privacy laws (i.e. within EU)