Joint Solution Brief

Detect Attacks with JASK and the Gigamon GigaSECURE Security Delivery Platform

The Challenge

Overwhelmed with endless security alerts and false postives, security analysts can often struggle to prioritize and focus their efforts as real attacks go undetected and with the potential to wreak significant havoc on networks. A Cybersecurity strategy without the complement of Artificial Intelligence (AI) can be a losing battle. JASK offers an AI-based Network Security Platform which helps predict real threats while minimizing false positives.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, JASK receives the rich and relevant data required to speed security analysis and discovery of actual, actionable data breaches. With Gigamon, JASK can provide critical security insights as a limitless scale SaaS platform, leveraging cloud compute and storage.

Joint Solution Benefits

- Broad and deep visibility across both physical and virtual network traffic gives JASK wide access to data to help solve the world's most complex big data problems
- The GigaSECURE platform accelerates processing throughput by effectively filtering and distributing relevant traffic from customer data centers to JASK
- JASK leverages the GigaSECURE platform's automatic traffic load balancing and aggregation functionality to reduce bottlenecking and port oversubscription
- With the GigaSECURE platform's real-time SSL decryption functionality, JASK gains increased visibility into traffic without performance degradation

Introduction

Integrated with the Gigamon GigaSECURE Security Delivery Platform, JASK brings together cybersecurity, artificial intelligence, and fast data expertise to help analysts hone in on and process the right data faster to uncover and take action against actual, ongoing attacks.

The Gigamon and JASK Joint Solution

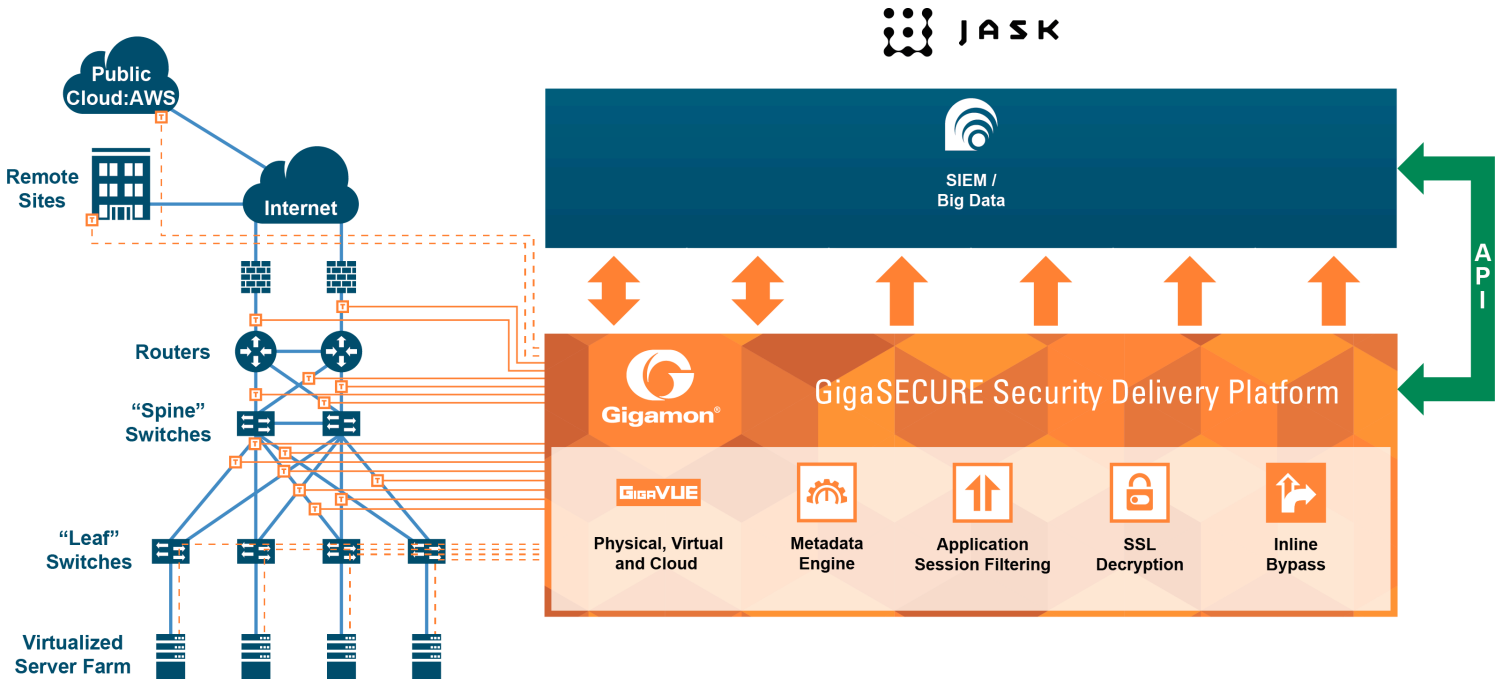
At its core, JASK is a Big Data platform built for quick, cost-effective, and scalable deployment for both real-time and historical analysis over the volume of stored data. Thanks to the GigaSECURE Security Delivery Platform, JASK collects the right data directly from the network and fuses it with other data sources such as threat intelligence to provide rich context into real threats.

Not only does JASK perform deep packet inspection (DPI) at scale, it leverages a hybrid AI engine to apply deep learning to reduce the number of false positives and provide a highly prioritized set of "smart alerts" that analysts can review and work from. With this type of artificial intelligence—which sits at a level above indicators—JASK can connect sequences of events and identify those that are indicative of an attack. This more complete and precise picture allows analysts to curtail the hunt and, instead, focus on analyzing and containing a true security incident.

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

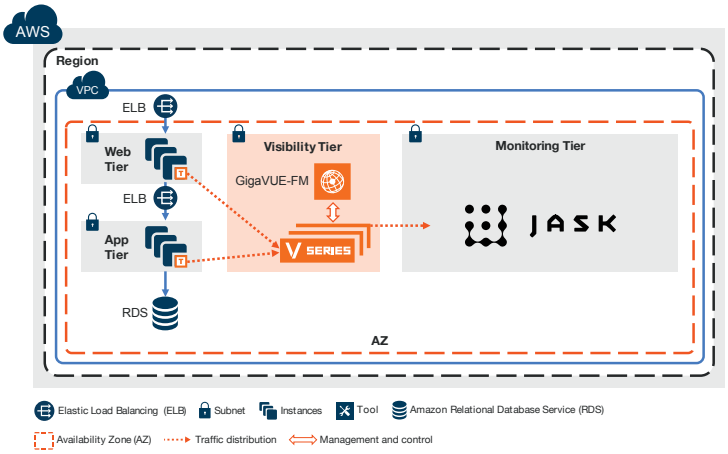
- **Easy access to traffic from physical and virtual networks:** The GigaSECURE platform manages and delivers all network traffic—in the format required—to JASK. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to the JASK cloud platform. This helps ensure that all traffic is monitored and analyzed together—avoiding blind spots and increasing the probability of spotting suspicious behavior.
- **Filtering traffic to only send relevant traffic:** The GigaSECURE platform can be configured to send only specific traffic or sessions to the JASK solution so that it only analyzes traffic that provides security value.
- **Aggregation to minimize tool port use:** Where links have low traffic volumes, GigaSECURE can aggregate these together before sending them to JASK minimizing the number of ports required. By tagging the traffic, the GigaSECURE platform can provide the identity of the traffic source.
- **SSL decryption:** Real-time SSL decryption integration increases traffic visibility for JASK.

© 2016 Gigamon. All rights reserved.



Hybrid Deployment Model

- **Header stripping for efficiency:** As needed, eliminates the need for JASK to decipher protocols, thus reducing its processing load and increasing efficiency.
- **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.
- **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 JASK, the GigaSECURE platform has a highly effective de-duplication engine that removes duplicates before they consume resources.



Public Cloud Deployment Model

Learn More

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

JASK
www.jask.io

Gigamon®
www.gigamon.com

© 2016 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

3214-01 12/16