

Overview

Customer:

Fortune 500 Enterprise

Industry:

Financial

Challenges:

- Global Network
- 50,000 Hosts
- 50 Locations
- 18,000+ Employees, Partners & Contractors
- Extensive Direct/VPN Connections to Partners & Contractors

Lancope Products

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



Continuous Real-time Management of Network Security Posture and Operations

Fortune 500 Financial Services Company Deploys StealthWatch To Improve Network Health & Security Posture Across The Enterprise

Challenge

Time is money when the networks of a global Fortune 500 financial services company are under attack. One such organization realized that it could not protect the internal networks without significantly slowing or disrupting normal business operations, despite an exceptionally well defended network perimeter.

The sheer volume of data generated by internal firewalls and intrusion detection/prevention (IDS/IPS) deployments rendered it virtually impossible for security staff to separate true crises from background noise. Furthermore, security information management (SIM) systems were incapable of post-processing such enormous amounts of data rapidly enough to ensure timely response and mitigation.

Administrators had tried but failed to distinguish serious security incidents from hundreds of thousands of less significant events. As a result, a dangerous gap existed between the onset of a critical security incident and attempts at successful resolution before corporate assets were compromised. More importantly, the timely reporting necessary to prove compliance with regulations, such as Gramm-Leach-Bliley or Sarbanes-Oxley, was all but impossible.

Both security and network operations managers needed a better solution to quickly identify and resolve critical threats to internal networks, hosts and applications. This new layer of defense must recognize threats overlooked by existing infrastructure, provide context for the risk inherent in each threat, then deliver workflow support to quickly isolate and mitigate critical issues demanding immediate response. Finally, the solution must provide rapid, system-wide aggregation and analysis of security performance to demonstrate compliance with industry and governmental regulations.

Solution

After an intensive search, the organization adopted Lancope's **StealthWatch**™ Network Behavior Analysis (NBA) and Response system to monitor network traffic on more than 50,000 hosts operating globally across 50 cities. These internal networks support over 18,000 employees, plus many direct and virtual private network (VPN) connections to business partners and contractors. The goal was simple – build a flexible, cost-effective solution that:

- Quickly isolates critical security events, especially internal misuse overlooked by firewalls, IDS/IPS and SIMs
- Stops worm infestations before they spread throughout internal networks
- Provides faster reaction time to, and mitigation of, malicious network events
- Increases the value of existing security infrastructure by providing detailed analyses of events and faster access to forensic data
- Requires less than 3 man-hours per week of management time

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

- *Rapid identification of previously hidden security risks, plus flexible, context-sensitive guidance to prevent recurrence of successful attacks*
- *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*
- *Security alerting and application change management at the network level*
- *Improved ROI for existing firewall, IDS/IPS and SIM infrastructure*

Results

The financial services company uses StealthWatch's NBA & Response approach to measure traffic patterns across networks and hosts in multiple data centers in the United States, England, Japan, Singapore and India, as well as critical WAN connections that link remote offices and partner connections to internal network resources. StealthWatch provides a high-level overview of current network behavior, which is benchmarked against expected behavior, in order to rapidly identify unauthorized or unexpected traffic patterns, such as zero-day worms.

The StealthWatch solution complements existing security infrastructure and improves its performance by bridging the gaps in coverage and response time left by firewall, IDS/IPS and SIM deployments. Rather than deploy costly appliances at every location around the world, StealthWatch leverages NetFlow traffic data, which is natively available in existing network infrastructure devices, to remotely gather information. The company's network and security teams now have the ability to quickly and easily identify internal misuse as well as hostile attacks – with significantly improved response and mitigation.

StealthWatch instantly prioritizes critical events, allowing security managers to filter non-critical security alerts and false positives, and then focus on immediately relevant threats.

With StealthWatch, security alerts requiring investigation have dropped from over 2,000,000 to only 20, and data analysis has been reduced from over 80 man-hours per month to just 3.

StealthWatch provides forensic information on all network traffic and requires minimal resources to isolate critical security events. This ability to help security administrators allocate staff and resources where they are most needed also helps the corporation prove compliance with government regulations, including Gramm-Leach-Bliley and Sarbanes-Oxley. StealthWatch's ability to measure security performance and response over time is a key asset in the corporation's ongoing efforts to prove security best practices.

Offering both NetFlow-compatible and native-capture appliances, the StealthWatch System is an extremely cost-effective solution that does not require signature updates. StealthWatch improves performance across all network security infrastructure by dramatically decreasing time spent analyzing logs and alerts, reducing the number of successful attacks and limiting the financial damage generated through downtime, theft and damage to critical online resources.

The corporation is now far more effective in its efforts to prioritize, preempt, isolate and resolve threats that originate inside the network. With less downtime and fewer hours and dollars associated with business interruption and loss, the corporation's customers, partners, vendors and employees are more productive. The security staff now can easily document the value of each dollar spent on protection against attacks or internal misuse.

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.

Contact Information

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

888.419.1462
sales@lancope.com
www.lancope.com