RSA CONFERENCE
CHINA 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

密钥与云：

混合云中的密钥管理战略

Robert W. Griffin 博士
RSA, The Security Division of EMC

RSA CONFERENCE CHINA 2012

课程安排

- 云中的密钥管理问题
- 私有、公共和混合云中的密钥管理模型
- 针对云的密钥管理协议
- 需要解决哪些问题

所有云模型都涉及密钥管理

云 应用程序 软件即服务	Google Docs　salesforce.com Success. Not Software.　Cisco webex
云 软件开发 平台即服务	amazon web services　Google　Windows Azure
基于云 基础架构 基础架构即服务	Telstra　Sun POWERED BY Network.com　hp invent　at&t　SAVVIS　IBM　amazon web services

常见密钥管理问题

- 密钥的所有权
- 传输中密钥的保护
- 静态密钥的保护
- 建立信任
- 管理对密钥的访问
- 定义并传播密钥策略
- 管理密钥生命周期
- 服务的可视性

在云中担心什么？

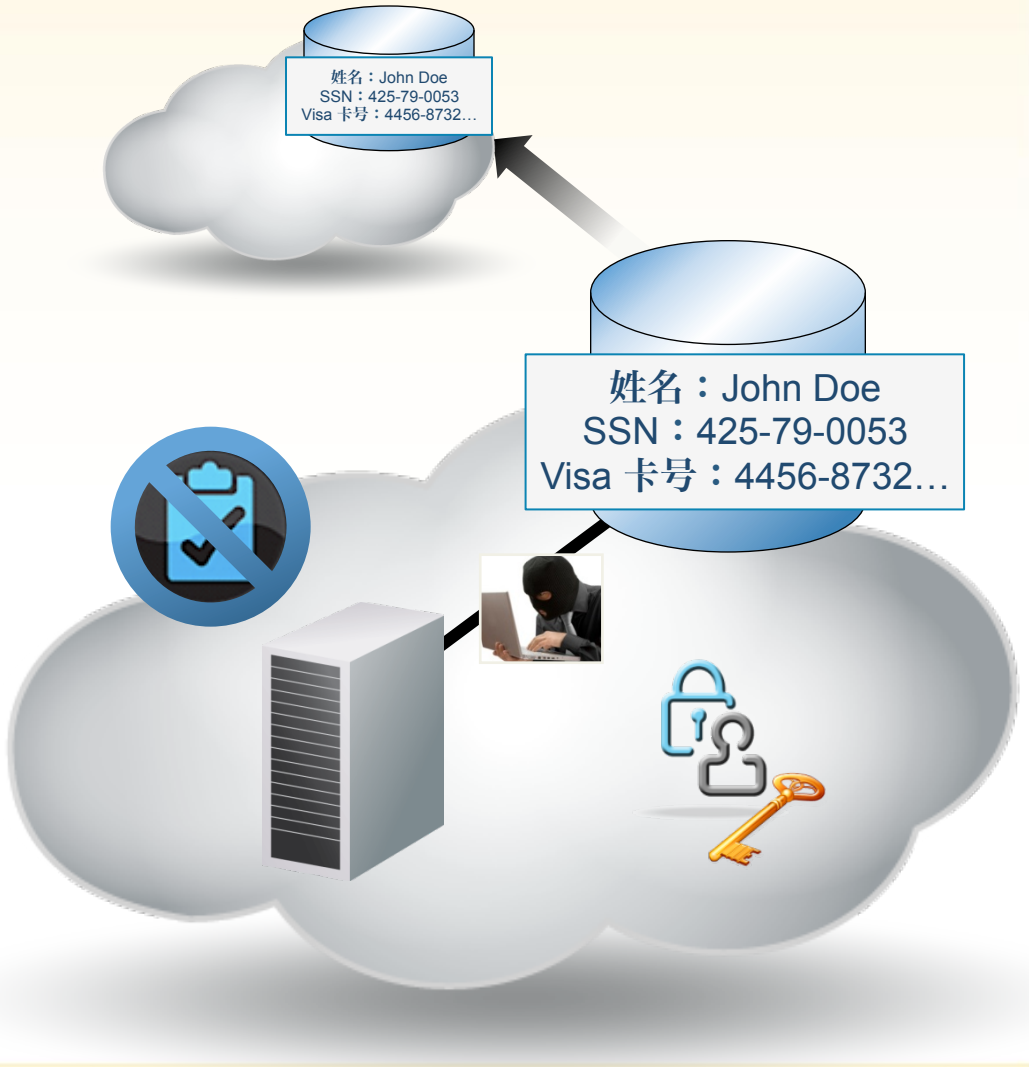
很少使用加密：
- 谁可以看到您的信息？

虚拟卷和虚拟服务器具有移动性：
- 您的数据具有移动性 — 它改变位置了吗？

流氓服务器可能会访问数据：
- 谁挂接到了您的卷上？

缺少丰富的审核和警报模块：
- 在您未照看期间发生了什么？

虚拟卷包含残留数据：
- 您的存储设备是否安全地进行了回收？



CSA 统计的几大威胁

- 威胁 1：滥用和以邪恶方式使用云计算
- 威胁 2：不安全的接口和 API
- 威胁 3：心怀恶意的内部人员
- 威胁 4：共享技术问题
- 威胁 5：数据丢失或泄露
- 威胁 6：帐户或服务劫持
- 威胁 7：未知风险特征

http://www.cloudsecurityalliance.org/topthreats/csathreats.v11.0.pdf

威胁 1：滥用和以邪恶方式使用云计算

RSA CONFERENCE CHINA 2012

问题：

云计算提供商 (IaaS) 频频成为攻击目标，部分原因是他们的注册环节相对薄弱，系统允许匿名制，而且提供商的防欺诈检测能力有限。

迄今为止发生的事情：

- IaaS 服务托管了 Zeus 僵尸病毒、InfoStealer 木马病毒，以及可能导致 Microsoft Office 和 Adobe PDF 滥用的下载内容。
- 僵尸曾使用 IaaS 服务器提供命令和控制功能。
- 垃圾邮件仍旧是问题 — 作为防御措施，整段的 IaaS 网络地址被公布为黑名单。

威胁 2：不安全的接口和 API

问题：

依赖于一组薄弱的接口和 API 让组织面临各种与保密性、完整性、可用性和责任划分相关的安全问题。

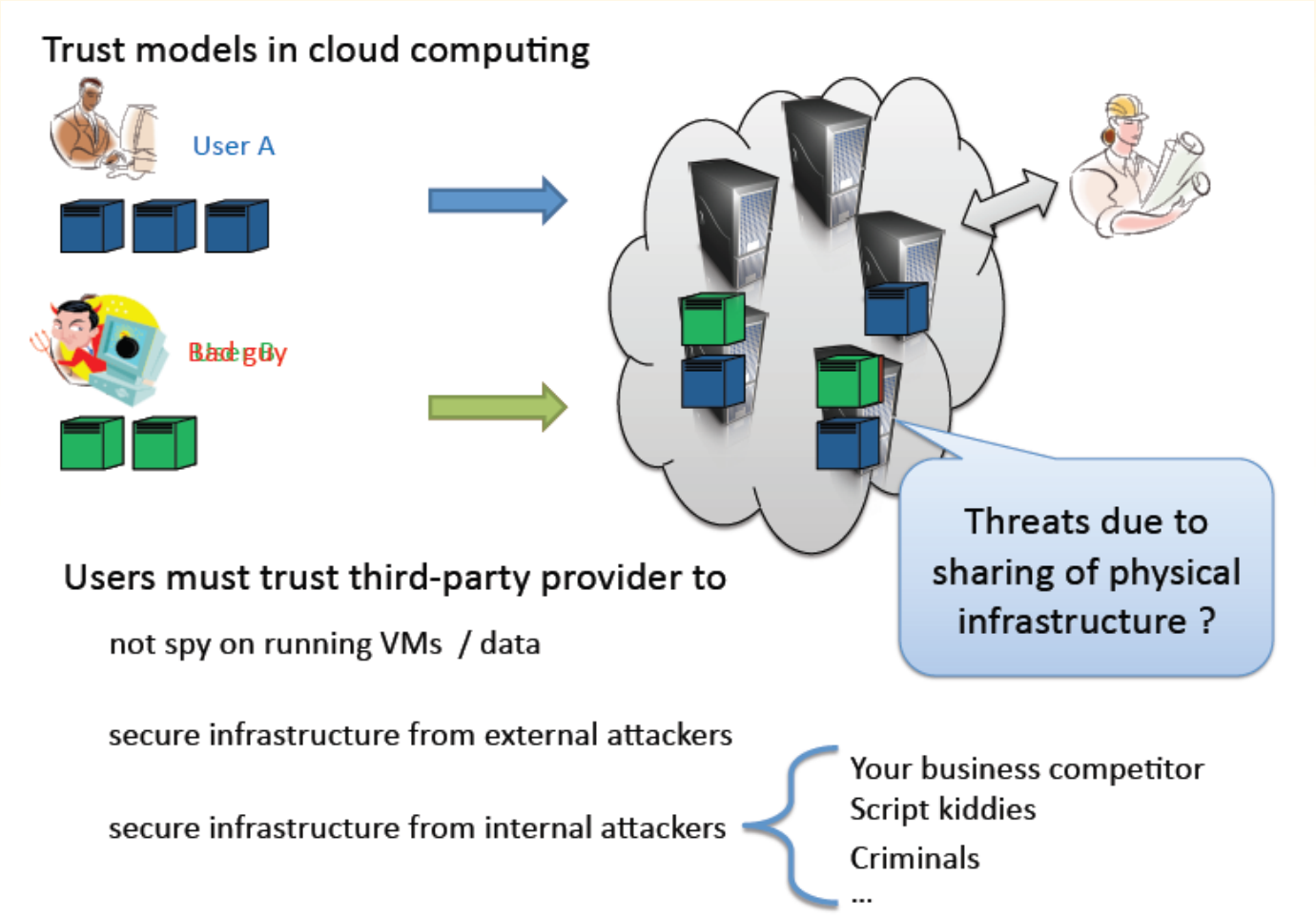
迄今为止发生的事情：

匿名访问和/或可重复使用的令牌或密码、明文身份验证或内容传输、欠灵活的访问控制或不当授权、有限的监控和记录功能、未知的服务或 API 互依关系。

威胁 3：心怀恶意的内部人员

“如果你在一家公司工作的时间足够长，最终你将有权访问一切内容，而且没人会知道。”

威胁 4：共享技术

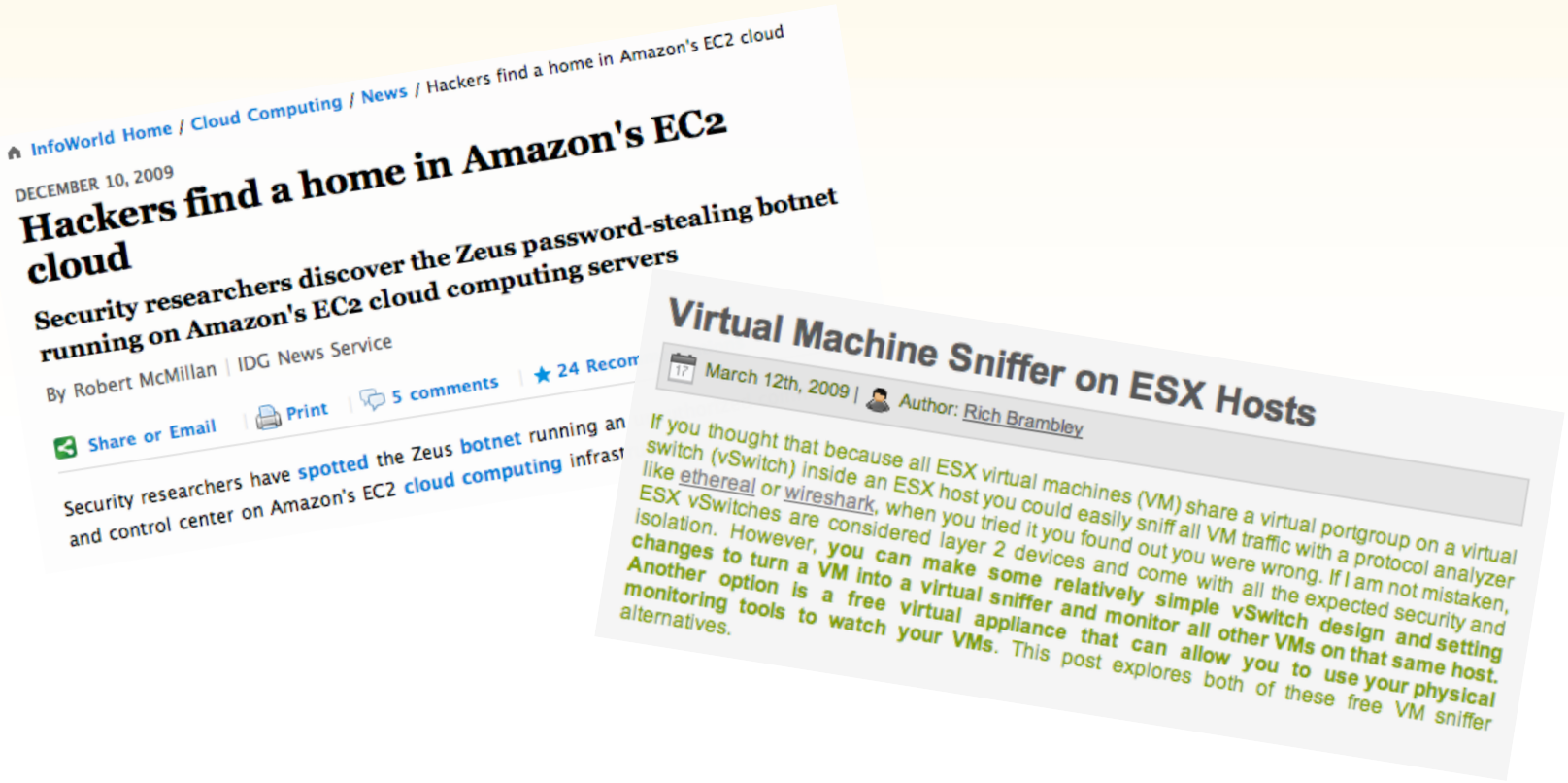


Tom Ristenpart：ristenpart-invited-csc2011.pdf

威胁 5：数据丢失

- Microsoft 在 2009 年发生的数据丢失事件，造成美国约 80 万智能手机用户暂时性丢失了移动手持式设备中的个人数据，如电子邮件、地址簿和照片。
- 保存这些数据的服务器是由 Microsoft 运行的。
- 当时，这被描述为影响云计算这一概念的最大灾难。

威胁 6：帐户或服务劫持



InfoWorld Home / Cloud Computing / News / Hackers find a home in Amazon's EC2 cloud

DECEMBER 10, 2009

Hackers find a home in Amazon's EC2 cloud

Security researchers discover the Zeus password-stealing botnet running on Amazon's EC2 cloud computing servers

By Robert McMillan | IDG News Service

Share or Email | Print | 5 comments | ★ 24 Recom

Security researchers have spotted the Zeus botnet running an and control center on Amazon's EC2 cloud computing infrast

Virtual Machine Sniffer on ESX Hosts

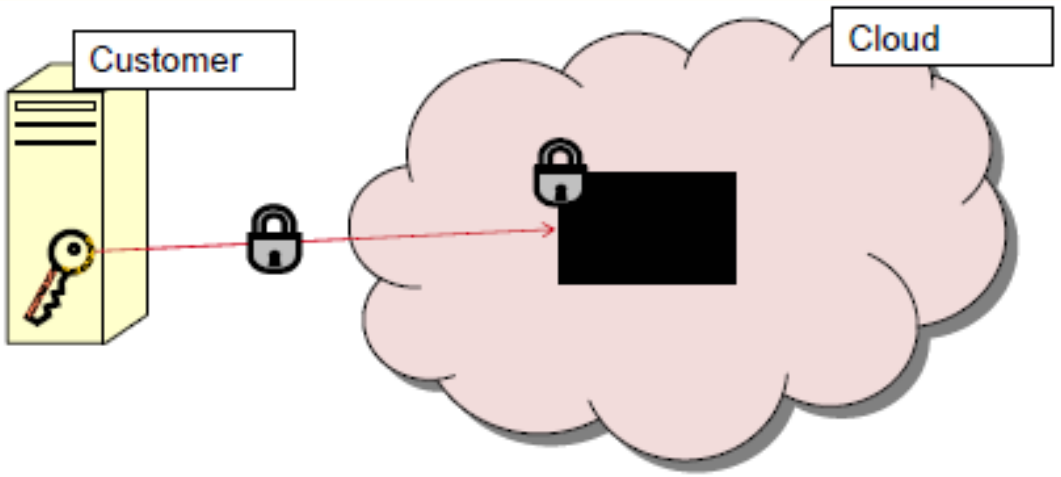
March 12th, 2009 | Author: Rich Brambley

If you thought that because all ESX virtual machines (VM) share a virtual portgroup on a virtual switch (vSwitch) inside an ESX host you could easily sniff all VM traffic with a protocol analyzer like ethereal or wireshark, when you tried it you found out you were wrong. If I am not mistaken, ESX vSwitches are considered layer 2 devices and come with all the expected security and isolation. However, **you can make some relatively simple vSwitch design and setting changes to turn a VM into a virtual sniffer and monitor all other VMs on that same host. Another option is a free virtual appliance that can allow you to use your physical monitoring tools to watch your VMs.** This post explores both of these free VM sniffer alternatives.

威胁 7：未知风险特征

信任提供商？

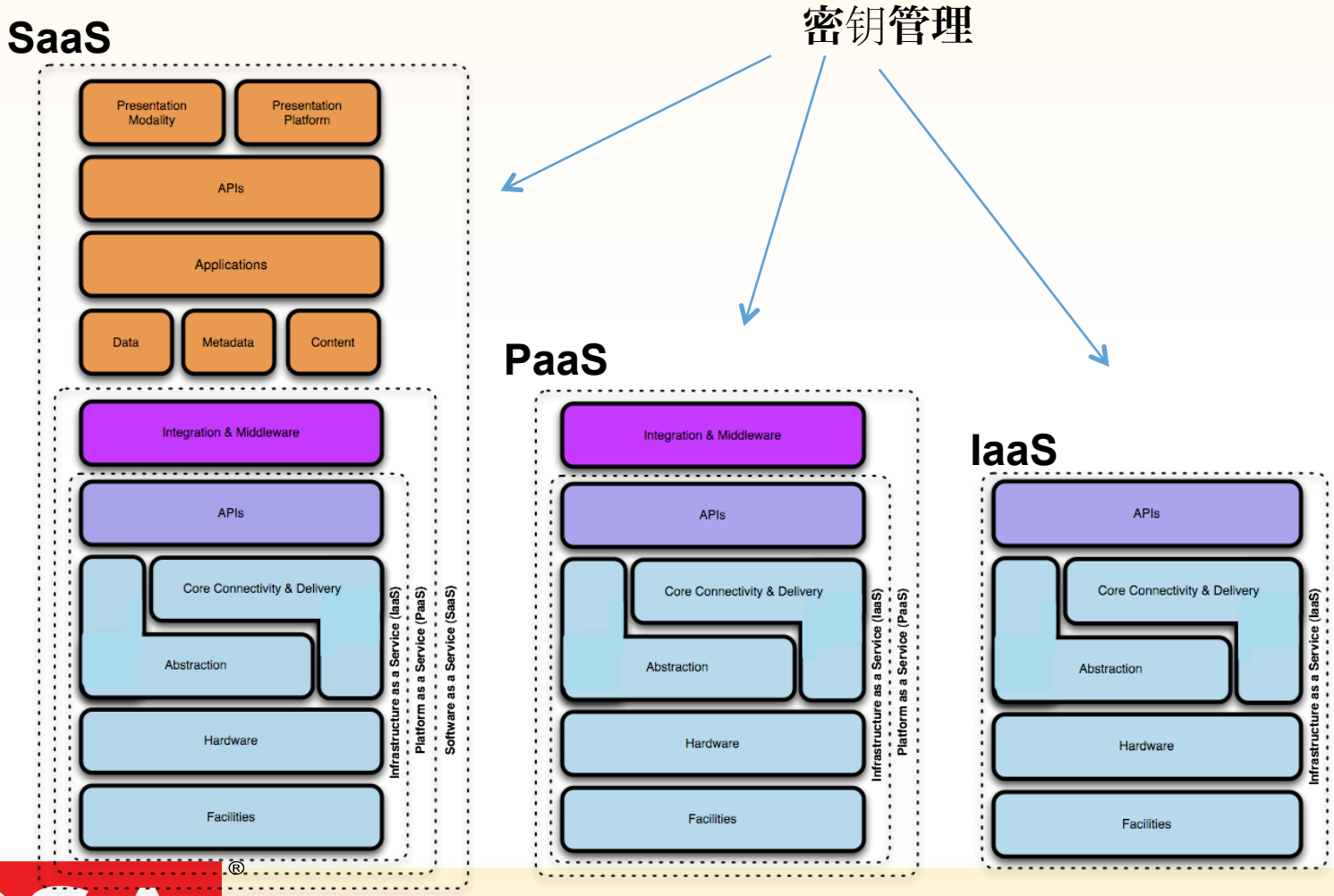
=> If you want to do anything useful with cloud computing, you have to trust the provider.



课程安排

- 云中的密钥管理问题
- 私有、公共和混合云中的密钥管理模型
- 针对云的密钥管理协议
- 需要解决哪些问题

所有云模型都涉及密钥管理 – 但是在什么位置呢？



CSA 安全指导

- **第 I 部分：云体系结构**
- 领域 1：云计算体系结构框架
- **第 II 部分：云中的监管**
- 领域 2：监管和企业风险管理
-
- **第 I 部分：云体系结构**
- 领域 1：云计算体系结构框架
- **第 II 部分：云中的监管**
- 领域 2：监管和企业风险管理
- 领域 3：法律查询和电子查询
- 领域 4：合规性和审计
- 领域 5：信息生命周期管理
- 领域 6：可移植性和互操作性
- **第 III 部分：云中的操作**
- 领域 7：传统的安全性、业务连续性和灾难恢复

  领域 8：数据中心运营

http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

CSA 加密指导

是有关方面极力建议做到的事情，而且有时是法律和法规的强制要求。云服务客户希望服务提供商加密他们的数据，以确保无论数据处于什么位置都能得到保护。同时，云服务提供商需要保护客户的敏感数据。

采用密钥管理的强加密，是云计算系统在保护数据时应使用的核心机制之一。尽管加密本身不一定能够防止数据丢失，但法律和法规中的安全港条款将丢失的加密数据视为根本未丢失。加密提供资源保护，而密钥管理则允许访问受保护的资源。

✓ 确保受管控和/或敏感的客户数据除了在处于静态时加密外，在云服务提供商的内部网络中传输时也经过加密。

✓在

IaaS 环境中，要知道使用传统加密保护的敏感信息和关键资料在使用期间可能会以怎样的方式暴露。

http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

CSA 密钥管理指导

✓将密钥管理从托管着数据的云服务提供商那里分离出来，形成一种隔离链。这样，在法律命令强制要求提供数据时，云服务提供商和客户之间将不存在冲突。

✓了解云服务提供商的设施是否以及如何提供角色管理和职责划分。

✓在云服务提供商必须执行密钥管理的情况下，要了解提供商是否定义了用于密钥管理生命周期的流程：密钥是怎样生成、使用、存储、备份、恢复、循环和删除的。另外，要了解是每一家客户都使用同一密钥，还是每个客户各有自己的密钥集。

http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

定义云密钥管理模型

- 密钥是在何处创建的？
- 密钥在哪里使用？
- 密钥在哪里存储？
- 密钥策略在哪里管理？

云密钥管理模型

企业

- 密钥由企业创建、使用、存储和管理

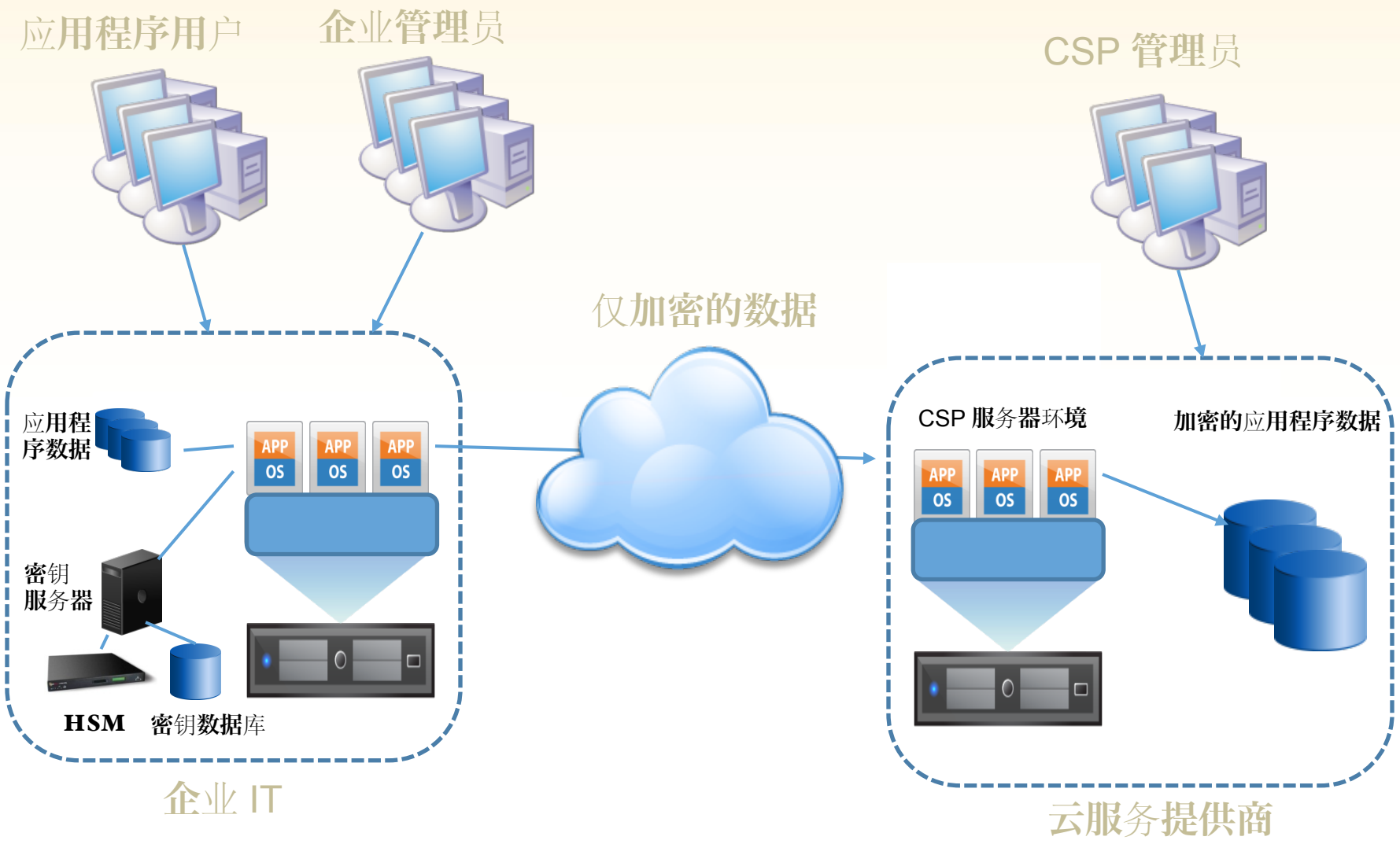
混合

- 密钥由企业创建、存储和管理，但由 CSP（云服务提供商）使用

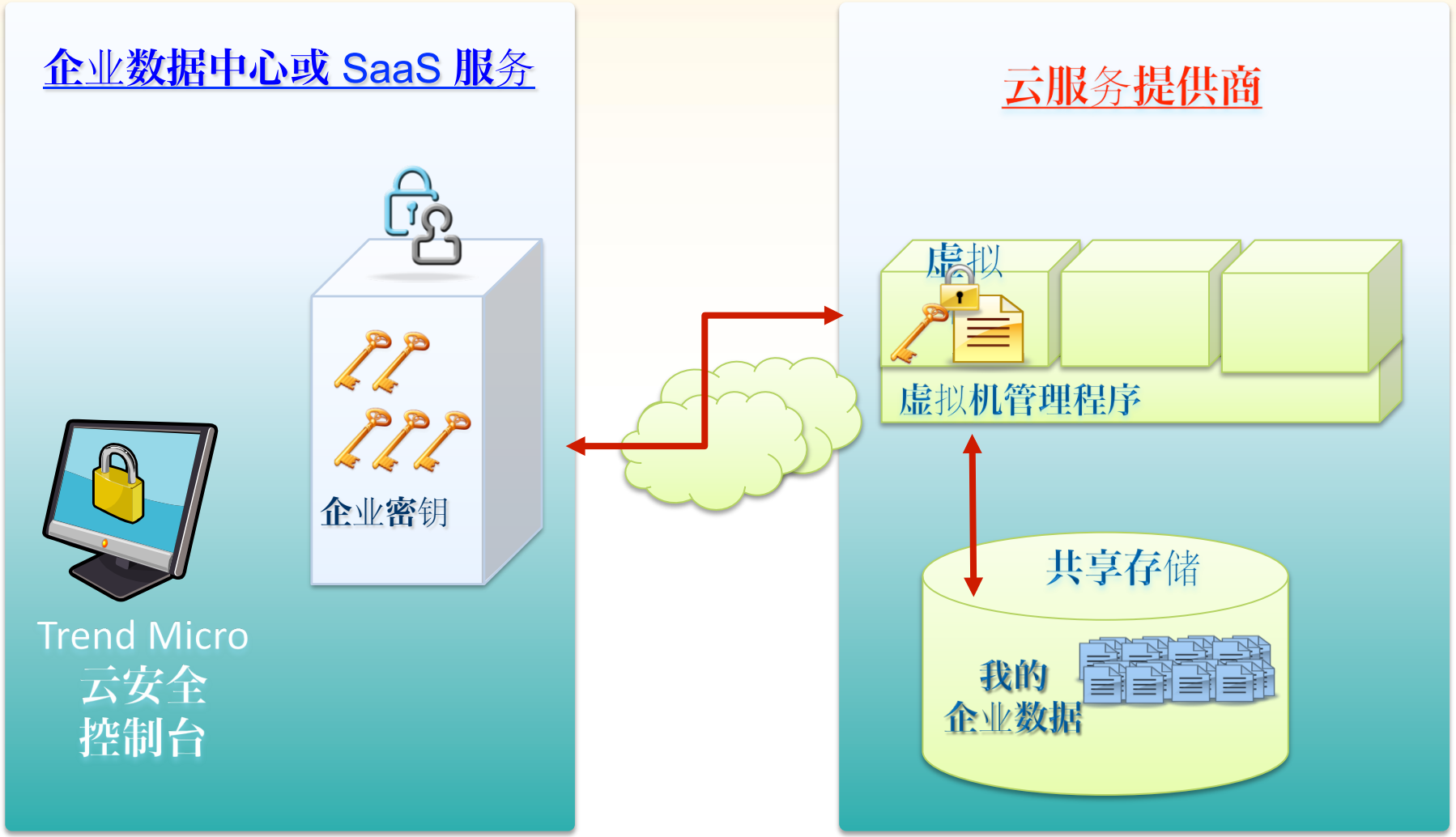
CSP

- 密钥由 CSP 创建、使用、存储和管理

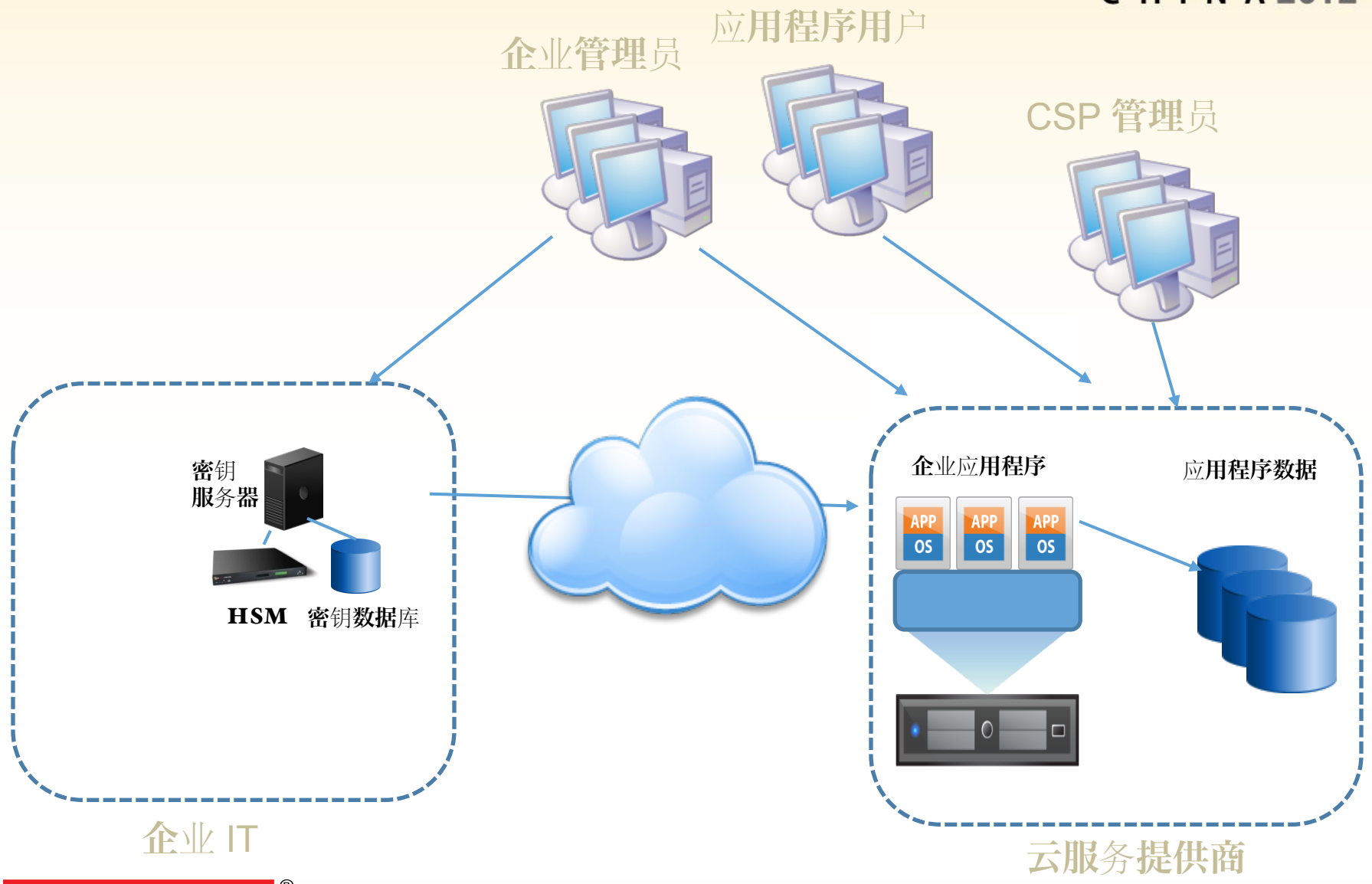
模型 1：企业密钥管理


应用程序用户
企业管理员
CSP 管理员
仅加密的数据
应用程序数据
APP
OS
密钥服务器
HSM
密钥数据库
企业 IT
CSP 服务器环境
加密的应用程序数据
云服务提供商

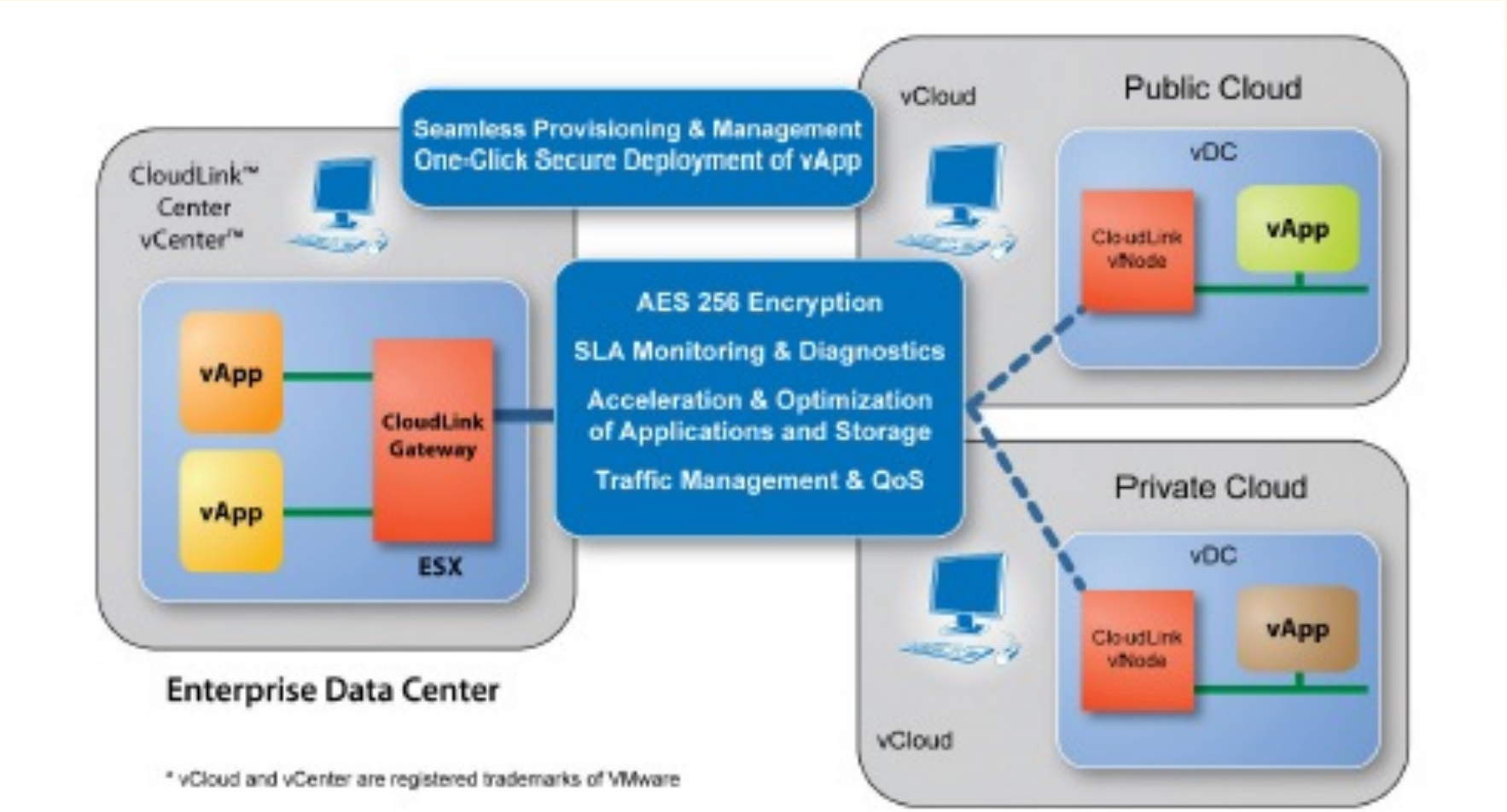
示例：TrendMicro SecureCloud



模型 2：混合密钥管理

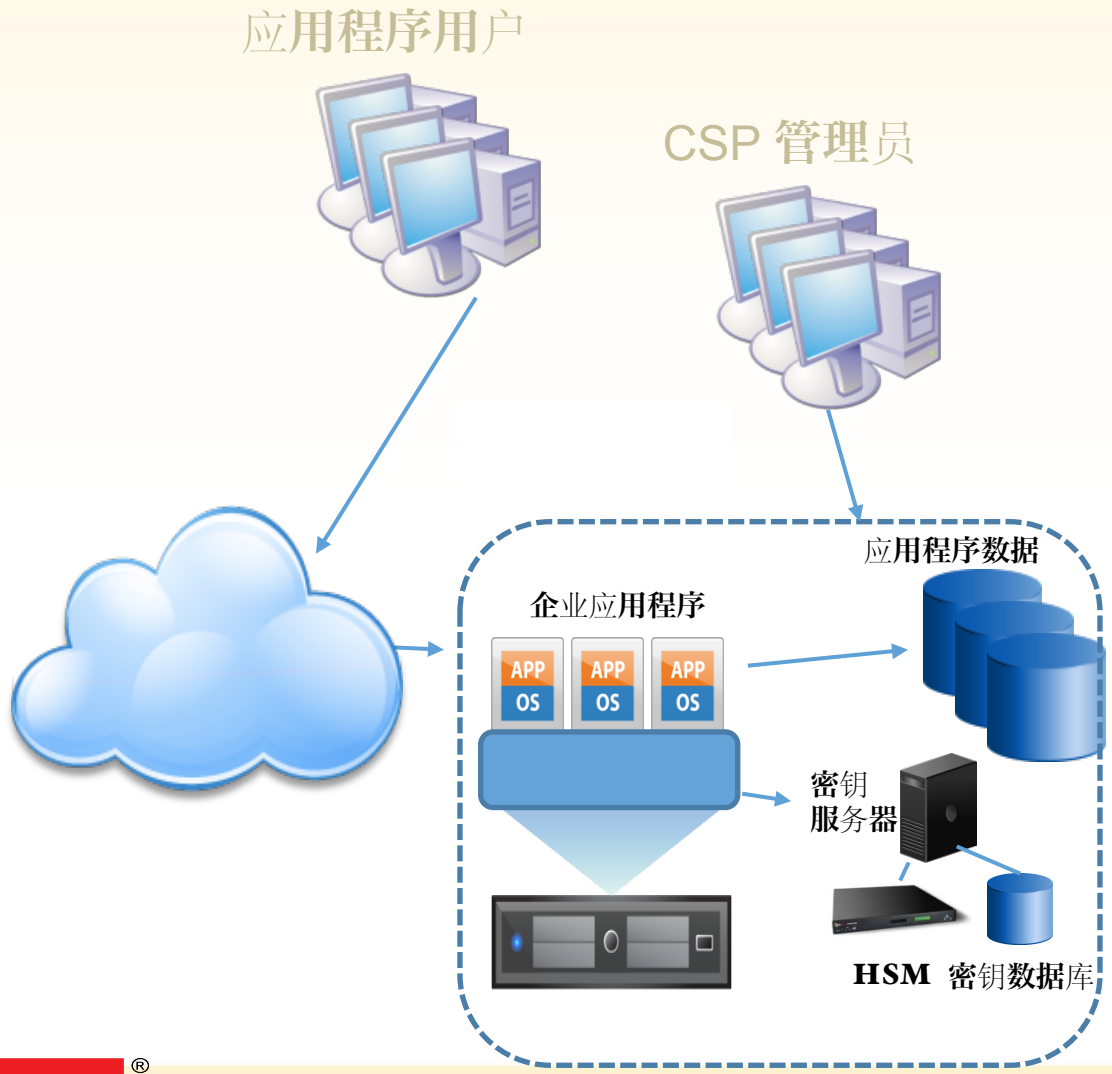

企业管理员
应用程序用户
CSP 管理员
密钥
服务器
HSM
密钥数据库
企业应用程序
应用程序数据
APP
OS
APP
OS
APP
OS
企业 IT
云服务提供商

示例：Afore CloudLink



AFORE CloudLink Product Brief.pdf

模型 3：CSP 密钥管理

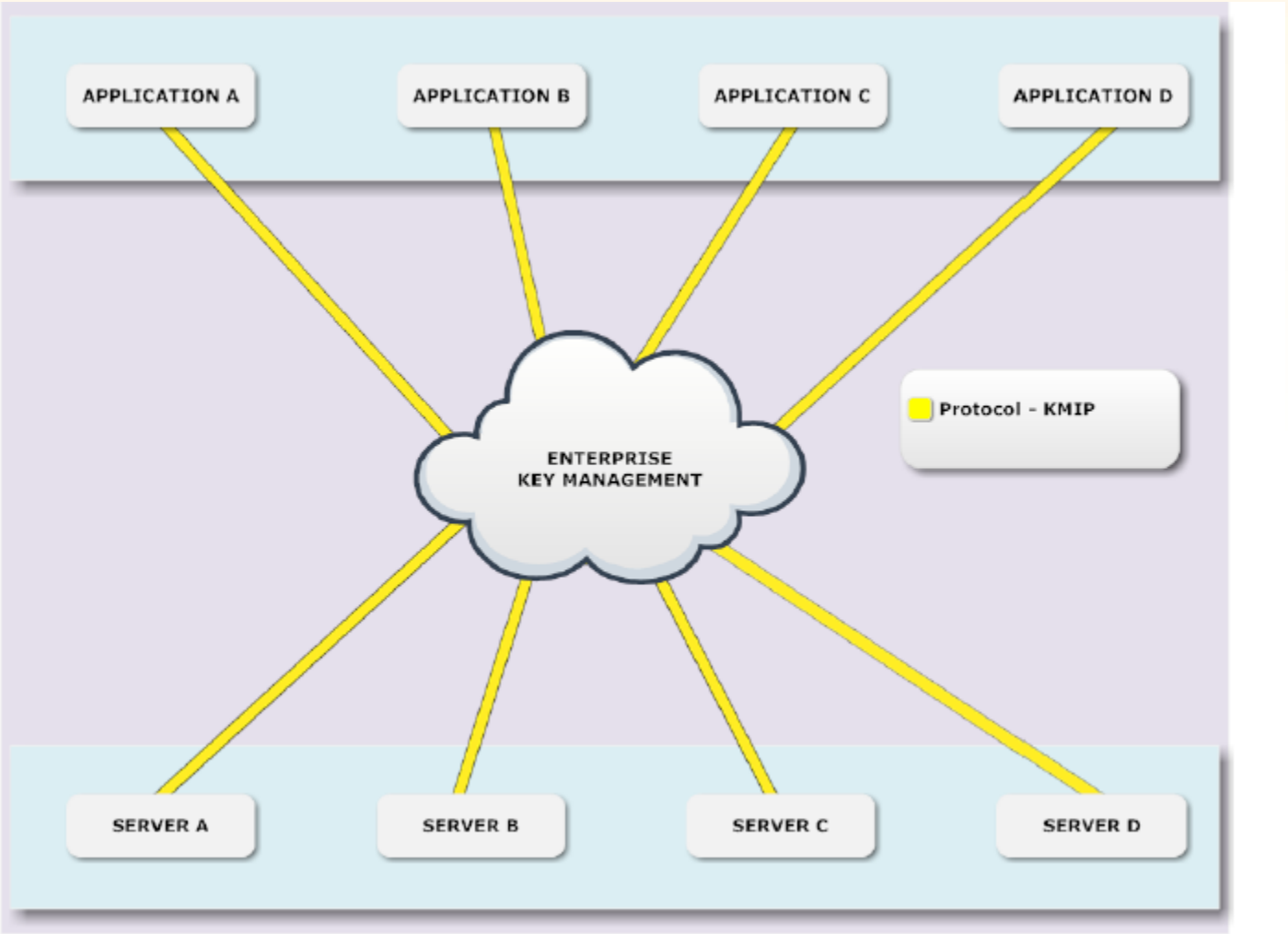

应用程序用户
CSP 管理员
应用程序数据
企业应用程序
APP
OS
APP
OS
APP
OS
密钥
服务器
HSM
密钥数据库

示例：Azure Trust Services

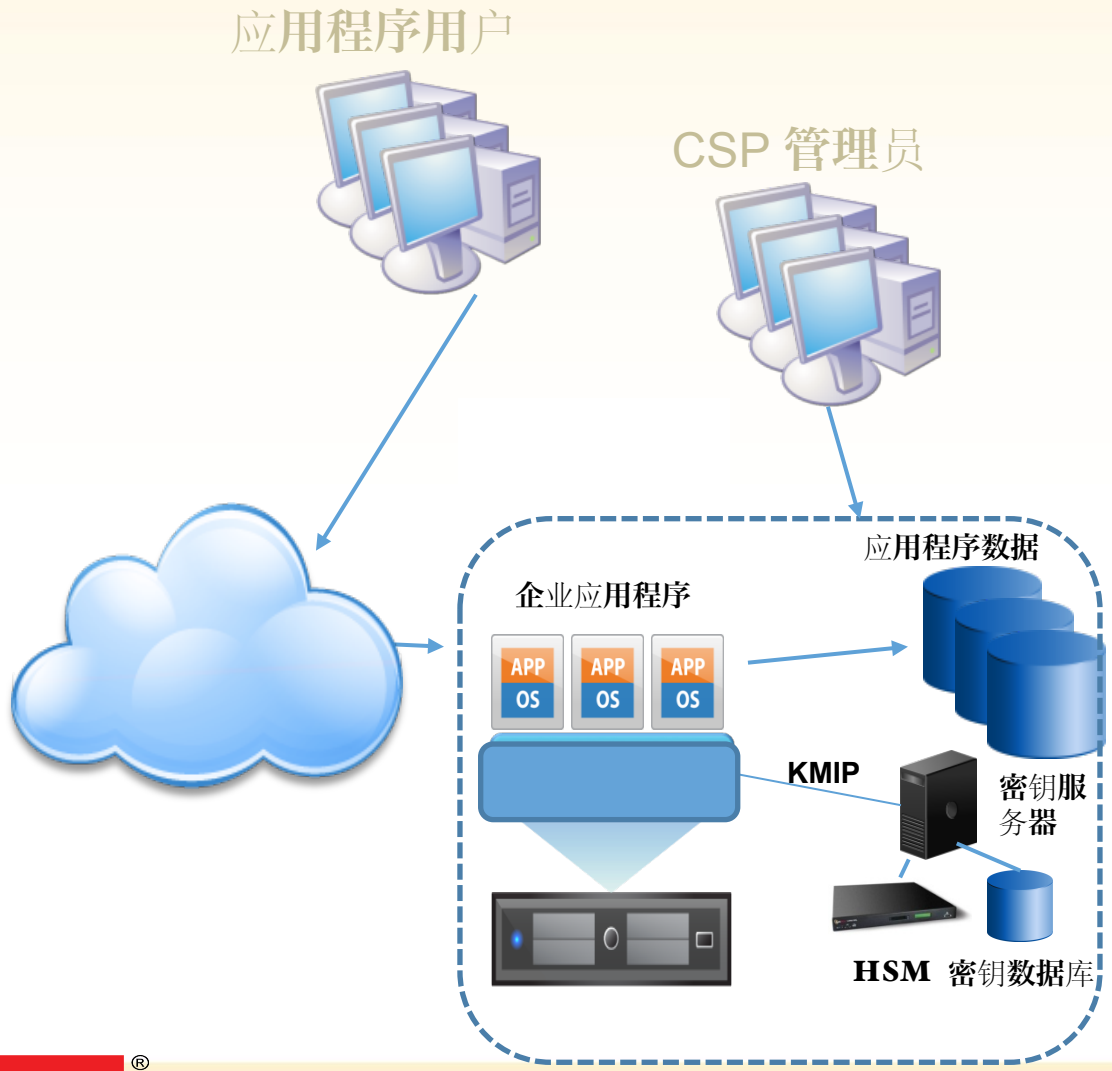
课程安排

- 云中的密钥管理问题
- 私有、公共和混合云中的密钥管理模型
- 针对云的密钥管理协议
- 需要解决哪些问题

OASIS 密钥管理互操作性协议 (KMIP)



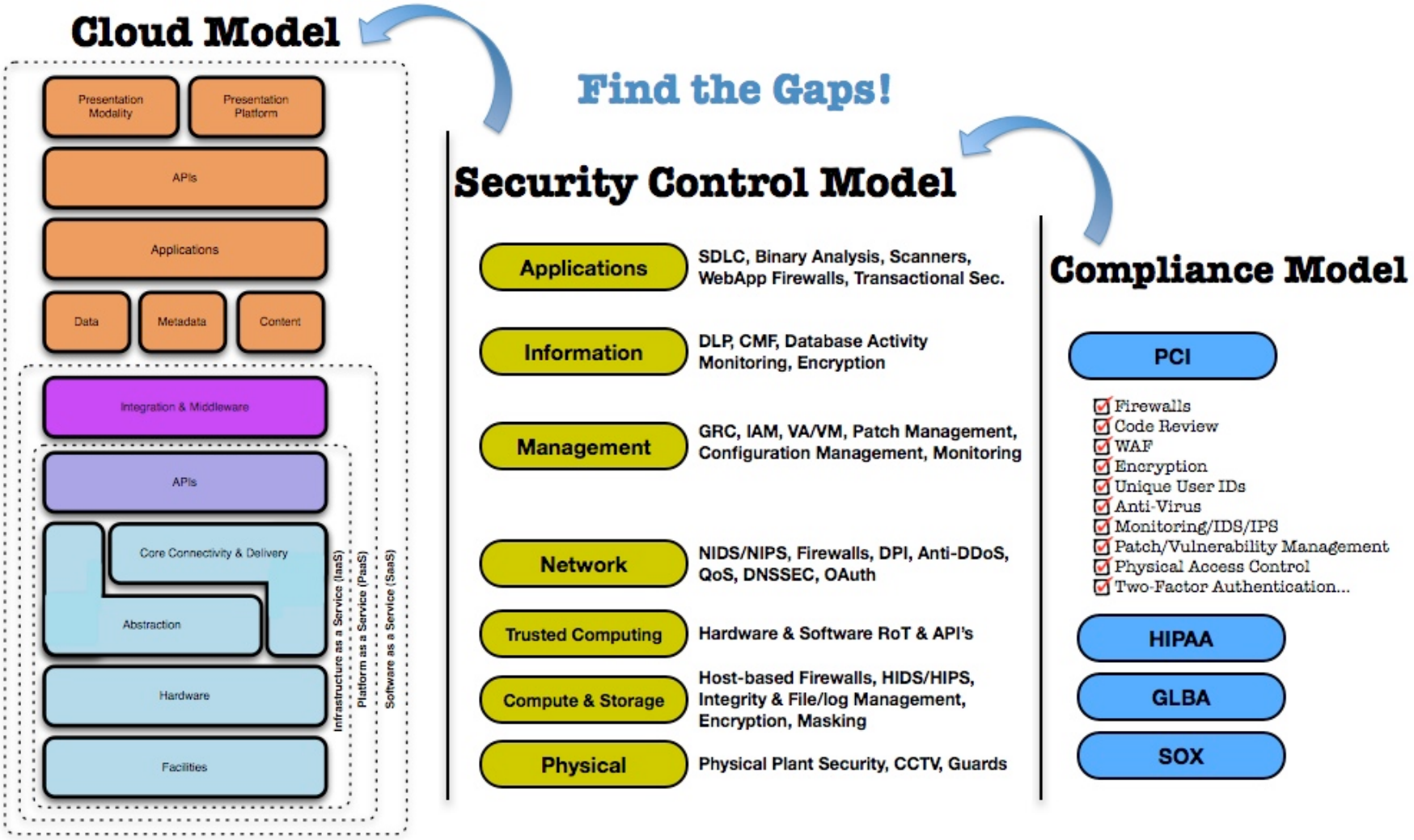
在 CSP 密钥管理中使用 KMIP



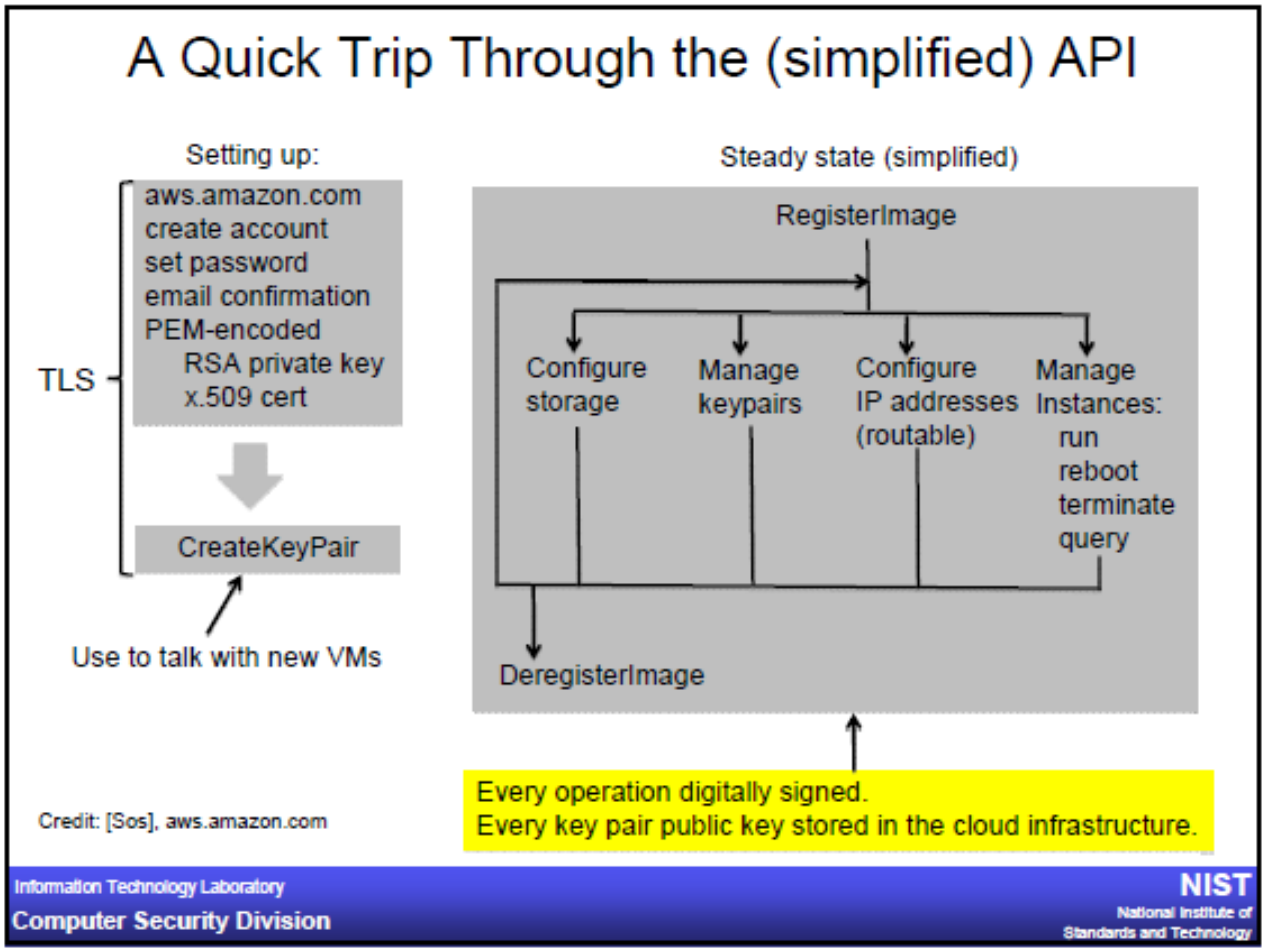
课程安排

- 云中的密钥管理问题
- 私有、公共和混合云中的密钥管理模型
- 针对云的密钥管理协议
- 需要解决哪些问题

密钥管理与合规性

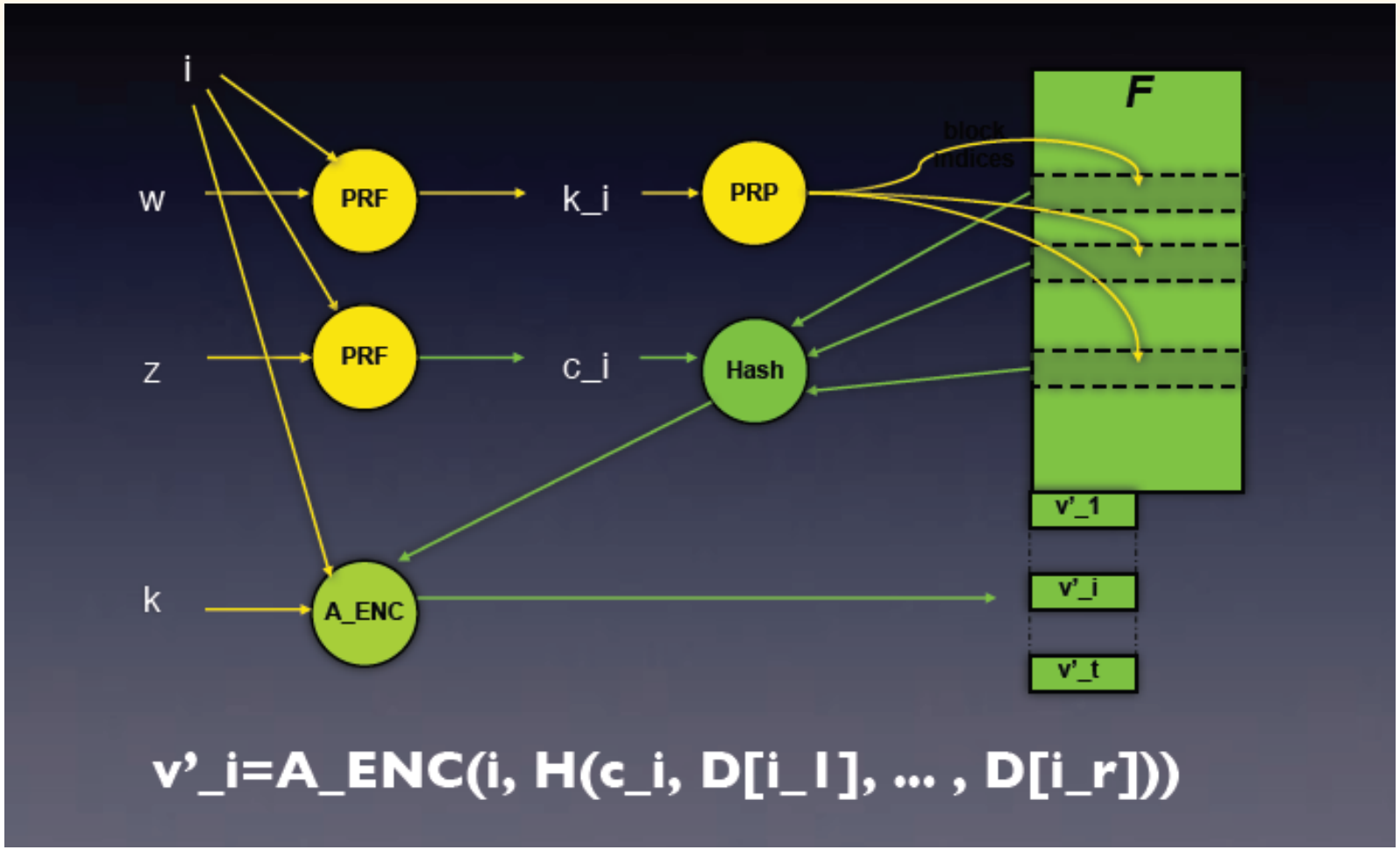

Cloud Model
Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Content
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Find the Gaps!
Security Control Model
Applications
SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information
DLP, CMF, Database Activity Monitoring, Encryption
Management
GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network
NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing
Hardware & Software RoT & API's
Compute & Storage
Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical
Physical Plant Security, CCTV, Guards
Compliance Model
PCI
Firewalls
Code Review
WAF
Encryption
Unique User IDs
Anti-Virus
Monitoring/IDS/IPS
Patch/Vulnerability Management
Physical Access Control
Two-Factor Authentication...
HIPAA
GLBA
SOX

是否需要新的加密或密钥管理标准？



lee_badger_KMWJune09_clouds_keys.pdf

我们是否必须为密钥建立所有权证明？



Giuseppe Ataniense：PDP1.pdf

谢谢大家！

robert.griffin@rsa.com

RSA CONFERENCE CHINA 2012