

# **RSA<sup>®</sup>CONFERENCE C H I N A 2012**

**RSA信息安全大会2012**

**THE GREAT CIPHER**

**MIGHTIER THAN THE SWORD**

**伟大的密码胜于利剑**



# The Pillar of Trust: Where Big Data Meets Security

**Branden Williams & Robert Griffin**  
RSA, the Security Division of EMC



CS-2002

Intermediate

**RSACONFERENCE**  
C H I N A 2012

# The Pillar of Trust

- The Big Data Security Challenge
- Securing Big Data
- Big Data's Role in Security

# The Big Data Security Challenge



# Who is already using Big Data?



Academic Research



Government



Industry



Health Sciences

# Case Study: Major Retailer



Market Trends



Customer Preferences



Supply Chain Optimization



Geographical Segmentation



# How Target Figured Out A Teen Was Pregnant Before Her Father Did

RSA CONFERENCE  
C H I N A 2012



# Who is after your Big Data Output?

RSA CONFERENCE  
C H I N A 2012

## Criminals

Petty  
criminals



*Unsophisticated*

Organized  
crime



*Organized, sophisticated supply chains (PII, financial services, retail)*

## Nation state actors



*PII, government, defense industrial base, IP rich organizations*

## Non-state actors

Terrorists



*PII, Government, critical infrastructure*

Anti-establishment  
vigilantes



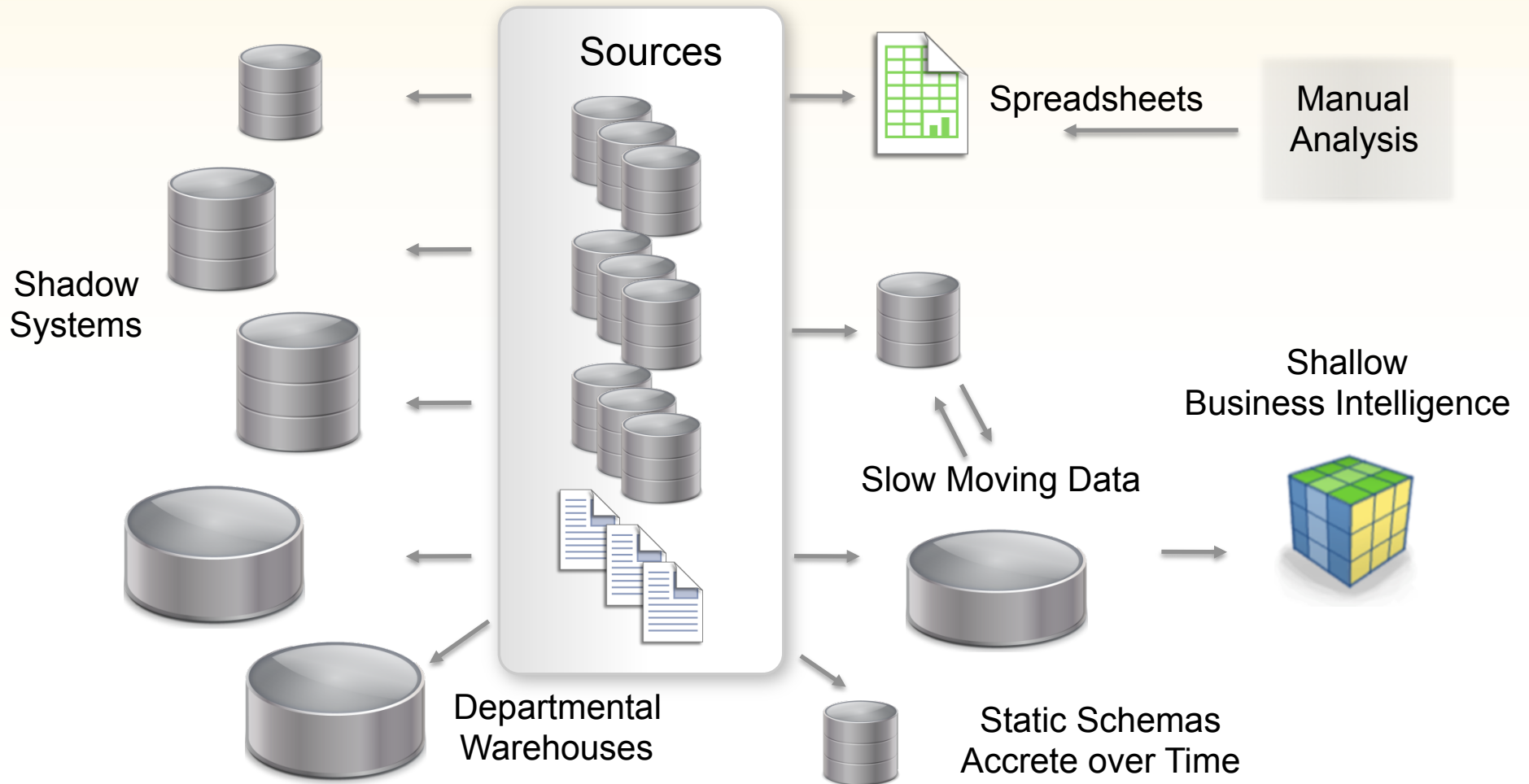
*"Hacktivists"  
Targets of opportunity*

RSA

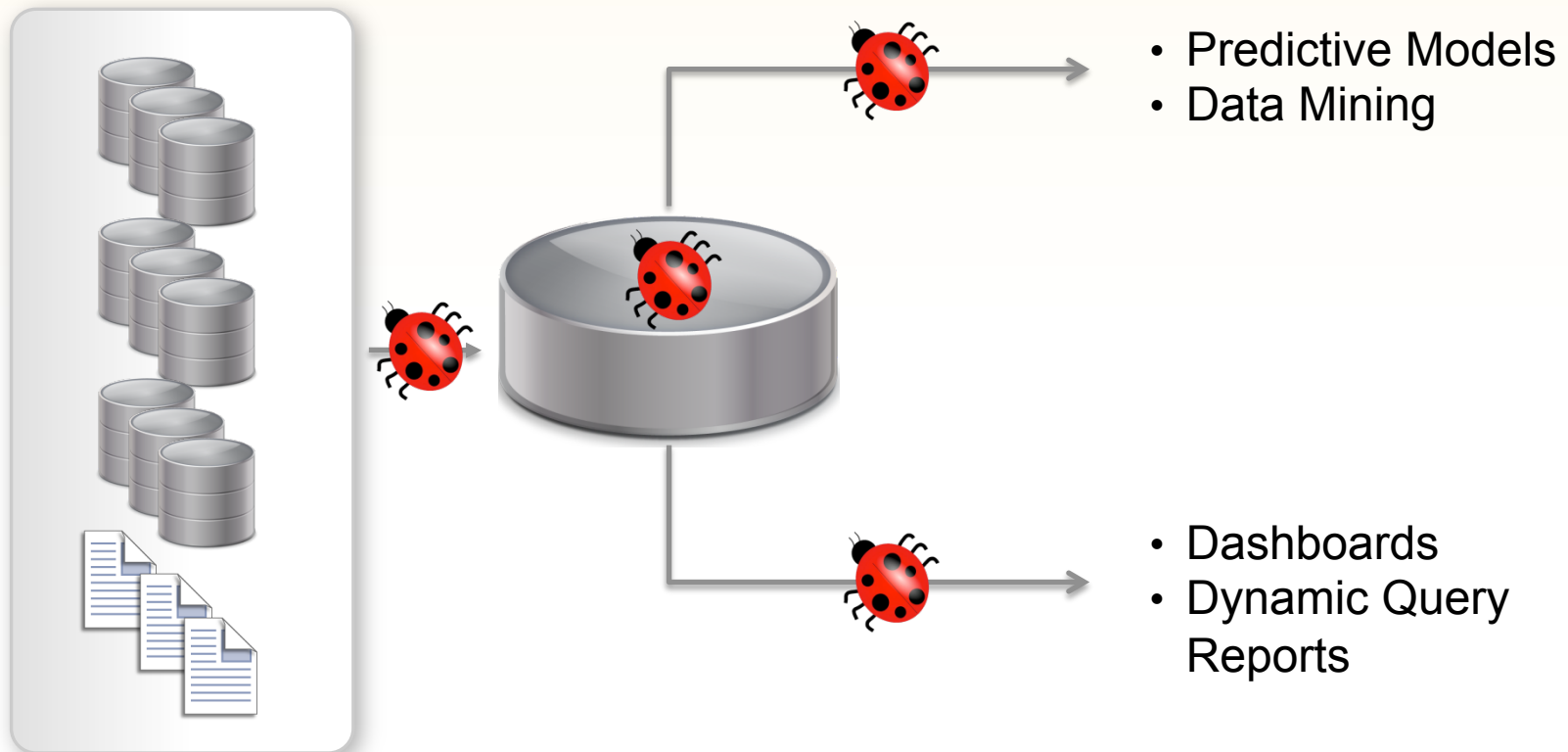
RSA信息安全大会2012



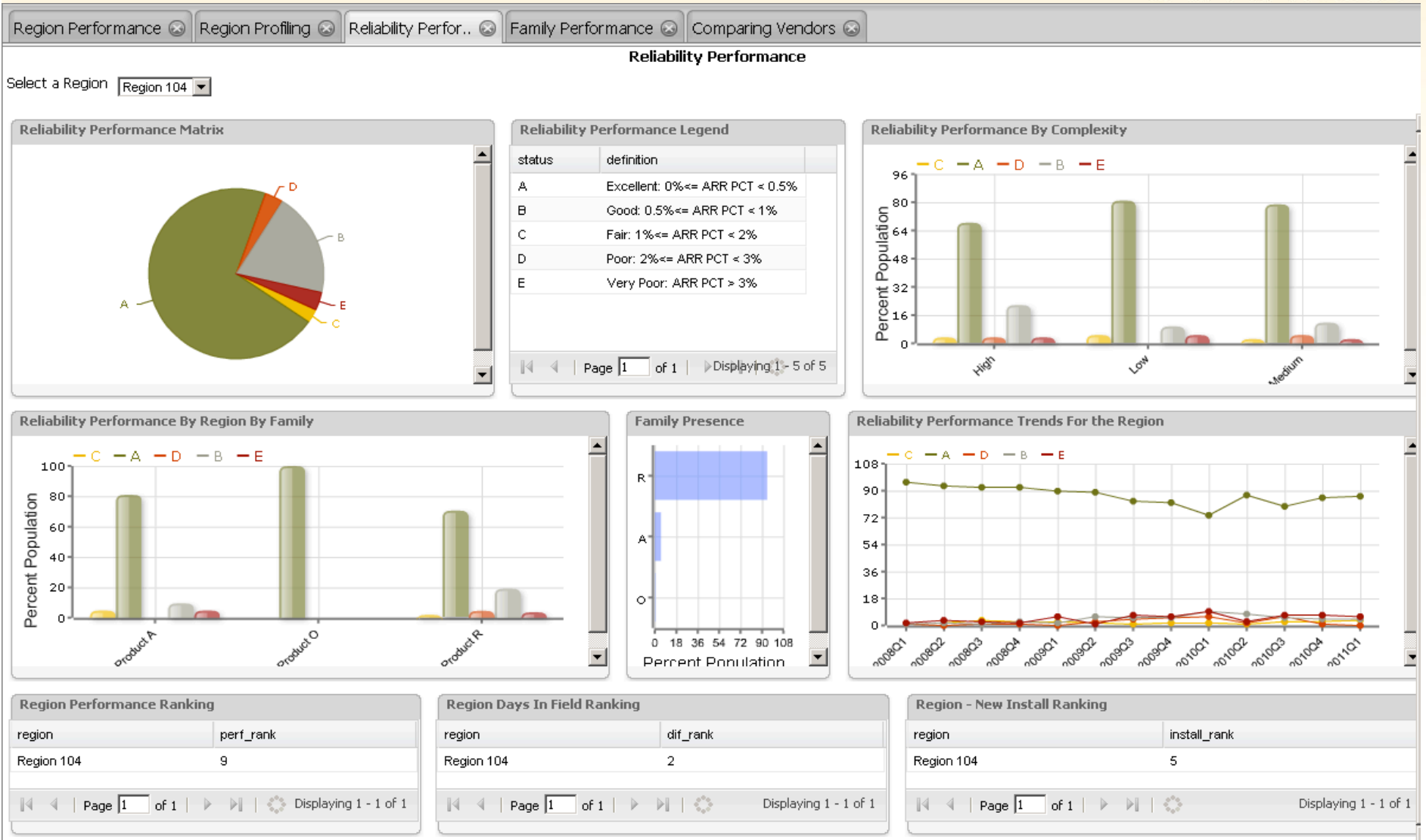
# Where does sensitive data live?



# Sensitive Analytics



# Sensitive Results

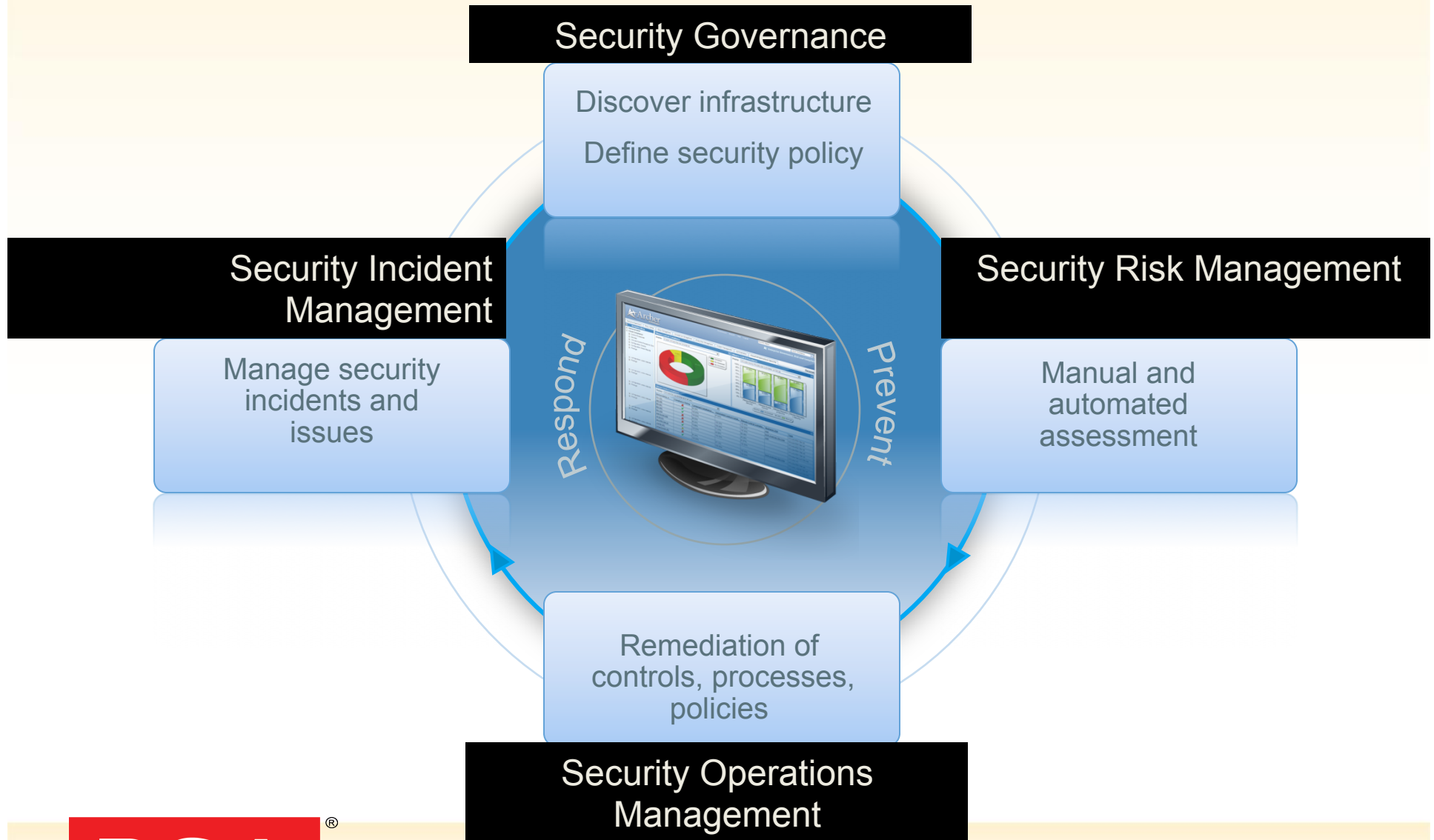


# Securing Big Data



# Securing Big Data is a Process

RSA CONFERENCE  
C H I N A 2012



RSA信息安全大会2012

# Security Governance

RSA CONFERENCE  
C H I N A 2012

- Define business objectives
- Define business-level risk targets
- Define business-critical assets

1



RSA Archer

**RSA**<sup>®</sup>

RSA信息安全大会2012

# Security Risk Management

Understand external and internal  
threat landscape

Identify vulnerabilities

Classify high-value assets

Assess security maturity

Establish target state

2



RSA<sup>®</sup>





# Security Operations Management



- Prioritize work by risk
- Add security controls where needed
- Maximize monitoring and visibility
- Manage events



# Security Incident Management

RSA CONFERENCE  
C H I N A 2012

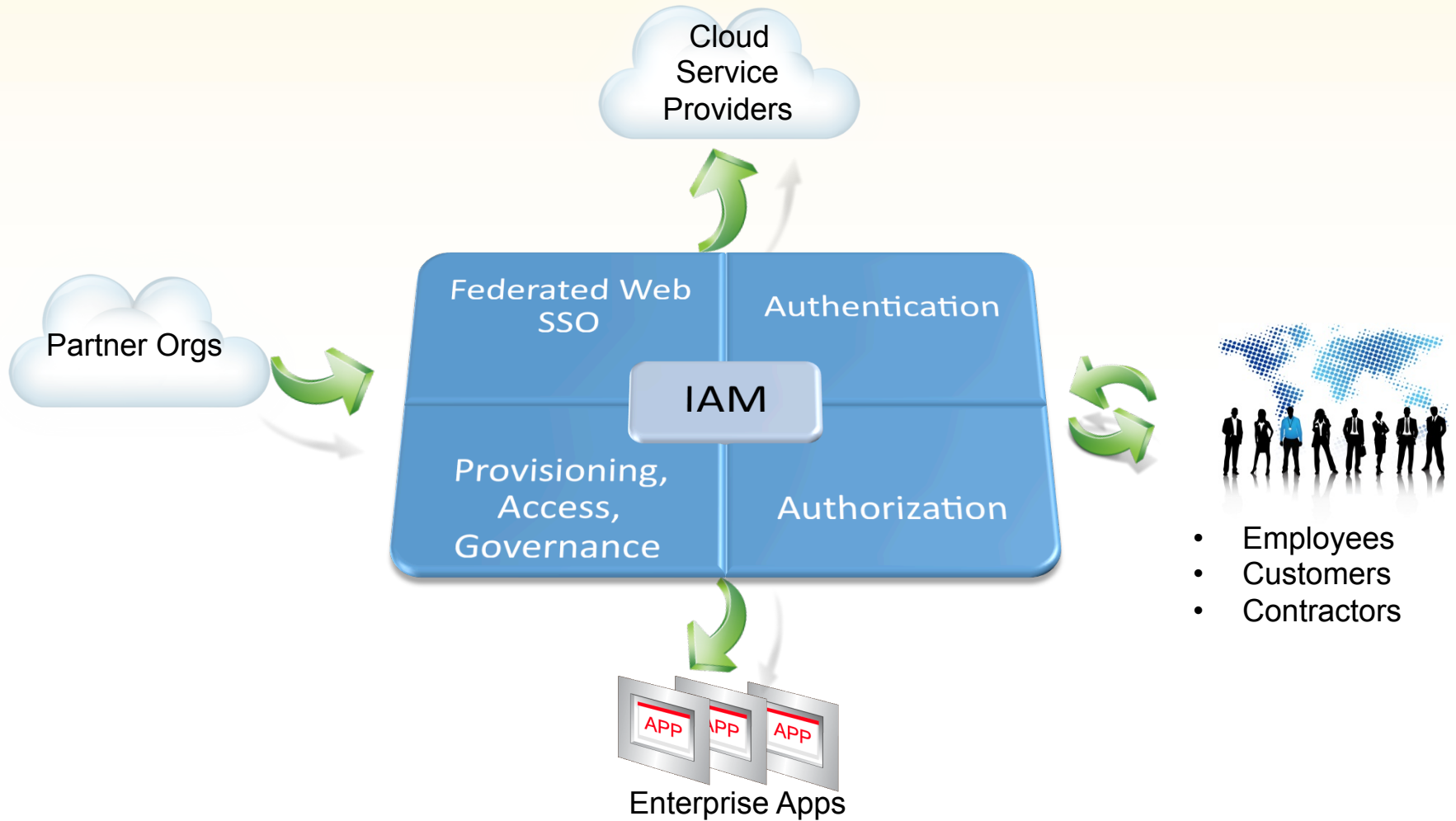


4

- Identify relevant security events
- Prioritize by business impact
- Report to business owners
- Reassess business risk and critical assets

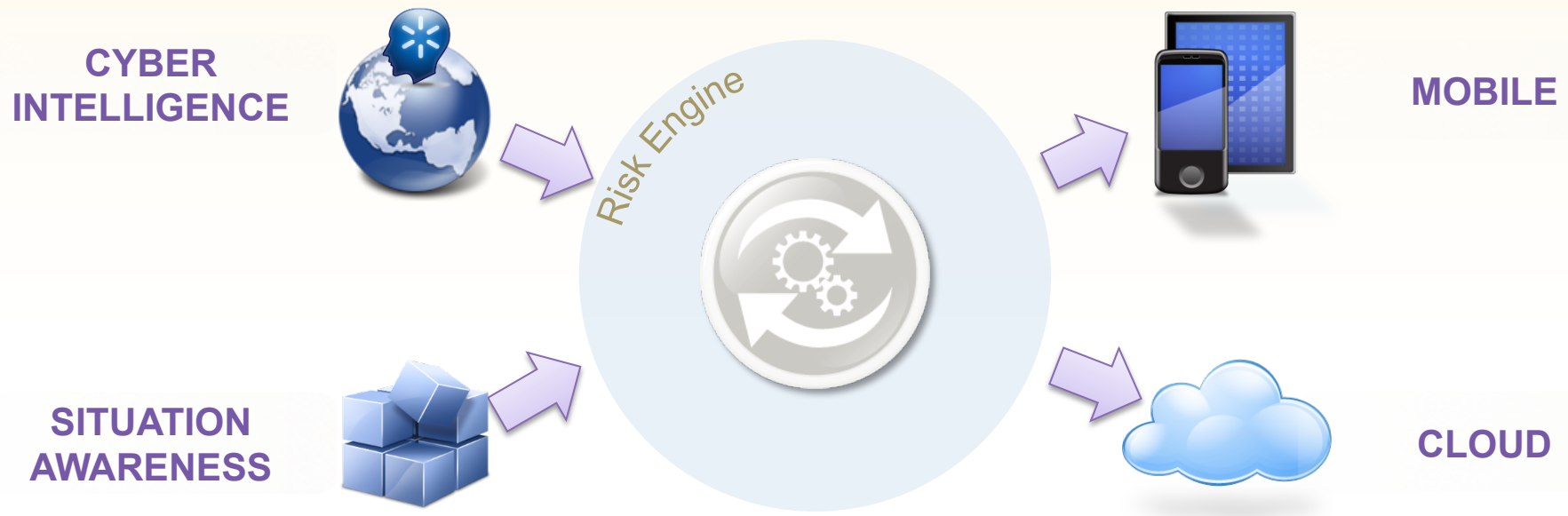


# Control who accesses the data



# Use Risk-based Adaptive Controls

RSA CONFERENCE  
C H I N A 2012



- Adaptive Identity Controls
- Adaptive Data Controls



# Big Data's Role in Security



# Visibility enables Analytics

RSA CONFERENCE  
C H I N A 2012



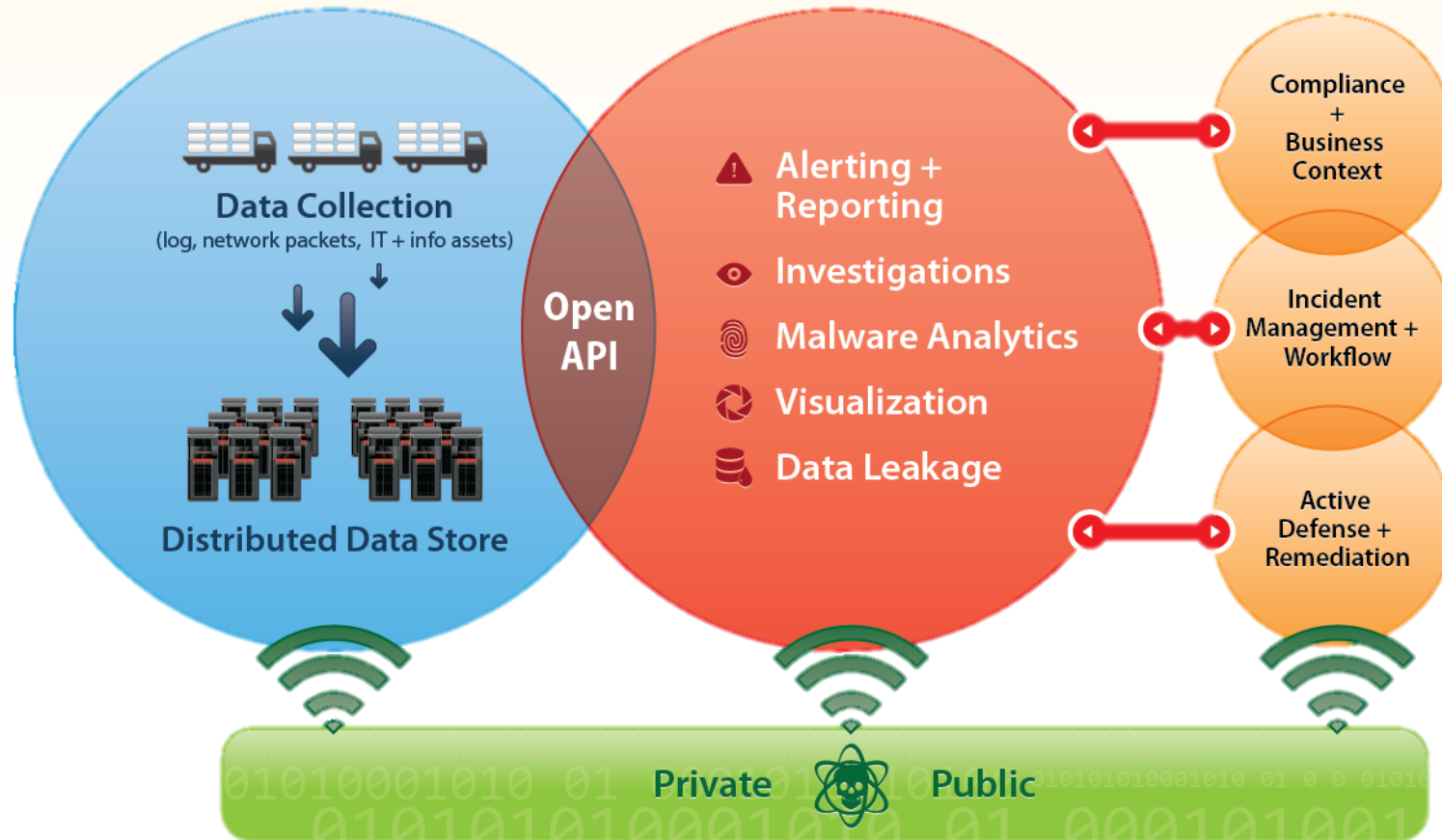
RSA信息安全大会2012

# Big Data Analytics is Essential to Security

## BIG DATA

## ANALYTICS

## GOVERNANCE





Thank You



RSACONFERENCE  
C H I N A 2012