SOLUTION BRIEF

LOW-LATENCY PERFORMANCE FOR DEMANDING EDGE WORKLOADS

Supermicro SYS-110D-FRDN8TP Accelerates Deployment of SASE Workloads and Supermicro SYS-211SE-31A Delivers Secure Container Tracking System for Maritime Ports

SYS-110D-8C/14C-FRDN8TP

SYS-211SE-31A

TABLE OF CONTENTS

Executive Summary

Processing data at the network edge, close to its point of origin, enables low-latency apps and services while also reducing backhaul bandwidth costs. However, enterprise architects must meet the following challenges when designing edge computing solutions:

- Provide robust, scalable compute at remote locations, including demanding edge workloads such as artificial intelligence (AI)/deep learning and analytics.
- Protect the expanded attack surface created by distributed services and work-from-home scenarios that operate outside any network perimeter.
- Deliver a cloud-native implementation that supports transformation with ease of use and agility through cloudification of the edge.

Supermicro, along with partners such as Intel®, has created two solutions for cloud-native applications at the edge.

Solution1: SYS-110D-8C/14C-FRDN8TP is a verified Intel Select Solution for SASE workload-optimized server solution based on the operating system(s) Red Hat/ Canonical Ubuntu that eases interoperability and speeds deployment.

Solution 2: SYS-211SE-31A is a verified container tracking application with Zscaler, Rafay, and Supermicro collaboration to create multi-access edge compute solutions and deployed ISSD ConScan to demonstrate the application with security service edge and orchestration capabilities.

Solution 1: Overview and Benefits

To serve this market, Supermicro has chosen to partner with Intel to develop and launch its SYS-110D-14C- FRDN8TP and SYS-110D-8C-FRDN8TP (https://www.supermicro.com/en/products/system/iot/1u/sys-110d-8c-frdn8tp) as a verified Intel Select Solution for SASE. Converging software-defined WAN (SD-WAN) network services with cloud-hosted security services, Intel Select Solutions for SASE provide pre-validated blueprints for edge compute points of presence based on Intel Xeon® D-2700 processors that lower the barriers to implementation and speeds deployment.

- High core counts and per-core performance ensure remote workloads have reliable, optimized computational throughput with agility, flexibility, and excellent ROI.
- Compact, power-efficient system-on-chip (SoC) platform with integrated accelerators and Ethernet, with networking accelerated by Remote Direct Memory Access (RDMA) and Dynamic Device Personalization (DDP).
- Streamlined path to cloud-native operations, replacing hub-and-spoke topologies that made data centers choke points with multi-cloud ones that embrace modern approaches such as microservices and DevOps.
- Accelerated AI inference using Intel Deep Learning Boost (Intel DL Boost), which eliminates unneeded precision in calculations so they can be completed more quickly.
- Accelerated encryption and compression to reduce workload overhead with enhanced Intel AES New Instructions (Intel AES-NI) and integrated Intel QuickAssist Technology (Intel QAT).

Servers Used	**Base Configuration**	**Plus Configuration**
Server Name	SuperServer SYS-110D-8C-FRDN8TP	SuperServer SYS-110D-14C-FRDN8TP
Processor	Intel Xeon D-2733NT Processor 8C/16T, TDP 80W	Intel Xeon D-2766NT Processor 14C/28T, TDP 97W
Memory	32GB	64GB
Intel QAT	Yes	Yes
Intel Ethernet option	4x 1GbE 2x 25GbE SFP28 2x 10GbE Base-T	4x 1GbE 2x 25GbE SFP28 2x 10GbE Base-T
Storage (NVMe / SATA)	256GB NVMe M.2 2280 Supports 2x Internal 2.5" drive bays (2x PCIe 4.0 NVMe x8 SlimSAS and 1x OCuLink options) 1x M.2 M-Key 2242/2280 (SATA/PCIe 3.0 x4)	512GB NVMe M.2 2280 Supports 2x Internal 2.5" drive bays (2x PCIe 4.0 NVMe x8 SlimSAS and 1x OCuLink options) 1x M.2 M-Key 2242/2280 (SATA/PCIe 3.0 x4)

Why Intel® Select Solutions for SASE?

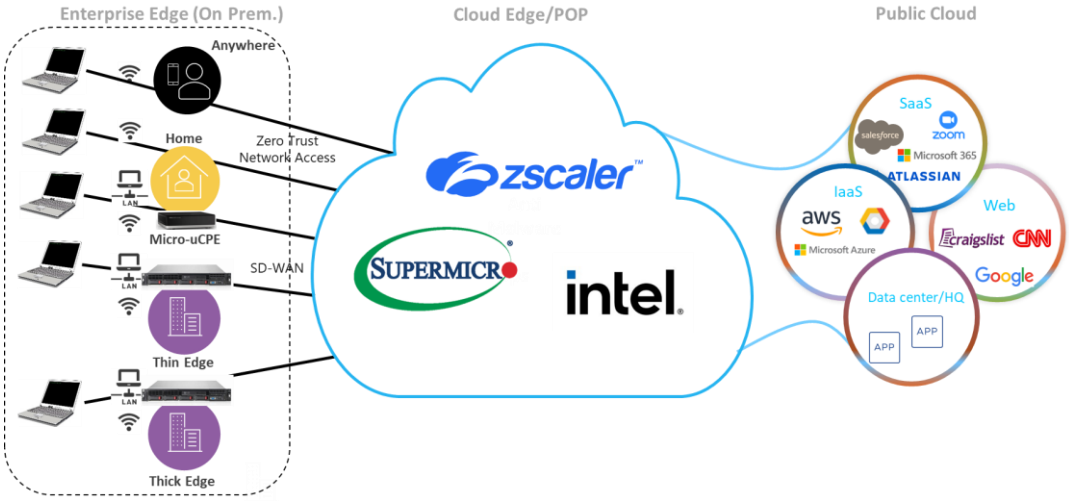


Figure 1 – Intel Select Solution for SASE for robust cloud-first initiatives that combine enterprise distributed networking and security services.

Benefits of Intel Select Solutions for SASE:

Intel Select Solutions for SASE provides a pre-validated solution blueprint that accelerates the time to production for robust cloud-first initiatives that combine enterprise distributed networking and security services.

- Superior performance for crypto and AI inference, boosting throughput with Intel QAT for public key exchange & cryptography acceleration, and crypto and AI inference instruction set architecture enhancements, silicon-integrated accelerators, and PCI Express add-in accelerator cards.
- Distributed, cloud hosted security services based on containerized network functions bound to individual workloads as they traverse private, public, and hybrid clouds.
- Enabler of cloudification at the edge, creating a converged, standards-based infrastructure based on containers and microservices that maintains high levels of performance and security.
- Software consistency with Intel Atom® and Intel® Xeon® Scalable Processors, with back-compatibility and a single standard architecture for Cloud Native and network functions virtualization infrastructure (NFVI).

Solution 2: Overview and Benefits

The chances are good that the item you ordered with next-day delivery started its journey to you months before on a ship and came to you through a maritime port.

According to the United Nations Conference on Trade and Development, ships carry 80%[1] of global trade volume, including food and farm products, fuel, forest products, iron and steel, clothing, shoes, electronics, toys, and cars. This makes ports a crucial connection to supply chains around the world.

The importance of maritime ports makes them a constant target of cyber criminals and hackers that want to steal goods or disrupt operations. The impact of a significant successful attack could be immense; insurance provider Lloyds reports that a single cyber-attack on ports in Asia could cost $110 billion[2].

Improving cyber security is a top priority for ports. Working with other partners, Intel is addressing this challenge by developing secure multi-access edge (MEC) solutions powered by 4th Gen Intel® Xeon® Scalable processors. One use case for this MEC solution is Marine Ports Container ID Recognition and Scanning, which scans shipping container identification information at the points of ingress and egress to the port and as they move through the port. This data is then used to track containers and to know if they are being misdirected, stolen, or lost. In addition, the MEC server that is the basis of this application supports security features to significantly inhibit cyber thieves from accessing or manipulating the data.

Figure 2 – The ConScan Container and Truck Identification Recognition and Tracking System Output

[1] https://unctad.org/publication/review-maritime-transport-2022

[2] https://www.lloyds.com/about-lloyds/media-centre/press-releases/cyber-attack-on-apac-ports-could-cost-110bn

A demonstration of this application was organized by Intel using ISSD ConScan as the workload and including Rafay for application orchestration. Zscaler provided Zero Trust Network Access to enable a secured environment, and Supermicro provided the compute platform.

Why Track Containers with ConScan?

The workload in this demonstration is ConScan, a marine port container ID recognition system from Integrated Systems and Systems Design (ISSD). The software automatically collects container information while transiting through the port. The software aggregates video streams from multiple cameras throughout a port and uses image processing technology and storage of collected data to track containers. ConScan is designed for complex and constantly moving port environments. This requires a highly automated solution with advanced data analysis.

All collected information is recorded in real time and is accessible to port staff and shippers via a web interface. As a result, ConScan reduces the need for humans at entrances and checkpoints and ensures containers are routed to the appropriate loading docks and ships.

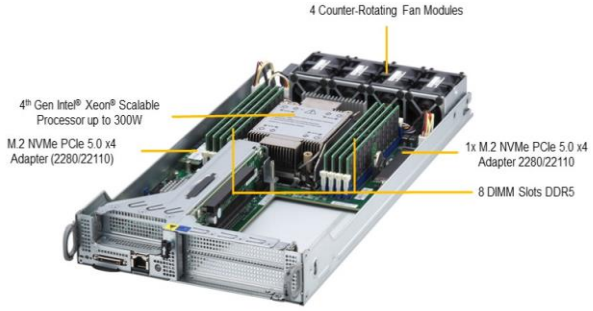
	Base Configuration
Server Name	SuperServer SYS-211SE-31A
Processor	4th Gen Intel® Xeon® Scalable processors Supports 85W - 300W TDP CPUs
Memory	Up to 2TB: DDR5
Intel Ethernet option	1 RJ45 GbE LAN port (shared with IPMI)
Storage	2 M.2 NVMe M-Key, 2280/22110

Supermicro MEC Server Uses Latest Intel CPUs

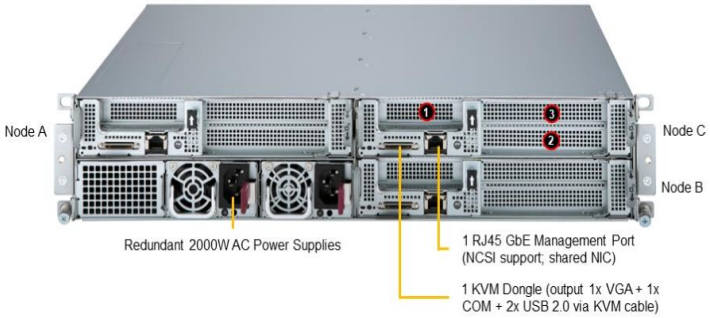
Supermicro provides the IoT SuperServer SYS-211SE-31A (https://www.supermicro.com/en/products/system/iot/2u/sys-211se-31a) servers powered by 4th Gen Intel Xeon Scalable processors with connectivity provided by the Intel® Ethernet 800 Series network adapters.

The 4th Gen Intel Xeon Scalable processor accelerates performance across the most demanding workloads. The new processor combines high-performance processor cores with up to eight built-in accelerators to help improve performance and processing efficiency for demanding workloads like cryptographic and artificial intelligence acceleration.

The Intel 800 Series Network Adapters improve application efficiency and network performance with innovative and versatile capabilities that optimize high-performance server workloads. The Intel 800 Series Network Adapters deliver bandwidth and increased application throughput required for demanding cloud workloads and provide packet classification and sorting optimizations for high-bandwidth network and communications workloads.



SYS-211SE-31A-Single Node



SYS-211SE-31A

Rafay Automates Edge Network Server Lifecycle

The MEC server in the container ID demonstration uses Rafay's Kubernetes Operations Platform (KOP) for Edge, a Software-as-a-Service (SaaS) platform for managing cloud-native edge network infrastructure. KOP for Edge is part of a family of SaaS platforms designed to simplify the lifecycle management of Kubernetes clusters and applications located in data centers, public clouds, or at the edge.

Benefits of KOP for Edge

- Network administrators can centrally manage the full lifecycle of their Kubernetes clusters and applications at remote edge locations, such as maritime ports.
- KOP for Edge integrates so-called "stovepipe" services such as continuous deployment (CD), logging, monitoring, policy management, authorization, and backups.
- The KOP for Edge interface is designed to deploy these integrated services in minutes via the cloud.
- KOP for Edge simplifies the deployment of Kubernetes in an edge network by providing central management of the infrastructure and applications each edge site depends on.
- Rafay's KOP for Edge delivers centralized, policy-based management, automation, standardized operations, and advanced security.

Key features of Rafay Kubernetes Operation Platform (KOP) for Edge:

- Multicluster Management
- GitOps Pipelines
- Zero Trust Access
- K8s policy management
- Backup and restore

- Visibility and monitoring

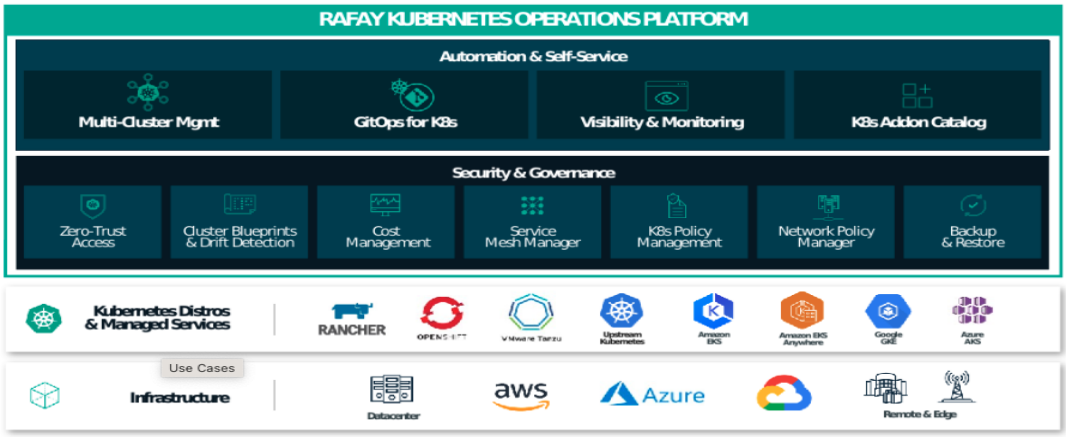


Figure 3 – The KOP platform offers lifecycle management services to a wide variety of Kubernetes distros and can be delivered via the most popular public data center providers

Creating the Secure Demonstration MEC Server

The architecture of the solution built for the Marine Ports Container ID Recognition and Scanning is shown in the Figure below.

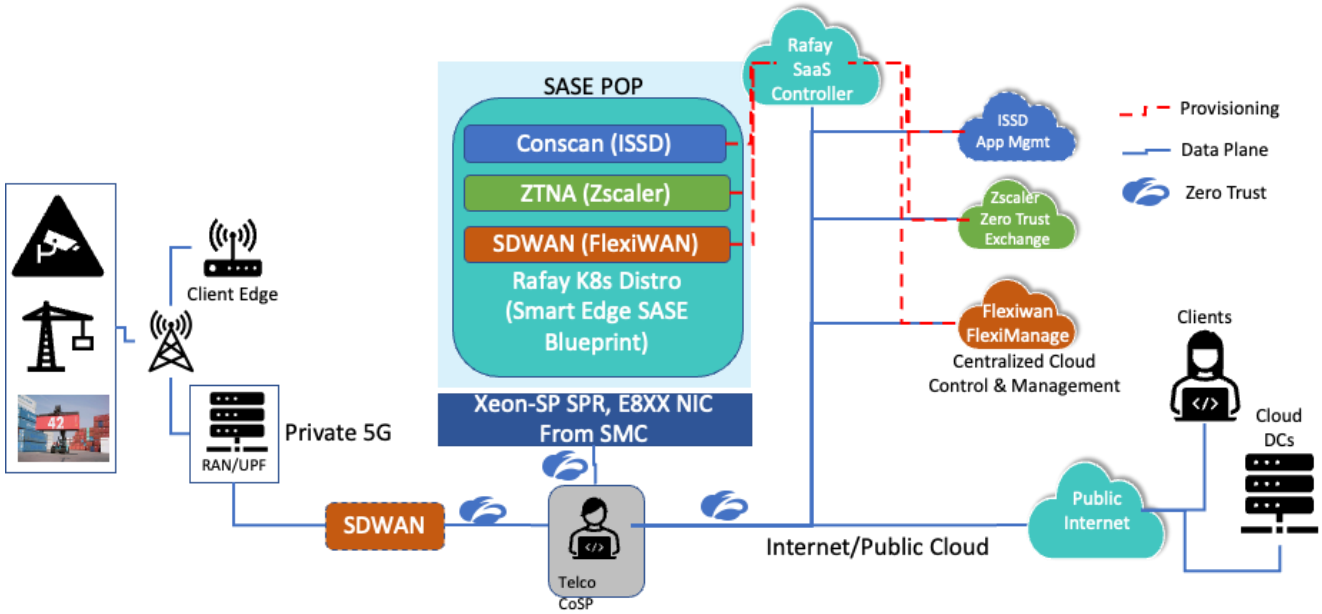


Figure 4 – The MEC server in the center of this figure is a security enabled Intel architecture server with remote management running a container scanning workload.

The ConScan application is the basis for the Marine Ports Container ID Recognition and Scanning server scans video streams from designated security cameras. In addition, it can isolate containers and record their identification information.

Benefits of ConScan:

A single ConScan deployment will support up to 256 cameras and scanners throughout the property, with cameras at each entry and exit point. The ConScan program will scan a container and track it through the port until it is either loaded on a ship or on a truck exiting the Port for local delivery.

Orchestrating the computer systems in a port environment is a challenge because ports are distributed and disaggregated, providing the potential for a large attack surface that is easy to infiltrate. Zscaler helps eliminate that risk. Server maintenance and ongoing patches and updates are critical components of securing the system. The Rafay KOP for Edge product is designed for the comprehensive and secure provision of software from a central control point. The software running on the computer systems can be maintained in an automated fashion using the Rafay platform.

Since a port is a location that has many moving parts and can cover a very large footprint, it is not reasonable to house IoT systems in a controlled data center environment with standard off-the-shelf rack mount servers. As a result, the computers required to support these devices and use cases must be designed for rugged environments and have the compute resources to support high demand processes. The Supermicro SuperServer platforms using the Intel Xeon processors are designed for such deployments. Additionally, these systems can be deployed in hardened cases that reside throughout the port to ensure reliable processing of ConScan data.

Zscaler Zero Trust SD-WAN:

One requirement is to establish zero trust access for all the cameras and scanners that connect to the ConScan application. With the Zscaler Zero Trust Exchange, all IoT devices and clients were authenticated and authorized before connecting to the application.

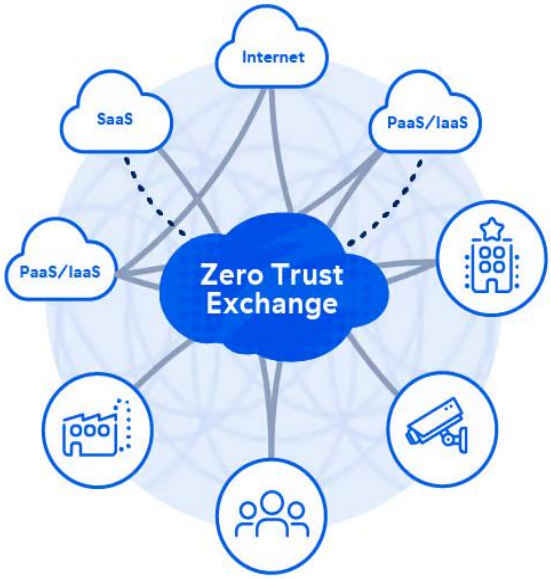


Figure 5 – The Zero Trust Exchange from Zscaler directly connects users with devices, applications, and machines reducing the cyber-attack surface.

Benefits of Zscaler:

- Reduced attack surface**:** By making apps visible only to authorized devices, the Zero Trust Exchange eliminates those apps from an organization's attack surface.
- Users connected to apps, not the network: The Zero Trust Exchange connects users directly to apps, providing a fast user experience and reducing latency by eliminating the need to backhaul traffic through centralized security controls.
- Proxy, not passthrough, architecture: Passthrough security applications can get bogged down by inspecting TLS/SSL-encrypted traffic, which is the vast majority of all traffic. The Zero Trust Exchange proxy architecture is designed for full content inspection, including encrypted traffic at scale, providing fast throughput and enabling effective cyber threat protection and data loss prevention.
- Secure access service edge: The secure access service edge (SASE) is defined as a framework for securely connecting users and machines to apps and services without regard to the device's physical location. As a SASE-based solution, Zero Trust Exchange can enforce policy at the edge and/or distributed across data centers globally.
- Multitenant Architecture: Zero Trust Exchange is built on a multitenant cloud architecture to provide the scalability to meet the growing security needs of the increasingly interconnected world.

Summary

With the SYS-110D-8C/14C-FRDN8TP verified as an Intel Select Solutions for SASE, Supermicro is delivering a differentiated Intel Xeon D-2700 processor based platform that can simplify and accelerate the process of selecting and deploying the hardware and software needed for today's enterprise edge workloads and applications. Intel Select Solutions for SASE represent the latest technology that will accelerate the transformation of the network from end to end.

With the SYS-211SE-31A verified as a marine port container ID recognition system, it is one of several "smart" use cases increasingly used in industry, cities, schools, and other public-facing organizations. However, all these smart use cases with the large number of IOT devices feeding and communicating information are prime targets for hackers who pose a real threat to the economy and people's private information. The MEC solution specified in this application has the performance, security features, and remote lifecycle management capabilities to be deployed in various use cases. In addition, it provides a security posture that significantly reduces the attack surface that hackers exploit.

Intel and its partners have demonstrated a streamlined approach to securing these use cases. We encourage further exploration and engagement for you to set up a SASE POP-based service or a marine port container ID recognition system on our servers. Reach out to us to set up an evaluation for your use case.

Learn More

To find out more about Supermicro Solutions, visit www.supermicro.com

https://www.supermicro.com/en/products/system/iot/1u/sys-110d-14c-frdn8tp
https://www.supermicro.com/en/products/system/iot/2u/sys-211se-31a

Intel Select Solutions: intel.com/selectsolutions
Intel: https://networkbuilders.intel.com/intel-technologies/intel-select-solutions/secure-access-service-edge

Zscaler: https://www.zscaler.com/resources/data-sheets/zscaler-zero-trust-sd-wan.pdf

RAFAY

Rafay delivers an enterprise-grade Kubernetes operations solution that enables companies to deploy and operate clusters and modern applications across data centers, public clouds, and edge environments. Rafay's Kubernetes Operations Platform is built from the ground up to add enterprise-class automation, security, visibility and governance capabilities to your infrastructure. Learn more at https://www.rafay.co

CONSCAN

The ConScan solutions facilitate and speeds up terminal-related works like always moving port environment, while reducing operating costs. This is achieved via a comprehensive data detection and storage service focused on Container identification data, images of the right, left and rear sides of the containers and trailer and truck number plate images, and information. Learn more at: https://www.issd.com.tr/en/46652

SUPERMICRO

As a global leader in high performance, high efficiency server technology and innovation, we develop and provide end-to-end green computing solutions to the data center, cloud computing, enterprise IT, big data, HPC, and embedded markets. Our Building Block Solutions® approach allows us to provide a broad range of SKUs, and enables us to build and deliver application-optimized solutions based upon your requirements.

ZSCALER

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform.