产品手册

思科 Stealthwatch 云许可证

使用思科 Stealthwatch™ 终端许可证，您可以对表现出可疑行为的终端执行深入、情景丰富的调查。

在我们的互联世界，移动性才是王道。相比以往，有更多的用户从更多的地方使用更多的设备连接到企业网络。普通员工一般使用三台个人设备用于处理工作事宜。如此一来，全球有 150 亿多台移动设备接入企业网络。事实上，这些设备中的大多数已经受侵害。

安全专业人员需要调查从网络边缘到远程设备的应用和进程。通过思科 Stealthwatch 终端解决方案，安全专业人员可以对表现出可疑行为的用户设备执行更加高效、情景丰富的调查。Stealthwatch 终端解决方案与思科 AnyConnect® 网络可视性模块紧密集成，提供更好的网络可视性，同时加强终端调查。它可提供对终端应用和安全分析师所需信息的便捷访问，从而加快事件响应，补救策略违规。

工作原理

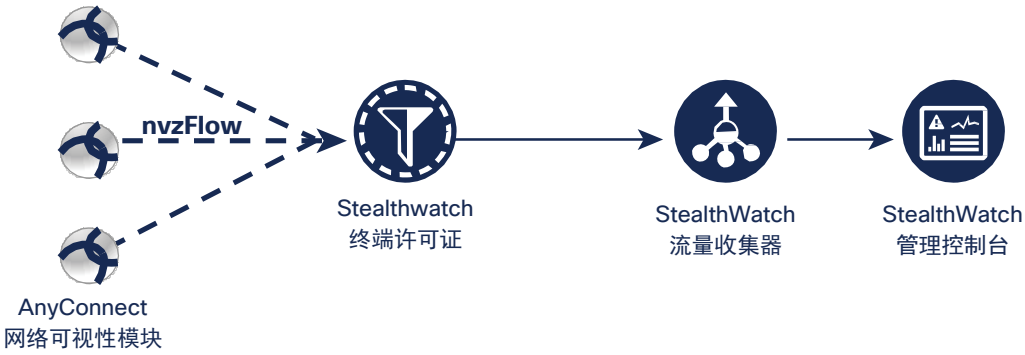
通过引入思科 AnyConnect 4.2 版网络可视性模块 (NVM)，终端许可证可提供对思科® 网络可视性流 (nvzFlow) 协议的支持。AnyConnect NVM 可收集高价值终端情景数据。它通过 nvzFlow 协议将该遥测数据导出到终端集中器，其中 nvzFlow 协议是基于标准的 IP 流信息导出 (IPFIX) 协议的延伸。终端集中器从多个终端收集这些遥测数据并将数据转发到流量收集器。在收集器中，通过拼接和去重过程，将特定终端的域插入到在流量收集器数据库中维护的对话流记录。随后，对终端数据进行分析，并在 Stealthwatch 控制台上进行显示，以通过单个视图显示整个网络上发生的活动。

从终端生成的遥测数据，可提供情景和感知。在获得保护终端所需的可视性的过程中，它是关键的一步。

组成部分和架构

图 1 显示了此解决方案的组成部分和架构。表 1 列出其主要优势。表 2 中提供了订购信息，表 3 列出虚拟版本的规格。

图 1. 思科 Stealthwatch 终端架构



组件

终端许可证：借助终端许可证，您可以从连接到网络的终端设备（例如台式计算机、笔记本电脑、智能手机和平板电脑）中捕获遥测数据。许可证允许 AnyConnect NVM 收集高价值终端情景数据，以导出到终端集中器，以便在管理控制台中进一步分析。

终端集中器：终端集中器从思科 AnyConnect 网络可视性模块中收集 IPFIX 数据。从所有终端设备中收集数据，并通过终端集中器将其传输至流量收集器。流量收集器是终端解决方案部署所必不可少的设备。

表 1. 终端许可证的主要优势

优势	说明
增强的可视性	将“网络即传感器”部署扩展到个人设备(例如：笔记本电脑、平板电脑和智能手机）。
增强的安全性	通过实时检测可疑活动和潜在攻击等威胁提供增强的安全性
更快的响应速度	通过复杂的安全性分析提供卓越的调查分析功能
提高合规性	提供实时情景感知能力和网络可视性，帮助您满足整个网络上的合规性规章。

表 2. 终端许可证订购信息

产品部件号*	分层
L-SW-EL-XY-S1	思科 Stealthwatch 终端许可证 XYR，1 – 99 位用户
L-SW-EL-XY-S2	思科 Stealthwatch 终端许可证 XYR，100 – 249 位用户
L-SW-EL-XY-S3	思科 Stealthwatch 终端许可证 XYR，250 – 499 位用户
L-SW-EL-XY-S4	思科 Stealthwatch 终端许可证 XYR，500 – 999 位用户
L-SW-EL-XY-S5	思科 Stealthwatch 终端许可证 XYR，1000 – 2499 位用户

表 2. 终端许可证订购信息（续）

产品部件号*	分层
L-SW-EL-XY-S6	思科 Stealthwatch 终端许可证 XYR，2500 – 4999 位用户
L-SW-EL-XY-S7	思科 Stealthwatch 终端许可证 XYR，5000 – 9999 位用户
L-SW-EL-XY-S8	思科 Stealthwatch 终端许可证 XYR，10000 – 24999 位用户
L-SW-EL-XY-S9	思科 Stealthwatch 终端许可证 XYR，25000 – 49999 位用户
L-SW-EL-XY-S10	思科 Stealthwatch 终端许可证 XYR，50000 – 9999 位用户
L-SW-EL-XY-S11	思科 Stealthwatch 终端许可证 XYR，100000 – 249999 位用户

*x = 1 年、3 年或 5 年

表 3. 终端许可证规格（虚拟版本）

预留 CPU	保留内存	最大帧率	最大导出进程数
2	8 GB	20,000	13,333

Stealthwatch 流量收集器：流量收集器可提供整个物理和虚拟环境的网络可视性和安全情报，从而帮助提高事件响应能力。从网络收集的 Netflow 遥测量由已部署的流量收集器的容量决定。可以安装多个流量收集器。流量收集器可通过硬件设备或虚拟机两种形式提供。在部署终端解决方案时,必须考虑流量收集器的容量。表 4 列出流量收集器的优势。

表 4. Stealthwatch 流量收集器的主要优势

优势	说明
更丰富的流情景	从代理服务器采集 URL 和代理用户数据，并将其与对应的网络流数据相关联。
更好的流量可视性	通过经过 Web 代理的给定网络对话，改善思科 Stealthwatch 系统的可视性。
威胁情报监控	自动将来自代理记录的 URL 数据与威胁情报源进行比较。
调查支持	人工调查控制台内的数据。
增加精确度	为思科 Stealthwatch 系统提供情景数据，提高安全事件预报的准确性。
关联代理和流数据	从代理服务器采集 URL 和代理用户数据，并将其与对应的网络流数据相关联。系统会自动将这些信息与威胁情报源进行比较。此外，这些信息也用于为通过控制台手动执行的调查提供支持。
可视性	允许组织查看与代理会话另一端关联的已转换地址，消除网络上的盲点。
威胁检测	采集代理记录并将其与流记录相关联，提供每个流的用户应用和 URL 信息，从而提高情景感知能力。此过程可以增强组织精确找到威胁的能力，缩短平均知道时间 (MTTK)。
事件响应	提供关于流经代理服务器的 Web 流量的附加情景，实现更精确的故障排除、事件响应和调查分析。
实时流量分析	为计费、带宽记帐和网络性能故障排除提供实时流量分析。
流流量监控	同时监控数百个网段上的流流量，这样您就能发现可疑的网络行为。此功能在企业层面上尤其重要。
确定安全问题的根本原因	在几秒钟内隔离根本原因，更快速地响应安全事件。
切实可行的见解	无需成本昂贵的探测，即可提供切实可行的性能分析。
长期数据保留	允许组织和机构长期保留大量的数据。
多种类型的流数据	使用多种类型的流数据（Netflow、IPFIX 和 sFlow），提供具成本效益的、基于行为的网络保护。
可扩展性	在速度极高的环境中保持出色表现，并且能够保护可通过 IP 访问的每个网络部分（无论大小如何）。
去重与拼接	执行重复数据删除，任何穿过多个路由器的流仅计数一次。然后，可以将流信息拼接在一起以全面了解网络事务。
端到端可视性	汇聚来自多个网络或网段的高速网络行为数据，提供端到端保护，改善分布于不同地区网络的性能。

表 4. Stealthwatch 流量收集器的主要优势（续）

优势	说明
交付方法选择	您可以订购 Appliance Edition，这是一款可扩展的设备，适合任何规模的组织。 或者，您可以订购 Virtual Edition。此版本可执行与 Appliance Edition 相同的功能，但运行于虚拟环境中。该解决方案可以根据所分配资源进行动态扩展。

当确定终端许可证支持的主机数量时，应将流量收集器作为一个指标，因为流量收集器在终端集中器之前会出现降级。影响流量收集器的最大终端流量为 50,000 fps；关于每秒流量 (fps) 的标准性能注意事项仍然适用。

管理控制台：管理控制台管理、协调及配置部署在企业重要网段的思科 Stealthwatch 设备。借助于管理控制台，管理员可通过单个界面轻松查看、了解和响应大量网络数据和安全数据。快照视图和先进的深入分析功能随时为您提供所需的信息。网络活动的高级图像和自定义视图可提供独特的见解，帮助网络和安全团队了解流量模式，识别偏离正常网络行为的行为。管理员可以查看高级详细信息，或者选择深入查看警报、安全事件详情、主机级视图以及更多内容，从而进行快速高效的故障排除和根本原因分析。动态查询、自定义报告和网络数据的直观可视化有助于缩短问题发生到问题解决之间的时间。管理控制台的主要优势列于表 5 中。各种型号规格在表 6 和 7 中列出。

表 5. 管理控制台的主要优势

优势	说明
最新实时数据	为同时监控数百个网段上的流量提供数据流，以便您发现可疑的网络行为。此功能在企业层面上尤其重要。
检测安全威胁并确定优先级的功能	通过单一控制中心提供以下能力：快速检测安全威胁并确定优先级、精确查找网络滥用和性能欠佳之处，以及管理整个企业的事件响应。
网络分组	创建网络分组和关系映射，轻松查看组织的流量状态。运营和安全团队能够在几秒钟内精确找到需要关注的方面。
图形表示	以整洁、易于理解的格式展现网络状态。
快速评估安全状态	在主控制面板上显示多个警报类别，使操作人员能够快速评估组织的安全状态。
管理思科 Stealthwatch 设备	可以配置、协调和管理各种设备，包括流量收集器和流量传感器设备。
使用多种类型的流数据	使用多种类型的流数据，包括 NetFlow、IPFIX 和 sFlow。成果：具成本效益的基于行为的网络保护。
可扩展性	支持最苛刻的网络需求。在速度极高的环境中保持出色表现，并且能够保护可通过 IP 访问的每个网络部分（无论大小如何）。
交付方法选择	您可以订购 Appliance Edition，这是一款可扩展的设备，适合任何规模的组织。 或者，您可以订购 Virtual Edition。此版本可执行与 Appliance Edition 相同的功能，但运行于虚拟环境中。
增强网络管理	通过趋势分析、防火墙和容量规划以及性能监控增强网络管理。
处理 APT、恶意软件和内部威胁	提供防御持续演进的威胁所需要的深入可视性和情景。这包括从蠕虫、病毒和其他恶意软件，到针对性攻击、DDoS 尝试、内部威胁和 APT 在内的所有安全威胁。所提供的信息还包括各种警报，以及安全人员快速采取决定性措施以降低潜在损害所需的情景信息。
网络事务审计跟踪	提供所有网络事务的完整审计跟踪，提高调查分析研究的效率。
实时可自定义关系流图	提供组织流量当前状态的图形视图。管理员可根据位置、功能或虚拟环境等任何标准轻松构建网络图。通过在两组主机之间创建连接，操作人员能够快速分析在它们之间传输的流量。然后，只需选择有问题的数据点，即可更加深入地洞察在任意时间点发生的情况。

表 6. 管理控制台型号

型号	支持的流量收集器最大数量	流存储容量
管理控制台虚拟设备	最多 5 台	1 TB
管理控制台 1000	5	1 TB
管理控制台 2000	25	2 TB

表 7. 管理控制台规格（按型号）

	管理控制台 500 和 1010	管理控制台 2010
网络	1 个管理端口：10/100/1000BASE-TX，铜端口	
数据库容量	1 TB（RAID 6 冗余）	2 TB（RAID 6 冗余）
硬件平台	R630	
硬件世代	第 13 代	
机架单元（可安装）	1RU	
电源	冗余 750W 交流电源，50/60 Hz，自动设置范围（100V 到 240V）	
散热量	2891 Btu/小时（最高）	
尺寸	高度：4.3 厘米（1.68 英寸）宽度：43.4 厘米（17.08 英寸）深度：69.2 厘米（27.25 英寸）	
单位重量	41 磅（18.6 千克）	
导轨	可滑行导轨，带线缆管理臂	
法规	FCC（仅美国）A 类 DOC（加拿大）A 类 CE 标记（EN 55022 A 类、EN55024、EN61000-3-2、EN61000-3-3、EN60950） VCCI A 类 UL 1950 CSA 950	

服务与支持

思科 Stealthwatch 提供多种服务计划。这些创新计划借助人员、流程、工具和合作伙伴的巧妙组合来实现，从而大幅提升客户满意度。这些服务有助于保护您在网络上的投资，优化网络运营，并合理地配置您的网络，通过使用新的应用程序来增强网络智能并拓展您的业务能力。有关专业服务的更多信息，请参见技术支持主页。

思科 Capital

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。了解详情。

相关详细信息

有关思科 Stealthwatch 的更多信息，请访问 www.cisco.com/go/stealthwatch。若要下单，请联系您的客户代表或发送邮件至 stealthwatch-interest@cisco.com。

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。