智能高效的云原生安全体系

Intelligent and Efficient Cloud-native Security System

左文树(华为云计算技术有限公司,广东 东莞 523808)
Zuo Wenshu(Huawei Cloud Computing Technology Co.,Ltd.,Dongguan 523808,China)

摘 要:
云计算作为"新基建"中信息基础设施的重要组成部分,是企业数字化转型的重要支撑。随着企业业务逐步上云,传统的安全防护和检测技术无法适应云计算环境带来的挑战。此外,云原生技术倡导应用敏捷、可靠、易扩展,随着该技术的广泛应用,如何保证云上业务系统的安全成为迫在眉睫的问题。分析云上所使用的技术以及所面临的安全风险及其带来的影响,结合云上安全运营的要点,为企业在上云后构建贴合业务的一体化云安全防护体系提供了思路。

关键词:
云原生;安全运营;云安全;云计算
doi:10.12045/j.issn.1007-3043.2024.08.016
文章编号:1007-3043(2024)08-0078-05
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:
As an important part of the information infrastructure in the "new infrastructure", cloud computing is an important support for enterprise digital transformation. As enterprise services are gradually migrated to the cloud, traditional security protection and detection technologies cannot meet the challenges brought by the cloud computing environment. In addition, cloud native technology advocates for agile, reliable, and easily scalable applications. With the widespread application of this technology, ensuring the security of cloud based business systems has become an urgent issue. It analyzes the technologies used by cloud applications, the security risks faced, and their impacts, and summarizes the key points of cloud security operations to provide guidance on how to build an integrated cloud security system tailored for cloud services.

Keywords:
Cloud-native; Security operations; Cloud security; Cloud computing

引用格式:左文树. 智能高效的云原生安全体系[J]. 邮电设计技术,2024(8):78-82.

1 概述

据Gartner预测,2025年全球企业在公有云计算领域的IT支出将超过传统IT服务支出,将有51%的IT支出从传统方案转向公有云(2022年为41%);将有65.9%的应用软件支出转向云技术(2022年为57.7%)。

Gartner分析数据显示,公有云市场的热点区域从欧美向亚太转移,2021—2023年亚太复合增速为23.8%,高于美洲(21.3%)、欧洲(14.5%)以及中东非(21.9%),2022年亚太公有云市场占比提升至20.4%,仅次于美洲;同时,对比欧盟、美国企业70%~85%的上云率,亚太企业的上云率还有很大的提升空间[1]。

从国内市场来看,互联网行业用户渗透率已超过70%,传统行业在加速上云,上云深度呈现"阶梯状"分布,第一梯队的政务、金融等行业基本完成首批上云,目前主要关注业务应用的云化改造,第二、三梯队行业的上云空间广阔,但在上云路径上存在较大的差

收稿日期:2024-07-10

异，比如政企客户往往倾向于采用混合云技术路线。

随着企业步入深度用云阶段，如何利用人工智能技术与云计算技术的充分融合来进一步提高生产效率、优化客户体验、推动业务增长，成为未来关注的焦点。IDC调研数据显示，2025年将有超过70%的企业使用基于云的人工智能服务。

以ChatGPT为代表的生成式人工智能大模型热潮引爆了智能算力需求，催生模型即服务（MaaS）的全新商业模式，推动云计算服务模式向算力服务模式演进，有望开启云计算产业发展新篇章。

2 传统安全技术无法应对云原生安全挑战

在全面云化的时代，企业应用系统可以充分利用云计算平台的云原生优势，实现更高效、更灵活、更可靠的运行。与传统的IT系统架构相比，云计算在引入新架构、新技术的同时，也对安全技术提出了更高的要求，继续套用传统的安全防护措施已无法有效应对云上安全威胁[2]。

2.1 全局资产难盘清

对企业来说，管理好资产是做好安全防护的首要工作。当前企业内部采用的设备、资产完全分散，没有统一管理，而且资产的变化无法及时同步到安全团队，导致很多安全人员只能采用IP资产发现或者扫描工具作为资产清点的主要手段，但这些方式能发现的资产有限，并且存在时效性低、覆盖度差、准确度低等致命问题。每次攻防演练，攻击者都是通过未知的资产作为攻击的突破口和跳板对企业进行下一步的渗透，影响整体的安全防护。

2.2 全局数据难联通

在传统的安全防护体系中，因建设周期以及由不同组织运维运营等原因，各类IT资产割裂，彼此之间缺乏数据互通，安全设备无法有效获取网络、应用和数据等日志进行攻击威胁检测，缺乏对全局的掌控和分析。特别是随着企业规模的扩大，庞大的资产也带来了威胁敞口增多的问题，这导致日常安全运营只能利用安全产品自身生成的数据进行关联分析，缺少系统和组件关键信息的关联，无法辅助安全人员进行全局决策，大大降低了风险的识别维度和准确性。

2.3 响应处置难协同

当前的网络攻击对抗性强，留给防御者的响应窗口短，而在传统安全体系的建设过程中，大部分企业平均会部署十几种安全设备和工具，各个安全组件都是烟囱式建设，独立运维运营，协同处置复杂，无法满足快速检测和响应的诉求[3]。安全业界也在持续推动互联互通标准，但实际上收效甚微，当前企业很难实现全局的安全威胁自动化联防联控。SANS的调查报告显示，在事件风险控制方面，仅有19%的组织能在1 h内进行风险控制，而75%的组织需要超过1 h；在事件恢复方面，只有11.6%的组织能在1 h内恢复，83%的组织恢复时间超过1 h（见图1）。这一数据揭示了大多数组织因缺乏有效的响应协同能力，在事件风险控制和恢复方面耗时较长。

2.4 性能瓶颈难弹性

传统的网络安全防御受制于安全产品本身的性能、规格瓶颈[4]，扩容或者更换时需要耗费很多时间，更换期间甚至会影响到资产的有效防护，而且购买大规格的安全产品又会带来成本上的巨大浪费。随着业务上云，业务的规模会随着业务的发展弹性伸缩，企业需要考虑的主要问题是如何利用云计算的特殊性质来更便捷、有效地保障安全。

3 面向云原生环境的安全体系实践

守护企业云上数字资产的安全需要坚持“三分靠建设、七分靠运营”的原则。当前先进企业为了充分释放生产力，对于系统的灵活性和弹性要求越来越高。企业资产，无论是人、权限，还是资产的攻击面，随时都在变化，而且攻击者的技术手段也在变化。这些因素都导致了安全风险是动态变化的，保障安全不是部署一套安全技术方案就可以实现的，必须通过“云平台内生的技术能力”与“自适应云业务的安全运营”2个体系的结合，才能提供端到端的完整解决方案[5]。

基于云上业务的灵活需求和动态变化，安全也必须具备与之匹配的敏捷与自适应能力。因此，建设能自适应业务动态性要求的云原生安全体系势在必行。

云原生安全防护体系可以总结为“七道防线，一个中心”，即构筑与云平台资源一体化、“内生”于云平台的安全技术能力；以及一套与云融合、“自适应”云上业务变化的安全运营体系。

3.1 “内生”的云原生安全技术体系建设

云原生技术体系包括“七道防线、一个中心”的安全技术基础设施。“七道防线、一个中心”具体为物理防线、身份权限防线、网络防线、应用防线、主机防线、数据防线、运维防线，以及“安全运营中心”（见图2）。

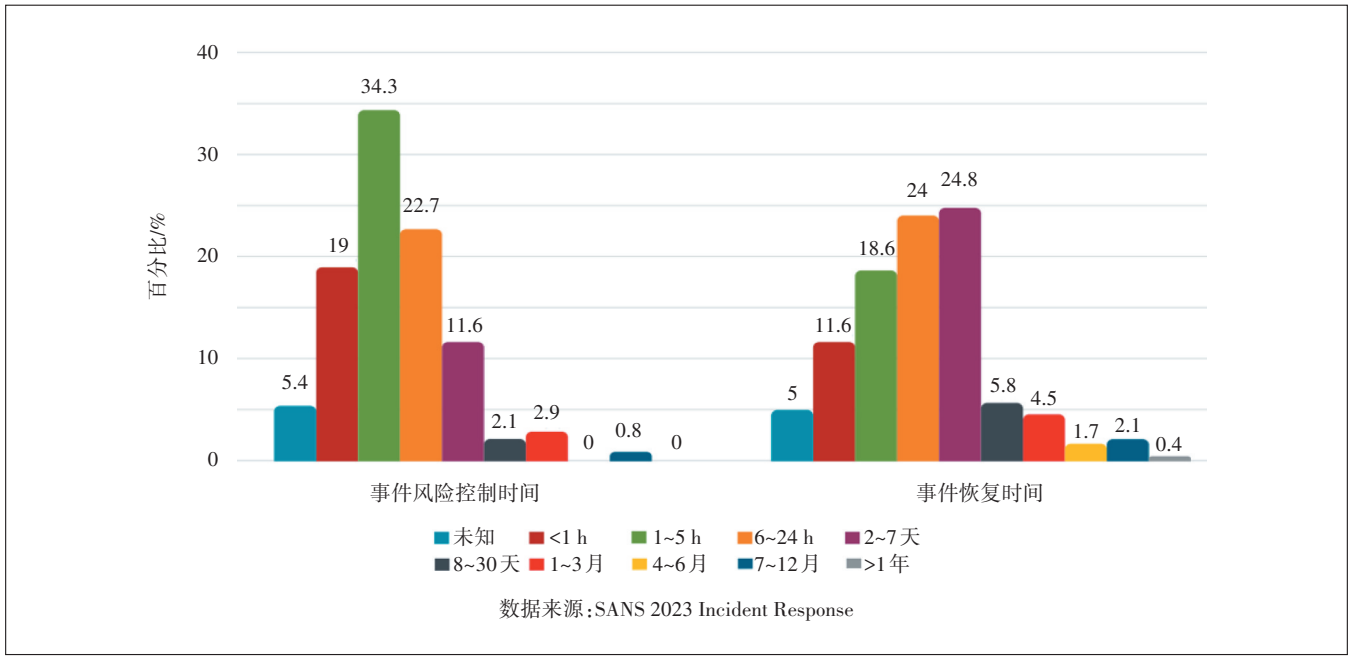

图1 网络安全事件响应时长

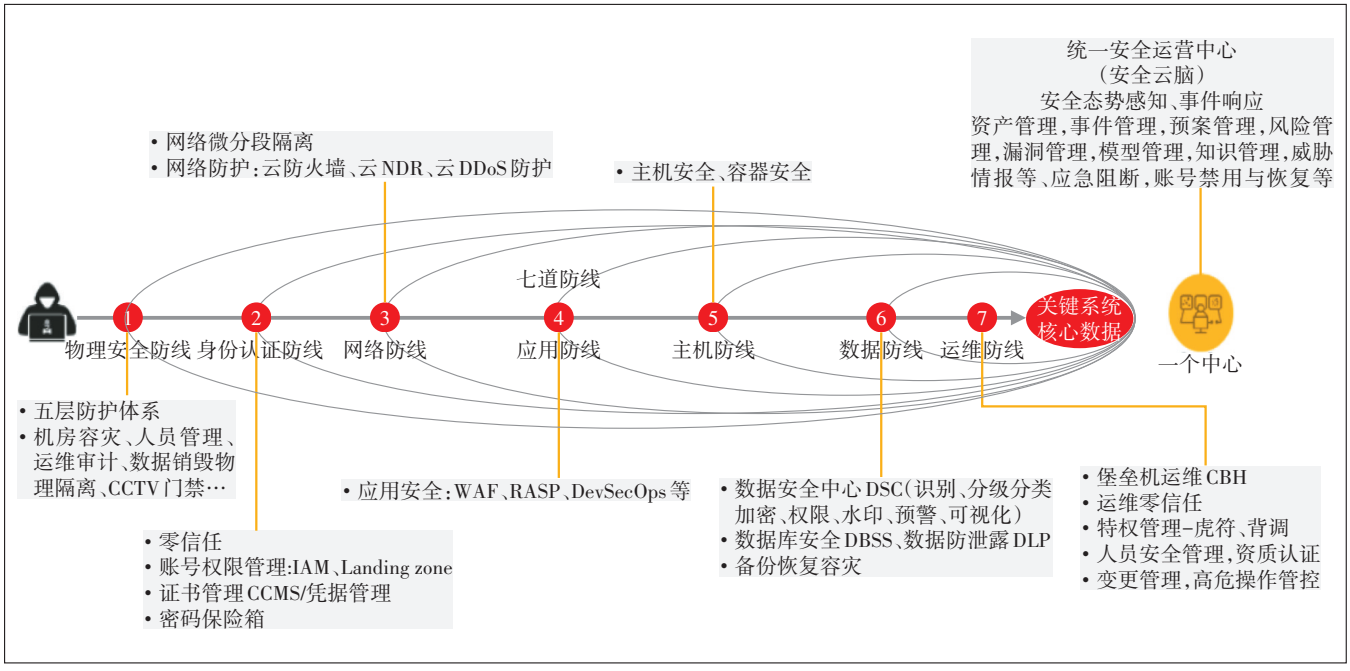

图2 某公司云原生技术体系,“七道防线,一个中心”

在云安全保障中,随着RASP、API安全、容器安全等成为基本的云安全机制[6],独立于云平台的安全资源池无法提供对应功能,而云原生安全基础设施是云平台“内生”的,安全与云实现了资源的一体化建设、服务的一体化部署、业务的一体化运行,使得云安全不再是独立于云的另一个业务,而是云平台自身的属性[7],从而可以保证安全能力时刻随云部署、动态扩缩、动态运行。基于上述“内生”的安全能力,云原生技术体系可以实现对云环境中可能的暴露面、攻击路径、资产的贴身防护[8]。

3.2 “自适应”云业务变化的云安全运营体系

由于企业的数字资产、使用模式、攻击威胁都在

不断变化，安全保障面临巨大的“不确定性”。这就需要在尽力而为的威胁防御之外，通过高效的安全运营体系，保证业务系统的安全与“韧性”。

所谓“韧性”，就是在所有防线都被攻破时，系统确保把损失控制在可接受范围内的能力。保证系统的韧性一方面要利用纵深防御思想，实现群防群控，使防线难以被突破；另一方面，由于没有绝对的安全，必须充分考虑当某些甚至所有防线都被攻破后，系统能够及时感知攻击所引发的异常，从而通过快速、高效的安全运营，实现对损失的阻断、纠偏与处置，保证系统的动态安全[9]。

参考美国《NIST CSF：信息安全保障框架》中的IPDRR模型，建立以系统韧性保障为目标的安全运营体系。在该体系中，基于识别、防御、检测、相应、恢复5个阶段，对系统中的资产、漏洞、网络、终端、平台、应用、数据、安全事件、威胁情报等不同的对象进行流程化的操作，从而构建端到端的系统安全运营能力（见图3）。

把IPDRR运营框架与国内“关键基础设施安全保障”等规范要求相结合，同时根据某公司云成功的安全运营实践，可以识别出云上安全运营体系应当具备的十大关键能力。

a）暴露面运营。资产变化实时感知[10]，确保资产配备该有的安全防护措施，避免不设防的暴露面。

b）漏洞运营。随时感知漏洞[11]信息，第一时间感知和修补业界发布的漏洞。

c）证书运营。对所有证书做到可视、可管，避免使用不合法证书，证书到期应及时更换。

d）配置运营。对各类产品（包括安全产品、存储、数据库等）的配置，都要建立配置基线，及时改正风险配置项。

e）账号权限运营。实现基于身份的精细化权限管理，敏感操作具备二次认证能力，通过凭据管理，对口令进行自动化定期轮转，建立安全基线并进行集中审计。

f）数据运营。充分识别企业关键数据，实现分级分类管理。对关键数据的使用制定规范，并落实保护、审计措施。此外，需要结合企业实际情况建立数据管理基线[12]。

g）情报运营。通过本地积累以及广泛的外部生态合作，获得全面的威胁情报。

h）威胁运营。建立全面的威胁检测模型，围绕企业自身IT场景实现情报分析，对海量告警、日志数据进行降噪处理，快速发现真正的风险；基于各类数据的行为实现关联分析，识别风险，并补充威胁情报库；建立快速响应的自动化剧本，以准确发现入侵，快速

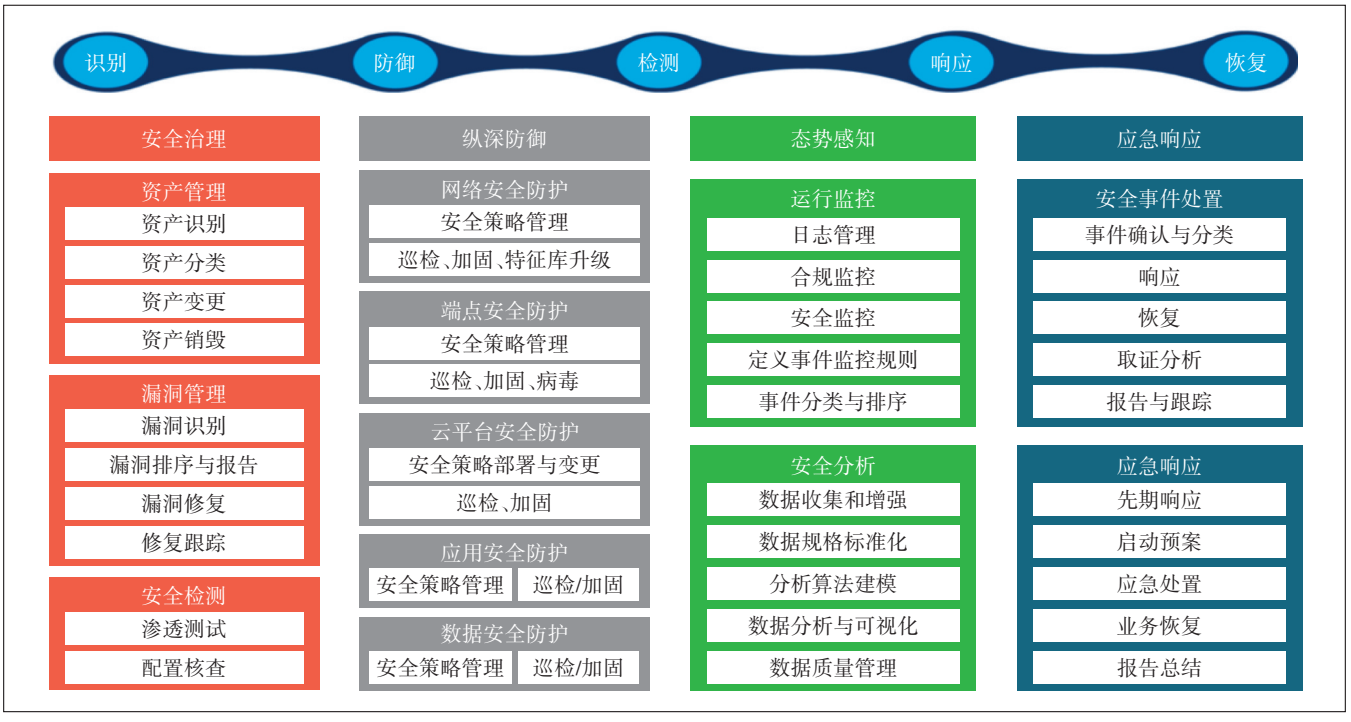

图3 某公司云原生安全运营能力框架

封堵、隔离、处置，避免损失扩大；将30年的安全运营经验固化为可复用的模型，不断提升运营系统的安全运营水平，使其成为一个永久的安全运维“专家”[13]。

i）攻防演练。通过常态化的攻防演练，查缺补漏，使安全保障满足实战化[14]要求。

j）制度和“安全场”的建设。要把上述运营措施端到端落地，企业必须从战略高度入手，“一把手”重视，否则就无法推行，这就是“安全场”的建设。同时，需要建立对应的管理流程和制度，明确责任，让每件事都有明确的主责方。要明确业务流程，把能力固化在流程中，而不是依赖个人；明确应急响应（war room）机制，在出现问题时不慌乱，成员之间能够有效协同。

“内生”的云原生安全技术体系是云安全的基础，“自适应”的安全运营体系是云安全的灵魂，两者结合所构成的云原生安全防护体系，可以实现对各种高效灵活、动态变化的云原生工作负载的有效保障[15]。

安全体系的有效性需要经得起实战的检验，在一年一度的国家级安全攻防演练活动中，有效部署云原生安全体系的企业和主流云服务商，均获得了很好的成绩。以某公司云为例，某公司云在全球有100多个数据中心、百万台服务器，服务全球170多个国家的客户；各重点行业TOP30客户的业务都运行在该公司云上，在这样的广度与复杂度下，在历次的国家级护网中，某公司云均取得了0失分的成绩。常态化安全运营数据显示，某公司云每年有效防御各类网络攻击达4 500亿次以上，平均每天防御12亿次以上的攻击；在所有的安全威胁中，99%实现了分钟级闭环。能获得上述安全成绩，主要得益于建设了云原生的安全体系，某公司云可以基于云上广泛的安全数据，利用云上AI的智能分析能力，实现安全能力的螺旋式上升，同时这些能力都对云上客户开放，实现对云原生安全能力的共享。

4 结束语

在云化时代，安全风险可以通过统一的安全技术架构、自适应的安全运营体系，基于海量的数据、智能的AI分析引擎来快速识别已知与未知的威胁，通过快速闭环处置有效消减风险，从而有效提升安全运营团队效率，帮助客户完成传统安全运营到智能化安全运营的跨越式转变。总而言之，云原生安全体系实现了安全建设的简单便捷、安全运营的智能高效、安全效果的突飞猛进，是保证云原生业务快速发展的安全基础。

参考文献：

[1] 王军民. 中国云安全市场发展特点和热点技术[J]. 中国信息安全，2022(5)：37-38.

[2] 何宝宏. 云与安全深度融合推动原生云安全发展[J]. 中国信息安全，2022(5)：29-33.

[3] 腾讯云计算（北京）有限责任公司，中国信息通信研究院，深信服科技股份有限公司，等. “云”原生安全白皮书（2019版）[R/OL]. [2024-01-23]. http://www.d1net.com/statics/images/ad/202211/221123_Tencent_whitepaper_01.pdf.

[4] 李雨航，郭鹏程. 云安全的发展与未来趋势[J]. 中国信息安全，2022(5)：39-42.

[5] 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.

[6] Cloud Native Computing Foundation. Cloud native security whitepaper[R/OL].[2024-01-23]. https://www.cncf.io/wp-content/uploads/2022/06/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf.

[7] 中国联通研究院. 中国联通云原生安全实践白皮书（2022）[R/OL]. [2024-01-23]. https://www.sohu.com/a/623943911_476857.

[8] 云原生产业联盟. 云原生架构安全白皮书（2021年）[R/OL]. [2024-01-23]. https://www.dosec.cn/security_detail/c-_detailId%3D1722104557822087168.html.

[9] 张峰，江为强，王光涛，等. 针对云计算服务环境下关键信息基础设施安全保障的思考[J]. 信息通信技术与政策，2022(8)：31-35.

[10] 云安全联盟大中华区. 云原生安全技术规范：CSA GCR C002-2022[S]. 上海：云安全联盟大中华区，2022.

[11] NLST. CVSS severity distribution over time [DB/OL]. [2024-01-23]. https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time.

[12] 赵洪业. 政务云安全运营体系建设发展研究[J]. 信息与电脑，2023，35(4)：65-68.

[13] 王欢. 云上实战化安全运营和常态安全监管研究[J]. 网络安全技术与应用，2021(11)：70-71.

[14] 沈昌祥. 按照《关键信息基础设施安全保护条例》筑牢网络空间安全底线[J]. 信息安全研究，2021，7(10)：890-893.

[15] 王竹欣，李红伟，崔涛. 新基建时代下云安全发展趋势分析[J]. 保密科学技术，2021(10)：32-36.

作者简介：

左文树，华为云安全总裁，主要从事华为云安全产品与解决方案的规划、竞争力构建，可信与领先的云安全服务产品与解决方案的打造、云安全的商业模式与产业生态的构建；华为云平台的安全体系建设、运营运维等工作。