云原生安全能力成熟度模型研究

Research on Cloud Native Security Capability Maturity Model

杜　岚[1]，鲁华伟[2]，韩　浩[2]，仇保琪[1]（1. 中国信息通信研究院，北京 100083；2. 联通数字科技有限公司，北京 100037）
Du Lan[1]，Lu Huawei[2]，Han Hao[2]，Qiu Baoqi[1]（1. China Academy of Information and Communications Technology，Beijing 100083，China；2. Unicom Digital Technology Co.，Ltd.，Beijing 100037，China）

摘　要：
构建云原生安全能力成熟度模型，旨在为电信运营商提供一个精准评估和持续增强云原生安全实践的方法论。该模型采用多维度评估方法，结合行业最佳实践和组织战略需求，综合考量了基础设施安全、云原生基础架构安全、应用安全、研发运营安全和安全运维5个关键领域，定义了5个成熟度等级，并制定了详细的评价指标和实施策略。通过该模型，运营商能够全面评估其云原生安全水平，识别安全短板，并制定相应的改进措施。

关键词：
云原生；云原生安全；云原生安全能力成熟度模型
doi：10.12045/j.issn.1007-3043.2024.08.018
文章编号：1007-3043（2024）08-0087-06
中图分类号：TP393
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
The cloud native security capability maturity model（CNMM-S）is designed to assess and enhance the cloud-native security practices of telecom operators. This model adopts a multidimensional evaluation method，combined with industry best practices and organizational strategic needs，comprehensively considers five key areas：infrastructure security，cloud-native infrastructure security，application security，DevSecOps and security operations. It defines five maturity levels and develops detailed evaluation indicators and implementation strategies. Through this model，operators can comprehensively evaluate their cloud native security level，identify security weaknesses，and develop corresponding improvement measures.

Keywords：
Cloud native；Cloud native security；Cloud native security capability maturity model（CNMM-S）

引用格式：杜岚，鲁华伟，韩浩，等. 云原生安全能力成熟度模型研究[J]. 邮电设计技术，2024（8）：87-92.

0 引言

党的二十大报告强调要构建现代化基础设施体系，云计算作为新型基础设施，成为提升企业竞争力的关键。企业加速上云、用云，使得云计算的技术内核逐步从服务化资源交付转向云原生化价值赋能。在此背景下，电信运营商坚持构建领先的信息基础设施，积极开展云原生平台建设和现代化改造，在助力内部数智化转型的同时，充分发挥云原生平台服务优势，赋能政务、国资企业等重要行业。然而，云原生技术栈的延展突破了传统的云安全防护体系，为适应云原生环境下多变的安全风险与挑战，电信运营商在开展数智化建设的同时也需高度重视云原生安全，同步开展云原生安全体系建设。

相较于传统安全防护，云原生安全防护更加复杂，目前尚无体系性综合评价云原生安全能力成熟度的方法模型。因此，电信运营商构建科学有效的云原生安全能力成熟度评价体系是亟待解决的关键问题，也是推动企业数字化转型的重要基础。云原生安全能力成熟度评价体系研究，以“保障业务安全运行、确保数字化转型安全”为总体目标，紧扣十四五信息化建设政策目标和企业发展战略，通过构建模型、定位现状、问题分析和改进升级等方法，助力企业云原生安全建设，确保企业数字化转型工作安全推进[1]。

收稿日期：2024-07-03

1 运营商云原生安全能力成熟度评价的价值

目前，电信运营商数字化转型中的云原生安全能力成熟度模型和指标体系均缺失，没有相关的技术和评估方法。因此，以云原生安全能力成熟度模型研究为抓手，开展云原生安全能力成熟度评价，是电信运营商等重点行业的关键问题。其价值体现在以下几个方面。

a）多维度把脉，准确定位企业建设水平。全面了解现有安全防护水平是开展安全建设的第一步。云原生安全成熟度模型从云基础设施、云原生基础架构、应用系统、研发运营流程、安全运维等多个维度对组织的云原生安全水平进行综合度量，深入分析、精准评估组织云原生安全建设的现状，为组织制定针对性的安全策略提供事实支撑。

b）差异化分析，详细诊断企业建设短板。全面评估后，需要找出组织在云原生安全建设中存在的潜在问题。依据云原生安全能力成熟度模型中的指标要求，通过全方位的差距分析，组织可以直观识别当前云原生安全建设的不足和缺失。

c）定制化提升，明确输出企业未来改进方向和计划。云原生安全建设是持续演进和优化的。在对组织云原生安全建设现有水平、存在问题进行诊断后，可对标模型中的高阶能力，针对性制定组织下一步的云原生安全能力改进方向和实施计划，保证云原生安全建设水平持续适应组织需求[2-4]。

2 云原生安全能力成熟度模型构建

2.1 构建思路

以“保障业务安全运行、确保数字化转型安全”为总体目标，紧密结合行业最佳实践和组织战略需求，构建云原生安全能力成熟度模型（Cloud Native Capability Maturity Model-Security，CNMM-S）。模型构建思路如下。

a）确定目标与范围。

（a）明确目标。模型是一种用于评估和提升组织在云原生环境中进行安全实践能力的框架，应兼具安全合规、可度量、可操作和可扩展等特性。

（b）界定范围。模型应全面覆盖云原生环境中的所有关键安全领域，包括基础设施、云原生基础架构、云原生应用、云原生研发运营与云原生安全运维5个安全域。

b）融合先进理念。

（a）零信任。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，从而降低网络威胁横向扩散的可能性。

（b）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、集成安全测试和审查、自动化安全扫描、提升开发人员安全意识等方面。

（c）持续监测与响应。持续监控云原生环境，建立持续响应的防护机制，快速分析和处理攻击，制定事件快速响应流程。

（d）可观测性。应用云原生细粒度的可观测能力，通过指标和仪表板发现和记录工作负载快速变化的应用行为，观察微服务和中间件的调用关系，为自动化的安全检测提供详细准确的运行状态数据。

c）制定评估标准。

（a）级别划分。为不同安全领域定义从基础到高级的成熟度级别。

（b）评估标准。制定每个级别的具体评估标准和指标。

d）反馈与持续改进。

（a）反馈机制。设计反馈机制，允许组织根据经验调整优化模型。

（b）持续更新。定期更新模型以适应新的安全挑战和技术发展。

e）工具与自动化。

（a）工具。推荐通过工具来支持模型评估的实施，同时也允许组织选择适合的工具。

（b）自动化。应鼓励企业使用自动化工具和流程提升安全性和效率。

2.2 云原生安全能力成熟度等级划分

云原生安全能力成熟度模型共划分为5级，从1级到5级云原生安全能力水平逐级递增，达到高级别需同时满足低级别全部的能力要求，其具体定义如图1所示。

2.3 云原生安全能力成熟度评价指标体系

云原生安全成熟度评价指标体系从基础设施、云原生基础架构、云原生应用、云原生研发运营与云原生安全运维5个能力域对组织的云原生安全能力水平进行量化评价。评价指标分为4级，共包含5个一级指标（对应5个能力域），15个二级指标（对应15个能力子项），46个三级指标（对应46个实践项），419个四

级别	英文	中文	定义
1级	Initial Level	初始级	具备概念级的云原生安全防护能力，基于安全的架构设计及云原生平台自身的安全机制
2级	Fundamental Level	基础级	具备基础的云原生安全防护能力，具备模块级的云原生安全防护体系；能够防御拥有少量资源的威胁源发起的恶意攻击，能够发现重要的安全漏洞和处置安全事件
3级	Comprehensive Level	全面级	具备较完整的云原生安全防护能力，具备多个模块和单系统级云原生安全防护体系；能够防御拥有一定量资源的威胁源发起的恶意攻击，能够及时发现、监测攻击行为和处置安全事件
4级	Excellent Level	优秀级	具备体系化的云原生安全防护能力，具备多个系统联动的云原生安全防护体系；能够防御拥有较丰富资源的威胁发起的恶意攻击，能够及时发现、监测攻击行为，并可通过自动化手段处置安全事件
5级	Fabulous Level	卓越级	具备超前的云原生安全防护能力，具备智能化的云原生安全防护体系；能够对云原生恶意攻击行为进行预判告警，具备自动化监测和威胁自愈能力

图1　云原生安全能力成熟度等级定义

级指标（对应5个等级共计419项能力要求）。前三级指标体系如图2所示[5-8]。

2.3.1 基础设施安全域

基础设施安全域是指承载云原生架构的底层云基础设施的安全，包括计算安全、网络安全和存储安全，评估指标结合了等保2.0中云安全的要求[9]（见图3）。

2.3.2 云原生基础架构安全域

云原生基础架构安全域是指以容器为核心的云原生PaaS平台安全，包括云原生网络安全、编排及组件安全、镜像安全及容器运行时安全[10-14]（见图4）。

2.3.3 云原生应用安全域

云原生应用安全域是指云原生PaaS平台上部署的应用安全，应用形态以微服务、Serverless应用为代表。各级核心能力要求如图5所示。

2.3.4 云原生研发运营安全域

云原生研发运营安全指结合人员管理体系、制度流程，在应用设计研发阶段便引入安全措施，实现安全左移，包括安全需求、开发安全和测试安全3方面的能力要求[15]（见图6）。

2.3.5 云原生安全运维域

云原生安全运维域是指对云原生平台与应用各层级对象进行统一的安全管理，以及全局覆盖和多点联动的安全运营能力，包括安全管理和安全运营2个

云原生安全成熟度模型															
能力域	基础设施安全域			云原生基础架构安全域				云原生应用安全域			云原生研发运营安全域			云原生安全运维	
能力子项	计算安全	网络安全	存储安全	云原生网络安全	编排及组件安全	镜像安全	运行时安全	微服务安全	无服务器安全	通用安全	安全需求	开发安全	测试安全	安全管理	安全运营
实践项	资源隔离	访问控制	数据保护	访问控制	访问控制	镜像仓库管理	容器运行时检测	容器资源隔离限制	无服务器安全	访问控制	安全需求分析	安全设计	渗透测试	资产管理	监测预警
	访问控制	安全通信	数据备份恢复	安全通信	集群组件安全加固	镜像扫描	安全策略管理			安全通信		代码安全	软件成分分析	安全审计	响应处置
	安全加固	网络攻击防护	剩余信息保护	网络攻击防护	敏感信息保护		容器数据信息加密			API安全				策略管理	溯源分析
	攻击防护						容器资源隔离限制			攻击防护				身份管理	情报管理
														密码管理	

图2　云原生安全成熟度评估指标体系

能力子项 / 等级	计算安全	网络安全	存储安全
L1	计算资源隔离	云基础设施管理流量和业务流量分离	限制平台管理员访问用户业务数据
L2	多租户计算资源管理和隔离；基于用户角色的访问控制；云主机系统软件漏洞扫描；云主机安全配置基线检测；云主机入侵检测	多租户网络隔离；ACL资源访问控制；网络安全组设置；通信传输、边界防护、入侵防范等安全机制	租户间数据隔离；数据存储备份和恢复与完整性校验；虚拟机回收时内存和存储空间完全清除；业务应用数据删除时对应删除云存储中所有副本
L3	漏洞扫描结果分析与修复方案建议；基线检测结果分析与修复方案建议；入侵行为告警和处置建议	网络安全策略设置；VPN加密通信	身份鉴别信息加密存储；备份策略设置
L4	强身份鉴别措施；威胁评级；自动修复；智能化异常行为检测；入侵行为自动处置；处理情况跟踪	安全策略合规审计、潜在风险检测；云内资源的主动外联网络侧检测与阻断；智能化异常流量检测与防护	异地备份与恢复；主备备份；云盘加密
L5	云主机自动安全加固和攻击防护	0day、高级可持续威胁攻击防护；攻击防护能力自适应优化	数据操作行为的异常检测；实时动态数据屏蔽

图3　基础设施安全域各等级核心能力要求

能力子项 / 等级	云原生网络安全	编排及组件安全	镜像安全	运行时安全
L1	网络架构业务与管理分离	编排组件访问控制	镜像集中管理	容器健康状态监测；资源隔离与使用限制
L2	容器外网访问限制；四层网络流量限制	安全基线扫描；安全漏洞扫描及修复；敏感信息加密；集群组件安全通信	批量化镜像漏洞扫描与修复建议；镜像仓库脆弱性检测与修复；镜像仓库访问控制；镜像传输加密	特权容器与特权行为限制；基于白名单的容器内程序运行控制；容器存储数据全盘加密
L3	七层网络流量限制；容器网络拓扑和流量可视化；攻击阻断	限制外网访问容器编排组件；敏感信息托管保护；集群共享存储内容加密	镜像推拉限制；镜像扫描策略设置；镜像内部配置及恶意程序扫描	容器内恶意文件、异常进程、高危行为、逃逸攻击检测；容器级别攻击阻断
L4	流量加密；流量审计和流量镜像能力；微隔离的自动生成与告警；自动化攻击阻断	集群编排组件的攻击检测和阻断；安全事件审计	DevOps流程中自动化镜像扫描；分阶段匹配处置手段；镜像风险评估及处置建议策略；风险镜像跟踪	基于行为分析的容器内异常行为检测；容器内资源级别的攻击阻断；自动化攻击阻断能力；安全容器
L5	全流量威胁检测和智能阻断	集群组件智能安全加固	环境自适应智能化漏洞威胁排序；基于漏洞风险排序结果自动加固	基于可信执行环境的数据保护；实时自动化、多级联动的威胁响应能力

图4　云原生基础架构安全域各等级核心能力要求

部分的能力要求，其各级核心能力要求如图7所示。

2.4 云原生安全建设阶段及对应等级

不同企业云原生安全建设阶段不同，所对应的云原生安全成熟度模型等级不同，其成熟度级别建议如图8所示。

3 云原生安全能力成熟度评价实施策略

云原生安全建设需要持续以“保障业务安全运行、确保数字化转型安全”为目标，通过打造云原生安全能力成熟度模型并实现测试、迭代复盘，实现企业云原生安全建设。

a）确定评价对象。结合电信运营商建设现状确定评价对象和范围。基础设施安全和基础架构安全分别面向IaaS和PaaS安全，可选择电信运营商公有云平台、私有云平台或分公司的自建平台分别进行评价；应用安全是面向某个具体云原生应用开展评价的，其中，可根据实际应用形态选择是否评价无服务器安全；研发运营安全是面向企业内部的研发运营流程开展评价的，若组织存在多条机制不同的研发运营线，每种机制应独立评价。

b）准备验证环境。尽量在生产环境中开展验证，部分安全模拟攻击验证或对业务连续性有较大影响，

能力子项 / 等级	通用安全	微服务安全	无服务器安全
L1	用户、服务访问控制	微服务高可用	用户权限控制
L2	基于角色的访问控制；API识别、监测与脆弱性扫描；南北向通信的机密性、完整性保护；南北向Web应用攻击防护	访问控制策略统一管理	函数隔离；函数权限控制
L3	内部应用间细粒度的访问控制；API异常行为检测与响应；东西向通信的机密性、完整性保护；南北向流量分析与异常拦截	服务降级与隔离；微服务组件安全扫描及修复建议	资源监控及告警；滥用攻击检测
L4	应用微隔离策略；东西向应用攻击防护；东西向流量分析与异常拦截；基于行为分析的API异常行为检测与响应	服务拓扑可视化；异常行为检测与响应	资产业务逻辑梳理；异常行为检测与响应
L5	智能化攻击检测与响应	微服务组件的自适应安全加固；智能化攻击检测与响应	智能化攻击检测与响应

图5　云原生应用安全域各等级核心能力要求

能力子项 / 等级	安全需求	开发安全	测试安全
L1	安全基本需求清单；产品基本安全能力需求	开源软件使用规范；项目级安全编码规范；安全设计规范	手动安全测试
L2	更全面的需求清单；有相应的安全测试用例；针对应用场景特点制定安全需求与用例	制品安全检查；开源组件自动化安全扫描；团队级安全编码规范；安全功能标准化设计	明确的安全测试要求与测试用例；安全测试和合规扫描
L3	安全需求与其他功能性需求同步开展测试；安全需求包括功能性需求和非功能性需求	制品可追溯性；建立标准化、安全的技术栈；在安全设计中进行威胁建模分析	安全测试流程和规范；端到端的测试工具链；流水线自动集成安全测试、生成测试结果
L4	自动化安全需求管理平台	制品自动化检查、清点；插件自动化安全检测能力；支持标准化的安全功能组件	人工渗透测试流程
L5	智能化安全需求管理平台 安全需求自动化验证能力	开源组件修复；编码工具安全问题自动化识别和修复；智能化威胁建模并输出安全设计方案	安全测试智能化并内嵌到开发与交付过程

图6　云原生研发运营安全域各等级核心能力要求

该部分的验证可在与生产环境架构相同的测试环境中进行。

c）开展实地验证。基于云原生安全能力成熟度评价指标体系与配套测试工具开展实地技术验证，对于各域中的指标，若不需要结合实际业务分析进行验证，则为参考性指标，否则为非参考性指标，非参考性指标需全部开展验证。

d）分域等级评估。对验证结果进行等级评估，各能力域的计分和分级方法为：统计非参考性指标通过符合性验证的数量，若L1~L(x−1)各级中的非参考性指标全部验证通过，且Lx中非参考性指标验证通过率大于等于90%，则该评价对象的该能力域定级为Lx。

e）专家技术评审。组织行业专家成立评审专家小组，审查企业云原生安全防护体系、云原生安全能力成熟度评价结果，形成最终评级和整改意见。

f）优化与改进。基于评价结果，对标企业安全目标和成熟度高阶能力指标，形成差异化分析报告，并给出改进方案，指导企业制定云原生安全能力提升计划，持续迭代、复盘、验证。

4　结束语

随着电信运营商数智化转型的不断深入，云原生安全的重要性日益凸显。云原生安全能力成熟度模型为电信运营商提供了一个全面的安全评估框架，通

能力子项 / 等级	安全管理	安全运营
L1	节点、容器级资产可视化	独立监测；手动处置
L2	云原生多层级资源可视化与查询；云原生平台日志采集和安全审计	统一监测；多设备联动的威胁响应；人工溯源分析；漏洞、IOC情报实时获取
L3	日志分析、安全行为审计；应用开发测试阶段策略统一配置管理；容器安全策略统一配置管理；网络安全策略统一配置管理	监测及处置进展可视化；安全事件情报自动化获取；情报处置
L4	网络拓扑可视化；服务访问关系可视化；资产的关联显示与查询；多账号统一身份管理与访问控制；身份滥用和异常身份操作监控告警；支持第三方密码管理系统	基于威胁情报的实时威胁检测与告警；智能化威胁检测能力；基于预设策略的自动响应能力；攻击路径自动化构建
L5	混合多云资产实时识别、关联关系智能化分析；研发运营全流程自动化安全审计	攻击诱捕；攻击者画像、定位、部分攻击反制；情报自主发现和分析预警

图7　云原生安全运维域安全域各等级核心能力要求

过云原生安全能力成熟度评价，电信运营商能够更准确地评估自身的安全建设水平，识别和弥补安全短板，制定并实施针对性的提升计划。这不仅有助于提升运营商自身的安全防护能力，也为其他行业的数字化转型提供了宝贵的参考和借鉴。展望未来，面对云原生技术的快速迭代和安全威胁的动态变化，该模型将持续迭代优化，以更好地应对新兴的安全挑战。同时，为了保持在数智化转型进程中的领先地位，电信运营商应不断强化安全人才的培育和技术制度的创新，确保其数智化道路安全稳健且可持续。

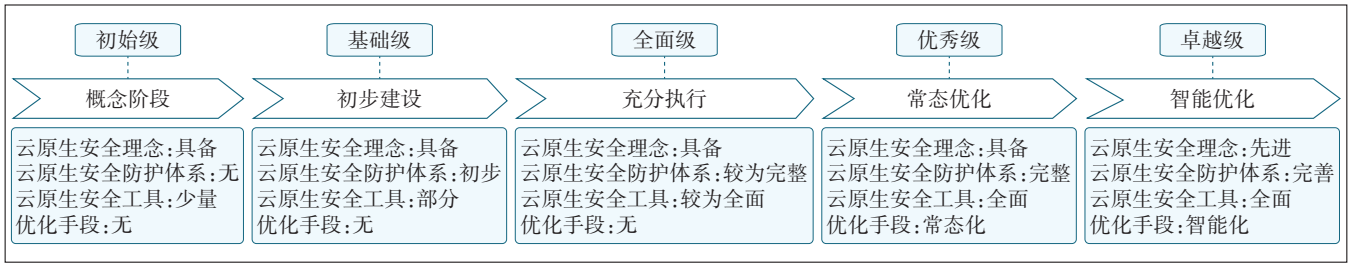

图8　不同阶段企业对应等级建议

参考文献：

[1] 云原生产业联盟．云原生架构安全白皮书（2021年）[R/OL]．[2024-01-24]．https://www.dosec.cn/newsn_detail/c-_detailId%3D1722104557822087168.html.
[2] 彭雨，葛玥，付钰，等．电信运营商信创化转型成熟度评价研究[J]．邮电设计技术，2024(3)：16-19.
[3] 中国信息通信研究院．电信业数字化转型发展白皮书（2022年）[R/OL]．[2024-01-24]．http://www.caict.ac.cn/english/research/whitepapers/202303/P020230316597689609032.pdf.
[4] 赵占纯，范琨，耿岩，等．电信运营商网络数智化转型思考[J]．邮电设计技术，2024(3)：7-11.
[5] 云原生能力成熟度模型 第3部分：架构安全：Q/KXY CT003-2022[S]．北京：云计算开源产业联盟，2022：4-25.
[6] Cloud Native Computing Foundation. Cloud native security whitepaper [R/OL]．[2024-01-24]．https://www.cncf.io/reports/cloud-native-security-whitepaper/.
[7] 李天萁．基于云原生的安全防护策略研究[J]．网络安全技术与应用，2024(1)：81-83.
[8] 朱萍．云原生信息安全风险及其防范研究[J]．网络安全技术与应用，2024(3)：60-61.
[9] 国家市场监督管理总局，国家标准化管理委员会．信息安全技术网络安全等级保护基本要求：GB/T 22239-2019[S]．北京：中国标准出版社，2019.
[10] 刘军，李雄清，孙琼巍，等．云原生系统的性能测试技术研究与实践[J]．信息技术，2024(3)：75-82.
[11] 丁攀，徐雷，刘安，等．容器镜像存储原理及其安全风险研究[J]．邮电设计技术，2022(9)：82-87.
[12] 王剑楠．云原生安全风险分析与对策探讨[J]．网络安全技术与应用，2024(1)：79-81.
[13] MILLS A，WHITE J，LEGG P. Longitudinal risk-based security assessment of docker software container images[J]．Computers & Security，2023(135)：103478.
[14] TYSON M. Continuous integration with Docker and Jenkins[EB/OL]．[2024-01-24]．https://www.infoworld.com/article/2270388/continuous-integration-with-docker-and-jenkins.html.
[15] 李亮．云原生应用开发与部署面临的挑战及其应对方案[J]．软件工程，2024，27(1)：6-9.

作者简介：
杜岚，毕业于北京大学，工程师，硕士，主要从事云原生与云原生安全领域的技术产业研究、标准制定、行业咨询等工作；鲁华伟，毕业于郑州大学，联通数科科技有限公司安全事业部应用安全产品部总经理，高级工程师，学士，主要从事数据通信咨询与设计、IP网络规划、网络空间安全等相关工作；韩浩，毕业于北京大学，工程师，博士，主要从事网络空间安全、密码安全、量子安全等相关工作；仇保琪，毕业于北京理工大学，助理工程师，硕士，主要从事云原生安全领域的技术产业研究、标准制定、行业咨询等工作。