



STEALTHWATCH® XE FLOWCOLLECTOR™

StealthWatch by Lancope® is the leading solution for flow-based security, network and application performance monitoring across physical and virtual environments. By leveraging NetFlow™, sFlow® and other flow data from existing routers and switches, StealthWatch provides in-depth, borderless network visibility.

With StealthWatch, 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.

StealthWatch delivers unified visibility across the network by removing borders between the various IT teams, thereby enhancing cooperation and efficiency. Bringing these disparate teams together, StealthWatch helps maximize resources and minimize costs to better manage application performance, network operations and security.

Gain Actionable Insight into Performance without Expensive Probes

At the heart of the StealthWatch System is the highly scalable StealthWatch Xe FlowCollector.

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 information 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 provides valuable insight into network anomalies. This visibility enables security and network operations teams to easily determine whether issues stem from the network itself or from

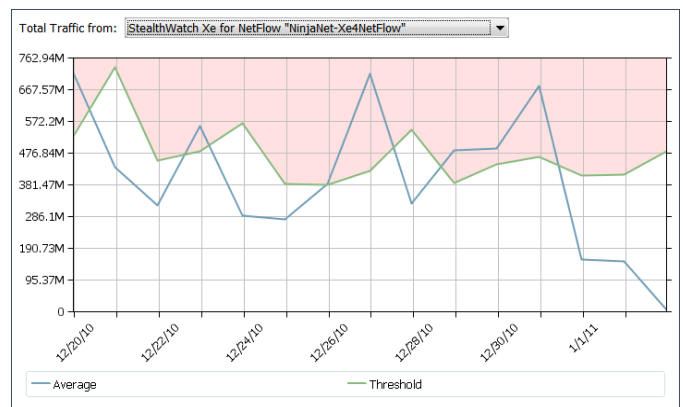


The StealthWatch Xe FlowCollector is the heart of the StealthWatch System by Lancope.

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).

Isolate Root Cause in Seconds, Enhance Operational Efficiency, Decrease Costs

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 damage. If the cause lies with a particular host, StealthWatch can even identify the user involved. Operators can use StealthWatch's unique drill-down features to identify and isolate the root cause within seconds, thereby reducing MTTK, enhancing operational efficiency and decreasing costs.



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

In addition, zero-day attacks and other threats that easily bypass network perimeter defenses create unexpected network traffic. The FlowCollector detects these threats without relying on signatures and helps administrators resolve them quickly.

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 1,000 flow sources at up to 60,000 **flows per second**¹ (fps). When fully scaled, StealthWatch can process data from as many as 25,000 flow sources beyond 1,000,000 fps. Easy upgrade paths enable an organization to start small and expand the system as capacity needs change over time.

Leverage NetFlow and sFlow

Regardless of the data source, StealthWatch 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.

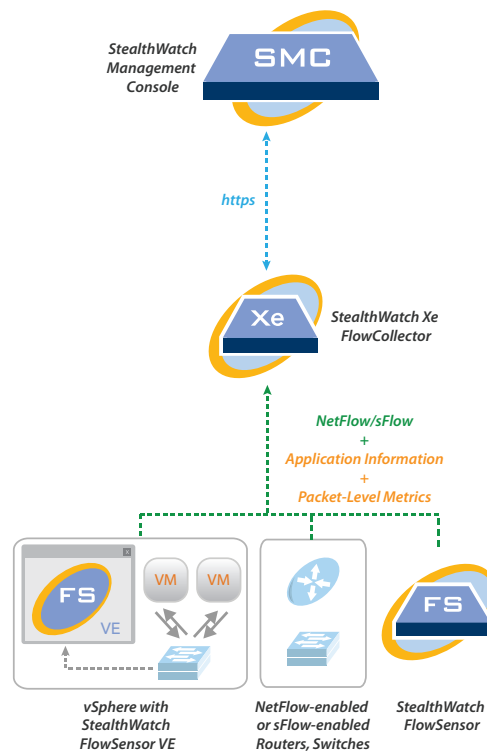
- ▶ **StealthWatch Xe for NetFlow collector** gathers data from StealthWatch FlowSensors², as well as cFlow, J-Flow, Packeteer-2, NetStream, IPFIX and NetFlow with NBAR.
- ▶ **StealthWatch Xe for sFlow collector** gathers data from existing sFlow-enabled routers and switches from network infrastructure vendors, such as Brocade, Extreme or HP ProCurve.

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 Console³ 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 Xe FlowCollector gathers data from various flow sources, analyzes it and creates a profile of normal network activity. Any behavior that falls outside of this profile generates an immediate alert.

¹ For more information, refer to the StealthWatch System Capacities & Sizing Guidelines.

² For more information, refer to the StealthWatch FlowSensor Data Sheet.

³ For more information, refer to the StealthWatch Management Console Data Sheet.

StealthWatch Xe FlowCollector Features Matrix

| Features | Network | Security |
|--|---------|----------|
| Automatic baselining of all IP traffic | ✓ | ✓ |
| Automatic anomaly detection in traffic/host behavior | ✓ | ✓ |
| Layer 7 anomaly detection* | ✓ | ✓ |
| Peer-to-Peer (P2P) file sharing detection | ✓ | ✓ |
| Host and service profiling | ✓ | ✓ |
| Index-based prioritization technology | ✓ | ✓ |
| OS fingerprinting** | ✓ | ✓ |
| Support application-aware flows such as NBAR* | ✓ | ✓ |
| Support for custom applications | ✓ | ✓ |
| Closest interface determination and tracking | ✓ | ✓ |
| Deduplication of flows | ✓ | ✓ |
| Virtual environment monitoring* | ✓ | ✓ |
| Host Group tracking and reporting | ✓ | ✓ |
| Router interface tracking and reporting | ✓ | |
| Bandwidth accounting and reporting | ✓ | |
| Packet-level performance metrics* | ✓ | |
| QoS (DSCP) monitoring | ✓ | |
| Interface utilization alarming | ✓ | |
| Unauthorized host access detection* | ✓ | ✓ |
| Unauthorized Web server detection | ✓ | ✓ |
| Misconfigured firewalls detection* | ✓ | ✓ |
| 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 | | ✓ |

*Limited functionality with sFlow
**Limited functionality with NetFlow

To learn more or request a demo, contact sales@lancope.com.

StealthWatch Xe FlowCollector Specifications

| | Xe 1000 | Xe 2000 |
|--------------------------|---|---|
| Maximum Flows Per Second | Up to 30,000* fps | Up to 60,000* fps |
| Maximum Exporters | 500 | 1,000 |
| Network | 1 – 10/100/1000 Copper | 3 – 10/100/1000 Copper (only one is active at a time) |
| Flow Storage | 1 TB (RAID-5 Redundant) | 2 TB (RAID-5 Redundant) |
| Rack Units (Mountable) | 1U | 2U |
| Power | Redundant 500W Auto Ranging (100V to ~240V) | Redundant 870W Auto Ranging (100V to ~240V) |
| Heat Dissipation | 1,706 BTU per hour maximum | 2,969 BTU per hour maximum |
| Dimensions | Height: 1.69 in. (4.3 cm) Width: 17.09 in. (43.4 cm) Depth: 24.69 in. (62.7 cm) | Height: 3.4 in. (8.64 cm) Width: 18.99 in. (48.24 cm) Depth: 28.4 in. (72.06 cm) |
| Weight | 35.02 lb (15.9 kg) | 57.54 lb (26.1 kg) |
| Rails | Sliding Ready Rails with Cable Management Arm | |
| Temperature | Operating: 50°F to 95°F (10°C to 35°C) with a maximum gradation of 50°F (10°C) per hour Note: For altitudes above 2,950 feet, the maximum operating temperature is derated 1°F per 550 feet. Storage: -40°F to 149°F (-40°C to 65°C) with a maximum gradation of 68°F (20°C) per hour | |
| Humidity | Operating Relative: 20% to 80% non-condensing with a maximum gradation of 10% per hour Storage Relative: 5% to 95% non-condensing | |
| Vibration | Operating Maximum: 0.26 Grms at 5-500 Hz for 15 minutes Storage Maximum: 1.54 Grms at 10-250 Hz for 15 minutes | Operating Maximum: 0.26 Gms at 5-350 Hz for 5 minutes Storage Maximum: 1.54 Gms at 10-250 Hz for 10 minutes |
| Shock | Operating Maximum: One shock pulse in the positive Z axis (one pulse on each side of the system) of 31G for 2.6 ms in the operational orientation Storage Maximum: Six consecutively executed shock pulses in the positive and negative X, Y and Z axes (one pulse on each side of the system) of 71G for up to 2 ms | Operating Maximum: Half sine shock in all operational orientations of 31G plus or minus 5% with a pulse duration of 2.6 ms plus or minus 10% Storage Maximum: Half sine shock on all six sides of 71G plus or minus 5% with a pulse duration of 2 ms plus or minus 10%; square wave shock on all six sides of 27G with a velocity change at 235 inches per second or greater |
| Altitude | Operating: -50 feet to 10,000 feet (-16 m to 3,048 m) Storage: -50 feet to 35,000 feet (-16 m to 10,600 m) | |
| Regulatory | <ul style="list-style-type: none"> ▶ FCC (U.S. only) Class A ▶ DOC (Canada) Class A ▶ CE Mark (EN55022 Class A, EN55024, EN61000-3-2, EN 61000-3-3, EN60950) ▶ VCCI Class A ▶ UL 1950 ▶ CSA 950 ▶ EN 60950 <p>Please call for a complete list.</p> | |

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

About Lancope, Inc.

Lancope®, Inc. is a leading provider of flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. Enterprises rely on Lancope to make better network decisions, respond faster to network problem areas and avoid costly outages and downtime — at a fraction of the cost of conventional network monitoring solutions.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

U.S. Sales

+1.770.225.6500
888.419.1462

International Sales

+44 (0)560 344 8075

Website: www.lancope.com

E-mail: sales@lancope.com

©2011 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners.

DSV1301262011