Joint Solution Brief

GigaSECURE Delivers Complete Network Visibility to Niara's Security Analytics Attack Detection and Incident Investigation Solution

The Challenge

Today's enterprise threat environment presents two fundamental challenges: 1) finding slowly gestating attacks that elude standard defenses before they inflict damage, and 2) once discovered, determining the extent of the threat and the appropriate response.

Integrated Solution

The GigaSECURE® Security Delivery Platform optimizes the collection of packet-level data and efficiently generates summary information about those packets or metadata (including NetFlow/IPFIX) from traffic flows across both physical, virtual and public cloud networks. Niara's security analytics platform applies machine learning algorithms, analytics, and forensics to data from the security infrastructure and data supplied by the GigaSECURE Security Delivery Platform.

Joint Solution Benefits

- Security context from all traffic flows – the GigaSECURE platform optimizes delivery of network data, extending Niara's behavioral analytics
- The GigaSECURE platform generates enriched metadata, including unsampled NetFlow/IPFIX, from packet-level traffic and delivers it to the Niara platform for analysis without requiring intermediate sensors
- Using rich network data and metadata integrated with logs, alerts, and external threat feeds, Niara automatically detects attacks and dramatically reduces the time and skill needed to investigate and respond to security events

Introduction, Detect, and Verify

Analytics based on metadata (including NetFlow/IPFIX) information traditionally have been relegated to forensic deep dives and one-off investigations. No longer. Because attack indicators for a compromised user or advanced malware are very subtle and difficult to see, network data is a crucial source of intelligence and insight for quickly surfacing attacks on the inside with advanced behavioral analytics.

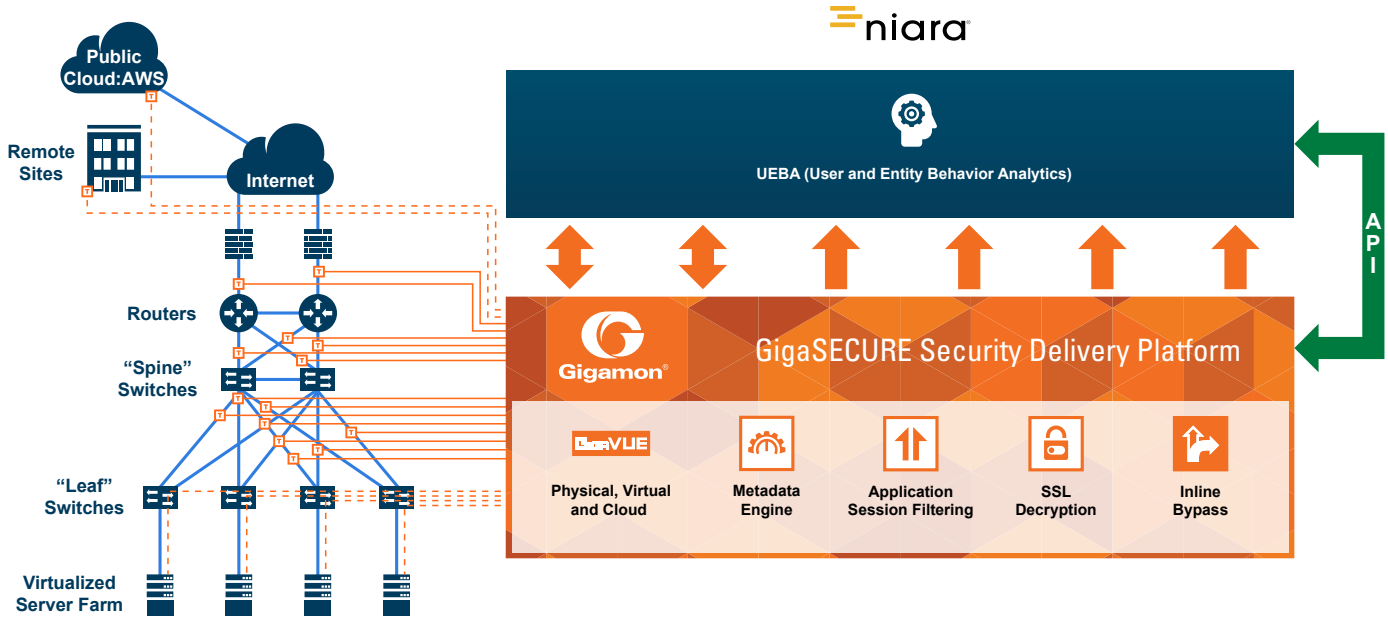
In addition, when faced with credible threats, security teams must quickly validate the conclusions of the analytics, determine the extent of the problem, and execute a remediation plan. This can take days or weeks when critical data is spread across many different platforms and data silos. In particular, network traffic or packets and metadata (including NetFlow/IPFIX) analytics are not typically integrated into the attack discovery and incident response workflow, making it nearly impossible to determine whether malicious intent can be assigned to an anomaly.

The Gigamon and Niara Joint Solution

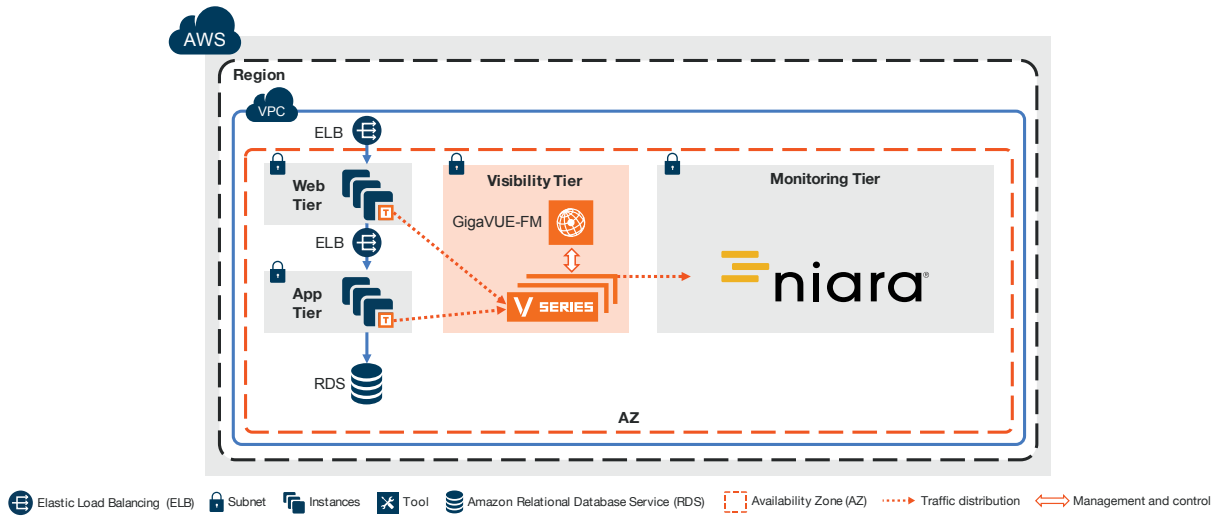
To address these challenges, the Niara platform seamlessly connects with Gigamon's GigaSECURE Security Delivery Platform to obtain packets and metadata, fusing context from network traffic with a wide variety of other security-relevant data (i.e., logs, alerts, and threat feeds). As network activity streams in from the GigaSECURE platform the Niara platform applies a precision set of analytics and machine learning (including unsupervised, supervised, and semi-supervised models) to not only detect attack signals, but to better link anomalies to malicious intent, all while maintaining one-click access to the complete forensic record. Comprehensive visibility is delivered through risk profiles for users, hosts, and devices with user-attribution for IP and MAC addresses.

The result is an enterprise-class solution for attack discovery and incident investigation that provides unmatched visibility by converging advanced analytics and forensics into a unified view of an attack.

For packet-level data forwarding, the Gigamon solution aggregates line-rate data from 100Mb, 1Gb, 10Gb, 40Gb (including BiDi) and 100Gb circuits, from network TAPs or SPAN ports, from GigaVUE-VMs (virtual machines) deployed on data center hypervisors, and from public cloud workloads. This provides the Niara platform critical visibility into network traffic across the physical, virtual, public cloud, and distributed infrastructure.



Hybrid Deployment Model



Public Cloud Deployment Model

Gigamon applies patented intelligent traffic processing, such as Flow Mapping®, de-duplication, and packet slicing, so that only the required packets and payload information are provided to the Niara solution while performing header-stripping and TLS/SSL decryption to ensure that each packet can be fully utilized by the Niara platform. Gigamon's inline bypass feature can provide an option for the Niara platform to be deployed inline for greater resiliency.

With the combination of the Niara platform and the GigaSECURE Security Delivery Platform, security analysts can be more expedient in detecting compromised users, hosts, and malicious insiders, speeding threat hunting efforts, and reducing the time for incident investigation and response by focusing security teams on the threats that matter.

Learn More

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

niara
www.niara.com

Gigamon®
www.gigamon.com

3187-03 11/16

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