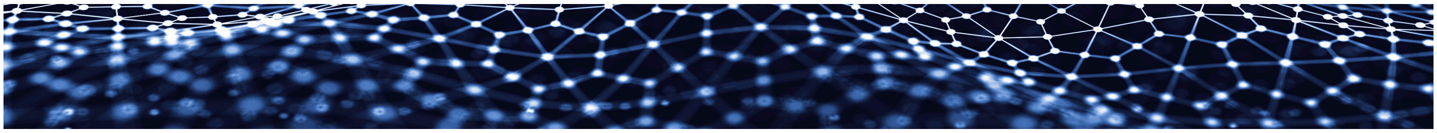
aria CYBERSECURITY SOLUTIONS

TECH BRIEF



ARIA SDS Packet Intelligence and Juniper JSA Solution

Detect and stop the most harmful network-borne attacks early in the kill chain

Benefits:

Superior Threat Detection: Detect hidden cyber-attacks within minutes as they become active within your network.
Stop Threats Earlier in Kill Chain: Stop the attacks immediately once detected – before harm is done.
Surgical Threat Containment: Improve threat containment by stopping attacks precisely without taking devices or application offline.
Accelerate Investigative Response: Gain insights into your internal network traffic to accelerate incident detection and response. Set, monitor, and enforce network communication policies.

The integration between Juniper Security Analytics SIEM and ARIA SDS Packet Intelligence application finds and stops the types of cyber-attacks that do the most harm.

The ARIA Packet Intelligence (PI) application integration with Juniper Security Analytics (JSA) detects internal network threats including ransomware, malware, and advanced persistent threat (APT) intrusions, including attacks involving IoT. It gives security operation center (SOC) teams the ability to stop the threats as detected to minimize harm. Further, the solution can be used to both set and enforce connectivity policies.

The ARIA PI application inspects network packets and generates IPFIX or NetFlow records for each packet. It also classifies each packet to determine and take the best action for a given traffic conversation. Such actions include:

- Redirecting specific source destination pair conversations over a given port to an IDS to look for known threats
- Making copies of the conversations for further analysis
- Dropping the conversation altogether if the ARIA appliance is inline rather than off a switch span port or a network tap

Juniper JSA SIEM ingest logs, indexes them to enable manual searches to identify issues and threats. Rules can be created to help trigger searches to be run periodically to generate results on an ongoing basis. Searches can be complex and can take long periods: minutes to even hours to run when looking through vast amounts of ingested data. The more dedicated server compute is set aside, the faster the solution works.

The Juniper JSA was one of the first SIEMs that can also ingest network data. Network data can help find threats if the correct data is available, and you know how to search for them. JSA can take network data in two forms:

- The JSA Flow Collector application can directly ingest and mine network data packets for metadata. This allows for the identification of the type, source and destination of the traffic, as well as the length and frequency of specific traffic flows. This is most effectively accomplished with the deployment of an ARIA hardware appliance, or on an ARIA Cybersecurity Myricom Security Intelligent Adapter (SIA).

- JSA's Flow Processor application can also ingest NetFlow or its IETF standardized version known as IPFIX. This save expense and delay related to capturing and generating the useful metadata from such packets. JSA recommends this approach for externally sourced data; for example, data from firewalls or routers that can only generate sampled versions of the data. Sampling means that a flow record is generated by such routers and firewalls at a periodic but constant rate. For instance, Cisco routers typically generate 1 NetFlow record for 1 in 10,000 packets seen. They create such a small percentage because they do not have the processing power to generate flow records and keep up.

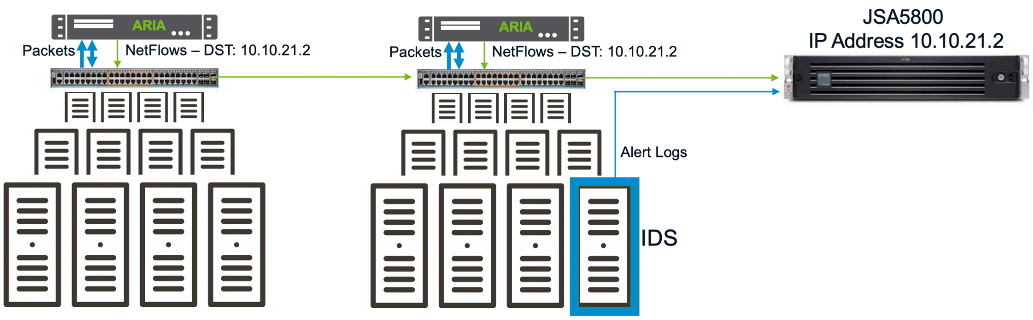
The ARIA PI application's wire rate processing provides the JSA IPFIX or NetFlow records for each packet seen (i.e., it doesn't sample data). The flow records are 1/1000th the size of the original packets, so it's a thousand times more efficient/faster than sending the packets directly to JSA. PI's approach does this for all network packets, allowing JSA to find threats that get past the firewall as well as potential internal threats from compromised devices or insiders.

The benefit of not using a sampling approach is significant. Sampling so infrequently can easily miss threats altogether, or at best, require the attacks to be active for a long time in order for JSA to stumble upon them.

Example Deployments:

1. **Attack Detection:** The ARIA PI application running on the ARIA Cybersecurity Solution's Myricom

   Secure Intelligent Adapter (SIA), a next generation SmartNIC, can send the data from protected servers to the IP address of the JSA Appliance Flow Processor at wire-rate. Alternatively, the ARIA security appliances with built-in SIAs can be fed data from network switch spans or taps to perform its flow and packet classification operations. With up to 50Gbps of wire-rate processing capacity per SIA, multi-SIA chassis can easily keep up with high line rates. SOC teams can instruct PI to send specific traffic streams to IDS or other tools, which can help verify threats, and whose logs in turn can be ingested by JSA to provide a complete correlation of the NetFlow-sourced threat information along with the IDS results.



- PI instances sending network generated NetFlow records to JAS5800 appliances NetFlow Processor app.
  - Searches of this data will help find network born attacks like ransomware, intrusions, etc.
- PI sending select traffic stream packet copies to IDS as instructed by SOC to verify threats

2. **Attack Containment:** The ARIA PI application can also take action to stop a threat or enforce a

   permanent policy. The Myricom SIA in-server deployments can do this, as can the ARIA security appliances when deployed with our inline bypass option.

Contact Us to Schedule a Technical Demonstration or Arrange an Evaluation ✉ **ARIAsales@ariacybersecurity.com**

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110

Follow Us: Linkedin • Facebook • Twitter • Blog

aria CYBERSECURITY SOLUTIONS   ariaSDS   nVoy SECURITY APPLIANCES   Myricom NETWORK ADAPTERS