UCLOUD优刻得 | intel

换个角度看云“原生”安全

-UCloud 宗泽-

UCLOUD优刻得 | intel

个人简介

一个搞了20年信息/网络安全的男人

各方面都略懂一点

腾讯 10年，UCloud 6年

UCLOUD优刻得 | intel

1. 地下黑客世界

2. 云原生安全?

3. 业务需要的原生安全

4. UCloud云原生安全实践

鷹眼

(2008)

Eagle Eye

UCLOUD优刻得 | intel

370万+

每年修复超过
370万漏洞

7万+

累计监测发现
7万+木马

2万+

全年防御超过
2万+次DDoS攻击

68亿次

每年防御超过
68亿次WEB攻击

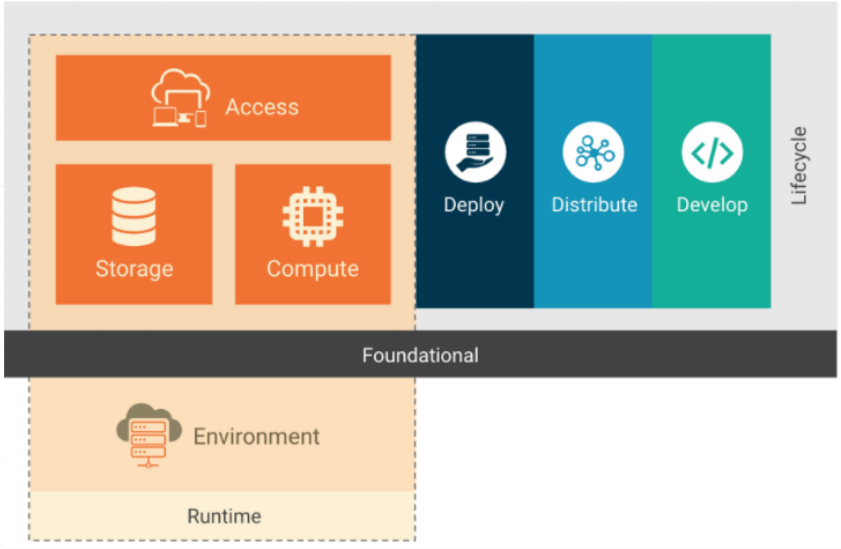
16亿条

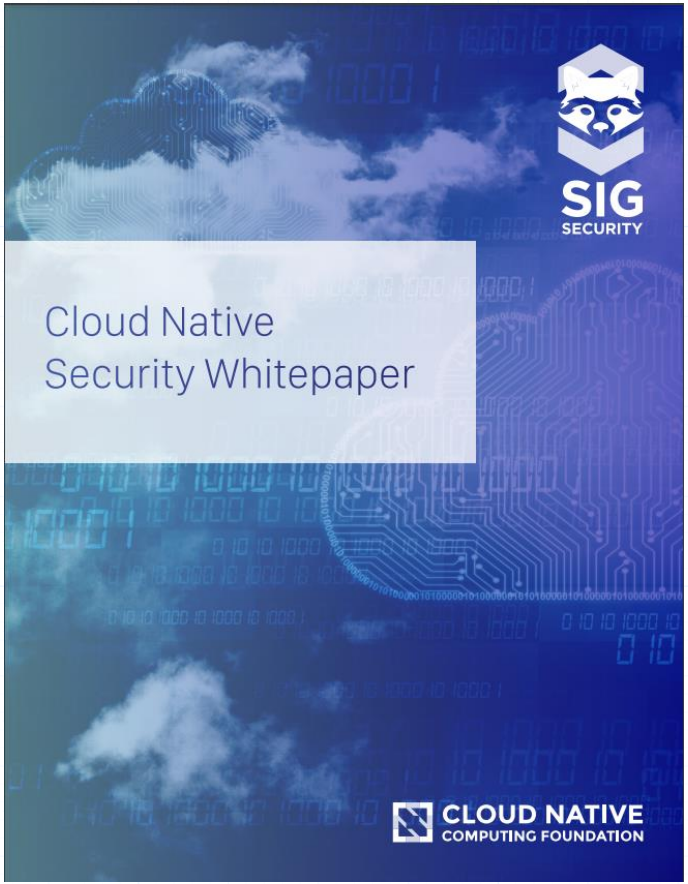
审计操作命令
16亿条

10万+

为超过10万家企业
提供安全服务

大家都在说的云原生安全，到底是什么？



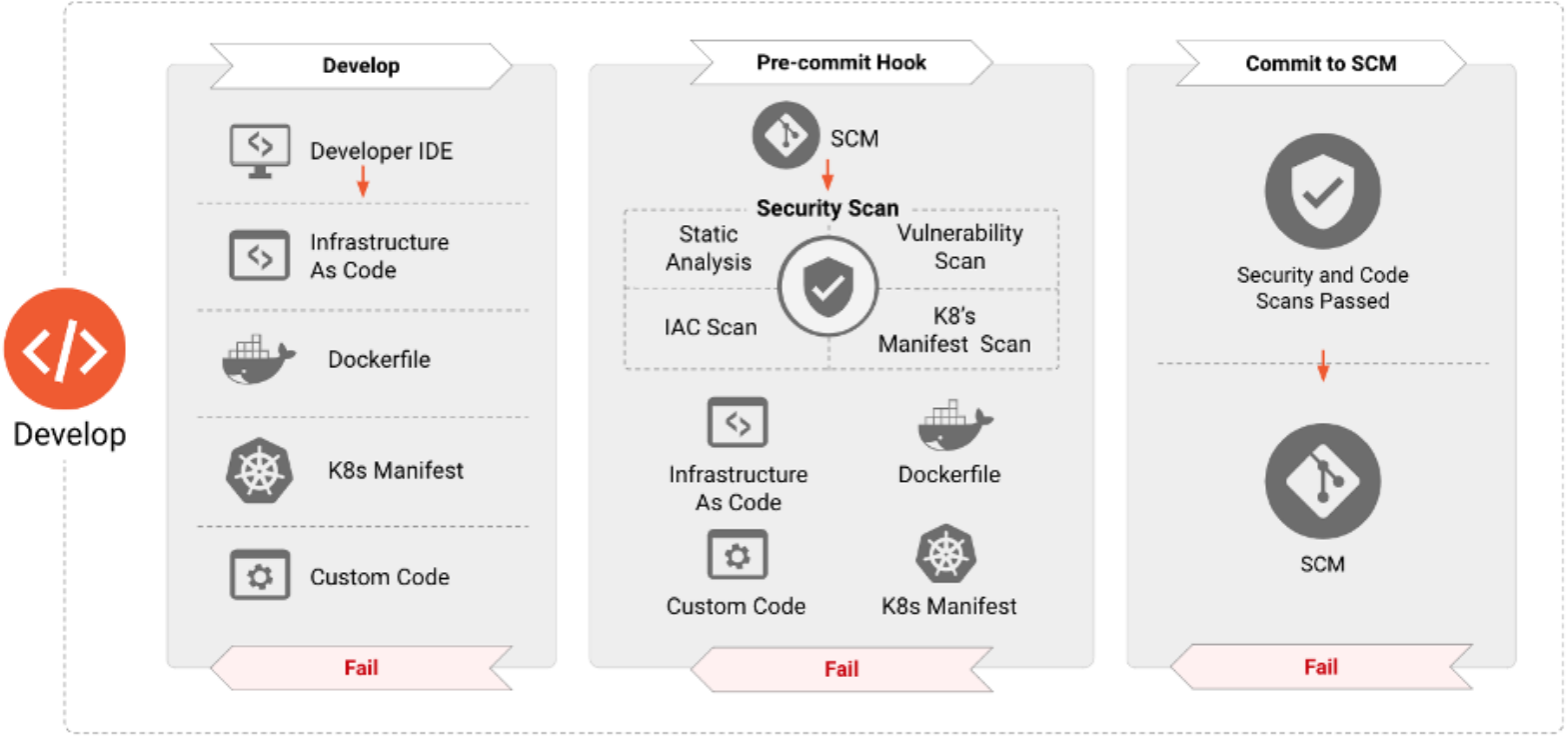


CNCF关于云原生安全的定义

开发-分发-部署-运行时

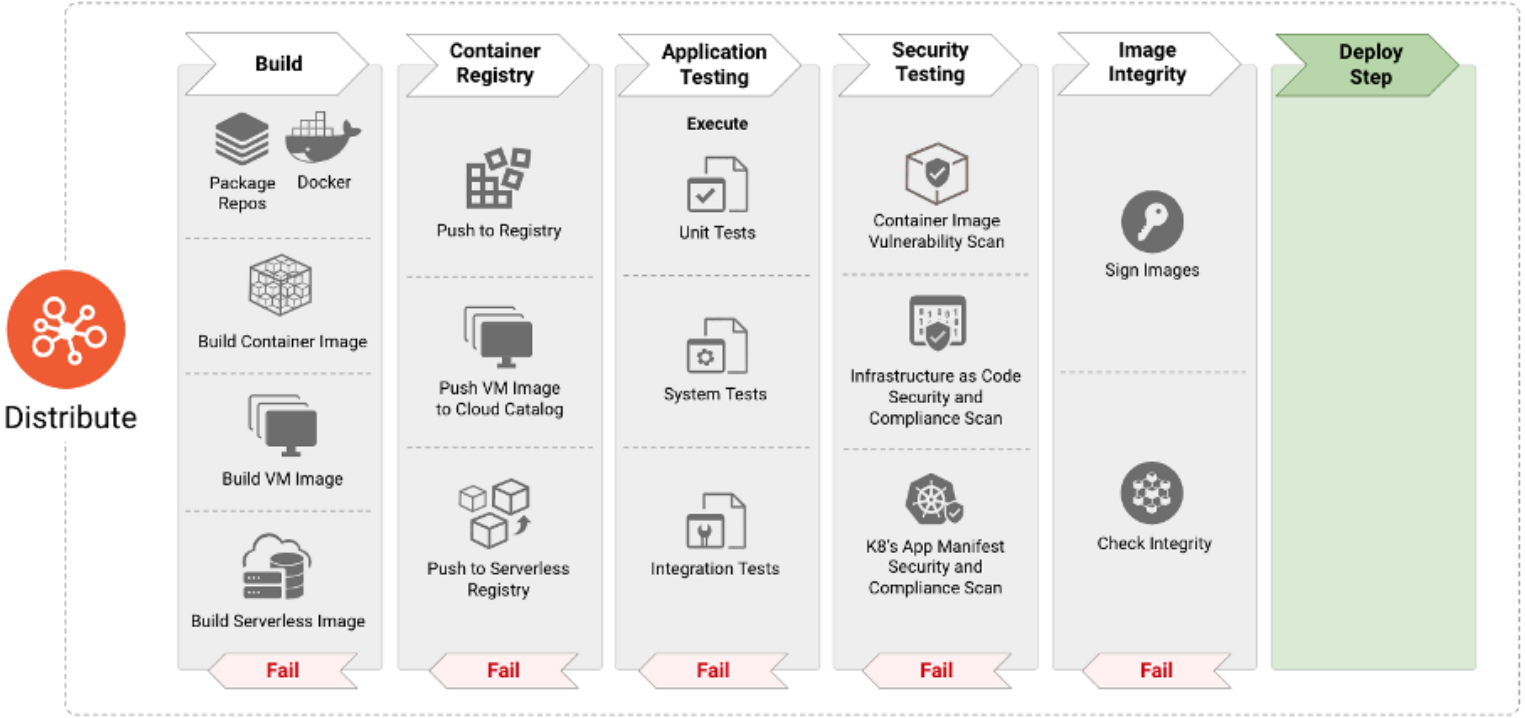
UCLOUD优刻得 | intel

云原生生命周期-开发安全

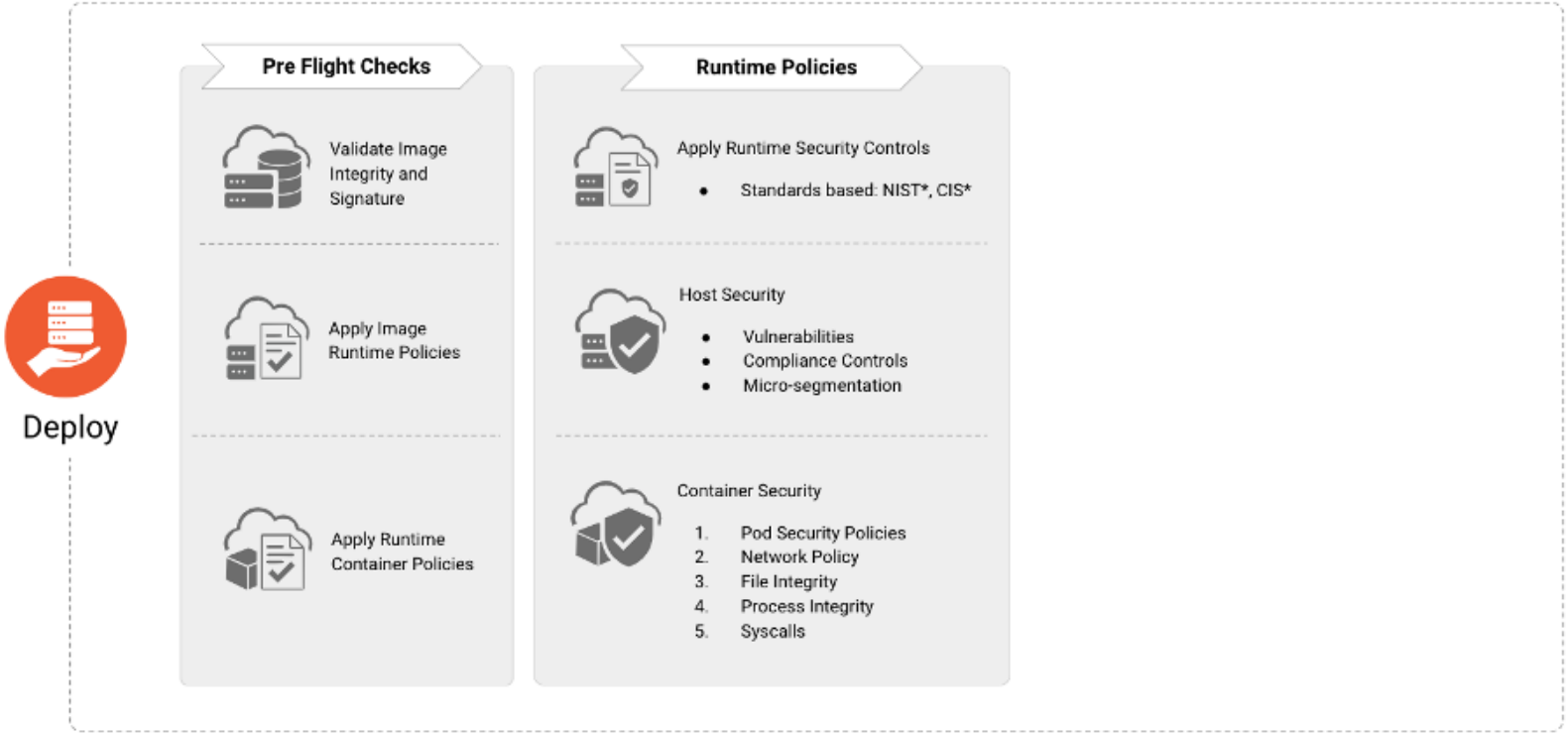


UCLOUD优刻得 | intel

云原生生命周期-分发安全

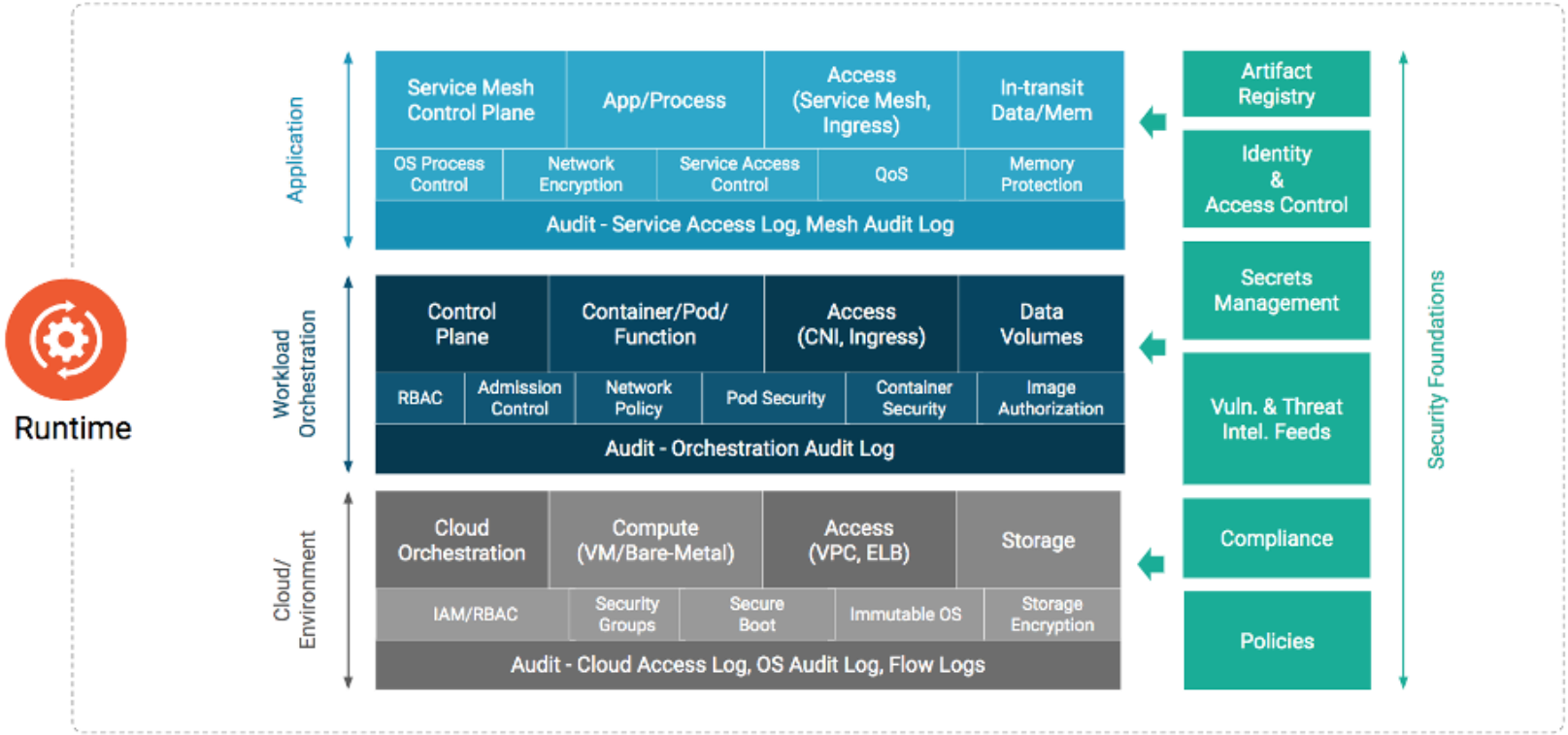


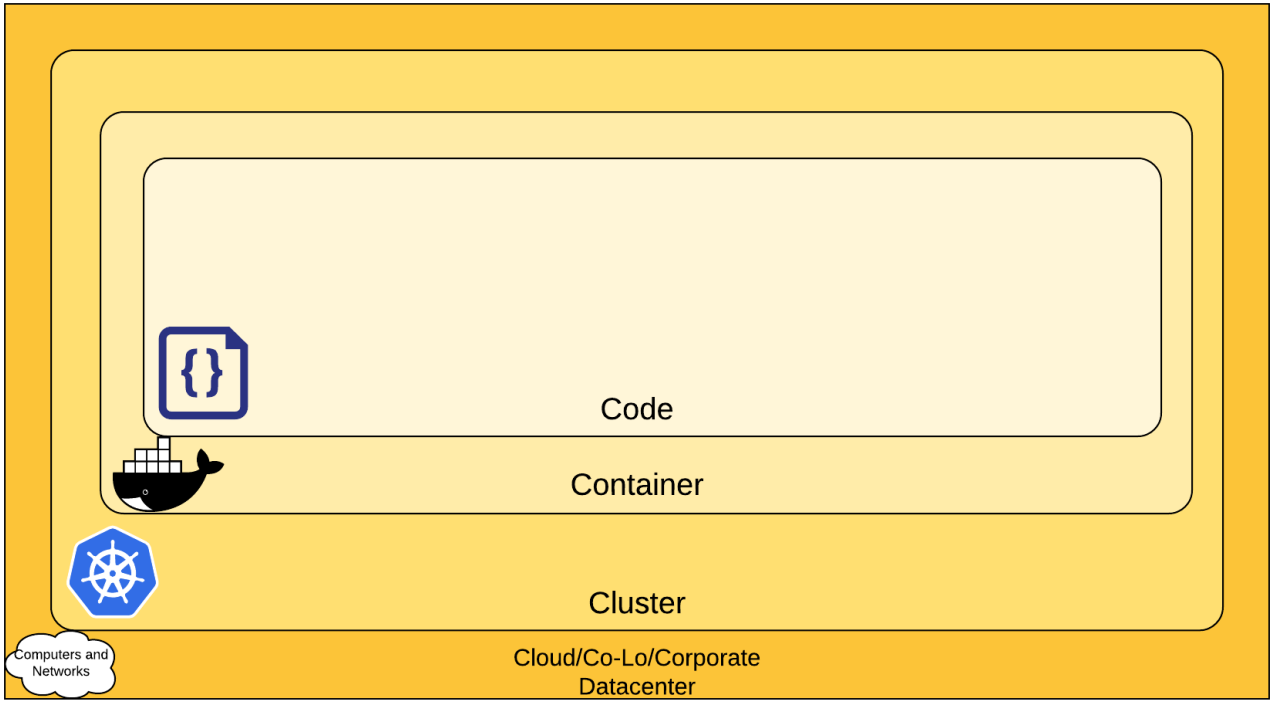
云原生生命周期-部署安全



UCLOUD优刻得 | intel

云原生生命周期-运行时安全

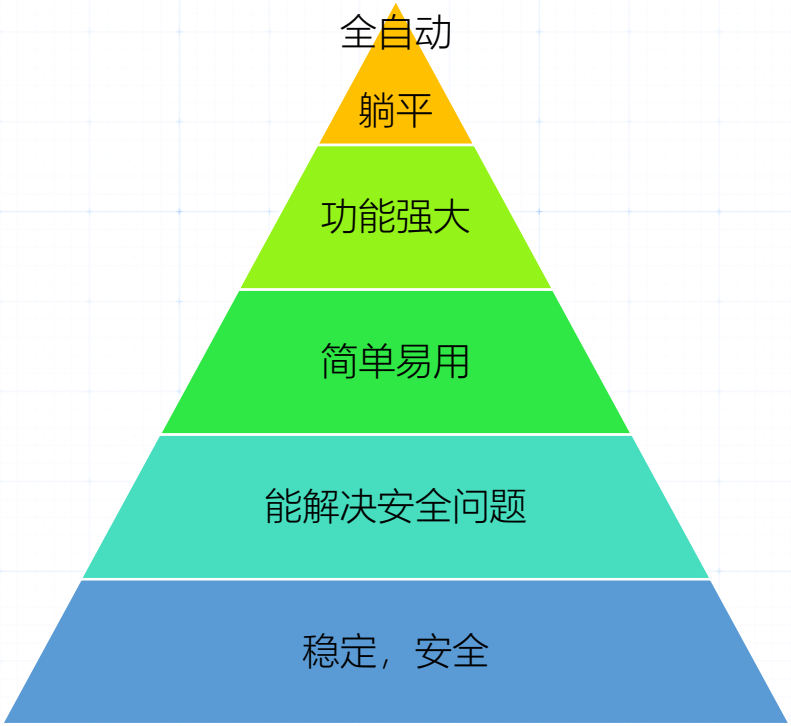




Kubernetes关于云原生安全的 4 个 C

业务需要什么样的云（原生）安全？

马斯洛《动机与人格》的需求层次



UCLOUD优刻得 | intel

云“原生”安全的特点

云自带安全能力

云平台与生俱来的安全特性

云基础架构融合

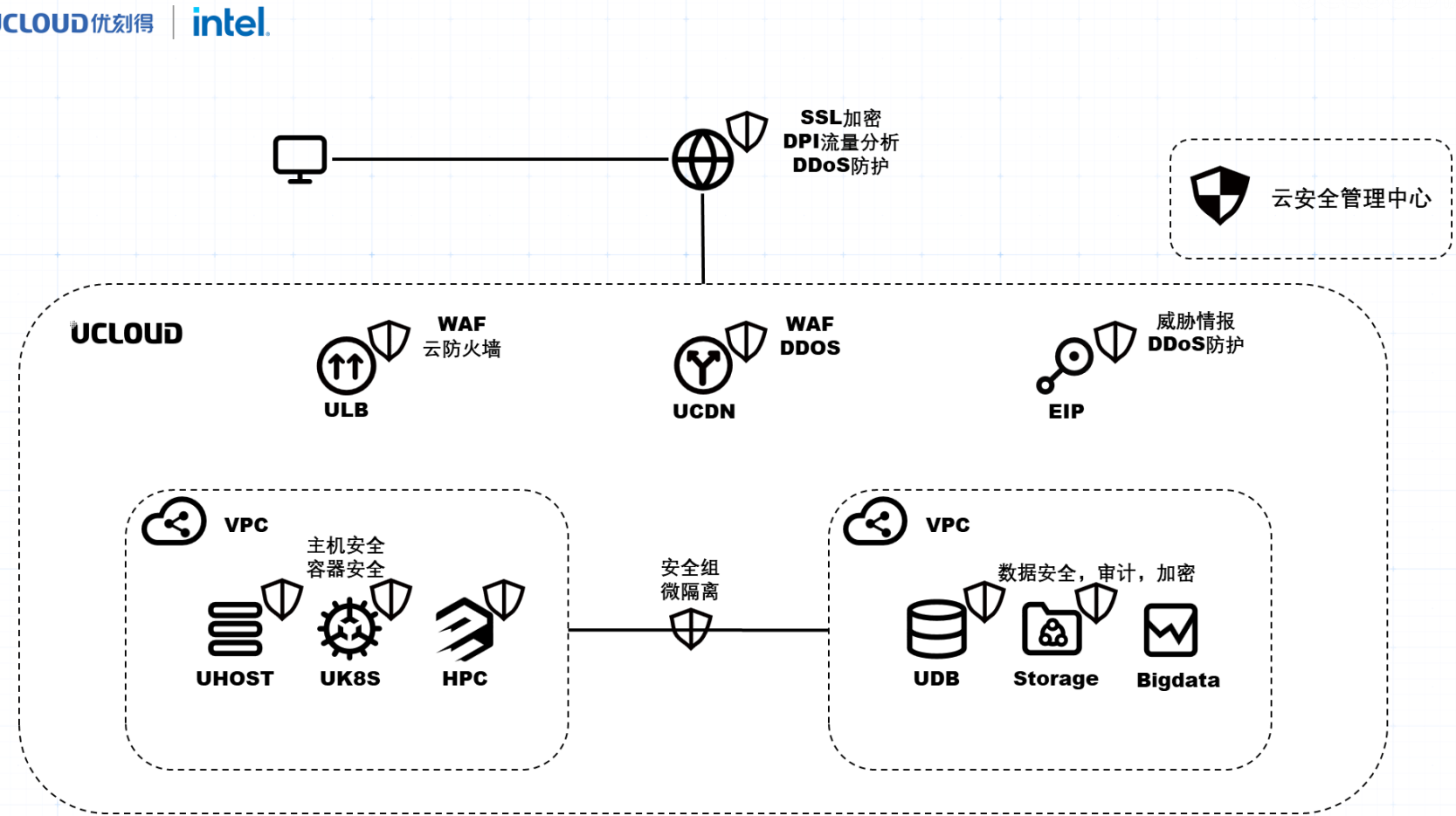
安全能力与云基础设施融合，无需额外的部署和业务调整

自动化

安全风险和事件的自动化发现处置

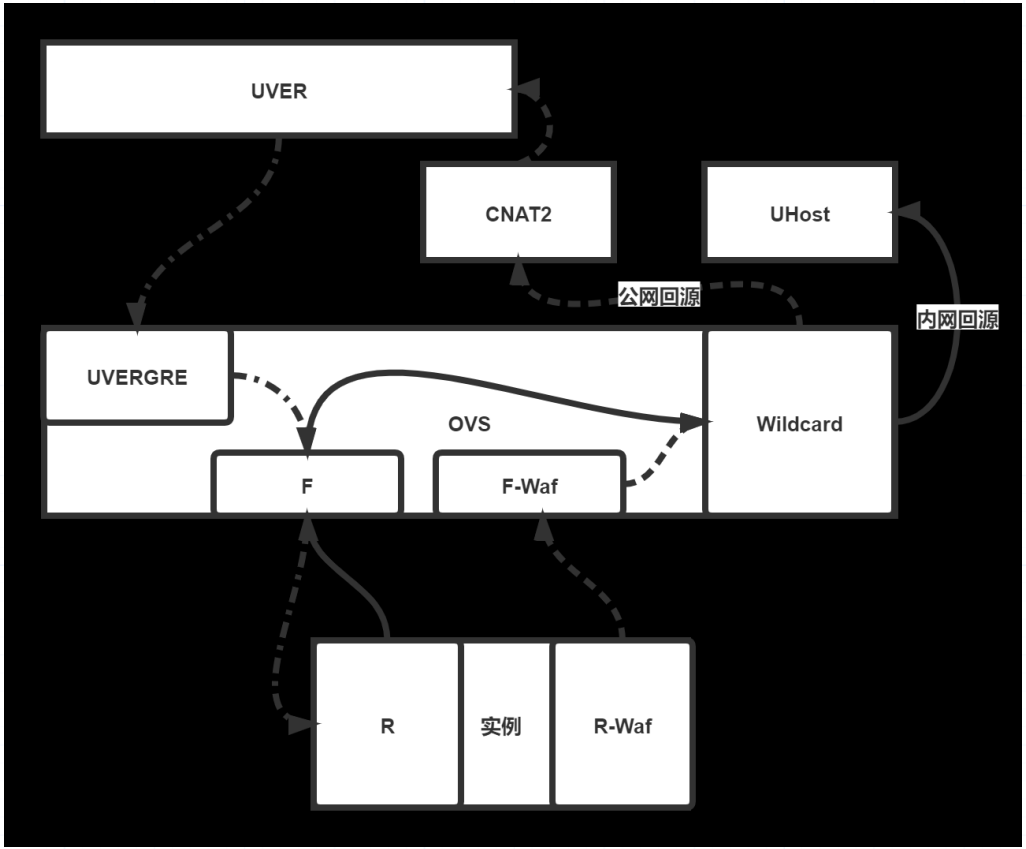
智能化

数据驱动的智能化安全


SSL加密
DPI流量分析
DDoS防护
云安全管理中心
UCLOUD
WAF
云防火墙
ULB
WAF
DDOS
UCDN
威胁情报
DDoS防护
EIP
VPC
主机安全
容器安全
UHOST
UK8S
HPC
安全组
微隔离
VPC
数据安全，审计，加密
UDB
Storage
Bigdata

WAF与负载均衡融合

将web应用防火墙功能内置于云负载均衡产品中



云WAF

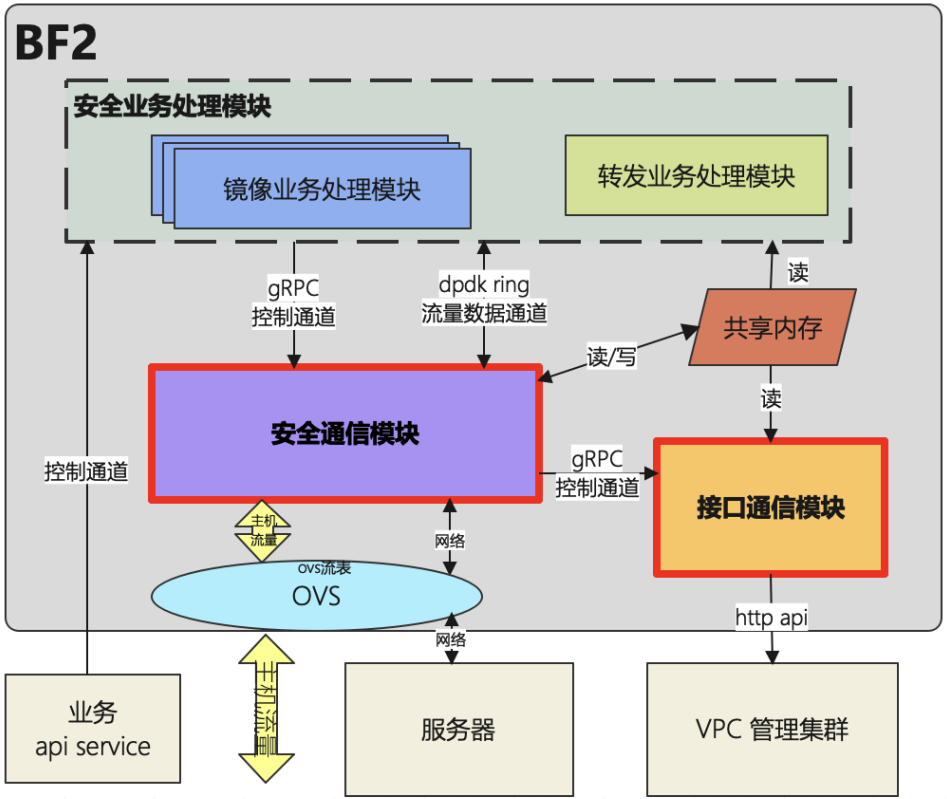
- 购买
- 配置转发规则
- 修改DNS域名解析
- 使用

云原生WAF

- 点击按钮，购买
- 使用

安全能力与云主机融合

- 设备自动发现，网内资产测绘
- 硬件级安全准入，非法设备无法接入网络
- 南北向防火墙，访问控制
- 小流量ddos防护
- 主机web应用防火墙
- 服务器级流量可视化，流量内容审计
- 东西向流量微隔离，进程级访问控制，防木马扩散
- 零信任安全，客户端身份管理，只允许特定客户端与服务器进行通讯
- 服务器间数据通讯自动加密



UCLOUD优刻得 | intel

特点

- Agentless，不占用云主机资源
- 云主机安全功能一键按需开启
- 独立系统，与主机环境隔离

UCLOUD优刻得 | intel

总结

云原生+安全?　　OR　　云+原生安全?

利用云的特点与优势，为用户提供稳定，方便，高效的云安全服务，才是用户需要的云”原生”安全

UCLOUD优刻得 | intel

THANKS!