

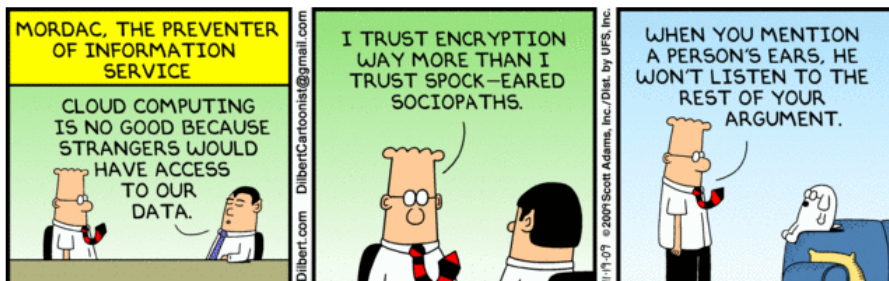
# Cloud Computing and Virtualisation Security

Jan-Willem Lammers  
Business Solutions Architect



© 2009 VMware Inc. All rights reserved.

## Cloud & Security



My main customers are Rabobank, Ministry of Defense, Dutch Police and the Government Shared Services Organisation (I&M)

When you talk about cloud you often hear: BUT what about Security?

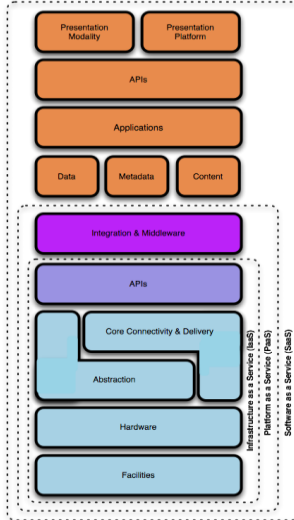
YES !! Security is also a good REASON to look at Cloud..... ☺

However the first step TOWARDS Cloud is to determine your EXIT strategy

## What is the Cloud and What Does it Means To Security

### SaaS

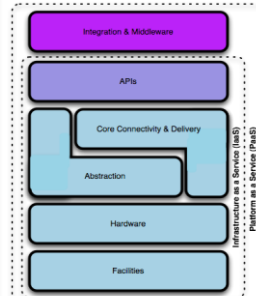
Salesforce.com, Google Apps, etc...



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

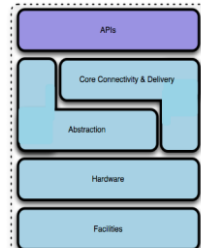
### PaaS

Vmforce, Google AppEngine, etc...



### IaaS

Terremark, Rackspace, Savvis, etc...



\*Graphics Courtesy of Chris Hoff and the Cloud Security Alliance

vmware

## 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

vmware

## VMware's Security Vision for Secure Clouds

Bring the benefits of Cloud Computing to the Enterprise, via  
**Secure Hybrid Clouds**

- **Virtualize Security** into Security VMs (SVMs)
- **Enable** programmable, logical trust zones & security policies
- **Integrate** ecosystem "best of breed" security solutions
- **Secure the VMware stack** – Infrastructure, Apps, End Users

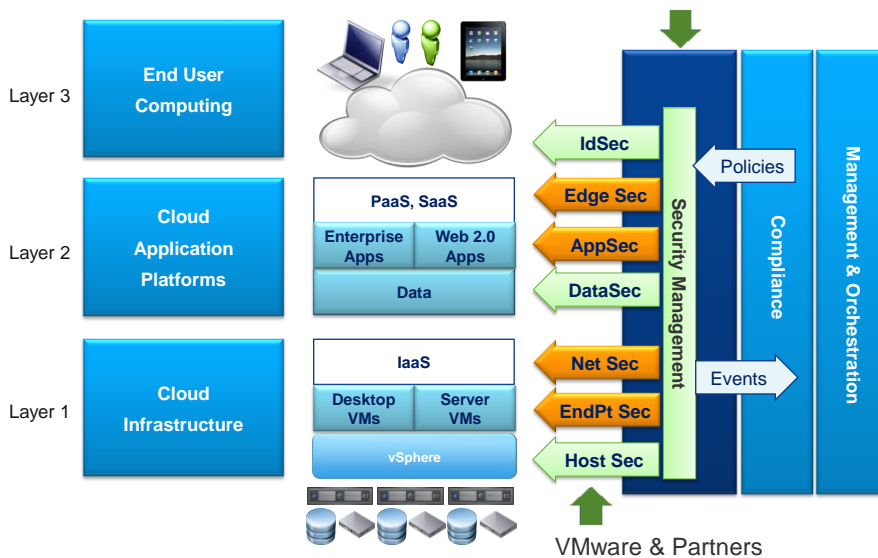
➔ **"Disruptively Simplified" Security**

5

Confidential

vmware

## Vision: Comprehensive Security across the VMware Stack



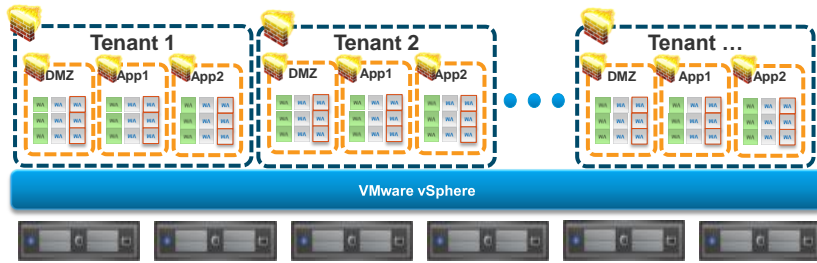
6

Confidential

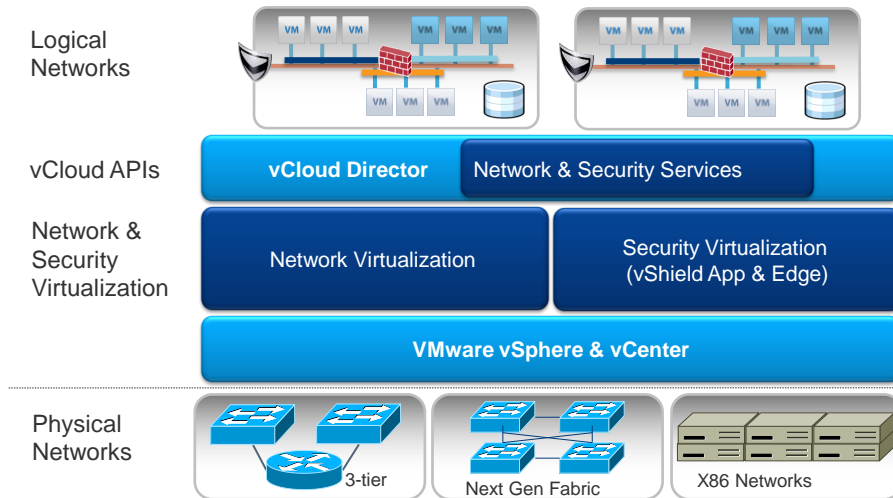
vmware

## Simple Definition of a Virtual Datacenter

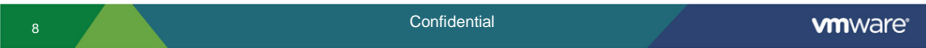
- The isolated and secured share of a virtualized multitenant environment.
- Like a physical datacenter shares the Internet for interconnectivity, the tenants of a cloud (public or private) share the local network within the private datacenter or in the service providers network, and also like a physical datacenter, each tenant also has their own private, isolated, and secured virtual networking infrastructure.



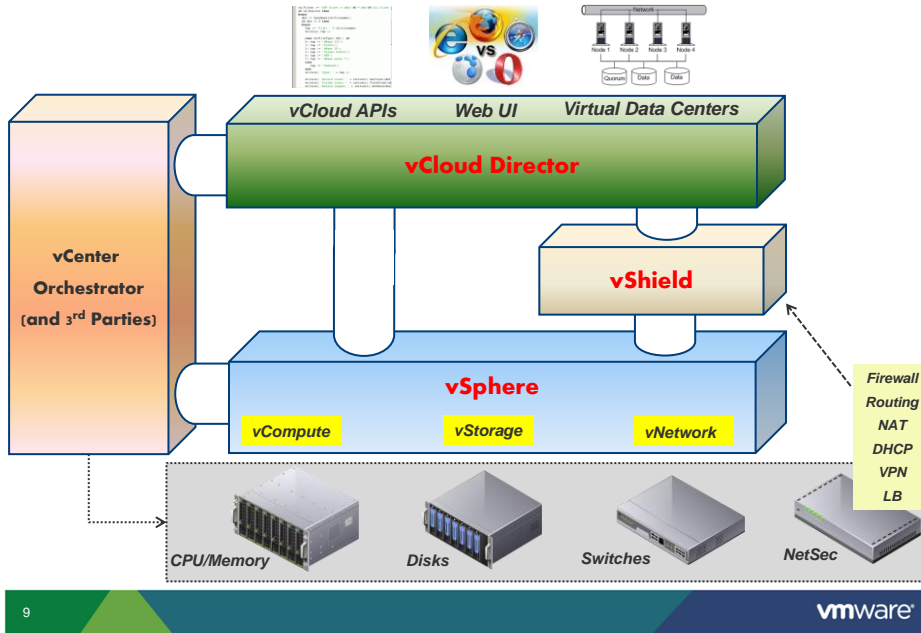
## VMware Solution – Network & Security Virtualization, Services



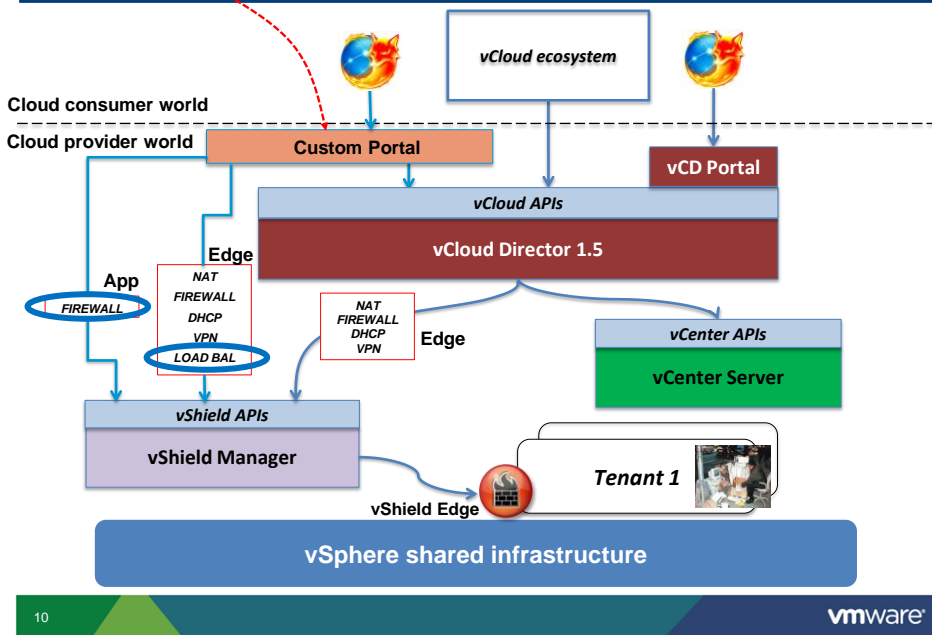
Enterprise-class network control and security with cloud automation, scale-out, self-service properties



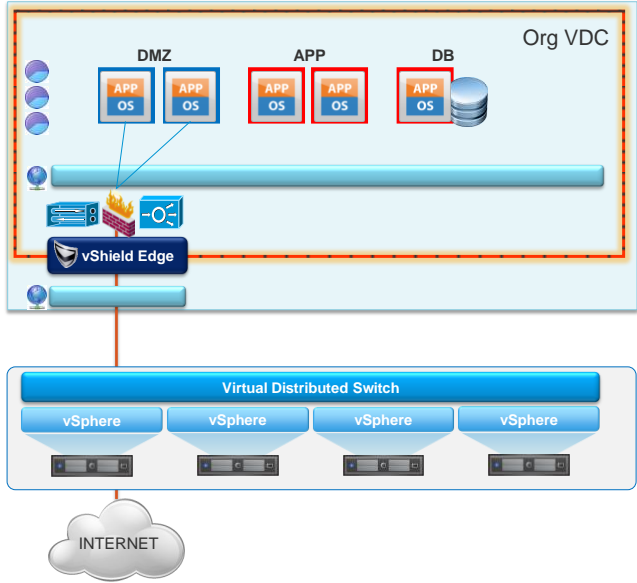
## We think clouds should look more like this (technologies aside)



## Self-Service with customization



## Automated Cloud VDC Perimeter Security with vShield Edge



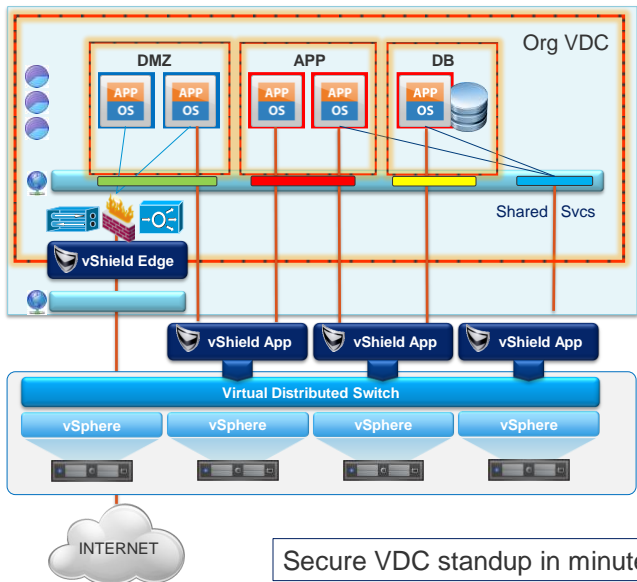
### Automated VDC Script

- **Create Provider VDC**
  - Assign Resource Pool
  - Assign Port Groups
- **Setup Perimeter services**
  - [Install vShield Edge](#)
  - External – Internal [Provision Services](#)
  - Firewall
  - NAT, DHCP
  - VPN
  - Load Balancer
- **Create, map Org VDC**
  - Provision vApps

11

vmware

## Automated Cloud VDC Interior Zones with vShield App



### Automated VDC Script

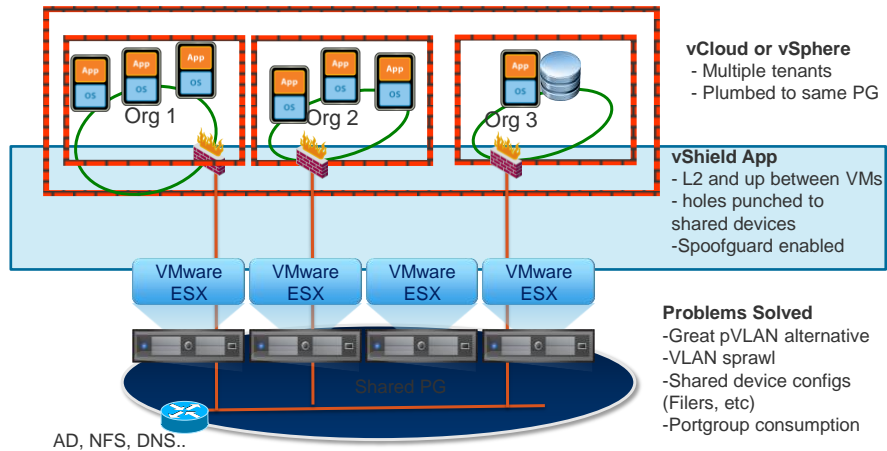
- **Create Provider VDC**
  - Assign Resource Pool
  - Assign Port Groups
- **Setup Perimeter services**
  - [Install vShield Edge](#)
  - External – Internal [Provision Services](#)
  - Firewall
  - NAT, DHCP
  - VPN
  - Load Balancer
- **Create, map Org VDC**
  - Provision vApps
- **Setup Internal Trust Zones**
  - [Install vShield App](#)
  - vDS / dvfilter setup
  - [Create interior zones](#)
  - Secure access to shared services
  - Segment internal net
  - Wire up VMs

Secure VDC standup in minutes, not weeks!

12

vmware

## Shared Services – solves backend network complexity



13

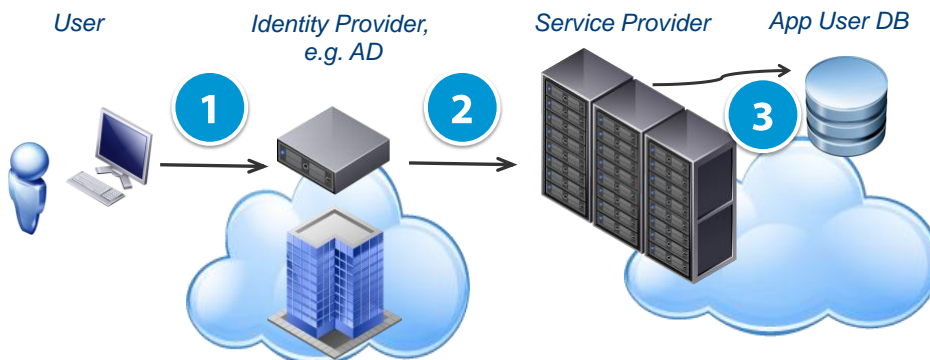
vmware

## Project Horizon: Usage of SAML

**SAML is an open standard supported by major SaaS vendors like Google, Salesforce.com, Webex, etc**

### SAML provides high security

- No passwords so eliminates phishing opportunities
- SAML tokens are digitally signed so cannot be tampered
- Provide a Time To Live duration to prevent replay attacks



14

vmware

## Conclusion

---

- The Cloud Had Great Benefits and like any Technology its Associated Risks
- These Risks Can Be Mitigated With Proper Controls
- The Classic Principles of Information Security Should be Applied
- Key Architecture Decisions must be made for Security
- Tools Designed for the Cloud Must Be Utilized

15

Confidential

vmware

## Q&A

---



Questions ?

[jw@vmware.com](mailto:jw@vmware.com)

16

Confidential

vmware