



The Security Division of EMC

Building a Secure Virtualized Data Center Platform for the Cloud

Bret Hartman, RSA CTO

June 2009

Desired State...

Trusted

Control

Reliable

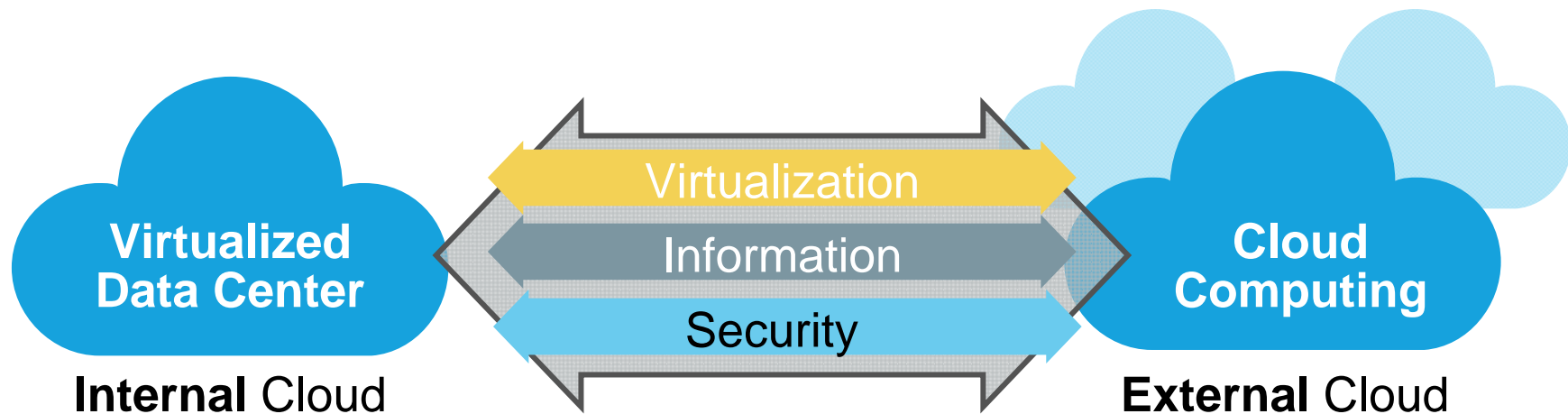
Secure

Flexible

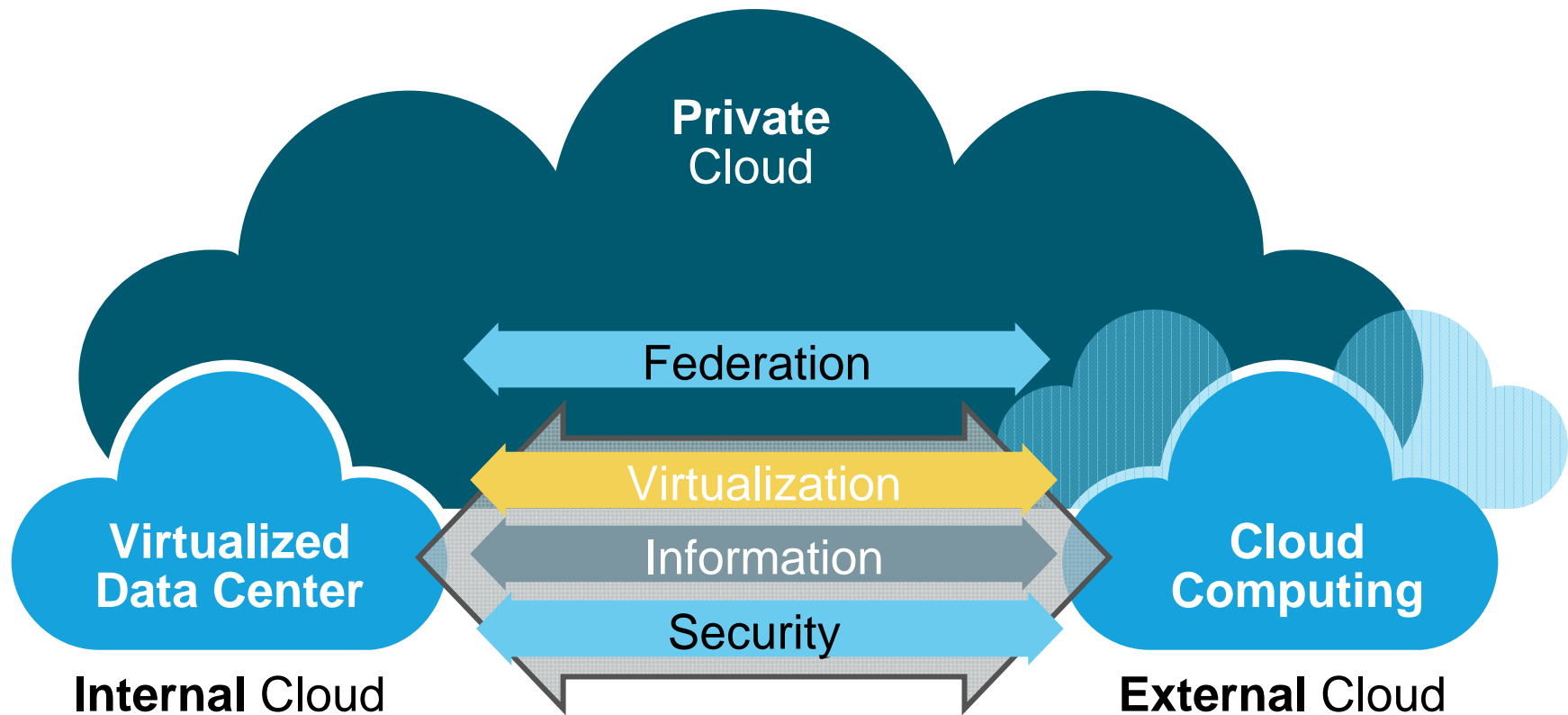
Dynamic

On-demand

Efficient



Desired State: Virtual Private Cloud

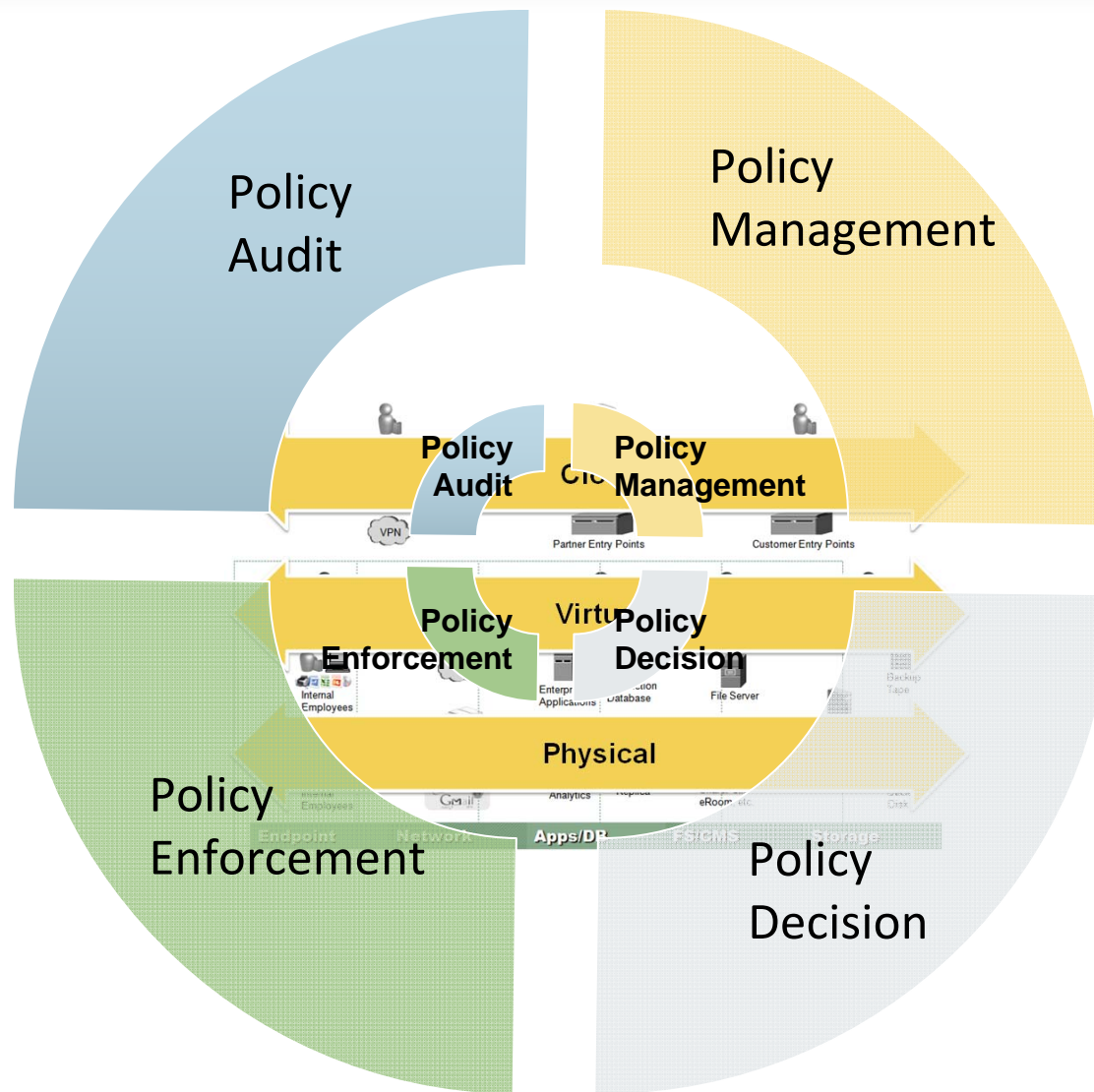


Do you trust the *Cloud*?

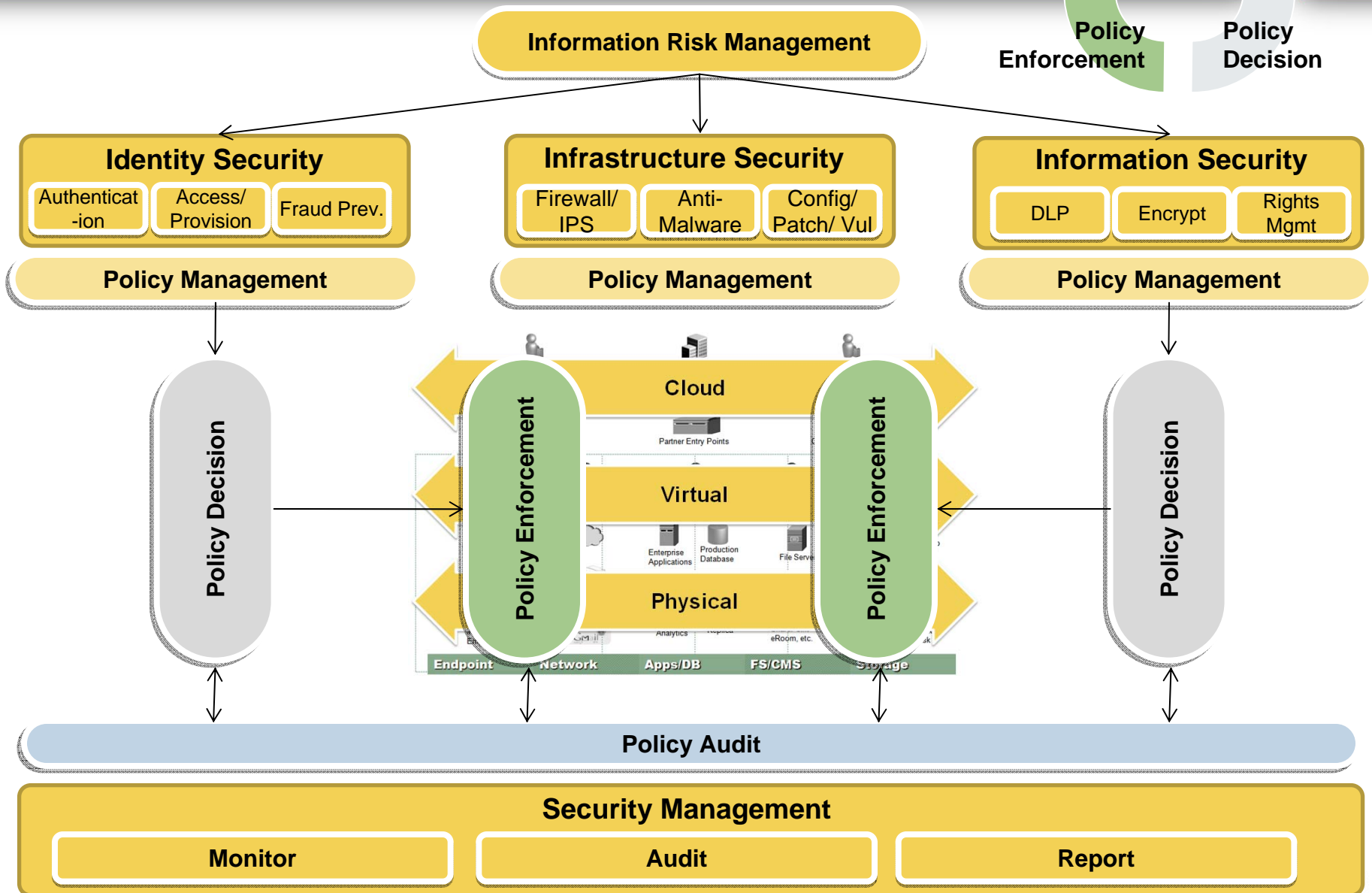
- ▶ Leap of faith?
 - Cloud services require customers to trust cloud providers with their sensitive information and processes
 - Consumers will often trust the service provider but enterprises have much higher standards
- ▶ To gain wide acceptance, cloud services must be perceived to be at least as trustworthy as in-house infrastructure
 - Provide *visibility*: comprehensive monitoring and reporting
 - Give enterprise customers *control* over the confidentiality of and access to their data and applications
 - Assure logical *separation* between multiple customers within the cloud
- ▶ Right mix of security technologies can make cloud services trustworthy
 - Security will separate the winners and the losers in the cloud market



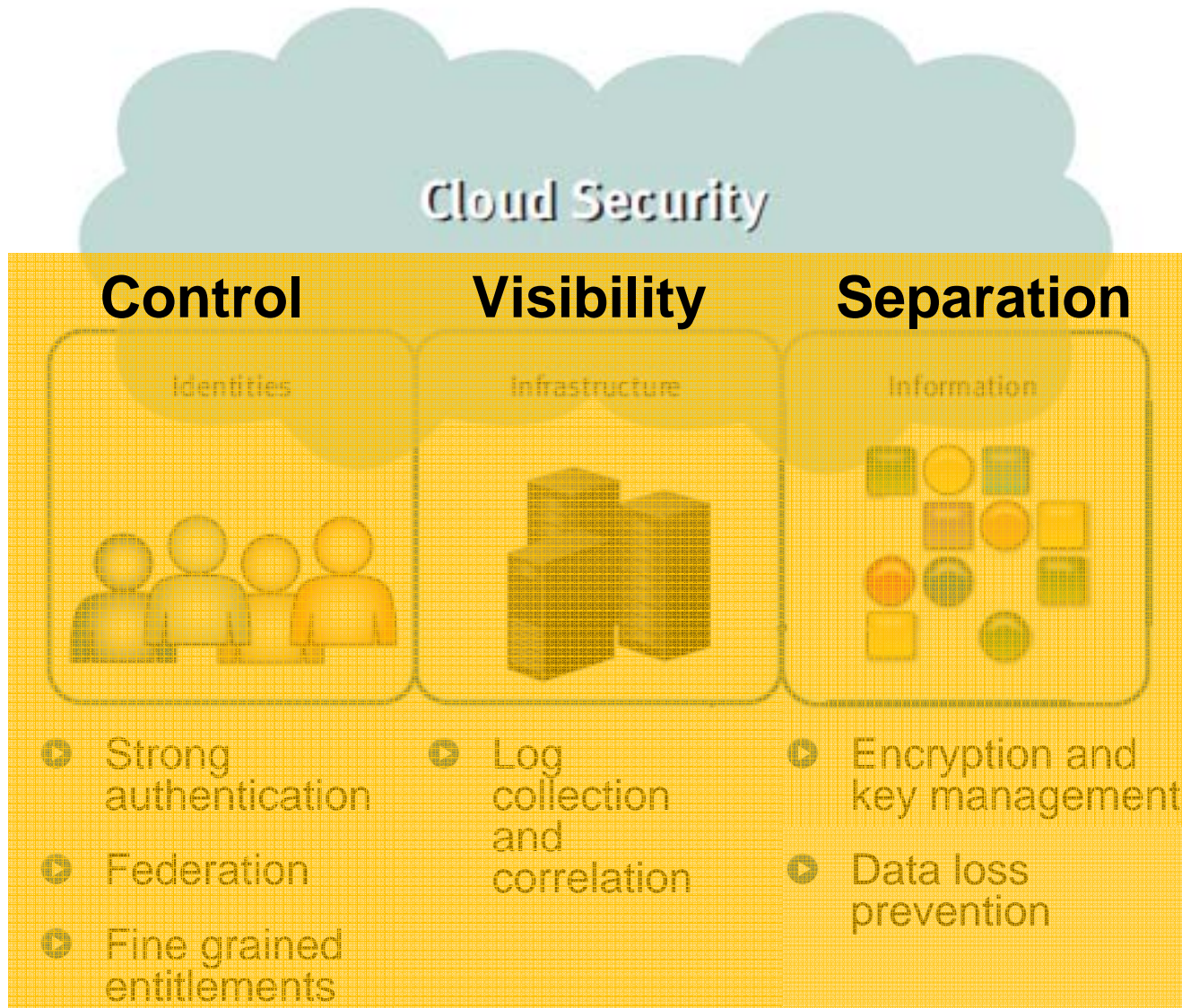
Building the Security System Architecture



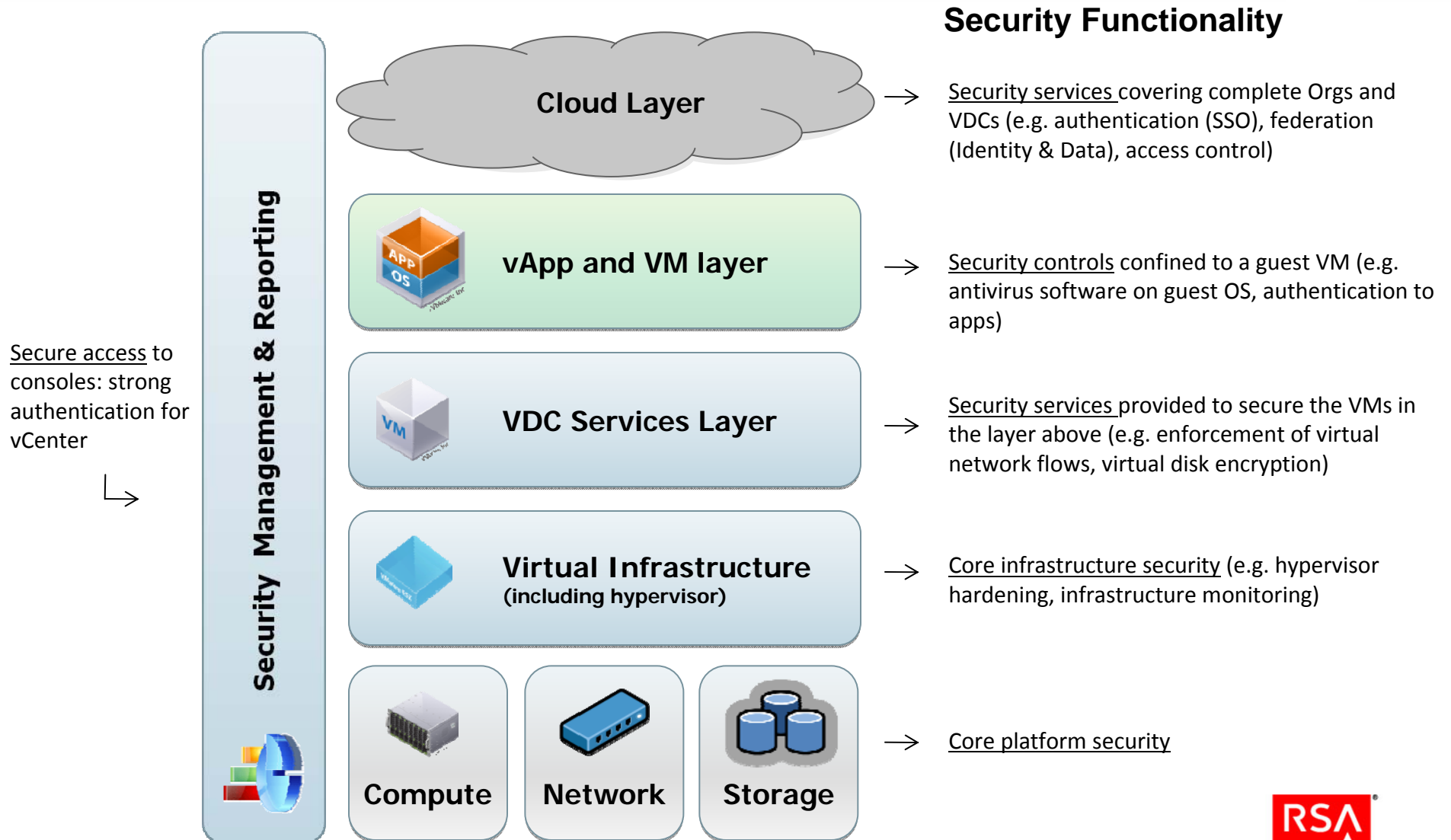
Building the Security System Architecture



Cloud Security Foundation: Identities, Information, and Infrastructure



Virtual Datacenter Platform for the Cloud: Layered Security Model



The Virtual Data Center Creates the Opportunity to Push Security Down the Stack



Today most security is enforced by the OS and application stack

- OS / application-based security is complex and ineffective

Our vision: Surpass the levels of security possible in today's physical infrastructures by pushing information security enforcement down the stack

- Out of applications and OS, into virtualization, network, and storage
- Simplified, unified security management
- Regardless of OS (Windows/Unix), patch levels, and application vulnerabilities



enVision Logging of ESX events

Copy of Copy of ESX / VC Top Events

Generated by RSA en

Copy of Copy of ESX / VC Top Events

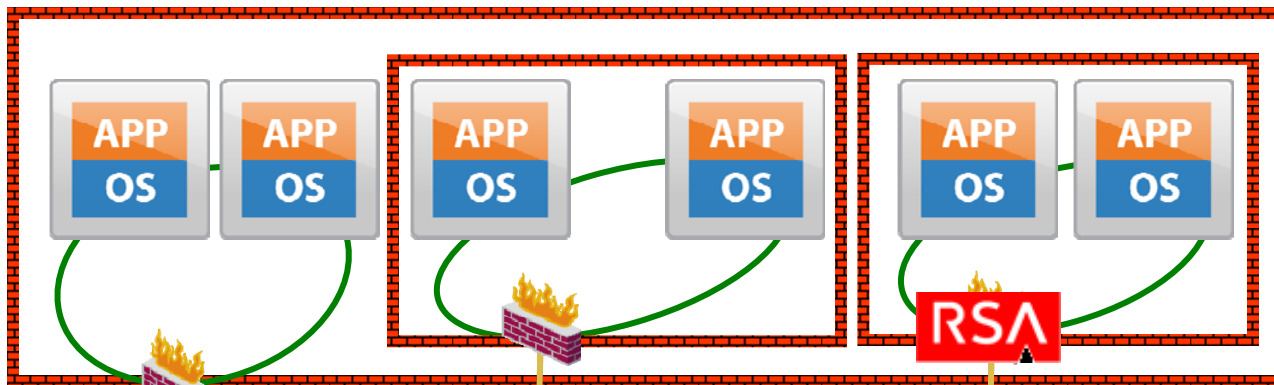
This report displays the top events recorded at ESX/VC over a time of period
: Wed Feb 11 21:05:21 GMT+05:30 2009 to Fri Feb 13 21:05:21 GMT+05:30 2009
results 73 of 73

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



Data Loss Prevention and vShield Zones



vmsafe-zones
Vmware vSphere

vmsafe-zones
Vmware vSphere

RSA
Manager

vShield
Manager

vCenter Server



vShield Zones/Data Loss Prevention PoC

The screenshot displays a Windows desktop environment. On the left, a mail client window titled 'mailClient on 10.31.247.221' shows a 'Compose: Travel Profile Update' email. The email body contains the following text:

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

Please update their travel profiles accordingly

On the right, a web browser window titled 'DLPEM on 10.31.247.221' displays the 'RSA Data Loss Prevention - Windows Internet Explorer' interface. The URL is 'https://localhost/incident/viewwinincident.html?id=697&pagenum=0'. The page shows 'Incident Details' for ID 697, with the following information:

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

The interface also shows 'smtp transmission details' and a 'Component Detail' table:

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

The 'Matched Content' section shows a snippet of the email body with credit card information highlighted in yellow:

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

RSA's Approach to Secure Virtualization

Customer roadmap

RSA Offering Strategy



Virtualize applications

Assess and plan security for virtualization

Secure virtualized applications

Secure management of virtualization

100% Virtual infrastructure

Virtualize Security Infrastructure

Secure virtual resources
(desktops, disks, networks, events)

Leverage virtualization to optimize security capabilities

Enable cloud computing

Secure cloud infrastructure

Security as a service

Enable trust in the cloud



The Security Division of EMC



The Security Division of EMC