aria CYBERSECURITY SOLUTIONS

PRODUCT BRIEF

ARIA Next Gen Network Response

ARIA's Next Gen Network Security Software (NSS) is designed to give OEMs, Private Cloud operators and service providers a means to leverage the latest SmartNIC and DPU technology to perform in-line advanced packet-level network and security operations cost-effectively at wire rate. The application can classify every network packet, create metadata, and take action to stop attacks all while running at rates up to 100Gbps

Features and Benefits

- Improves the threat detection and containment effectiveness of security tools, including SIEMs, IDS/IPS, and forensic packet recorders
- Stops network-borne threats and attacks by dropping harmful traffic
- Runs at 10G, 25G, or up to 100Gbps wire rate without impacting network or application performance
- Offloads packet handling to scale OEM and service provider value-add applications
- Deploys easily and provides simple API connectors to OEM and service provider applications
- Runs on the latest generation SmartNICs and DPUs deployable in OEM appliances or provider servers
- Enforces Network Traffic Flow Policies – governing what can connect and communicate over the network
- Generates NetFlow or IPFIX Analytics for every packet used to detect advanced network threats
- Delivers API-driven automatic disruption of network threats immediately upon detection with the ARIA ADR Platform (see below), through IPS integration or with security orchestration, automation, and response (SOAR) tools. Ideal for MDR services deployment
- Two deployment options: out-of-band for passive monitoring or inline (in-band) to automatically stop threats with its advanced traffic filtering

By feeding a steady stream of metadata to SIEMs and IPS/IDS solutions and applying advanced rules, ARIA Network Security Software (NSS) allows these devices to detect the presence of ransomware, malware, and intrusions as they become active. These threats are typically missed if the internal network is not monitored.

Enabling the correlation of this data with other sources can improve threat detection effectiveness by 80% while dramatically reducing the number of false positives. In addition, the NSS software can be programmed to send packet-level traffic streams, such as “send select conversations to and from SQL databases in a specific subnet to tools, including “IDS/IPS” to ensure critical asset traffic is fully monitored for threats.

If a threat is detected, SOC teams can use our automated workflows to tell the ARIA NSS instances to send conversations, in their entirety, for further analysis. Security tools that support automated workflows such as the ARIA ADR (Advanced Detection and Response) application or SOARs, can communicate via APIs to ARIA NSS to take one, or multiple actions, against suspicious traffic conversations.

In real time, the ARIA NSS software can generate multiple copies of specific traffic streams as needed and enable multiple workflows to occur independently and in parallel. The result is enhanced speed and effectiveness of the security team members’ success at detecting network-borne attacks.

This can be thought of as a passive approach to threat detection. Passive in that ARIA NSS software 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 NSS software.

However, the ARIA NSS software, when deployed as a component within our ARIA Zero Trust Security Gateway, can take active measures to prevent and stop detected network-borne threats in real-time. The AZT Gateway provides the hardware to allow the solution to be deployed “in-line” as a bump in the wire. The NSS application classifies all traffic in real time while also applying a set of rules to that live traffic enabling the stopping of attack traffic dynamically as detected or by blocking undesired communications per policy.

This approach can stop threats in four ways:

1. Network policy enforcement: 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.

2. Pre-specified investigation analysis: Redirect traffic stream conversations as specified by policy or dynamically, such as directing certain file transfers and/or email traffic streams through an IDS/IPS to identify and stop known threat traffic.

3. Dynamic redirect: Leverage workflow automation tools to dynamically redirect particular traffic stream conversations 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.

4. Network-based remediation: Stop specified conversations, as identified by the security team or in seconds automatically through scripts/API commands from ARIA ADR or third-party tools.

When used in any of these combined or separate manners, the ARIA NSS software enables the real-time automatic execution of preventative actions on specified traffic flows. The solution allows for up to 100s of 1000s of such rules to be active at any time.

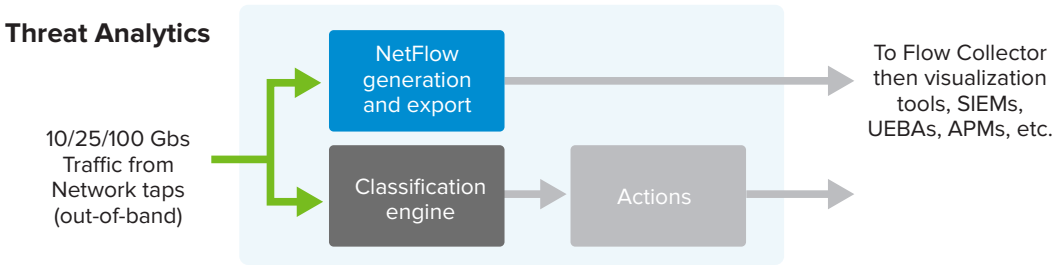
Another benefit of the ARIA NSS software is that it executes at full line-rate, up to 100G, without affecting application performance.

The ARIA Network Security Software (NSS) solution is comprised of two major blocks.

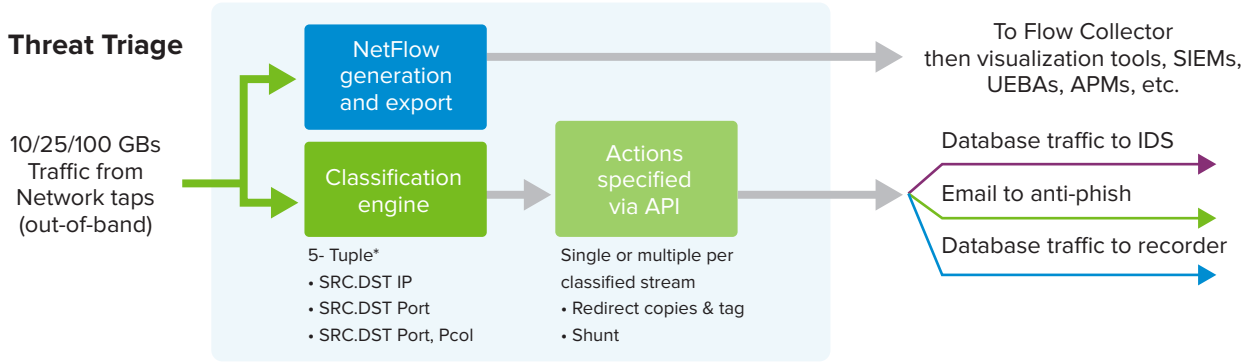
Network Analytics

This block provides a simple, low-cost approach to improve the visibility and intelligence gathering of network communications. This fully automated solution identifies and classifies all network traffic at full line rates of 10G, 25G or 100G with no loss of application performance. This block improves network visibility by providing NetFlow metadata (v5, v9 or IPFIX format among others) and/or provides application identification information for each traffic stream. This "meta information," provided to new or existing tool sets, allows for faster identification of threats.

In addition to network Netflow generation, the ARIA NSS software directs the appropriate classified traffic streams to security toolsets, including SIEMs, IDS/IPS tools, and recorder applications for further analysis. This intelligent filter capability redirects specific flows to each tool as specified.



ARIA NSS can also shunt certain flows, such as streaming video and audio-only, sending a specified number of bytes for inspection. Such adaptive filtering allows detection tools to operate more effectively by only analyzing the most relevant traffic. For SIEMs like Splunk and QRadar that charge by ingested bit, this translates into dramatic cost savings.



Built-in integration with ARIA ADR

Combining ARIA NSS with ARIA ADR provides a complete turnkey approach to fully automated network-based threat detection and response. ARIA Advanced Detection and Response (ADR) is an automated AI SOC solution purpose-built with the capabilities of seven security tools — including SIEMs, IDS/IPSs, EDRs, Threat Intel tools, NTAs, UEBAs, and SOARs. The out-of-the box integration of NSS with our ARIA ADR application, allows ADR to quickly detect the complete range of network attacks and to take automatic action to stop or disrupt threats transparently to the devices and applications from within the network. Ideal for protecting IoT, container-based compute architectures, and mission-critical applications. Learn more by referencing our ADR data Sheet.

This advanced solution gives organizations a fully automated means to secure their environment – ideal for those who do not have a dedicated security team that works 24x7, as well as the ability to improve the effectiveness and productivity of existing security team resources to identify and stop attacks.

FEATURE	NETWORK ANALYTICS	NETWORK RESPONSE	INTEGRATION WITH ARIA ADR APPLICATION
Security analytics (NetFlow records)	✓	✓	✓
Creates analytics for every packet	✓	✓	✓
Classifies traffic flows	✓	✓	✓
Drops, redirects, or copies traffic flows	✓	✓	✓
Performs multiple operations / Traffic Flow	✓	✓	✓
Does not impact traffic performance	✓	✓	✓
Passively detects threats			✓
Dynamic redirect		✓	✓
Deploys actively		✓	✓
Redirects traffic flows to prevention tools		✓	✓
Enforces connectivity policy		✓	✓
AI automated attack detection & response			✓
API-driven to stop threat traffic		✓	✓
Network-based remediation		✓	✓
Automated remediation out of box			✓
High availability option		✓	✓
SIEM transparent deployment	✓	✓	✓

ORDERING INFORMATION	
AZT-SW-NSS-LIC	Single instance of ARIA AZT Network Security Software

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