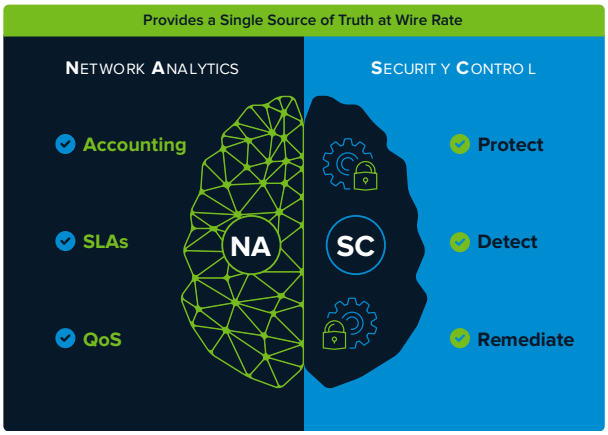
aria CYBERSECURITY SOLUTIONS

DATASHEET

ARIA Packet Intelligence

Lossless, wire-rate packet operations for network service accounting and control, and/or cyber-threat detection, containment, and high-speed protection.



Features and Benefits – Network Analytics

- Meets a wide variety of wire-rate network service monitoring and control functions, as well as cybersecurity requirements, including threat detection, investigation, and containment
- Provides visibility into all network traffic by feeding analytics to packet delivery accounting tools, quality of service (QoS), and service level agreement (SLA) monitoring applications
- Performs full network monitoring of all critical assets and application data, including lateral traffic flow
- Allows for the setting and enforcement of network policies, all while maintaining wire rates

Features and Benefits – Security Control

- Improves the threat detection and containment effectiveness of security tools, including SIEMs, IDS/IPS, and forensic packet recorders
- Stops network-borne threats by isolating infected devices or dropping harmful traffic
- Runs at full 10G, 25G, or up to 100Gbps wire rate without impacting network or application performance
- Offloads packet handling to scale OEM and service provider applications
- Deploys easily with simple API connectors to OEM and service provider applications
- Runs from within any OEM appliance or service provider server via ARIA Cybersecurity's Myricom SIA SmartNIC

ARIA's Packet Intelligence (PI) is designed to give OEMs and service providers a means to leverage the latest SmartNIC techlogy to perform in-line advanced packet-level network and security operations cost-effectively while at wire rate. The application can classify every network packet, create metadata, and take actions on each packet all while running at wire rate when deployed upon our ARIA SIA or ARIA SIA Express SmartNICs.

The ARIA PI application provides value in two use cases: network analytics and cybersecurity control.

1. **Network Analytics**

- **Packet-level accounting for usage based billing or capped services**

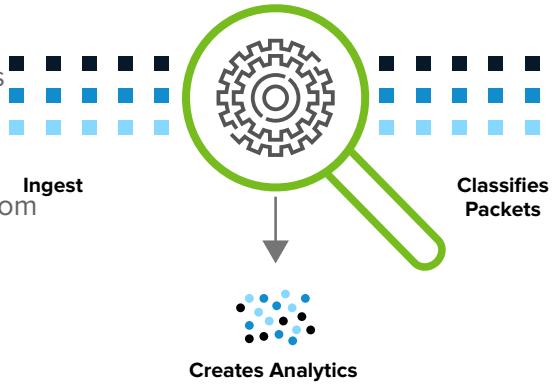
Accurate packet counts are critical for organizations whose revenue stream is tied to usage-based billing. As such, packet counting applications cannot drop or lose track of any packet details. Since the size of packets can widely vary, when measuring the amount of data transferred, every byte must be counted on a per-service, per-subscriber basis.

At low packets per second for instance, in the single gigabits range, most OEM's or service provider's homegrown applications can keep pace (assuming they are running on today's class of dedicated x86 appliances). The challenge however, is as the number of service instances increase across a provider's footprint, it may result in the deployment of thousands of dedicated service edge appliances.

The second challenge is that the bandwidth of today's services is increasing tenfold. Most providers need to deal with service-edge infrastructure running at line rates of 100Gbps. Increasing the number of appliances tenfold or more, into unmanned service edge offices makes little operational sense, especially if these locations don't have data center power and cooling infrastructure. Even the envisioned 5G edge data centers have highly constrained space, power and cooling limitations.

ARIA PI Advantage:

- **20 X improvement** in application service density when deployed on the Myricom SIA
- **75% reduction** in power draw and cooling requirements
- **Off-loads X86 environments** by running on ARM based SmartNICs in any standard PCIe slot
- **Off-loads the packet-counting functions** onto the NIC from the host, providing summarized metadata NetFlow records to the host-based application across the PCIe bus.
- **Marks packets for SLA enforcement** or tagging and steering packets upon classification onto the appropriate network path, for appropriate upstream handling.
- **Rate limiting** may be imposed by the host application when by instructing the ARIA PI to do so for managing subscriber service streams, enforcing policy, or as a result of thresholds that have been exceeded.



- **Network Monitoring and Policy Enforcement**

The ARIA PI application can easily classify all network packets and apply, as well as enforce policies such as rate limiting. In addition, ARIA PI can perform operations such as packet marking or tagging while maintaining wire rates of up to 100Gbps.

ARIA PI Advantages:

- **Marking packets for SLA enforcement** or tagging and steering packets upon classification onto the appropriate network path, for appropriate upstream handling.
- **Rate limit** certain subscriber service streams by policy, or after certain thresholds have been exceeded.

These functions are accessible via API (or manually via UI control) making it straightforward for OEMs or service providers to harness the data and control provided by ARIA PI.

2. Cybersecurity Control

- **Threat Detection**

Today, cyber threat detection is largely conducted at the network edge or upon the end devices. However, many threats are missed and not discovered until long after the damage is done. Those that typically do the most harm are intrusions that “land and expand” like zero-day malware, ransomware, network intrusions, and data exfiltrations.

ARIA PI Advantage:

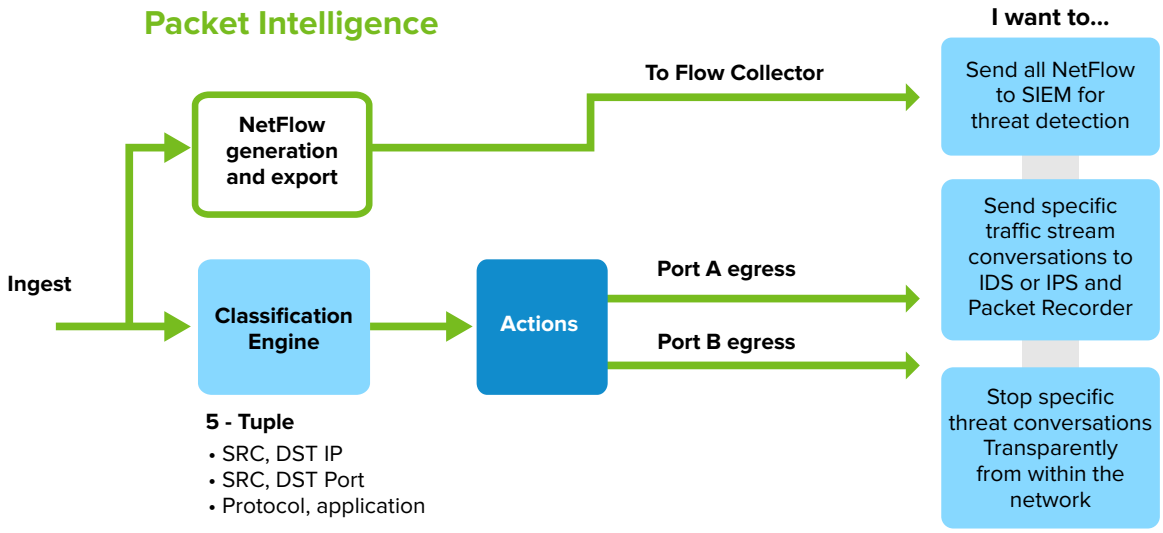
- **Feeds metadata to threat detection tools for complete network visibility** including lateral traffic movement by feeding a steady stream of metadata into threat detection tools, providing enhanced internal network level threat visibility.
- **Detects network-borne threats by their lateral movement**, as they move through the network. This also applies to any data exfiltrations through DNS and other application tunnels that typically go unmonitored.
- **Prevents and protects against undesired connectivity** of devices and applications both internally and to the outside world.

- **Investigative Response**

  The ARIA PI application classifies every packet traversing the network allowing security teams to redirect specified traffic conversations for further analysis, such as those detected by metadata. They can direct copies into an IDS, or conversely, the original packet stream can be redirected to an IPS for a closer look before being sent to their destination. In parallel, these suspect streams can also be copied and directed to packet recorders for even further analysis or recording for later forensic inspection.

ARIA PI Advantage:

- **Enables detection of network-borne threat** including ransomware, malware, and intrusions as they become active. Typically security tools, like SIEMs, IDS/IPS, etc. miss this if the internal network is not monitored.
- **Automate workflows** to take the appropriate actions against suspicious traffic conversations. Security solutions that support automated workflows, such as our ARIA Advanced Detection and Response
  (ADR) solution, or third party SOAR tools, can communicate via APIs to direct the ARIA PI instances to send conversations, in their entirety, for further analysis.
- **Improve speed and effectiveness of threat analysis** by generating as many copies of specific traffic streams as desired in real-time – enabling multiple workflows to occur independently and in parallel.
- **Flexible operating modes** for passive detection and active response:
  - Passive in that the ARIA PI application will typically run out-of-band through the use of network taps or switch/v-switch span ports. In such an implementation, threats can be detected, but will not be directly acted upon by the application.
  - If deployed actively in-line, as a bump in the wire, the application can classify traffic in real time while also applying a set of rules to that live traffic as it passes through the network – such as stopping threats as they are detected by isolating infected devices or blocking threat communications.



- ## Network-Based Threat Remediation

When used in any of the manners detailed below, the ARIA PI application enables the real-time automatic execution of remediative actions on specified traffic flows.

ARIA PI Advantage:

- **Create, apply, and enforce microsegmentation** rules to determine which set of devices, groups, or applications within these groups can talk to each other outside the group. All of this occurs inside the network, including between the on-premises networks and the public cloud, as well as microservices running within and between applications.
- **Identify and stop known threat traffic by** redirect traffic stream conversations, such as certain file transfers and/or email traffic streams, as specified by policy, or dynamically, through an IPS for analysis.
- **Dynamically redirect traffic streams** by leveraging workflow automation tools for additional investigation. For example, upon API instruction, send all traffic from a potentially malware-infected device group through an extensive IPS rule set, while also sending a copy of the traffic to a packet recorder for forensic analysis and future audit.
- **Stop specified threat conversations** using the ARIA PI user interface as identified by the security team, or automatically through scripts/API commands from ARIA ADR or third-party tools.

- ## High-Speed Firewall

The ARIA PI application can also be used to help build high-speed wire rate firewalls that can run up to 100Gbs.

ARIA PI Advantage

- **10x improvement** over today's appliances at one tenth the price for effective high-speed internal east-west networks.
- **Cost-effective firewall offload** onto the ARIA SIA that is deployed within critical servers or OEM appliances. This approach not only maintains wire-rate, but it also avoids the need to upgrade and/or replace servers, or fund expensive appliance development.
- **100Gwire rate** stateless firewall functionality.
- **API driven** as part of 3rd party integrated or OEM solution

Easy Deployment, Centralized Management

The ARIA SDS Orchestrator simplifies and automates the deployment and provisioning of the ARIA PI application. This makes it easy to deploy, update, and run one, or hundreds of instances across a widespread organization with zero-touch.

Service chaining of ARIA PI instances allows for the running of multiple feature sets in the appropriate combination and to allow services to scale. This can be configured directly by an API or provisioned through the ARIA SDS Orchestrator.

The ARIA Packet Intelligence solution is offered in feature suites, each designed to meet a variety of security needs.

Use Case Comparison by Feature Set

FEATURES	Accounting and Network Enforcement	Threat Detection	Threat Investigation	Threat Remediation	Highspeed Wire Rate Firewall
Security analytics (NetFlow records)	✓	✓	✓	✓	
Creates analytics for every packet	✓	✓	✓	✓	
Classifies traffic flows	✓		✓	✓	
Drops, redirects, or copies traffic flows	✓		✓	✓	✓
Performs multiple operations/traffic flow	✓	✓	✓	✓	
API Driven	✓	✓	✓	✓	✓
Does not impact traffic performance	✓	✓	✓	✓	✓
Deploys passively	✓	✓		✓	
Passively detects threats		✓		✓	
Dynamic redirect		✓	✓	✓	
Deploys actively			✓	✓	✓
Redirects traffic flows to prevention tools			✓	✓	
Enforces network connectivity policy			✓	✓	✓
Network-based remediation				✓	
Up to 100G Stateless Firewall					✓
Up to 100G Statefull Firewall					✓
Automated remediation out of box				✓	
Automated provisioning	✓	✓	✓	✓	✓
“Set and forget” configuration	✓	✓	✓	✓	
Orchestrated option	✓	✓	✓	✓	✓
Service chaining capable operation	✓	✓	✓	✓	✓

SPECIFICATIONS		
Country of Origin	USA	
Warranty	1 Year	
Support	Annual support licenses required for ARIA Packet Intelligence, SDSo and any deployed Myricom SIA SmartNICs.	
ORDER DETAILS		
Packet Intelligence Bundled Offerings	25G-PCIE3-8C-PACKAN	Myricom SIA Express – Dual 10/25G low-profile, (HHHL). Includes 16 GB of DDR4 memory. Perpetual license, ARIA Packet Intelligence, Accounting and Network Enforcement
	100G-PCIE4-8D-PACKAN	SIA - Dual 25/50G Security Intelligent Adapter (low profile). Includes 16 GB of DDR4 memory. Perpetual license, ARIA Packet Intelligence, Accounting and Network Enforcement
	25-PCIE3-8C-PI	Myricom SIA Express – Dual 10/25G low-profile, (HHHL). Includes 16 GB of DDR4 memory. Perpetual license for ARIA Packet Intelligence Software. Complete Packet Intelligence Suite. This bundle combines all of the features provided by Threat Analytics, Threat Investigation and Threat Remediation.
	Contact Factory	Annual license, ARIA Packet Intelligence, Stateless Firewall Offload
Orchestrator *Note: ARIA SDS Orchestrator is required for the deployment, configuration and monitoring of the ARIA PI applications on the MYRICOM SIA SmartNICs*	SDS-SDSo-LIC-Perpetual	SDSo - Perpetual license for SDS Orchestrator Software. Manages an unlimited number of deployed instances. Required for HA configuration.
	SDS-SDSo-L-LIC-Perpetual	SDSo Light - Perpetual license for SDS Orchestrator Software. Manages up to 10 deployed instances.

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