概览

思科 StealthWatch 和思科安全数据中心

提升数据中心威胁可视性，加快修复时间

当今，您的组织的成功可能取决于对您的数据中心资源和信息安全的有效保护。数据中心运营商面临着不断调整流量和基础设施以满足业务需求和期望，同时遵守所有必要的安全规则的挑战。最成功的数据中心威胁防御战略的一个主要元素是对数据流量的清晰可视性。这也正是您能从思科 StealthWatch® 和思科® 安全数据中心解决方案中收获的。

StealthWatch 与安全数据中心解决方案组件（包括思科 NetFlow、思科自适应安全设备、思科身份服务引擎和思科 TrustSec® 技术）配合使用，可充分利用网络分段和用户情景。这有何益处？更好的数据中心流量可视性，从而显著提高威胁防御姿态。

如有需要，该解决方案通过流量传感器收集安全数据中心设施的 NetFlow 数据。所有数据均发送至思科的 Flow Collector 平台，由该平台分析数据中是否存在威胁在网络内传播的迹象。然后，由 StealthWatch 控制台显示该数据和有关可疑行动的所有警报。StealthWatch 还可以读取思科 TrustSec 安全组标签，用于更好地关联流量分段数据，并通过身份服务引擎共享流量数据，从而响应威胁并隔离可疑活动。这有助于实现更好的规划和安全策略、高级威胁检测，以及在发生漏洞时，更好地调查和执行事后活动。

后续步骤

有关更多信息，包括思科 StealthWatch 和思科安全数据中心的思科验证设计，请访问 www.cisco.com/go/designzonesecuredc。

优势

- 获得从网络边缘到数据中心的系统流量可视性（包括虚拟机），揭露来自任何威胁载体的潜在攻击
- 检测包括从试图泄露敏感数据的恶意内部人员到从主机到主机的内部恶意软件在内的各种数据中心问题
- 通过网络活动综合视图，改善突发事件响应、调查分析和合规性

“通过 StealthWatch 系统，我们可以发现我们的数据中心中存在的问题，不然，这些问题会被忽略，其中有一些问题非常关键。”

Henrik Strom
挪威 Telenor 的 IT 安全与 CERT 部门主管

C45-736266-01 08/16