# 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.

Alternatively, it can run native applications, 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.

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, without impacting network performance.
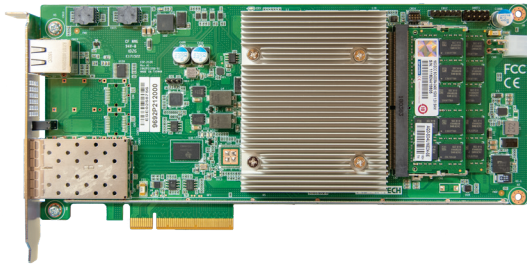
Features and capabilities of the Myricom SIA include:

- Line rate packet capture (PCAP) without dropping any traffic

- Support for, and the acceleration of, various security functions, such as symmetrical and asymmetrical 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.

Benefits:

- **Multi-port 10 or 25G NIC capability**

  Allow new or existing servers to run security services at 50G network wire rates with no performance penalties.

- **Multiple uses cases**

  The ARM cores can intercept traffic from the network side (wire) or the host side (PCI) and perform processing on it.

- **The ability to add strong security applications to new or existing servers with negligible use of CPU cores**

  Myricom SIA provides real-time east-west threat detection and prevention and crypto services with zero host CPU or application performance impact.

- **Impenetrable encryption key storage and execution**

  Keys can be securely stored and executed on the SIA by leveraging on-board HSM functions.

  Keys in use cannot be captured, stolen, or lost.

- **One tenth the deployment cost**

  Take advantage of significant savings as opposed to running software-based encryption capabilities on server at 50G wire rate.

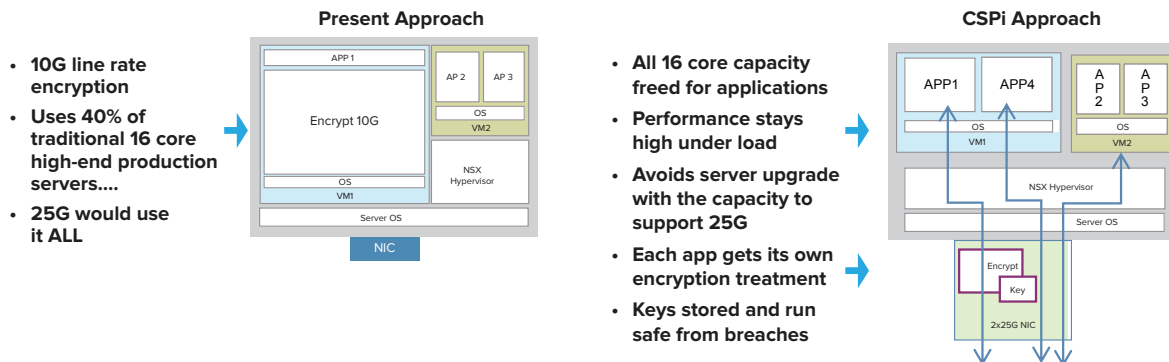- **Automatic, centralized control and management by the SDS Orchestrator**

  Applies per-application or per-tenant policies to each, groups of, or all SIAs.

  Can provide programmatic control of any applications running on the SIA cores.

FEATURES

One of the biggest benefits of the Myricom SIA is the ability to off-load server-intensive operations, such as those found in IPSEC encryption:

- 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.

- 25G could consume all of a 16-core high-end production server's CPU.

- Offloading this task to the NIC allows the recovery of CPU cycles for application's processing use.

Present Approach

- **10G line rate encryption**
- **Uses 40% of traditional 16 core high-end production servers....**
- **25G would use it ALL**

APP 1
AP 2 AP 3
OS
VM2
Encrypt 10G
NSX Hypervisor
OS
VM1
Server OS
NIC

CSPi Approach

- **All 16 core capacity freed for applications**
- **Performance stays high under load**
- **Avoids server upgrade with the capacity to support 25G**
- **Each app gets its own encryption treatment**
- **Keys stored and run safe from breaches**

APP1 APP4
A P 2 A P 3
OS
VM1
OS
VM2
NSX Hypervisor
Server OS
Encrypt
Key
2x25G NIC

Leveraging the SIA for server offload allows organizations to dramatically reduce costs when adding advanced security applications that are distributed into sever 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 from production applications.

A software development kit (SDK) is available 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 assist in improved application performance, an application offload development kit is available to allow 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' trust zone 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 data center power saving can be realized using this approach.

For organizations that leverage OVS or the VMware NSX architecture, 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 to a Myricom SIA network adapter. CSPi's ARIA SDS solution allows security policies to be bridged beyond NSX domains into containerized or other DevOps worlds in the public as well as private cloud infrastructures.

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 CSPi

CSPi (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPi Corporate Headquarters
175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPi High Performance Products
800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPi Technology Solutions
800.940.1111
us-ts-sales@cspi.com

www.linkedin.com/company/csp-inc   @ThisIsCSPi   us-hpp-sales@cspi.com   www.cspi.com