



混合云与安全

王涛

资深系统架构师



高级分析
服务



新型的线上
生活服务



自助服务体验



数据定义的
业务流程



工业IoT

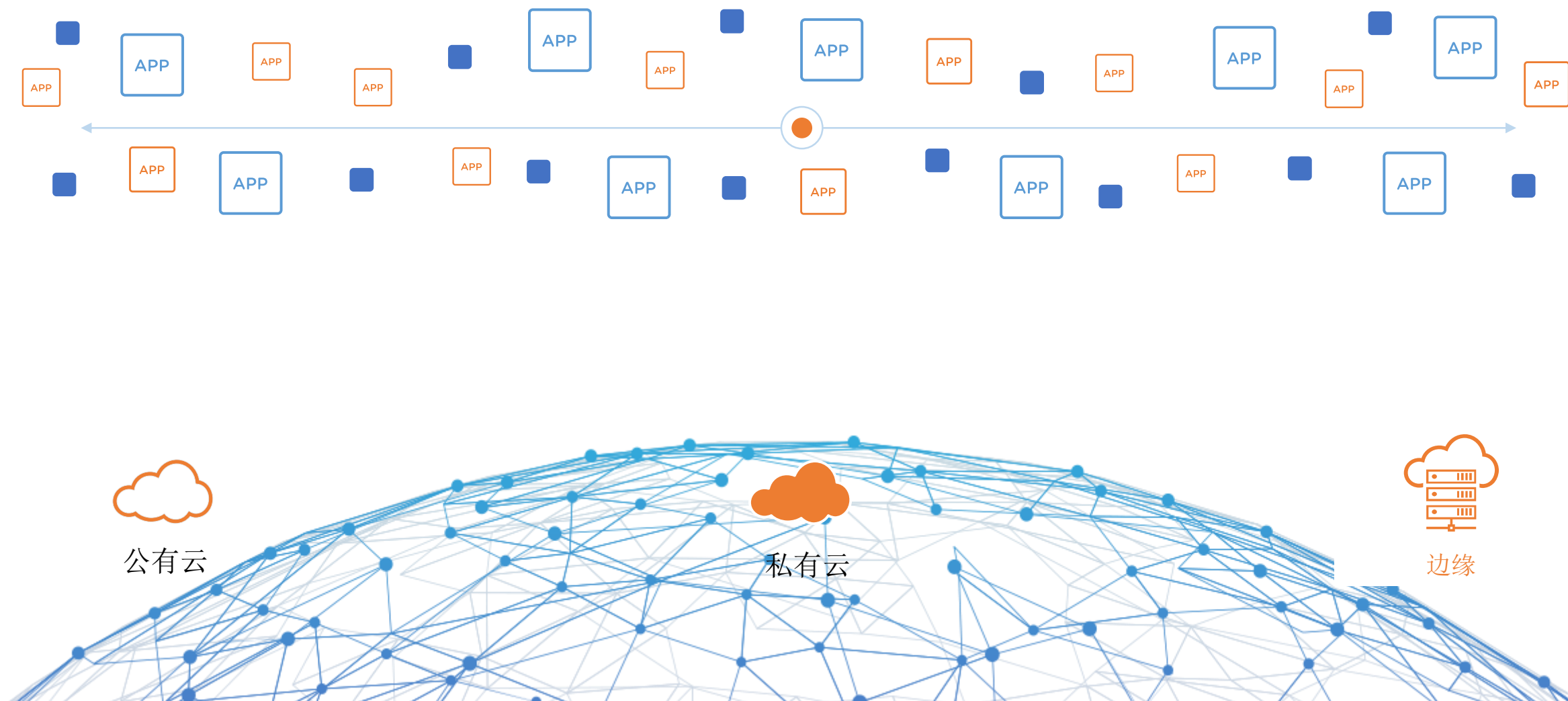


业务流程
自动化

在未来的5年
将会有更多的应用和解决方案被交付
超过过去40年总和

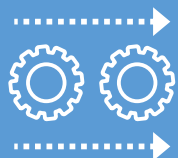
现代业务应用需要灵活性

....用混合云来交付一致的基础架构与运维管理

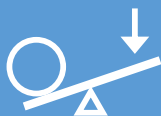


客户的混合云需求与挑战

挑战与复杂性



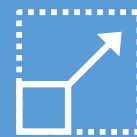
运维一致性



不同的技术和工具



多种类型的管理工具
和安全控制



不一致的
云和应用SLA



不兼容的
虚拟机格式

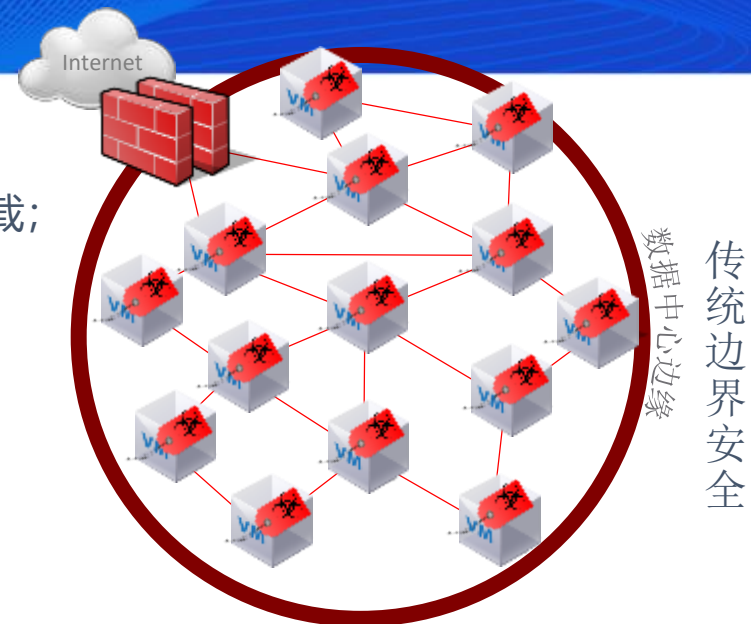


客户需求，从私有云到混合云到多云管理

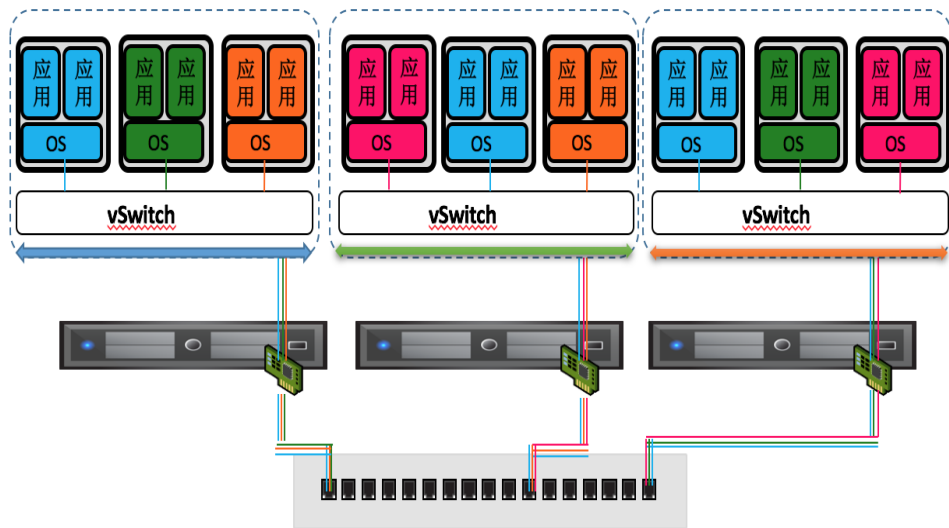


传统安全无法满足混合云的需求

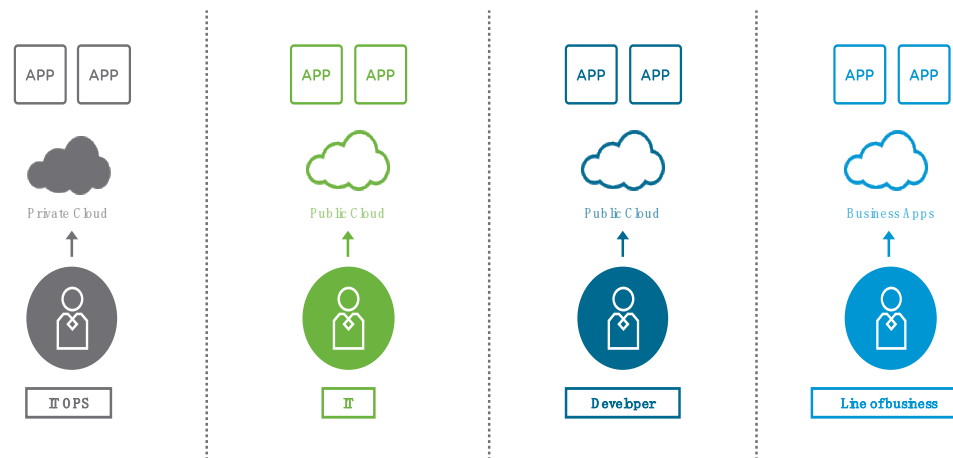
- ✓ 边界下移到主机内部，基于边界的网络安全已被证明是不够的。
- ✓ 基于操作系统的主机安全防火墙和安全防护运维管理复杂，消耗资源多，容易被关闭和卸载；
- ✓ 大量安全威胁来自内部，如何实现东西向任意虚机之间安全？如何实现安全服务插入？
- ✓ 多云如何提供一致网络和安全的管理？
- ✓ 业务动态变化，传统安全防护无法适应业务动态变化
- ✓ 流量不可视，无法获取流量
- ✓ 安全威胁在变，内部攻击、蔓延



虚拟化内部安全边界发生改变



多云独立安全管理



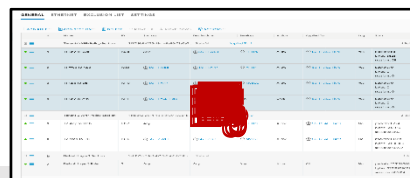
统一安全策略

统一的可视化、
安全和运维

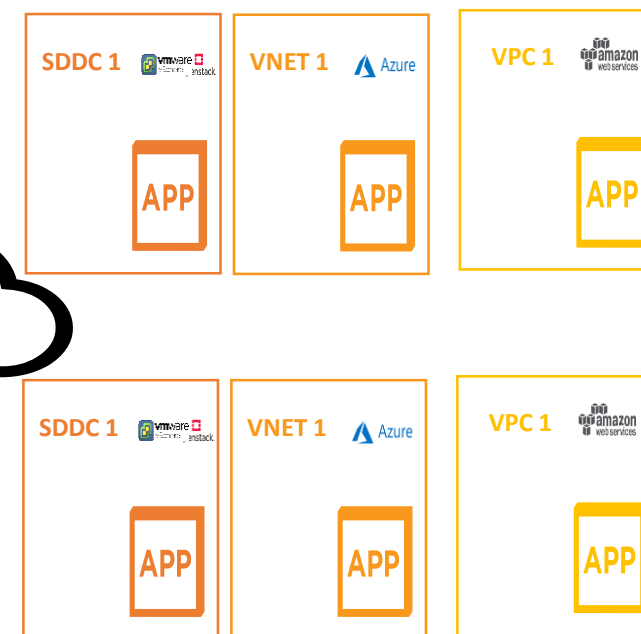
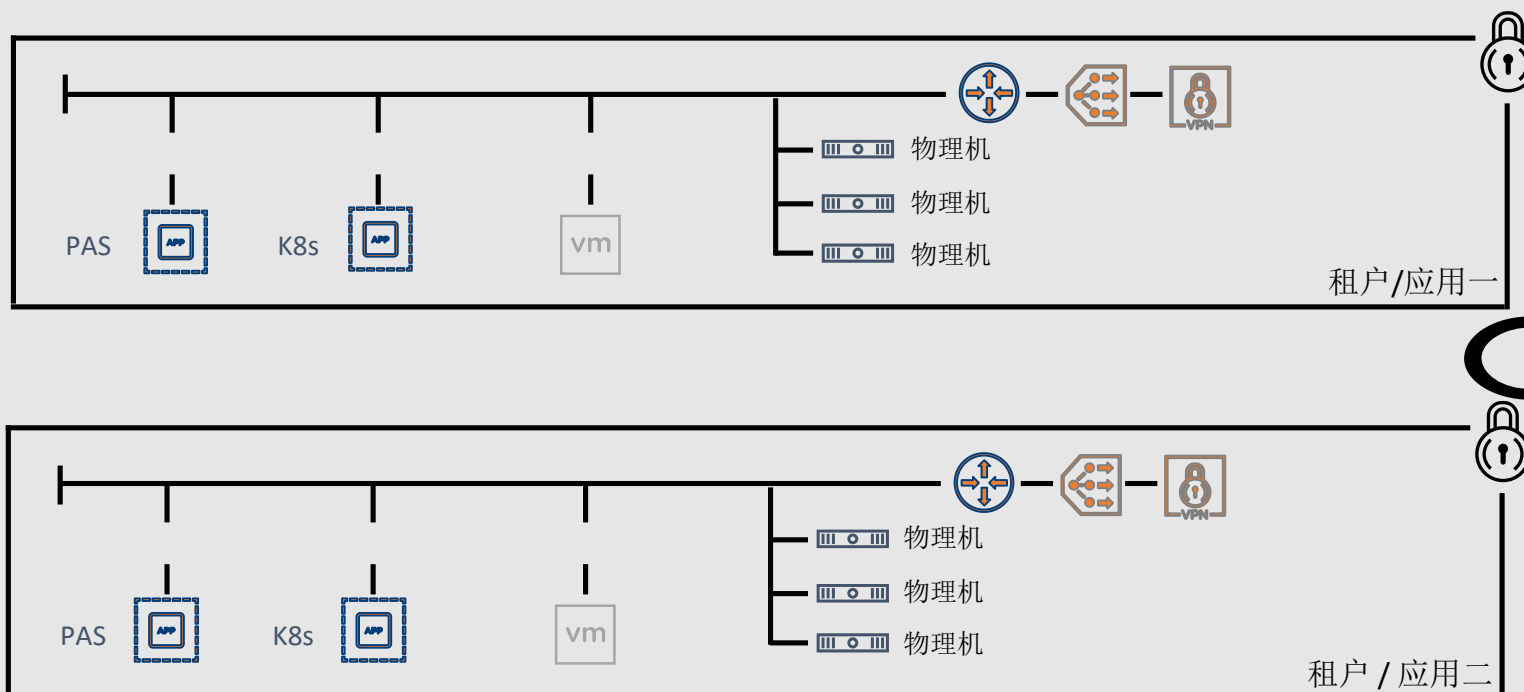
数据中心扩展

灾备和恢复

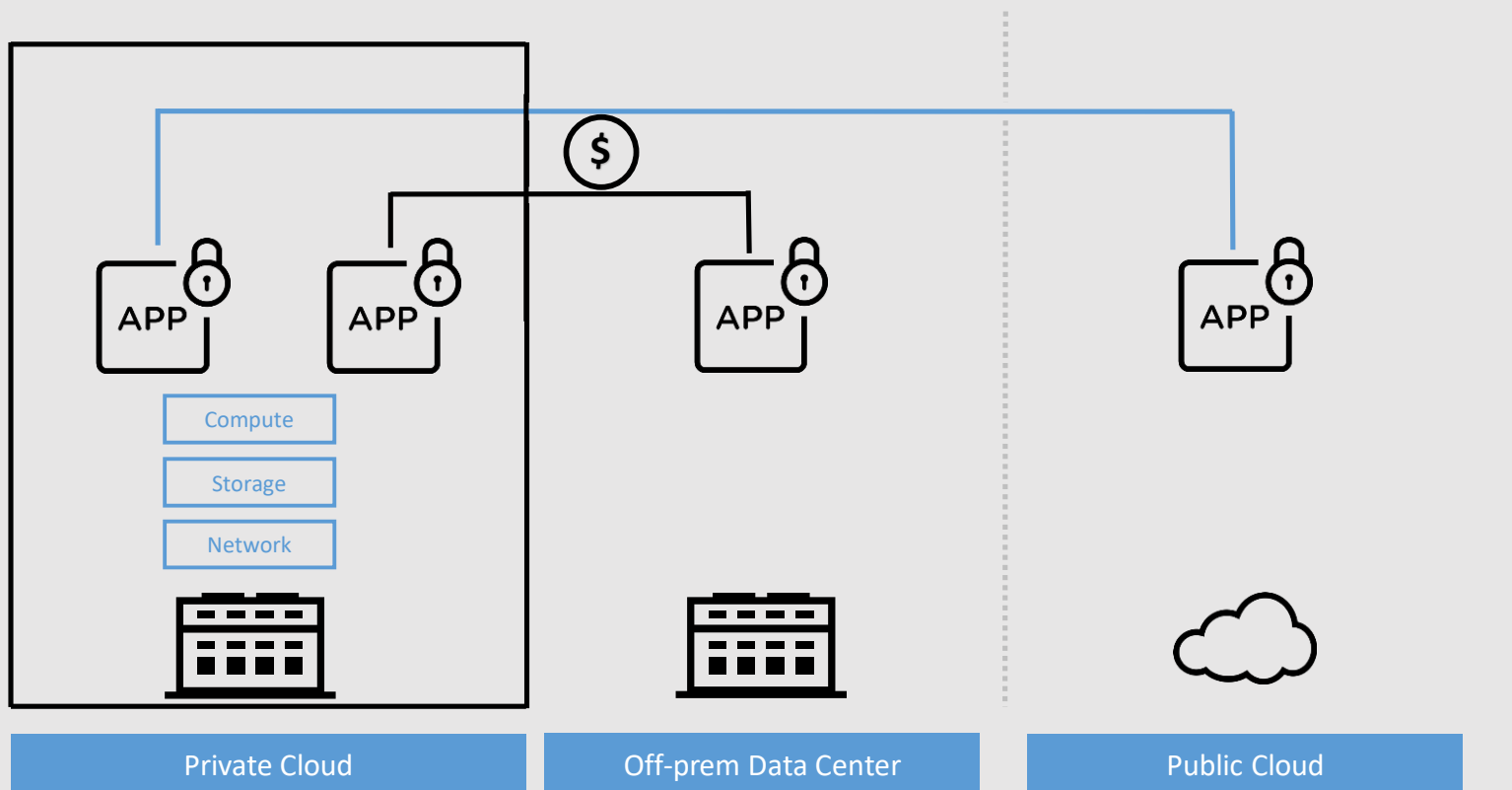
工作负载移动性



| 资源名称 | 资源类型 | 状态 | 操作 |
|------------------|------|-----|------|
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |
| VMware ESXi Host | 虚拟机 | 运行中 | 更多操作 |

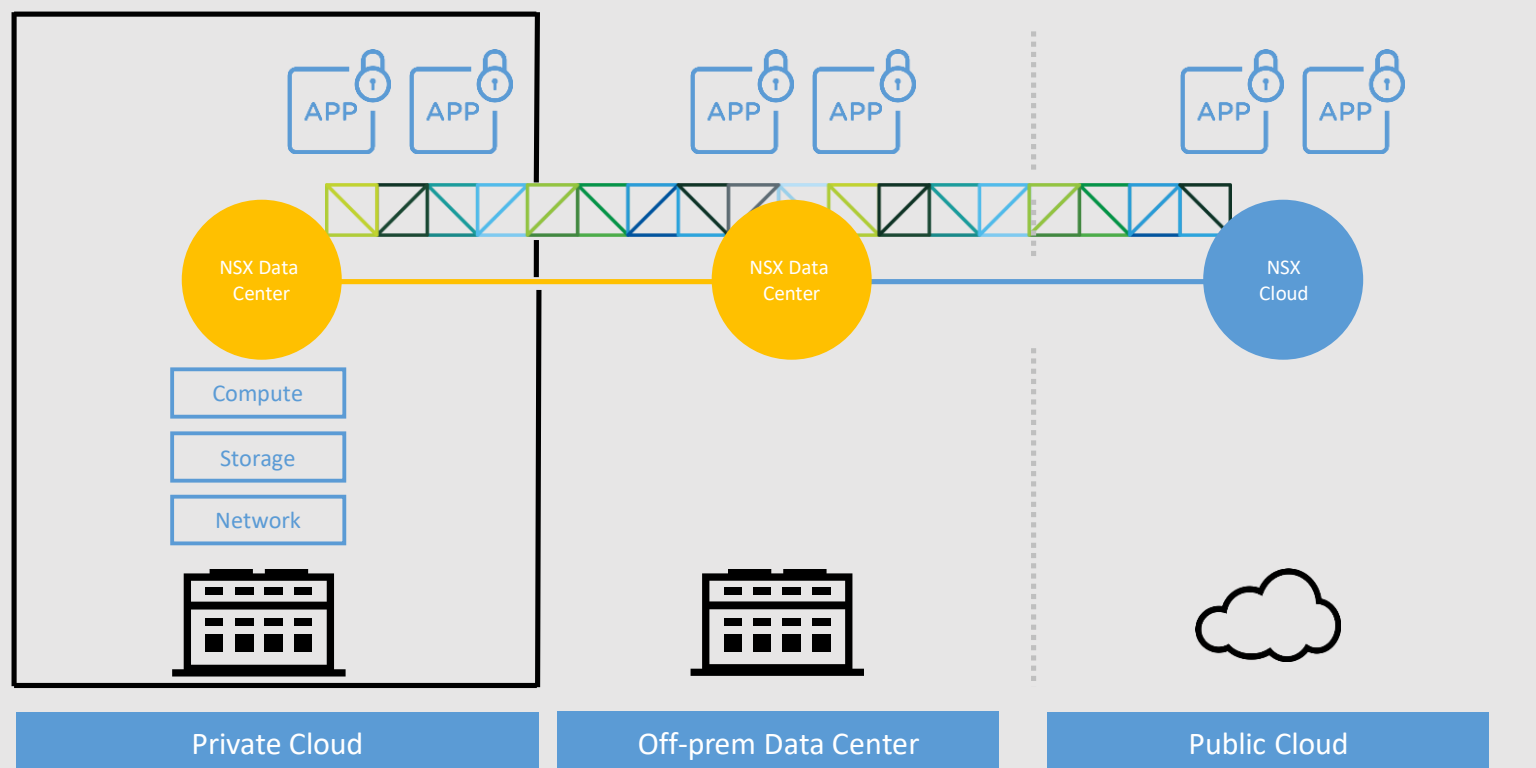


传统数据中心扩展费用高运维挑战



- 昂贵(例如：裸光纤)
- 部署复杂 (例如： OTV, LISP)
- 硬件依赖 (例如： OTV)
- 专有协议/厂商 锁定
- 硬件/软件 互操作问题

无缝扩展到多个位置

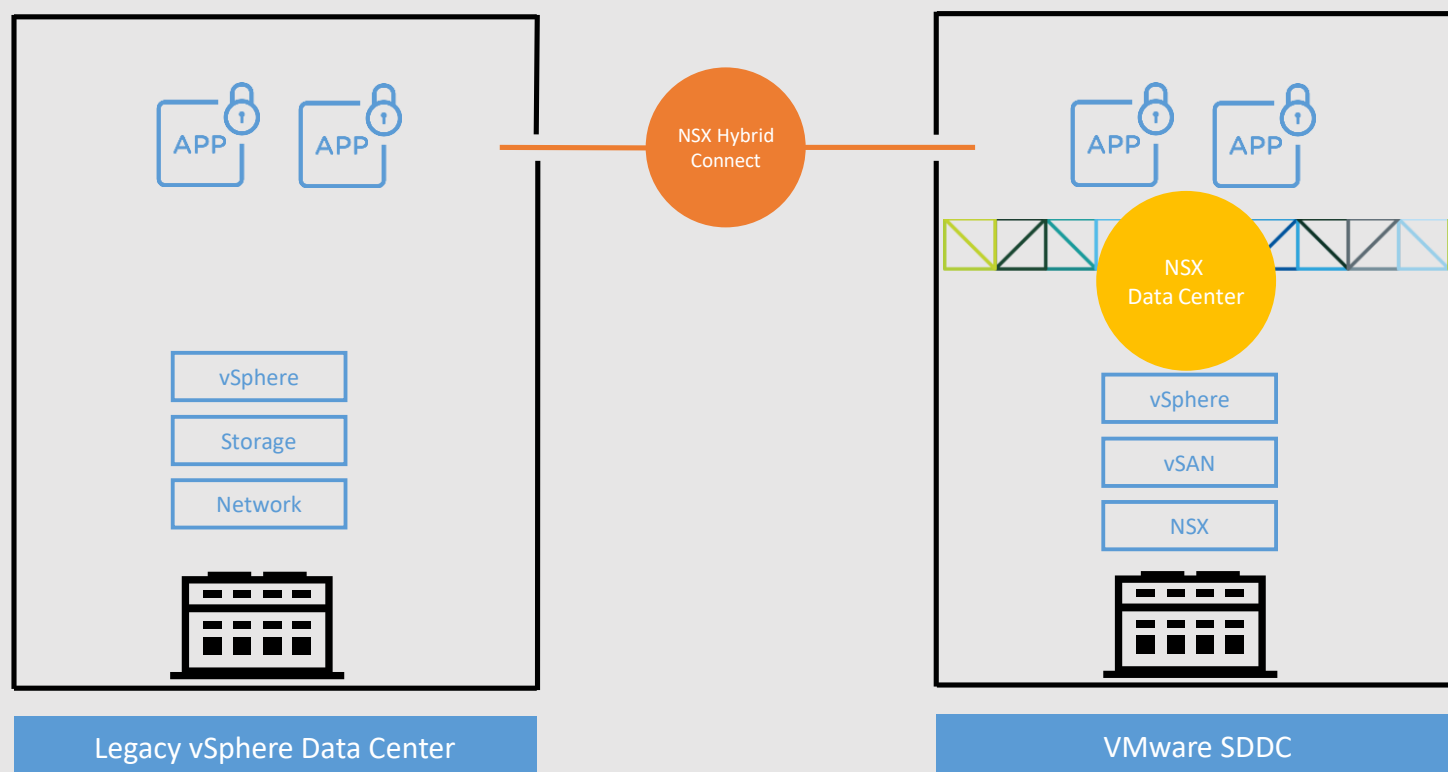


一致的网络

- 平滑迁移
- 资源池扩容

硬件无关性

简单实现传统数据中心和基于SDDC数据中心的扩展



- 安全的经过广域网优化的网络扩展

非NSX 到 NSX 环境

私有云-到- 私有云或私有云-到-公有云

到VMC on AWS的数据中心扩展

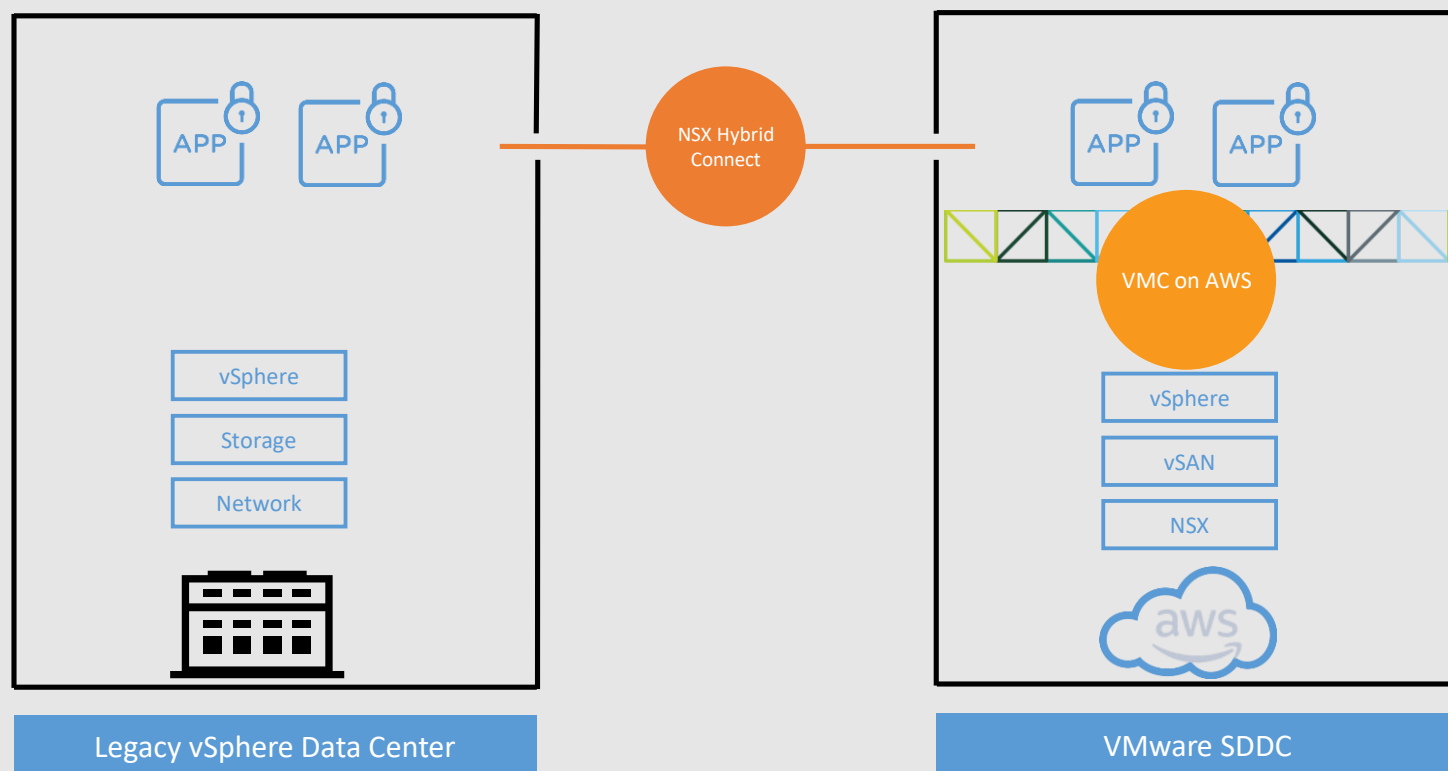
统一的可视化、
安全和运维

数据中心扩展

灾备和恢复

工作负载移动性

简单实现传统数据中心和基于SDDC公有云数据中心的扩展



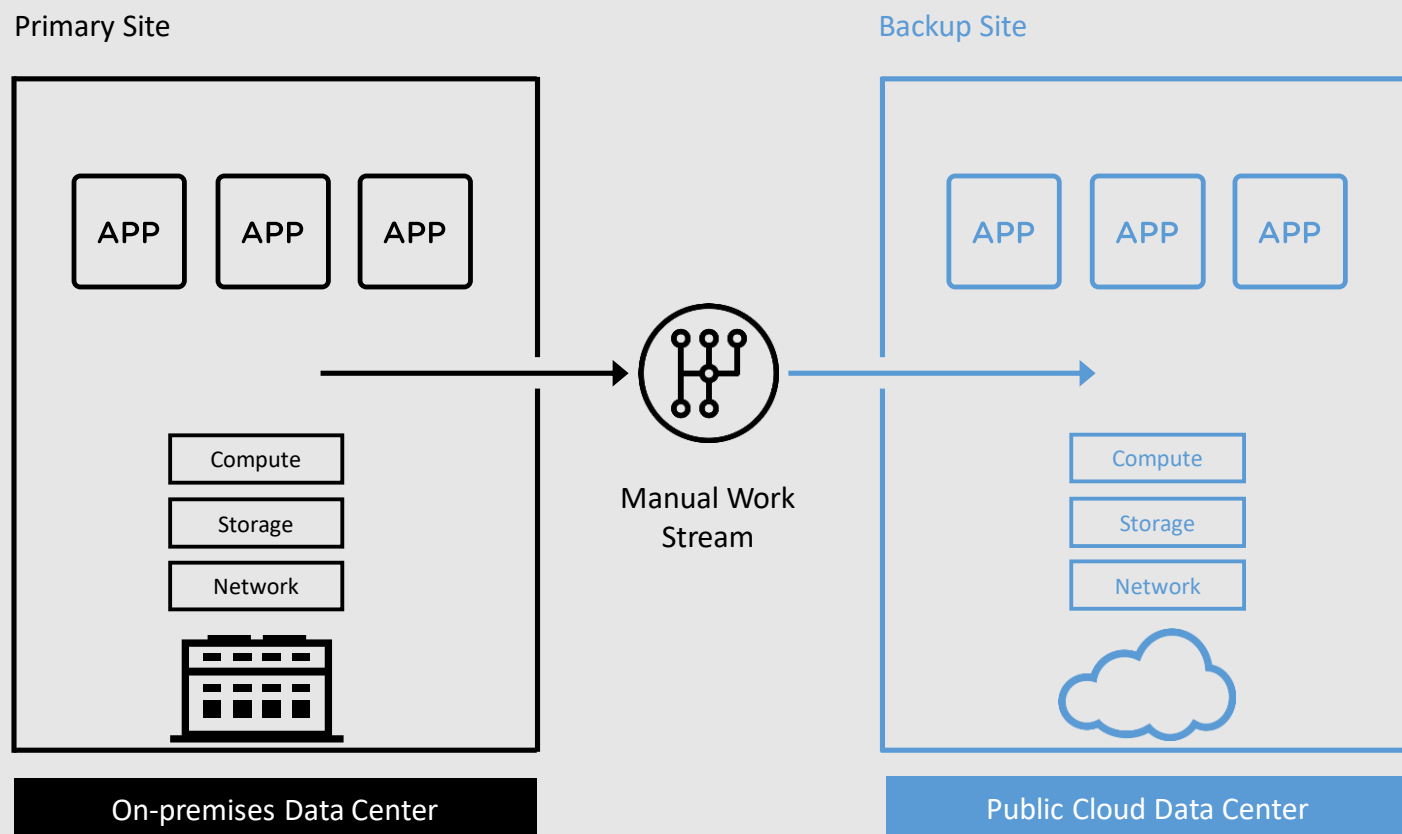
- 安全的经过广域网优化的网络扩展

非NSX 到 NSX 环境

私有云-到- 私有云或私有云-到-公有云

- 比传统方式快 **10倍**, 大大减少迁移时间（从几个月到几天）

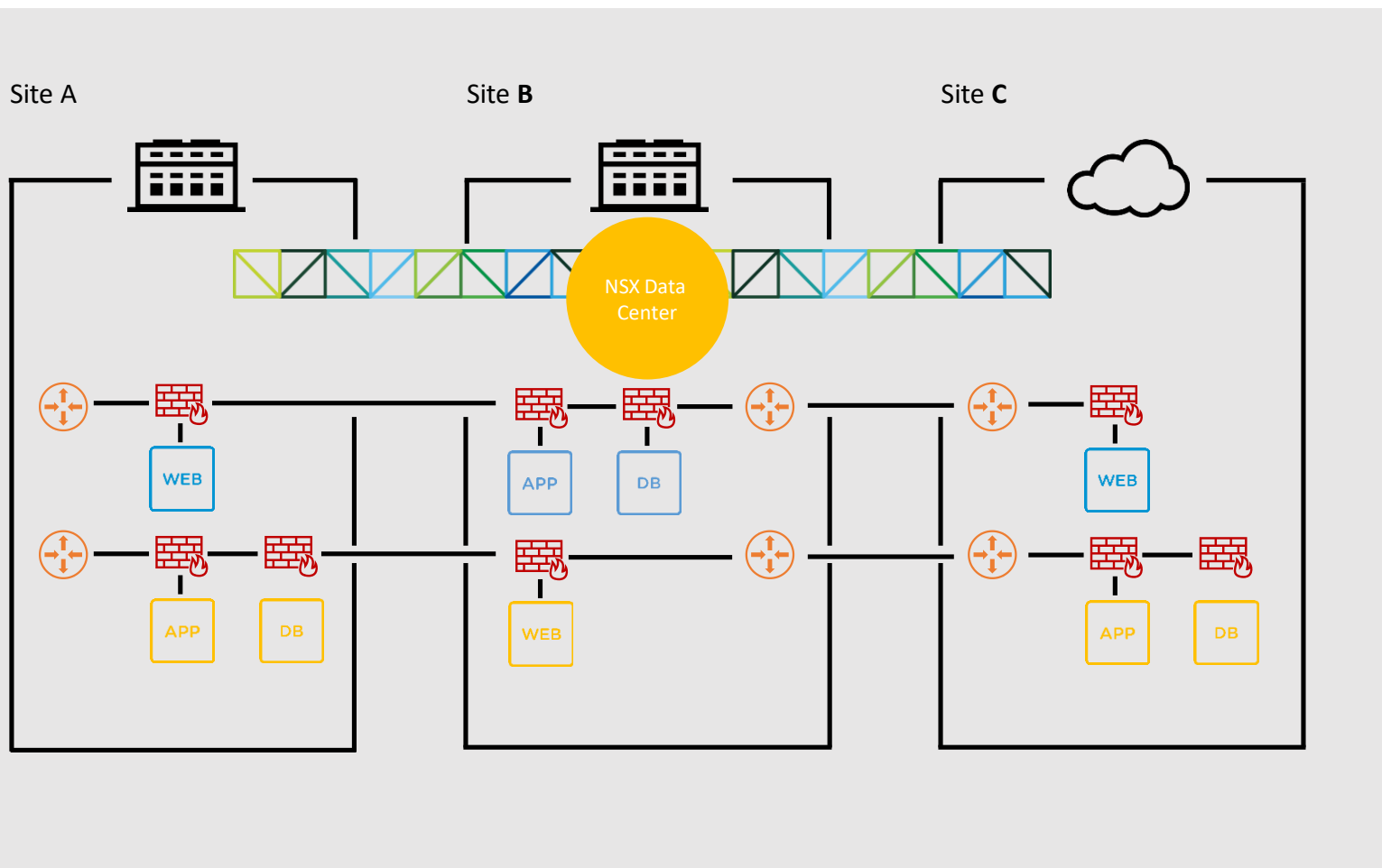
复杂性和运维挑战



恢复可能需要几个小时甚至几天

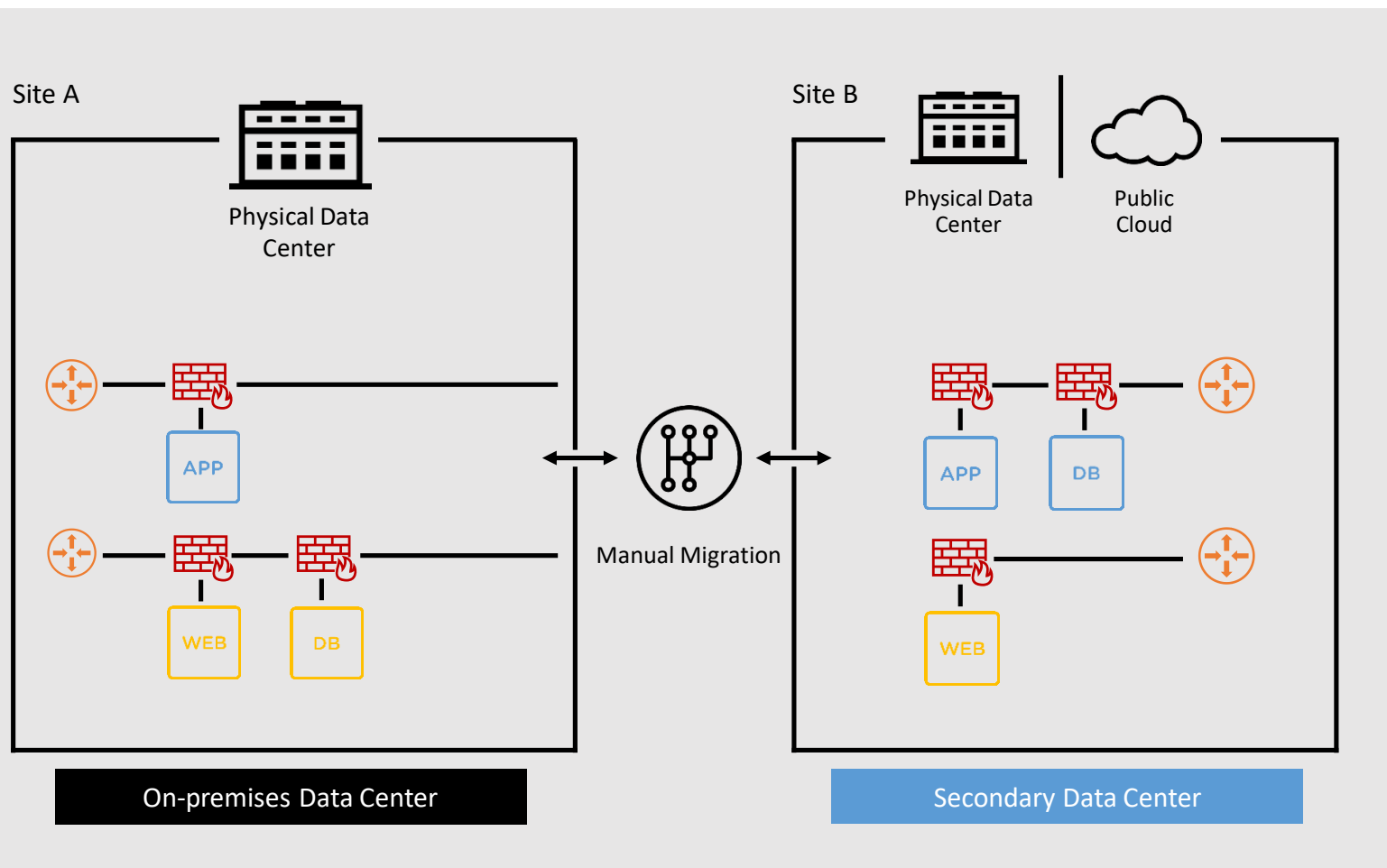
- 有限制的或不完整的恢复策略
- 运维复杂
- 手动流程和重配

利用多站点资源池技术最小化故障的影响



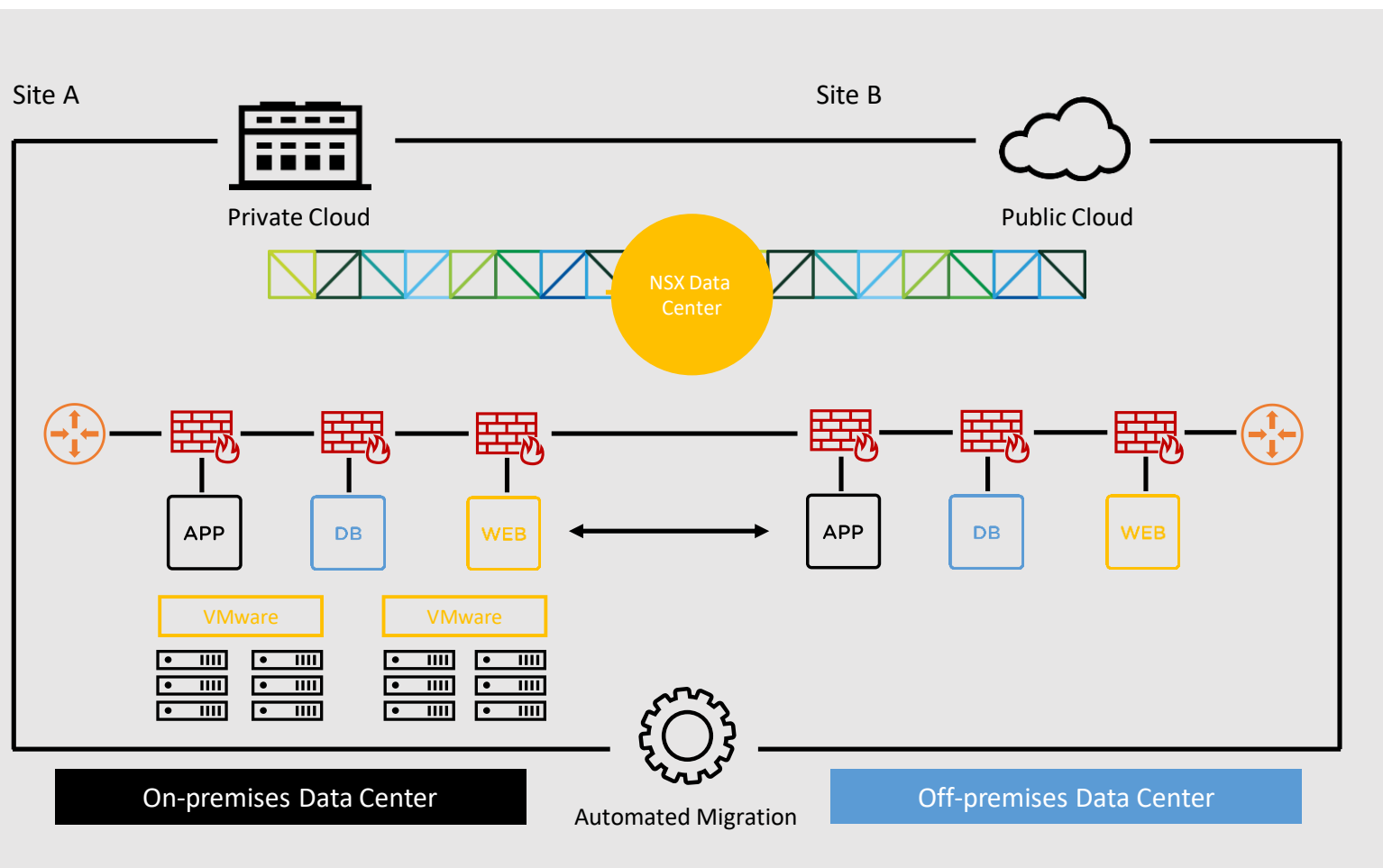
- 共享资源作为一个统一的资源池处理
- 每个资源池维护自己的 SLAs 和 QoS 规则
- 无缝连接部署在任何位置的应用
- 即使需求有变化，保证应用无中断运行

站点的不兼容限制了工作负载的迁移



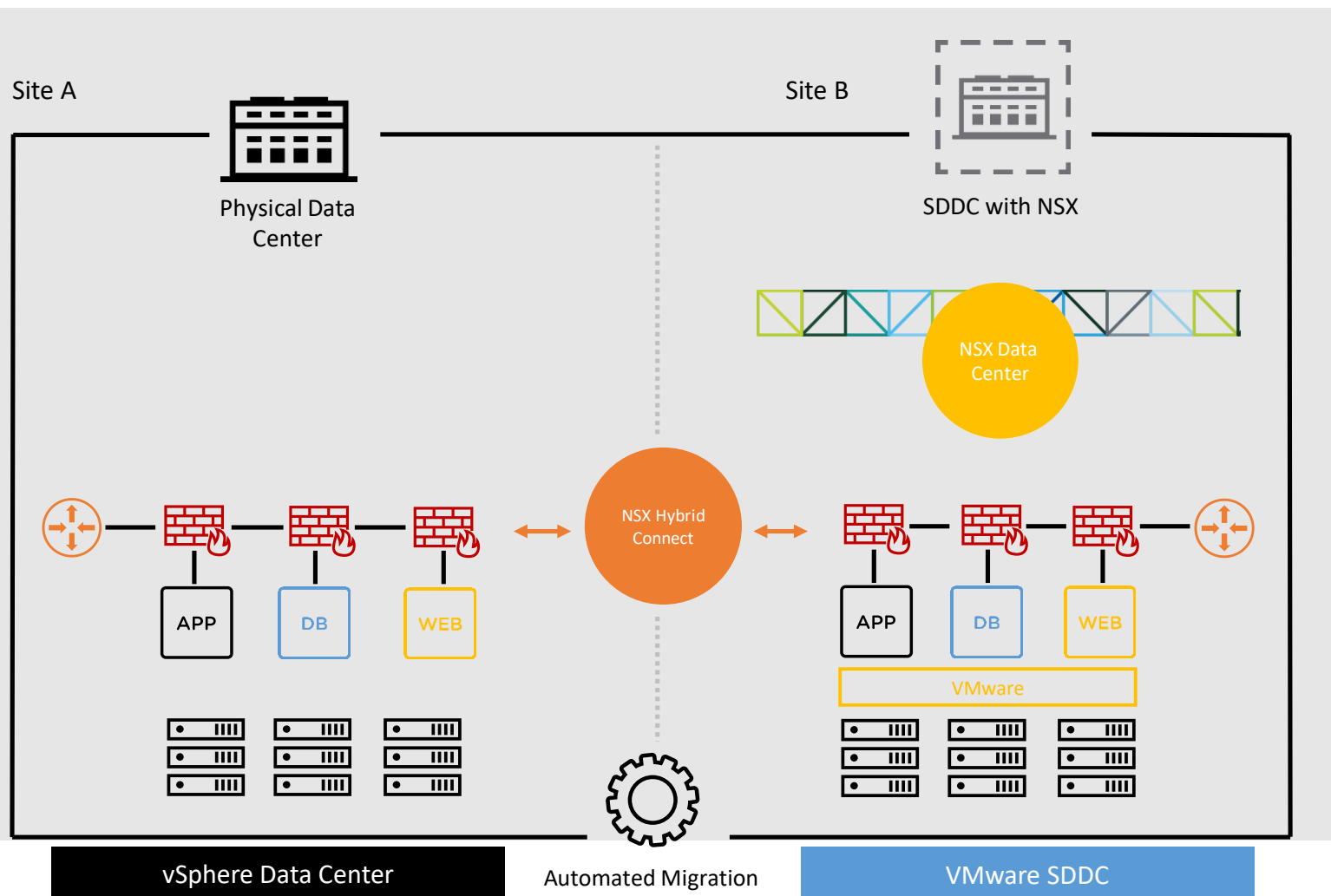
- 手动迁移费用高耗时长
- 缺少兼容性经常意味着需要修改IP地址
- 不一致的安全和合规

高效的工作负载迁移



- 简化工作流迁移
- 一致的网络安全
- 自动化流程

规模迁移



- 从 非NSX环境到现代化SDDC的迁移
 - 批量迁移
 - 零宕机 实时迁移和 计划的大规模迁移
 - 保持IP和路由
- 多站点, 高速二层扩展

工作负载迁移（示例）：从私有云到VMware的迁移

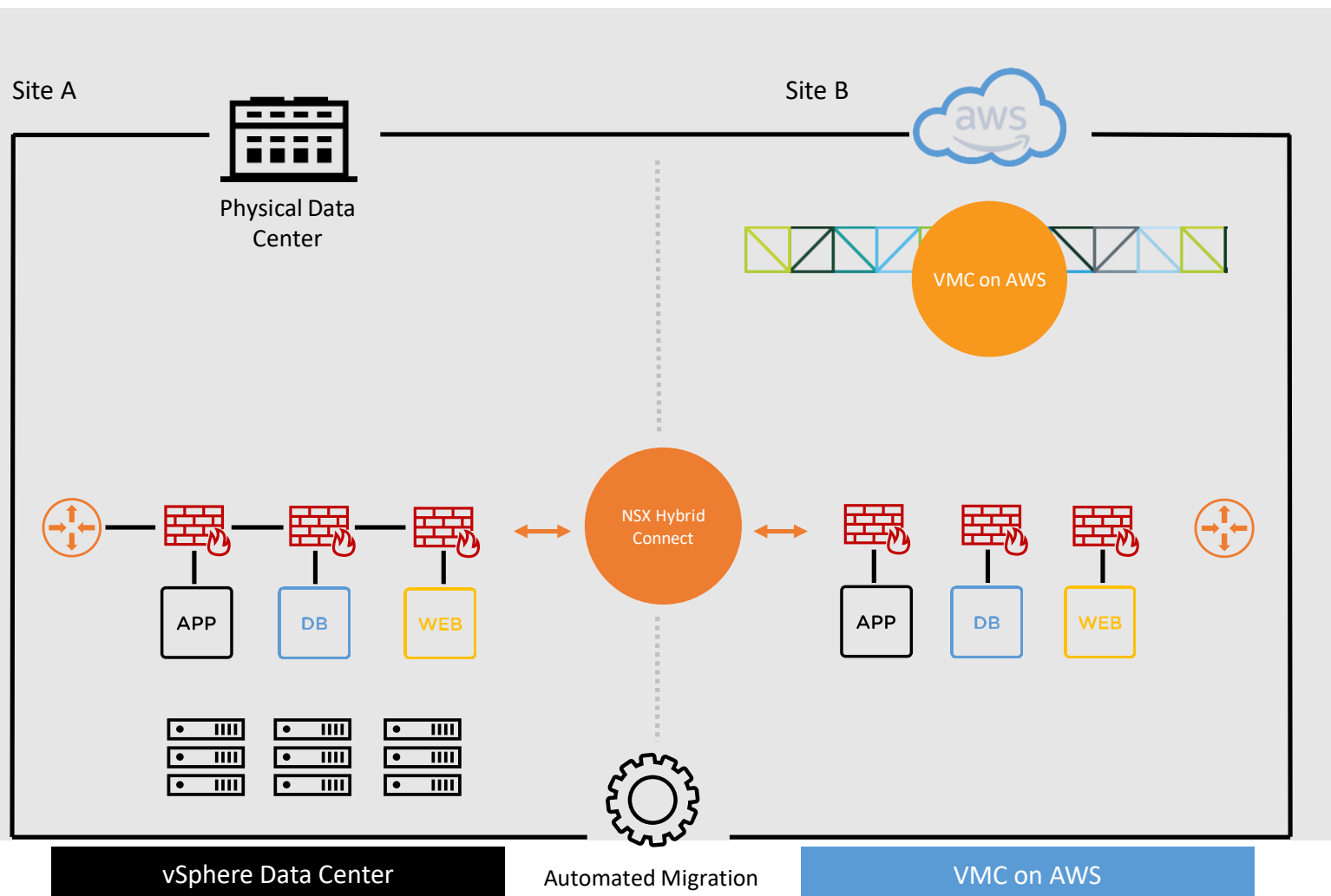
统一的可视化、
安全和运维

数据中心扩展

灾备和恢复

工作负载移动性

规模迁移



- 从非NSX环境到VMware on public
 - 零宕机实时迁移和计划的大规模暖迁移
 - 保持IP和路由
- 多站点, 高速二层扩展

VMware 多云网络

应用场景



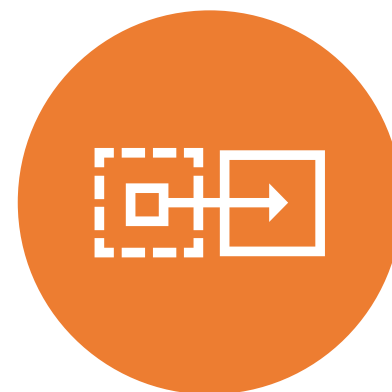
统一的可视化、
安全和运维



数据中心扩展



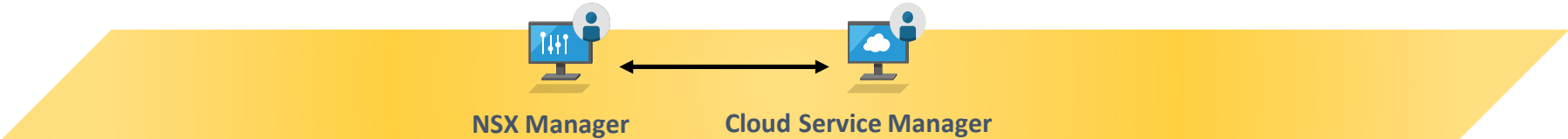
灾备和恢复



工作负载移动性

原生云多云互联架构

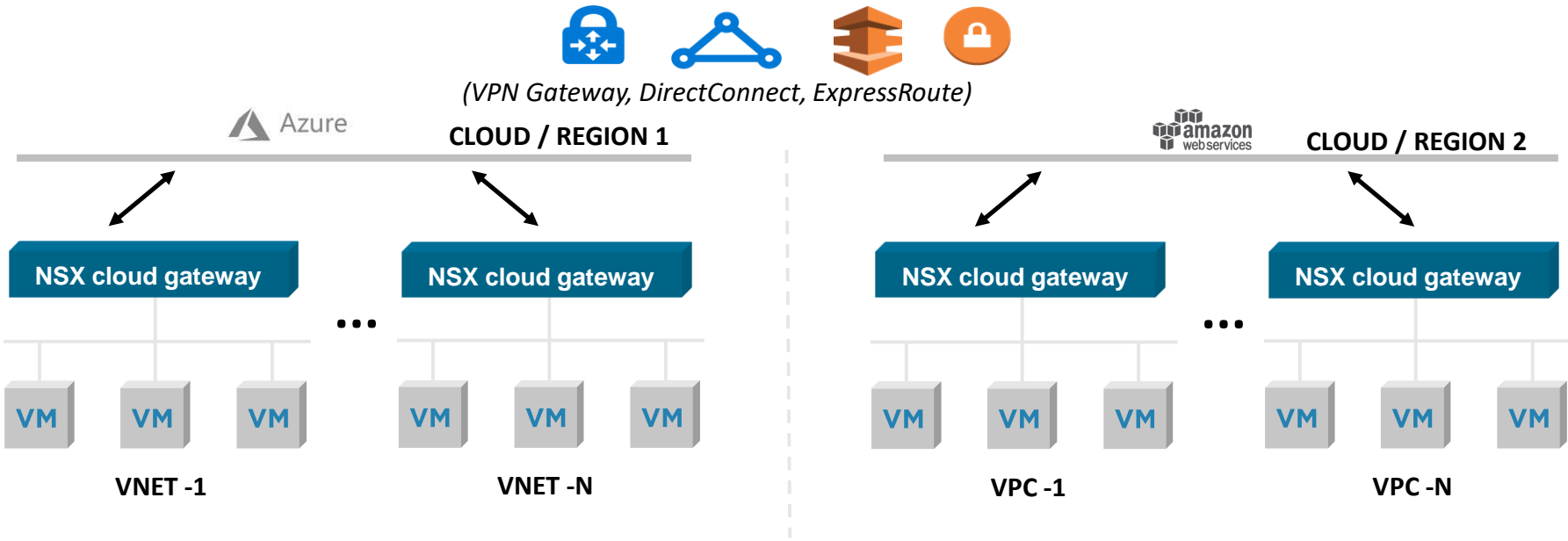
管理平面



控制平面



公有云
VPCs / VNETs



一致性、可扩展的微分段安全

安全策略一次性定义, 可以部署在任何云



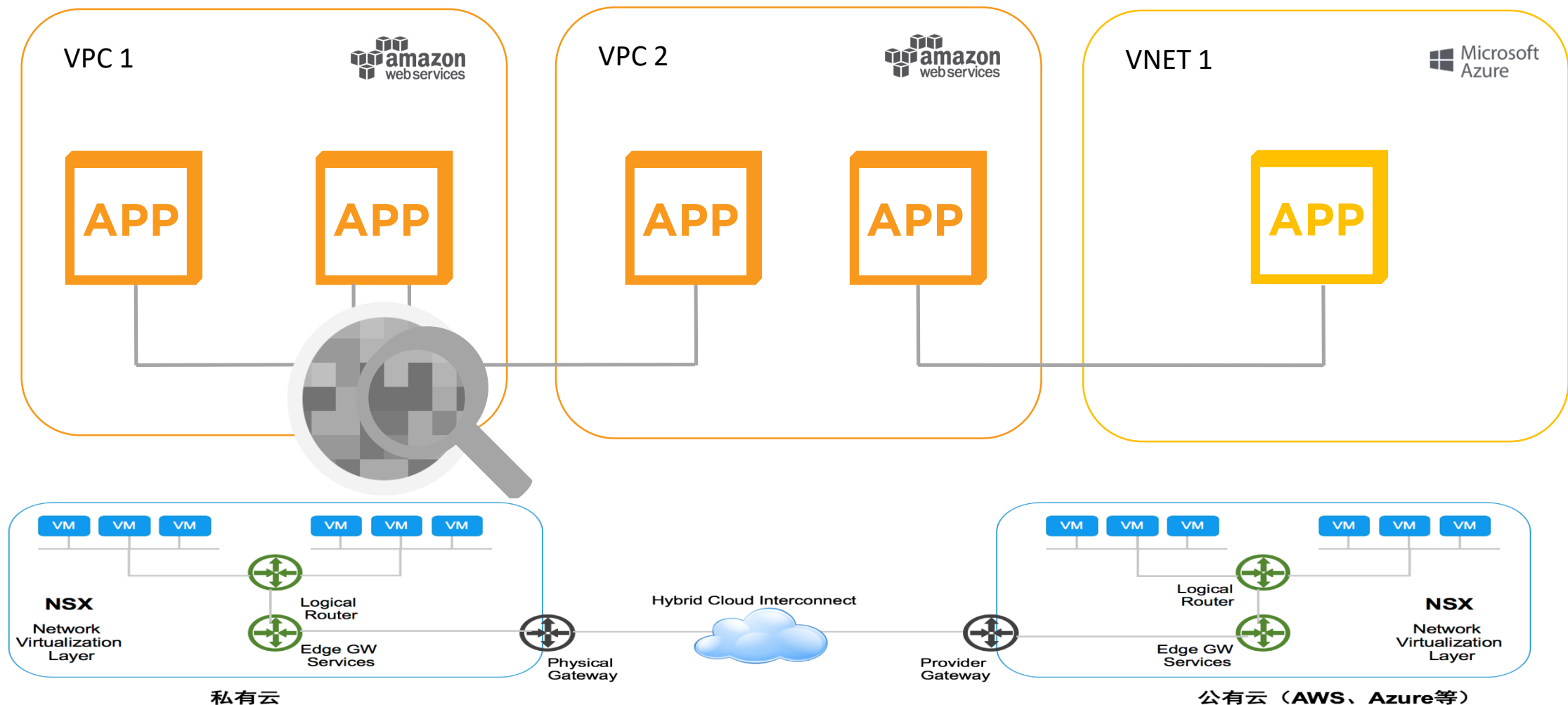
Security Group 1


Policy



端到端的Day 2运维一致性

跨VPCs、Availability Zones、Region和云的
端到端可视化和运维工具跨



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE