



SUCCESS STORY: FOUNDRY NETWORKS

Foundry Networks Deploys StealthWatch by Lancope Most Widely Used Network Behavior Analysis (NBA) Solution Transforms sFlow® Data into Actionable Intelligence to Improve Network Performance and Enhance Protection

Customer



FOUNDRY
NETWORKS

Industry

Enterprise Network Switching and Routing

Challenges

- Complex, global network
- 14 worldwide locations
- Extensive global VPN connections
- Identifying misconfigured devices manually using log files
- Only remedial tools available for tracking user activity

Benefits

- Cost-effective, scalable solution for optimizing security and network operations
- End-to-end network visibility of all host behaviors and network traffic
- Reduced the time spent on problem resolution by 80%
- Immediate identification, prioritization and remediation of network incidents
- Continuous audit controls for regulatory and policy compliance

Lancope Products

- StealthWatch Xe for sFlow
- StealthWatch IDentity-1000
- StealthWatch Management Console

Challenge

As a leading provider of high-performance enterprise and service provider switching, routing, security and application traffic management solutions, Foundry Networks recognizes the importance of collecting actionable network and security intelligence without taxing internal resources. Foundry serves 10,400 customers worldwide, including the world's premier ISPs, metro service providers, and enterprises in the healthcare, financial, manufacturing, entertainment and government space.

Foundry operates a large, complex network supporting 14 global locations with extensive VPN connections and an MPLS network extended to remote sites. In the past, Foundry had to manually examine vast amounts of log files to identify misconfigured devices. And with only remedial tools, Foundry's internal IT staff tried to determine which users were accessing particular systems, which never proved effective.

Foundry already possessed top-of-the-line networking expertise and equipment, but its IT resources were hampered with the arduous task of reviewing log files to find security and network performance problems. Its widespread, complex network only accentuated the need for increased network visibility and a more efficient, sophisticated approach to optimizing network operations and security. But Foundry was adamant that its resources should not be taxed by a new solution, and the company did not want to burden the network with more devices.

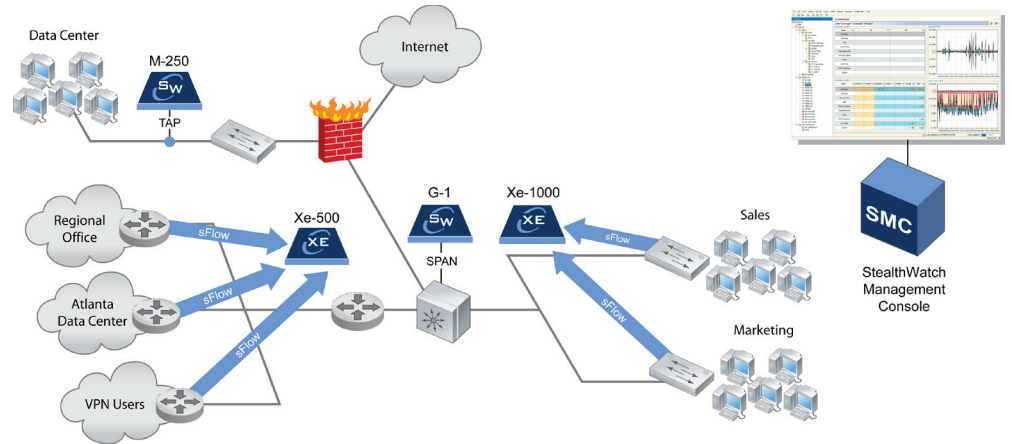
Solution

Foundry Networks has been a Lancope Technology Alliance Partner since 2005. Foundry knew that Lancope's StealthWatch™ System for network behavior analysis (NBA) and response provides end-to-end network visibility with detailed views of anomalies and network utilization for security analysts, network engineers and network planners. For Foundry, StealthWatch offered ideal capabilities, including:

- Streamlining network optimization and security into one process.
- Reducing the time and resources allocated to network optimization and network security.
- Eliminating the cost and complexity associated with non-integrated point solutions.

StealthWatch met all of Foundry's requirements with its ability to:

- Enhance Foundry's network visibility at the click of a mouse, with advanced user identity tracking that reveals the usernames and IP addresses associated with network events.
- Provide a consolidated snapshot of events and alerts with drill-down capability for Foundry's entire worldwide operations without having to invest and deploy numerous devices across multiple sites.
- Quickly identify misconfigured devices to find the point of origin for network slowdowns.
- Perform traffic analysis (peer-to-peer and peer-to-port), and provide greater detail, host snapshots and user information with a simple right click.
- Group devices logically by networks and locations.
- Efficiently monitor traffic on high-speed 10 Gbps core networks as well as 1 Gbps out to the desktop.
- Operate without requiring a dedicated IT resource to manage the StealthWatch System.



Since Foundry's routers and switches have sFlow® already embedded within, half the solution was already in place. All that remained was to implement StealthWatch in order to transform Foundry's sFlow data into actionable network intelligence. Leveraging the existing network infrastructure, StealthWatch collects and analyzes Foundry's sFlow traffic statistics to optimize network and security operations.

On the front end, StealthWatch appliances collect sFlow data exported from Foundry routers and switches. StealthWatch then normalizes, analyzes and converts the flow data into actionable network security intelligence which governs immediate blocking mechanisms instituted within the same Foundry routers and switches.

Ultimately, Foundry's solution includes StealthWatch Xe for sFlow collector appliances which aggregate high-speed network behavior data from multiple networks or network segments to extend protection across Foundry's geographically dispersed IT environment. The collector appliances are complemented by the StealthWatch IDentity-1000 (ID-1000) appliance, which directly links individual users with specific network events. Foundry's IT staff no longer needs remedial tools to try to match users with the network services they utilize and the periodic, unexpected events they may cause.

Both StealthWatch Xe for sFlow and the StealthWatch ID-1000 are centrally managed by the StealthWatch Management Console (SMC). The SMC manages, coordinates and configures StealthWatch appliances to correlate security and network intelligence from StealthWatch components deployed at critical segments throughout Foundry's network. With real-time insight into current network behavior, Foundry has been able to increase network and security team efficiency and decrease operating costs, while simultaneously improving overall security posture and operational awareness.

Results

StealthWatch extends the value of Foundry routers and switches by collecting exported sFlow data, then analyzing and converting the data into actionable intelligence for security and network operations. The Foundry team utilizes StealthWatch data to implement mitigation that blocks security threats and prevents bandwidth hogs from abusing the network. As part of a continuous, streamlined solution, StealthWatch initiates mitigation actions through the same routers and switches that originally exported the sFlow data.

With the StealthWatch solution, Foundry does not need to place probes at remote sites. StealthWatch makes distance irrelevant. Since Foundry switches essentially serve as sFlow “collectors” at remote sites, the data is simply reported back to the StealthWatch System where it is analyzed further. Foundry has also been able to reduce the time required for problem resolution—from four-to-five hours down to one hour. IT resources are now able to focus on other critical initiatives and the problem-solving they do conduct involves minimal manual effort.

StealthWatch has afforded Foundry with several security and compliance-related benefits as well. The advanced user identity tracking helps Foundry maintain its security policies by monitoring which users are dialing into particular servers and which users are making large data transfers. In addition, Foundry is now able to correlate network and security activity with the responsible

“NBA technologies are decision support systems that give visibility to a knowledgeable operator who can interpret, investigate and appropriately respond to a variety of suspicious activities on the network. Enterprise organizations will find tremendous value in the ability to access historical network data for capacity planning and trending purposes as well as view current network incidents, such as walk-in worms, unauthorized protocols and suspicious connections, which may impact performance.”

- Gartner, Inc.

“Foundry has also been able to reduce the time required for problem resolution—from four-to-five hours down to one hour.”

end user. The StealthWatch System enables Foundry to report on the specific users who have accessed a particular financial server or even a file, and when they gained access. The StealthWatch SMC also automatically sends Foundry a Concern Index that enumerates the greatest risks on Foundry’s network and helps pinpoint remediation efforts.

With the StealthWatch solution in place, Foundry has not experienced any performance degradation, even on its high-speed 10 Gbps internal network. Plus, the IT staff can more easily identify the source of network issues with the StealthWatch SMC interface. Previously, Foundry’s resources had to investigate issues manually.

Foundry Networks has only just begun to tap the advantages of a network behavior analysis system for optimizing network performance and simultaneously enhancing security. In the future, Foundry could utilize StealthWatch for greater visibility into security threats like viruses and worms. Foundry also sees value in accessing policy violations from the StealthWatch SMC, and may implement this capability at a later date.

StealthWatch’s advanced Point-Of-View™ UI technology is another untapped resource for Foundry Networks. Point-Of-View technology would extend the value of StealthWatch network and security operational intelligence to all groups within Foundry’s IT department. The role-based technology enables customized views, delegated operation and reporting of security, traffic accounting, interface utilization and host or user behavior. Having such customized views would cater to the specific operational needs of Foundry’s IT personnel from a central, real-time database of network and security information.

“Lancope’s StealthWatch combines behavior-based anomaly detection with traffic reporting and network optimization data. The resulting visibility enables network teams to efficiently manage complex networks without the need for additional hardware and software. StealthWatch can also detect zero-day, targeted, low-slow and unknown attacks which enhances network operations and security as well.”

- Yankee Group

With a number of capabilities still available from StealthWatch, Foundry could employ additional StealthWatch features to improve network capacity planning. In addition, Foundry will be implementing Closed Loop Remediation through interoperability with StealthWatch and Foundry’s IronView® Network Manager (INM). Through this integration, StealthWatch directs INM to initiate blocking and unblocking actions for a particular host on the network. Combine StealthWatch’s rapid response with surgical precision capability with INM’s governance of existing routers and switches results in a pervasive and precise mitigation solution.

About Foundry

Foundry Networks, Inc. (Nasdaq: FDRY) is a leading provider of high-performance enterprise and service provider switching, routing and Web traffic management solutions including Layer 2/3 LAN switches, Layer 3 Backbone switches, Layer 4–7 Web switches, wireless LAN and access points, access routers and Metro routers. Foundry’s 10,000 customers include the world’s premier ISPs, Metro service providers, and enterprises including e-commerce sites, universities, entertainment, health and wellness, government, financial, and manufacturing companies. For more information about the company and its products, call 1.888.TURBOLAN or visit www.foundrynetworks.com.

About Lancope

Lancope is the provider of the StealthWatch™ System, the most widely used network behavior analysis (NBA) and response solution that unifies behavior-based anomaly detection and network optimization capabilities to protect critical information assets and ensure network performance by preventing costly downtime, repair and loss of reputation. StealthWatch streamlines security and network operations into one process, reduces time and resources, and eliminates the costs and complexity associated with non-integrated point products. Both OPSEC and Common Criteria-certified, StealthWatch was named Best of Show at Interop2006. Defending the networks of Global 2000 organizations, academic institutions and government entities, StealthWatch protects hundreds of enterprise customers worldwide, more than all direct competitors combined. A contributing member of the Trusted Computing Group, Lancope also partners with fellow best-of-breed solution providers through its Technology Alliance Program, which includes Foundry Networks, IBM Tivoli, Check Point, TippingPoint, ArcSight and A10 Networks. Lancope is a privately held, venture-backed company headquartered in Atlanta, Georgia. For more information, call 888-419-1462 or visit www.lancope.com.

For more information, please contact 888.419.1462 (US), +1 770.225.6522 (International), or sales@lancope.com