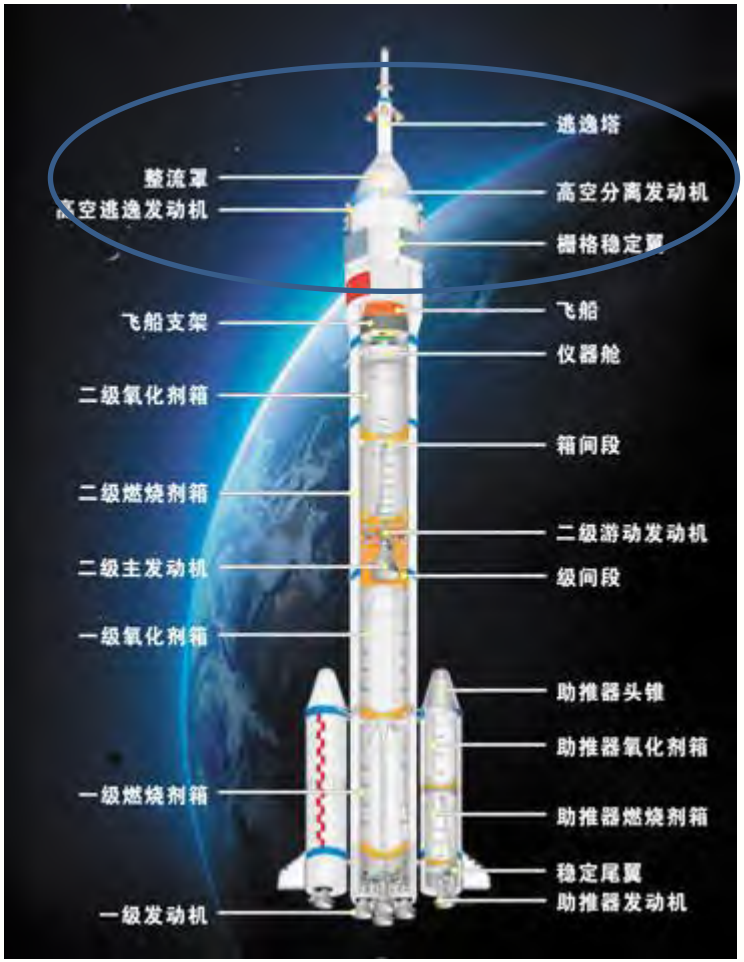
2017 可信云大会
可信云标准新一代
客户满意是未来
Cloud Computing Summit 2017.7.25-26

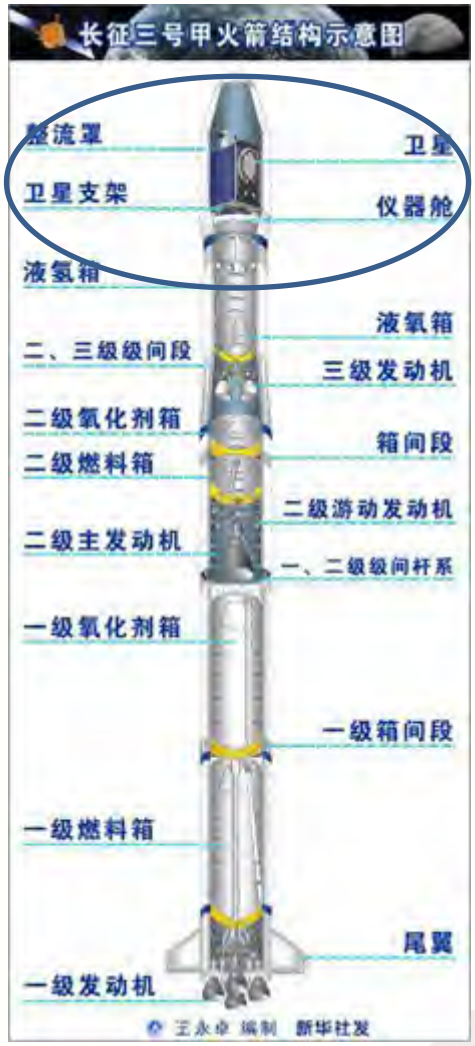
# 云工作负载安全保护最佳实践

青藤云安全
程度

# 工作负载举例

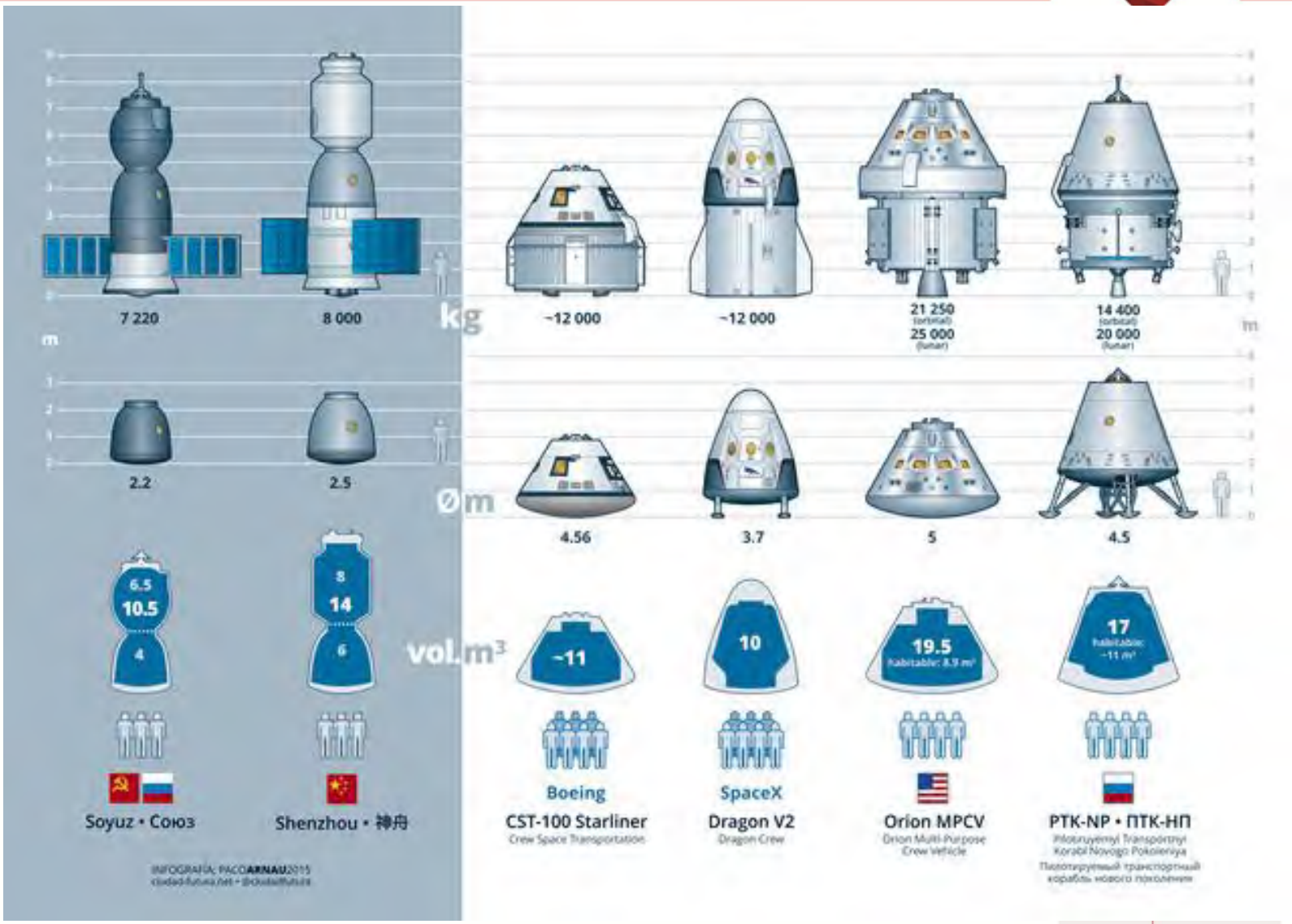



逃逸塔
整流罩
高空分离发动机
高空逃逸发动机
栅格稳定翼
飞船支架
飞船
仪器舱
二级氧化剂箱
箱间段
二级燃烧剂箱
二级游动发动机
二级主发动机
级间段
一级氧化剂箱
助推器头锥
助推器氧化剂箱
一级燃烧剂箱
助推器燃烧剂箱
稳定尾翼
助推器发动机
一级发动机


长征三号甲火箭结构示意图
整流罩
卫星
卫星支架
仪器舱
液氢箱
液氧箱
二、三级级间段
三级发动机
二级氧化剂箱
箱间段
二级燃料箱
二级游动发动机
二级主发动机
一、二级间杆系
一级氧化剂箱
一级箱间段
一级燃料箱
尾翼
一级发动机
王永卓 编制 新华社发

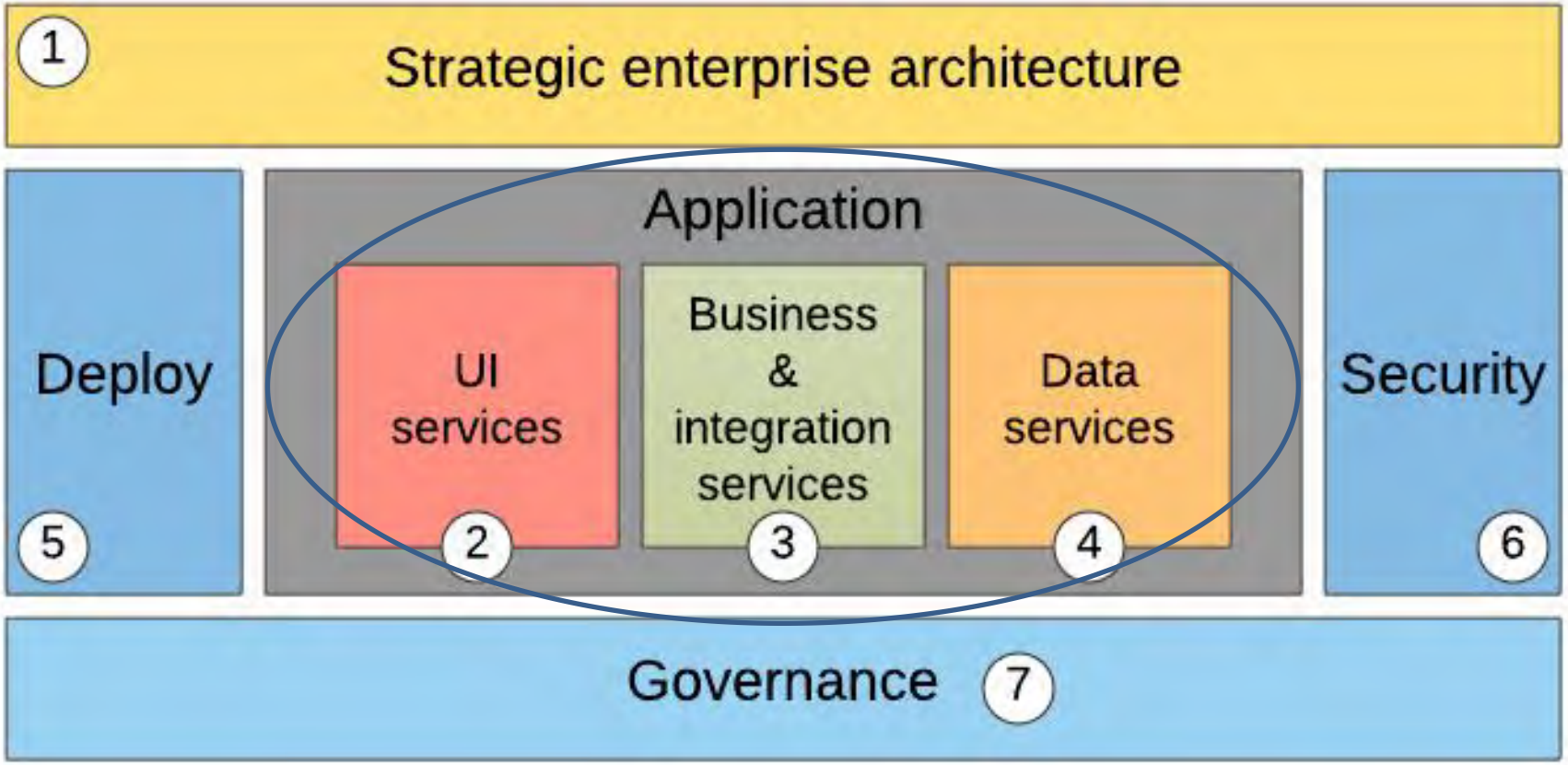
# 工作负载举例




m
7 220
8 000
kg
~12 000
~12 000
21 250
25 000
14 400
20 000
m
2.2
2.5
Øm
4.56
3.7
5
4.5
6.5
10.5
4
8
14
6
vol.m³
~11
10
19.5
17
Soyuz • Союз
Shenzhou • 神舟
Boeing
CST-100 Starliner
Crew Space Transportation
SpaceX
Dragon V2
Dragon Crew
Orion MPCV
Orion Multi-Purpose Crew Vehicle
PTK-NP • ПТК-НП

# 云工作负载模型

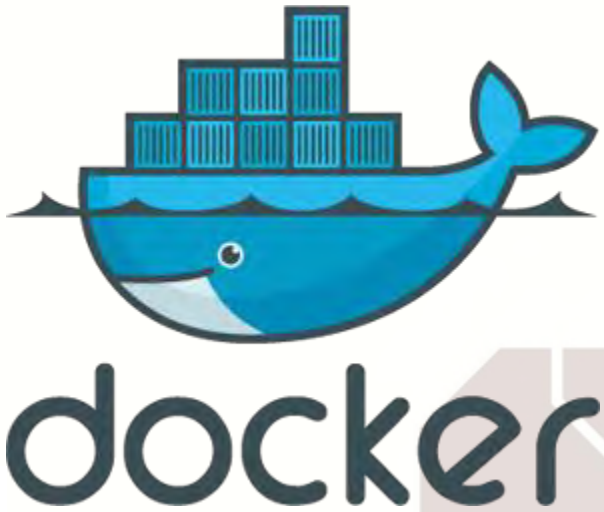


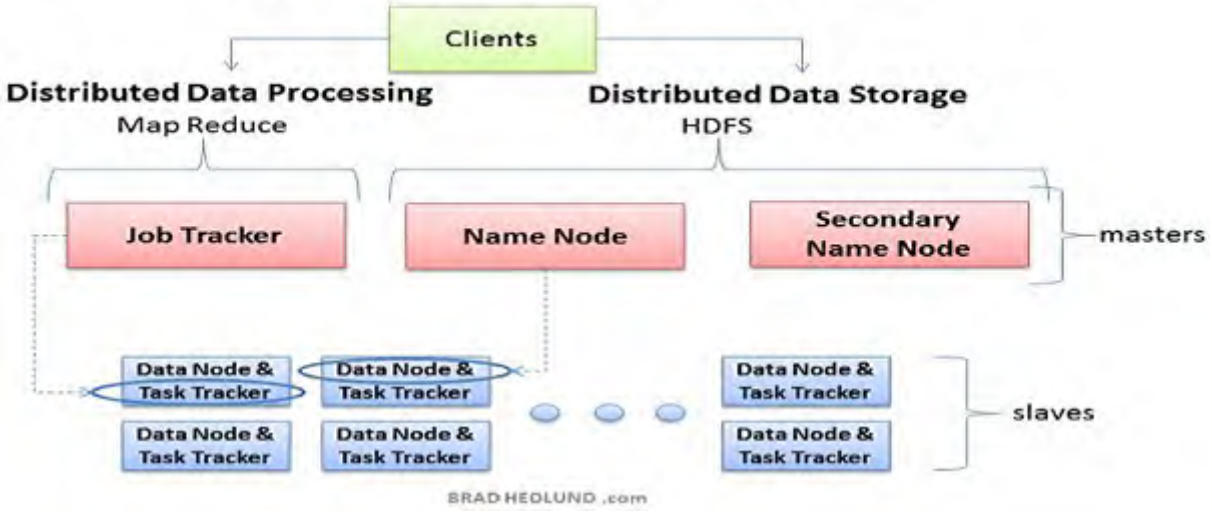

1
Strategic enterprise architecture
Deploy
5
Application
UI services
2
Business & integration services
3
Data services
4
Security
6
Governance
7

# 云工作负载定义



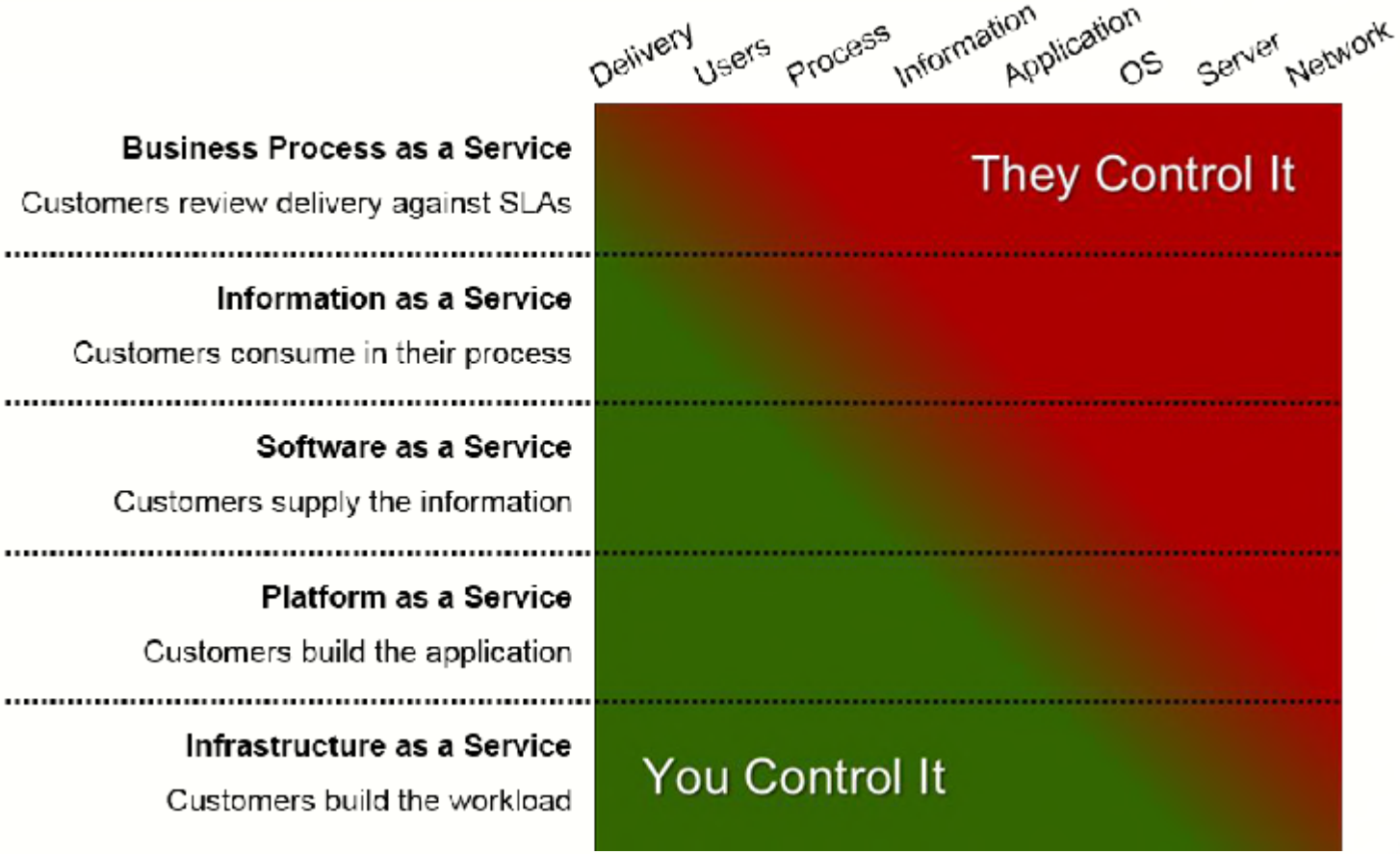
云工作负载：是一个独立的服务或者能力，运行在云计算的实例上。

# 云工作负载安全负责角色



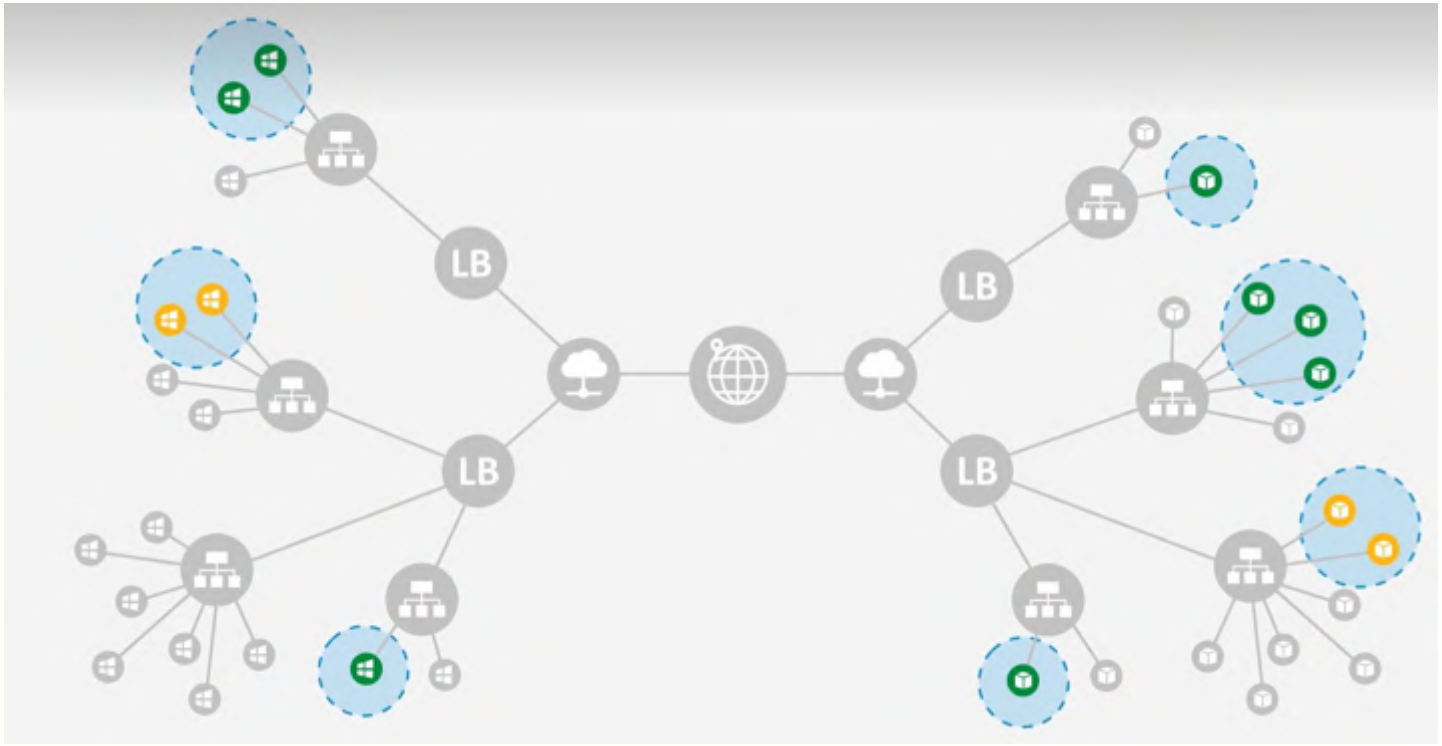



# 要对自己的工作负载负责！

# 保证工作负载可见性



你不能保护你看不到的东西！

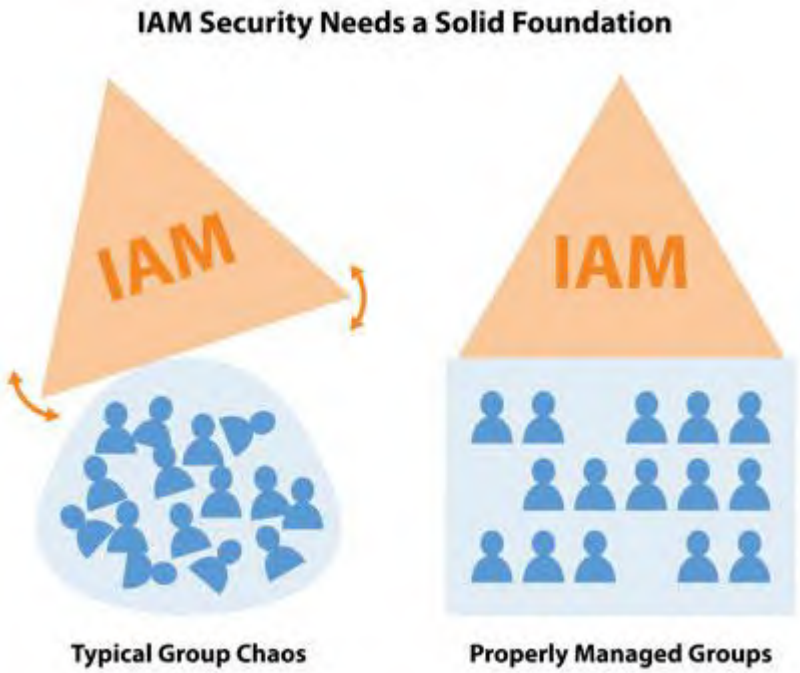



**TIPS：资产清点、资产发现**

# 保证严格的IAM机制



最小权限原则，账号分组，RBAC，身份取消




**TIPS：账号管理、权限管理、OTP**

# 加入自动化安全机制



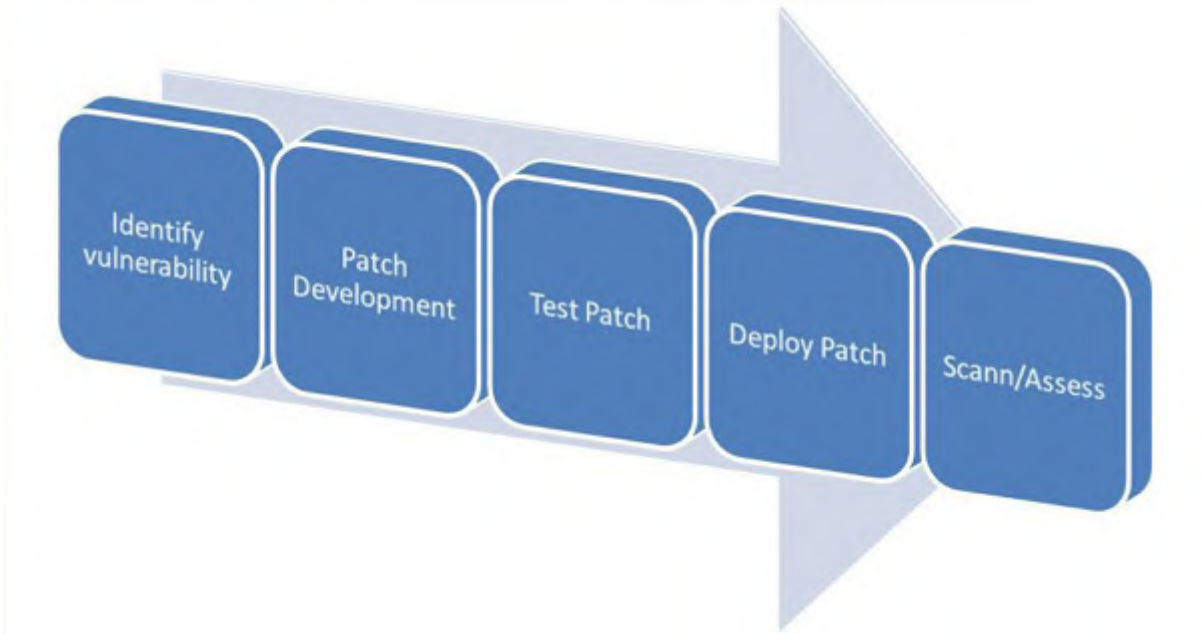
DevSecOps


**TIPS：使用脚本、API或者自动化安全产品**

# 使用“No patch”策略



不给线上系统打补丁




**TIPS：使用最新的镜像构建应用，持续进行漏洞扫描**

# 加密网络流量



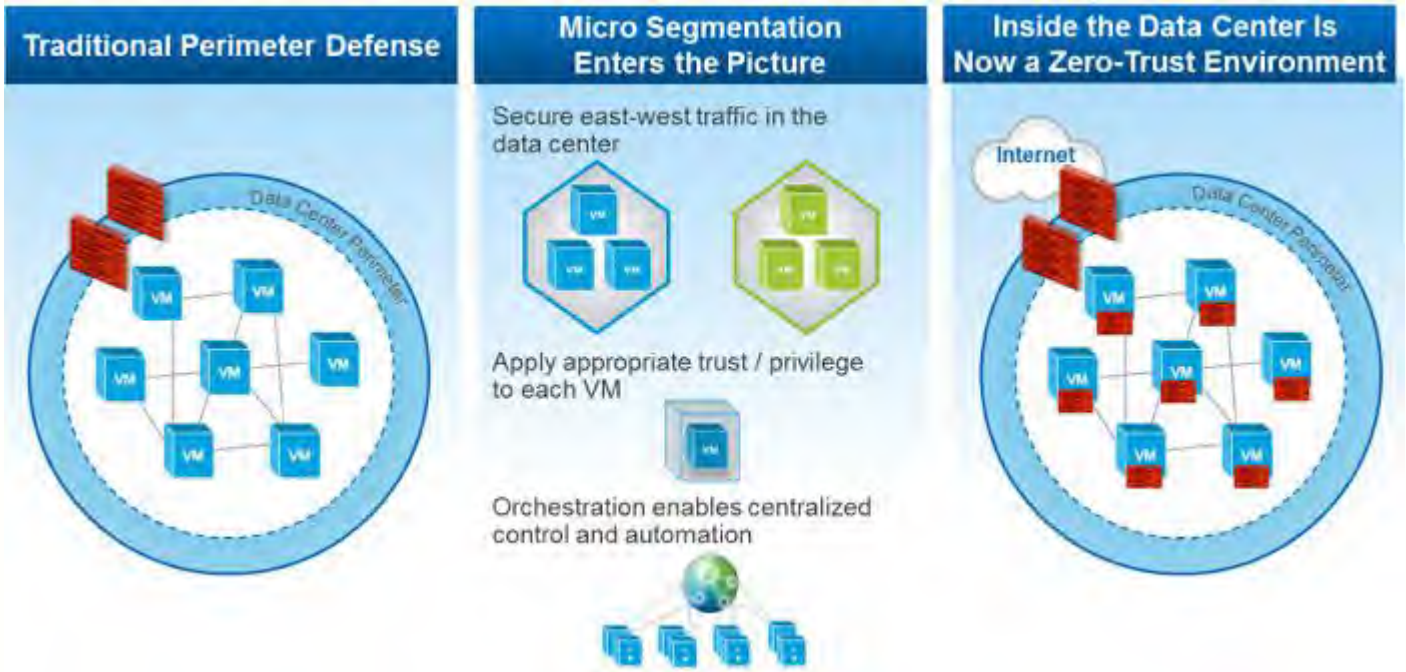
VPC=VPN+NAT


**TIPS：使用VPC、IPSEC、TLS、SSH**

# 应用安全组进行 “微隔离”



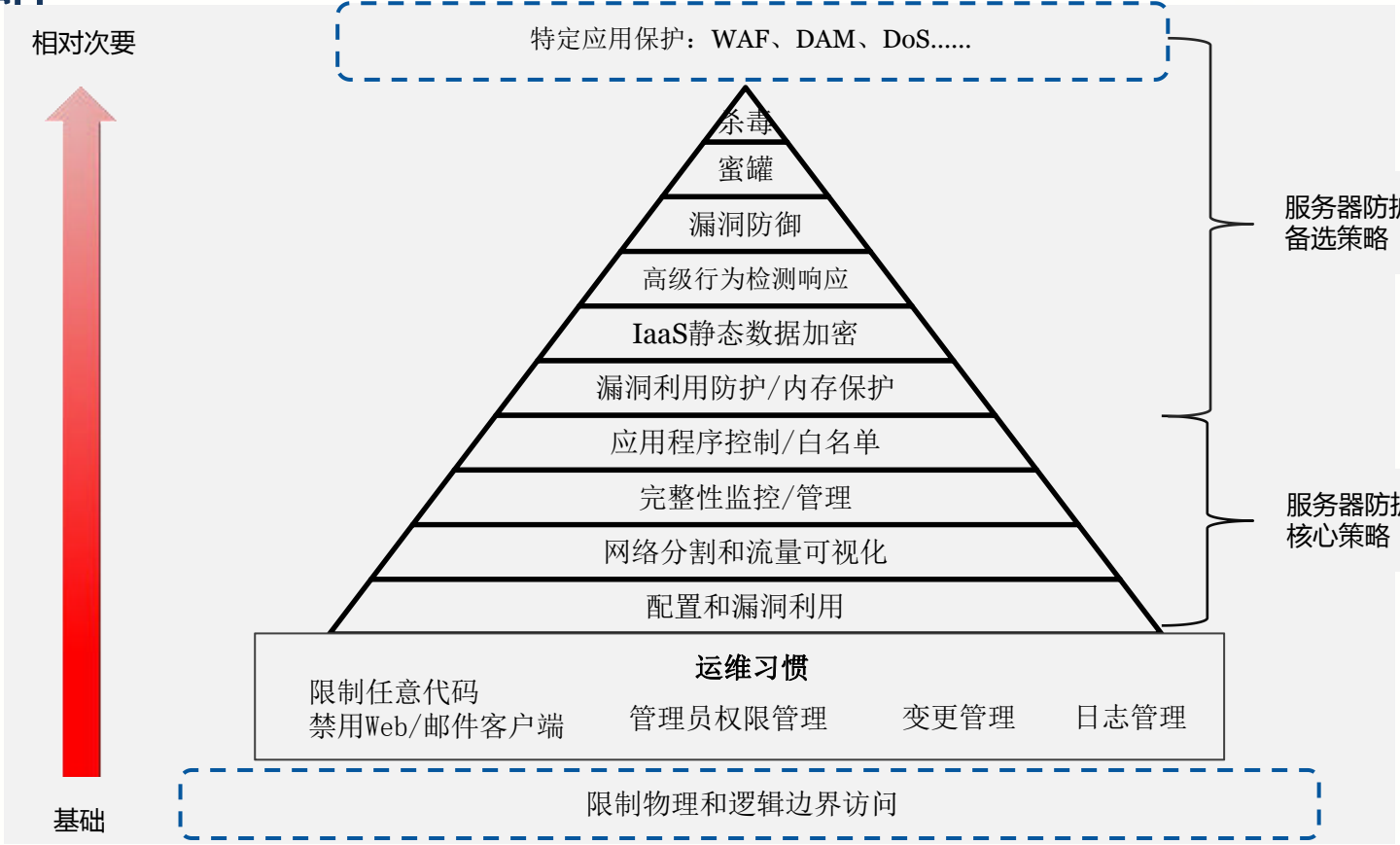
防火墙




**TIPS：进行安全组划分、采用微隔离以及访问关系模型**

# 采用工作负载为中心的安全策略






**TIPS：采用CWPP产品**

# 数据静态加密



加密数据

**TIPS：对敏感数据进行静态加密，使用秘钥管理服务（KMS）**

# 不能忽略应用和网络架构安全



应用安全


**Figure 1**: Application Security Triad

**TIPS：采用WAF，保证DNS、DHCP、NTP安全，使用AD或者LDAP以及考虑DDOS攻击**

# 使用能够“云化” 的安全产品



软件定义安全


**TIPS：采用可以“云化”的安全产品或者直接使用云安全产品。**


# 谢谢！