Cisco FirePOWER 下一代入侵防御系统 (NGIPS) 解决方案

保护网络资产和数据免受当今的威胁并非易事。您需要拥有对所有网络层和网络资源的详细可视性。Cisco FirePOWER™ 下一代入侵防御系统 (NGIPS) 解决方案可以满足您的这一需要！ 该可视性解决方案可以为您提供所需的情景感知能力，使您能够正确评估网络中的用户、主机和应用、检测多方位威胁，并进行自动防御响应。此外，FirePOWER NGIPS 解决方案不仅可以在各种已知和未知威胁发动攻击之前保护您的网络，而且能将保护一直持续到攻击中和攻击后。在世界领先的信息安全研究与咨询公司 NSS Labs 开展的独立测试中，Cisco FirePOWER NGIPS 解决方案阻止威胁的有效性评分为 99.4%，而且防御各种检测逃避方法的有效性评分达到了满分 100%。

为什么您需要一种新方法来应对当今的威胁

很多组织寄希望于使用访问控制策略来应对威胁。但是，此方法显然效果不佳。据 Verizon 2013 年数据漏洞调查报告显示，在 Verizon 去年调查的全球 621 个漏洞中，92% 的漏洞来自外部代理，52% 的漏洞来自某种黑客活动，而 40% 的漏洞中植入了恶意软件。

您需要一种新方法来防御威胁。首先，这种方法应该能够收集有关网络中发生情况的关键信息。这是因为您无法保护看不到的内容。利用智能自动化，NGIPS 解决方案可快速向您展示以下信息：被作为目标的主机；正在运行的操作系统版本、服务器和应用；所使用的移动设备和客户端应用；用户执行的操作等等。这些信息通常很难收集，过去必须访问多个源才能获得。使用 Cisco FirePOWER NGIPS 解决方案可从一个位置实时获取所有这些信息。

Cisco FireSIGHT NGIPS 解决方案的功能

- **实时情景感知：**查看和关联以下与 IT 环境相关的大量事件数据 – 应用、用户、设备、操作系统、漏洞、服务、进程、网络行为、文件和威胁。
- **高级威胁防御：**利用经过独立第三方测试验证并让全球数千客户感到满意的现有最佳威胁防御系统，抵御最新威胁。
- **智能安全自动化：**大幅降低总拥有成本，帮助您增强适应不断变化的环境的能力， 使您能够充分利用自动事件影响评估、IPS 策略调整、策略管理、网络行为分析和用户身份识别等功能。
- **高性能和可扩展性：**借助采用低延迟单通设计的专用设备获得出色的性能和可扩展性。
- **可选应用控制、URL 过滤和高级恶意软件防护 (AMP)：**通过精确控制超过 1800 个应用和 80 多个类别的数亿 URL，减小攻击面。发现、跟踪和阻止可疑文件和恶意软件的活动，防止感染蔓延以及再次感染。

为什么选择思科?

众所周知，手段高超的攻击者现在拥有足够的资源、专业知识和毅力，可能随时危害任何组织的安全。随着攻击变得越来越复杂，采用的手段越来越多，传统的防御措施已不再有效。

为当前环境寻找恰当的以威胁为中心的安全产品、服务和解决方案比以往任何时候都更为迫切。如今，您的扩展网络已经超越了传统边界，将端点、移动设备、虚拟机、数据中心和云包括在内。所以，此类解决方法必须还能轻松实现自适应，以满足您的扩展网络不断演变的需求。

近三十年来，思科一直在网络安全保护、创新和投资方面保持领先。凭借自身的专业知识和经验，我们可以提供更多情报，并将威胁防御扩展到覆盖整个攻击过程，使您获得放心开展业务所需的安全级别。

思科提供贴近现实世界的智能网络安全解决方案。

后续计划

有关 Cisco FirePOWER NGIPS 解决方案的详情，请访问 www.cisco.com/go/ngips。

C45-732341-00 10/14