数世咨询
Digital World Consulting

云原生安全能力指南

免责申明：

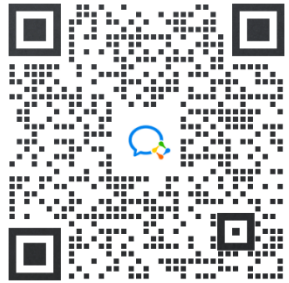
本内容非原报告内容；

报告来源互联网公开数据；如侵权请联系客服微信，第一时间清理；

报告仅限社群个人学习，如需它用请联系版权方；

如有其他疑问请联系微信。

行业报告资源群



微信扫码 长期有效

1. 进群福利：进群即领万份行业研究、管理方案及其他学习资源，直接打包下载
2. 每日分享：6+份行研精选、3个行业主题
3. 报告查找：群里直接咨询，免费协助查找
4. 严禁广告：仅限行业报告交流，禁止一切无关信息

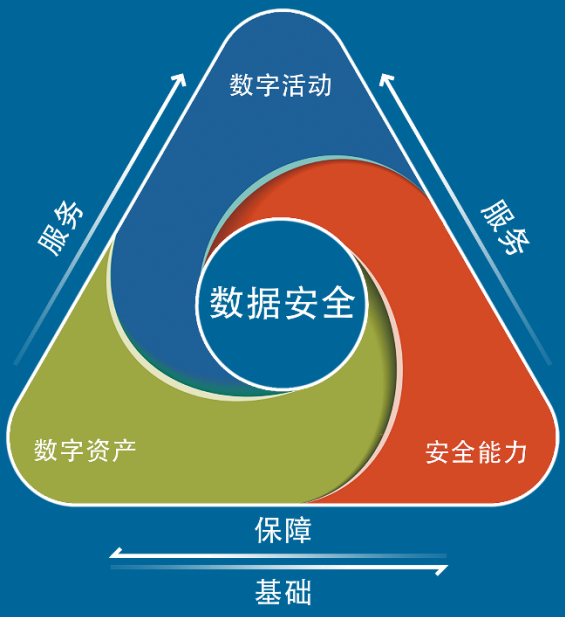
微信扫码 行研无忧

知识星球 行业与管理资源

专业知识社群：每月分享8000+份行业研究报告、商业计划、市场研究、企业运营及咨询管理方案等，涵盖科技、金融、教育、互联网、房地产、生物制药、医疗健康等；已成为投资、产业研究、企业运营、价值传播等工作助手。

数世咨询
Digital World Consulting

云原生安全能力指南



数字安全的三个元素分别为，安全能力、数字资产和数字活动。数字资产是安全能力的保护对象，数字活动是安全能力以及数字资产的服务对象，而数据安全则是三元论的核心目标。对于这四者关系的深度理解和相关技能掌握是做好数字安全工作的关键。

数字安全能力模型研究的基础，来自于数世咨询 2020 年首次提出的“网络安全三元论”。三元分别为，网络攻防、信息技术和业务场景。

随着数据成为第五大生产要素为典型标志的数字时代来临，“网络安全三元论”在 2022 年进行了更新迭代升级为“以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核”的“数字安全三元论”，以适应我国数字中国建设的进程。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构．网安企

业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

主笔分析师 **陈发明**

首席分析师 **李少鹏**

分析团队：**数世智库** 数字安全能力研究院

目 录

前言

随着企业业务上云成为潮流和趋势，“云原生”（Cloud Native）作为一种新的应用程序开发和部署的方法，可以提高应用程序的可靠性、弹性和可扩展性，同时降低开发和运维的成本。云原生概念诞生已十年有余，但是采用云原生的业务开发和部署模式直到最近几年才逐渐被企业所关注。

针对云原生开发及运营相关的云基础设施、主机、容器、业务应用等的安全防护方案，业界统称为“云原生安全”。云原生安全是云安全的进阶阶段，它不仅继承了云安全的理念和方法，而且在技术和服务模式上有所深化和发展。

当前许多甲方用户对于云原生安全的认知并不十分清晰，许多人可能刚刚开始理解云安全的具体涵义，现在又迎来了云原生安全概念。面对新的技术方案，笔者也曾遇到很多困惑，本报告尝试通过一个简洁明了的方式，对云原生安全相关的技术点进行系统性的总结，对关键的技术进行介绍。

近两年来，云原生安全市场在快速增长，为了得到一手的市场资料，数世咨询邀请了九家国内云原生安全代表企业和部分甲方用户进行实际考察，对安全厂商近三年来的产品营收数据进行了收集和分析，结合与安全厂商相关的研发、市场负责人等多轮线上线下访谈，以图客观真实地反映云原生安全市场及应用情况。

本报告**技术部分**主要内容：云原生概念、云原生安全挑战、云原生安全定义、云原生安全能力全景图、数世咨询定义的“全栈云原生安全”能力要素。

本报告**市场部分**主要内容：云原生安全市场规模、行业应用、能力企业点阵图、能力企业主要业务特点、云原生安全趋势分析以及代表厂商优秀案例。

尽管本报告尽笔者所能尽量充分的进行了技术以及市场方面的调研，但受能力所限或有错误和偏颇之处，欢迎同行与我联系交流。

本报告仅供参考。

勘误或进一步沟通，请联系主笔分析师：陈发明 chenfaming@dwcon.cn

关键发现

- ✓ 应用软件的云上迁移，并逐渐云原生化，安全问题是影响云原生应用落地的重要因素之一。
- ✓ 2023 年国内云原生安全市场规模约为 26 亿元，受经济环境影响 2024 年市场规模应该增幅不大，预估 31 亿元左右。
- ✓ 云原生安全在行业的应用 TOP4 为：金融（27.5%）、互联网（25.5%）、工业制造（15 %）、运营商（9.4%）。
- ✓ 国内行业的云原生项目近两年来有显著增加， 2023 年安全厂商所实施的云原生安全相关的项目跟往年同比增长 50%到 300%不等。
- ✓ 云原生安全应用依赖于企业业务开发的 DevOps 建设流程，对云原生不同阶段的单项安全工具，仍然有单独的安全需求。
- ✓ 由于各厂商的技术发展路线不同，不同厂商在云原生安全领域的技术起点以及技术深度各不相同。尽管如此，各安全厂商均把打造全流程云原生安全能力体系视为云原生安全的终极能力。
- ✓ 数世咨询将覆盖了业务开发、构建、部署、运行以及数据保护全业务流程的安全能力称为“全栈云原生安全”，调研发现，目前仅有个别安全厂商能够接近实现“全栈”。
- ✓ 由于云原生体系的复杂性和阶段性，国内企业存在云安全和云原生安全并存的安全需求，同时具备云安全与云原生安全解决方案的安全厂商在混合安全需求的项目竞争中更具优势。

1.概念与技术

1.1. 云原生

先聊聊云原生。

2013 年 Pivotal 公司首次提出了云原生概念，认为云原生是一种构建和运行应用程序的方法，是一套技术体系和方法论。它意味着应用程序从设计之初就考虑到云的环境，原生为云而设计，在云上以最佳方式运行，充分利用和发挥云平台的弹性和分布式优势。

2015 年，推动云原生应用和发展的著名组织云原生基金会（Cloud Native Computing Foundation，简称 CNCF）成立， CNCF 致力于推广容器化、微服务架构和开源项目，当前已建立了庞大的社区和生态系统，对全球云计算产业产生了深远影响。国内众多企业和机构也积极参与 CNCF 项目，据统计我国已经成为其第二大开源项目贡献国。

CNCF 的对云原生的解释是“容器化、微服务化和自动化”，通过容器技术实现应用的高效部署和管理，通过微服务架构提高应用的模块化和可维护性，并通过自动化工具减少人工干预和降低运维成本。CNCF 对“云原生”的定义中特别指出了以下几种代表性技术：不可变基础设施、容器、微服务、服务网格和声明式 API 。

图例：云原生代表性技术

有个别概念过于抽象，笔者尝试通俗化的解释一下这几个概念。

不可变基础设施

不可变基础设施是指基础设施的配置和状态不可变，一旦部署不应该被修改。以搭建服务器为例，在传统 IT 建设的时代，为了降低风险使服务器运行稳定，其运行环境总是面临不断的更改，比如：系统升级、打补丁、更新应用的依赖组件等，运行环境的变化经常影响其所承载的业务，所以让管理员焦头烂额的事情时有发生。而在云计算环境中，服务器在完成部署后，就不再进行更改。云计算通过引入虚拟化技术，实现了方便地打包构建应用及其运行时的依赖环境，减少人为错误和提高系统的可靠性。

容器

容器和微服务相信不少人耳熟能详了，通俗来讲容器是一种打包技术，它将应用及其依赖环境打包在一起，实现了在不同内核的主机上运行，保证了业务的一致性，流行的实现比如 docker。

微服务

微服务可理解为搭积木，先将大型的应用系统分解为一组小的、

独立的服务，然后象搭积木一样通过轻量级通信协议（比如API）再搭建起来。其主要目的是实现单个服务的独立部署、扩展和更新，提高开发效率和系统的可维护性。

服务网格

服务网格算是为微服务提供服务的一个基础设施层，当大的应用分解为小的微服务，微服务之间的数据通信、网络连接就更为复杂，服务网格就相当于一个代理管家，提供了服务间的通信、安全、监控和可观察性等服务。Istio 和 Linkerd 是服务网格技术的代表。

声明式 API

声明式 API 可对比到编程模式，以前编程是手工敲代码写函数，现在不用了，只需要建个配置文件，写下来你想“要什么”就可以了。比如大名鼎鼎的 Kubernetes（K8S） 就使用声明式 API 来配置云原生基础环境，进行容器编排。

概括来说， “云原生”是一种构建和运行云应用程序的方法，云原生充分利用云计算基础架构，结合 CI/CD 自动化开发和部署流程，实现业务的快速开发与运行，从而在根本上提高工作效率和实现成本节约。流行多年的 DevOps（开发与运营）理念天然的适配云原生，当前其已成为云原生事实上的开发模式。

调研发现，近两年来，采用云原生开发与部署的方式正逐步成为行业内重点考虑的方向。国内的金融、互联网、智能制造以及运

营商等行业，已经开始构建云原生化开发流程，进行试点或将部分业务以云原生的方式发布。预计在未来几年，云原生化的“业务上云”将会成为云计算发展的趋势之一，引领云计算的潮流发展。

1.2. 云原生安全挑战

任何系统都有安全风险，云原生业务同样有其特别的脆弱性。

云原生应用运行于云计算环境，长时间暴露于互联网，除了遭受传统的 DDoS、网络扫描、暴力破解、远程注入等网络攻击以外，大量云端数据带来的诱人黑产回报也同时吸引着黑客不断尝试突破安全防御。新的安全挑战来自：新的边界、动态变化的资产、极致自动化的开发流程、云原生特征的攻击面等方面。

图例：云原生安全挑战

新边界带来新的安全挑战

云计算技术的出现使得传统的安全边界变得模糊不清，而云原生架构更是加深了这一变化趋势。在传统 IT 基础设施中，资源是按照物理区域划分的，如机房中的机柜等设备，这些资源的标识通常是机柜编号，安全边界为房间墙壁和防盗门。然而随着云计算的兴起，资源开始虚拟化，安全边界开始转变为由虚拟机和主机 IP 来定

义，隔离措施则通过防火墙或虚拟化防火墙来实现。

在云原生时代，资源的划分已不再是依据物理设备或者虚拟机，而是以业务为中心的微服务占据了主导地位。为了更有效地利用云计算资源，通过将应用程序分解为松耦合的微服务组件，并实现服务的互访，微服务之间需要的安全控制成为新的边界。在这种情况下，安全防护不再依赖于 IP 地址或端口，而是基于微服务标识来进行策略管控，新的边界带来新的安全挑战。

动态变化的资产带来的安全挑战

云原生环境强调“不可变的基础设施”的概念，它通过牺牲基础设施的可变性来换取更高的稳定性、一致性和应用部署的灵活性。比如，在云原生环境中，应用程序的每一次发布都是全新发布， 在传统环境中直接在服务器上打补丁来修复漏洞，但在云原生环境中要修复漏洞需要停止旧的容器并重新构建新的镜像来修复漏洞，同时进行重新发布。

动态资产增加了系统的复杂性，需要更高级的监控和管理工具来跟踪和维护资产状态，同时对动态资产的资源管理、策略管理等方面提出了更高的要求。

适配极致自动化开发流程的安全挑战

云原生应用开发普遍采用 DevOps、面向服务等理念构建业务系统，重塑了整个 IT 流程，同时实现了高效、极致的自动化，极大缩

短了业务从开发到上线运行的时间窗口。这要求安全防护手段也要实现高度自动化，能够与 DevOps 流程对接，实现紧密集成。

云原生特征的攻击面带来的安全挑战

云原生的微服务、容器化技术带来了新的攻击面，比如：对镜像仓库的保护、容器编排系统的安全配置、微服务间的安全控制、容器运行时的入侵防御、以及自动化 CI/CD 流程中的代码和镜像安全等，对构建一个覆盖云原生全生命周期、动态且适应性强的安全防护体系带来巨大挑战。

Red Hat 公司发布的《Kubernetes 安全防护状况报告》（2024 版）报告中的统计显示，在过去的一年中，有 9 成的应用云原生的企业组织至少发生过 1 起容器或 Kubernetes 安全事件，有 2/3 的企业组织由于担心 Kubernetes 安全问题而延缓了业务部署，46% 的企业由于容器或 Kubernetes 安全事件产生了损失。

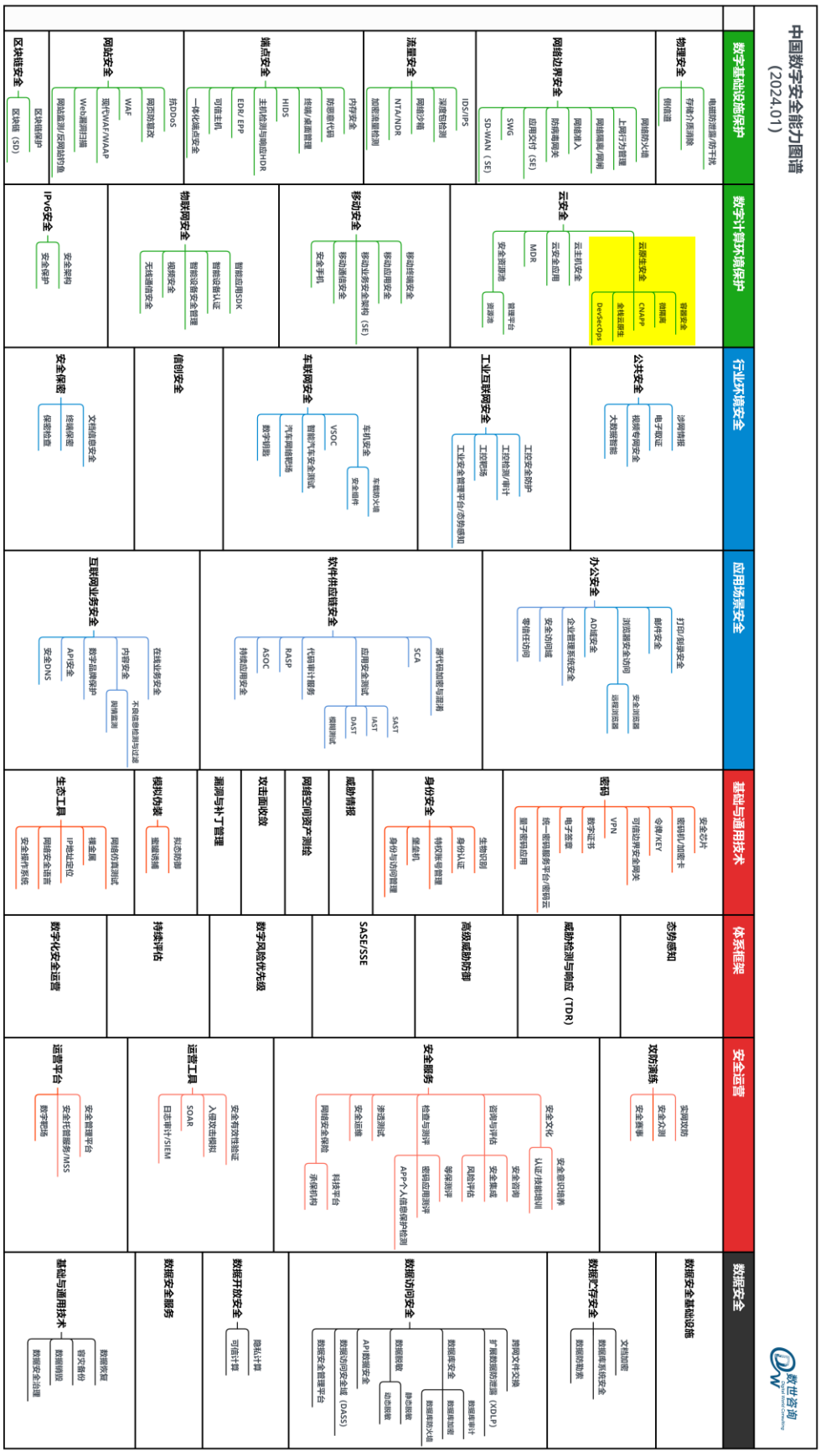
云原生应用的开发和交付转型是一次全方位的变革，一方面，企业的组织架构、组织流程等为适配云原生环境要发生变化，安全责任主体也需要有所调整。另一方面，在安全技术上云原生引入了大量新的基础设施、安全防护对象，发生了颠覆性变化，面对这些新技术带来的安全防护对象，企业需要引入新的安全手段。

1.3. 云原生安全能力体系

相比于云安全，云原生安全更关注对云原生基础设施、容器镜像、容器运行时、微服务、无服务器（Serverless）等实施安全保护。综合行业诸多专家的观点，数世咨询将**云原生安全**定义为：

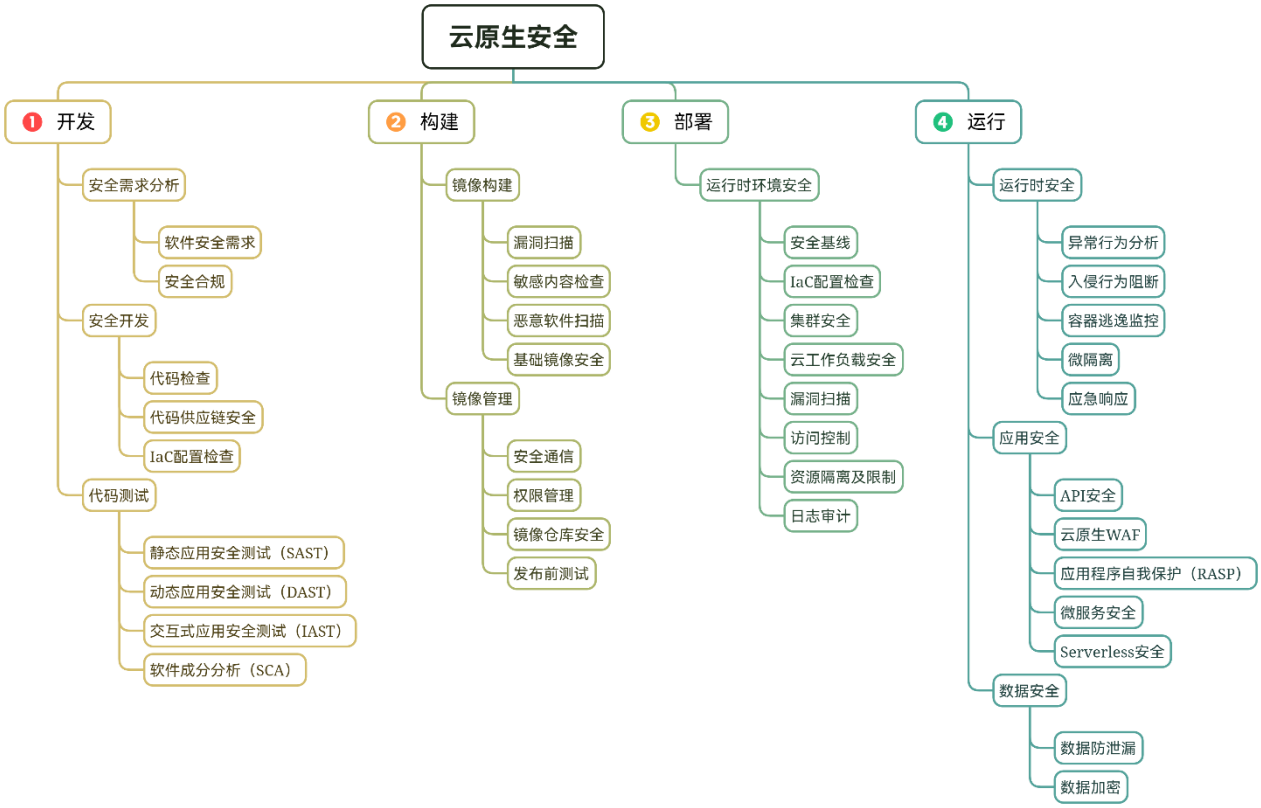
云原生安全是指在云原生环境中应用的一种全新的安全方法，这种方法强调安全能力与云原生环境相结合，跨越云原生应用开发、构建、部署和运行全生命周期提供一种综合的安全能力，旨在对云原生基础设施、容器镜像、容器运行时、微服务、服务网格等关键组件提供全面的安全防护。

在 2024 年初，数世咨询发布的《中国数字安全能力图谱》中，云原生安全属于“数字计算环境保护”领域中“云安全”细分领域，如下图：



图例：2024 年度《中国数字安全能力图谱》

关于云原生安全的整个能力体系，常见的有两种维度视角的考虑，一种是依据整个业务系统的逻辑分层，比如Kubernetes提出的4C模型【云（Cloud），集群（Cluster），容器（Container），代码（Code）】，一种是依据云原生开发-构建-部署-运营的全生命周期流程，基于对云原生安全项目需求以及厂商解决方案的相关调研，笔者认为后者在安全能力的分步建设方面逻辑更为清晰，如下图所示：



图例：云原生安全能力全景

考虑到报告的篇幅，对云原生安全全景图中的技术能力点，笔者不打算一一科普，仅对业务流程及其中关键的安全能力简要介绍如下：

i.开发

云原生安全需要将安全能力规划到软件开发生命周期的早期阶段，即“安全左移“，重要意义在于通过在设计和开发阶段就识别和修复潜在的安全漏洞，可以显著降低后期修复的成本和复杂性，减少安全风险。试想一个安全漏洞被打包进镜像，在后期运行时，这个镜像被复制为千万个容器副本，那么安全风险便被指数级放大。

在开发阶段，安全编码是核心。开发者需要遵循安全编码的最佳实践和规范进行编码，期间定期进行代码审查和必要安全扫描，以发现和修复潜在的安全漏洞。还要考虑代码供应链安全，确保所有第三方库和组件都是安全的，没有已知的安全漏洞。代码测试阶段，静态应用安全测试（SAST）、动态应用安全测试（DAST）以及交互式应用安全测试（IAST），是发现安全问题的有力工具。

ii.构建

当代码开发完成，进入编译打包和容器镜像构建的阶段。此时需要进行漏洞扫描和敏感内容检查，除对自建组件进行安全扫描之外，还需对从公共镜像库下载的基础镜像等进行安全检查。

安全工具需要具备全面且不断更新的漏洞库和指纹特征，以确保能够识别和防御广泛的安全威胁。其次，高效的扫描效率是必不可少的，工具应支持分层扫描，这样可以快速识别和修复各个层中的安全问题，而不是对整个镜像进行重复扫描。

镜像构建完成后通常会进入镜像仓库统一管理，需要注意镜像仓库的安全防护，包括对镜像的权限控制，实施安全加密的通信，保证镜像的完整性可用性。

iii.部署

部署阶段安全措施的关键在于确保容器编排平台的安全性和稳定性。需要对容器编排平台，如 Kubernetes，进行安全基线扫描、对基础设施即代码（Infrastructure as Code，IaC）的配置进行检查，以确保集群设置、云工作负载、虚拟化主机满足合规，没有配置漏洞。

对容器运行环境设置必要的资源隔离和限制策略，比如，使用命名空间、网络策略和资源配额来隔离不同的工作负载，限制容器的资源使用，避免任何单一容器的异常行为对整个系统造成影响。此外，日志审计可以帮助监控和记录所有关键操作，为安全事件的追踪和响应提供支持。

iv.运行

即使在业务流程的开发阶段对镜像、容器应用了充分的安全措施，容器在运行时仍然容易遭受各类攻击，需要考虑容器运行时的网络安全、应用安全、数据安全等。

运行时网络安全

运行时安全的核心任务是确保应用和容器的安全性，防止恶意

行为和入侵。运行阶段通过实施微隔离策略，将网络流量限制在最小必要范围内，限制容器之间的不必要网络访问，减少攻击面并提高整体安全性。

应用安全

在应用安全层面，也是容器运行时重点考虑的方向。多数情况下，容器是对外提供服务的，以提供 WEB 服务为主。所以，可以应用云 WAF 或者云原生 WAF 以防范基于特征库的常见威胁。而运行时应用自我防护技术（RASP）能够提供更深层次的安全保护，它可以嵌入到应用程序中，实时检测和阻止那些 WAF 可能忽略的入侵和恶意行为。当前，serverless （“无服务器”）服务也越来越流行，Serverless 安全也需要重视和关注。

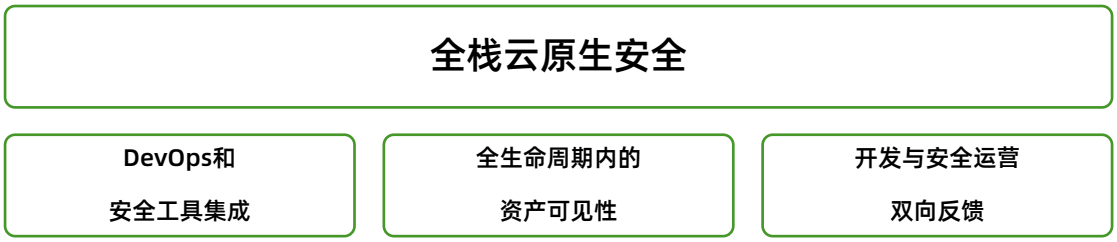
数据安全

云原生环境中的数据有诸多分类，需要区别对待分别实施保护。对于用户或者应用程序产生的数据，一般都是存储在一个单独挂载的存储空间中，实际上可以应用传统的数据安全工具来实施保护。对于云原生环境自身的配置文件，代码等数据，也需要考虑应用敏感的数据防泄露以及加密保护等措施。

1.4. 全栈云原生安全

以上简单总结了云原生应用全生命周期内不同阶段所需的典型安全能力，目前也存在诸多单点的安全工具来实现这些能力，用户基于云原生建设的不同阶段，可以选择集成这些工具到 DevOps 流程中。

但必须要提到的是应用单点的安全工具或不同安全厂商的产品同时也带来安全体系的割裂，给真正实现开发与安全运营的一体化带来巨大挑战。单一供应商的整体解决方案对云原生安全体系化建设来说是最好的选择。数世咨询将覆盖了业务开发、构建、部署、运行以及数据保护全业务流程的安全能力称为“全栈云原生安全”，要实现“全栈”能力，除了具备以上导图中提及的各阶段安全能力以外，还有三个必备要素：



图例：全栈云原生安全

- **DevOps 和安全工具集成**

DevSecOps 的实践将安全无缝融入开发和运维流程，自动化安全工具的集成使得安全评估、漏洞检测和合规性审核变得更加高效，减少了手动干预，确保了安全措施的持续自动化执行。

- **全生命周期内的资产可见性**

云原生全生命周期中出现的虚拟化主机、镜像、容器以及微服务等资源可能数以万计，且动态变化。资源的全面可见性不仅仅意味着实现对海量资产的管理，同时还需实现追踪和监控这些资产之间的动态关系，为管理员提供资产状态和配置的实时洞察。

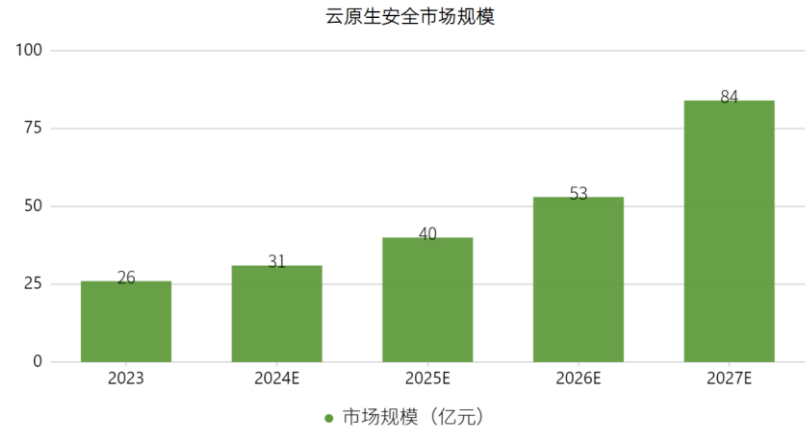
- **开发与安全运营双向反馈**

双向反馈机制是云原生应用开发与安全运营间的信息沟通，可以让开发团队依据生产环境的表现来优化代码和应对安全威胁，同时使运维团队能够依据开发阶段的反馈来优化部署和安全策略。

2.市场情况

2.1. 市场规模

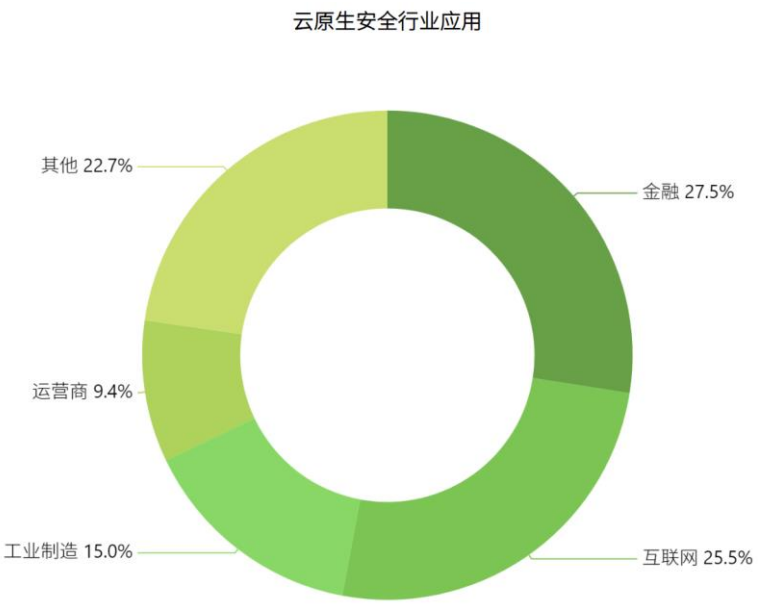
本报告的调研选择了九家具备云原生安全能力的典型企业、并结合线上线下客户访谈。根据统计，2023 年云原生安全市场规模约为 26 亿元，受三年疫情及国内数字经济大环境的影响，预估 2024 年市场规模增幅不大，预估 31 亿元左右。相信从 2024 年开始 ，市场规模逐渐有较大增长，预计到 2027 年云原生安全市场有望达到 84 亿元。



图例：云原生安全市场规模及预测

2.2. 行业应用

云原生安全在行业的应用 TOP4 为：金融（27.5%）、互联网（25.5%）、工业制造（15%）、运营商（9.4%）。



图例：云原生安全行业应用

金融行业在数字化转型的进程中一直扮演着排头兵的角色，云原生在金融领域的应用已经逐步由“面向云迁移应用”的阶段演进到“面向云构建应用”的阶段。近两年来，几大国有银行加速利用云原生技术进行底层架构的云化升级，实现业务的快速迭代和灵活部署。最大集群节点数量达数万规模，同时在运行业务容器超过 20 万。

互联网行业对业务快速迭代、高可用性和弹性有很高的内在需求，在云原生化方面表现出极高的活跃度和创新能力，据估计，80%以上的互联网企业已经实现了云原生化。业务集群从小规模的几十个节点到大规模的数十万个节点不等。

随着 IT 架构的革新，传统行业也在不断拥抱云原生。**工业制造**比如新能源汽车企业普遍应用云原生架构实现业务的快速部署。**政**

务、能源、交通等部分行业试点应用云原生化改造，使用容器搭建业务系统。

运营商的云原生安全需求更多的来自对软件及容器镜像供应链的管理，主要对镜像来源、软件成分分析、以及组件准入的检查等。部分研发单位，开始构建 DevOps 流程，融合云原生安全工具进行业务试点。

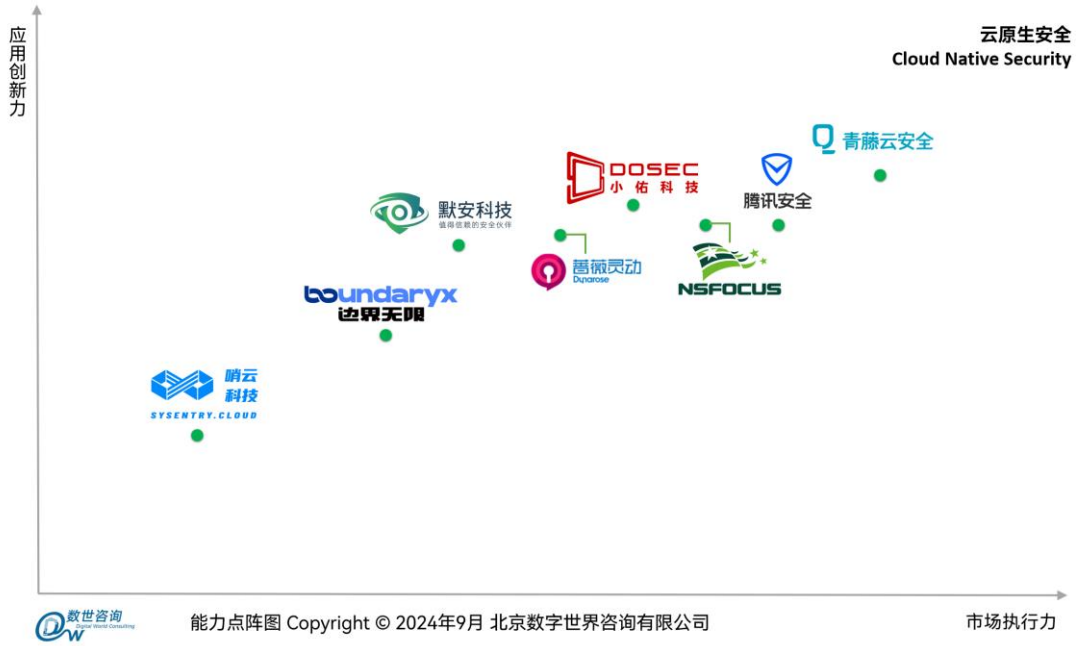
国内行业的云原生项目近两年来有显著增加，据调研的安全企业反馈，2023 年所实施的云原生安全相关的项目跟往年同比增长 50%到 300%不等。

云原生安全应用依赖于企业业务开发的 DevOps 建设流程。调研发现，目前大多数的国内企业在云端业务改造时，往往是根据自己的预算以及技术能力有选择的分步进行， 因此对于云原生不同阶段的单项安全工具，仍然有单独的安全需求。比如，代码安全测试及代码供应链管理，容器扫描与漏洞管理、针对云原生开发及运营环境的配置检查工具等。

3.能力企业

国内九家具备云原生安全解决方案和产品的厂商参与了本次调研，分别是（按公司简称首字母排序）：**边界无限、绿盟科技、默安科技、蔷薇灵动、青藤云安全、山石网科、哨云科技、腾讯安全、**

小佑科技，按照横轴市场执行力、竖轴应用创新力，通过能力点阵图 的方式展现如下：



图例：云原生安全企业点阵图

由于各厂商的技术发展路线不同，不同厂商在云原生安全领域的技术起点以及技术深度多有不同。调研发现，尽管安全厂商都在着力打造全流程云原生安全能力体系，但目前仅有个别厂商能够接近实现“全栈”。

尽管云原生安全技术的重要性和需求不断增长，实际应用场景中对传统云安全产品仍然存在较大比重的需求，比如云防火墙、云WAF、云工作负载安全产品等。同时具备云安全与云原生安全解决方案的厂商在有混合安全需求的项目竞争中更具优势。

安全厂商在云原生领域的产品及能力：

技术起点	厂商	产品或方案	能力标签
云工作负载安全	青藤云安全	青藤蜂巢·云原生安全平台	全栈云原生安全能力 基于一个 Agent 实现云工作负载&容器一体化安全 8 年主机安全/容器安全技术积累
容器安全	小佑科技	镜界容器安全防护平台	容器视角出发的云原生全流程安全防护能力 基于安全容器的轻量级、无侵入式部署
	绿盟科技	云原生容器安全平台	云原生漏洞发现和风险管理领域领先 容器全生命周期一体化安全管理 融合代码供应链安全管理
微隔离	蔷薇灵动	蔷薇蜂巢微隔离平台	内生于容器平台的微隔离能力 支持跨集群部署

			高性能的流量分析和策略管理
	山石网科	云铠主机安全防护平台	基于主机/容器的微隔离能力 云主机/工作负载综合安全能力 多云一体化安全管理
代码安全/供应链安全	默安科技	尚付 CNAPP 云原生保护平台	全栈云原生安全能力 业务全流程资产及安全可视化、云原生安全态势感知 8 年 代码/供应链安全技术积累
容器运行时安全	边界无限	靖云甲 ADR 应用检测与响应系统	兼容多种运行环境的运行时安全防护（RASP） 云原生环境流量安全、API 安全、数据安全防护能力
云原生配置安全/API 安全	哨云科技	哨云景御安全管理平台	无代理的云原生基础设施安全检查与风险管理 多云安全管理快速部署
SaaS 化云原生	腾讯安全	“ 4+n ”一体化安全	防火墙、WAF、主机安全、数据安

安全		防护体系	全四道核心防线 可定制 SaaS 化云原生安全能力 基于大数据/AI 技术的威胁发现与安全管理

4.发展趋势

云原生安全与业务深入结合

许多业务系统对安全的要求不仅仅是安全合规，更多的需要安全与业务深度集成。以金融行业微隔离安全管控为例，由于涉及大量敏感的交易数据和个人隐私信息，对安全管控的要求极为严格。还有其安全需求和安全策略经常性地变化，这就需要安全产品不断贴合用户需求，进行功能进化。当安全策略在成千上万个主机节点、几十万容器间进行下发或更改，这给安全工具的专业度与处理性能提出了很高的要求。

云原生安全向“全栈”安全能力方向进化

前文提到目前国内许多企业在构建云原生项目时，还是根据自己的预算以及技术能力分步进行的，主要影响因素有两个，一是企业的云原生化变革，需要组织架构也要做相应的调整。二是要实现开发与运营的全流程化，在与业务融合时也存在不少技术上的困难。

但降本增效是企业永远的追求，业务的云原生化改造实现开发与运营的一体化恰恰很好的满足了企业的根本诉求，云原生安全也会向“全栈”安全能力方向进化。

人工智能与云原生安全互驱动

人工智能（AI）在安全领域的应用正随着大型模型的发展而迅速进化，其核心优势在于提高安全检测的准确性、响应速度和管理效率。AI 通过机器学习和深度学习算法，能够从大量数据中识别异常行为和潜在威胁。而 AI 的有效运作离不开丰富的安全知识库和大量的安全数据，云原生安全与开发运营流程的深度结合产生的实时、动态、细粒化到微服务级别的安全数据，也会促进人工智能在安全领域的能力进化。

云原生安全能力 SaaS 化

数世咨询在“云安全资源池”报告中提到：“安全资源池与云原生技术融合，实现更灵活便捷的部署和扩展”。实际上，云原生正在重塑云安全的业务模式并为云服务商带来更大的益处。比如以腾讯安全为代表的公有云服务商已开始将云安全能力，通过云原生化模式部署，以实现降本增效。与传统的虚拟化资源池模式的安全 SaaS 相比，云原生模式的安全 SaaS 更能充分利用云计算资源，真正实现了安全能力可编排和弹性调度。

信创安全产业助推云原生安全发展

信创安全专注于提升国产软硬件的安全性和自主可控性，面对多样化的 CPU 架构和操作系统，国产安全产品的适配工作充满挑战。而采用容器化技术的安全解决方案能够提供对不同软硬件环境的广泛适应性，从而简化信创安全产品在国产化过程中的适配工作。根据数世咨询信创安全市场报告中的调研分析 ，信创安全市场按 35%的年复合增长在加速发展，预计 2027 年市场规模超过 160 亿，信创安全产业的浪潮，也在同时助推云原生安全的快速发展。

5.代表厂商优秀案例

某股份制银行一站式智能化云原生安全运营平台建设案例

（本案例由 青藤云安全 提供）

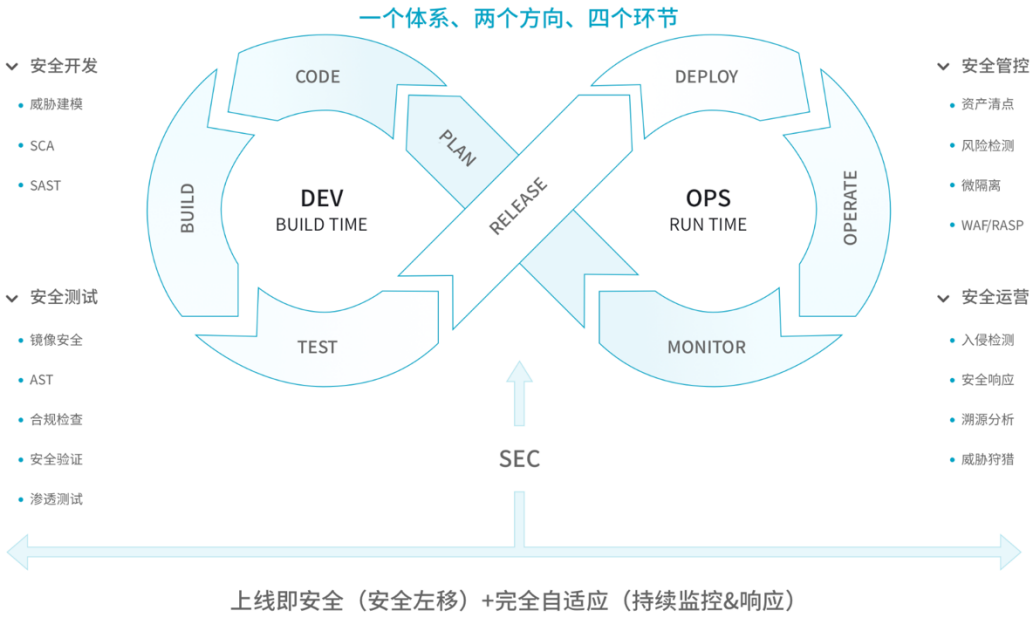
项目背景

在政策、市场的双轮驱动下，金融数字化转型进入关键阶段，以容器、微服务、Serverless 为代表的云原生技术凭借其快速部署、弹性、可扩展性等特性，成为金融机构数字化转型过程中降本增效、提升自身业务敏捷性的重要引擎。与此同时，云原生引入了大量新的基础设施，安全防护对象发生了颠覆性变化，容器以及容器云逐渐成为工作负载的主流。面对这些新技术带来新的安全挑战，某股份制银行急需引入新的安全手段。

解决方案

青藤通过对该股份制银行业务及其支撑平台进行调研梳理和风险评估，遵循国家和行业信息安全相关标准并借鉴国内外最佳实践，充分考虑云原生业务性能和安全防护的契合点，为客户打造了一站式智能化云原生安全运营平台。

整个平台通过“一个体系、两个方向、四个环节”，以 DevOps 流程为中心，覆盖云原生的整个开发过程，将安全防护嵌入到每个步骤，如下图所示：



方案说明：

1. 在开发阶段（Dev），遵循“安全左移”原则，做到上线即安全。

通过早期定位和解决安全问题，减少攻击面和潜在的运行问题，做到“上线即安全”，而不是把安全问题都留到线上环境中去解决。例如对镜像层安全检查、应用层风险检查、基础设施层安全检查。

（1）镜像层安全检查

通过“镜像安全”，发现镜像的软件漏洞、木马病毒、敏感信息等。通过“容器风险”，发现运行容器中的应用漏洞、应用弱密码等问题。

（2）应用层风险检查

微服务安全，通过 web 扫描组件，发现微服务中的 web 漏洞问

题。

（3）基础设施安全检查（包括主机、K8S 编排工具等）

通过“集群风险”功能，对集群中各组件的安全漏洞进行检查。

通过“合规基线”，设置安全基准线，检查不安全配置问题。

2.在运行阶段（OPS），遵循“持续监控&响应”原则，做到自适应安全。

在整体安全落地的时候，进行云原生安全的全生命周期管理，包括对工作负载清点与可视化、微隔离、入侵检测、安全响应、溯源分析等。

（1）工作负载清点与可视化

细粒度清点工作负载，并可视化容器访问关系。

（2）微隔离

使用微隔离可对容器的网络访问进行控制。

进行事件应急，发生问题后，可以采用隔离方式阻止威胁进一步扩散。

（3）入侵检测和响应

针对运行时的入侵行为进行检测和发现，并提供响应处理方式。

（4）溯源分析

通过威胁狩猎主动发现未知威胁，犹如网络空间的“黑匣子”，记录各种日志数据，可用于各种网络安全事件分析，溯源整个攻击过程。

目前，该平台支撑客户 400 余个业务系统，3500 余个应用，超过 4 万余个应用容器和 2 万余个业务进行全生命周期安全防护和监测服务，支持 ARM 架构、AMD 架构，支持在此架构下的任何操作系统上部署，并且平台 Agent 可以支持所有的国产化操作系统，例如 ARM 架构的银河麒麟、中标麒麟等。通过 2 年多的稳定运行，该项目完成 DevSecOps 安全实践落地，实现业务上线即安全，完全自适应。

方案优势

青藤一站式智能化云原生安全运营平台建设方案，通过真实场景验证，能够有效解决各行业云原生发展中的安全问题，具备 3 大显著特征：

先进性：该方案是云原生安全防护创新性的代表。230 万行代码，全部自主开发。每一行代码，都会经过严格的 SDL 审查。整个方案提供覆盖 Build、Ship、Run 全生命周期安全保护，助力企业完成 DevSecOps 安全实践落地，实现业务上线即安全。

实用性：该方案能够帮助安全人员看得清、管得了、防得住、同时还能原生融合到企业的平台环境中。整体上，能够全自动化、细粒度的对工作负载进行分析，并可视化工作负载之间的网络访问

行为，让安全人员真正做到看得清。还能集成到企业的 DevOps 流程中，实现覆盖容器全生命周期的安全风险管理，真正实现管得了。此外，还提供多锚点的基于行为的检测能力，能够实时、准确地感知入侵事件，并快速进行响应处理，真正做到防得住。整个方案还能实现与企业其它安全产品进行联动和融合，以实现信息共享，协同作战。

可推广性：该方案目前已经能够适配所有行业，此外在国产操作系统和芯片适配上也已经做到了行业第一，已经具备全行业推广的条件。

客户价值

青藤一站式智能化云原生安全运营平台建设方案，凭借科学的、结构化的、全生命周期的云原生安全保障体系，帮助客户安全人员清晰了解容器资产、准确定位风险漏洞，有效提高工作效率，同时提升了安全人员的综合管理能力和技术能力。同时，该方案的威胁监测能力，聚焦在系统层的威胁监测，关注系统层的入侵行为及影响，较网络层威胁监测具有高的准确性和有效性。相较于统扫描工具的流程，过去需要用 1 小时的漏洞扫描已经缩减到 6 分钟，效率提升 10 倍，成为行业示范项目。

在近两年的行业攻防演练中，该平台顺利完成基于容器的租户安全漏洞扫描、渗透测试、镜像安全加固、安全威胁监测与应急等服务内容，共计发现安全漏洞 1500 余项，分析高危组件 5 大类，拒

绝内部攻防演练获取权限 196 次。平台上线以来，共计发现恶意命令 169021 条，Web 后门、本地提权等高危操作 1000 余次。方案的实际安全能力获得用户的认可和好评。

数世咨询
Digital World Consulting

第三方独立

- 完全第三方背景
- 独立分析师团队

调研对象

- 700+网络安全企业
- 年均500+深度沟通
- 年均2000+小时访谈时长

服务对象

- 国家、行业监管机构
- 行业客户及用户
- 网络安全产品&服务供应商

服务内容

- 国家、行业智库
- 细分领域等调查研究报告
- 为服务对象提供面对面咨询
- 为产业各方提供资源对接

合作方式

- 各类报告定制
- 年度企业观察列表
- 活动赞助
- 投资FA

北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布过《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全 100 强》、《中国数字安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业 700 余家，以及 150 余家有网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区鲜鱼口街 90-2 号网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆

免责申明：

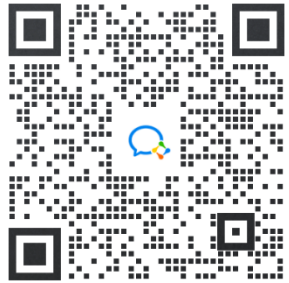
本内容非原报告内容；

报告来源互联网公开数据；如侵权请联系客服微信，第一时间清理；

报告仅限社群个人学习，如需它用请联系版权方；

如有其他疑问请联系微信。

行业报告资源群



微信扫码 长期有效

1. 进群福利：进群即领万份行业研究、管理方案及其他学习资源，直接打包下载
2. 每日分享：6+份行研精选、3个行业主题
3. 报告查找：群里直接咨询，免费协助查找
4. 严禁广告：仅限行业报告交流，禁止一切无关信息

微信扫码 行研无忧

知识星球 行业与管理资源

专业知识社群：每月分享8000+份行业研究报告、商业计划、市场研究、企业运营及咨询管理方案等，涵盖科技、金融、教育、互联网、房地产、生物制药、医疗健康等；已成为投资、产业研究、企业运营、价值传播等工作助手。

数世咨询
Digital World Consulting
数字安全领域独立第三方调研机构