



Games of Keys and Clouds: Finding a (Nash) Equilibrium of Trust

Robert W. Griffin

RSA, the Security Division of EMC

Session ID: **STAR-303**

Session Classification: Advanced


RSACONFERENCE
EUROPE 2012

Agenda

- The challenge of key management for the hybrid cloud
- Key management models for the hybrid cloud
- Making the deployment decision
 - Cost/benefit
 - Defender/attacker games
 - Security investment game
- Conclusions



Key management has a role in all cloud models

<p>Cloud Applications Software-as-a-Service</p>	  
<p>Cloud Software Development Platform-as-a-Service</p>	  
<p>Cloud-based Infrastructure Infrastructure-as-a-Service</p>	      



Common Key Management Issues

- Ownership of the keys
- Protection of keys in transit
- Protection of keys at rest
- Trust establishment
- Managing access to keys
- Defining and propagating key policy
- Managing key life-cycle
- Visibility of services



What is there to worry about in the cloud?

Use of encryption is rare:

- Who can see your information?

Virtual volumes and servers are mobile:

- Your data is mobile — has it moved?

Rogue servers might access data:

- Who is attaching to your volumes?

Rich audit and alerting modules lacking:

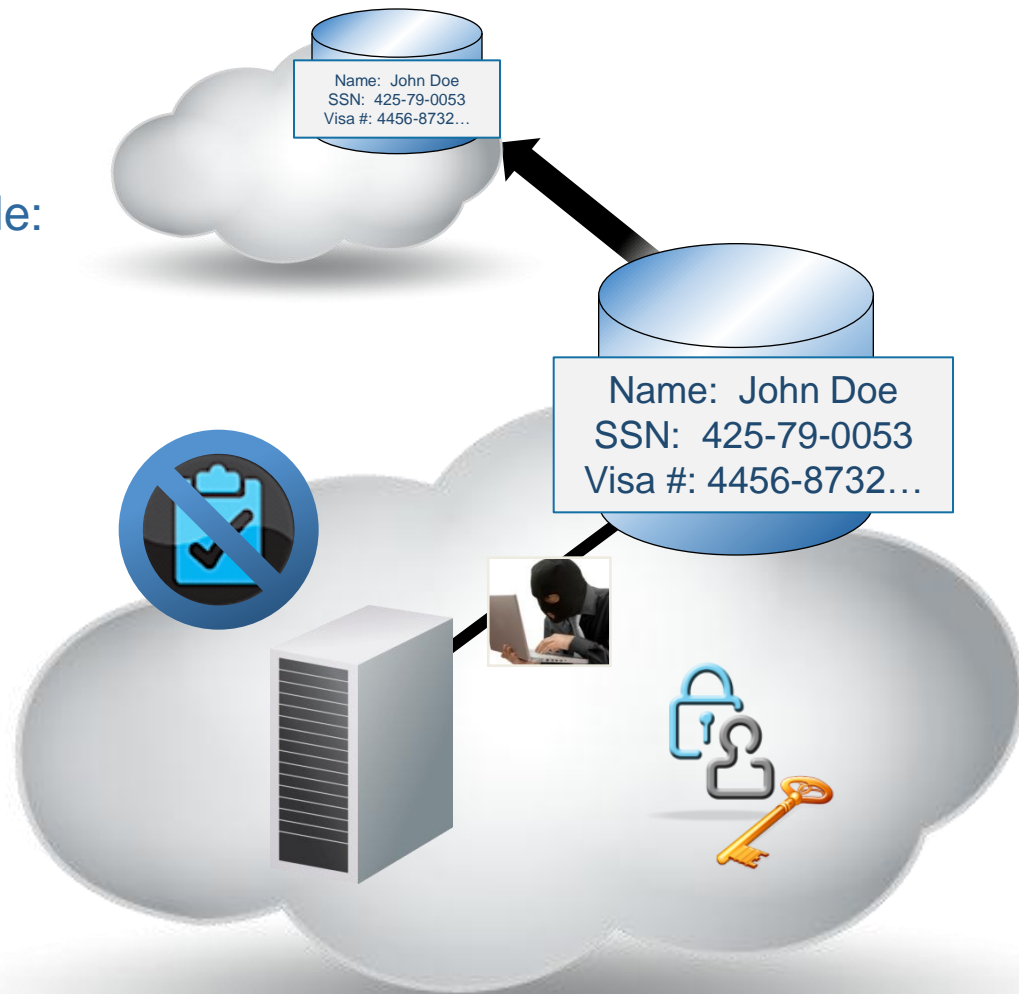
- What happened when you weren't looking?

Virtual volumes contain residual data:

- Are your storage devices recycled securely?

Forensics are more complex.:

- Where is the detailed information you need?



Cloud Security Alliance (CSA) Top Threats

- **Threat #1:** Abuse and Nefarious Use of Cloud Computing
- **Threat #2:** Insecure Interfaces and APIs
- **Threat #3:** Malicious Insiders
- **Threat #4:** Shared Technology Issues
- **Threat #5:** Data Loss or Leakage
- **Threat #6:** Account or Service Hijacking
- **Threat #7:** Unknown Risk Profile

<http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>



Key Management Models for the Hybrid Cloud



Cloud Key Management Models

Enterprise

- Keys created, used, stored and managed by enterprise

Hybrid

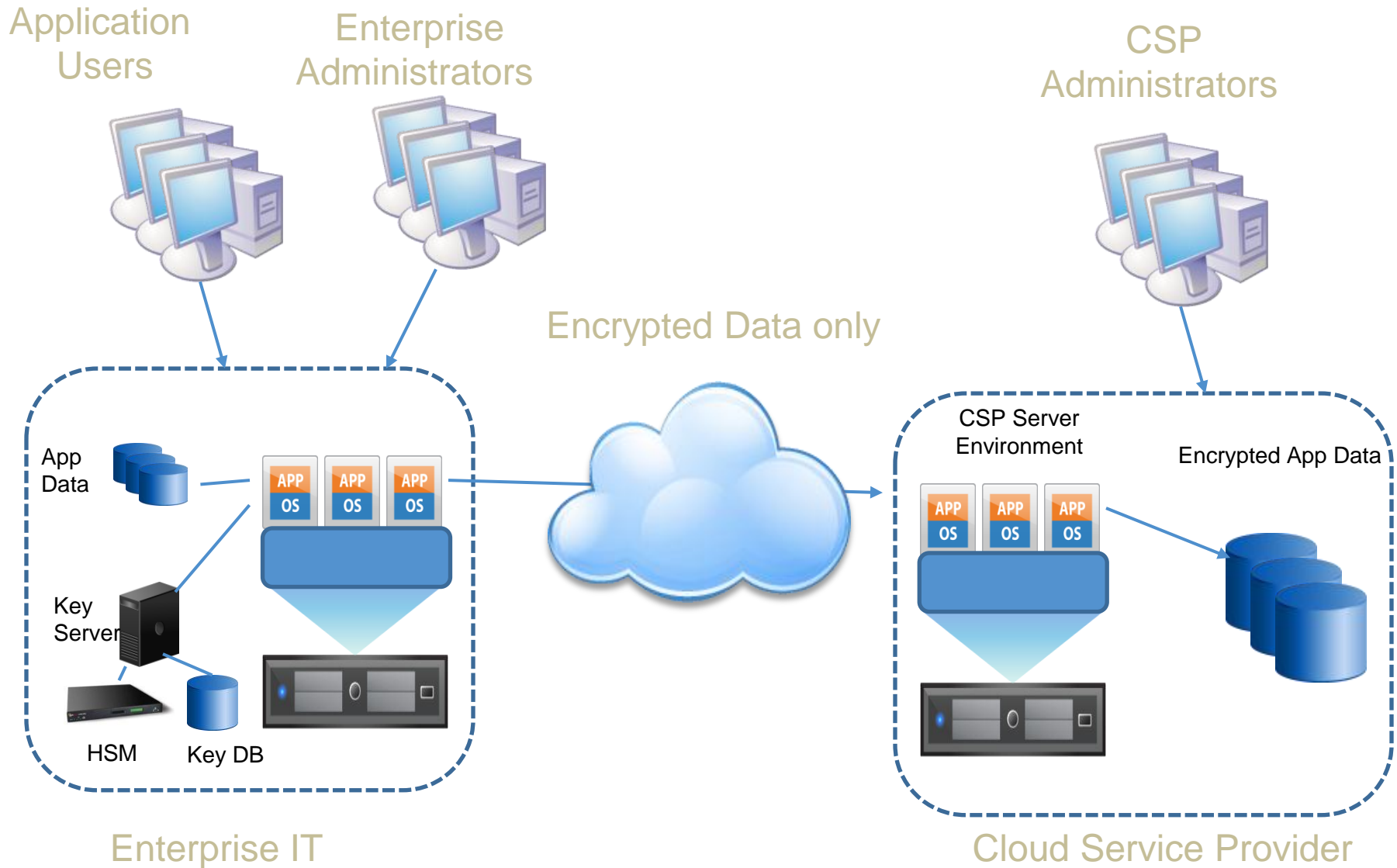
- Keys created, stored and managed by enterprise, but used by CSP

CSP

- Keys created, used, stored and managed by CSP

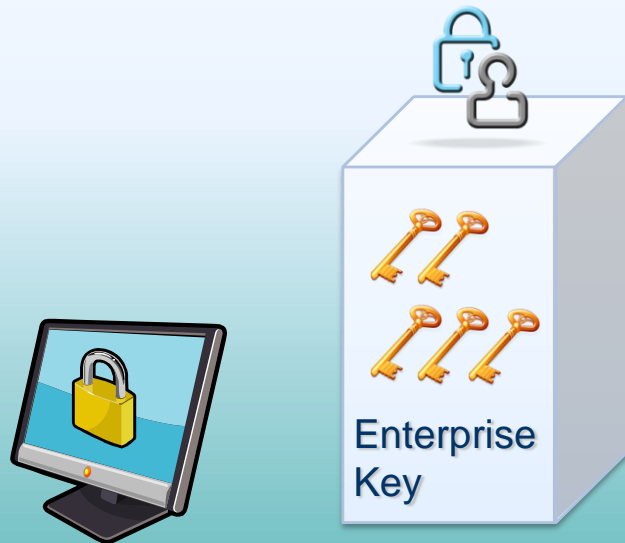


Model 1: Enterprise Key Management

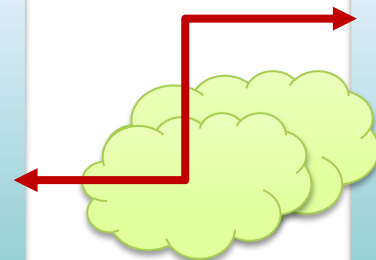


Example: TrendMicro SecureCloud™

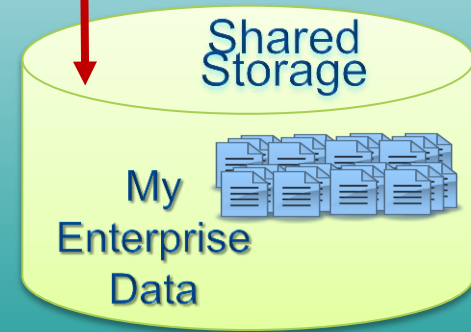
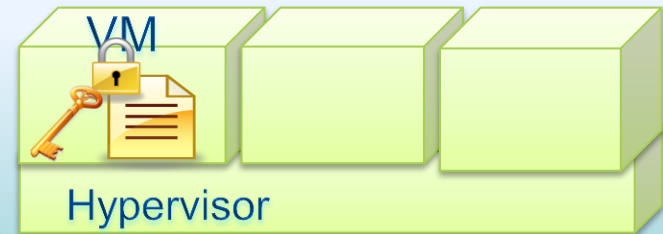
Enterprise Datacenter or SaaS Offering



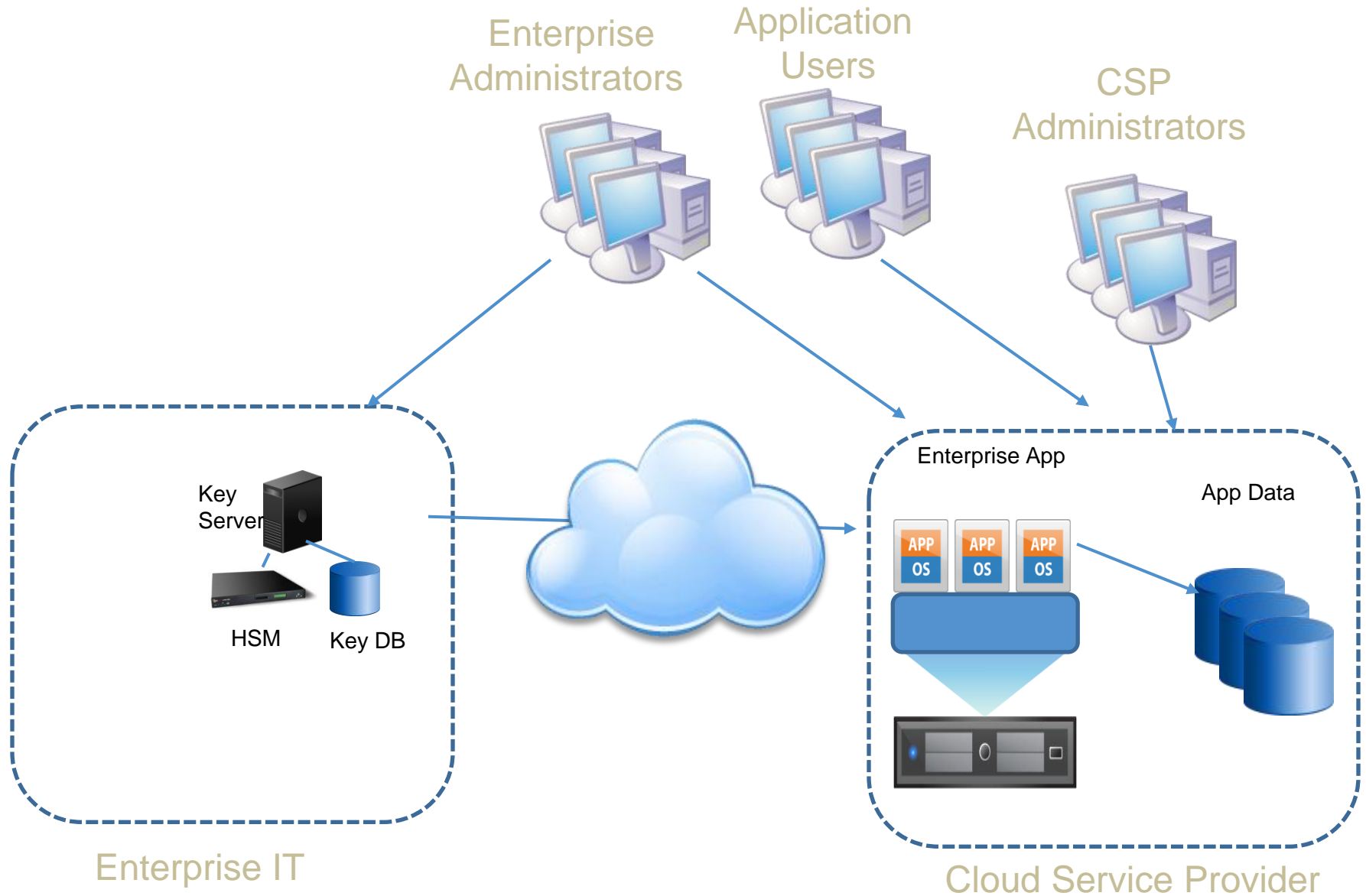
Trend Micro
Cloud
Security
Console



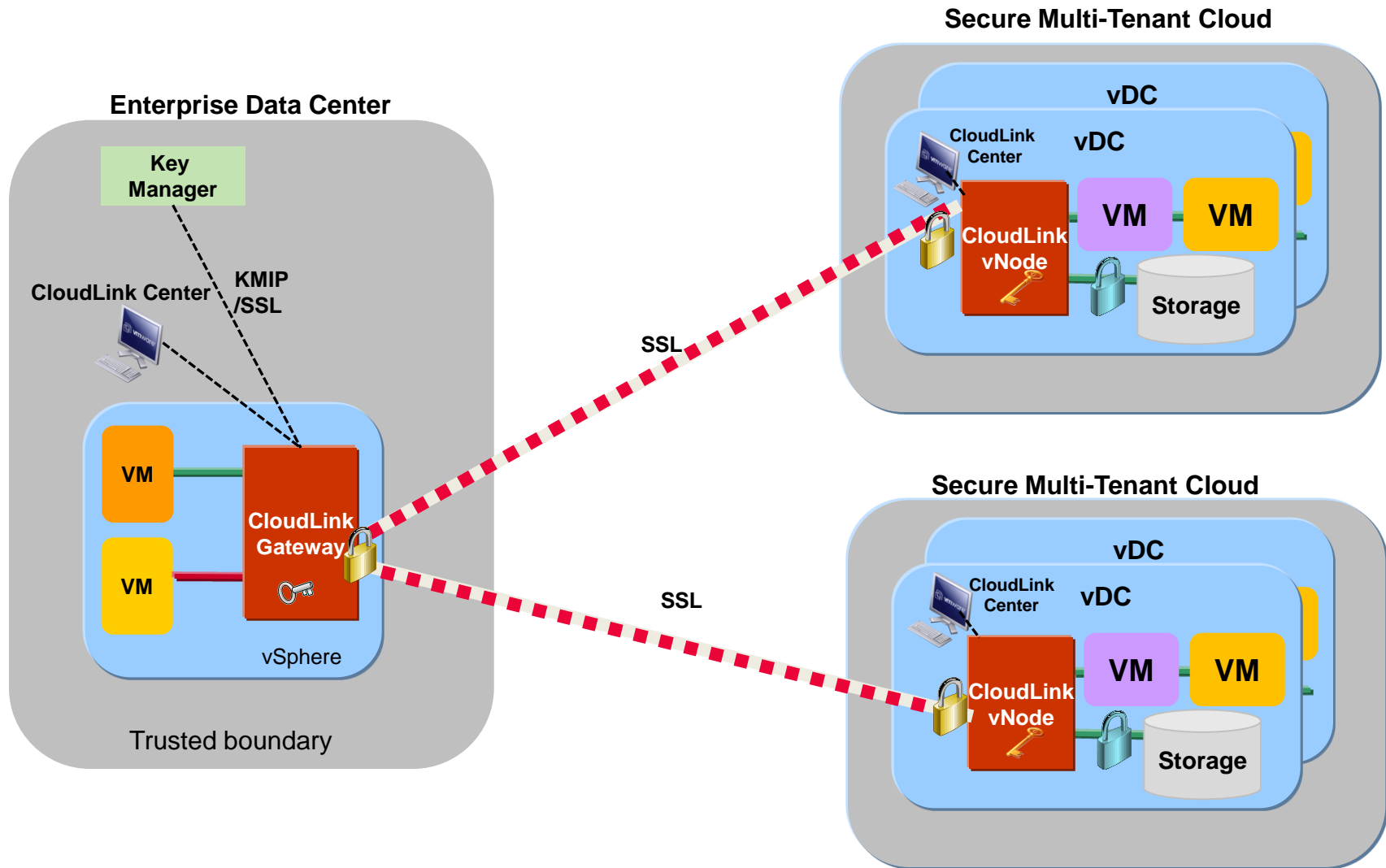
Cloud Service Provider



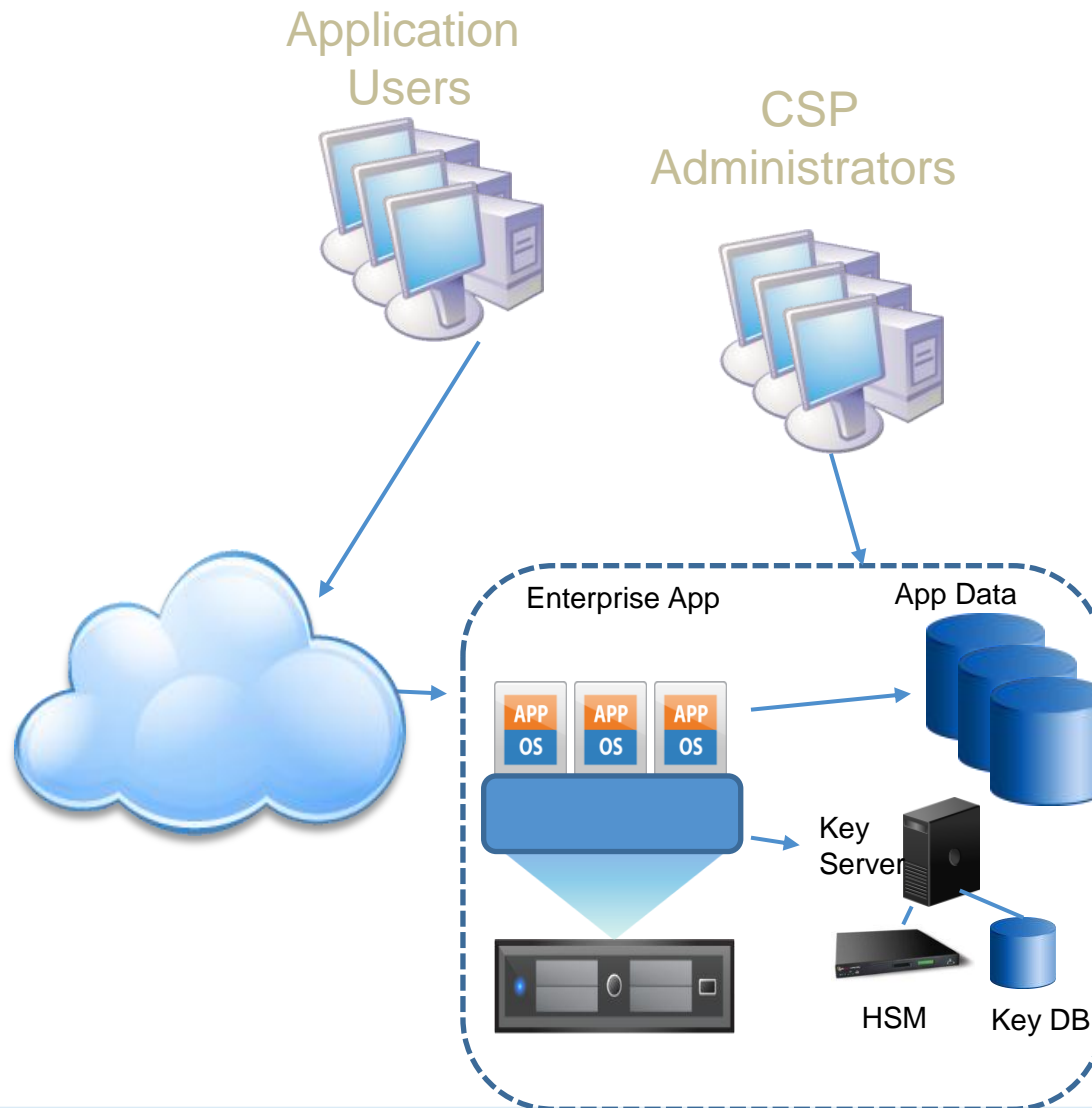
Model 2: Hybrid Key Management



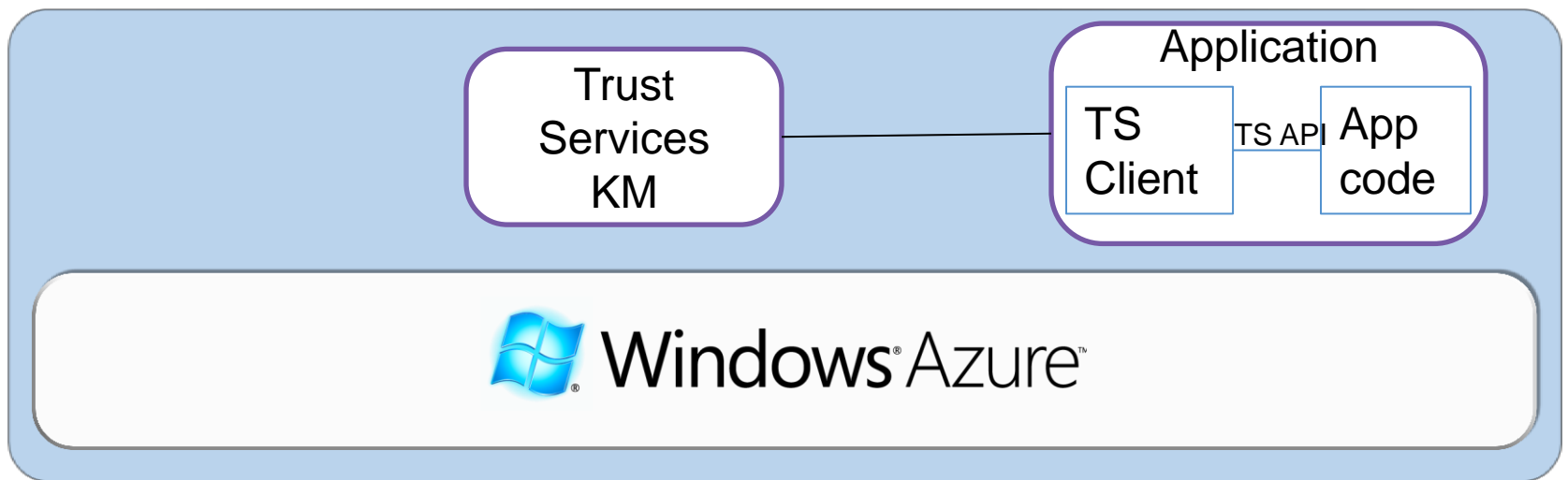
Example: Afore Solutions CloudLink™



Model 3: CSP Key Management



Example: Windows Azure™ Trust Services



Making the Deployment Decision



Cost/Benefit Analysis

- “There are many benefits that explain **why** to migrate to clouds
 - Cost savings, power savings, green savings, increased agility in software deployment
- Cloud security issues may drive and define **how** we adopt and deploy cloud computing solutions
 - Private clouds may have less **threat exposure** than community clouds which have less threat exposure than public clouds.
 - All else being equal, massive public clouds may be more **cost effective** than large community clouds which may be more cost effective than small private clouds.”

Peter Mell / Tim Grance, “Effectively and Securely Using the Cloud Computing Paradigm”, 2009



Security Posture

Enterprise

- Offers significant operational and security benefits by retaining control of keys and key-related operations.
- Represents significant investment and expertise in effective security processes, personnel and technology

Hybrid

- Enables enterprise to take greater advantage of CSP resources for data processing and security.
- Exposes data and keys to new risk in motion, at rest and in use.

CSP

- Provides significant reduction in investment and expertise in key-related processes, personnel and technology.
- Increases difficulty of oversight, incident response, audit and forensics.



Attacker / Defenders Games: Nash Equilibrium in the Battle of the Bismarck Sea

A Nash equilibrium is a point in which neither player benefits by deviating from it in isolation



Battle of the Bismarck Sea, 1943

	Japanese sail north	Japanese sail south
Allies search north	2,-2	2,-2
Allies search south	1,-1	3,-3

Source: O. G. Hayward, Jr. 1954



Using Attacker / Defender Games

- Insight from Nash equilibria in defender/attacker games can be used in making deployment decisions
 - Strategies encouraging attacker defection
 - Strategies strengthening defender response
- Differences in defender/attacker games for enterprise and CSP may reveal different Nash equilibria for the enterprise options for key management for the cloud
 - Segregation of application at CSP and key store at enterprise increases the number of environments that an attacker must compromise
 - Segregation of tenant key stores at CSP increases the number of credentials that an attacker must compromise
 - Consolidation of key management in CSP key manager increases visibility into attacker activity



Attacker / Defender Games

- “A game theoretic framework for evaluation of the impacts of hackers diversity on security measures [Moayedi, Azgomi] published in 2011
 - Paper uses Nash equilibria in defender/attacker games with diverse attackers and full knowledge in participants to evaluate security measures.
- “FLIPIT: The Game of “Stealthy Takeover”[Van Dijk, Oprea, Juels, Rivest] published in 2012
 - Paper describes game-theoretic framework to model security scenarios with stealthy, complete compromise of critical resource.
 - Nash equilibria provide insights regarding defender strategy to encourage attacker defection.



Flipit

- Flipit creates a simultaneous game between attacker and defender.
 - Players don't know when the other player has moved.
 - Players take control of a mutually desirable resource by moving, including paying a certain cost for the move
 - Goal of each player is to maximize the fraction of time the player controls the resource minus the average move cost.
- Implications for key management are derivable for various combinations of strategies and phases. For example:

Forcing the attacker to drop out We make the observation that if the defender plays extremely fast (periodic with rate $\alpha_0 > 1/2k_1$), the attacker's strongly dominant non-adaptive strategy is to drop out of the game. The reason is that in each interval between defender's consecutive moves (of length $\delta_0 = 1/\alpha_0 < 2k_1$), the attacker can control the resource on average at most half of the time, resulting in gain strictly less than k_1 . However, the attacker has to spend k_1 for each move, and therefore the benefit in each interval is negative.



Conclusions from Flipit

- The modeling provided by Flipit results in several general conclusions about the attacker/defender relationship:
 - Aggressive play by the defender can motivate the attacker to drop out of the game
 - Any amount of feedback received during the game about the opponent benefits a player
- These conclusions can be applied to decisions about key management in the cloud.
 - Immediate detection of stolen keys and extensive collection of attack information are essential. For many enterprises, this will favor entrusting keys to a cloud service provider that can afford the expertise and technology to support this capability.
 - The cost of aggressive pursuit of attackers (complementing aggressive key rotation, segregation of admin duties, virtual machine deployment etc) may be more readily borne by cloud service providers.



Using Investment Games

- “Information Security Investment Game with Penalty Parameter” [Sun] published in 2008 (IEEE)
 - Paper identifies Nash equilibria related to security investment by two participants
 - Also explores the impact of strategic moves on changing the Nash equilibria revealed by the analysis



Payoffs

organization one	organization two	
	investment	no investment
investment	$E - C + I,$ $E - C + I$	$E - C - qL + I,$ $E - pL$
no investment	$E - pL,$ $E - C - qL + I$	$E - pL - (1 - p)qL,$ $E - pL - (1 - p)qL$

E = normal proceedings of organization

C = incremental cost of security investment

I = intangible asset resulting from security investment

L = information security loss suffered by the organization

pL = probability of information security loss from organization itself

qL = probability of information security loss resulting from other organization



Identifying the Nash Equilibrium for Pure Strategy

$$\begin{cases} E - C + I > E - pL \\ E - C - qL + I > E - pL - (1 - p)qL \end{cases}$$

To simplify the mathematical expression, we

$$\begin{cases} C < pL + I \\ C < p(1 - q)L + I \end{cases}$$

That is,

$$C < p(1 - q)L + I$$

For the Nash Equilibrium analysis of pure strategy, the necessary and sufficient condition for the two organizations to select investment strategy is no matter what strategy the other player chooses, the investment strategy is always better than the strategy of no investment.



Prisoners' Dilemma

organization one	organization two	
	investment	no investment
investment	$E - C + I,$ $E - C + I$	$E - C - qL + I,$ $E - pL$
no investment	$E - pL,$ $E - C - qL + I$	$E - pL - (1 - p)qL,$ $E - pL - (1 - p)qL$



Changing the Equilibrium through Penalty

$$\begin{cases} E - C + I > E - pL - P \\ E - C - qL + I > E - pL - (1 - p)qL - P \end{cases}$$

To simplify the above expression, we get

$$\begin{cases} P > C - I - pL \\ P > C - I - pL + pqL \end{cases}$$

Further, that is,

$$P > C - I - pL + pqL$$

This fruitful result reveals that if the investment cost can not satisfy the demand $C < p(1 - q)L + I$, we can make the penalty parameter $P > C - I - pL + pqL$ to force the defender organization to invest in information security.



Strategic Moves and Changing the Game

- Enterprise / CSP relationship is a complex system in which penalty as incentive has undesirable consequences
 - Focus on penalty avoidance rather than security by CSP
 - Information concealment by CSP
 - Adversarial relationship can encourage Prisoners' Dilemma
- Possible to re-define relationship as coordination game
 - Strong mutual benefit in strategic approaches and/or Schelling points that reduce risk of information exposure
 - Signal / promise investment
 - Screening risk areas such as insufficient segregation of duty
 - Reinforcement of assumptions about unavoidability of compromise



Coordination Game

organization one	organization two	
	investment	no investment
investment	$E - C + I,$ $E - C + I$	$E - C - qL + I,$ $E - pL$
no investment	$E - pL,$ $E - C - qL + I$	$E - pL - (1 - p)qL,$ $E - pL - (1 - p)qL$



Conclusion



Conclusions

- Insights from game theory provide a valuable complement to decision theory cost/benefit analysis
 - Identifies important considerations that are not immediately visible in cost/benefit or security posture
- Game theory offers valuable insights into the deployment decisions for key management for the cloud
 - Reveals significant benefits in visibility through consolidation of key management by CSP
 - Shows critical value in approaches that reinforce coordination between enterprise and CSP
 - New research with RSA Labs and Ron Rivest on “Applying FlipIt” will be presented at the Gamesec conference (Budapest) in November 2012.



Applying this Session

- In the first three months following this presentation you should:
 - Examine your cloud key management strategy in the light of the ideas in this session
 - Develop your understanding of game theory and cyber security (see resources on next slide)
 - Send comments / questions to me regarding the ideas discussed in this session (robert.griffin@rsa.com)
- Within six months you should:
 - Identify a security issue for which game theory may be a useful tool
 - Experiment with applying game theoretic approaches to that security issue



Resources

- Bruce Schneier: Liars and Outliers
- RSA “Speaking of Security”
(<http://blogs.rsa.com/author/griffin/>)
- Gamesec Conference
(<http://www.gamesec-conf.org/>)
- Fliplt paper
(<http://www.rsa.com/rsalabs/node.asp?id=3911>)





Thank You