StealthWatch 提供无处不在的网络可视性与安全性，增强威胁防御能力

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。StealthWatch 系统采用先进的行为分析，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。持续演进的威胁格局以及云计算和物联网等趋势使情况变得更加复杂。遗憾的是，随着更多用户和设备添加到网络中，获得对现状的可视性更加困难。并且您无法保护您看不到的事物。

StealthWatch 则使这个问题迎刃而解。它能够收集并分析大量的数据，为规模最大、最活跃的网络提供全面的内部可视性和保护。StealthWatch 帮助安全运营团队获得对扩展网络上所有用户、设备和流量的实时状态感知，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，您可以广泛检测各种攻击。您可以抵御零日恶意软件、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，StealthWatch 不仅可以监控传入和传出网络的流量，还可以监控网络内部的横向或东-西流量，识别网络滥用和内部威胁。

攻击更频繁，可视性不足

今天的政府和企业正面临着网络攻击的持续泛滥。显而易见，防火墙、杀毒工具和入侵防御系统 (IPS) 已经不足以保护机密数据不落入攻击者之手。无论公司在其网络边缘部署了多少种技术，入侵者总能通过某种方法进入。他们将利用零日攻击、窃取的访问凭证、已感染的移动设备、易受攻击的业务合作伙伴或其他方法。

渐渐地，攻击者甚至不需要入侵，他们只是访问可用的凭证并登录。攻击者只需找到一名适于操控的员工，瞬间即可享有内部用户的所有权利。由于这种社会工程趋势，员工渐渐变成了内部威胁，而他们通常意识不到这一点。公司正在遭遇困境，因为他们过于关注保护周边环境，而需要花费很多的时间，来检测其网络内部的攻击者。

如果您想赢得网络战争，就必须知道网络内部的当前状况，而不只是了解周边环境以外正在发生什么。今天尤其如此。80% 以上的网络流量在数据中心里从东向西传输，绝不会超出周边。遗憾的是，安全信息和事件管理 (SIEM) 系统和完整数据包捕获等传统的安全技术几乎无法提供对内部网络的可视性。此外，从有限部署向外进行扩展时，这些方法往往不可行。

StealthWatch 架构和组件

双层 StealthWatch 架构包括 StealthWatch FlowCollector 和 StealthWatch Management Console 设备。它们可通过硬件设备或虚拟设备两种形式提供，并随附流收集许可。

StealthWatch FlowSensor 通过深度数据包检测 (DPI) 交付全面的网络和服务器性能指标可视性。如果组织的网络不支持 NetFlow，将部署 FlowSensor 作为生成网络遥感勘测数据的设备。FlowSensor 的遥感勘测数据发送到 FlowCollector，以实施行为分析。它可以识别应用和协议，优化安全性、网络运行和应用性能。

通过 FlowCollector，StealthWatch 能够以每秒 240,000 个持续流的速率存储和分析最多 4000 个遥测源。可在同一网络上汇聚最多 25 个 FlowCollector，每秒最多 600 万个流。

> “StealthWatch 使问题解决时间从几天减少到几秒。借助 StealthWatch，我们能够提前防御潜在攻击和破坏。”
>
> **- 边缘 Web 托管**

主要功能

StealthWatch 利用您的现有基础设施投资跨整个企业网络提供真正无处不在的可视性和安全情报。

持续网络监控

通过深入洞察网络上发生的一切，任何类型和规模的组织都能快速设定其环境的正常行为基准。确立基准有利于更轻松地识别可疑行为。此外，组织还可以识别重要的网络资产并进行适当分段，从而改善访问控制和保护。

早期威胁检测

StealthWatch 应用情景感知安全分析自动检测异常行为。它可以识别各种攻击，包括恶意软件、零日攻击、DDoS、APT 和内部威胁。与其他安全监控解决方案不同，它不仅监控传入和传出网络的流量，还监控横向（东-西）流量。因此，它可以揭示网络错用和滥用情况以及在网络内部进行操作的攻击者。

事件后调查分析

StealthWatch 不仅仅改善实时威胁检测。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，因而对于实施精确的事件后调查分析研究至关重要。

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

StealthWatch 与其他安全技术对比

StealthWatch 可以从您的路由器、交换机和防火墙收集并分析网络遥感勘测数据（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，人们会将 StealthWatch 与其他监控解决方案进行比较，例如 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。

由于具有高度可扩展性，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 Lancope 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时，进行快速检测和响应。”
>
> **- Westinghouse Electric Company, LLC 信息安全架构师 Jeff DeLong**

StealthWatch 组件

StealthWatch 可定制，但其核心组件是 FlowCollector 和 Management Console。如上所述，这些组件可通过硬件设备或虚拟设备两种形式提供。下面列出了这些组件协同运行的方式：

- FlowCollector 利用 NetFlow、IPFIX 和其他来自您的现有基础设施的遥感勘测数据，在整个企业网络上提供具成本效益的端到端可视性。
- Management Console 管理、协调和配置所有 StealthWatch 产品，以关联整个企业的实时安全和网络情报。
- FlowSensor 使用 DPI 和行为分析组合，识别网络上正在使用的应用和协议。
- 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。然后，它通过单一数据流，将信息转到一个或多个目标，例如 FlowCollector。
- StealthWatch Labs Intelligence Center (SLIC) 威胁源可利用全球威胁情报。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。
- ProxyWatch 采集代理记录，将它们与流记录进行关联。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。

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	• 远程监控数百个远程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 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

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 利用遥感勘测数据获得深入的网络和安全见解。通过收集和分析 NetFlow、IPFIX 和其他类型的网络遥感勘测数据，StealthWatch 将网络转化为一个无间断虚拟传感器，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 产品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 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 StealthWatch 部署，满足具体的业务要求，提高生产力并降低风险。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 StealthWatch，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**

Cisco Capital

提供融资服务，助您实现目标

Cisco Capital 可帮助您获得所需的技术来实现目标并保持竞争力。我们可以帮助您减少资本支出、加速业务发展、优化投资和投资回报率。借助 Cisco Capital 融资，您可以灵活地获得硬件、软件、服务以及第三方补充设备。同时只提供一种可预测的支付方式。Cisco Capital 现已在 100 多个国家/地区推出。了解详情。

后续计划

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。

美洲总部
Cisco Systems, Inc.
加州圣何西

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。

美国印刷 C22-736505-00 01/16