CAICT 中国信通院　中国通信标准化协会 China Communications Standards Association

云原生成熟度模型集成方案介绍

郑剑锋
中国信息通信研究院 云计算与大数据研究所 工程师
2021年7月27日

2021 可信云大会
2021 TRUSTED CLOUD SUMMIT
数字裂变　可信发展

目录

CONTENTS

01 云原生安全工作综述

PART ONE

云原生安全工作概述

云原生安全工作组成立

2020.10，云原生产业大会（2020年）

首批成员单位：中国信通院、阿里云、华为云、腾讯云、奇安信、绿盟、深信服、青藤云

《云原生能力成熟度模型 第3部分：架构安全》标准

2020.4，启动；

2020.5.6，TC1WG5第10次会议，立项

2021.4.26，TC1WG5第16次会议，征求意见

2021.5.18， 工信部科技司立项

《基于容器的平台安全能力要求》标准

2019.8，启动；

2019.10.10，TC1WG5第8次会议，立项；

2019.11.19，TC1WG5第9次会议，征求意见；

2020.5.18， TC1WG5第11次会议，征求意见；

2020.11.23， TC1WG5第14次会议，送审；

2021.5.6，**报批。**

《云原生架构安全白皮书（2021年）》

2020.10，启动；

期间召开5次研讨会，共形成6稿；

阿里云、华为云、腾讯云、百度、小佑科技、青藤云、绿盟、奇安信、中国移动等18家企业参与；

2021.5.26云原生产业大会，**发布。**

02 云原生安全成熟度模型

PART TWO

云原生技术架构及应用模式变化，带来全新安全隐患

API

API爆发式增长
增加滥用风险

Serverless

Serverless计算模型和平台呈
现新型安全威胁

微服务

服务细粒度切分和东西向流量
显著增加引入应用风险

研发运营工具链

DevOps模式提升研运流程和
安全管理防范难度

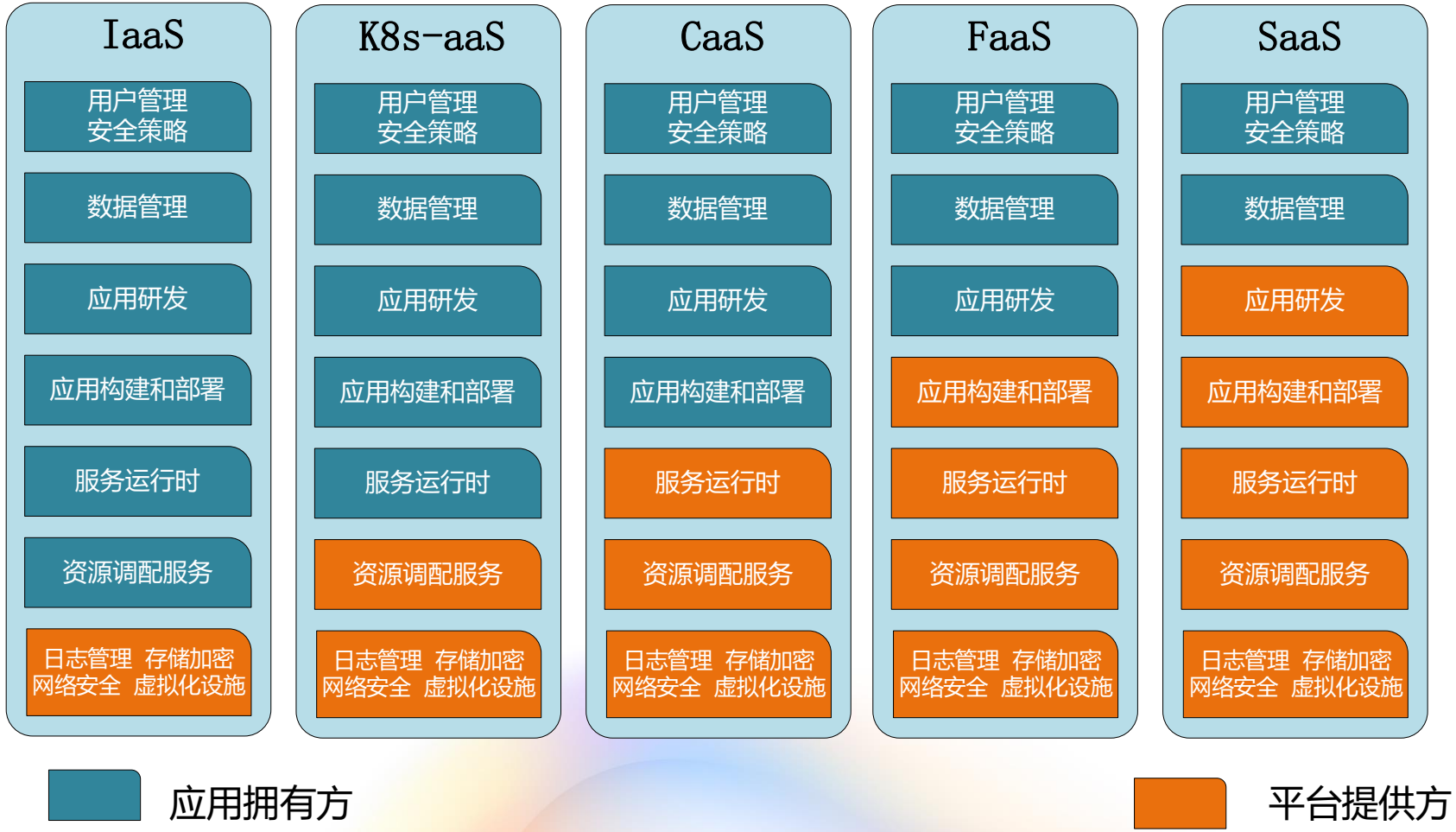
云原生计算环境

容器的构建、部署和运行过程中
产生多种安全风险

云原生的安全风险包含**云原生基础设施自身的安全风险**，以及**上层应用云原生化改造后新增和扩大的安全风险**。
云原生基础设施包括以容器为主的云原生计算环境、DevOps工具链；云原生化应用主要包括微服务、Serverless、以及显著扩大的API应用规模。

云原生安全防护范围及责任划分

云原生安全所保护的对象，是指以**容器**技术为基础底座，以**DevOps、面向服务**等云原生理念进行开发，并以**微服务**等云原生架构构建的业务系统所共同组成的信息系统。



容器服务、Service Mesh与Serverless等均属于云原生范畴。

不同服务模式，具有不同的责任模型，各自关注不同的防护重点。

云原生安全遵循的设计原则

零信任

假设环境中随时存在攻击者，不能存在任何的隐形信任。

通过细粒度拆分构建微边界的架构模型，并通过执行策略限制消除数据、资产、应用程序和服务的隐式信任。

安全左移

在云原生安全建设初期将安全投资更多地放到开发安全，包括安全编码、供应链（软件库、开源软件）安全、镜像及镜像仓库安全等。

持续监控和响应

转被动为主动，持续监控尽可能多的云原生环境，如网络活动层、端点层、系统交互层等；

同时应建立持续响应的防护机制，对攻击进行迅速分析和处理，并建立数据收集池进行溯源追踪，发现系统中的安全缺陷。

工作负载可观测

运用可视化工具发现和记录容器快速变化的应用行为，清晰地观察微服务和中间件调用关系。

为自动化的安全检测提供详细准确的运行状态数据，为自动化的云原生安全提供充足的决策依据。

云原生安全防护体系

传统安全

防护边界为物理机

主要以MAC/IP为标识

云安全

防护边界为虚拟机

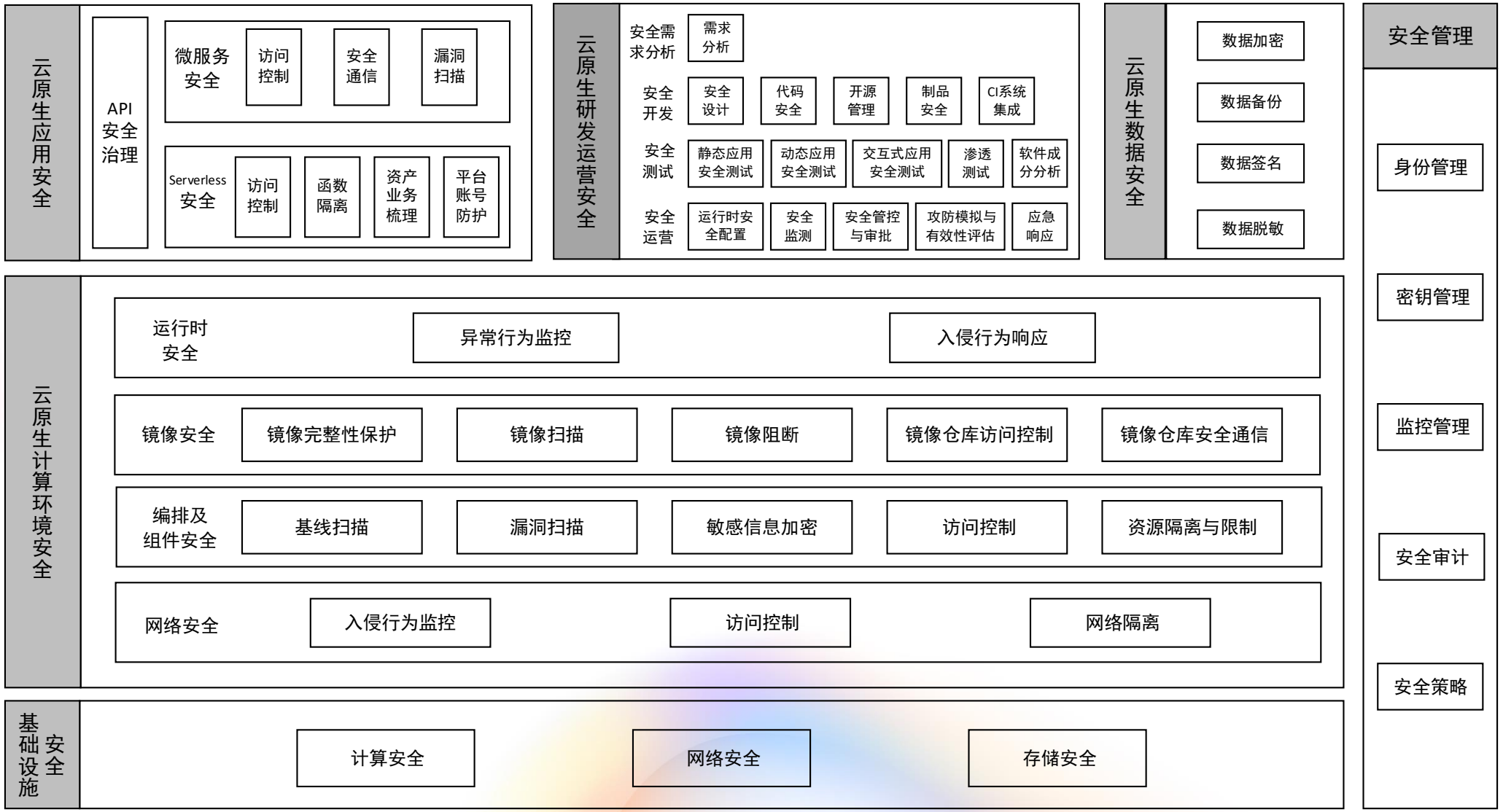
主要以IP为标识

云原生安全

防护边界为服务或应用

主要以标签为标识

云原生安全防护体系


云原生应用安全
API安全治理
微服务安全
访问控制
安全通信
漏洞扫描
Serverless安全
访问控制
函数隔离
资产业务梳理
平台账号防护
云原生研发运营安全
安全需求分析
需求分析
安全开发
安全设计
代码安全
开源管理
制品安全
CI系统集成
安全测试
静态应用安全测试
动态应用安全测试
交互式应用安全测试
渗透测试
软件成分分析
安全运营
运行时安全配置
安全监测
安全管控与审批
攻防模拟与有效性评估
应急响应
云原生数据安全
数据加密
数据备份
数据签名
数据脱敏
安全管理
身份管理
密钥管理
监控管理
安全审计
安全策略
云原生计算环境安全
运行时安全
异常行为监控
入侵行为响应
镜像安全
镜像完整性保护
镜像扫描
镜像阻断
镜像仓库访问控制
镜像仓库安全通信
编排及组件安全
基线扫描
漏洞扫描
敏感信息加密
访问控制
资源隔离与限制
网络安全
入侵行为监控
访问控制
网络隔离
基础设施安全
计算安全
网络安全
存储安全

云原生安全成熟度模型

第5级（卓越级）：具备**超前的**云原生安全防护能力，具备**自我提高和引领级**的云原生安全防护体系，有**丰富的项目经验**；能够对云原生恶意攻击行为进行**预先研究和预判告警**，具备**自动化监测**和**威胁自愈**能力。

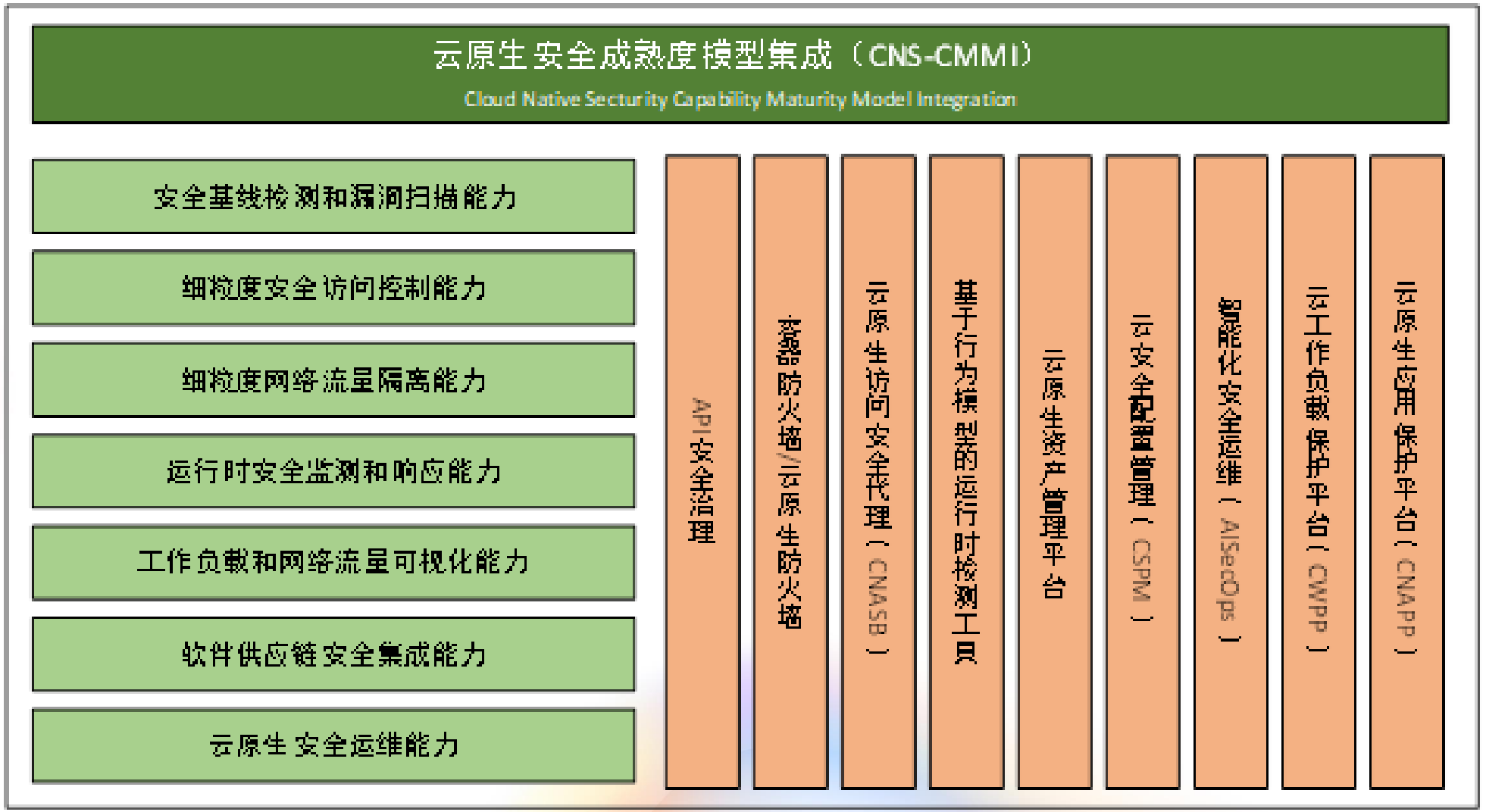
第4级（先进级）：具备**完备的全链条**云原生安全防护能力，具备系统级云原生安全防护体系，有**较丰富的项目经验**；能够防护拥有**较丰富资源**的威胁发起的恶意攻击，能够**及时发现、检测较完备的攻击行为**，并采用自动化手段做出应对。

第3级（成熟级/系统级）：具备**较完整**的云原生安全防护能力，具备**多个模块和部分系统级**云原生安全防护体系，有**多个项目经验**；能够防护拥有**一定量资源**的威胁发起的恶意攻击，能够**发现、检测常见的攻击行为**并做出应对。

第2级（基础级/模块级）：具备**基础级**云原生安全防护能力、具备**模块级**的云原生安全防护体系；能够防护拥有**少量资源**的威胁发起的恶意攻击，并对**部分攻击行为**做出应对。

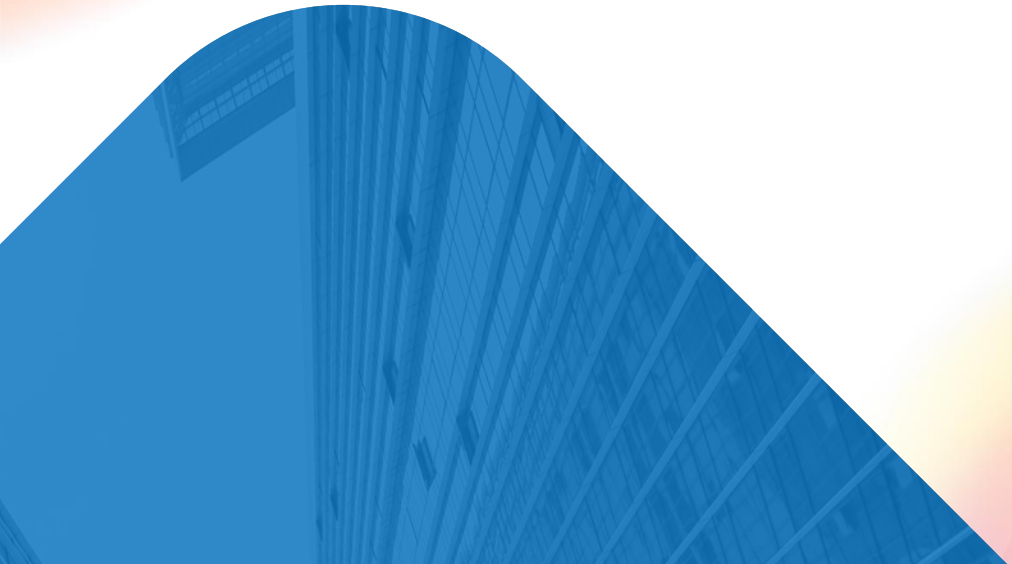
第1级（零级/概念级）：具备传统云平台安全技术能力，具备**概念级**的云原生安全防护能力；

云原生安全成熟度模型集成框架



03 工作展望

PART THREE



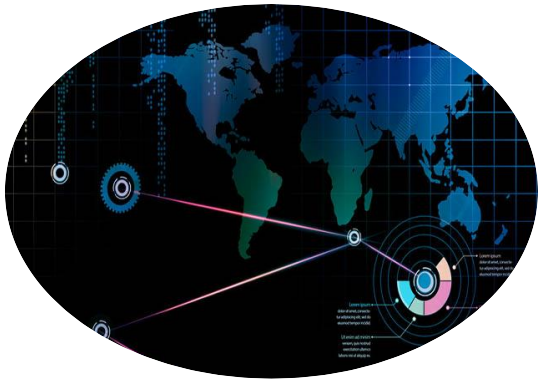
共创共享 共筑生态

技术沙龙

云原生安全大讲堂

行业合作

深入发掘行业安全需求



攻防平台

成立云原生安全实验室

THANKS!

2021
TRUSTED CLOUD
SUMMIT