aria CYBERSECURITY SOLUTIONS

How to Accelerate Incident Response with ARIA SDS

Stronger Cybersecurity Starts with a Smarter Approach

The Problem We Are Solving

Today, there are more cybersecurity solutions than ever before, yet security incidents and data breaches are at an all-time high. What's scary is that some of the most famous data breaches resulted from missed threats on internal networks, resulting in extensive amounts of exfiltrated data over long periods of time. These breaches could have been minimized or even completely avoided if the affected companies had better visibility into their internal network, most importantly, their east-west traffic.

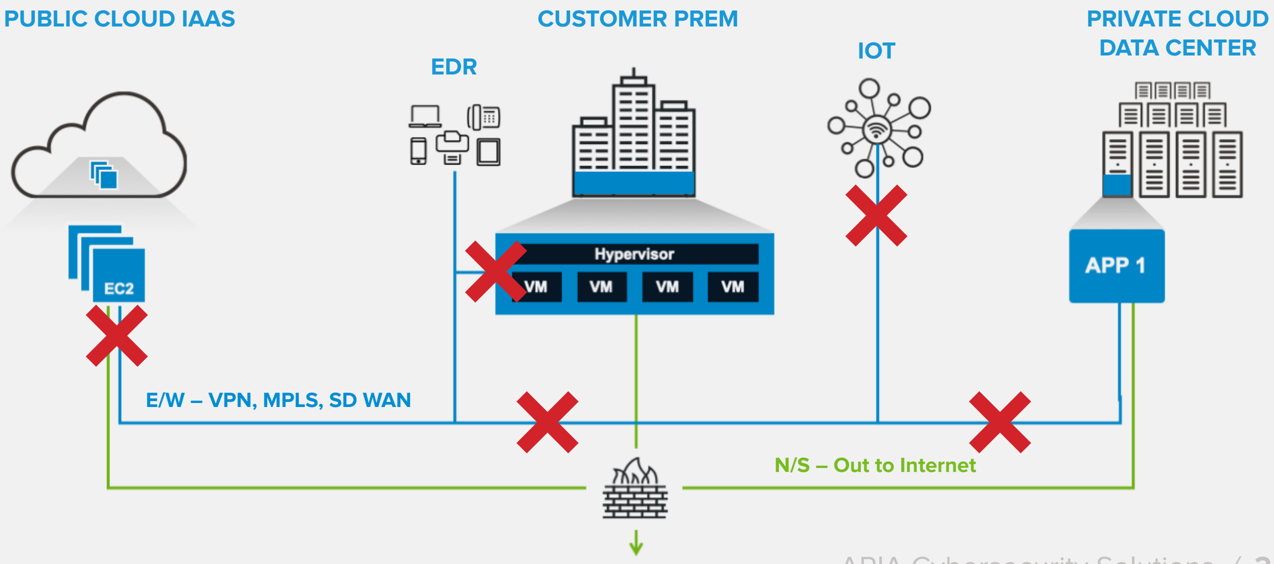
Given this, it's clear the industry needs a solution that can provide complete visibility, as well as effective protection, within a holistic, open architecture. Yet over the past 15 years, cybersecurity companies and tools have focused on perimeter protection with firewalls and endpoint detection and response (EDR) solutions that can only provide threat detection for what they see, and only on devices on which they can be deployed. This isn't practical as EDRs can't be used on most IoT devices and many legacy applications and systems. The mass adoption of IoT devices and container workloads creates a new open threat attack surface that is now being exploited due to inadequate protection and improper visibility into network-borne threats.

According to Forrester and ZK Research, 90% of the security budget is spent on perimeter measures, yet only 20% of the threats are found this way.

The other 80% of threats appear on the internal network, but are often missed or typically found too late due to significant gaps in detection and investigative response processes.

TODAY'S INTERNAL NETWORKS LACK THREAT VISIBILITY AND PROTECTION

An organization's internal network consists of traffic over VPN, private circuits, intra-VM, intra-containers, or within and between network segments.



What We Are Doing About It

ARIA Cybersecurity Solutions solves these challenges by focusing on internal network visibility and data protection through a unique software-defined security (SDS) platform. We recognized that creating yet another standalone point product wouldn’t be the answer, so we designed our platform to augment your already-existing incident response processes and security tools and improve their ability to detect, remediate, and protect you from threats and breaches.

Our ARIA SDS solution fills the gaps where existing tools fall short, and by operationalizing with a software-defined platform, ultimately leads to effective processes capable of quickly stopping more threats, with less effort and expense. Using the same staff and tools you have now, you can conduct threat investigations in hours, not days, weeks, or months, leading to significant cost savings.

Additionally, ARIA SDS’ a la carte approach to the deployment of security services and applications provides crucial missing elements for on-demand and automated assistance to best integrate with your existing incident response (IR) processes and tools.

ARIA SDS CLOSES THE GAPS OF INCIDENT RESPONSE TOOLS AND PROCESSES

Incident Response Stage →

Detection		Investigation		Containment		Prevention	
Whats Missing	ARIA SDS Advantage	Whats Missing	ARIA SDS Advantage	Whats Missing	ARIA SDS Advantage	Whats Missing	ARIA SDS Advantage
Threats avoid or are missed by perimeter and endpoint defense tools	**Utilize east-west network data to find threats previously missed and speed up threat detection**	IR has too much data to sift through to be accurate/ productive	**Correlate alerts with network data to create the best evidence and enable processes to focus on critical data**	Remediation takes down critical assets when infected and subsequently tends to be process bound = slow	**Quickly shut down only threat conversations and keep devices and/or applications fully operational**	Encryption is difficult to deploy for its value Device-based microsegmentation is ineffective for full network coverage and doesn’t work for IoT devices, critical workloads	**Cost-effective and simplified encryption management system** **Pragmatic, cost-effective network-based microsegmentation under SecOps control**

How ARIA Addresses Top incident Response Challenges

IoT Security		Time to Data Breach identification		Security Resources are Overloaded	
Whats Missing	ARIA SDS Advantage	Whats Missing	ARIA SDS Advantage	Whats Missing	ARIA SDS Advantage
Can’t accept EDR application, thus left unsecure	**Provide network-based protection and generate detection data and feeds tools such as SIEMs, IPSs and UEBAs**	Lack tools to quickly and effectively prevent data exfiltration	**24x365 automated data breach and exfiltration detection, verification and containment**	Lack of training and resources to be effective	**Integrated with security tools, such as SOARs, to develop playbook to guide and automate IR and threat containment**

ARIA SDS Provides a Smarter Approach for Stronger Cybersecurity

Powerful Platform, Powerful Results

ARIA SDS is a secured cybersecurity platform designed to properly secure your network and compute infrastructure, enterprise-wide. It is easily deployed in east-west traffic paths to inspect, record, and segment all network communications within and between customer premises, datacenters, and the public cloud.

Utilizing ARIA SDS' unique architectural approach allows you to:

- **Significantly improve detection and accelerate investigation of network-borne threats**
- **Effectively discover and protect IoT devices**
- **Improve protection of critical data no matter where it resides or is used**
- **Dramatically decrease MTTR with the reduction of operational costs**
- **Reduce the need for highly trained and siloed SecOps/InfoSec staff**
- **Cap spending on ingestion-based detection and IR tools**
- **Reduce risk**

Bringing it all Together: ARIA Orchestrator

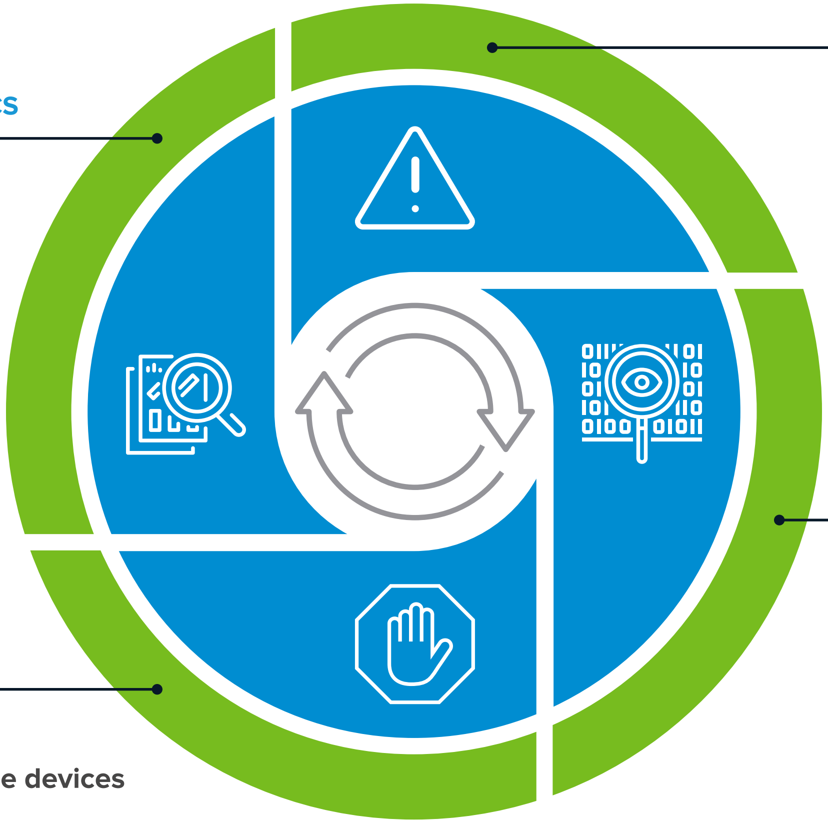
What makes all of this achievable is the ARIA Orchestrator. This software-defined delivery system provides the central provisioning and control your organization needs to gain a powerful advantage in your network and data security:

- **One system capable of deploying different applications and providing security services on-demand, on any compute infrastructure.**
- **Complete visibility across cloud, on-premise, datacenter, and WAN services, accelerating threat detection and response process by seeing threats immediately when they originate and spread no matter where they are.**
- **Ease of use with one-touch push provisioning across the entire network and without hardware dependencies.**
- **Open ecosystem that can be fully automated, using RESTful open APIs, and integrated with other tools like modern SIEM/SOAR/ IPS/IDS/FW/UEBA solutions, eliminating the need for proprietary ecosystems.**

ARIA SDS is easily deployed in east-west traffic paths to inspect, record, and segment all network communications within and between customer premises, datacenters, and the public cloud.

The Return on Investment is Clear

ARIA SDS helps organizations solve serious challenges presented by shortcomings in today's threat detection and prevention tools and processes. Using our approach, organizations have a clear advantage in detecting and disrupting intrusions, as well as remediation and forensic analysis.



FIND THREATS

- Cost avoided of missed threats
- Reducing log ingestion and indexer fees
- Tool consolidation

DATA BREACH VERIFICATION & FORENSICS

- Cost avoided by stopping exfiltration immediately
- Cost reduction of external auditors determining data breach impact
- Reduction in risk – cost savings

SIFT THROUGH DATA & DETERMINE ACTION

- Reduction in hours to investigate threats
- Capped operations expense to deploy and maintain tools
- Number of highly skilled analysis required in SecOps team
- Cost saved from reduced training
- Cost and risk saved through automation

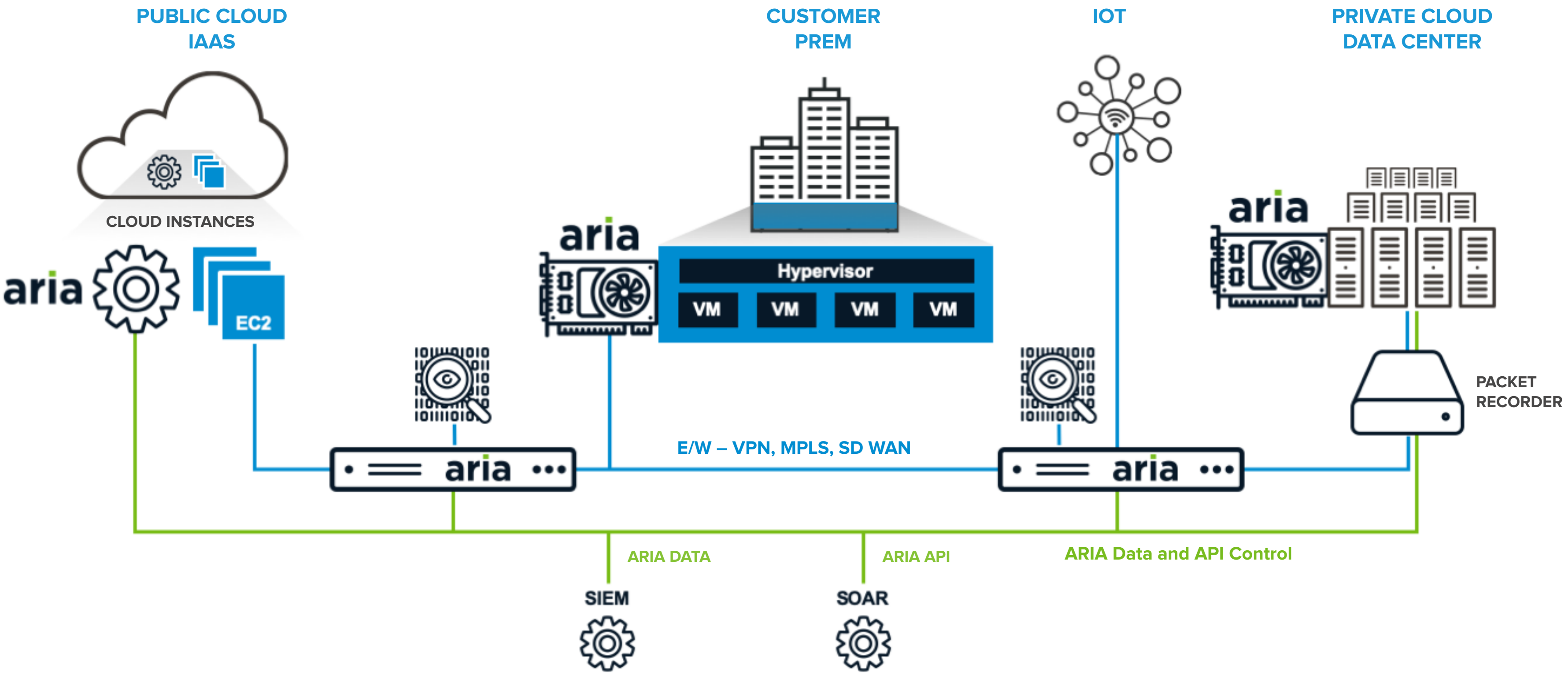
CONTAIN THREATS

- Cost of shutting down critical devices
- Cost of replacing IoT with EDR-capable devices
- Cost of ineffective and inefficient and microsegmentation solutions
- Cost of fragmented & slow remediation processes

Accelerated Incident Response and Enterprise-wide Protection

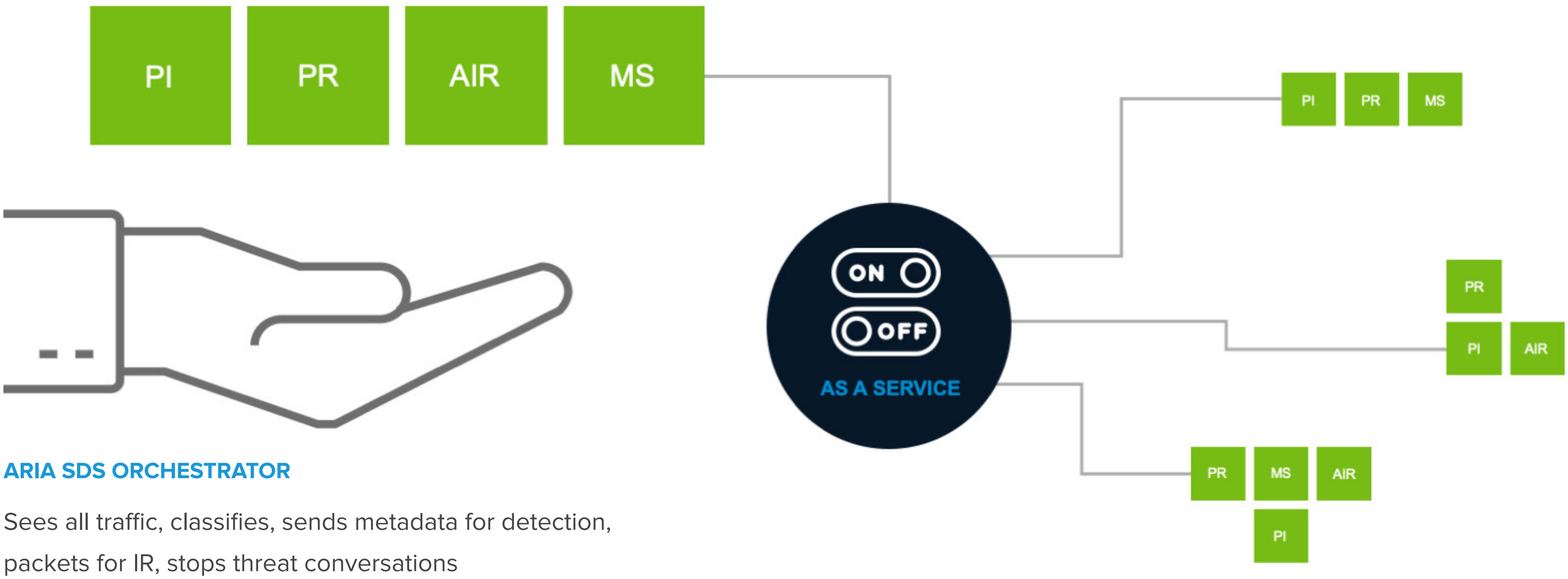
ARIA SDS orchestrates the security and protection of high-value critical assets from cyber attacks. It has become critical that any potential threats are detected and verified very quickly but given the fluid east-west communication paths, presented by the use of public cloud, data center and on-prem data and application stores this has proved extremely difficult as they create sizable gaps in network traffic visibility.

- ✓ Find and stop network-borne threats
- ✓ Improve performance of threat detection tools, such as SIEMs
- ✓ Surgically contain and disrupt validated intrusions, including IoT devices via the network
- ✓ Automatic deployment of security services, including microsegmentation to prevent further threats.



The Product Behind the Promise

The ARIA à la carte and on-demand approach to the deployment of security services and applications provides crucial missing elements for automated assistance.



ARIA SDS ORCHESTRATOR

Sees all traffic, classifies, sends metadata for detection, packets for IR, stops threat conversations

PACKET INTELLIGENCE

PI Sees all traffic, classifies, sends metadata for detection, packets for IR, stops threat conversations

PACKET RECORDER

PR Records selective packets sent by PI – for IR and compliance processes

AIR

AIR Automatically validates and notifies of breaches, enabling rapid investigation and response.

MICROSEGMENTATION

MS Applies and enforces connection policies from within the network

Integrated with Leading Technologies

We add significant value to industry-leading security vendors by providing east-west visibility and protection, and ultimately to filling the gaps in their product offerings and adding significant value to their solutions.

paloalto NETWORKS®

FORTINET®

Check Point® SOFTWARE TECHNOLOGIES LTD.

RSA

IBM

JUNIPER NETWORKS

splunk>®

DELL

DEMISTO

CISCO

vmware®

seceon

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.

Contact Us

sales@ariacybersecurity.com

800.325.3110

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA 01854

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

aria CYBERSECURITY SOLUTIONS

ariaSDS

nVoy SECURITY APPLIANCES

Myricom NETWORK ADAPTERS