DaoCloud 助力企业

释放
数字野心

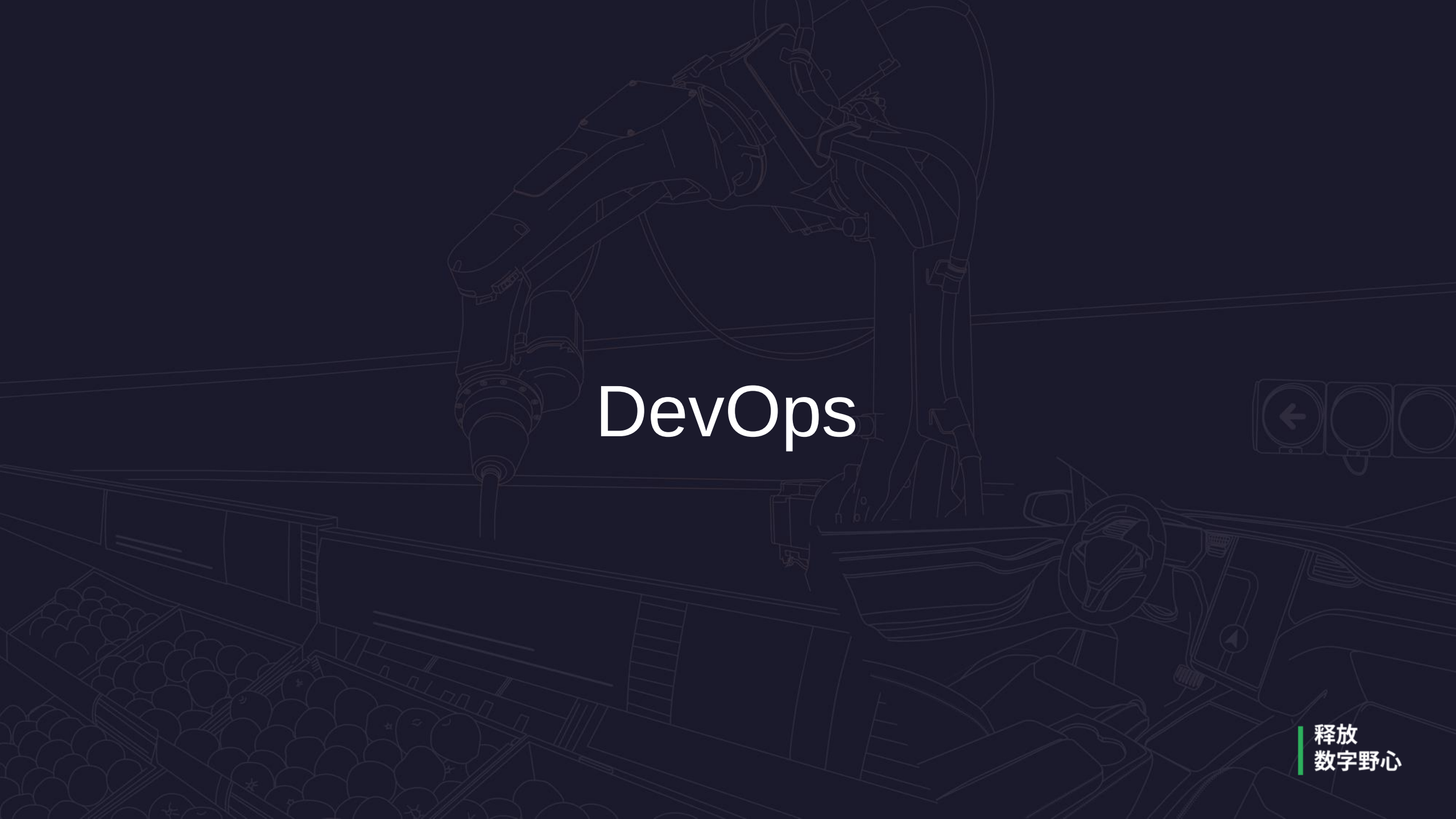
www.daocloud.io

持续交付演化之路：从 DevOps 到 DevSecOps

2019年　王天青 | DaoCloud

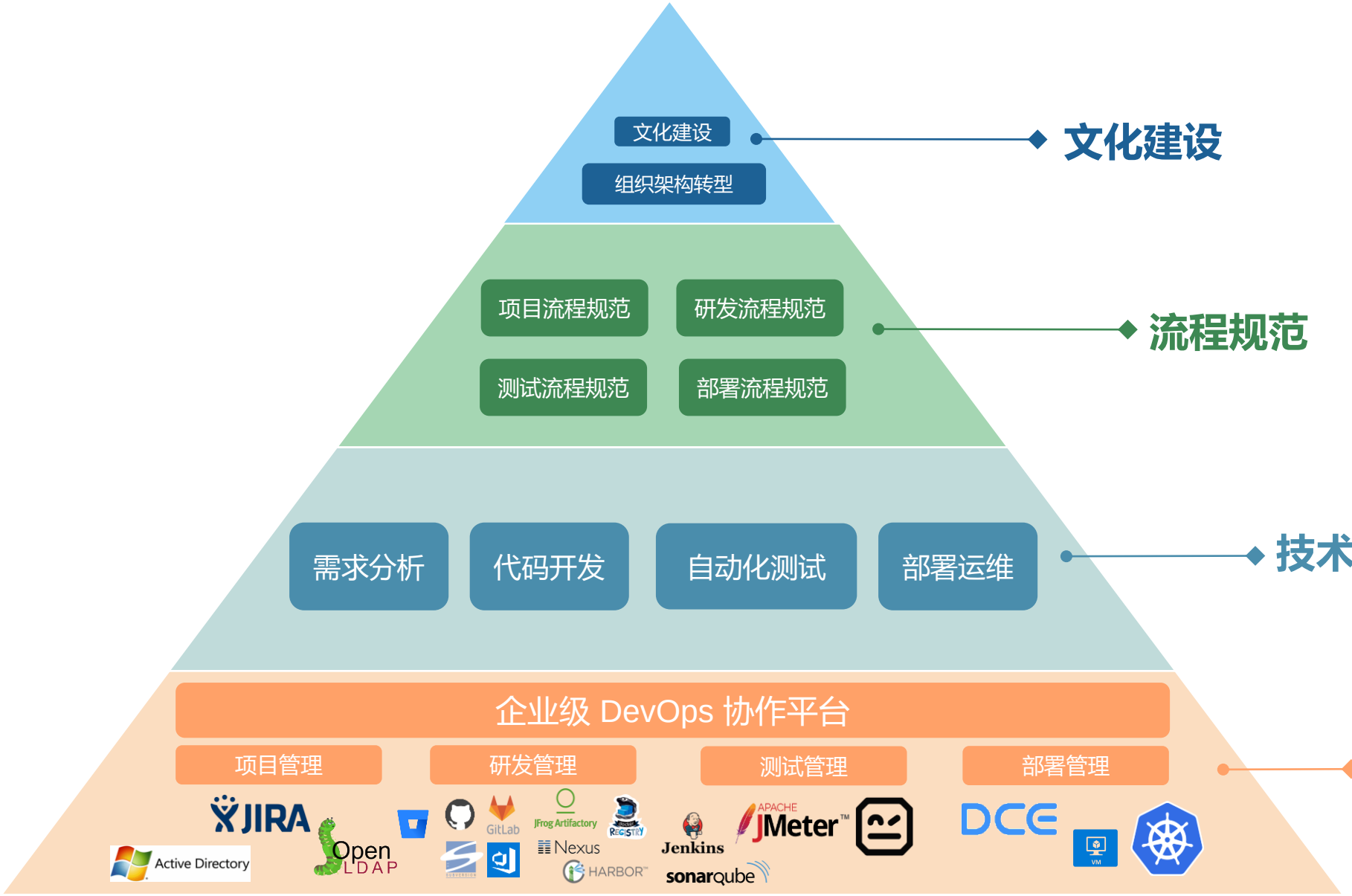
About Me

- 南京大学计算机科学与技术系硕士。
- 资深Java程序员，2003年开始从事J2EE开发，从软件开发做到架构设计。
- 08年加入EMC中国研究院，最高担任云平台主任研究员，长期从事云计算创新技术解决方案设计和实现。
- 2015年9月加入麻袋理财，任首席架构师
- 2016年12月加入 DaoCloud，任首席架构师，负责微服务和DevOps相关产品研发与咨询工作
- 2017 年 NJSD 讲师 - 基于容器的应用微服务架构转型实践
- 在工作期间，分别在中国和美国提交了20+专利申请，截止到2018年5月，其中有10个专利被美国专利局授权，12个专利被中国专利局授权。

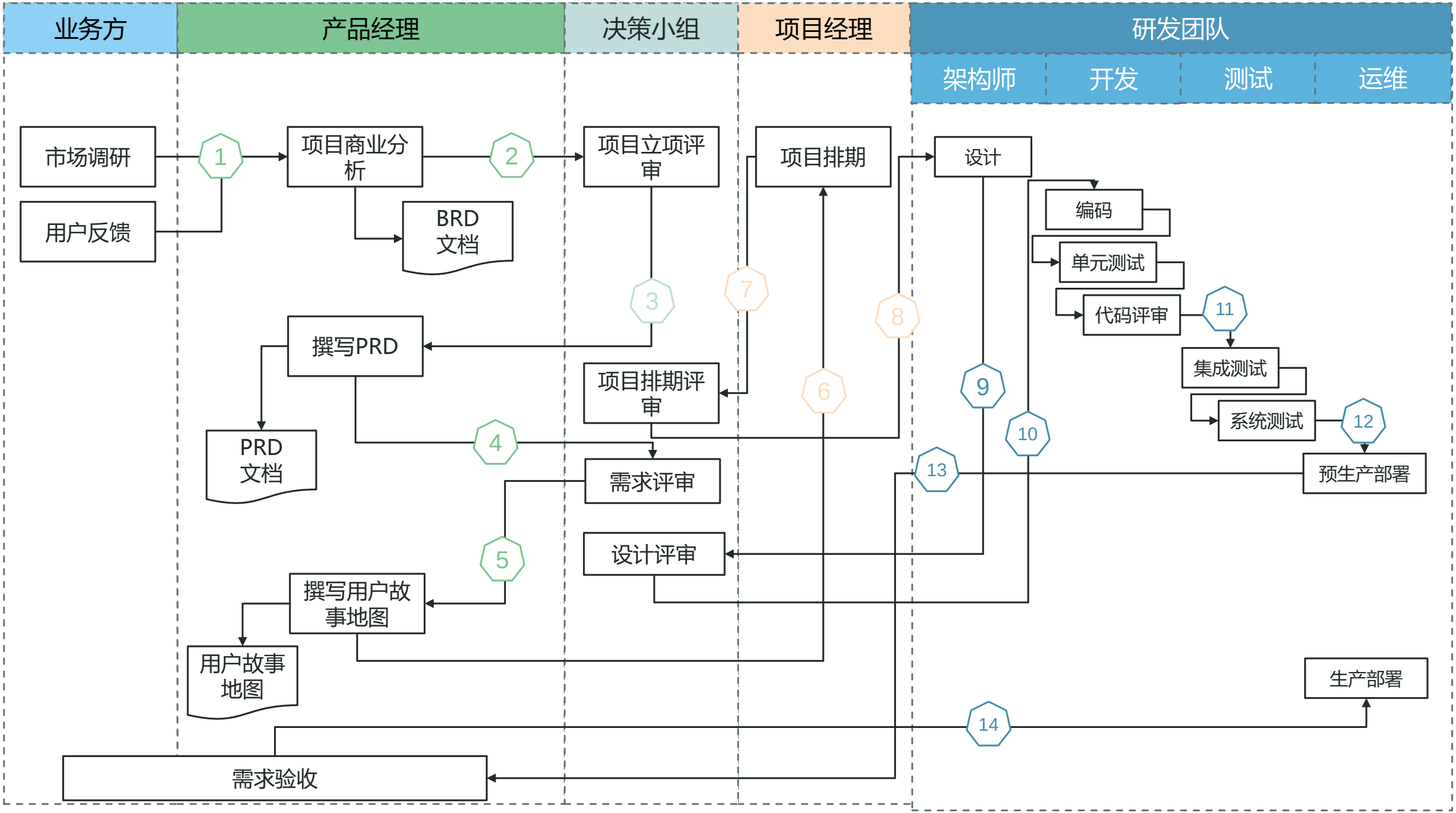


DevOps

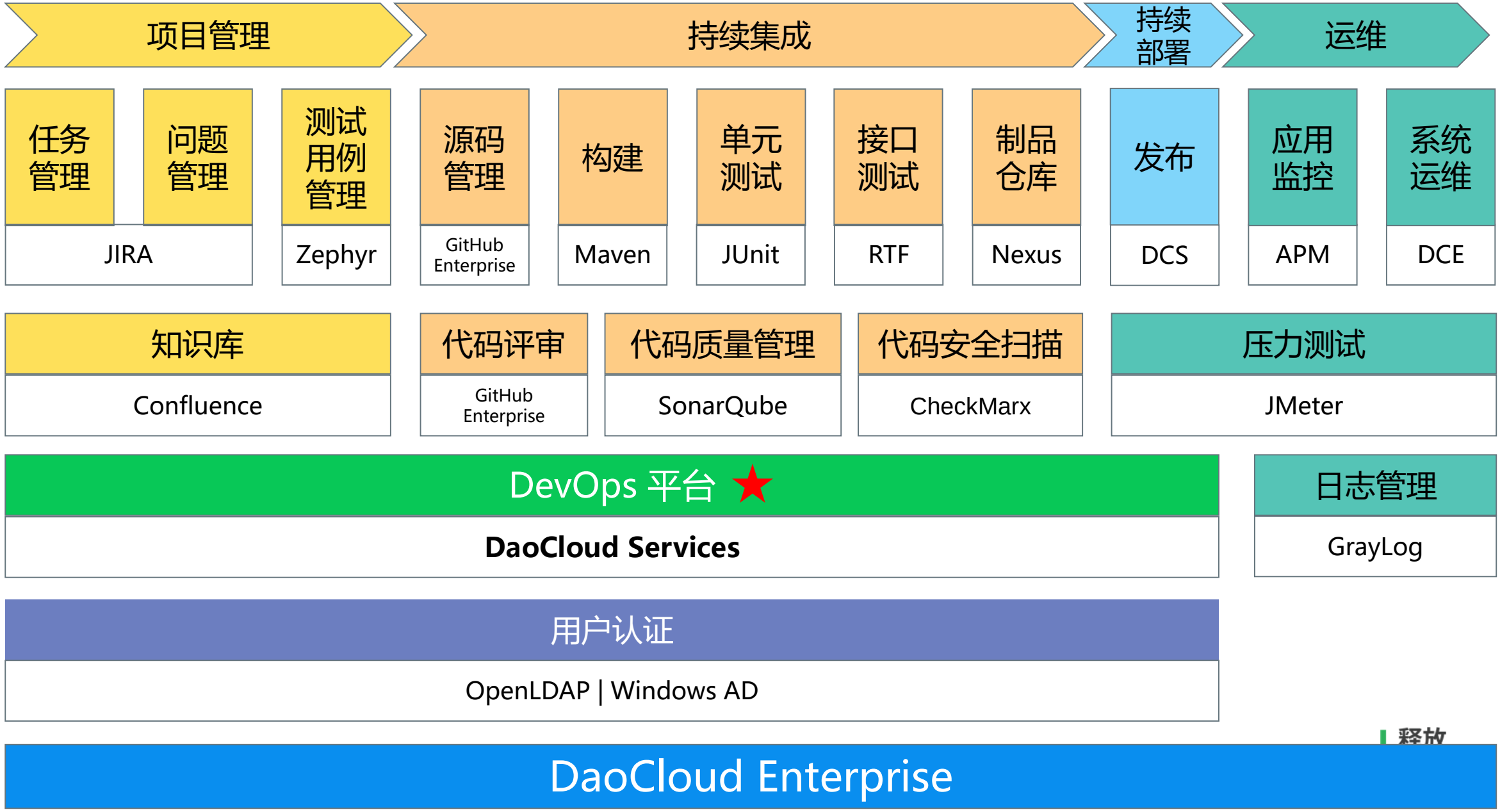
DevOps 的本质



释放
数字野心


业务方
产品经理
决策小组
项目经理
研发团队
架构师
开发
测试
运维
市场调研
用户反馈
1
项目商业分析
2
BRD 文档
项目立项评审
项目排期
设计
编码
单元测试
代码评审
11
集成测试
系统测试
12
预生产部署
3
撰写PRD
PRD 文档
4
项目排期评审
7
8
6
9
10
13
需求评审
5
设计评审
撰写用户故事地图
用户故事地图
生产部署
14
需求验收

DevOps 典型工具链

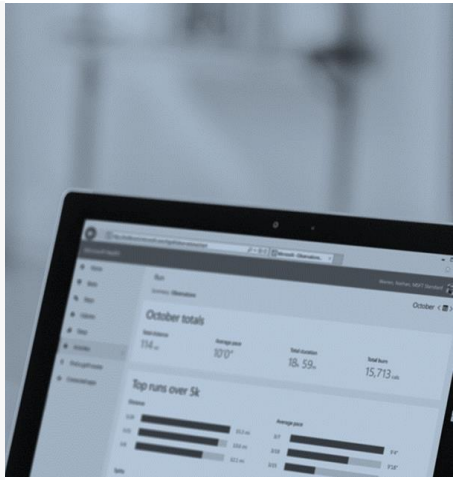


企业面临的安全挑战

万物互联时代，企业面临日益严峻的网络安全风险

8.29亿
中国网民规模

8.17亿
中国手机网民规模



4.9万 控制端
526万 中国境内被控制主机数
655万 受感染主机
3710个 大规模僵尸网络

木马和僵尸网络

5946万
受恶意攻击国内IP总数

4000次 每月10G bit/s以上的攻击数量
60% 由僵尸网络发起
2108个 命令控制端

拒绝服务攻击

数据泄露事件频繁发生，导致隐私问题，网络欺诈和诈骗

数据泄露

283万
移动互联网恶意程序
11.7%
较去年增长
1.24亿次
恶意程序传播

移动互联网恶意程序

14201 安全漏洞
4898 高危漏洞
5,381 零日漏洞
39.6% 较去年增长

安全漏洞

5.3万 仿冒页面
7049个 网站被篡改
216个 政府网站被篡改
1.7万 网站植入后门

网页仿冒/篡改

《2018 年我国互联网网络安全态势综述》国家互联网应急中心 2019年2月发布

特斯拉云服务器遭黑客劫持，变为加密货币矿机，机密数据遭泄漏

第一财经

特斯拉遭黑客入侵云系统“挖矿”，官方称漏洞已解决

第一财经APP • 2018-02-22 14:36

钱童心

虚拟货币热度不减，黑客也开始瞄准这一市场，窃取硬件的计算能力用来挖矿。

软件安全公司RedLock的研究人员近日发现，黑客攻击了特斯拉在亚马逊云系统AWS上的账户，并用它来运行挖矿软件。这一最新的网络攻击案还暴露了特斯拉的某些非公开数据，其中包括与特斯拉汽车相关的敏感遥测信息。但特斯拉方面称，根据初步调查，目前并没有发现对用户数据或者汽车安全性产生影响。

此前，黑客还利用类似的方法攻击过咖啡零售巨头星巴克、谷歌旗下的视频网站YouTube、英国政府信息部门、英国保险公司Aviva和荷兰SIM卡制造巨头金雅拓等。而此次特斯拉受到的黑客攻击进一步暴露了这种新型网络袭击手法的狡猾。

THE VERGE

TECH | SCIENCE | ENTERTAINMENT | MORE

TRANSPORTATION | CARS | TESLA

4

Tesla’s cloud was used by hackers to mine cryptocurrency

Mining bitcoin on Elon’s dime

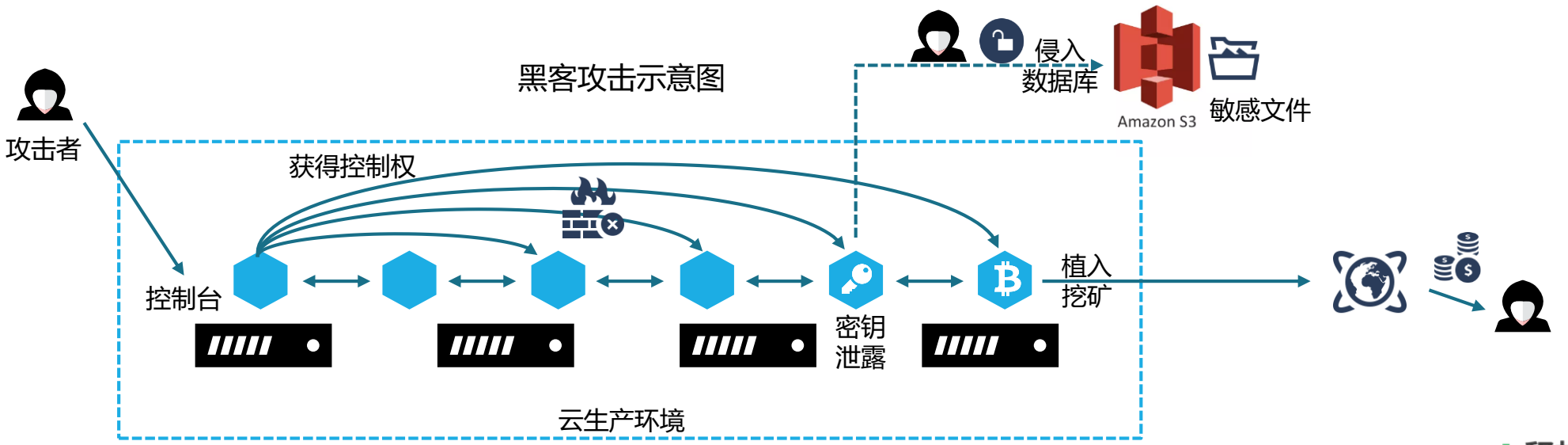
By Andrew J. Hawkins | @andyjayhawk | Feb 20, 2018, 1:39pm EST

SHARE

Photo by James Bareham / The Verge

Tesla’s cloud account was hacked and used to mine cryptocurrency, according to a security research firm. Hackers gained

黑客入侵攻击路径

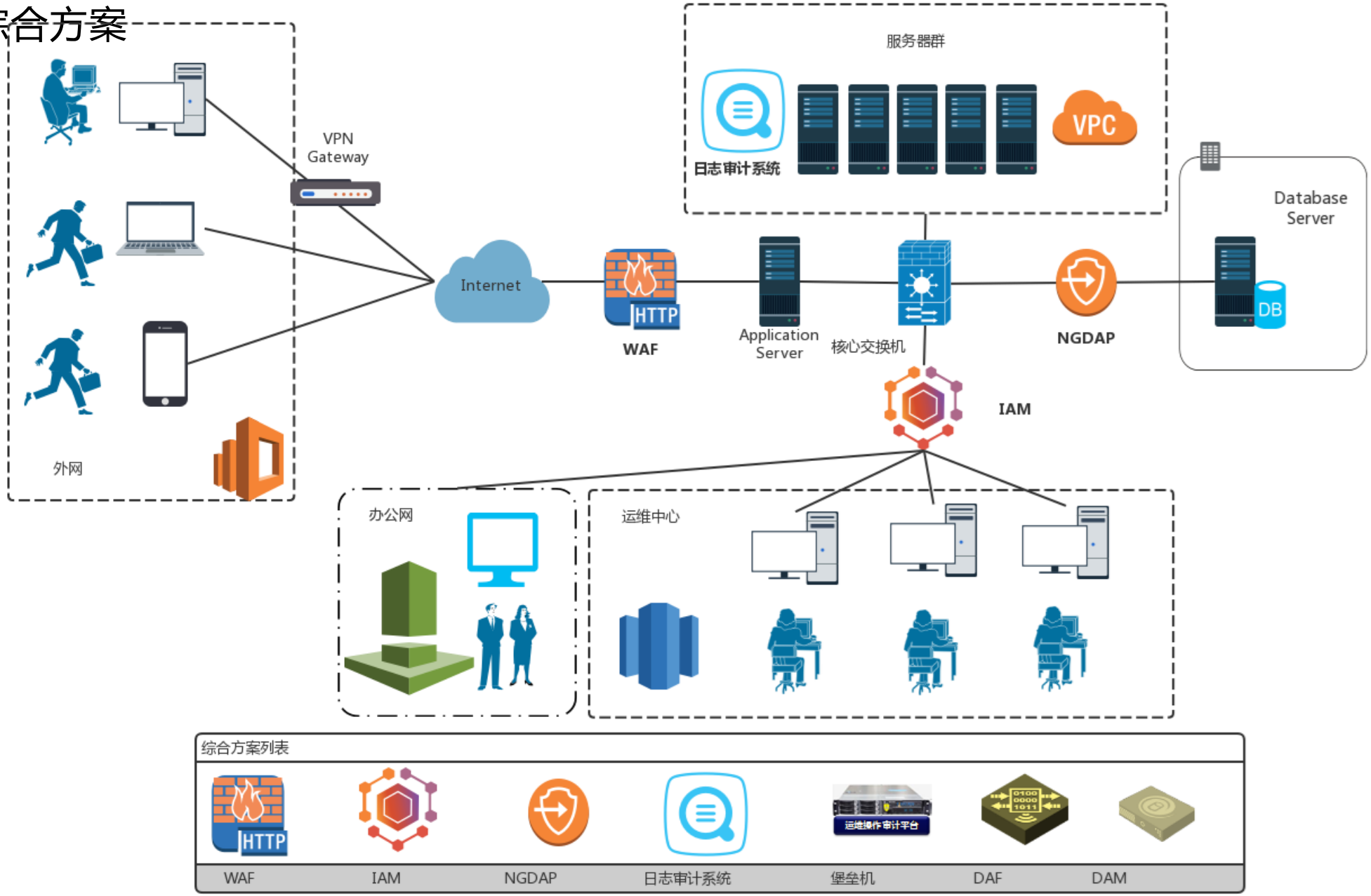


释放
数字野心

传统安全解决方案

释放
数字野心

安全综合方案



释放
数字野心

云原生安全

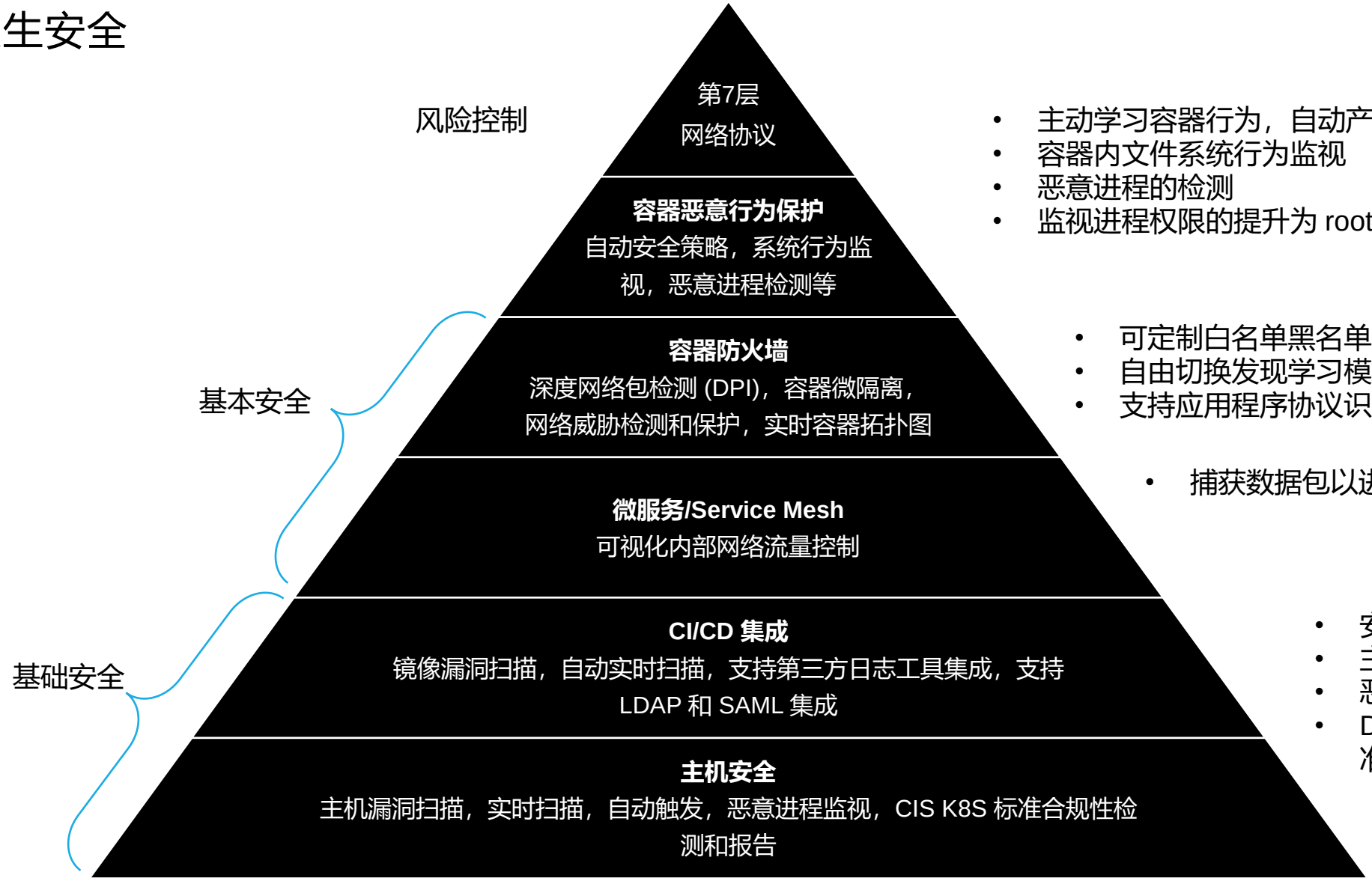
释放
数字野心

云原生应用

	部署 可以预测性	抽象性	弹性能力	开发运维模式	服务架构	恢复能力
云原生应用	可预测	操作系统抽象	弹性调度	**DevOps**	微服务解耦 架构	自动化运维 快速恢复
传统应用	不可预测	依赖操作系统	资源冗余缺乏 扩展能力	瀑布式开发 部门孤立	单体耦合架构	手动运维 恢复缓慢

云原生技术实践白皮书*

云原生安全

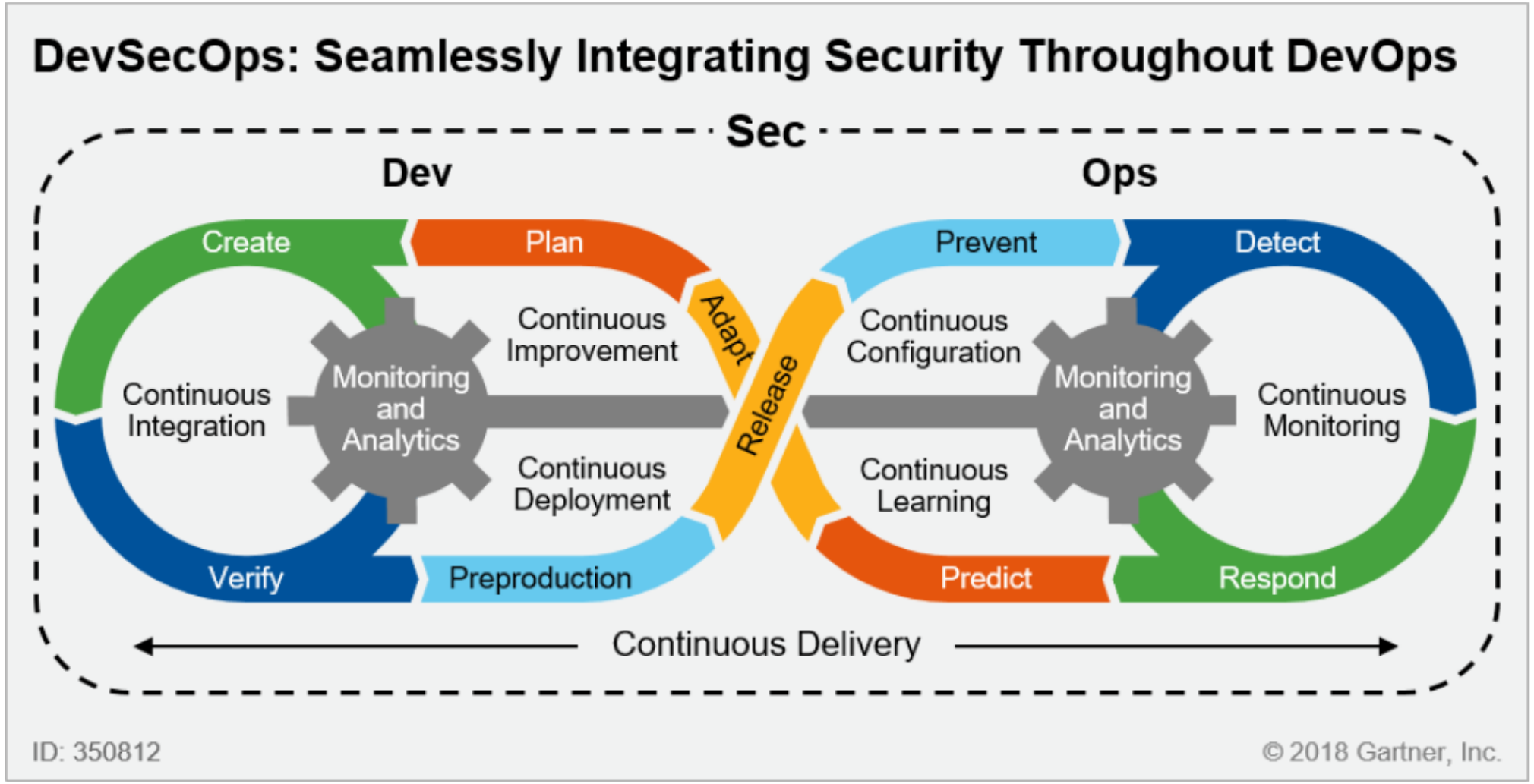


- 主动学习容器行为，自动产生白名单安全策略
- 容器内文件系统行为监视
- 恶意进程的检测
- 监视进程权限的提升为 root 的行为

- 可定制白名单黑名单安全策略
- 自由切换发现学习模式、监视模式与保护模式
- 支持应用程序协议识别和保护

- 捕获数据包以进行调试和威胁调查

- 安全合规审计
- 主机漏洞扫描
- 恶意进程监视
- Docker/Kubernetes 标准合规性检测和报告



Source: Gartner (May 2018)

云原生应用的安全

CI/CD

Registry

Container Platform

Gartner 容器安全评估建议

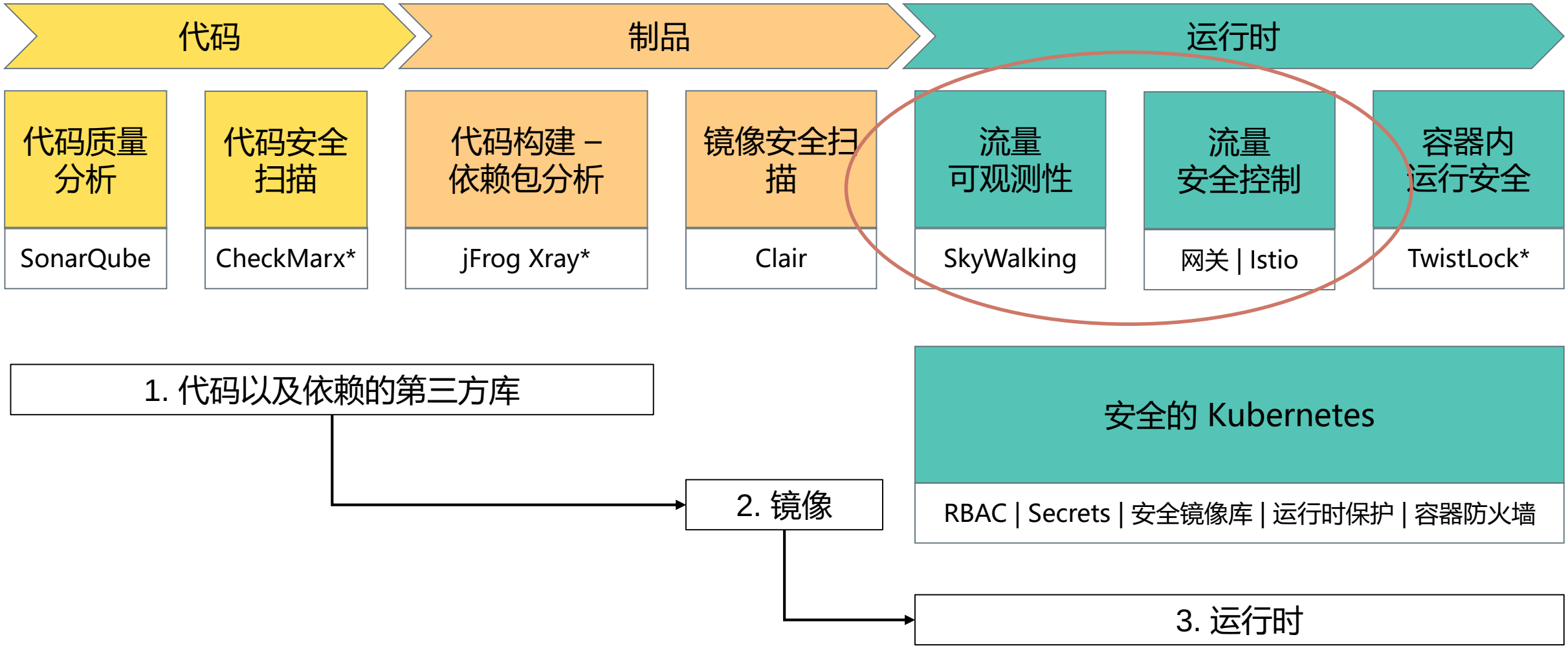
Gartner

- “Secure containers holistically through integrating controls at key steps in the CI/CD pipeline. ”
- 需要通过在 CI/CD 持续集成/持续交付的整个关键环节中全面保护容器安全。

- “Add Layer 7 network segmentation for operational containers that require defense in depth.”
- 为需要深度保护的运行容器添加第 7 层网络保护。

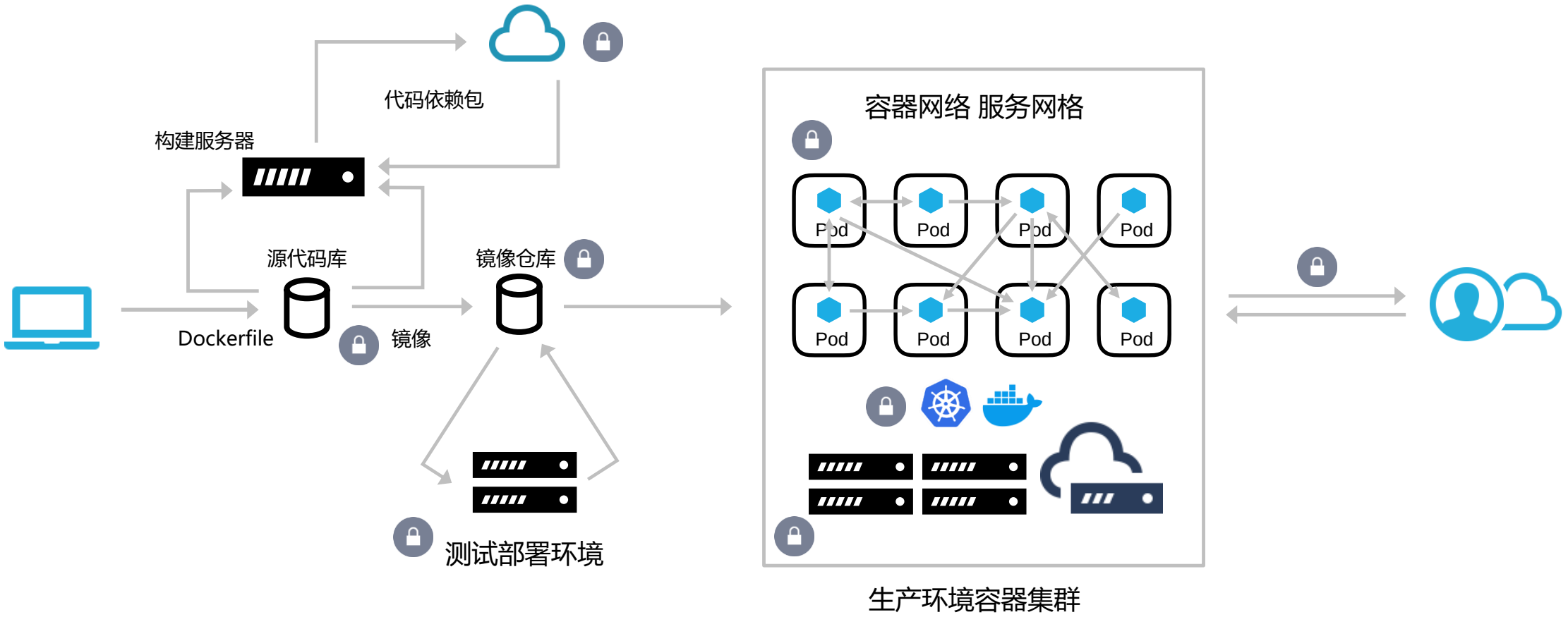
Gartner 《Container Security — From Image Analysis to Network Segmentation, Options Are Maturing》
https://www.gartner.com/document/3888664

DevSecOps 典型工具链



DevSecOps 流程

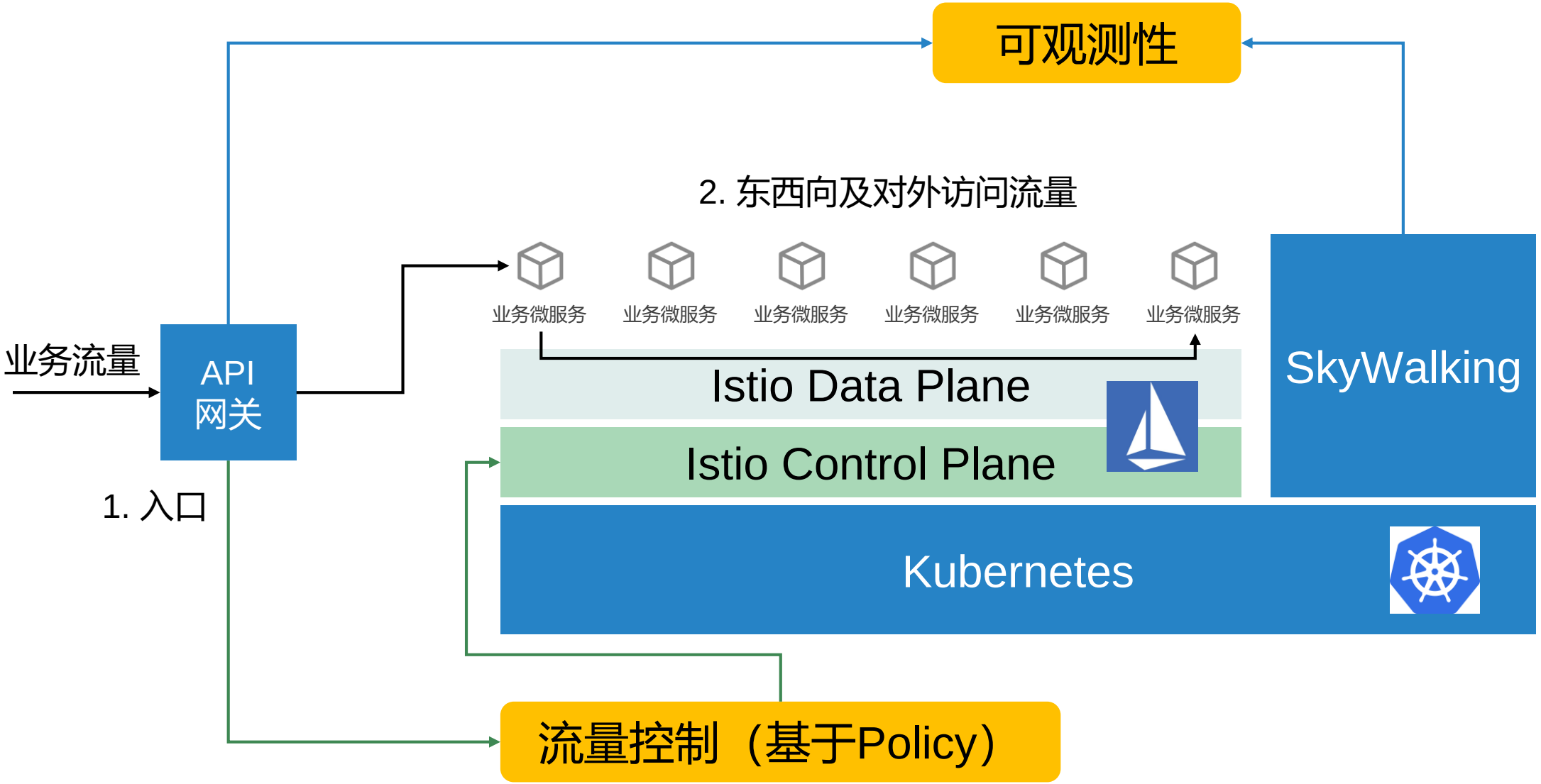
Gartner



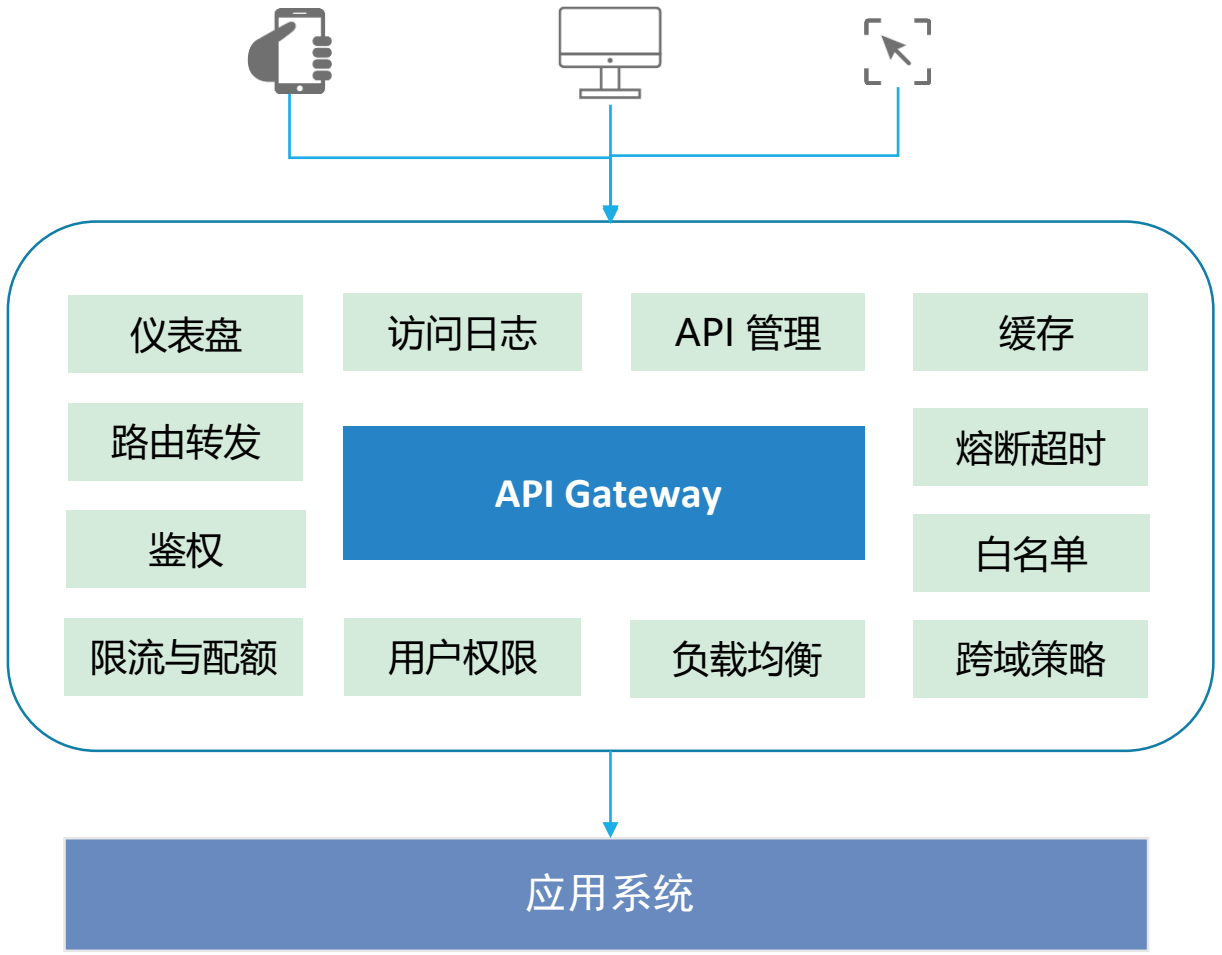
流量安全监测与控制

释放
数字野心

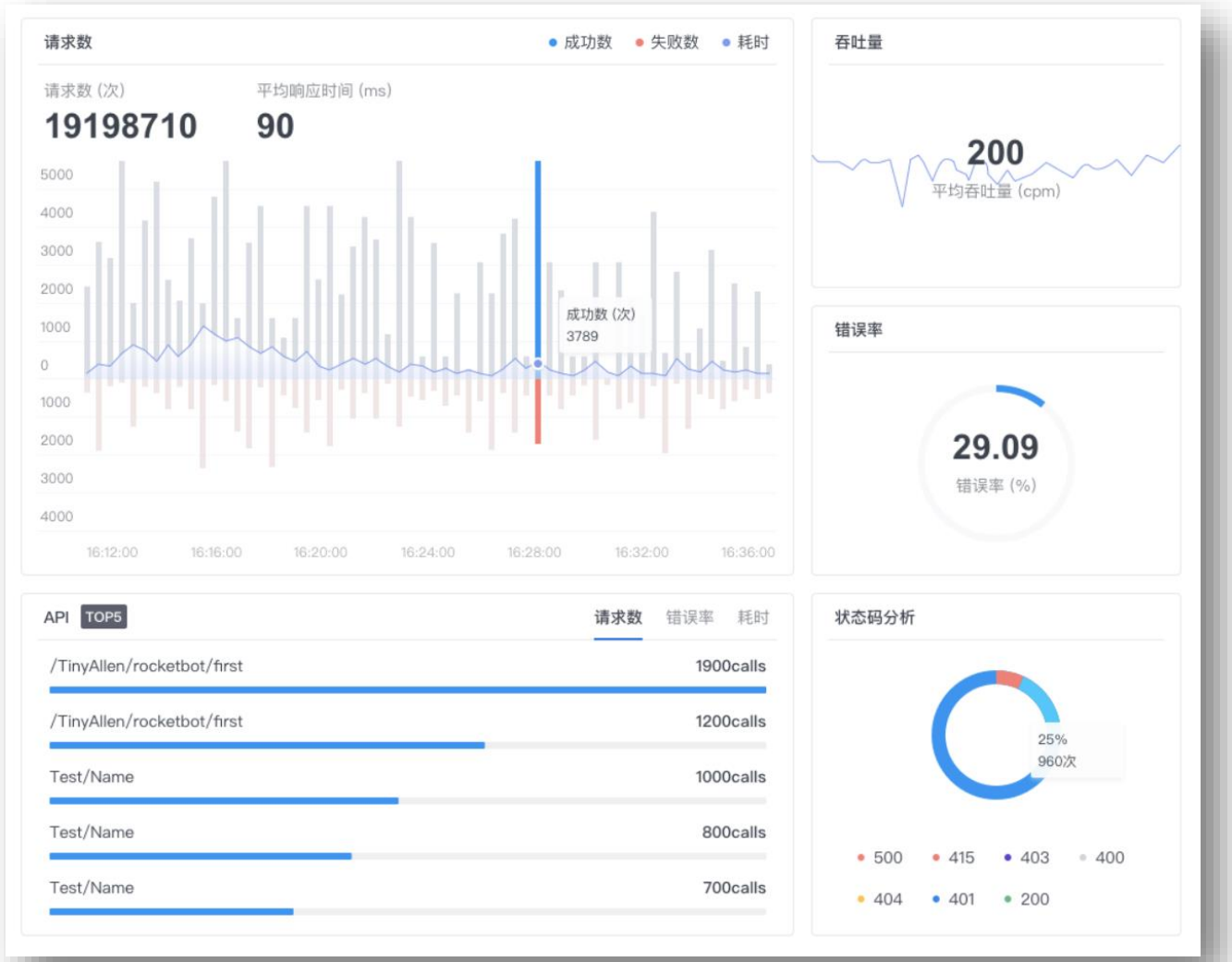
Security Mesh – 流量角度

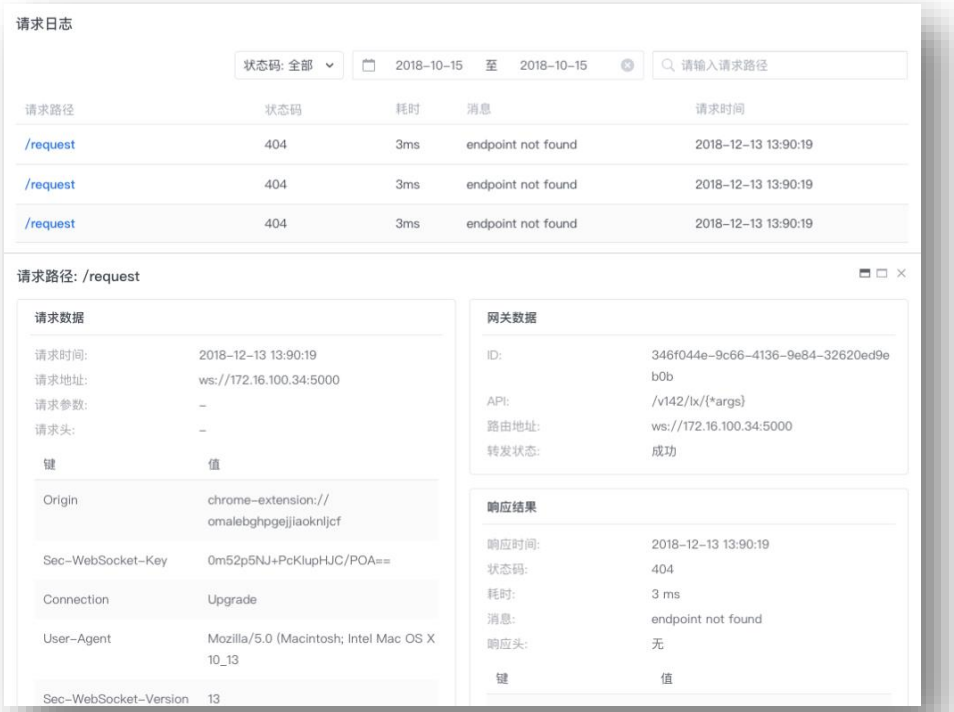


API 网关 – 入口流量可观测性与控制



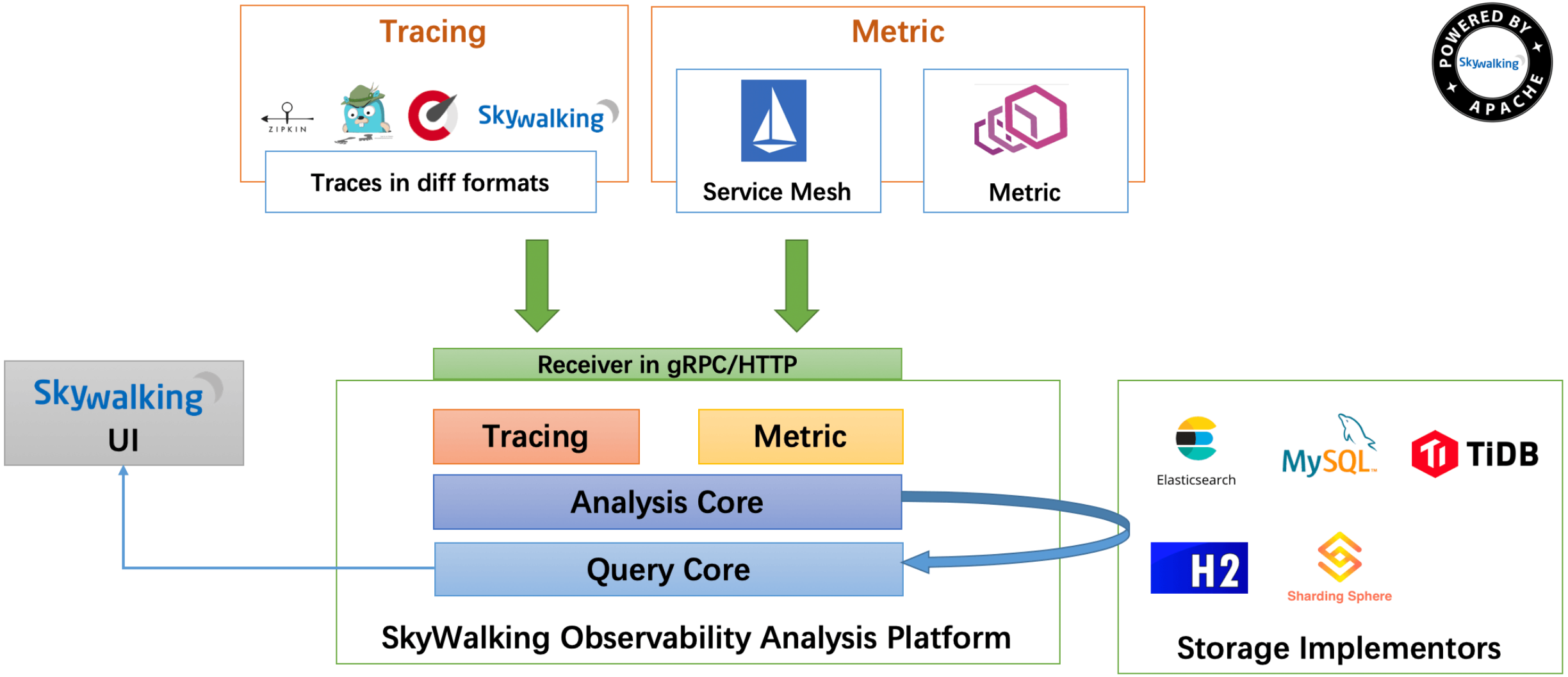
API 网关 – 入口流量可观测性与控制





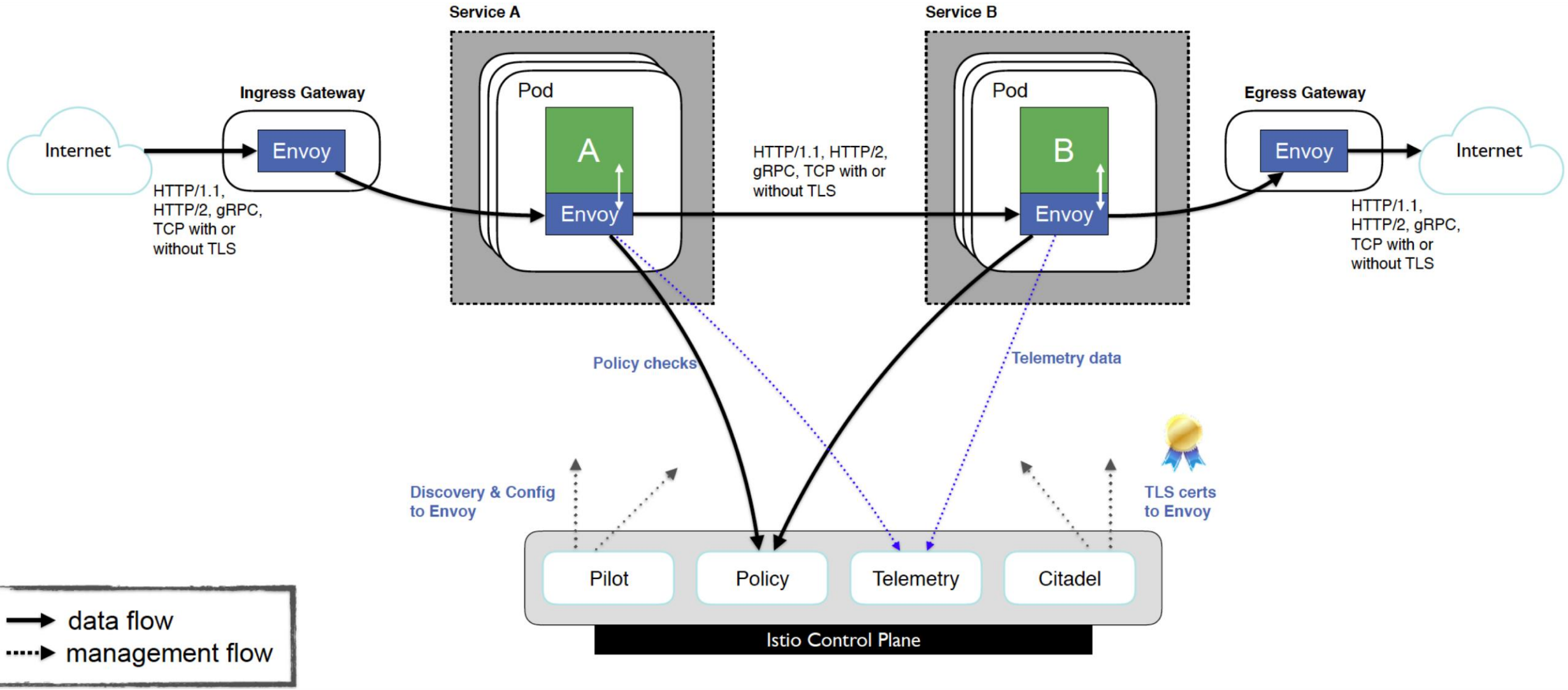
释放
数字野心

SkyWalking – 流量可观测性



SkyWalking -流量可观测性

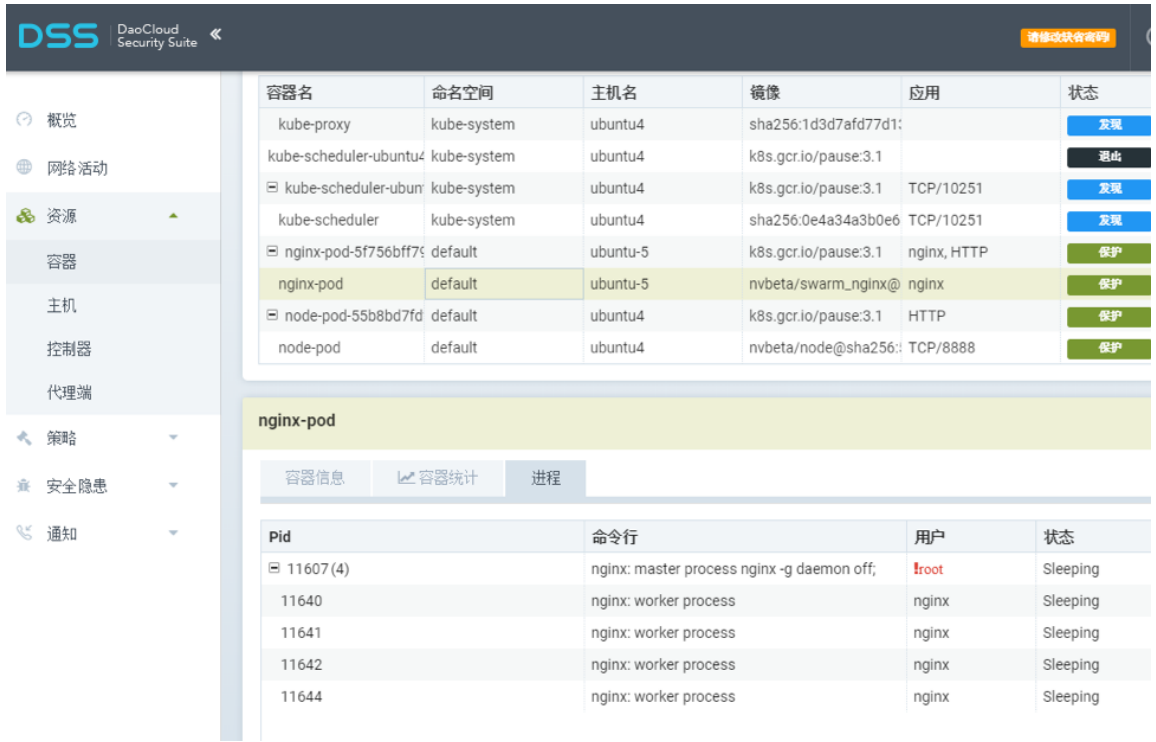
Istio – 东西向流量控制



云原生安全平台

释放
数字野心

云原生安全平台



深入的容器环境可视化

监视和保护容器网络，服务节点和内部行为。

守卫微服务特别是有对外端口的服务

基于行为的应用隔离，阻止来自东西向和南北向容器网络的威胁攻击，深度网络报文检测识别功能。

安全自动化

轻便快速的集成 DevOps 流程，自动学习生成安全策略，免除手动防火墙配置和安全规则配置。

支持多种云环境和混合云环境

云原生安全技术，符合未来发展趋势。适应各种容器运行环境。

释放
数字野心

Q&A

是时候释放你的数字野心了

DaoCloud

info@daocloud.io
www.daocloud.io

释放
数字野心