信息安全管理
先锋论坛

跟我学信息安全管理

01、安全的云　徐雪松

信息安全管理专家委员会发布
2016年4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YY频道89519382 ）
- 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

徐雪松

拥有ITIL Foundation 、 ISO27001 LA、高级软件设计师、 CCM云安全评估师、 CISP等资质。拥有5年的管理咨询和信息安全从业经验，对信息科技风险治理、信息安全管理和技术有着多年的从业经验，目前在北京趋势引领咨询事业部华南区担任咨询顾问，曾在国内知名安全厂商从事多年的信息安全工作。为四川农信、上海银天下、中国农业银行、郑州商品交易所、攀枝花商业银行、南充商业银行、盛京银行、哈尔滨银行、四川电信、四川移动、西藏移动、西藏联通、红河供电局等组织提供过信息安全管理咨询工作。

近三年的主要咨询项目：

作为项目经理，负责四川省农村信用社信息科技中心信息安全管理体系建设；
作为项目成员，参与郑州商品交易所可用性深化项目；
作为项目成员，参与盛京银行ISO20000&ISO27001双体系建设项目；
作为项目成员，参与哈尔滨银行ISO27001体系建设项目；
作为项目成员，参与上海银天下科技ISO27001&ISO20000双体系建设项目；
作为项目经理，负责攀枝花商业银行科技达标咨询项目；
作为项目经理，负责四川移动ISO20000&ISO27001体系建设项目；
作为项目经理，负责西藏移动信息安全管理优化项目；
作为项目经理，负责西藏移动安全运行项目；
作为项目经理，负责四川电信省监控维护中心（NOC）服务项目；
作为项目成员，参与贵州电网信息安全标准规范建设及完善项目；
作为项目经理，负责云南红河电网ISO27001体系建设项目；

1

什么是云

什么是云呢？


cloud
computing
SaaS
PaaS
IaaS
HaaS
pricing
Service
model
private
Virtual
data
Amazon
Google
Engine
Cloud-provider
Cloud-broker
Cloud-Oriented
Azure
Services
Internal
Architecture
Hosted
Private
Cloudware
technology
Mashup
Cluster
self-service
Apps
Pay
Live
App
Middleware
migration
Utility
External
center
application
Elastic
Subscription-based
Cloud-operating
Cloud-portability
IBM
Cloudsourcing
Cloudstorming
Windows
Smart
Public
Cloud-storage
Vendor
Customer
CDN
lock-in
Salesforce.com
Consumption-based
Vertical
On-demand
Disruptive
Business
Hybrid
service
provider
Advertising-based
VPC
EC2
Microsoft

IT模式的转变

传统IT模式

单位机房

各单位独立购买硬件，自行建设政务系统。

独立管理

各自单位的管理人员进行IT规划建设和日常管理

目前到未来IT模式

虚拟化

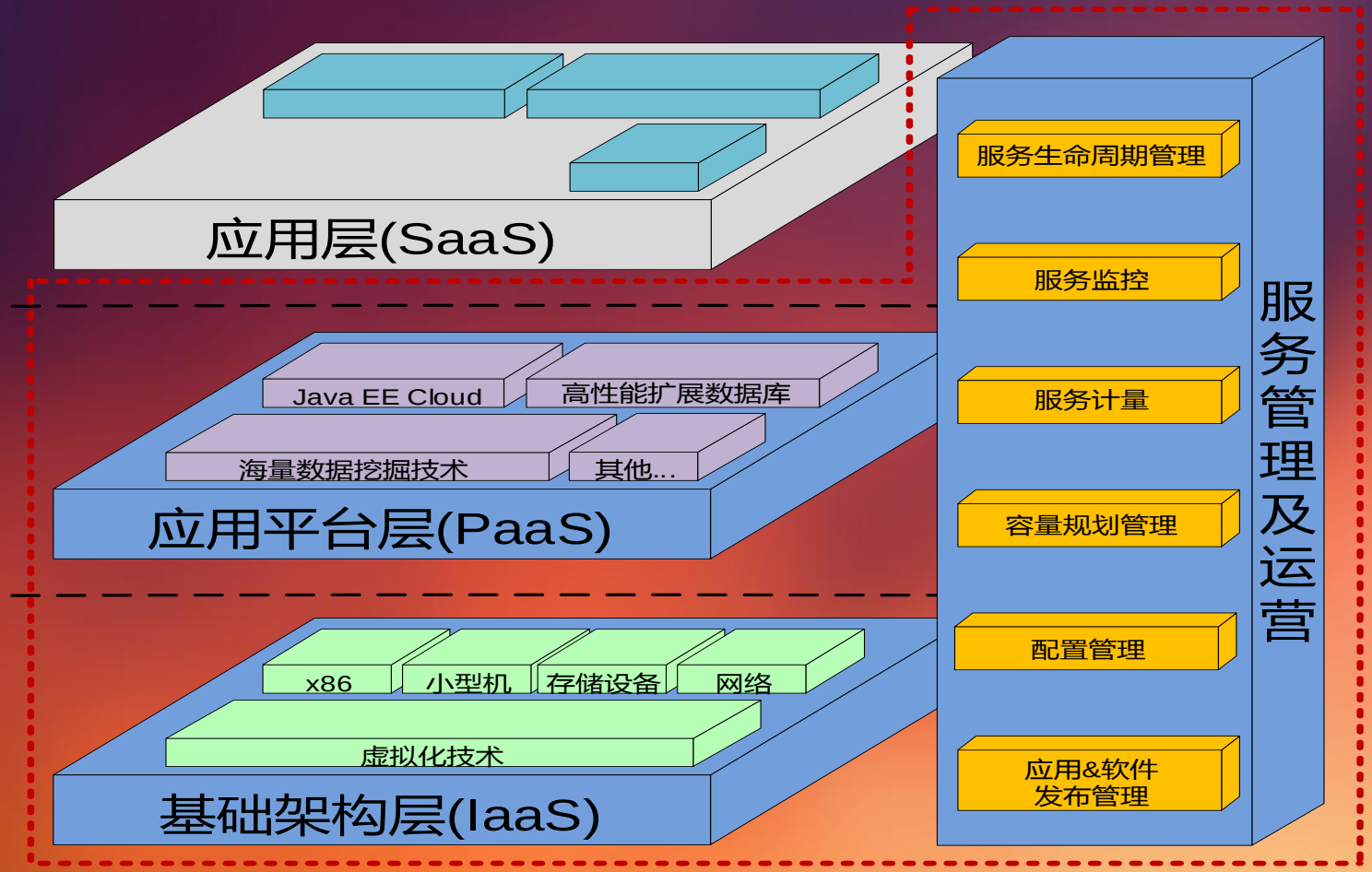
通过更好地利用资源，产生更高的IT效率

云计算、大数据

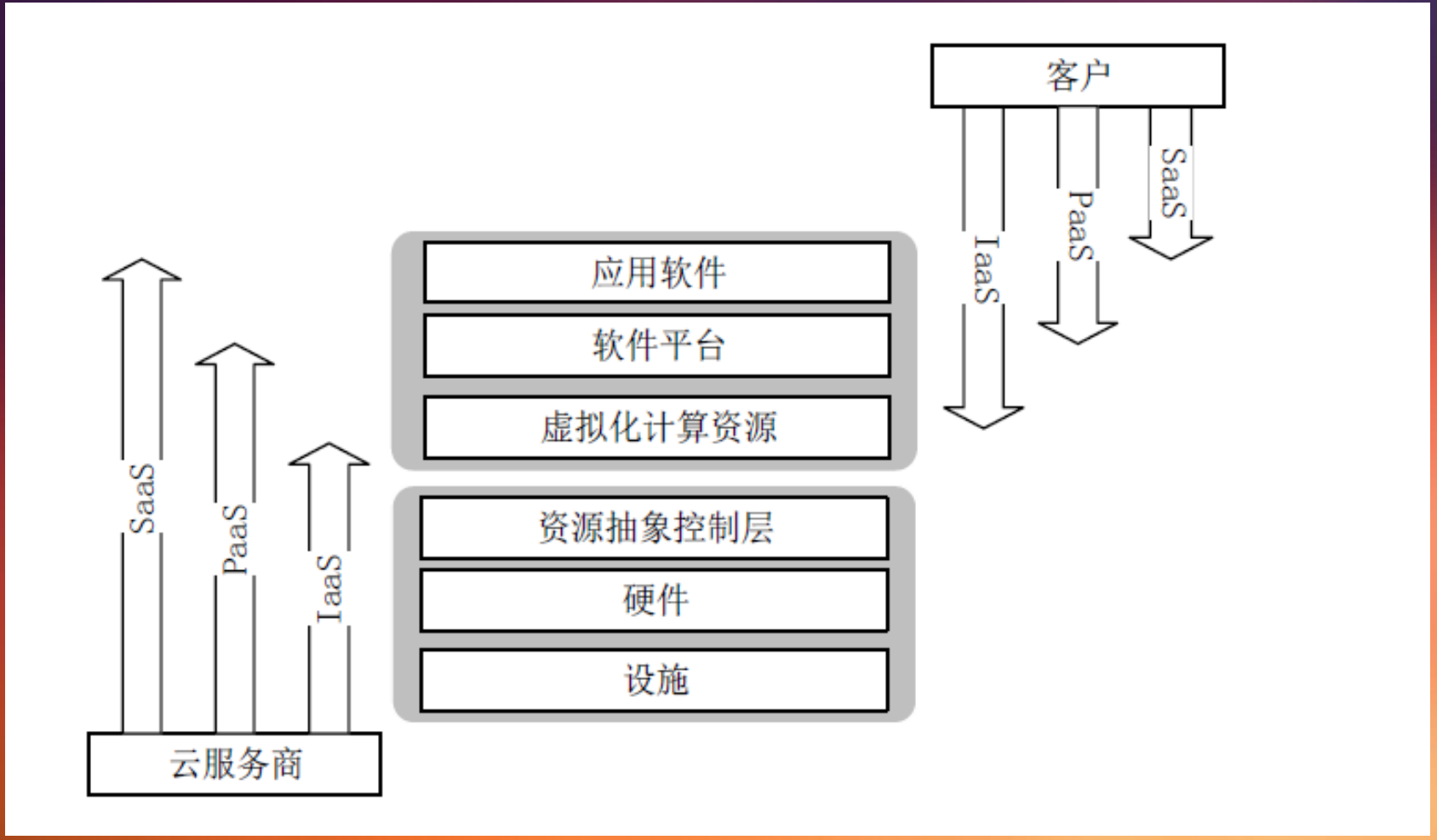
公共云和私有云解决方案，推动更高的敏捷性。

但云计算并不适用于所有场景

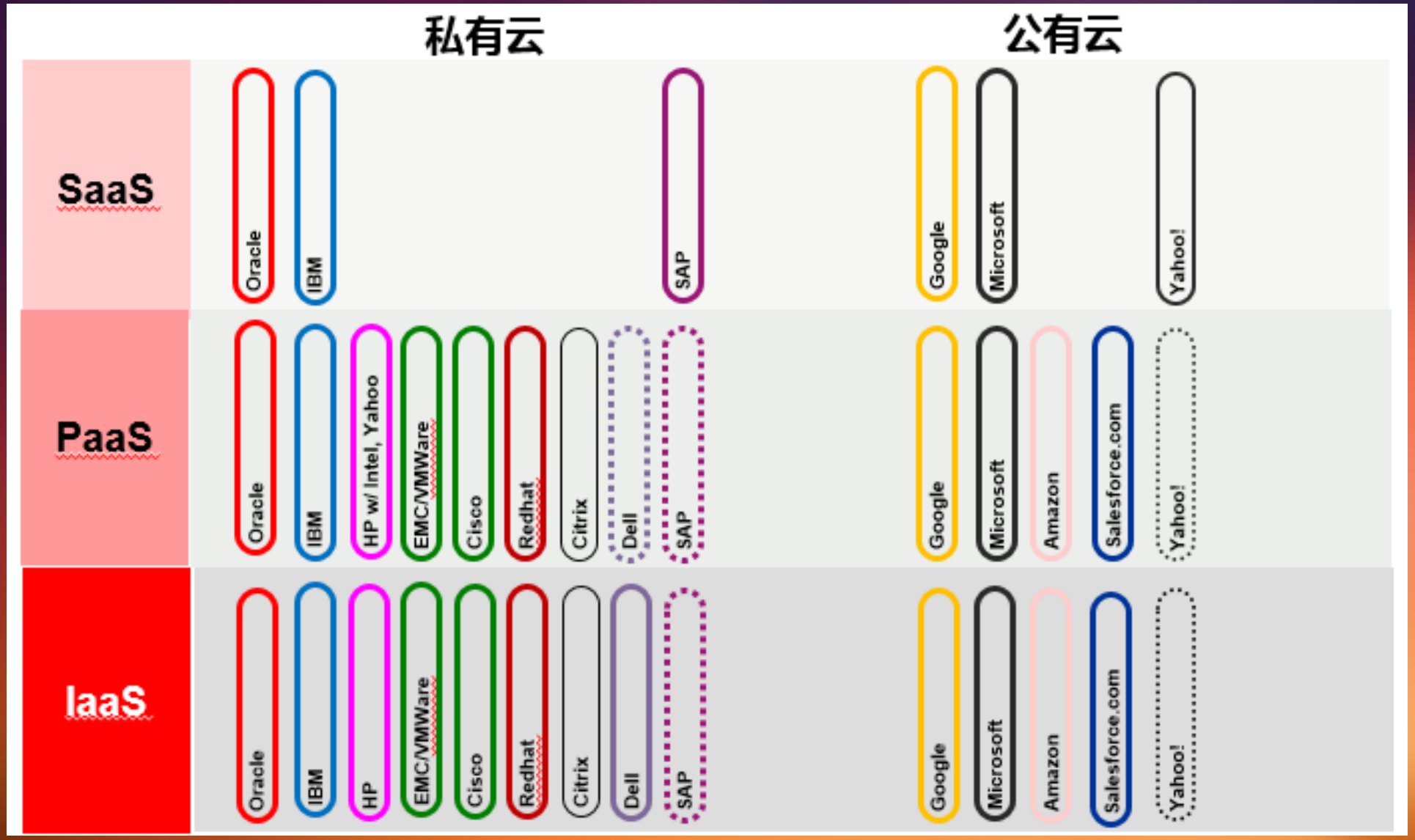
云的形态


应用层(SaaS)
Java EE Cloud
高性能扩展数据库
海量数据挖掘技术
其他...
应用平台层(PaaS)
x86
小型机
存储设备
网络
虚拟化技术
基础架构层(IaaS)
服务生命周期管理
服务监控
服务计量
容量规划管理
配置管理
应用&软件
发布管理
服务管理及运营

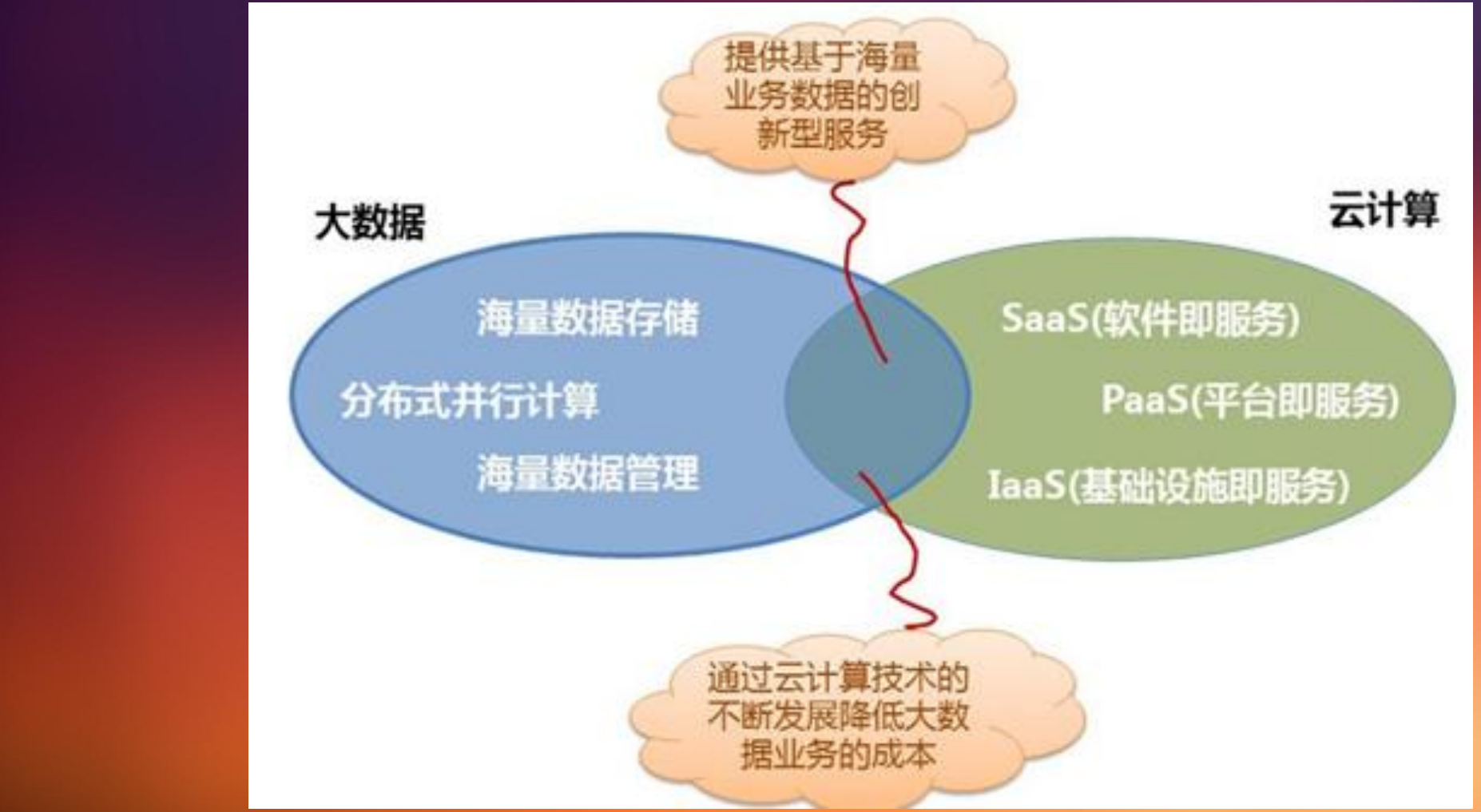
云的模式


客户
SaaS
PaaS
IaaS
应用软件
软件平台
虚拟化计算资源
资源抽象控制层
硬件
设施
SaaS
PaaS
IaaS
云服务商

已有产品


私有云
公有云
SaaS
PaaS
IaaS
Oracle
IBM
SAP
Google
Microsoft
Yahoo!
HP w/ Intel, Yahoo
EMC/VMWare
Cisco
Redhat
Citrix
Dell
HP
Amazon
Salesforce.com

云计算和大数据


提供基于海量业务数据的创新型服务
大数据
云计算
海量数据存储
分布式并行计算
海量数据管理
SaaS(软件即服务)
PaaS(平台即服务)
IaaS(基础设施即服务)
通过云计算技术的不断发展降低大数据业务的成本

云安全吗？

安全问题

问题

- 客户对数据和业务的控制能力减弱
- 客户与云服务商之间的责任难以界定
- 可能产生司法管辖权问题
- 数据所有权保障面临风险
- 数据保护更加困难
- 数据残留
- 容易产生对云服务商的过度依赖

安全的威胁

模块	威胁源	管理员	用户	黑客
端	用户端	权限滥用 非法操作	恶意用户：仿冒其他用户登录，破解密码，具有获取VM数据的能力	伪造管理员 漏洞攻击 植入木马，非法获取VM数据
管	网络		截获其他用户密码 PC等设备绕过安全网关	常见网络攻击
云	虚拟机	非法重置用户密码 误挂卷 利用虚拟机备份文件非法恢复用户数据 虚拟机自然损坏	用户非法登录：弱口令或口令保管不善 攻击相邻虚拟机，如ARP攻击 非授权访问相邻虚拟机 攻击虚拟化平台 利用虚拟化资源从事非法活动，如攻击外网虚拟机迁移过程中安全策略失效	类似PC的常见攻击
	虚拟化层	管理员非法登录：利用弱口令或口令保管不善 权限滥用：在缺少三权分立的情况下，易发生关键操作无法回溯 破坏镜像文件：植入木马 管理员权限扩大化：如节点间采用互信，则获取单节点权限即可控制整朵云 非法获取敏感信息，如数据库口令 非法监视用户虚拟机流量 非法获取用户密码	还原出前一用户硬盘数据 还原出前一用户内存数据	利用租用的虚拟机攻击虚拟化平台 利用租用的虚拟机攻击虚拟化管理平台，如利用OS/Web漏洞 虚拟机迁移中截获用户数据

核心的安全问题

失去控制权

挑战

- 用户信息资产物理上失去控制：数据迁移到服务提供商云平台；
- 虚拟化技术带来的多租户基础设施共享

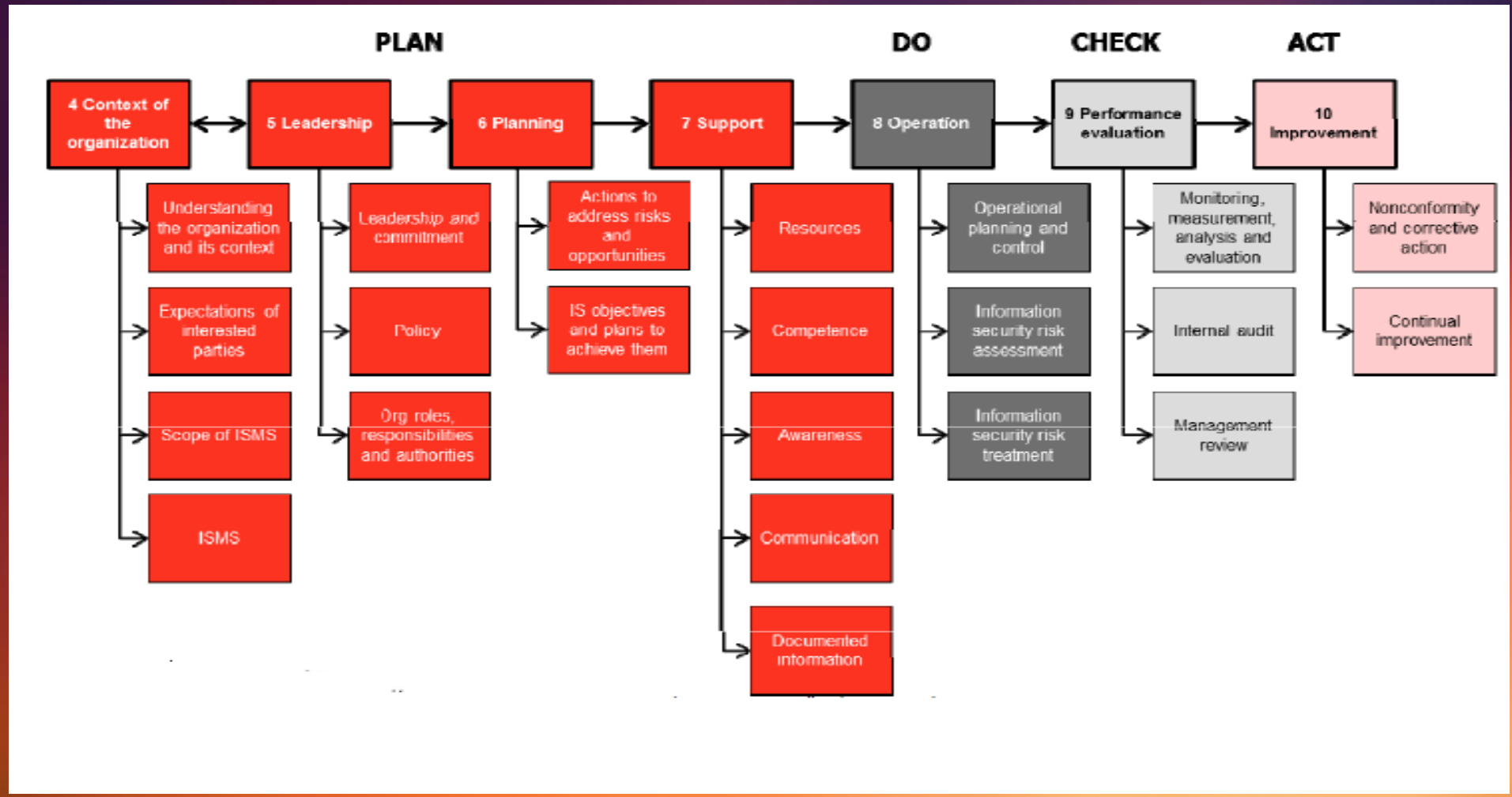
问题

- 数据集中，方便黑客发动攻击，事故影响范围广，后果严重
- 传统基于物理安全边界的防护机制在云计算的环境难以得到有效的应用
- 虚拟化下的多租户环境是否会导致数据泄露
- 是否有法规约束服务提供商的管理行为

2

云安全管理

ISO27001 : 2013



CCM

Domain	Name	中文	控制措施
1	Application & Interface Security	应用与接口安全	4
2	Audit Assurance & Compliance	审计保证与合规	3
3	Business Continuity Management & Operational Resilience	业务连续性管理与操作弹性	11
4	Change Control & Configuration Management	变更控制与配置管理	5
5	Data Security & Information Lifecycle Management	数据安全与信息生命周期管理	7
6	Datacenter Security	数据中心安全	9
7	Encryption & Key Management	加密与密钥管理	4
8	Governance and Risk Management	治理与风险管理	11

CCM

Domain	Name	中文	控制措施
9	Human Resources	人力资源	11
10	Identity & Access Management	识别与访问控制	13
11	Infrastructure & Virtualization Security	架构与虚拟化安全	13
12	Interoperability & Portability	协同与交互性	5
13	Mobile Security	移动安全	20
14	Security Incident Management, E-Discovery & Cloud Forensics	安全事件管理与电子调查/云取证	5
15	Supply Chain Management, Transparency and Accountability	供应链管理，透明度和问责制	9
16	Threat and Vulnerability Management	威胁与弱点管理	3

云安全的治理

	没有奖励	铜奖	银奖	金奖	金奖
分数	**1 至 3**	**4 至 6**	**7 至 9**	**10 至 12**	**12 至15**
要素	**没有正式的方法**	**消极**	**积极**	**改进**	**创新**
沟通和利益相关者的参与	1. 对利益相关方的识别是有限的或者不存在的。2. 已经识别出某些利益相关方但未进行沟通。3. 沟通发生了，但不存在沟通有效的证据。	4. 存在一些识别出利益相关方的有效证据，并且某些沟通是有效的。5. 进行一些重要的沟通。 6. 存在大部分沟通有效的相关证据。	7. 对利益相关方进行系统性的识别。8. 在经历预想的变化后，向利益相关方进行咨询。 9. 沟通流程的有效性受到监督和审查。	10. 利益相关方积极参与控制的改进措施。11. 利益相关方清楚地了解控制区域内的变化对其责任区域有哪些影响。12. 对沟通方法进行审查，以确保其有效性。	13. 相关的利益相关方了解控制区域内的监督和测量流程。14. 利益相关方了解控制区域将需要获得怎样的发展，从而实现企业的战略目标。15. 控制区域的管理者积极分享最佳实践，以支持企业其它领域内的发展。
政策、计划和程序，以及一种系统性方法	1. 不存在生效计划、流程或程序的证据。2. 遵循数量有限的未备案程序。3. 未备案的流程很明显涉及一些重要领域。	4. 有证据表明某些员工了解重要控制区域的相关已备案计划、政策 或程序。5. 有证据表明这些计划、政策 或程序通常被予以遵循。 6. 大多数计划、政策 或程序是最新的。	7. 对计划流程和程序进行例行审查，以确保它们是最新的。8..综合性的计划流程和程序涵盖大多数受控制的操作领域。 9. 大多数员工能够发现如何获得相关的计划、流程和程序。	10. 计划流程和程序涉及应急行动和例行操作。11. 在操作程序所属系统的背景下，对操作程序进行审查，以便在了解它们对系统其它区域可能产生的影响的情况下，进行相关变动。12. 已经识别出计划流程和程序方面的风险区域，并且尽可能地予以缓解。	13. 存在调整控制区域内所有计划流程和程序的强大领导力，以推动它们所属系统内的协调变动。14. 在了解如何根据组织愿景来调整计划流程和程序的情况下，对它们进行变动。. 15. 将计划流程和程序与组织内外的最佳实践进行比较。
技术和知识	1. 控制区域内的操作人员仅拥有执行基本职能的有限技能。 2. 仅部分了解技能要求3. 仅存在技能要求的部分定义。	4. 有证据表明员工有能力实施控制区域内的核心活动。5. 对操作控制区域所需的能力进行定义。6. 有一些证据表明员工能够对控制区域内发生的问题做出反应。	7. 员工有能力执行控制区域范围内定义的各种活动。 8. 对员工的能力进行监督，并进行相关记录。9. 对员工能力进行正式的监督。	10. 对员工能力进行持续监督，以发现任何弱点，并且积极改进薄弱点。11. 员工培训包括全方位的业务持续性计划。12. 考虑到员工培训的成本效益。	13. 建立了接班人计划，以确保技术的持续性。 14. 对人力资源进行管理，以确保始终存在在相关的时间尺度内对问题做出反应的称职员工。15. 考虑跨组织的培训方法最佳实践。
所有权，领导和管理	1. 可以识别出被指定的控制区域负责人。2. 控制区域负责人认可其职责。3. 控制区域负责人了解控制区域的范围。	4. 控制区域负责人了解控制区域内的重要活动。5. 控制区域负责人了解控制区域范围内所采取行动的更广泛涵义。6. 控制区域负责人有权力提供解决控制区域内问题所需的资源。	7. 控制区域负责人积极审查控制区域，以确保根据顾客要求对它们进行调整。8. 在处理审查时所发现的问题方面存在明确的领导。 9. 控制区域负责人有权在存在正当理由的情况下，提供采取预防性措施所需的资源。	10.在推动控制区域内的改进活动方面存在明确的领导。11. 有权力采取行动的人员定期对风险分析进行审查。12. 提供相关资源来进行积极的改进，以防止能够造成问题的潜在风险。.	13. 在根据整体经营战略对控制区域范围内的活动进行调整方面存在明确的领导。14. 能够迅速上报控制区域内问题的含义，并采取相关行动。 15..为领导职位建立了明确的接班人计划。
监督和测量	1. 对系统的某些领域进行信息监督。2. 信息监督将检测控制区域内的某些问题。 3.信息监督涵盖大多数的控制区域。	4. 正式监督涵盖重要的操作领域。5. 监督将对可能的问题进行检测。 6. 及时对监督信息进行审查。	7. 对监督信息进行正式分析。8. 监督均涵盖控制区域内的活动。9. 监督能够检测出控制区域内的各种问题。.	10..利用统计技术对监督信息进行分析，以发现异常。 11. 对异常进行调查，并采取恰当行动。 12. 根据对风险的仔细分析，定期对监督流程进行审查。	13. 定期对用来检测问题的监督程序的能力进行测试。 14. 每次在重要区域内发生重要变化时，都对监督流程进行审查。15. 根据行业最佳实践，对监督方法的基准进行例行的确定。

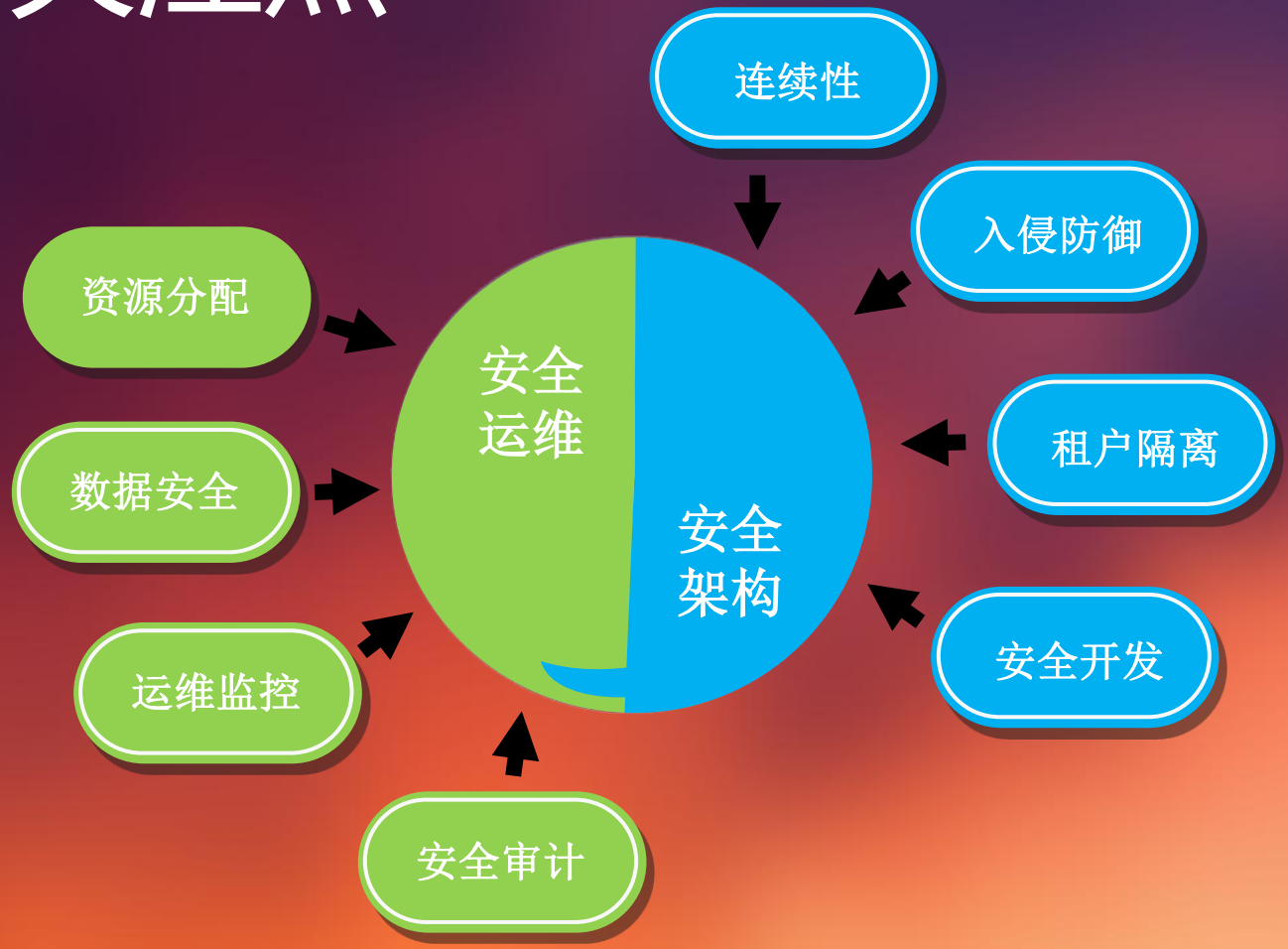
云安全的评价

Score	1 to 3	4 to 6	7 to 9	10 to 12	12 to 15
	没有正式的方式	被动式	主动式	改进级	优化级
Evidence/ Definition 证据/定义	1. 在相关的控制领域中没有管理的证据或系统	4. 在控制领域中，有系统化的证据涵盖关键操作。当需求时，具有文档化系统。	7.有一个强大的控制系统，包括控制区域内的所有的常规操作。	10.有证据表明控制区的系统能够管理应急事件以及日常活动。	13.控制领域责任人，可以证明他们积极主动评估最佳实践，在行业中和组织内，并运用在相关控制区域。
Managed 已管理	2. 有一些证据表明，具有文档化系统或可接受的工作方式	5. 在控制领域上，识别了清晰的责任人，理解其在该范围上的职责。	8.有证据表明，控制区域被主动监控和测量，并利用证据开展评价活动。	11.从各种来源的输入来决定如何管理风险和改进该控制区域的操作。	14.控制区域责任人积极分享最佳实践，基于他们在相关控制领域中的经验，来支持组织其他控制领域的发展。
Followed / Effective 遵守/有效	3.有一些证据表明，可接受的工作方式呗广泛理解和遵守	6.有证据表明该系统被一贯地理解和遵循	9.有证据表明，关键控制区域内的操作人员获得了适当的培训/技术，管理控制区管理的日常操作。	12.有证据表明，改进控制区域操作时，从系列的利益相关方获得输入，并且开展了监控和测量系统，	15. 对控制区域的变化，基于该组织的战略目标进行评估，

3

云安全技术

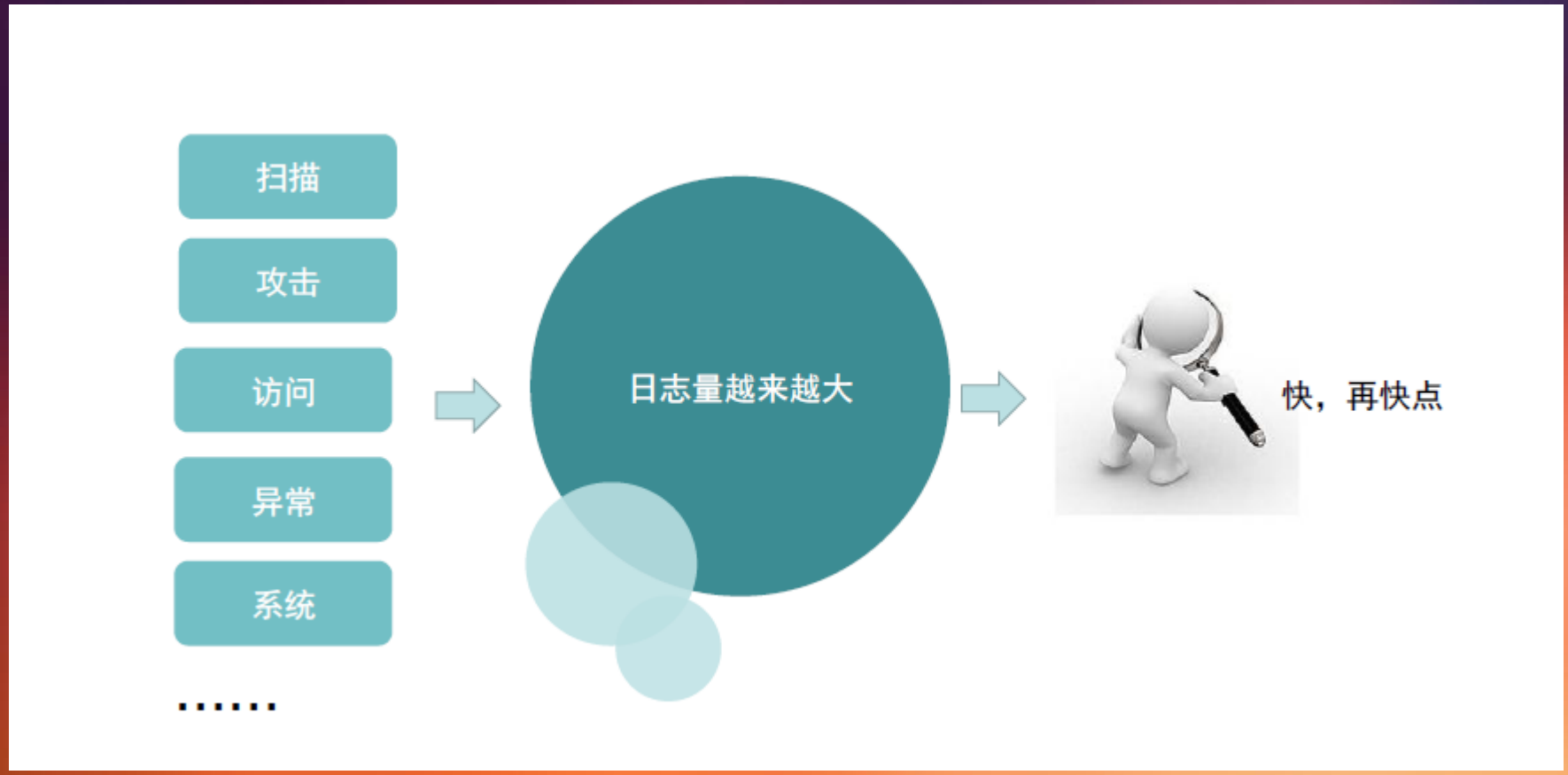
云安全的关注点



云安全架构层


安全检测能力
规则
异常算法
聚类算法
人机识别
关联分析
统计
大数据能力
分布式消息件
分布式流式处理引擎
分布式搜索引擎
分布式计算
日志收集能力
syslog
AD日志
http日志
数据库日志
bash
DNS
Windows主机
自定义日志

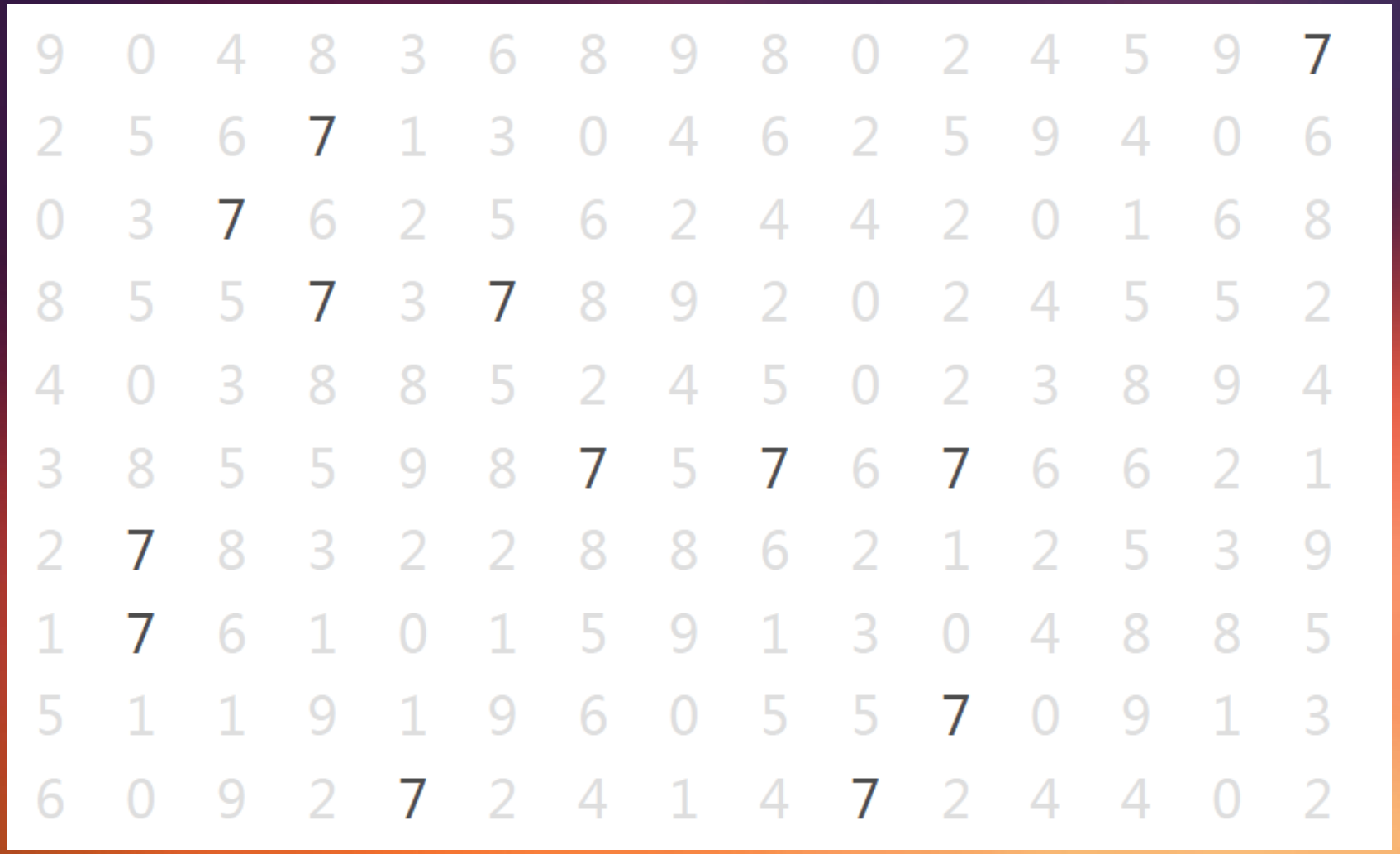
为什么选择做日志分析



大数据的难点

9	0	4	8	3	6	8	9	8	0	2	4	5	9	7
2	5	6	7	1	3	0	4	6	2	5	9	4	0	6
0	3	7	6	2	5	6	2	4	4	2	0	1	6	8
8	5	5	7	3	7	8	9	2	0	2	4	5	5	2
4	0	3	8	8	5	2	4	5	0	2	3	8	9	4
3	8	5	5	9	8	7	5	7	6	7	6	6	2	1
2	7	8	3	2	2	8	8	6	2	1	2	5	3	9
1	7	6	1	0	1	5	9	1	3	0	4	8	8	5
5	1	1	9	1	9	6	0	5	5	7	0	9	1	3
6	0	9	2	7	2	4	1	4	7	2	4	4	0	2

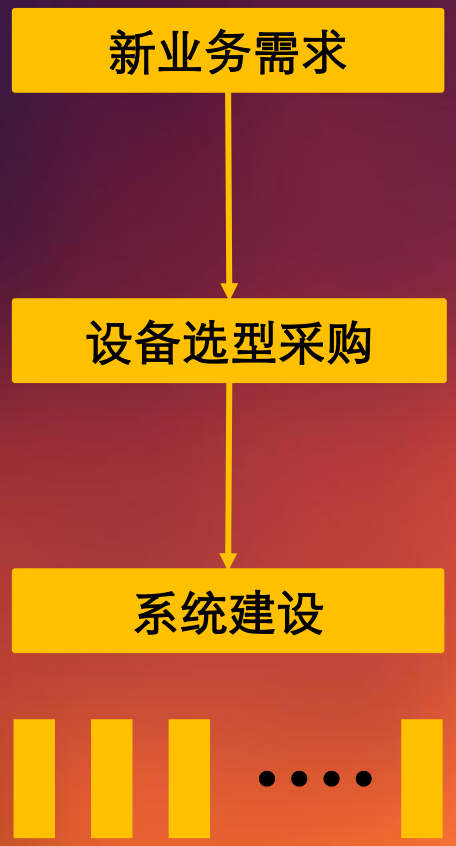
大数据


9 0 4 8 3 6 8 9 8 0 2 4 5 9 7
2 5 6 7 1 3 0 4 6 2 5 9 4 0 6
0 3 7 6 2 5 6 2 4 4 2 0 1 6 8
8 5 5 7 3 7 8 9 2 0 2 4 5 5 2
4 0 3 8 8 5 2 4 5 0 2 3 8 9 4
3 8 5 5 9 8 7 5 7 6 7 6 6 2 1
2 7 8 3 2 2 8 8 6 2 1 2 5 3 9
1 7 6 1 0 1 5 9 1 3 0 4 8 8 5
5 1 1 9 1 9 6 0 5 5 7 0 9 1 3
6 0 9 2 7 2 4 1 4 7 2 4 4 0 2

数据分析很大，我们做的事情很小

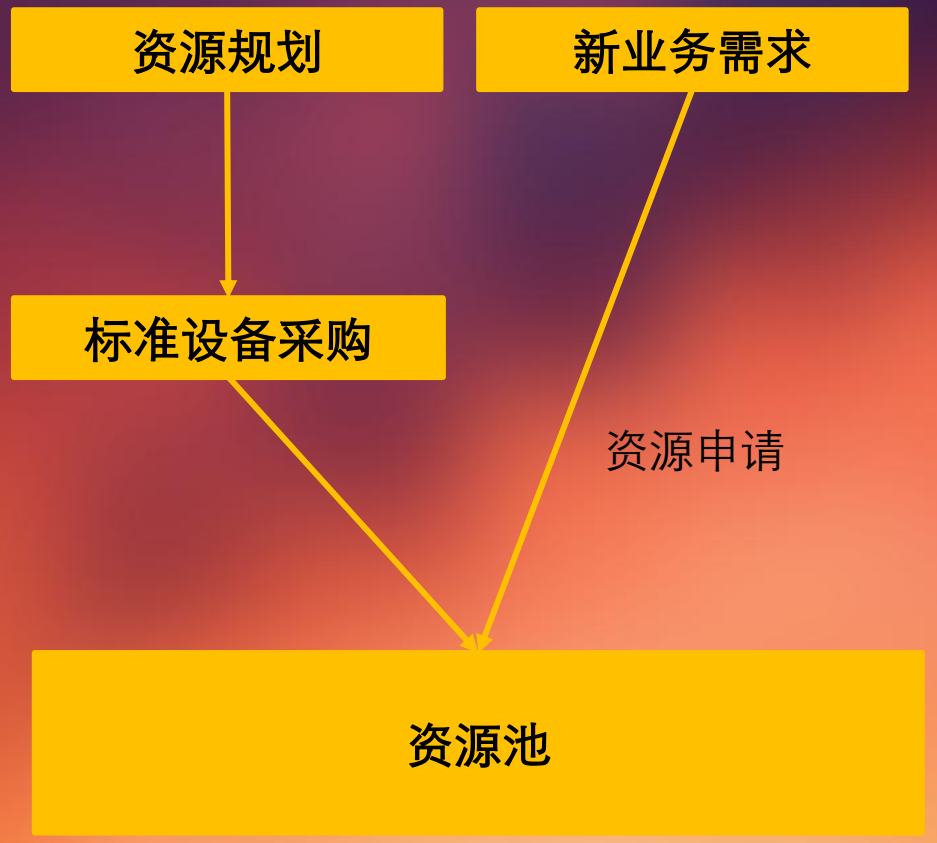
建设与运维

传统建设与运维方法



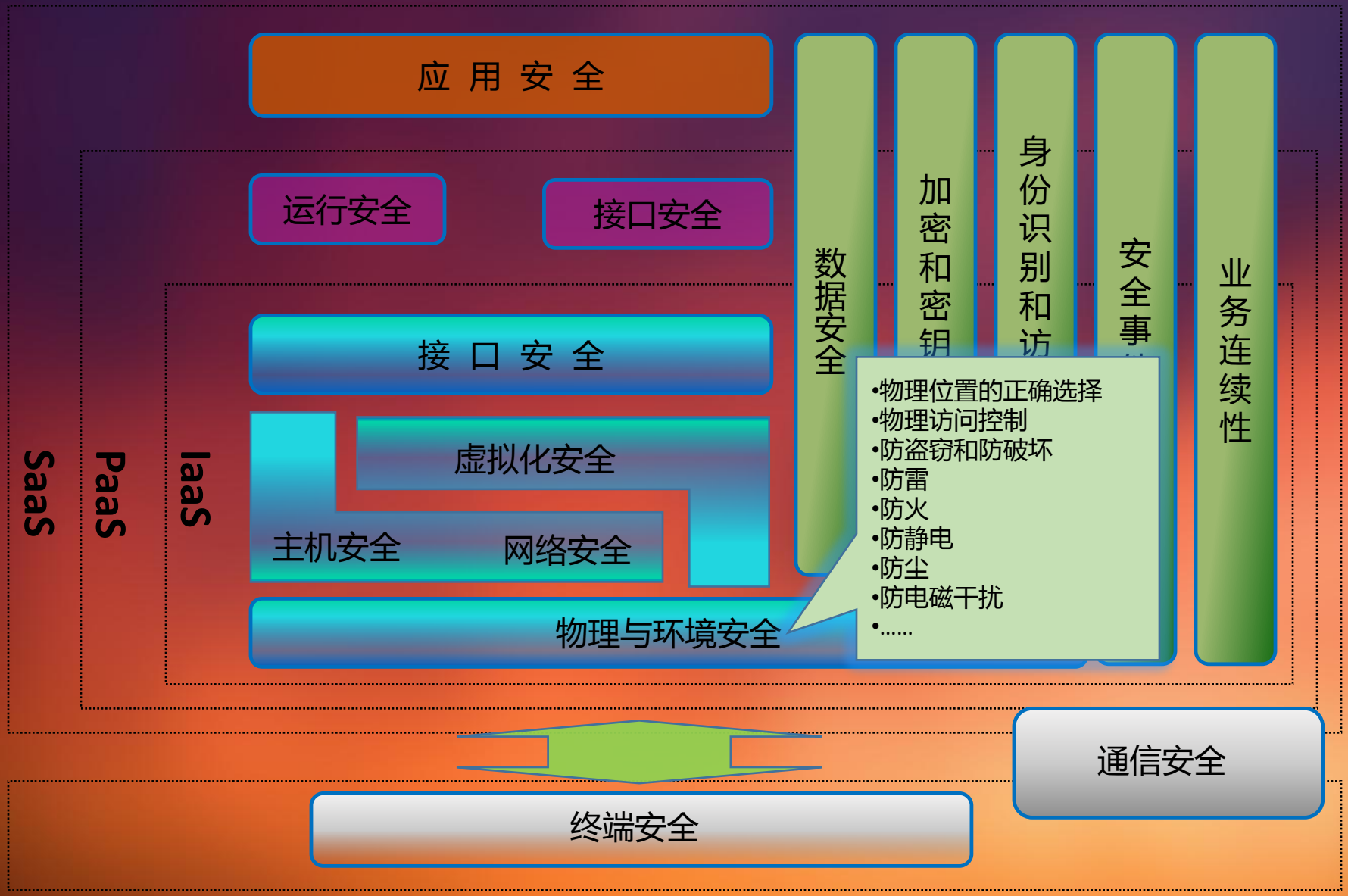
众多异构的纵向业务系统
各自独立运维

云计算的建设与运维方法



统一架构的资源池
统一系统运维，独立业务运维

云计算平台安全技术体系框架



云计算平台安全技术体系框架

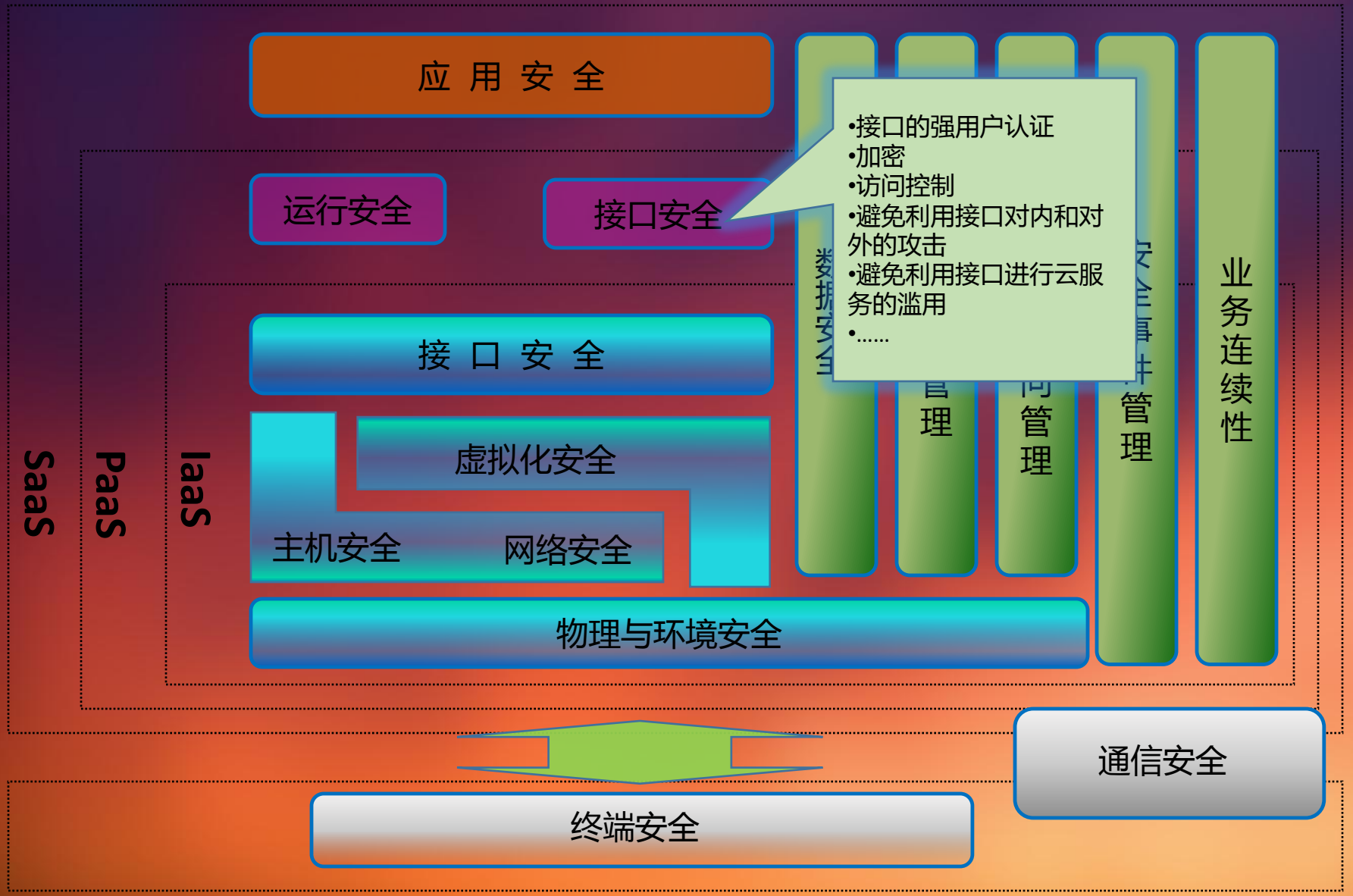
云计算平台安全技术体系框架

云计算平台安全技术体系框架

云计算平台安全技术体系框架

云计算平台安全技术体系框架

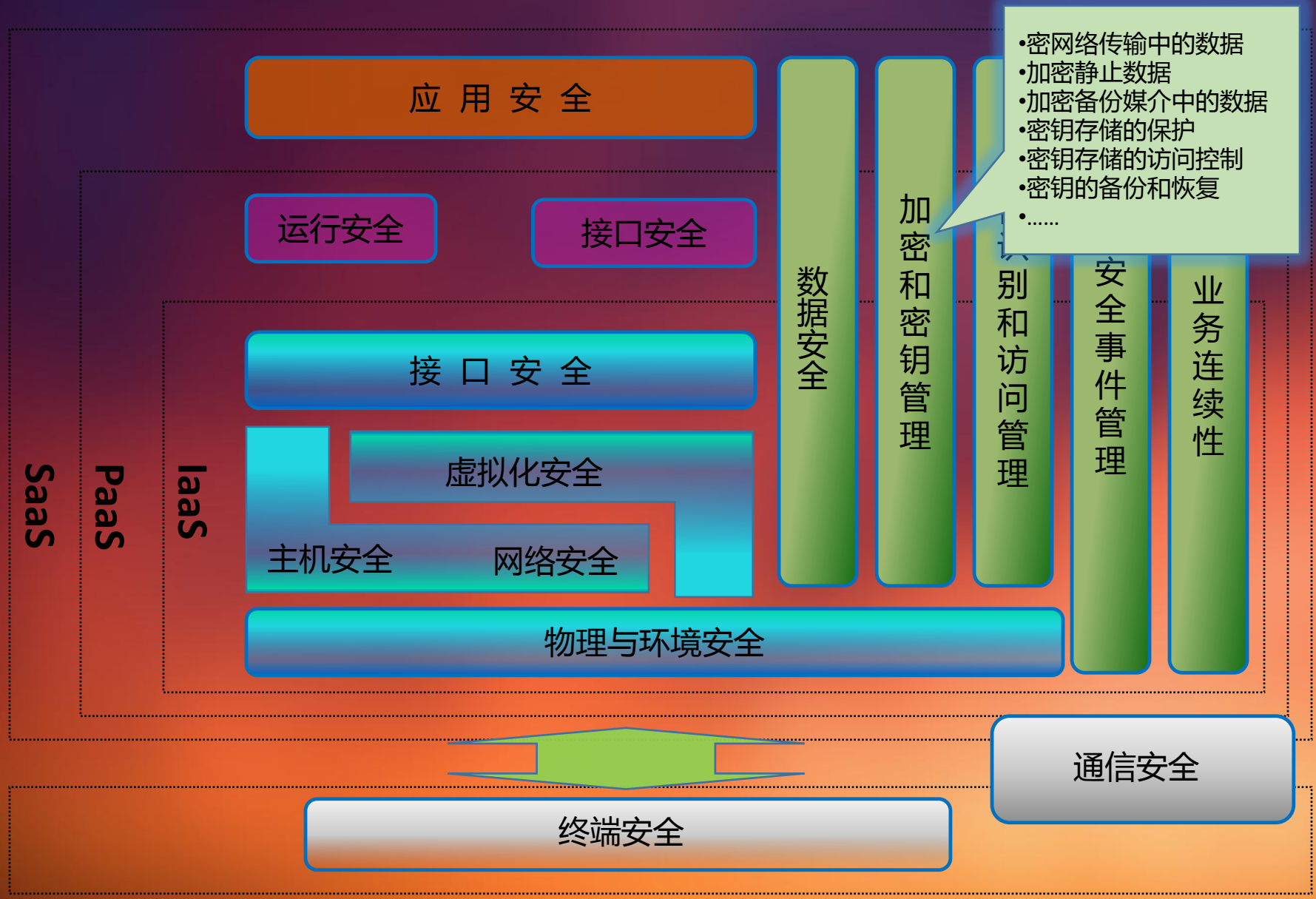
云计算平台安全技术体系框架



云计算平台安全技术体系框架

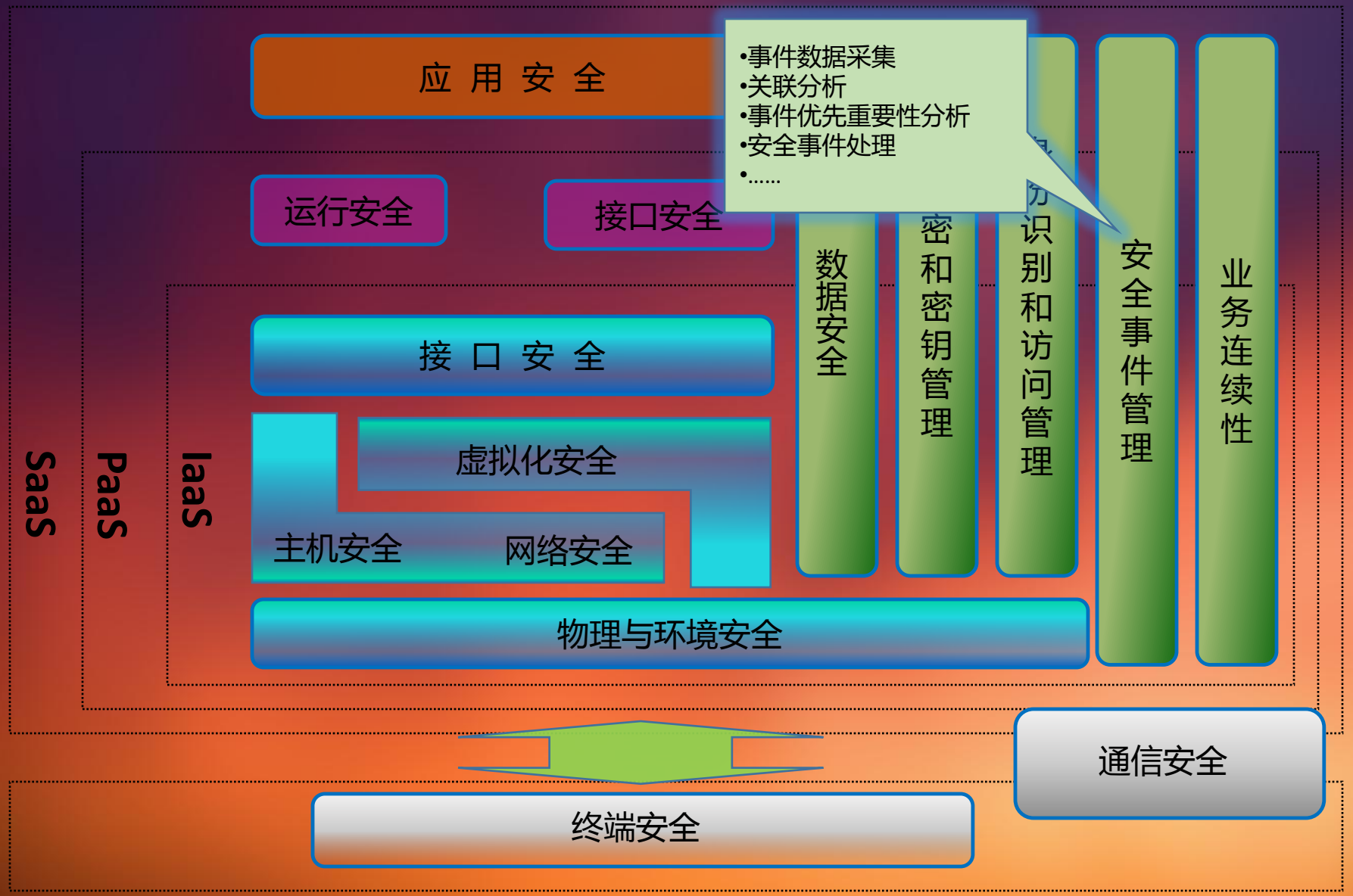
云计算平台安全技术体系框架

云计算平台安全技术体系框架



云计算平台安全技术体系框架

云计算平台安全技术体系框架



云计算平台安全技术体系框架

Thank you

云安全

徐雪松

特别鸣谢

小标题

北宙咨询 North Universe

Trendsetting Consulting

艾拓咨询 AituoXianfeng Consulting

特别鸣谢