aria CYBERSECURITY SOLUTIONS

DATASHEET

ARIA SDS Packet Intelligence

Benefits

- Helps detect and automatically stop network-borne threats.
- Runs wire rate at 10G or up to 25G without impacting network or application performance.
- Performs full network monitoring of all critical assets and application data, including lateral traffic flow
- Gives many flexible deployment options: out-of-band for passive monitoring or inline (in-band) for automatic traffic filtering for network policy enforcement and dropping and/or redirecting threat traffic streams.
- Leverages and improves the effectiveness of existing security tools including SIEMs, UEBA, IDS/IPS, DLP, and forensic packet recorders.
- Delivers UI- and API-driven options for automatic disruption of network threats immediately upon detection. Works with SOAR tools. Ideal for MDR services deployment.
- Provides four deployment options optimized to meet a wide variety of security requirements: threat analytics, passive protection, active protection, and complete, out-of-the box turnkey protection.

Using the ARIA PI application, flow-level metadata can be created for all packet traffic and directed to existing security tools like SIEMs or UEBA solutions.

By feeding a steady stream of data to these devices, it is more likely that the algorithms will find network-borne threats. Enabling the correlation of this data with other sources can improve threat detection effectiveness by 80% while also reducing the number of false positives. In addition, the ARIA Packet Intelligence application can be programmed to send certain packet-level traffic streams, such as “send all conversations to and from SQL databases in this subnet to this group of devices,” to threat detection tools, including IDS or SIEMs.

If a threat is detected, and the detection tool has the appropriate built-in automation, it can tell the ARIA Packet Intelligence instances to send conversations, in their entirety, for further analysis. Security tools that support automated workflows can communicate via APIs to the ARIA Packet Intelligence application to take

one, or multiple actions, against suspicious traffic conversations. In real time, ARIA can generate as many copies of specific traffic streams as needed and enables multiple workflows to occur independently and in parallel. The result is enhanced speed and effectiveness of a broad array of tools, as well as the security team members' success detecting network-borne attacks.

This can be thought of as a passive approach to threat detection. Passive in that the Packet Intelligence 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 not directly acted upon.

However, the Packet Intelligence application can also take active measures to prevent and/or stop detected network-borne threats. If deployed in-band, or "in-line", the Packet Intelligence application can classify traffic in real time while also applying a set of rules to that live traffic as it passes through network.

This approach can stop threats in four ways:

1. **Network policy enforcement:** Create, apply, and enforce microsegementation 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 a DLP system to identify and stop data leaks.
3. **Dynamic redirect:** Leverage workflow automation tools to dynamically redirect particular traffic stream conversations for additional investigation; such as 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:** Through the ARIA UI, stop specified conversations as identified by the security team, or automatically through including scripts/API commands from third-party threat detection tools.

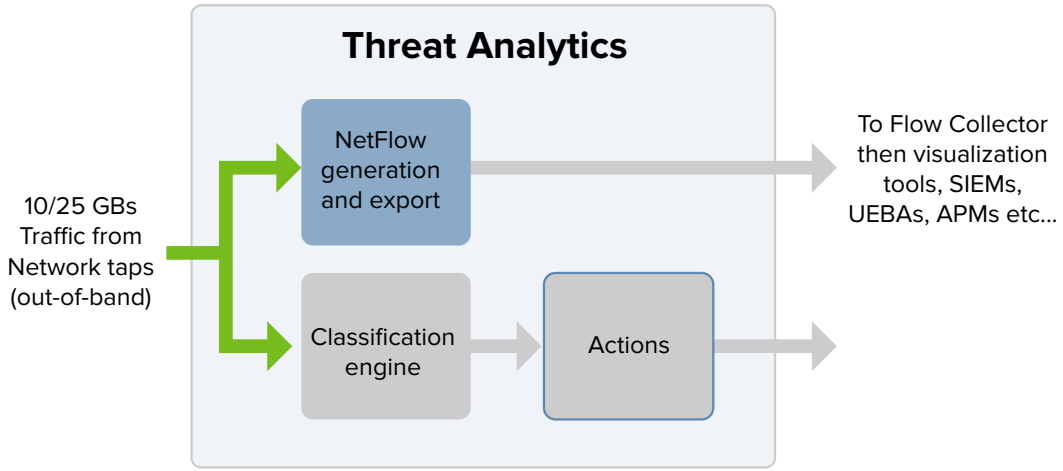
When used in any of these manners, the ARIA Packet Intelligence application enables the real-time automatic execution of preventative actions on specified traffic flows. Another benefit of the ARIA Packet Intelligence application is that it executes at full line-rate, up to 25G, without affecting application performance. For organizations that desire data protection capabilities, our solution can direct traffic to additional ARIA applications to provide crypto services.

The ARIA SDS platform simplifies and automates the deployment, and provisioning of the ARIA Packet Intelligence application. This make it as easy to deploy and run one or hundreds of instances across a wide-spread organization.

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

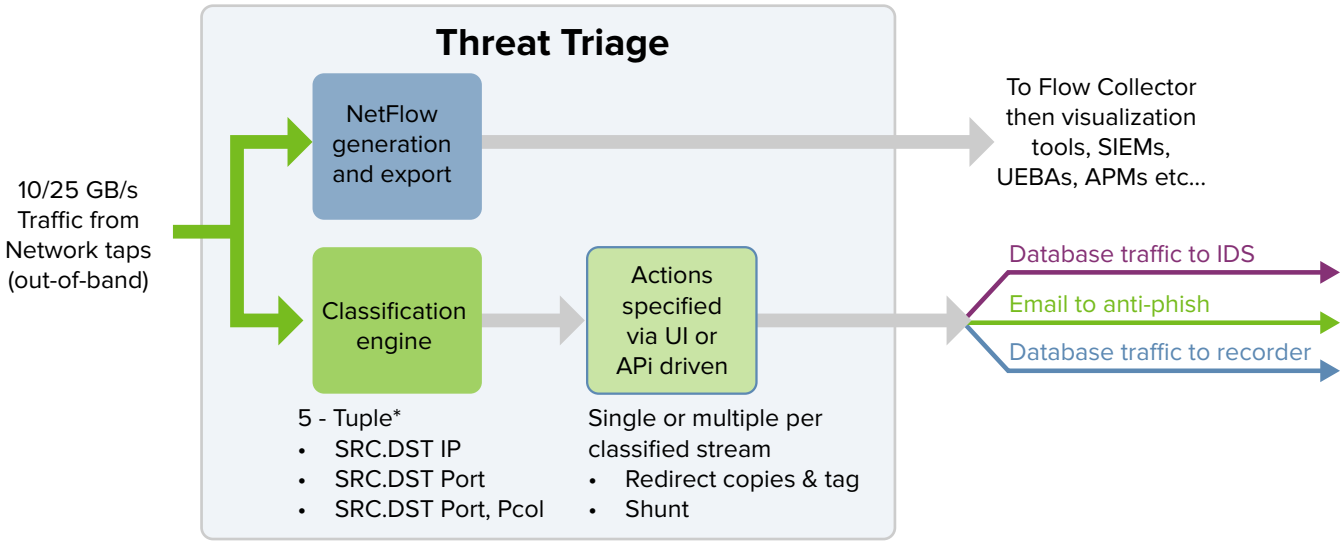
Threat Analytics

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 or 25G with no loss of application performance. The PI Threat Analytics configuration improves network visibility by providing NetFlow metadata (v5, v9 or IPFIX format) 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.



Threat Triage

The Threat Triage configuration deployed either through tap or switch span directs the appropriate classified traffic streams to security toolsets, including SIEMs, IDS, UEBA, and DLP applications, for further analysis. This intelligent filter capability redirects specific flows to each tool as specified.



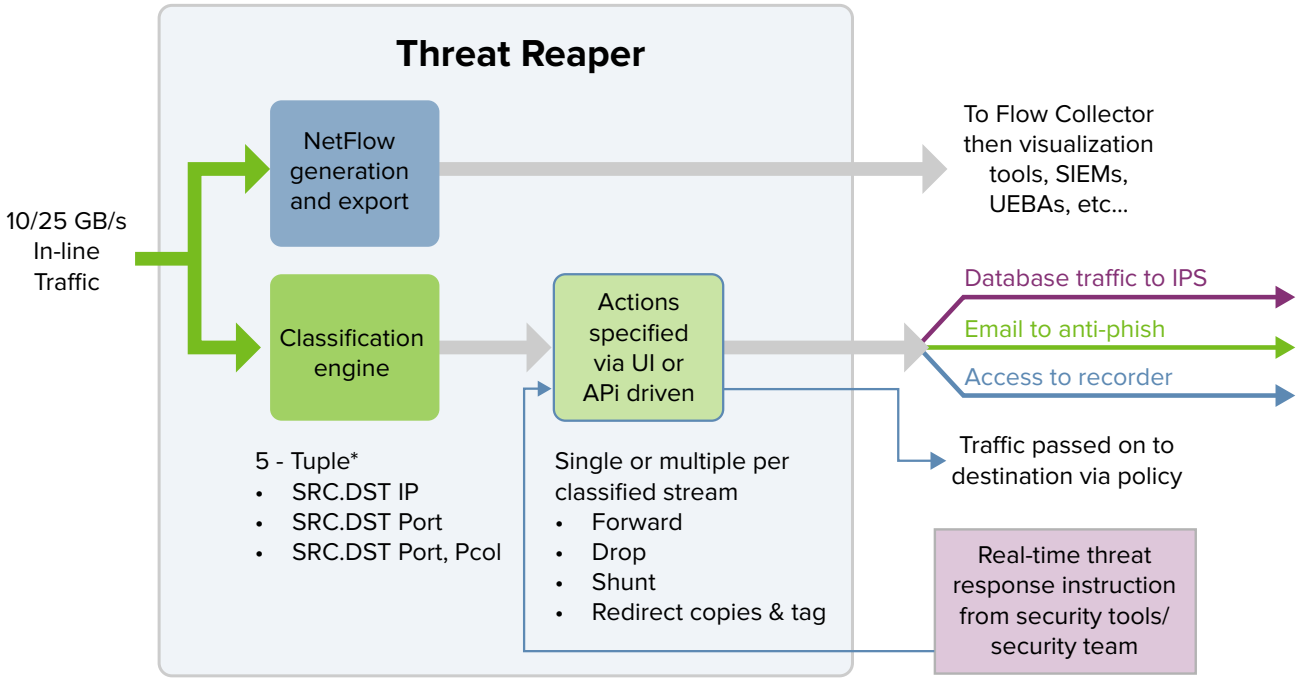
ARIA Packet Intelligence can also shunt certain flows, such as streaming video and audio-only, sending a specified number of bytes. Such adaptive filtering allows detection tools to operate more effectively by only analyzing the most relevant traffic. For SIEMs like Splunk and QRadar that charge by ingested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

Threat Reaper

The in-band deployment of the Threat Reaper configuration not only provides the same level of automated network monitoring capabilities as found in passive offerings (Threat Analytics and Threat Triage), but it also enables the real-time ability to stop network threats, as well as perform network policy enforcement. It works with third-party tools that support security orchestration, automation, and response (SOAR) solutions, and or automated scripts and workflows that allow such tools to communicate with ARIA to stop the threats as they are detected.

This greatly increases an organization's ability to take the appropriate actions against certain traffic streams, including forward, drop, replicate, redirect, shunt, and alert. Dynamic interaction directly or via automated workflow APIs gets the specified suspect traffic conversation streams to the right toolsets for proper analysis.

Additionally, the Threat Reaper configuration is centrally managed, through ARIA Packet Intelligence's user interface, and once set up, eliminates the manual effort and potential errors when managing a complex environment. For organizations that have requirements around redundancy and resiliency, there are also options for high availability.



Threat Suite

The last and most robust configuration is a complete turnkey approach to full network-based threat detection or protection. The Threat Suite solution integrates third-party security tools, such as IDS tools, to detect threats and, IPS to detect and to take automatic, actions to stop or disrupt threats once detected.

This preconfigured solution gives organizations a centralized and orchestrated way to secure their environment, as well as the right data needed for security team resources to identify and stop potentially destructive network activity.

FEATURE	THREAT ANALYTICS	THREAT TRIAGE	THREAT REAPER	THREAT SUITE
NetFlow analytics	✓	✓	✓	✓
App ID analytics	✓	✓	✓	✓
Creates analytics for every packet	✓	✓	✓	✓
Classifies traffic flows	✓	✓	✓	✓
Sends copies of flows to tools	✓	✓	✓	✓
Performs multiple operations/ traffic flow	✓	✓	✓	✓
Does not impact traffic performance	✓	✓	✓	✓
Deploys passively	✓	✓		
Passively detects threats		✓		
Dynamic Redirect		✓	✓	✓
Deploys actively			✓	✓
Redirects traffic flows to prevention tools			✓	✓
Enforces connectivity policy			✓	✓
Performs micro-segmentation			✓	✓
API Driven to stop threat traffic			✓	✓
Network based remediation			✓	✓
Automated deployment	✓	✓	✓	✓
Set and forget configuration	✓	✓	✓	✓
High Availability option		✓	✓	✓
Traffic decryption option		✓	✓	✓
IDS or IPS integrated option				✓
Email anti-phish option				✓

Contact Us Today: sales@ariacybersecurity.com or (978) 954-5038

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 01854

Connect with Us: ariacybersecurity.com / Linkedin / Twitter / Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS