

# the adventures of alice & bob



## Three Best Practices for Securing the Cloud – Identities, Infrastructure and Information

Speaker : Rashmi Knowles, Robert Griffin

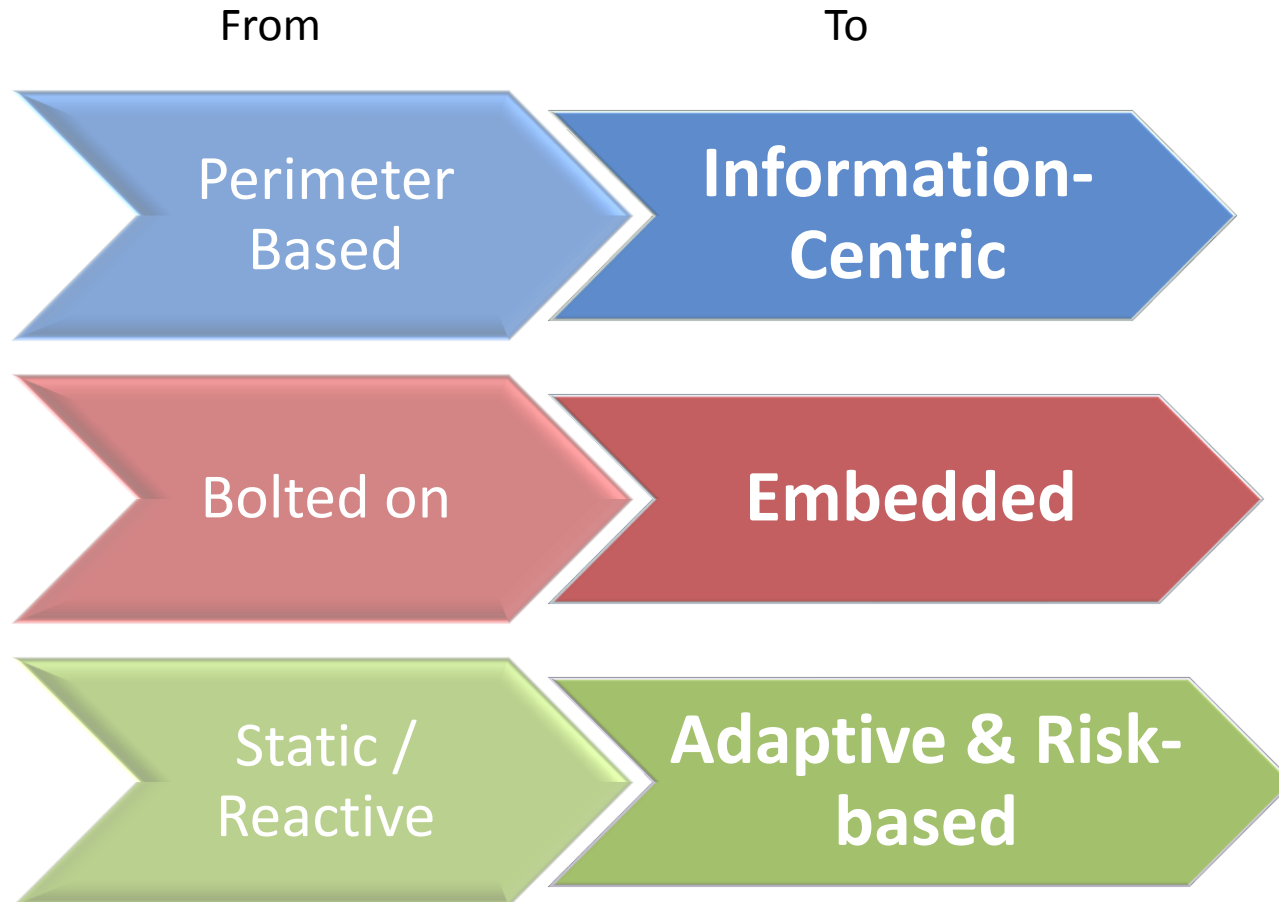
Job Title : Chief Security Architect

Company Name : RSA, The Security Division of EMC

# Agenda

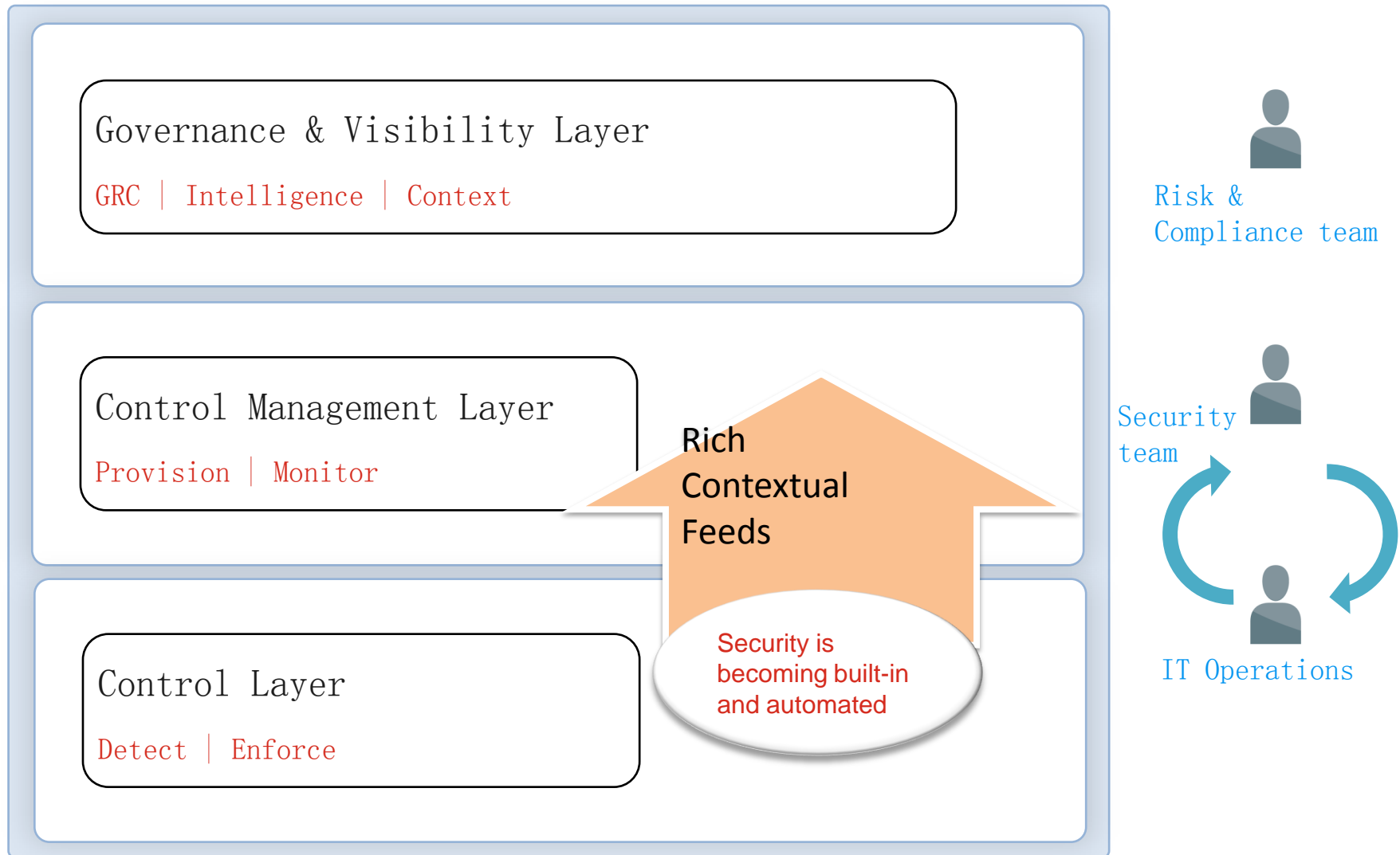
- New Concepts in Security
- Solving the Trust equation
- Securing Information, Identities and Infrastructure
- Cloud Trust authority
- Conclusion

# Cloud Demands a Change in Security Dynamics



# Rethinking the Security Stack

**RSACONFERENCE CHINA 2011**  
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING



# Achieving Security in the Cloud

## Right Information



## Trusted Infrastructure



## Right Identities



## The Result ?

*A dangerous void of trust has opened up, standing squarely between organizations and their ability to reap the cloud's well documented benefits.*







Trust = Visibility +  
Control

A photograph of three men in business suits, all blindfolded with black cloth. The man in the center is in sharp focus, looking directly forward. The two men on either side are slightly out of focus. The background shows a blurred building with windows.

“We are wondering, do we have all risks identified?  
•••we are flying blind.”

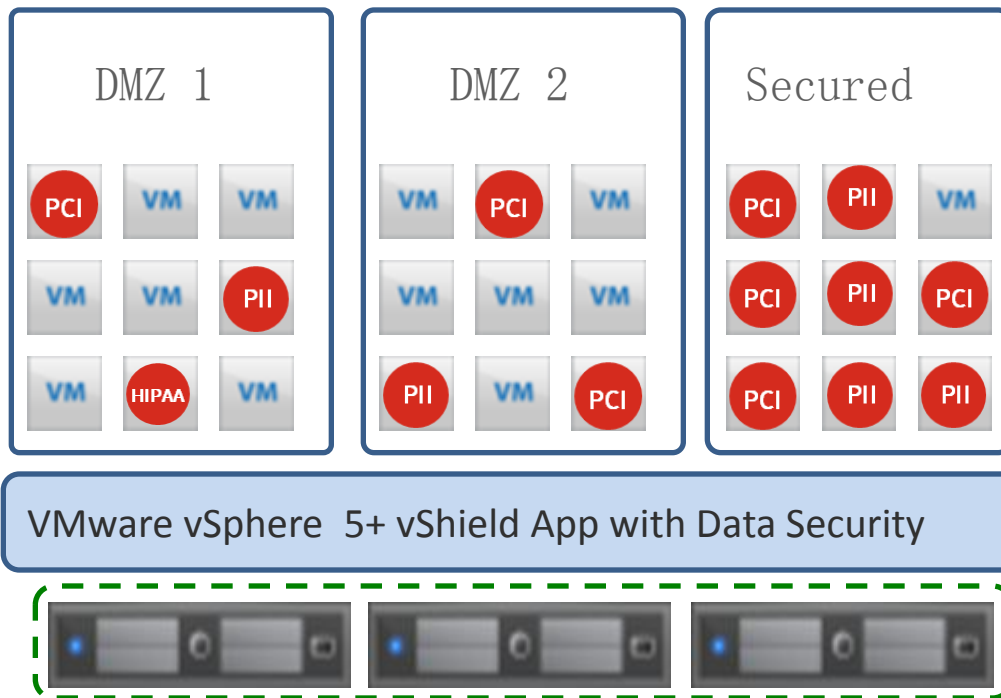
(Global 1,000 CISO)



# Control and Visibility over *Information*

- Information Challenges
  - Cloud is ‘information blind’
  - Mobility
  - Geolocation
- Discovering and Controlling Sensitive Information
  - Identify high risk information
  - Automated remediation functions
  - Logical zoning at Hypervisor level
- Cloud storage based on policy

# Example of Built-in Data Classification

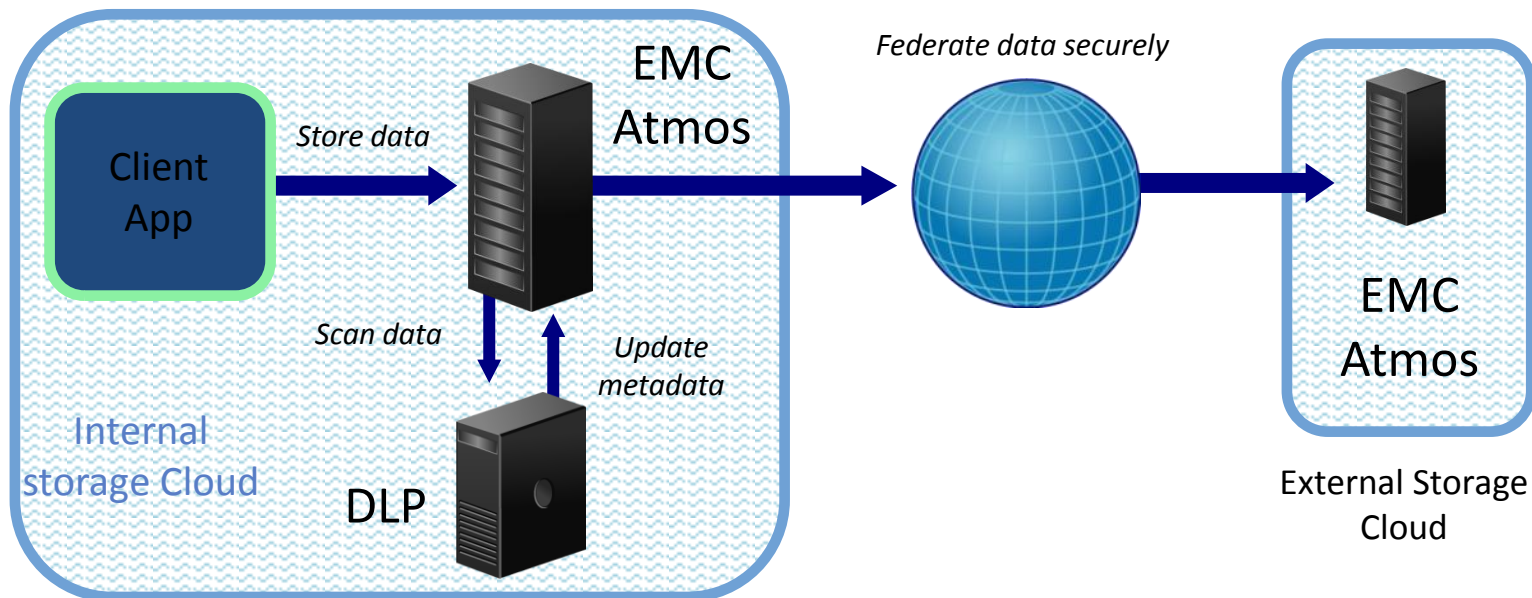


## Content Aware Infrastructure

- Classify files within VMs
- RSA DLP classification technology embedded into VMware vShield App with Data Security
- No agents or 3<sup>rd</sup> party software
- Includes 80+ expert RSA policies out of the box
- Consistent classification across both physical and virtual environments

# Content-aware Clouds

- Atmos metadata update based on DLP policy
- Sensitive data never leaves customer sites or is only sent to trusted external cloud sites
- Build content-aware private storage clouds



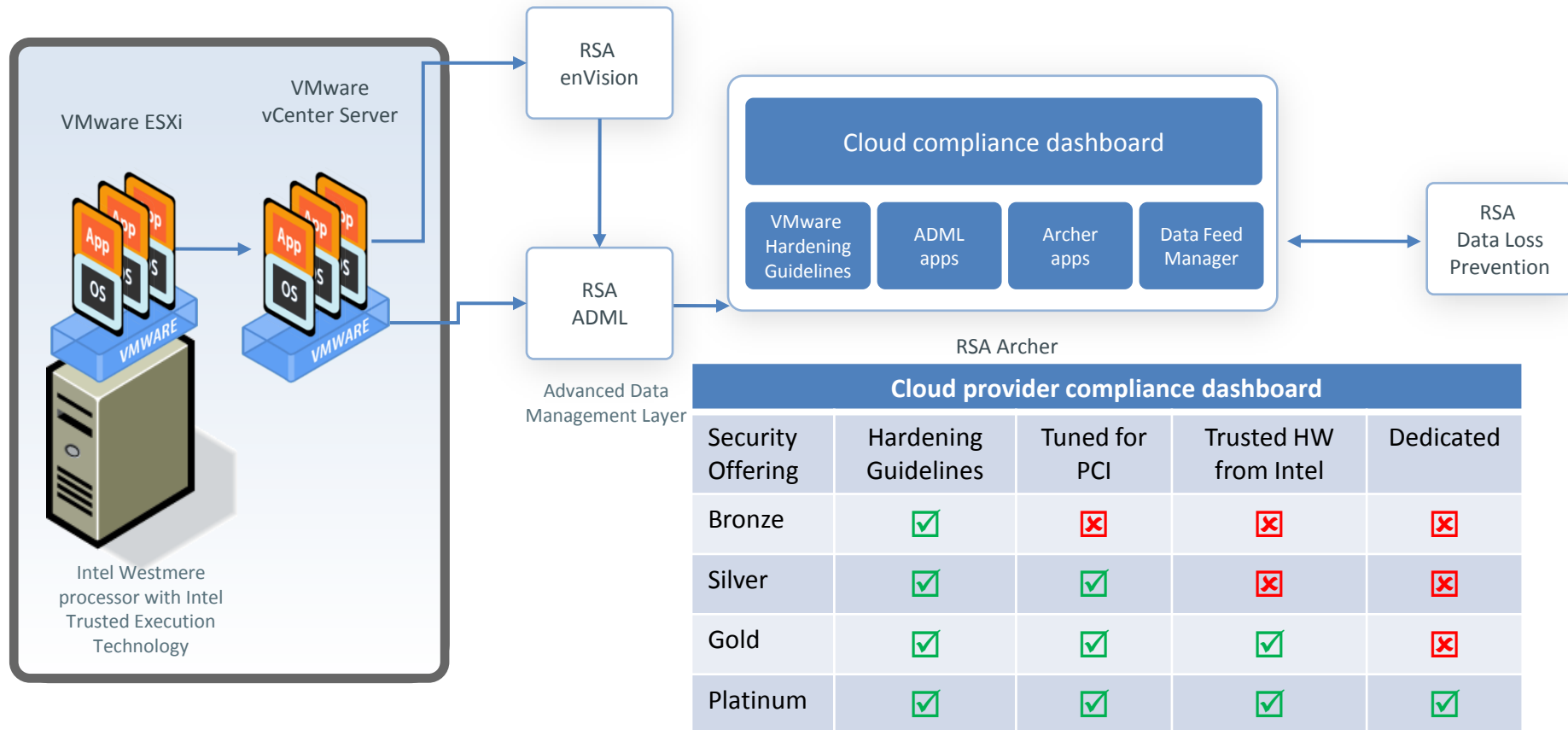
# Control and Visibility over ***Infrastructure***

- Inspecting the Clouds foundations
- Setting the roots for Secure Multi-tenancy
- Accelerating deployment of Trusted Clouds

# RSA/VMware/Intel Vision

## Verifying the Chain of Trust to control VM in the Cloud

Proof of Concept for Measuring and Monitoring Cloud Infrastructure Security at RSA Conference





# Secure Multi-tenancy

Trusted Multi-tenancy model is built on the following six foundational elements:

- Secure separation
- Service assurance
- Security and compliance
- Availability and data protection
- Tenant management and control
- Service provider management and control

Elements of Vblock Trusted Multi-Tenancy



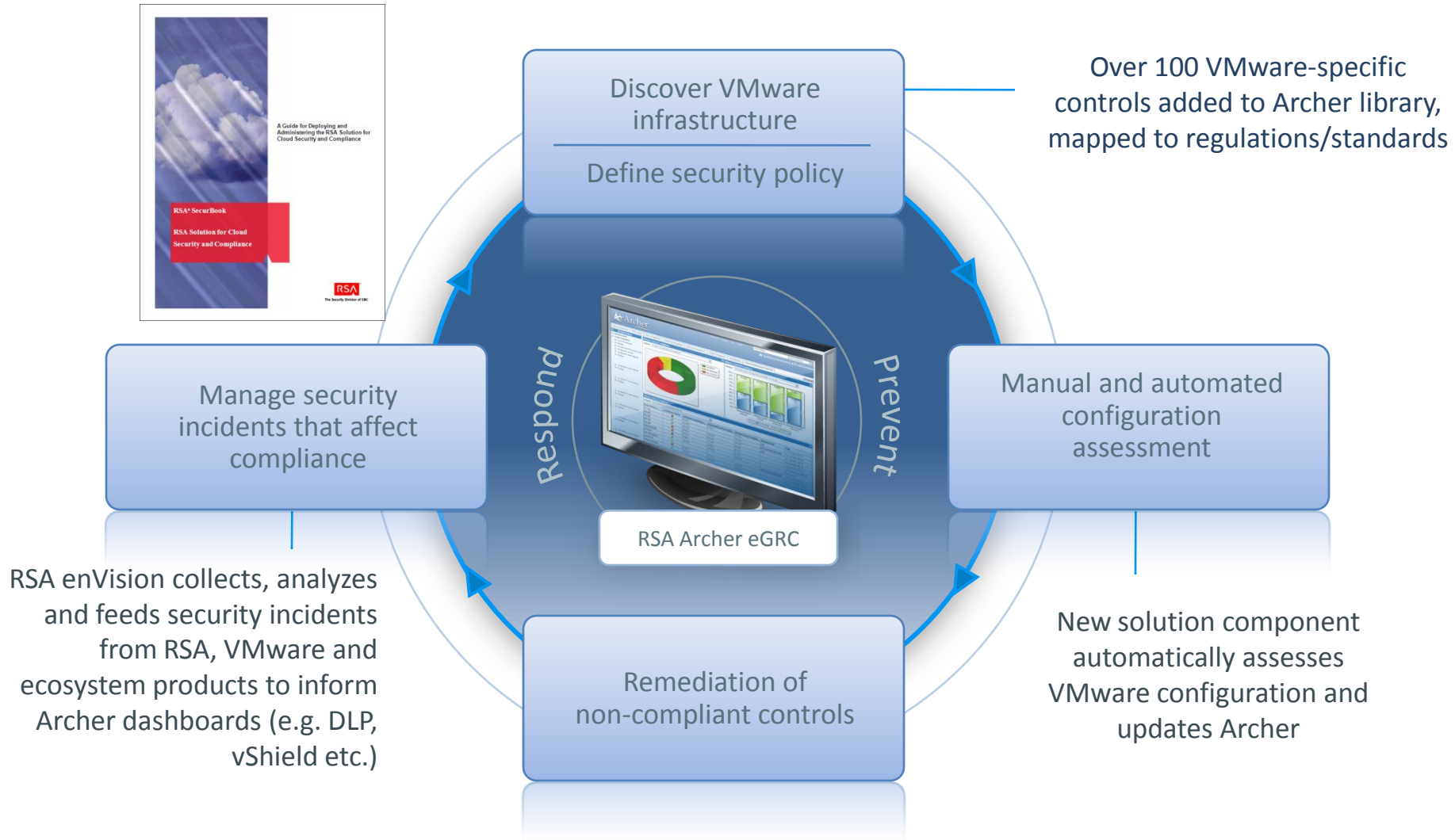
# Control and Visibility over *Identity*

- Increased potential points of exposure
  - Identities (individuals and machines)
  - Mobile devices
  - Social media platforms
- Verifying users in high-risk transactions
  - Instantaneous risk assessments
  - RSA Adaptive Authentication
- Detecting Fraudulent users inside clouds
  - RSA Transaction Monitoring

## Value of Unified ***Control and Visibility***

- Conventional Security Management
  - Too slow and rigid
  - Relies on manual process or human intervention
  - Unreliable and unscalable
  - Multiple silo's of implementation
- Automating Security and Compliance
  - Efficiency, control and scalability
  - Ensure services are secured to a common standard
  - Guidance from industry coalitions e.g. CSA  
([www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org))

# Example of Cloud Security and Compliance



# Cloud Security Alliance



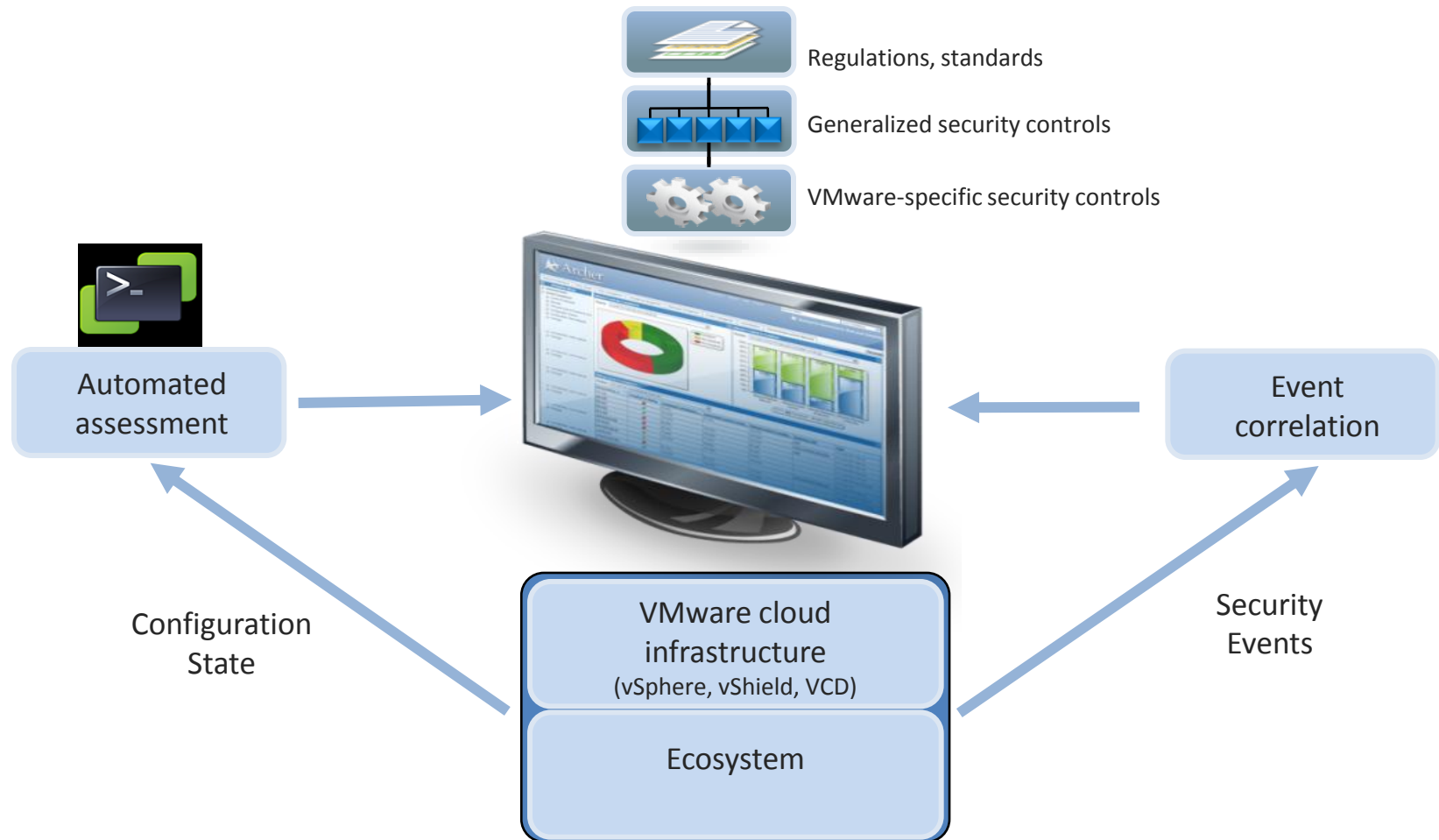
Cloud Security Alliance's 13 domains of focus for cloud computing

## Assessing Service Provider Compliance

RSA Solution for Cloud Security and Compliance aligns with CSA Consensus Assessment Questions by automating 195 questions that customers can issue to assess cloud service providers.



# Automating Cloud Security and Compliance

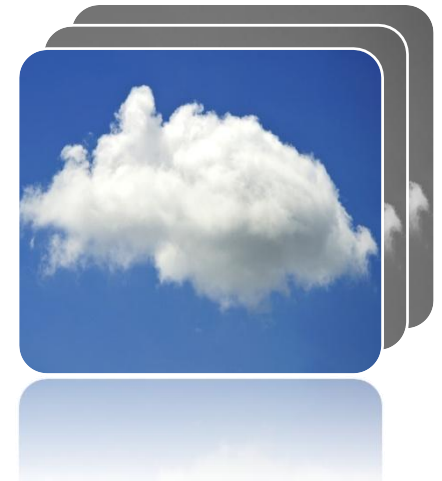


# Key Security Concerns in Leveraging Cloud Service Providers

Enterprises



Cloud Service Providers



- Secure federation of enterprise identities to cloud services
- Security and residency of the workloads in the cloud
- Confidentiality, integrity, availability, residency of data
- Visibility, control and compliance of assets in the cloud

# Cloud Trust Authority

Enterprises



Security & Compliance



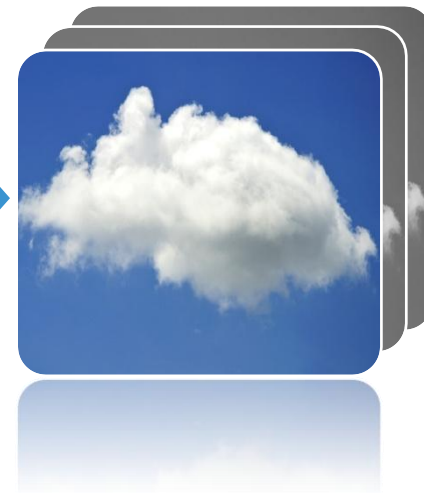
Identities

Infrastructure

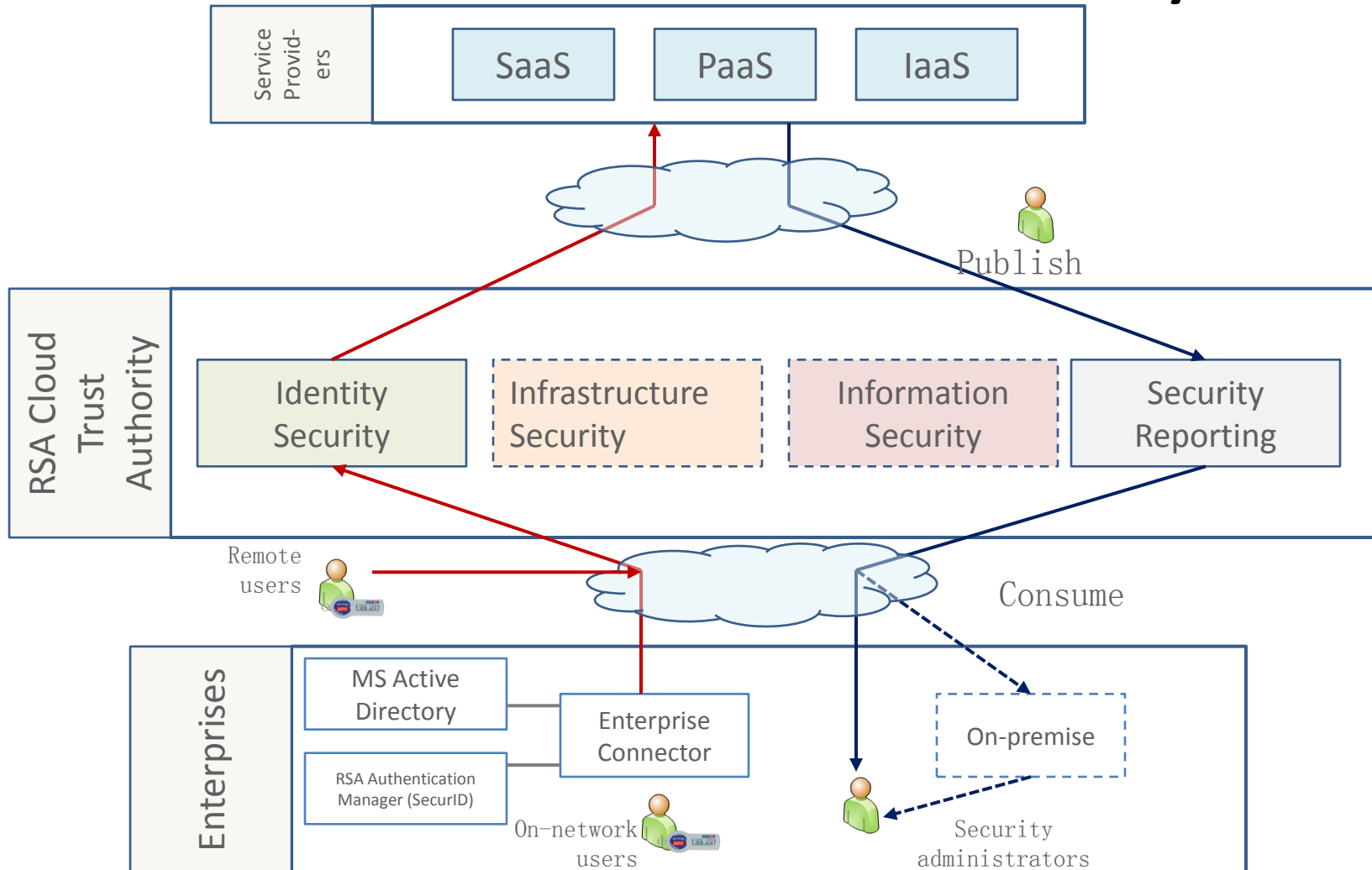
Information



Cloud Service Providers



# Cloud Trust Authority



# Security Reporting Service :

## Sample Report for a Cloud Provider

196 of 196 Completed

**CSA Cloud Assessment Initiative**

Actions

★ Questionnaire ID: 111221

Target: NewCloud.com

Due Date: 12/23/2010

Progress Status:  100%

History Log: [View History Log](#)

Overall Status:

Submitter: smith, bob

Submission Status: In Process [Edit](#)

Reviewer: smith, bob

Review Status: Awaiting Review [Edit](#)

▼ Quantitative Summary

Category	Correct	Incorrect	% Correct	Inherent Score	Residual Score	Open Findings
Compliance	15	1	94	15	15	0
Data Governance	16	0	100	16	16	0
Facility Security	9	0	100	9	9	0
General	1	0	100	1	1	0
Human Resources Security	4	0	100	4	4	0
Information Security	73	1	99	73	73	0
Legal	3	1	75	3	3	0
Operations Management	8	1	89	8	8	0
Release Management	6	0	100	6	6	0
Resiliency	11	1	92	11	11	0
Risk Management	13	0	100	13	13	0
Security Architecture	31	1	97	31	31	0
<b>TOTAL</b>	<b>190</b>	<b>6</b>	<b>97</b>	<b>190</b>	<b>190</b>	<b>0</b>



## The Bottom Line.....

- Cloud offers untold Business opportunity
- Don't wait for all the stars to line up....
- Security is a perceived risk and can be overcome
- Enterprise hybrid cloud may offer the perfect balance
- Real risk is not an IT risk but a business risk.....



THANK YOU