智算时代云安全威胁态势分析与防御机制研究

祁会波[1] 陈龙[2]

1 中国移动通信集团甘肃有限公司，甘肃省兰州市，730000；

2 杭州迪普科技股份有限公司，甘肃省兰州市，730000；

摘要：随着云计算向智能化演进（云计算 3.0 时代），云环境面临更复杂、动态化的安全威胁，亟需构建深度融合智能技术的防御体系。云中存储的敏感数据因配置错误、API 漏洞或内部威胁导致泄露，攻击者可窃取用户隐私或商业机密。云安全威胁是攻击者通过技术或非技术手段，针对云环境弱点发起的、可能造成实际损害的行为集合。

关键词：智算时代；云安全；威胁态势分析；防御机制

DOI：10.69979/3041-0673.26.01.014

安全运营中心（SOC）引入 AI 智能体，实现威胁预测与自动化处置。中国通信标准化协会已推动 20 余项云智算安全标准，覆盖零信任、AI 物料清单等技术。基于云原生特性设计自愈系统，硬件故障时无缝迁移业务负载。云安全需持续协同技术创新（如安全大模型）、政策规范及跨企业联防联控，方可应对智算时代动态化威胁。

1 云安全威胁定义

1.1 定义要点

攻击载体性质，威胁是攻击者利用漏洞实施的主动破坏行为，如数据窃取、服务瘫痪等恶意活动。区别于“风险”（漏洞被利用的可能性）和“挑战”（实施防护的障碍）。典型破坏目标，机密性：未经授权访问敏感数据（如用户隐私、商业机密）；完整性：篡改云存储或传输中的数据；可用性：通过 DDoS 攻击等使云服务不可用。关键攻击场景，利用配置错误或 API 漏洞入侵云环境；通过账户劫持、恶意软件或内部威胁突破访问控制；针对容器、微服务等云原生组件的供应链攻击。

1.2 威胁成因关联

云安全威胁的产生通常与漏洞利用直接相关：技术漏洞（如系统缺陷）、管理漏洞（如权限配置错误）或流程漏洞（如变更控制不足），被攻击者利用形成实质性威胁。云安全威胁是攻击者通过技术或非技术手段，针对云环境弱点发起的、可能造成实际损害的行为集合。

2 云安全威胁的类型

核心威胁类型。数据泄露与盗窃，敏感数据因配置错误（如公开存储桶）、API 漏洞或内部失误暴露于未授权访问。攻击者可窃取用户隐私、商业机密等资产，账户劫持（身份盗窃），攻击者通过钓鱼攻击、弱密码爆破或密钥窃取控制合法账户，劫持后可能操控云资源、窃取数据或发起进一步攻击。服务中断攻击，DDoS 攻击：淹没云服务带宽致业务瘫痪，勒索软件：加密关键数据勒索赎金（如 LockBit 3.0），配置错误与变更失控，权限设置不当（如过度授权）、网络配置疏漏导致攻击面扩大，动态云环境中缺乏自动化审计工具加剧风险，内部威胁，员工恶意操作（数据窃取）、疏忽（误删数据）或第三方供应商滥用权限。恶意软件渗透，勒索软件、木马通过云存储或共享服务传播，破坏数据完整性，供应链攻击，污染容器镜像、第三方库植入后门代码，实现云环境横向渗透，共享技术漏洞，虚拟化层等底层缺陷突破多租户隔离机制（如 CVE-2019-11270 提权漏洞），云环境威胁本质是技术漏洞（系统缺陷）、管理漏洞（权限配置错误）与流程漏洞（变更控制不足）被攻击者利用的产物。

3 云安全防御机制研究

3.1 多因素身份验证在云安全中的应用

多因素身份验证（MFA）通过结合多种认证方式（如密码、生物识别或动态令牌）强化用户身份验证，在云安全中扮演核心防护角色。其核心应用场景包括：登录二次认证：用户完成密码登录后，云平台自动发起额外验证（如短信码、移动应用令牌），防止账户劫持和数据泄露风险。例如，Cloudflare 可通过移动应用验证器实现双因素身份验证流程。敏感操作验证：用户执行高

风险操作（如删除云资源或变更配置）时，系统触发二次认证（如人脸识别或硬件密钥），实时阻断非法访问。实施 MFA 面临挑战，包括部署复杂度高（需整合多系统）和用户培训成本（部分用户抵触额外验证步骤）。为应对这些挑战，云环境采用以下革新方案：云原生 MFA 与 IAM 集成：基于身份目录即服务（DaaS）的云 MFA 方案，支持动态令牌（如 Google Authenticator）和跨平台统一管理，简化企业级部署。智能自适应风险评估：AI 分析用户行为（如打字节奏或设备指纹），动态调整认证策略——高风险操作自动触发多因素验证，提升防御深度伪造攻击的能力。

3.2 动态威胁情报云安全获取与更新

情报获取的多元化渠道，云端原生情报源，云厂商威胁情报平台（如阿里云 ThreatIntelligence 组件）提供实时 IP/域名/文件哈希的恶意性检测 API，支持自动化查询集成，云安全中心采集全球攻击链数据，形成针对云环境优化的威胁特征库（如异常登录行为模式库）。开源情报(OSINT)整合，抓取暗网论坛、黑客社区泄露的云凭据和漏洞交易信息，监控 GitHub 等代码托管平台中意外暴露的云服务密钥。商业情报订阅服务，采购专业威胁情报厂商的动态数据流（如 FortiGuard 的 APT 攻击指标），接入 ISAC（信息共享与分析中心）的行业级云威胁预警。云环境落地场景，策略自动化编排，将最新威胁指标（如恶意 IP 列表）实时同步至云防火墙策略引擎，自动阻断高危访问，基于情报动态调整容器安全策略（如检测到新漏洞时即时收缩权限）。攻击面持续监控，利用 CSPM 工具扫描云资源配置错误，关联威胁情报库评估风险等级，当情报显示新型勒索软件活跃时，自动启用云存储版本锁与异地备份。智能响应加速，SOAR 平台接收情报触发剧本：自动隔离被入侵云主机+重置 IAM 凭证，AI 辅助决策：结合威胁情报预测攻击路径，生成防御规则建议，当前云威胁情报体系正经历三重进化：从人工采集到 AI 驱动、从静态库到实时流、从单点防御到云网端协同。华为云安全云脑等平台已实现 70%威胁 1 分钟响应，印证动态情报的核心价值。

3.3 云环境应急响应机制建立

事前准备阶段，预案体系设计，制定分级响应预案：根据攻击类型（如勒索软件、DDoS）和影响范围（单实例/VPC 跨区域）划分事件等级，明确不同级别的处置流程与责任人。合规性融合：将《网络安全法》、GDPR 等法规要求嵌入预案，确保数据泄露通报、审计留痕等操作合法合规。资源预部署，工具链就绪：预置云原生取证工具（如 AWS CloudTrail 日志捕获）、隔离脚本及备份恢复系统；响应团队演练：定期开展红蓝对抗演习，模拟云环境 APT 攻击链的处置全流程。事中响应阶段，快速检测与确认，多源日志关联：通过 SIEM 平台聚合云平台操作日志、网络流量及容器行为数据，利用 AI 算法识别异常模式（如非常规 IAM 权限变更）；影响评估：定位受感染资源边界（实例/存储桶/数据库），判定数据泄露风险等级。攻击遏制与取证，动态隔离：自动触发安全组规则更新，隔离受控虚拟机/容器；冻结高危存储桶访问权限，阻断数据外传。证据保全：对受攻击云主机创建只读快照，保存内存及进程状态；采用区块链技术存证操作时间线，确保法律效力。威胁根除，清除持久化攻击组件（如 Webshell、挖矿程序），修补利用漏洞（如未授权 API 接口）；重置泄露的 IAM 凭证及 API 密钥，实施最小权限原则。事后恢复与改进，业务连续性保障，从隔离环境恢复数据：优先启用异地备份副本，验证数据完整性后逐步上线；服务灰度发布：按业务优先级分批重启云服务，避免二次故障。复盘优化机制，攻击溯源报告：分析入侵路径（如初始攻击向量→横向移动手法），输出 TTPs（战术、技术与过程）画像；防御加固：更新 WAF 规则拦截同类攻击模式；部署 CSPM 工具持续监控配置偏差（如开放端口、过度授权）。完善的云应急机制可使事件平均处置时间（MTTD）缩短 60%以上，需持续迭代预案并强化云平台与第三方安全工具的 API 级集成。

4 云环境弹性与恢复能力提升方法

4.1 弹性架构优化

混合伸缩策略，结合按需扩展与预留实例：根据业务负载预测预留基准资源，突发流量时自动扩容按需实例，平衡成本与性能需求（参考某电商案例：突发流量处理能力提升 2.3 倍，闲置成本降 18%），动态扩缩容：通过 Kubernetes HPA 监控 CPU/内存等指标自动调整实例数，确保高并发场景响应时间稳定（如金融支付系统峰值扩容至 300 实例，响应<200ms），跨区域容灾部署，多可用区同步：在异地部署相同业务集群，利用 VPC 跨区域路由实现故障秒级切换(阿里云方案支持 RPO<1 秒、

RTO<30 秒）。无状态设计：剥离会话数据至 Redis 等分布式存储，使业务实例可随时销毁重建，

4.2 智能备份与恢复

备份策略强化，分级备份机制：高频数据：每日增量备份（仅保存变化部分）减少存储压力，核心数据：每周全量备份+跨区域存储（如天翼云跨区域备份提升抗灾能力）。自动化验证：定期模拟恢复操作，检测备份数据完整性与可恢复性，故障恢复优化，冷迁移容灾：物理机故障时自动迁移云主机至健康节点（需配合云硬盘备份保障数据一致性），并行恢复技术：加速备份读取过程，缩短业务中断时间（如跨地域恢复服务）。关键限制：GPU 等特殊硬件不支持自动恢复；备份需考虑加密与合规性（采用 KMS 管理密钥）。企业应定期更新灾难恢复计划，并测试多云协同策略。

5 云安全态势感知与响应机制

5.1 关键流程闭环

动态感知，资产清点：API 自动发现云主机、容器等资源，构建带版本指纹的资产库，风险标记：关联漏洞库与配置基线，实时标注高危资产（如暴露的数据库端口），智能决策，行为分析：AI 模型检测偏离基线的异常操作（如非办公时段数据批量下载），攻击推演：结合威胁情报预测横向移动路径，输出 TTPs 战术画像，协同响应，自动遏制：隔离受控实例：动态更新安全组规则阻断恶意流量，冻结异常凭证：实时禁用异常 API 密钥或 IAM 账号，取证溯源：创建云主机只读快照，区块链存证攻击时间线，持续优化，闭环验证：处置后自动扫描残留攻击组件，确保根除，策略调优：基于攻击复盘数据强化防护规则（如收紧 SSH 访问策略）。

5.2 实施核心要点

架构兼容性：需支持混合云/多云环境，通过 OpenDXL 协议实现跨平台策略同步，隐私合规：数据采集脱敏处理，符合 GDPR 及《数据安全法》要求，误报管控：建立威胁置信度分级机制，优先处置高危云相关事件，实践表明，该机制使云平台威胁检出率提升至 99.99%，勒索软件等攻击影响范围降低 80%。未来将深化 AI 驱动的情报联邦学习，实现跨机构攻击链协同阻断。

6 如何实时监测云环境安全状况

6.1 云环境安全实时监测体系构建方案

全维度资产感知与风险标记，自动化资产发现，通过 API 集成自动识别云主机、容器、存储桶等资源，构建带版本指纹的动态资产图谱。关联漏洞库与合规基线，实时标记高危暴露面（如开放数据库端口、未修复漏洞）。实时可视化监控，统一仪表盘展示全局风险态势：安全评分、活跃威胁分布、合规状态，穿透式查看具体资产详情（如容器漏洞、异常访问记录），智能威胁检测与分析，多源数据关联分析，聚合网络流量、主机进程日志、云操作记录。

6.2 云安全事件对未来防御的启示和建议

核心启示，配置错误是最大突破口，70%的云安全事件源于存储权限开放、默认密码未修改等低级疏漏，需通过自动化工具持续扫描修复。Ivanti 事件表明，未及时修补的漏洞可被国家级攻击者精准利用。供应链攻击威胁升级，第三方组件漏洞（如 Log4Shell）和污染容器镜像成为入侵跳板，2025 年近半数企业将遭遇此类攻击。需建立软件物料清单（SBOM）并扫描依赖项风险。身份滥用风险加剧，弱密码、权限泛滥及离职账号未回收导致横向移动，需强制多因素认证（MFA）并实施最小权限原则。关键防御建议，技术层面，零信任架构落地：基于身份与应用构建微隔离，持续验证访问请求，替代传统边界防御。AI 驱动的威胁狩猎：利用机器学习分析行为基线，识别 API 异常调用等高级威胁，误报率可压至 0.1%。全链路加密与密钥轮换：覆盖静态存储与动态传输数据，防范中间人攻击与数据泄露。管理层面，自动化合规审计：实时检测云配置偏离安全基线（如开放数据库端口），生成修复方案。攻防演练常态化：通过混沌工程模拟云环境入侵，优化应急响应流程（如将 MTTR 缩短至 90 秒）。供应链安全管控：对第三方组件进行沙箱检测，限制容器镜像仅从可信仓库拉取。协同防御，共享威胁情报（如恶意 IP 库），联动云防火墙与 WAF 实现攻击链快速阻断。

总之，未来防御需平衡技术创新与基础加固，尤其关注 AI 攻击与防御的博弈升级。

参考文献

[1]陈华.关于智算时代云安全威胁态势分析与防御机制探究.2023.

[2]杨红艳.智算时代云安全威胁态势分析与防御机制探讨.2022.