州政府和地方政府网络可视性

思科 Stealthwatch 可帮助机构实现以下 NIST SP 800-53 安全属别：

- 审核和问责
- 安全评估和授权
- 事件响应
- 规划
- 系统和信息保护
- 项目管理

政府机构发现打印机遭到侵害以及数百个可疑连接

在一项思科 Stealthwatch 评估中，一家政府机构发现数百个来自 10 多个国家/地区的到其网络的异常连接。经过进一步调查，该机构发现了一台为加快项目而安装的打印机。这台打印机仍未使用默认凭证打补丁并且可通过互联网进行访问。攻击者发现了该打印机并利用它获得网络访问权限，造成严重破坏。

如果该机构已安装思科 Stealthwatch，它便可以在数据遭窃取之前识别该可疑活动。

互联网和互联技术改变了世界，州政府和当地政府也不例外。除了管理公民的个人信息之外，机构通常会：

- 在线提供重要服务
- 维护关键基础设施（例如公共设施）
- 与联邦网络共享机密信息

随着智慧城市和物联网等趋势的攀升，州政府和地方政府网络只会变得更加复杂。

即使是资金最充足的机构，确保这些网络安全也是一项挑战。预算不足和赤字使得很多其他机构难以保护它们的系统。好消息是州长级别的网络安全意识正在提高，因此，现在大多数州设有企业级首席信息安全官 (CISO)。但是，缺乏资金仍是美国至少四十个州的最大障碍之一。[1] 每个州都仍然存重大网络安全漏洞。[2]

要实现优于攻击者的有利条件，州机构和地方机构需要拥有全面的网络可视性。您无法保护您看不到的东西，而且太多组织无法检测到网络中发生的恶意活动。

了解网络

全面可视性使安全人员可以获得对网络中发生的所有活动的实时情景感知能力。这一点可通过从网络基础设施设备（例如交换机、路由器和防火墙）收集 NetFlow 和其他形式的遥测数据实现。

NetFlow 是网络流量元数据。对于每项网络事务，NetFlow 都会记录发送方和接收方的 IP 地址、时间、日期、数据传输量等。此方法在提供精细见解的同时，保持足够轻量级以能够长期存储数据。很多组织会保留 NetFlow 数据长达数月或数年以协助事件响应和调查分析。

由于 NetFlow 直接从基础设施设备进行收集，它可将网络转变为一个功能强大的安全传感器。可视性可扩展到最大的分布式网络，无需依赖昂贵的检测器。NetFlow 还允许组织监控可能与终端监控软件不兼容的专用网络设备。

[1] 德勤-NASCIO，“2016 年德勤-NASCIO 网络安全研究”，2016 年

[2] 佩尔中心，“各州网络安全状态”，2015 年 11 月

“在运行 StealthWatch 的第一天，我们检测和解决了困扰我们网络团队数月的两个长期问题。它是我见过的最快可用的网络监控软件。”

– **监控网络分析师**
内华达州克拉克县

“[Stealthwatch] 对我们的安全状态和运营控制产生了重大影响。它使得我们可以快速确定网络流量异常或问题。”

– **网络和安全架构师**
弗吉尼亚最高法院

通过 StealthWatch 将数据转化为有价值的情报

但是仅有 NetFlow 并不够。收集的数据量十分巨大，在没有其他设备协助的情况下很难从中收集有用的信息。思科 Stealthwatch™ 解决方案解决了此问题。它通过强大的安全分析将大网络数据转化为有价值情报，安全专业人员可以借此应对攻击。

思科 Stealthwatch 使用行为分析。传统上，安全解决方案依赖于签名来检测威胁，而这会忽略高级、前所未见以及定向的攻击。思科 Stealthwatch 监控网络行为，从而标识出可疑活动进行调查。即使是最老练的和狡猾的威胁发起者也可以快速识别出来。

攻击者可通过多种方式进入网络，但是，他们仍必须对内部网络执行某些操作，例如扫描和数据收集。思科 Stealthwatch 会根据这些操作识别威胁。此外，思科 Stealthwatch 在所有主机上建立了预期行为基准，当观察到异常活动时会触发警报。

异常检测有利于识别各种高级威胁，包括恶意软件、高级持续性威胁、内部威胁和使用已破解访问凭证的攻击者。例如一位会计部的用户通常每天只访问几兆字节的网络资源，但突然有一天在几小时内下载了上千兆字节的敏感公民信息。这可能是存在内部威胁的迹象。思科 Stealthwatch 可以足够快速地检测到此活动，确保安全人员在敏感数据丢失之前进行干预。

将网络审计追踪用于事件响应

思科 Stealthwatch 还可帮助事件响应人员和网络操作人员调查安全和网络事件。Stealthwatch 使用 NetFlow 构建审计跟踪历史记录，以记录网络中发生的每项事务。调查员便可以使用该审计追踪快速发现事件的根本原因。

成功的调查关键在于调查员从一个数据点转移到另一个数据点的能力。例如安全操作人员仅需单击几次，便能从命令和控制警报转移至负责该行为的设备的主机快照。如果发现恶意软件，操作员可以跟踪其传播路径，并在几分钟内确定感染起始点。

同样，网络操作员人员可以从一个顶层报告中快速发现某些用户在访问重要数据中心时出现异常长的往返时间。操作员仅需单击几次，便可确定传播时间是否缓慢（表明网络存在问题），或者服务器响应时间是否比正常时间要长（可能表示服务器存在问题）。操作人员还可以确定问题的开始时间以及问题是否持续。

通过 Stealthwatch 确保州政府和地方政府的网络安全

州政府和地方政府通常负责管理重要服务和大量敏感数据，而保护其资源的安全变得更具挑战性。当技术和威胁形势不断演变时，机构需要了解其内部网络以及网络周界。

思科 Stealthwatch 提供的全面网络可视性和安全分析可使机构在数据丢失之前检测到威胁，无论攻击者使用哪种方式进入网络。要了解 Stealthwatch 如何保护您的网络，请发送邮件至 stealthwatch-sales@cisco.com 与代表联系。

C22-738160-00 11/16