Lancope StealthWatch 系统

提高整个网络的可视性，从而增强威胁检测

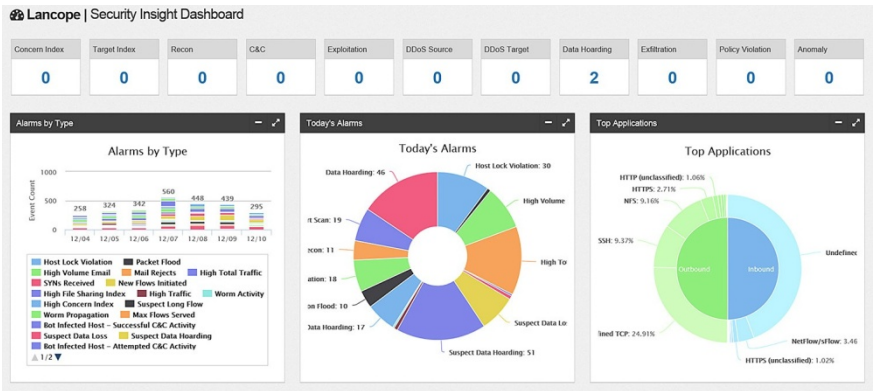
当今的企业网络比过去更加复杂、更加分散。各种新安全挑战层出不穷。在不断变化的威胁形式以及云计算和物联网等趋势的影响下，问题变得更加棘手。更令人头疼的是，随着越来越多的用户和设备添加到网络中，想要了解网络中发生的情况简直是难上加难。而在一无所知的状况下，您如何能做出保护呢？

要确定网络中是否有异常行为发生，关键是需要对网络中所有已知和未知的流量、应用、用户及设备一目了然。StealthWatch 系统采用高度完善的行为分析技术，将来自现有基础设施的数据转变为切实可行的情报，从而有效提高网络的可视性和安全性，并加快事件响应速度。

通过持续的网络流量分析加快事件响应和调查分析

StealthWatch 系统不仅可以显著改善网络可视性和安全性，还能大大缩短对整个网络中各种可疑事件的响应时间。借助于该系统，安全运营团队可以实时感知网络、数据中心和云中的所有用户、设备和流量的状态。不仅如此，StealthWatch 系统还能持续实时监控所有流量并提供全面的视图，使安全团队能够在安全事件发生前、发生时和发生后快速有效地应对各种威胁。

由于 StealthWatch 采用情景感知安全分析来自动检测异常行为，所以它能识别广泛的攻击类型，包括恶意软件、零日攻击、分布式拒绝服务 (DDoS) 攻击、高级持续性威胁 (APT)，以及各种内部威胁。



优势

- 获得对所有网络对话（包括东-西流量和北-南流量）的可视性，轻松检测内部和外部威胁
- 通过执行高级安全分析并掌握深入的情景信息，广泛检测各种可能预示攻击活动的异常行为
- 在整个网络范围加快并改善威胁检测、事件响应和调查分析
- 借助网络活动审计历史记录，实现更深入的调查分析扩展对整个网络的可视性，
- 进而简化合规性、网络分段、性能监控和容量规划等工作

“部署 StealthWatch 后，我们立即发现了 400 个行为异常的主机，而且将网络威胁减少了 90%。”

达特茅斯学院

“借助 StealthWatch，MEMC 电子材料公司在网络基准制定、实时威胁检测、事件响应、调查分析和网络故障排除等方面实现了全面改进。”

Brian Barry
MEMC 电子材料公司
安全经理

“Lancope 的 StealthWatch 系统对网络中实际发生的情况提供了非常丰富的见解，而且将预先问题通知与基于标准流数据的历史报告完美地结合到一起。”

Steve Mould
益博睿信息技术有限公司
高级 IT 架构师

StealthWatch 的优势源于以下功能：

- 跨网络周界、内部环境、数据中心，以及私有云和公共云的深入可视性
- 通过使用 NetFlow 建立基准，帮助您更轻松地了解标准网络行为，从而毫不费力地发现异常行为
- 持续监控整个分布式网络中的设备、应用和用户
- 结合高级安全分析和情报，检测各种可能预示攻击活动的行为
- 通过实时威胁检测缩短事件响应时间
- 通过全面的网络审计跟踪，实现出色的调查分析
- 提供简化的网络规划、分段、诊断及合规性验证功能
- 与网络基础设施、思科®身份服务引擎，以及支持 Cisco TrustSec®技术的硬件相集成，使网络成为安全传感器和执行器

后续行动

StealthWatch 通过收集并分析大量网络数据，为您的网络提供全面的可视性和保护，即使是规模最大、变动最频繁的网络，也尽在其掌握之中。有关 StealthWatch 的更多信息，请访问 www.cisco.com/go/stealthwatch，或者联系您当地的思科客户代表。

C45-736510-00 01/16