思科 Stealthwatch 通过网络可视性和安全分析改善威胁防御

优势

- 获得跨所有网络对话（包括东-西流量和北-南流量）的可视性，以检测内部和外部威胁
- 实施高级安全分析，获得深入的情景，广泛检测各种可能表示攻击的异常行为
- 在整个网络上加速和改进威胁检测、事件响应和调查分析，降低企业风险
- 通过网络活动的审核历史记录，实现更深入的调查分析研究
- 跨网络扩展可视性，简化合规性、网络分段、性能监控和容量规划

如果您想获得跨内部网络和分布式网络的全面网络可视性，StealthWatch 是您的绝佳之选。思科 StealthWatch™ 系统采用成熟的行为分析技术，将数据转化为可以使用的信息情报。增强安全性，并更快地响应事件。

当今的企业网络比过去更加复杂、更加分散。每周都会出现新的安全性挑战。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。

思科 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。StealthWatch 使安全运营团队能够实时了解扩展网络上所有用户、设备和流量的状态，以便能够快速、高效地响应威胁。

通过 StealthWatch 的持续监控和信息情报，您可以检测各种攻击。您可以识别零日恶意软件、内部威胁、高级持久性威胁 (APT)、分布式拒绝服务 (DDoS) 尝试以及其他威胁，防止这些威胁对您的网络造成严重破坏。与其他安全监控解决方案不同，思科 StealthWatch 不仅可以监控进出网络的流量，还可以监控网络内部的横向或东/西向流量，识别网络滥用和内部威胁。

© 2017 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

攻击更频繁，可视性不足

当今的威胁情况变得前所未有地突出和复杂。网络无处不在，而且公司持续地收购新公司，增加新地点和设立分支机构。用户可随时随地通过自己的智能设备访问公司网络。企业应用、服务器和数据已迁移到云。随着网络不断扩大，网络情况可视性方面的挑战也在不断加大。

同时，攻击者也变得前所未有的富有经验、敏捷和有组织性，因此，对网络中可疑行为的方方面面获得可视性对防御攻击至关重要。对安全的了解源于可视性。

要实现更有效的安全，我们需要可视性，才能全面了解整个网络的情况。缺乏可视性会大大地限制提供网络诊断和合规性验证的能力。而且增加了保护网络免受网络内外威胁的工作难度。要保护复杂的企业环境，网络可视性至关重要。您需要深入了解已知和未知的流量、应用、用户和设备的状况，才能确定是否存在异常行为。

思科 StealthWatch 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事件的响应时间。StealthWatch 使安全运营团队能够实时感知网络、数据中心和云中所有用户、设备和流量的状态，以便能够快速、高效地响应威胁。

架构和组件

流量收集器、流量传感器和管理控制台是思科 Stealthwatch 系统提供网络可视性所需的核心组件。这些组件可以作为物理或虚拟设备提供，并带有各自的许可证。

流量收集器采集来自网络设备和装置的遥测数据。其中包括思科基于网络的应用识别 (NBAR)、NetFlow 安全事件记录 (NSEL)、NetFlow 和系统日志。流量收集器对数据进行收集、分析和存储。在一个网络部署中，至少需要一个收集器，最多可支持 25 个流量收集器

流量传感器适用于设备本身无法支持 NetFlow 的网络区域。流量传感器从业务关键型对等网络、社交媒体和移动应用收集应用信息和数据包层性能统计数据。流量传感器生成的流记录还提供 URL 信息。可发送流量数据至流量传感器，然后传感器可以将其发送至流量收集器。

流量收集器中的所有信息将传送至中心点管理控制台，并且仅需一个控制台便可直观地呈现收集的所有数据。

> “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。”
>
> **— Elavon CISO Phil Agcaoili**

© 2017 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

持续网络监控

对网络中所有状况的深入了解让您可以快速地为环境中的正常行为确立基准，无论您组织的规模或类型如何。确立基准有利于更轻松地识别可疑行为。您还可以确定和适当分割关键的网络资产以改善访问控制和保护。

事件后调查分析

思科 Stealthwatch 系统不仅可以改善实时威胁检测，它能够动态地加快事件响应速度，通常将故障排除时间从几天或几个月减少到几分钟。StealthWatch 可以将网络数据存储几个月甚至几年，对所有网络活动提供重要的审核跟踪，因而您可以很容易地实施精确的事件后调查分析。

除了提供对网络流量的全面了解，StealthWatch 还可以提供额外等级的安全情景，包括用户和设备感知、云可视性、应用感知以及威胁源数据。

思科 StealthWatch 与其他安全技术对比

思科 StealthWatch 可以从您的路由器、交换机和防火墙收集并分析网络遥测数据（例如流，NetFlow、sFlow、JFlow 等），监控网络和用户行为。该系统对网络数据进行先进的专有分析，自动检测可能代表攻击的异常行为。

有时会将思科 Stealthwatch 与其他监控方案进行比较，例如安全信息和事件管理 (SIEM) 和完整数据包捕获。SIEM 技术跟踪网络资产的系统日志，从基于签名的工具发布警告和警报。遗憾的是，源自受侵害计算机的系统日志不可靠，而且基于签名的监控工具只能监控它们有访问权限的内容，不监控行为变化。

同时，由于极高的成本和复杂性，完整数据包捕获只能部署在网络的有限区域内。通过无处不在的基于行为的监控补充这些信息源，是填补危险的安全漏洞的关键。此外，思科 Stealthwatch 可以与思科® 安全数据包分析器一起用于捕获和检查与思科 Stealthwatch 警报生成的异常流量关联的数据包。

由于具有高度可扩展性，思科 StealthWatch 的功能比同类安全技术更胜一筹（包括其他基于流的监控工具）。它能够删除重复数据和融合单向流记录，为最大、最复杂的企业网络带来具成本效益的流监控和存储。

> “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。”
>
> **— Westinghouse Electric Company，信息安全架构师 Jeff DeLong**

组件

用户可定制思科 Stealthwatch 系统，不过其核心组件是流量收集器、流量传感器和管理控制台。如前所述，这些组件可以作为物理或虚拟设备提供，并带有各自的许可证。下面列出了这些组件协同运行的方式：

- 流量收集器利用 NetFlow、IPFIX 和其他来自您现有基础设施的遥测数据，在整个企业网络上提供具成本效益的端到端可视性。
- 管理控制台管理、协调和配置所有思科 StealthWatch 产品，以关联整个企业的实时安全和网络情报。
- 流量传感器结合深度数据包检测 （DPI） 和行为分析，识别网络上正在使用的应用和协议。它用在网络中不支持 NetFlow 的位置。
- UDP Director 是一个高速的高性能设备，可从多个位置接收重要的网络和安全信息。它通过单一数据流，将信息转发到一个或多个目标，例如流量收集器。

© 2017 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

- 威胁智能许可证让您可以利用全球威胁情报。它生成警报和事件关注指数，标记可疑通信，以便快速展开调查研究。
- 代理许可证采集代理记录并将其与流记录相关联。它为每个流提供原始用户、应用和 URL 信息，使您能够监控通过 Web 代理的网络对话。
- 终端解决方案组件包括终端许可证和终端集中器。终端集中器从思科 AnyConnect® 可视性模块收集 IPFIX 数据。数据从所有终端设备处收集并通过终端集中器传送至流量收集器，提供对管理控制台中已分析的终端数据的可视性。
- 云许可证是是一种附加至思科 Stealthwatch 系统的虚拟许可证，能够将您的“网络即传感器”部署扩展到云中，因此您可以看到管理控制台中虚拟实例中的流。
- 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，以获得特定分支机构路由器流量的深度可视性。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检测等功能结合使用。

使用案例

各行各业	• 持续监控扩展网络 • 实时检测威胁 • 加速事件响应和调查分析 • 简化网络分段 • 满足合规性要求 • 改善网络性能和容量规划
零售	• 远程监控数百个系统是否存在安全和性能问题 • 保护销售点 (POS) 终端 • 维护 PCI 合规性
医疗	• 保护病历 • 阻止对救生医疗仪器进行的网络攻击 • 维护 HIPAA 合规性 • 保护知识产权 • 维持高级别的性能 • 快速发现和保护新的网络设备
金融服务	• 检测外部和内部威胁 • 保护客户数据 • 满足严格的合规性要求 • 维护对重要金融信息的 24 小时访问 • 查找和解决威胁和性能问题，防止它们变成危机
政府	• 持续监控整个网络是否存在高级攻击 • 保护机密信息 • 确保遵从严格的安全法规 • 检测内部威胁
高等教育	• 保护移动设备 • 检测端到端 (P2P) 文件共享 • 保护敏感信息 • 防止网络错用和滥用 • 维护高级别的可用性和性能 • 简化安全工作流程 • 满足法规遵从要求

© 2017 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

为什么选择思科？

作为 NetFlow 的发明者，思科具备得天独厚的优势，能够提供一个利用流数据实现网络可视性的安全解决方案。自 2000 年开始，Lancope 率先通过 StealthWatch 系统利用遥测数据深入了解网络和安全。通过收集和分析 NetFlow、IPFIX 和其他类型的网络遥测数据，StealthWatch 将网络转化为一个无间断的虚拟传感器，运用高级行为分析快速检测各种攻击，改善全球数百家企业的安全状况。现在，思科 StealthWatch 可以让您充分利用这两项并行技术的开发成果。

StealthWatch 部署既简单又专业

经认证的专业服务组织和经认证的合作伙伴在思科 StealthWatch 产品系列的设计、部署和管理方面拥有多年的丰富经验。凭借广泛的客户和行业经验，外部服务团队可以帮助组织优化部署，满足具体的业务要求，提高工作效率并降低风险。利用独一无二的网络和安全技能，团队能够快速、高效地实施思科 StealthWatch 系统，满足如今对高级威胁环境的强烈需求。

思科专业服务包括初步安装、运行状况检查和调整、主机分组自动化、代理集成和系统培训，以及自定义咨询和集成服务。

> “[StealthWatch] 使我们能够获得内部网络可视性……轻松审核我们的安全区域，确保某些类型的流量不会离开这些网络。”
>
> **— Central Michigan University 网络管理员 Ryan Laus**

思科 Capital

提供融资服务，助您实现目标

思科 Capital® 融资有助于您获得所需的技术来实现目标和保持竞争力。我们可以帮助您减少资本支出。加速业务发展。并优化投资和投资回报率。借助思科 Capital 融资服务，您在购买硬件、软件、服务和第三方补充设备时将拥有更多灵活性。思科 Capital 可以为您提供一种可预测的支付方式。思科 Capital 现已在 100 多个国家/地区推出。[了解更多信息](#)。

后续行动

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。

© 2017 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

思科和思科徽标是思科和/或其附属公司在美国和其他国家或地区的商标或注册商标。有关思科商标的列表，请访问此 URL： www.cisco.com/go/trademarks 。本文提及的第三方商标均归属其各自所有者。使用"合作伙伴"一词并不暗示思科和任何其他公司存在合伙关系。(1110R)

美国印刷

C22-736505-01 03/17

© 2017 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。