



CAN YOU SEE WHAT IS REALLY HAPPENING ON YOUR NETWORK?

Both Malicious and Accidental Actions Raise Business Risk

"Numerous sources indicate that 80% of all attacks come from external parties, yet there are also indications that 80% of all security-related losses are attributed to the remaining 20% of attacks – that is, those that are attributed to internal parties...For example, with Blaster, numerous META Group customers acknowledged that the worm did not penetrate their perimeter controls. Rather, their computing systems were thoroughly "taken down" after an otherwise mobile user visited a corporate office and connected an infected machine on to the local-area network."¹

Arguably the insider threat is growing and will continue to do so. Compounding this business risk are internal misuse as well as unnecessary network exposures, such as:

- worm propagation
- firewall misconfigurations
- unsecured site-to-site communications that bypass secured hubs
- peer-to-peer file sharing
- inappropriate server access
- unauthorized employee web server implementation over the network

These problems persist on all networks because of an inability to see what is actually happening on the network.

Ever-Changing Networks Compound the Problem

Further escalating business risk is the fact that networks are constantly changing, creating even more opportunities for internal misuse and abuse. Following are common network scenarios that frequently cloud a corporation's network visibility:

- MPLS rollouts
- Datacenter consolidations, server virtualization
- Mergers of once separate networks
- Bandwidth upgrades to core networks

Many organizations wrestle with the same questions:

How Can I...
see what is actually happening across my entire network?
move beyond a perimeter-based security strategy as perimeters are crumbling around me?
regain control of my network?
quickly identify compromised hosts and rapidly squelch the resulting infection?
promptly detect and troubleshoot network performance and availability issues?
monitor network usage by employee, customer, partner and consultant?
focus my limited resources on the most critical issues?

What Can You Do?

Ideally, you want "x-ray vision into the network" - a level of visibility that clearly reveals network and security issues as well as quickly troubleshoots and resolves them. StealthWatch™, the most widely used Network Behavior Analysis (NBA) solution, provides that Enterprise-wide visibility into host and network behaviors, adding a broader context around point-in-time security events. Hundreds of customers attest to StealthWatch's effectiveness in identifying compromised hosts and misconfigured devices, remediating network incidents and promoting network availability.

"Immediately upon deployment, StealthWatch uncovered 400 misbehaving hosts and helped reduce network threats by 90 percent. Email worms, which used to propagate quickly, are now immediately stopped with StealthWatch. New attacks, for which no signatures exist, now fail to gain a foothold unlike before."

Dartmouth College

¹ Meta Practice (since acquired by Gartner), 4 August 2004

About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® System, the most widely used network behavior analysis (NBA) solution combines 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.

MB11042009