



# Sichere Virtualisierung mit VMware

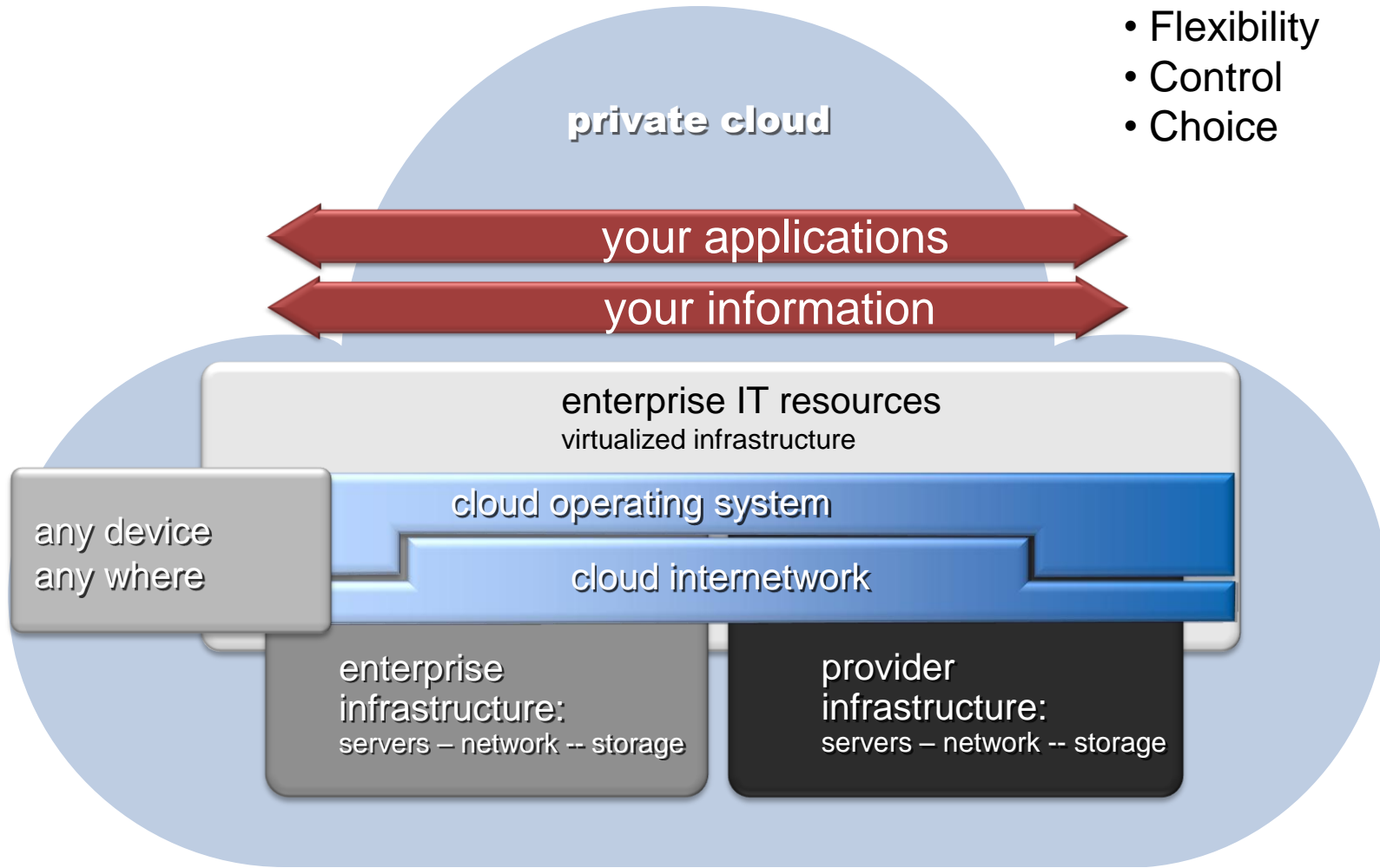
Stefan Bohnengel, VMware

Harald Speckbrock, RSA

Neuss, 12.11.2009

# Building The Private Cloud

- Flexibility
- Control
- Choice



The Security Division of EMC



# Security and Virtualization: New Opportunities, New Approaches

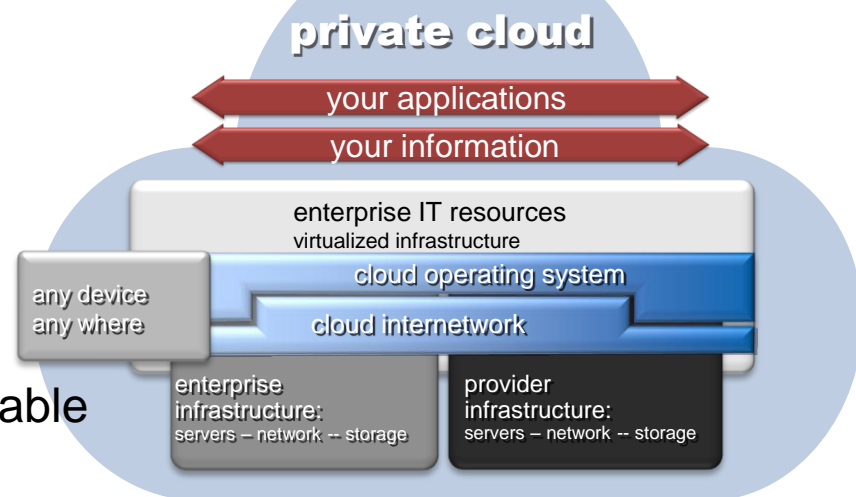
## In the virtual world:

- > IT infrastructure is more agile
- > Information is more fluid
- > Entire applications and computing processes are portable

**Organizations need to rethink and adjust how they keep information secure in a virtual world where classic perimeters and boundaries no longer exist**

**The key: an information-centric, risk-based approach to security**

- > Make security pervasive in the infrastructure
- > Make security persistent with the information itself
- > Apply security based on risk to the business



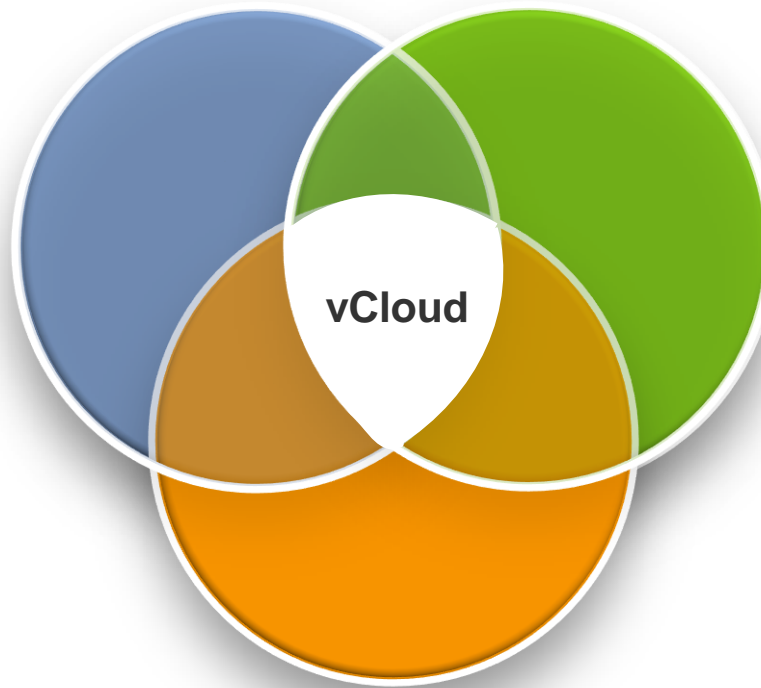
The Security Division of EMC



# VMware vCloud Initiative

## Enterprise Ready

- Proven robust platform used by 150K+ customers
- Policy-based management, SLA, security, high availability for the cloud



## Choice

- Across internal and external clouds
- Broadest ecosystem of service providers

## Broad Application Compatibility

- Optimized for new and existing applications
- No need to rewrite or re-implement your applications



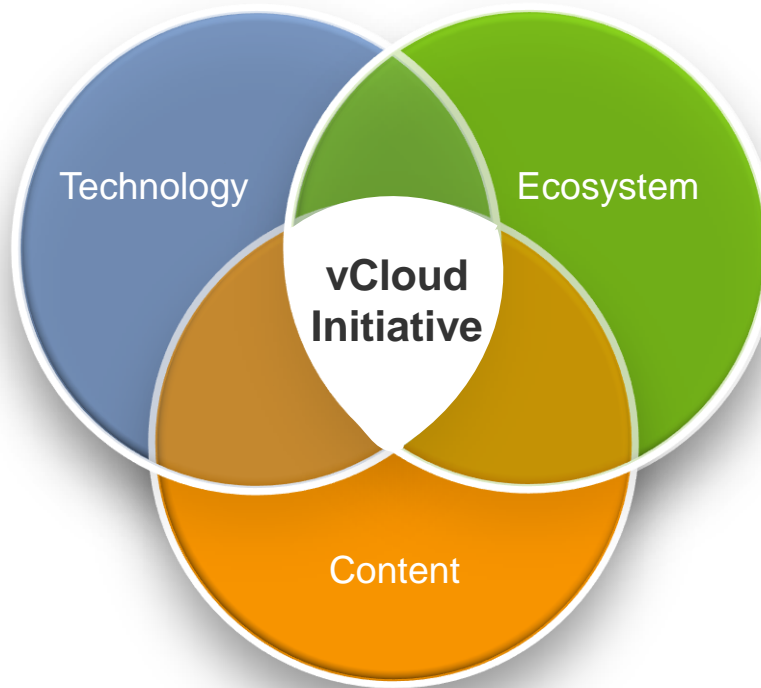
The Security Division of EMC



# vCloud: Summary of VMworld Announcements

## Enterprise Ready

- vSphere
- vCenter
- vCloud API **\*NEW\***



## Choice

- 1000+ service providers **\*NEW\***
- Major new cloud services:  
Verizon, Savvis **\*NEW\***
- vCloud Express **\*NEW\***

## Broad Application Compatibility

- New vCloud ISV partners **\*NEW\***
- SpringSource **\*NEW\***



The Security Division of EMC



# VMware Security Strategy



## Core Platform Security

- New platform hardening features further enhance robust security capabilities
- Thin-hypervisor strategy

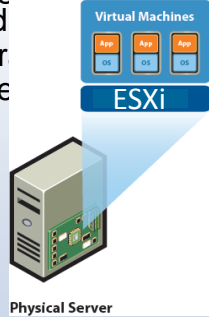


## Phase 1: Surface Area Reduction

- Shrink size of core platform
- Eliminate interfaces (service console, etc.)
- Utilize "standard" interfaces

Open

- Integrate VMware prod oper the e



## Phase 2: Lockdown, Configuration

- Best practices on configuring, deploying and locking down system
- Eliminate or turn off unused processes and interfaces

## Phase 3: Hardening Host Services

- Integrity on disk
- Integrity in memory
- De-privilege VMX
- Consistent Authentication and Authorization



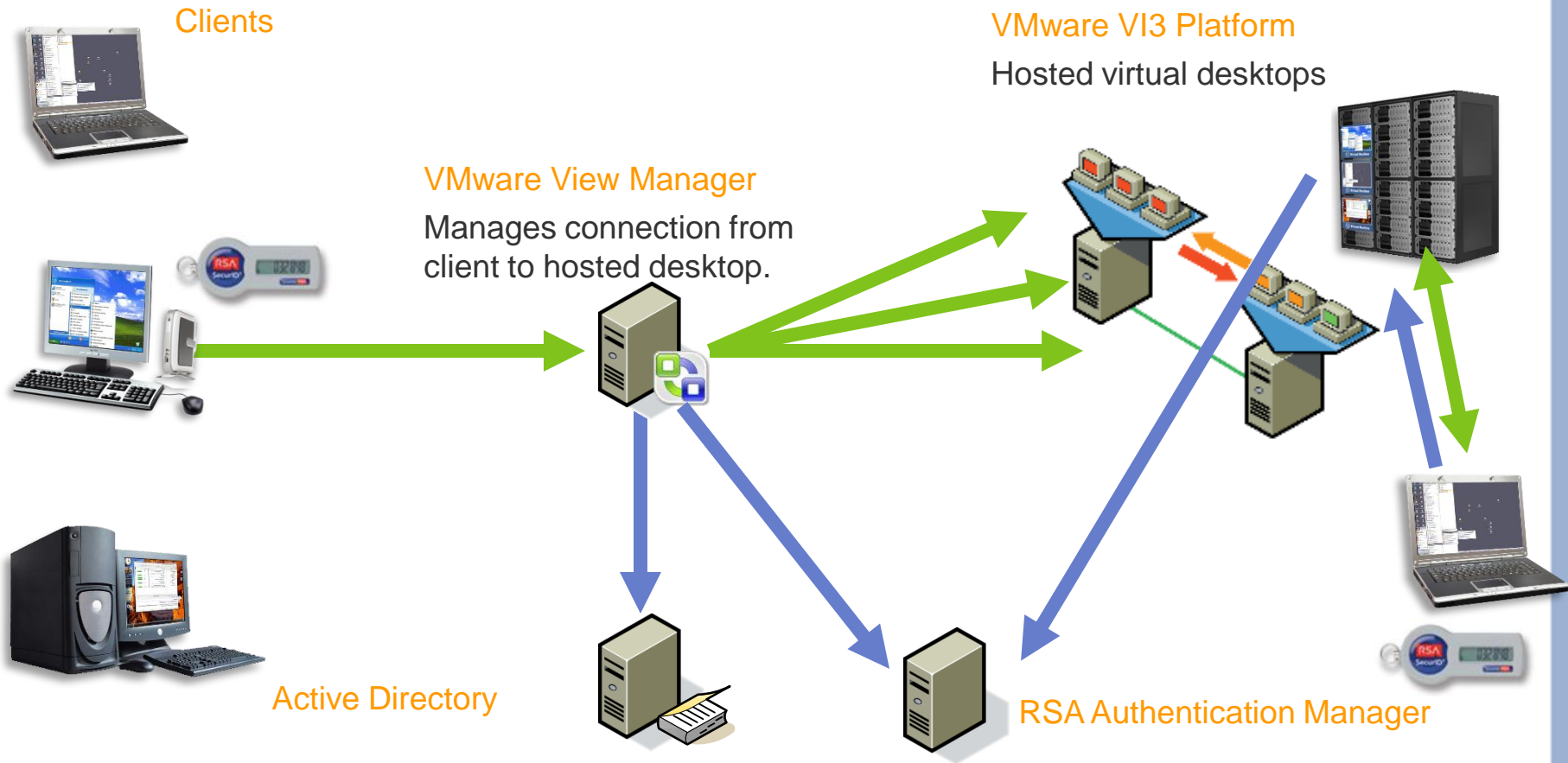
- TPM (Trusted Platform Module) support
- Code & driver signing
- Memory Protection



The Security Division of EMC



# Example: Securing VMware View Infrastructure with Strong Authentication

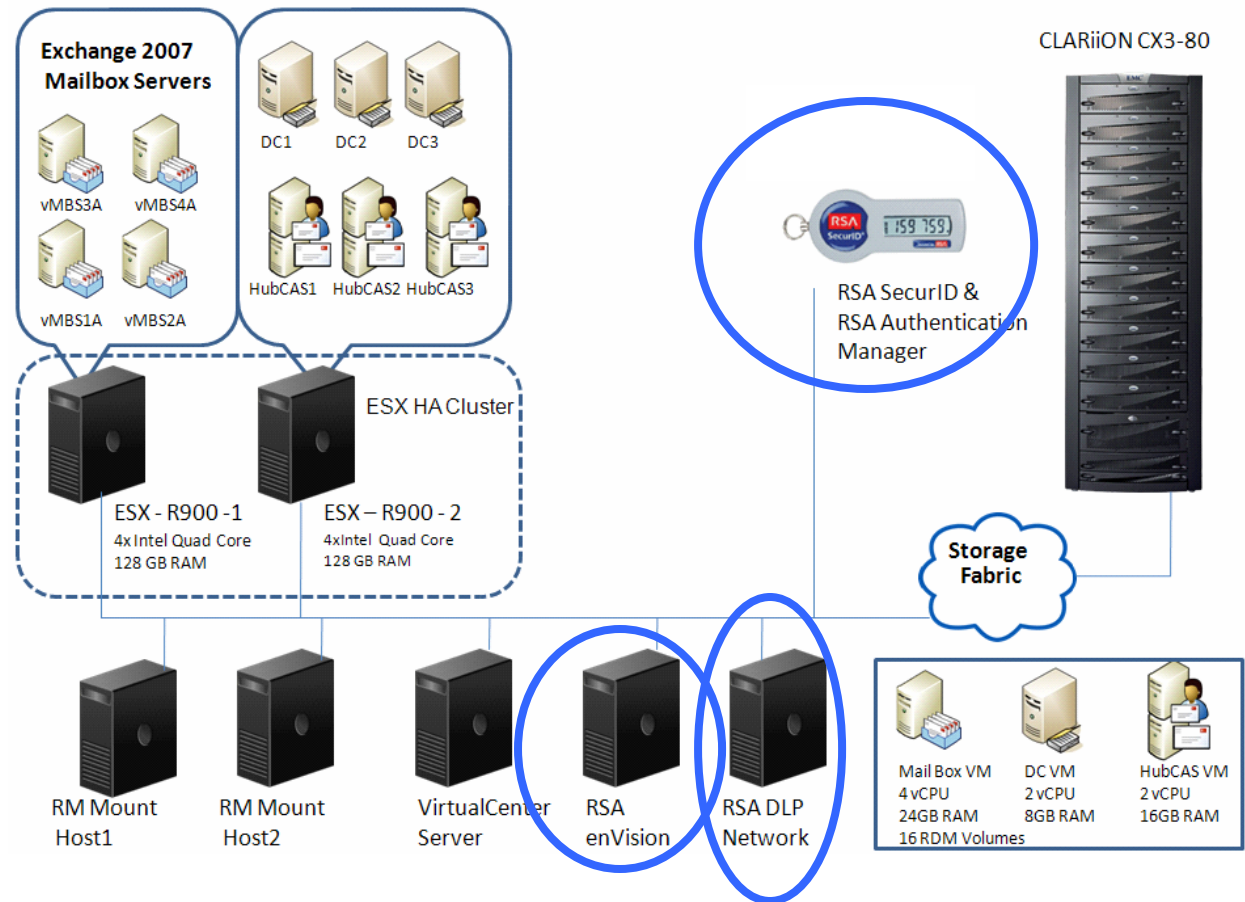


The Security Division of EMC



# Example: EMC's Proven Solution for Scalable and Secure Architecture for Virtualizing MS Exchange

- RSA SecurID for Strong Authentication of Admin users
- RSA Data Loss Prevention Network for monitoring of sensitive content in email
- RSA enVision platform for overall security Compliance monitoring



The Security Division of EMC

**EMC<sup>2</sup>**  
where information lives<sup>®</sup>

vmware<sup>®</sup>

# VMware Security Strategy



## Core Platform Security

- New platform hardening features further enhance robust security capabilities
- Thin-hypervisor strategy



## Operationalize Security

- Integrate VMware products into existing operational policies in the enterprise



## Security Virtual Appliances

- Enable broad-based security for every VM in the environment
- “Democratize” security



## Better Than Physical: Adaptive Security Infrastructure

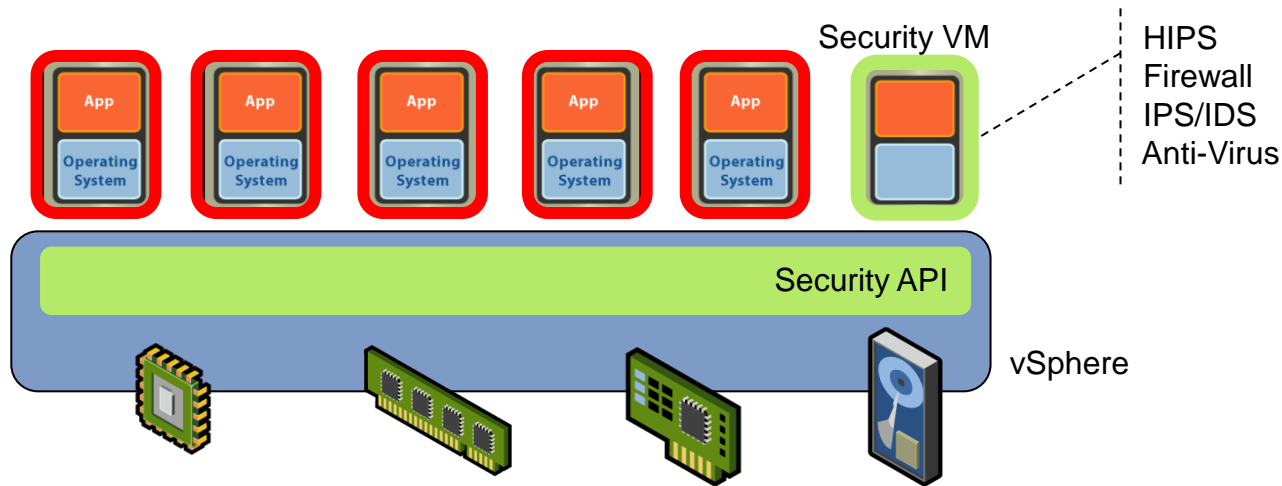
- Self-describing, Self-configuring security
- Impact security by taking advantage of unique VMware technologies
- Focus on products and operations



The Security Division of EMC



# VMsafe™



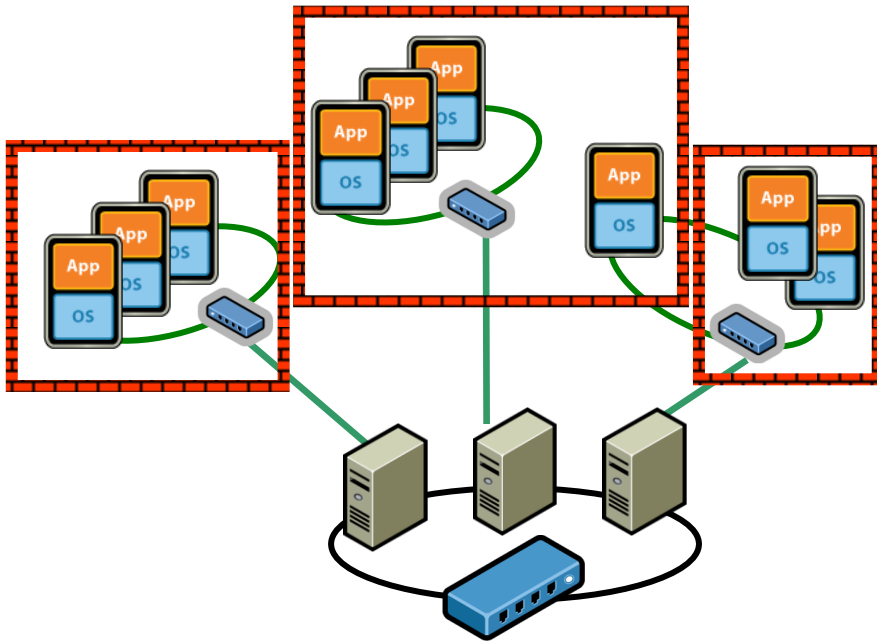
- > New security solutions can be developed and integrated into VMware virtual infrastructure
- > Protect the VM by inspection of virtual components (CPU, Memory, Network and Storage)
- > Complete integration and awareness of VMotion, Storage VMotion, HA, etc.
- > Provides an unprecedented level of security for the application and the data inside the VM



The Security Division of EMC



# vShield Zones: Capabilities and Benefits



## Capabilities

- Bridge, firewall, or isolate VM zones based on familiar VI containers
- Monitor allowed and disallowed activity by application-based protocols
- One-click flow-to-firewall blocks precise network traffic

## Benefits

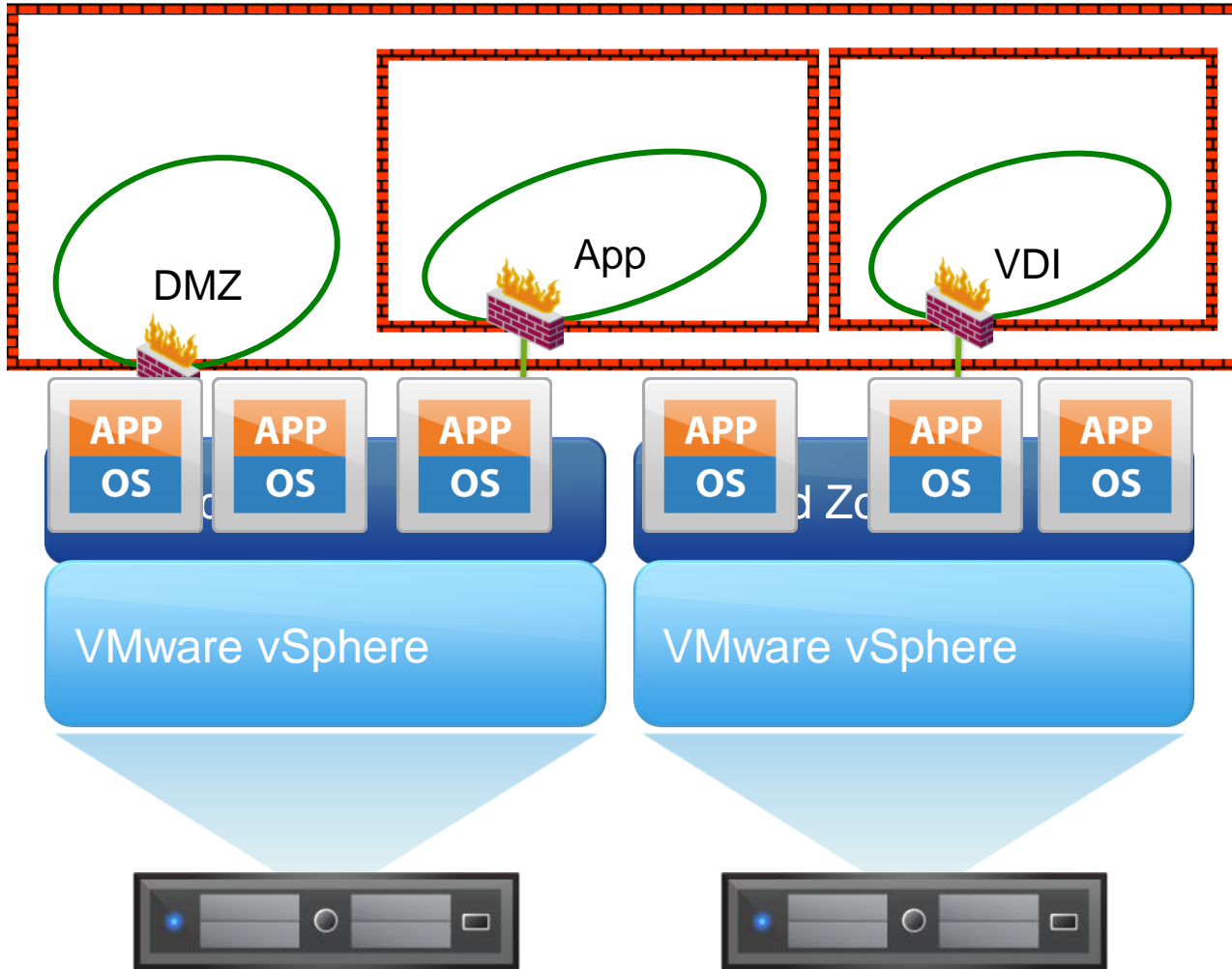
- Well-defined security posture within virtual environment
- Monitoring and assured policies, even through VMotion and VM lifecycle events
- Simple zone-based rules reduces policy errors



The Security Division of EMC



# vShield Zones



The Security Division of EMC



# Key Use Cases for vShield Zones

## Virtualizing the datacenter DMZ servers

- > Collapsing DMZ boundary using virtual firewalls

## Compliance

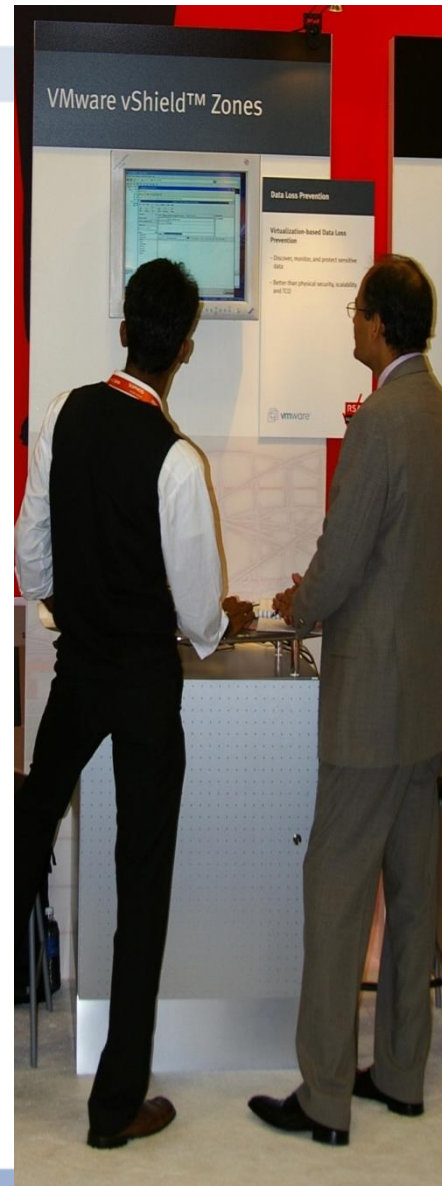
- > Intrusion prevention, web app firewalls, other prescribed network security
- > Monitoring of successful and unsuccessful network connections

## Consistent network security policies for replicated environments

- > Failover and high availability backups

## Datacenter-in-a-box for SMB and Remote Office/Branch Office

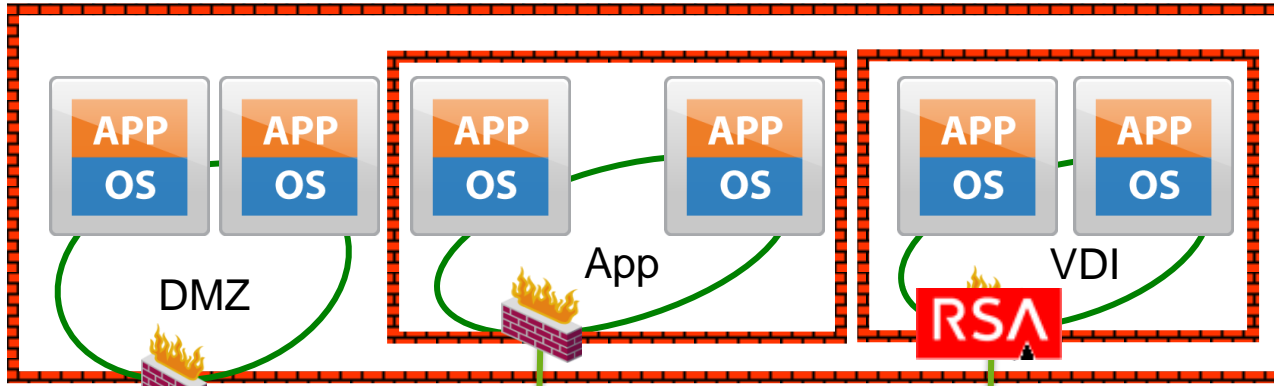
## Network isolation for multi-tenant clouds



The Security Division of EMC



# RSA Data Leakage Prevention & enVision



- RSA enVision (SIEM)
- RSA DLP (future)

VMsafe-zones

VMsafe-zones

vShield Manager

VMware vSphere

VMware vSphere

vCenter Server



The Security Division of EMC



# vSphere Integration with RSA enVision

Copy of Copy of ESX / VC Top Events

Generated by RSA en

**Title: Copy of Copy of ESX / VC Top Events**

This report displays the top events recorded at ESX/VC over a time of period  
 Wed Feb 11 21:05:21 GMT+05:30 2009 to Fri Feb 13 21:05:21 GMT+05:30 2009  
**Results 73 of 73**

Page Layout

DeviceHostName	DeviceTypeName	MessageID	DeviceAddress	EventCategory	Date
10.31.245.10	ESXVC	UserLoginSessionEvent	10.31.245.10	User_Activity.Successful Logins	2009-02-11
10.31.245.10	ESXVC	CreateVM_Task	10.31.245.10	Config.Changes.Add	2009-02-11
10.31.245.10	ESXVC	Unknown	10.31.245.10	Unassigned	2009-02-11
10.31.245.10	ESXVC	UserLoginSessionEvent	10.31.245.10	User_Activity.Successful Logins	2009-02-11
10.31.245.10	ESXVC	PowerOffVM_Task	10.31.245.10	Config.Changes.Modify	2009-02-11
10.31.245.10	ESXVC	UserLoginSessionEvent	10.31.245.10	User_Activity.Successful Logins	2009-02-11
10.31.245.10	ESXVC	PowerOffVM_Task	10.31.245.10	Config.Changes.Modify	2009-02-11
10.31.245.10	ESXVC	PowerOnVM_Task	10.31.245.10	Config.Changes.Modify	2009-02-11
10.31.245.10	ESXVC	CreateVM_Task	10.31.245.10	Config.Changes.Add	2009-02-11
10.31.245.10	ESXVC	ReconfigVM_Task	10.31.245.10	Config.Changes.Modify	2009-02-11
10.31.245.10	ESXVC	UserLoginSessionEvent	10.31.245.10	User_Activity.Successful Logins	2009-02-11
10.31.245.10	ESXVC	Unknown	10.31.245.10	Unassigned	2009-02-11
10.31.245.10	ESXVC	CreateVM_Task	10.31.245.10	Config.Changes.Add	2009-02-11
styx.ap.rsa.net	ESXVC	UserLogoutSessionEvent	10.31.253.118	User_Activity.Logoff	2009-02-11
styx.ap.rsa.net	ESXVC	UserLoginSessionEvent	10.31.253.118	User_Activity.Successful Logins	2009-02-11
styx.ap.rsa.net	ESXVC	UserLogoutSessionEvent	10.31.253.118	User_Activity.Logoff	2009-02-11
styx.ap.rsa.net	ESXVC	UserLoginSessionEvent	10.31.253.118	User_Activity.Successful Logins	2009-02-11
styx.ap.rsa.net	ESXVC	UserLogoutSessionEvent	10.31.253.118	User_Activity.Logoff	2009-02-11



The Security Division of EMC

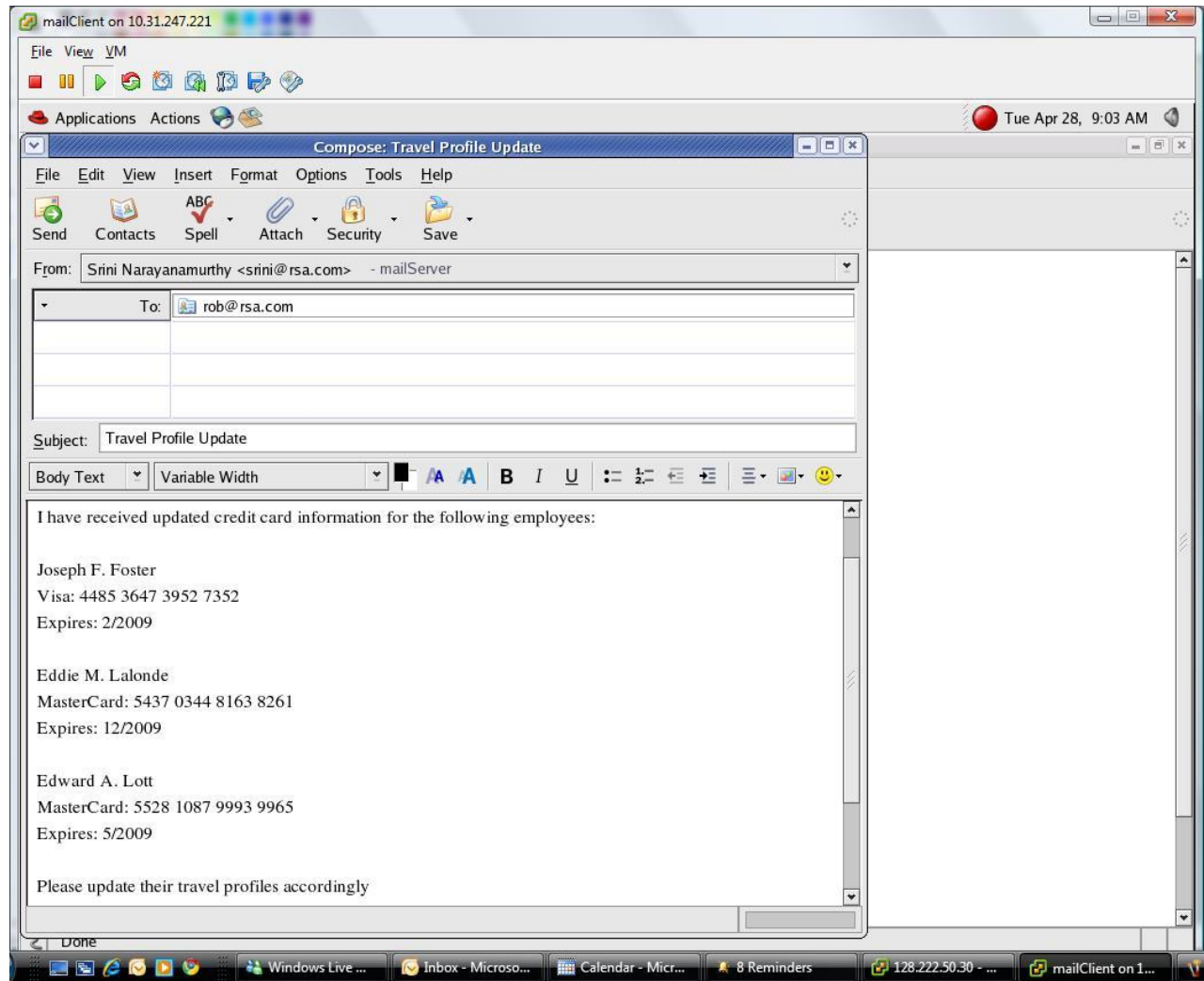


where information lives



# RSA – Data Leakage Prevention

- User sends email
- Sends Credit card info



The Security Division of EMC



# RSA – Data Leakage Prevention

- Breach detected
- Alert sent
- Details of breach available for review

DLPEM on 10.31.247.221

RSA Data Loss Prevention - Windows Internet Explorer

https://localhost/incident/viewwinincident.html?id=697&pagenum=0

Incident Details

Start Assign Comment Set Severity Set Validity Close Delete Print

Network ID: 697 Severity: Low Policy Matched: Credit Card Numbers (View all 1 policies matched) Match Count: 3  
Date: 04/28/2009, 06:34 PM Status: Open Policy Action: audit Risk Factor: 30  
Sender: srini@rsa.com Assignee: admin Content Blade: Credit Card Number Validity: Real Issue

View all incidents by this sender View Event Detail

smtp transmission details

Protocol: smtp  
Device Type: sensor  
From: srini@rsa.com  
To: [root@rsa.com, rob@rsa.com]  
Date Sent: 04/29/2009, 12:12 AM  
Email Subject: Travel Profile Update  
Action Taken: audit

Component Detail: Items 1 - 2 of 2

Component	File	Content Blades	Match Count	Risk Factor	Encrypted	
original message	Message.eml	n/a	n/a	n/a	No	Download
body	Message.mail/body.txt	Credit Card Number	3	30	No	Download

Matched Content:

file Update  
ACME Travel,  
I have received updated credit card information for the following employees: Joseph F. Foster Visa: 4485 3647 3952 7352 Expires: 2/2009 Eddie M. Lalonde MasterCard: 5437 0344 8163 8261 Expires: 12/2009 Edward A. Lott MasterCard: 5528 1087 9993 9965 Expires: 5/2009

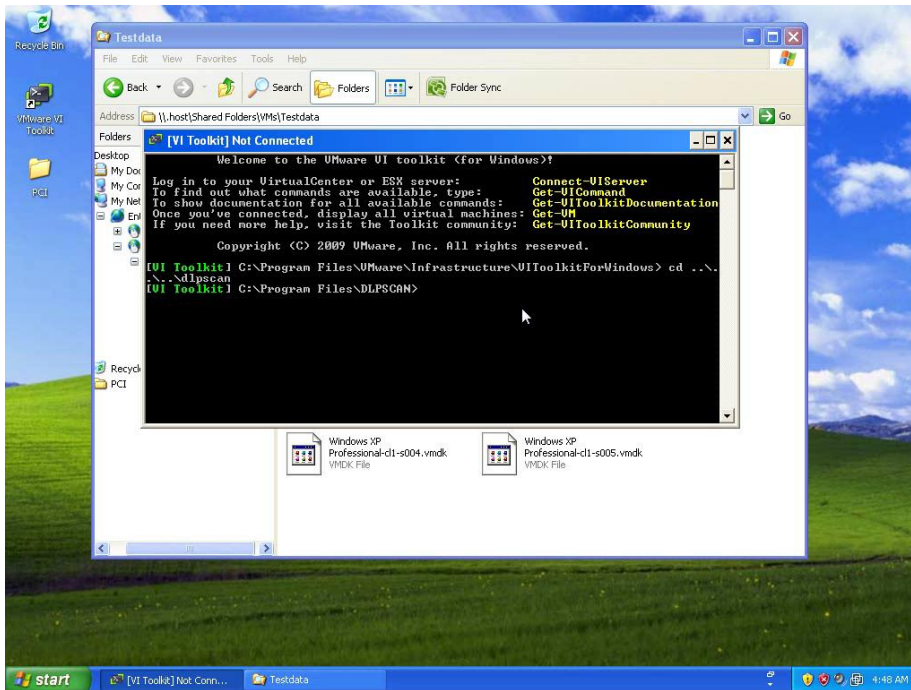


The Security Division of EMC

EMC<sup>2</sup>  
where information lives<sup>SM</sup>

vmware

# RSA Solutions Center POC for DLP PCI Use Case



Leverage VMware's hardening guidelines

Re-examine current security practices in terms of effectiveness in a virtual world

- Engage EMC/RSA Professional Services

Secure infrastructure

- Strong authentication

- SIEM

Secure information

- DLP

- Encryption

- Leverage VMware View to consolidate and manage the endpoint



The Security Division of EMC



Thank you



The Security Division of EMC

