概览

“思科身份服务引擎可拦截任何未经授权的网络访问，同时提供高度灵活的操作访问管理。”

Mirko·Berlier，思科工程师和 Expo 2015 博览会架构师

“StealthWatch 内置的行为报警具备前所未有的全新检测功能”。

Mike Sheck 思科 CSIRT 事件响应团队

借助 StealthWatch 和 ISE，获得真正的可视性

将安全用作增长推动力

在移动性、物联网、云和高级分析等趋势的推动下，许多组织正在竞相从全数字化获益。获益的关键在于调整网络以数字化速度运行，并维护网络安全不受威胁。公司对网络的安全十分放心，便能进行创新、采用新技术和开发新服务。遗憾的是，近期一项调查表明，39% 的组织因为网络安全问题，而停止关键任务项目。

即使人们发现系统遭到侵害，也始终找不到它发生的位置以及方式，使网络更易受到网络滥用和内部威胁的影响。组织需要一个可以提供全面的网络可视性的解决方案，且这种网络可视性可通过丰富的用户和设备详细信息得到增强，从而可以加速威胁检测和响应。

唯有 Stealthwatch 与思科身份服务引擎相结合方能帮助组织获得 360°视野，更快地对威胁做出响应，并为日益增长的数字业务保驾护航。

获得 360° 视野

对威胁做出更快的响应

为日益增长的数字业务保驾护航

获得 360°视野

通过 StealthWatch 和 ISE 的集成，可获得无与伦比的可视性和可控性。

- 借助 StealthWatch，持续监控、分析、隔离、分类、存储您网络的主机和用户信息。
- 管理员借助 ISE，能够查看各个设备的详细信息，包括类型、操作系统、合规性状态、连接方法、地理位置等等。
- 发现您所处环境中的异常流量。由于 StealthWatch 采用情景感知安全分析，可以自动检测异常行为，所以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。
- 精确掌握个人用户行为变为可疑的时间。通过 Stealthwatch，管理员可以设置行为阈值，一旦用户超过阈值，便会触发警报。

一家领先的医疗保健公司借助 ISE 和 Stealthwatch 获得可视性并战胜网络攻击。

挑战：

- 保护网络中 500 个站点和 250,000 台设备
- 获得对网络威胁的可视性和可控性
- 满足 HIPAA 合规性要求

解决方案：

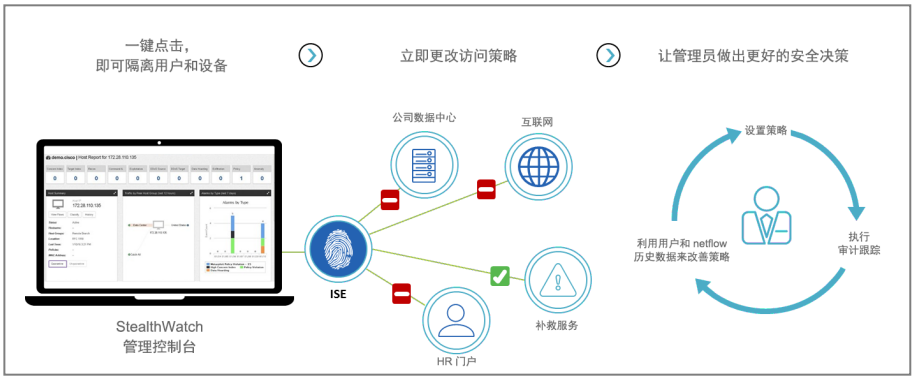
- 通过思科 ISE 和 Stealthwatch 实现网络即传感器和网络即执行器
- 实施网络分段和用户访问控制策略

结果：

- 提前 6 个月在所有站点部署
- 将威胁响应时间从几天缩短到几分钟
- 确保信息安全且符合 HIPAA 标准

通过快速遏制威胁进行响应

无论安全技术有多么先进，威胁始终会乘虚而入。解决方案不在于修筑铜墙铁壁，而在于加速响应方式。



- 一旦 StealthWatch 检测到异常流量，便会发出警报，让管理员可以选择隔离用户。通过 pxGrid，Stealthwatch 可以将隔离命令直接发送到 ISE。
- 管理员可以根据分析结果进行决策，只需点击一下，便可取消用户访问，并通过 ISE 隔离。因为 ISE 重新分配已隔离的单个用户的访问策略，所以管理员无需修改或更改整个系统策略。
- 使用事件后审计追踪，找出漏洞的根本原因。Stealthwatch 存储所有网络活动记录达数月乃至数年。

有关更快响应威胁的详情，请访问：www.cisco.com/go/rtc

为日益增长的数字业务保驾护航

为了满怀信心地推进新计划或技术，企业必须知道如何拓展业务而不带来新的安全问题。

- 不要将安全视为障碍，应该为网络分段奠定基础以实现安全的访问和可视性。
- 使管理员能够谨慎地控制对敏感资产的访问、精确知道某人尝试访问信息的时间，并将此可视性延伸到网络、环境或云的任何新区域。
- 添加用户、设备和业务，而不会影响网络可视性。通过不断从 ISE 更新设备配置文件源来减少设置新设备的管理负担。
- 在不产生盲点的情况下对环境进行扩展。单个 Stealthwatch 部署能够在拼接和去重流量的同时以 6 百万流/秒 (fps) 的速度处理来自 50000 个流量源的数据。
- 减少与信息孤岛式的管理源相关的管理负担。全网流量在 Stealthwatch 管理控制台集中显示。通过 REST API 轻松集成第三方技术和服务。

后续行动

了解详情，请访问 www.cisco.com/go/Stealthwatch、www.cisco.com/go/ise