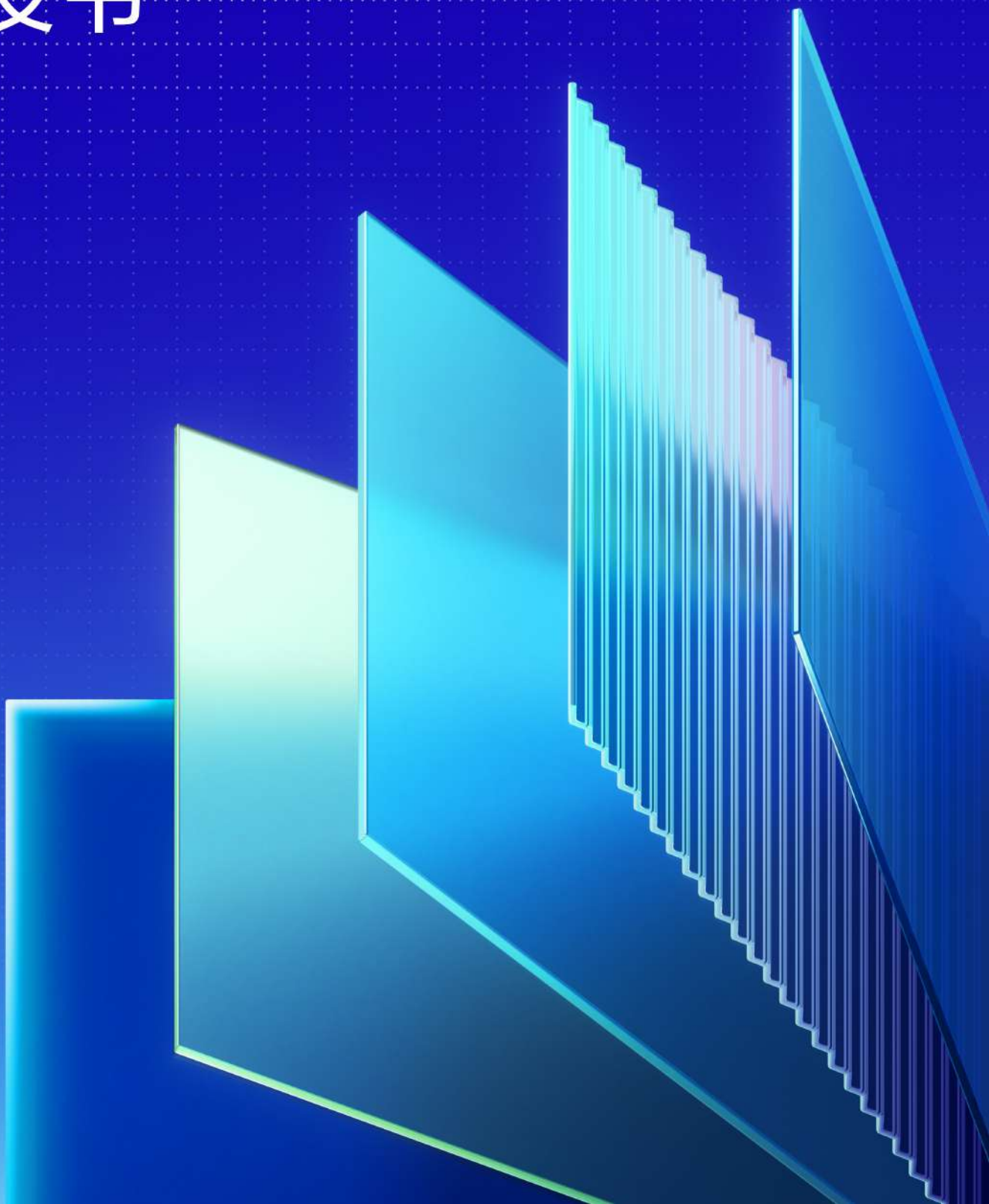
信众智
CIO智力输出及社交平台

企业网 D1Net
企 业 I T 第 1 门 户

腾讯安全
Tencent Security

中国云原生安全实践

白皮书



中国云原生安全实践白皮书

主编：潘贤真 纪庆 殷皓 张志强

编委：董文辉 徐展 付蓉洁 Eric Yong 唐共军
陈娟娟 查士加 刘亚萍

出品：信众智CIO智力输出及社交平台
企业网D1Net
腾讯安全

前言

近年来，随着新技术的持续发展，数字化已成为推动社会经济发展的重要路径。云计算成为底层基础设施，助推企业数字化转型，加速产业互联网落地；但云计算出现以来，安全性一直是云计算所面临的最大挑战。

为缓解传统安全防护建设中存在的痛点，促进云计算成为更加安全可信的信息基础设施，助力客户更加安全地使用云计算，云原生安全理念兴起。国内外第三方组织、服务商纷纷提出以原生为核心构建和发展云安全。

2015 年是云原生进入系统性、有序发展的年份。云原生经历 7 年的发展，已经进入到大规模实践阶段。企业网 D1Net 云安全专家认为，伴随云原生进入到大规模实践阶段，中国云原生安全市场也正迎来爆发式增长态势。

为了进一步了解中国云原生安全市场需求，描绘云原生安全典型规划方案，提炼云原生安全成功实践模式，企业网 D1Net 采取案头研究、专家访谈、问卷调查等方式收集了大量的云原生安全数据。企业网 D1Net 联合业内知名的云原生安全技术专家、信众智 CIO 专家、研究专家，组成云原生安全研究工作组，对这些数据进行了广泛而深入的挖掘。现在，呈现在大家面前的《中国云原生安全实践白皮书》，就是云原生安全研究工作组的最新成果。

本白皮书共分四章。第一章，中国云原生安全需求分析；在简要介绍了云原生理念

兴起的背景与优势后，分析了中国云安全市场企业信息安全投入状况、当前云原生安全市场所处的发展阶段，随后重点分析研究了企业全生命周期对云原生安全的关注点，当前云原生架构面临的安全风险，以及企业对云原生安全产品的需求和云原生安全建设管理需求。这些分析研究，为后续云原生规划方案的编制和最佳实践的选择与提炼提供了逻辑依据。第二章，典型云原生安全规划方案；首先明确了云原生安全总体规划原则，强调了云原生安全能力架构搭建的核心原则，提出了云原生安全的六大支柱；对业内大家较为关注的云原生安全方案选型问题，本白皮书主要介绍了主流云原生安全平台与工具，以及选型注意事项；最后，分别从两个视角介绍了云原生安全体系。第三章，中国云原生安全最佳实践；首先介绍了业内知名的腾讯云原生安全的功守道，然后分享了游戏行业、文创行业、物流业云原生安全最佳实践。第四章，中国云原生安全未来展望；首先对云原生安全未来发展趋势进行了展望，并结合行业洞察、调研数据与统计工具，对中国未来几年的云原生安全市场规模进行了预测；其后，针对大中型、中小型企业云原生实践提出了相关建议。

本白皮书的重点观点与主要发现如下：

- **企业上云状况。**调研数据显示，当前只有 17%的企业是私有化部署，公有云占比在 25%以上的混合云部署企业占比达到 51%。分行业来看，互联网和相关服务业、金融业中有更高比例的企业在实施 25%以上的混合云部署。分营收规模来看，大中型企业中实施公有云、混合云部署的比例更高。
- **企业云安全支出。**今年企业安全投入占整体投入的比例约为 2.9%；对比前几年，信息安全支出占比从 2019 年的 0.98%提升到 2020 年的 1.08%，再到 2022 年调查时的 2.9%；这表明，近几年中国信息安全投入占比在迅速提升，已接近全球信息安全支出占比水平（约为 2.5~3.2%）。调查数据还显示，明年中

国企业安全投入将以较大幅度增长，预计年增速达到 23%。

- **企业对云原生产品的需求。**企业对云原生安全产品有更高的要求。调研显示，企业认为云原生安全产品体系应覆盖数据加密（60%）、主机安全（58%）、防火墙（56%）、容器安全（55%）等。
- **云原生安全规划原则。**根据云原生安全的最佳指导建议，云原生安全建设一定要遵循三同步原则，“同步规划、同步建设和同步运营”，围绕要保护的对象来逐层构建。这与传统的安全防御体系有较大差异。
- **腾讯云原生安全的攻守道。**腾讯安全总结了企业云原生安全运营能力建设需要注意的四个关键点：一是做好镜像的安全管控；二是主动容器集群层面的安全加固；三是强大容器运行时的安全防护；四是建立基本的容器资产大盘应急。
- **云原生安全发展趋势。**纵观历史，信息安全总是伴随业务的发展而演进，在这样的大背景下，云原生安全自然而然成为未来几年云安全的主要发展方向。未来几年，云原生安全发展将呈现四大趋势：生态化、服务化、内生化、轻量化。

我们希望，通过白皮书中的观点和经验总结，有助于企业数字化转型中云原生安全能力的建设，使广大企业能够尽早将云原生安全方面的风险防患于未然。

目 录

图表目录

第一章

中国云原生安全需求分析

第一节 从云安全到云原生安全

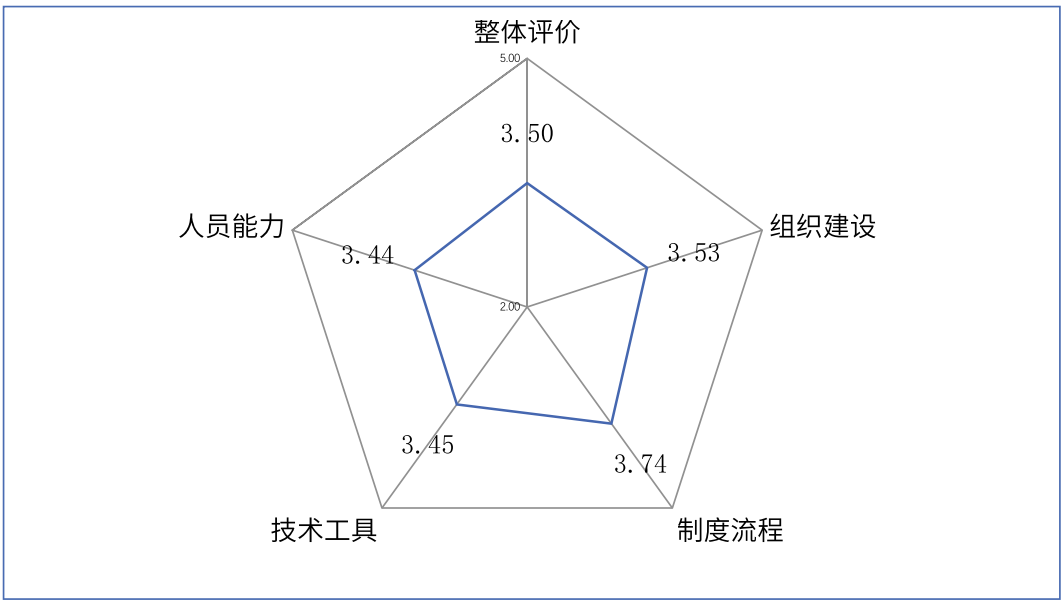
一、传统云安全存在痛点

近年来，随着新技术的持续发展，数字化已成为推动社会经济发展的重要路径。云计算成为底层基础设施，助推企业数字化转型，加速产业互联网落地；但云计算出现以来，安全性一直是云计算所面临的最大挑战。

相比传统 IT 模式，对云计算的安全性提出了更高且更复杂的要求。传统网络结构中时常遇到的 DDoS、黑客入侵、病毒木马等安全问题在云平台上仍旧存在，又增加了诸如虚拟机逃逸、服务横向穿透、云资源被盗用、发布不良内容或攻击其他服务器的滥用行为等一些新的安全问题。与此同时，由于数据上云使得数据安全逐渐成为云计算安全的核心，在云计算环境中，数据被集中存储到统一管理控制的云存储区域内，一旦发生安全问题，后果将更为严重。

为了解目前企业在云安全方面面临的挑战，企业网 D1Net 于 2022 年 8 月围绕云安全主题，针对互联网、金融、制造等行业企业开展了问卷调查。调研数据显示，在采用 1-5 分制评价中，当前企业安全建设完善度整体评价得分只有 3.50 分，尤其是人员能力、技术工具偏低，分别得分为 3.44 分、3.45 分；这表明，当前企业云安全建设存在明显短板。

图表 1 企业安全建设完善度评估

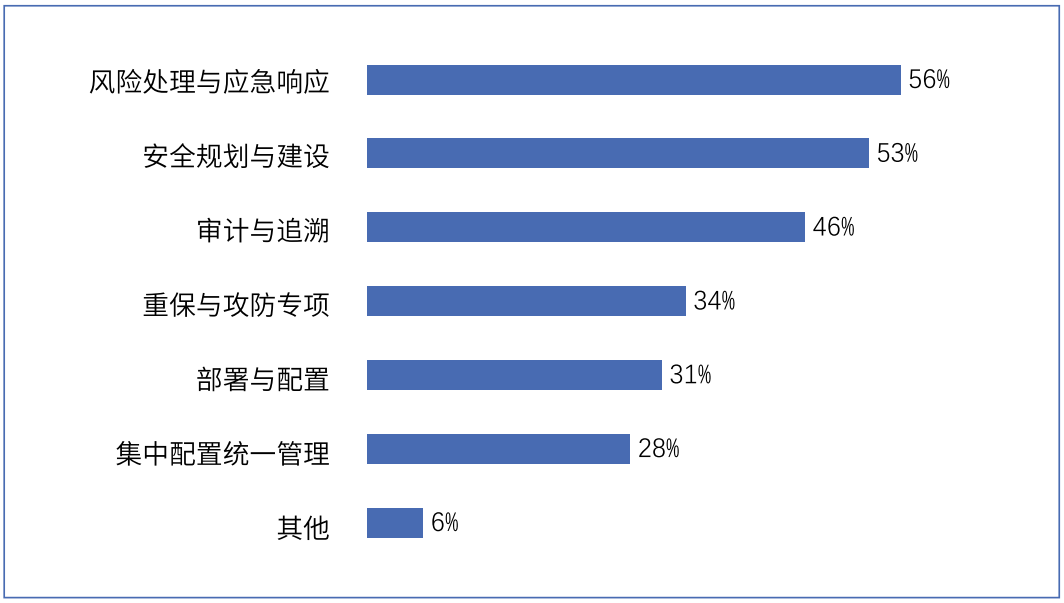


注：调查采用 1-5 分制评价，1 分为最低分，5 分为最高分，上述数据为得分平均值。

资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

进一步的调研表明，当前企业面临的安排挑战主要来自以下几个方面：风险处理与应急响应（56%）、安全规划与建设（53%）、审计与追溯（46%）。

图表 2 当前企业面临的安全挑战



资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

实践是检验真理的唯一标准。让我们听听企业用户是如何说的吧！在企业网 D1Net 对部分行业企业的开放式访谈中，我们听到了来自企业一线的声音：

—“数据安全，权限安全，网络安全。需建立更短的响应时间。”

—“安全要求和用户体验的矛盾，安全审阅的效率和项目建设的紧急性等。”

—“挑战在如何把安全推广至全企业的安全意识，在工作中人人都有信息安全意识和保护概念。”

—“人员信息安全意识不足，没有独立的信息安全部门，外部信息安全环境恶化。”

—“勒索防护、业务系统控制、生产业务数据安全。”

—“方法体系不足，技术沉淀不够。”

通过大数据分析、词云图呈现，我们发现，当前企业信息安全风险点主要来自数据安全、病毒、勒索以及安全和体验的矛盾、安全风险监测等。

图表 3 当前企业信息安全风险点词云图

序号	文字	权重
1	数据安全	80
2	病毒	45
3	勒索	42
4	信息安全	34
5	安全意识	31
6	泄露	26
7	漏洞	20
8	内部人员	17
9	人才	15
10	攻击	15
11	网络安全	15
12	意识	15
13	应急	15
14	信息	15

资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

二、云原生安全理念兴起

〔一〕云原生安全理念

为缓解传统安全防护建设中存在的痛点，促进云计算成为更加安全可信的信息基础设施，助力客户更加安全地使用云计算，云原生安全理念兴起。国内外第三方组织、服务商纷纷提出以原生为核心构建和发展云安全。

Gartner 提倡以云原生思维建设云安全体系。基于云原生思维，Gartner 提出的云安全体系覆盖八个方面。其中，基础设施配置、身份和访问管理两部分由云服务商作为基础能力提供，其他六部分，包括持续的云安全态势管理，全方位的可视化、日志、审计和评估，工作负载安全，应用、PaaS 和 API 安全，扩展的数据保护以及云威胁检测，客户需基于安全产品实现。

Forrester 以 37 项指标评估公有云平台原生安全能力。Forrester 认为公有云平台原生安全（Public cloud platform native security, PCPNS）应从三大类、37 个方面去衡量。从已提供的产品和功能，以及未来战略规划可以看出：一是考察云服务商自身的安全能力和建设情况，如数据中心安全、内部人员等；二是云平台具备的基础安全功能，如帮助和文档、授权和认证等；三是为用户提供的原生安全产品，如容器安全、数据安全等。

云原生安全厂商、服务商提出的云原生安全理念能否有效落地，就要看它是否与企业用户头脑中期望的云原生安全理念相吻合。企业网 D1Net 围绕“您认为一个好的云原生安全产品体系应该有哪些核心理念？”问题，通过对行业企业的开放式访谈，听到了很有代表性的声音：

—“贯穿数字化全生命周期的安全防护和持续监控、分析。”

—“好用、易用、实用、弹性可扩展、性价比高。”

—“API 资产生命周期管理、API 敏感数据管控、API 攻击防护、API 资产发现、API 访问行为管控。”

—“平台安全，集中管控，事前安全方案设计和审阅，安全与用户体验的平衡等。”

—“安全防护融入整个生命周期，让业务、技术和安全协同工作以生产更安全的产品。”

通过大数据分析、词云图呈现，我们发现，当前企业认为一个“好”的云安全产品体系理念，要突出管控、生命周期、API、易用等要素。

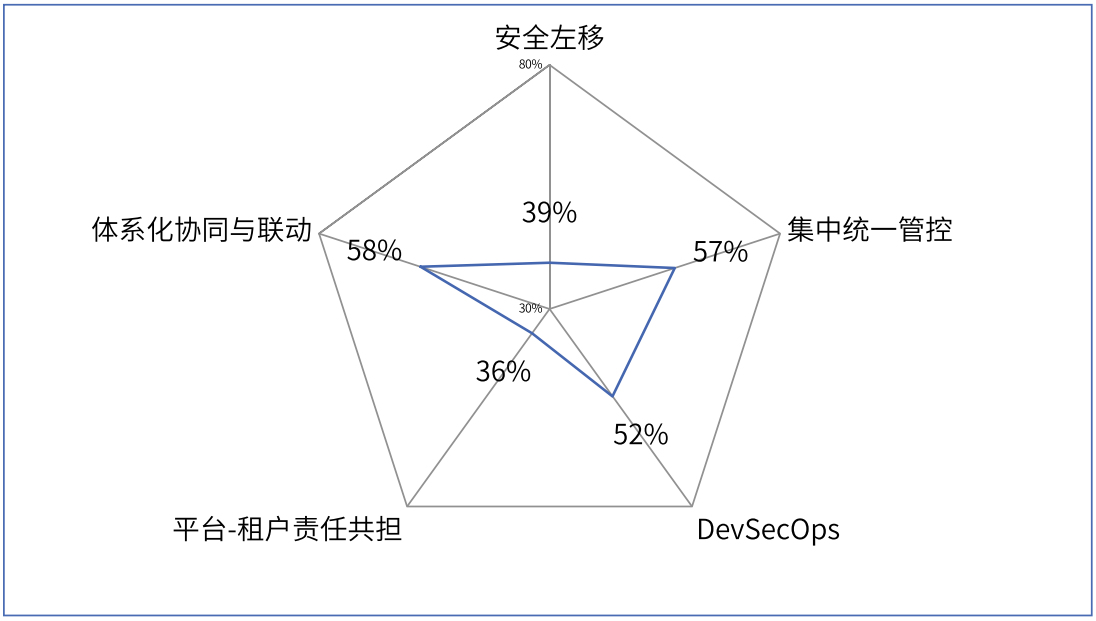
图表 4 企业认为一个“好”的云安全产品体系应具有的理念

序号	文字	权重
1	管控	80
2	生命周期	76
3	API	64
4	易用	60
5	防护	57
6	体系化	53
7	管理	45
8	架构	38
9	信任	38
10	容器	38
11	实用	34
12	监控	34
13	安全可靠	34
14	技术	30
15	简单	30
16	原生	30

资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

在企业看来，云原生安全最为核心的理念，应是体系化协同与联动：云上、终端和边界的安全产品需要体系化协同与联动（58%），集中统一管控：安全产品体系需要集中统一管控（57%），DevSecOps：安全防护融入整个生命周期，让业务、技术和安全协同工作以生产更安全的产品（52%）。

图表 5 企业认为与安全相关的最为核心的理念



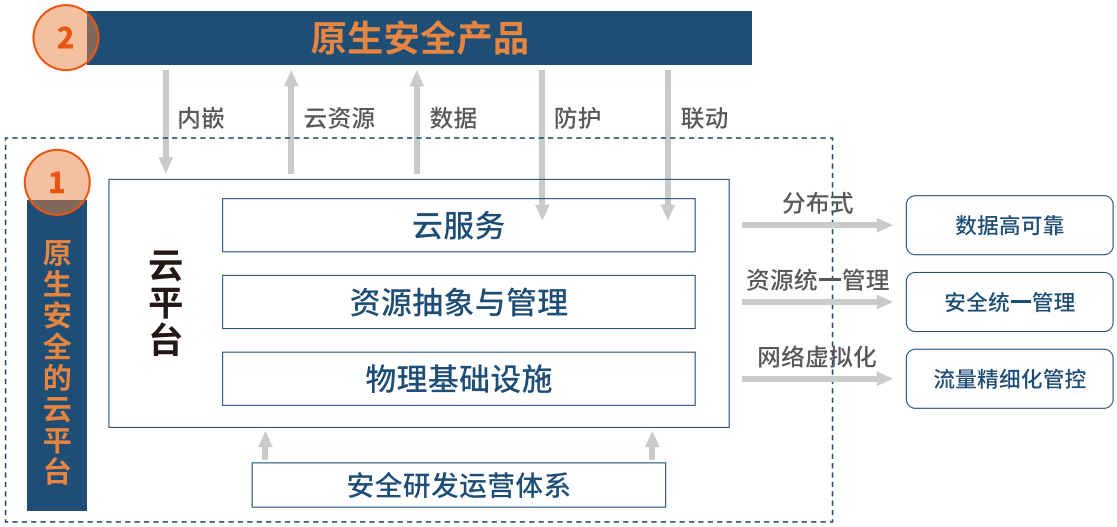
资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

〔二〕云原生安全定义

国内外各组织、企业对云原生安全理念的解释略有差异。结合我国产业现状与痛点，我们认为，云原生安全是指云平台安全原生化和云安全产品原生化。安全原生化的云平台，一方面通过云计算特性帮助用户规避部分安全风险，另一方面能够将安全融入从设计到运营的整个过程中，向用户交付更安全的云服务；原生化的云安全产品能够内嵌融合于云平台，解决用户云计算环境和传统安全架构割裂的痛点。

作为一个全新的安全理念，云原生安全旨在将安全与云计算深度融合，推动云服务商提供更安全的云服务，帮助客户更安全地用云。

图表 6 云原生安全架构



资料来源：《“云”原生安全白皮书（2019 版）》

〔三〕云原生安全价值

云原生安全价值主要体现为四个方面：保持动态价值实现，推动安全与云计算的深度融合，实现系统更广泛意义上的安全，促进实现安全普惠。

在动态变化中保持业务价值的实现。传统数据中心时代，安全问题就是企业 IT 管理所要面对的重大挑战，云计算时代，企业仍面临巨大的安全挑战。伴随云原生开发部署模式渐成趋势，整个技术生态环境包括产品、标准、技术方法以及解决方案都在持续演进，这就要求 IT 决策者要能时时刻刻跟踪并理解复杂的技术设计，特别是 IT 安全主管领导，要能在动态发展变化的技术领域中保持业务价值的实现，并在技术实践的过程中将安全集成到各个流程环节中。

推动安全与云计算的深度融合。作为一种新兴的安全理念，云原生安全并不只是为了解决云原生技术所带来的诸多安全问题，而是更加强调以原生的思维来构建云安全，推动安全与云计算的深度融合。一方面，用户在实际业务生产中所遇到的部分安全风险问题，可以通过云计算的特性来规避；另一方面，在涉及运营的整个 IT 流转过程中，要能够将安全管控融入其中，将更加安全的云服务交付给用户；合理有效地利用云计算所具备的弹性伸缩、分布式存储、资源统一调度、网络虚拟化等特性，对大部分安全风

险问题进行有效遏制，更为方便地实现系统的高可用性和数据的高可靠性，还能够让安全管理统一化、精细化、实现流量管控隔离等多种安全能力。

有助于系统实现广泛意义上的安全。如果在企业规划上云之时或在云平台建设的过程中就开始考虑融入安全建设，那么将对解决传统安全防护模式中存在的主要问题提供更多帮助。云原生安全的一部分能力实际上是将安全能力内嵌于云平台，这让基于云的产品在部署之后可以很好地实现数据的互联互通，让安全产品得以联动，分配的安全资源也能充分地得到利用，基于安全的各种解决方案的成本都能得到有效降低，实现真正意义上的安全。

云原生安全体系促进实现安全普惠。与传统 IT 系统架构相比，云计算将资源和数据的所有权、管理权和使用权进行了分离，云上安全由云服务商和云客户共同分担，云计算责任共担模式已成为业界共识。云原生安全体系能够全面保障云计算安全责任的落实，让安全惠及各类上云客户。

三、云原生安全的优势

云原生安全的特点是强调安全产品原生化。服务商提供内嵌于云、能够有效解决云上安全风险的原生安全产品；用户能够利用原生安全产品，建设与云计算环境融合的安全体系与架构，规避传统安全架构与云计算环境割裂等问题，更加安全地使用云计算。内嵌于云的原生安全产品，能够充分了解和利用云平台，最大限度发挥安全防护能力，极大程度提升云计算客户体验。

原生安全产品的特性和优势主要体现在四个方面：

采用内嵌方式而无需外挂部署。内嵌方式具备多种优势：一是无需安装，云计算客户通过简单配置即可使用，比外挂部署更加便捷。二是运行更加稳定和安全，外挂部署通常基于代理实现，代理本身存在一定的安全和稳定性风险，同时代理部署可能对云上 IT 系统造成影响；而原生安全产品与云平台相融合，运行更加稳定和安全。

充分利用云平台原生的资源和数据优势。一方面，原生安全产品利用云计算的计

算、存储、网络等资源，实现自身安全防护能力的弹性扩容，解决传统安全产品数据存储空间受限、计算能力不足等问题；另一方面，与传统安全产品相比，原生安全产品能够更便捷、全面地获取云平台内数据，通过整合、关联分析云平台内各类数据，深入挖掘潜在的安全风险。

可以与用户云资源、其他原生安全产品有效联动。原生安全产品因与云平台深度融合，能够对云资源进行更有力的控制，各原生安全产品之间能够有效协同：一是能够自动识别云资源，迅速感知云资源的状态和信息；二是对风险资源进行主动处置，在发现安全事件时，不仅仅生成告警信息，还能够自动联动相关云资源或其他原生安全产品，对安全事件采取处置措施和防护手段，实现从检测、告警到处置的安全运营自动化闭环。

解决云计算面临的特有安全问题。与传统 IT 系统架构相比，云架构因引入新技术、运营模式变化等原因，面临新的安全风险，如虚拟化、容器技术实现了 IT 资源的细粒度隔离，物理设备不再是资源承载调度的最小单元，物理安全边界消失，用户之间、用户与云平台之间的安全隔离十分关键；云计算资源按需分配，可随时释放，动态性强，因此，资源的迅速识别和有效管理成为难点；云服务的不当配置是造成云上安全事件的重要原因……总之，原生安全产品能够充分考虑云计算面临的新安全风险，为客户云计算环境提供更有力的保障。

第二节 中国云原生安全现状分析

一、中国云安全市场企业信息安全支出

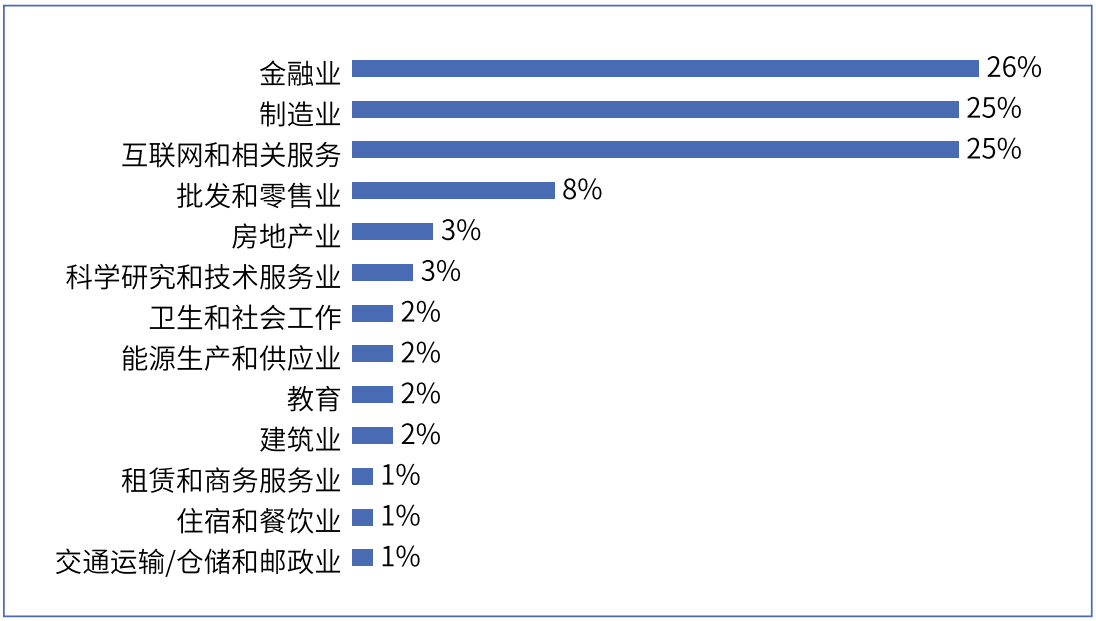
〔一〕云安全企业用户特征

2022 年 8 月，企业网 D1Net 围绕云安全主题，采用网上调查方式，对相关企业进行了问卷调查，共调查了 119 个有效样本；样本覆盖不同行业、不同营收规模、不同 IT 预算、不同上云状况企业。

调研显示，受访企业所属行业主要分布在金融业（26%）、制造业（25%）、互联

网和相关服务业（25%）。在调查实施前，基于企业网 D1Net 云安全研究专家对行业现状与未来发展潜力洞察，我们采用重点抽样调查方法，特选择部分重点行业企业进行调查，以最大限度地反映中国云安全市场企业用户实际分布状况和未来发展潜力。

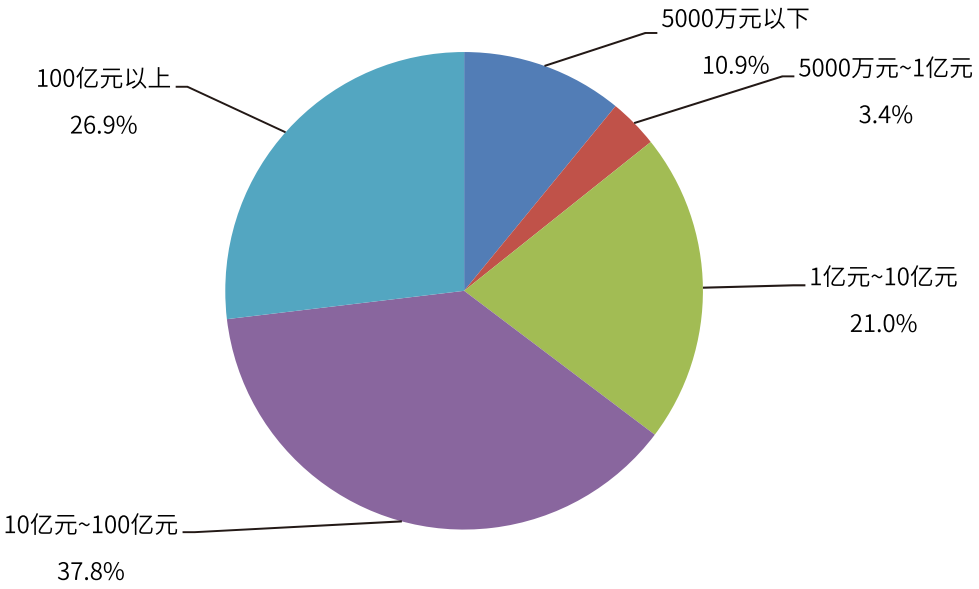
图表 7 受访企业所属行业分布



资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

企业营收规模可从一定程度上反映用户的云安全服务购买能力。调查统计数据显示，在受访企业中，上年年营收规模在 10 亿元~100 亿元的企业占比最高，为 37.8%；年营收规模超 100 亿元的企业占比 26.9%；年营收规模为 1 亿元~10 亿元的企业占比 21.0%；年营收规模为 5000 万元~1 亿元的企业占比 3.4%；年营收规模为 5000 万元以下的企业占比 10.9%。

图表 8 受访企业上年年营收规模分布

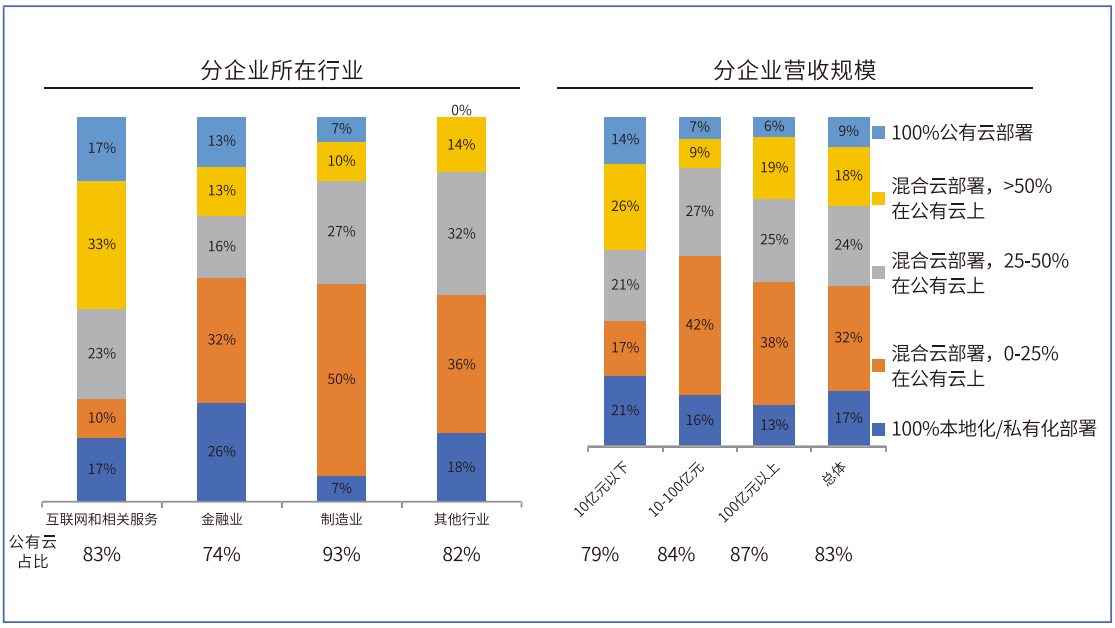


资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

〔二〕云安全企业上云状况

近年来，随着新技术的迅速发展，中国企业上云亦风起云涌。调研数据显示，当前只有 17%的企业是私有化部署，公有云占比在 25%以上的混合云部署企业达到 51%。分行业来看，互联网和相关服务业、金融业中有更高比例的企业在实施 25%以上的混合云部署。分营收规模来看，大中型企业中实施公有云、混合云部署的比例更高。

图表 9 当前中国企业上云状况

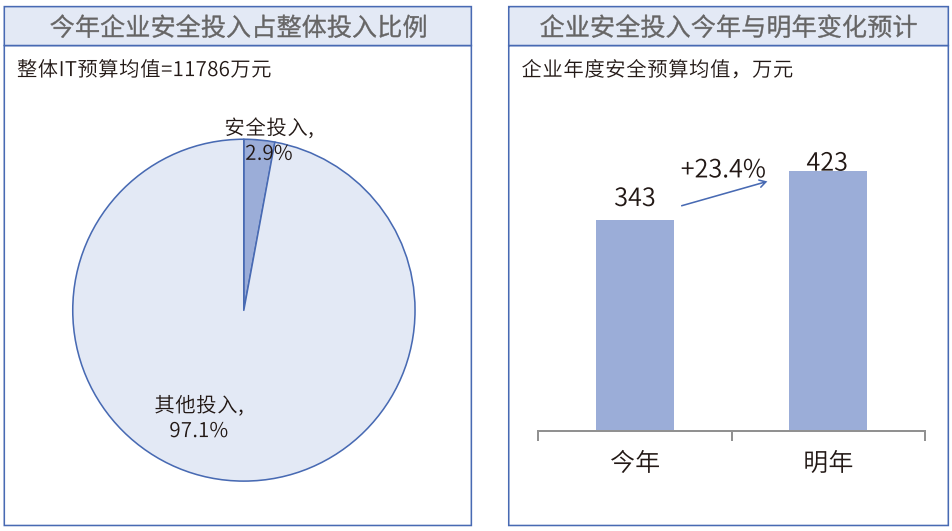


资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=30/31/30/28/42/45/32/119 个样本

〔三〕云安全企业安全支出

企业信息安全支出金额直接与云安全市场规模相关，也会明显影响企业的战略布局与市场开拓决策。调研显示，当前中国企业的整体 IT 预算平均每家为 11786 万元。今年企业安全投入占整体投入的比例约为 2.9%；对比前几年，信息安全支出占比从 2019 年的 0.98%提升到 2020 年的 1.08%，再到 2022 年调查时的 2.9%；这表明，近几年中国信息安全投入占比在迅速提升，已接近全球信息安全支出占比水平（约为 2.5~3.2%）。调查数据还显示，明年中国企业安全投入将以较大幅度增长，预计年增速达到 23%。

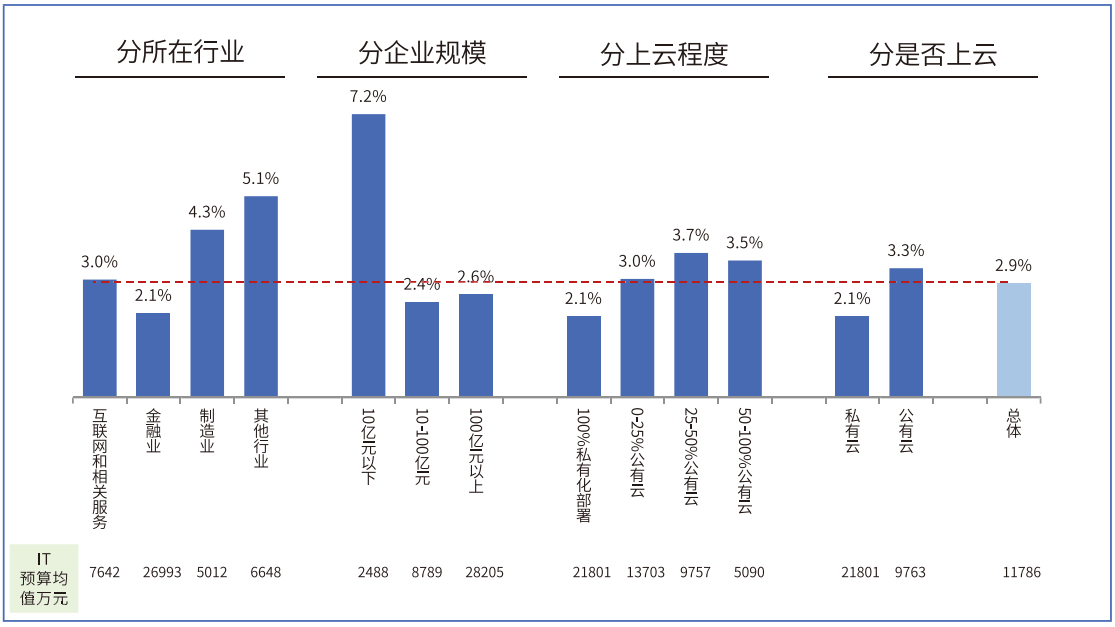
图表 10 中国企业 IT 总预算额及安全投入占比



资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

分类型来看，制造业及其他行业企业、营收规模在 10 亿元以下的企业、公有云部署在 25%以上的企业，其安全投入占比较高。

图表 11 不同类型企业今年安全投入占企业 IT 总预算的比例



资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查；
n=30/31/30/28/42/45/32/20/38/29/32/20/99/119 个样本

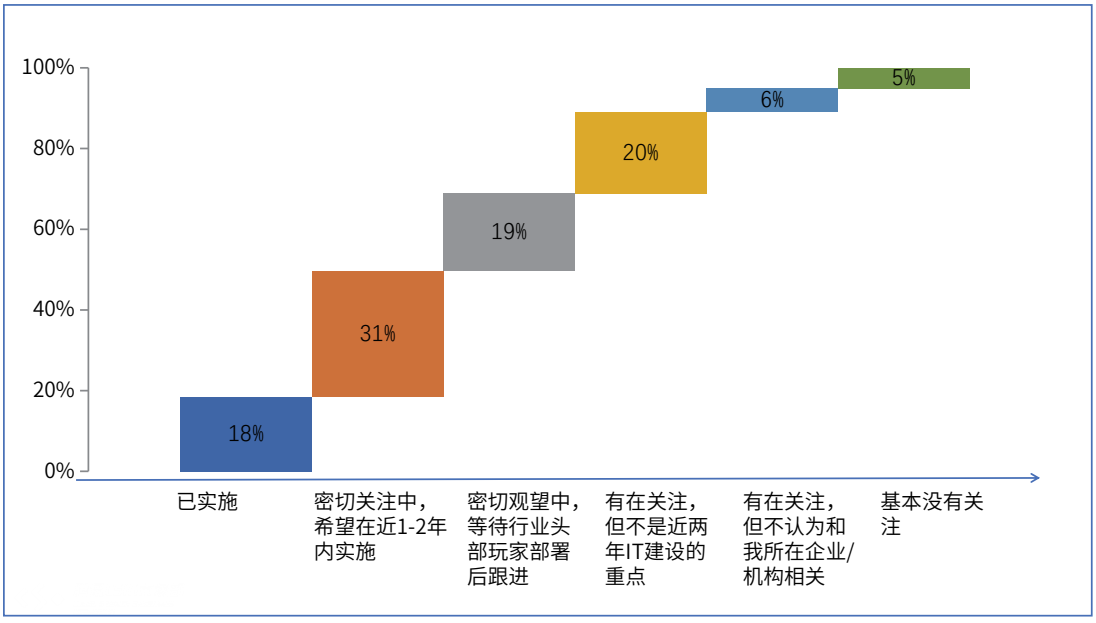
二、当前云原生安全市场所处发展阶段

2015 年云原生计算基金会（CNCF）成立，是云原生进入系统性、有序发展的标志。云原生经历 7 年的发展，已经进入到大规模实践阶段。

云安全能力一直是云计算平台发展的主要方向，快速增长的云计算需求也会带来云安全发展的新趋势。根据相关机构统计数据，中国云安全市场呈现爆发式增长趋势。2021 年中国云安全市场规模达到 117.7 亿元，同比增长 46.4%。预计 2022 年，中国云安全市场规模将达到 173.3 亿元左右，同比增长 47.2%。这意味着，中国云安全市场规模将连续 4 年增速均超过 45%。

企业网 D1Net 云安全专家认为，伴随云原生进入到大规模实践阶段，中国云原生安全市场也正迎来爆发式增长态势。企业网 D1Net 最近调查数据显示，当前已有 18%的企业实施了云原生安全建设；有 31%的企业表示在密切关注中，希望在近 1-2 年内实施；还有 19%的企业在密切观望中，表示等待行业头部玩家部署后跟进；而只有 5%的企业表示基本没有关注。

图表 12 当前企业对云原生安全的实施与关注状况



资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

三、中国云原生安全应用现状

在数字化阶段，数据对于任何企业来说都是最重要的资产，尤其是企业的核心业务数据和用户数据。时至今日，企业对于数据是否上云的问题一直存在疑虑，最主要的原因是出于数据安全的考量，数据上云后，一旦出现问题，再从架构上进行迁移并非易事。即便如此，在数字化浪潮的推动之下，越来越多的企业逐渐将业务应用和数据（包含了越来越多的敏感数据）部署到云上，新的安全问题不断出现，安全形势十分严峻。因此从整体来看，数据的安全性保护已经成为所有企业在云计算时代必须直面的挑战。目前来看，我国各类云计算环节的整体安全态势依然不容乐观。

由于基于传统安全防护的方法天然存在一些问题，且很难再有更大的改善，因此在业务系统上云之后的云计算时代，云上安全也开始呈现原生化的发展趋势。上云是大势所趋，在国家推出的各项相关政策的指引下，各行各业都已经接受并开始或正在积极地推进企业应用上云。然而云服务安全体系的建设却相对缓慢。在大部分企业应用开始上云的过程之初，通常安全设计并没有同步开始，也就是说安全方面的建设往往都是相对滞后的，直到云平台架构搭建完成，业务应用开始投产后，安全管理部门才开始介入，基本上整个安全管理仍是作为补充措施来保护云平台服务的各方面安全，而且大部分防护方法仍旧以传统安全防护模式为主。

传统安全防护方案，基本是针对各个环节、以各类安全软硬件设备进行堆砌的方式来构建安全管控能力。仔细分析会发现，传统安全设备的软硬件价格不菲，但资源利用率较低，而且由于云环境已经不同于传统数据中心结构，安全设施部署变得困难，云上数据的捕获也出现了问题，同时传统安全产品都很封闭，各自之间的联动性很差，数据很难在相互之间流转。总体来看，此时的安全防护主要依赖于安全人员的人工投入和安全设备的不断叠加来实现，因此安全成本不断堆积、提高，使得企业对安全管理问题的态度和安全效果不断地出现摇摆。

放眼全球，排名前列的公有云服务商在安全投入上都不遗余力，而且在主动防御、执法联动方面做了大量投入。2022 年 8 月微软官方宣布，在过去 12 个月中

（2021.7-2022.6），微软通过漏洞奖励计划支付了 1370 万美元（约 9299 万元）奖金，期间发出的最大单笔奖金达到 20 万美元，平均每个漏洞的奖金超过 12000 美元（约 8.5 万元）。

国内排名靠前的公有云服务商，各自在安全领域也投入了大量的建设资金，而且拥有较为完善的运营机制。针对安全隐患的监控预警响应能力，安全漏洞的及时修补能力，基于其核心（云）业务的需求，都作为核心产品能力的一部分来驱动安全建设。如果从简单的边界防御能力而言，基于上述公有云的边界防御能力，已经远远超过了任何一家传统企业自身所能够建设的安全能力。公有云服务商动辄几百、上千人的信息安全团队，与传统企业几人到几十人的规模相比，是不可同日而语的。

随着公有云的普及，企业对云安全的认知发生了颠覆性的改变。数据存储在年投入 100 万元的环境里安全，还是存储在年投入几千万甚至上亿元的环境里安全呢？答案是显而易见的。但是安全管理的关键是打开环境的密钥和通道。再厚重的保险箱，如果把钥匙和密码公开，那么安全防护就形同虚设了。

针对安全投入不足的现状，充分利用云上的安全建设，借力、共享云服务公司在安全防护上的大力投入，成为今天中国企业在安全防护能力提升方面弯道超车的一个捷径。在这一基础上，企业也可以战略性地调整信息安全的投资方向：充分利用云原生环境的能力，把资源投入聚焦在安全运营，而非基础设施建设方面，反而可以给企业带来更大回报。企业可以合理投入运维管理，享受千万元级别的安全基础设施的防护能力，以及 7x24 小时运营商级别的实时防护。

我们曾见过各种乐观的上云预测，但是除了互联网、游戏等“云原生”公司的核心业务，大量传统企业上云的占比并没有那么高，尤其是公有云占比。在这样的前提下，传统非云原生体系的安全挑战，并未彻底解决，仍旧是大量企业的首要安全防护对象。由于大量紧耦合的 ERP 系统以及历史遗留系统的存在，如果没有强烈的业务需求，还是会持续存在于私有云或 IDC 环境中。

相关调研显示，当前超过 90%的现代应用融入了开源组件，平均每个应用包含超过

124 个开源组件，49%的开源组件存在高危漏洞，企业安全防御充满“未知恐惧”。

企业，尤其是传统企业，伴随着数字化转型的驱动，未来信息化、数字化的投入方向一定是更激进地向云原生的方向发展。基于云原生安全的考虑，公有云（有规模可行的商业化运营云服务）毋庸置疑，是最佳选择之一。同时，传统的边界防御模式，也要积极地向运营+云原生 SDL（安全研发生命周期管理）过渡，以适应未来的技术发展方向。

第三节 当前云原生安全需求分析

一、云原生应用全生命周期对云原生安全的关注点

企业需关注的首要重点是云原生的运营安全。传统安全更重视边界防护，而云原生安全更重视持续安全。云原生场景下的敏捷开发部署模式对传统边界防御的安全模式而言是一个极大挑战。传统应用研发人员可以大量依赖安全运维来提供基础的边界保护，但是，在云原生模式下，云原生应用的工作负载（workload）是安全保护的关注点，而不再是应用边界，这就需要研发团队对安全防护有颠覆性的认知改变。

云原生的一大关键特性是应用的横向扩展能力，而工作负载、应用功能的可扩展性往往成为研发人员的聚焦点。当工作负载需要扩展时，安全往往会被忽视。如何在敏捷响应业务需求做开发交付的过程中，保持对安全的关注度，需要研发人员做出重大的文化转变。

云原生安全需要从研发起始就开始关注，而不是一个事后的管控动作。围绕敏捷开发的全生命周期，云原生安全也可以从四个阶段进行管理：研发、分发、部署、运营。

研发阶段：

安全必须在云原生研发过程中的起始阶段就得到充分重视。这一阶段的安全测试要尽早寻找违规及配置错误。通过快速的反馈闭环机制，运用需求迭代的方法，推进研发团队持续改进，并尽可能在同一功能发布周期内完成工作。

云原生应用全生命周期的安全必须基于代码级别的最佳设计，以下是需要关注的十二大关键要素：

1）代码库管理：版本管控、多重发布均能跟踪；

2）依赖关系：显式声明和隔离依赖项；

3）配置：将配置存储在环境中；

4）后备服务：将后备服务视为附加资源；

5）构建、发布、运行：严格分离构建和运行阶段；

6）过程：将应用作为一个或多个无状态进程执行；

7）端口绑定：通过端口绑定导出服务；

8）并发：通过流程模型向外扩展；

9）可处置性：通过快速启动和正常关机实现稳健性；

10）开发/生产环境奇偶校验：尽可能保持开发、过渡和生产环境相似；

11）日志：将日志重新格式化为事件流；

12）管理流程：将管理/管理任务作为一次性流程运行。

分发阶段：

和传统应用开发相比，云原生开发的持续迭代发布非常频繁。当团队启用 CI/CD 流程后，一定要建立测试机制来验证工作负载的完整性、发起工作负载的流程以及运维方式。尤其需要关注的是当开源被大量使用，且包含第三方 runtime（运行时），复杂程度会大大提高。

在云原生场景下，分发的基础运算环境是容器，而容器依赖于镜像。这个镜像很可能成为整个安全里最危险的一个环节。下载镜像时必须高度关注，扫描漏洞、恶意软件、代码漏洞，否则整个网络可能被轻易侵入。

部署阶段：

云原生应用的部署一定要经过以下测试工作量的验证来确保其完整性，而不是仅仅依靠自动化测试或者用户验收测试：

1）验证项目已签名；

2）容器映像遵循安全策略；

3）可以验证主机适用性。

云原生应用在部署阶段也可以高度关注其“可观察性”。日志、系统指标都可以在云原生环境下，集成应用本身的安全设计，提供更透明的安全监控：

1）指标：显示问题发生；

2）跟踪：指向问题；

3）日志：帮助问题溯源。

运营阶段：

云原生的生产运营环境需要极其严谨的安全策略以及资源/权限授予。类似于 Linux 内核的 cgroup，限制、隔离，以及对资源/流程资源的监控都是非常重要的关注点。

Runtime 执行指令通常包含调用第三方程序，互相调用的组件必须得到充分的保护。下列三点也需要特别关注：

1）仅允许批准的进程在容器命名空间中运行；

2）防止未经授权的资源访问；

3）网络监控用于检测恶意工具的活动。

二、当前云原生架构面临的安全风险分析

随着 DT（大数据时代）的来临，云计算已经成为企业的大数据承载平台，与大数

据、人工智能一并，成为新的基建核心。伴随云计算市场规模的不断扩大，应用场景涉及个人数据存储、企业数据及应用支撑、国家公共基础设施支撑等多个领域，云计算的发展趋势自然已成为业界关注的焦点。

如果仅仅是简单粗暴地将本地系统迁移到云平台，很难发挥云计算的多种天然优势，如弹性扩展、敏捷灵动、资源池化和服务化等特征。为此，提出在云上设计应用程序的理念，使应用程序得以在云中以最佳的模式运行，从而充分发挥出云平台的弹性、敏捷及分布式架构的优势，这就是今天所谈到的云原生架构。当然，新的技术、新的架构一定会伴随新的安全问题，引发新的安全事件。

〔一〕云原生安全典型事件

1. 特斯拉 K8S 挖矿事件

2018 年 2 月 20 日，云安全公司 RedLock 发文披露特斯拉公司的 K8S 集群曾在数月前被入侵，黑客在特斯拉的 K8S 集群中部署了挖矿程序。据报道，特斯拉 Kubernetes 被入侵的直接原因是，其 Kubernetes 集群的 Dashboard 处于未授权即可访问状态，且暴露在互联网上。对于一个 Kubernetes 集群来说，控制 Kubernetes Dashboard 意味着能够直接向集群下达指令，严重情况下攻击者甚至能够逃逸出容器，进而轻易控制集群中所有宿主机节点。这是一种等同于甚至超过域沦陷的风险，却往往得不到相应的重视。

在应用云原生技术时，不少人还保持着传统安全意识和观念，对 Web 攻防、系统攻防加强防范，对密码暴力破解和反弹 shell 不会掉以轻心。然而，安全总是存在短板效应的。一个简单的未授权访问漏洞没有及时处理，就可能为攻击者提供不费吹灰之力、长驱直入的机会，固若金汤的城池也会因此沦陷。

2. Docker Hub 容器挖矿事件

随着云原生的发展，云原生容器的应用也日益广泛。Docker Hub 作为全球最大的公共容器镜像仓库提供商，其所提供的镜像的安全风险直接对整个生态产生巨大影响。

根据互联网信息披露，某个挖矿黑产团伙曾利用 Docker Hub 上传特制的挖矿镜像，通过蠕虫病毒快速感染 Docker 主机，进而下载相关镜像进行挖矿。期间共制作 21 个恶意镜像，累计下载传播量达 342 万，获取了不低于 313.5 个门罗币，获利 54 万余元。

据分析，随着容器应用发展加速，频繁爆出容器相关的安全事件，黑产团伙通过容器服务器漏洞传播的蠕虫病毒，通过下拉挖矿镜像进行获利，已然是现阶段容器相关黑产的主流手段。当企业在享受云原生带来的技术红利时，更应该重视和建立容器安全防护体系。

〔二〕云原生架构下的安全风险

云原生实质上是一种软件架构设计的思想，对应用架构进行变革，最大化地利用云提供的分布式、松耦合、弹性、敏捷、易扩展与可靠等能力。在早期的云计算时代，安全和云平台的结合不算紧密，大部分以安全资源池这种外挂形式来实现云安全，而云原生安全需要安全能力和云原生平台紧密结合，真正成为内生安全，这将是云安全的巨大挑战和机遇，也可以说云安全的未来是云原生安全。云原生架构的诞生，大幅度地提升了业务的部署效率，同时安全威胁依然无处不在，而且手法更加新颖，难以及时排查。

1. 多变的威胁源

云原生系统一般都具备轻、快、不变的基础设施、弹性服务编排、微服务化等特征，引入云原生架构的同时，也衍生出各种新型安全风险和潜在的威胁源。云原生系统初始就包含各种原生的云组件，架构涉及公有云、私有云、云服务等等，每种架构都有不同的漏洞、安全风险和复杂的攻击面。

企业现有的系统安全管理方法已经无法适应快速迭代更新的云原生架构，事实上，云原生架构已经从根本上打破了应用程序的安全性，传统静态视图的安全漏洞管理方式无法跟上云原生架构下的动态环境，容易出现盲点，急迫需要一种新的方法来帮助企业更好地识别潜在风险，并使其能够在开发和交付流程中快速解决安全风险。随着云原生环境部署规模的扩大，功能组件将成倍增加，对于运维人员来说，维护这些组件的可用

性，将变得难上加难。

2. 复杂的技术架构

云原生架构充分利用了云平台的弹性扩展、敏捷灵活、资源池化和服务化等特性，在改善云应用的生命周期和运行模式的同时，复杂的架构也带来了新的安全风险。

以容器为例，作为重要的应用实例载体，其轻、快、不变的基础设施特性，使其大幅缩短了应用的生命周期，秒级启动或消失，以及持续频繁的动态变化，增加了安全检测和防护的难度，如准确捕捉容器间的网络流量和异常行为等。

微服务的应用普及，将单个架构拆分成多个独立服务，组件间的交互端口数量暴增，攻击面增加，也增加了应用在端口防护、访问权限、授权机制等方面的难度。

当然还有更多，如容器的实例共享化，也带来了单个漏洞的集群化扩散，一个存在漏洞的服务被攻陷，很可能会导致运行在同主机上的其他服务受到影响，逃逸风险大大提高。

3. 模糊的安全边界

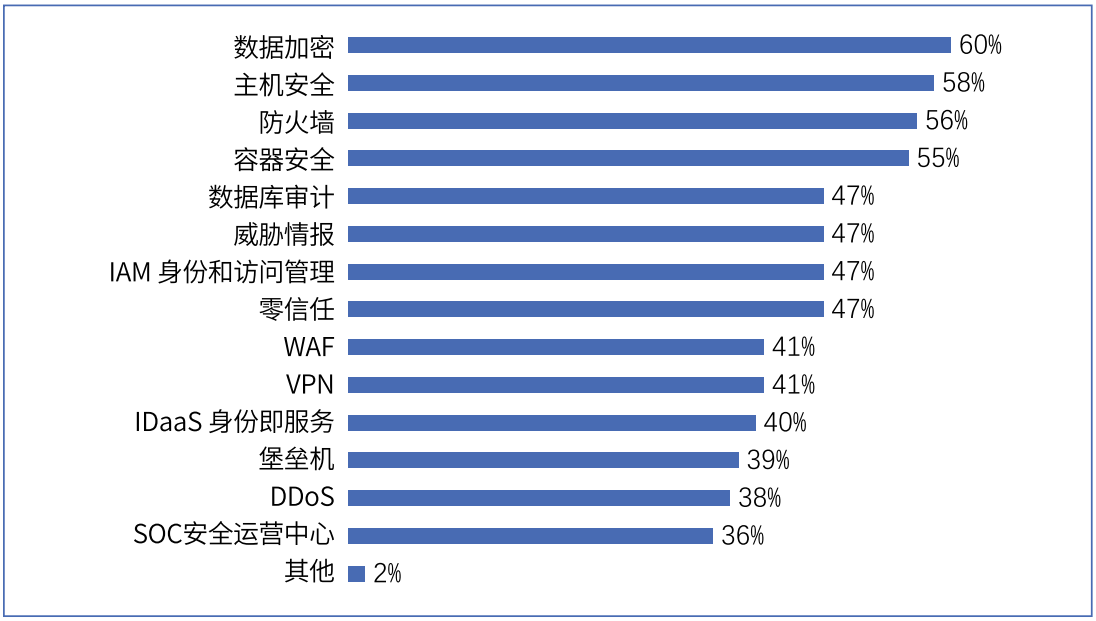
对于某些行业来说，云原生安全可能还是个新概念，企业内的安全人员还停留在传统的安全意识和观念上。比如典型的 Web 攻击、DDoS 防护、弱口令爆破等等。安全总是存在“短板效应”，任何一个被忽视的漏洞没有及时被发现和处理，都有可能造成整体安全体系的崩塌。不得不承认，云原生时代已来，云原生将成为企业新的基础设施发力点，也将成为攻击者聚焦的新阵地。

由于云原生架构原生具备轻、快、灵活、敏捷、分布式等特点，传统的安全防御体系已无法满足云原生架构的需求，这就要求新的安全体系要更加贴近资源、贴近业务，具备及时动态更新、按需动态工作负载的属性。除此之外，云原生时代也要求安全人员要具备安全左移的架构思想，从应用的开发阶段开始，就要与业务进行互动，贯穿整个生命周期，否则仍然沿用传统的后知后觉方式，复杂的结构、繁杂的组件，将会给运维及开发人员带来无法估量的工作量，甚至是无用功。

三、企业对云原生安全产品的需求

企业对云原生安全产品有更高的要求。调研显示，企业认为云原生安全产品体系应覆盖数据加密（60%）、主机安全（58%）、防火墙（56%）、容器安全（55%）等。

图表 13 企业认为云原生安全产品体系应覆盖的方面



资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

四、企业云原生安全建设管理需求

随着市场环境的变化，为适应市场，越来越多的企业意识到，要想把握新一轮的产业变革机遇，必须转变传统发展模式，从研、产、供、销及企业文化等多方面进行数字化转型，善用数据驱动业务发展，形成新的商业模式。

人工智能、大数据、5G、物联网、云计算等新技术的发展，加速推动了企业数字化转型的步伐，更好地赋能数字化。作为数字化底座，云计算一直以来都发挥着重要的功能。随着技术更新和发展，伴云而生的云原生，其实施的步伐和速度已进入爆发式增长，从消费互联网到企业级应用，赋能企业、行业的数字化转型。如何确保云原生架构的安全，建设适度的云原生安全架构，成为企业安全人员首要思考的问题和工作的重点。

〔一〕云原生安全建设技术管控需求

1. 安全技术栈

无论是业务弹性还是敏捷交付，云原生的爆炸式应用都带来颇具规模的价值。然而在云原生安全领域，攻防不对等的情况，也比其他架构严重得多，因为其技术架构多样且复杂，给企业传统安全防御体系带来诸多挑战，这也是云原生技术在企业内全面铺开的重要阻力之一。

云原生安全提出了贴近业务、安全内生等多个新概念，这就要求企业内的安全防御体系可以针对云原生架构的特性进行优化。优化的内容至少包括云原生计算环境安全、云原生应用安全、研发运营安全和数据安全，还有基础设施安全等。每个安全领域的落地都牵扯到不同的技术要求，这对企业内传统的安全技术架构造成了本质的挑战与冲击，甚至颠覆了现有的安全架构。

2. 开发安全

按照 Gartner 的云原生安全建设指导思路，要保护云原生业务的安全，就是要从应用开发阶段入手，构建应用全生命周期的安全防护体系。虚拟化安全与云原生安全是有本质区别的，虚拟化安全关注的是资源，而云原生安全关注的是应用，安全左移是云原生安全的必经之路，必须在企业内贯彻安全左移的方法论，从应用程序的源头加强应用安全防御能力。虽然这与很多企业内固化的先功能开发、再安全优化的开发流程相冲突，对研发人员的要求也有所提高，但从长远角度上会提高整体的安全水平，降低安全投入。

众所周知，在云原生时代，根据业务的需要按需调整、上线、变更的频率将会越来越频繁，这促使 DevOps、敏捷交付成为云原生重要的组成部分，并在企业中得到深度应用。如何在应用的生命周期内及时发现安全风险，成为云原生安全体系落地的重要指标。

3. 流程化与自动化

DevOps 作为重要的云原生组成部分，保证了云原生应用的发布效率，但安全性与

便捷性往往是冲突的，很难兼顾。传统安全措施对效率的影响在非全自动化流程中可能不明显。一般情况下，业务上线的安全测试和检测一般是在质量保证流程完成后进行，等所有的功能经过安全测试完成后，再确认上线。这些工作会通过邮件或 ITSM 等系统来流转，内部对其及时性有一定的容忍度。

但在云原生体系下，DevOps 作为云原生的重要组成部分，是应用的生命周期管理流程。这就要求安全管控无缝植入到这个流程中，也就是当前流行的开发安全运营一体化（DevSecOps）。DevSecOps 作为一个大的体系，除了代码安全测试，还包括制品库安全管理、运行安全策略等，所以将云原生安全产品或者工具嵌入到 DevOps 流程，也成为企业云原生安全落地的一大挑战。

〔二〕云原生安全建设文化管理需求

建立信息安全、个人隐私保护的企业文化，来应对云原生的发展趋势已经刻不容缓。信息安全风险是企业的几大最高风险之一。信息安全隐患往往会给企业带来数千万元量级甚至更大的直接金融损失，以及持久且难以估量的品牌负面影响。个人隐私保护要成为企业关注的焦点。不仅仅从合法合规角度考虑，个人隐私保护也逐渐成为企业是否关注用户利益的一个标杆，负面案例往往会导致大量用户流失，对企业的收入产生极大的负面影响。

建立企业安全文化，需要贯穿应用的全流程，从需求、设计、研发、测试、验收、发布、运营的全生命周期以及后续迭代，需要持续管理。

除了保证应用本身的安全外，安全文化还需要贯彻到应用者。系统不是万能的，也无法完全防护系统之外的安全性弱点。在系统与用户的交互中，如何让用户，尤其是企业用户，具备信息安全的警惕意识，是信息安全文化宣贯的重点之一。定期培训、案例宣传、知识测试都是手段之一；以游戏化方式，让文化宣传变得更有趣也是一个有效途径。此外，安全演练是重要的宣传手段之一，比如利用模拟钓鱼的方式让用户切身感受，进一步提升对安全隐患的警惕。

〔三〕云原生安全建设组织变革需求

1. 运营成本

云原生安全运营体系与传统的安全运营体系是有本质区别的，因为整个运维技术栈发生了很大的变化。而且云原生安全体系在运营上要求把所有的安全产品进行联动，能够对资产数据、安全数据、日志数据进行统一的管理和分析。以前的运维主要是面向操作系统安全和多种软件的安全，而现在我们需要转型和聚焦到统一的、面向云原生的、以 K8S 为通用的云资源控制层面的自动化的安全运维。企业数字化转型过程中，全面拥抱云原生的同时，为确保应用全生命周期的安全，在云原生安全方面的人才投入将会出现大幅度的成本增加，对于传统型企业而言是个不小的挑战。

2. 流程变革

大多数传统企业的安全运营方式对安全的责任主体定义明确，一般都会有专门的部门进行信息安全的建设与维护。按照以往的流程，业务系统在开发、测试后，相关人员会通过 ITSM 等系统通知安全部门进行架构或者系统安全方面的评审，通过评审之后，再正式上线。这种上线流程已经无法适应云原生架构的敏捷、快速交付需求。安全运营团队必须找到更好的运营流程，实现快速业务迭代的同时，确保云原生环境的安全。

3. 能力要求

传统企业的信息安全能力通常建立在边界防护和运营体系之上，包括网络安全、主机安全、终端安全，并逐渐延伸到数据安全、以及基础瀑布式项目交付的 SDL。基于云原生环境，企业不需要对云端集群容器做私有化建设，相对应的基础建设能力不再是关注点，但严谨的运维、运营能力变得至关重要。同时，围绕代码的安全管理，传统不具备信息安全专业能力的团队，比如研发团队、产品经理等，都需要具备安全防护思维。云原生安全能力不仅仅需要建设在云端基础设施、企业运维管理之上，同时需要赋能产品研发团队，让云原生应用变得“原生”安全。

第二章

典型云原生安全规划方案

第一节 云原生安全规划原则

一、云原生安全总体规划原则

随着技术的不断成熟与发展，企业应用云原生的范围不断扩大，云原生正加速推动企业的数字化进程。

云原生是新的技术栈，更是一种新的思维模式，只有深入地了解和理解云原生，才能更好地利用它。根据 Gartner 的调研结果，到 2025 年，超过 85%的企业将接受云优先原则，超过 95%的新数字工作负载将被部署在云原生平台上。企业已经看到云原生的应用场景所带来的红利，例如缩短应用开发周期、提升开发效率、降低总体成本等。

新技术必然伴生新的安全隐患。近年来云原生环境中的各类安全风险日益频发，云上的对抗也成为现实。如何规划、建设云原生环境中的安全架构，部署相应的安全防御能力，变得尤为重要。

根据云原生安全的最佳指导建议，云原生安全建设一定要遵循三同步原则，“同步规划、同步建设和同步运营”，围绕要保护的对象来逐层构建。这与传统的安全防御体系有较大差异。

〔一〕同步规划

在对云计算平台的基础架构进行设计规划的过程中，企业需要同步考虑安全架构，将安全融入到云架构中，并结合云计算的特点，围绕应用系统的全生命周期进行安全设计，使之具备云原生轻、快的属性，让云计算用户获得最优的安全防护能力，更加融入云原生的环境。

〔二〕同步建设

正如安全左移所强调的，在业务系统建设的初期就需要将安全控制节点植入到开发过程中，第一时间发现系统建设的问题，并及时解决，提升代码安全强度的同时，降低后期运营成本。对云原生平台进行建设的过程中，同步进行安全防护建设，同时要求参

与其中的安全产品必须具备原生特质，如弹性敏捷、轻量级、可编排。这样就可以使云内安全产品也可以像其他云内资源一样灵活、按需地进行配置。

〔三〕同步运营

一般企业的运维和安全是两个团队，因此团队之间的信息存在滞后性和差异性，相互之间不了解彼此具体的资产在云上的分布情况、使用情况和风险威胁情况。

运维团队针对云上资源的调配和处理，安全部门无法及时获悉，甚至使云上资源的安全风险逐步扩散到云下。遇到突发或紧急事件，两个团队的响应速度由于无法匹配，可能错失风险的最佳处置时间，带来不可预知的风险。

在云原生时代，企业需要构建一个符合云原生特性的安全运营机制，不要按照以前传统运营的思路去建设安全运营机制和工作运营，应该以云原生的思路去构建云安全运营体系，比如：强化“安全左移”的理念，具备事前检查风险、处理风险的能力；利用“数据驱动”的思想，收集云环境中的关键数据，进行统一纳管和分析，逐步优化；利用“自动化”手段，针对云原生环境中的安全事件和问题进行自动化的处理等。当然这需要一定时间，但是中间态的“人机共治”可以大幅度地降低人工介入的成本，提升安全事件的处理效率和准确性，逐步符合云原生架构下云原生安全运营的基本要求。

二、搭建云原生安全能力架构的核心原则

〔一〕安全能力原生化

云原生依托容器、服务网格等关键技术，实现了更轻量的隔离方式、更灵活的负载管理、更复杂的容器网络、更短的容器生命周期、以及更敏捷的开发流程。这些重要变化，使得传统的安全防护手段很难发挥应有的作用。要实现云原生安全或容器安全，一定要充分匹配云原生的特性，采用原生安全的方式，这里的原生安全包括两个方面：

一方面是原生的基础安全，也就是在基础设施和基础架构上原生地提供安全能力，使得云原生应用能够做到上线即安全。

另一方面是安全能力的云原生实现，充分利用云原生的技术优势，来实现安全检测

与防护能力，使相关的安全能力同样具备云原生的低成本、高效率和高可用等特性。

安全能力原生化有别于传统第三方外挂的安全方案，云原生安全产品和解决方案利用云计算的技术优势、数据优势，根据云的网络和基础架构，量身定制了云原生的安全产品，如下。

1.云原生的网络安全防护

可为云上用户提供免费的 DDoS 基础防护服务，默认自动开启，免安装、零维护。

2.云原生的安全访问控制

可提供基于公有云环境下的 SaaS 防火墙，主要为用户提供互联网边界的防护，解决云上访问控制的统一管理与日志审计的安全与管理需求，是用户业务上云的第一个网络安全基础设施。同时无需客户进行任何硬件和软件镜像资源的部署，即开即用，性能可弹性扩展。

3.云原生的主机安全防护

以腾讯云主机安全（CWP）为例，基于腾讯在安全方面积累的海量威胁数据，利用机器学习为用户提供资产管理、木马文件查杀、黑客入侵检测、漏洞风险预警及安全基线等安全防护服务，解决当前服务器面临的主要网络安全风险，同时支持用户对腾讯云外服务器统一进行安全防护，轻松共享腾讯云端安全情报，让私有数据中心拥有云上同等级别的安全体验。

4.云原生的 Web 应用防护

Web 业务一旦出现安全事件，将给组织带来直接业务损失及严重的品牌负面影响，甚至触犯《网络安全法》，因此具备云原生的 Web 安全防护能力至关重要。

以国内云计算腾讯云原生的 Web 应用防火墙为例，帮助腾讯云内及云外用户应对 Web 攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫等网站及 Web 业务安全防护问题。通过部署腾讯云 WAF 服务，用户可以将 Web 攻击威胁压力转移到腾讯云 WAF 防

护集群节点，分钟级获取腾讯 Web 业务防护能力，为所在企业的网站及 Web 业务进行安全运营。

〔二〕安全左移

云原生架构下，容器实例生命周期短，业务迭代更新快，同时主机上容器密度高、业务复杂，而且很多传统的安全设备和安全手段无法发挥有效的作用。在这种情况下，增加运行时安全的投入对于整体安全性的提升很难有显著的帮助。该如何降低安全运营成本，同时提升安全防护效果呢？

一个有效的方法就是最近两年经常被提及的安全左移（Shift Left），在软件生命周期的更早阶段，投入安全资源和安全能力，更有效地收敛安全问题，包括安全编码、供应链（软件库、开源软件）安全、镜像（仓库）安全等。这些方面的资源大多是白盒，相应的安全投入相对较少；而且这些资源生命周期较长，如果能保证安全性，攻击者在攻击运行实例得手后更难持久化。

基于 DevOps 协作框架实现敏捷高效的 IT 流程，是云原生架构的一个重要应用场景。Gartner 很早便提出 DevSecOps。安全左移也是实现 DevSecOps 的一个重要原则，将安全能力全面融入到 DevOps 体系中，实现面向 DevSecOps 的全生命周期安全防护。

因此想要降低云原生场景下的安全运营成本，提升运营效率，首先就要进行“安全左移”，也就是从运营安全转向开发安全，主要考虑开发安全、软件供应链安全、镜像安全和配置核查四个方面。

开发安全：需要团队关注代码漏洞，比如进行代码审计，找到因缺少安全意识造成的漏洞和因逻辑问题造成的代码逻辑漏洞。

供应链安全：可以使用代码检查工具进行持续性的安全评估。

镜像安全：使用镜像漏洞扫描工具对自由仓库中的镜像进行持续评估，对存在风险的镜像进行及时更新。

配置核查：核查包括暴露面、宿主机加固、资产管理等，来提升攻击者利用漏洞的难度。

〔三〕全生命周期的安全防护

目前，云原生的生态布局越来越大，且处于高速发展之中，基本上覆盖云原生生命周期的全技术栈。比如容器编排、微服务架构、不可变基础设施、持续交付/持续集成、DevOps 等代表性技术。DT 时代，在管理方面越来越多的企业开始从端到端进行流程优化，更关注用户的核心需求，以客户为中心；在技术方面采用云原生技术（DevOps、容器、微服务、Kubernetes 等）加速软件的开发与部署，充分发挥云原生的敏捷性、轻快性和弹性扩展的优势，优化用户响应能力和软件的迭代更新能力，从而提高业务生产效率。

云原生在提升生产效率的同时，也带来了新的安全挑战。从组织形态看，云原生安全建设和云基础设施之间的关系非常紧密，导致安全职责越发模糊，需要重新考虑安全的责任范围。云原生重新定义了组织的责任边界和协作流程，改变了组织协作方式。新的安全模式对组织、流程、技术等都有了新的要求。传统边界防护的安全理念，缺乏敏捷的部署能力，根本满足不了云原生环境下的网络安全需要。

伴随云原生技术在企业的深度应用，新的安全防护对象也在逐渐增加。比如宿主机、容器、应用、编排工具等，从而引发了一系列新风险，例如编排风险、镜像风险、微服务风险、运行时风险、网络安全风险、数据安全风险等，也增加了安全人员理解的难度，迫使原有安全措施必须进行重构，从而将安全的工作重心从过往的重视核心业务的外围安全转移到云原生环境下的内生安全，符合云原生框架下的安全要求。

面对云原生背景下的多重挑战，企业需要重新考虑云原生环境下全生命周期的云原生安全防御能力。云原生环境下，管理员看到的不是一个个虚拟机，而是一个个业务系统。云原生加速了应用开发和运维角色的融合，使云原生的 DevOps 实践成为趋势，充分发挥出 DevOps 的敏捷性和响应力，将安全防护手段融入“从软件开发到运营”的每个环节成为必经之路。

安全元素直接与云原生架构融合，形成内生安全，所以云原生安全必须以应用的生命周期为基准进行防护。针对云原生安全的生命周期安全防护，近年来业界提出了 DevSecOps 的概念，即“开发、安全和运营”的缩写，在软件开发生命周期的每个阶段自动集成安全性，从最初的设计到集成、测试、部署直至软件交付。通过这一理念，实现云原生安全的全生命周期管理，将安全能力融入整个 DevOps 流程中。

整个生命周期分为“左”，“右”两个方面。一方面，在应用开发阶段将安全的控制节点从运营侧向开发侧倾斜，开发侧主要涉及开发安全、软件供应链安全和镜像安全。这种左侧的安全节点把控，也就是前文反复提及的“安全左移”，它也是实施云原生安全的必经之路。通过以上措施的把控，以“准入”+“准出”进行安全管控，落地安全左移，减少攻击面，实现上线即安全，可以有效降低系统的运营成本和改造成本，提升系统的安全防御能力。

另一方面，在系统的运行阶段，实施“持续监控&响应”，确保自适应安全。自适应安全理念是一种以检测为主的思路，以“工作负载”进行持续的监控和分析为核心，来完成运行时的安全闭环。如对云原生工作负载进行细粒度的清点，了解运行的容器、容器内运行的 Web 原理、数据库应用等，对容器工作负载之间的访问关系进行梳理，进一步了解业务间的调用关系，锁定攻击范围，辅助策略生成等。运行时阶段中的微隔离、入侵检测、安全响应、溯源分析和威胁狩猎都是核心环节，每个环节环环相扣，来完成运行时的安全闭环。自适应安全理念通过持续的安全运营，对失陷容器进行溯源分析，找到受影响范围和入侵路径，不断进行威胁狩猎，主动发现网络中的恶意数据及潜在的威胁行为。这就是右侧的安全防护理念。通过这两个方向的安全分析和部署，建立系统性的防护体系，实现全方位安全防御。所以全生命周期的安全防御体系也是云原生安全能力架构的重要核心原则之一。

〔四〕零信任安全架构

“零信任”不是某个产品，更不是某个体系架构，而是一种理念。最初的零信任框架模型是在 2010 年由 Forrester 分析师 John Kindervag 提出的，在 Google 公司的

Beyond Corp 项目中得到应用后逐渐被国内所知。零信任框架基于身份认证和授权，重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信，是一个全面的安全模型，涵盖了网络安全、应用安全、数据安全等各个方面，致力于构建一个以身份为中心的策略模型，从而实现动态的访问控制。零信任的核心思想是“永不信任，持续认证”，一直以最小授权进行验证，阻止权限爆破的发生。

企业建设安全体系的前提是为合法对象建立信任关系，通过信任在保证业务正常的前提下降低安全成本，在运行时及时检测并消除非法主体的恶意行为，所以信任是网络安全的前提要求。在云原生场景中，微服务架构比比皆是，应用的颗粒度会被切分得非常细，一个容器通常只完成一个功能，实现整体应用系统的功能需要多个微服务之间的频繁交互，不能依靠传统固化的访问控制手段，必须采用基于业务的逻辑确定微服务之间的安全访问策略，划分微服务的边界，持续进行有效地隔离。

NIST 在 2020 年 8 月发布了最新的零信任架构。在零信任安全模型中，原生地假设业务所处的环境中随时存在未知的攻击行为，默认不存在任何信任关系，必须不断分析和评估其资产、网络环境、业务功能等安全风险。根据实际的业务行为和需求制定相应的防护措施来杜绝风险。在零信任中，这些防护措施通常要保证尽可能减少对资源（比如数据、计算资源、应用和服务等）的访问，只允许那些被确定为需要访问的用户和资产进行访问，并且对每个访问的身份和安全态势进行持续地认证和授权。

云原生的信任机制都是零信任的，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，从而减轻了网络威胁横向扩散的可能性。零信任架构最常见的实现方法依赖于加密概念。首先要用硬件或者令牌来保护特定的密钥信息，并且能够用安全的方式和平台进行通信。每个实体都能创建自己的标识，每个实体都能独立地认证其他实体（例如用公钥体系），实体之间的通信是加密且不可篡改的。最小权限原则非常重要，甚至被认为是云原生架构中最重要的内容之一，云原生技术栈的所有层面在进行认证授权的设计和实现的过程中，都需要考虑这一原则。

所以“原生的零信任安全架构”从设计上就体现了零信任理念，融合了多种安全能力，可适配各类应用场景的安全体系。基于零信任的理念，融合自适应安全的安全体系，有机形成预防、检测和响应的能力。利用云原生安全的架构和能力，通过软件定义的架构，可适配多种应用场景。此外，云中虚拟资源频繁迁移、业务按需秒级变更，所以安全策略能否跟随业务，业务间的隔离粒度能否达到最小，也是零信任的原生需求。

三、云原生安全的六大支柱

〔一〕开发安全

随着云原生的普及和发展，其技术架构复杂且业务应用越发频繁。作为云原生新基础设施载体的容器实例生命周期也变得越来越短，甚至是秒级；而且存在与操作系统虚拟化环境中现有的物理或虚拟化的安全设备无法有效协同工作的情况。此时，一味地增加系统内的安全投入无助于提高整体的安全水平。因而在云原生安全建设中，业内提出了安全左移的思路，即在云原生安全建设初期将安全投资更多地放到开发安全，包括且不限于安全编码、供应链（软件库、开源软件）安全、镜像及镜像仓库安全等。

安全左移强调在产品上线之前，更早地进行安全动作的融合。软件代码的安全漏洞是影响软件最终运行安全性的重要因素。在研发前需要进行安全方面的需求分析与设计，从用户视角优化设计并提供安全功能，引导客户安全地使用各项服务，满足产品的基本安全需求。自有代码产生脆弱性的主要原因是代码开发者缺乏安全经验和安全意识，在编写代码时没有进行必要的安全检查。为了应对代码产生的漏洞，应该在研发阶段对代码进行安全审计，包含关注第三方组件的安全，同时可以通过交互式应用测试等手段进行上线前的安全测试，将安全问题在上线前收敛，实现云安全服务的内生环境。

安全左移所投放的资源大多是白盒的，如果可以保证安全性，攻击者在攻击运行实例得手后，将更难持久化，云服务原生安全属性的发展也将满足客户的基本安全需求。

〔二〕镜像/容器安全

容器的出现直接改变了业务系统的运行方式与交付模式，实现了应用程序运行在容

器内而软件的交付变成了容器镜像的打包交付。随着云原生时代到来，容器的采用频率逐年上升。根据 Anchore 发布的《Anchore 2021 年软件供应链安全报告》显示，容器的采用成熟度已经达到较高水平，65%的受访者表示已经在深度使用容器，而其他 35%的用户则表示已开始对容器的研究和使用。容器是由容器镜像生成的，如何保证容器的安全，在很大程度上取决于如何保证容器镜像的安全。而对于容器镜像安全的保证，可以从以下几方面着手，从而提升容器安全镜像构建的效率与安全性。

1. 镜像完整性保护

确保镜像完整性是容器镜像安全的基础工作。云原生系统应为用户提供用于保障镜像完整性的机制或功能，并通过一定的控制手段阻止无法通过完整性校验的镜像部署到容器集群中。例如可通过签名技术实现镜像完整性保护，并通过与镜像构建的 CI/CD 流水线工具进行整合，实现镜像构建过程控制，从构建、测试、扫描到完整性检测的全流程管控镜像内容安全。

如果用户构建一个新的镜像，使用镜像签名与 CI/CD 流水线结合的机制进行镜像安全控制，流水线中每一个环节（如漏洞扫描、测试等）完成后均会基于镜像 Hash 值完成一次签名，最终在容器平台侧需要验证待部署镜像具备 CI/CD 流水线每一个环节的合法签名，容器平台才能够基于该镜像进行容器启动。缺失任何环节的非法镜像或被篡改镜像均无法通过最终的验证环节，从而有效地保障了镜像的全流程控制与内容完整性。业界已有类似 Google 开源的 Kritis 组件以及 Docker 提供的 DCT（Docker Content Trust）机制用于镜像完整性检测以及基于完整性进行安全控制。

2. 镜像安全基线检查

根据最佳实践的经验，制定镜像安全基线检查项，通过安全基线检查机制，针对镜像中的配置文件进行自动化检查，可及时发现不符合项。镜像安全基线主要包括所创建容器内的必要用户、容器使用可信的基础镜像、容器中必要的软件包、必要的安全补丁；还有启用容器内容信任机制、将健康检查说明添加到容器镜像、不在 Docker file 中单独使用更新命令、在 Docker file 中使用 copy 而不是 add、镜像中删除 setuid 和 setgid

权限、涉密信息不存储在 Docker file、已安装的软件包全部经过验证等。

同时，云原生系统应为用户提供功能全面的镜像漏洞扫描工具，对镜像仓库中的镜像和工作节点中运行容器的镜像进行定期检测扫描。检测扫描的内容应包括但不限于：基于权威漏洞库信息（如 CVE、CNNVD、RHSA 等）的镜像内组件安全漏洞情况、镜像不安全配置信息、镜像是否含有恶意代码、镜像是否感染病毒、镜像是否存在密钥等机密信息的硬编码情况等。

3. 镜像访问控制

与镜像仓库之间建立加密的通信通道，防止信息泄漏。同时需要对用户的访问进行身份认证、访问权限控制，对镜像变更或者提交代码进行认证，避免用户提权访问其他用户的镜像资源。

4. 容器隔离

云原生系统根据细粒程度的不同，划分为网络隔离和微隔离。网络隔离在云原生系统中多指二层子网隔离、以租户划分的隔离，其划分粒度较粗。微隔离主要针对的是东西向流量的隔离，重点是为隔离分区提供基于业务流向的视角，用于阻止攻击者进入网络内部后的东西向移动，能够有效阻止容器逃逸，平台应支持但不限于：基于命名空间的隔离、基于容器间的隔离、基于容器和节点间的隔离。具体的微隔离方案包括但不限于：基于 Network Policy 实现微隔离、基于 Sidecar 实现微隔离。

〔三〕工作负载保护

随着云原生时代的到来与发展，承载计算的宿主节点不再局限于云计算 1.0 时代的云主机；云计算 2.0 时代，容器、无服务已成为越来越多用户的选择。云原生时代的安全防护不能仅关注主机层面的威胁，更要参考云原生应用防护平台（Cloud-Native Application Protection Platform，CNAPP）的防护模型，其基础能力包括 IAC 扫描、容器扫描、CWPP、CIEM、CSPM。云工作负载保护平台（Cloud Workload Protection Platform，CWPP）背后的想法是提供一种机制，以一致的方式保护这些工作负载。CNAPP

平台的重点在于对云原生应用，跨越开发环境到运行时环境，提供全生命周期的安全防护，因此，CWPP 作为运行时环境中的主要安全能力，是 CNAPP 中非常重要的一环。

工作负载安全必须提供跨越公有云与私有云中的 VM、容器、无服务全栈的安全保护。从云工作负载的角度出发，对主机层面、容器层面、应用层面及其上承载的数据等工作负载进行全面的安全防护，自动化获取信息，智能化主动防御，与主机进行联动。一方面自动化获取主机内各类资产的信息，另一方面支持自动查杀病毒、木马，主动防御入侵行为，自主完成漏洞、基线修复，构建安全闭环和可感知能力。海量数据的关联分析能力，利用采集到的主机内各类数据，如进程、文件、系统、DNS 等的行为日志，结合云平台全网威胁情报数据，基于 AI 算法，实现多维度、高效的关联分析，提升威胁检测率与准确率。

〔四〕自动化响应

随着 DT 时代的来临，云计算获得更进一步的普及和发展，企业的云化率逐年升高，更多企业体验到了云计算给业务应用带来的灵活性、扩展性及可用性等特性，并且还有上升之势。当然，企业在拥抱云计算的同时，也开放了自己的网络，共享了资源，给网络上的各种攻击行为提供了便利。这也符合我们常说的：“互联时代，方便自己的同时，也方便了他人”。云时代的应急响应趋势也早已从“被动响应”转变为“主动感知”，传统单点对抗的应急响应已无法满足云时代的复杂攻击形态和规模。如何在攻击前做好预防措施，攻击后快速有效的自动化溯源取证和风险收敛，已经成为云时代应急响应技术的核心竞争力。

安全从业人员都非常清楚，任何高级或者复杂度很高的安全防护系统都不可能给业务提供绝对安全的运行环境。当系统遭到破坏、被意外入侵时，会不可避免地导致业务不可用，业务连续性受到影响。而应急响应的核心价值体现在突发安全事件时能够被快速有效地处理，最大限度地快速恢复业务和把损失降到最低，因此响应和恢复速度将是云上应急响应的核心竞争力。

业内通常使用的 PDCERF 方法学（最早由 1987 年美国宾夕法尼亚匹兹堡软件工程

研究所在关于应急响应的工作会议上提出），将应急响应分成准备（Preparation）、检测（Detection）、抑制（Containment）、根除（Eradication）、恢复（Recovery）、跟踪（Follow-up）6 个阶段的工作。一次完整的应急响应需要做很多事情。

通过第三方机构的调研，业内大多数企业的应急响应能力一般都可以达到第二阶段，比较好的运营商会达到第四阶段。无论第二还是第四阶段，都是建立在解决问题的角度，远未达到持续性运营和方案优化的地步。

在云时代，常规的应急响应方式对人员能力和系统的要求很高，且无法实现“主动感知”的能力。为了更好地在云上做好应急响应，做到“主动感知”，自动化响应是必经之路。通过自动化的响应机制，企业在提升云时代突发事件处理能力的同时，可降低云环境的运营成本，提升用户满意度。

〔五〕应用与数据安全

如今，数据已经成为企业新的生产要素，并作为重要的支撑依据，助推企业数字化转型。基础设施作为坚实的底座为上层应用提供稳定、可靠的服务，应用系统产生数据，而数据反哺业务产生价值。根据第三方机构统计，数据泄露是目前企业面临的最大的信息安全风险，也是当前企业各种安全防护系统建设的主要目的之一。

从业界的实践来看，数据安全对应的防护主体主要包括资产类数据（代码、算法、模型等）、办公/业务数据（方案文档、客户资料、合同资料等）、公司运营数据（财务数据、人力资源数据等）、生产数据（生产活动、售后活动等）及用户相关数据等。数据安全防护体系的思路已相对成熟，几乎都是围绕数据生命周期展开，从数据的采集、传输、存储、使用、交换、销毁等阶段，来针对不同类型数据在不同场景下区别化实施安全防护，从相关法律法规的数据安全要求，到各大云服务商的数据安全产品/云产品数据安全能力，都给云计算时代数据安全防护做了不错的指引。

在云计算向云原生架构演进升级的过程中，数据安全面临的威胁以及防护思路本质上没有明显的变化。云原生环境下，随着企业业务迭代及运维效率的提升，势必会对数

据安全防护的实施成本与运营效率提出更高的要求。

因此，云原生架构下，为了进一步显著释放云计算的效能和特性，需要在数据安全防护所需各个环节的安全能力上与云原生架构结合做升级，比如容器安全登录鉴权与租户企业组织信息映射、密码/凭据安全托管能力内嵌到对应云产品/DevOps 基础设施上，基于 Sidecar 模式做细粒度网络访问控制/API 调用异常监测等，以确保数据安全防护方案与业务层更加解耦、方案应用操作方面对上层业务更加透明。

〔六〕身份安全

在云计算背景下，业务逐渐云化、生态逐渐产业化，混合云的场景已经在企业内生根发芽。以往通过传统边界防火墙的 ACL 对业务访问进行控制的时代已经一去不复返。在云原生时代，企业已经打通了云上系统与本地系统间的身份认证体系，对内部员工和外部合作伙伴的账号、权限、行为进行统一管控，业务应用之间不再产生孤岛，可以更好地为用户提供顺畅和精准的服务，由此，身份安全成为云原生时代新的安全需求。

云原生安全要求认证和访问管理（IAM）具备面向云原生架构的身份管理、用户及服务认证能力，能够对各种对象身份进行管理。同时根据云原生环境内资产生命周期较短的特性，通过使用临时安全令牌的方式实现应用和服务的访问和鉴权，以满足云原生架构下对身份凭证的短暂性控制需求。利用 IAM，企业可以轻松管理和跟踪每个身份，并最小化地授权，甚至可以通过 IAM 识别个人和设备之间的可疑活动，利用大数据+人工智能自动化识别风险。基于零信任理念，云原生内的所有工作负载和服务都需要根据控制策略，进行持续的身份认证。

四、云原生安全的科技〔IT〕组织及流程设计

针对市场环境变化，云和 DevOps 带给业务的是无与伦比的敏捷响应能力。在这个大前提下，云原生彻底改变了企业的开发和运营模式。由此带来的组织、流程变化，也是每个企业必须面对的挑战。

通常企业的信息安全团队或者专业信息安全专家，都不是云原生应用敏捷交付过程

中的团队成员。安全团队擅长于响应控制性的流程节点，而不是作为交付流程中的资源。

受限于信息安全人才匮乏，大部分企业缺乏独立的信息安全团队，开发团队不具备专业的安全能力且无权做安全相关决策。信息安全工具大部分只是以监控、审计为目的。传统的信息安全管控大量依靠人为控制节点，例如审计、评审等，因此持续敏捷的研发交付在时间维度上就会和这一类安全管控产生冲突。同时团队往往会妥协于业务速度需求，违反安全管控的独立性，做出很多让步，这种做法通常会产生严重的安全后果。由于开发团队本身很难在放慢交付速度（影响业务结果）和规避安全管控（引入重大风险）的取舍上直接决策，因此企业必须针对云原生安全这一新要求做出改变。

组织功能设计包括以下方面：

1）**应用安全管理**：这个团队在很多信息安全组织已经存在，或者作为功能存在。作为传统 SDL（安全研发生命周期管理）的延伸或者迭代，云原生时代的 SDL 更加强调对产品研发团队本身的赋能，聚焦自有研发代码和研发过程管理。除了建设安全测试、分析工具，安全培训教育、漏洞扫描/闭环等工作，更重要的任务是在日常研发过程中，让这个团队的专家成为产品研发团队的合作伙伴，推动安全习惯的养成。

2）**安全工程**：安全工程的核心工作，有别于安全测试团队，是建设并运营自动化的安全测试工具，帮助安全管控自动化/智能化，从而在快速 CI/CD 过程中降低手工审查所需要的时间、资源。这个组织也有可能作为应用安全管理的一部分存在。

3）**安全运营**：很多在安全方面做过认真投入的企业，或多或少都会设立安全运营中心，或者在 IT 的运营部门设定相应职责。针对云原生安全，传统安全运营不仅仅要关注围绕边界防御（例如网络攻击）的传统运营模式，更要覆盖云上 4C 的安全，即 Cloud（云）、Cluster（集群）、Container（容器）以及 Code（代码）。整个监控、响应以及防御手段都要联动每一个“C”的责任方，包括研发团队。每个责任方都需要有 7x24 的运维文化。

第二节 云原生安全方案选型

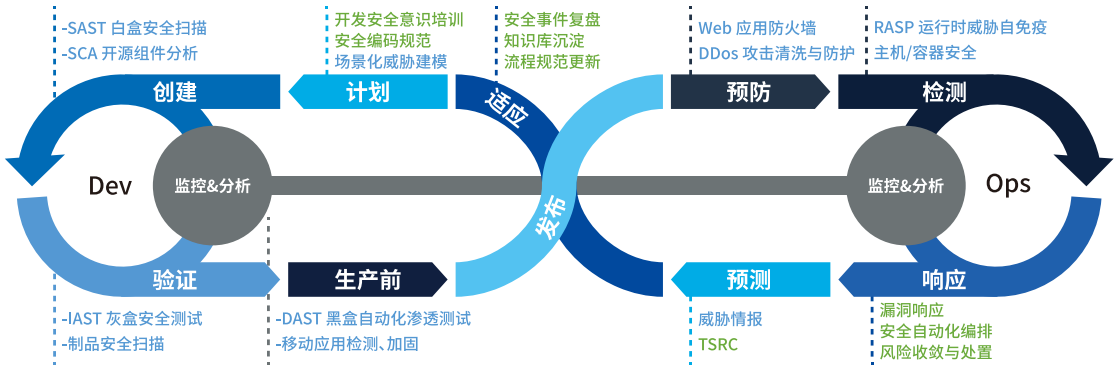
一、主流云原生安全平台及工具

〔一〕云原生 DevSecOps

腾讯 DevSecOps 解决方案遵循安全开发生命周期（Security Development Lifecycle）、安全左移（Shift Security Left）理念和原则，在更早的环节中进行安全介入和安全管控，通过实施应用开发安全编码规范、安全设计要求、软件成分管理等最佳安全实践来全面提升应用的安全韧性。

DevSecOps 的核心是流程、技术和文化，最难的是文化。在文化建设方面，腾讯安全可提供 DevSecOps 知识库培训；在流程方面，提供 DevSecOps 流程咨询服务；在技术方面，提供从计划、开发、构建、测试、上线、运行到安全开发管控各个阶段的安全工具链产品，可助力企业客户进行 DevSecOps 的实施落地。

图表 14 腾讯安全 DevSecOps 整体解决方案



注：蓝色部分为标准化安全检测软件产品；绿色部分为需要建设的流程、规范、制度等内容。

资源来源：腾讯安全于 2022 年 6 月的《腾讯自身 DevSecOps 最佳实践分享》

以腾讯自身的 DevSecOps 最佳实践为例，分为四个发展阶段：第零阶段，通过边界管控规避入侵风险，通过人工测试发现重点问题；第一阶段，从无到有初步建立安全框架和安全体系，补齐相关安全能力与安全活动；第二阶段，从有到核心，追求精细化运营，通过专项将问题收敛，消减核心安全风险；第三阶段，从有到标准高效，落实安全

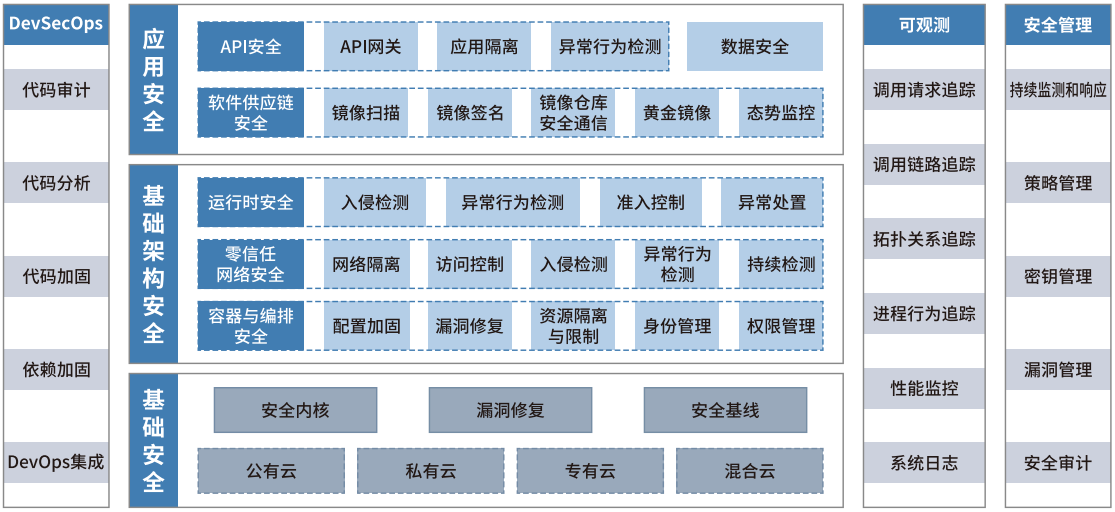
左移，通过安全质量可视化与度量，提升安全效率，提高业务团队在安全方面的参与度。

〔二〕云原生容器安全

云原生架构下，容器安全风险存在于应用的开发构建、部署、运行时的全生命周期阶段。目前，容器逃逸是用户最关注的容器安全问题，虽然容器安全能力已有不同程度的落地应用，但总体比例不高，技术门槛高是影响容器安全落地部署的主要因素。

腾讯云原生容器安全服务（Tencent Container Security Service, TCSS）提供容器资产管理、镜像安全、运行时入侵检测等安全服务，保障容器从镜像生成、存储到运行时的全生命周期，帮助企业构建容器安全防护体系。

图表 15 腾讯云容器安全体系



资料来源：《腾讯云容器安全白皮书》

企业在制定容器云的安全方案时，可以分别从两个方面进行设计：对于南北向的网络安全，通常可以直接复用传统的安全产品和能力，比如 WAF、抗 DDoS、Web 漏洞扫描、入侵检测和防御服务（Intrusion Detection and Prevention Service，IDPS）等，实现相应的安全检测与防护。对于容器云内部的安全，可以通过相应的容器安全机制来实现。

〔三〕云原生工作负载保护平台

云工作负载保护平台，又称“云主机保护平台”，是以工作负载的保护为主的安全产品，可以保护混合云、多云和数据中心的服务器工作负载。与 EDR 不同的是，云工作负载保护平台专注于保护服务器负载主机，为物理机、虚拟机、容器和无服务工作负载等所有主机提供保护，无论它们在数据中心还是云上，都能提供一致性的可见控制。

腾讯云主机安全（Cloud Workload Protection，CWP）具备轻量化、云安全情报共享、集中化安全运维三大特点，为企业提供入侵检测（文件查杀、异常登录、密码破解、恶意请求、高危命令、本地提权、反弹 Shell）、漏洞管理（系统组件漏洞、Web 应用漏洞、应急漏洞）、基线管理、高级防御（攻击检测、网络防篡改）、安全运营等安全防护功能，帮助企业及时发现安全风险并提供防护解决方案。

图表 16 腾讯云主机安全的产品架构图

资料来源：《云原生工作负载：腾讯安全主机安全产品白皮书》

基于腾讯安全积累的海量情报数据，腾讯云主机安全利用机器学习为用户提供资产管理、木马文件查杀、黑客入侵检测、漏洞风险预警及安全基线等安全防护服务，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。腾讯云主机安全现支持用户对腾讯云外服务器统一进行安全防护，轻松共享腾讯云端安全情报，让私有数据中心拥有云上同等级别的安全体验。

〔四〕云原生安全态势感知

传统安全防御体系往往建立在“防得住”的前提下构建，大量的检测与防御设备，如 IDPS、防火墙等都部署在网络边界，同时多采用基于特征规则的检测方法。此种安全体系思路的优点是，一旦有安全攻击则立马实时阻断。但是近年来爆发的大量安全事件表明，仅仅有这种基于经验的“栅栏式”安全体系是不够的，一旦被攻破，那么内部便畅通无阻。

腾讯云安全运营中心（Security Operation Center，SOC）是建立在一种新的“假设传统安全体系防不住”的安全观基础上，通过在传统安全体系上新增一种主动感知体系，依靠流量、主机日志分析、日志回溯等机制，帮助企业建立起传统安全体系外的一套新的安全机制，及时发现内网失陷流量，追溯失陷主机，挖掘并遏制被感染资产。腾讯云安全运营中心集成腾讯 AI 能力，更能发现经验之外的异常行为。例如采用机器学习检测等技术，以资产为维度，学习“外到内”、“内到外”及“横向”流量画像，与资产自身历史流量进行纵向对比，与同类别资产流量进行横向对比，采用先进的人工智能算法，发现未知异常。

〔五〕云原生 Web 防护与数据安全治理平台

腾讯云 Web 应用防火墙（Web Application Firewall，WAF）是一款基于 AI 的一站式 Web 业务运营风险防护方案，提供两种类型的云上 WAF：SaaS 型 WAF 和负载均衡型 WAF。两种 WAF 提供的安全防护能力基本相同，接入方式不同。

腾讯云 WAF 可以有效防御 SQL 注入、XSS 跨站脚本、木马上传、非授权访问等

OWASP 攻击。还可以有效过滤 CC 攻击、提供 0day 漏洞补丁、防止网页篡改等，通过多种手段、全方位保护网站核心业务安全和数据安全。

腾讯云数据安全中心（Data Security Center，DSGC）依据《数据安全法》，帮助企业自动梳理数据资产，提供资产管理与授权、敏感数据识别、数据分类分级、人工打标、数据资产地图、安全能力协同等主要功能，对企业云上数据进行分类分级和安全风险评估，并协同腾讯云各安全能力，形成闭合的数据安全防护网，帮助企业最大化提升安全效益。

〔六〕云原生身份管理平台

基于云原生的数字身份管理平台，可为企业提供集中式的数字身份管控服务。

腾讯云数字身份管控平台（Identity and Access Management）具备多样化协议支持、灵活访问控制规则、多种部署方式、有效识别风险、稳定高可用等特性。在企业 IT 应用开发时，腾讯云数字身份管控平台可助力企业集中管理用户账号、分配访问权限以及配置身份认证规则，避免因员工账号、授权分配不当导致的安全事故。在互联网应用开发时，腾讯云数字身份管控平台可助力企业打通应用的身份数据，更好地实现用户画像，也可为用户提供便捷的身份认证体验，提升用户留存。

二、云原生安全方案选型注意事项

企业在进行云原生安全方案选型时，应着重从下面几个维度去考察相应的安全产品和解决方案：

产品和方案建设的便捷性。企业需要评估购买的安全产品和解决方案，是否能提供免费产品/服务试用，是否能提供快速的部署和交付能力。一般云原生的安全产品都需要具备分钟级的交付能力，支持安全能力随时可用，因此产品和方案建设的便捷性是企业进行云原生安全产品和方案选型时首要考量的因素。

使用的便捷性和运营的及时性。企业需评估购买的安全产品和解决方案，是否提供便捷的图形化操作界面，同时需提供灵活的告警接收和处置能力。一般云原生的安全

产品都具备短信甚至小程序的告警和处置能力，可实现告警随手处置。

资源的弹性扩展能力。企业需评估购买的安全产品和解决方案，是否具备弹性扩展能力。用户云上的业务规模会随着业务的发展弹性伸缩，因此安全资源也需要随着业务的伸缩而伸缩，即云上安全需要具备安全资源池弹性伸缩的特点。一般云原生的安全产品都需要具备弹性扩展能力，使安全能力随业务的扩展而弹性扩展，满足云时代的高效扩展需求。

合规性。出于政策合规、行业合规、安全合规、数据合规、配置合规等因素的考量，企业需评估购买的安全产品和解决方案，是否能满足上述合规需求。

整体拥有成本。企业需整体评估购买的安全产品和解决方案，对降低企业的 CAPEX（Capital Expenditure，即资本性支出）和 OPEX（Operating Expense，即运营支出）带来的影响和变化。通常采用云原生的安全产品和方案，可以实现按需购买，大幅降低客户对安全的初始采购成本和整体运营成本。

第三节 云原生安全体系建设的实践路径

云原生安全体系建设的实践路径可以分为两种视角：一是应用生命周期视角，二是 IT 架构视角。

一、应用生命周期视角下的云原生安全体系

企业建设云原生安全体系时，安全能力应贯穿云原生应用从构建、部署到运行的整个生命周期。由于云原生应用涉及容器集群、容器集群的编排调度以及容器 PaaS 平台等，因此所承受的攻击面会大大增加，面临的安全风险也更加复杂，这使得企业对整个安全能力的建设需求较高。

在开发阶段，企业要能提前发现风险隐患，因此需要集成的代码级安全及合规检测能力，或通过向开发者提供安全 SDK，使产品具备内生安全能力。处于发布阶段的制品（例如容器镜像）需要持续地进行自动扫描和更新，从而避免遭受漏洞、恶意软件、危

险代码以及其他不当行为的侵害。完成这些检查之后，应该对制品进行签名来保障其完整性和不可否认性。

在部署阶段，集成的安全性能够对工作负载的属性进行实时的持续验证（例如完整性签名、容器镜像和运行时的安全策略等）。

在上线运行阶段，企业要对应用、服务和工作负载的运行时进行安全防护，并通过态势感知能力和云平台的灵活、弹性机制，对网络安全事件进行实时自动化响应并进行协同处置，实现高效的安全防护及合规。

安全云原生部署达标参考标准如下：

- 代码安全漏洞和开源合规检测；
- 自动化镜像加固及扫描；
- 镜像签名及安全策略的实时校验；
- 应用、服务、工作负载的动态可弹性扩展运行时防护；
- 安全事件的自动化响应。

二、IT 架构视角下的云原生安全体系

在传统 IT 架构视角下，云原生安全体系架构涉及六大组成部分：

一是云的基础设施安全。基于企业使用的云环境及整个云底层，真正实现落地的是基于云厂商所提供的原生主机安全、原生容器安全、原生应急响应和取证等。因此，云厂商所提供的底层安全能力至关重要。

二是应用层的应用安全。这是企业投入精力最大的重要环节，需要从攻击者的角度出发，进行优先防护。云原生应用安全涉及安全开发、安全测试、应用安全防护等诸多环节。

三是网络层的安全防护。在接触新产品或考虑流量压力时，需要在应用级别搭建

云安全架构，可以采用 SaaS 化的云网络安全产品，融合云原生安全（如云防火墙、云 WAF、主机安全、容器安全等），以云原生平台的网络防护手段，进行云网络边界治理。

四是业务层面的安全治理。从合规角度出发，围绕身份治理、风险治理、数据治理等方面，进行业务风控及访问来源的监控，并降低业务运营成本。

五是云原生数据安全。数据是企业最核心的资产，在云架构中，数据安全与业务安全、应用安全密切关联。通过对线上数据、C 端数据等进行分类分级，可对数据脱敏，进行隐私保护、数据加密、数据的访问管理等，从数据安全的全生命周期角度进行 API 监控，实现云原生数据安全。

六是安全管理。企业需要从管理要求出发，在企业内部建立安全运营中心，通过审计、认证等进行安全管理，并结合上述五个维度的堡垒层层打通之后进行联动，针对“云、网、端、应用、数据”几大层级，进行日常安全运营。

云原生安全指标体系

信息安全管理体系，需要解决历史遗留问题以及安全威胁风险。所以，最终的落地措施是云原生安全整体的统一管理，需要通过指标体系来评价目标的建设情况。

云原生安全指标体系包括了建设指标和运营指标两大类。建设指标的两个参数是覆盖率和完成率，运营指标的两个参数是响应时间和发现时间。

第三章

中国云原生安全最佳实践

第一节 腾讯云原生安全的攻守道

一、开发背景

腾讯安全专注于云安全技术研究和创新工作，在大规模云安全防护和治理、云原生安全技术、密码学和云数据安全、容器和虚拟化安全、硬固件和基础设施安全等多个领域展开技术研究和产品创新工作；同时负责腾讯云平台自身的安全建设、防护和治理工作，通过安全治理体系建设、持续性安全攻防对抗、大数据安全运营平台和云原生安全托管服务（Cloud-MSS）持续保障腾讯云平台及云上数百万租户的安全。

云原生架构在逐步成熟、落地的过程中面临众多安全风险，容器的短生命周期、密度大、云原生下的 DevSecOps、安全能力云原生等对企业的安全运营能力带来极大挑战。

首先是技术门槛，懂安全的不懂云原生，懂云原生的不懂安全，因此安全运营人员需要逐步补齐云原生知识和运维知识；其次是流程规范，业务野蛮生长，配套的安全能力建设和安全运营流程规范跟不上，这些问题亟待解决；第三是人和资产，涉及开发、安全、容器 PaaS 平台方、运维等诸多角色，存在安全意识薄弱、资产归属不清晰等问题。

二、解决之道

- 知攻：容器在野攻击、安全攻防矩阵

近几年，腾讯安全在对容器在野攻击的研究和监测中发现，绝大多数应用云原生技术的企业都经历了容器安全事件。而对 DockerHub 黑产的监控分析显示，黑产已经攻陷了在网约 1.9 亿个容器，并且攻击种类和对抗还在持续提升，安全问题已成为影响用户落地云原生的重要考量因素。

- 懂防：腾讯云的云原生安全能力架构

承载了整个腾讯全量云原生业务的腾讯云容器平台，有着业内超大规模的自研上云容器应用。腾讯在安全体系架构中遵循了四大原则：一是安全能力原生化，二是安全左

移，三是全生命周期的安全防护，四是零信任的安全架构。腾讯云的容器安全防护体系框架，按照云原生架构层次化的方式，可以逐层地实现安全防护，打造出承载腾讯业务的云原生安全的容器云，也能够助力企业安全实现云原生转型。

- 内功：腾讯云容器安全管理及运营实践

安全运营是目标，安全能力是手段。在内部推进容器安全运营时，可以参考 NIST 的网络安全框架，将容器的安全运营分为五个并行且连续的步骤，分别是：识别、防护、检测、响应和恢复。

腾讯安全总结了企业云原生安全运营能力建设需要注意的四个关键点：一是做好镜像的安全管控；二是主动容器集群层面的安全加固；三是强大容器运行时的安全防护；四是建立基本的容器资产大盘应急。

三、未来扩展

腾讯安全已与信通院、清华大学联合成立了行业首个云原生安全实验室，发布了首个云原生安全的测试平台，目前测试平台的基础框架已经建设完成，未来在实战演练阶段会扩展到实战演练环境，聚焦云原生技术实战化验证。

第二节 游戏行业云原生安全最佳实践

一、项目背景

作为互联网领域的一大热门行业，游戏行业正随着时代的诸多变化而不断演进。在众多行业趋势中，上云已成为游戏行业的重要趋势之一！游戏发行时间短，上线速度快，一般在游戏上线初期就会进入高峰期，上线后业务需要快速扩展，资源要快速部署，而传统线下的 IDC 资源，其快速部署能力已经无法满足游戏行业的快速扩展需求。

为了应对业务挑战，某在美上市游戏公司选择将业务迁移到云端，在确保游戏性能、

稳定性和安全性的同时，给用户带来顺滑、流畅的游戏体验。目前，该游戏公司在云上部署的云服务器数量达 2000 余台，互联网流量高达 10+Gbps。

该游戏公司在本地 IDC 仍有部分业务，因此需要在云上和本地 IDC 进行双份安全投入，成本较高。其次，由于本地 IDC 经常出现安全事件，会渗透到云上，影响云上的关键业务。第三，该游戏公司安全专业人员匮乏，难以应对专业黑客的攻击，可能造成业务中断、公关危机以及数据泄露等风险。因此，构建基于混合云的整体安全架构刻不容缓。

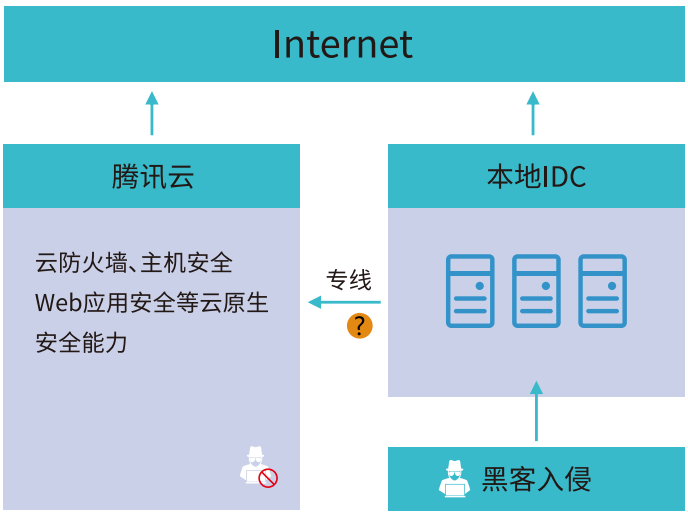
二、解决方案

该游戏公司为保障混合云架构下的网络安全，采用了腾讯云原生安全解决方案（包括云防火墙、主机安全、Web 应用安全等云原生安全能力），不仅实现了资源的快速弹性扩展，以及安全服务的按需部署和调用，与此同时腾讯云的安全能力可渗透到线下 IDC，实现对本地 IDC 安全能力的统一纳管。

针对挖矿木马、恶意病毒等安全威胁，T-Sec 主机安全可发现主机恶意行为，通过云防火墙自动阻断恶意外联；当系统检测到暴力破解时，主机安全可实时拦截，通过云防火墙收敛暴露面；针对恶意爬虫，可使用云 WAF 提供的防爬防刷防 Web 入侵攻击的场景化功能，有效防护恶意爬虫等风险；针对 DDoS 流量攻击，T-Sec 云原生 DDoS 防护包可有效提升 DDoS 防护能力，且无需改变客户的网络架构；腾讯云防火墙小时级别的虚拟补丁，可实时拦截漏洞利用，抵御各种网络及高级威胁攻击；腾讯云 SOC、主机安全的配置检测功能，可及时补齐安全配置疏漏，防患于未然。

针对该游戏公司安全投入不足的问题，腾讯安全混合云整体安全方案（方案架构如图表 17 所示），将云原生能力覆盖到线下，帮助客户节约成本投入，与此同时，云的 MSSP 服务，通过混合云延展到线下 IDC，可有效破局该游戏公司安全专业人才匮乏的现状，补齐安全短板。

图表 17 方案架构



资料来源：腾讯安全云原生安全行业标杆案例

三、项目收益

项目完成后，该游戏公司的资源可弹性扩展，安全服务可按需部署和调用，既节约了安全投入成本，又将安全能力延展至线下，使本地 IDC 安全事件显著减少，破解了公司安全投入不足、安全专业人才匮乏的难题，提升了整个混合云架构的安全能力，保障了用户顺滑、流畅、安全的游戏体验。

第三节 文创行业云原生安全最佳实践

一、项目背景

2019 年初，中央广播电视总台党组提出要集合总台优势资源，建设以“央视频”为品牌、短视频为主打的视听新媒体旗舰。为了支撑“央视频”视听新媒体旗舰的建设和运营，启动打造支撑总台新媒体内容共享和数据共享的新平台。

“央视频”5G 新媒体平台为新媒体业务提供内容汇聚、制作、分发、运营、归档等全链条媒体服务，同时聚合社会机构和专业及准专业创作者的优质账号，打造“央视频号”生态，构建 5G 时代智能化、移动化，支撑总台新媒体内容汇聚、共享、制作和

数据应用的技术支撑新平台。内容形态上主打短视频，兼顾长视频，包括对接 4K 超高清视频节目。腾讯云与智慧产业事业群（CSIG）、平台与内容事业群（PCG）、技术工程事业群（TEG）和企业发展事业群（CDG）通力协作，至 2019 年 11 月 20 日“央视频”上线，这标志着中央广播电视总台媒体融合迈出了关键性的步伐。

中央电视台 5G 新媒体平台项目采用混合云模式，在保证云平台自身安全的同时，更要适应和保障云平台所承载的“央视频”业务应用的安全。央视频系统具备极高的网络安全保护要求，承载该系统的云平台包括私有云、专有云和公有云，属于复杂的混合云架构，需要充分识别系统整体的网络安全风险，为系统网络安全防护体系建设提供坚实的基础。而项目交付时间较短，既要充分论证，又要加快方案设计，需要边规划、边设计、边建设。

二、解决方案

央视频为保障系统和混合云基础支撑平台的网络安全，设定了以业务安全为核心，以等保合规为基线的安全目标，采用了腾讯云原生安全解决方案，在央视频的公有云、专有云和私有云平台均内嵌安全系统。其中，公有云采用 T-Sec Web 应用防火墙，T-Sec DDoS 防护，T-Sec 安全运营中心，T-Sec 堡垒机，T-Sec 漏洞扫描服务；私有云采用 T-Sec 安全运营中心、T-Sec 高级威胁检测系统、T-Sec 威胁情报平台、T-Sec 主机安全、T-Sec Web 应用防火墙、T-Sec 数据安全审计、T-Sec 堡垒机、T-Sec 漏洞扫描服务和 T-Sec 安全专家服务等，各云平台全程融入安全能力，充分利用云平台原生的安全资源和数据优势，与用户和各系统资源有效联动。

在腾讯云原生安全解决方案的助力下，央视频打造了全链路和全时段的主动防御体系设计，建立了基于时空纵深的主动防御体系。从空间维度，全链路主动防御，从外部威胁情报、互联网态势、安全日志、网络和主机日志、流量和 APT 分析、全链路主动发现、检测和识别，构建网络空间主动防御体系。从时间维度，全时段的主动防御。从威胁情报和流量日志感知分析，进行安全事件预测，到动态安全策略调整、主动防护策略配置和安全检测，再到快速响应和溯源，实现全时段闭环主动防御体系。

三、项目收益

央视频系统上线后，腾讯项目团队和中央广播电视总台密切配合，在春晚、疫情等重要关头合理部署，运用灵活且稳定的技术能力，推动了央视频 APP 的爆发式增长。为保障系统的安全稳定，云原生安全系统平均每日监测的云内安全事件告警数千余条，高危十余条、中危百余条、低危千百余条。在不影响业务的情况下，提高项目 7 大系统、58 个子系统的自身安全防护能力，保障央视频各业务系统始终安全、稳定运行。

客户评价：“作为本次项目建设的产品技术提供方，腾讯以领先的技术、专业的运营指导和敬业的态度，基于‘5G+4K+AI’等新技术，全面助力总台打造央视频有品质的视频社交媒体。央视频客户端在业内受到了广泛关注，在产品设计、用户体验方面均达到一线平台水平，市场反馈口碑良好”。

——中央广播电视总台，视听新媒体中心

第四节 物流业云原生安全最佳实践

一、项目背景

自 2016 年开始，中国外运在原虚拟化计算平台基础上开始组建私有云平台。2017 年，中国外运与腾讯云合作，启动“私有云+公有云”的混合云模式的构建工作。目前，中国外运混合云架构已顺利实现，并完成了所有核心业务系统的“上云”工作，凭借着混合云的架构优势，云计算平台正助力中国外运全国 30 个省、自治区、直辖市及特别行政区、海外 41 个国家和地区的服务网络，以及全球 67 个自营网点的系统平稳运行。

作为行业数字化转型的先锋，中国外运不断提升物流系统的全球化布局和快速响应能力。在中国外运加快数字化转型推进企业智慧化、智能化的同时，腾讯云作为中国外运的重要合作伙伴，以其国内外 17 个区域、29 个数据中心节点，覆盖欧美及亚太等地区海外 13 个节点的全球多区域数据中心节点能力，充分助力中国外运物流应用前端在全球的快速部署、迭代和按需扩展，支持中国外运保链、固链、强链，实现高质量发展。

随着业务的发展，中国外运的核心物流应用架构逐渐呈现云原生化趋势，信息系统在全球多地的前端部署也对安全管控提出了更为严苛的挑战，传统系统架构基于边界的安全管控已经无法满足安全防控的管理需求。同时由于系统全球化的特点，越来越多的服务正呈现在互联网上，外部网络安全问题愈发予以重点关注。面对日益复杂的网信安全形势，企业需要及时改变以往的安全规范和方式来更有效地对应用进行保护，让云原生应用可以适应不断变化的需要，满足云原生应用的规模化需求。

二、解决方案

借助腾讯云平台海外节点，中国外运建立了更加稳固高效的全球供应链系统，提升了全球区域资源的快速交付能力、快速扩缩容能力，实现对全球业务拓展有效支撑的同时，还通过细粒度的安全组策略、权限控制等云安全组件的简单配置，有效解决了云原生安全整体性原则下多云环境基础设施的安全问题，实现了集团提出的“云管边端”的高效协同。其中，中国外运直接使用了腾讯云原生安全解决方案（包括主机安全、云防火墙、云 WAF、云原生 DDoS 防护包、虚拟补丁以及启用了云安全运营中心），通过以下方式，有效解决了互联网访问方面的安全问题：

1）使用主机安全技术或工具（如主机安全）发现主机恶意活动（木马病毒、暴力破解等）并进行实时拦截，配合云防火墙收敛或直接阻断恶意攻击连接。

2）对于 Web 入侵或恶意爬虫可以通过云 WAF 进行拦截。云 WAF 通常由云服务商提供，其特点是不需要用户额外安装部署软硬件设施就可以实现对企业网站的安全防护。启用云 WAF 后，用户的请求会首先发送到相应的云端节点进行检测，正常的请求会转发到真正的服务器，而异常请求则可以直接进行拦截。

3）即使云原生应用有较强的高可用能力，但由于 DDoS 攻击仍会对应用服务以及其依赖的上下游网络造成洪泛式攻击，从而导致服务中断，因此对于云原生应用使用云服务商的云原生 DDoS 防护包可以很好地防护 DDoS 流量攻击，无需额外防护。

4）云安全运营中心（SOC）是基于云原生构建的统一的安全运营平台，可以提供互联网攻击测绘、云安全配置风险检查、流量入侵检测、泄露监测以及日志审计等云安全能力。启用 SOC 后，结合主机安全、云防火墙等功能，可以实现威胁告警集中分析、自动事件调查、威胁集中处置、自动化编排与响应、用户行为分析等能力，提升了威胁检出率和威胁响应效率。

5）特别是对于老旧系统、组件，通过虚拟补丁的方式，无需在业务系统中安装真实补丁，既避免了升级后因为版本兼容性问题对应用程序的潜在影响，又开启了针对热门漏洞、常见漏洞和高危漏洞的防护功能。

三、项目收益

腾讯云原生安全解决方案不仅有效解决了安全管理门槛高、人力不足的难题，还因其以按需采购云安全服务代替购买昂贵的传统软硬件设施的方式，较好地控制了安全投入，为中国外运节省了大量成本。作为云原生安全受益最大的物流业务应用，在提升了快速弹性扩展能力的同时，全面保障了全球服务的安全性与可靠性，为企业的高质量发展持续创造价值。

第四章
中国云原生安全未来展望

第一节 中国云原生安全趋势展望

一、中国云原生安全发展趋势

随着企业数字转型步伐的加速，更多企业已经从 IT 时代步入了 DT 时代。云计算作为数字化底座，已经成为企业部署新业务的首选。当前云计算已经进入了下半场，竞争越发激烈，新概念也层出不穷。其中最为亮眼的就是云原生技术，甚至可以说云原生是云计算的下半场，称之为云计算 2.0 版本。云原生的出现是云计算与企业业务场景和 DevOps 不断碰撞融合的结果，是一场由业务驱动的、对云端基础设施、编排体系的重构。

云计算 2.0 时代，既带来了对应用“云原生（Cloud Native）”的需求，也带来了对安全机制“云原生”的需求。纵观历史，信息安全总是伴随业务的发展而演进，在这样的大背景下，云原生安全自然而然成为未来几年云安全的主要发展方向。

〔一〕云原生安全的生态化发展

2020 年 4 月 20 日，国家发改委指出，新型基础设施主要包括三方面内容，其中之一就是信息基础设施，主要是指基于新一代信息技术演化生成的基础设施，比如，以 5G、物联网、工业互联网、卫星互联网为代表的通信网络基础设施，以人工智能、云计算、区块链等为代表的新技术基础设施，以数据中心、智能计算中心为代表的算力基础设施等。

随着国家新基建项目的快速推进，云原生技术与新的基础设施融合成为一个明显趋势，所以很多服务提供商、运营商或者产品提供商在基础设施的规划、设计、部署、实施和运营方面，都充分考虑了云原生技术相关的安全防护手段，以及如何更好地识别云原生环境内的威胁、识别风险。

时至今日，网络安全环境日益严峻，恶意攻击频发，云原生安全所涉及的范围也越来越广，架构也越来越复杂，包括从云原生基础设施到云原生应用、再到 DevOps 运营

管理的全方位的安全防御体系。面对如此庞杂的安全链条，如果仅仅凭借某一家安全厂商的技术能力和产品，是不可能保障云原生环境安全与稳定的。未来，云服务提供商可以深度绑定不同领域的安全厂商，结合厂商的产品能力、研发能力等经验和优势，基于云原生的技术架构，建设一个开放且较为有效的云原生安全环境。因此生态化的强强联手，深度合作势必成为发展趋势。

〔二〕云原生安全的服务化发展

以前较为传统的业务系统主要是采用“烟囱”式的架构，通常是单体应用系统，从前端到中间件再到后端，各个组件集中式部署在服务器上。之后进化为“面向服务的架构”，提升了应用组件的标准化程度和系统集成效率。但是在云原生的架构中，微服务架构将传统的单体应用拆解成大量独立、细颗粒度的服务。每个服务聚焦独立的功能，每个功能通过 API 进行调用，通过应用编排组装，共同作用，实现单体应用的复杂功能。这就是以服务为基础的微服务架构，发挥云原生技术底座的弹性、敏捷特征。

这就要求云原生安全必须是具备云原生技术特性的、满足容器实例短生命周期的不变基础设施特性的、频繁且海量的东西向网络流量交互的。总而言之，云原生是真正以云的模式管理和部署资源，租户看到的不再是一个个虚拟机或者 IT 系统，而是一个个业务单元。所以，以服务为中心构建的容器安全防护措施、持续监控响应模型和可视化平台，将成为云原生安全防护的主流发展趋势。

〔三〕云原生安全的安全内生化发展

安全产品服务商一定会紧跟云原生时代的步伐，抓住云原生时代的安全红利。在云原生技术框架下，传统的信息安全纵深防御模型依然存在。只是物理安全边界将变得模糊，甚至消亡，逐步变成了无处不在的云原生安全边界。从基础架构的安全、统一身份认证、数据安全、应用安全到安全事件的可视化、安全运营等，都给安全市场带来了更多机遇。

随着云原生技术加速落地应用，为更好地保证云原生架构的安全，云原生安全必须

与云原生平台、应用深度融合，提供针对云原生基础设施的防护、检测和响应能力，并赋予安全产品、应用和解决方案云原生的特性。从安全生态来看，细分领域的安全服务商必须把产品做深做精，嵌入到云原生运行的实例和应用内部，实现更细颗粒度的防护能力、微隔离访问控制、全流程实时监控响应，实现安全方案的内生配置和深度融合。

〔四〕云原生安全的轻量化发展

相对于传统的云技术，云原生技术具有非常突出的优势和特点。云原生拥有极致的弹性扩展能力、敏捷交付能力、故障自愈能力和大规模可复制能力。在云原生环境中，支撑基础设施的通常是容器技术，容器技术作为云原生的底座被广泛应用，容器部署的环境也越来越复杂多样，包括一些对资源比较敏感的嵌入式领域。容器生命周期非常短，大部分以秒级或者分钟级为单位，资源占比也比虚拟化小得多，所以容器天然具备轻、快的特性。

为了更好地适应云原生环境下的业务增长与迭代，云原生安全解决方案也必须足够轻量化，避免因安全方案的引入占用过多资源，进而影响业务的正常运行，成为系统轻量化的阻力。另据调查统计，容器的生存时间将会随着业务的发展越来越短，生存时间可能会小于 10s。此时就要求安全方案的反应链条必须足够短，必须迅速、及时发现容器启动，密切跟踪容器行为，并在发现异常时迅速反应，必须具备敏捷性。同时，云原生提供的服务粒度越来越细，相应的安全方案的防护粒度也必须越来越细。从过去的容器粒度，到目前的函数粒度，未来可能是语句粒度、变量粒度，安全方案的防护粒度需小于提供的服务粒度，所以也必须具备精细化的特性。

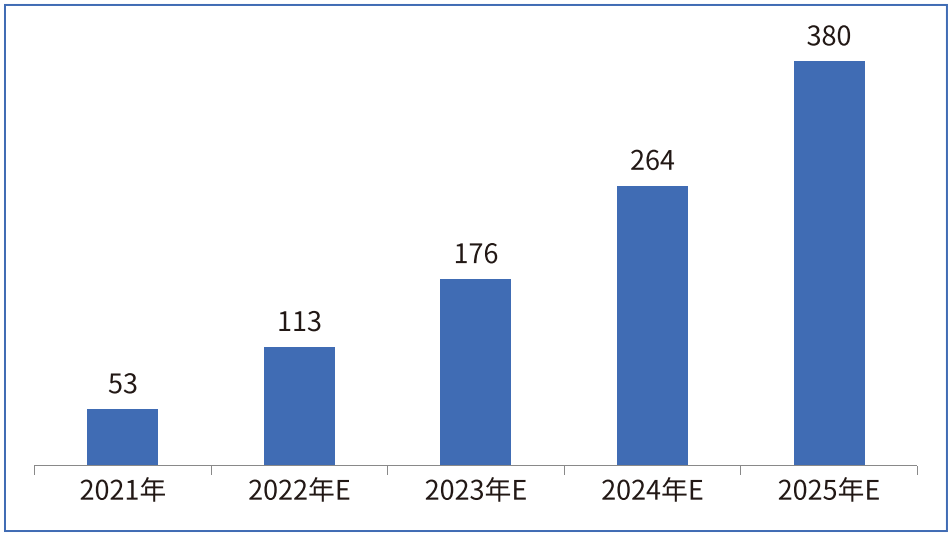
云原生以其技术优势和不断扩大的应用场景，已逐步普及到各行各业的敏捷开发与业务创新中，可以说“云原生正在吞噬一切”，所以云原生安全势必成为安全服务商捍卫和守护的主要战场。

二、中国云原生安全市场规模预测

根据相关机构统计数据，2022 年中国云安全市场规模达到 173 亿元。结合企业网

D1Net 云原生调研数据，按照云原生安全市场增长一般规律模型，我们预测，2022 年中国云原生安全市场规模为 113 亿元，2021-2025 年均增速为 58%，至 2025 年云原生安全市场规模将达到 380 亿元。

图表 18 中国云原生安全市场规模预测



资料来源：企业网 D1Net 于 2022 年 8 月的行业企业问卷调查，n=119 个样本

第二节 中国云原生安全实施建议

随着企业业务上云加速，云上安全成为一个不容忽视的问题。当前许多企业面临着云上资产管理难、漏洞风险高、流量不可控等难题，攻击者对互联网上资源的攻击也越来越频繁。

一、针对中小型企业的实施建议

针对中小型企业，建议将整体云预算的 10%～15%用于基础安全投入，防患于未然。同时把握下面几个安全指导方针：

〔一〕非必要，不暴露

可以利用云的安全组和云防火墙产品，梳理资产与暴露面。在腾讯云防火墙的资产中心，企业可以全局视角获取云上资产情况：例如，哪些资产有暴露端口？对应的服务

是什么？这些服务是否存在漏洞？另外，腾讯云防火墙可以将资产进行分组管理，并将分组应用到防火墙所有 ACL 中，当有新增资产或者暴露面时，便会提供自动化告警。

〔二〕如需暴露，优先白名单策略

云上常见攻击一般来源于 ssh/rdp 的爆破和一些 OA、Mail、VPN 系统的漏洞攻击。随着远程办公和混合办公的常态化，IP 白名单变得不够灵活。

腾讯云防火墙零信任防护可以支持微信的身份访问控制，屏蔽管理端口，避免爆破攻击；同时支持 SSH 和 RDP，用户只需在防火墙上配置白名单即可完成对脆弱业务的访问控制。

〔三〕管控主动外联

需重点关注 vpc 的外联流量，一般攻击成功后都会进行 C2 通信、下载后门等动作，腾讯云防火墙通过 NAT 边界防火墙、互联网边界的外联管控以及入侵防御能力，可以快速检测到攻击事件并进行实时阻断。

〔四〕加强主机安全，加固脆弱业务

企业云上安全最后一道防线之一是主机安全。作为企业云上的最后屏障，主机一旦被攻陷，企业核心资产将岌岌可危，甚至会威胁到整个内网的安全。

腾讯云主机安全从资产清点、安全加固、入侵防御、安全运营四个维度，深入拆解日常主机防护最佳实践，帮助企业夯实最后一道防线。

二、针对大中型企业的实施建议

如果将云上业务的“安全加固”工作比作“防御工事”的构建，如何建设并加固有层次、能联防的组合防线，是实现高效防御的重中之重。安全“防御工事”的构建可以从网络、边界、主机等各层面入手，部署完备的安全工具加固防线，并通过云安全中心、威胁情报等实现安全的一站式联动控制，以及功能互通和数据协同。

针对大中型企业，在之前的基础安全建设之上，建议加强以下四项安全工作：

〔一〕重视容器安全

作为云原生“三驾马车”之一，容器化技术在助力企业技术架构升级、应用效能提升的同时，也给企业安全防护带来了全新的挑战。在传统模式下，攻击者控制了单台节点后，仍需横向对其他节点进行缓慢渗透，才可控制整个系统。而在容器环境下，一旦攻击者控制了单个容器，可通过容器敏感目录挂载或漏洞利用等方式逃逸至宿主机获取更高权限，从而控制宿主机以及上面运行的所有容器业务，通过集群漏洞、配置不当等风险控制整个集群业务。原本“一次打包，到处运行”的便利，变成了“一次入侵，控制一切”的被动。

〔二〕加强基础安全防护的同时，加强 Web、API 等重点业务的安全防护

- 注重 Web 攻击识别和防御，如 OWASP 定义的十大 Web 安全威胁攻击；
- 结合 0day 漏洞虚拟补丁，防护紧急漏洞；
- 多端接入安全管控，并配置细粒度的处置策略；
- 重视业务终端、账号的异常识别，结合情报发现并禁止恶意访问源；
- 通过 BOT 行为管理实现对恶意流量的快速感知及自动化进化的处置策略，自动化对抗 BOT 及 CC 攻击。

〔三〕做好分区各类管控，可以增设陷阱，加强溯源取证的能力

除常规防护外，腾讯云防火墙还提供网络蜜罐的能力。防火墙的蜜罐支持一些常用的 OA 系统和具备溯源攻击者能力的特殊蜜罐，可将其部署在公网来欺骗攻击者的攻击流量；也可将蜜罐部署在内网中，一旦攻击者突破了层层防御，在做内网探测时便会被防火墙及时发现并做相应的隔离处置。在重保场景下，防守方可以化被动为主动，设置“陷阱”完整记录攻击方的行为，作为防守方的防守依据；并且由于攻击方将矛头对准蜜罐中的模拟业务，防守方的真实业务可得到保护。

〔四〕做好企业的安全合规，加强数据安全

依据《数据安全法》，梳理数据资产，对企业云上数据进行分类分级和安全风险评估，并协同各安全能力，形成闭合的数据安全防护网，帮助企业最大化提升安全效益。

参考文献

[1]《“云”原生安全白皮书（2019 版）》

[2]《腾讯云原生最佳实践合集》

[3]《云原生工作负载：腾讯安全主机安全产品白皮书》

[4]《腾讯云容器安全白皮书》

[5]《腾讯自身 DevSecOps 最佳实践分享》

版权声明