



Visions of Clouds and Cloud Security

Rob Randell, CISSP

Senior Security and Compliance Specialist

VMware, Inc.

Visions of Clouds and Cloud Security

What is the “Cloud”?

- > PAAS
- > SAAS
- > IAAS

Chris Hoff’s Model of the Cloud

Cloud Security Alliance’s 15 Domains

We will focus on IAAS

- > Virtualization is the Basis
- > Basic Virtualization Overview

What is the private cloud?

- > Internal Cloud
- > External Cloud
- > Internal Cloud + External Cloud = Private Cloud
- > Benefits of the Private Cloud
- > Limitations of the Private Cloud

Cloud Security Reference Architecture

What is the Cloud?

“X as a Service” Types of Clouds

> **Software** as a Service (SaaS)

- Salesforce.com
- Google Apps

> **Platform** as a Service (PaaS)

- Google App Engine
- Force.com

> **Infrastructure** as a Service (IaaS)

- Amazon EC2
- Rackspace
- Savvis

Security Considerations of Each Type of Cloud

> Software (SaaS)

- Least extensibility and greatest amount of security responsibility taken on by the cloud provider

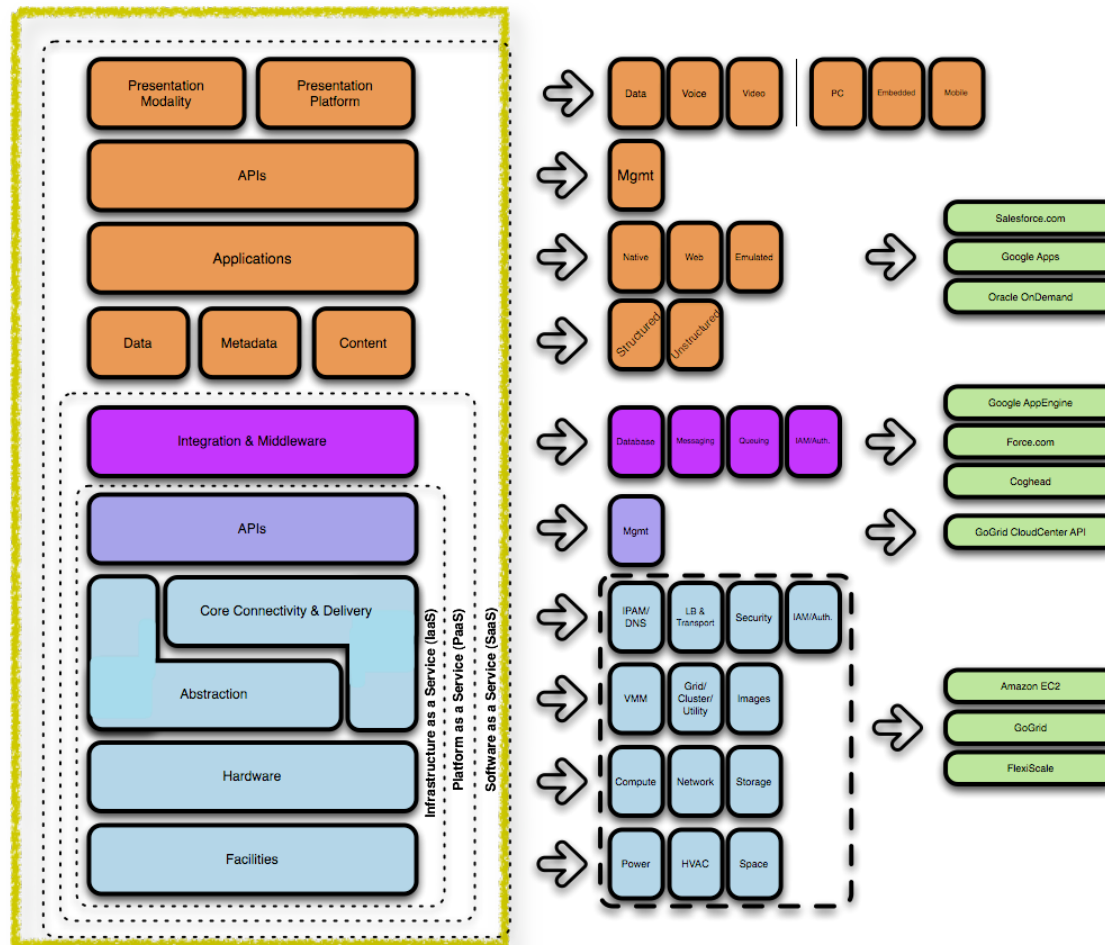
> Infrastructure (IaaS)

- Greatest extensibility and least amount of security responsibility taken on by the cloud provider

> Platform (PaaS)

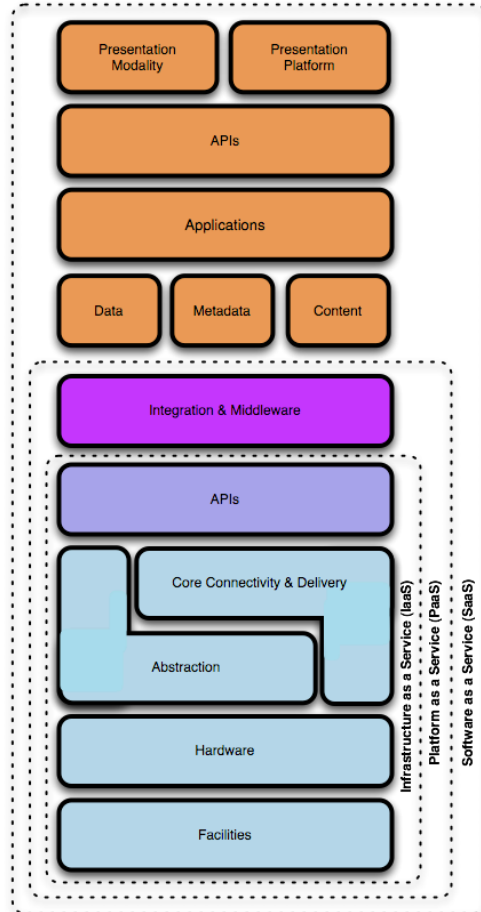
- Lies somewhere in the middle, with extensibility and security features which must be leveraged by the customer

Cloud Model



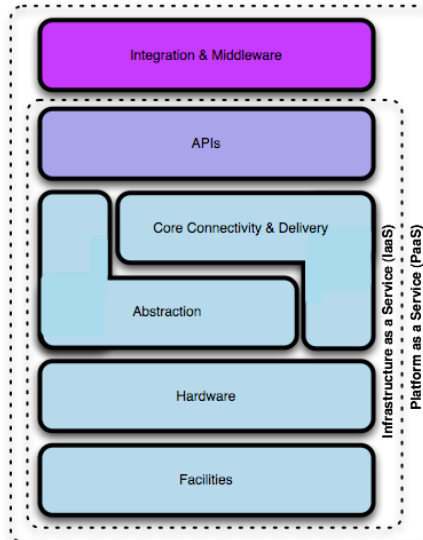
What This Means To Security

Salesforce - SaaS

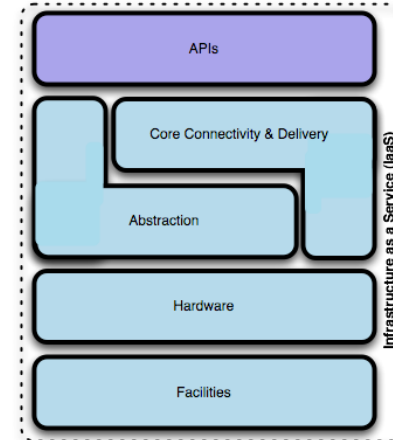


The lower down the stack the Cloud provider stops, the more security **you** are tactically responsible for implementing & managing yourself.

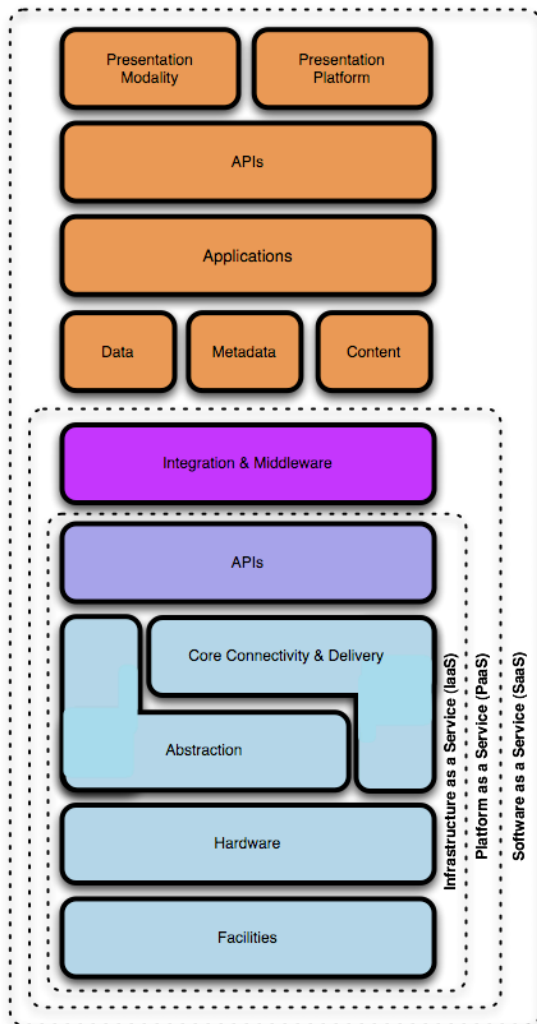
Google AppEngine - PaaS



Amazon EC2 - IaaS



Cloud anatomy



Infostructure

- **Content & Context -**
Applications, Information, Services



Metastructure

- **Glue & Guts -**
IPAM, IAM, BGP, DNS, etc.

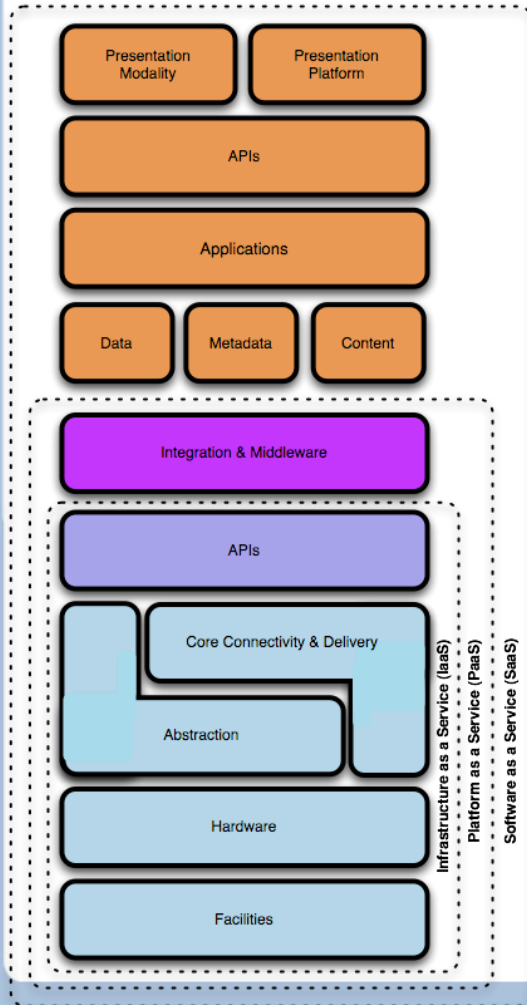


Infrastructure

- **Sprockets & Moving Parts -**
Compute, Network, Storage

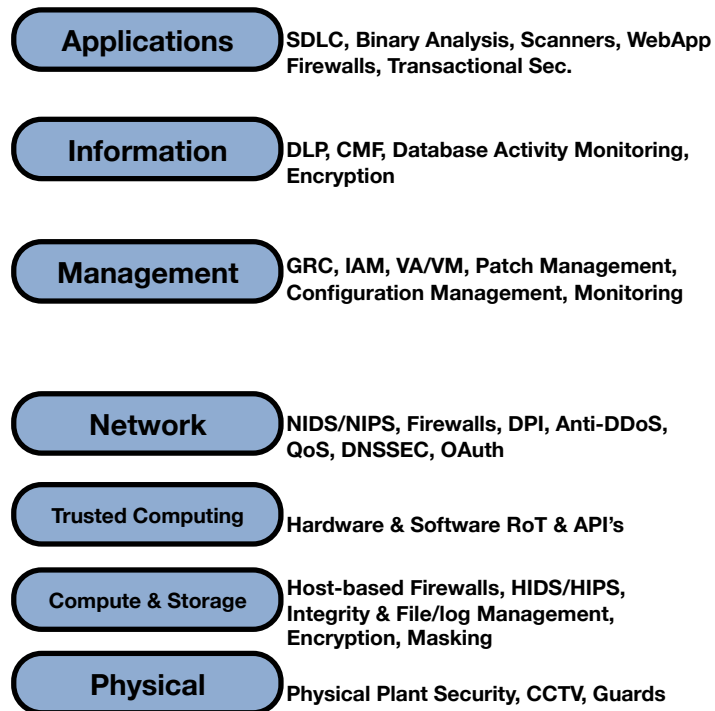
Mapping the Model to the Metal

Cloud Model

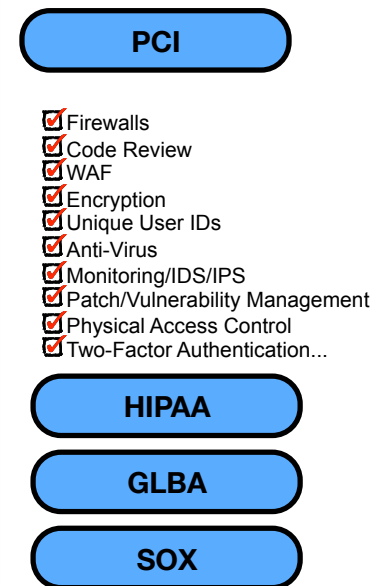


Find the Gaps!

Security Control Model



Compliance Model



Cloud Security Alliance's 15 Domains of Cloud Computing

1. Cloud Computing Architectural Framework
2. Governance and Enterprise Risk Management
3. Legal
4. Electronic Discovery
5. Compliance and Audit
6. Information Lifecycle Management
7. Portability and Interoperability
8. Traditional Security, Business Continuity and Disaster Recovery
9. Data Center Operations
10. Incident Response, Notification, Remediation
11. Application Security
12. Encryption and Key Management
13. Identity and Access Management
14. Storage
15. Virtualization

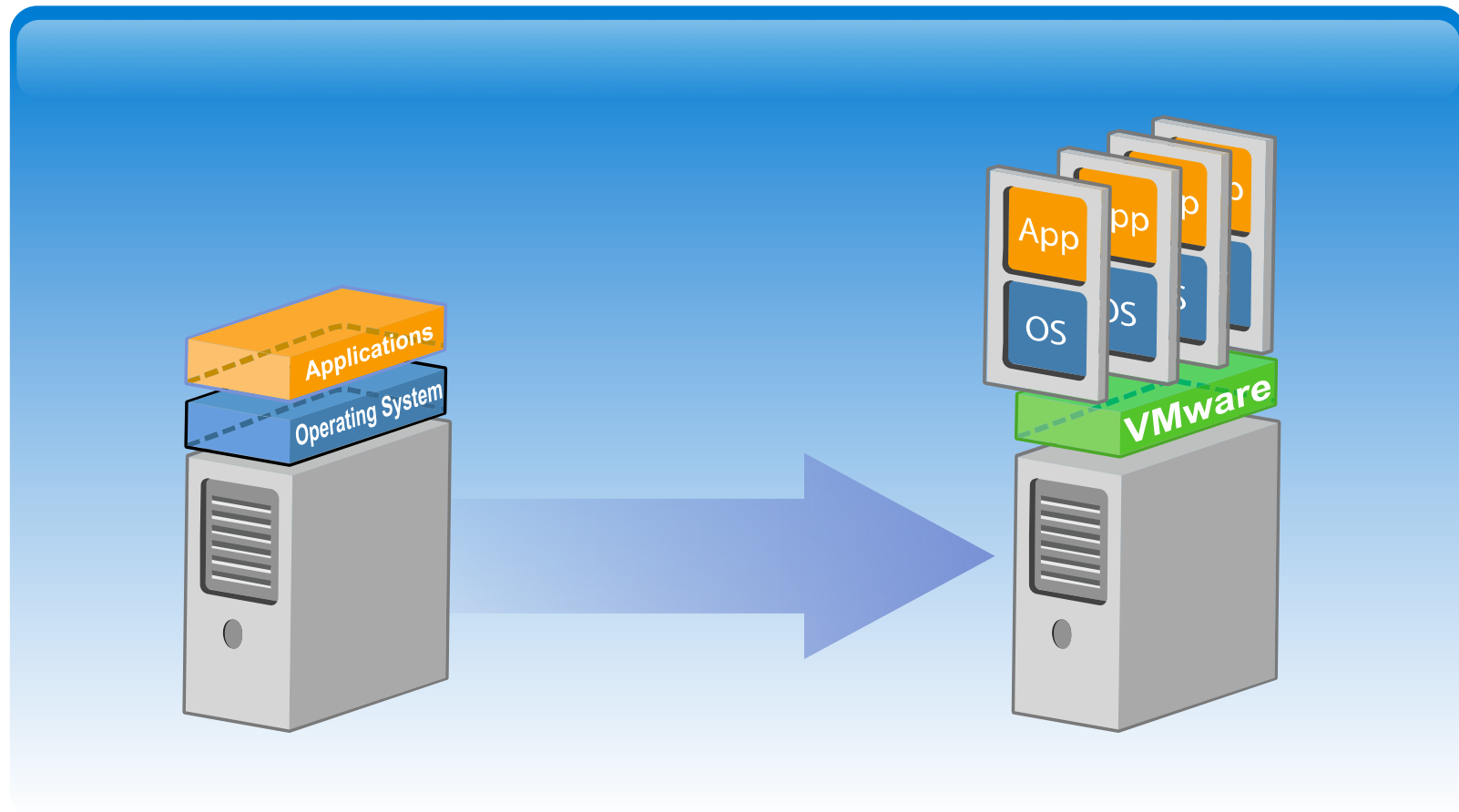
Infrastructure as a Service

Hardware Virtualization is the basis of the IaaS Model

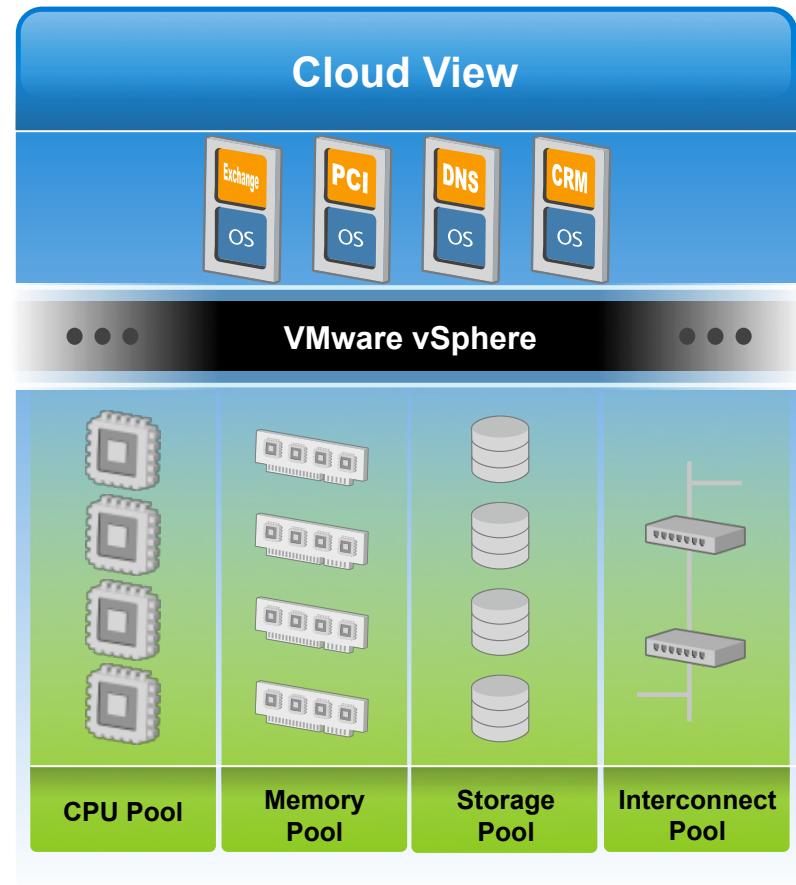
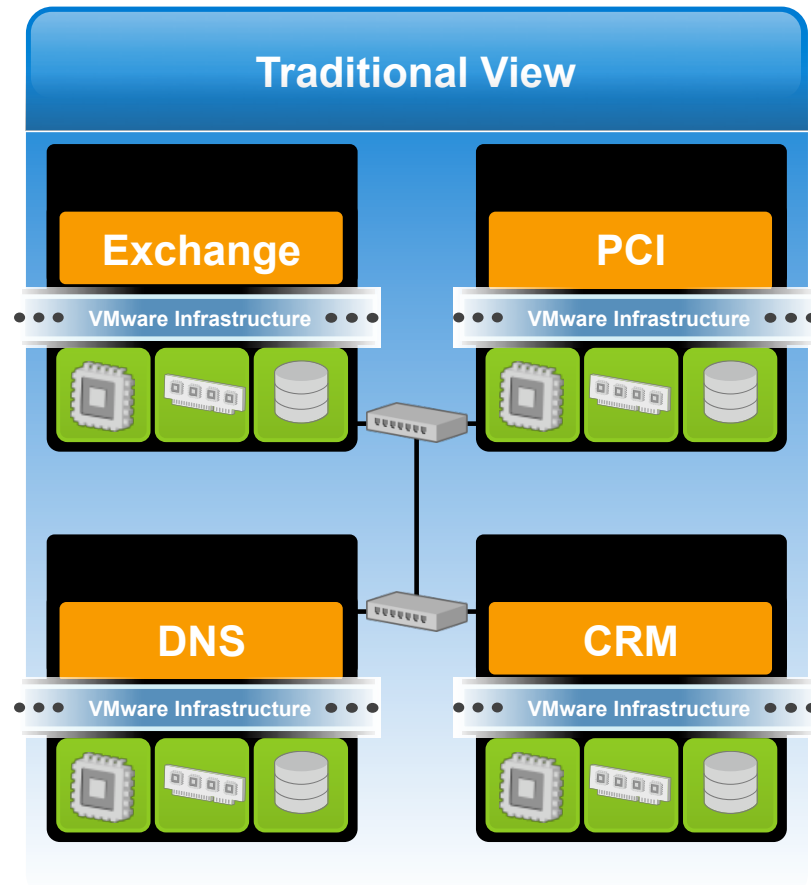
Examples include:

- > VMware vSphere
- > MS HyperV
- > Citrix XenServer

Virtualization Basics



Pools of Shared Resources



The Datacenter Today

Trusted

Control

Reliable

Secure

**Data
Center**

Cloud Computing

Trusted

Control

Reliable

Secure

**Data
Center**

Flexible

Dynamic

On-demand

Efficient

**Cloud
Computing**

Bring the Cloud to the Enterprise...

Trusted

Control

Reliable

Secure

Flexible

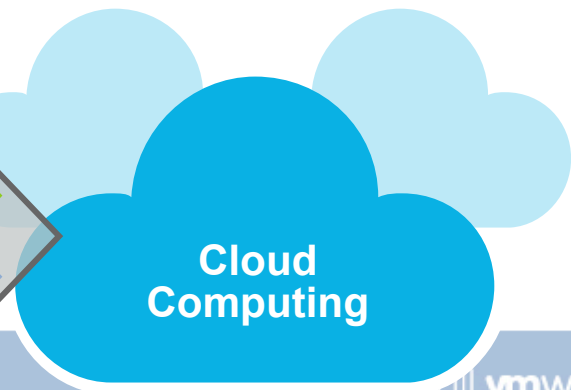
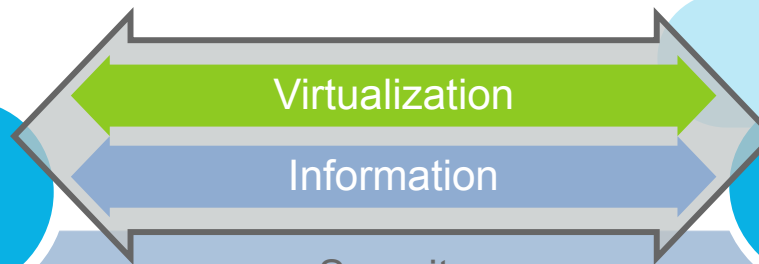
Dynamic

On-demand

Efficient



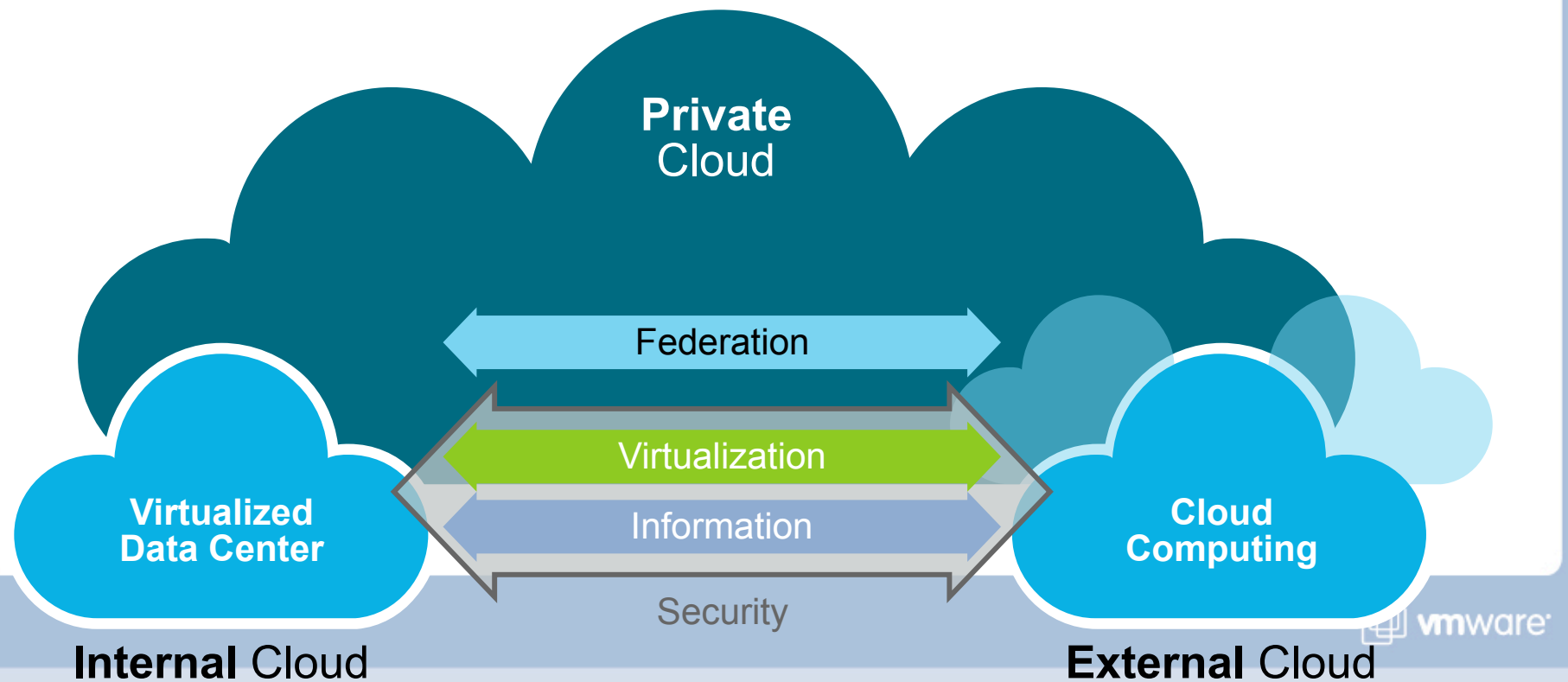
Internal Cloud



External Cloud

 **vmware**

...To Build a Private Cloud



Benefits of the Private Cloud

What are the benefits of a private cloud?

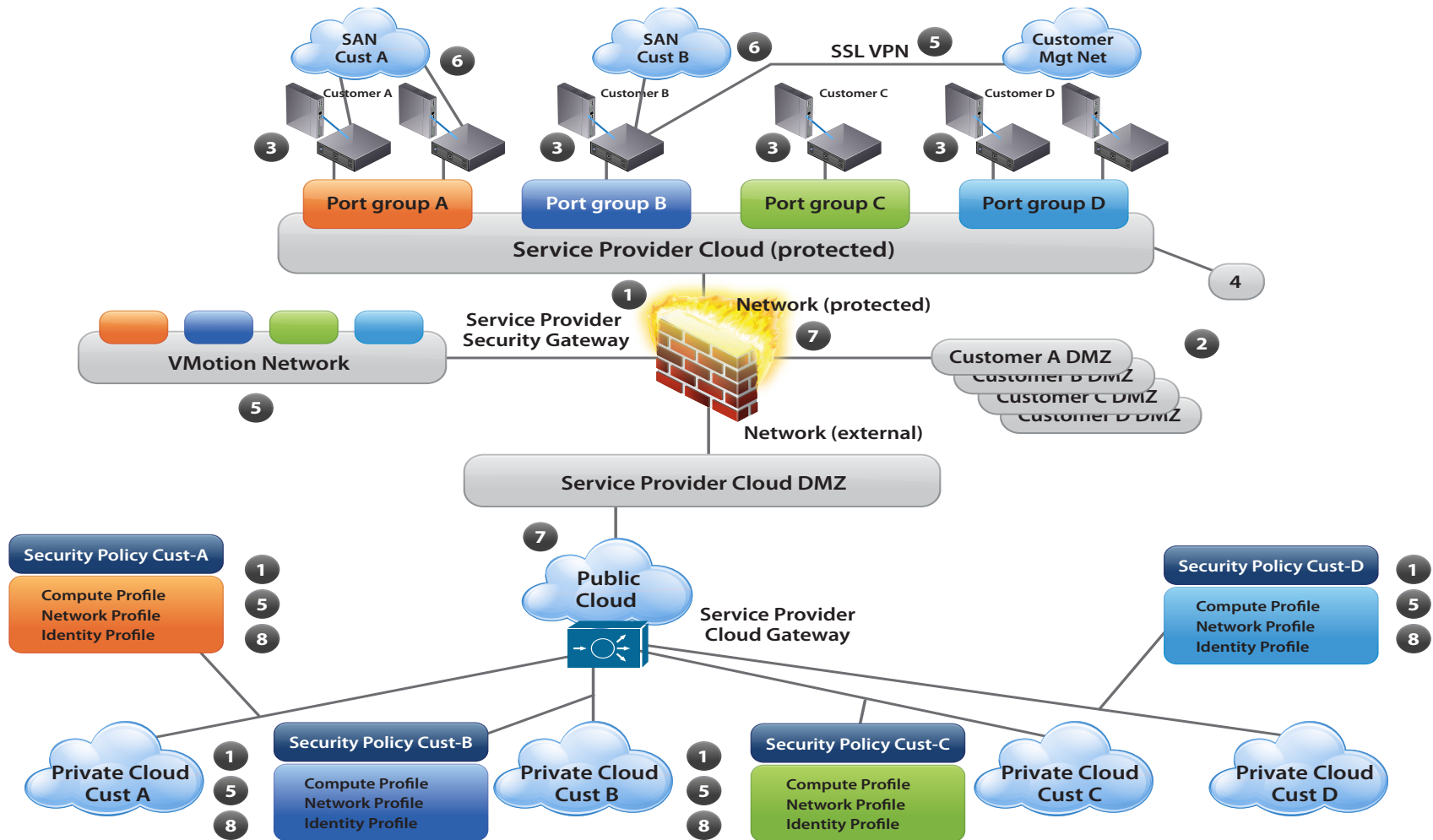
- > Expand scalability**
- > Lower infrastructure**
- > Increase utilization**
- > Improve end-user productivity**
- > Improve reliability**
- > Increase security**
- > Gain access to more sophisticated applications**
- > Downsize the IT department**
- > Save energy**

Limitations of the Private Cloud

Limitations of Existing Cloud Computing Solutions

- > A lack of interoperability**
- > Application Compatibility**
- > Difficulty in meeting compliance regulations**
- > Inadequate security**

Cloud Security Reference Architecture



Cloud Security Reference Architecture

1. **Security profile per compute profile**
2. **Security DMZ per vApp**
3. **OS Management**
4. **Resource Management**
5. **Security profile per network**
6. **Data Security**
7. **Security Authentication, Authorization, and Auditing**
8. **Identity Management**



Questions?

Rob Randell, CISSP

Senior Security and Compliance Specialist

VMware, Inc.