JOINT SOLUTION BRIEF

Real-Time Threat Detection with Reservoir Labs R-Scope and the Gigamon GigaSECURE Security Delivery Platform

The Challenge

As the bandwidth and complexity of networks continue to increase and the sophistication of cyber attacks continues to grow, security professionals often struggle to see the full context of unusual network behavior required to adequately monitor and defend their businesses.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, Reservoir Labs R-Scope® network sensor provides deep and wide network visibility to detect advanced threats and enhance hunting, at great scale.

Joint Solution Benefits

- Enhanced visibility and easy access to traffic from across physical, virtual and public cloud networks through the GigaSECURE Security Delivery Platform enables R-Scope to see the full context of unusual network behavior
- R-Scope leverages GigaSECURE's automatic traffic load balancing and aggregation functionality to reduce bottlenecking, guarantee high port density, and optimize performance at minimal cost
- The GigaSECURE de-duplication engine removes duplicate traffic packets to reduce processing overhead on Reservoir Labs R-Scope sensors
- Resilient architecture helps ensure maximum performance and reliability

Introduction

The goal? Security professionals tasked with monitoring large, multi-gigabit networks must be able to see the full context of unusual network behavior.

The challenge? Processing demands. To protect against today's multifaceted threat environment (phishing, Trojans, worms, spam, viruses, and sophisticated hackers), security systems face unprecedented processing demands in providing the visibility and context required by security professionals. The sophistication and frequency of new attacks combined with ever-increasing network speeds surpass the capabilities of many security appliances to monitor, analyze, filter, and defend.

The answer? Reservoir Labs R-Scope, a powerful, open technology network sensor that not only interoperates with all leading network and analytic tools, but can scale up in access and performance. Combined with the Gigamon GigaSECURE Security Delivery Platform, R-Scope offers one of the most flexible and high-performing intrusion detection system (IDS) deployment options on the market. Architected to connect to major security information and event management (SIEM) systems, R-Scope leverages the breadth and depth of the Bro/Zeek open-source analytics language and incorporates the most advanced threat intelligence technologies available to provide deep and wide network and threat visibility, advanced situational awareness, and real-time security event detection by extracting cyber-relevant data from network traffic.

The Gigamon and Reservoir Labs Joint Solution

With a hyper focus on what's happening at any moment in and around the network, the Gigamon and Reservoir Labs joint solution gives security professionals the visibility they need to hunt for and identify sophisticated and targeted attack behaviors, reference historical data when necessary, and link non-obvious data patterns across the network to detect and stop threats in real time.

Situated to protect the border or as an ideal "top of rack" security tool, R-Scope uses advanced metadata extraction to catch exfiltration, network breaches, or lateral movements between systems inside the firewall. Moreover, the featurerich GigaSECURE platform enables R-Scope deployments to scale from small 1Gb network segments to large 100Gb networks by gathering, distributing, and load-balancing packet data across multiple R-Scope appliances. GigaSECURE also delivers high availability with GigaStream failover across R-Scope systems; provides VLAN tagging support; and offers de-duplication of data coming from overlapping network chokepoints.

Key GigaSECURE Security Delivery Platform features that augment the value of Reservoir Labs technology include:

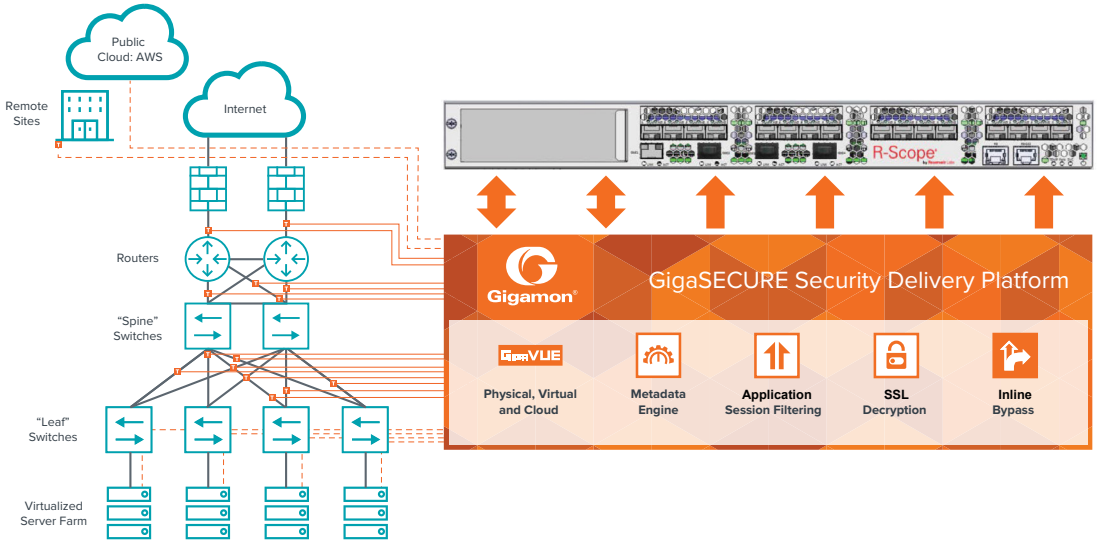
Easy access to traffic from physical, virtual and public cloud networks: The GigaSECURE platform efficiently manages and delivers relevant traffic from across the network to the Reservoir Labs R-Scope devices in the format required.

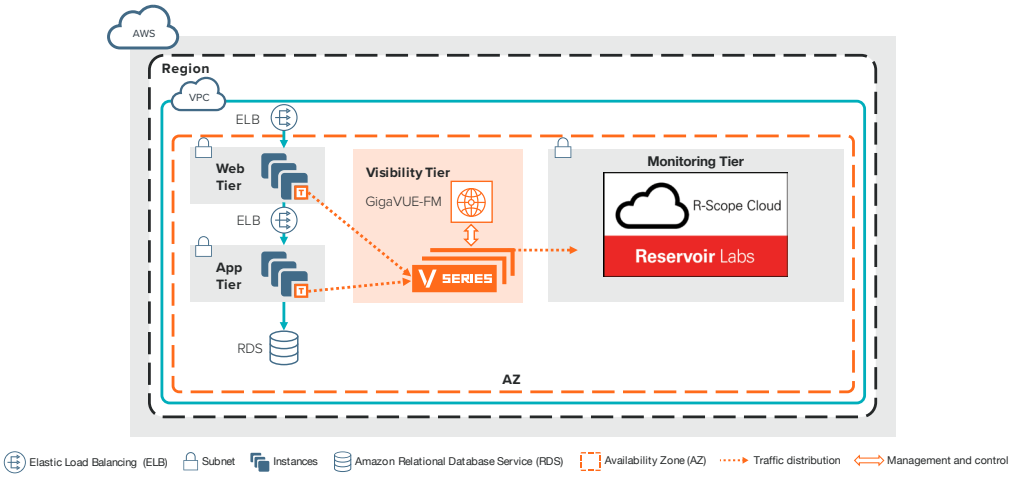
Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single tool can handle, the GigaSECURE platform can split the flow across multiple tools while also helping to ensure that sessions are kept together and tool numbers can be incrementally grown by adding new devices to those already connected.

Aggregation to minimize tool port use: Where links have low traffic volumes, GigaSECURE can aggregate these before sending them to the R-Scope network sensor and minimize the number of ports needed. By tagging the traffic, GigaSECURE can also identify the traffic source.

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 unnecessary packet processing overhead on R-Scope, GigaSECURE uses its highly effective de-duplication engine to remove duplicates before they consume resources and help balance monitoring coverage.

Masking for security: GigaSECURE is able to mask any sensitive data (e.g., credit card numbers in e-commerce and patient identification in healthcare) within packets before sending them to other tools where operators or other unintended recipients may see them.





For more information on Gigamon and Reservoir Labs solutions,

visit: www.gigamon.com and www.reservoir.com

Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

3144-03 10/18