



## STEALTHWATCH/ARCSIGHT INTEROPERABILITY DELIVERS INTELLIGENT INCIDENT RESPONSE™

StealthWatch® by Lancope® integrates with several ArcSight products, including Enterprise Security Manager (ESM) and Threat Response Management (TRM). Through this interoperability StealthWatch events are displayed within ESM, and StealthWatch can direct TRM to initiate blocking actions for any host on the network. This capability extends the value of existing routers, switches, firewalls and VPN concentrators by enabling them to participate in Intelligent Incident Response. Furthermore, because both Lancope and ArcSight products operate out of band, Intelligent Incident Response does not introduce additional inline devices into the corporate network.

### Intelligent Incident Response through Existing Network and Security Devices

StealthWatch extends the value of existing network infrastructure by converting flow data (e.g. NetFlow™, sFlow®) collected from routers and switches into actionable network intelligence. Further leveraging the network infrastructure, StealthWatch combines its rapid identification of malicious hosts with TRM's vendor-agnostic governance of existing routers, switches, firewalls and VPN concentrators to offer Intelligent Incident Response. The result is a far-reaching, sophisticated mitigation solution that is a cost-effective alternative to an enterprise-wide IPS deployment.

*"NBA eliminates the cost of having to put an IPS on every segment by directing remediation into the existing infrastructure (i.e., switches, routers and security devices) as a result of anomalies that have been detected, so IPSs can be deployed only in high-risk areas such as the perimeter, DMZ, business unit gateways and segments that house sensitive data"<sup>1</sup>*

Not only do Lancope and ArcSight solutions jointly provide an intelligent incident response solution, but they also demonstrate how effectively Network Behavior Analysis (NBA), Network Management and Security Information and Event Management (SIEM) complement one another.

### How Does It Work?

Through the StealthWatch Management Console (SMC), StealthWatch provides mitigation capabilities that are configured to either run automatically or with administrator authorization. Once StealthWatch detects excessive anomalous activity and raises an alarm configured for mitigation it then sends the alarm to TRM. In turn, TRM quickly determines the precise location of the problem host within the network (down to the specific switch port) and dynamically configures the appropriate network devices to completely disable the node's network access. TRM's sophisticated mitigation methodology explores various levels of mitigation and selects the appropriate action for the issue at hand.

Together, StealthWatch and TRM dramatically reduce the time required to effectively respond to cyber security incidents, preventing a minor incident from creating significant damage. This powerful interoperability increases staff productivity and morale through reduced incident clean-up costs and efforts. Moreover, because routers, switches, VPN concentrators and firewalls are widely deployed across the corporate network, Lancope and ArcSight, when combined, provide a broader, more pervasive mitigation solution than is otherwise possible with an IPS deployment.

### Other StealthWatch Benefits

**Operates Out of Band to Provide Enterprise-Wide Visibility** – StealthWatch provides Enterprise-wide visibility into host and network behaviors including graphical representation of traffic and attention focusing visual cues.

**Cost-Effective and Highly Scalable Solution** – StealthWatch provides a cost-effective alternative for both securing and understanding what you don't already know about your network.

**User Accountability** – StealthWatch promotes ever increasing levels of accountability by integrating with many common authentication stores to identify users, not just IP address.

<sup>1</sup> Yankee Group, "Internal Threat Protection with Net-Based Detection, Prevention and Behavioral Systems), January 10, 2006

## About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® for flow-based anomaly detection and network performance monitoring. Delivering unified visibility across physical and virtual networks, StealthWatch eliminates network blind spots and reduces total network and security management costs.

## Lancope Headquarters

3650 Brookside Parkway  
Suite 400  
Alpharetta, GA 30022

+1.770.225.6500 (US)  
888.419.1462 (Toll Free)  
+1.770.698.8827 (International)

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

**E-mail:** [sales@lancope.com](mailto:sales@lancope.com)

©2009 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; 7,185,368; 7,475,426; 7,512,980 and other U.S. and foreign patents pending.

ID11062009