大规模安全管理

云原生应用保护平台 (CNAPP) 需要考虑的因素

执行摘要

各种规模的企业都在积极实施全数字化转型，以期获得竞争优势。在此过程中，开发运维 (DevOps) 团队发挥着重要作用，因为他们的工作会对业务产生直接的影响。然而，安全运维 (SecOps) 团队必须确保在开发和测试阶段降低云原生应用的安全风险，然后再将这些应用投入生产环境。考虑到云原生应用通常会部署成百上千个实例，其底层容器化和微服务架构会进一步增加威胁风险，使挑战变得更加复杂。这与过去的传统单体应用形成鲜明对比，传统单体应用在设计上比较简单，敏捷性和大规模可扩展性都不高。

企业应该怎么做，才能确保为云原生应用提供最高级别的安全保护？此外，哪些方面风险最高？是持续企业集成和持续交付 (CI/CD) 管道、合规性考虑因素，还是会导致漏洞攻击的其他违规行为？很可能所有这些方面都存在极高风险，而且不仅限于这些方面。为了应对这些安全挑战，云原生应用保护平台 (CNAPP) 应运而生。但是，并非所有解决方案都同样行之有效。本报告将介绍 CNAPP 的特性、功能和整体能力，它致力解决的问题，以及它可以产生显著积极影响的具体使用案例。

完整 CNAPP 的定义

CNAPP 旨在集成并自动执行云安全功能，将所有必要的功能整合到单个集成式平台中，最重要的是贯穿于云原生应用的整个生命周期，包括开发、测试、部署和持续管理各个阶段。这种平台截然不同于以往多年来的 “业界最佳” 方法，后者往往采用大量单点安全解决方案，加剧了碎片化和管理挑战。那些方法使得企业需要管理多个控制面板和很多警报，对企业而言已难以为继。考虑到云原生应用的复杂性，这种现象会产生被动管理的态势，导致可视性和相应安全保护范围出现缺口。

更深入地说，CNAPP 的起源可以追溯至企业希望整合各种不同的工具，这些工具有助于实施云安全监控、警报、安全状态评估和控制，以及预防和缓解出现的各种漏洞。相比之下，云工作负载保护平台 (CWPP) 在物理或虚拟计算机和容器上使用代理，仅致力于保护工作负载安全性。它的缺点是不能在开发周期内始终应用于云原生应用运行时。

Moor Insights & Strategy 认为，一个完整的 CNAPP 应包括以下四个关键要素。

1. 它必须保护各个微服务架构、容器和无服务器部署。
2. 它应包括前述 CWPP 功能作为基础，还应包括两个附加元素：云安全状态管理 (CSPM) 和云基础设施授权管理 (CIEM)。CSPM 在将自动化应用于可观察性和产生威胁时，识别并解决风险。
3. CIEM 旨在对应用和底层硬件生成的警报进行实时分析。
4. CNAPP 必须涵盖云原生应用的整个生命周期，包括从开发、测试到生产各个阶段。这样一来，CNAPP 能够在开发阶段的早期发现漏洞，并在运行时持续监控是否存在漏洞或配置错误，实现非常理想的安全保护。

CNAPP 的价值

部署 CNAPP 可以带来不可估量的优势。云安全功能的整合可以简化 SecOps 管理。此外，还可以显著提高对盲点的可视性，从而减少安全漏洞。如此一来，就可以加快云原生应用的部署并减少代价高昂的违规操作和业务中断，所有这些都提高了企业盈利能力。CNAPP 可以使各种企业受益，尤其是那些受到严格管制的行业的企业，例如制造、金融服务、保险、医疗和制药行业。

行动建议

云原生应用能够提供现代企业所需的可扩展性和功能；然而，既要确保安全性，同时又要让 DevOps 团队可以不断创新，这可能极具挑战性。鉴于新型混合办公模式的高度分布式性质以及云原生应用的采用和部署，企业的受威胁面将继续扩大。企业需要一种简化的方法来管理云原生应用整个生命周期内的安全性，而 CNAPP 恰好能够满足这一需求。此外，并非所有 CNAPP 都同样行之有效。因此，务必确保各平台提供必要的能力和功能，以满足云安全的各项需求。

Moor Insights & Strategy 认为，思科完全有能力通过 Panoptica 提供企业在 CNAPP 中所需的功能。Panoptica 是 Outshift by Cisco 推出的 “多云应用安全解决方案”，提供涵盖从开发到运行时的完整生命周期保护，可以全面保护各种应用和包括容器、无服务器和应用程序接口 (API) 环境在内的基础设施。结合使用 Cisco AppDynamics，企业还可以及时观察到各种安全风险并通过自动补救功能缓解这些风险。所有这些功能都可以促进开发人员和安全团队高效协作，消除开发过程中的阻碍。

要了解更多信息，请访问思科 “重塑应用” 解决方案网页。

供稿人

Will Townsend，Moor Insights & Strategy 网络与安全实践副总裁兼首席分析师

发布人

Patrick Moorhead，Moor Insights & Strategy 创始人、总裁兼首席分析师

咨询问题

如果您希望探讨本报告的相关问题，请联系我们，Moor Insights & Strategy 将及时对您的问题做出回复。

信息引用

经官方认可的媒体和分析师均可引用本报告，但不得进行有悖原意的引用，并须注明作者姓名、文章标题和 “Moor Insights & Strategy”。非新闻媒体和非分析师必须事先获得 Moor Insights & Strategy 的书面许可，方可引用。

声明

本文受思科委托撰写。Moor Insights & Strategy 为本报告提及的多家高科技公司提供研究、分析、建议和咨询服务。本公司的任何员工在本文档提及的任何公司均未持有任何股权。

免责声明

本文档提供的信息仅供参考，可能包含技术上的不准确性、遗漏和印刷错误。Moor Insights & Strategy 对此类信息的准确性、完整性或充分性不做任何保证，对此类信息的错误、遗漏或不足之处不承担任何责任。本文档包含 Moor Insights & Strategy 的观点，不应理解为事实陈述。本文表达的观点如有更改，恕不另行通知。

Moor Insights & Strategy 提供的预测性和前瞻性陈述均为方向性的指示，而不是对未来事件的精确预测。尽管我们的预测性和前瞻性陈述代表了我们目前对未来的判断，但这些陈述将会受到风险和不确定因素的影响，进而可能导致实际结果与预期产生重大差异。我们提醒您不要过分依赖这些预测性和前瞻性陈述，因为这些陈述仅反映了我们截至本文档发布之日的观点。请注意，我们没有义务根据最新信息或未来事件修改或公开发布对这些预测性和前瞻性陈述进行任何修改的结果。