aria CYBERSECURITY SOLUTIONS

DATASHEET

Myricom SIA Advanced Server Offloading for Data Security Tasks

CSPi's Myricom® Secure Intelligent Adapter (SIA) can improve server and application performance by offloading a variety of core-intensive functions.

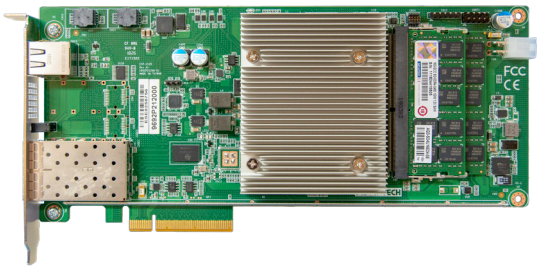
The Myricom SIA can also run native applicationsw, including third-party applications developed for the Intel x86 processor, on its ARM cores. The Myricom SIA can also host any of the ARIA Software-Defined Security (SDS) applications, which are designed to enhance network security, perform key management and packet capture, and offload encryption functions.

Myricom SIA benefits

- **Enjoy easy installation and configuration:** ARIA SDS orchestrator offers zero touch configuration capabilities; apply per-application or per-tenant policies to each, groups of, or all SIAs.
- **Increase network throughput:** Achieve performance boosts for critical security applications.
- **Avoid server replacement costs and hassles:** Add Myricom SIA to existing infrastructure instead of replacing servers, at 1/10th the cost. This provides additional performance and increased network throughput.
- **Secure encryption keys:** Myricom SIA provides onboard TrustZone to store and serve keys—and keep them safe from a breach.

The best way to offload server-intensive functions

The Myricom SIA combines the functionality found in a next-generation high-speed network adapter with the programmability of a multi-core ARM processor to provide flexible application-specific feature support. The capabilities of this 10 or 25GB dual port adapter card opens new possibilities for accurate threat detection and disruption, such as allowing new or existing servers to run security services at 50G network wire rates without impacting network performance.



Features and capabilities of the Myricom SIA include:

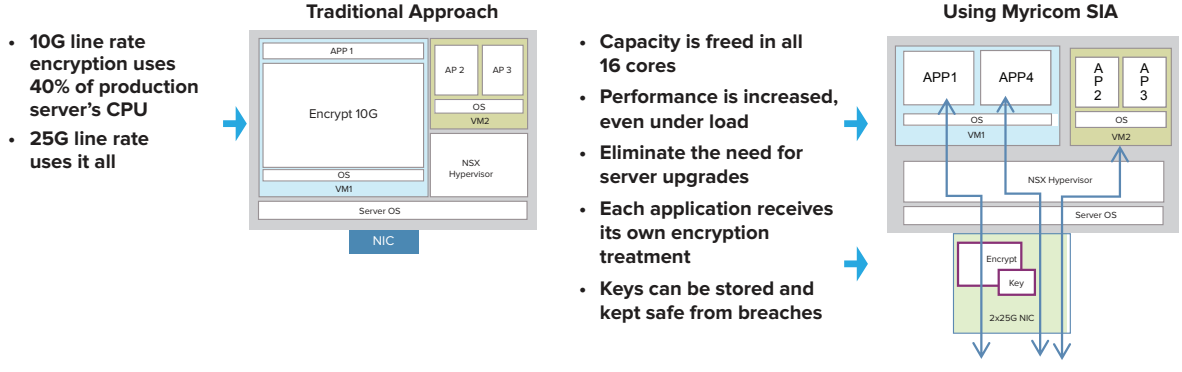
- Line rate packet capture (PCAP) without dropping any traffic
- Support for, and the acceleration of, various security functions, such as symmetrical and a symmetrical encryption
- Line rate packet classification
- Deep packet inspection (DPI)
- Flow generation
- Deep multi-rule filtering

The Myricom SIA also provides a local secure zone of trust to store and run the encryption keys, which is also referred to as TrustZone. This execution environment prevents the exposure of encryption keys in the event that the host server is breached.

A new approach to overcome traditional challenges

One of the biggest benefits of the Myricom SIA is its ability to offload server-intensive operations, such as those found in Internet protocol security (IPsec) encryption. Consider these potential scenarios:

- At 10G, IPsec could use up to 40% of a 16-core, high-end production server's CPU.
- Latency of production applications can vary dramatically with encryption load.
- At 25G, IPsec could consume all of a 16-core server's CPU.
- Offloading these tasks to the NIC frees CPU cycles for improved processing and performance.



Additional advantages

Leveraging the SIA for server offload allows organizations to dramatically reduce costs when adding advanced security applications that are distributed into server infrastructure. This is an advantage over deploying heavy-weight, server-based security applications that compete for server cores and rob performance and response time when the device is under load.

We provide a software development kit (SDK) for those organizations and OEMs that require the ability to run third-party applications within their own offerings. The SDK allows the Myricom SIA to act as a standalone system or as an intelligent IO subsystem to manage pre- or post-processing data coming in or out of a host device.

Also, to improve application performance, an application offload development kit is available that allows applications to offload specific compute-intensive workloads from the server host CPU onto the ARM cores of the SIA. This includes leveraging the ARM cores' TrustZone in which to run or boot processes that need to be secured, such as compressing, encrypting/decrypting, and monitoring application output. Such functionality can work across the host PCIe bus, allowing such services to be provided as required by virtual machines (VMs) or microservices running within or outside the physical host server.

The programmability of the SIA allows it to take on additional workloads based on evolving security needs. In addition to crypto acceleration (including VPN, storage, encryption, tokenization, and more), many other network and security solutions and services (e.g., firewalls, IDS, packet capture, DPI, deep rule-based filtering, application routing, reverse proxy, etc.) can run concurrently on the SIA, reducing the need to rack separate appliances. Significant datacenter power saving can be realized using this approach.

For organizations that leverage OVS or the VMware NSX architecture, Myricom SIA allows access to specific traffic flows between any VM (intra-server or inter-server) to take advantage of the ARIA security features. OVS or NSX installations leveraging SIA functionality can experience a tenfold improvement in application performance by offloading key functions such as encryption and key management.

MYRICOM SECURE INTELLIGENT ADAPTER KEY SPECIFICATIONS	
Bus Interface	PCI Express Gen 3, 8 lanes wide
Form Factor	PCI Express Full Height, 3/4 Length
Electrical Power	Less than 70W with transceivers installed
Environmental	If used in a datacenter environment, CSPi recommends that adapters be installed into servers that provide airflow over the PCIe slots.
Throughput	Support for dual-port (25G) lossless packet transfer. Sustained 50G wire rate encryption
Timestamps	TXCO for stable nanosecond resolution timestamps with support for PTP
Processor	16 Cores @ 2.0GHz
Memory	8-32GB DDR4 64GB Flash
Software Support	Drivers available for Linux (CentOS, RHEL, and Ubuntu) Supports DPDK for Linux (high-performance packet processing) Support for SR-IOV for VM Isolation Support for OVS Host-side driver support for Linux and Windows Low latency and high message rate Network overlay offloads for NVGRE, VxLAN, and MPLS encapsulated traffic High performance network storage with full protocol offloads for iSCSI, iSCSI Extensions for RDMA (iSER) to support NVMe, and FCoE Support for Symmetric and Asymmetric Encryption algorithms Support for RSS and TSO
Network Connectivity	Dual SFP+/SFP28 ports; 10 or 25G use
OTHER DETAILS	
Warranty and Support	One year for hardware. Refer to the support datasheet for support offerings and provided services.

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.

CSPi Cybersecurity Products • 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