Joint Solution Brief

Pervasive Network Visibility as a Service with Talaia Networks and Gigamon

The Challenge

Network engineers need visibility to diagnose congestion, unearth bandwidth hogs, detect attacks, and retain data for forensics. Unfortunately, visibility in high-speed networks doesn't always come easily, quickly, or cost-effectively.

Integrated Solution

Combined with the Gigamon Visibility Platform, the Talaia cloud-based SaaS solution provides network engineers with the turnkey visibility they need to better and more quickly understand what applications are consuming bandwidth, identify abusers, detect attacks, and perform forensic analysis of network activity.

Key Benefits

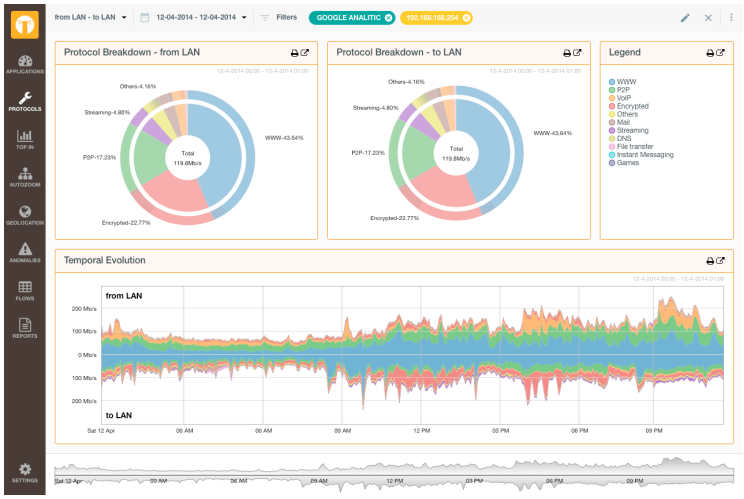
- Easily deployed SaaS service offering traffic analysis, detection of denial-ofservice (DoS) attacks, and more.
- Analysis of metadata generated by Gigamon provides rapid insights into threats on your network.
- Gigamon's GigaSECURE® platform provides pervasive visibility to traffic crossing your network and creates an efficient stream of metadata that Talaia analyzes to help you secure, manage and understand your business.

Introduction

For high-speed network customers, pervasive visibility shouldn't have to require time-consuming, expensive development of homegrown applications. It should be readily available and without maintenance headaches. And it can be.

Packaged as a Software-as-a-Service (SaaS) solution, Talaia is a network intelligence solution offered by Talaia Networks that can be deployed in minutes—even from the cloud—quickly, easily, and cost-effectively to provide customers with intuitive, multi-tenant dashboards that enable traffic analysis, detection of denial-of-service (DoS) attacks, and more. The solution offers:

- Bandwidth monitoring: Track bandwidth usage per application to spot congestion and understand network traffic flow.
- Forensics NetFlow database: Store raw traffic for in-depth incident analysis and forensics.
- Top talker identification: Determine bandwidth hogs and enforce company usage policies.
- Attack detection: Proprietary machine learning based algorithms enable signature-less flagging of anomalous traffic patterns, only using NetFlow data.
- Traffic geolocation: See where your traffic comes and goes in geographical terms.
- SaaS/cloud or on-premise: Offered as a service from the cloud or on-premise for physical or virtualized servers.
- Areas of interest: Create logical traffic views as needed (e.g., focus in subnets, interfaces, ports, data centers, physical locations).



The Gigamon and Talaia Joint Solution

By combining a Big Data platform with artificial intelligence, Talaia delivers insights for network operation, security, and planning. The solution can ingest, process, and enrich flowbased network traffic metadata, and it can do so at scale.

Integrated with Gigamon's Visibility Platform, Talaia helps high-speed network customers gather network metadata without resorting to statistical sampling. For example, the Gigamon Visibility Platform can feed Talaia metadata records with extended information that routers cannot provide. The combination of Gigamon's Visibility Platform and Talaia's network traffic analytics platform is compelling for any customer—including Internet Service Providers (ISPs)—with extended visibility and metadata requirements.

Key Gigamon solution features that augment the value of Talaia technology deployments include:

Easy access to traffic from physical, virtual, and public cloud networks: The Gigamon Visibility Platform manages and delivers all network traffic to the Talaia solution, efficiently and in the correct format. To monitor east-west data center traffic and public cloud workloads, Gigamon taps virtual traffic and incorporates it into the Gigamon Visibility Platform for delivery to the Talaia solution on the physical network. This eliminates blind spots and ensures that all traffic is monitored and analyzed together.

Traffic filtering: The Gigamon Visibility Platform sends specific traffic or sessions to Talaia so that irrelevant traffic is discarded early and the anlysis can focus only on information of interest.

Metadata generation: The generation of unsampled NetFlow/IPFIX metadata for any traffic flow as well as extended metadata records (e.g., for HTTP response codes and DNS queries) enables highly detailed contextual analysis when looking at network and security events.

De-duplication: Pervasive visibility requires tapping or copying traffic from multiple points in the network, which, in turn, means tools may see the same packet more than once. To avoid the unnecessary packet processing overhead on Talaia, Gigamon offers a highly effective de-duplication engine that removes duplicates before they consume resources.

Learn More

For more information on the Talaia Networks and Gigamon solutions, contact:

Talaia
www.talaia.io

Gigamon®
www.gigamon.com

3239-01 07/17