信息安全管理
先锋论坛

跟我学信息安全管理大型讲座

欢迎加入QQ群信息安全管理_微信直播，清扫一下二维码，点右下角

信息安全管理专家委员会发布
2016年11月

信息安全管理论坛（http://www.iso27001cn.com）成立于2014年9月，为国内目前最专业的信息安全管理学习和实践交流平台。是学习信息安全管理方法、分享实战经验、提升实践水平的好地方！

关于我们

我们提供

- 最全的信息安全管理资料
- 信安经理高薪工作机会推荐
- 每周专家讲堂（ 每周四晚上8点半QQ群207723402 ）
- 物美价廉的ISO27001课程团购

- 信息安全管理学习实践QQ群 207723402
- 微信 IT管理精英圈 itilxf_(记得有下划线)

欢迎关注

授课专家

长河

资深IT服务管理专家、云计算平台架构师、云数据中心整体解决方案架构师，20多年IT服务管理经验，曾服务于众多全球运营商和金融机构，Exin国际授权认证讲师，ITIL Expert/ISO20000LA/Huawei云平台实施认证/WmwareVCP/RHCE/MCSE

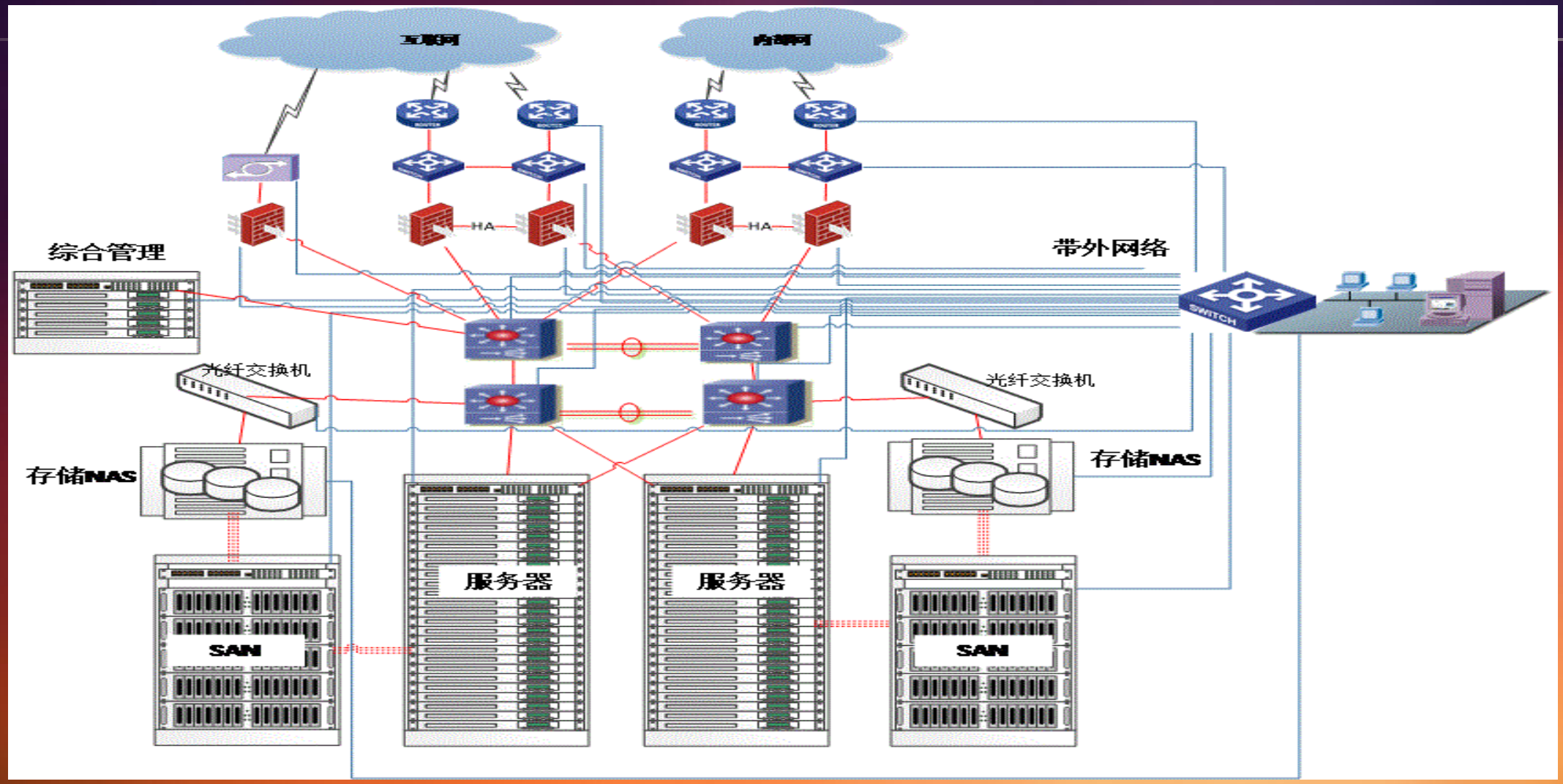
云环境下的信息安全管理

云环境下信息安全管理问题分析

云安全保障体系框架设计

云计算安全的新技术驱动力

云计算系统典型物理架构



云环境下信息安全管理的优势

- 云计算的资源弹性、按需调配、高可靠性及资源集中
- 安全服务内容、实现机制和交付方式的创新和发展
- 云计算模式通过将数据统一存储在云计算服务器中，加强对核心数据的集中管控，使得安全审计、安全评估、安全运维等行为更加简单易行
- 更容易实现系统容错、高可用性和冗余及灾备恢复

云环境下信息安全管理的问题

- CSA在2013年的报告中列出了九大安全威胁。依排序分别为
  - ✓1.数据泄露
  - ✓2.数据丢失
  - ✓3.帐户劫持
  - ✓4.不安全的接口（API）
  - ✓5.拒绝服务攻击（DDoS）
  - ✓6.内部人员的恶意操作
  - ✓7.云计算服务的滥用
  - ✓8.云服务规划不合理
  - ✓9.共享技术的漏洞问题。

网络安全威胁

- 业务高峰时段或遭遇DDoS攻击时的大流量导致网络拥堵或网络瘫痪
- 重要网段暴露导致来自外部的非法访问和入侵
- 单台虚拟机被入侵后对整片虚拟机进行的渗透攻击，并导致病毒等恶意行为在网络内传播蔓延
- 虚拟机之间进行的ARP攻击、嗅探
- 云内网络带宽的非法抢占
- 重要的网段、服务器被非法访问、端口扫描、入侵攻击
- 云平台管理员因账号被盗等原因导致的从互联网直接非法访问云资源
- 虚拟化网络环境中流量的审计和监控
- 内部用户或内部网络的非法外联行为的检查和阻断
- 内部用户之间或者虚拟机之间端口扫描、暴力破解、入侵攻击等行为

主机安全威胁

- 服务器、宿主机、虚拟机的操作系统和数据库被暴力破解、非法访问的行为
- 对服务器、宿主机、虚拟机等进行操作管理时被窃听
- 同一个逻辑卷被多个虚拟机挂载导致逻辑卷上的敏感信息泄露
- 对服务器的Web应用入侵、上传木马、上传webshell等攻击行为
- 服务器、宿主机、虚拟机的补丁更新不及时导致的漏洞利用以及不安全的配置和非必要端口的开放导致的非法访问和入侵
- 虚拟机因异常原因产生的资源占用过高而导致宿主机或宿主机下的其它虚拟机的资源不足

虚拟化平台威胁

- 虚拟机之间的资源争抢或资源不足导致的正常业务异常或不可用
- 虚拟资源不足导致非重要业务正常运作但重要业务受损
- 缺乏身份鉴别导致的非法登录hypervisor后进入虚拟机
- 通过虚拟机漏洞逃逸到hypervisor，获得物理主机的控制权限
- 攻破虚拟系统后进行任易破坏行为、网络行为、对其它账户的猜解，和长期潜伏
- 虚拟机的内存和存储空间被释放或再分配后被恶意攻击者窃取
- 虚拟机和备份信息在迁移或删除后被窃取
- hypervisor、虚拟系统、云平台系统漏洞导致的攻击入侵
- 虚拟机镜像遭到恶意攻击者篡改或非法读取

数据安全威胁

- 数据在传输过程中受到破坏而无法恢复
- 在虚拟环境传输的文件或者数据被监听
- 云用户从虚拟机逃逸后获取镜像文件或其他用户的隐私数据
- 因各种原因或故障导致的数据不可用
- 敏感数据存储漂移导致的不可控
- 数据安全隔离不严格导致恶意用户可以访问其他用户数据

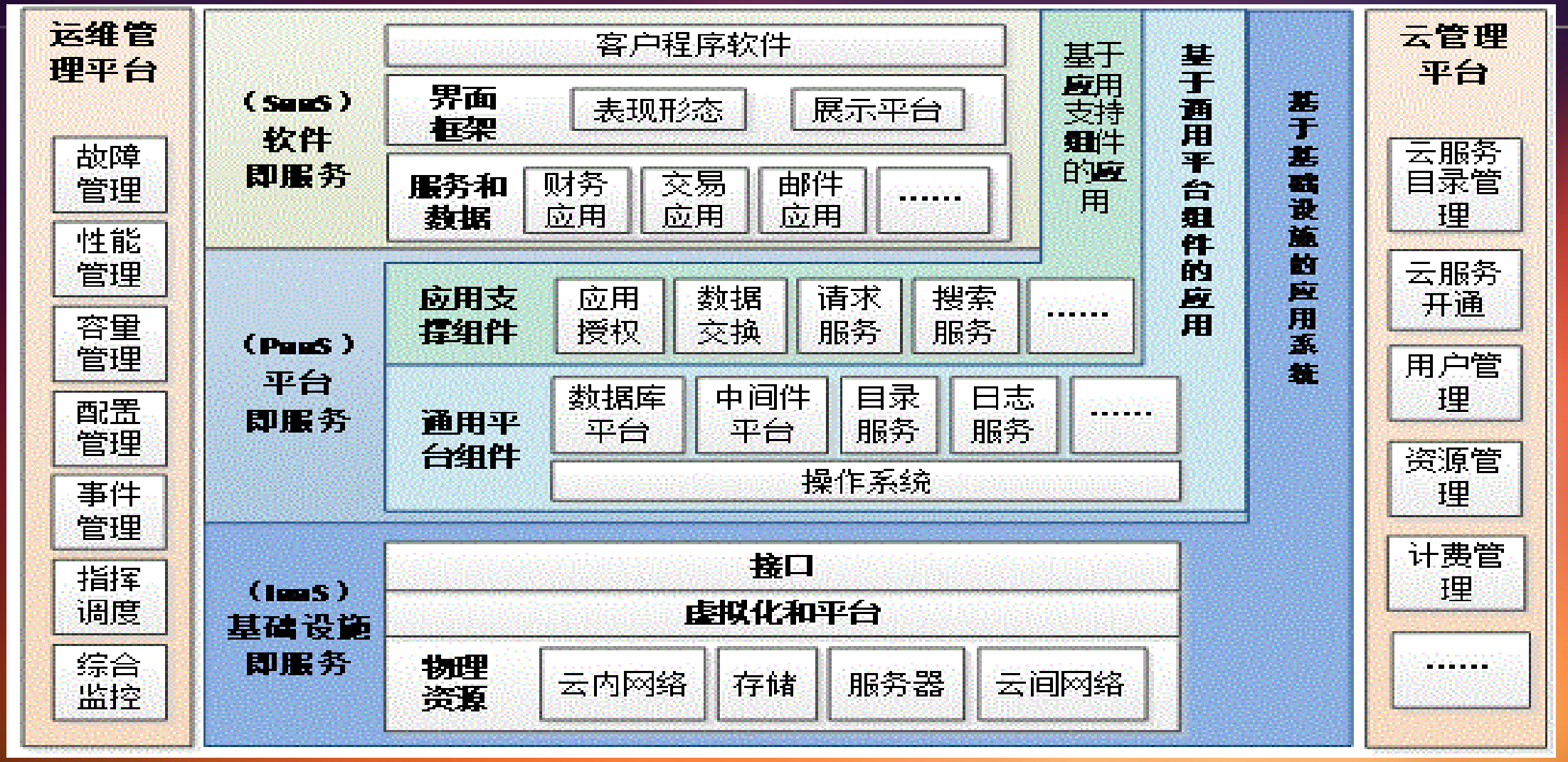
云环境下的信息安全管理

云环境下信息安全管理问题分析

云安全保障体系框架设计

云计算安全的新技术驱动力

云计算系统逻辑结构


运维管理平台
故障管理
性能管理
容量管理
配置管理
事件管理
指挥调度
综合监控
（SaaS）软件即服务
客户程序软件
界面框架
表现形态
展示平台
服务和数据
财务应用
交易应用
邮件应用
……
基于应用支持组件的应用
（PaaS）平台即服务
应用支撑组件
应用授权
数据交换
请求服务
搜索服务
……
通用平台组件
数据库平台
中间件平台
目录服务
日志服务
……
操作系统
基于通用平台组件的应用
（IaaS）基础设施即服务
接口
虚拟化和平台
物理资源
云内网络
存储
服务器
云间网络
基于基础设施的应用系统
云管理平台
云服务目录管理
云服务开通
用户管理
资源管理
计费管理
……

云安全防护总体架构设计思路

- 保障云平台及其配套设施
- 基于安全域的纵深防护体系设计
- 以安全服务为导向，并符合云计算的特点
- 充分利用现有安全控制措施及最新技术
- 充分利用云计算等最新技术
- 安全运营

云安全保障体系框架


安全管理
安全风险管理
安全设计与获取
安全开发与集成
安全事件管理
安全运维管理
业务连续性
应用安全
Web应用防火墙
网站安全检测
网页防篡改
Email安全
主机安全
主机安全防护
OS安全配置与加固
服务器防病毒
设备安全
网络安全
安全域划分
访问控制
流量清洗
入侵检测
恶意代码防护
VPN接入
虚拟化安全
物理环境安全
门禁系统
机房安全
安全支撑基础设施（PKI、身份管理等）
数据安全
数据加密
数据防泄露
数据库防火墙
数据库审计
•物理环境安全：在物理层面，通过门禁系统、视频监控、环境监控、物理访问控制等措施实现云运行的物理环境、环境设施等层面的安全；

云安全保障体系框架


安全管理
安全风险管理
安全设计与获取
安全开发与集成
安全事件管理
安全运维管理
业务连续性
应用安全
Web应用防火墙
网站安全检测
网页防篡改
Email安全
主机安全
主机安全防护
OS安全配置与加固
服务器防病毒
设备安全
网络安全
虚拟化安全
虚拟机加固
Hypervisor加固
虚拟机映像安全
虚拟机管理安全
物理环境安全
门禁系统
机房安全
数据安全
数据加密
数据防泄露
数据库防火墙
数据库审计
安全支撑基础设施（PKI、身份管理等）
•虚拟化安全：在虚拟化层面，通过虚拟层加固、虚拟机映像加固、不同虚拟机的内存/存储隔离、虚拟机安全检测、虚拟化管理安全等措施实现虚拟化层的安全；

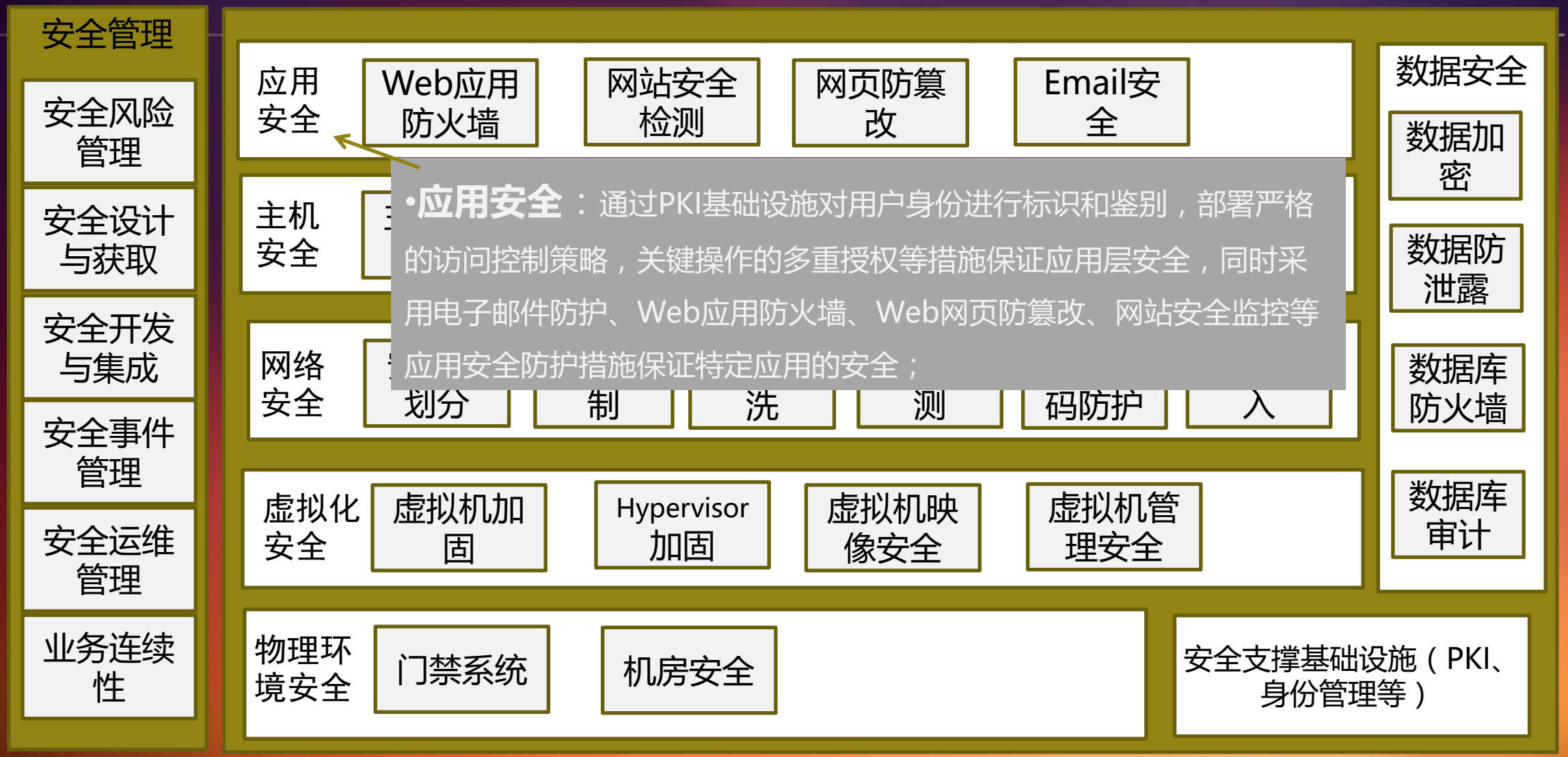
云安全保障体系框架

•网络安全：在网络层，基于安全域划分，通过防火墙、IPS、VLAN ACL手段进行边界隔离和访问控制，通过VPN技术保障网络通信安全和用户的认证接入，在网络的重要区域部署入侵监测系统（IDS）以实现对网络攻击的实时监测和告警，部署流量监测和清洗设备以抵御DDoS攻击，部署恶意代码监测和防护系统以实现对恶意代码的防范。需要说明的是这里的网络包括了实体网络和虚拟网络，通过整体防御保障网络通信的安全；

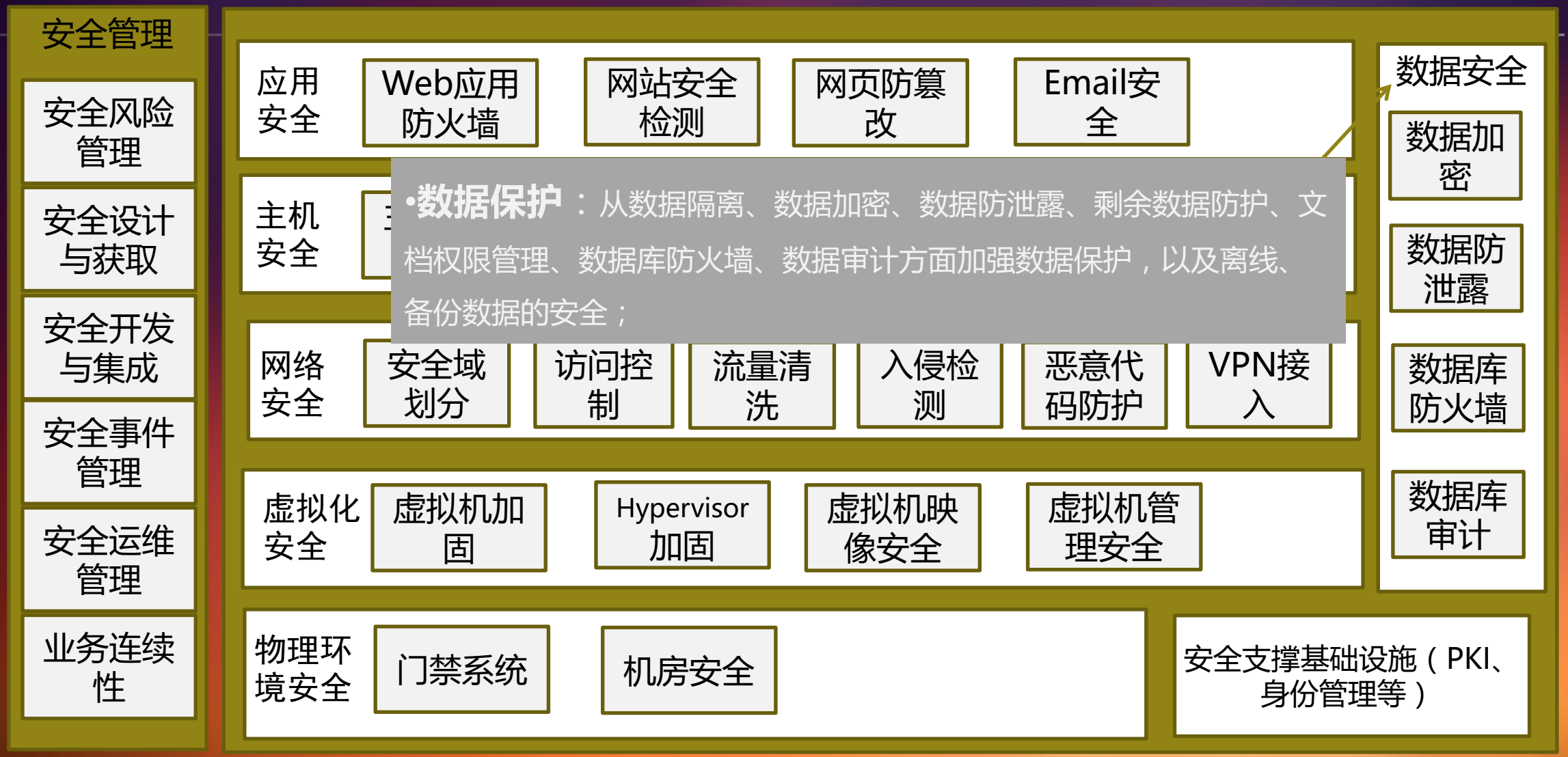
云安全保障体系框架


安全管理
安全风险管理
安全设计与获取
安全开发与集成
安全事件管理
安全运维管理
业务连续性
应用安全
Web应用防火墙
网站安全检测
网页防篡改
Email安全
主机安全
主机安全防护
OS安全配置与加固
服务器防病毒
设备安全
网络安全
虚拟化安全
虚拟机加固
Hypervisor加固
虚拟机映像安全
虚拟机管理安全
物理环境安全
门禁系统
机房安全
数据安全
数据加密
数据防泄露
数据库防火墙
数据库审计
安全支撑基础设施（PKI、身份管理等）
•主机安全：通过对服务主机/设备进行安全配置和加固，部属主机防火墙、主机IDS，以及恶意代码的防护、访问控制等技术手段对虚拟主机进行保护，确保主机能够持续的提供稳定的服务；

云安全保障体系框架


安全管理
安全风险管理
安全设计与获取
安全开发与集成
安全事件管理
安全运维管理
业务连续性
应用安全
Web应用防火墙
网站安全检测
网页防篡改
Email安全
主机安全
网络安全
划分
制
洗
测
码防护
入
虚拟化安全
虚拟机加固
Hypervisor加固
虚拟机映像安全
虚拟机管理安全
物理环境安全
门禁系统
机房安全
数据安全
数据加密
数据防泄露
数据库防火墙
数据库审计
安全支撑基础设施（PKI、身份管理等）
•应用安全：通过PKI基础设施对用户身份进行标识和鉴别，部署严格的访问控制策略，关键操作的多重授权等措施保证应用层安全，同时采用电子邮件防护、Web应用防火墙、Web网页防篡改、网站安全监控等应用安全防护措施保证特定应用的安全；

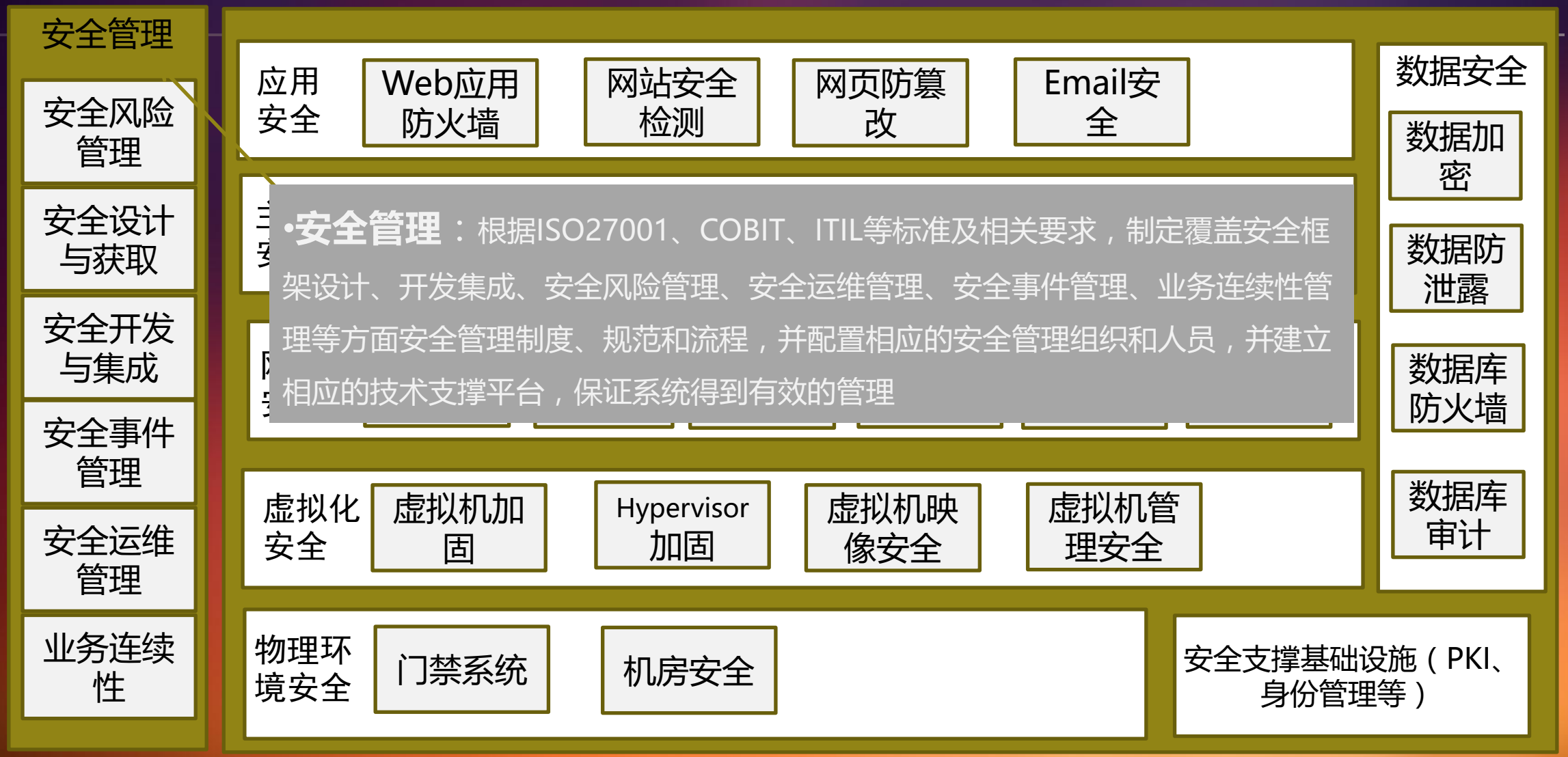
云安全保障体系框架


安全管理
安全风险管理
安全设计与获取
安全开发与集成
安全事件管理
安全运维管理
业务连续性
应用安全
Web应用防火墙
网站安全检测
网页防篡改
Email安全
主机安全
网络安全
安全域划分
访问控制
流量清洗
入侵检测
恶意代码防护
VPN接入
虚拟化安全
虚拟机加固
Hypervisor加固
虚拟机映像安全
虚拟机管理安全
物理环境安全
门禁系统
机房安全
安全支撑基础设施（PKI、身份管理等）
数据安全
数据加密
数据防泄露
数据库防火墙
数据库审计
•数据保护：从数据隔离、数据加密、数据防泄露、剩余数据防护、文档权限管理、数据库防火墙、数据审计方面加强数据保护，以及离线、备份数据的安全；

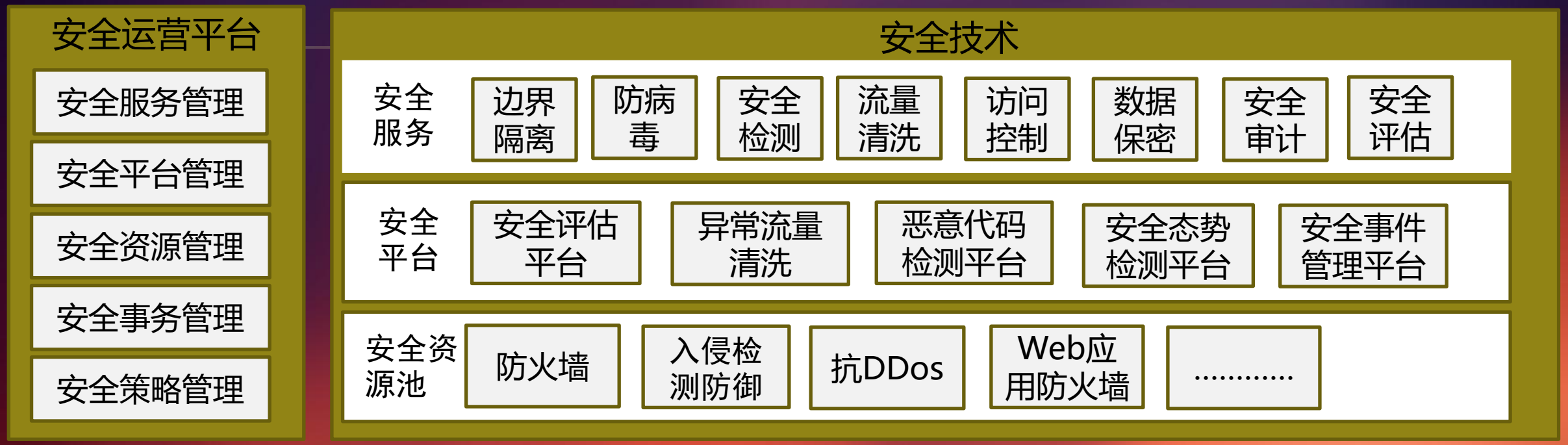
云安全保障体系框架

- **身份认证：**上述安全保障内容和目标的实现，需要基于PKI、身份管理等安全基础支撑设施，综合利用安全成熟的安全控制措施，并构建良好的安全实现机制，保障系统的良好运转，以提供满足各层面需求的安全能力

云安全保障体系框架


安全管理
安全风险管理
安全设计与获取
安全开发与集成
安全事件管理
安全运维管理
业务连续性
应用安全
Web应用防火墙
网站安全检测
网页防篡改
Email安全
数据安全
数据加密
数据防泄露
数据库防火墙
数据库审计
虚拟化安全
虚拟机加固
Hypervisor加固
虚拟机映像安全
虚拟机管理安全
物理环境安全
门禁系统
机房安全
安全支撑基础设施（PKI、身份管理等）
•安全管理：根据ISO27001、COBIT、ITIL等标准及相关要求，制定覆盖安全框架设计、开发集成、安全风险管理、安全运维管理、安全事件管理、业务连续性管理等方面安全管理制度、规范和流程，并配置相应的安全管理组织和人员，并建立相应的技术支撑平台，保证系统得到有效的管理

安全保障体系总体技术实现架构

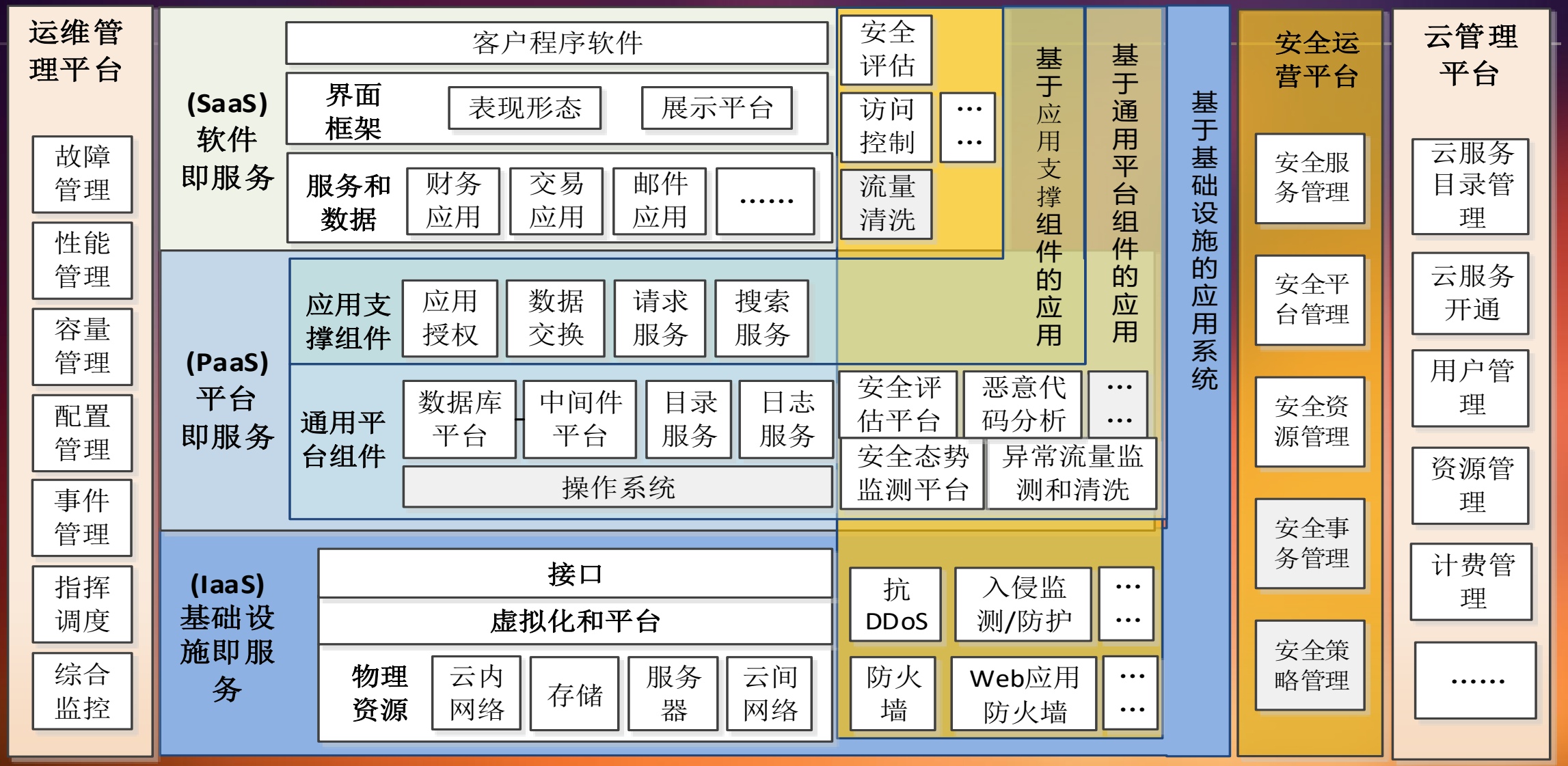


安全资源池：可以由传统的物理安全防护组件、虚拟化安全防护组件组成，提供基础的安全防护能力；

安全平台：提供对基础安全防护组件的注册、调度和安全策略管理。可以设立一个综合的安全管理平台，或者分立的安全管理平台，如安全评估平台、异常流量检测平台等；

安全服务：提供给云平台租户使用的各种安全服务，提供安全策略配置、状态监测、统计分析和报表等功能，是租户管理其安全服务的门户

安全防护措施与云平台体系架构的无缝集成



云环境下的信息安全管理

云环境下信息安全管理问题分析

云安全保障体系框架设计

云计算安全的新技术驱动力

云计算安全的新技术驱动力

- SDN、NFV技术的采用，为存储、网络资源的自动化部署和分权分域管理提供了技术手段
- 大数据技术的出现和应用，也为安全态势分析提供支撑手段。
- 云计算的安全防护体系技术体系和实现方法也跟随着云计算的技术演进步伐，不断演进和完善
  - ✓安全防护措施的部署-主要通过合理设计虚拟化网络逻辑结构，将虚拟化安全设备部署在合理的逻辑位置，同时保证随着虚拟主机的动态迁移，能够做到安全防护措施和策略的跟随
  - ✓安全防护技术体系架构-由硬件变化了软件，检测类：捕获相应的数据流量，但不再进行转发。如vNIDS、网络流量检测等；控制类：拦截网络流量，并进行安全处理后进行转发。如防火墙、Web应用防火墙等

Thank you

本讲义素材来自网络，仅做个人学习之用！

特别鸣谢

小标题

北宙咨询 North Universe

Trendsetting Consulting

特别鸣谢

艾拓咨询 AituoXianfeng Consulting