Private & Hybrid Cloud:
Risk, Security and Audit

Job Simon, Scott Lowry, Hassan Javed

VMware, Inc.

November 2011

Private and Hybrid Cloud - Risk, Security and Audit

Objectives:

- ❑ **Explain the technology and benefits behind private and hybrid cloud adoption**
- ❑ **Present a private cloud case study**
- ❑ **Provide a framework for assessing risks and auditing private and hybrid clouds**

Private and Hybrid Cloud - Risk, Security and Audit

Agenda

- Defining the Cloud
- Cloud Computing Models
- Future of Cloud Computing
- Case Study: VMware's Journey to the Private & Hybrid Cloud
- Private & Hybrid Cloud Risk Assessment
  - Governance
  - IT Strategy
  - Roadmap
  - Cloud Service Layer
  - Application Portfolio
- Maturity Assessment

Defining the Cloud

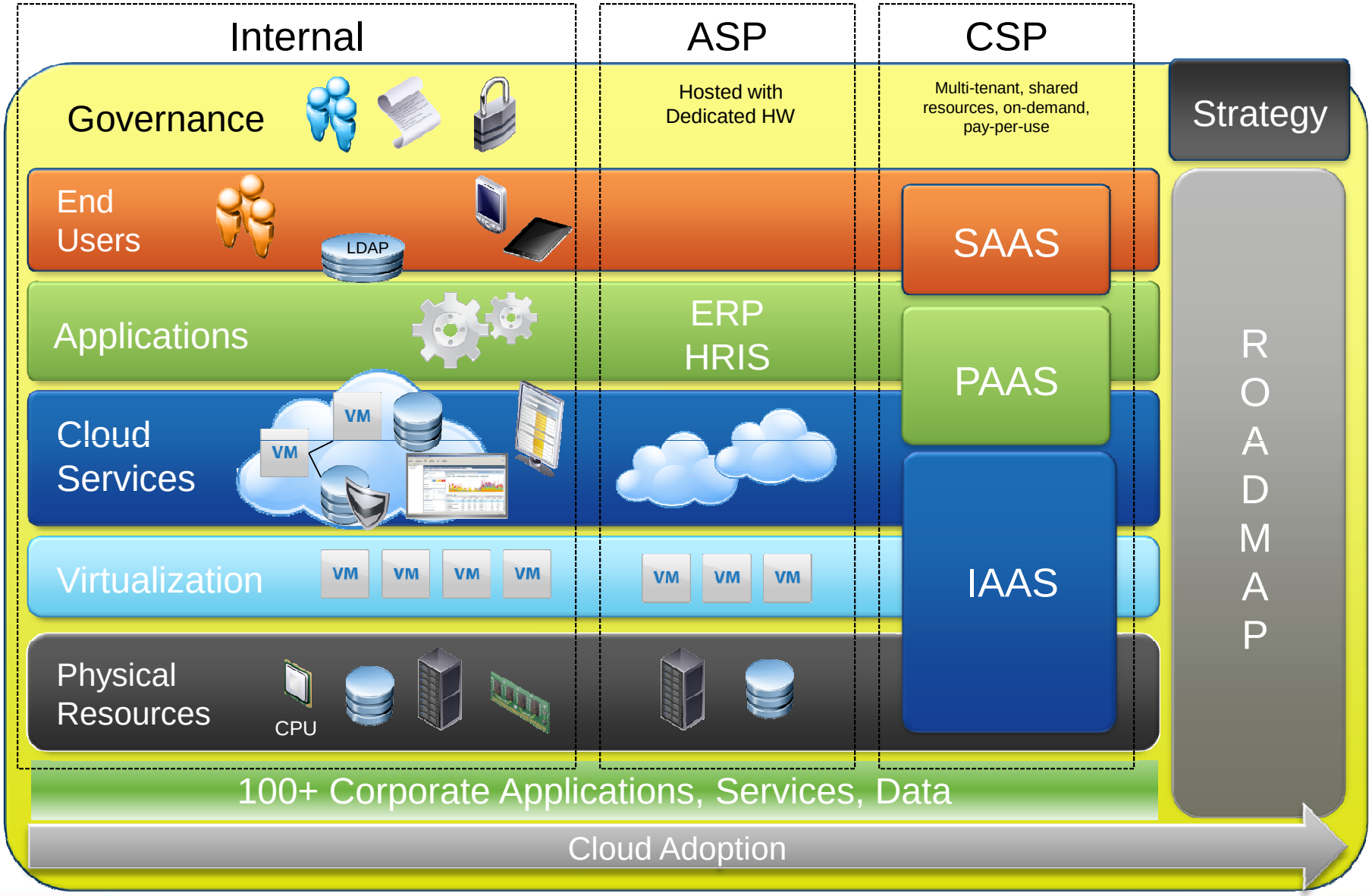
- Cloud computing is Internet based computing, whereby shared resources, software and information, are provided to computers and other devices on demand, like a public utility. – ***Result of VMware vCloud Twitter poll 5/12/2010.***
- Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). – ***Wikipedia (October, 2011)***
- The electrification of computing. – ***Nicholas Carr, The Big Switch (2010)***
- Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being announced regularly. – ***Mather, Kumaraswamy, Latif, Cloud Security and Privacy (2009)***

Defining the Cloud

Five "Essential Characteristics of Cloud Computing" (CSA & NIST both use the same):

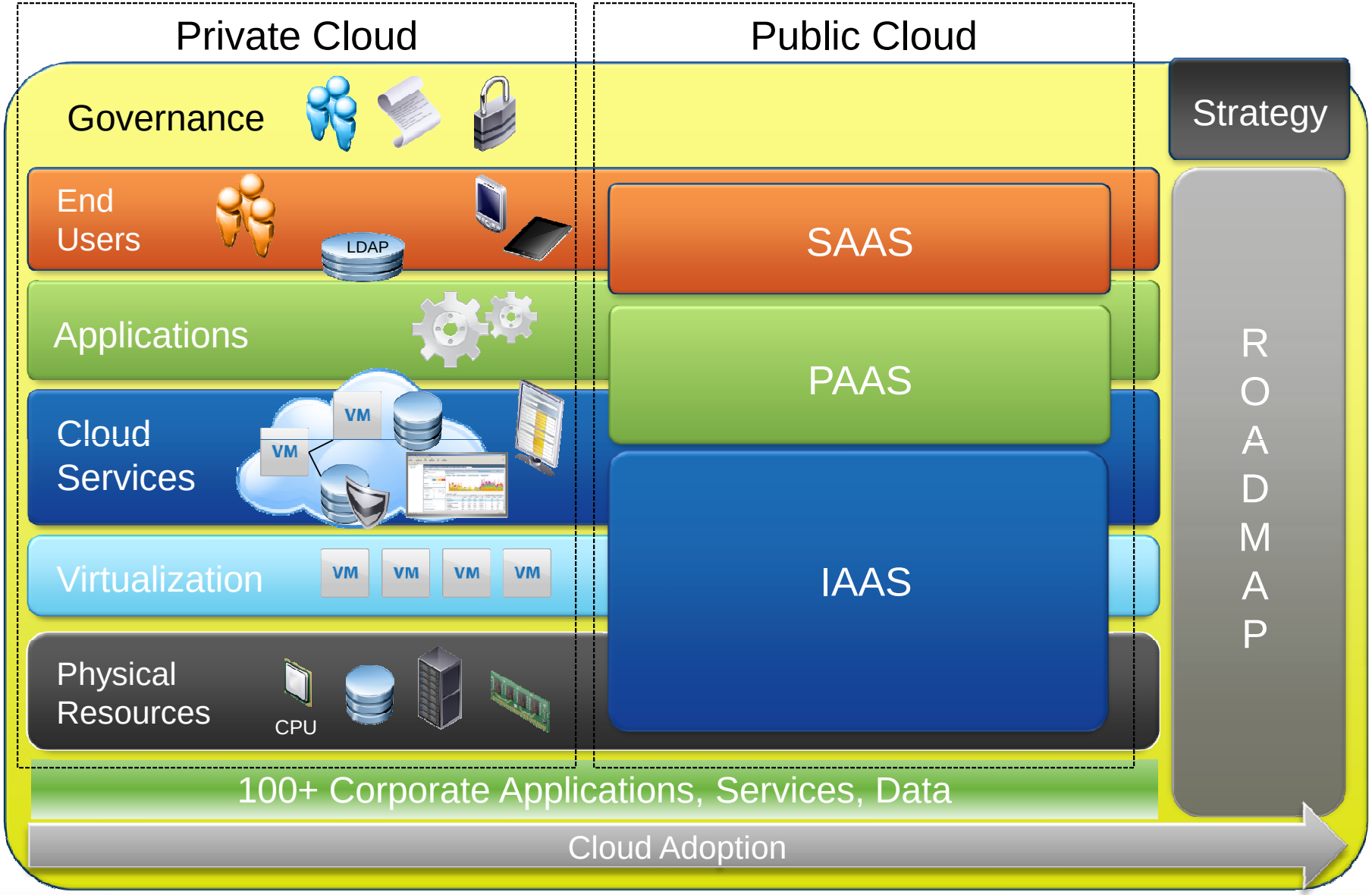
1. ***On-demand self-service –*** *The CSP can automatically provision computing capabilities such as server and network storage as needed, without requiring human interaction with each service's provider*
2. ***Broad network access –*** *The cloud network should be accessible anywhere, by almost any device (smart phone, tablet, etc.)*
3. ***Resource pooling –*** *The CSP's computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand.*
4. ***Rapid elasticity –*** *Capabilities can be rapidly and elastically provisioned – in many cases, automatically – to accommodate customer needs. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.*
5. ***Measured Service –*** *Systems automatically control and optimize resource usage by leveraging a metering capability. Resource usage can be monitored, controlled and reported.*

Cloud Computing Model – History



vmware

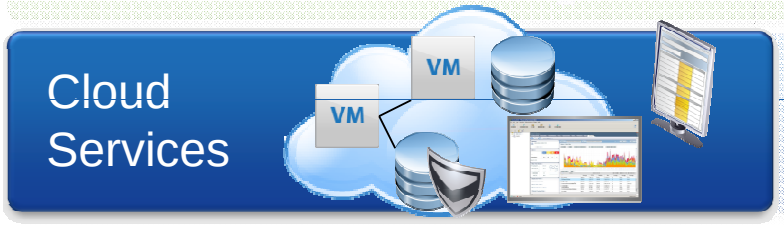
Cloud Computing Model – Simplified



vmware

Cloud Computing Model – Cloud Services

Cloud services enable the characteristics that are associated with cloud computing. These services control the deployment of virtual machines and virtual applications (vApps) and provide for the following cloud characteristics:

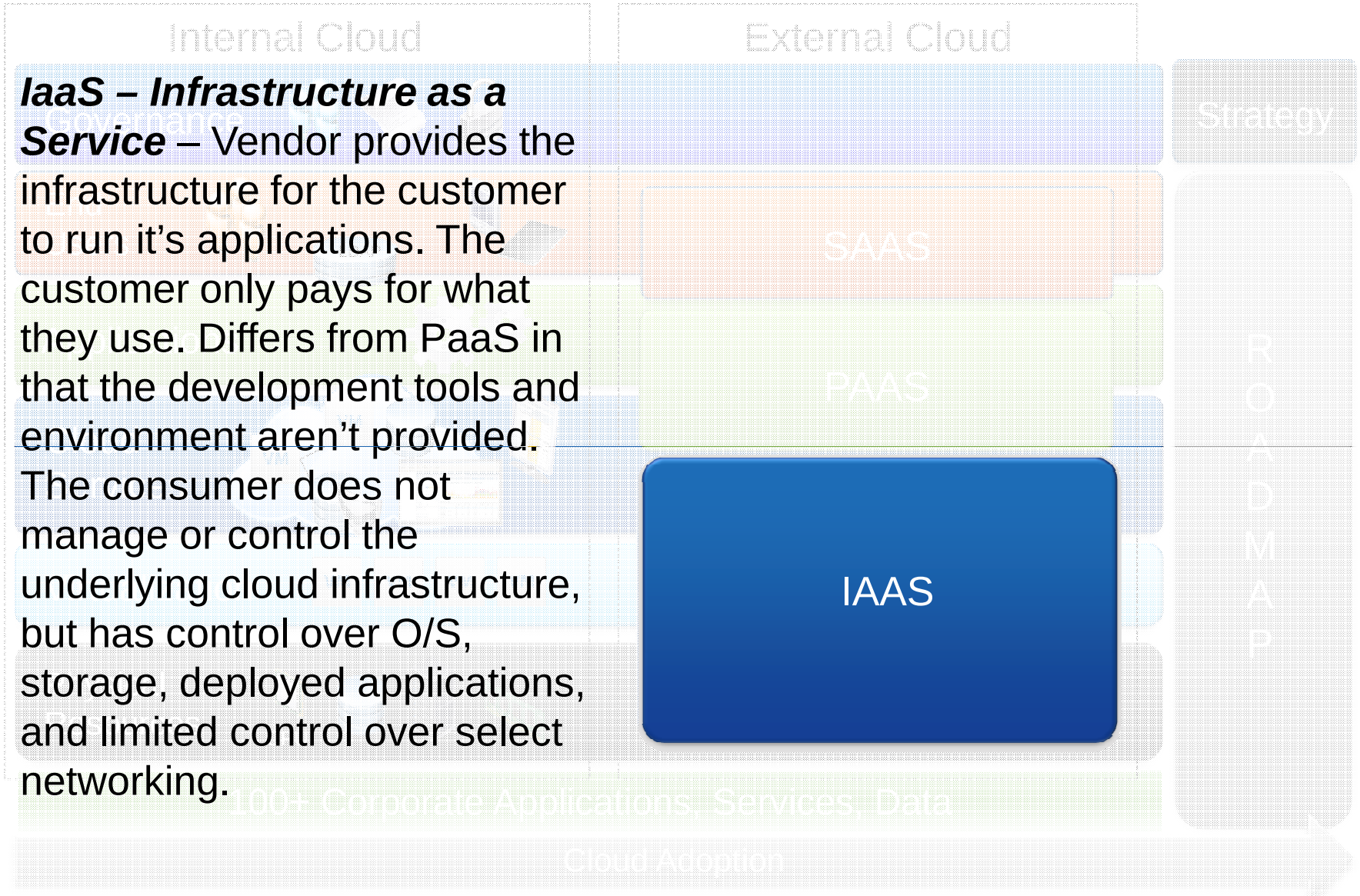


- Simplification
- Rapid Application Deployment
- Extreme Scalability
- Self-provisioning
- Ease of management
- Independence from physical location
- High Availability and DR
- On-demand elastic networking
- Pay-per-use
- Security

Examples of VMware Cloud Services products include:
vCenter Server; vCloud Director; vMotion; vShield; Site Recovery Manager; vCloud Operations; vCloud Orchestrator; vCenter Chargeback

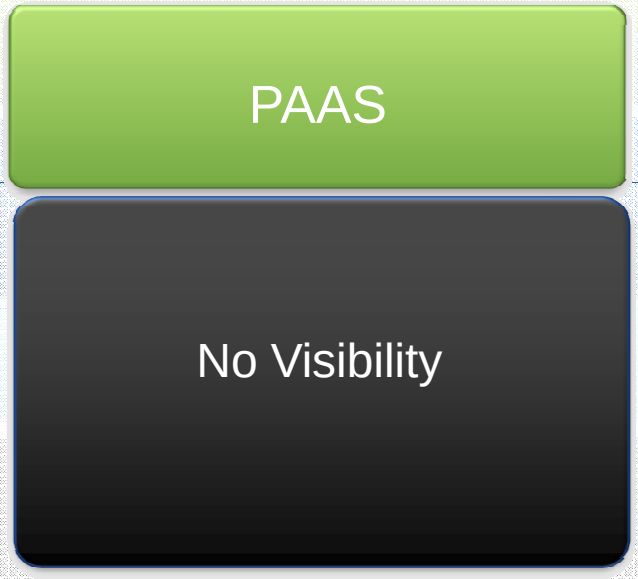
Cloud Computing Model – *SPI Service Model*

IaaS – Infrastructure as a Service – Vendor provides the infrastructure for the customer to run it's applications. The customer only pays for what they use. Differs from PaaS in that the development tools and environment aren't provided. The consumer does not manage or control the underlying cloud infrastructure, but has control over O/S, storage, deployed applications, and limited control over select networking.



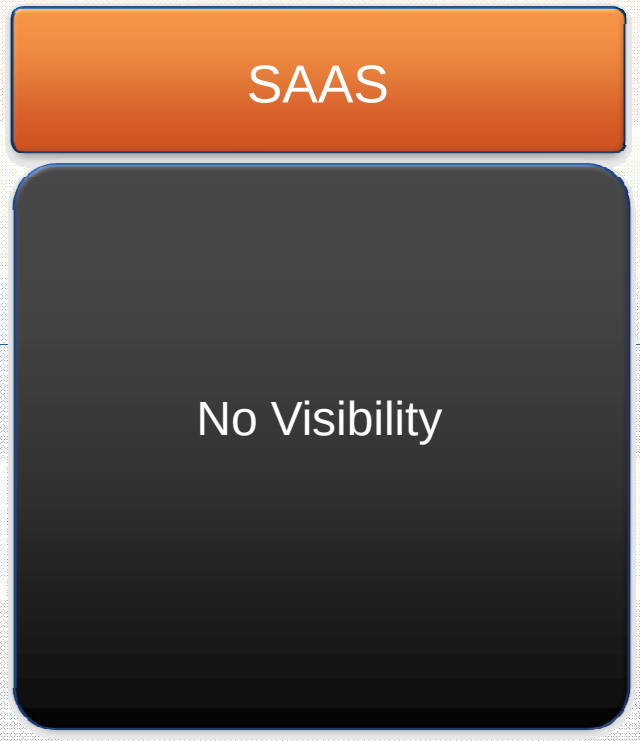
Cloud Computing Model – *SPI Service Model*

PaaS – Platform as a Service – Vendor offers a development environment for the customer. Customer builds and deploys applications using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (network, servers, O/S, databases), but has control over the applications and sometimes the application hosting environment configurations.



Cloud Computing Model – *SPI Service Model*

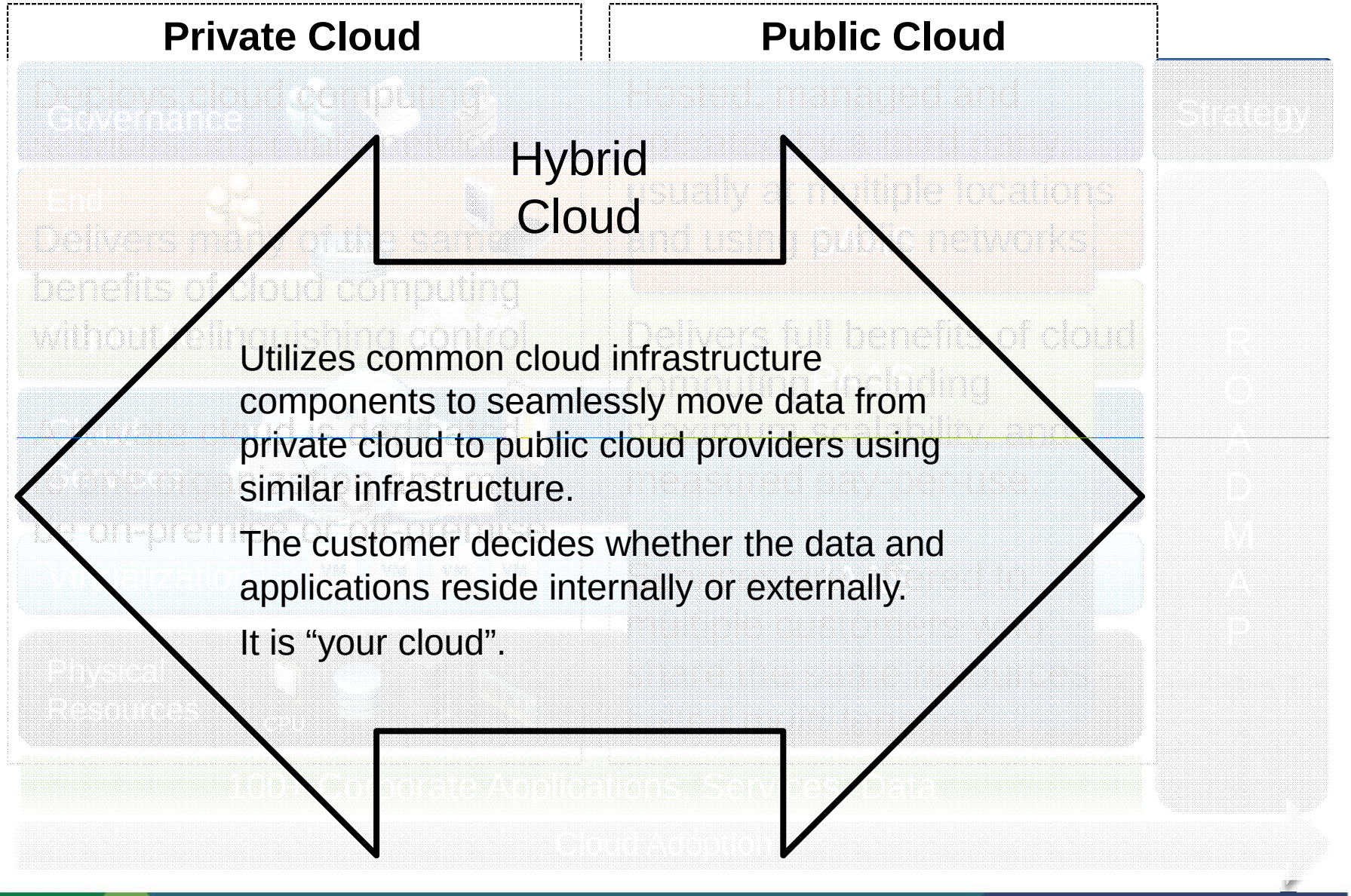
SaaS – Software as a Service – A provider licenses an application to the customer as a service. This differs from the "non-cloud" ASP, where the customer had a dedicated application infrastructure. SAAS is usually deployed in a multi-tenancy environment. The consumer does not manage or control the underlying cloud infrastructure (network, servers, O/S, databases, or application capabilities).



Cloud Computing Model

Private Cloud	Public Cloud
Deploys cloud computing services on private networks.	Hosted, managed and operated by a third party, usually at multiple locations and using public networks.
Delivers many of the same benefits of cloud computing without relinquishing control.	Delivers full benefits of cloud computing, including maximum scalability, and measured pay-per-use.
A private cloud is dedicated to one organization and may be on-premise or off-premise.	Services are offered to multiple customers who share the same resources – called *multi-tenancy*.

Cloud Computing Model



Future of Cloud Computing

Results of 2011 IDG Research Survey:

- *88 % rate cloud computing as a priority at their organization over the next 18 months.*
- *88 % say they would use cloud more if they could achieve the same or better security as their internal data center.*
- *75 % say business agility is the top driver for cloud.*

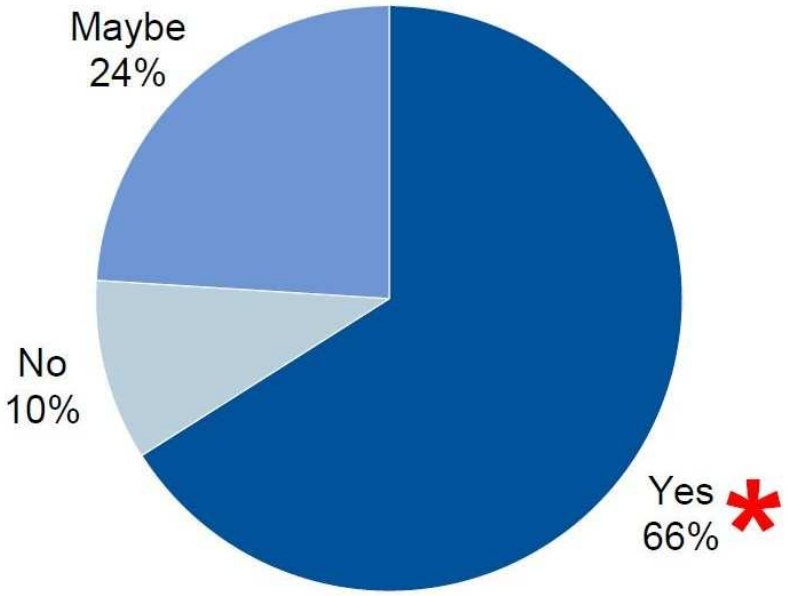
"Respondents reported that their heads were in the cloud: 60 percent use or are planning to use cloud computing for non-mission-critical IT services, and ***more than 40 percent use or are planning to use it for mission-critical IT services.*** *For companies that do not have plans to use cloud computing the main reasons are data privacy and security concerns."*
– IT Governance Institute poll of 834 executives (2011)

"With the Cloud First Policy, we've already seen agencies such as GSA, we've seen the Recovery Board and USDA adopt a Cloud First policy. [Take] something as simple as e-mail; we're able to cut the cost down to $42 million by moving it to the Cloud. And imagine the opportunity as we look at applications across the board. We projected that ***we could move, in the next couple of years, about $20 billion worth of IT projects to Cloud, saving the federal government $5 billion, very, very quickly."***
– Vivek Kundra, CIO US. Government (8/30/11)

Future of Cloud Computing

Private Cloud Intentions

Message: The market may not understand "private cloud", but they are on the bandwagon.



Gartner Data Center Conference Poll, December 2010:

Will your enterprise be pursuing a private cloud computing strategy by 2014? (n=655)

Gartner

VMware on VMware:
Private Cloud Case Study

Agenda

- VMware IT landscape
- Motivations for the Cloud
- Private Cloud Stack

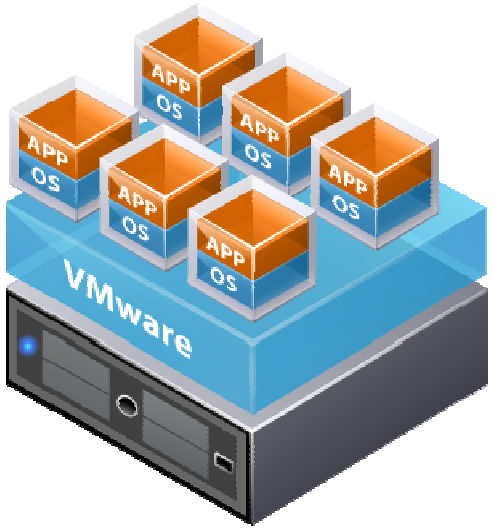
Server Virtualization at VMware

Objectives

- Cost savings, improved uptime and business agility

Results

- VMware's corporate IT servers are 98% virtualized
- 6300 VMs on 289 physical hosts (22:1 Consolidation)
- 4000 Server and 2300 View VM's
- Server VM's 2/3 Linux and 1/3 Windows
- 3,100 SF of datacenter space
- 3 Petabytes of storage
- No downtime for hardware maintenance, and virtual environments can be provisioned within minutes to support critical projects
- Managed by 9 Cloud Administrators



Business Impact

- Estimated saving of 50%+ over non-virtualized environment

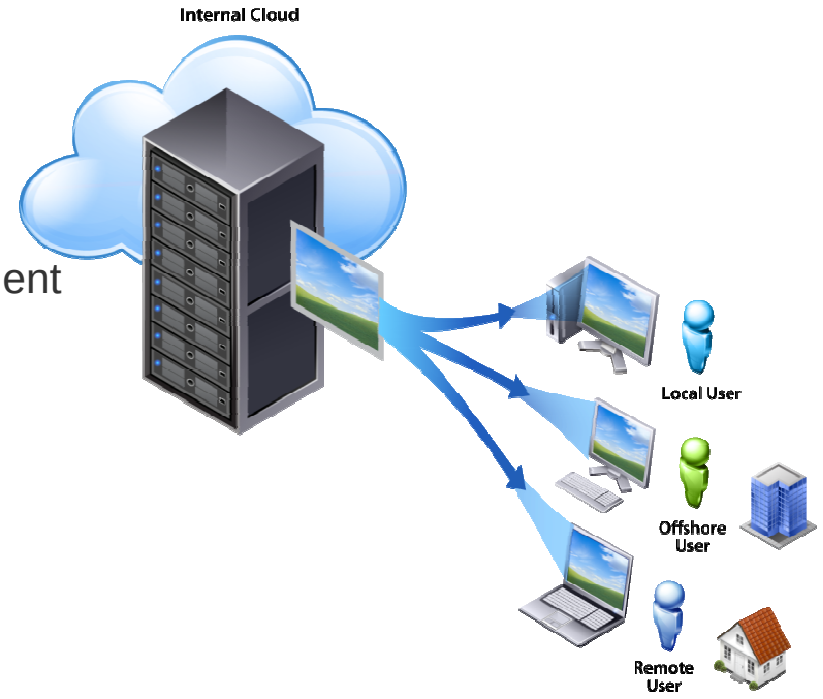
Desktop Virtualization at VMware

Objectives

- Reduce overall cost of desktop support, improve customer service and improve security profile

Results

- Approximately 3000 staff using virtual desktop client today
- One full-time and three shared staff manage current environment
- Environment is scalable to 4000 users without adding incremental staff
- Speed troubleshooting capability and minimize impact on staff productivity
- Faster provisioning and extended h/w lifespan (server vs. desktop)



Business Impact

- 50% reduction in hardware costs ($1500 thick client vs. $650 thin client)
- 30% reduction in Help Desk support costs (centralized change management and control of desktop images)

Agenda

- VMware IT landscape
- Motivations for the Cloud
- vCloud Stack and Application Profile
- Impact of moving to the Cloud

End to End Business Application Provisioning Is A Complex Process

vmware

Business Application Provisioning Is More Than VM Provisioning

End to End Business Application provisioning is 3X longer than VM provisioning

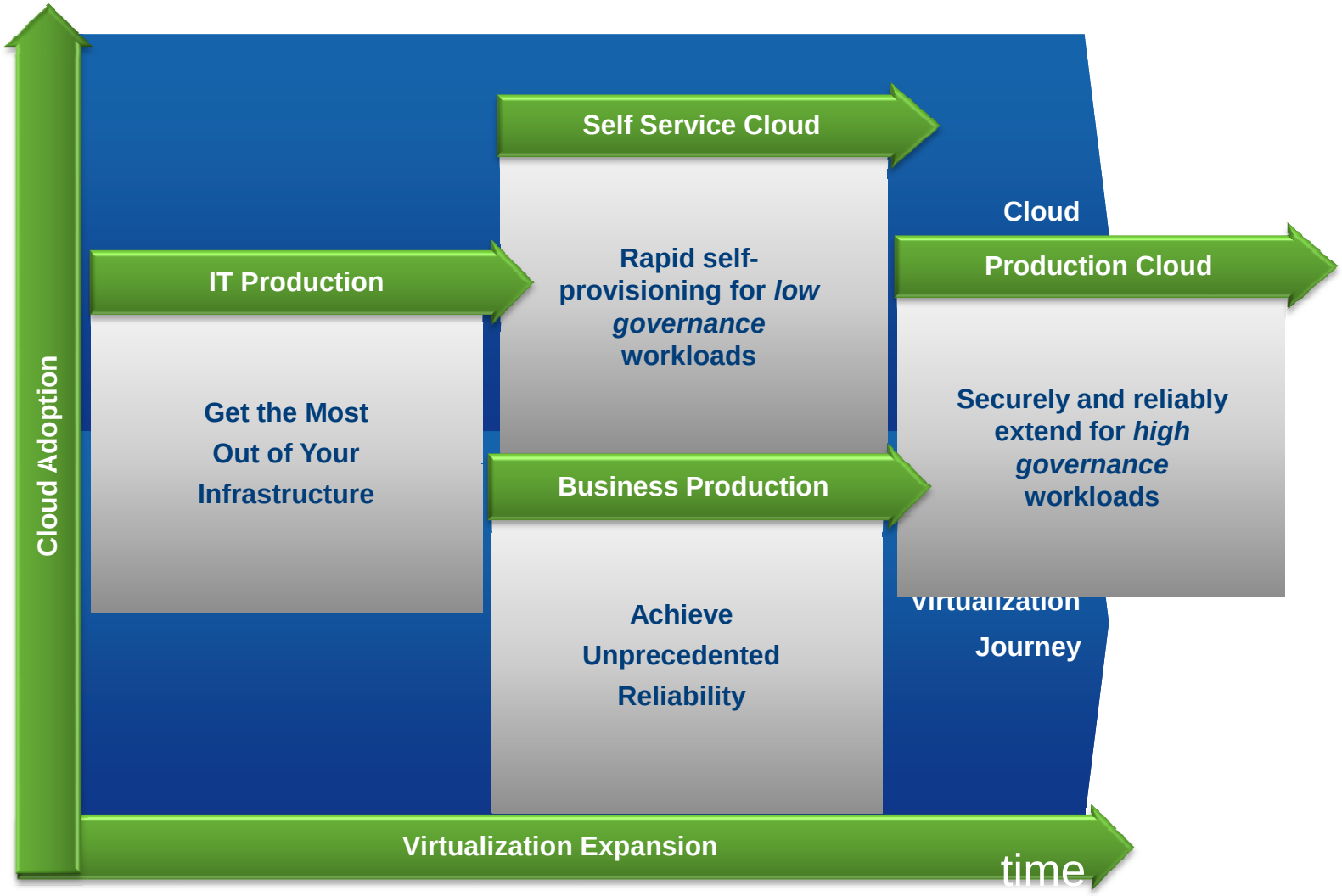
Hybrid Cloud Is The Solution

VMware is transforming it's Enterprise IT to increase end to end business application agility by reducing provisioning time and cost of operations while improving security and control

CIO Goals For Hybrid Cloud

	Previously - Highly virtualized datacenter	Now - Hybrid cloud
End to end business application provisioning and scaling time	• 3 days to 8 weeks • Manual and complex	• **- 90% time reduction** • **Highly repeatable and predictable**
Cost of VMware IT (infrastructure and operations)	• 50% less than physical	• **20% less than virtualized**
Security and compliance	• Rigid, manual – physical security products	• **Flexible, agile purpose built for cloud**
Business Application SLA	• Reactive multi-vendor non integrated solution	• **Proactive integrated vCenter Operations solution monitoring application down to infrastructure**
Networking	• Rigid, manual – physical networking products	• **On-demand elastic networking built for the cloud**

Hybrid Cloud Journey



vmware

Two Paradigms for Cloud Emerge

	Self-Service cloud for Pre-Prod (Low Governance" Cloud)	Production Cloud ("High Governance" Cloud)
	The Amazon EC2 home turf	**Early enterprise customer cloud RFIs**
Users	• App developers (otherwise bypassing IT infrastructure managers) • Engineers and scientists procuring their own infrastructure • Business owners procuring technology directly • Training professional	• IT infrastructure and operations staff
User characteristics	• Limited budgets, short time frames • Willingness to go to public clouds to get the flexible resources and quick setup their internal IT organization can't or won't give them	• Within the enterprise IT organization • Looking to lower their costs for robust offerings that can handle their traditional enterprise workloads
Types of Workloads	• Development, training, demonstration • Production use for internal (rather than customer) facing workloads (collaboration; portals; file servers; business intelligence; HPC) • Web workloads	• Tier 1, 2 business apps • Tier 1-2 IT applications
Main Cloud Value Prop	• "Give me a VM … fast!" • Fast, self-service provisioning of new VMs	• Provisioning doesn't happen often; but change happens fast and often • Ability to continuously meet SLAs with little human intervention
Required Technology Capabilities		
Self-service	• Self-service access without pre- deployment controls; no approvals	• Self-service access with structured and customizable approval processes
Integration	• IP Address management	• CMDB • Compliance logging and reporting
Service Catalog	• Catalog content - Image templates	• Highly customizable service catalog

VMware IT successfully implemented Low Governance Clouds in 2010

Self Service Cloud

Rapid self-provisioning for *low governance* workloads

VMworld Labs and vSEL (Virtual Sales Enablement Cloud)

VMware R&D (vCloud Director Engineering)

VMware IT is taking a phased approach to High Governance cloud

Phase 1

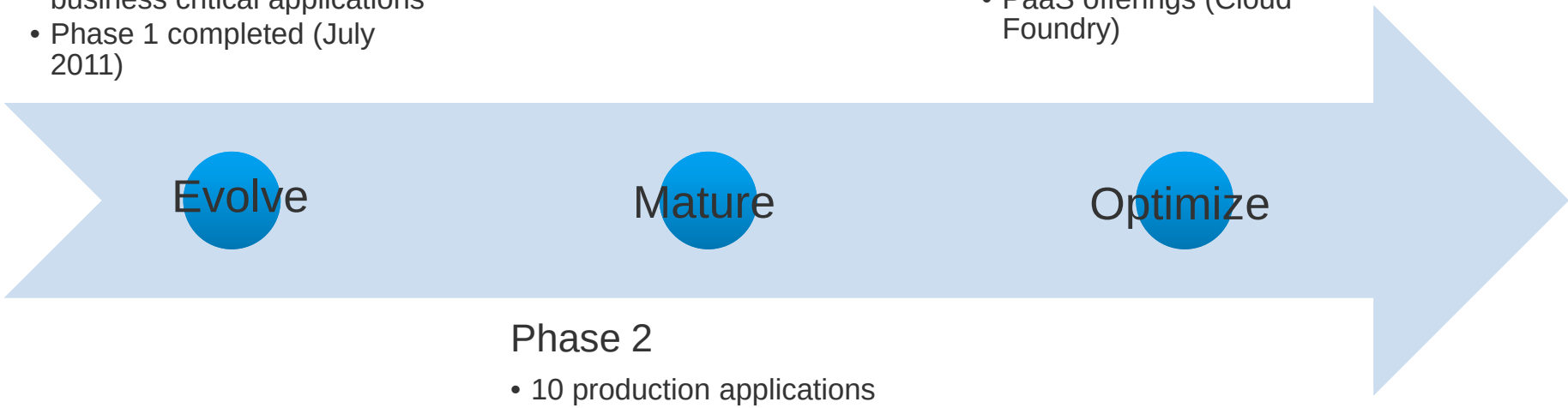
- 2 production applications running in a high governance cloud
- Batch mode integration for business critical applications
- Phase 1 completed (July 2011)

Phase 2

- 10 production applications
- Real time integrations for business critical applications
- SaaS secured by Horizon
- In progress

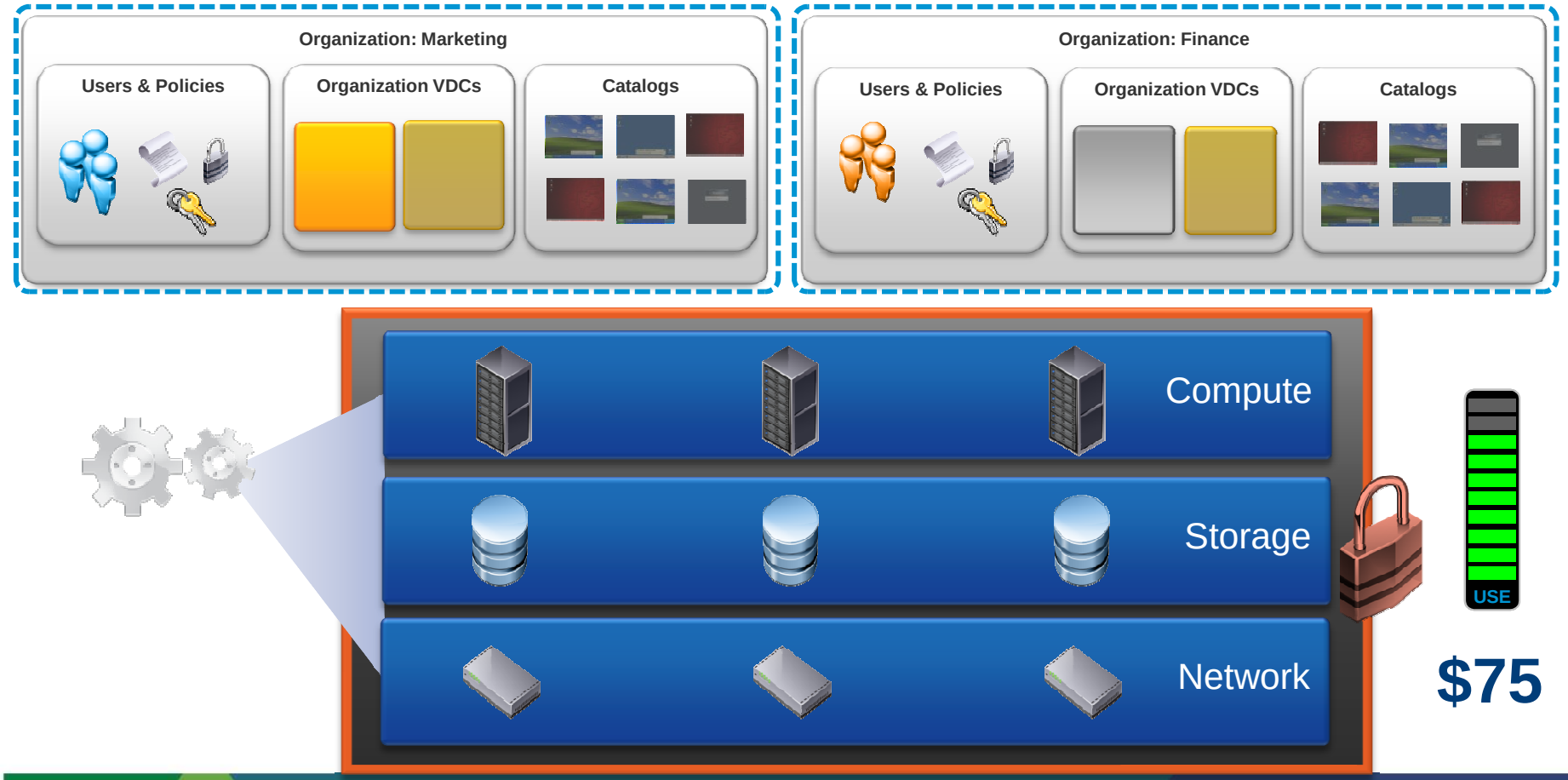
Phase 3

- Move to a hybrid cloud
  - Cloud SP for burst capacity
- Real time mission critical and complex applications
- CMDB, IPAM integrations
- PaaS offerings (Cloud Foundry)

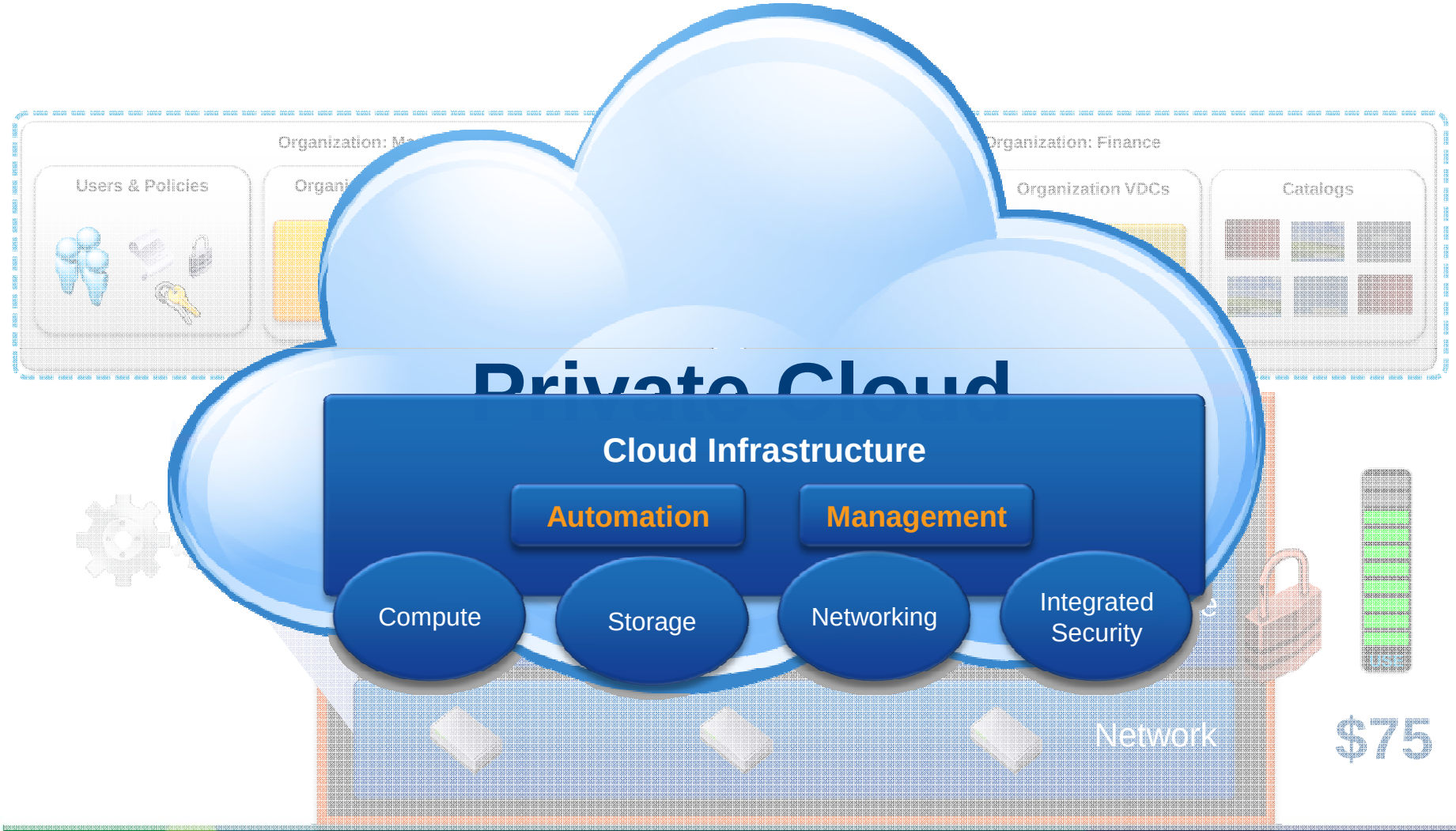


Phase 1 – Evolve The Virtualized Datacenter To Private Cloud

- ✓ *Leverage virtualization to transform physical silos into elastic, virtual capacity*
- ✓ *Increase automation thru built-in policy-driven management*
- ✓ *Move from static, physical security to dynamic, embedded security*
- ✓ *Enable secure, self-service to pre-defined IT services, with pay-for-use*

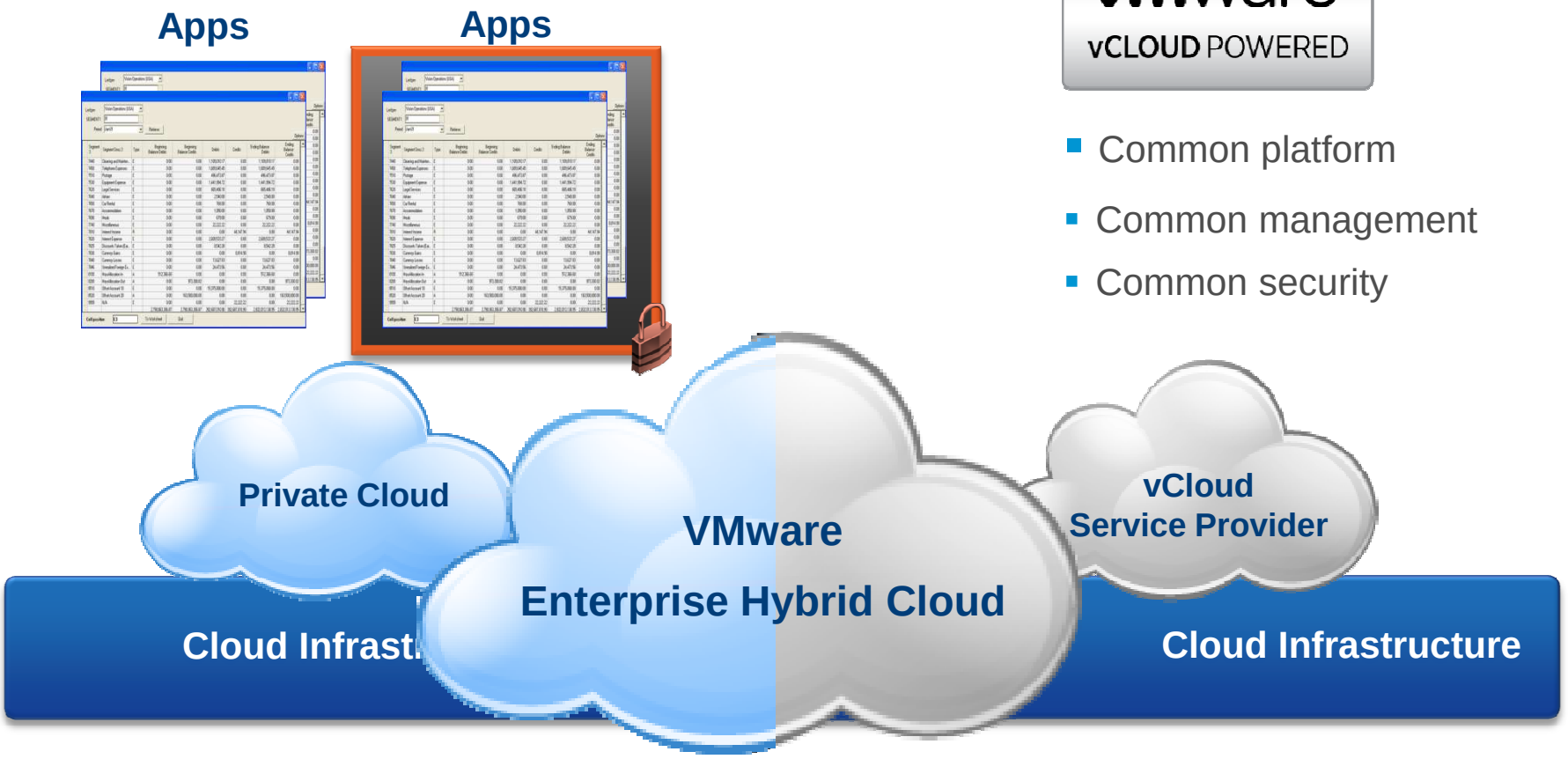


Phase 2 – Mature The Private Cloud



vmware

Phase 3 – Optimize and evolve to the Hybrid Cloud



vmware
vCLOUD POWERED

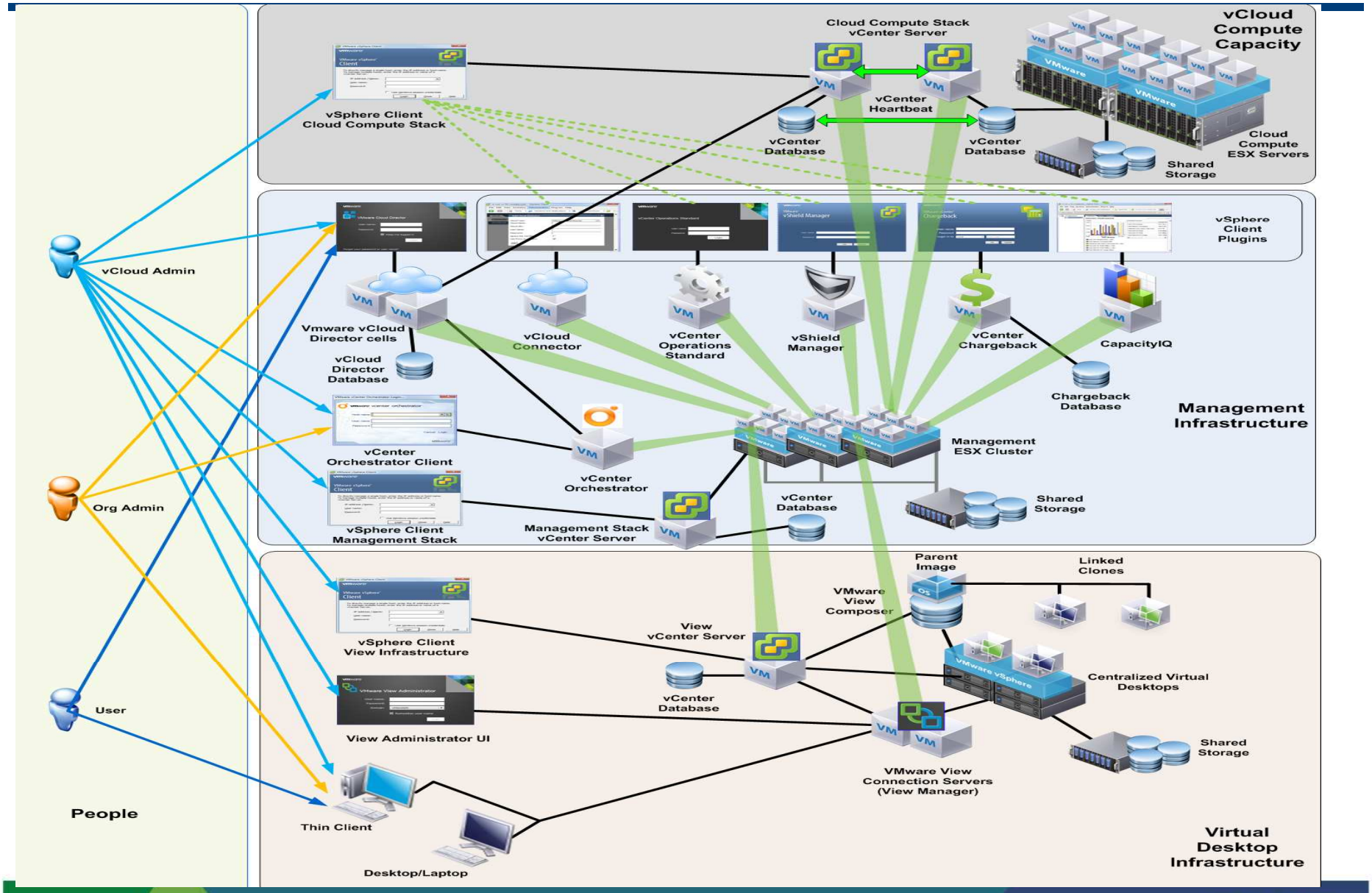
- Common platform
- Common management
- Common security

Cloud Computing Moves from a Technology Discussion to a Business Decision

Agenda

- The VMware IT landscape
- Motivations to move to a Cloud
- vCloud Stack and Application Profile
- Impact of moving to the Cloud

vCloud Components



Application Profile: SR Viewer/ Eforms

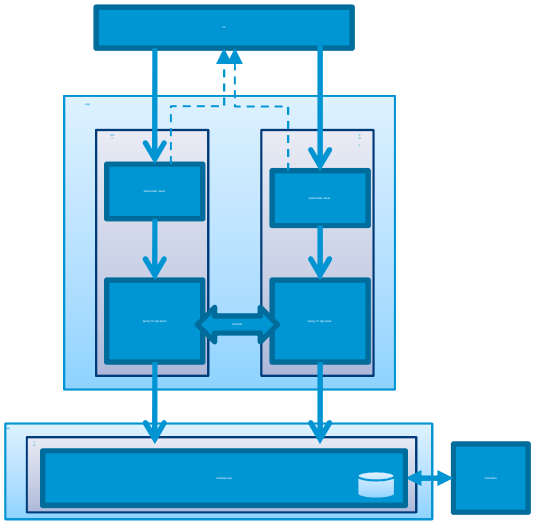
Business Critical app serving the Global Support organization with two major functionalities.

- SR Viewer: to provide deep visibility to the customer support requests like activity information (case history), attachments etc. in chronological view.
- eForms: It is an off-line tool that enables VMware to handle the SR creation and management for the CSR and TSE during Salesforce.com planned and unplanned outages.

- **Applications Stack:**
- Application Server: Spring TC Server 2.0.0.RELEASE

Database: MySQL Database Server 5.1.51
Web Layer: Apache 1.2
OS: Linux
Monitoring: Spring Hyperic 4.5

- **Applications Stats:**
- 200 concurrent users with almost 3000 internal users usage, with approx 5000 transactions/hr.

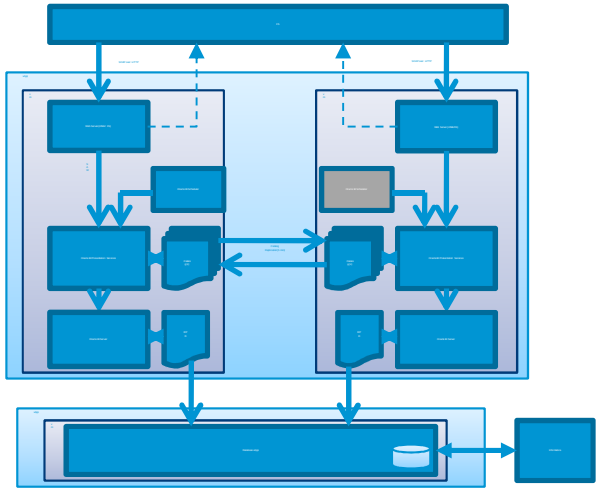


Application Profile: Business Intelligence (Marketing)

Business Critical BI App with a Data Mart serving the reporting and analytical needs for Marketing providing insight into Leads, Territories etc. across the Geos.

- **Applications Stack:**
- Application Server: Oracle Business Intelligent Enterprise Edition 10.1.3.3.1 (OBIEE)
- Database: Oracle Database Enterprise Edition 10.2.0.4
- Web Layer: IIS
- OS: Windows 2003 SP2

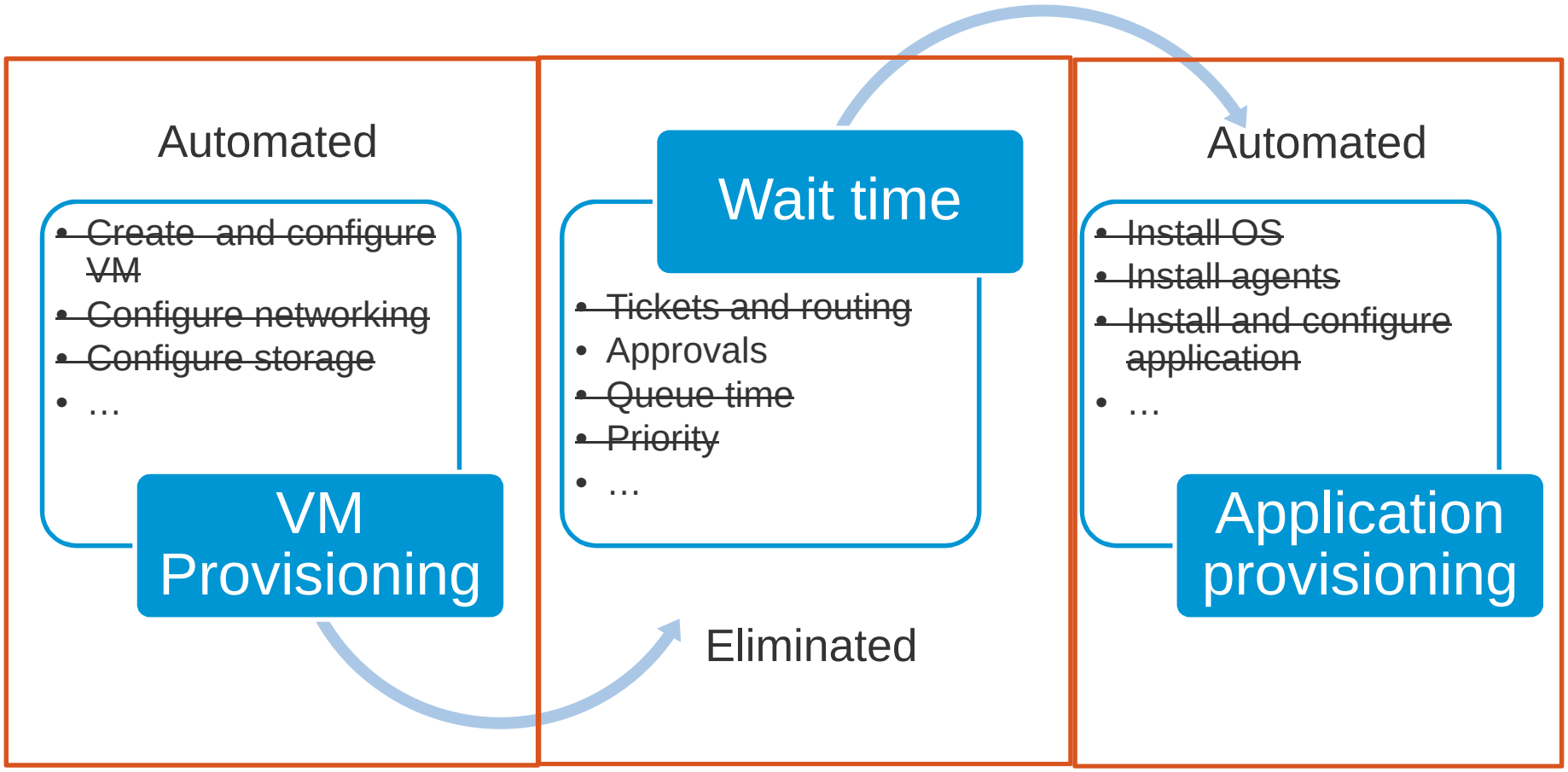
- **Applications Stats:**
- 60 concurrent users and 500 internal users, with approx 1500 transactions/day.



Agenda

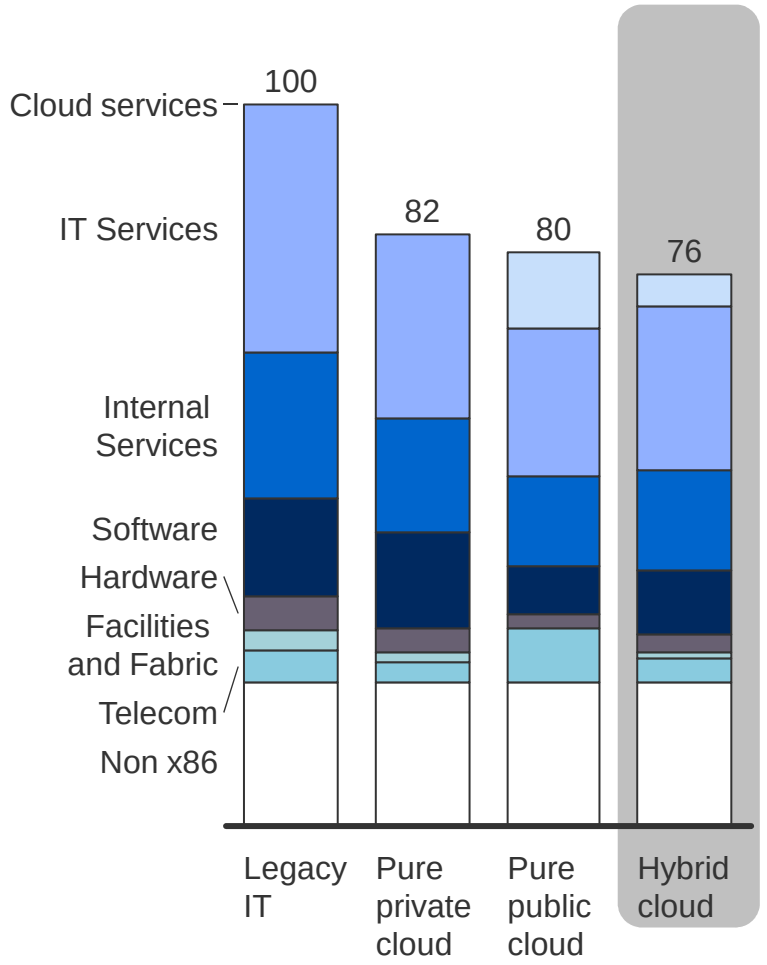
- The VMware IT landscape
- Motivations to move to a Cloud
- Cloud Stack and Application Profile
- Cloud Impact

vCloud Positively Impact Business Application Provisioning



Hybrid cloud is the most elastic and cost effective model

Annual total IT spend
(100=Total IT spend with all on-premise infrastructure)

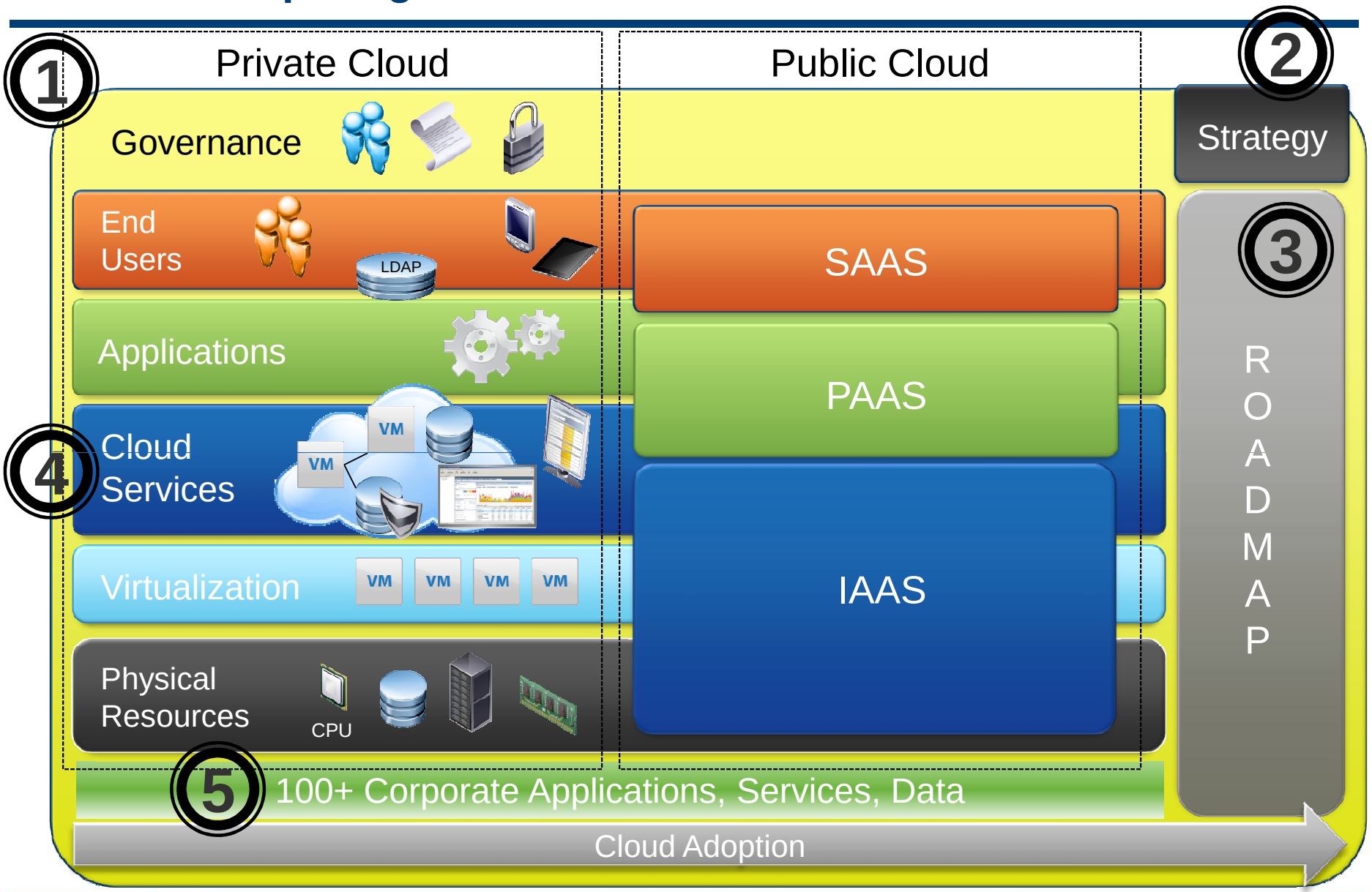


- **Hybrid cloud offers lower IT spend through:**
  - Virtualization and consolidation
  - Optimized workload sourcing
  - Optimized provisioning
  - Higher productivity in application development and maintenance
- **This requires standardization of frameworks & infrastructure across public and private cloud:**
  - Common platform
  - Common management
  - Common security

SOURCE: Gartner, IDC market data; Gartner IT Key Metrics Data 2009; EMC and VMware team analysis
SaaS, Private cloud and IaaS savings modeled only for x86 workloads (assumed 80% of spend)

Framework for Private & Hybrid Cloud Risk Management

Cloud Computing Model



vmware

1 Governance

Risks

- ❑ Failure to deliver value from cloud technology
- ❑ Non-compliance with laws and regulations
- ❑ Loss of data, intellectual property
- ❑ Contractual non-compliance
- ❑ Reputational damage associated with data loss, non-compliance
- ❑ Abdicating security and risk decisions to third parties, losing control and increasing the chances of all of the above

Considerations

- ✓ Cloud service decisions are made at the right level in the organization and involve cross-functional stakeholders (eg., legal, security, etc.)
- ✓ The organization has defined it's needs for confidentiality, integrity and availability of systems and data and has designed appropriate controls
- ✓ Roles and responsibilities are defined and understood between the organization and service provider for various service deployment models

Strategy

Risks

- ❑ Making short-term gains that hurt in the long-term
- ❑ Misalignment of IT Technological Direction and Business Risk Tolerance
- ❑ Failure to align technologies with overall cloud strategy
- ❑ Business units pursue their own cloud initiatives creating silos and incompatible technologies
- ❑ Vendor lock-in or buyer's remorse

Considerations

- ✓ Involve cross-functional roles in Cloud Strategic Discussions
- ✓ Integrate cloud initiatives into IT Steering Committee discussions
- ✓ Examine how IT Org structure will change with cloud
- ✓ Examine how strategic vendor relationships will be transformed
- ✓ Evaluate early adoption benefits and risks
- ✓ Create and document viable exit strategies

Roadmap

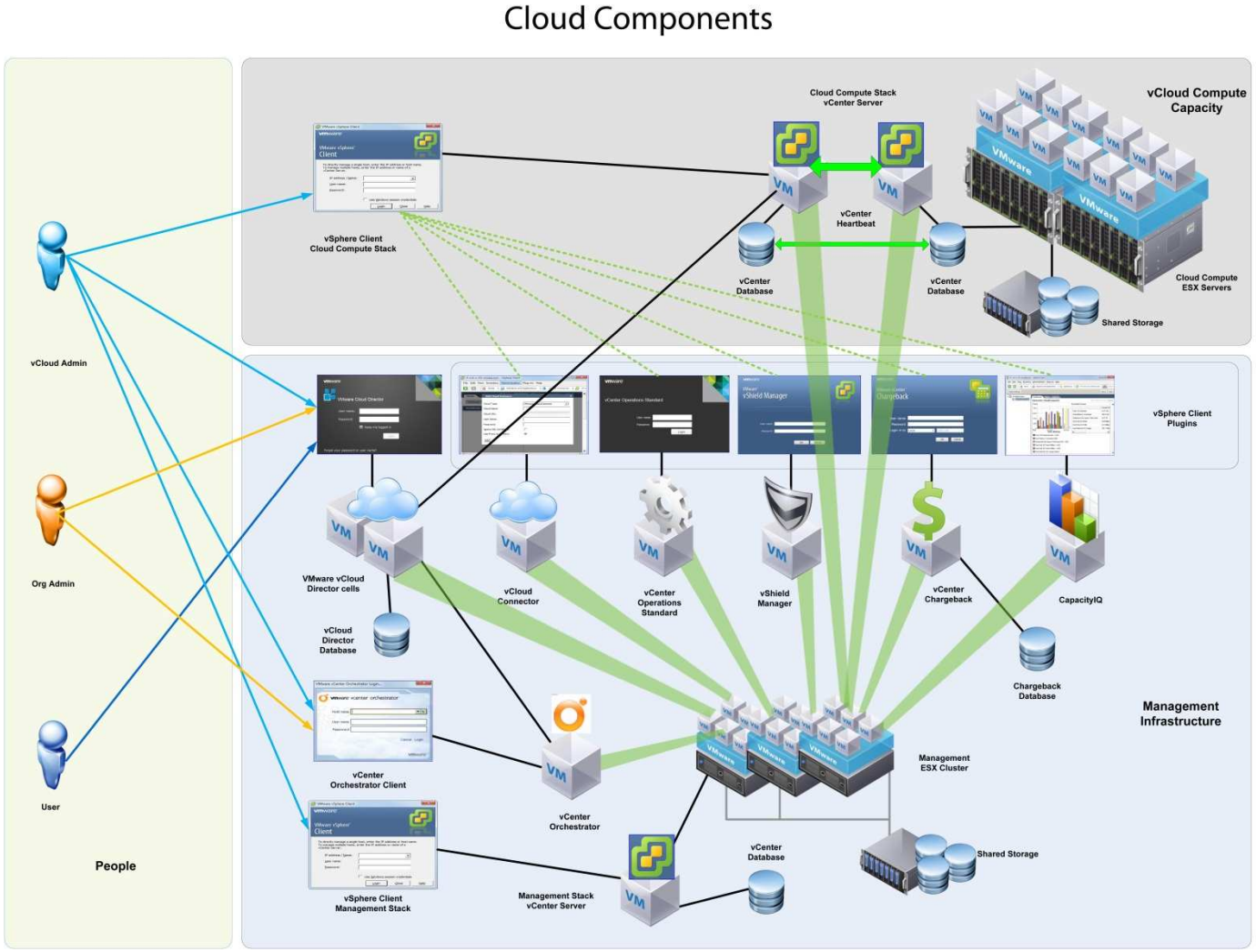
Risks

- ❑ Increased costs, failure to achieve benefits
- ❑ Disruption of service to customers
- ❑ Loss of competitive advantage
- ❑ Fines from failed regulatory compliance
- ❑ Loss of revenue
- ❑ Negative impact on reputation
- ❑ Loss of expected return-on-investment
- ❑ Excessive project costs

Considerations

- ✓ Move applications/data in the right order to maximize value, reduce risk
- ✓ Implement cloud processes and dependent technologies prior to migrating high governance applications and data
- ✓ Utilize DR to facilitate path to cloud services
- ✓ Implement security and monitoring controls on the front end
- ✓ Coordinate roadmap with end-users and cross-functional stakeholders

Cloud Service Layer



4 Cloud Services Layer

Risks

- ❑ Unauthorized access to data and applications
- ❑ Data loss
- ❑ Disruption of service to customers

Considerations

- ✓ Assess cloud management tools the same way we would assess other management applications. Who has access, what can they do with the access
- ✓ Understand how the cloud management tools work – are they using a superuser account
- ✓ Log and monitor access at the cloud layer
- ✓ Implement logical security in the cloud layer
- ✓ The cloud layer enables very fast change to the environment – this should be controlled

Cloud Applications

- Inventory applications, data and technologies
- Determine characteristics of each
- Use attributes to determine the risks associated with each

Application	Developed	Virtual	Cloud	SPI	Public	Hosted
ERP System	In	No	No	N/A	Private	Internal
CRM	Out	Yes	Yes	SAAS	Public	Amazon
HR	Out	Yes	Yes	SAAS	Public	Acme
BI	In	Yes	Yes	PAAS	Public	Rackspace
Ticketing	In	Yes	Yes	IAAS	Private	Internal
Expense	In	Yes	Yes	IAAS	Private	Internal

Maturity Assessment (Benefits)

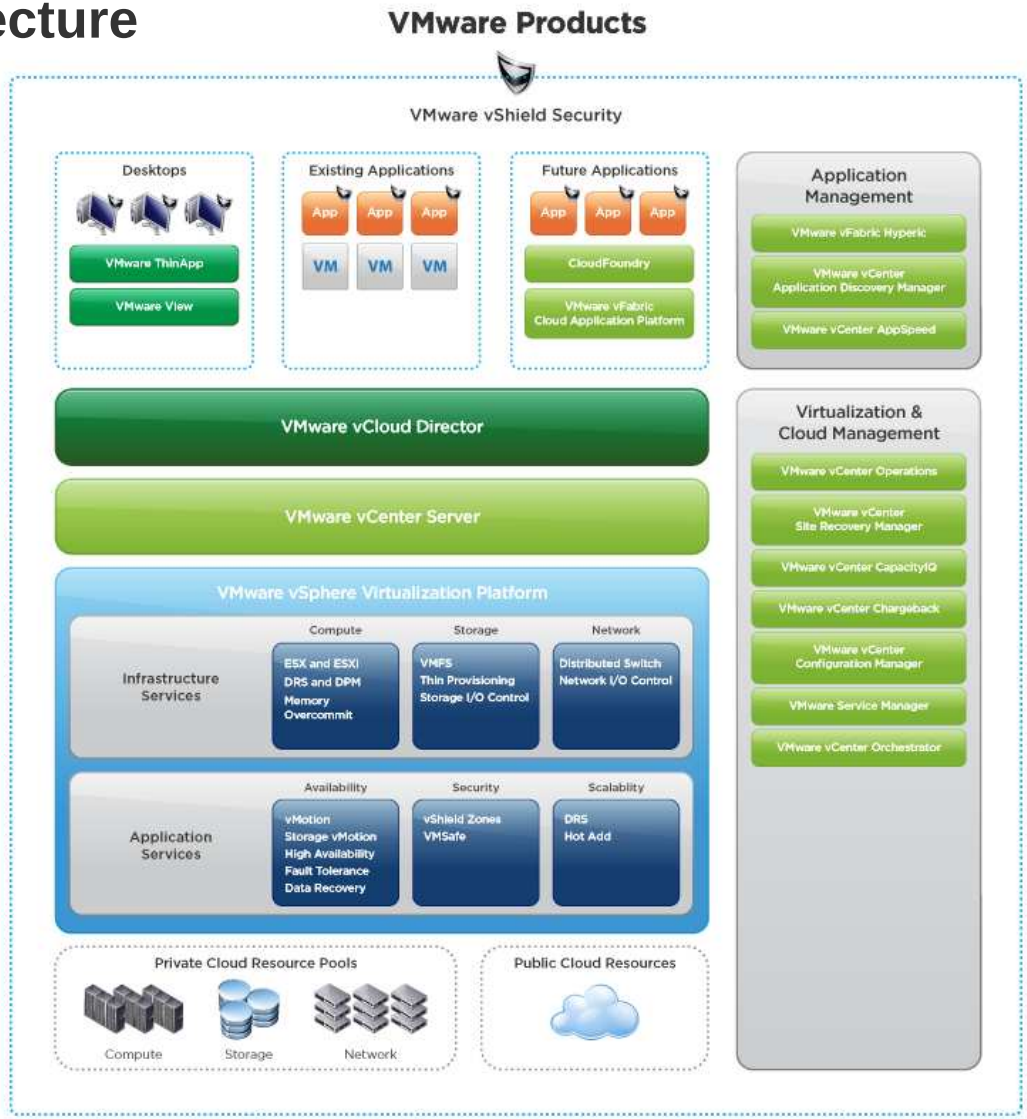
	Benefit	1	2	3	4	5
	Simplification					
	Rapid Application Deployment					
	Extreme Scalability					
	Self-provisioning and Quick-provisioning					
	Ease of Management					
	Independence from Physical Location					
	Availability, SLAs, Disaster Recovery					
	On demand, elastic Networking					
	Pay-per-use					
	Security					

Maturity Assessment (Processes)

	IT Process	1	2	3	4	5
	System Development Lifecycle					
	Configuration Management					
	Service Desk Management					
	Incident and Problem Management					
	Change and Release Management					
	Information Security					
	Disaster Recovery					
	Capacity Planning					
	Availability Management & SLAs					
	Financial Planning and Management					

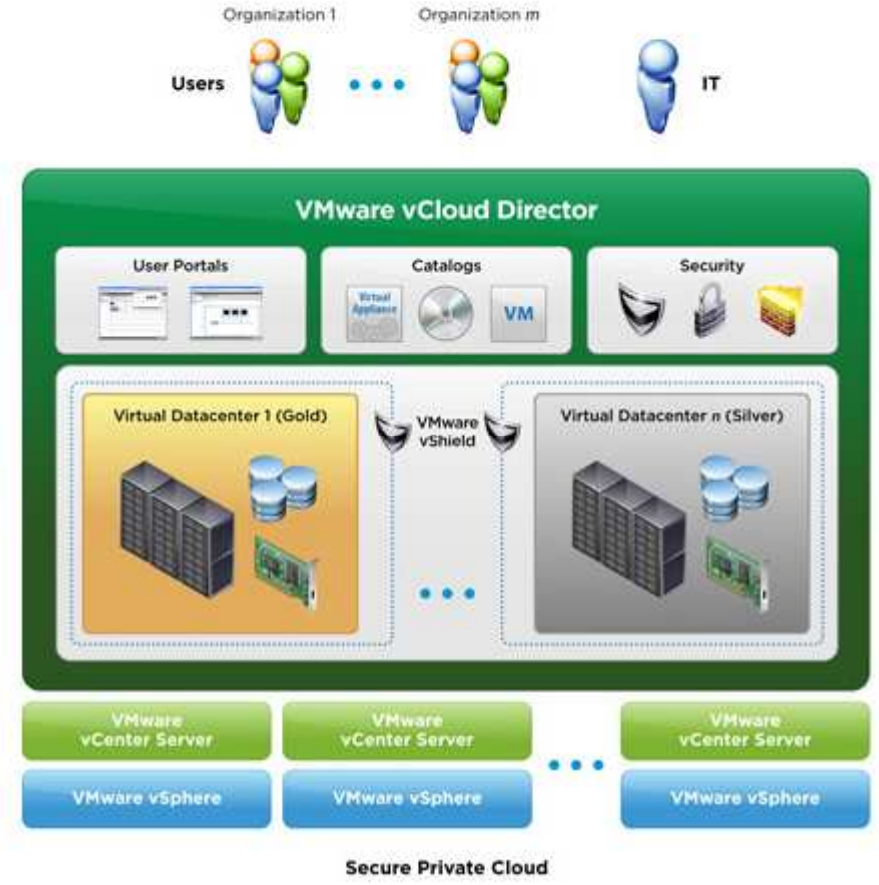
vCloud Demonstration

vCloud Architecture



vCloud Demonstration

vCloud Director



vmware

vCloud Demonstration

vCloud Helpful Terms –

A vApp is a grouping of virtual machines all working together to provide an application. When a vApp is deployed, the goal is to deploy the application that the groupings of VMs within that vApp serve up. Therefore when a vApp is deployed in a virtual datacenter, all of the VMs in that vApp are deployed simultaneously and treated with the same policies that are applied to the vApp. Note: A vApp can have one or more VMs.

A Catalog is an inventory of software media, such as ISO images, and prebuilt vApps. Once a vApp is created the first time, it can be cloned and checked into a catalog as a vApp Template. If more instances of a vApp are needed in the future, they can be cloned over and over again from the template vApp in the catalog.

A Virtual Data Center is simply a pool of resources, compute, storage, and network, to run applications on by way of running one or more virtual machines.

vCloud Demonstration

Auditing Tips:

- **User Access**
- **Logging and Monitoring**
- **Resource Allocation**
- **High Availability**
- **Backup and Recovery**
- **Service Level Agreements (SLA)**
- **Governance Structure (for Approvals)**
- **Security Hardening/Compliance (e.g. vCloud Director, vCenter, vSphere, Database, Operating System)**
  - vSphere 4.1 Hardening Guide: http://www.vmware.com/resources/techresources/10198
  - vCloud Director Hardening Guide: http://www.vmware.com/resources/techresources/10138
  - VMware Security and Compliance Blog: http://blogs.vmware.com/security/

Resources for further Learning

vmworld General Sessions:

- http://www.vmworld.com/community/conference/us/learn/generalsessions

VMware Cloud Computing information:

- http://www.vmware.com/solutions/cloud-computing
- White papers (no registration required)
- Product information

RSA Cloud Security Blog

- http://blogs.rsa.com/category/cloud-security/

More Resources – Cloud Computing

Some resources for Cloud Computing:

- **ISACA**
  - IT Control Objectives for Cloud Computing (free for members)
  - Cloud Computing Management Audit Program (free for members)
  - Control Objectives for IT (COBIT)
- **Cloud Security Alliance**
  - Security Guidance for Critical Areas of Focus in Cloud Computing v2.1
  - Cloud Controls Matrix v1.2
- **IT Governance Institute**
  - IT Governance Global Status Report (free – www.itgi.org)
- **Institute of Internal Auditors**
  - Global Technology Audit Guide (GTAG-15) – IT Governance