



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

CSA

打造面向应用的云安全体系架构 The Construction of Cloud Security System Facing Application

臧铁军

VMware资深解决方案架构师
全球CTO大使

Senior Architect of Solutions in VMware China Excellence Centre
Global Ambassador of CTO

目录

Agenda

趋势与需求

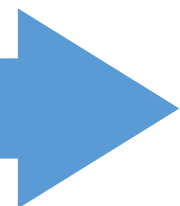
Trend and Requirements

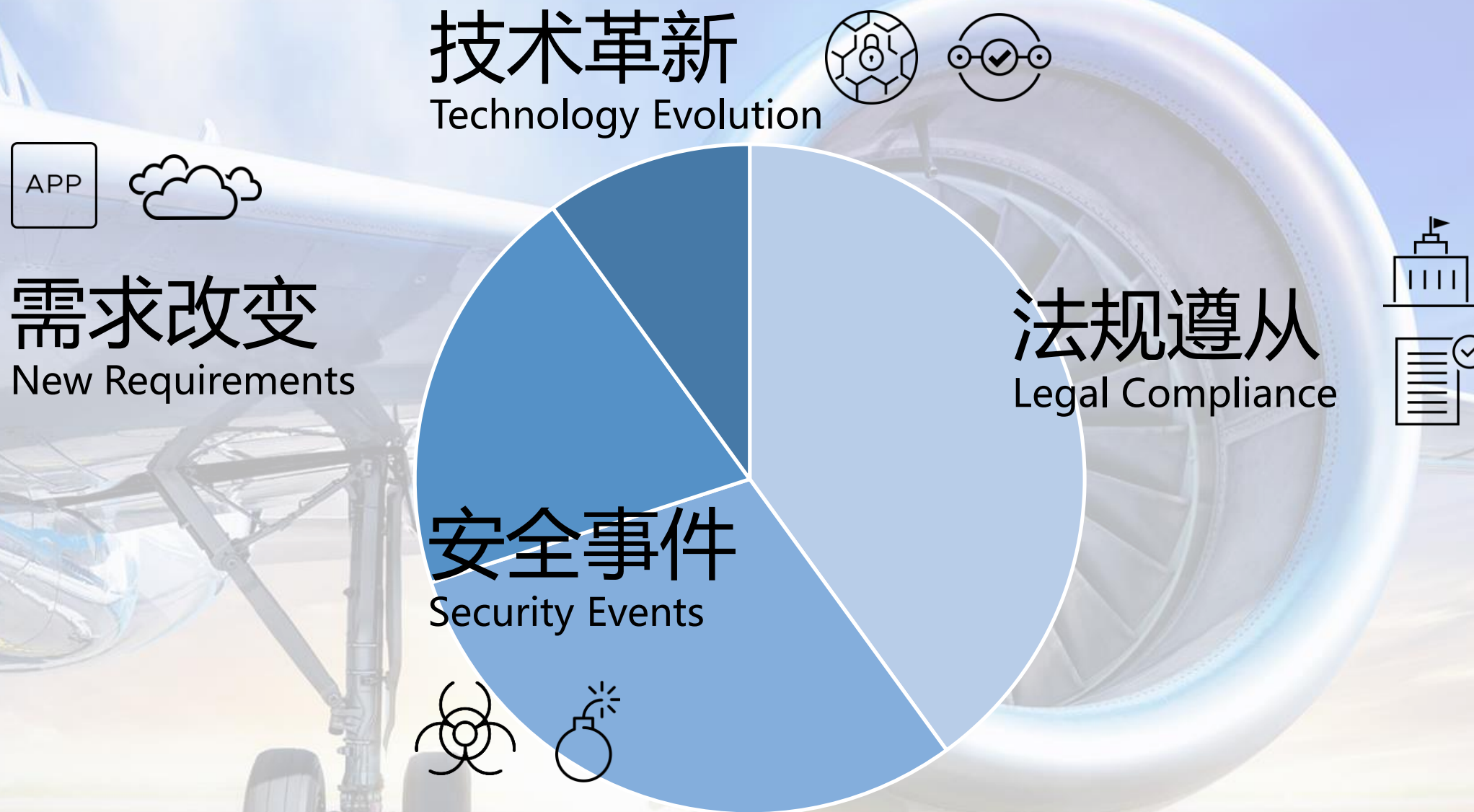
解决方案建议

Solutions

策略与路线

Strategy and Approach





以终为始 BEGIN WITH THE END IN MIND

不忘初心

Stay Focused

与时俱进

Be Adaptive



从“云的安全”到“安全的云”



From Cloud Security to Secured Cloud

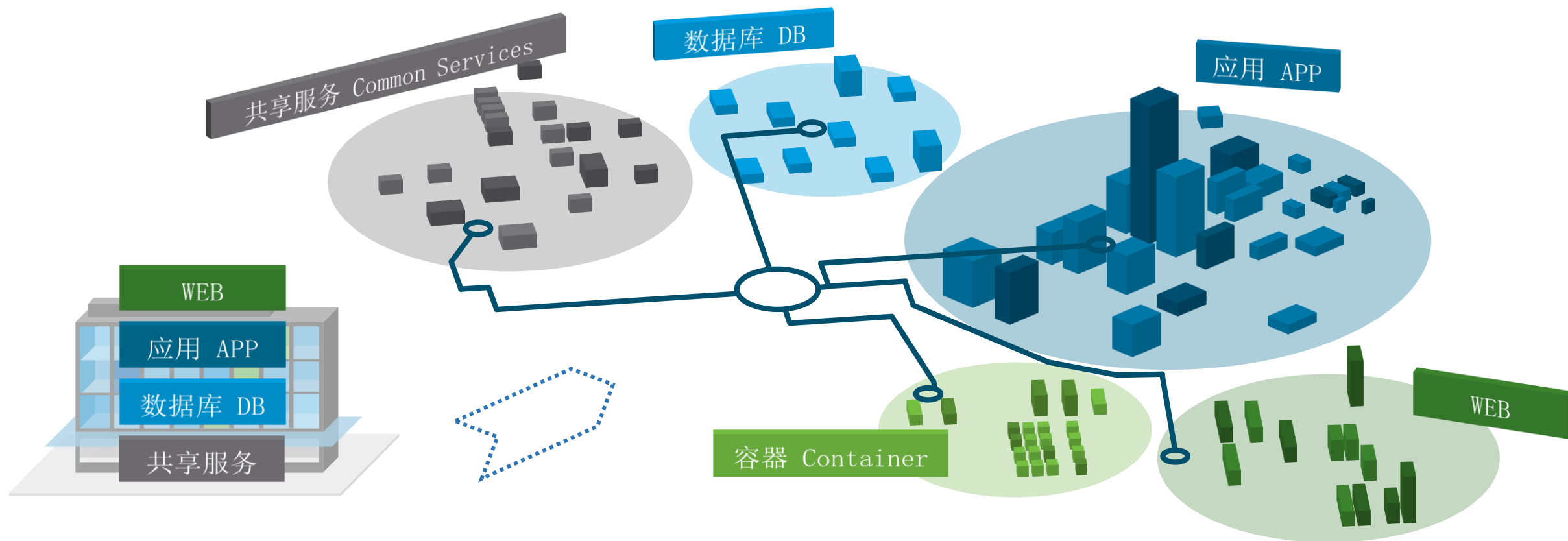
企业IT无处不在 SPREAD OF ENTERPRISE IT



企业IT无处不在 SPREAD OF ENTERPRISE IT



应用定义 APPLICATION DEFINED



分布式 (Distributed)

Remote Collaboration

新旧并存 (Coexist)

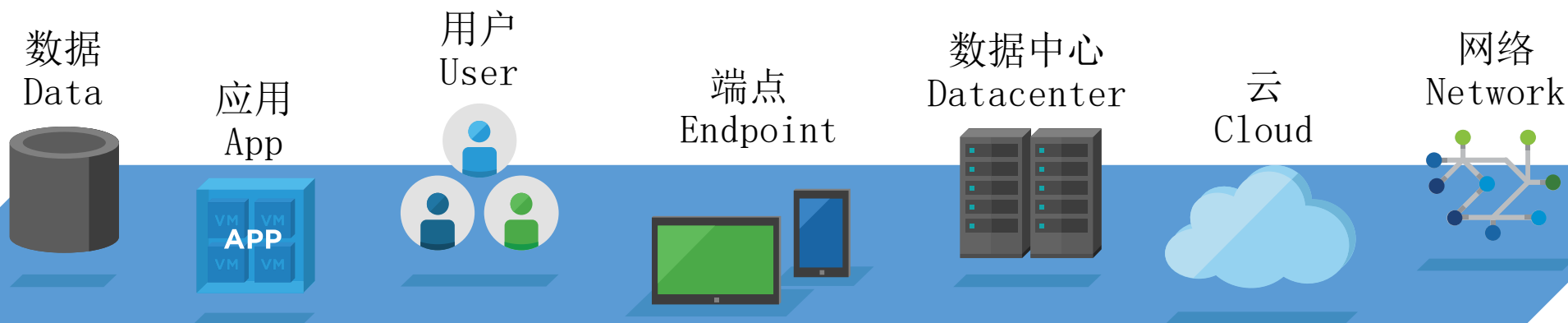
Trad. | Cloud Native

多平台 (Heterogeneous)

Hybrid | Multi-Cloud

敏捷创新 (Agile)

DevOps



无处不在的安全防护需求 Security at Everywhere

重构安全体系 (Rebuild)

软件定义 Software Defined
面向混合云 For Hybrid Cloud
分布式 Distributed Protection

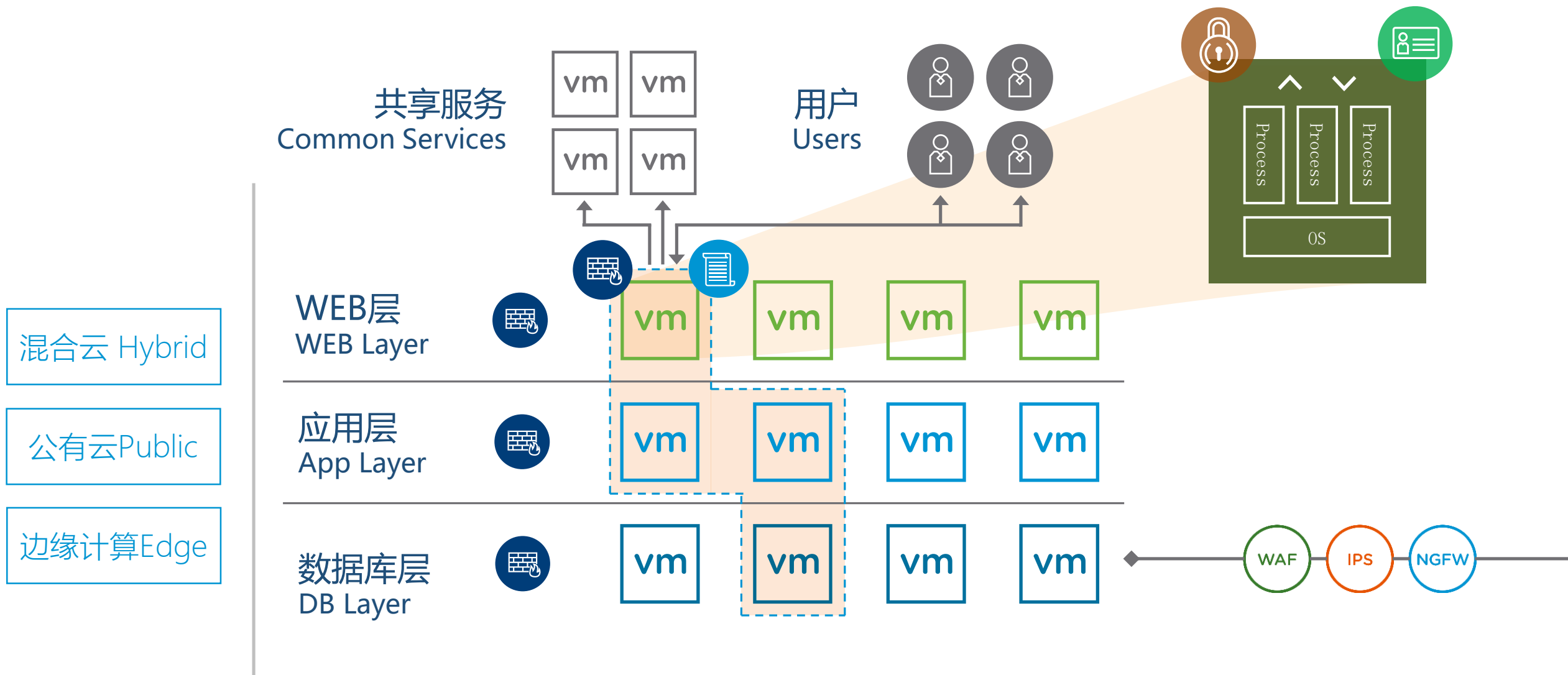
提升防护能力 (Enhance)

精细化管控 Granular Control
动态适配 Adaptive
连续合规 Continuous Compliance

管理自动化 (Automation)

安全协同 Collaboration
集成到云 Integration
服务化 As a Service

平台-零信任 ZERO TRUST MODEL



新应用-声明式 DECLARATIVE SECURITY

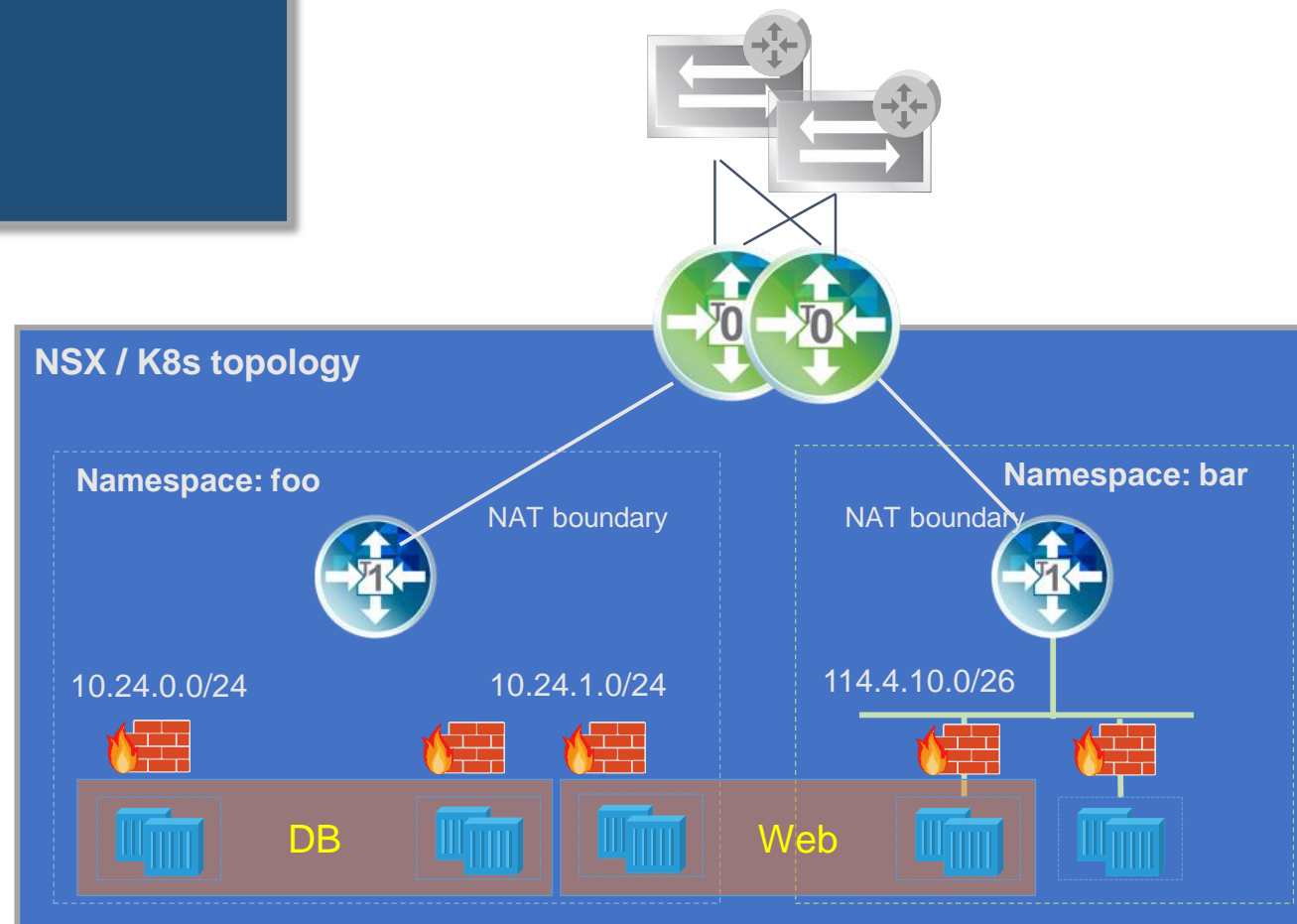
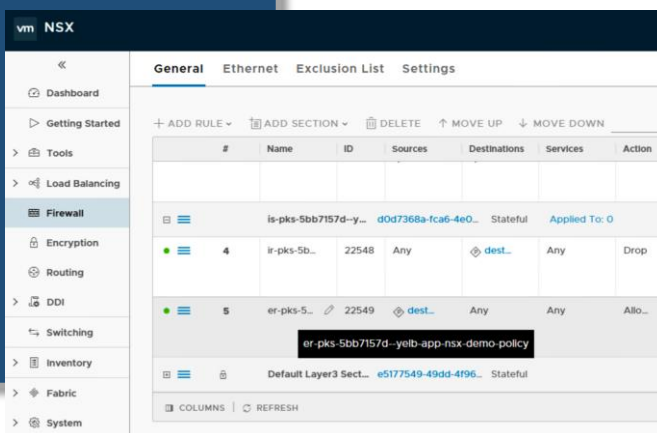
```
admin@k8s-master:~$ kubectl label pods nginx-foo-3492604561-nltrf secgroup=web -n foo
Pod "nginx-nsx-3492604561-nltrf" labeled

admin@k8s-master:~$ kubectl label pods nginx-bar-2789337611-z09x2 secgroup=db -n bar
pod "nginx-k8s-2789337611-z09x2" labeled

admin@k8s-master:~$ kubectl get pods --all-namespaces -Lsecgroup
NAMESPACE   NAME                                READY   STATUS    RESTARTS   AGE   SECGRP
k8s          nginx-foo-2789337611-z09x2         1/1     Running   0          58m   web
nsx          nginx-bar-3492604561-nltrf        1/1     Running   0          1h    db
```

定义Security Groups并配置入站/出站方向 安全策略
Security Group可以实现微分段以保护Pods间互访

```
admin@k8s-master:~$ cat nsx-pod-policy.yaml
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: nsx-demo-policy
spec:
  podSelector:
    matchLabels:
      app: db
  ingress:
    - from:
        - podSelector:
            matchLabels:
              app: nginx
      ports:
        - port: 80
          protocol: TCP
```



**APPS AND
IDENTITY**

DESKTOP | MOBILE

**MANAGEMENT
AND SECURITY**

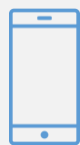
消费级便利性
Consumer Simple

企业级安全性
Enterprise Secure

我们的愿景 OUR VISION

构建必不可少，无处不在的数字基石
Deliver the Essential, Ubiquitous Digital Foundation

任何设备 Any Device



任何应用 Any App



Cloud Native



Containerized



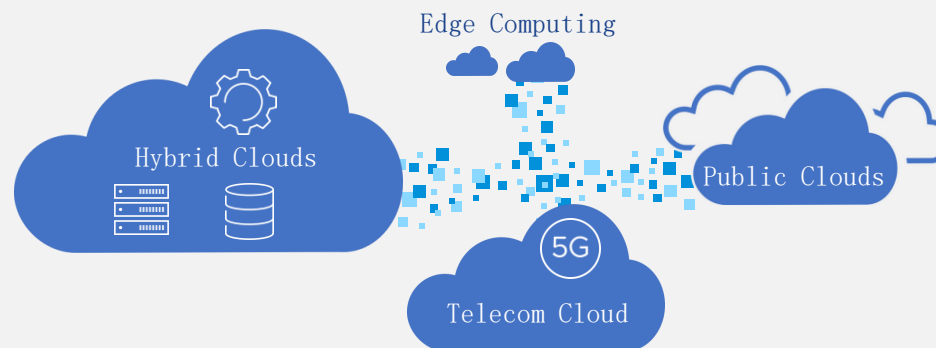
SaaS



Traditional



任意云 Any Cloud



识别

防护

检测

响应

修复

利用在虚拟化、移动性和混合云管理方面的核心能力实现无处不在的安全保护

奇安信

Hillstone
NETWORKS

Check Point
SOFTWARE TECHNOLOGIES LTD.

ca HYTRUST
Cloud Under Control

Symantec

Bitdefender

面向
混合云

精细化
集成服务

最小颗粒度隔离
微分段

可见 | 可防 | 可控

无处不在

最小权限计算
应用防御

面向
应用

灵活
动态适配

AsialInfo | 亚信安全


天融信
TOPSEC

paloalto
NETWORKS

eSet Kaspersky
Internet Security

McAfee RAPID7

FORTINET



THANKS