FORRESTER®

云原生安全构筑企业云战略基石

中国云原生安全市场现状与趋势白皮书

开始 →

火山引擎委托FORRESTER撰写的市场洞察研究报告 2023年7月

云原生安全成为企业全面实施云战略的保障

随着云计算成为千行百业数字化转型的核心驱动力，企业上云的步伐不断加速，云上开发已成为企业构筑数字化业务的首选。为了更加充分地利用云计算弹性、敏捷、资源池和服务化等特性，并解决应用开发及运行全生命周期面临的挑战，以云上开发为核心，以容器、服务网格、微服务、不可变基础设施以及声明式API为代表的云原生技术得到了广泛采用。云原生在改变了企业上云及构建新一代基础设施的同时，作为一项新兴技术也带来了一系列新的问题，对企业原有的信息安全防护模式提出了新的挑战。

企业安全专业团队的任务不仅需要加强和健全安全基础设施，还必须帮助企业实现关键业务目标，如改善客户和员工的体验。将云原生安全整合到现有的企业信息安全战略中，不仅仅是增加一些控制点或扩充安全技术栈，还需要对组织资源和业务需求进行评估，为云上开发之旅制定现代的网络与信息安全方法，从而更好地保障企业数字化转型和业务的持续创新。

关键发现

云原生技术发展的同时带来了一系列全新的安全挑战与冲击。77%的企业信息安全与风险管理决策者发现在云原生时代需要面对层出不穷的新威胁，比以前更加具有挑战性。

云原生技术生态仍在不断发展过程中。且由于云原生技术和架构的特性，在保障云原生应用、平台及基础设施安全的过程中，安全团队面临着前所未有的技术复杂性、企业内部组织及文化等层面带来的多重挑战。

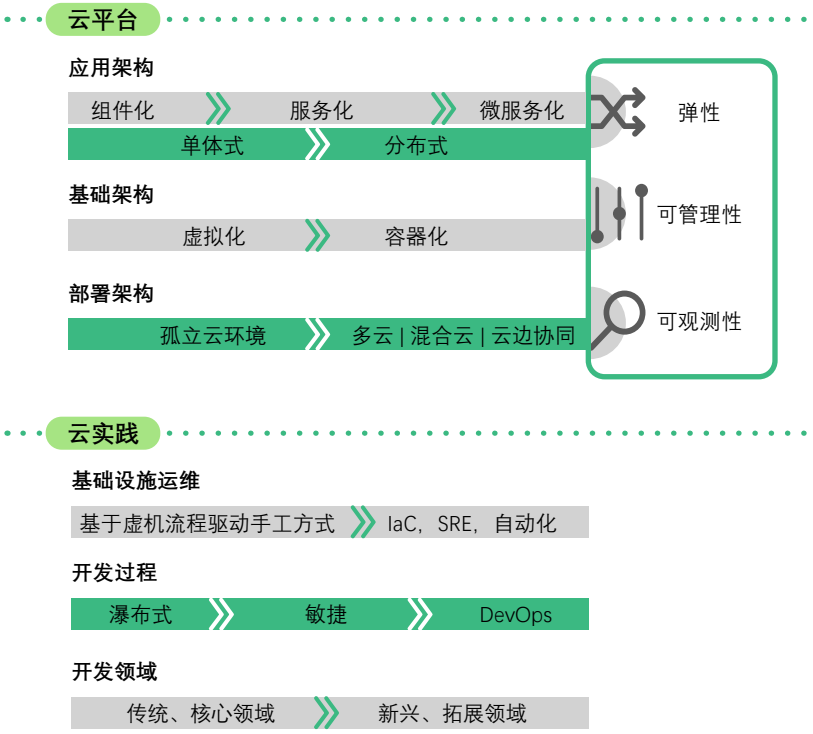
保障云原生安全的紧迫性日渐提升，企业需要评估安全需求及现状，参考并借鉴现代化的信息安全架构，例如零信任架构，并借助合作伙伴的能力和经验构建云原生安全体系，为企业云战略的实施保驾护航。

云原生技术的应用引发从“云优先”到“云原生优先”的范式转变

云原生技术使得云计算进入新的发展周期，以现代型基础设施架构、分布式云应用负载以及平台化创新为代表的第三代云原生技术推动了企业云战略由“云优先”到“云原生”优先的范式转变。

根据Forrester预测，2023年全球超过40%的企业将会采用云原生优先战略[1]。云原生是构建适应未来的现代企业的核心引擎，对企业的自适应性、创造性和韧性都具有战略意义：云原生使得企业架构师和平台团队能够在多云、混合云以及云边协作的模式中实现关键基础设施自动化及现代化，以便应用开发人员能够与业务更紧密地结合。云原生可以帮助企业在包括公有云、私有云和边缘节点在内的分布式环境内部署与支撑各类应用负载，而且可以在实现应用快速迭代的同时确保应用在异构环境下的可迁移性。Kubernetes正在重塑IT基础设施，云原生平台集成并使能各种新兴技术，加速企业数字应用创新步伐。随着传统的流程驱动、手动方式的基础设施运营被基础设施即代码（IaC）、站点可靠性工程（SRE）和自动化（RPA）取代，DevOps进一步提升了企业应用开发的灵活性及敏捷性。

从云优先到云原生优先的战略转变



资料来源：Forrester Consulting

云原生技术发展的同时也带来了新的安全挑战

容器、服务网格、微服务、不可变基础设施及声明式API这些云原生技术的发展在推进应用上云和云上开发实践的同时也带来了新的安全问题，不仅包括面向云原生基础设施的传统安全威胁，也包括针对云原生技术特征的挑战：

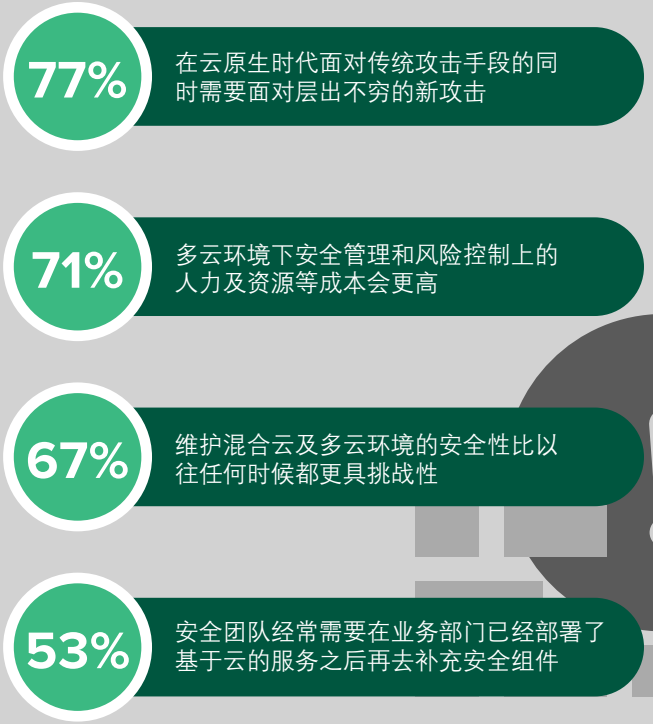
云原生环境面临的传统安全威胁。企业越来越多地构建云原生混合、分布式架构，实践云原生应用开发。在这个趋势下，不仅是更多技术栈所带来的威胁面增加，而且针对云原生基础设施和平台的攻击手段和路径也在不断进化。

云原生技术带来的新原生安全问题。微服务、容器运行时的短生命周期、持续集成和持续交付（CI/CD）全流程监控缺失、镜像及供应链的复杂性等成为新的安全挑战。不仅如此，云原生技术的快速迭代和部署频率更高，给安全团队带来了诸多困惑。

调研发现，超过七成的受访者认为面对传统的攻击手段的同时需要应对各种层出不穷的新的安全挑战。面对这些新的领域不仅需要保障基础设施的安全，更加需要根据云原生技术的特征强化相应的安全机制。

云原生技术的发展为企业带来了新的风险挑战

(只显示“比较认同”及“完全认同”)



样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

层出不穷的云原生相关安全事件

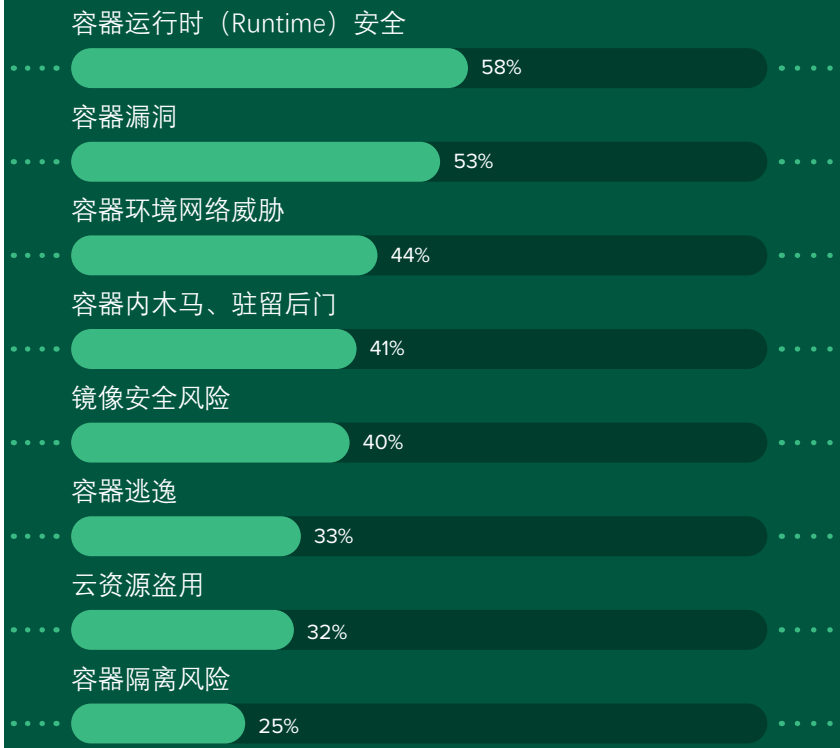
云原生系统的攻击手段越来越多样，然而当前云原生系统普遍欠缺系统化的安全防护手段。调研中发现，半数以上受访者的企业在过去一年中至少经历过一次云原生相关安全事件。

相对于过去，针对云原生系统的攻击涵盖云原生应用、容器、镜像、编排系统平台以及基础设施。58%的受访者表明他们的企业在过去12个月中经历了针对容器运行时（runtime）安全事件，例如异常进程、执行恶意程序、数据转移及高危系统调用等。53%的企业反馈发现了包括第三方组件漏洞、代码安全漏洞等造成的容器相关漏洞。44%企业遭受到了容器环境网络威胁，例如地址解析协议（ARP）欺骗，域名系统（DNS）劫持等。

此外，云原生架构允许应用程序在不同的云平台上部署和迁移，但不同的云平台可能有不同的安全性能和配置要求。如果在跨云平台迁移时未正确配置和保护数据，可能导致数据在迁移过程中被泄露或篡改。在安全领域的攻防不对等的情况，云原生架构相较于其它架构更需要企业关注。

过去一年中企业经历的云原生相关安全风险及事件

(只显示Top 8)



样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

云原生安全管理的变革

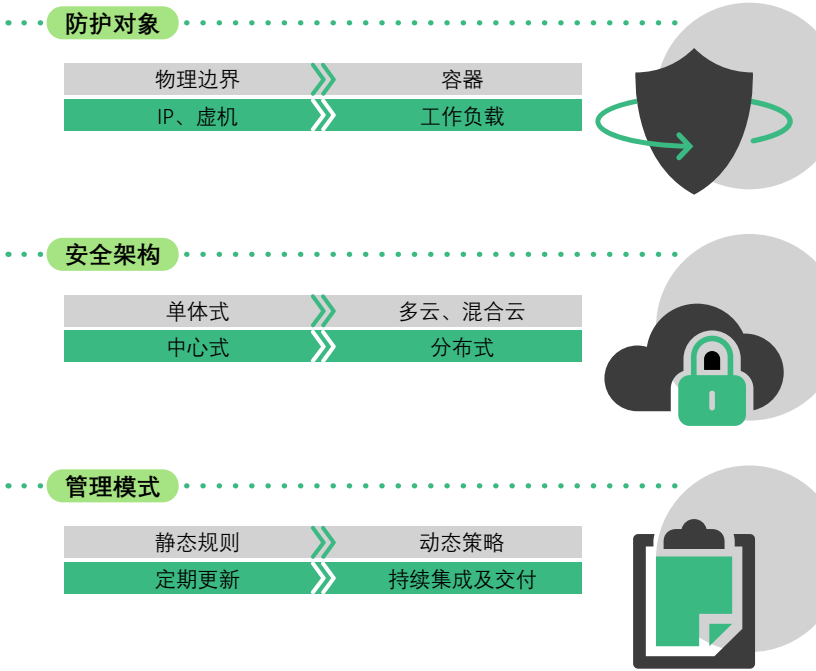
云原生技术生态涵盖基础设施到DevOps开发多个维度，势必要打破原有的信息安全视角。在应对不断出现的针对云原生基础设施、平台及容器的安全威胁过程中，原有的安全体系亟待变革：

防护对象的变化。安全管理的边界扩展到了容器层面，需要采用新的安全策略和工具来保护容器的安全性，如容器镜像的验证和加密、容器漏洞扫描和运行时监测等。

架构的变化。多云及混合云下的应用架构及工作负载更加复杂，需要采用分布式安全策略和技术，如服务间的身份验证和授权、服务网格的加密通信、微服务的监测和异常检测等。

管理模式的变化。云原生应用的快速迭代和部署频率也对安全治理模式提出了新的要求。传统的安全治理模式通常是基于静态的规则和策略，针对云原生DevOps安全治理需要采用持续安全集成和交付的实践，结合自动化的安全测试、漏洞扫描和合规性检查等工具，以确保安全策略和控制的持续有效性。

云原生安全防护主体及管理模式的演进



资料来源：Forrester Consulting

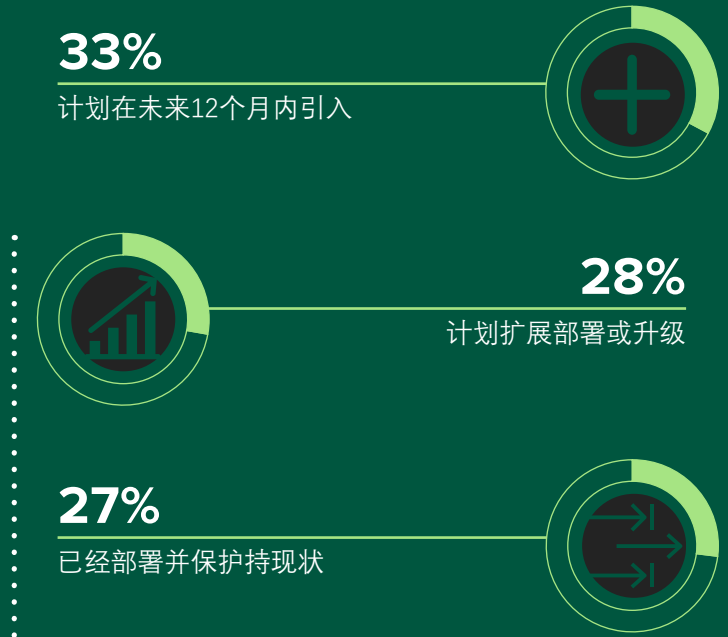
企业逐渐开始重视并部署云原生安全解决方案

超过六成（67%）的受访者声称企业具有明确的、定期更新的云安全战略。然而，云原生技术的发展突破了云安全原有的范畴，云原生安全将取代传统的云安全。通过此次调研发现，企业反馈原有的云安全战略以及传统的云安全技术组件已经不能满足云原生时代的要求。

针对日益突出的安全风险，云原生计算基金会（CNCF）、云安全联盟（CSA）等开源组织以及行业联盟等纷纷提出云原生安全标准及参考技术规范。同时，主要经济体国家标准也在制订和完善过程中，使得行业逐步走向规范，推动了产品和解决方案逐步走向成熟。在此趋势下，企业已经关注并开始尝试及引入安全技术组件。

超过半数（55%）的受访者表示企业部署容器安全技术组件保障容器镜像及运行时安全。企业重视并部署云原生安全解决方案是出于对数据和系统安全的日益关注和对云原生环境中的安全挑战的认识。然而，从全生命周期视角来看，针对云原生系统的安防防护仍然存在诸多盲区和薄弱环节。

企业部署容器安全技术工具及产品现状



样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

构建云原生安全面临诸多技术层面的挑战

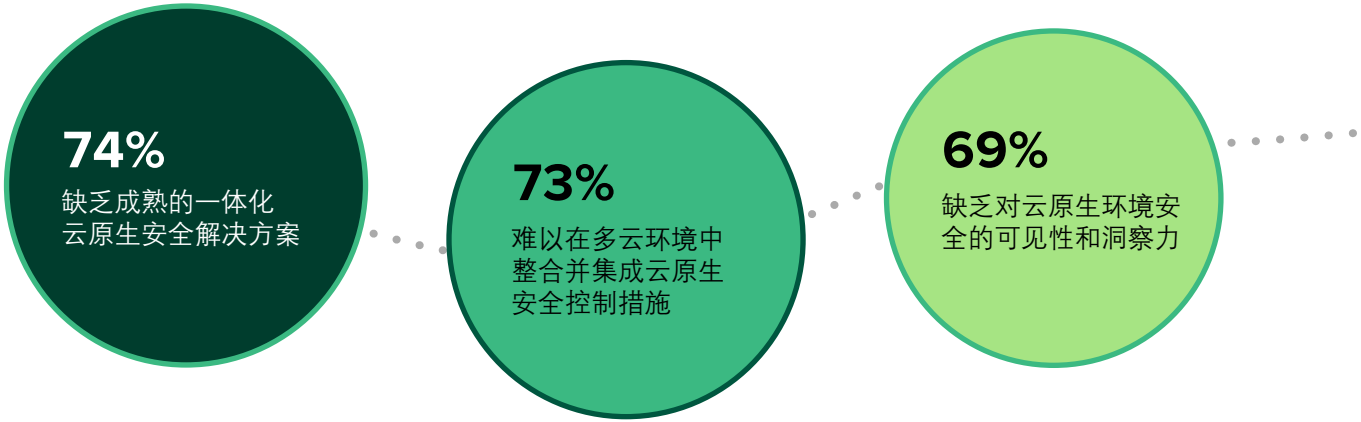
作为新兴的技术生态，云原生给企业原有的应用开发模式带来了变革，同时也给企业安全团队带来了种种技术层面的挑战：

安全技术及工具。传统的安全技术和工具无法满足云原生环境的需求：74%的受访者认为企业目前缺乏成熟的一体化解决方案以覆盖所有的云应用数据及工作负载。

复杂性和动态性。云原生环境的复杂性和动态性使得安全管理变得更加复杂。73%的受访者反馈，为了保障云原生系统安全既需要整合企业现有的安全组件和产品，同时需要应对大规模的容器化部署、微服务架构和多云环境等挑战。

可见性及洞察力。由于以工作负载为代表的资产更加多样化和复杂化，69%的受访者认为提升云原生环境可见性及洞察力也是安全团队需要持续解决的问题。

企业在构建云原生安全体系过程中主要面临的技术层面的挑战
(只显示Top 3)



火山引擎委托FORRESTER撰写的市场洞察研究报告 2023年7月

样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

构建云原生安全还面临组织及文化的挑战

云原生技术带来了涵盖应用构建、基础设施构建等一系列变革，涉及到企业多个部门。因此，保障云原生应用及环境的安全，不仅涉及到跨部门的合作，还涉及到组织及文化。首先，云原生安全需要跨团队的合作，包括开发团队、运维团队和安全团队等。75%的受访者认为在跨团队合作，共同制定和实施安全策略等方面面临挑战。其次，云原生安全是一个相对新的领域：74%的受访者表示其企业在云原生安全的控制机制、最佳实践、新兴技术和漏洞趋势等方面缺乏相关的经验和洞察，并且在企业内部难以形成对云原生安全的一致认知。最后，全球经济下行及市场的不确定性为企业IT投资带来了较大压力。因此，74%的受访者认为如何使云服务提供商的产品价值最大化：既能满足企业多方面的需求，又能尽量保护原有安全技术投资，这也是企业面临的难题。

此外，构建云原生安全体系需要建立安全意识和文化。将安全意识融入到组织的DNA中，使所有员工都能够理解和履行安全责任，以推动安全文化的转变和持续改进。

企业在构建云原生安全体系过程中面临的来自组织及文化层面的挑战

(只显示Top 3)

75%

内部不同部门及团队间难以形成统一的认知及内部协同

74%

缺乏对云原生安全控制机制的深入理解及相应技能

74%

如何使得云服务供应商的产品价值最大化

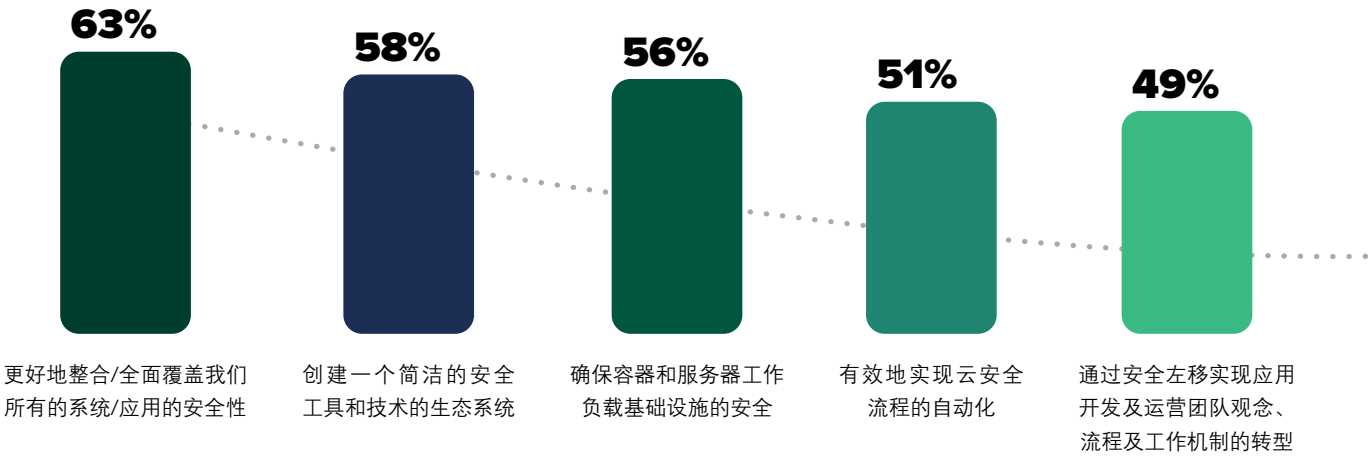
样本量：163名中国企业IT安全团队、CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

云原生安全是企业实现云战略及业务转型的基石

云原生安全不仅仅是解决云计算普及所带来的各种安全问题，其作为一种新兴的安全理念，强调以原生的思维实现云上安全并推动安全与云计算深度融合。

在调研中发现，企业构建云原生安全体系的首要目标包括全面覆盖所有系统及应用的安全性，创建简洁的安全工具和技术生态系统，以及通过安全左移实现变革等，这些都反映了保障业务持续性及可靠性，促进业务创新和敏捷性以及降低合规性风险的企业战略层面的要求，同时也体现了云原生安全是企业实现云战略的前提条件。

企业建立云原生安全体系的首要目标



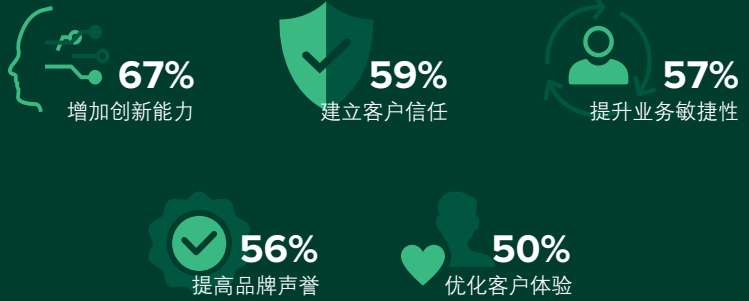
样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

构建云原生安全可以为企业带来显著收益

在快速变化以及竞争激烈的市场中，企业不仅需要通过基于云上开发提升数字化业务能力，更需要保护企业的应用程序和数据免受安全威胁和攻击。构建全面的云原生安全体系不仅可以提高业务运营安全性和降低风险，还可以增强企业的可信度和声誉，支持合规性要求，并提高业务灵活性和创新能力。这些收益将有助于企业提高竞争力，和实现可持续增长。

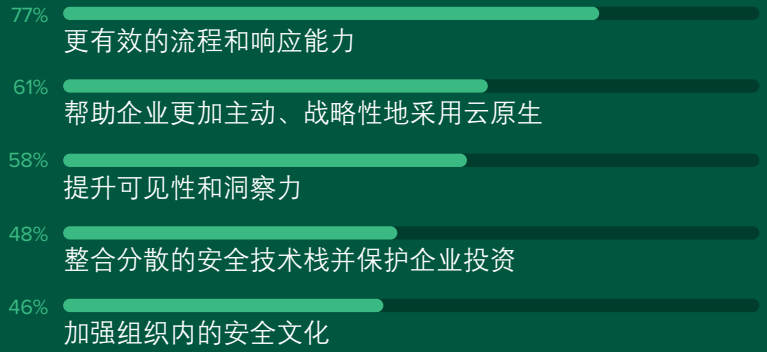
受访者认为，构建云原生安全体系可以从业务及安全两个层面为企业带来显著收益。首先，**从业务层面看**，全面的云原生安全体系可以在创新能力、客户信任、业务敏捷性、品牌声誉以及客户体验等方面，帮助企业构建差异化的竞争能力。**从安全方面看**，全面的云原生安全不仅可以提升企业面对风险以及安全事件时的响应能力，也可以帮助企业在更加主动、更具战略性地采用云原生技术等诸多方面提供巨大的价值。

通过构建云原生安全体系带来的业务收益



火山引擎委托FORRESTER撰写的市场洞察研究报告 2023年7月

提升对云原生体系的管控带来的安全层面的收益



样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

企业需借助领先的安全思维构建全面的云原生安全基础

在考虑构建云原生安全体系时，需要注重包括安全左移在内的全生命周期原生安全。这流程意味着在软件开发和部署过程中将安全性考虑纳入早期阶段，并嵌入全生命周期流程，保障镜像构建、存储、分发以及运行时的安全。

可参考并采取的设计原则包括：1.确保安全策略和控制在整个多云及混合云环境中的统一和一致性；2.实现自动化安全，包括自动化漏洞扫描、强化的CI/CD流程，以及自动化响应和恢复机制等；3.采用零信任原则来构建云原生应用和基础设施，包括最小权限原则、网络隔离、身份验证和授权、容器和微服务的隔离，以及强密码和密钥管理等；4.可见性及可观察性，确保对云原生环境的监控和日志记录足够全面和详细，包括实时监控、日志聚合和分析、行为分析，以及异常检测和警报等；5.安全需求和威胁是不断变化的，因此云原生安全体系需要持续演进，包括定期评估和更新安全策略、及时升级和修补漏洞，以及跟踪最新的云原生安全技术和最佳实践等。

采用现代的安全思维建设云原生安全

资料来源：Forrester Consulting

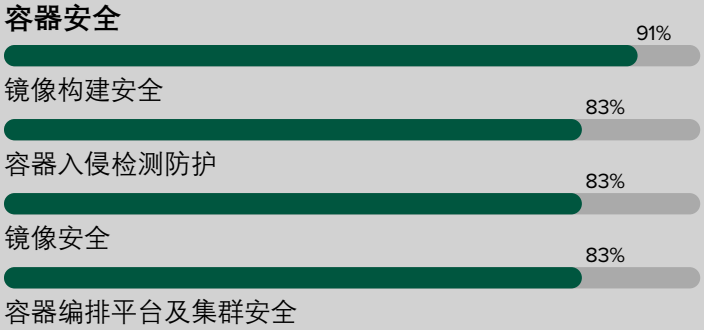
提升云原生安全关键能力：容器、代码及应用安全

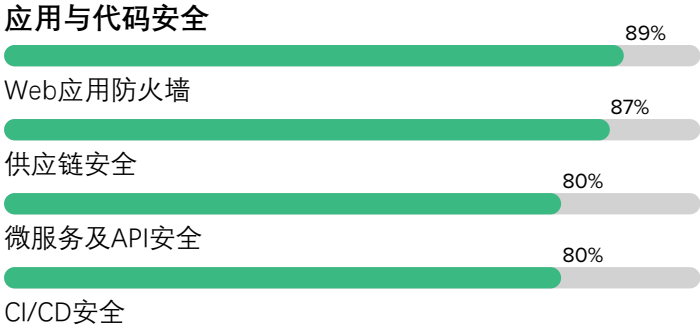
由于云原生安全的核心是要保证云原生应用及数据安全，因此云原生安全防护体系的建设也要围绕云原生应用的生命周期来构建关键的安全能力。这同样也是敏捷开发中DevSecOps所倡导的应用安全模式。云原生安全包括容器安全、代码及应用安全、平台安全以及基础设施安全在内的四层关键能力，以及相应的云原生安全治理体系。

通过此次调研，针对容器安全，受访者表示企业迫切希望提升镜像构建安全、容器入侵检测防护、镜像安全以及容器编排平台等安全能力。而在应用与代码安全层面，Web应用防火墙、供应链安全、微服务及API安全以及CI/CD安全是企业迫切希望提升的能力。

企业迫切希望提升的云原生安全关键能力：容器、代码及应用安全

(只显示Top 4)





火山引擎委托FORRESTER撰写的市场洞察研究报告 2023年7月

样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

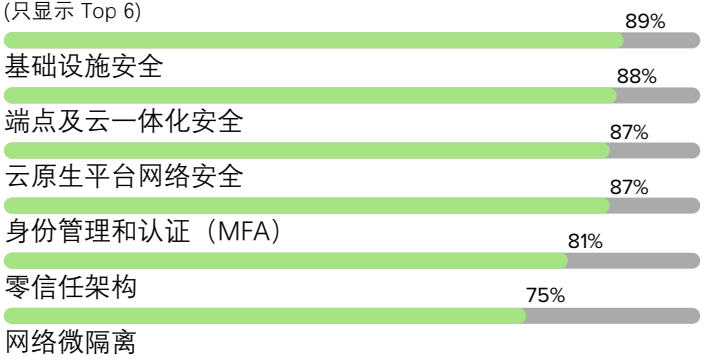
提升云原生安全关键能力：平台、基础设施安全及治理

容器技术的普及应用使得攻击者逐渐从以单个容器为攻击目标扩展到整个容器编排平台和基础设施。正是由于Kubernetes架构的复杂性使得企业重视包括云端一体化安全、网络安全、多因素认知（MFA）以及网络微隔离等关键能力的建设，以保障云原生系统每个组件的安全。

在调研中发现，更多的安全隐患仍来自于配置错误、资产管理混乱、特权账号以及不安全的密码等问题。因此，云原生系统的安全治理尤为重要，其中核心的是聚焦各种工作负载的云原生平台资产治理，不仅包括监控、日志、追踪、分析、响应、审计在内的可观测性能力，以及进行安全性评估和合规性检查，修复安全漏洞和合规性问题，并保持符合监管方要求的合规基线能力。

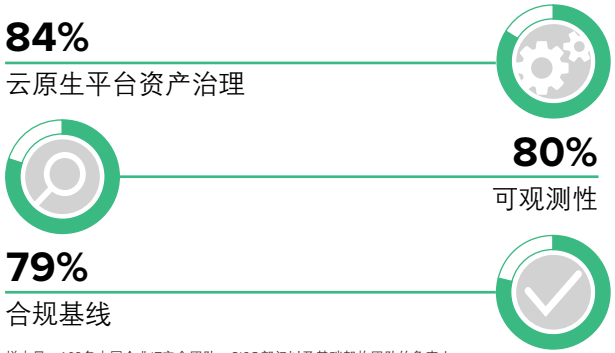
企业迫切希望提升的云原生安全关键能力：平台、基础设施安全及治理

平台、基础设施
(只显示 Top 6)



火山引擎委托FORRESTER撰写的市场洞察研究报告 2023年7月

云原生安全治理
(只显示 Top 3)



样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

基于零信任架构，实现云原生微服务治理，支持不同颗粒度自定义以及自适应隔离管控

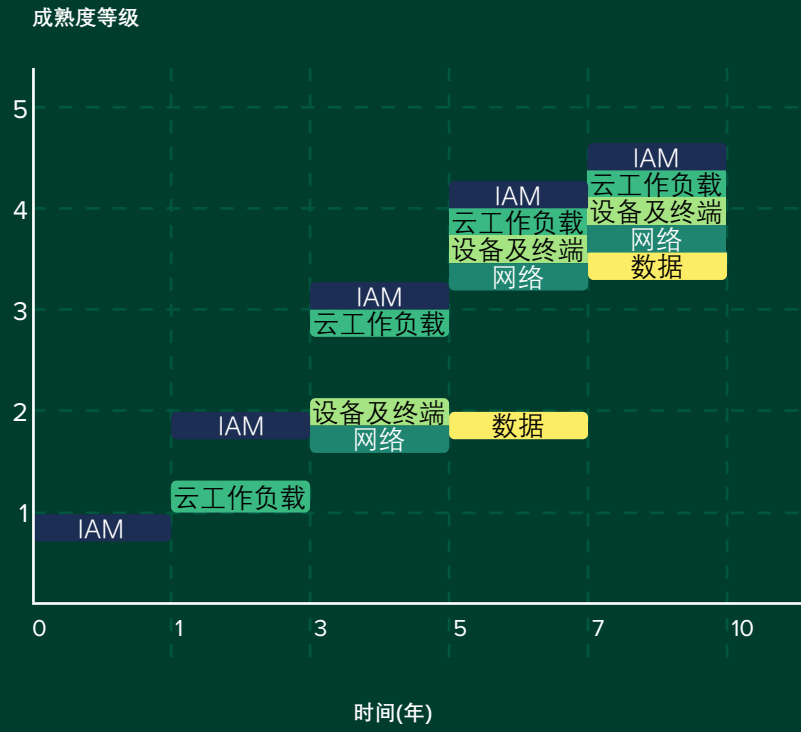
至今，零信任已经被公认为是下一代信息安全的参考架构。零信任所涵盖的安全能力和技术组成的综合、动态生态系统更加适合于构建云原生安全体系：

在云原生环境中，应用和服务被拆分为更小的容器和微服务，通过服务网格进行通信，数据流动更加复杂。零信任模型提供了一种基于身份、上下文和行为的访问控制方法，可以在云原生环境中实现更精确的权限管理和安全保护。

云原生环境的弹性和可扩展性要求安全策略能够与应用程序的动态变化保持同步。零信任模型通过实时的身份验证、会话管理和持续监控，能够适应云原生环境中应用和服务的快速变化，并及时检测和响应潜在的安全威胁。

企业构建基于零信任架构的云原生安全体系，需要基于自身安全现状及业务需求的评估，审视规划有效的实施路径。

零信任实施路径



资料来源：Forrester Consulting

云原生安全架构需要涵盖云、边、端一体化的全生命周期安全防护

云原生应用数据往往分布在多个云平台和地理位置上，需要支持和集成多云环境的安全产品和技术，以确保在不同云平台上的一致的安全策略和防护措施。不仅如此，IoT以及边缘计算的发展不仅使得计算和存储被推向了终端及边缘侧，还需要考虑端点和边缘设备的身份验证、数据加密、安全连接等方面的保护措施。

在需求设计阶段，从全生命周期阶段确保DevSecOps，即在云原生应用的需求设计阶段，需要做到安全融入产品设计，实现“设计安全”，从代码及供应链上进行主动漏洞扫描、异常代码检测等。

在开发阶段（Dev），要遵循“安全左移”原则，达到上线即安全。

在运营阶段（Ops），要遵循“持续监控及响应”原则，融合资产清点、微隔离、入侵检测、安全响应、溯源分析、威胁狩猎等安全能力，形成预测、防御、检测、响应的安全闭环，做到“自适应安全”。

最终，通过云原生架构及全生命周期安全保障，赢取原生安全的目标。

云原生安全参考架构

K8S安全态势管理

- 入侵检测
- 行为风险监控
- 异常配置检测
- 用户和权限动态管理

工作负载保护

- 网络可视化
- 入侵检测
- 微隔离
- 容器WAF
- 漏洞扫描
- 配置扫描
- API扫描
- 主机
- 镜像
- 容器
- 应用

身份管理

- 权限审计追溯
- 动态鉴权
- 服务身份管理
- 运维身份管理

多云防护

资料来源：Forrester Consulting

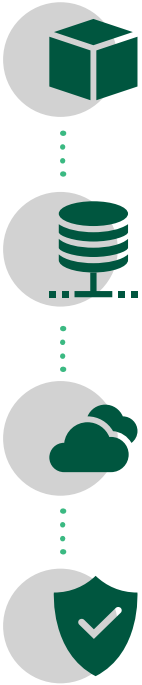
借助合作伙伴的产品及技术研发能力，构建可信、合规的云原生安全体系

依靠企业自有的团队难以应对诸多问题，选择合适的合作伙伴可以帮助企业缩短学习曲线并快速建立云原生应用开发及基础设施安全的能力。

选择合适的合作伙伴首先需要注重考察企业的产品及技术研发能力。62%的受访者希望合作伙伴能够提供满足企业需求的一站式解决方案并根据企业安全需求提供定制化解决方案。除此以外，企业更加关注合作伙伴云原生安全相关产品的能力：

- 首先，能够覆盖全形态工作负载、全生命周期以及全技术栈的一站式防护方案；
- 其次，基于零信任架构的底层身份管理和动态鉴权体系，以满足更加复杂的业务场景；
- 最后，在企业架构向多云、混合云及混合架构转变的趋势下，云原生安全产品需要兼容多云扩展检测能力，通过数据整合、响应联动实现全面洞察与防护。

企业认为安全合作伙伴需要具备的产品能力



62%
完善的产品及定制化解决方案

58%
安全技术及产品集成能力

56%
对接不同云基础设施、云平台的生态能力

52%
强大的安全技术研发能力

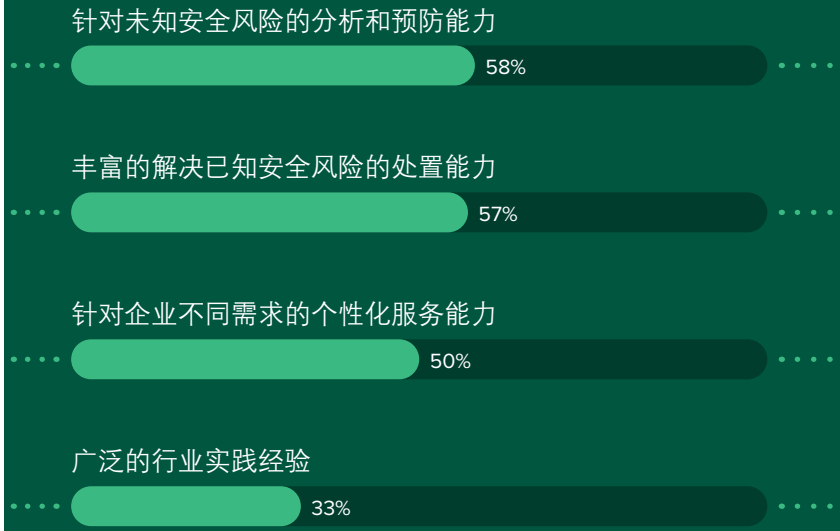
样本量：163名中国企业IT安全团队，CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

依托合作伙伴的服务能力，缩短学习曲线并规避风险

云原生技术生态仍在不断地演进和发展，由此所带来的云原生安全防护也处于不断完善和迭代过程中。在这个过程中企业安全团队不仅需要持续建设和优化原有安全体系，还需要面对各种安全威胁，对安全专业服务的需求在不断增长。

因此，选择合作伙伴在评估产品和解决方案以外，还需要重点考察合作伙伴的服务能力。在调研中企业普遍看重针对未知安全风险的分析和预防能力，针对各种安全威胁的处置能力以及针对企业不同需求个性化服务能力。除此以外，合作伙伴在服务不同行业过程中积累的经验，不仅可以为企业提供贴身服务，而且帮助企业规避误区并保护企业投资。

企业认为云原生安全合作伙伴需要具备的服务能力



样本量：163名中国企业IT安全团队、CISO部门以及基础架构团队的负责人
数据来源：2023年4月火山引擎委托Forrester Consulting进行的调研

结论及建议

云原生安全作为一种新兴的安全理念，不仅解决云计算普及带来的安全问题，更强调以原生的思维构建云、端一体化的安全，推动安全与云计算深度融合，达到安全左移、持续监控与持续响应目标。针对企业开启的云原生安全实践，Forrester建议：

- 评估安全需求与现状。企业需要根据自身的业务特征评估业务的安全需求和风险状况，包括敏感数据的位置和分类、业务流程的关键节点、合规性要求等。
- 制定安全策略和架构。确定安全目标、原则和指导方针，包括身份和访问管理、容器和微服务安全、网络安全、数据保护和加密等方面，使得安全策略与业务目标以及企业当前云原生环境的特点相匹配。
- 采用零信任模型。采用零信任模型来实现细粒度的访问控制和权限管理，通过多因素身份验证、动态访问策略和持续监控，确保只有经过验证的实体可以访问敏感资源。
- 选择合适的安全工具和技术。根据安全策略和需求，选择适合的安全工具和技术来支持云原生安全体系。确保所选工具和技术能够与云原生环境无缝集成，并提供全面的安全防护和监控能力。
- 实施持续安全监测和漏洞修复。建立实时的安全监测和漏洞修复机制，及时检测和响应。
- 强化安全培训和意识。加强员工的安全培训和意识，确保他们了解云原生安全的最佳实践和安全政策。

尾注

[1] “Predictions 2023: Cloud Computing,” Forrester Research, Inc., 2022年10月27日。

参考资料

Forrester 相关研究：

“Decoding Zero Trust,” Forrester Research, Inc., 2023年4月27日。

“Predictions 2023: Cloud Computing,” Forrester Research, Inc., 2022年10月27日。

项目团队:

谷丰, 高级顾问

研究支持团队:

Forrester信息安全与风险研究团队

研究方法

在本次调查研究当中，Forrester Consulting对163家来自金融、消费、汽车制造、互联网、能源及运营商行业的大中型企业进行了线上调研，以便对云原生安全现状以及行业趋势进行评估和研究。接受此次调查的人员当中也包括了企业CISO以及安全团队的负责人以及决策者。所提出的问题主要针对的是接受调查人员所在企业当前对云原生安全技术及产品的采纳情况和期望，以及所面临的挑战和需要优先解决的问题。研究于2023年4月开始，并于2023年5月完成。

调研概况

行业数据	
金融行业	20%
消费品及零售行业	20%
汽车制造行业	20%
互联网行业	20%
能源行业	10%
电信运营商行业	10%

所在部门及职能	
IT	49%
信息安全及风险管理CISO	51%

企业人员规模	
500至999名	21%
1000至4999名	34%
5000至19999名	28%
2万名及以上	17%

职位级别	
C级别高管	21%
副总裁	37%
总监	41%

FORRESTER CONSULTING 简介

Forrester Consulting提供独立客观、基于研究的咨询服务，以帮助商业领导者在其组织机构中取得成功。在Forrester定义的"客户至上"的研究支持下，我们的资深顾问与企业领导者们凝心聚力，通过因地制宜、历久弥新的工作模式和方法，帮助企业推进关键战略目标的执行。如需更多信息，请访问forrester.com/consulting。

火山引擎委托FORRESTER撰写的市场洞察研究报告 2023年7月

FORRESTER®