Gigamon® Lancope®

Joint Solution Brief

Uncompromised NetFlow-based Security Visibility

The Challenge

With today's determined attackers, security experts agree that it's not a matter of if your perimeter defenses will be breached, but when. Network owners need complete visibility into what is happening on their network so they can detect "kill-chain" activities such as network reconnaissance, covert command and control communications and internal pivoting.

Integrated Solution

By leveraging flow data with sophisticated, behavioral analysis, Lancope's StealthWatch can help uncover attacks, pinpoint suspicious behavior and track the spread of any malware that does infect the network. The GigaSECURE® Security Delivery Platform enhances the efficacy of the StealthWatch solution through its ability to generate high fidelity NetFlow and IPFIX flow data without taxing the packet processors routing production traffic.

Joint Solution Benefits

- **Extended visibility into the network infrastructure** – Monitor traffic throughout the network from both physical and virtual network links.
- **Offload flow metadata production from existing network elements** – Allows for unsampled flow telemetry to be used from anywhere, even where flow data is not supported by the network element. Removes the need to settle for sampled data.
- **Identify anomalies from within the network** – Detect botnet communication to compromised hosts, combat APTs, detect DDoS attacks and track the spread of malware.
- **Can offload unnecessary traffic from being sent to the security tool** – Increasing efficacy and capacity with Application Session Filtering.

The Challenge

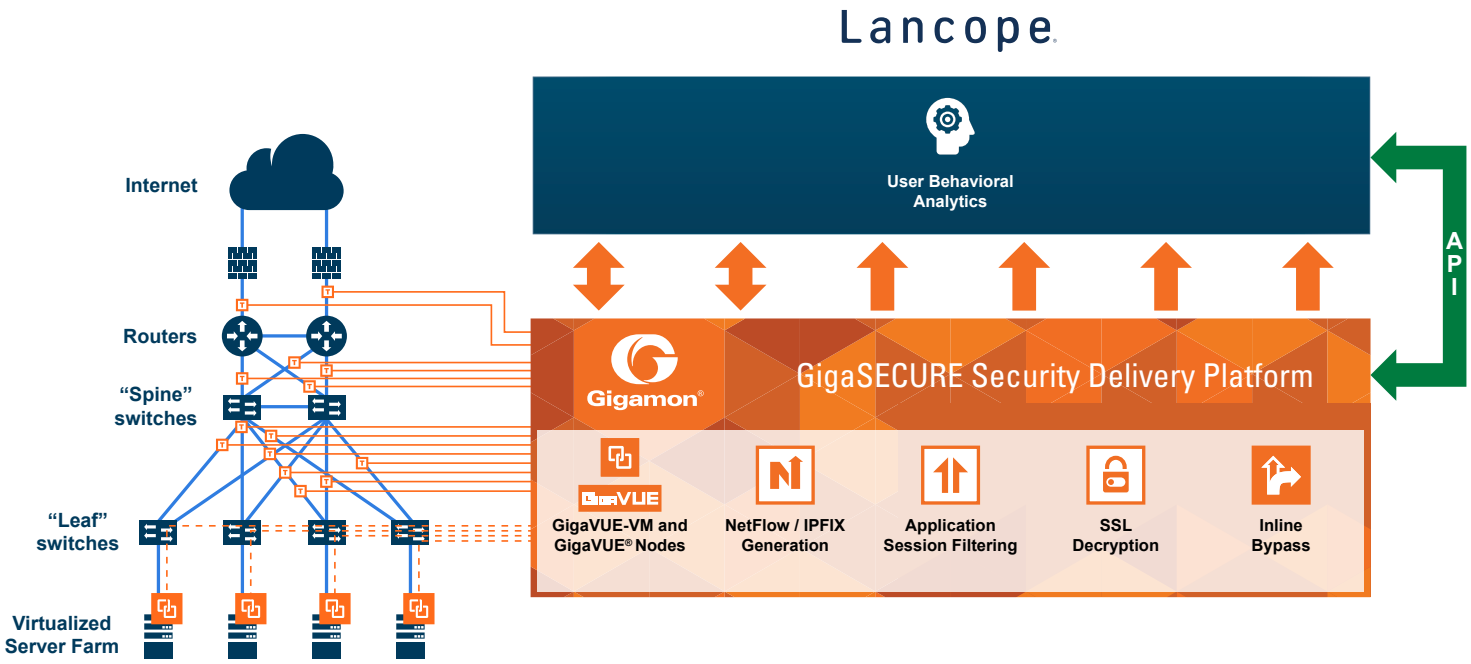
Network and security administrators today need to understand and respond to network incidents in a matter of seconds. In order to accomplish this task, information about network transactions is necessary. The most common method of observing these transactions is NetFlow or IPFIX. However, the availability of this data can be limited. Not all network elements support NetFlow. Even if available, flow data is often disabled because it causes performance degradation. To keep up with network speeds, flow data is generated by sampling the traffic; this means anomalies may be missed and threats overlooked. Analyzing the large volumes of flow data is a challenge for security monitoring which needs to quickly identify any anomalies within the network that could signify any type of APT, DDoS or insider threat attack.

The Gigamon and Lancope Joint Solution

The joint solution using Gigamon and Lancope products provides context-aware security information by leveraging transactional records sent from Gigamon to Lancope collectors in the form of NetFlow or IPFIX records. By not sampling traffic, Gigamon provides a comprehensive and accurate view into network activity.

Lancope's StealthWatch system makes sense of this sea of data created by transactional logging. By collecting and analyzing the flow data, StealthWatch provides visibility into anomalies that could represent attacks such as malware, insider threats, DDoS or APTs. Continuous monitoring of host and network communications, combined with advanced security intelligence and behavioral analytics helps organizations find the proverbial "needle in a haystack" and shut down security and performance issues before they impact day-to-day operations.

Gigamon's GigaSECURE Security Delivery Platform receives traffic inline or out-of-band from any number of TAP points or SPAN ports. As well as sending that traffic to packet-based monitoring tools, the GigaSECURE platform generates flow data from these raw packets, deduplicates and applies post-filtering if desired and then sends specific flow data to StealthWatch. There it is processed, correlated, and analyzed to identify threats using a mix of behavioral and policy driven alerts. The port density offered by Gigamon's platform uniquely positions it to gather data from many different areas of a network at once.



About Lancope

Lancope, Inc. is a leading provider of network visibility and security intelligence to defend enterprises against today's top threats. By collecting and analyzing NetFlow, IPFIX and other types of network telemetry, Lancope's StealthWatch System helps organizations quickly detect a wide range of attacks from APTs and DDoS to zero-day malware and insider threats. Through pervasive insight across distributed networks, including mobile, identity and application awareness, Lancope accelerates incident response, improves forensic investigations and reduces enterprise risk. Lancope's security capabilities are continuously enhanced with threat intelligence from the StealthWatch Labs research team.

About Gigamon

Gigamon provides the GigaSECURE® Security Delivery Platform to enable the management of increasingly complex networks. Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies, centralized management and a portfolio of high availability and high-density fabric nodes, network traffic is intelligently delivered to management, monitoring and security systems. Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.

Learn More

For more information on the Lancope and Gigamon solution, contact:

Lancope

3650 Brookside Parkway, Suite 500
Alpharetta, GA 30022
Phone: +1 (888) 419-1462
www.lancope.com

Gigamon®

3300 Olcott Street
Santa Clara, CA 95054
Phone: +1 (408) 831-4000
www.gigamon.com

3154-03 07/15