云安全前瞻

Jay Heiser
@JayHeiser1

战略规划假设

到2020年，95%的云安全故障都是客户的错误所致。

不会发生的原因：

- 如果出现供应商错误，可能产生巨大的影响。
- 云市场经济依然疲软。

发生的原因：

- 公有云计算历史已经明显不存在供应商错误。
- 云服务供应商面临巨大的市场和互联网压力：
  - 他们必须优先考虑安全，别无选择。

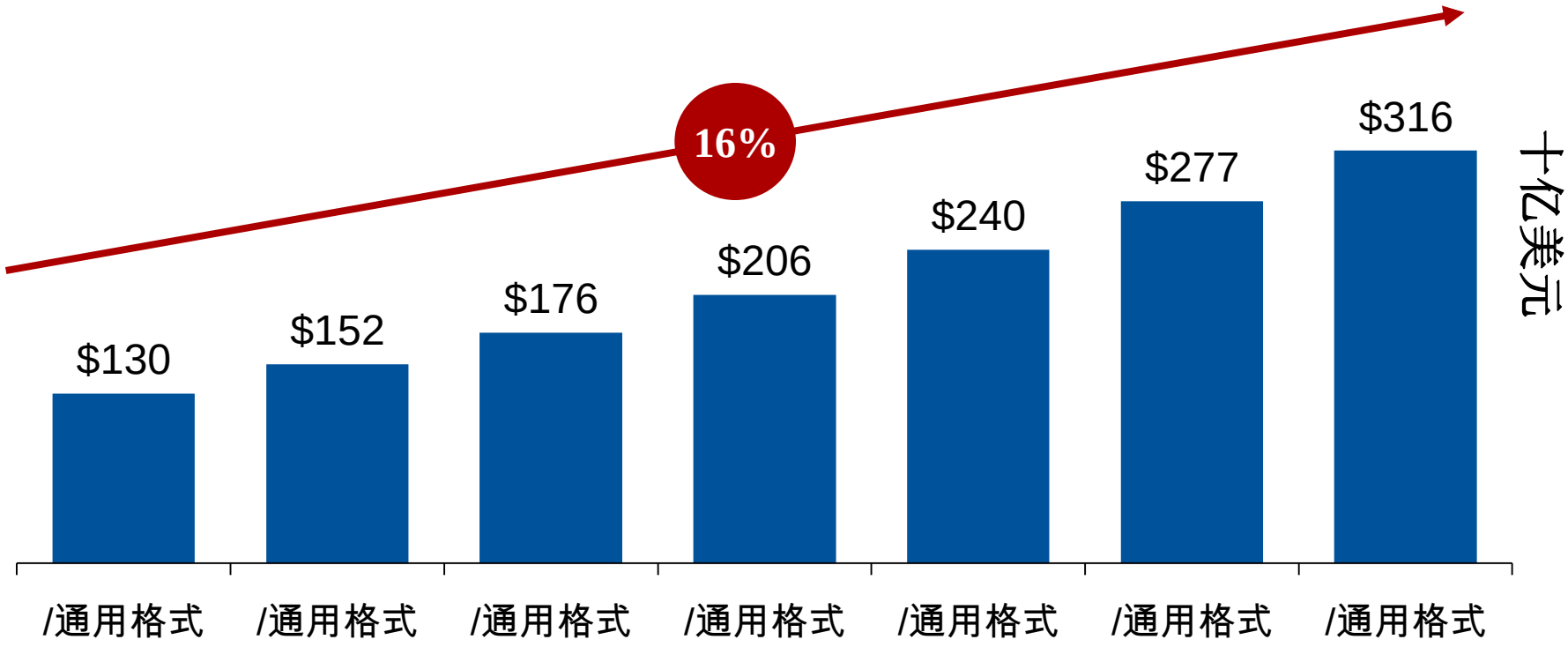
关键问题

1. 您应该担心哪些公有云风险？

2. 您需要做些什么来管理这些风险？

15.7%复合年增长率
Gartner公有云服务预测，2015年第一季度

在未来五年，企业将在公有云服务方面投入12000亿美元
(2015年至2019年)。



来源：“2013年到2019年全球公有服务预测，2015年第一季度更新”（G00275962）

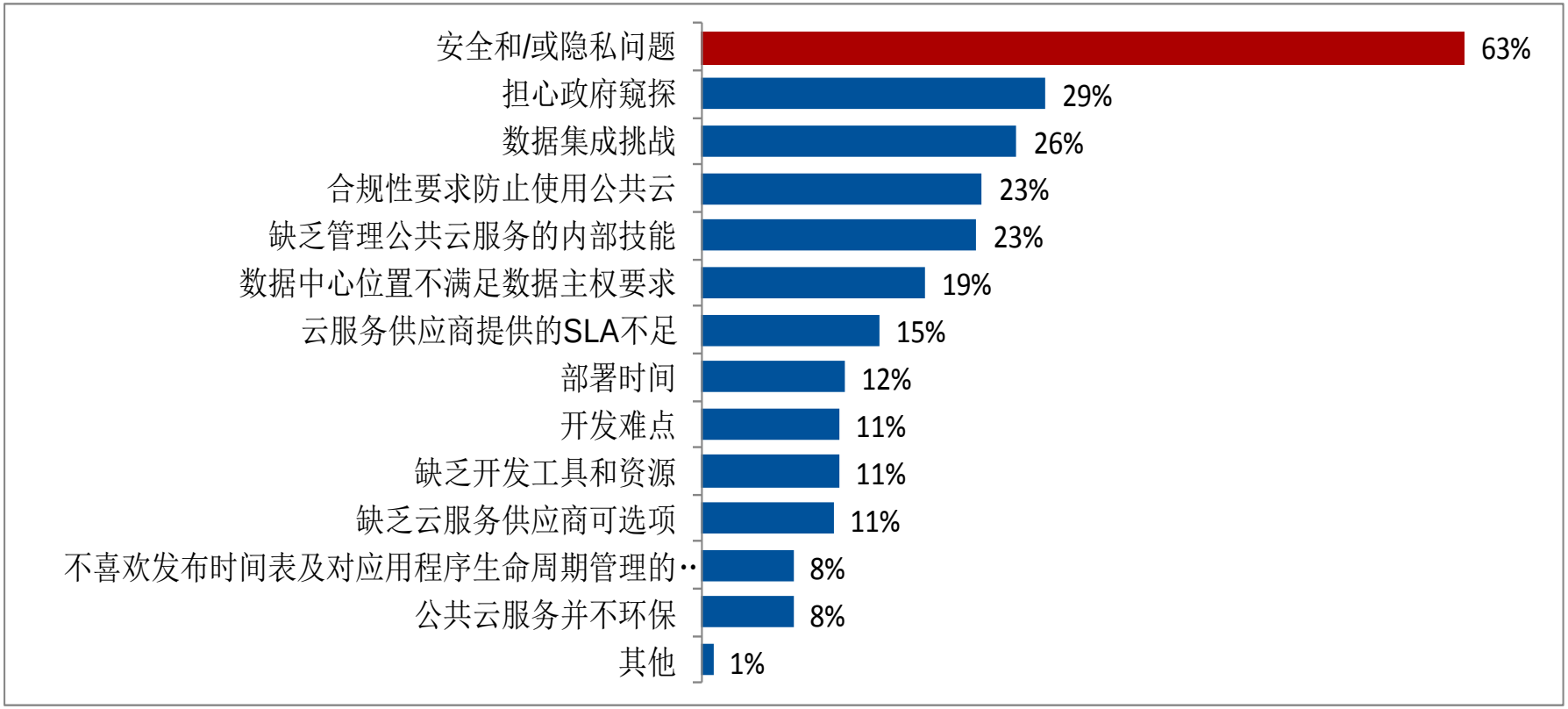
云计算使用情况分布

不了解这种模型　　寻找云策略　　开发最佳办法　　多种云

安全性如何？云应用调查（2014年）

不考虑公有云计算模型的三大原因是什么？

n = 210，基础：IaaS、Paas和/或/SaaS主要不采用公有云



允许3种回答

网络罪犯不是窃取云存储，而是窃取用户帐户。

网络钓鱼是最大的云安全故障来源。

企业专注于用错误的团队来提高安全性

云服务没有得到突破。

大多数安全事件都是客户的错误所致。

云安全方面的重大事件是还没有发生过重大侵入和故障事件。

各种组织争相采用云
低估了控制如何使用云所需的工作

- 帐号及虚拟机管理。
- **访问控制：**
  - **内部份额不当。**
  - **公有份额。**
- **可见性及活动控制：**
  - 核准使用和未经核准使用。
  - 事件响应。
  - 电子化搜寻。
- 与其他服务集成。
- 供应商破产或发生事故后恢复。

您将如何支持别人的中断应用程序？

不同云模型的重点不同

- 基础设施即服务：

- 人员及流程可进行安全远程访问
- 防止操作系统和应用程序漏洞
- 管理和跟踪虚拟机

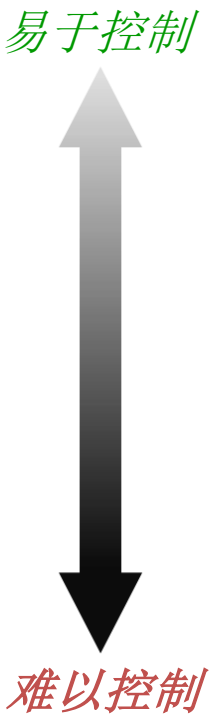
- 软件即服务：

- 访问供应商安全态势和控制功能
- 管理不同供应商的多个应用程序
- 确保正确使用数据
- 安全可靠连接移动设备、合作伙伴及 BYOD

您必须明确一致地进行身份和访问管理（IAM），
尤其是特殊访问权限管理（PAM）。

50道云灰色暗指不同的投入水平

- IT协调整个企业使用：
  - IaaS、SaaS和PaaS
  - -电子邮件和个人生产力
  - -文件同步和分享
- 部门协调使用：
  - IT支持策略服务：CRM、ERP、HR
  - 行业寻求其他应用程序
- 个人使用
- 合作伙伴强加

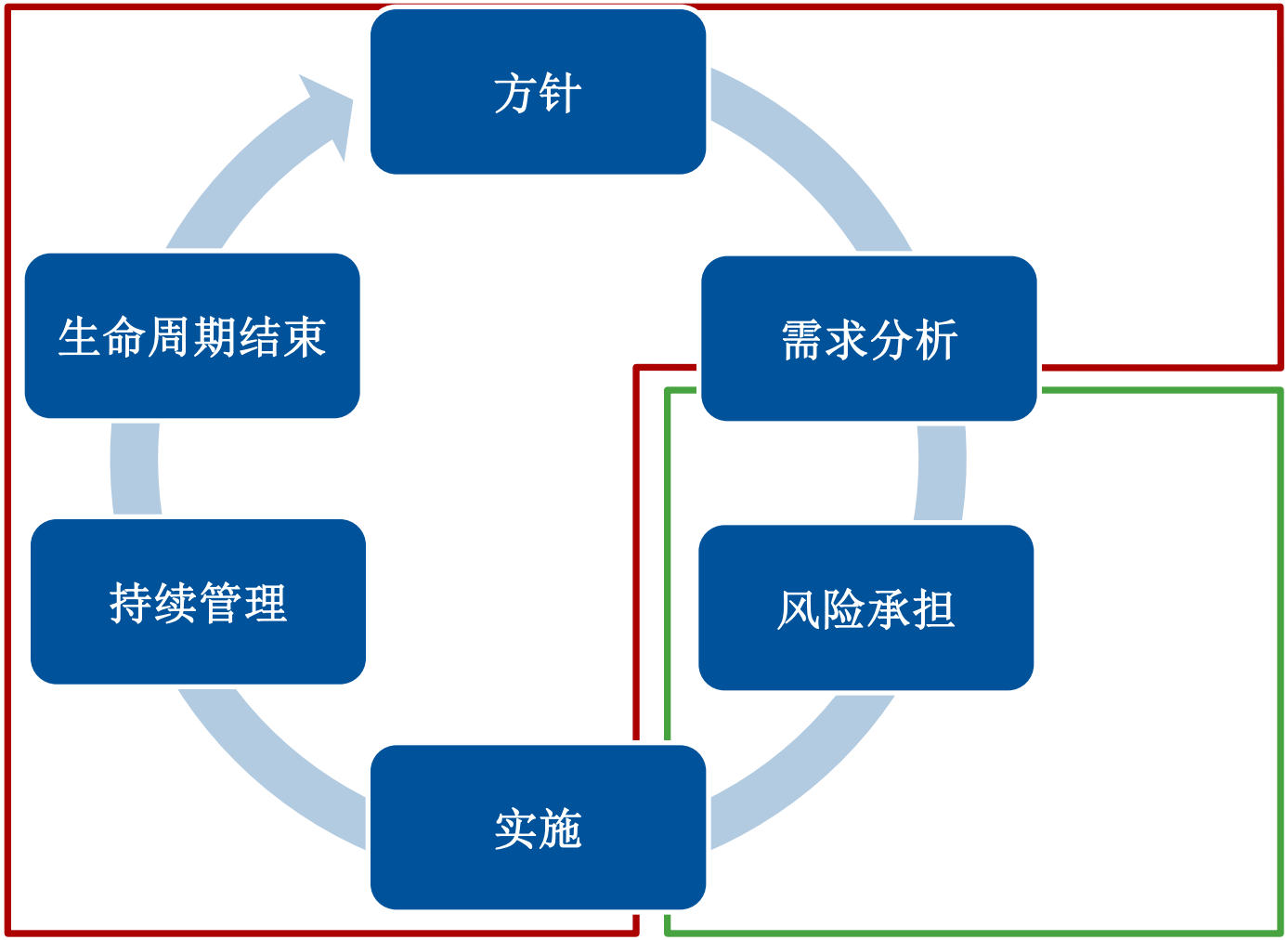


您需要云治理策略

- 以企业云策略开始：
  - 在哪种情况下应使用哪种云服务？
  - 职责分工？
- 实施方针和流程：
  - 风险承担和服务所有权
  - 云使用管理：
- 集中管理用户、数据和档案
- 持续监控供应商状态
- 事件响应和恢复

如果没有公司云策略，您最多能期望得到战术上的安全便利。

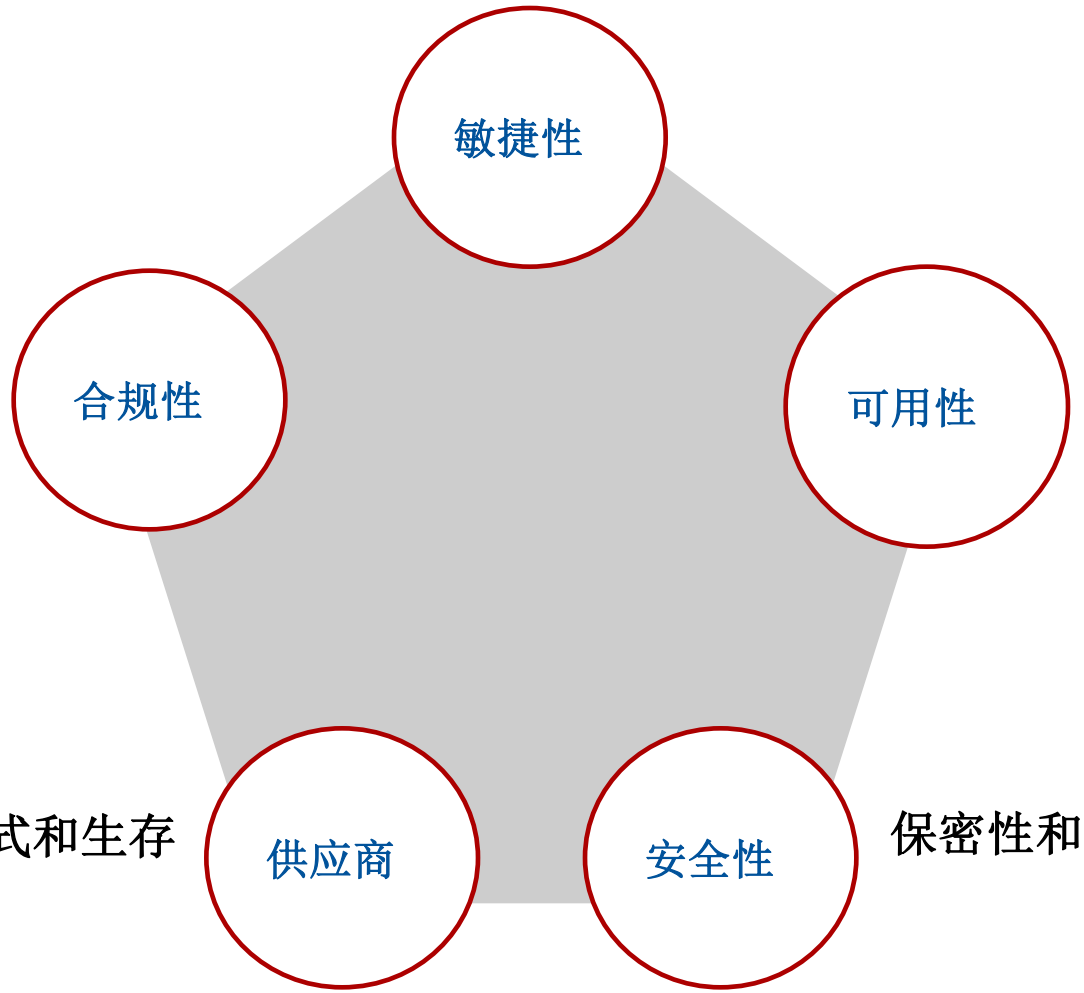
采用生命周期法进行云治理



通常需要更多的关注

大多数企业只满足一部分生命周期

根据公有云风险领域做出云使用决策



持续管理和控制过程
您必须实现各种形式的公有云

- 配置
- 身份和访问管理：
  - 用户权限管理
  - 身份、认证、权利
- 供应商：
  - SLA、绩效、交付和财务健康
- 用途：
  - 计费准确性、使用、成本优化、合同调整
- 用户活动监控：
  - 法规符合性
  - 电子证据和事件调查
- 数据备份和恢复：
  - 应急计划维护和调用

您不能外包这些控制责任

必须针对IaaS实施的控制

- 重要：
- 使用以工作为中心的安全方法
- 使用DevSecOps确保工作量得到加强
- 同样重要：
- 采用防火墙
- 加密所有网络流量
- 不要修补正在运行的机器
- 加密所有本机虚拟机存储
- CSP、虚拟机和操作系统安全和强化

需要安全技术能力，但可外包。

需要特定SaaS方法的控制活动

持续的

- 身份和访问管理
- 用户活动监控：
- 用户和实体行为分析
- 合规报告：
- 敏感信息的状态
- 数据管理和归档
- 年度应用程序组合评审

根据需要

- 问题解决
- 文件和对象恢复
- 定制化和集成
- 服务或数据恢复
- 事件响应/调查
- 电子化搜寻
- 转移到下一项服务
- 数据销毁和归档

云存储加密不能防止最可能出现的安全故障形式

- 云存储密码不能防止：
  - 帐号被窃取
  - 危害台式计算机
  - 权限低
  - 移动数据同步

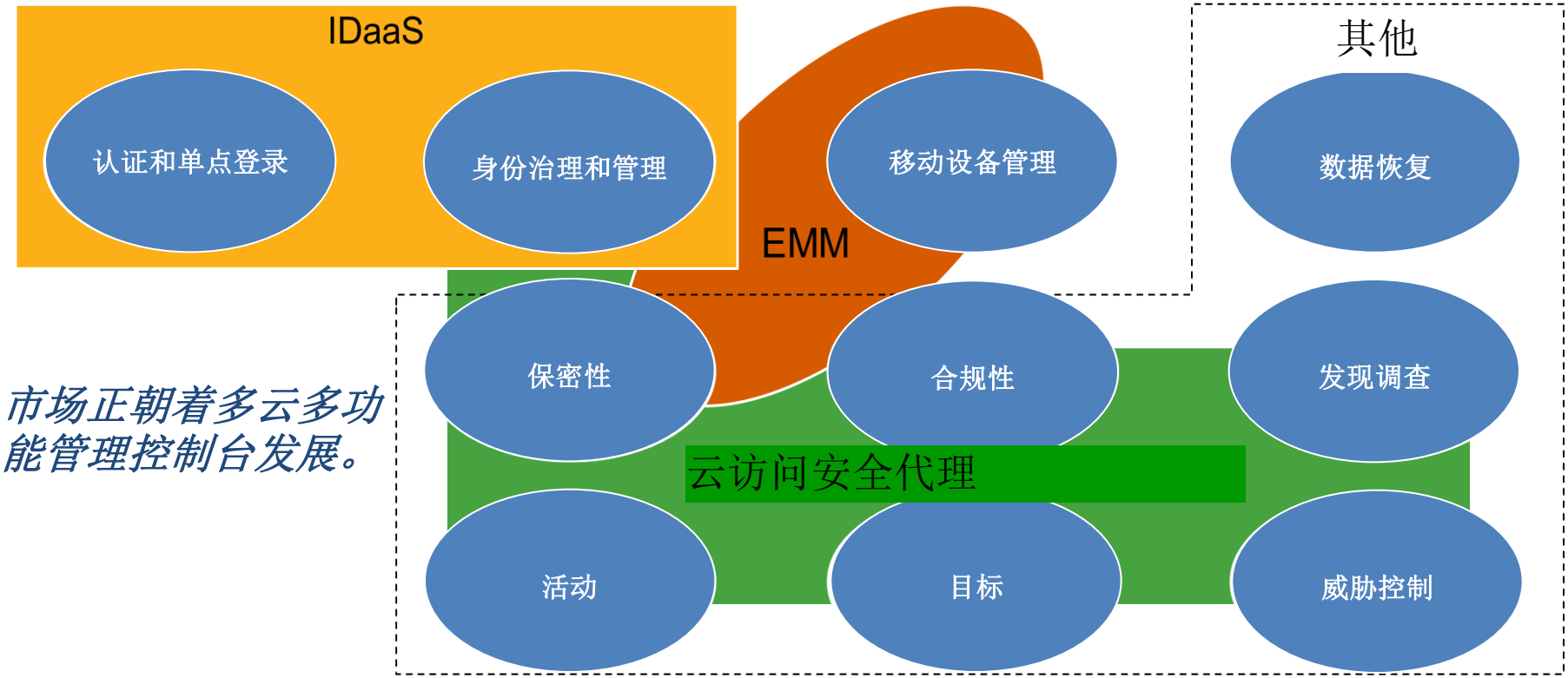
您是否将加密作为达到合规性所使用的遮挡方式？

云加密方法不断发展

- 相对容易：
  - 将数据加密扩展到端点
- 更容易：
  - 客户管理密钥（CMK）
- 困难或不可能：
  - 对保留格式加密
  - 可搜索
  - 同态

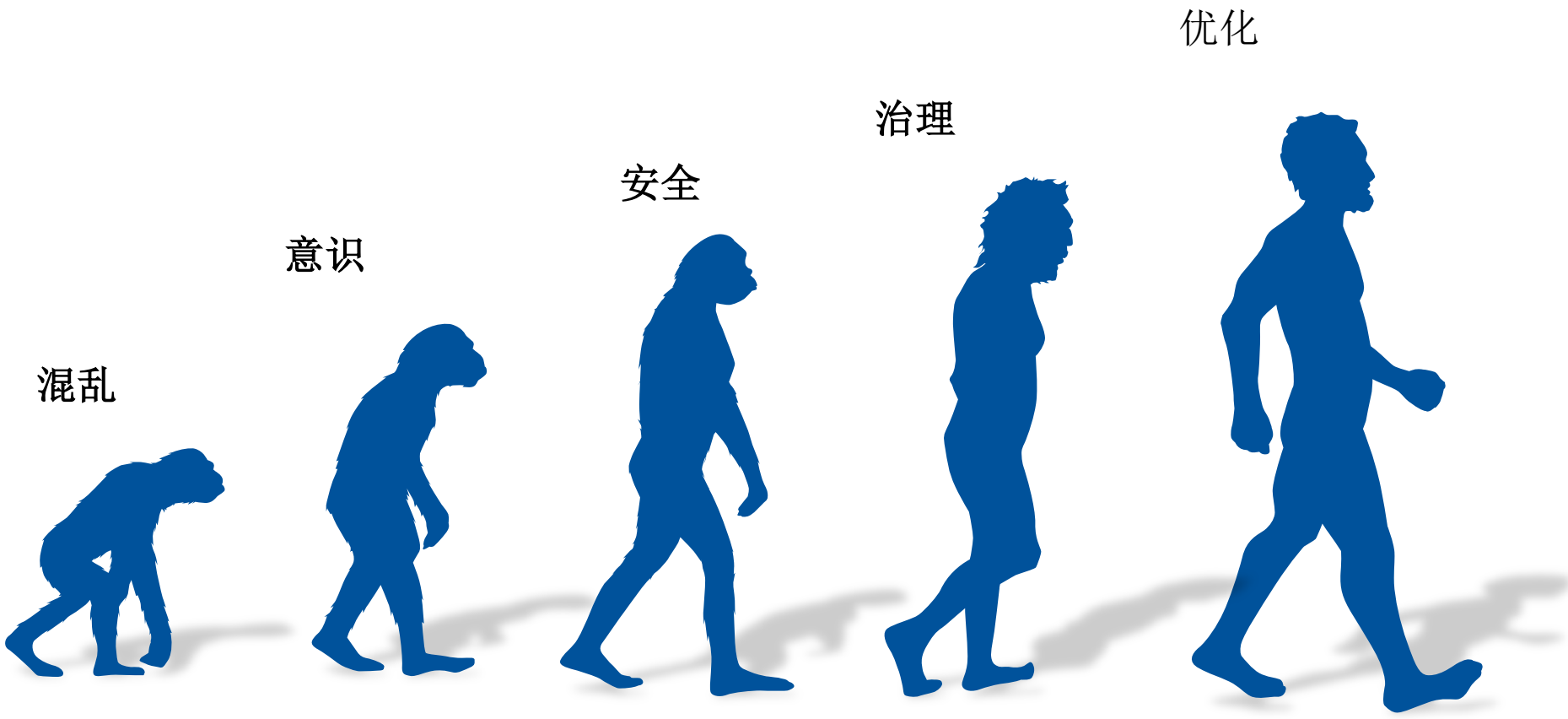
外部加密可能破坏云应用功能。

SaaS 控制附加的多样性不断增长



市场正朝着多云多功能管理控制台发展。

云控制是进展到什么程度？



不要停在安全阶段

建议

- ✓培养云安全和控制能力
- ✓制定并实施云治理方针：
  - 数据分类和风险承担；
  - 数据及部门应用程序的“所有权”。
- ✓管理帐号（特别是特权帐号）。
- ✓确保有应急预案。
- ✓要求符合标准，并提供第三方安全评估。

对自己的安全负责

Gartner建议研究

- *开发SaaS治理框架*

Jay Heiser (G00274895)

- *确保亚马逊网络服务工作量的最佳实践*

Neil MacDonald和Greg Young (G00275221)

- *公有云风险模型：接受云风险没问题，但忽略云风险会出现问题。*

Paul E. Proctor、 Daryl C. Plummer和 Jay Heiser (G00261246)

- *云 IaaS：安全注意事项*

Lydia Leong和Neil MacDonald (G00210095)

- *云安全技术成熟度炒作曲线，2015*

Jay Heiser (G00272321)

- *您对SaaS安全的所有认识都是错的。*

Jay Heiser (G00260951)

更多信息请见Gartner研究专区。

谢谢