

StealthWatch

StealthWatch® 系统可提供行业领先的网络可视性和安全情报，帮助提高威胁检测、突发事件响应和调查分析的速度和精确度。

该系统能够利用 Netflow 和现有基础设施中的其他遥感勘测数据，以具有成本效益的方式将整个网络转化为一个传感器网。它能够检测各种异常流量和行为，包括零日恶意软件、分布式拒绝服务 (DDoS) 攻击、内部威胁和高级持久性威胁 (APT)。StealthWatch 的 Web 界面十分直观。它通过单一视图展示流量在网络中的横向移动。而且，它的信息情报和警告功能非常先进。这个简单、精致且功能强大的平台可全面增强可用性、安全分析和早期威胁检测。

优势

通过独特的网络流量视图和分析，StealthWatch 可在以下方面带来显著改善：

- 实时威胁检测
- 事件响应和调查分析
- 网络分段
- 网络性能和容量规划
- 满足监管要求的能力

StealthWatch Management Console

StealthWatch Management Console 为不同的 IT 组提供单一观测点，用于查看整个网络中所有活动的情景信息。简单的概览界面使操作人员能够快速找到故障并做出适当响应。

控制台的容量决定可以分析和呈现的 Netflow 数据量，以及可部署的 StealthWatch FlowCollector 的数量。控制台可通过硬件设备或虚拟机两种形式提供。

表 1 到表 3 列出了控制台的优势、型号和规格。

StealthWatch Management Console 的主要功能包括：

- 用户身份跟踪
- 灵活的部署选项，包括虚拟设备
- 快速根源分析和故障排除
- 相关流图
- NAT 拼接
- 自定义控制面板
- 自定义报告
- 自动拦截、修复和速率限制

- 应用、服务、端口、协议、主机、对等设备和会话的“主要排名”报告
- 流量组成分解
- 基于 Point-of-View™ 技术的可自定义用户界面
- 支持多千兆和大规模多协议标签交换 (MPLS) 网络环境
- 高级流可视化
- 强大的可扩展性
- 合并的内部和外部监控
- 容量规划与历史流量趋势分析
- WAN 优化报告
- 差分服务代码点 (DSCP) 带宽使用
- 蠕虫传播可视化
- 适合高速网络的内部安全功能

表 1. StealthWatch Management Console 的主要优势

优势	说明
实时更新数据	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、精确查找网络滥用行为和性能欠佳之处，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。
StealthWatch 设备管理	配置、协调和管理 StealthWatch 设备，包括 FlowCollector、FlowSensor 和 IDentity 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、Internet Protocol Flow Information Export (IPFIX) 和 sFlow。这使您能够以具有成本效益的方式获得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。
实时可定制关系流图	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 2. StealthWatch Management Console 型号

型号	支持的 FlowCollector 的最大数量	流存储容量
StealthWatch Management Console VE	最多 5 台	1 TB
StealthWatch Management Console 1000	5	1 TB
StealthWatch Management Console 2000	25	TB

表 3. StealthWatch Management Console 规格（按型号）

	SMC 500 和 SMC 1010	SMC 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	18.6 千克（41 磅）	
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	

注：这些规格适用于 StealthWatch 6.7。

StealthWatch FlowCollector

StealthWatch FlowCollector 跨物理和虚拟环境提供网络可视性和安全情报，帮助提高事件响应能力。

从网络收集的 Netflow 遥感勘测数据量由已部署 FlowCollector 的容量决定。可以安装多个 FlowCollector。

FlowCollector 可通过硬件设备或虚拟机两种形式提供。表 4 概述了 FlowCollector 的优势，表 5 列出了其规格。

表 4. StealthWatch FlowCollector 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	针对经过 Web 代理的指定网络会话，提高 StealthWatch 系统的可视性。
SLIC 威胁源监控	自动将来自代理记录的 URL 数据与 StealthWatch Labs Intelligence Center (SLIC) 威胁源进行比较。
调查支持	人工调查控制台内的数据。
增加精确度	为 StealthWatch 系统提供情景数据，提高安全事件的精度。
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 SLIC 威胁源进行比较。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)。
应急响应	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，这样您就可以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见解。
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)。
重复数据删除与拼接	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。
在分布于不同地区的网络上实现端到端可视性	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。
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。

表 5. StealthWatch FlowCollector 规格 (按型号)

	FC 1010	FC 2010	FC 4010	FC 5000
说明	冗余的电源、存储和额外的接口，易于在多个接口上收集流。适合于大中型网络的功率要求。	适合于极大型 Netflow、sFlow 或 IPFIX 环境的全硬件冗余和流处理功率要求。	大规模可扩展性，具备可扩展的存储功能以及处理海量流数据的能力。	大容量流采集解决方案，满足企业级客户对卓越性能的需求。
每秒最大流数	最多 30,000 个	最多 60,000 个	最多 120,000 个	最多 240,000 个
最大导出设备或路由器数量	500	1000	2000	4096
网络	1 个管理端口： 10/100/1000BASE-TX，铜缆端口 3 个监控或侦听端口			<ul style="list-style-type: none"> • 1 个管理、监控或侦听端口：10/100/1000BASE-TX • 1 个为未来预留的端口：10/100/1000BASE-TX • 1 个数据库节点连接端口：10 Gbps • 1 个为未来预留的端口：10 Gbps
流存储	1 TB (RAID 6 冗余)	2 TB (RAID 6 冗余)	4 TB (RAID 6 冗余)	6 TB (RAID 10 冗余)

	FC 1010	FC 2010	FC 4010	FC 5000
硬件平台	R630	R630	R630	<ul style="list-style-type: none"> 引擎: R620 数据库节点: R820
硬件世代	第 13 代			
机架单元 (可安装)	1RU		2RU	<ul style="list-style-type: none"> 引擎: 1RU 数据库节点: 2RU
电源	冗余 750W 交流电源, 50/60 Hz, 自动设置范围 (100V 到 240V)			<ul style="list-style-type: none"> R620: 两个可热插拔冗余电源 (1+1), 750W R820: 两个可热插拔非冗余电源 (2+0), 1100W
散热量	2891 Btu/小时 (最高)			<ul style="list-style-type: none"> R620: 2891 Btu/小时 (最高) R820: 4100 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)	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)	高度: 8.7 厘米 (3.4 英寸) 宽度: 44.4 厘米 (17.5 英寸) 深度: 69.2 厘米 (27.25 英寸)	R620 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) R820 高度: 8.7 厘米 (3.4 英寸) 宽度: 44.4 厘米 (17.5 英寸) 深度: 74.1 厘米 (29.2 英寸)
重量	18.6 千克 (41 磅)		29.5 千克 (65 磅)	R620: 29.03 千克 (64 磅) R820: 38.5 千克 (85 磅)
导轨	可滑行导轨, 带线缆管理臂			
法规	FCC (仅美国) A 类 DOC & ICES (加拿大) A 类 CE 标记 (EN55022 A 类、EN55024、EN61000-3-2、EN 61000-3-3、EN60950) VCCI A 类 UL 1950 CSA 950			

注: 这些规格适用于 StealthWatch 6.7。

每秒最大流数量可能根据网络条件不同有所变化。

StealthWatch FlowSensor

FlowSensor 是一个组件, 可为不支持 Netflow 的交换和路由基础设施片段生成 Netflow 数据。它可以在各种环境下工作, 在这些环境中, 重叠监控解决方案更加适合 IT 机构的运营模式。FlowSensor 能够为不启用思科® 基于网络的应用识别 (NBAR) 的环境提供第 7 层应用信息。

FlowSensor 提供网络和服务器性能指标全面的可视性。它将深度数据包检测 (DPI) 和行为分析结合在一起, 识别应用和协议, 从而优化安全性、网络运营和应用性能。

从网络生成的 Netflow 数据量由已部署 FlowSensor 的容量决定。可以安装多个 FlowSensor。FlowSensors 可通过硬件设备或监控虚拟机环境的软件两种形式提供。表 6 和 7 列出了 FlowSensor 的主要优势和规格。

StealthWatch FlowSensor 的主要功能包括：

- 第 7 层应用情景
- 流可视性
- Netflow 生成
- 虚拟环境可视性
- 针对当前威胁进行实时更新
- 计算 TCP 连接的往返时间 (RTT) 和服务器响应时间 (SRT)

表 6. StealthWatch FlowSensor 的主要优势

优势	说明
第 7 层应用可视性	通过收集应用信息以及数据包层的性能统计数据，提供真正的第 7 层应用可视性。
数据包层性能和分析	通过收集应用信息以及数据包层的性能统计数据，提供真正的第 7 层应用可视性。
网络异常警报	指出任何异常网络行为并立即发送警报和情景情报，使安全人员能够快速采取行动，降低损害。
降低成本	在几秒内识别和隔离问题或事件的根本原因，提高运营效率，降低成本。
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。

表 7. StealthWatch FlowSensor 规格

	FS 1010	FS 2010	FS 3010	FS 4010
通信				
吞吐量	1.0 Gbps (512 字节数据包) 400 Mbps (64 字节数据包)	2.5 Gbps (512 字节数据包) 800 Mbps (64 字节数据包)	5.0 Gbps (512 字节数据包) 1.2 Gbps (64 字节数据包)	20.0 Gbps (512 字节数据包) 4 Gbps (64 字节数据包)
接口				
管理端口	1 个端口：10/100/1000BASE-TX，铜端口			
监控端口	3 个端口：10/100/1000BASE-TX，铜端口	5 个端口：1 GB (5 个铜端口或 3 个铜端口和 2 个光纤端口)； 额定监控速度为 2.5 Gbps	2 个端口：10 GB， 光纤；总计额定监控速度为 5 Gbps	4 个端口：10 GB， 光纤；总计额定监控速度为 20 Gbps
控制台端口	基于内核的串行虚拟机(KVM)			
物理				
硬件平台	R220	R630		
硬件世代	第 12 代	第 13 代		
外形		堆叠式		
尺寸	高度： 4.24 厘米 (1.67 英寸) 宽度： 43.4 厘米 (17.09 英寸) 深度： 39.37 厘米 (15.5 英寸)	高度： 4.3 厘米 (1.68 英寸) 宽度： 48.24 厘米 (18.99 英寸)，含机架栓锁；43.4 厘米 (17.08 英寸)，不含机架栓锁 深度： 74.3 厘米 (29.25 英寸)		
重量	15.4 千克 (35 磅)	18.6 千克 (41 磅) 最大配置		
存储	500 GB，非冗余	300 GB (RAID 1 冗余)		

	FS 1010	FS 2010	FS 3010	FS 4010
环境				
电源	单个：250W（非冗余）	冗余 750W 交流电源，50/60 Hz，自动设置范围（100V 到 240V）		
散热量	1040 Btu/小时	2891 Btu/小时（最高）		
温度	工作温度：10° 到 35°C （50° 到 95°F） 存储：-40° 到 65°C （-40° 到 149°F）	工作温度：10 到 35°C（50 到 95°F），最大级变为每小时 10°C（50°F）。注意： 海拔超过 900 米（2950 英尺）时，每上升 168 米（550 英尺），最大工作温度 下降 17°C（1°F）。 存储温度：-40 到 65°C（-40 到 149°F），每小时最大级变为 20°C（68°F）。		
相对湿度	工作湿度：10% 到 80%（非冷凝），最大级变为每小时 10%。存储湿度：5% 到 95%（非冷凝）			
合规性	CE 排放/FCC Class A/RoHS	FCC（仅美国）A 类 DOC（加拿大）A 类 VCCI A 类/UL 1950/CSA 950 CE 标记（EN 55022 A 类、EN 55024、EN 61000-3-2、EN 61000-3-3、EN 60950）		

注：这些规格适用于 StealthWatch 6.7。

StealthWatch UDP Director

UDP Director® 可简化在整个企业内收集与分发网络数据和安全数据。通过从多个位置接收重要的网络和安全信息，然后将信息转发到单一数据流并再转发到一个或多个目标，有助于降低网络路由器和交换机的处理压力。

表 8 和 9 概述了该指示器的主要优势和规格。

表 8. StealthWatch UDP Director 的主要优势

优势	说明
减少意外停机和服務中断	仅在 UDP Director 2000 设备上提供 UDP Director 高可用性。UDP Director 1000 设备不支持 UDP Director 高可用性。
简化网络安全与监控	UDP Director 汇聚 Netflow、sFlow、syslog 和 Simple Network Management Protocol (SNMP) 信息并为其提供单一的标准化目标。这样，它可以显著简化大型企业内多种类型网络和安全数据的集成。UDP Director 设备可以从任何无连接 UDP 应用接收数据，然后将数据重新传输到多个目标，还可以根据需要复制数据。
支持任何无连接 UDP 应用	从多个路由器发送的 tFlow 记录可以复制到多个 Netflow 收集器。这种灵活性不需要在 Netflow 导出设备配置中设置许多 Netflow 目标规范。从多个路由器和交换机发送的 sFlow 样本可以复制到多个 sFlow 收集器上。至于 Netflow 示例，这种用法不需要在 sFlow 导出设备配置中设置多个 sFlow 目标规范。系统日志消息可以自动复制到多个系统日志收集器中。来自路由器、交换机和其他网络设备的 SNMP 陷阱可以自动收集并分布到多个 SNMP 管理站。
可将 UDP 数据从任意来源定向到任意目标	从任何无连接 UDP 应用接收数据，然后重新将数据传输到多个目标，还可以根据需要复制数据。
不需要重新配置基础设施	将点日志数据（Netflow、sFlow、系统日志、SNMP）定向到单一目标，添加或删除新工具时，无需重新配置基础设施。
提供详细的流统计	使用详细的流统计功能，帮助组织估算其环境中的每秒流数 (fps)，确定其监控要求。
缩短网络基础设施的配置时间	简化网络安全与监控。
减少带宽	减少网络日志数据重复，降低 WAN 带宽使用量。
减少服务中断	减少意外停机和服務中断。

表 9. UDP Director 规格

	UDP Director 1010	UDP Director 2010
数据包复制速率（输入）**	25,000 pps	37,500 pps
数据包复制速率（输出）**	50,000 pps	75,000 pps
网络	<ul style="list-style-type: none"> • 1 个管理端口：10/100/1000BASE-TX，铜端口 • 1 个监控或侦听端口 • 集成的 HTTPS web UI：对命令行接口 (CLI) 进行串行和 KVM 访问 	<ul style="list-style-type: none"> • 1 个管理端口：10/100/1000BASE-TX，铜端口 • 3 个监控或侦听端口 • 可选：2 个附加 Gbps 光纤信号端口 NIC
存储	160 GB，非冗余	300 GB，RAID 6，冗余
硬件平台	R220	R630
硬件世代	第 12 代	第 13 代
机架单元（可安装）	1RU	
电源	单一电源 (250W)	<ul style="list-style-type: none"> • 冗余 750W 交流电源，50/60 Hz • 自动设置范围（100V 到 240V）
散热量	1039 Btu/小时（最高）	2891 Btu/小时（最高）
操作系统	经过强化的 Linux	
尺寸	高度： 4.24 厘米（1.67 英寸） 宽度： 43.4 厘米（17.09 英寸） 深度： 39.37 厘米（15.5 英寸）	高度： 4.3 厘米（1.68 英寸） 宽度： 48.24 厘米（18.99 英寸），含机架栓锁；43.4 厘米（17.08 英寸），不含机架栓锁 深度： 74.3 厘米（29.25 英寸），含电源和嵌槽；69.2 厘米（27.25 英寸），不含电源和嵌槽
单位重量	15 千克（34 磅）	29.5 千克（65 磅）
导轨	带 Versa 导轨的机架底盘，带圆孔，可安装第三方机架	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	

ProxyWatch

Lancope 的 ProxyWatch 组件可以为安全分析师提供更多的网络可视性和威胁检测功能。它从代理的另一端获取关于对话的附加情景，帮助分析师在处理安全威胁时制定更明智的决策。

ProxyWatch 功能支持以下 Web 代理：

- Blue Coat
- McAfee
- Squid
- 思科

表 10 列出了各种 ProxyWatch 型号。

表 10. ProxyWatch 订购信息

部件号	说明
PX-100-U	代理记录的收集、关联和分析许可最多可供 100 个用户使用
PX-1000-U	代理记录的收集、关联和分析许可最多可供 1000 个用户使用
PX-10000-U	代理记录的收集、关联和分析许可最多可供 10,000 个用户使用
PX-25K-U	代理记录的收集、关联和分析许可最多可供 25,000 个用户使用
PX-50K-U	代理记录的收集、关联和分析许可最多可供 50,000 个用户使用
PX-100K-U	代理记录的收集、关联和分析许可最多可供 100,000 个用户使用

StealthWatch 流许可

在 StealthWatch Management Console 上汇聚流需要流许可。流许可还定义可被收集的流数量。许可可以任意组合，以实现所需级别的流容量。可用的许可功能包括：

- 1,000 个流
- 10,000 个流
- 25,000 个流
- 50,000 个流
- 100,000 个流

订购信息

StealthWatch 系统订购指南可帮助您了解系统的型号、组件和许可类型。

若要下单，请联系您的客户代表。

服务与支持

有许多服务计划适用于 StealthWatch。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。

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、并优化投资和投资回报率。借助 Cisco 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。Cisco Capital 可以为您提供一种可预测的支付方式。Cisco Capital 目前已在 100 多个国家/地区推出融资服务。[了解详情](#)。

更多详情

请访问 Lancope.com 或通过 info@lancope.com 联系销售人员。

有关 StealthWatch 系统的更多信息，请访问 <http://lancope.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。

 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)