Sysdig 2023 云原生安全和使用报告

sysdig

目录

01 概要

在过去的六年里，我们分享了对客户数据的分析，为社区提供了对容器使用和安全趋势变化的报告。这份报告是基于我们的客户在过去一年中运营的数十亿个容器、数千个云账户和数十万个应用程序所收集的数据。这使我们能够真实地提供容器和云的多种实际使用情况。

云安全领域最大的两个风险是错误配置和漏洞，它们通过软件供应链越来越多地被引入到我们的环境中。2023年的报告中我们专门深入探讨了这些数据，我们将这两个安全领域内的 众矢之的 在2023年的报告中做了深入研究。不幸的是，生产环境中运行的 87% 容器镜像存在严重或高风险漏洞。尽管团队越来越多地采用左移安全策略来尽早和频繁 review 代码，但它们仍需要保证容器运行 时的安全。这一点从 Falco 等技术的广泛应用中得到了佐证，作为云原生计算基金会（CNCF）的开 源项目之一，Falco 可以帮助组织在云、容器、主机和 Kubernetes 环境中检测运行时威胁。

我们的发现让负担过重的开发者看到了希望之光，因为数据显示很多运行在运行时上有漏洞的镜像都可以进行集中修复。只有 15% 的高或严重漏洞（存在可用修复方案）在运行时实际被使用。通过基于运行时使用的软件包进行优先处理并筛选，这能够显著减少团队在追踪无尽的漏洞上花费的时间。

安全领域将零信任视为头等大事，然而我们的数据显示，零信任架构的基础之一：“最小权限访问权限” 并未得到充分执行。实际上，我们发现90%的授权许可未被使用，这为窃取证书的攻击者留下了许多机会。团队需要强制执行最小权限访问权限，因此，这需要了解哪些权限实际上正在被使用。

在当前宏观经济挑战下，大多 IT 团队正在研究减少云计算成本的方法。由于这些环境的短暂性，获取有关 Kubernetes 部署的准确利用率和成本信息 或权益调整是一项艰巨的挑战。报告显示超过 72% 的容器寿命不到5分钟，这与我们之前的分析结果相比大幅上升。

当你将短暂的生命周期与集群密度与今年再次增长的数据相结合时，很明显团队需要寻找控制成本的方法。我们的数据显示，各种规模的团队在其 Kubernetes 环境中可能存在成本超支的情况，最大的部署可能会导致浪费超过 1000 万美元。

非常荣幸地向大家呈现Sysdig 2023云原生安全与使用报告。这些信息对于确定容器和云环境的安全和使用状态非常有帮助。这些数据还可以帮助制定网络安全策略和优先事项。我们相信，这些调研结果可以帮助各种规模和各种不同上云阶段的团队。

关键趋势

安全

87% 容器镜像有高危或严重的漏洞

90% 授予的权限未被使用

15% 高危或致命漏洞在运行时中被使用

容器使用

运行超过 1,000个节点的公司可以节省超过 **1000 万美元**

72% 容器寿命不到5分钟（去年为44%）

69% 的CPU资源未被使用 (去年为34%)

02 企业在管理供应链风险方面的努力

针对软件供应链的攻击越来越多。SolarWinds 的事件提高了人们对这种风险的警惕性。就在最近发生的事：美国联邦文职行政部门（FCEB）遭受了攻击，它加剧了人们对这类风险的担忧。与此同时，伊朗政府利用 Log4Shell 漏洞部署了一个加密货币挖矿器，通过窃取凭据在 FCEB 环境中持续进行挖矿服务。开发团队越来越依赖开源软件和第三方代码，这也带来了接触已知和未知安全漏洞的风险。

> “在云原生环境中，漏洞的数量和复杂程度可能会令人不知所措。我们的开发人员和安全团队采取分层方法来审查和分类漏洞的实际风险。通过关注那些具有较高风险的漏洞，即那些被认为是高危或严重级别的漏洞，或者是那些存在的公共漏洞，可以让我们能够有效地优先考虑和集中精力采取强力措施。
>
> - Michael Bourgault, IT Security Manager, Arkose Labs

87%的镜像存在高危或严重的漏洞

出于像 Log4Shell和Text4Shell这些备受瞩目的漏洞和攻击工具，加上政府组织对网络安全的加强指导，已经导致许多团队将注意力集中在应用程序安全测试上。即使面对这些备受瞩目的漏洞，实际上解决这一风险的进度仍然很低。

令人震惊的是，87% 的镜像包含高危或严重的漏洞，比我们去年报告的 75% 还要高。当您按照镜像中漏洞数量而不是受漏洞影响的镜像数量来查看数据时，71% 的漏洞有可用的修复方案，但尚未应用。请注意，有些镜像可能存在多个漏洞。团队尽管意识到了危险，但在保持软件发布速度的同时解决漏洞仍然是一项挑战。

修复被认为是重要的东西：15% 的高危和严重漏洞在运行时被使用

尽管需要修复的软件漏洞清单好像一眼望不到头，但仍然可以有机会减少时间浪费，转而提高网络安全。根据我们的研究发现，仅有 15% 的严重和高危的漏洞在运行时加载的软件包中存在可用的修复方案。通过筛选那些实际使用中的漏洞软件包，组织团队可以将他们的精力集中在修复真正有风险的、有可修复方案的这小部分上。这是一个更具可行性的数字，并且可以缓解一些与发布决策相关的担忧，集中整改工作，前提是组织使用了相关的安全功能。

运行时聚焦于 “左移” 的功效

在镜像中每天都会发现新的漏洞，但是在规模化地维护多个 Workloads 时，修复每一个漏洞是不切实际的。成功的现代漏洞管理模式，需要安全团队根据漏洞对组织实际风险做评估，综合考虑。