SOLUTION BRIEF

FortiCWP 威胁检测与响应

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。

多云威胁检测与响应

- 对威胁的集中可见性
- 预定义和自定义威胁检测规则
- 自动化威胁响应工作流
- 对高级威胁的实时情报

云的作用巨大，但是也蕴藏了大量风险

公有云服务市场在 2019 年达到了 17.3% 的增速，全球市场规模达到 2060 亿美元 [1]。使用公有云的收益是显而易见的：比如提供了更强的灵活性，更快的价值实现，以及在应用运行过程中能够进行高度的弹性扩缩，并只需为使用的资源而付费，从而节省大量成本。

然而，在快速增加 10 个或更多云资源后，安全团队开始在“云中乱象”中开始挣扎。多云中的资源通常被不同的业务组部署在不同的 Region 中，同时缺乏集中控制。这就让区分合法行为还是不合法行为变得很难。FortiCWP 提供了完善的威胁规则，包括预定义规则和用户自定义规则。此外，通过利用 FortiGuard Labs 多年积累的威胁情报，FortiCWP 还能提供预定义威胁规则来解决常见的大多数错误配置以及与行为相关的威胁。

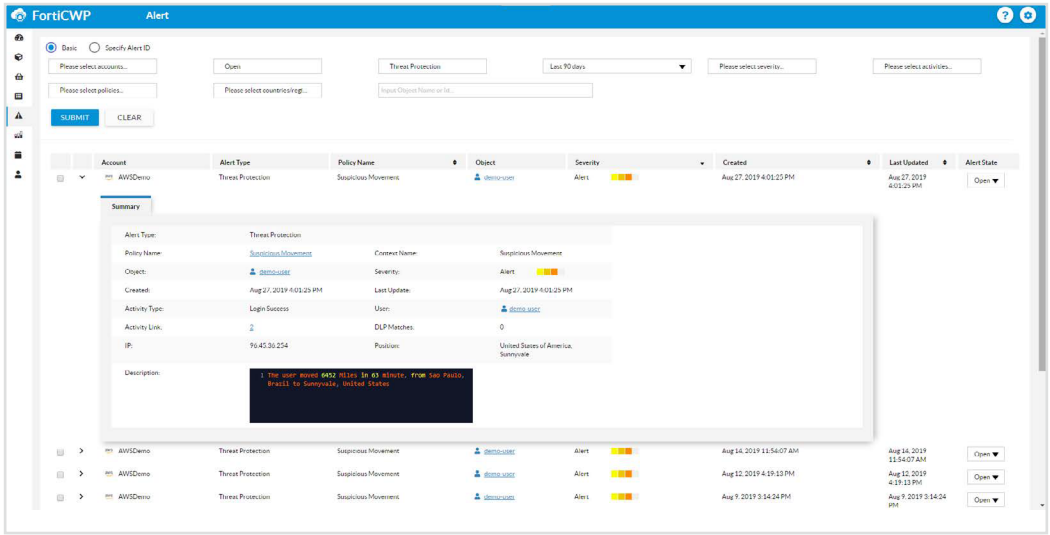
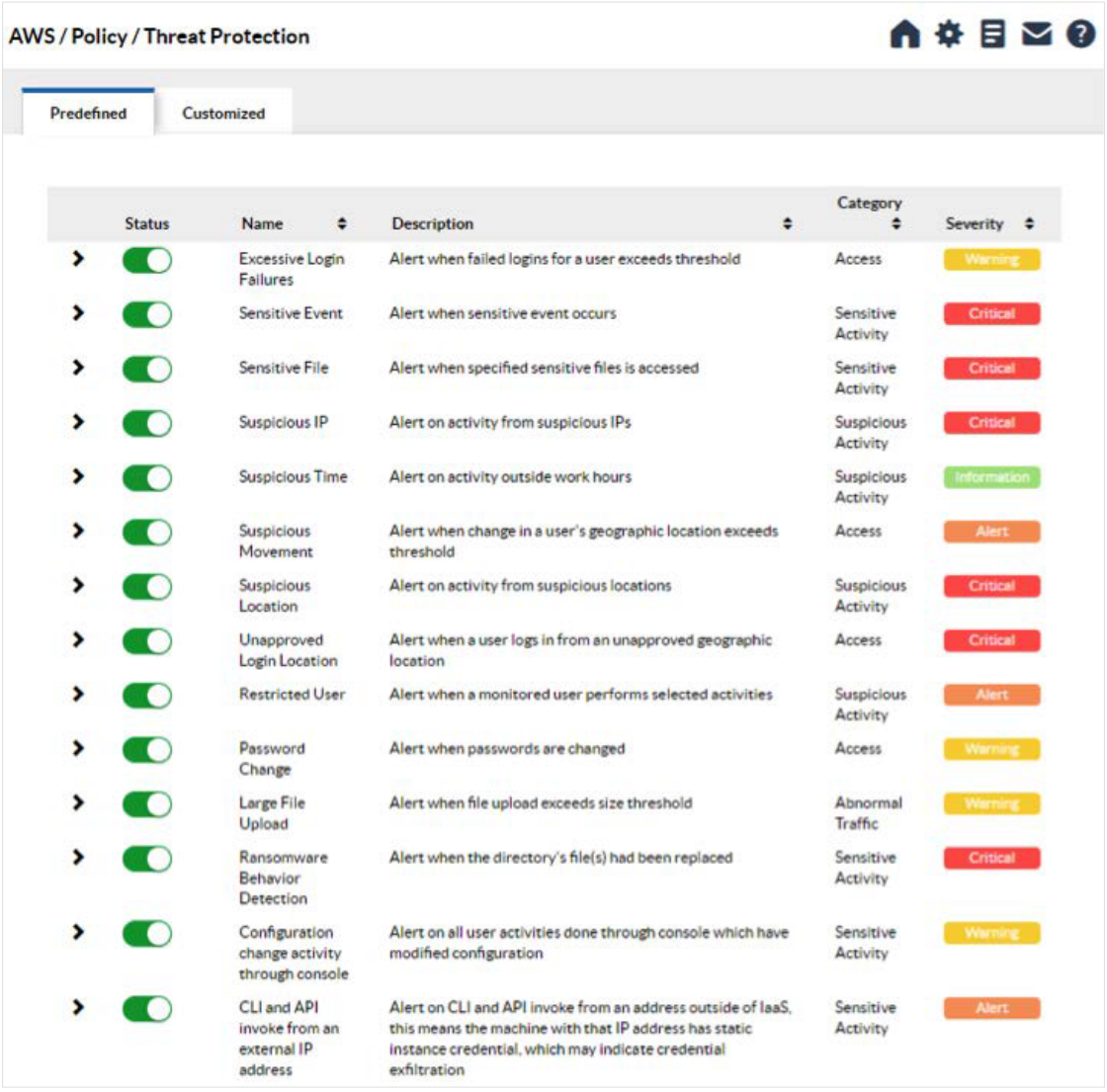


Figure 1: FortiCWP dashboard.

一个集中化Dashboard整合了针对高级威胁的实时全球威胁情报和跨多云的安全检测能力



Status	Name	Description	Category	Severity
	Excessive Login Failures	Alert when failed logins for a user exceeds threshold	Access	Warning
	Sensitive Event	Alert when sensitive event occurs	Sensitive Activity	Critical
	Sensitive File	Alert when specified sensitive files is accessed	Sensitive Activity	Critical
	Suspicious IP	Alert on activity from suspicious IPs	Suspicious Activity	Critical
	Suspicious Time	Alert on activity outside work hours	Suspicious Activity	Information
	Suspicious Movement	Alert when change in a user's geographic location exceeds threshold	Access	Alert
	Suspicious Location	Alert on activity from suspicious locations	Suspicious Activity	Critical
	Unapproved Login Location	Alert when a user logs in from an unapproved geographic location	Access	Critical
	Restricted User	Alert when a monitored user performs selected activities	Suspicious Activity	Alert
	Password Change	Alert when passwords are changed	Access	Warning
	Large File Upload	Alert when file upload exceeds size threshold	Abnormal Traffic	Warning
	Ransomware Behavior Detection	Alert when the directory's file(s) had been replaced	Sensitive Activity	Critical
	Configuration change activity through console	Alert on all user activities done through console which have modified configuration	Sensitive Activity	Warning
	CLI and API invoke from an external IP address	Alert on CLI and API invoke from an address outside of IaaS, this means the machine with that IP address has static instance credential, which may indicate credential exfiltration	Sensitive Activity	Alert

Figure 2: FortiCWP提供的预定义规则能够发现大多数常见错误配置问题

用户可以通过 FortiCWP 配置自定义那些与组织和云运营模型相关的特定行为的威胁规则。用户可以基于严重性来定义威胁规则，FortiCWP 还提供了配置向导来帮助定义自定义规则，包括由什么自定义行为触发，并且可以调用包括 AWS SNS/SQS 在内的自定义消息通知，来整合用户自身的自动化响应流水线。

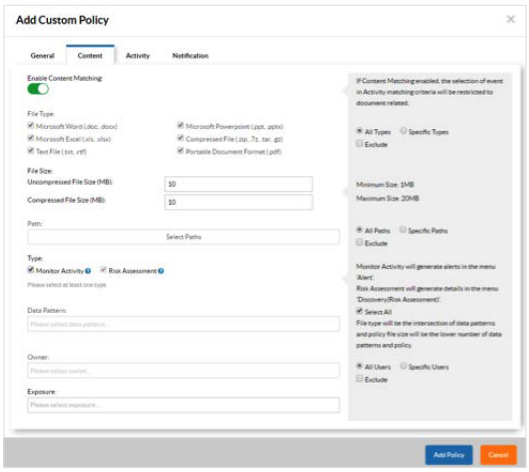


Figure 3: 安全管理员可以在FortiCWP Web管理控制台中配置自定义威胁规则

要真正检测公有云环境中的复杂威胁，就需要对行为有集中化的可见性和基于配置的规则。威胁情报也需要实时更新，以提升威胁检测和防御能力，不管哪个云是威胁攻击的目标。在云环境中，可疑行为和失陷账号需要被持续检测和屏蔽。由先进的人工智能和机器学习驱动的威胁情报，如来自 FortiGuard Labs 的失陷信标(IOC)，能够帮助用户识别和防御新威胁的传播。

集中化的多云威胁可见性与响应

由 Fortinet 提供的云安全管理解决方案，FortiCWP 通过提供四大能力来帮助组织应对上述挑战：

- 持续且集中化的安全监控。对包括配置、用户行为、流量 Flow Log，和存储在公有云环境中的数据进行持续且集中化的安全监控与评估。
- 开箱即用的预定义威胁检测规则。这些规则能够识别如恶意流量、可疑用户行为和脆弱的配置在内的潜在威胁。这些规则还是安全团队的有力帮手，弥补网络安全专家人力短缺和云基础设施用量不断增加所需安全管理的差距。
- 自定义规则。可以让用户定义出满足企业特殊需求的威胁检测规则。FortiCWP 能够让用户基于风险容忍度和企业所面临的潜在威胁来定义符合企业需求的个性化规则。
- 更快的调查。由于 FortiCWP 提供的告警包含详细数据分析和上下文信息，可以缩短安全事件调查时间。

利用全球威胁情报

FortiCWP 可以收到来自 FortiGuard Labs 的实时威胁情报，这些情报是由遍布在全球的 200 余名攻防对抗经验丰富的安全研究员 [2]，从遍布全球的 440 余万个传感器产生的数据中分析并生产而来。这个网络还结合了战略性全球安全机构，关键技术合作伙伴以及网络安全联盟。所有这些信息都支撑着 FortiCWP，提供最新最及时的保护，防御 0-day 威胁、僵尸网络、病毒和其他恶意漏洞利用。被 FortiCWP 使用的 FortiGuard Labs 包括：

0-day漏洞。FortiGuard Labs研究员已经发现并定义了超过680个0-day漏洞。通过将FortiCWP与FortiSandbox集成，可以提供额外的0-day威胁防御能力。

来自FortiGuard Labs的实时更新是由分布在全球的440万传感器驱动的

IOC(失陷信标)。FortiCWP 还通过从每日产生的数十万恶意软件样本抽取的 IOC 信息来对云环境进行监控与安全分析。此项数据服务是来源于 FortiGuard Labs 的人工智能和机器学习能力，自动化抓取恶意 IP 地址、域名和 URL，并分析和生产 IOC。

僵尸网络 IP 数据。FortiGuard Labs 使用的僵尸网络数据库每分钟都能阻断 32000 次僵尸网络的 C&C 连接。

DevOps 漏洞数据。FortiCWP 检测可疑 DevOps 行为或可能已经被攻陷的账号，并通过电子邮件或已经集成的其他消息服务如 AWS SNS/SQS 向 DevOps 和安全团队发送告警。

照亮云中威胁

FortiCWP 通过多云可见性、深入洞察以及威胁防护来有效解决公有云中的安全威胁，以此确保多云环境上的业务安全。FortiCWP 提供的关键保护能力包括：

- 监控正在进行的运维行为，配置变更，以及其他云中行为
- 通过数据关联分析来检测恶意和危险的云上行为
- 预定义威胁防御和检测规则可以防御常见云中威胁
- 用户也可以根据企业特殊需求自定义威胁防御规则
- 帮助用户针对威胁和可疑行为进行快速调查

[1] Louis Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018," Forbes, September 23, 2018.

[2] "FortiGuard Labs," Fortinet, accessed March 15, 2019.

September 21, 2019 8:08 AM

377322-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiCWP threat detection\sb-FA-forticwp-threat-detection-and-response\sb-FA-forticwp-threat-detection-and-response