Solution Brief

FortiCWP为公有云提供风险管理能力

管理层摘要

使用公有云来构建和运营应用带来了新的安全风险—云管理接口和应用编程接口(API)。不像静态的本地环境，公有云是一个十分动态的环境。这就有可能产生配置失误或忽略需要的配置更新。尤其是当组织同时使用多个公有云的时候，不同的功能，不同的管理工具，以及不同的 API 都会严重碎片化组织对公有云环境的可见性。这就让组织更难在离散的环境中发现错误配置，检测复杂攻击，评估和降低资源风险，也更难保障环境的持续合规和有效的治理。

FortiCWP 中的持续配置评估和分析能够为安全团队提供可执行的信息，从而让安全团队聚焦在最高优先级的安全事件上，快速执行响应动作，自动化修复已知配置错误来快速高效的管理和缓解风险。可执行的告警让组织来根据事件的严重程度和资源对象来决定响应优先级，FortiCWP 支持的公有云资源包括：AWS S3，AWS EC2，AWS EKS，AWS IAM Roles 等等。

FortiCWP风险管理的关键能力：

- 通过集中化的可见性和控制能力降低动态公有云环境的风险
- 基于风险评分来帮助用户优化威胁缓解动作的优先级
- 提供跨多个公有云的风险管理
- 与DevOps中的配置管理生命周期集成，提供更安全的CI/CD（持续集成/持续交付）

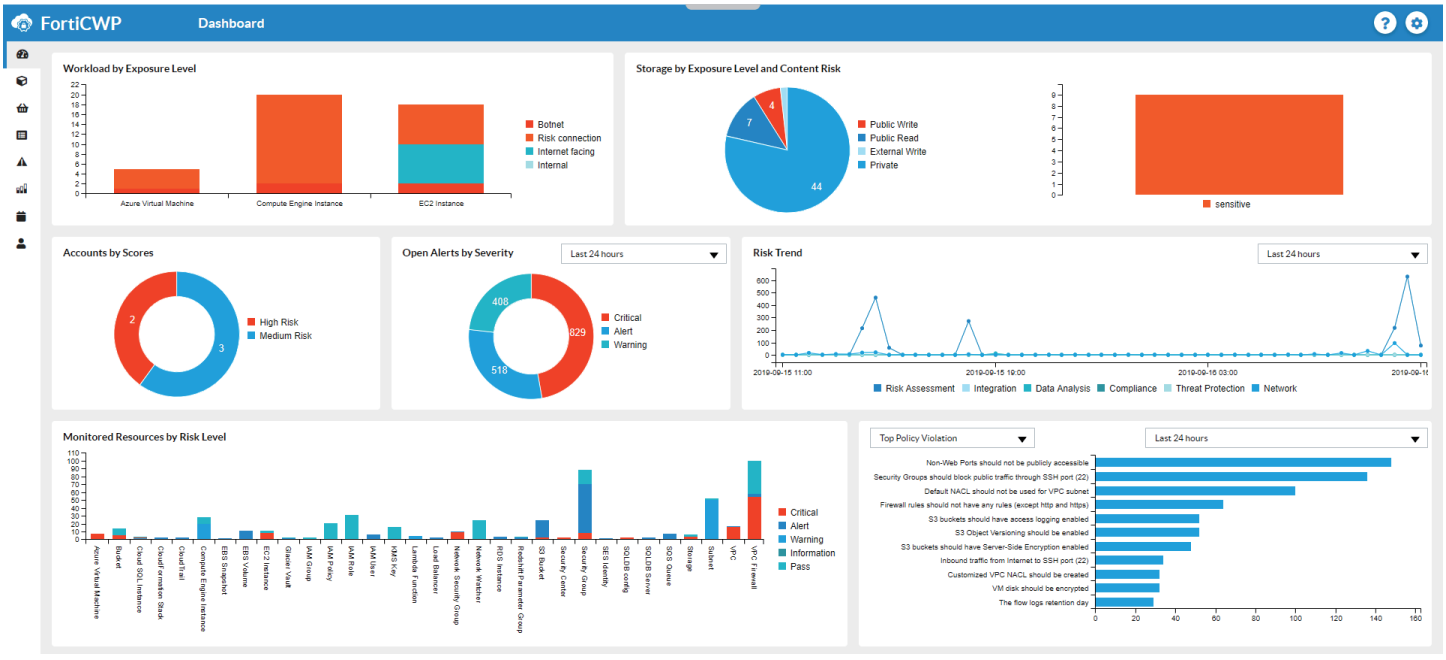

Figure1：FortiCWP对多公有云同时持续执行风险评估，帮助安全团队确定安全事件优先级

难以对碎片化的公有云基础设施做风险管理

在如今快速演进的 IT 环境中，只是管理组织中不同的人对云资源或不同服务的访问已经不够了。每个组织必须持续评估它的 IT 风险态势，并根据其风险容忍度来确定针对性的安全项目。在公有云环境中，IT 风险的一个关键来源就是针对公有云基础设施的错误配置。

使用多云，多区域的公有云，让公有云环境趋于碎片化，会提升配置管理的难度，让攻击更容易发生

组织通常依靠公有云平台中各自的原生安全工具来管理云上的服务，这无疑更加提升了配置问题发生的可能性，进而可能导致无法检测到高级复杂攻击。即使安全团队花费数小时人工来手动检查配置，这个流程也仍然会引入新的风险—人为失误，也不可能为最紧急的事件做第一时间的配置修复。更严重的是，当整个处置流程最终完成，因为云基础设施和应用团队对配置进行的频繁修改，产生的数据也已经过时了，无法为安全事件调查所用。

FortiCWP：赋能主动风险管理

FortiCWP 为组织使用的公有云基础设施提供风险评估和持续分析能力，包括 IaaS 和 PaaS 中的数百个配置项进行评估。“ 自动修复 ” 选项被启用后，FortiCWP 能够自动化处理确定的配置问题而无需人工介入，并且提供可执行的告警来帮助安全团队来识别和聚焦最高优先级的安全事件，并快速执行缓解措施。开箱即用的配置评估规则很容易配置，并且也可以由用户自己定义规则。

FortiCWP 还可以基于 Fortinet 安全评分服务为组织使用的公有云基础设施进行风险评分，较高的得分意味着较高的风险。安全团队可以查看 “ 缓解指南 ” 里的所有提升了风险评分的条目，来执行主动的安全管理措施。他们还可以在管理界面中下钻到资源描述细节中来理解配置是如何被执行变更的，变更了什么内容，来帮助他们诊断和优化配置。FortiCWP 使用每个云平台提供的 API 来获得对配置最佳的可见性，确保运营效率，准确评估多云的安全态势。

组织除了使用 FortiCWP 的预定义配置评估规则来管理风险之外，还可以使用高级脚本能力来创建自定义规则来评估云中的配置。这就让组织能够将统一的配置管理和风险管理整合进 DevOps CI/CD 流水线中。

主动管理风险

一个跨多云环境的整合安全架构能够让安全策略和安全最佳实践在整个组织级别保持一致，提升组织的安全态势水平并降低风险。FortiCWP 能够让安全团队真正进行主动风险管理，并对不同角色团队提供可执行的风险洞察，帮助弥补安全专家和云架构师之间的分歧。

[1] Asher Benbenisty, “Don’t Go Once More Unto the Breach: Fix Those Policy Configuration Mistakes,” Infosecurity, October 30, 2018.

FORTINET

www.fortinet.com

September 20, 2019 10:33 AM

377196-0-1-EN

Mac:Users:susiehwang:Desktop:ATSK223553315467215187 7:sb-forticwp-risk-management Folder:sb-forticwp-risk-management