

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

释放
数字野心



About Me

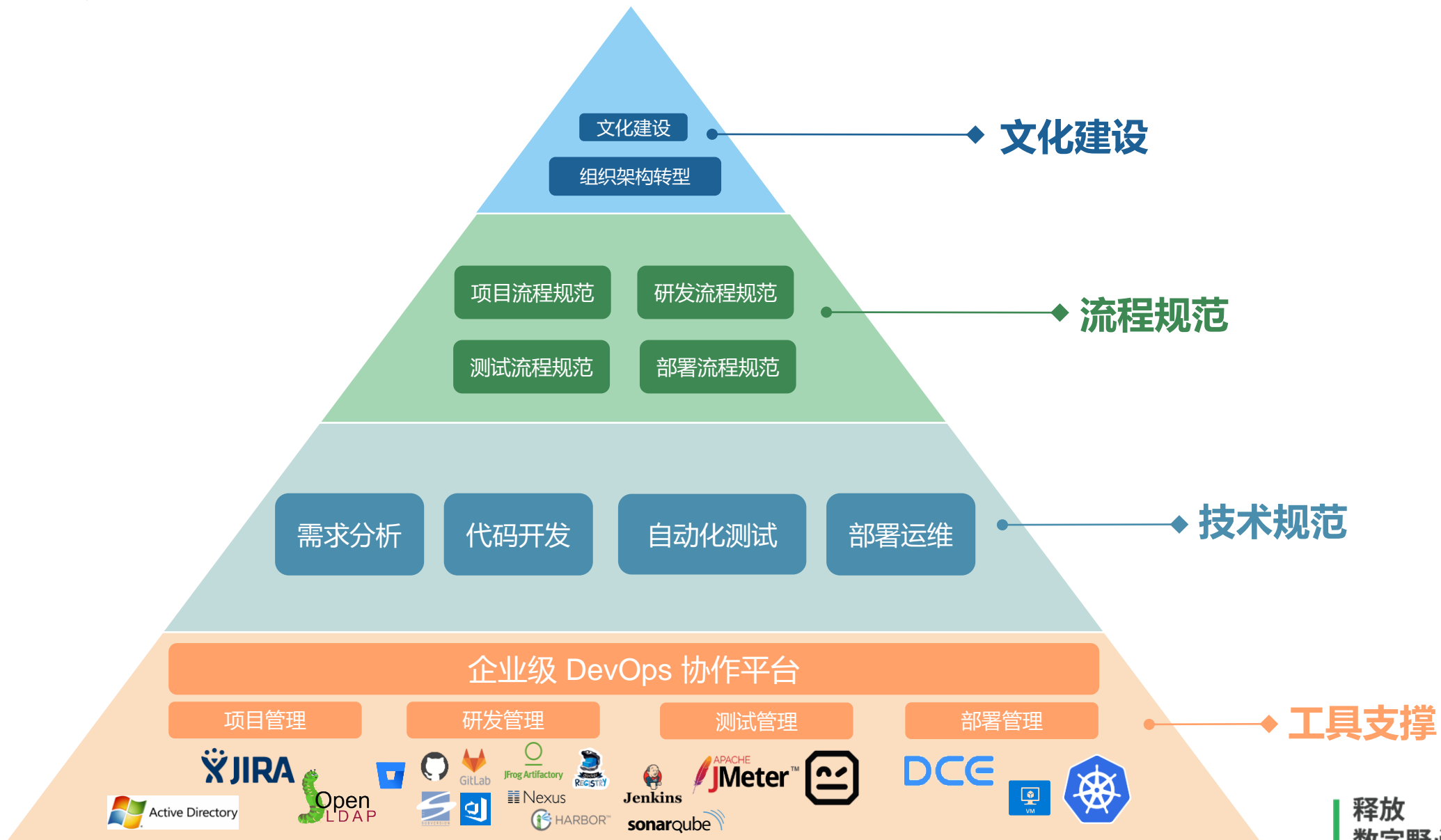
- 南京大学计算机科学与技术系硕士。
- 资深Java程序员，2003年开始从事J2EE开发，从软件开发做到架构设计。
- 08年加入EMC中国研究院，最高担任云平台主任研究员，长期从事云计算创新技术解决方案设计和实现。
- 2015年9月加入麻袋理财，任首席架构师
- 2016年12月加入 DaoCloud，任首席架构师，负责微服务和DevOps相关产品研发与咨询工作
- 2017年 NJSD 讲师 - 基于容器的应用微服务架构转型实践
- 在工作期间，分别在中国和美国提交了20+专利申请，截止到2018年5月，其中有10个专利被美国专利局授权，12个专利被中国专利局授权。

The background features a white line-art illustration on a dark blue background. On the left, a robotic arm is shown in a dynamic pose, holding a tool. On the right, the interior of a car is depicted, including the steering wheel, dashboard, and seats. The overall aesthetic is technical and futuristic.

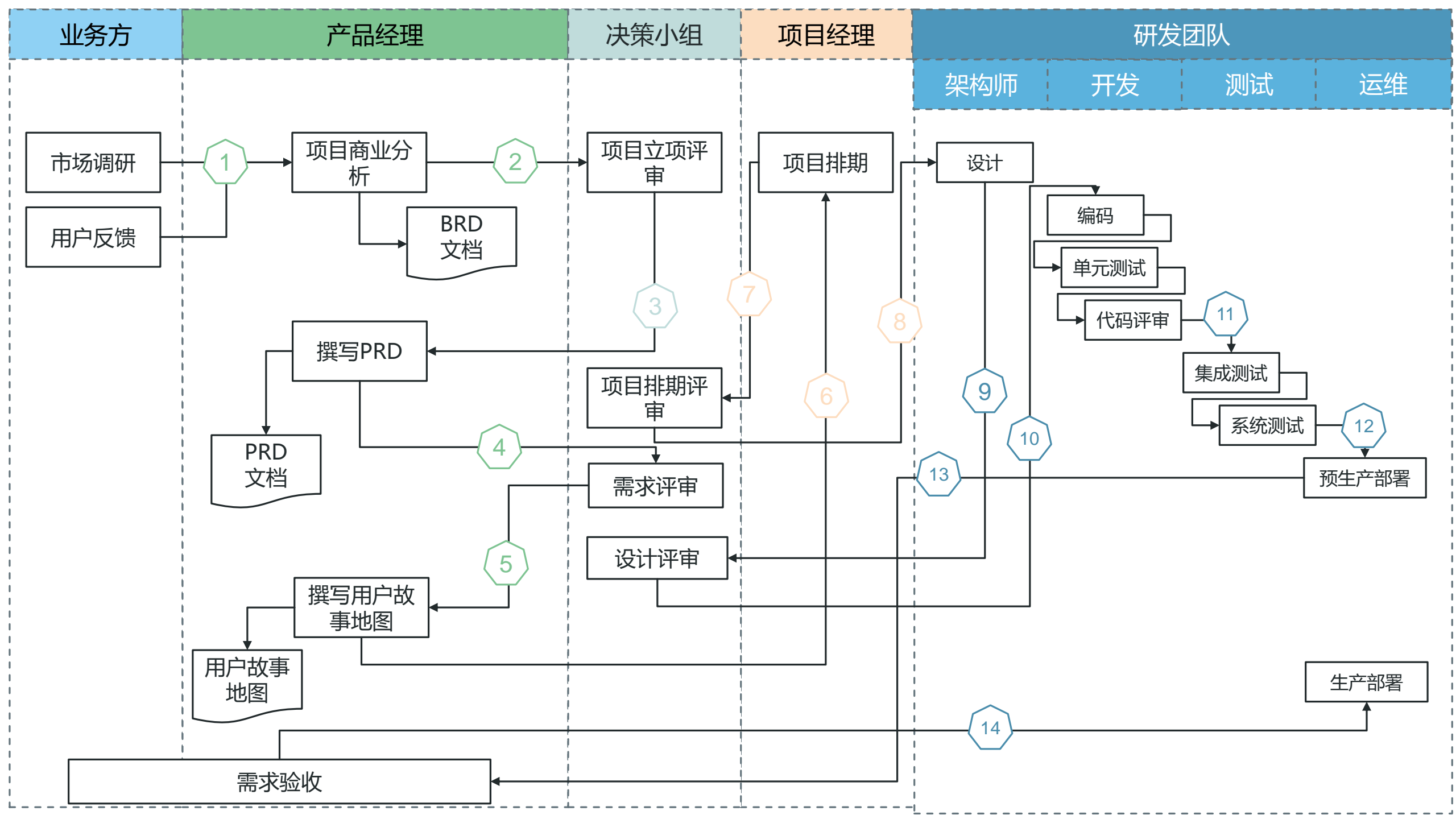
DevOps

释放
数字野心

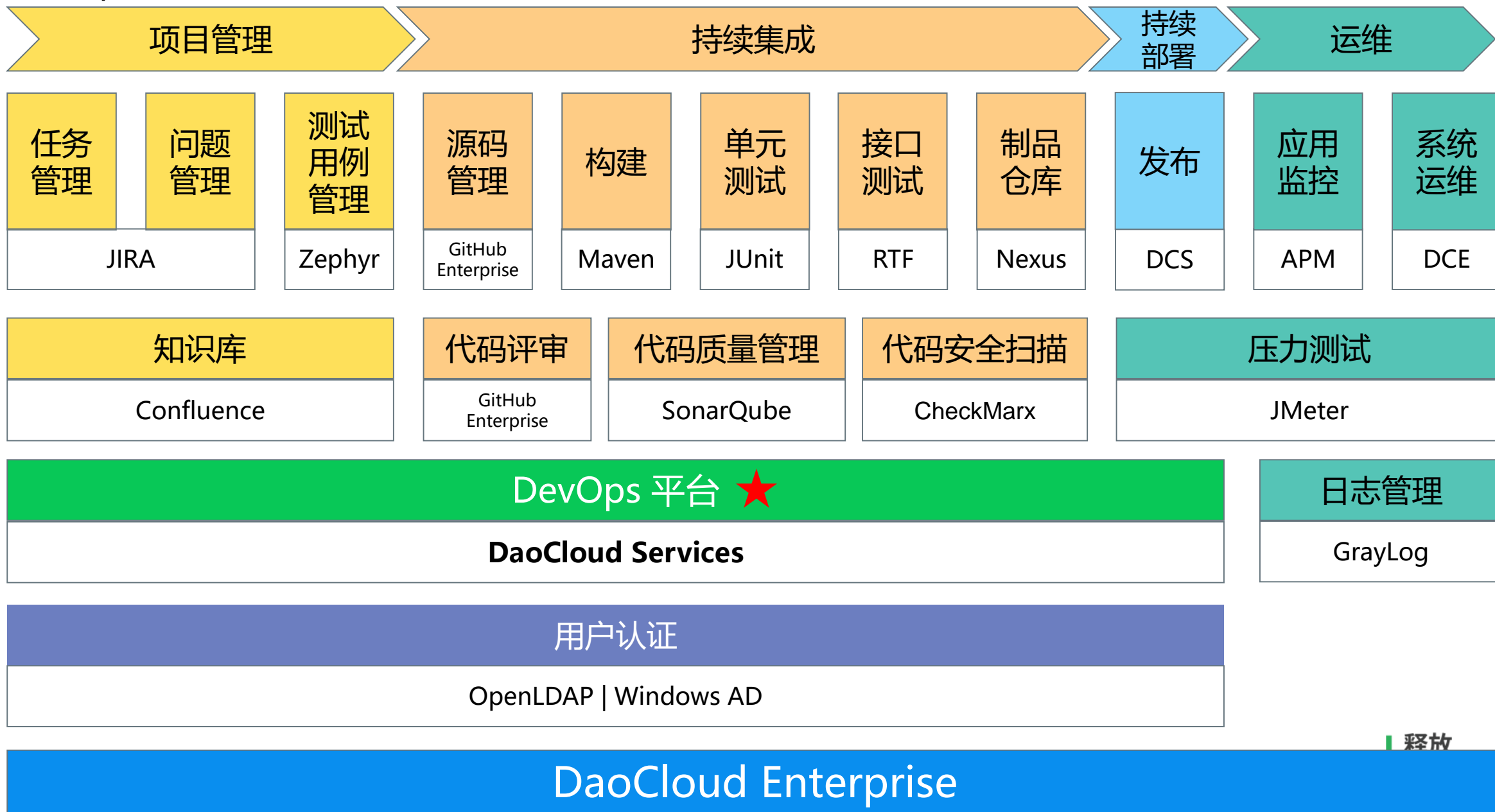
DevOps 的本质



释放
数字野心



DevOps 典型工具链



企业面临的安全挑战

释放
数字野心

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

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 用户头像 搜索

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



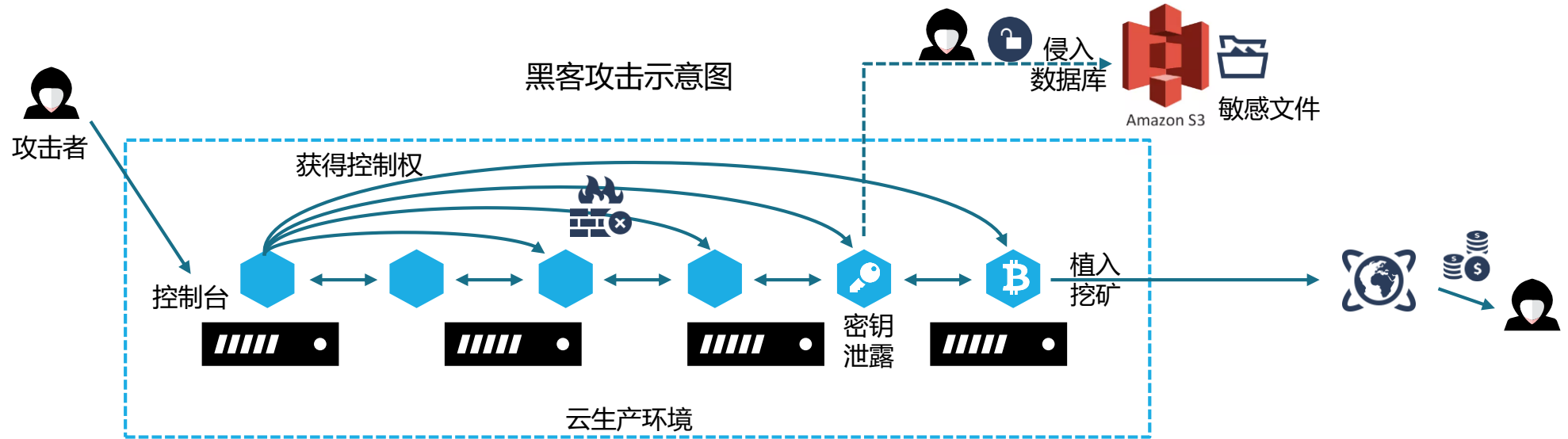
SHARE



Photo by James Bareham / The Verge

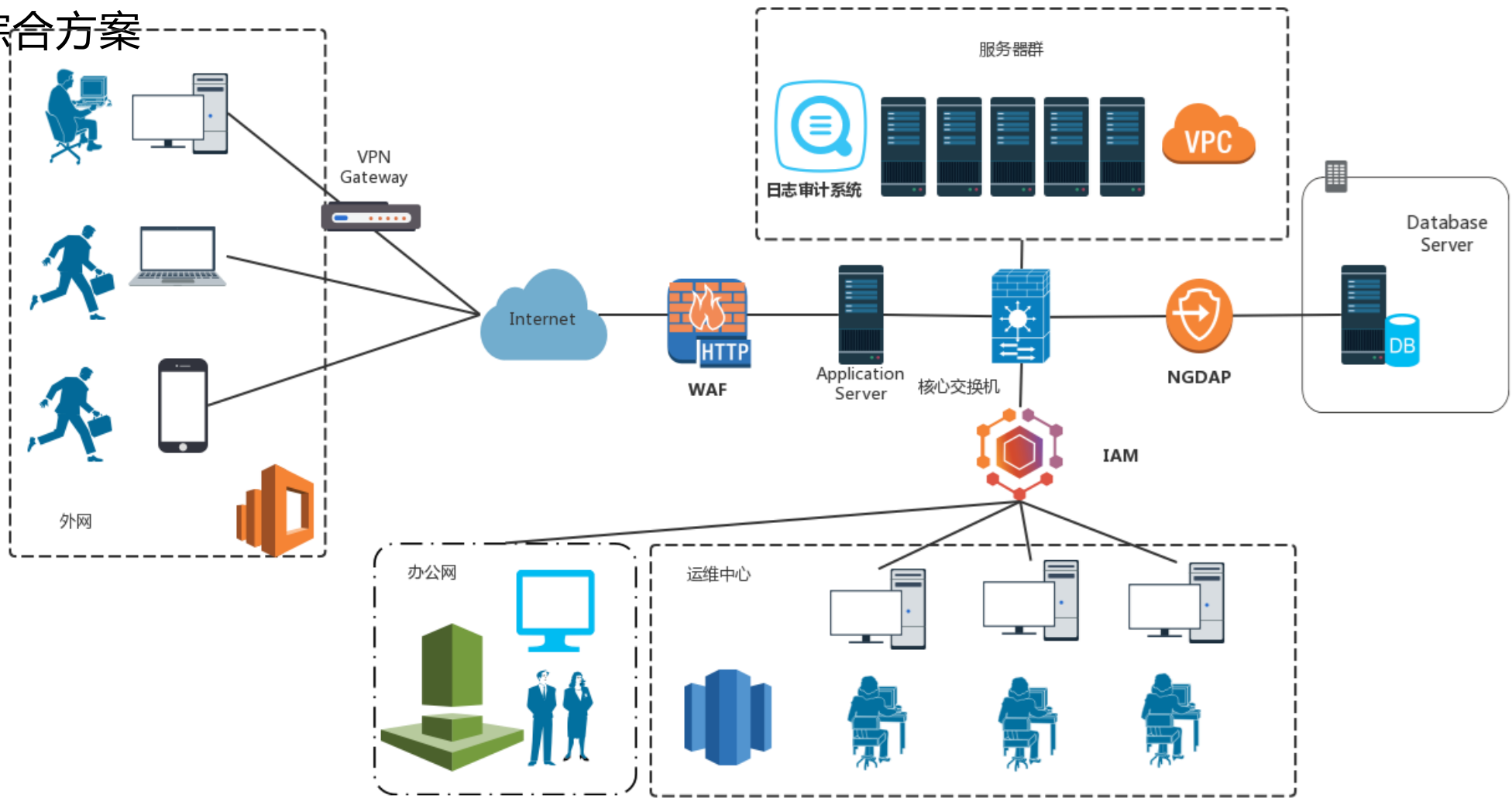
Tesla's cloud account was hacked and used to mine cryptocurrency, according to a security research firm. Hackers gained

黑客入侵攻击路径



传统安全解决方案

安全综合方案



综合方案列表

						
WAF	IAM	NGDAP	日志审计系统	堡垒机	DAF	DAM

The background features a dark blue line-art illustration. On the left, a robotic arm is shown in profile, holding a tool. On the right, the interior of a car is depicted, including the steering wheel, dashboard, and seats. The overall style is technical and futuristic.

云原生安全

释放
数字野心

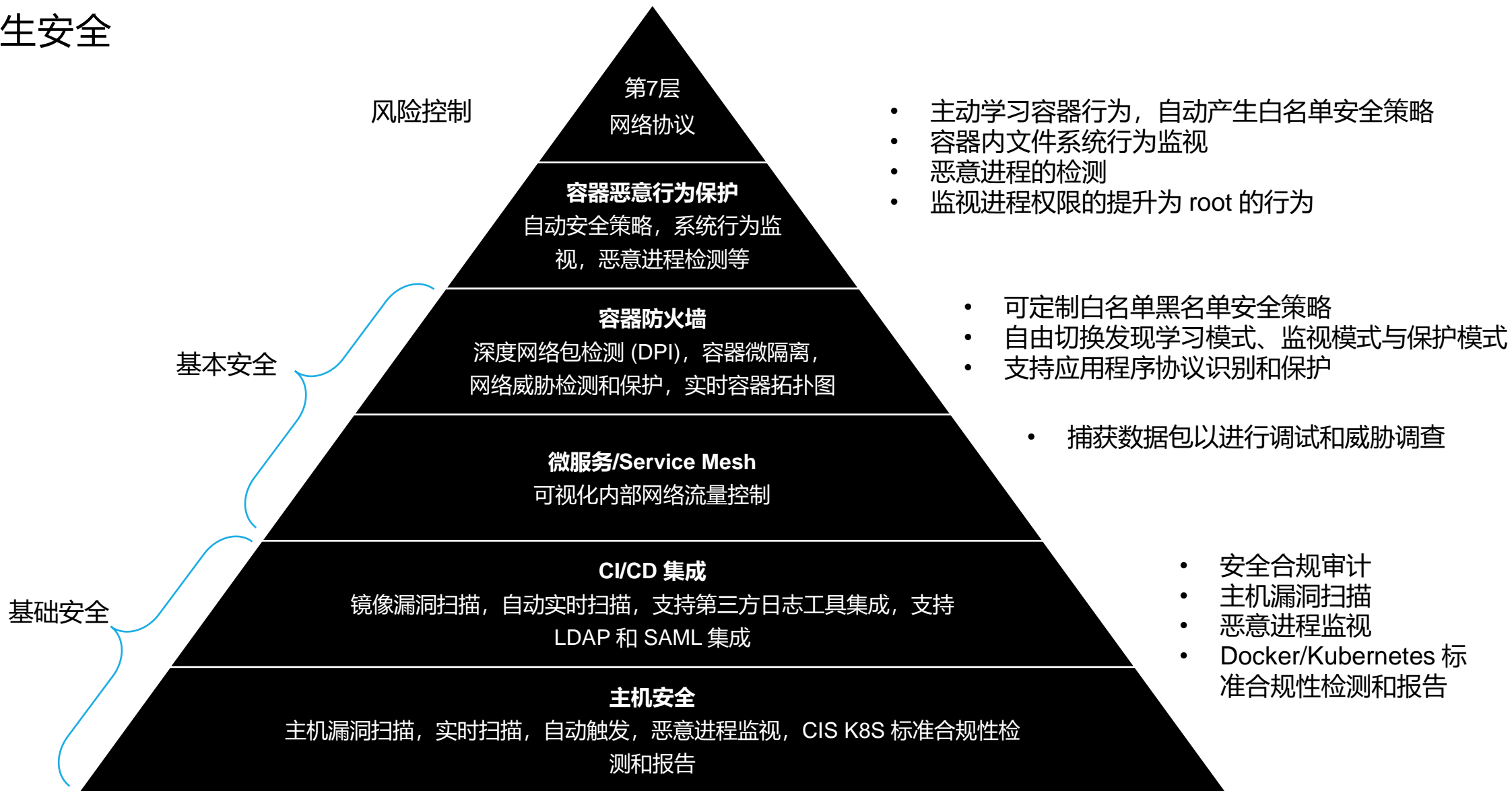
云原生应用

	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

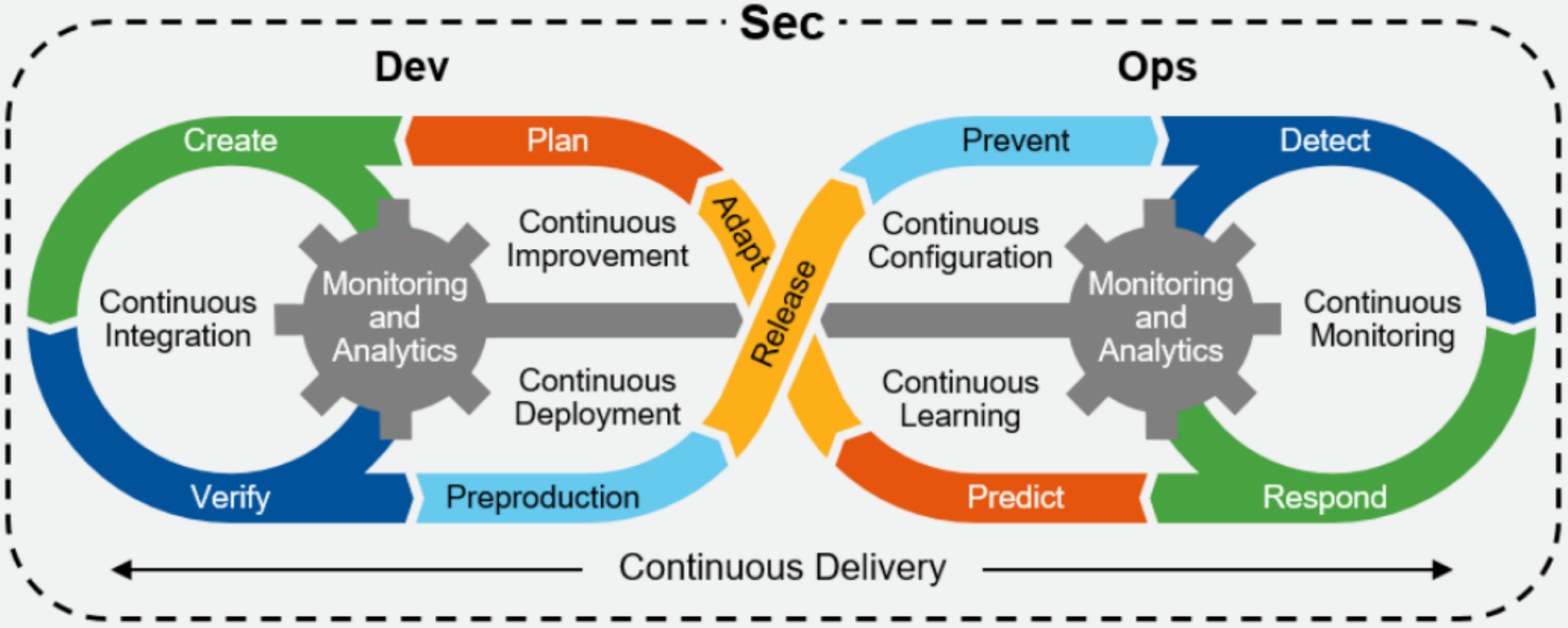
云原生技术实践白皮书*

释放
数字野心

云原生安全



DevSecOps: Seamlessly Integrating Security Throughout DevOps

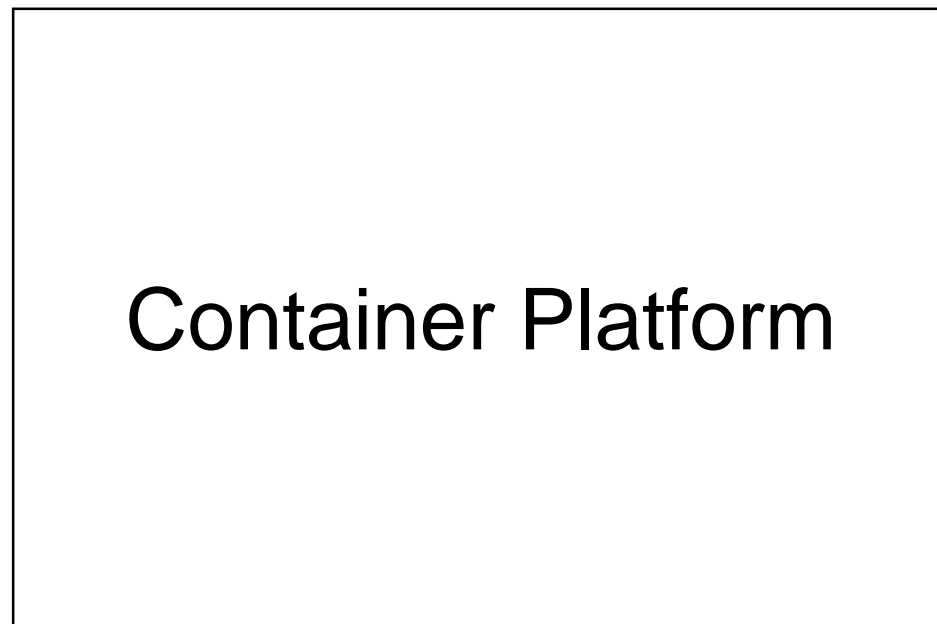
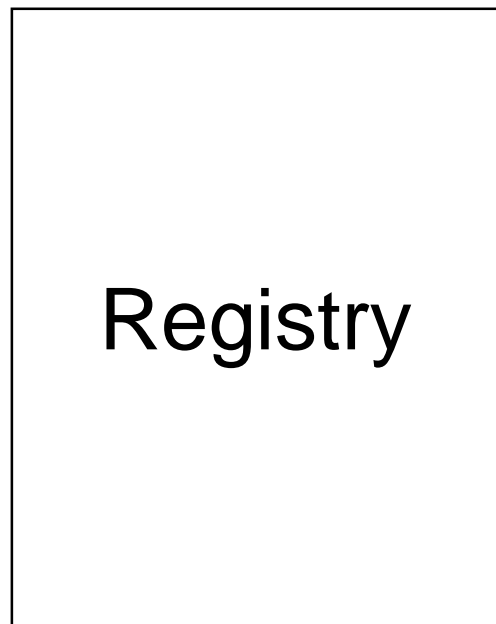
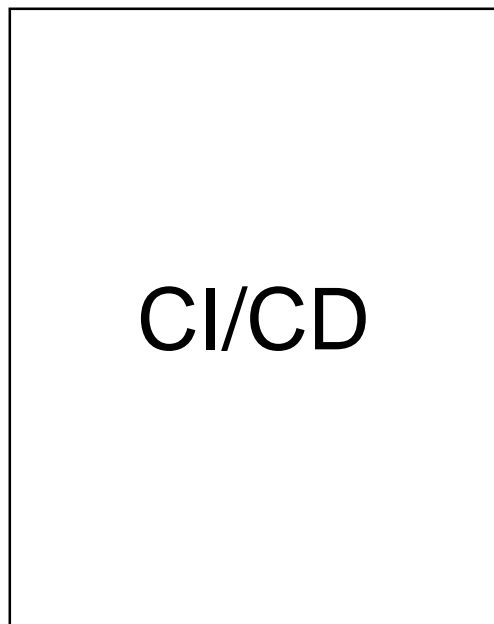
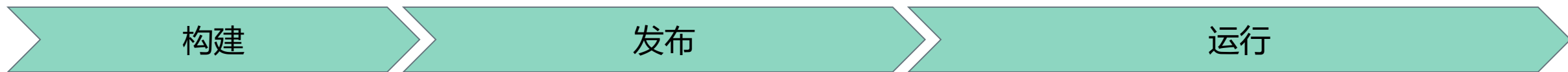


ID: 350812

© 2018 Gartner, Inc.

Source: Gartner (May 2018)

云原生应用的安全

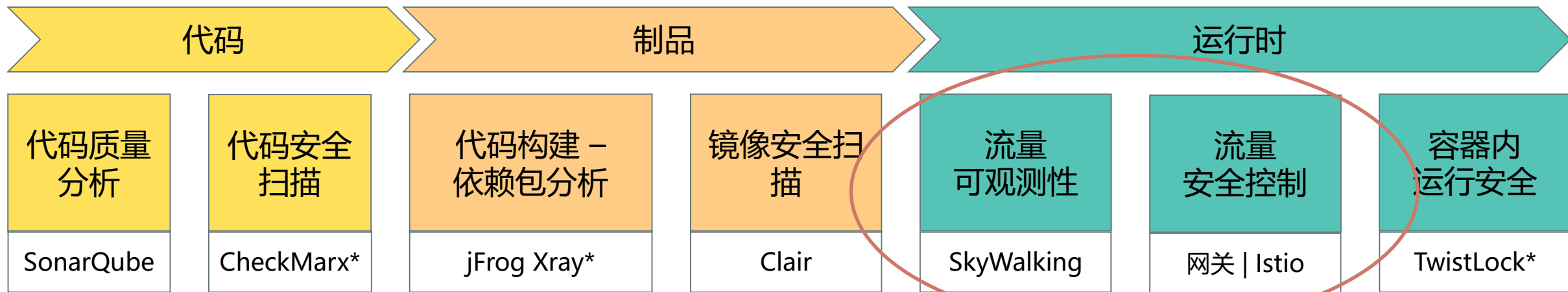


- “Secure containers holistically through integrating controls at key steps in the CI/CD pipeline.”
- 需要通过在 CI/CD 持续集成/持续交付的整个关键环节中全面保护容器安全。
- “Add Layer 7 network segmentation for operational containers that require defense in depth.”
- 为需要深度保护的运行容器添加第 7 层网络保护。

Gartner 《Container Security — From Image Analysis to Network Segmentation, Options Are Maturing》

<https://www.gartner.com/document/3888664>

DevSecOps 典型工具链



1. 代码以及依赖的第三方库

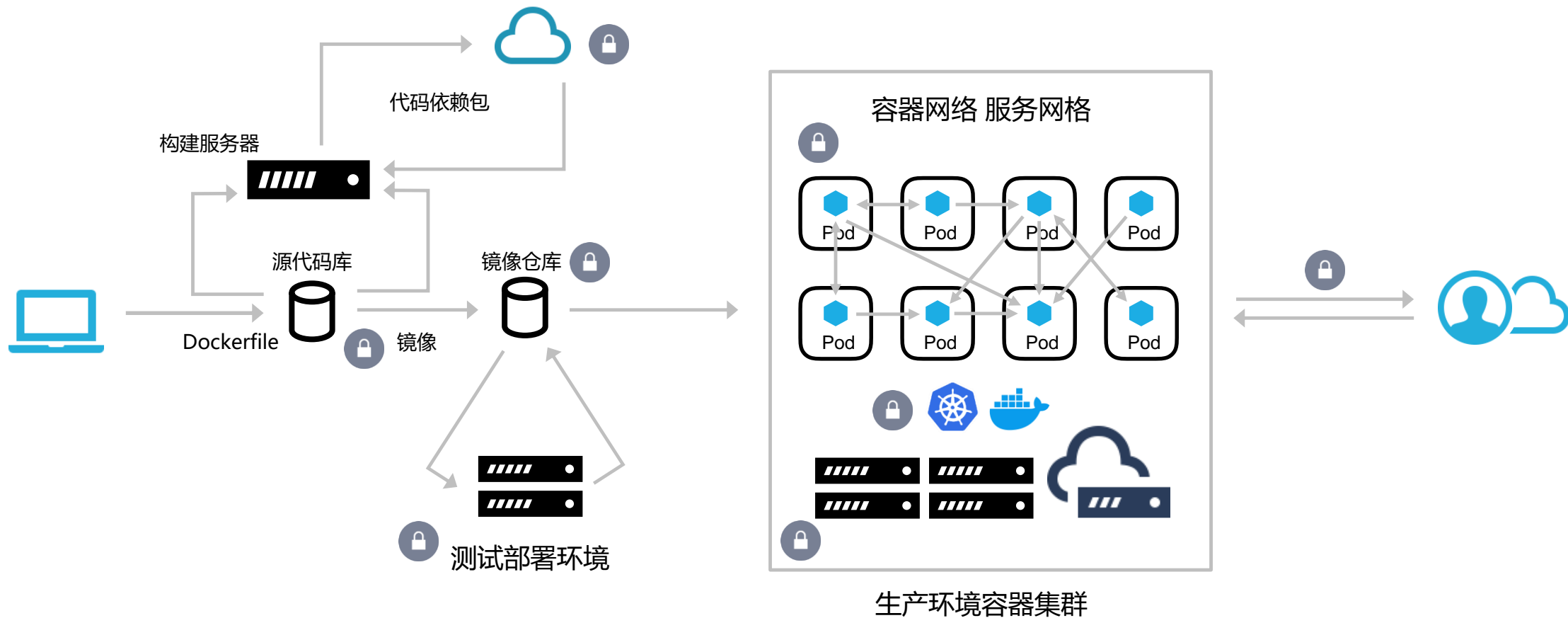
2. 镜像

安全的 Kubernetes

RBAC | Secrets | 安全镜像库 | 运行时保护 | 容器防火墙

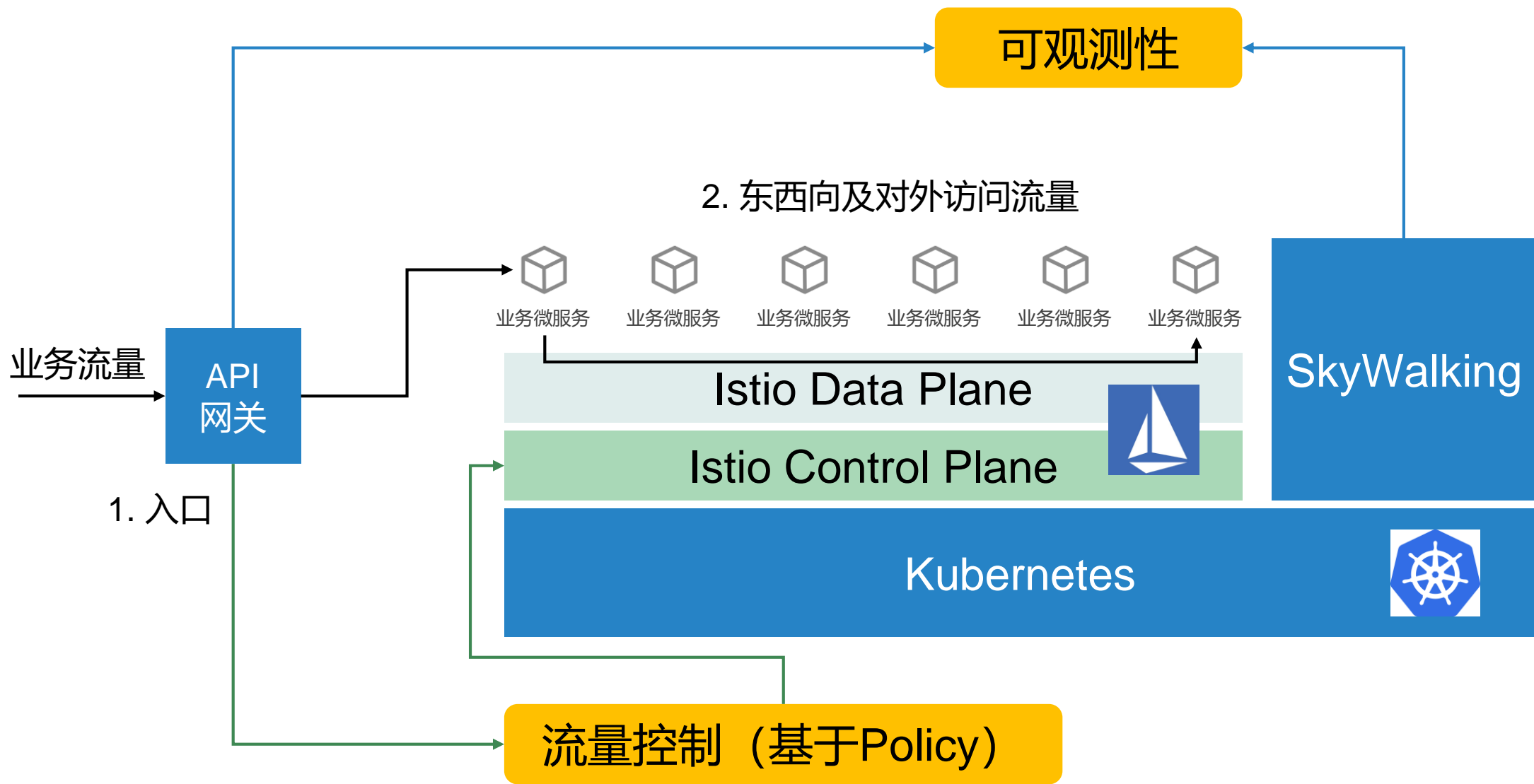
3. 运行时

DevSecOps 流程

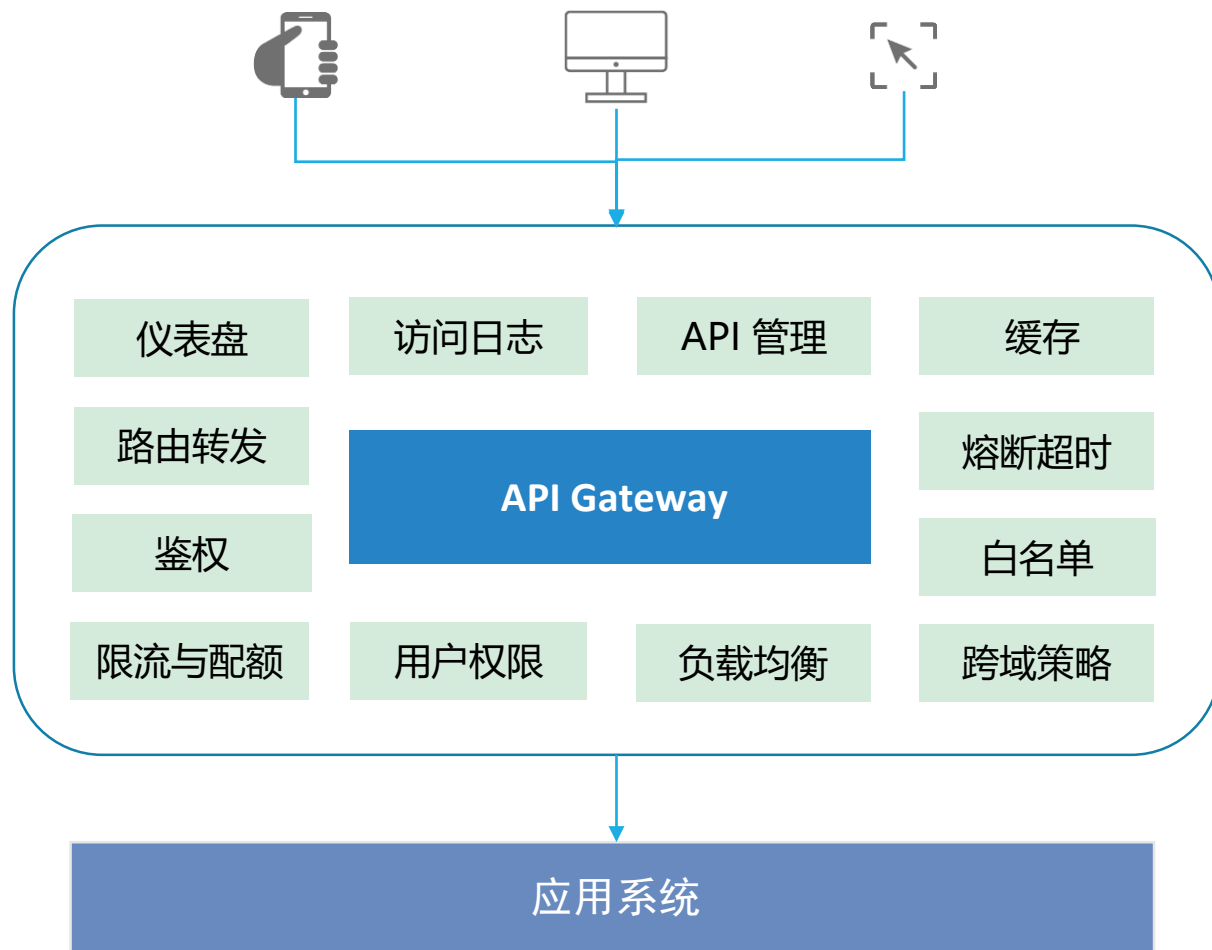


流量安全监测与控制

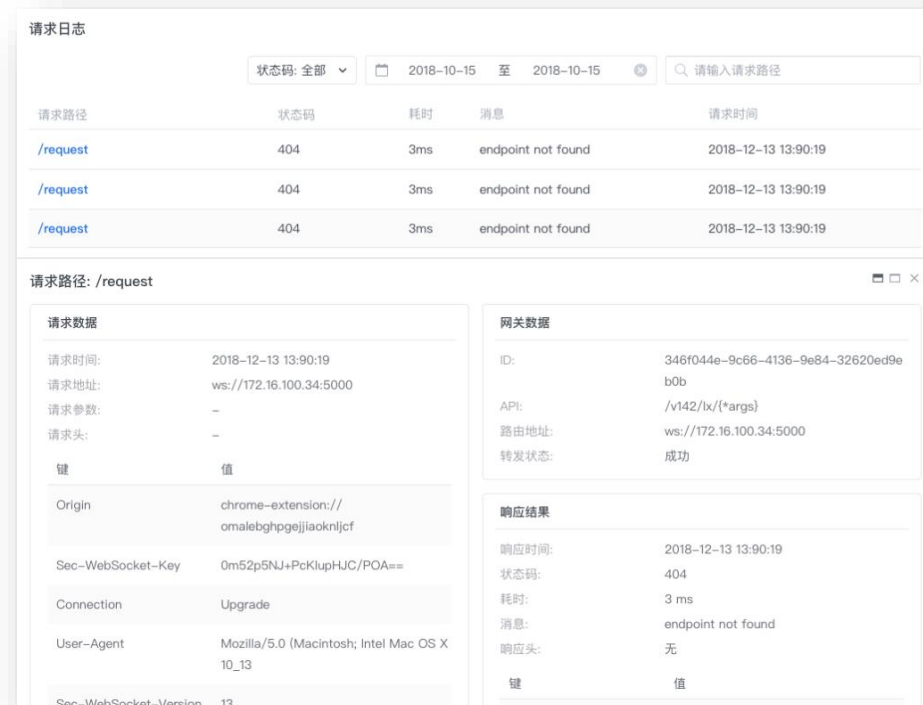
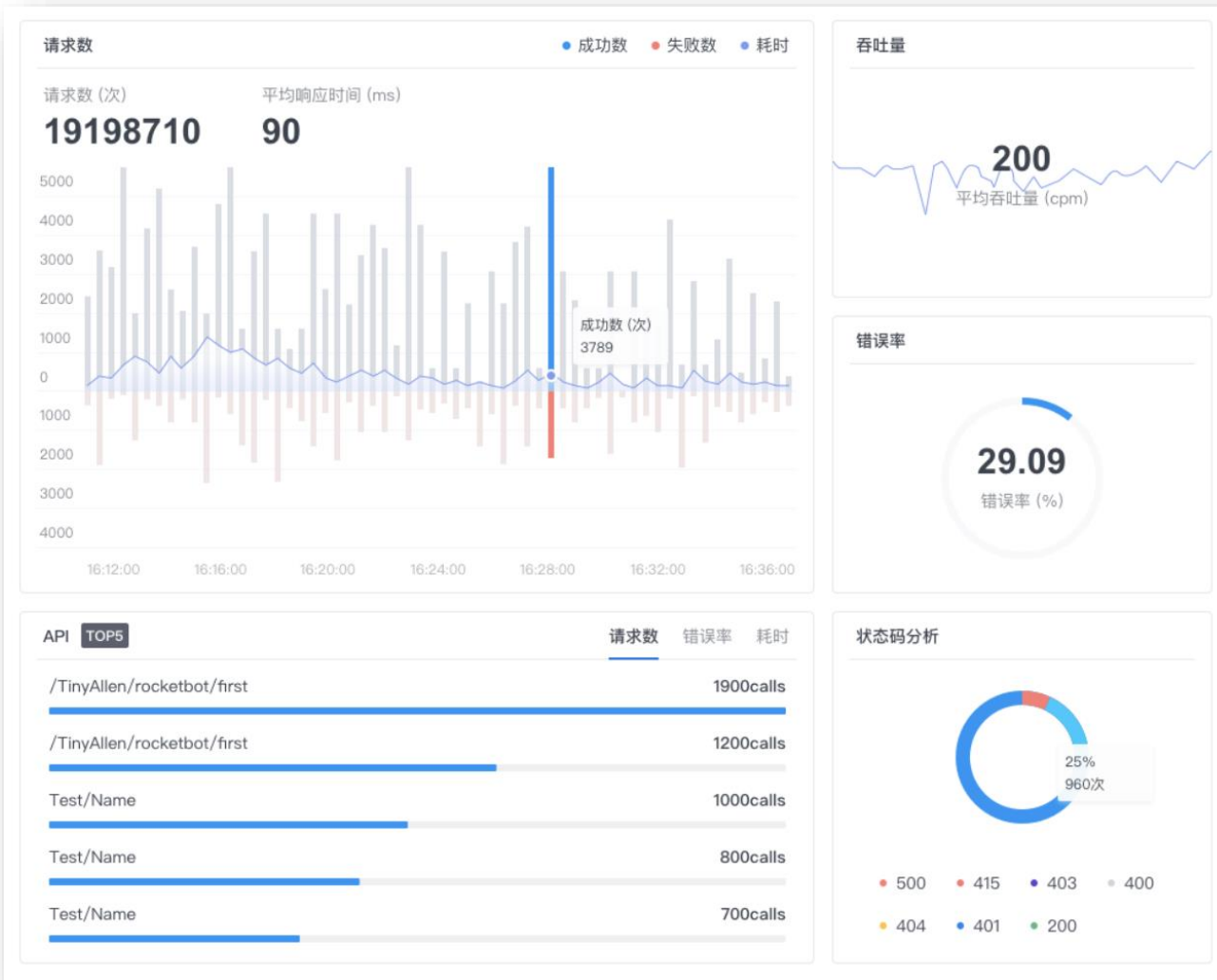
Security Mesh – 流量角度



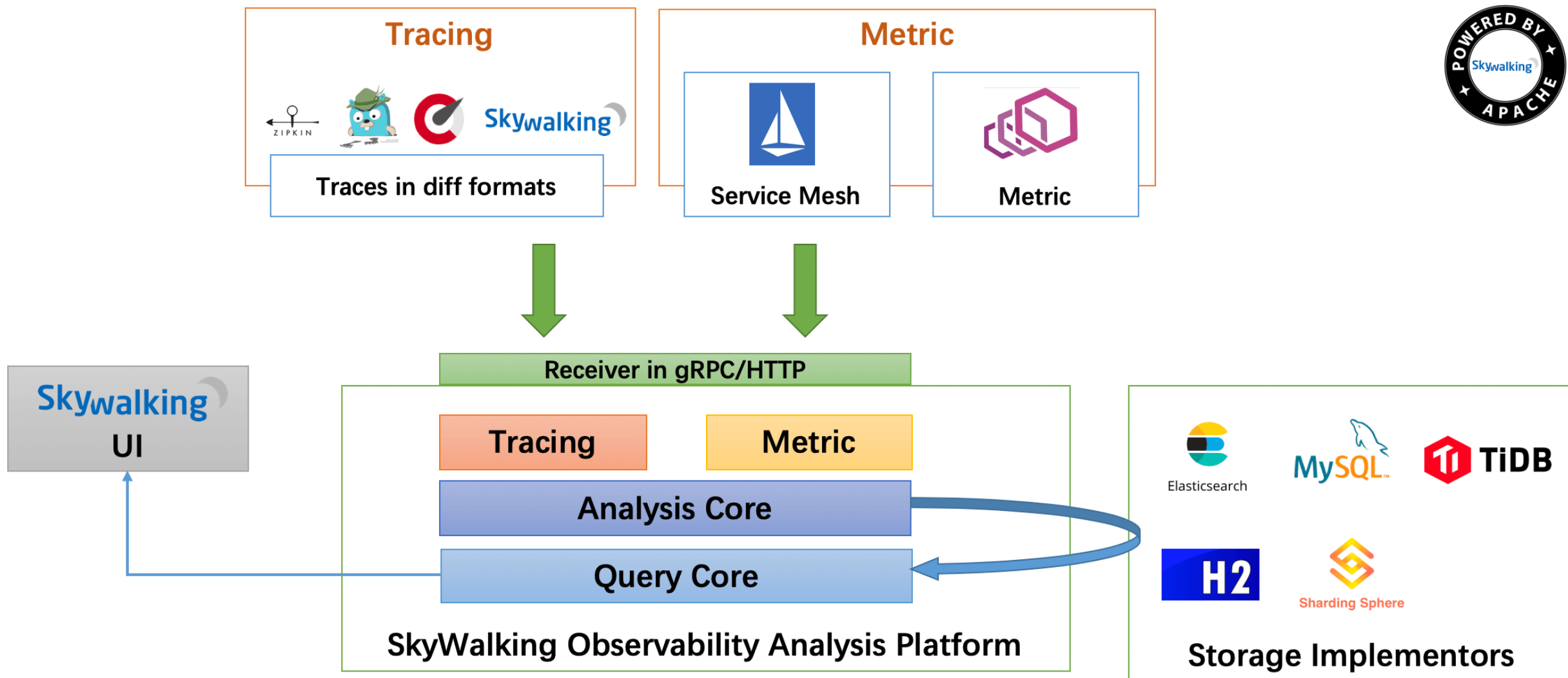
API 网关 – 入口流量可观测性与控制



API 网关 - 入口流量可观测性与控制



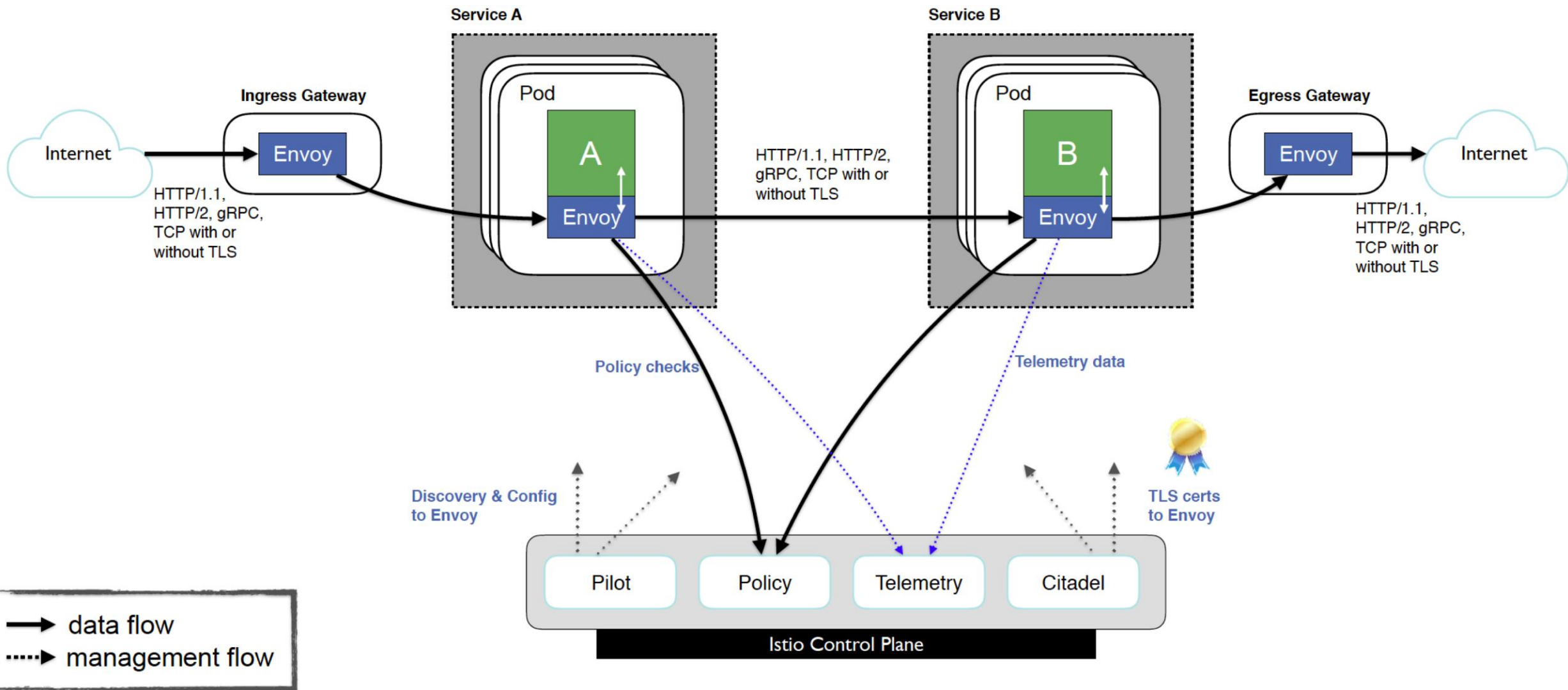
SkyWalking – 流量可观测性



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

The screenshot shows the DSS (DaoCloud Security Suite) interface. The top navigation bar includes the DSS logo, 'DaoCloud Security Suite', and a '请修改状态密码' button. The left sidebar contains navigation items: 概览, 网络活动, 资源, 容器, 主机, 控制器, 代理端, 策略, 安全隐患, and 通知. The main content area displays a table of containers with columns: 容器名, 命名空间, 主机名, 镜像, 应用, and 状态. Below this, the 'nginx-pod' is selected, showing tabs for 容器信息, 容器统计, and 进程. The '进程' tab displays a table of processes with columns: Pid, 命令行, 用户, and 状态.

容器名	命名空间	主机名	镜像	应用	状态
kube-proxy	kube-system	ubuntu4	sha256:1d3d7afd77d1:		发现
kube-scheduler-ubuntu4	kube-system	ubuntu4	k8s.gcr.io/pause:3.1		退出
kube-scheduler-ubun	kube-system	ubuntu4	k8s.gcr.io/pause:3.1	TCP/10251	发现
kube-scheduler	kube-system	ubuntu4	sha256:0e4a34a3b0e6	TCP/10251	发现
nginx-pod-5f756bff79	default	ubuntu-5	k8s.gcr.io/pause:3.1	nginx, HTTP	保护
nginx-pod	default	ubuntu-5	nvbeta/swarm_nginx@	nginx	保护
node-pod-55b8bd7fd	default	ubuntu4	k8s.gcr.io/pause:3.1	HTTP	保护
node-pod	default	ubuntu4	nvbeta/node@sha256::	TCP/8888	保护

Pid	命令行	用户	状态
11607 (4)	nginx: master process nginx -g daemon off;	root	Sleeping
11640	nginx: worker process	nginx	Sleeping
11641	nginx: worker process	nginx	Sleeping
11642	nginx: worker process	nginx	Sleeping
11644	nginx: worker process	nginx	Sleeping

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。

Q&A

是时候释放你的数字野心了



info@daocloud.io
www.daocloud.io

释放
数字野心