

The ARIA ADR Advantage

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

The ARIA Advanced Detection and Response (ADR) application provides superior threat detection and containment functionality in a single, purpose-built solution. It finds, validates, and stops threats — inside the box, no SOC required.

FIND ATTACKS THAT DO THE MOST HARM

Those that other tools miss.

STOP ATTACKS EARLY IN THE KILL CHAIN

In real-time before harm is done.

RECEIVE VALIDATED ALERTS

Surface threats that matter without the noise.

MINIMIZE RESOURCES

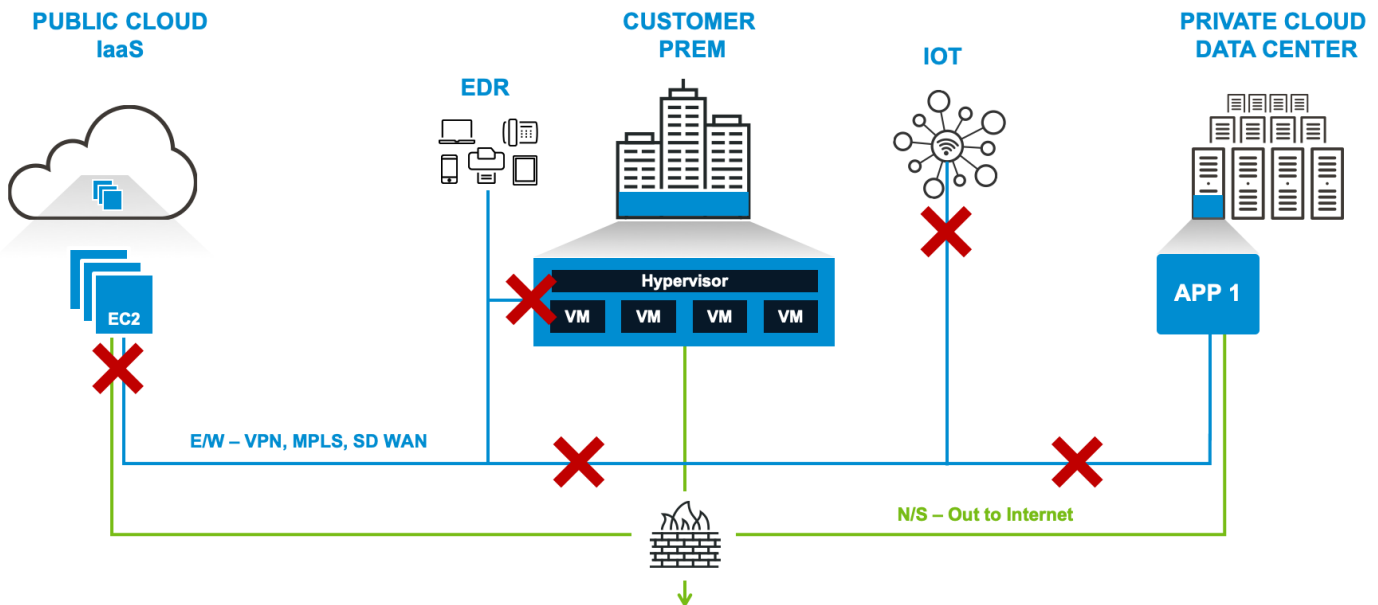
Enjoy easy operation — no rules, no searches — the system does it all.

REDUCE COSTS






Our SOC-in-a-box approach does the work without expensive staff.

What Makes ADR Different?

First, ARIA ADR provides **complete visibility** to every corner of your network where other solutions are limited or completely blind. If it's communicating internally, ADR sees it using the integrated ARIA SDS Packet Intelligence (PI) application. This allows ADR to find the most harmful threats faster and earlier in the attack lifecycle (or kill chain) before they can do significant damage.












Second, ADR leverages the **industry’s most comprehensive analytics** generated from alerts, logs, threat intelligence, and our own ARIA PI network analytics to find the threats quickly and accurately. Without this capability, it would typically require investments of SIEM, UEBA, NTA, IDS, and threat intel solutions to provide a similar approach. But these tools inevitably lead to an overabundance of noise (extraneous alerts), making it nearly impossible to find threats quickly, if at all.

				
EXISTING SECURITY SYSTEMS Events and Alerts	TRAFFIC FLOWS NetFlow, IPFix and Raw Traffic	USER Windows AD, DNS, DHCP, LDAP	CLOUD LOGS IaaS, PaaS, SaaS, Office365, VPC, Identity	RAW LOGS OS, Applications, Services, Processes

Instead, the ARIA ADR application makes this wealth of information manageable by utilizing artificial intelligence (AI) to feed it through machine learning **(ML) based predefined threat models** that understand how each threat behaves. The application quickly identifies all suspicious activities and correlates them to produce incredibly accurate results by eliminating false positives and producing valid alerts. All of this is done automatically with no human effort required. This is a major advantage over typical rules-based SIEM solutions that need constant updating.

Threats Detected by ARIA ADR

	INTRUSIONS		RANSOMWARE		INSIDER THREATS
	BRUTE FORCE ATTACKS		DDOS ATTACKS		DATA EXFILTRATIONS
	MALWARE		COMPROMISED CREDENTIALS		POLICY VIOLATIONS

Next, ARIA ADR’s AI **automatically contains these threats** before they can spread to other devices. This is critical in stopping the spread of attacks like ransomware or protecting exposed legacy operating systems or IoT devices that can’t support security applications like EDR. ADR enables organizations to stop these attacks with full or partial automation and little to no human intervention.

Security professionals can deactivate a user or a device’s compromised credentials, block attacks at the firewall to isolate infected devices from the network, or even contain threats by stopping their network conversations. This enables business-critical resources to stay operational and buys time to get back-up systems in place before taking compromised systems down.

Finally, ARIA ADR is also valuable for **assuring regulatory compliance** and **enforcing connectivity policies** – preventing future violations. This gives organizations a solution that provides a superior, longer-lasting security posture, one that will evolve with and stay ahead of attacks, even as they become more sophisticated.

Sustainable Security Posture – No Matter What Comes Next



**COMPREHENSIVE
VISIBILITY**



**PROACTIVE
THREAT
DETECTION**



**AUTOMATED REAL-TIME
THREAT CONTAINMENT
& POLICY ENFORCEMENT**



**CONTINUOUS
COMPLIANCE REPORTING**

The end result is a powerful cybersecurity solution that fully automates threat detection and response and delivers a complete “SOC In a Box.” This enables today’s organizations to:

- Stop more threats with improved visibility, analytics, speed, and accuracy
- Take advantage of a single platform to replace multiple IR tools and ineffective processes
- Reduce the need for 24x7 highly trained, expensive human employees

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 01854

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

Follow Us: [Linkedin](#) • [Facebook](#) • [Twitter](#) • [Blog](#)