Akamai

白皮书

兑现容器的承诺

简化并加速关键资产和应用程序的分段

简介

容器技术迅速兴起，成为在云环境和混合环境中部署应用程序的首选解决方案，而容器的普及速度还在不断加快。根据 Gartner 的数据，到 2026 年，90% 的全球企业将在生产环境中运行容器化应用程序，而 2021 年这一比例仅为 40%。[1] 根据 Forrester 为 Capital One 开展的一项调研，**在参与调研的 IT 领导者中，有 86% 将为更多应用程序使用容器列为优先任务**。[2]

> 根据 Gartner 的数据，到 2026 年，**90% 的全球企业**将在生产中运行容器化应用程序，而 2021 年这一比例仅为 40%

当然，所有这些都给负责 IT 环境安全的人员增加了压力，要求他们跟上容器部署的步调，在以快速采用和扩展为头等要务的 DevOps 模式下更是如此。虽然已经出现了许多专门的容器安全解决方案，但这些面向特定平台、仅考虑容器的实体最终会增加复杂性和管理开销，无法从整体上解决企业数据中心的问题，进一步增加安全团队工作的复杂度。我们需要的是单一、全面的安全解决方案，它应该能覆盖本地、云和混合环境（包括容器在内）中运行的所有应用程序和技术，始终如一地发挥作用。

但在深入探讨解决方案之前，让我们先快速盘点一下容器技术现象、其背后的推动力量，以及从安全角度来看，这种现象产生的影响。

压力不断增加：业务需求推动采用

容器的发展及其采用率的预计增长可以回溯到企业 IT 部门需要应对的业务需求。现代企业需要能快速、敏捷地应对竞争威胁和市场机遇。他们需要支持创新、加快产品上市的解决方案。提高效率是他们始终不懈的追求。在互连互通程度日渐增加的世界中，他们希望能更轻松地与供应商、业务合作伙伴——尤其是与客户通过数字化方式进行业务往来。

这些都是企业 IT 转移到云的主要原因，或者更准确地说，是他们转移到本地/云混合模式的主要原因。这些因素也是 DevOps 趋势背后的主要推动力量。DevOps 的主旨是消除从构思到实施过程中的摩擦点，利用自动化和自动扩展来加快关键应用程序的部署，从而更快地将应用程序投入到生产环境之中。

> “对于在生产环境中使用容器所需的工作量，企业往往估计不足”。
>
> — Gartner

所有这一切都有助于解释 IT 部门采用容器化技术的原因。相较于虚拟机，容器的启动更轻松、更快速，可实现几乎无延迟的即时交付，让团队可以专注于“启动服务，而非服务器”。容器有一项关键优势，就是在当今动态数据中心环境中的可移植性；容器让应用程序可以更轻松地在本地设施与多云实例之间来回迁移。通过 Kubernetes（简称“K8s”）实现的容器编排进一步增强了这一功能，让团队能在多个环境中大规模部署和管理数量更多的容器化应用程序。业界逐渐将编排视为容器实施与管理方面的最佳实践。

简而言之，相较于其他技术，容器让 IT 部门能够以更低的总拥有成本更好地满足业务对速度、自动化、弹性和可用性的需求。但其实施并不是十全十美。Gartner 于 2019 年发布了一份有关容器化技术最佳实践的报告，其中提到：“对于在生产环境中使用容器所需的工作量，企业往往估计不足”。[3] 虽然容器化技术引起了广泛的关注，但这项技术仍处于起步阶段，安全部署的最佳实践尚未得到充分整合。Red Hat 发布的《2022 年 Kubernetes 安全状况报告》(2022 State of Kubernetes Security) 指出：“安全性 [仍然] 是容器采用过程中最令人担忧的问题之一，依然会造成应用程序未能及时部署到生产环境中”。[4] 显然，如果不具备实施策略（其中必须涵盖网络安全），企业就无法获得容器的所有潜在优势。

> Red Had 发布的《2022 年度 Kubernetes 安全状况报告》(2022 State of Kubernetes Security) 指出：“**安全问题 [仍然] 是容器采用所面临的最大问题之一，**迄今依然导致许多应用程序迟迟未能部署到生产环境”

这对安全团队意味着什么?

Gartner 在其最佳实践报告中指出：“不能等到事后才去考虑安全性，必须将其嵌入到 DevOps 流程之中”。但在现实中，情况并非如此。在仓促实施容器化技术的过程中，安全团队有时会感觉自己身处“不可能三角形”，这是一种又称为“彭罗斯不可能三角形”的视错觉图形（在 Akamai 也叫做“Klein 与 Howard 不可能三角形”）。

> 传统安全解决方案无法适应现代企业。安全解决方案必须速度快、适应性强、动态性高，并且能够与“DevSecOps”方法无缝衔接。

就像这个三角形的顶点看起来要比另外两个角远得多一样，安全性也似乎总是严重落后于业务需求以及为满足这些需求而制定的 IT 计划。然而，就像“不可能三角形”本身是一种视错觉图形一样，安全性解决方案实际上也并不像看起来那样遥远。团队要做的只是开拓思路，超越既往依赖的那种繁琐、传统的解决方案，寻求与当今企业 IT 交付方式相符，并能无缝融入“DevSecOps”方法的解决方案。这意味着解决方案需要速度快、适应性强、动态性高，并且本身就采用了 DevOps 行动方案的方法。最重要的是，解决方案要与底层操作系统和平台脱钩，从而简化实施和管理。

Klein 和 Howard 不可能三角形

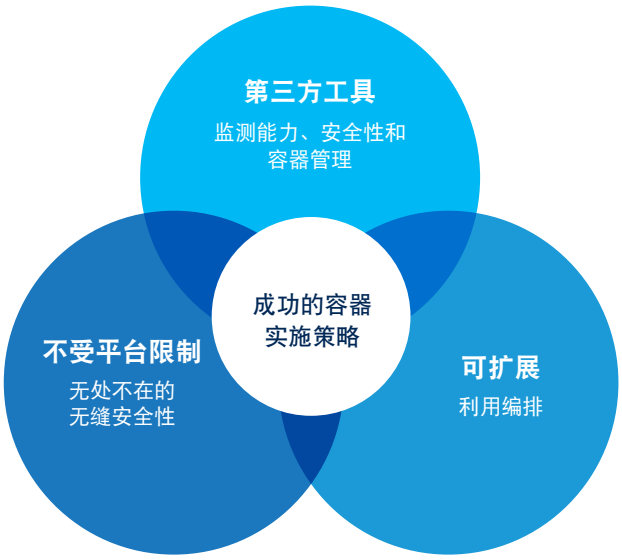
为什么“原生”不足以满足要求

在虚拟化和云迁移发展初期，企业往往被蒙蔽，误以为云原生控制措施足以满足工作负载的监测、管理和保护需求。经过反复的试错，IT 经理才认识到，他们需要一种整合第三方解决方案的叠加管理模型，以提供超越原生控制措施的安全性。

正如 Gartner 和 Forrester Research 所说，成功的容器实施策略基于“容器三要素”：

- 通过可移植、不受平台约束的方式运行容器，可在多云和本地架构内的任意位置无缝实施
- 利用编排大规模运行和管理容器
- 使用第三方工具进行容器管理、监测和安全保护

与过去的虚拟化和云技术不同，容器行业从最初起就承认，云原生管理系统（特别是安全控制措施）不足以实现有效的容器策略。在 Gartner 对容器管理解决方案开展的调研中，**65% 的受访者表示，他们打算利用第三方管理工具来监测、管理和保护容器化工作负载。**[5] 但这些第三方工具需要在本地和云实例中无缝运行，并采用精细的方法，以避免过去使用的那些繁琐、混合的方法（如安全组、VLAN 和防火墙）的零监测能力和极差的精细度造成的隐患。



利用 Akamai Guardicore Segmentation 支持企业采用容器

Akamai Guardicore Segmentation 旨在应对当今动态混合式数据中心基础架构的挑战。我们支持全面监测在多个环境中运行的所有应用程序和工作负载，并围绕单个应用程序或逻辑分组的应用程序快速创建、部署和实施安全策略，从而轻松实现精细的软件定义式分段。

更明确地说：Akamai Guardicore Segmentation 并不是一款纯容器式单点产品。容器安全是该平台的关键能力之一，该平台可在混合环境中一致地工作，除了容器之外，这种环境中还可能包括裸机服务器、虚拟机、无服务器工作负载和远程设备。因此，无论数据中心和云资产位于何处或采用何种部署方式，我们都能为企业提供单一、全面的解决方案，确保所有数据中心和云资产安全无虞，从而消除管理多个单点解决方案的需要。此外，我们的解决方案与底层平台和操作系统分离，因此在应用程序和工作负载在本地环境和云环境中移动时，安全策略也会随之移动，提升了可迁移性，也让容器成为混合云基础架构中一种更具吸引力的应用程序部署方案。

容器安全是 Akamai Guardicore Segmentation 平台的一项关键功能，可在动态、异构的数据中心环境中一致地发挥作用

在容器方面，Akamai Guardicore Segmentation 的运作机制是在容器主机节点上设置代理，从而实现对整个容器集群的监测能力，包括 pod 到 pod 以及 pod 到虚拟机的通信流。这样就可以按进程、用户和完全限定域名 (FQDN) 实施和执行高度精细化的安全策略。在编排场景中，我们支持 K8s 编排，并允许查看 Kubernetes 和 OpenShift 元数据，以获得出色的上下文。灵活的标签模型让操作人员能够使用原生 K8s 术语来表达策略。对于 K8s 的执行，我们利用原生容器网络接口 (CNI)，这是一种在 K8s 中执行策略的非侵入式方法，不会制约扩展能力。其专用模板允许用户为 Kubernetes 业务关键型应用场景提供安全围栏，无论这种应用场景是域名空间、应用程序还是任何其他对象。我们还支持根据 K8s 工作负载量和变化率进行扩展。我们的解决方案也能以类似的方式跨所有其他企业工作负载运行，因此它能作为监测、管理和保护全企业资产的统一解决方案。

在 DevOps 环境中，尤为重要的一点在于，您创建的安全策略将有效集成到持续集成/持续部署 (CI/CD) 流程中，从而确保安全性不会成为“事后诸葛”，而是完全集成于交付模型之中。

结论

容器逐渐成为许多业务环境中不可或缺的一部分。它们可以提高资源使用效率、简化流程，并提升可移植性和可扩展性。但与此同时，它们提供的内置安全机制并不足以满足需求，在采用混合环境的企业中尤其明显。

在您寻找能随着公司的成长而发展完善的安全解决方案时，请务必选择一款不受平台限制的工具，确保无论您的端到端流程在何处发生，您都能获得细致入微的见解。Akamai Guardicore Segmentation 不仅能做到这一点，还提供了现代企业为满足当下需求、迎接未来发展而需要的一系列特性和功能。

使用 Akamai Guardicore Segmentation，您的安全团队可以在动态、异构的数据中心环境内实现始终如一的安全性。这样，您就可以帮助 IT 团队兑现容器化技术的承诺，快速、经济、安全地开发和部署关键应用程序，为满足企业的业务需求打下基础。

简化整个环境的安全性。如需进一步了解我们功能强大、适用于容器的统一安全解决方案，请访问：akamai.com/guardicore。

1 Chandrasekaran, Arun 和 Wataru Katsurashima。《面向创新领导者的指南：驾驭云原生容器生态系统》(The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem)，Gartner，2021 年 8 月 18 日。

2 《企业对云容器的采用》(Cloud Container Adoption In The Enterprise)，Forrester，2020 年 6 月。

3 《在生产环境中运行容器和 Kubernetes 的最佳实践》(Best Practices for Running Containers and Kubernetes in Production)，Gartner，2019 年 2 月 25 日。

4 《Kubernetes 安全状况报告》(State of Kubernetes Security Report)，Red Hat，2022 年 5 月。

5 “Gartner 预测，全球容器管理软件和服务收入的强劲增长趋势将持续到 2024 年”(Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024)，2020 年 6 月 25 日。

Akamai 可在您创建的一切内容和体验中融入安全性——无论您在何处进行构建，将其分发到何处，从而保护您的客户体验、员工、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，让您信心十足地不断创新、发展和转型。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2023 年 5 月。

扫码关注・获取最新CDN前沿资讯