思科 Stealthwatch 系统

优势

- **获得对所有网络对话的可视性**（包括东-西流量和北-南流量），轻松检测内部和外部威胁
- **执行高级安全分析**并掌握深入的情景信息，以检测各种可能预示攻击活动的异常行为
- **加快并改善威胁检测**、事件响应和调查分析（面向整个网络）
- **更深入的调查分析研究**，通过网络活动的审核历史记录来实现
- **简化合规性**、网络分段、性能监控和容量规划

扩展整个网络的可视性，增强安全分析和威胁检测

当今的企业网络比过去更加复杂、更加分散。新的安全挑战层出不穷，即使不是每天出现，也可以说是每周出现。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。并且您无法保护您看不到的事物。

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。思科 StealthWatch 系统采用复杂的行为分析，将来自您现有基础设施的数据转化为切实可行的信息情报。您可以获得更好的网络可视性和安全分析，从而实现更快的事件响应。

通过持续的网络流量分析加快事件响应和调查分析

思科 Stealthwatch 系统提供对所有网络流量的实时、持续监控和全面观察。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。

您的安全运营团队会获得对所有用户、设备和流量的实时情景感知，以便能在安全事件发生前后或期间对威胁做出快速有效的响应。

思科 Stealthwatch 系统采用情景感知分析，可自动检测异常行为。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) 尝试、高级持续性威胁 (APT)，以及各种内部威胁。

将可视性扩展到云

工作负荷日益从运营现场转移至云环境中。这虽然提高了组织的灵活性，但不利于您查看这些虚拟实例中的流量。然而，有了 StealthWatch 云许可证，即可在公共云、私有云和混合云环境中获得思科 Stealthwatch 提供的所有网络可视性、威胁检测和分析功能。StealthWatch 云许可证是一种附加至思科 Stealthwatch 的虚拟许可证，能够将您的“网络即传感器”部署扩展到云中，让您拥有对整个基础设施的实时情景感知能力，并获得增强的安全性。

此许可证支持安装在 Amazon Web Services (AWS) 云计算服务中。此许可证目前支持以下主机操作系统：

- Linux
- CentOS 5、6 和 7（仅限 64 位）
- Red Hat Enterprise Linux 5、6 和 7（仅限 64 位）

将可视性扩展到终端

在我们的互联世界，移动性才是王道。但是，要真正地监控所有网络活动，安全专业人员需要了解到出现在网络边缘以及远程设备上的应用和进程。借助思科 Stealthwatch 终端解决方案，安全专业人员可以对存在可疑行为的用户设备执行更加高效和情景丰富的调查。

与思科 AnyConnect® 网络可视性模块紧密集成，Stealthwatch 终端许可证在增强对终端的调查的同时提供网络可视性。安全分析师获得对所需的终端应用和信息的轻松访问权限，以加快事件响应和快速补救策略违规。

终端解决方案组成部分

- **Stealthwatch 终端许可证：**在 Stealthwatch 控制台中提供对所分析的终端数据的可视性。
- **Stealthwatch 终端集中器：**从思科 AnyConnect 可视性模块收集 IPFIX 数据。从所有终端设备收集数据并通过终端集中器将其传送到 StealthwatchFlow 收集器。

将可视性扩展到代理服务器

许多组织依靠代理服务器增强其安全状态和实施 Web 策略。这对组织很有帮助，但是，代理服务器可能破坏可视性并为攻击者创造藏身地。思科 Stealthwatch 解决方案旨在通过使用代理日志并将其集成至流记录来弥补这一缺口。代理许可证从该代理的另一端获取围绕对话的更多情境信息。通过集成代理日志并将其与适当的流关联，将代理服务器转变成安全工具而非阻碍。用户、应用和 URL 数据将会保留。这样不仅保持了对整个代理的流量监控，从而减少调查所需的时间，而且还会进一步通知 Stealthwatch 分析引擎，这样安全操作人员可以更加快速准确地识别威胁活动。

代理许可证功能支持以下 Web 代理：

- 思科® 网络安全设备
- Blue Coat
- McAfee
- Squid

将可视性扩展到分支机构

获得对分支机构流量以及分支机构之间流量的可视性对于保护您的网络至关重要。思科 Stealthwatch 学习型网络许可证将思科集成多业务路由器 (ISR) 用作安全传感器，以获得对特定分支机构路由器的流量的深度可视性。它还将行为分析与机器学习、数据包捕获和分支机构层面威胁的即时本地检测配合使用。学习型网络许可证是一个基于算法的异常检测器。思科 Stealthwatch 解决方案是一种历史型和统计型异常检测器。这些解决方案一同提供全面且深入的分支机构层面的可视性。

思科 Stealthwatch 提供以下功能：

- 对网络周界、网络内部、数据中心、私有云、公共云以及终端的深度可视性
- 通过 NetFlow 轻松了解正常网络行为，从而建立基准以便轻而易举地发现异常行为
- 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
- 简化网络分段、合规性验证和故障排除与诊断功能

“当我走进一个组织时，我知道我需要基本了解发生了什么状况或目前的状况如何，Stealthwatch 总能为我提供答案。……Stealthwatch 是我们团队最宝贵的资产，在任何人都没有注意的情况下，Stealthwatch 仍然在后台监控着一切。”

— Phil Agcaoili。
Elavon 首席信息安全官 (CISO)

“作为一家跨国企业，借助 [Stealthwatch] 的解决方案，我们能够更好地了解整个企业的网络活动。近乎实时的数据报告和警报功能使我们的团队能够在安全事件发生期间，进行更快速的检测和响应。”

— Jeff DeLong。
Westinghouse Electric Company, LLC 信息安全架构师

“[Stealthwatch] 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。它与出色的技术支持、销售、营销和与客户的积极协作相结合，形成一个胜券在握的解决方案”。

— Steve Mould。
益博睿高级 IT 架构师

跨思科产品组合进行集成

思科 StealthWatch 增强了思科的“安全无处不在”策略，在整个扩展企业中支持网络安全和可视性。

作为网络即传感器 (NaaS) 和网络即执行器 (NaaE) 计划的一个重要部分，思科 Stealthwatch 将 NetFlow 数据转变为切实可行的情报。Stealthwatch 有助于您将网络转变为传感器。您获得对所有网络流量的深度可视性以识别潜在的网络威胁。

思科 Stealthwatch 和思科身份服务引擎 (ISE) 的组合可帮助组织获取 360 度视角，更快地响应威胁，并保护不断发展的全数字化业务。通过结合这两种解决方案，您可以看到有关每台设备的详细信息：类型、操作系统、合规性状态、连接方法、地理位置等。发现您环境中的异常流量，明确掌握单个用户的行为何时变得可疑。

思科现将 NetFlow 分析和数据包分析功能相结合：我们将思科 Stealthwatch 解决方案和思科安全数据包分析器进行了整合。这两种类型的技术都可以协助对安全和网络事件进行故障排除，但通常情况下，因为预算问题或缺乏资源，两者时常以牺牲对方为代价。我们有针对性的方法可让您仅存储感兴趣的数据包，从而降低存储成本，同时提供关于网络状况的更详细、情景丰富的记录。NetFlow 提供的更强的可视性和安全情境与更准确、更具成本效益的数据包层数据获取方法相结合，将有助于在必要时进一步检查特定问题。

后续行动

思科 StealthWatch 解决方案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 http://www.cisco.com/go/Stealthwatch 或者联系您当地的思科客户代表。

C45-736510-01 03/17