



STEALTHWATCH HELPS DEMONSTRATE PCI COMPLIANCE

Executive Brief - How StealthWatch Helps Demonstrate PCI Compliance

StealthWatch, an easy to use, Network Behavior Analysis (NBA) solution for Enterprises, delivers the level of visibility, accountability and measurability into both individual host and broad network communications required for maintaining ongoing PCI compliance. Providing continuous network monitoring, StealthWatch helps demonstrate network-wide compliance for sections of PCI requirements* 1, 2, 8, 10, 11 and 12 by:

- supplying real-time visibility and awareness of network and host-based behaviors
- increasing accountability for introducing network security risks as well as jeopardizing network availability
- tracking, measuring and prioritizing network and host-based risk

Ensure Network Availability and Internal Security through Network Visibility and Patented Security Technology

Compliance calls for "visibility into the risk management controls, the business and the assets being protected."¹ StealthWatch supplies organizations with the means to:

- monitor and investigate individual host and broad network communications
- maintain network availability and performance so crucial to business process integrity
- passively discover and inventory the underlying assets of the corporate network

Provide User Accountability for Security and Network Risks through Network Visibility and Authentication Stores

Compliance also calls for increased levels of accountability within the Enterprise. This includes identifying users responsible for all malicious, suspicious and accidental actions. StealthWatch supplies organizations with the means to:

- tie individual users to internal network performance problems
- tie individual users to the introduction of security risks inside the internal network
- support the principles of segregation of duties and of least privilege

Supply Risk Measurement, Prioritization and Optional Mitigation through Network Visibility and Customizable Thresholds

Compliance also calls for measuring levels of risk or quantifying your risk exposure. StealthWatch supplies organizations with the means to:

- rapidly identify and prioritize the greatest sources of internal risk
- quickly respond to security incidents not addressed by perimeter defenses
- determine and enhance the effectiveness of traditional security controls currently in place

*Specifically how StealthWatch facilitates demonstrating compliance for sections of PCI requirements can be found on page two.

Detailed Brief - How StealthWatch Helps Demonstrate PCI Compliance

PCI Data Security Standard Requirements 1 and 2

StealthWatch facilitates demonstrating compliance for sections of PCI requirements 1 and 2 by:

- verifying that real-time network communications match the policies implied in the network diagram (1.1.2)
- monitoring and profiling all services and ports in use on the network
In this way, StealthWatch
 - confirms that ports and services are necessary for normal business
 - highlights those ports and services that may have been overlooked
 - profiles and optionally blocks unnecessary ports and services (1.1.5)
- verifying firewall policy configurations by quickly identifying traffic that's out of compliance (1.2)
- optionally mitigating violations to firewall configuration policy (1.2)
- facilitating network segmentation planning, simulation and monitoring efforts
In this way, StealthWatch
 - Provides valuable host and network communication patterns useful for network segmentation planning efforts.
 - Provides "zone locking" to simulate network segments without disrupting actual network communications
 - Provides continuous network monitoring to ensure accidental misconfigurations are identified and remediated
- providing a means for restricting inbound internet traffic to only those IPs within the DMZ (1.3.1)
- ensuring that unnecessary protocols aren't being consumed (2.2.2)

PCI Data Security Standard Requirements 8 and 10

StealthWatch facilitates demonstrating compliance for sections of PCI requirements 8 and 10 by:

- determining when accounts are active and what they did during this activity (8.5.6)
- auditing access to anything on the network and tying activity to an individual user, including administrative accounts (10.1)

StealthWatch takes these PCI requirements several steps further in the following ways:

- tying the offending IP address to the actual person using that IP, enabling much quicker resolution of both network and security issues
- supporting segregation of duties within the StealthWatch Management Console. StealthWatch provides different user interfaces and reports to different roles within the organization. This also supports the principle of least privilege in granting the minimum access necessary for a StealthWatch user to perform their job functions.

PCI Data Security Standard Requirements 11 and 12

StealthWatch facilitates demonstrating compliance for sections of PCI requirements 11 and 12 by:

- continuously but passively monitoring host behaviors looking for deviations from normal processes. StealthWatch not only identifies signs of zero-day compromise but also identifies anomalous network communications resulting from misconfigured files as well. (11.2)
- detecting compromised hosts based on how that host is behaving regardless of signature availability. When traditional IDS/IPS fails, StealthWatch fills the gap to detect zero day attacks that bypass perimeter defenses, including walk-in worms and internal misuse and abuse. (11.4)
- supplying both the insight and tools necessary to respond quickly to security incidents with surgical precision (12.9).

StealthWatch takes these PCI requirements a step further by building a prioritized risk profile of your organization's network and host behaviors ensuring that the greatest risks are responded to first.

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.

MB11182009