



## REVOLUTIONIZE THE WAY YOU VIEW YOUR NETWORK

GAIN A UNIFIED VIEW OF SECURITY AND NETWORK OPERATIONS

Lancope®



# STEALTHWATCH™ BY LANCOPE®



Lancope expertly provides flow-based optimization solutions for security and network operations that maximize limited resources by:

**STREAMLINING** the optimization of security and network operations into one process

**REDUCING** the time and resources allocated to network security and network operations

**ELIMINATING** the cost and complexity associated with non-integrated point solutions

Lancope's StealthWatch System meets the needs of both security and network administrators with an integrated platform that leverages network intelligence for both parties. A comprehensive offering, StealthWatch unifies and optimizes network operations and behavior-based anomaly detection to ensure network performance and protect critical information assets.

The StealthWatch architecture delivers the six critical components necessary to streamline security operations and optimize network performance.

## CHANGING THE VIEW OF YOUR NETWORK

As today's IT environments continue to grow in both scope and complexity, security and networking increasingly overlap. The convergence of these previously separate worlds is both inevitable and demanding. Security and network managers face a significant challenge as they delicately balance open access to enable business with the need to protect information and maintain high availability of the network. Moreover, security and network administrators are being asked to do more with less.

To help these overburdened teams meet the ongoing challenges of security and network management, Lancope provides the StealthWatch System. A proven Network Behavior Analysis (NBA) and Response solution, StealthWatch is a single, unified system for security and network operations that provides detailed views of anomalies and network utilization for security analysts, network engineers and network planners.

## FLOW-BASED OPTIMIZATION OF SECURITY AND NETWORK OPERATIONS

StealthWatch is the first and only flow-based solution to combine powerful network performance monitoring with behavior-based anomaly detection to deliver total network visibility, ensuring network security, performance and availability. This flow-based approach enables cost-effective protection of hosts and networks without requiring probes, agents or continuous signature updates.

StealthWatch leverages existing network infrastructure investment by analyzing NetFlow™ and sFlow® inherent in Cisco®, Juniper®, Foundry®, Extreme® or HP® ProCurve network environments. As flows enter the StealthWatch System, flow collectors generate and track over 90 unique flow statistics to build a baseline of behavior exhibited by network hosts.

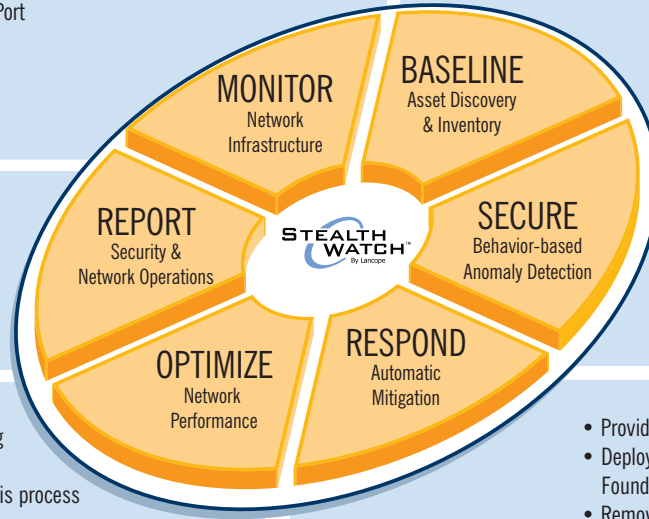
Applying a series of over 130 proprietary behavioral algorithms to the flow statistics, StealthWatch generates an index or "point system" for suspicious network activity called the Concern Index™. The patent-pending Concern Index prioritizes suspicious host behavior and allows for threshold-driven response and automated mitigation actions using existing routers, switches or firewalls to quarantine or remove hosts.

Lancope's innovative user identity tracking technology integrates user identity and system awareness into the StealthWatch System, tying flow data, alarms, alerts and host behaviors directly to the actual user responsible for the activity. User identity tracking overcomes troublesome environments such as DHCP and VPN address pools. At the click of a mouse, StealthWatch operators can quickly reveal both which user and which system is logged into a network node or view a given user's network activity.

- Flow data: NetFlow, sFlow, SPAN/Mirror Port
- All network communications
- Network infrastructure device status
- Track past and present host behavior, user identity and systems

- Network-centric reporting
- Security-centric reporting
- Role-based Point-of-View™ dashboard
- Continuous flow-based auditing
- Track user identity and system reporting
- SOAP-compliant API

- Root cause determination
- Capacity planning and traffic engineering
- Identify traffic bottlenecks and problems
- Closed-loop network security/ops analysis process
- Monitor dscp traffic



- Normal versus anomalous traffic
- Zone and host behavior
- Automatically establish thresholds and policies
- Change management

- Detect network faults, policy violations and zero-day threats
- Prioritize most significant problems with Concern Index™
- Identify rogue traffic, hosts and applications
- Collect and track user identities

- Provide automatic or manual mitigation using network infrastructure
- Deploy ACLs, OPSEC, Cisco PIX, Cisco Guard, ArcSight TRM, Foundry INM, TippingPoint Quarantine and Bradford Networks
- Remove/quarantine malicious hosts, systems and users

StealthWatch offers several unique benefits over non-integrated point solutions:

- **Easy-to-Deploy, Cost-Effective, Flow-Based Solution**

StealthWatch's architecture and deployment flexibility enables organizations to achieve the broadest internal enterprise coverage at the lowest possible cost. In addition to consuming NetFlow and sFlow data, StealthWatch further leverages the existing network infrastructure for mitigation action rather than introducing an "in-line" security device for blocking commands.

- **Highly Scalable Enterprise Deployment**

StealthWatch network appliances can be centrally managed enterprise-wide through the StealthWatch Management Console.

- **Point-Of-View™ Technology**

StealthWatch's advanced Point-Of-View UI technology uniquely extends the value of the StealthWatch network and security operational intelligence to all groups within IT. This role-based technology enables customized views, delegated operation and reporting of security, traffic accounting, interface utilization and host or user behavior. These customized views cater to the specific operational needs of IT personnel from a central, real-time database of security and network operational information.



# OPTIMIZING NETWORK OPERATIONS

STEALTH

NETWORK

## USER & APPLICATION MONITORING

- Gain end-to-end network visibility
- Continuous network performance monitoring
- Tie user identity to network activity and systems affected
- Identify rogue devices and applications
- Monitor host behavior and communications among all network infrastructure devices

## TRAFFIC ACCOUNTING & ENGINEERING

- Leverage network infrastructure by analyzing NetFlow, sFlow or SPAN/Mirror Port flow data
- Analyze normal versus anomalous traffic
- Effective risk management
- Identify rogue traffic/hosts, bandwidth hogs
- Facilitate interdepartmental billing

## NETWORK PLANNING

- Network performance analysis
- Facilitate capacity planning and traffic engineering
- Streamline network planning process
- Audit change management process
- Enable historical and trend analysis
- Monitor dscp traffic

Today's network administrators face many challenges. With limited, minimally integrated views of network usage, performance and host integrity, network incidents are difficult to diagnose and the source or root cause determination can significantly delay response time. Lack of insight from both security and network operations and the resulting conflict between them only exacerbate this problem. In addition, the absence of a single operational system of network intelligence means there is no historical data to indicate trends or to facilitate network performance, capacity planning and resource management.

StealthWatch meets one of the most important requirements for assuring network availability and integrity – it presents a combined security and network operations optimization solution that is flexible enough to provide visibility within a complex network while uncovering network issues before they wreak havoc. StealthWatch enables overburdened network administrators to:

- Minimize the time, complexity and cost of network operations
- Increase overall network efficiency
- Effectively manage the enterprise network across platforms
- Maximize IT investments

# STREAMLINING SECURITY OPERATIONS

WATCH™

## SECURITY

### SECURITY ANALYSIS

- Detect policy violations, zero-day threats
- Concern Index™ identifies and prioritizes most significant problems
- Tie user identity to network activity
- Identify internal and external threats
- Pinpoint root cause and affected users, systems and hosts

### DOS/THREAT REMEDIATION

- Automatic or manual mitigation using network infrastructure (ACLs, OPSEC, Cisco PIX, Cisco Guard, ArcSight Threat Response Management, Foundry INM, TippingPoint Quarantine, Bradford Networks)
- Remove/quarantine malicious hosts
- Pinpoint root cause and affected hosts
- Streamline remediation process
- Facilitate forensic analysis

### POLICY ENFORCEMENT

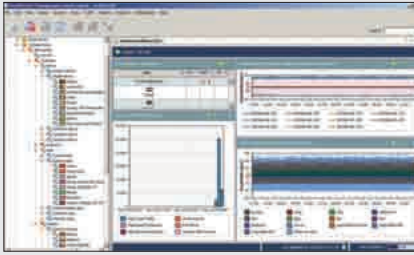
- Discover unauthorized applications
- Prevent network misuse by internal users
- Detect peer-to-peer (P2P) activity
- Remove/quarantine malicious hosts and users
- Establish thresholds, policies and detect any deviations thereof
- Identify users, rogue devices and applications that violate policy
- Ensure regulatory compliance

Organizations have found that network perimeter defenses, including firewalls, antivirus and intrusion detection/prevention systems (IDS/IPS), are inadequate for defending internal networks. Compounding this failure is the combination of growing insider threats and inability to track and audit network behavior and access by user.

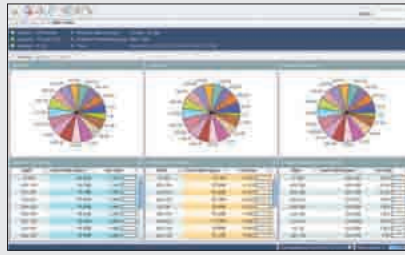
Unlike traditional perimeter-based security technologies, Lancope's StealthWatch NBA and Response solution represents a far simpler, less expensive and more effective means of protecting internal networks against attack or misuse. In addition, StealthWatch streamlines enterprise network security by providing an integrated view for optimizing security and network operations.

With its flow-based architecture, StealthWatch provides security and network managers with the continuous visibility and intelligence about the behavior of workstations, servers and network devices to more efficiently monitor and enhance the security and operations of their network.

# MEETING THE NEEDS OF SECURITY TEAMS AND NETWORK ADMINISTRATORS



Advanced User Interface



Network Traffic Analysis



Worm Outbreak Visualization

Security and network teams must continually meet IT demand, optimize efficiency, simplify management – and accomplish it all quickly and cost-effectively. StealthWatch offers a single solution that integrates seamlessly with the network, provides each operator with exactly the information he/she requires and offers the unique ability to easily track issues by individual user and/or system.

StealthWatch continuously monitors network behavior, detects anomalies and isolates known and unknown threats. Expanding beyond the capabilities of traditional network security products, StealthWatch collects, categorizes and analyzes network traffic to create comprehensive intelligence at both network and host levels. Providing a cost-effective, single point of reference for optimizing security and network operations, StealthWatch enables organizations to improve the security and health of their networks.

There are several key features which distinguish the StealthWatch solution from competitors.

## • Integrated Solution

The StealthWatch NBA and Response solution is the first flow-based, unified security and network monitoring system. By leveraging NetFlow and sFlow, StealthWatch provides deep network performance monitoring capabilities that empower the network operations team with network intelligence for effective capacity planning, performance monitoring and traffic analysis.

This is in addition to the proven security functionality which has made Lancope's StealthWatch product the acknowledged leader in network behavior-based systems. StealthWatch defends internal networks against zero-day attacks, internal misuse and unnecessary network exposures.

## • Personalized Dashboard

Advanced Point-Of-View UI technology gives each StealthWatch operator a personalized dashboard view with actionable information based on his/her role within the IT organization.

When network engineers log into StealthWatch, they immediately access traffic trending reports, top talker lists, router interface utilization information and other relevant network operations focused information. Similarly, security operations personnel receive information related to worm activity, covert communication channels, policy violations and security-related issues. Other IT groups (e.g. helpdesk, server administrators) also have customized Point-Of-View dashboards that provide unique views of the network, which are specifically catered to their unique operational and reporting needs.

## • Identity Tracking

StealthWatch IDentity-1000™ automates the process of identifying the activities of individual users, providing the ability to identify specific network events with actual user logins and systems. This allows administrators to significantly improve audit controls and assure regulatory compliance by linking the event directly to an individual user. Quarantine and remediation efforts are streamlined by the immediate identification of the responsible party.

Administrators simply request the user name(s), MAC address(es) and/or IP address(es) associated with an event from the StealthWatch Management Console, and the system returns the appropriate information in real time. Because multiple administrators can access this data simultaneously, the StealthWatch IDentity-1000 is an essential component for optimizing both security and network operations across the enterprise.

# LANCOPE, THE LEADER IN NETWORK BEHAVIOR ANALYSIS

Lancope created StealthWatch, the most widely used Network Behavior Analysis (NBA) and Response solution, which unifies and optimizes behavior-based anomaly detection and network operations to protect critical information assets and ensure network performance by preventing costly downtime, repair and loss of reputation. StealthWatch streamlines network operations and security into one process, reduces time and resources, and eliminates the costs and complexity associated with non-integrated point products.

Both OPSEC and Common Criteria-certified, StealthWatch received the 2008 and 2007 Product Excellence Awards in Network Behavior Analysis and was named Best of Show at Interop2006.

Defending the networks of Global 2000 organizations, academic institutions and government entities, StealthWatch protects hundreds of enterprise customers worldwide, more than all direct competitors combined.

## THE STEALTHWATCH FAMILY

**StealthWatch Management Console** manages, coordinates and configures all StealthWatch appliances to correlate security and network intelligence across the enterprise. This ability to deliver real-time insight into current network behavior increases security and network team efficiency and decreases operating costs, while simultaneously improving overall security and operational awareness.

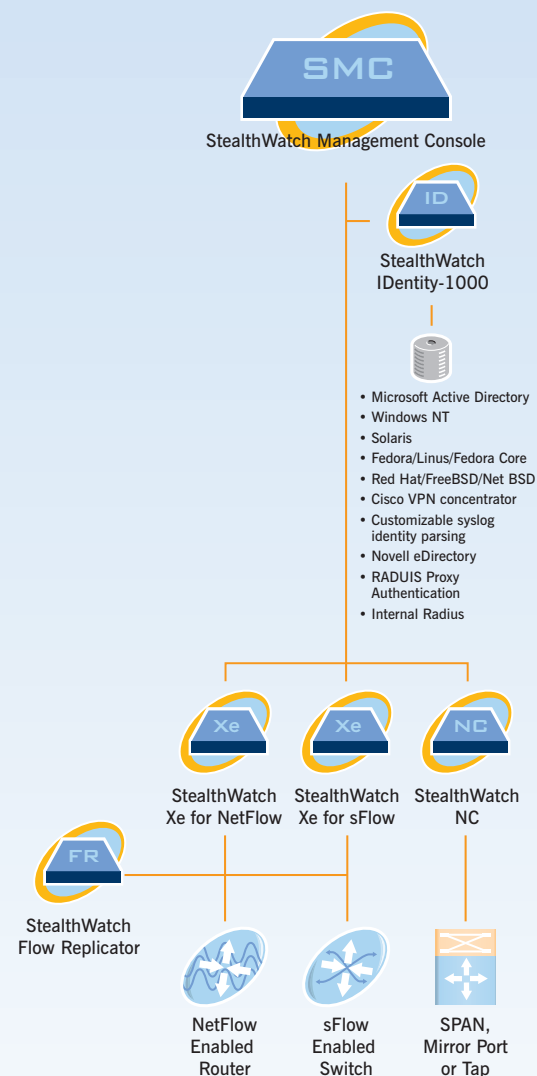
**StealthWatch IDentity-1000** automates user and system identification, streamlines remediation efforts and delivers powerful auditing capabilities for regulatory compliance. Its agent-less approach enables scalable, cost-effective user tracking and reporting for optimizing security and network operations.

**StealthWatch NC** defeats threats from external and internal sources, regardless of known or unknown targeted vulnerability. With native flow capture to provide more detailed coverage and greater packet inspection for sensitive areas of the network, StealthWatch NC prioritizes risks and helps ensure compliance with security and network usage policies. It also captures and summarizes transaction records for all network communications to enable powerful forensic analysis and expedite incident investigation and remediation efforts.

**StealthWatch Xe for NetFlow** leverages Cisco NetFlow traffic accounting technology to cost-effectively extend network protection and traffic analysis across geographically dispersed or multi-gig enterprise networks. StealthWatch Xe for NetFlow gives operators broad, continuous awareness of activity across the enterprise network.

**StealthWatch Xe for sFlow** leverages traffic information from sFlow, natively available in routers and switches from Foundry, HP ProCurve and Extreme, to cost-effectively extend network protection and traffic analysis across geographically dispersed and/or multi-gig enterprise networks. StealthWatch Xe for sFlow gives operators broad, continuous awareness of activity across the enterprise network.

**StealthWatch Flow Replicator** improves enterprise network performance by aggregating NetFlow, sFlow, syslog and SNMP information in a single, high-speed appliance. This high-speed UDP packet replicator gathers essential network optimization and security information from multiple locations into the StealthWatch Flow Replicator, and then forwards this information in a single data stream to one or more StealthWatch collectors.





See how StealthWatch can help your organization **streamline** security and network operations, **reduce** time and resources, and **eliminate** cost and complexity of non-integrated solutions.

Call +1-770-225-6500 or visit [www.lancope.com](http://www.lancope.com).

## Lancope®

*Optimizing Security and Network Operations*

### CORPORATE HEADQUARTERS

#### LANCOPE

3650 Brookside Parkway  
Brookside Concourse 100, Suite 400  
Alpharetta, GA 30022  
770.225.6500  
[sales@lancope.com](mailto:sales@lancope.com)

[www.lancope.com](http://www.lancope.com)

©2008 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. StealthWatch is covered by U.S. Patent Nos. 7,290,283 and 7,185,368, and other U.S. and foreign patents pending.

DS12142007