

# 思科 Stealthwatch 系统

思科 Stealthwatch™ 系统可提供业界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准确性。

思科 StealthWatch 能够提供扩展的可视性，帮助您更好地洞察网络中正在发生的活动。您可以将这种可视性扩展到云、整个网络、分支机构、数据中心，并深入到终端。

思科 Stealthwatch 系统的核心是流量收集器、流量传感器和管理控制台。可针对额外功能提供额外许可证。请查看这些许可证的单个数据手册，以了解更多详细信息。

- 思科 Stealthwatch 云许可证：将可视性扩展到公共云、私有云和混合云环境
- 思科 Stealthwatch 终端许可证：将可视性扩展到终端
- [思科 Stealthwatch 学习型网络许可证](#)：使用思科® 集成服务路由器 (ISR)，将可视性扩展到分支机构
- 思科 StealthWatch 代理许可证：将可视性扩展到代理服务器

## 优势

Stealthwatch 可通过独特的网络流量视图和分析，帮助您在以下方面获得显著改善：

- 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

## 系统架构

### 管理控制台

管理控制台管理、协调及配置部署在整个企业重要网段的思科 Stealthwatch 设备。

控制台的容量决定了可分析和展示的 Netflow 数据量，以及可部署的流量收集器数量。控制台可通过硬件设备或虚拟机两种形式提供。表 1、2 和 3 分别列出了控制台的优势、型号和规格。

表 1. 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、精确查找网络滥用行为和性能欠佳之处，以及管理整个企业的事件响应。
管理设备	配置、协调和管理各种思科 Stealthwatch 设备，包括流量收集器、流量传感器和 UDP Director
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。成果：基于行为的有效网络保护。
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）。
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。
灵活的交付选项	您可以订购设备版本，它是一种适用于任何组织规模的可扩展设备；或者，您可以订购虚拟版本，其功能与设备版本相同，但是在 Vmware 环境中运行。

表 2. 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
Stealthwatch 管理控制台虚拟设备	最多 5 台	1 TB
Stealthwatch 管理控制台 1000	5	1 TB
Stealthwatch 管理控制台 2000	25	2 TB

表 3. 管理控制台规格（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	41 磅（18.6 千克）	
导轨	可滑行导轨，带线缆管理臂	
法规	FCC（仅限美国），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	

注意： 这些规格适用于思科 StealthWatch 6.9。

## 流量收集器

流量收集器可在整个物理和虚拟环境中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。表 4 和表 5 分别列出流量收集器的优势和规格。

表 4. 流量收集器的主要优势

优势	说明
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)。
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。
长期数据保留	允许组织和机构长期保留大量的数据。
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。
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. 流量收集器规格（按型号）

	FC 1010	FC 2010	FC 4010	FC 5020
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，构建于思科 UCS® 平台之上，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
硬件平台	R630	R630	R630	<ul style="list-style-type: none"> <li>引擎：UCSC-C220-M4S</li> <li>数据库节点：UCSC-C240-M4S2</li> </ul>
网络	1 个管理端口： 10/100/1000BASE-TX，铜端口 3 个监控或侦听端口			<ul style="list-style-type: none"> <li>1 个 1 Gbps 专用管理端口</li> <li>1 个 10000 SFP+ 上行链路端口到引擎/数据库节点</li> <li>2 个 Intel i350 GbE 以太网控制器端口（LAN1、LAN2）</li> </ul>
流存储	1 TB (RAID 6 冗余)	2 TB (RAID 6 冗余)	4 TB (RAID 6 冗余)	8 TB (RAID 10 冗余)
硬件世代	第 13 代			
机架单元（可安装）	1RU		双机架单元	
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"> <li>引擎：冗余 770W 电源 (1+1)</li> <li>数据库节点：冗余 1200W 电源 (1+1)</li> </ul>

	FC 1010	FC 2010	FC 4010	FC 5020	
<b>散热量</b>	2891 Btu/小时 (最高)			<b>引擎:</b> 最高每小时 2891 Btu <b>数据库节点:</b> 最高每小时 4100 Btu	
<b>尺寸</b>	<ul style="list-style-type: none"> <li>• <b>高度:</b> 4.3 厘米 (1.68 英寸)</li> <li>• <b>宽度:</b> 43.4 厘米 (17.08 英寸)</li> <li>• <b>深度:</b> 69.2 厘米 (27.25 英寸)</li> </ul>	<ul style="list-style-type: none"> <li>• <b>高度:</b> 4.3 厘米 (1.68 英寸)</li> <li>• <b>宽度:</b> 43.4 厘米 (17.08 英寸)</li> <li>• <b>深度:</b> 69.2 厘米 (27.25 英寸)</li> </ul>	<ul style="list-style-type: none"> <li>• <b>高度:</b> 8.7 厘米 (3.4 英寸)</li> <li>• <b>宽度:</b> 44.4 厘米 (17.5 英寸)</li> <li>• <b>深度:</b> 69.2 厘米 (27.25 英寸)</li> </ul>	<b>引擎</b> <ul style="list-style-type: none"> <li>• <b>高度:</b> 4.32 厘米 (1.7 英寸)</li> <li>• <b>宽度:</b> 43.0 厘米 (16.89 英寸)</li> <li>• <b>深度:</b> 75.6 厘米 (29.8 英寸)</li> </ul> <b>数据库节点</b> <ul style="list-style-type: none"> <li>• <b>高度:</b> 8.7 厘米 (3.43 英寸)</li> <li>• <b>宽度:</b> 44.8 厘米 (17.65 英寸)</li> <li>• <b>深度:</b> 73.8 厘米 (29.0 英寸)</li> </ul>	
<b>重量</b>	41 磅 (18.6 千克)		65 磅 (29.5 千克)	<ul style="list-style-type: none"> <li>• <b>引擎:</b> 38 磅 (17.24 千克)</li> <li>• <b>数据库节点:</b> 65 磅 (29.48 千克)</li> </ul>	
<b>导轨</b>	可滑行导轨, 带线缆管理臂			可滑行机架导轨 (UCSC-RAILB-M4)	
<b>法规</b>	<ul style="list-style-type: none"> <li>• FCC (仅美国) A 类</li> <li>• DOC &amp; ICES (加拿大) A 类</li> <li>• CE 标记 (EN55022 A 类、EN55024、EN61000-3-2、EN 61000-3-3、EN60950)</li> <li>• VCCI A 类 UL 1950</li> <li>• CSA 950</li> </ul>			<ul style="list-style-type: none"> <li>• 根据 2004/108/EC 和 2006/95/EC 指令, 产品应符合 CE 标记</li> <li>• UL 60950-1, 第二版</li> <li>• CAN/CSA-C22.2 No. 60950-1 第二版</li> <li>• EN 60950-1 第二版</li> <li>• IEC 60950-1 第二版</li> <li>• AS/NZS 60950-1</li> <li>• GB4943 2001</li> </ul>	
<b>虚拟流量收集器</b>					
<b>L-LC-FC-NF-VE-K9</b>	适用于 NetFlow 的流量收集器虚拟版本	30,000 <sup>*</sup>	1,000 <sup>*</sup>	1.0 TB	虚拟
<b>L-LC-FC-SF-VE-K9</b>	适用于 sFlow 的流量收集器虚拟版本	30,000 <sup>*</sup>	1,000 <sup>*</sup>	1.0 TB	虚拟
<b>L-LC-SW-VE-CONV-K9</b>	从物理设备转换为虚拟版本				

\* 每秒最大流数量可能根据网络条件不同有所变化。

**注意:** 这些规格适用于 StealthWatch 6.8.2。

## 流量传感器

流量传感器组件用于为不支持 Netflow 的交换和路由基础设施分段生成 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。流量传感器能够为未启用思科基于网络的应用识别 (NBAR) 功能的环境提供第 7 层应用信息。流量传感器可提供对网络和服务器性能指标的全面可视性。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 数据量由已部署的流量传感器的容量决定。可以安装多个流量传感器。流量传感器可通过硬件设备或虚拟机环境监控软件两种形式提供。表 6 和表 7 分别列出了流量传感器的主要优势和规格。

表 6. 流量传感器的主要优势

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. 流量传感器规格

	FS 1010	FS 2010	FS 3010	FS 4010
<b>通信</b>				
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)
<b>接口</b>				
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)			
<b>物理</b>				
硬件平台	R220	R630		
硬件世代	第 12 代	第 13 代		
外形规格			堆叠式	
尺寸	<b>高度：</b> 4.24 厘米 (1.67 英寸) <b>宽度：</b> 43.4 厘米 (17.09 英寸) <b>深度：</b> 39.37 厘米 (15.5 英寸)	<b>高度：</b> 4.3 厘米 (1.68 英寸) <b>宽度：</b> 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 <b>深度：</b> 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)		
<b>环境</b>				
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) 存储温度：-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 A 类/RoHS	FCC (仅限美国) 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)		

注意： 这些规格适用于思科 StealthWatch 6.9。

## 虚拟流量传感器

产品部件号	说明	最大网络流量	网络监控端口	外形规格
L-LC-FSVE-VMW-K9	适用于 VMware 的流量传感器虚拟设备	*	-	虚拟
L-LC-SW-VE-CONV-K9	从物理设备转换为虚拟版本			

\* 视虚拟机的资源而定。

## UDP Director

UDP Director 可简化整个企业内网络数据和安全数据的收集与分发过程。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 和表 9 分别列出了 UDP Director 的主要优势和规格。

表 8. 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目标。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。
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。

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"> <li>1 个管理端口: 10/100/1000BASE-TX, 铜端口</li> <li>1 个监控或侦听端口</li> <li>集成的 HTTPS web UI: 对命令行接口 (CLI) 进行串行和 KVM 访问</li> </ul>	<ul style="list-style-type: none"> <li>1 个管理端口: 10/100/1000BASE-TX, 铜端口</li> <li>3 个监控或侦听端口</li> <li>可选: 2 个附加 Gbps 光纤信号端口 NIC</li> </ul>
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"> <li>冗余 750W 交流电源, 50/60 Hz</li> <li>自动设置范围 (100V 到 240V)</li> </ul>
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	<b>高度:</b> 4.24 厘米 (1.67 英寸) <b>宽度:</b> 43.4 厘米 (17.09 英寸) <b>深度:</b> 39.37 厘米 (15.5 英寸)	<b>高度:</b> 4.3 厘米 (1.68 英寸) <b>宽度:</b> 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 <b>深度:</b> 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	34 磅 (15 千克)	65 磅 (29.5 千克)
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

	UDP Director 1010	UDP Director 2010
法规	FCC (仅限美国), 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	

## 虚拟版 UDP Director

产品部件号	说明	最大输入 (pps)	最大输出 (pps)	监控端口	外形规格
L-LC-UDP-VE-K9	UDP Director VE 许可证	15,000	30000	不适用	虚拟

\* 视虚拟机的资源而定。

## 流速许可证

在管理控制台上汇聚流需要流速许可证。流速许可证还将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。

## 订购信息

思科 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

思科 Stealthwatch 系统提供多种服务计划。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 <http://www.cisco.com/go/stealthwatch> 或发送电子邮件至 [Stealthwatch-interest@cisco.com](mailto: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](http://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](http://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)