



STEALTHWATCH / TIPPINGPOINT INTEROPERABILITY PROVIDES “SECOND CHANCE MITIGATION”

StealthWatch® by Lancope® recently announced a level of integration with 3Com’s TippingPoint Intrusion Prevention Systems (IPS) such that StealthWatch can now initiate quarantine (blocking) and unquarantine (unblocking) actions for a particular IP address on the network, thereby extending the value of TippingPoint IPSes already deployed in the network.

Second Chance Mitigation

In cases such as walk-in worms, misconfigurations, access policy violations, targeted attacks and bots, which may never be seen by perimeter-based IPS appliances, StealthWatch uniquely extends the value of the TippingPoint IPS by leveraging its quarantine capabilities to limit the impact of both malicious and accidental acts. For just such malicious or accidental acts, StealthWatch can now institute TippingPoint’s quarantine functionality to further contain undesirable behaviors. Read below what Gartner’s Paul Proctor has to say about the security value proposition Network Behavioral Analysis solutions, such as StealthWatch, provide for existing IPS solutions:

“Network behavior analysis (NBA) can fill the gap left by policy- and signature-based point solutions . . . they can help an organization catch an infection early and limit the impact. Now that many organizations have deployed firewall, IDS/IPS and SIEM technologies, they are now exploring what to do about the fact that they still have problems . . . This includes addressing the spread of worms and the exploitation of vulnerabilities, malicious (attacks) and accidental actions that raise the risk and lower the security posture of the organization.”¹

How Does It Work?

Through the StealthWatch Management Console (SMC), StealthWatch provides mitigation capabilities that can be enabled to run either automatically or under proper authorization only. Once StealthWatch raises an alarm configured for mitigation, it directs the TippingPoint Security Management System (SMS) to quarantine the IP address specified. All TippingPoint IPS appliances will be sure to drop all traffic originating from or destined for that specific IP address.

StealthWatch provides additional value by offering a configurable window of time within which the host remains under quarantine. After such window of time has elapsed, the host is then released from quarantine and granted access back into the network by the TippingPoint IPS appliances. This quarantine automation provided by the StealthWatch SMC results in reduced helpdesk costs and higher quality of service ensuring that users are not left stranded on an “IP island” for hours or even days at a time.

Other StealthWatch Benefits

Operates Out of Band to Provide Enterprise-Wide Visibility - Unlike IPS appliances that are deployed inline, StealthWatch provides Enterprise-wide visibility into host-based and network behaviors through flow collection and analysis. This approach ensures internal security without jeopardizing network availability.

Cost-Effective and Highly Scalable Solution - In contrast to a network wide deployment of IPSes which would be extremely costly, StealthWatch provides a cost-effective alternative for both securing and understanding what you don’t already know about your network. Yes, StealthWatch customers can protect their entire network with a minimum number of sensors.

User Accountability - And finally, since StealthWatch by Lancope integrates with many common authentication stores, it associates user identities with IP addresses to provide increasing levels of accountability.

¹ Gartner, “MarketScope for Network Behavioral Analysis, 2H06, 21 November 2006, ID Number: G00144385

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

E-mail: 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.

ID11192009