

利用业界首创的 AIOps for NGFW 革新防火墙运行

各个企业都希望通过现有安全投资获得更多收益，但他们如今都面临重重挑战。网络安全运营仍有大量操作需要人工手动完成，不仅耗时费力，而且较为被动。许多企业不了解自己的网络安全态势，或者对错误配置一知半解，这可能导致他们的安全态势出现漏洞，最终面临更大的泄露风险。技能欠缺的企业可能不具备充分利用防火墙功能的产品专业知识，从而导致安全投资无法产生可观回报。最终后果便是，企业不了解具体安全状况且缺乏相关产品知识，无法阻止因防火墙相关错误导致的业务中断事件。一旦遭受影响，它们需要花费大量时间和资源来应对这种情况，尽全力找出根本原因，同时还要承受将业务转至线上的巨大压力。

市面上的现有解决方案不足以应对企业面临的现状，原因如下：

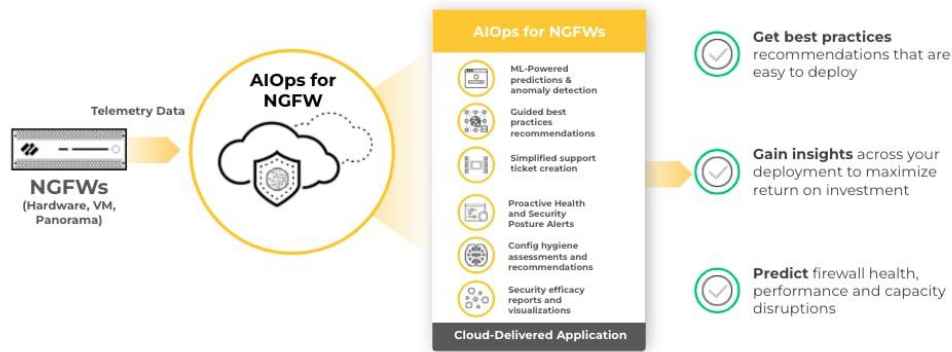
1. 无法窥探企业当前的安全态势并改善现状。
2. 无法主动出击，总是后知后觉，且无法预测并预防业务中断。
3. 无法轻松评估后续部署方案的影响。

采用行业领先的 PAN-OS 软件的最新升级版本 Nebula (PAN-OS 10.2) 后，可以利用 IT 运营人工智能 (AIOps) 解决这些问题。Palo Alto Networks (派拓网络) 推出了业界首个面向新一代防火墙 (NGFW) 的以域为中心的 AIOps。AIOps for NGFW 可在相关问题对业务产生影响之前说明、预测并解决问题，从而重新定义防火墙运行体验。

了解 **AIOps for NGFW** 如何为您提供帮助：

- **加强安全态势：**利用内置最佳实践，以及针对企业的独特部署情况量身定制的策略建议，减少攻击面并加强安全态势。最佳实践建议将由机器学习 (ML) 依照行业标准、安全策略情境以及从所有 Palo Alto Networks 防火墙收集的高级遥测数据而提出。
- **主动解决防火墙中断问题：**深入了解公司的部署情况，通过主动调查减少 NGFW 停机时间，维持防火墙的最佳运行状态和性能，保障您的 NGFW 可以平稳运行。AIOps 最多可提前 7 天智能预测防火墙运行状态、性能和容量问题，并提供可行方案来解决预测到的中断问题。

- 借助 **Palo Alto Networks 安全服务** 获得前所未有的透彻了解：一站式查看企业中各应用、威胁、网络、用户和云交付安全订阅（如 DNS Security、高级 URL 过滤和 WildFire）的相关活动。



AIOps for NGFW 通过全面了解安全状况来增强防火墙运行体验，以便提升安全态势并主动维护部署健康状况。

借助 AIOps for NGFW，您可以主动应对如今面临的主要运营挑战，例如解决错误配置和人为错误、遵循最佳实践、使用各类资源、解决硬件和软件故障，以及应对手动、重复和耗时流程。

AIOps for NGFW 是一个基于云的模块，依赖于硬件防火墙 (PA-Series)、软件防火墙 (VM-Series 和 CN-Series) 以及我们的管理平台 (Panorama™) 提供的遥测数据。这些数据会迁移至我们的 AIOps 云中，我们将在云中应用机器学习算法来生成建议并检测异常。AIOps for NGFW 由 PAN-OS® 遥测技术提供全部支持。用户可轻松部署，无需额外安装任何硬件或软件，只需在 NGFW 上打开遥测功能即可。