aria CYBERSECURITY SOLUTIONS

DATASHEET

# ARIA SDS: Uncompromised Enterprise-wide Security

**With the proliferation of containers, virtual machines (VMs), and cloud instances, organizations are struggling to secure their most critical data. This is causing security teams to search for a comprehensive, yet simple solution to secure enterprise-wide data while also complying with data-privacy regulations.**

## Uncompromised Enterprise-wide Network Security

The ARIA Software-Defined Security (SDS) platform can secure and encrypt containers and/or VMs as they spawn in private data centers or in public cloud instances. With no manual intervention, the ARIA software automatically applies the appropriate contextually aware security policies.

### Benefits

**Impenetrable encryption key storage and execution:**

- Securely stored and executed on the SIA by leveraging the on-board HSM onboard
- Keys in use cannot be captured/stolen/lost

**Add strong encryption to new, or existing servers, with negligible use of CPU cores:**

- Run sustained 50G wire rate encryption on a per-app, per-tenant basis
- No reduction in performance or increase in response times when under load

**Multi-port 10/25G NIC capability:**

- Allow new or existing servers to run these services at 50G network wire rates

**Deploy with any application or SDDC architecture:**

- Works with containerized applications such as those running in VMs or on bare-metal servers
- Works with any SDDC architecture, including NSX

**Automatic, centralized control and management by the SDS Orchestrator:**

- Applies per-application or per-tenant encryption policies to each, groups of, or all SIAs
- Provides control capabilities for other security applications

**One-tenth the deployment cost:**

- As opposed to running software-based encryption capabilities on servers at 50G wire rate

The ARIA solution is implemented through a series of lightweight software-defined security instances (SDSi), which are deployed in all corporate environments – on-premise, private data center, or public cloud. These instances support a broad set of security policy enforcement services, including but not limited to:

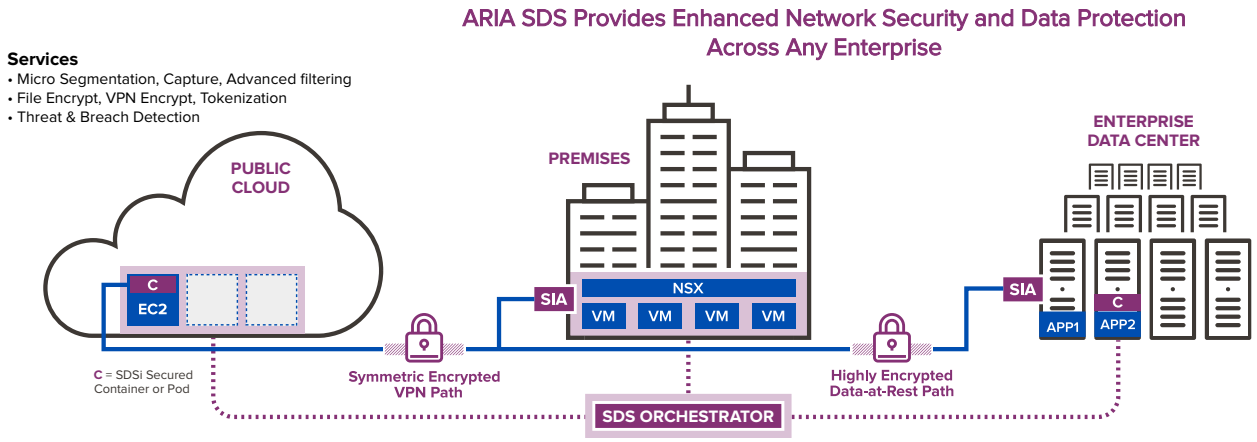
- Secure sourcing of containers and VMs
- Micro-segmentation control over what process and application can access what data, and from where
- Bulk encryption or applied per-application type, per tenant for data-at-rest or data-in-motion
- Format-preserving tokenization, which works within today's common database applications. This approach replaces actual customer data, often PII in nature, with format-preserving substitutes to avoid the prevalent concern of misuse or mistakes by operations staff.
- Selective deployment of software IDS, packet capture and classification, and recording of critical data conversations. This is critical for use in breach detection and record-exposure verification to ensure PII regulatory compliance.
- Security platform as a service—fool proof set of services for developers application to integrate with Security teams will be able to centrally set and locally enforce security policies at each instance from a single pane of glass. The ARIA Orchestrator (SDSo) will ensure that the SDSi are deployed with every server and cloud instance. The ARIA SDS will also control where VMs and containers are spawned, including which registries can be utilized and the conditions where protected data can be accessed. The SDSo will set-up a bulk policy and programmatically deploy and manage each instance as well as provide a place where the solution's analytics can be monitored, visualized, and reported from.

## The Collision of DevOps and IT

Across the board, organizations feel the urgency to move their business operations forward to support critical goals. One way to do this is to adopt an iterative and rapid approach to business application development. Yet as enterprises take on agile and more flexible DevOps practices, application vulnerabilities and data security issues become more challenging to combat. With the ARIA solution, resources are able to implement security policies across disparate public private cloud infrastructure in a timely and consistent methods. This ensures that proper security tools and controls are in place so that critical data and applications are fully secured.

## The Need to Secure Data at Rest, in Motion, and in Use

Up until now, security teams have had to balance data security against the speed and ease of business operations. However, securing data, no matter where it resides throughout the organization, only represents one side of the proverbial coin. There is still the concern of how to protect data as it moves across the network, including how it is accessed, stored, and used. The ARIA solution automatically, and uniformly, applies the appropriate encryption policies, whether by application, device, and/or data type accessed anywhere, under any use, and at any time. All of this is achieved with the highest throughput and at the lowest cost per processed bit.




## ARIA Advanced Security Applications

Application developers benefit from ARIA as it provides a security platform as a service, making it easy to leverage predefined security applications that can be called upon. This abstracts the need for in-depth knowledge of security practices and techniques, allowing for the proper, more foolproof application of services including, proper registry access, image verification, and per-application/per-tenant encryption services with appropriate key management provisioning—automatically applied.

Application and server performance will improve by offloading CPU-intensive functions, such as encryption, authentication, and key management onto CSPi's Myricom ARC Series Secure Intelligent Adapter (SIA). In addition to the application offload capabilities provided by the onboard ARM cores, this 10/25 Gb network interface card provides a secure zone of trust to store and run the encryption keys. The Myricom SIA ensures that organizations will be able to dramatically reduce server costs and protect the use of the keys during encryption. For the highest level of security, ARIA allows a direct integration to any third-party key management system. Deployment of the SIA, like that of the SDSi itself is zero touch. SIA cards can be installed in the infrastructure and will be enabled and configured automatically by the ARIA Orchestrator (SDSo).

## Be Confident in Your Network Security

The ARIA SDS solution improves server performance, enables efficient and effective centralized security management – all while having little to no impact on business operations. Security teams can implement the right security for their critical data, allowing rapid scale, deployment, and management of their business data, whether it is on-premise or in a public cloud. Central execution of the correct access controls, micro segmentation, encryption service types and levels, and tokenization techniques protect when accessed within, or between, data centers and public clouds.

ARIA allows organizations to embrace the flexibility and efficiency offered by DevOps models and provides the policy enforcement and instrumentation to manage the policies which IT and security staff need, but not impact the performance developers and operations demand.

**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 O1854**

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

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS