CORTEX® XDR™ | paloalto® NETWORKS

利用 Palo Alto Networks 解决云安全挑战

加速向云过渡

云计算正在普及：根据IDC的数据，到2022年，全球超过90%的企业将依靠本地或专用私有云、多个公共云和传统平台的组合来满足基础设施需求。[1]

随着云计算的普及，它越来越成为网络攻击的主要目标。迁移到云有助于简化和提高某些方面的安全性，例如基础架构层面。

但是，云部署也带来了安全方面的新挑战，许多企业要么不习惯处理这些挑战，要么还没有学会如何有效地解决这些挑战。在尝试解决云安全问题时，许多企业发现他们的本地部署方法并不能直接或轻松地过渡到云。

1. “IDC 预言 2021 年将成为‘多云之年’，因为全球疫情再次证明了企业对业务灵活性的迫切需求，”IDC，2021 年 3 月 30 日 https://www.idc.com/getdoc.jsp?containerId=prMETA46165020。

云安全中的多种角色

云安全所涉及的活动范围广泛，包括配置管理（确保从安全角度正确设置云资产）和深度调查和响应（应对企业环境中任何位置检测到的威胁并查找与该威胁相关的恶意活动），等等。

根据企业的不同，这些活动由与云安全相关的许多不同角色和团队职能负责，包括：

- 云基础架构工程师和架构师
- 安全架构师和工程师
- DevOps 和 DevSecOps 团队
- 监管、风险与合规性 (GRC) 团队
- SOC 经理
- 安全分析人员、事件响应人员和威胁搜寻人员
- CISO

同样，根据云计划的运行和组织方式的不同，每个团队可能对其责任范围有着不同的要求。根据计划的不同，部分团队的责任范围可能不同。

表 1：云安全角色和职责

团队/角色	关键职责
云基础架构工程师和架构师	设计云环境；云和容器平台的部署和总体职责
安全架构师和工程师	覆盖云和 SOC 团队；为公有云环境和新的云原生架构（例如，云虚拟机、容器、Kubernetes 和无服务器）实施安全性
DevOps 和 DevSecOps 团队	管理云基础架构部署；设计大规模云原生架构
GRC 团队	监控风险并将风险传达给企业
SOC 经理	确保安全运营与企业保持同步；降低驻留时间
安全分析人员、事件响应人员和威胁搜寻人员	对跨云和本地的威胁进行监控、检测、调查和响应
CISO	云端之旅和投资的总体安全性

云安全挑战

云安全挑战与负责解决这些挑战的团队一样具有多样化特征。一般来说，存在特定于云原生环境和特定于混合云/多云环境的要求。

云安全团队在很大程度上接纳了“唯快不破”的 DevOps 思维方式。他们负责保护云原生应用，同时也直接连带负责从构建到运行的流程。他们面临的挑战是确保这些应用在“构建到运行”周期的连续和快速迭代过程中和之后不会成为各种威胁和安全问题的受害者，这其中就包括：

- **应用中的漏洞**：如果未使用正确的工具扫描应用代码，则可能导致将已知 CVE 引入重要环境中，从而被攻击者所利用。在各种不同的环境和应用程序生命周期中，这一问题尤其具有挑战性。
- **配置不安全**：无论是应用本身还是运行应用的基础架构，一旦配置错误，就会增加风险。例如，存储桶配置错误、网络配置不安全或者以 Root 权限运行应用程序会导致企业的整体风险增加。
- **缺乏运行时保护**：如果没有涵盖文件系统活动、网络通信、进程活动和系统调用活动的适当可视性和保护，正在运行的应用可能会受到攻击。如果不具备合适的安全解决方案，企业就会暴露在危险之中，无法防御威胁和捕获取证活动，也就无法进一步进行事件分析。

- **网络通信可视性和控制**：微服务和应用工作负载可以彼此通信，也可以对外界通信。安全和基础架构团队需要了解应用的依赖关系，减少云网络威胁面并控制任何网络攻击。
- **公有云过度授权**：随着企业招聘大量的开发人员、DevOps 工程师、平台工程师和其他关键利益相关者，他们希望确保每个用户都拥有正确的云权限。但是，无论是单云环境还是多云环境，不得不手动针对每个用户进行配置、无法自动审核云权限以及缺乏适当大小的权限仍然是困难的挑战。

安全运营团队负责跟上云应用开发和生产推出的步调，确保在工作流中考虑云环境，以进行威胁检测、调查和响应。他们的挑战是需要同时关注本地环境和云环境，不仅要具有可视性，还要能够在不应用新方法或将本地方法转换为云方法的情况下充分利用这种可视性。他们的核心挑战包括：

- **检测跨整个企业的威胁**：威胁检测机制无法轻松提供收集、处理和分析云数据以及本地环境和资产的能力。
- **简化云环境中的事件响应**：安全运营团队经常需要在本地活动和云活动之间进行情境切换，因为它们经常通过不同的工具受到访问，或者使用单独或不相关的工作流来分类警报、执行临时分析或深入调查威胁—无论是为了界定范围还是进行取证分析。
- **跨多个数据源关联威胁活动**：对于维护本地数据收集的运营团队，他们无法实际将云数据发送到中央日志平台以运行跨数据分析。对于云托管数据记录，从云、端点、网络和用户数据将深度情境统一到一处位置可能需要高昂的成本和/或技术方面存在挑战（或者不可行），并且用来检测威胁的分析功能并没有以适当的整合深度来处理这些数据源，也就无法完全呈现事件的来龙去脉。
- **跨云和本地获取针对威胁的情境**：事件响应团队需要随时掌握来自威胁警报、事件、资产、威胁情报和所有第三方数据源（包括云和本地数据源）的全部威胁情境，这样他们就可以进行完整的调查，得出可采取行动的结果。
- **由不同的云警报造成的复合警报疲劳**：监控和分类团队无法轻松地将可疑的云活动纳入其更广泛且业已很嘈杂的警报队列，从而导致上报信息没有得到很好的验证、对因果关系缺乏理解或理解浅薄、无法轻松构建事件时间线以及整体流程碎片化现象普遍增加。

一般而言，云原生安全团队和相对传统的 SOC 团队对安全性、用户体验、调查方法和响应工作流的要求将有显著差异。

这主要是因为云安全团队将更密切地反映云应用开发和部署的“从构建到运行”周期的过程，这首先需要：

- 云安全基础方面的深度和广度
- 云活动的最大覆盖范围
- 加深对云环境的了解

但是 SOC 团队通常已经具备现有的流程，并且专注于：

- 统一企业范围内的观点，以获得威胁检测和分析所需的关键调查情境和正确的遥测
- 确保云环境深入集成到整个企业的威胁活动的更大图景之中

Palo Alto Networks 提供全面的云安全

如今，大多数企业都组合使用传统 SOC 工具（例如 SIEM 加上 CSPM 或 CWPP 解决方案）来应对这些挑战的特定方面。这种方法的主要问题在于，它无法将端点、网络、云和身份数据在本地整合在一起，以在更广泛的混合环境中将云威胁情境化。

另一种方法是评估市场上的云安全工具 EDR 或 XDR，以尝试解决整个端到端问题。这种方法的主要挑战在于 EDR/XDR 是 SOC 优化工具，无法满足云安全团队独特的安全、可用性和速度要求。

Palo Alto Networks 提供独特的云安全解决方案，可满足云安全团队和传统 SOC 团队的深度、覆盖范围和运营要求。

Prisma® Cloud 提供全生命周期漏洞管理、合规性监控和运行时保护，使云安全团队能够优先解决在云中运行的应用的风险。Prisma Cloud 还确保云资源和环境的安全配置，识别公有云中的过度授权，并结合使用网络可视性和微分段来提供全面的云网络安全。

Cortex® XDR™ 为专注于企业范围威胁监控的 SOC 团队提供云功能。Cortex XDR 的云功能正是 SOC 团队将检测、监控和调查扩展到云环境所需要的。XDR 将云主机数据、流量日志、审核日志、Prisma Cloud 数据和第三方云安全数据与非云端点、网络和身份数据源集成，供 SOC 团队使用，以将其覆盖范围扩大至跨越本地和多云环境。

表 2：Prisma Cloud 和 XDR 云功能

功能	Prisma Cloud	XDR 中的云功能
运行时安全	应用控制和允许列表可以自动剖析主机和应用行为，以警示或防御恶意进程和网络行为；文件完整性监控；数据源提供漏洞、可疑 IP 列表、反恶意软件和高级威胁防护数据；OWASP 排名前 10 的防护；DOS 防护；机器人防护；虚拟补丁	Linux 主机 EDR 提供行为威胁保护、暴力破解防护、内核完整性监控、文件/dll/宏本地分析、权限升级防护、shellcode 防护、共享对象劫持防护
分析技术	对云应用、主机、Kubernetes 和无服务器进行分析，以识别威胁的来源（出处，例如，漏洞、镜像、设置、更改者），并通过网络和用户行为分析来检测异常活动	跨数据分析涵盖端点、网络、身份和云，用于自动关联、整合以进行检测和响应，从而识别与事件相关的所有证据和恶意活动
事件管理	专为云和 DevSecOps 团队设计，用于识别威胁并为应用和资源的漏洞、配置、权限和可疑活动提供证据，并提供针对这些资源的操作历史记录	专为 SOC 分析师而设计，可通过自动和临时关联收集证据和其他情境来调查威胁的影响，这些关联可揭示与警报相关的所有其他恶意活动
威胁检测	基于机器学习的 Prisma Cloud 检测器可以自动捕获网络流量日志、审核日志以及公有云、主机和公有云和本地应用中的云资源的数据	基于机器学习的 XDR 检测器，其结果会自动在端点、网络和身份数据源中进行关联
使用警报分组、因果关系和时间线自动生成事件	警报用于显示与用户行为和网络流量相关的配置数据中的配置错误和威胁情境；对云数据泄露、云帐户入侵、违反云策略和未遵守行业基准的行为进行可视化调查	专注于以自动化方式整合警报、情境和威胁数据，为需要查看企业范围内、跨本地和多云环境的所有相关威胁活动范围的事件响应者提供端到端的事件故事

Prisma Cloud 和 XDR 的云功能共同提供了当今最全面的云安全解决方案，实现了从构建到运行再到安全操作的完整云安全。

请访问我们的网站了解 Prisma Cloud 和 Cortex XDR 的更多信息，或查看以下资源：

- Prisma Cloud 技术摘要
- Prisma Cloud 产品文档
- Cortex XDR 产品文档
- 新时代降临：第三代 XDR 推出

paloalto NETWORKS | Cybersecurity Partner of Choice

免费咨询热线：400 9911 194
网址：www.paloaltonetworks.cn
邮箱：contact_salesAPAC@paloaltonetworks.com