Lancope®

FLOWCOLLECTOR

The StealthWatch System by Lancope is a leading solution for network visibility and security intelligence across physical and virtual environments. With the StealthWatch System, network operations and security teams can obtain actionable insight into who is using the network, what applications and services are in use, and how well they are performing.

This comprehensive insight dramatically improves security incident response, threat detection and forensics while increasing network availability and reducing enterprise risk. By bringing disparate IT teams together, the StealthWatch System also helps maximize resources and minimize costs.

Isolate Root Cause in Seconds for Improved Security Incident Response

At the heart of the StealthWatch System is the highly scalable StealthWatch FlowCollector, available as a physical or virtual appliance. The FlowCollector uses flow-based anomaly detection to zoom in on any unusual behavior and immediately sends an alarm with the contextual intelligence that allows personnel to take quick, decisive action to mitigate any issues. If the cause lies with a particular host, the StealthWatch System can even identify the user involved.

Operators can use the StealthWatch System's unique drilldown features to identify and isolate the root cause within seconds, enhancing operational efficiency, decreasing costs and dramatically reducing the time from problem onset to resolution. In addition, the FlowCollector can detect zero-day attacks, APTs, DDoS, insider threats and other issues that easily bypass network perimeter defenses, without having to rely on signatures.

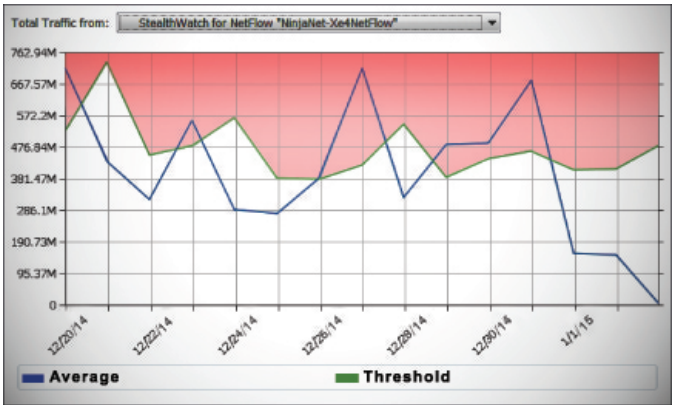
Key Benefits:

- Isolate root cause in seconds for improved security incident response
- Gain actionable insight into performance without expensive probes
- Scale as needed, when needed
- Leverage NetFlow and sFlow

Gain Actionable Insight into Performance without Expensive Probes

The FlowCollector looks deep into network traffic to gather and analyze flow data, including application and network performance metrics from across the enterprise. By taking information from existing infrastructure about all conversations occurring on the network, the FlowCollector provides the details necessary to resolve the majority of network issues without deploying costly and resource-intensive probes.

Complete, real-time visibility into all hosts and traffic on the network enables security and network operations teams to easily determine whether issues stem from the network itself or from specific applications. It also enables them to quickly pinpoint the root cause of issues down to the exact application and user, dramatically reducing Mean Time To Know (MTTK).



If suspicious behavior occurs, the StealthWatch FlowCollector sees it immediately and alerts the appropriate personnel.

Scale as Needed, When Needed

A FlowCollector exists for any organization to monitor and protect every part of the network that is IP-reachable, regardless of size. With unmatched scalability, a single FlowCollector can store and analyze data from as many as 4,000 flow sources at up to 240,000 flows per second (fps). When fully scaled, the StealthWatch System can process data from as many as 50,000 flow sources at up to 6 million fps. Easy upgrade paths enable an organization to start small and expand the system as capacity needs change over time.

> "...a **single** FlowCollector can store and analyze data from as many as **4,000 flow sources** at up to **240,000 flows per second.**"

The FlowCollector Virtual Edition (VE) is designed to perform the same function as the appliance editions, but in a virtual environment.

Leverage NetFlow and sFlow

Regardless of the data source, the StealthWatch System provides a cost-effective and highly scalable network monitoring and behavior analysis solution to optimize the end user experience, as well as existing network and security resources.

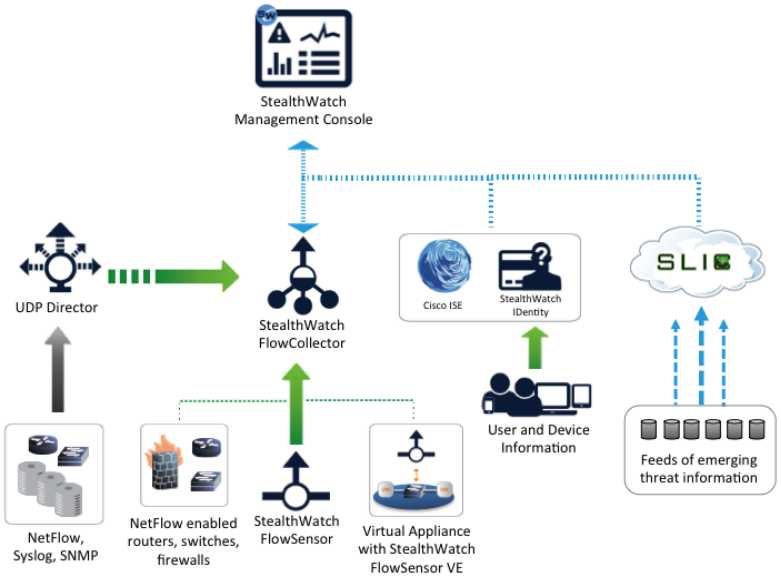
- **StealthWatch for NetFlow collector** gathers data from StealthWatch FlowSensors, as well as cFlow, J-Flow, Packeteer-2, NetStream, IPFIX, NSEL and NetFlow with NBAR.
- **StealthWatch for sFlow collector** gathers data from existing sFlow-enabled routers and switches from network infrastructure vendors such as Brocade, Extreme or HP ProCurve. Versions 2, 4, and 5 of sFlow are supported.

How It Works

As TCP/IP packets move through physical and virtual networks, flow-capable devices such as routers/switches and the StealthWatch FlowSensor produce records and statistics about those packets. These devices send this information to the FlowCollector as unidirectional flows, which the FlowCollector stitches together to create bidirectional conversations.

For each conversation, the FlowCollector tracks each router/interface through which the flow traveled, but maintains a single deduplicated count for bytes, packets, etc. Deduplication ensures that any flows that might have traversed more than one router are counted only once as a bidirectional conversation, while maintaining the statistics for each router/interface crossed.

In addition, the FlowCollector monitors, analyzes, separates, categorizes and stores information from each flow, creating a baseline of typical network activity. If unusual activity occurs, the FlowCollector immediately sends an alarm to the StealthWatch Management Console with the contextual information necessary for the appropriate IT personnel to isolate the root cause and take quick, decisive action. The FlowCollector can identify and alert on known or unknown attacks, internal misuse or misconfigured network devices, regardless of packet encryption or fragmentation.



The StealthWatch FlowCollector collects and analyzes data from various flow sources to provide in-depth network visibility and security context.

StealthWatch FlowCollector Features Matrix

Features	Network	Security
Automatic baselining of all IP traffic	✓	✓
Automatic anomaly detection in traffic/host behavior	✓	✓
Layer 7 anomaly detection*	✓	✓
Massive scalability	✓	✓
Flexible deployment options, including virtual	✓	✓
NAT stitching	✓	✓
Peer-to-Peer (P2P) file sharing detection	✓	✓
Host and service profiling	✓	✓
Index-based prioritization technology	✓	✓
OS fingerprinting**	✓	✓
Support for application-aware flows such as NBAR2	✓	✓
Support for custom applications	✓	✓
Closest interface determination and tracking	✓	✓
Deduplication of flows	✓	✓
Virtual environment monitoring*	✓	✓
Host Group tracking and reporting	✓	✓
Unauthorized host access detection*	✓	✓
Unauthorized web server detection	✓	✓
Misconfigured firewalls detection*	✓	✓
Combined internal and external monitoring	✓	✓
Router interface tracking and reporting	✓	
Bandwidth accounting and reporting	✓	
Packet-level performance metrics*	✓	
QoS (DSCP) monitoring	✓	
Interface utilization alarming	✓	
Full flow logging		✓
Worm detection		✓
Botnet detection*		✓
DoS/DDoS detection (SYN, ICMP or UDP flood)		✓
Fragmentation attack detection**		✓
Network scanning and reconnaissance detection		✓
Large file transfer detection		✓
Rogue server detection		✓
Long term flow retention	✓	✓

**Limited functionality with sFlow **Limited functionality with NetFlow*

LEARN MORE. REQUEST A DEMO.

sales@lancope.com

StealthWatch FlowCollector Specifications

	FC 1010 *	FC 2010 *	FC 4010 *	FC 5000 *
Description	Provides redundant power, storage and extra interfaces for flow collection on multiple interfaces while providing enough horsepower for mid- to large-sized networks	Delivers full hardware redundancy and enough flow-processing horsepower for extremely large NetFlow, sFlow or IPFIX environments	Offers a massively scalable option to process very high volumes of flow data and features extensible storage capabilities	High capacity flow ingestion solution created for enterprise customers needing superior performance capabilities
Maximum Flows Per Second	Up to 30,000** fps	Up to 60,000** fps	Up to 120,000** fps	Up to 240,000** fps
Maximum Exporters	500	1,000	2,000	4,096
Network	Management Port: 1 – 10/100/1000 Copper Monitor/Listening Ports: 3			1 Management/Monitoring/Listening Port: 10/100/1000 1 Reserved Port: 10/100/1000 (Reserved for future use) 1 Database Node Connection Port: 10G 1 Reserved Port: 10G (Reserved for future use)
Flow Storage	1 TB (RAID-6 Redundant)	2 TB (RAID-6 Redundant)	4 TB (RAID-6 Redundant)	6 TB (RAID-10 Redundant)
Hardware Platform	R630			Engine: R620 Database Node: R820
Hardware Generation	13G			12G
Rack Units (Mountable)	1U	1U	2U	1U – Engine 2U – Database Node
Power	Redundant 750W AC 50/60 Hz Auto Ranging (100V to 240V)			R820 - Dual, Hot-plug, Non-Redundant Power Supply (2+0), 1100W R620 - Dual, Hot-plug, Redundant Power Supply (1+1), 750W
Heat Dissipation	2,891 BTU per hour maximum			R620 - 2,891 BTU per hour maximum R820 – 4,100 BTU per hour maximum
Dimensions	**Height:** 1.68 in. (4.3 cm) **Width:** 17.08 in. (43.4 cm) **Depth:** 27.25 in. (69.2 cm)	**Height:** 1.68 in. (4.3 cm) **Width:** 17.08 in. (43.4cm) **Depth:** 27.25 in. (69.2 cm)	**Height:** 3.4 in. (8.7 cm) **Width:** 17.5 in. (44.4 cm) **Depth:** 27.25 in. (69.2 cm)	R650- **Height:** 1.68 in. (4.3 cm) **Width:** 17.08 in. (43.4 cm) **Depth:** 27.25 in. (69.2 cm) R820- **Height:** 3.4 in. (8.7 cm) **Width:** 17.5 in. (44.4 cm) **Depth:** 29.2 in. (74.1 cm)
Weight	41 lb (18.6 kg)	41 lb (18.6 kg)	65lb (29.5 kg)	R620: 64 lb R820: 85 lb
Rails	Sliding Ready Rails with Cable Management Arm			
Regulatory	• FCC (U.S. only) Class A • DOC & ICES (Canada) Class A • CE Mark (EN55022 Class A, EN55024, EN61000-3-2, EN 61000-3-3, EN60950) • VCCI Class A • UL 1950 • CSA 950 *Please email sales@lancope.com for a complete list.*			

**StealthWatch v6.7 specifications **The maximum fps can change depending on varying network conditions. Please contact a Lancope representative for details.*

FlowCollector VE Specifications

The StealthWatch FlowCollector Virtual Edition (VE) mirrors the performance of the physical appliance and supports both VMware and KVM virtual environments. Specifications are applicable to the FlowCollector VE 1000, 2000 and 4000. For the FlowCollector VE to operate effectively, be sure to allocate resources so that they are reserved for the FlowCollector VE and not shared with any other virtual machine.