GOTC

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

OPEN SOURCE , OPEN WORLD

「CNCF云原生」专场

本期议题：拥抱云原生，原有安全需要升级

黄鹤清 2021年07月10日

探真科技Co-Founder CTO Background

GOTC

黄鹤清, 美国宾夕法尼亚州立大学博士, 云安全专家，国家级海外高层次引进人才

- 中科院信工所教授，博导
- Manager, Senior Researcher，字节ByteDance US AI Lab
  - Security Team Founding Member
  - 字节跳动美国硅谷第三位员工
- Research Staff Member, IBM T.J. Watson Research Center
- Research, Palo Alto Networks，WildFire 2.0 Key Contributor
- Research, FireEye Lab
- Research, Samsung Knox Team

Awards

- 曾代表IBM研究院总部领导美国国防部高级研究计划局(DARPA)透明可信云计算安全项目
- 全球计算机安全年会35年来首位华人获奖者(下一代智能企业安全方向)
- 曾是火眼骇客松冠军，FBI采纳并发表其在火眼的研究成果
- 宾夕法尼亚州里大学最佳博士生研究奖2015 （全EECS系3位）
- Hicool全球创业大赛100强，Cisco全球创业大赛一等奖--4000美元，5110-B类；杭州创业大赛复赛
- 美国杰出人才EB1A, O1A获得者
- 美国审批专利15项, 安全领域国际高质量文章数量30+
- {被引用次数 : 1200+，h-index: 15，i10-index: 17}
  - 引用来自5大洲的101所大学和27家研究机构
  - 其中包括Stanford、CMU、奥斯丁大学、乔治亚理工大学、UIUC等知名学府，北大、上交
  - 以及美国空军实验室、贝尔实验室、微软研究院、Intel研究院, FBI

探真科技 TensorSecurity

ByteDance 字节跳动

IBM Watson

FireEye SECURITY REIMAGINED

paloalto NETWORKS

探真科技 TensorSecurity

探真科技
TensorSecurity

GOTC

探真科技 由硅谷网络安全专家归国创建，基于AISecOps理念，专注于提供全栈内生的云原生安全解决方案。探真方案植根于云原生应用的整个生命周期之中，在云原生应用的开发，部署以及运行的三个阶段层层递进，提供环环相扣的安全解决方案提高整体云原生安全运营的ROI。在云场景威胁日益复杂的环境下，帮助企业充分释放云原生优势，实现云上资产、应用、数据生命周期安全，为企业的云原生业务系统保驾护航，助力企业数字化转型。

企业数字化驱动应用架构的现代化变革

GOTC

2020年43.9%的国内用户已在生产环境中采纳容器技术，超过七成的国内用户已经或计划使用微服务架构进行业务开发部署

数据中心整合

·硬件抽象
·资源池化
·统一运维

IT支撑业务

数据中心云化

·计算、存储、网络、资源的虚拟化建设
·关键应用云化
·智能化运维
·资源交付自动化

IT服务业务

应用现代化

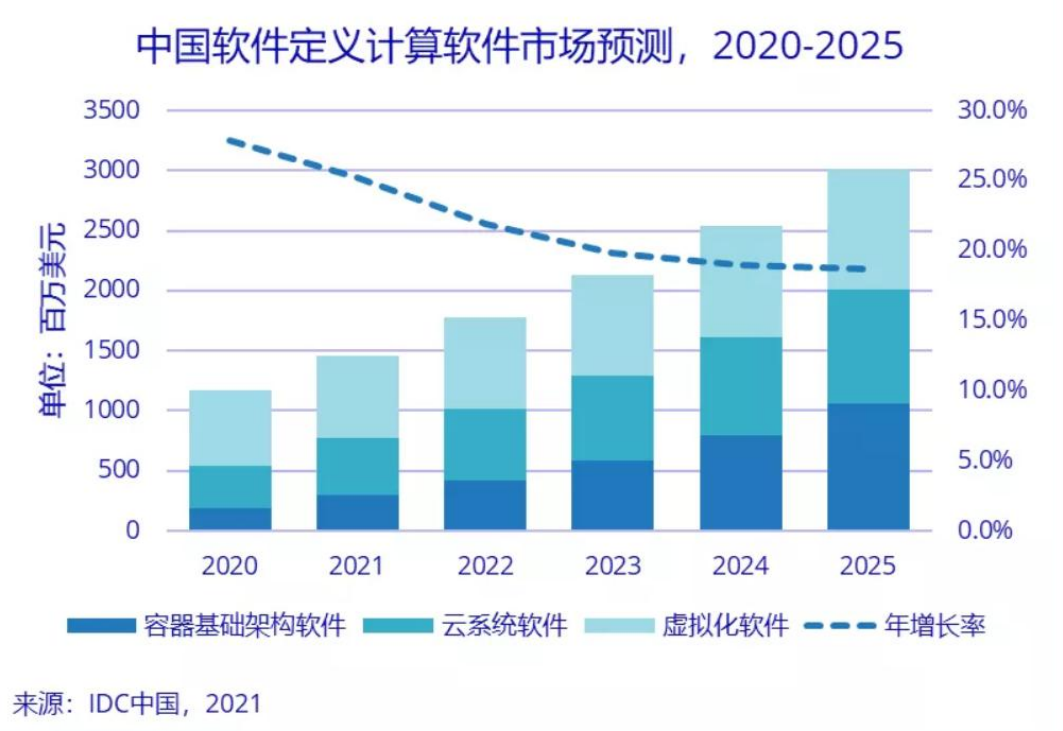
·容器化建设
·微服务架构变革
·云原生构建
·DevOps实现

IT驱动业务

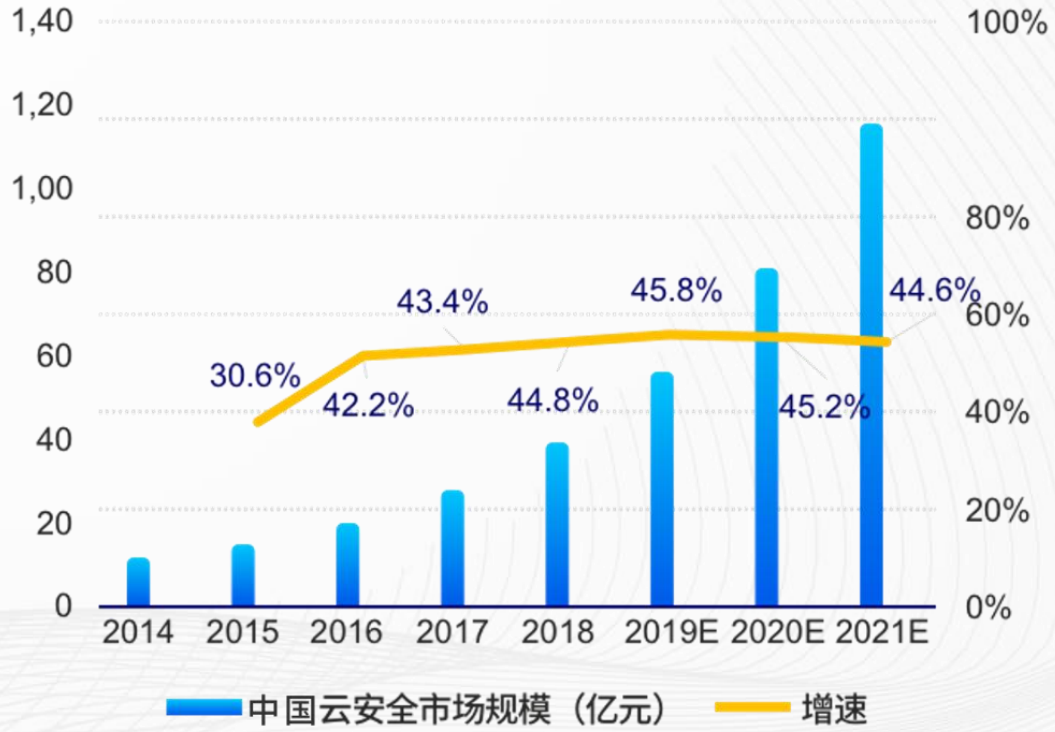
中国软件定义市场

GOTC

- IDC预测，中国软件定义市场在未来五年的复合增长率将达到20.9%，到2025年市场规模将达到30.1亿美元，占据全球软件定义计算软件市场的28.7%，一跃成为仅次于美国的全球第二大市场。



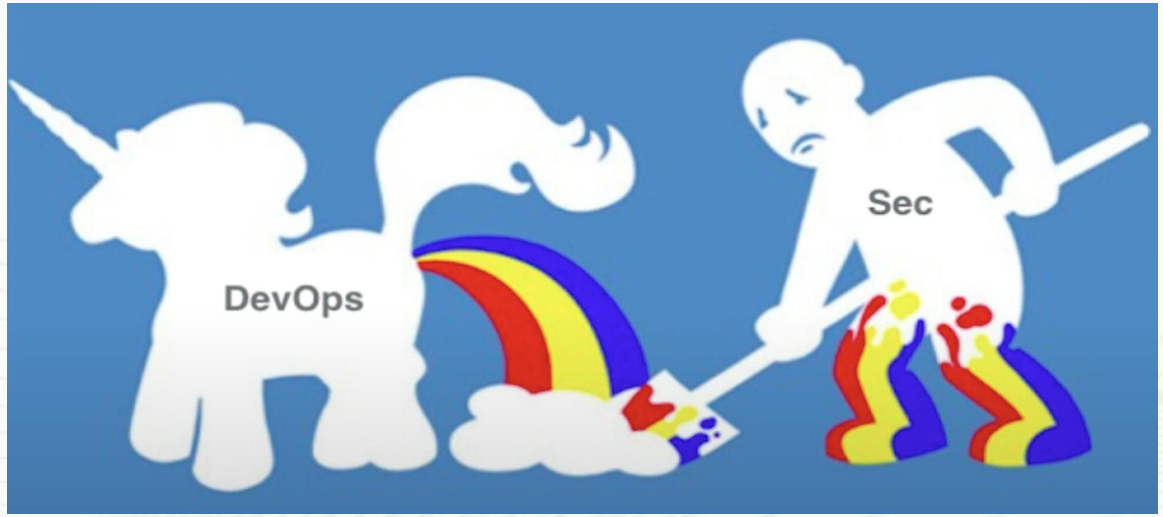
来源：IDC中国，2021



需要重新构建基于云原生的安全

- 传统的安全工具无法解决云原生特定场景下的安全问题，这里举个例子，容器内部是基于网桥模式进行通讯，隔离性差，黑客一旦进入，所有容器都成为可被入侵风险点，通过逃逸提权等方式进行大范围入侵，造成数据泄露，集群资源滥用（如：加密矿工）。而基于传统虚拟化场景下，并不存在类似情况。

- 传统安全工具不是云原生的，不能匹配云原生自身灵活、轻量、高效、可伸缩、可随时启停的诉求。这就导致安全防护效率跟不上应用迭代速度， 安全防御无法随服务进行动态伸缩随时启停



目录

CONTENTS

01
风险的“不确定性”需要“原生”安全

“黑天鹅和灰犀牛”

安全风险的“不确定性”—— 云“原生”安全

GOTC

黑名单，已知特征匹配
基于ATT&CK攻击矩阵的恶意行为模型检测，

云原生开源漏洞：
Golang Concurrency BUG自动化检测和响应

“原生”安全

大数据安全分析，图数据库关联等，例如：SIEM态势感知->SOAR->XDR

基于AI/ML的异常偏移侦测和
基于“零信任”的动态鉴权

02

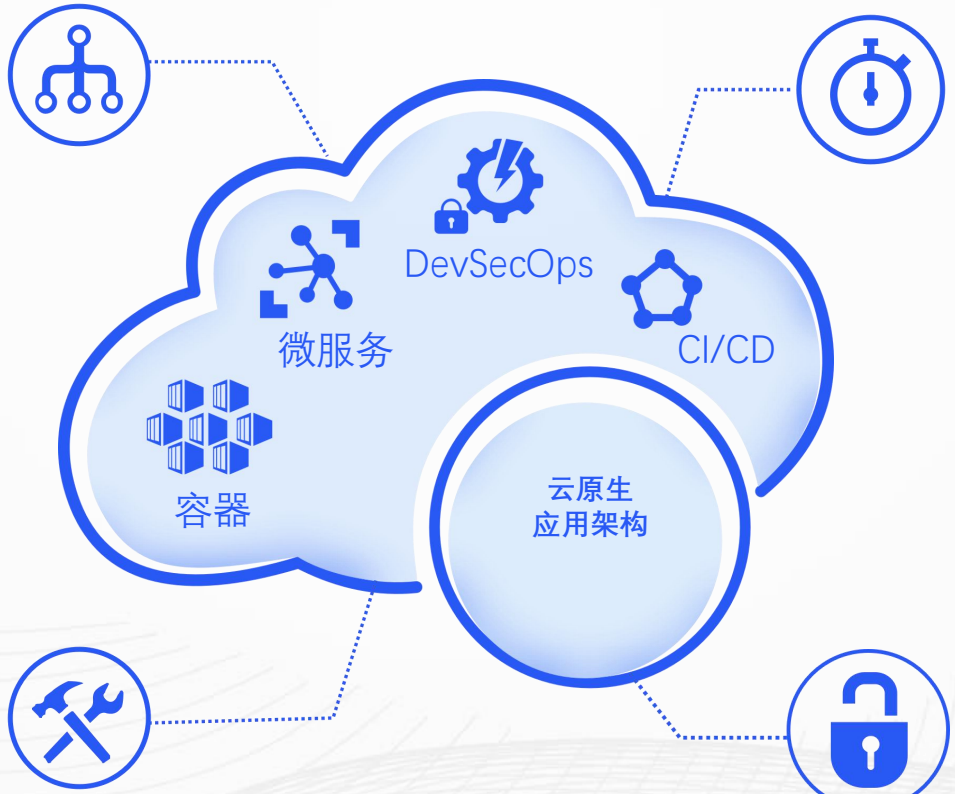
云“原生”安全设计理念

云原生带来的新的安全隐患

GOTC

传统的安全问题
在云原生环境依然存在

Web攻防和系统攻防，暴力破解和反弹Shell等问题依然存在，但传统工具无法工作在云原生环境中



云原生计算环境
引入新的安全风险

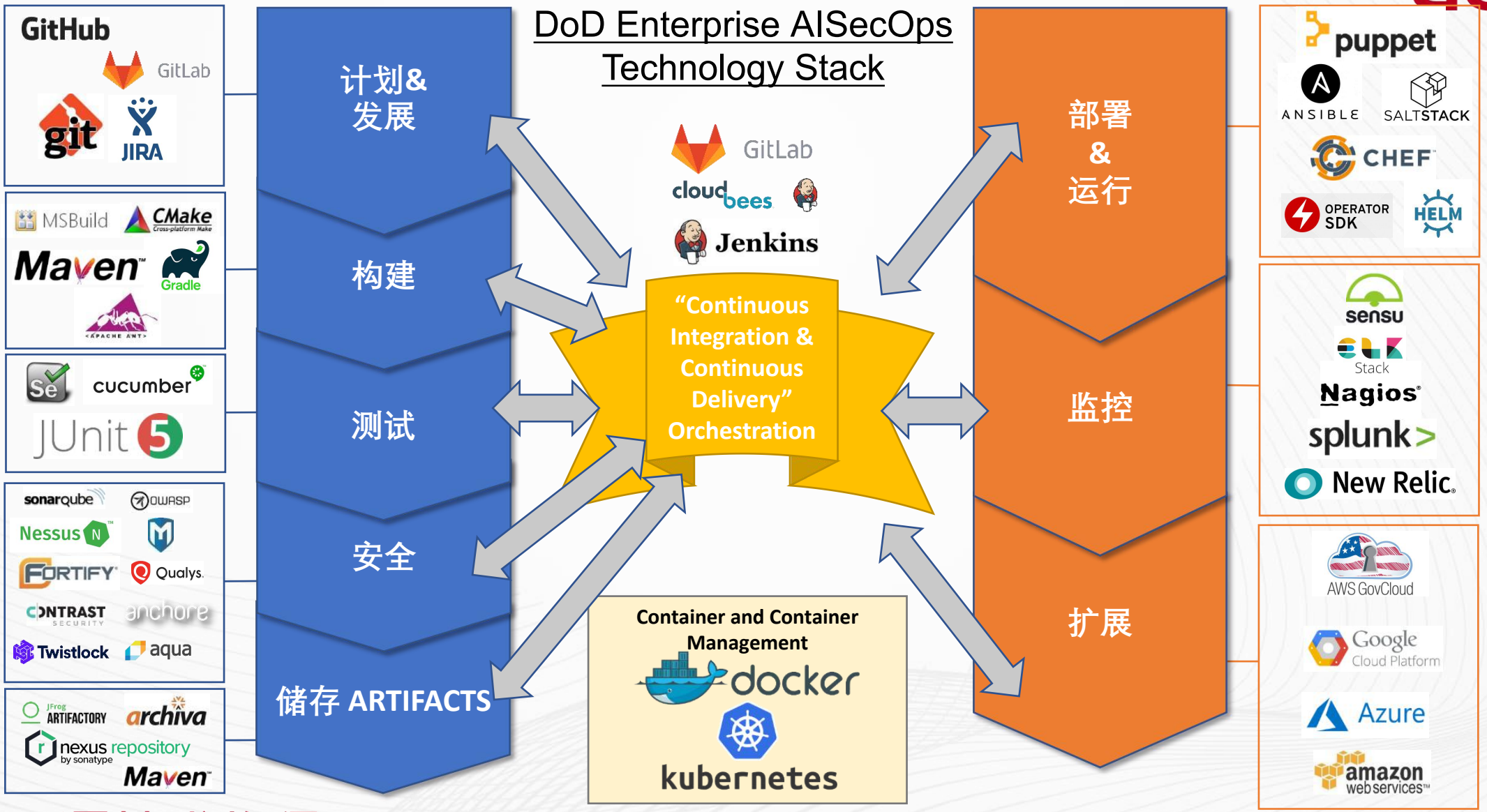
开发IDE安全，编排系统及组件安全，镜像及镜像仓库安全，容器网络安全，容器逃逸，运行时入侵

运维管理流程和服务模型变化带来的管理难题

云原生资产风险深度可视化难题，Dev**Sec**Ops流程难题，云服务商和企业的安全防护责任和边界不清晰等

云原生化应用
引入新的安全风险

凭证泄露，微服务的攻击敞口及治理难度，Serverless模型安全，API爆炸产生的权限管控和资源滥用


DoD Enterprise AISecOps Technology Stack
GitHub
GitLab
git
JIRA
MSBuild
CMake
Maven
Gradle
Apache Ant
Selenium
cucumber
JUnit 5
sonarqube
OWASP
Nessus
FORTIFY
Qualys
CONTRAST SECURITY
anchore
Twistlock
aqua
JFrog ARTIFACTORY
archiva
nexus repository by sonatype
Maven
计划&发展
构建
测试
安全
储存 ARTIFACTS
GitLab
cloudbees
Jenkins
"Continuous Integration & Continuous Delivery" Orchestration
Container and Container Management
docker
kubernetes
部署&运行
监控
扩展
puppet
ANSIBLE
SALTSTACK
CHEF
OPERATOR SDK
HELM
sensu
ELK Stack
Nagios
splunk>
New Relic
AWS GovCloud
Google Cloud Platform
Azure
amazon web services

云“原生”安全6大核心设计理念

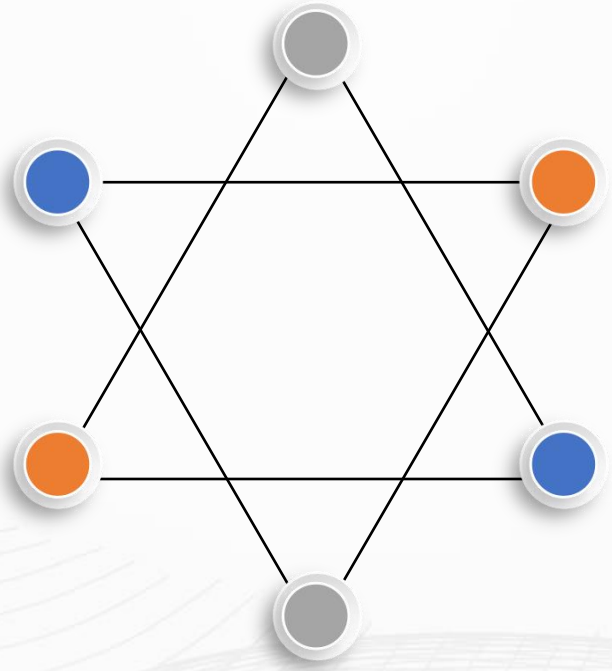
GOTC

安全内生

将安全能力的部署、数据获取、检测及防御内生到云原生环境中， 利用云原生能力围绕数据、服务、容器等动态工作负载做到可自动发现，持续观测，风险态势感知、与处置闭环。

安全左移

深度内生于CICD流程，左移于上线前进入安全流程。上线前，开发、分发、构建阶段做镜像与容器安全静动态扫描准入与加固



安全智能化

智能发现、自动扫描，智能加固、智能生成ACL、自动部署、自动化处置

安全运维闭环

安全不止于发现、告警。最终的安全是要有安全运维的持续闭环能力，在海量数据信号中高效的寻找核心安全事件做响应

基于AI的风险免疫

利用云原生的不可变性，基于“初信任”状态，利用机器学习能力生成系统调用, 文件系统访问，进程，网络，数据交换等多层次行为免疫画像，运行时开启偏移侦测，当发现行为异常时进行智能告警和阻断。

零信任

用零信任的逻辑对所有资源访问做鉴权，并且有能力持续监控与控制

云“原生”安全需要具备的13大能力

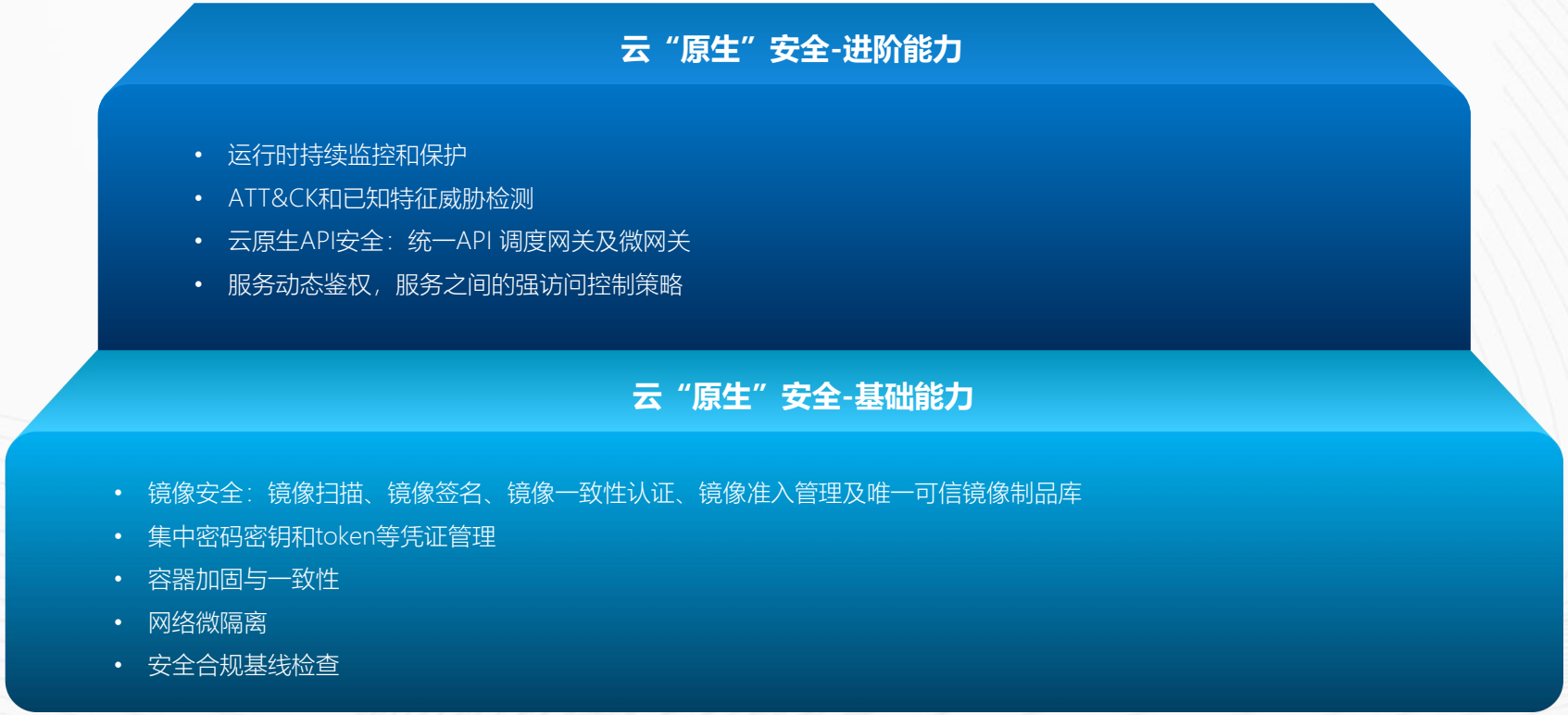
GOTC

云“原生”安全-基础能力

- 代码和镜像安全：镜像扫描、镜像签名、镜像一致性认证、镜像准入管理及唯一可信镜像制品库
- 集中密码密钥和token等凭证管理
- 容器加固与一致性
- 网络微隔离
- 安全合规基线检查

云“原生”安全需要具备的13大能力

GOTC



云“原生”安全需要具备的13大能力

GOTC

云“原生”安全需要具备的13大能力

GOTC

03

云“原生”安全最佳实践

探真云“原生”安全方案

GOTC

获得奖项

GOTC

- 探真科技凭借自身过硬的云原生安全技术实力、创新的技术理念以及丰富的实践经验，在云原生安全领域屡获殊荣。

CLOUD NATIVE COMPUTING FOUNDATION

探真科技入选CNCF Landscape
荣获CNCF推荐的**国产云原生安全厂商。**

极狐 GITLAB

探真科技
入选开源GitOps产业联盟

HARBOR

探真科技出品的镜像安全扫描器
荣获HARBOR官方认证

HICOOL

探真科技
荣获Hicool全球创业大赛优胜奖

腾讯云原生加速器
Tencent Cloud Native Accelerator

探真科技
入选腾讯云原生加速器30强

人才创新创业大赛
ovation and Entrepreneurship Competition

探真科技荣获
中国-南宁 2020海（境）外人才创新创业大赛三等奖
中国-南京 2021海（境）外人才创新创业大赛一等奖

GOTC

微信搜索“探真科技”关注我们

获取最新云原生安全情报

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

探真科技 TensorSecurity