

## Overview

### Customer:

Fortune 2000 Enterprise Healthcare Information Clearinghouse

### Industry:

Healthcare

### Challenges:

- Extensive deployments of:
  - Firewall
  - IDS/IPS
  - SIM
- Continuous worms, zero-day attacks and employee misuse
- Unproven HIPAA compliance

## Lancope Products

- StealthWatch NC
- StealthWatch Xe for NetFlow
- StealthWatch Xe for sFlow
- StealthWatch Management Console



Continuous Real-time Management of Network Security Posture and Operations

## Enterprise Healthcare Prescribers StealthWatch to Match Auditory Requirement

### Challenge

One healthcare information clearinghouse suffered serious migraines trying to prove compliance with HIPAA regulations covering data security and patient privacy. Although major deployments of firewalls and intrusion detection/prevention systems (IDS/IPS) both inside and outside the network perimeter appeared to enforce the corporate security policy, they generated an overwhelming number of security events and alarms. The resulting avalanche of information made it almost impossible for security and network administrators to separate truly critical threats from the background noise generated by normal network usage. Despite security information management (SIM) systems which help identify areas for remediation, the sheer volume of events collected from multiple technologies (with only partially compatible reporting formats) meant that results were rarely available quickly enough to stop new attacks.

The clearinghouse recognized two challenges that its existing security strategy failed to address. First, its existing investment worked far more effectively at the network perimeter than on internal network segments. As a result, threats such as worms, zero-day attacks and employee misuse introduced from inside the perimeter put overall HIPAA compliance at risk. Second, administrators worried about potentially overlooking serious security exposures or responding too slowly to imminent attacks. They realized that the only means to ensure regulatory compliance was another layer of security that could identify and resolve critical threats to internal network resources far faster and more efficiently than possible with the current solution.

### Solution

Having invested significantly in its security infrastructure, the clearinghouse needed a solution that would allow existing appliances and applications work to more effectively, thereby enabling the staff to focus quickly on the most critical threats. Senior management also demanded rapid access to key security information in order to prove regulatory compliance. Not only must the solution help audit and verify the performance of security infrastructure according to the security policy, but it also needed to track these results over time.

The company realized an urgent need to:

- Quickly isolate critical security events, especially zero-day attacks, misapplied or misconfigured security policies or employee misuse overlooked by current infrastructure
- Stop worm and virus infestations before they could spread
- Provide faster reaction time to, and mitigation of, malicious network events
- Increase the value of existing security infrastructure by providing detailed analyses of events, faster access to forensic data and comprehensive audit capabilities over time
- Minimize man-hours per week of management time

*Lancope's StealthWatch solution was an obvious choice, with clear advantages over other vendor's offerings, including:*

- Automatic tuning that requires fewer staff resources to manage
- Mature, scalable products with comprehensive and responsive support
- Superior security data correlation capabilities that do not require large numbers of appliances to function
- Both security alerting and application change management at the network level
- Improved return on investment (ROI) for all firewall, IDS/IPS and SIM infrastructure



# Success Stories

## Results

The healthcare information clearinghouse chose Lancope's StealthWatch™ system to augment its existing security infrastructure and provide the advanced auditing capabilities demanded by HIPAA and other regulatory requirements. By using StealthWatch, the company was able to meet HIPAA standards far faster than with other vendor's offerings, while simultaneously earning over 300% ROI via improved network availability and more efficient risk and incident management processes.

StealthWatch's Network Behavior Analysis (NBA) and Response technology enables exceptionally rapid detection and prioritization for security incidents – whether known or not. Its flexible mitigation capabilities leverage existing network and security infrastructure to differentiate quickly and accurately between security crises and less critical network events.

---

*StealthWatch helps meet HIPAA regulations faster and earns over 300% ROI.*

---

Network and security operations managers now identify, prioritize and control unexpected host and network behavior far faster than was possible prior to the StealthWatch deployment. StealthWatch also recognizes new or unauthorized devices and applications immediately upon connection to the network. As such, worms, viruses and other internal threats can be isolated quickly before they can put sensitive data resources at risk.

The most important advantage the company receives is exceptional support for its ability to protect the privacy and confidentiality of sensitive client data. StealthWatch delivers real-time and historical access to any incident and its response, eliminating the company's reliance on manual audits of firewall and IDS/IPS log to determine impact – often weeks after the fact prior to StealthWatch's deployment.

Because StealthWatch concentrates on deviations from normal behavior, the number of incidents requiring urgent investigation has dropped to a small fraction from before. StealthWatch is also exceptionally easy to manage, since it self-tunes based on network traffic profiles and does not require attack signature updates to maintain its effectiveness. The StealthWatch prognosis is an obvious prescription for success: faster response to security events and easier proof of HIPAA compliance.

## About Lancope®

Lancope is the leading provider of network behavior analysis (NBA) and response solutions that defeat zero-day worms, internal network misuse and other anomalies that compromise network integrity. Lancope's StealthWatch System integrates security and network management technology to reduce network risks and maximize network availability by rapidly identifying, prioritizing and mitigating critical threats, whether new or well-known. Both OPSEC and Common Criteria-certified, StealthWatch was named an InfoWorld 2005 Technology of the Year. Defending the networks of Global 2000 organizations, academic institutions and government entities, StealthWatch protects over 200 enterprise customers, more than all direct competitors combined. Lancope's Technology Alliance Partners include Foundry Networks, ArcSight, IBM Tivoli, LURHQ and CheckPoint. Lancope is a privately held, venture-backed company headquartered in Atlanta, Georgia. For more information, call 888-419-1462 or visit [www.lancope.com](http://www.lancope.com).

## Contact Information

Lancope, Inc.  
3650 Brookside Parkway  
Suite 400  
Alpharetta, GA 30022

888.419.1462  
[sales@lancope.com](mailto:sales@lancope.com)  
[www.lancope.com](http://www.lancope.com)