aria CYBERSECURITY SOLUTIONS

DATASHEET

ARIA SDS ADR Application

A single platform for enterprise-wide automated threat detection and remediation

Benefits

- **Find the threats that matter:** Those that other security tools typically miss.
- **Stop attacks early in the kill chain:** Real-time identification before harm is done.
- **Validate alerts:** Drastically reduce the volume of alerts and surface the real threats and attacks.
- **Resource light:** Easy to deploy; system does the work of a SOC analyst for you out of the box.
- **Reduce costs:** Functionality equal to security operations center without the expense.
- **MDR services platform:** Effective and highly automated for very profitable MDR service offerings

ARIA Cybersecurity Solutions' Advanced Threat Detection and Response (ADR) application provides superior threat detection and containment functionality in a purpose-built solution. Now, using a single platform, security resources can find, validate, and stop threats in minutes. Today, this level of functionality is only achieved through multiple tools requiring continuous tuning and run by a highly trained security operations center (SOC).

Achieving complete visibility into network conversations is critical to finding threats faster and earlier in the attack lifecycle. The ARIA ADR application solves for this by first ingesting the NetFlow metadata for every network packet as generated by the integrated ARIA Packet Intelligence (PI) application. Then, it ingests alerts and logs from across the environment: like firewalls, endpoints and server infrastructure, cloud provider, as well as production applications. Using this wealth of information, it can quickly home in on any suspicious activities and correlate them using artificial intelligence (AI) based threat models included in the application.

Included are models for every known threat types, leveraging machine learning (ML) and dynamically created rule sets to find each threat by telltale behavior patterns. The ARIA ADR application self-correlates the individual behaviors to verify the threat, its target, and its progress through the kill chain before declaring an alert. By this process, it eliminates false positives and elevates high-priority attack alerts.

Examples of threat telltale behaviors include lateral spread, new or threatening log-in behaviors, new data connections to critical resources, and many more. There are hundreds of behaviors, most of which are innocuous until they are put into context as a series of activities that match threat behavior clusters in our threat models.

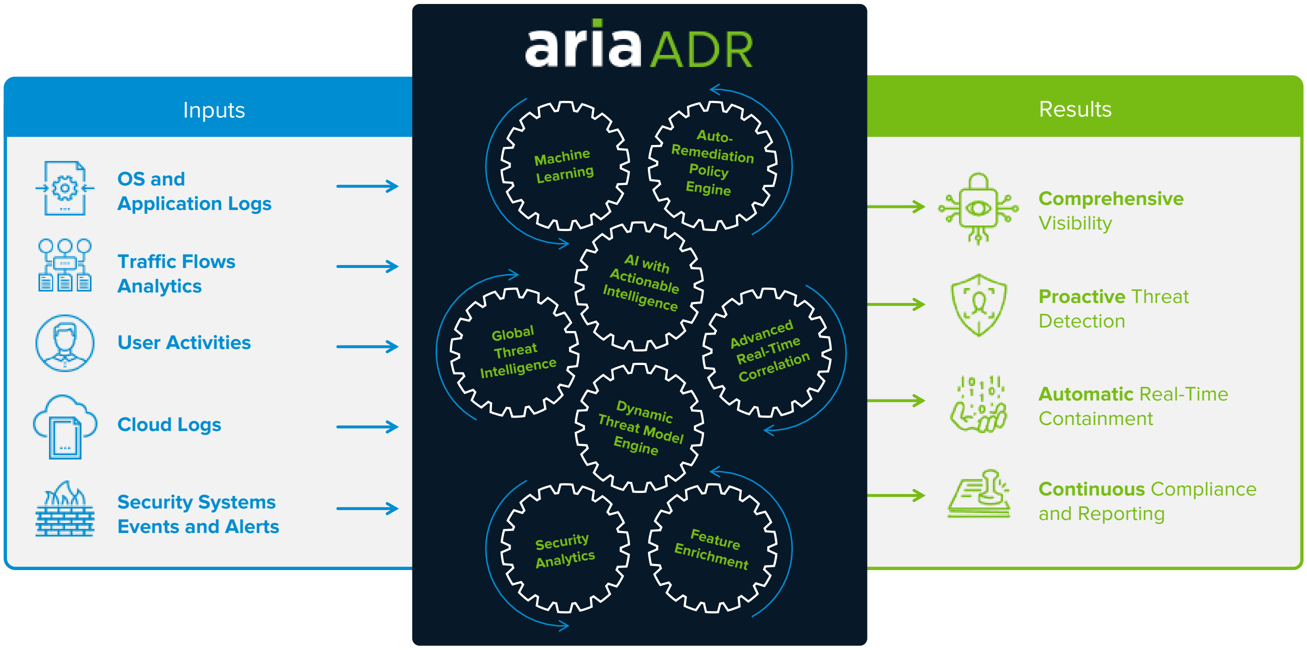
While AI and ML science may sound complicated, it's all contained within the ARIA ADR application. The result is threats can't hide. The application doesn't need signatures or continuous community updates on the latest type of threat. Analysts don't need to create any rules or perform searches – the system does all that. Meaning when an alert is generated, it is real and it is actionable.

Types of Threats Found by ARIA ADR		
Attacks	Intrusions	Breaches
Ransomware	Exploits	Data Exfiltrations
Malware		
Bots	APTs	
Brute-Force Attacks		Policy Violations
Compromised Credentials	DNS Stuffing	
Insider Attacks		
DDoS Attacks		

A key aspect of the ARIA ADR application is that once a threat is validated, it can communicate back by API to the ARIA PI application and instruct it to stop the conversations specific to that threat. It does this out of the box – no special configuration required. This is critical in containing threats like ransomware. It blocks all communication of infected devices or applications – isolating them off-line. However, since the application is intelligent, it can also tell the ARIA PI instances to only block the threat communication. This leaves critical devices and applications safely online, ensuring the continuation of normal business-critical operations until back-ups can be brought online.

There are other forms of containment ARIA ADR can execute upon. For instance, it can block specific external communications by writing polices to the firewall, and it can also deactivate a user or a device's compromised credentials. All of this is done by the system, either by the click of a button on the ADR UI – or automatically as the threats are alerted upon if so configured.

Our single pane of glass approach ensures ease of use. This process can be done through its UI or can be fully automated with no user involvement, leveraging the application's industry-leading AI-SOC™ capabilities. This is a major advantage over other security tools. AI-SOC™ is capable of automating – or removing the need for – most tasks a SOC performs. Most SIEMs and supporting detection tools that the ARIA ADR application replaces have a need for continual updating which adds a heavy eight-hour-a-day workload by a highly trained SOC team. The AI-SOC functionality removes the need for human tasking including defining rules, filtering responses, creating and executing playbooks, verifying threats, and then taking action to contain the threats. Finally, it autogenerates reports telling the status of your organization's security posture, and provides reports required to prove industry compliance with PCI, HIPPA, and NIST. It truly can be viewed as having a SOC-in-a-box.


aria ADR
Inputs
OS and Application Logs
Traffic Flows Analytics
User Activities
Cloud Logs
Security Systems Events and Alerts
Machine Learning
Auto-Remediation Policy Engine
AI with Actionable Intelligence
Global Threat Intelligence
Advanced Real-Time Correlation
Dynamic Threat Model Engine
Security Analytics
Feature Enrichment
Results
Comprehensive Visibility
Proactive Threat Detection
Automatic Real-Time Containment
Continuous Compliance and Reporting

The ARIA ADR results are incredibly accurate due to the ML and AI techniques used to eliminate false positives and validate all alerts. The AI-SOC capabilities are also valuable in establishing automated remediation actions and enforcing connectivity policies, thereby preventing violations. This gives organizations a solution that will evolve with attacks as they become more sophisticated, allowing them to maintain the upper hand.

ARIA ADR is ideal for service providers looking for a better managed SIEM or MDR service platform. It finds, investigates and verifies the real threats and attacks impacting your customers. It provides simple manual or fully automated actions to stop the threats with no complicated playbooks and processes. It does the hard work allowing you to bring on more customers supported by fewer and less highly trained staff.

Flexible Deployment Option for Every Environment

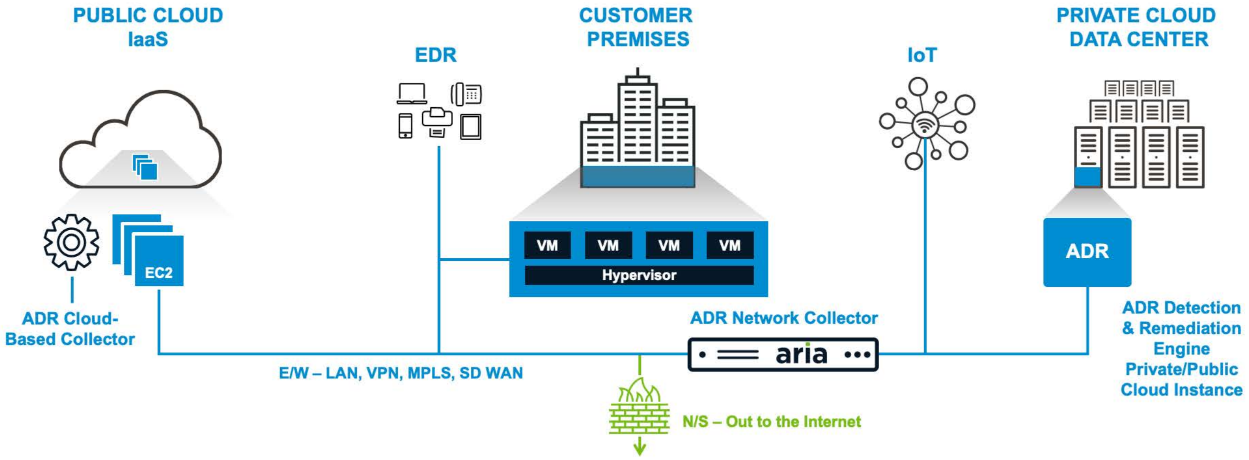
An ARIA ADR collector is provided in two configurations:

- A physical 1U appliance that can be deployed in the data center using ARIA Packet Intelligence to provide network visibility and remediation capabilities to ARIA ADR.
- A virtual collector that can be deployed in customer Cloud infrastructure to provide application and traffic visibility to ARIA ADR.

The ARIA ADR Analytics Engine, is the resource that ingests collected information and performs indicator of compromise detection, correlation and alert generation. It is the second piece of the ADR solution that can be deployed in multiple configurations:

- A physical 1U appliance that can be deployed in the customer premises.
- A virtual appliance that can be deployed in customer Cloud infrastructure.
- Hosted in ARIA’s SOC 2 compliant data center.

ARIA ADR – Solution Architecture



With ARIA ADR organizations gain:

- Multiple technologies deployed in one application that provide the most thorough threat detection.
- Deep visibility into network traffic to detect threats missed by traditional means.
- Identification of attacks as they land and spread before harm is significant.
- Protection of their IoT environments.
- Precise containment based on threat conversation, leaving critical devices or applications online.

The end result is a powerful cybersecurity solution for organizations that do not wish to invest in a SOC.

	On-Premise Collector	Cloud Instance Collector	Analytics Engine
Network Connectivity	4 x 1, 10, 25G	N/A	N/A
Dimensions	1 Rack Unit	N/A	N/A
Form Factor	**1 U Appliance bump in the wire**	Software image	Software image
Power	115v AC	N/A	N/A
High-Availability	Hardened bypass module. Multiple collectors can be deployed	N/A	Optional
Security	Parses logs and flow records creating analytics compressed and encrypted for transmission to the Analytics Engine	Parses logs and flow records creating analytics compressed and encrypted for transmission to the Analytics Engine	Receives compressed and encrypted analytics from ADR collectors only.
Instance requirements	N/A	Minimum instance requirements: CPU: 4 Cores (8 vCores), RAM: 16 GB, Storage: 250 GB	Minimum server or instance requirements for 5000 protected IP addresses CPU: 32 cores @2.35 Ghz, RAM: 8 x 32GB DDR4, Network: 2 x 1Gbps, Storage: 2 x 1TB M2 Drive, System: 1 x512GB 7200RPM HD. Additional drives, configured as RAID, may be required to support on-line Long Term Storage. Minimum server or instance requirements for 10000 protected IP addresses. CPU: 64 cores @2.0 Ghz, RAM: 8 x 64GB DDR4, Network: 2 x 1Gbps, Storage: 4 x 1TB M2 Drive, System: 1 x512GB 7200RPM HD Additional drives, configured as RAID, may be required to support on-line Long Term Storage.
Country of origin	USA	USA	USA
Compliance	UL, CSE, RoHS	N/A	N/A
Warranty	1 Year	1 Year	1 Year
Order Details	Each ARIA ADR solution is highly-configurable and built to customer specification. Please refer to our configuration guide and consult with one of our cybersecurity experts to design the optimal solution for your environment.		

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

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions provides new better ways to find and stop cyber thretas. 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