SOLUTION BRIEF

FortiCWP 保护公有云中的数据安全

管理层摘要

随着应用向 IaaS 迁移，以及公有云中的安全风险在提升，组织已经不能再简单的在他们的混合云和多云环境中检测并足够快速的响应威胁了。FortiCWP 提供了集中化的安全监控和威胁检测能力，并通过全球化的实时更新的威胁情报来增强，涵盖包括僵尸网络和 0-day 漏洞等等威胁情报。这就让人资短缺的安全团队能够快速检测和响应威胁，提升安全效率和有效性。

保护云中的敏感数据

- 集中了解多云中的数据安全状况
- 识别数据存储的错误配置
- 映射敏感数据
- 防止数据泄露
- 检测恶意软件与其他威胁

保护云中的数据需要一个统一的安全方案

组织在加速采用云服务。到 2020 年，95% 的组织表示他们将会使用 SaaS 应用，还分别有 83% 和 74% 的组织会采用 IaaS 和 PaaS。[1]

但是如欧盟 GDPR 这样的新合规要求，以及不断演进行业合规要求如围绕个人身份信息(PII)的 PCI DSS，都在让公有云中的特定应用和数据存储要求变得愈发复杂。

传统公有云安全解决方案，不论是那些由云服务供应商开发并维护的或者单点安全方案，都不能提供充分的数据安全保护能力。一个通常的战略是部署多个独立割裂的云安全解决方案来解决每个风险点。但是这些解决方案无法协同工作，更重要的是，他们非但没有实现更好的安全效果，反而创造了更多的安全盲点，不准确的威胁情报，也不可能在攻击发生时快速检测到并执行及时有效的响应。[2]

一个统一的云安全方案必须能够解决如下挑战：

- **对存储在多个不同的公有云中的多种类型文件提供完整、实时的可见性**。很多组织都会犯的一个错误就是使用多种不同的单点安全工具，并分别部署在他们使用的不同公有云上，这便造成了一个割裂的碎片化基础设施架构，也就丧失了对公有云的全局可见性。
- **识别云存储服务的错误配置**。大多数的云安全事件都是由于错误配置导致的。有研究员表示，其对互联网扫描了 3 个月的时间，发现了 15 亿敏感文件，包含工资单信息、信用卡信息、医疗数据、知识产权专利，这些都是存储在被错误配置的存储服务中的，比如 AWS S3 桶。[3]
- **防止云中的数据泄露**。组织必须能够对使用公有云服务中的数据泄露情况进行集中化的监控、追踪并有一致性的了解。这就需要对数据进行持续监控，不论是存储中的还是在传输的。不执行这些控制手段，组织就会将自身置于风险之中。举例来说，有超过 90 家公司表示他们经历过由于员工共享了被设置为公开访问的企业云存储账号中的文件，被无意间泄露过企业和客户敏感数据。[4]
- **检测和缓解云中的恶意软件**。恶意软件的规模、传播速度和复杂度都让组织越来越难以防御。在各种不受监管的云存储中存放各种文件，会放大安全风险。有研究员发现，有10%由云服务提供商托管的数据受到恶意软件成功攻击。[5]

FortiCWP提供中央化的可视化和控制能力

由 Fortinet 提供的云安全管理解决方案，FortiCWP 通过提供三大能力来帮助组织应对上述挑战：

- 完善的配置评估 来确保云中存储数据的安全。FortiCWP评估云存储服务配置，让安全团队能够识别公有云中可能导致数据泄露和引发未期风险的错误配置和脆弱点，比如存储的文件被感染恶意软件，或敏感信息被未授权用户下载。在这种情况下，FortiCWP评估存储服务配置是否符合最佳实践和企业自行定义的存储配置安全策略。

- 强化合规与DLP。FortiCWP提供数十项预定义的DLP规则来帮助组织缓解敏感信息外泄给未期访问者的风险，以及这些风险导致的相关不利因素。这需要高度可定制的DLP工具来识别和监控敏感数据，防御数据泄露，并提供一系列预定义的与敏感信息安全有关的合规报告。
- 屡屡获奖的威胁检测和恶意软件检测能力。FortiCWP通过使用FortiGuard反病毒服务，并自动扫描存储在云中的数据来解决组织云中的勒索软件和恶意软件相关的风险。与FortiSandbox-Cloud集成，FortiCWP还可以提供针对0-day恶意软件威胁的防御能力。这两个服务都被包含在FortiGate Enterprise Protection Bundle 和 Fortinet 360 Protection Bundle订阅服务中，而无需支付额外费用。

威胁检测和恶意软件扫描两个能力，都是由Fortinet获得的AV-Comparative的最高奖：Advanced+，来提供的。

此奖证明了Fortinet在文件检测和真实世界防护方面具有极高安全水平。[6]

FortiCWP为组织采用公有云提升信心

目前看来，没有任何迹象表明公有云采用速度在放缓。随着组织部署越来越多的应用和迁移更多数据到云上，他们的网络风险也随之加大，因为他们缺乏针对全部公有云环境的一致可见性和集中化控制能力。通过使用 FortiCWP，用户能够主动管理公有云中的风险，尤其是保护关键数据，通过将原本独立、分散的云态势信息进行整合，从而对全部公有云环境提供完善的中央化可见性和统一策略管理。

FortiCWP 对多云进行集中监控，来找到错误配置，保护敏感数据，防御数据泄露，并提供预定义合规报告。

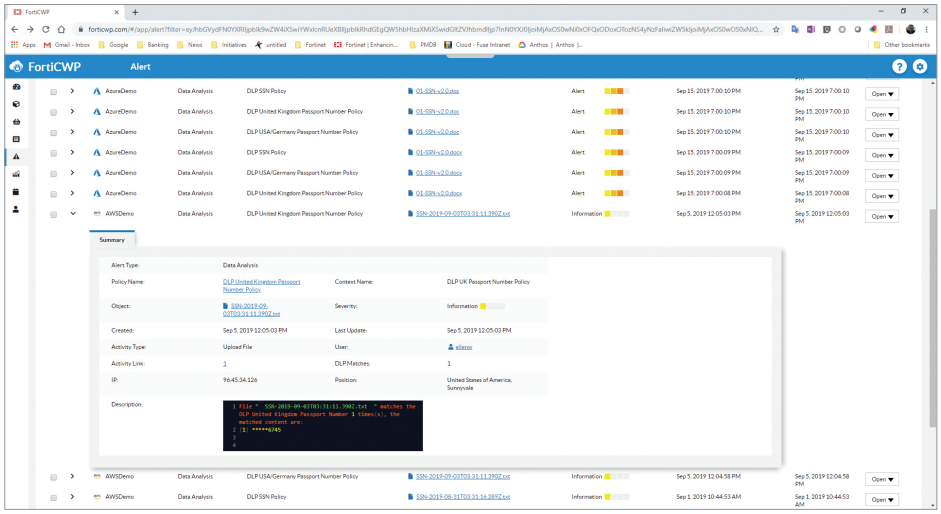

Figure 1: 统一的多云安全

[1] Louis Columbus, "State Of Enterprise Cloud Computing, 2018," Forbes, August 30, 2018.

[2] Bill Hogan, "Benefits of Using CASBs in Financial Services," Fortinet, September 26, 2017.

[3] Danny Palmer, "1.5 billion sensitive files exposed by misconfigured servers, storage and cloud services," ZDNet, April 5, 2018.

[4] Zack Whittaker, "Dozens of companies leaked sensitive data thanks to misconfigured Box accounts," TechCrunch, March 11, 2019.

[5] Patrick Nelson, "Major cloud is infested with malware, researchers say," Network World, November 10, 2016.

[6] "Anti-Virus," FortiGuard Labs, accessed March 18, 2019.

FORTINET®

www.fortinet.com

September 20, 2019 8:32 PM

488577-0-0-EN

D:\Fortinet\Work\2019\September\092019\sb-forticwp-protects data-in-public-cloud