工业互联网云安全

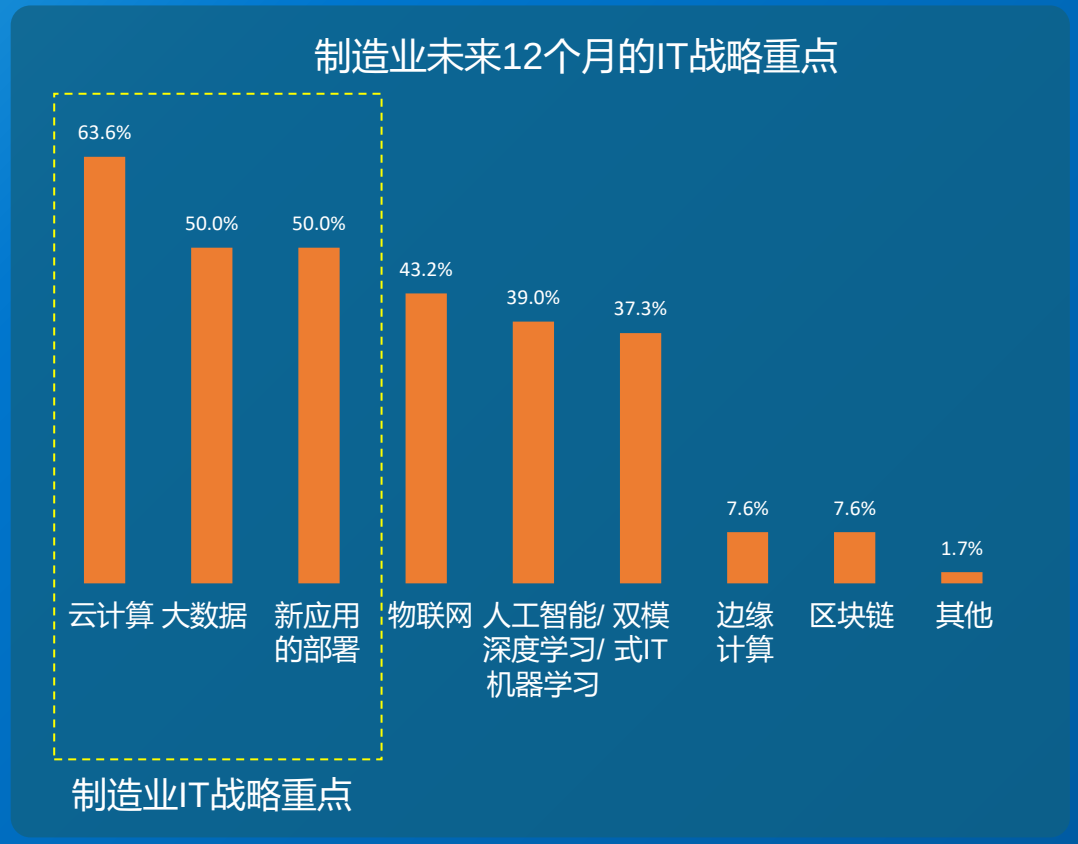
吴天耀
制造业业务拓展高级经理
大中华区存储平台及解决方案事业部

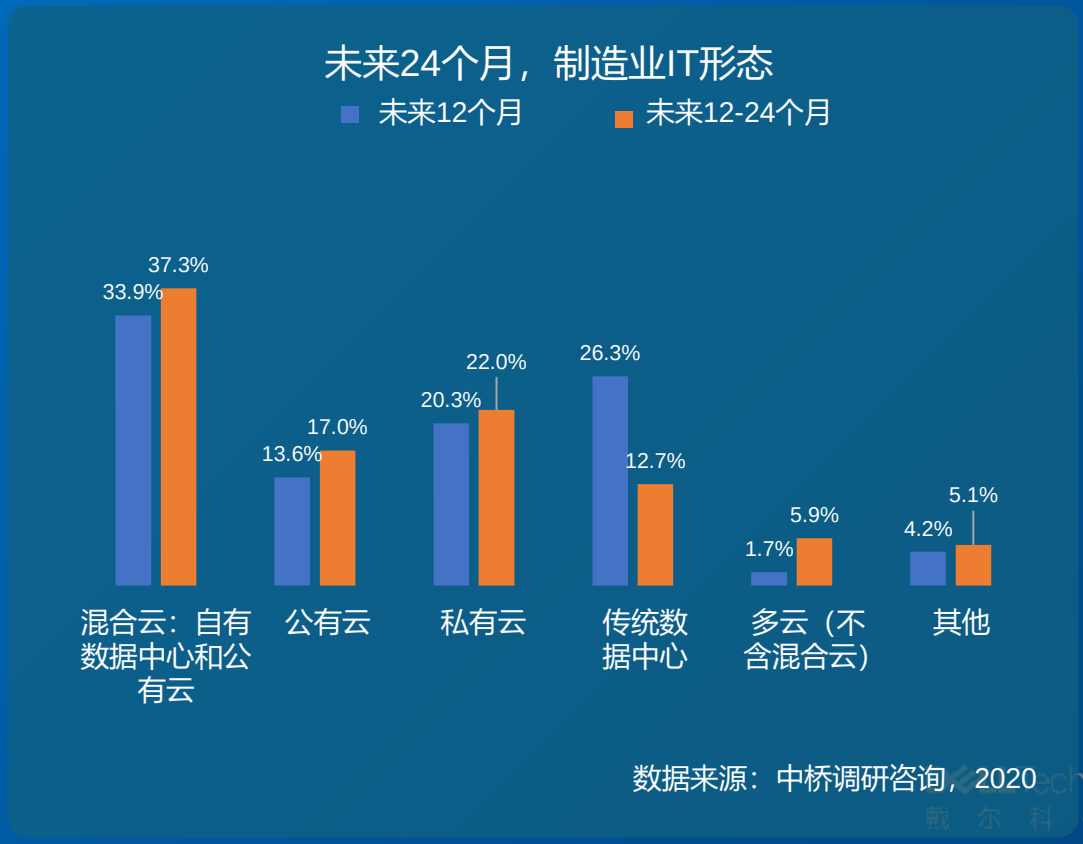
DELL Technologies
戴 尔 科 技 集 团

2021 中国制造业趋势及IT战略重点

“十四五规划，中央提出的要保持**制造业**稳定，推进基础设施建设，特别强调 ‘推进**数字产业化和产业数字化**’，这和我们通过对市场的观察得到的结论是一致的…外资IT企业在中国市场规模的发展和产业链、供应链的深化，对于稳定和巩固中国在**制造业**、信息通信技术产业的**全球供应链**的核心地位具有积极意义。”

-- 2021年2月4日 黄博士与全国政协副主席万钢的谈话





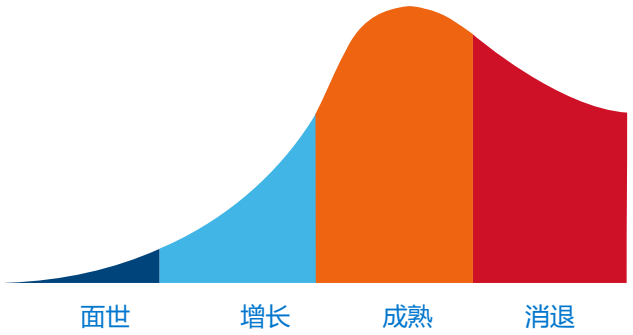
数据来源：中桥调研咨询，2020

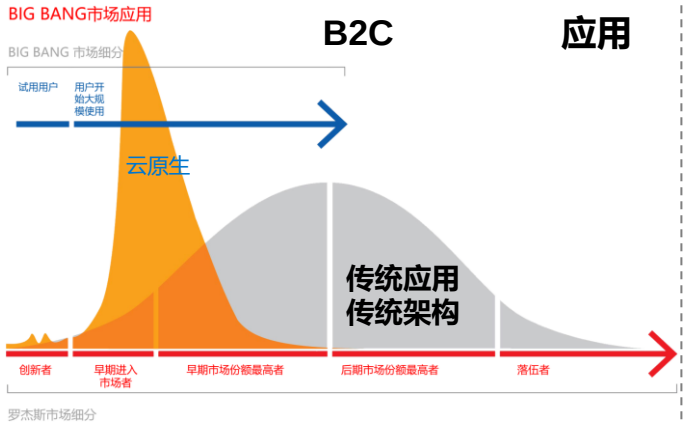
新基建和后疫情加速中国云计算市场和技术格局改变

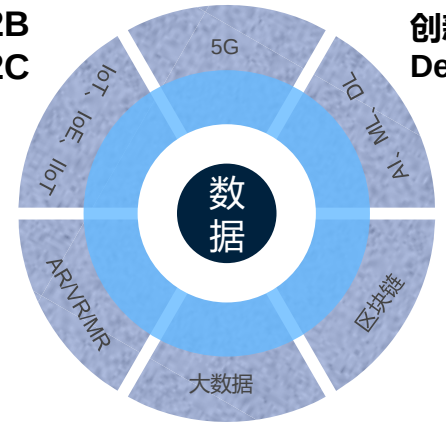
“新基建“从资源平台到创新平台

“疫情“全数字化最大POC，加速IT转型，企业跳跃式云计算2.0就绪

传统经济	互联网经济	工业互联网
B2B IT	B2C 应用	C2B C2C 创新平台 DevOps







各阶段云重点	传统IT	多云资源平台	边缘 - 核心 - 多云 现代化应用交付平台
云价值	降低IT CapEX	降低云业务风险	多云安全协作创新

新基建七大领域：，5G,云计算，人工智能，物联网，大数据中心，超高压电，城际交通

DELL Technologies 戴尔科技集团

新基建，数据为核心数字化协作创新平台和智能物联升级

创新平台

2023,500万现代化企业级应用
2/3企业用户生产环境每**日**部署

应用开发交付（百行千态场景驱动）
VM, 容器，微服务，服务网格，容器集群

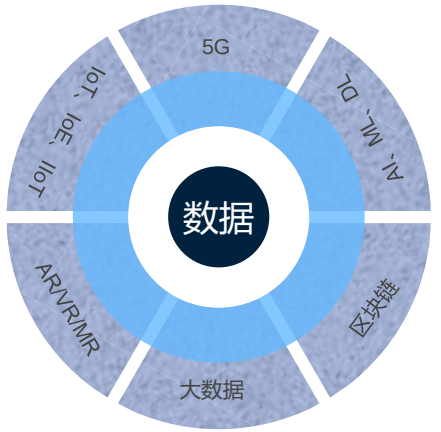
应用生命周期管理
开发，部署，升级，打补丁

应用高可移动
核心，远程分支，工作**站点**或设备终端，任意云，任意边缘

突出基于开源，一朵云在数字创新潜在风险，突出跨任意云现代化应用生产环境持续安全可靠交付AIOPs和LCM核心价值

集群，虚机，容器，微服务
AIOPs自动化管理

应用持续交付和生命周期自动化创新平台



数据核心企业级一致性资源平台

架构，资源，负载
LCM

资源平台

跨已有IT、边缘计算、多云资源平台

综合最新架构技术（CPU、GPU、FPGA、SCM、NVMe、Optane、AMD
EPYC满足新应用需求

虚机、容器、微服务应用、DevOps

应用资源自动化管理，监控，安全

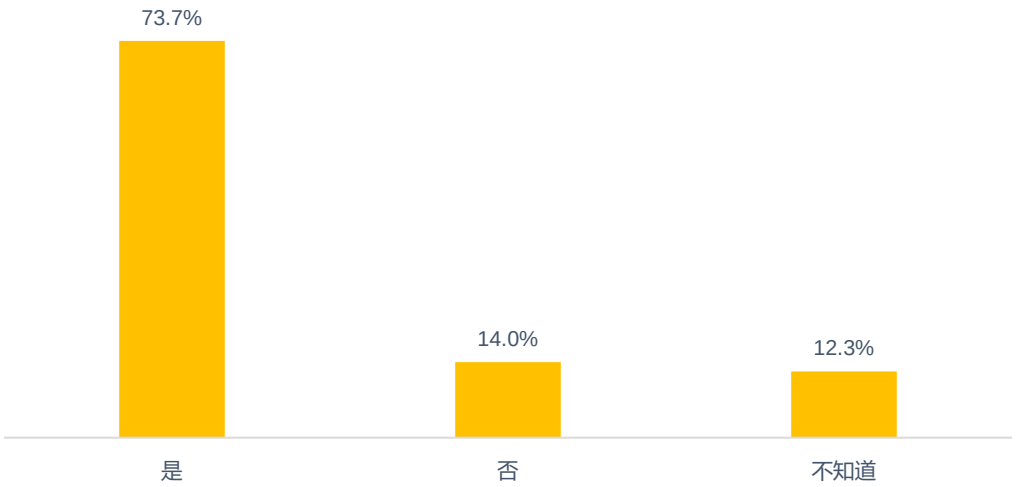
梳理呈现后疫情，新基建，企业级构建数字业务引擎路线图，突出跨核心-边缘（千行百业）-多云自动化资源平台业务价值

中国用户快速布局工业互联网

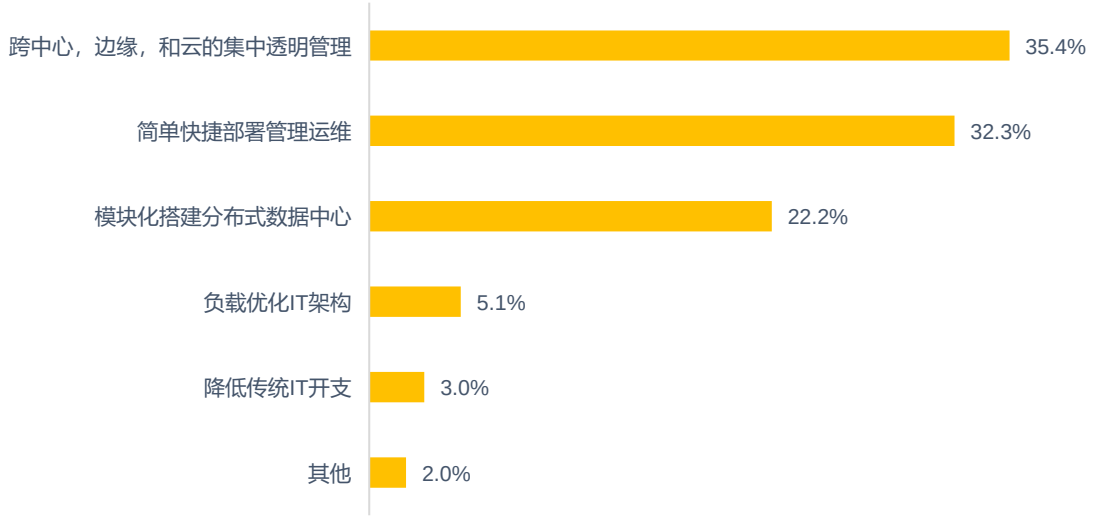
73.7%的中国用户选择企业级一致性跨核心-边缘-多云构建工业互联网就绪架构，推动中国企业对现代化云平台需求增长

35.4%中国用户采用超融合布局跨核心，边缘和云构建工业（产业）物联网架构

跨现有数据中心和多云以及跨边缘计算构建物联网就绪架构，企业级一致性是否会成为贵公司选择技术最重要评估指标?



贵公司考虑采用超融合架构最主要的因素是什么?



所有超融合都能做到工业互联网架就绪?

企业级一致性

模块化部署，跨核心-边缘-多云统一智能监控管理

数据来源：中桥调研咨询，2020

未来工业数据互联变化趋势

移动式连接

DELL Technologies

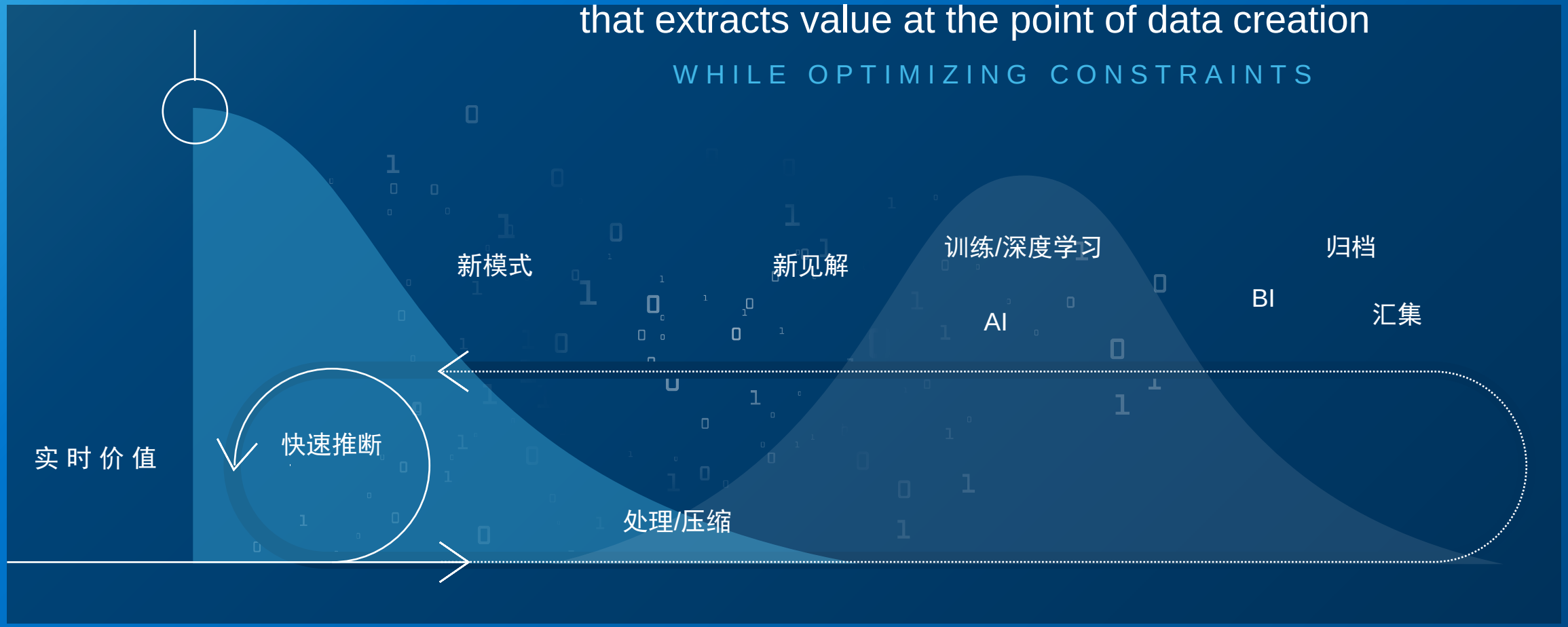
工业数据互联

数据创建/访问点

拥有您自己的边缘计算

with a system-wide compute and analytics strategy,
that extracts value at the point of data creation

WHILE OPTIMIZING CONSTRAINTS



约束

控制

戴尔科技集团边缘计算一览

Edge applications | Data collection | **Edge computing & analysis** | **Real-time analytics** | Data protection | **AI | deep learning**

- Autonomous vehicles
- Retail
- Smart manufacturing
- Telco / 5G

Dell Industrial PC

PowerEdge XE2420

PowerEdge XR11

PowerEdge XR12

PowerEdge XR2

Dell EMC Streaming Data Platform

PowerStore

VxRail

PowerProtect X400

Integrated Data Protection Appliance

HPC Ready Architecture with AI and Data Analytics

DELL EMC SD-WAN SOLUTION POWERED BY VMWARE

DELL TECHNOLOGIES CLOUD VMWARE CLOUD FOUNDATION

戴尔科技集团数字化工厂与工业互联网平台打造能力

建立立起研发、采购、制造、储运、销售及服务一体化的数字化工厂，实现工厂的纵向集成和企业价值链的横向集成

智造 IT技术

企业战略与变革

- 企业战略
- 业务流程再造
- 组织结构设计
- 关键绩效指标设计
- 变革管理
- 运营体系设计
- 精益生产管理

IT战略及系统整合

- 信息战略与规划
- 企业信息治理
- 信息服务管理
- 企业数据规划、建模
- 企业安全及合规
- 企业信息标准
- 主数据管理

智造 IT服务

企业应用与解决方案

- 智能制造数字化工厂方案及实施
- 生产管理
- 供应链管理
- 营销销售管理
- Sap 、Siemens定制化实施
- 架构设计、需求分析、设计
- 开发实施

IT技术服务与基础设施

- 技术架构设计
- 基础设施架构设计
- 云平台（IaaS/PaaS/SaaS)及实施服务
- 大数据平台及实施服务
- AI平台及实施服务
- 物联网集成及服务
- IT运维

戴尔供应链定义灯塔工厂标准

全面的数字化工厂转型方案

采用独特的方法论，我们对客户具体情况快速制定针对性的解决方案，且任何两个方案都不会相同。

智能制造数字化工厂项目交付

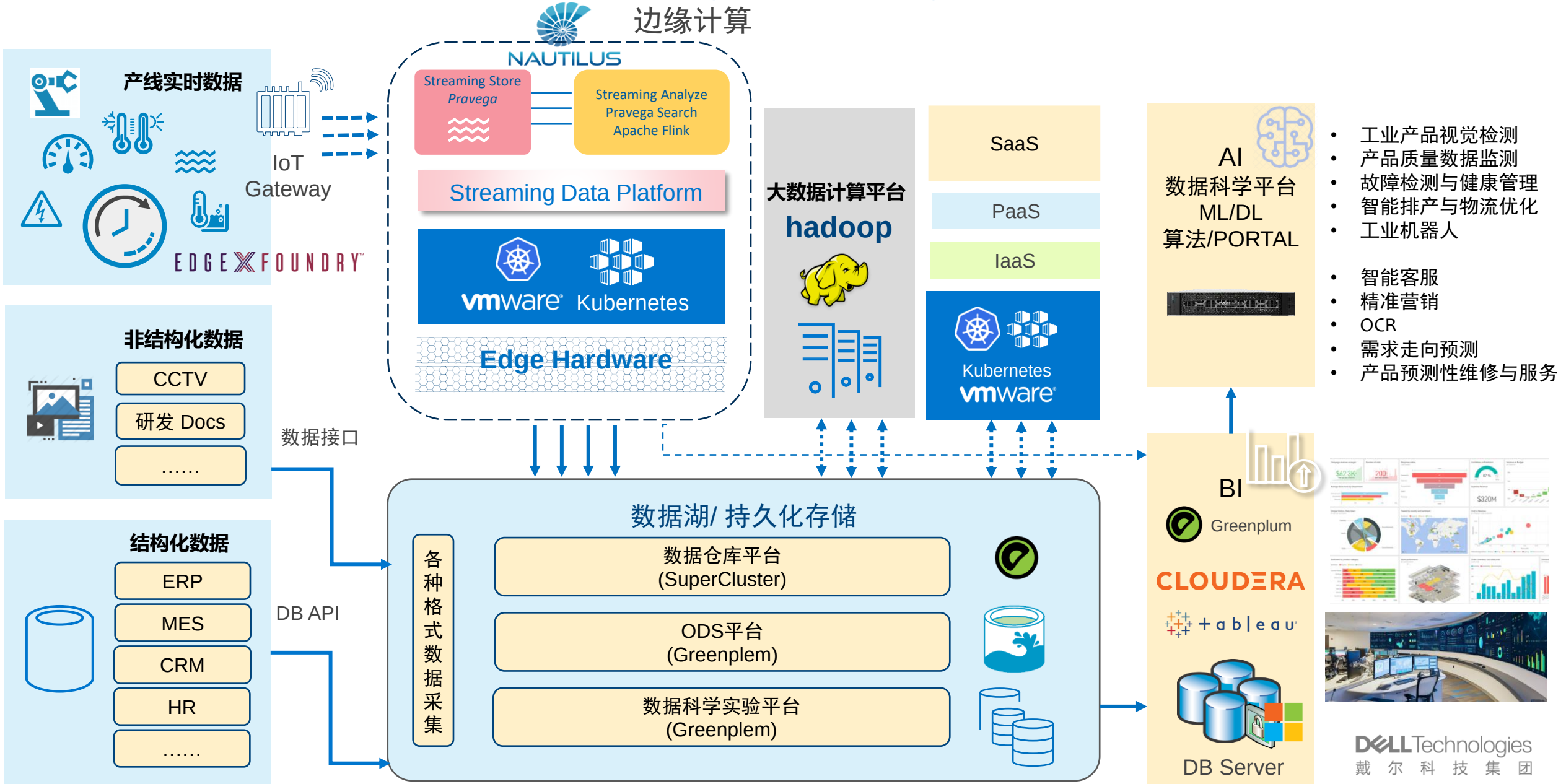
采用敏捷项目管理，支持传统应用开发交付和PaaS云原生微服务开发交付，助力企业数字化转型。

- 作为全球领先的咨询服务与IT产品提供商，戴尔服务能帮助客户应对瞬息万变的外部环境，设计供应链协同模式，有效解决棘手企业智能制造相关业务和技术问题。我们与客户携起手来，拓展密切协同的伙伴合作关系，籍由精深专业经验、久经实践验证的最佳实践方法和工具，能有效协助客户实现战略目标。

DELL Technologies

intel

业务全流程数据流动 IoT + Streaming Data + Big Data + BI + AI



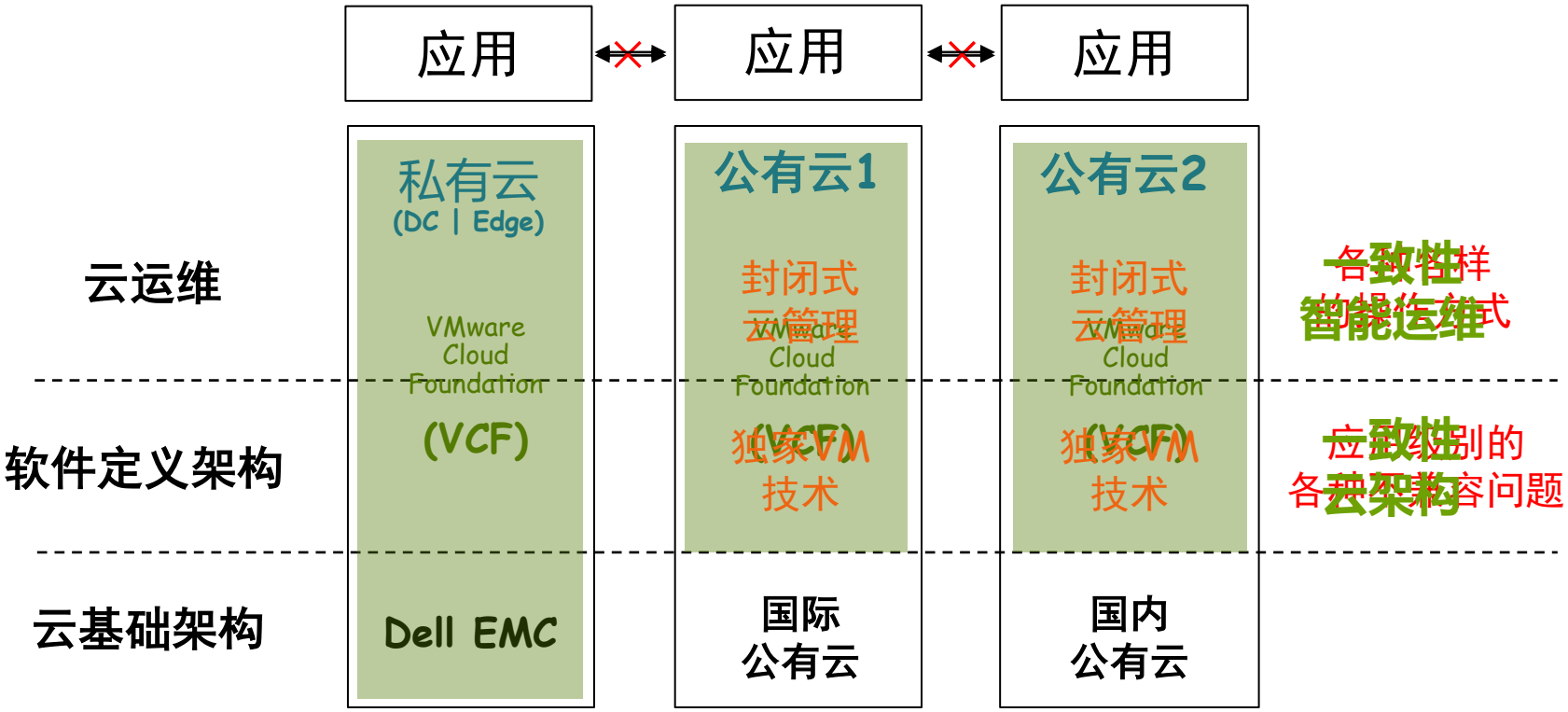
戴尔科技云平台：真正的多云治理!

✓ 软硬件一体化全生命周期管理

✓ 应用灵活跨云弹性部署

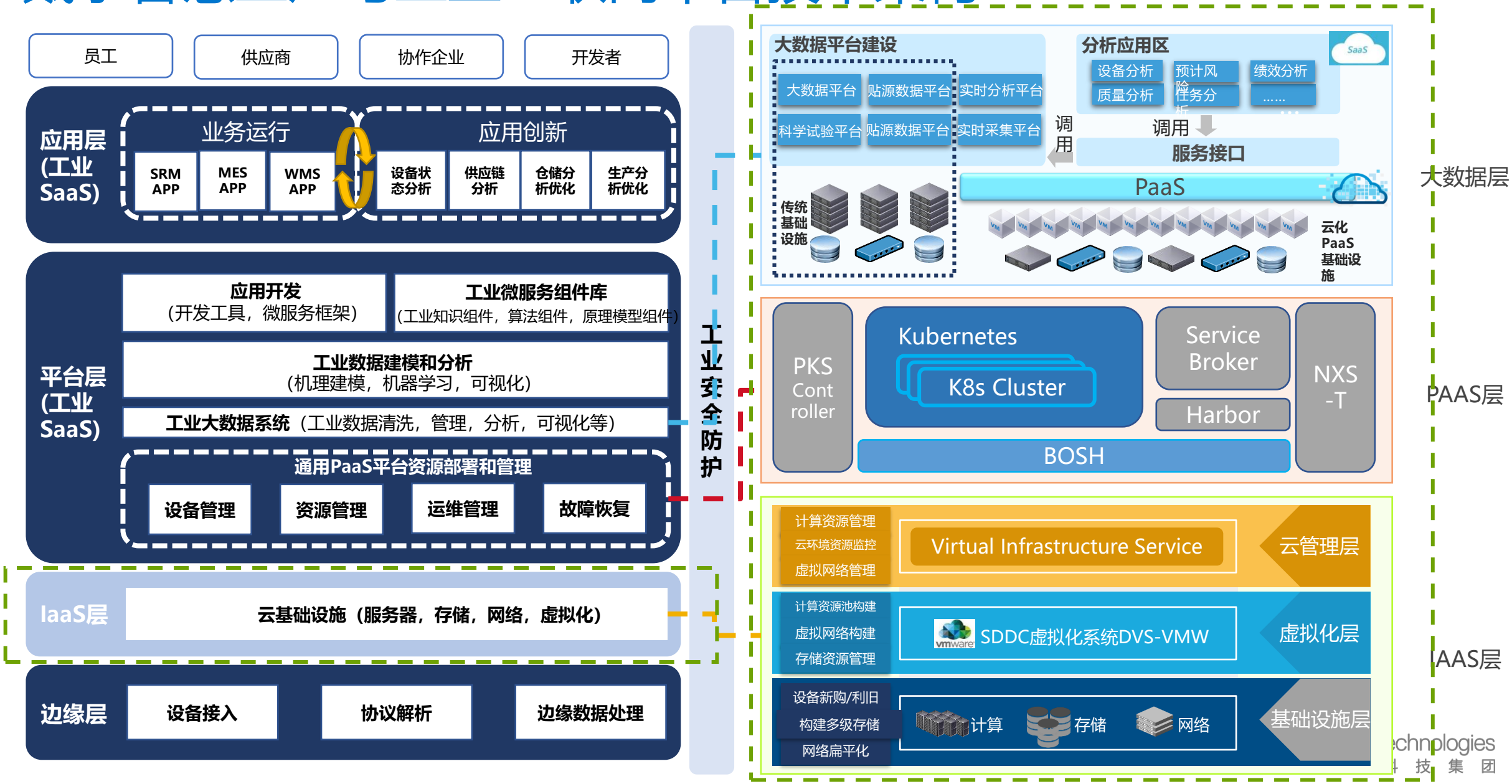
✓ **由应用驱动的多云平台**

戴尔科技云平台
一致性的云策略



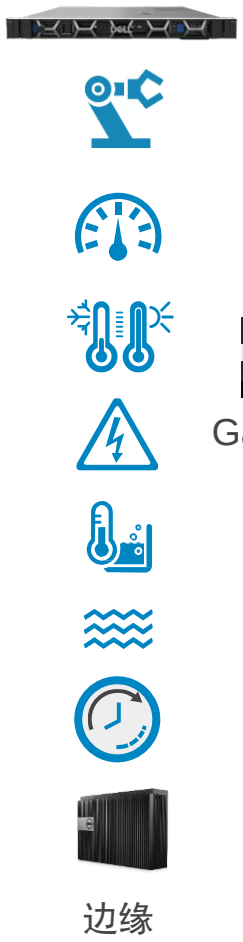
DELL Technologies 戴尔科技集团

戴尔智慧工厂与工业互联网平台技术架构



工业互联网现代化应用交付平台

工 业 互 联 网



边缘

Gateway

PowerEdge

PowerMax

PowerConnect

PowerStore

PowerProtect
Data protection

PowerOne
PowerFlex

Hyper Converged Infrastructure(HCI)

核心

vmware

Kubernetes

Hyper-V

OpenStack

现代化应用交付平台
-- Dell Technologies
Cloud Platform

戴尔科技云平台

CRM | PLM | MES
SCM | ERP | SRM

工业
SaaS

DevOps | Data Lake | DB
Big Data | AI | Email

工业
PaaS

虚拟机服务 | 容器服务PKS
主机托管服务

IaaS

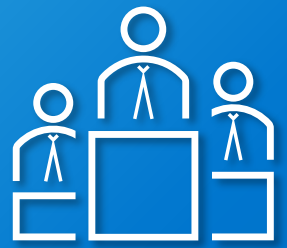
多云

Cloud

多云安全协作创新

戴 尔 科 技 集 团

数字化战略面临的最大挑战



建立数字化组织

混合云

混合工作负载

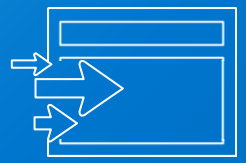
安全

企业的多云旅途: 简单 v.s. 复杂

期望

现实

多云：在激发业务创新的同时**也提高了IT的复杂性**

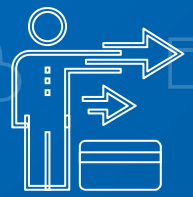


复杂的工作负载
迁移和周期管理

运营孤岛

分散的运管工具

不确定 & 不一致
的安全策略

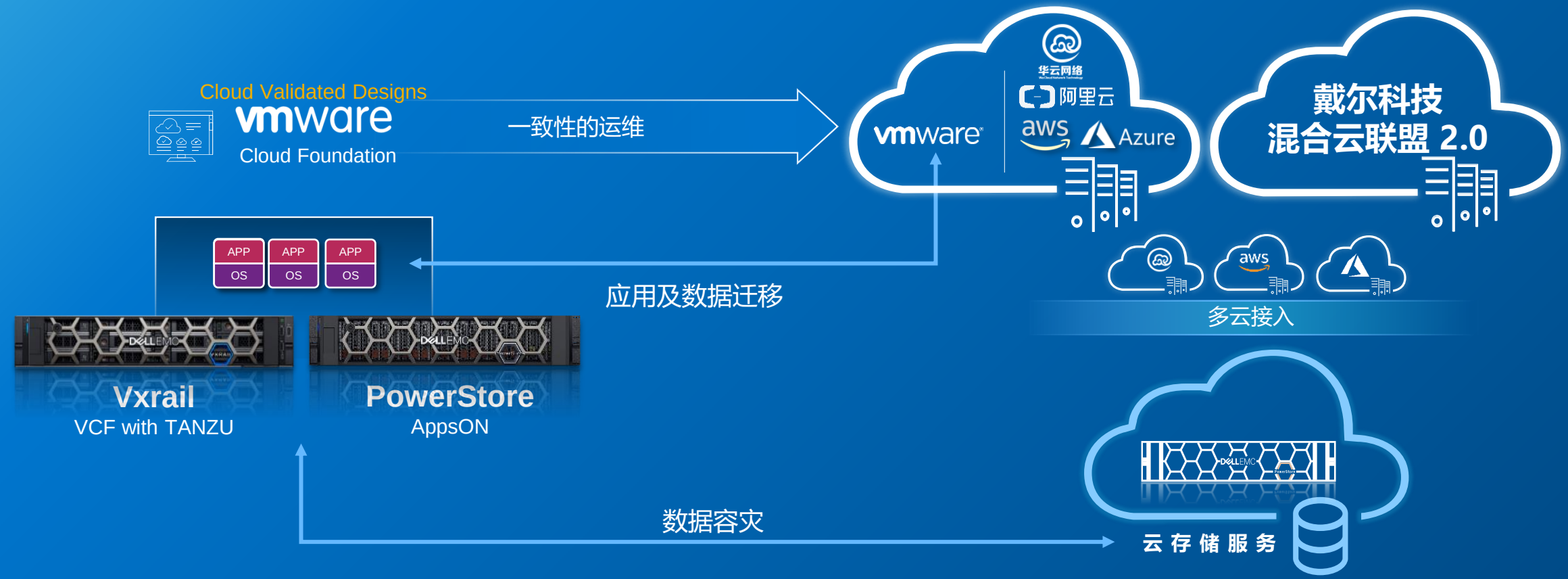


需要学习
新技能+新流程

不一致的SLA

影响了初衷/进度… 云对业务的实效性

戴尔科技云平台　混合云服务



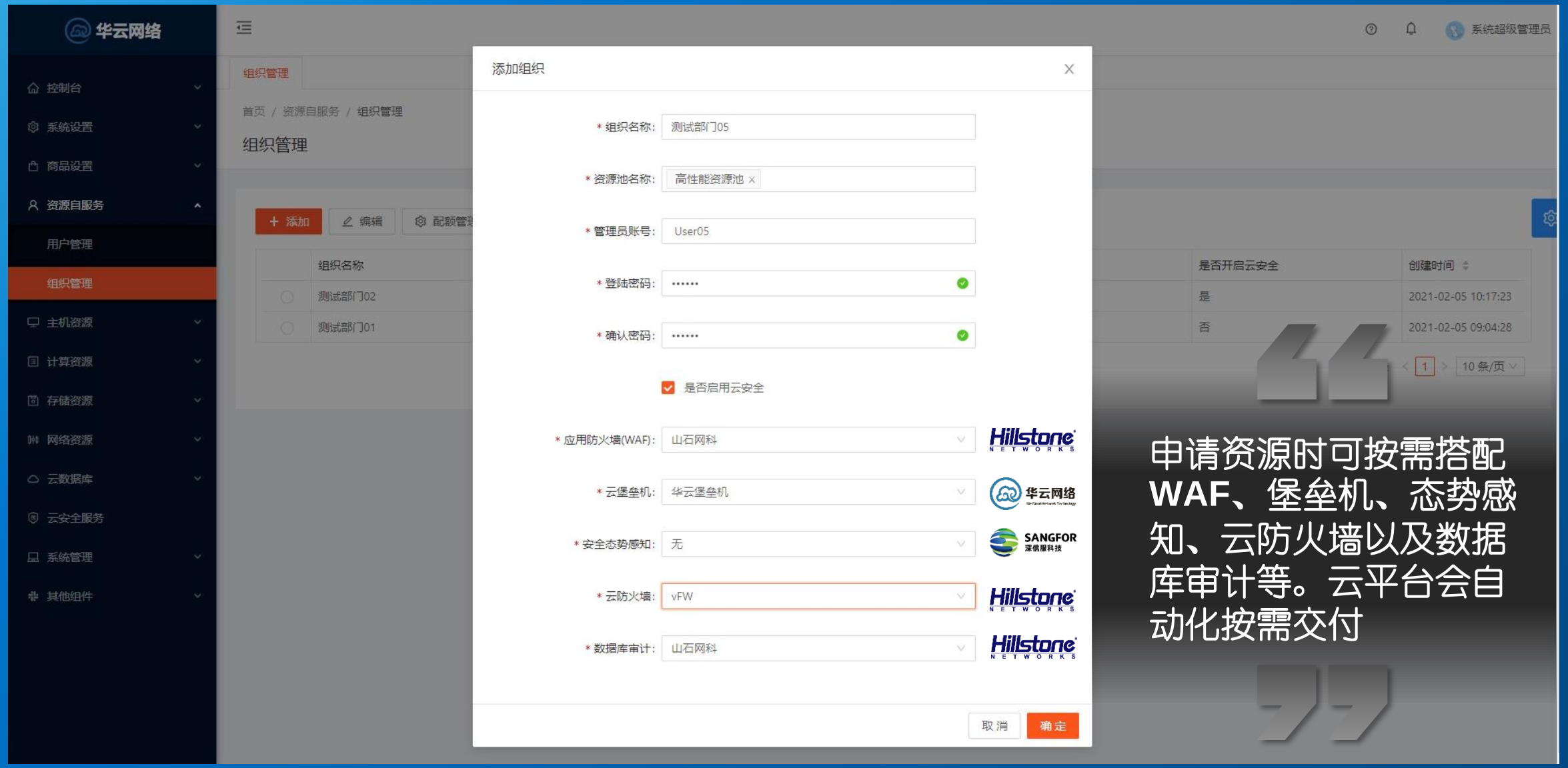
借助VCF实现
无缝的应用移动性

用于工作负载
迁移、分析、测试/开发的多云

可扩展、弹性强的
云连接存储

定制化云管平台

云安全管理



申请资源时可按需搭配WAF、堡垒机、态势感知、云防火墙以及数据库审计等。云平台会自动化按需交付

安全问题的梳理——

主机数量 x 虚拟机数量 x 容器数量 x 微服务数量

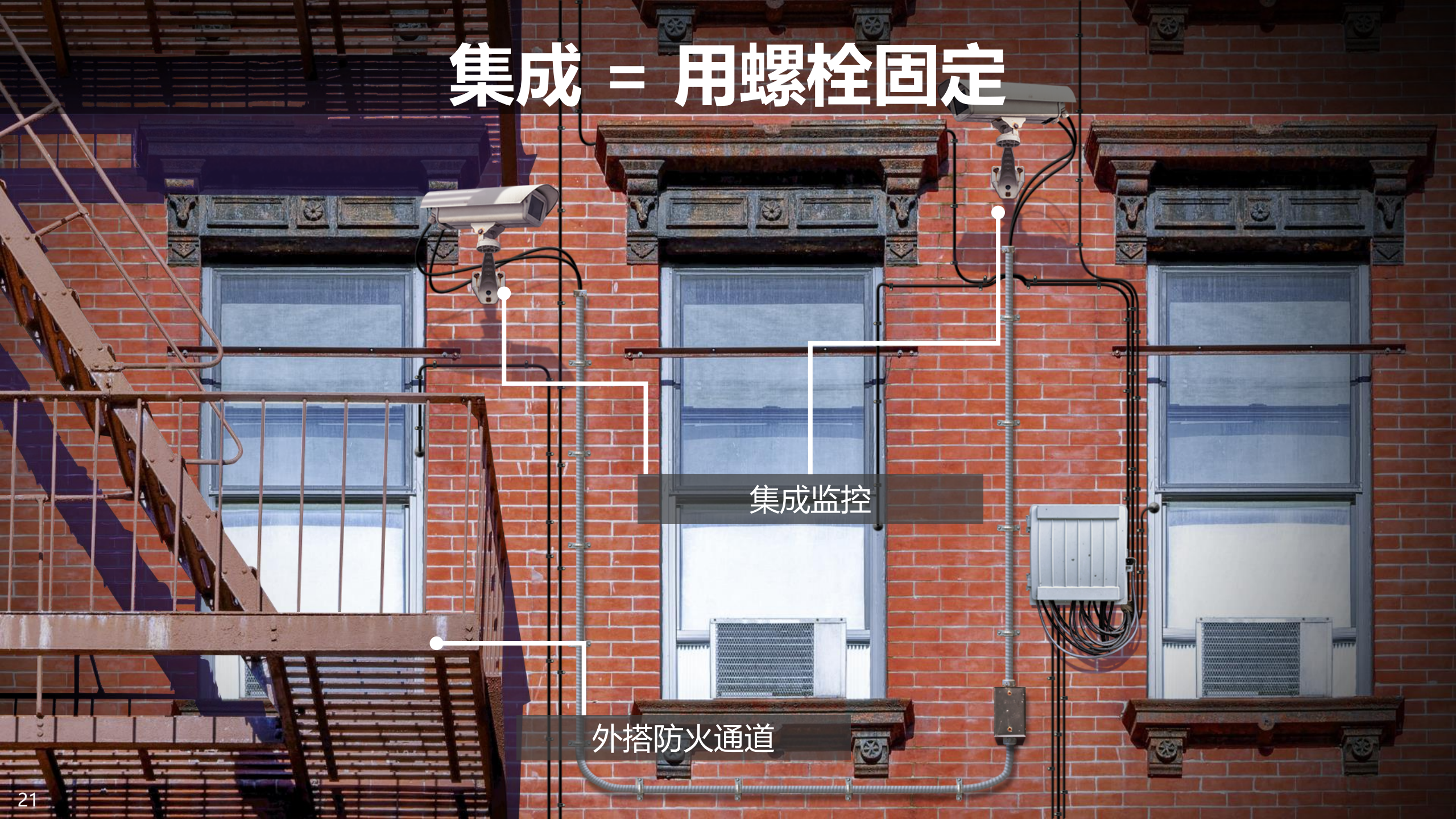
参考《GB/T 37956—2019 信息安全技术 网站安全云防护平台技术要求》、《GB/T 37972—2019 信息安全技术 云计算服务运行监管框架》，共梳理35个风险，其中19个风险属于云计算新引入。

工作量随之指数级增长

“集成”的代名词就是“高度复杂”

“复杂”本身正是“安全”的天敌

集成 = 用螺栓固定

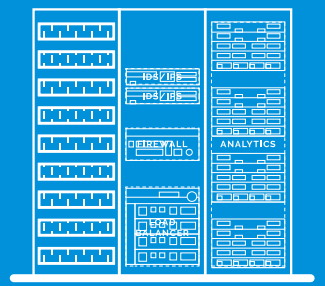


原生 = 内建... 这有本质的不同

云内生安全

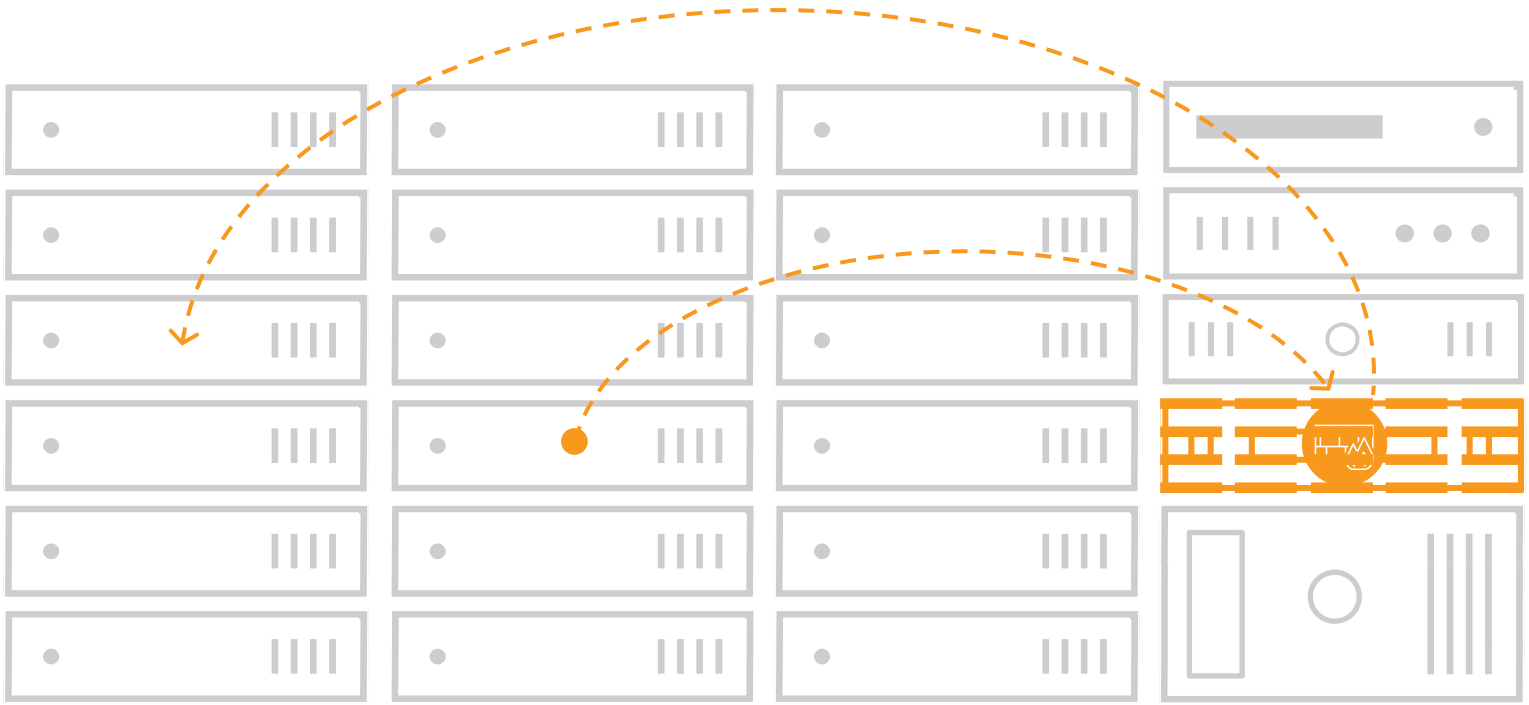
为云内流量设计

分布式架构防火墙



策略紧随虚机和业务，无需重构网络，多种策略部署方式（标签、业务类型、用户身份等），灵活高效投入小.

过去 所有流量要绕行至边界防火墙和IDS/IPS



传统边界安全的缺陷

流量发卡弯

转发效率低

存在吞吐瓶颈，延时高

需要复杂的网络改造

靠近每台虚机/容器的云内防火墙和IDS/IPS

专为大规模设计的控制平面

开放的安全平台

支持第三方无代理安全产品

AsiaInfo 亚信安全 | paloalto NETWORKS | Check Point Software Technologies Ltd. | Symantec | KASPERSKY | FORTINET | TREND MICRO | Hillstone NETWORKS

没有边界瓶颈

流量本地处理，无需绕行；为东西向流量提供了全面保护，线性扩展无性能瓶颈

业内唯一Hypervisor内生安全解决方案

天然集成在Hypervisor内核，任何攻击无法Bypass

软件定义分布式技术

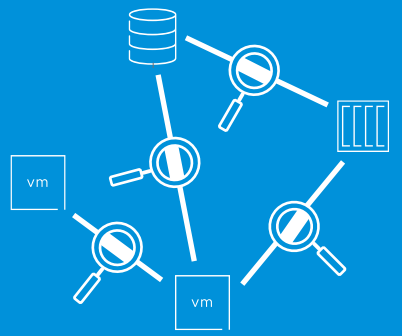
控制平面与数据转发分离，易于扩展，可以支持XXXX个节点或通过联邦技术支持YYYY个

云内生安全

为云内流量设计

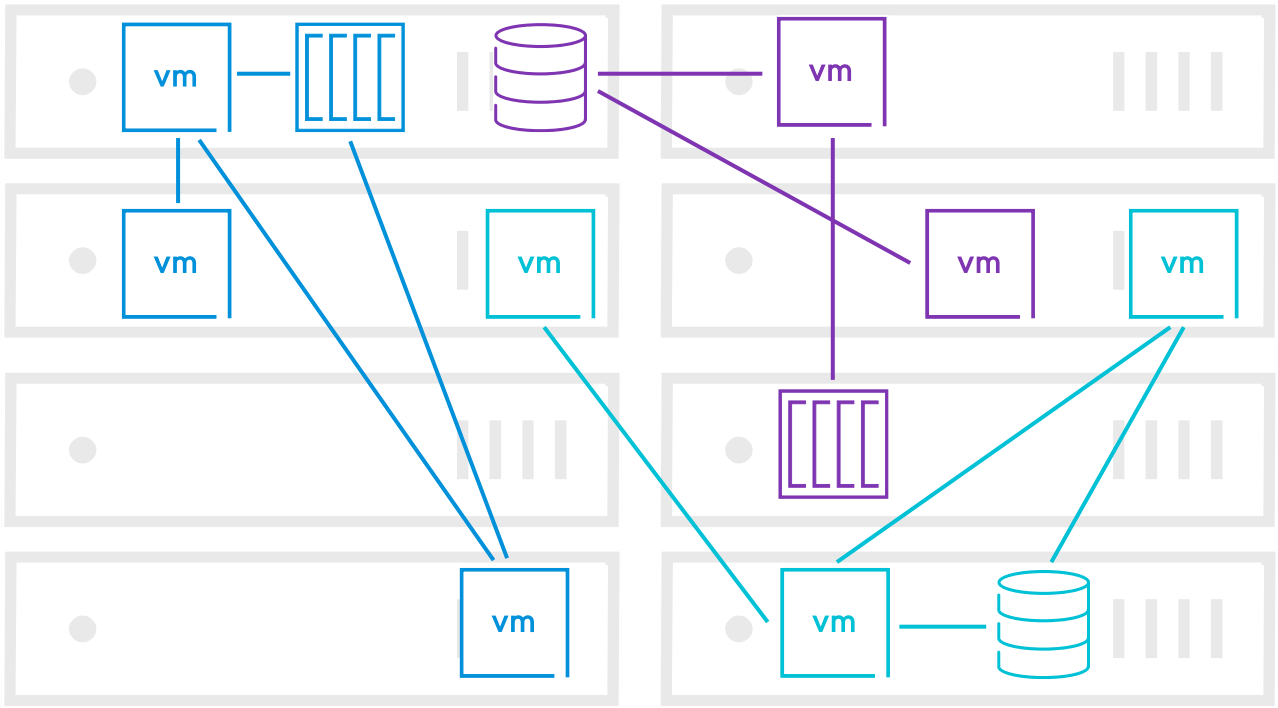
分布式架构防火墙

业务感知



根据上下文场景，业务类型，自动化推荐安全策略，有针对性的为应用开启相关策略和行为特征库

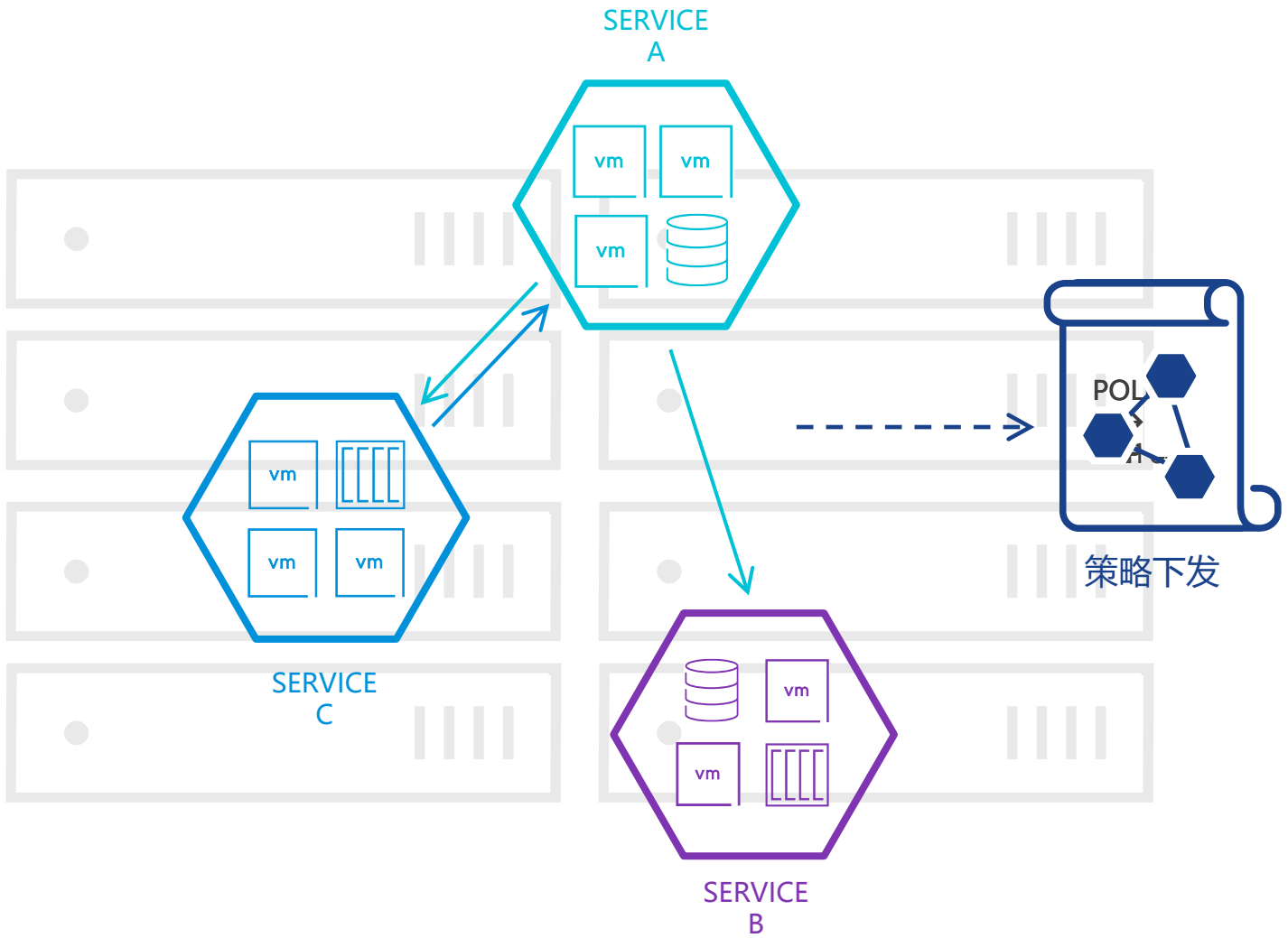
NSX Intelligence–学习和梳理应用行为基线



安全策略规划

拥有完整的应用流量和进程可视化，自动评估应用行为基线

学习和梳理应用行为基线



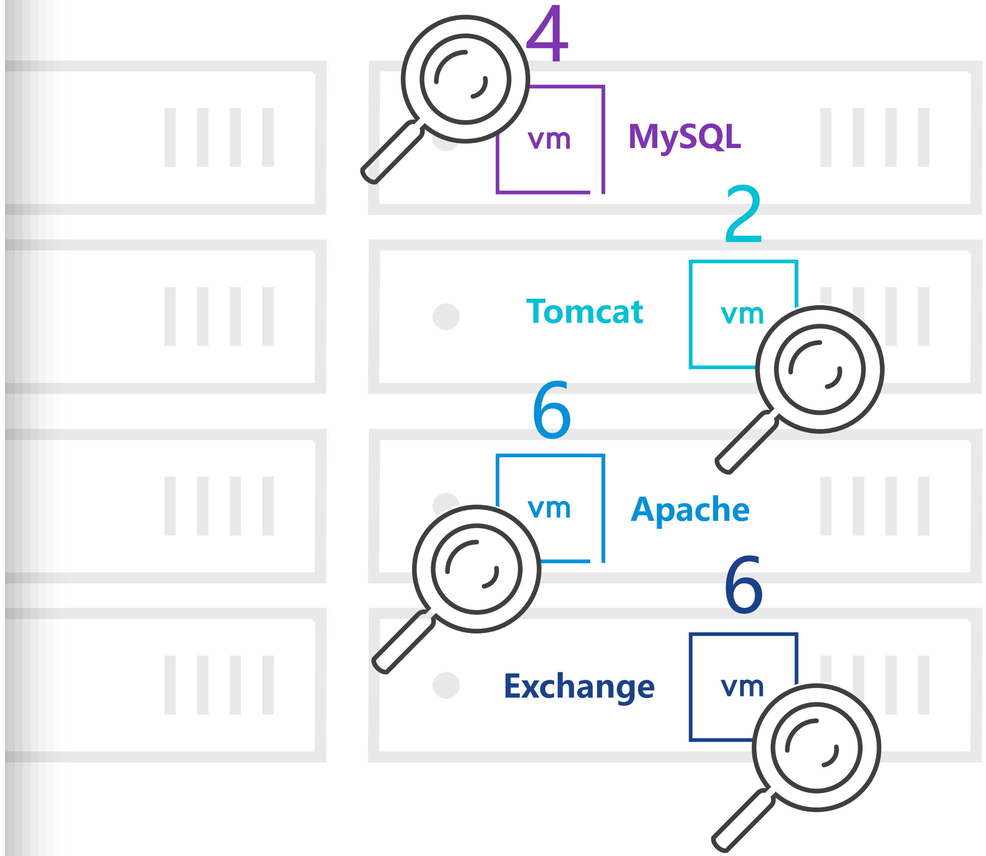
安全策略规划

拥有完整的应用流量和进程可视化，自动评估应用行为基线

自动梳理应用访问关系，并基于应用行为和属性进行策略分组

主动推荐微分段安全策略

学习和梳理应用行为基线



安全策略规划

拥有完整的应用流量和进程可视化，自动评估应用行为基线

自动梳理应用访问关系，并基于应用行为和属性进行策略分组

主动推荐微分段安全策略

个性化安全策略推荐

根据业务种类，业务所在位置，有针对性的推荐相关的IDS/IPS特征库和防火墙策略，从而避免了传统边界安全的无效监控

DELL Technologies 戴尔科技集团

云内生安全

为云内流量设计

分布式架构

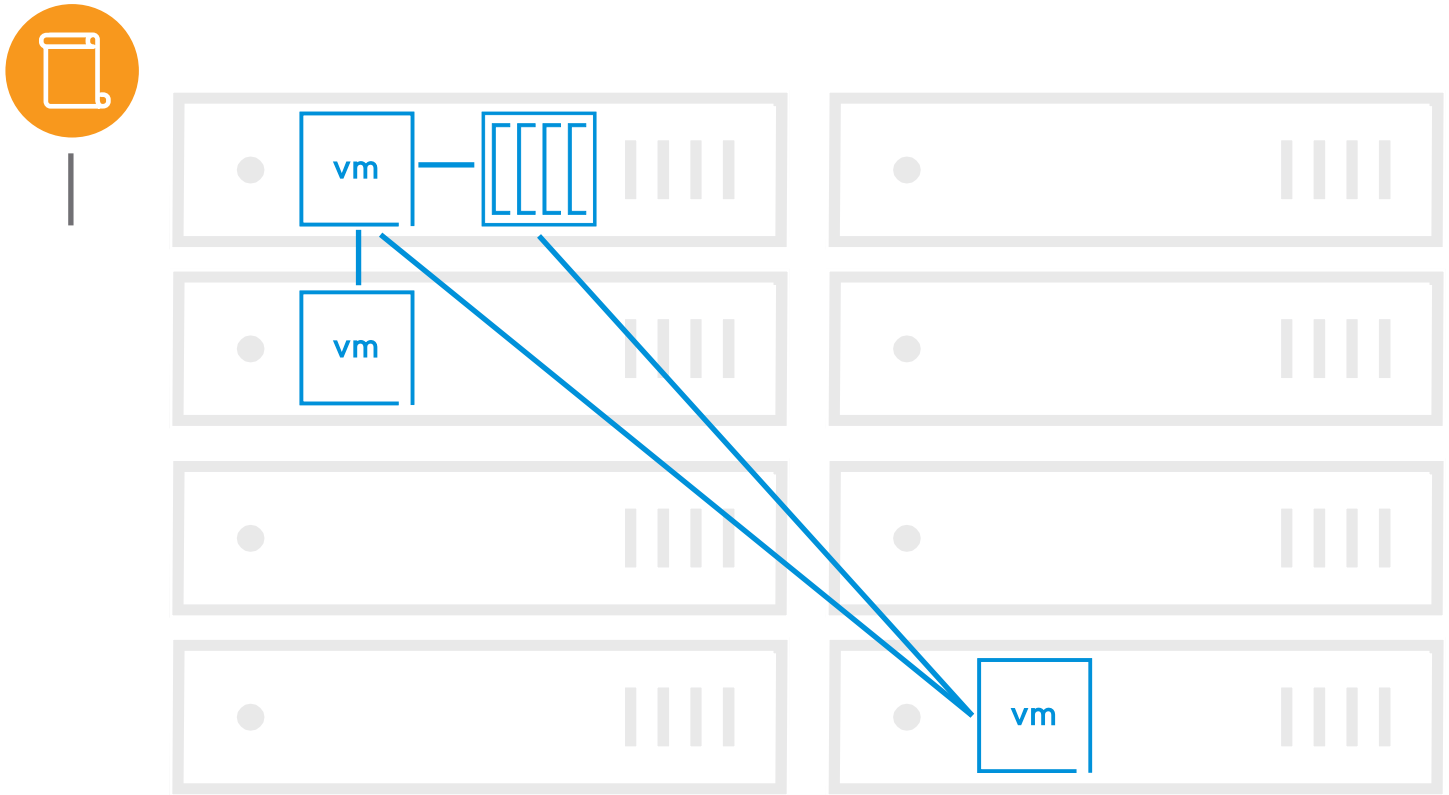
业务感知

操作简单

策略配置简单，紧随应用位置漂移，
高度自动化助力敏态应用

灵活多样化的策略分发机制

FW RULES



过去：基于网络，IP子网，VLAN

Access-list 100 permit TCP any 192.168.1.1 255.255.255.255 80
Access-list 101 permit TCP any 192.168.1.2 255.255.255.255 80
Access-list 102 permit TCP any 192.168.2.1 255.255.255.255 80
Access-list 103 permit TCP any 192.168.2.2 255.255.255.255 80
Access-list 104 permit TCP 192.168.1.1 192.168.2.1 255.255.255.255 8080
Access-list 105 permit TCP 192.168.1.2 192.168.2.2 255.255.255.255 8080
Access-list 106 permit TCP 192.168.2.1 192.168.4.1 255.255.255.255 3306
Access-list 107 permit TCP 192.168.2.2 192.168.4.2 255.255.255.255 3306
Access-list 108 permit TCP 192.168.1.1 192.168.2.1 255.255.255.255 6379
Access-list 109 permit TCP 192.168.1.2 192.168.2.2 255.255.255.255 6379
Access-list 110 permit TCP 192.168.2.1 192.168.4.1 255.255.255.255 3306
Access-list 111 permit TCP 192.168.2.2 192.168.4.2 255.255.255.255 3306
Access-list 112 permit TCP 192.168.1.1 192.168.2.1 255.255.255.255 8080
Access-list 800 deny any any

安全策略基于“分组”，而不仅仅是基于“网段”

分组可以细致到每个虚拟机的虚拟网卡，实现同网段内部的安全防护

采用预定义规则进行智能分组，实现高效的安全防护

虚拟网络内部的分布式防火墙，策略跟着业务走

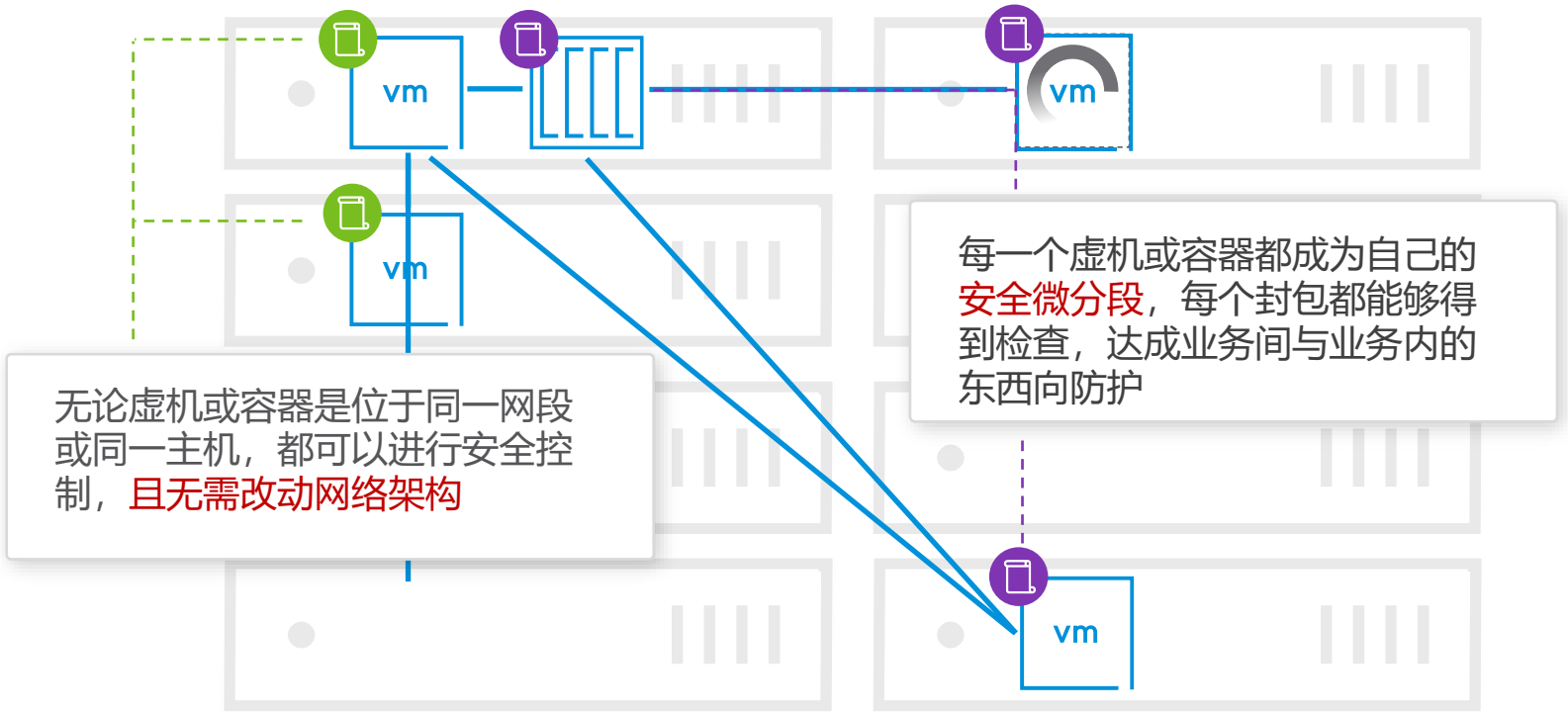
K8S标签 | VM安全标签 | VM名字

应用层次 | 操作系统 | AD用户

几十条至几百条基于IP的策略

无法与业务生命周期同步
无法自动跟随业务位置调整

灵活多样化的策略分发机制



基于业务属性智能分组

可以根据Intelligence梳理的信息业务分组，参考智能推荐的策略，实现快速安全策略规划

为业务分组

为不同业务组打标签，定义组策略

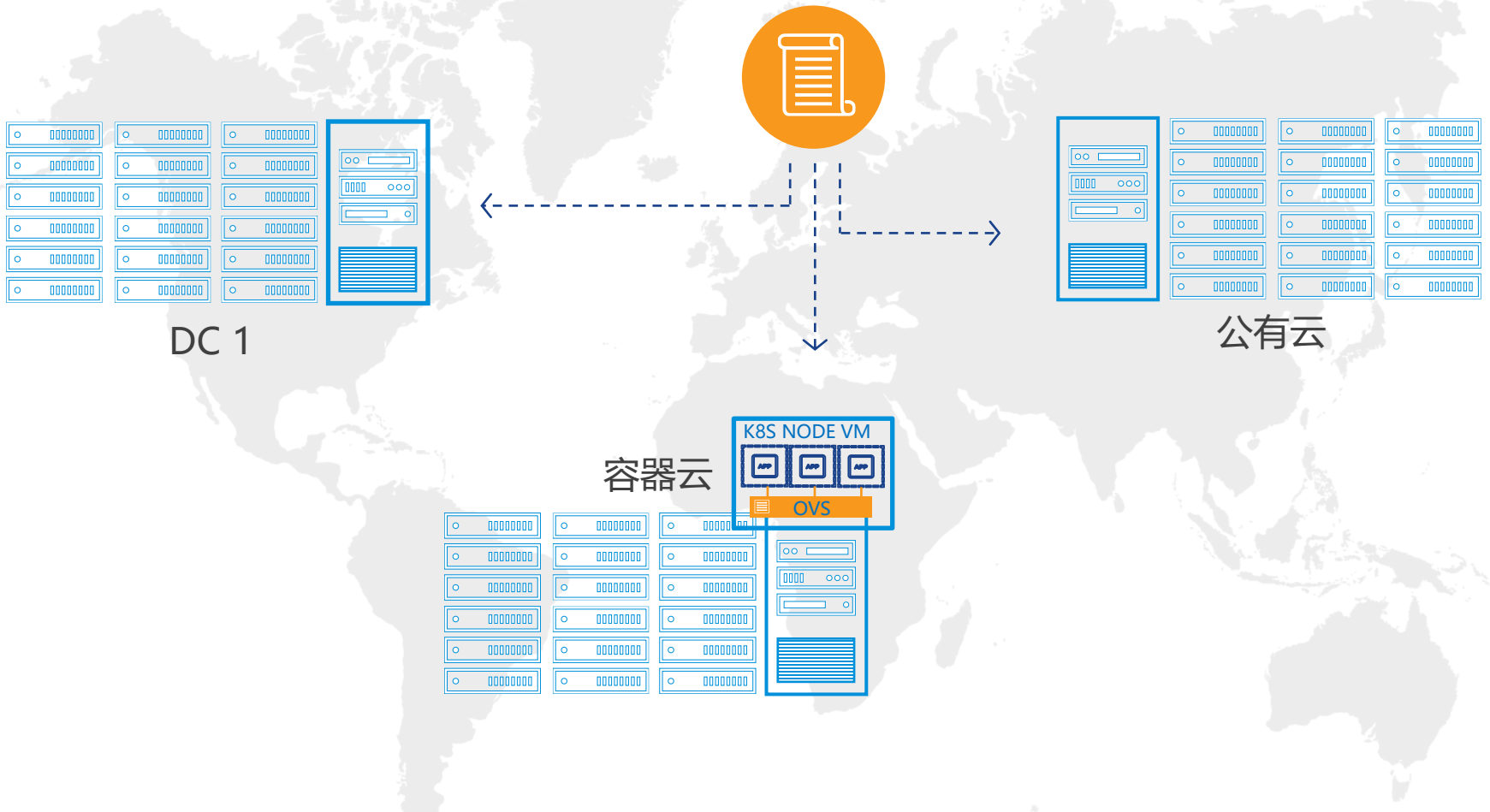
跟随业务自动化部署

为业务组内新创建的虚机自动化关联相关组策略

安全策略跟随业务漂移，无需人工干预

当业务下线时，相关安全策略会自动删除，与业务生命周期同步，简化运维难度

多云环境策略统一部署



基于业务的策略定义:

一次定义，可以分发至不同部署位置

策略紧跟业务漂移，无需干预，适合容器化敏捷业务场景

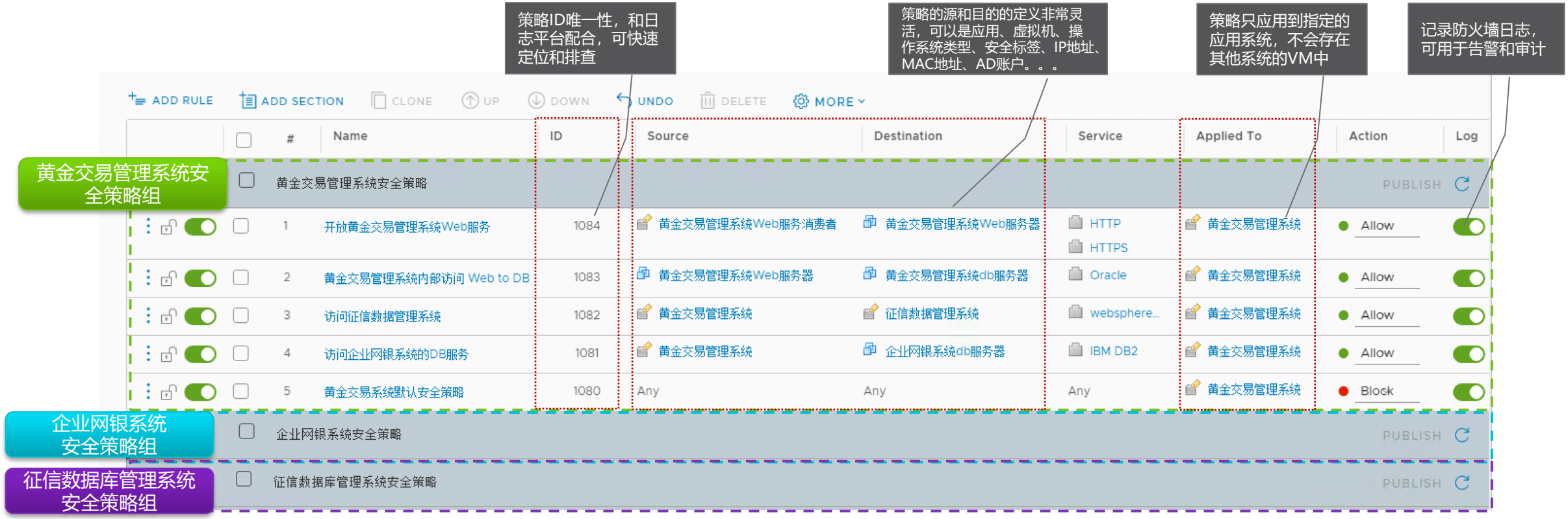
本机云服务端点发现和实施。

可以选择NSX强制实施(基于代理)或本地云强制实施(无代理)

结合专家经验和NSX Intelligence得出安全策略

操作简单 易于维护

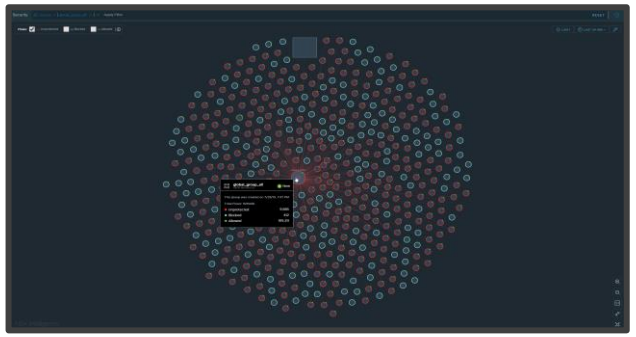
- 以应用系统/虚拟机为单位，从应用的视角/语言进行安全策略控制
- 单个应用系统/虚拟机安全策略的变更调整，不会影响其他应用系统
- 分布式架构，每个应用系统/虚拟机的安全策略更少，带来更好的性能



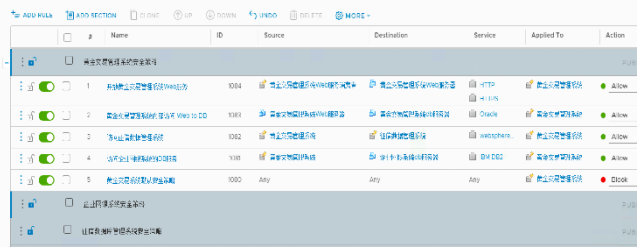
助力用户应对等保安全法 网络攻防演练

以*NSX Data Center*和*vRealize Network Insight*组成的“云安全四步方法论”，帮助客户快速应对“网络攻防演练”，对虚拟化环境实现“安全、可视、可控”。

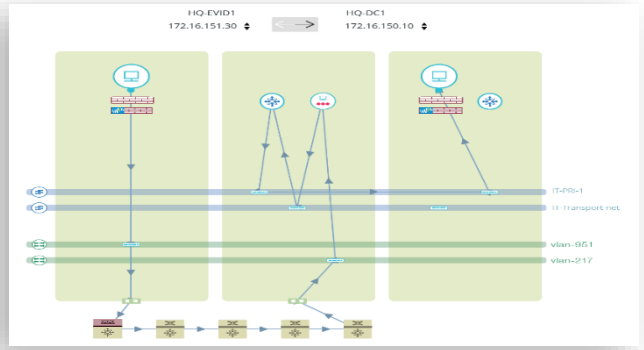
通过NSX和vRNI彻底梳理虚拟化内部访问和流量



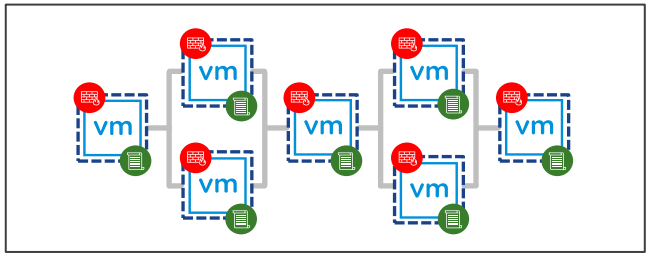
“人机结合”的安全检查，精确整理和制定安全策略



基于NSX Log，vRNI和vRLI等的持续监控、反馈和改进



通过NSX DFW构建零信任架构



DELL Technologies
戴 尔 科 技 集 团

您知道吗？

K8S的两位创始人在VMware负责vSphere7的代码研发

Cloud Foundry是VMware的开源项目

Greenplum是VMware的开源项目

Spring 是VMware的开源项目

12306正是使用了GemFire才让中国人能在春运顺利购票

HARBOR是VMware 中国研发团队在CNCF毕业的开源项目

NSX是唯一支持虚拟机——容器——原生公有云的SDN

世界最大的公有云都支持VMware混合云服务

案例

某数字化工厂
工业互联网建设

Nanjing

Requirement 1:	Requirement 2:	Requirement 3:		Requirement 4:	
ECN EIT block	ECN EIT file	EFN SM		ECN BIT	
VxRail P570F	Isilon H500a	VxRail V570	Isilon H500b	VxRail P570F	Isilon H500a
Requirement 7-9（combined with 5）:				Requirement 6:	
ECN DMZ block				ECN DMZ/IoT file	
VxRail E560				Isilon H500a	

*Nanjing is supposed to be DC for both ECN&ECN; may ECN be ...

DATA CENTER

NANJING DC:

DTCP solution: VCF on VxRail+Isilon+DPS

- ECN and EFN are physically isolated, which VxRail cluster has each management domain.
- ECN VxRail would be divided into two workload domains:

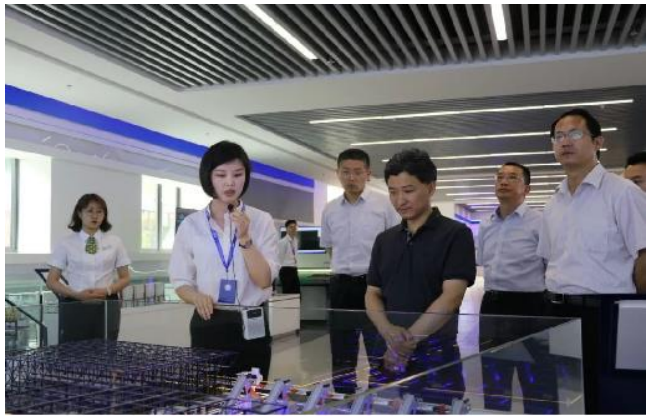
1. P570F for ECN EIT &BIT hosting block data;
2. E560 for ECN DMZ block data;
3. EIT,BIT and DMZ are logically isolated within ECN.

- EFN VxRail has one workload domain V570 for SM block data.
- Two Isilon H500 are used for ECN file data and SM HDFS data.
- Two DD6900 with DPS package and NDMP Accelerator Node would be used for ECN and EFN.

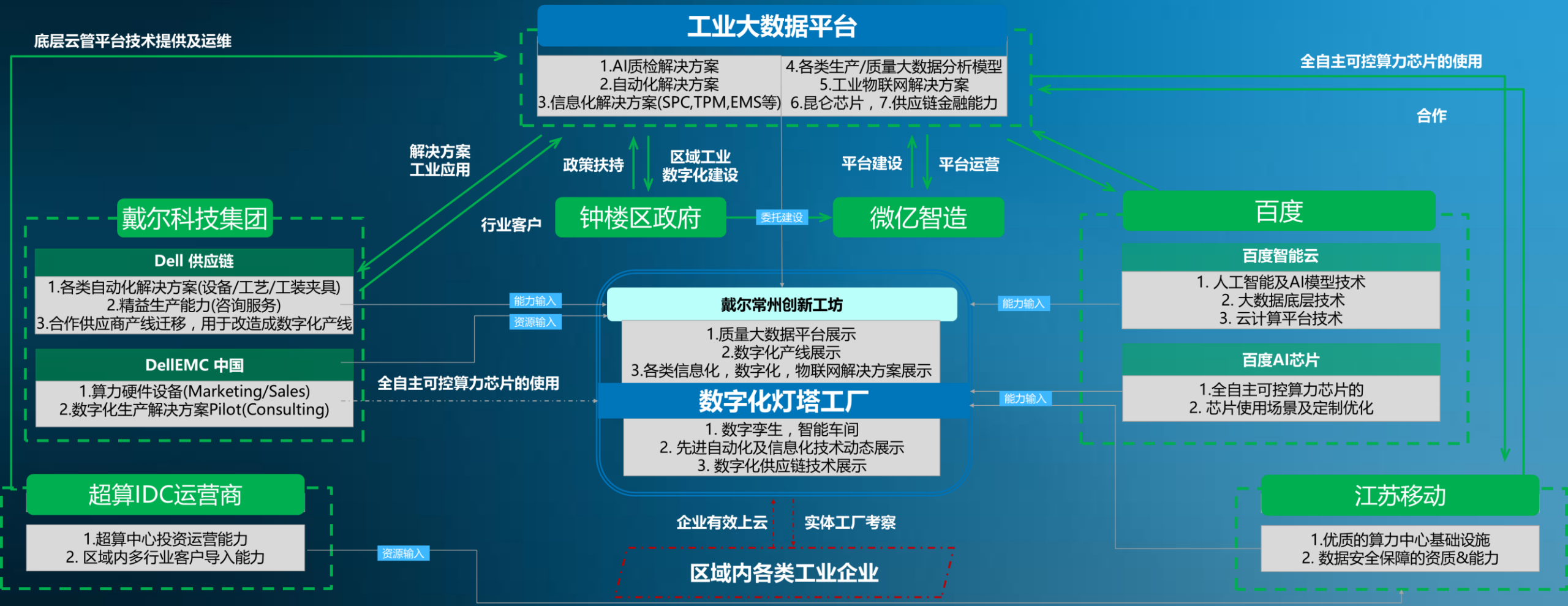
扬州市工业互联网平台及创新基地

2019-10，扬州市委书记谢正义一行在戴尔科技峰会，与戴尔科技集团董事长兼首席执行官迈克尔·戴尔先生会谈交流，并一同见证扬州生态科技新城管委会与戴尔科技集团签署“戴尔—扬州创新基地”战略合作备忘录。

2020-08，“戴尔-扬州创新基地”人才培养训练营一期开营仪式在扬州市生态科技新城扬州软件园举办，训练营首批116位学员参加了开营仪式。



某市工业大数据智能云 – 项目支持架构



案例：某智能制造系统共享平台

长期计划

年度销售计划　年度生产计划　年度需求计划　年度采购计划

KPI统计分析

生产统计分析　供应链统计分析　销售统计分析

客户

客户管理

周期性销售计划

销售结算

销售机会　客户管理　销售执行　销售渠道　销售合同/订单

销售部

销售管理、客户管理、产品管理、销单交付准备、订单生产进度查询

销售发货计划　销售发货单

销售发货单

产品管理

图纸文档管理

产品结构化管理　零部件

新产品研发　产前工艺准备　工艺路线工序　产品结构及配置

产前准备

技术部

产前工艺准备

生产订单

运输需求

配送计划

配送过程

配送结算

生产部

主计划和日计划各级安排、进度跟踪、车间各类生产指标问题解决

生产建模　生产人员管理　看板管理

生产计划/作业计划　生产排产　生产调度　生产工艺及工序

采购仓储部

采购寻源、采购成本控制、供应商管理、仓储物流管理

物料管理

资源计划

物资需求

采购订单　采购合同　采购需求　采购计划

供应商

供应商管理

原材料出库

领料申请单

领料申请

采购结算　原材料入库

原材料入库检测

领料出库单

车间收货管理

物料管理

工艺卡送达

现场作业管理

产成品出库单

产成品入库申请

质量管理　产成品入库　产成品出库　车间发货管理


DELL Technologies