Solution Brief

Infrastructure Architects, Systems Administrators, DevOps, FinOps, Operations Managers
IOT Edge, Ports, Telco, SASE, Enterprises, Industrial, Healthcare

Intel Delivers Secure Container Tracking System for Maritime Ports

Intel partners including Zscaler, Rafay and Supermicro to create multi-access edge compute solutions and deploy ISSD ConScan to demonstrate container tracking application with security service edge and orchestration capabilities

The chances are good that an item you ordered with next-day delivery started its journey to you months ago in a shipping container.

These containers get loaded at factories, they may be sent to a dry port for staging, are sent to a cargo terminal, and then loaded onto a ship. From the ship to you there is a similar process. Each stage of the process can have a detrimental impact on the supply chain costs and the economy. A transformation of the supply chain is occurring to automate logistics operations to reduce cost and boost productivity. This paper will illustrate how secured artificial intelligence and visual computing is assisting in this transformation.

According to the United Nations Conference on Trade and Development, ships carry 80%[1] of the volume of global trade 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 who want to steal goods or disrupt operations. The impact of a significant successful attack could be immense; insurance provider Lloyds estimated that a single cyber-attack on maritime ports in Asia could cost $110 billion[2]. As such, many countries consider maritime ports to be critical national infrastructure[3].

Improving cyber security is a top priority for ports. Intel, working with its partners, is addressing this challenge by developing secure multi-access edge (MEC) solutions that are powered by 4th Gen Intel® Xeon® Scalable processors. One key use case for this MEC solution is container ID recognition and scanning at maritime ports. This solution scans shipping container identification information at the points of ingress and egress to the port and as they move through the port. This data can be used to track containers and to know if they are being mis-directed, stolen, or lost. The MEC server that is the basis of this application supports security features to significantly inhibit cyber thieves from accessing or manipulating the data – this being a key attack vector capable to doing everything from surveilling cargo movement to disrupting port operations.

A demonstration of this maritime port solution was organized by Intel using ISSD ConScan as the workload and Rafay for application orchestration. Zscaler provided zero trust cybersecurity and Supermicro provided the compute platform. Here's what each company contributed to the demo:

Tracking 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 information from containers while they are transiting through

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 always moving port environment. This requires a highly automated solution with advanced data analysis.

The ConScan solution facilitates and speeds up terminal-related works 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
- Trailer and truck number plate images, and information

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

Figure 1. The ConScan container and truck identification recognition and tracking system output.

Zero Trust Security from Zscaler

Application security is provided by the Zscaler Private Access and Zscaler Zero Trust Exchange which is a cloud- and edge-delivered zero trust network access (ZTNA) service connecting users, workloads, and devices (see Figure 2). Zscaler ZTNA reduces the security risks and complexity associated with conventional perimeter-based security solutions.

The Zero Trust Exchange is built around five core attributes:

- **Reduced attack surface:** By making apps visible only to devices that are authorized to use them, the Zero Trust Exchange significantly reduces the attack surface of applications. In the maritime port solution, this means attackers would be unable to locate or attack the protected applications on the port networks.
- **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 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 cyberthreat 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. This allows all parts of the solution to be located where they are more cost effective to deploy (e.g., edge, regional data center, private cloud, and/or public cloud). The same high level of security is maintained for all components.
- **Multi-tenant Architecture:** Zero Trust Exchange is built securely on a multitenant cloud architecture to provide the scalability to meet the growing security needs of the increasingly interconnected world.

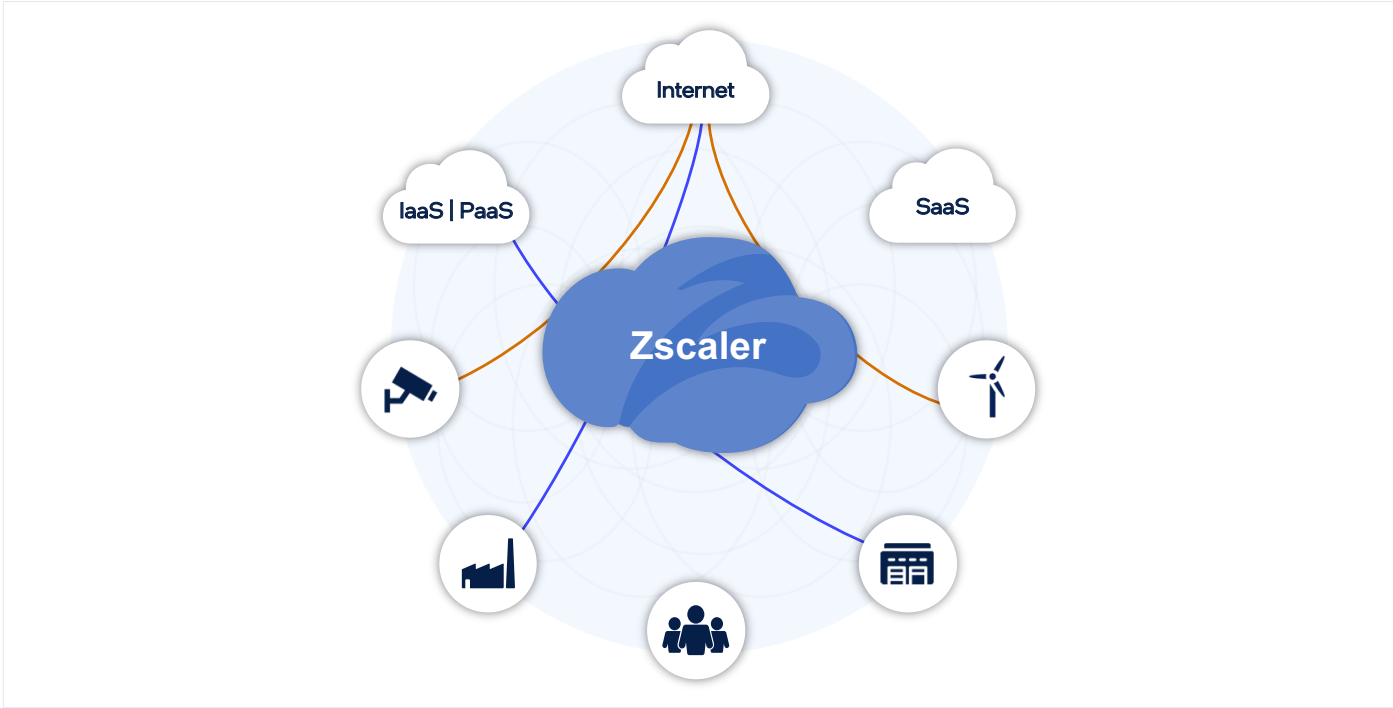

Figure 2. The Zero Trust Exchange from Zscaler directly connects users with devices, applications and machines reducing the cyber-attack surface.

Rafay Automates Edge Network Server Lifecycle

The MEC server used in the container ID demonstration, uses Rafay's Kubernetes Operations Platform (KOP) for Edge, which is 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 that are designed to simplify the lifecycle management of Kubernetes clusters and applications located in data centers, public clouds or at the edge.

With 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 KOP for Edge can be seen in Figure 3.

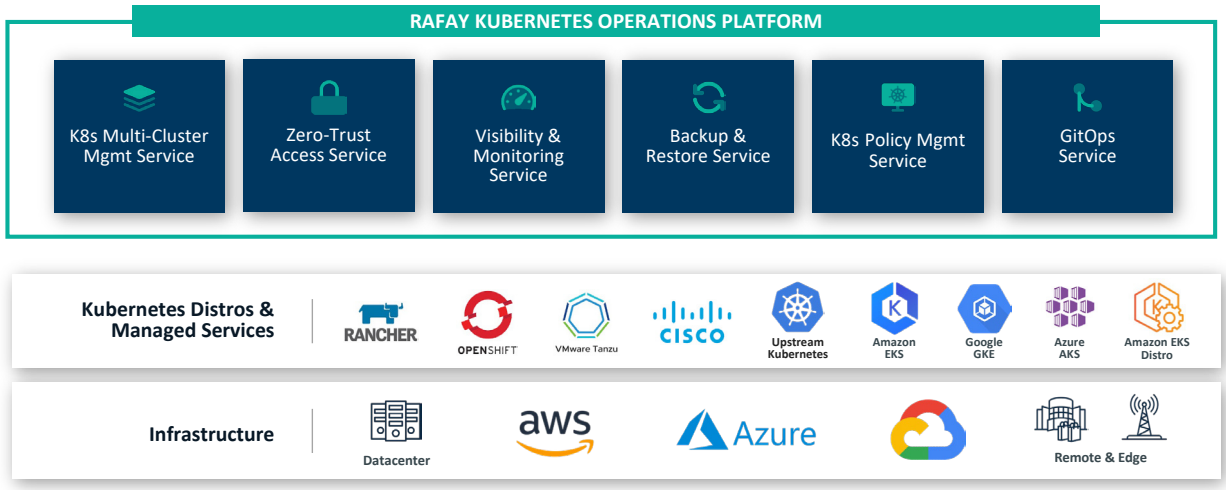

Figure 3. The KOP platform offers lifecycle management services to a wide variety of Kubernetes distros and can be delivered via the most popular public data center providers.

Supermicro MEC Server Uses Latest Intel CPU

Supermicro provides the IoT SuperServer SYS-211SE-31A servers that are powered by 4th Gen Intel Xeon Scalable processors with connectivity provide 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 Ethernet 800 Series Network Adapters improve application efficiency and network performance with innovative and versatile capabilities that optimize high-performance server workloads. The Intel Ethernet 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.

The SuperServer SYS-211SE-31A uses both the processor and the network adapter in a 2 RU-high rack mount form factor that contains three single-socket server sleds. This design is ideal for MEC use cases being deployed on the edge. Each sled can support up to 2TB of DDR5 memory, features 2 PCIe Gen5 x16 FHHL slot and 1 PCIe Gen5 x16 HHHL slot with 2 NVMe M.2 storage bays. The high availability system comes with redundant power supplies.

Figure 4. Front view of the SuperServer SYS-211SE-31A powered by 4th Gen Intel Xeon Scalable processors.

Creating the Secure Demonstration MEC Server

The architecture of the solution built for the Marine Ports Container ID Recognition and Scanning can be seen in Figure 5.

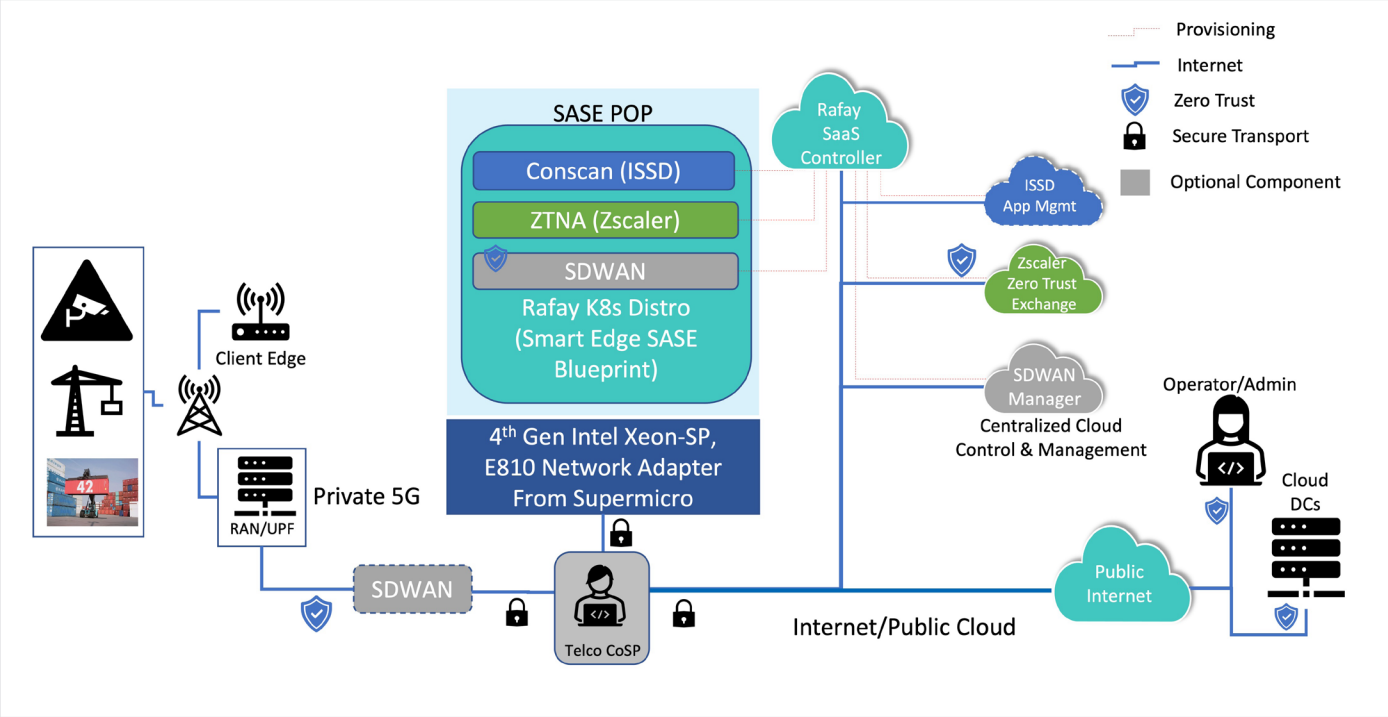

Figure 5. The MEC server in the center of this figure is a security-enabled Intel architecture server with remote management running a container scanning workload.

The ConScan application used as the basis for the Marine Ports Container ID Recognition and Scanning server scans video streams from designated security cameras and is able to isolate containers and record their identification information. A single ConScan deployment supports up to 256 cameras and scanners throughout the property with cameras at each entry and exit point. The ConScan program scans a container and tracks it through the port until its either loaded on a ship or on a truck exiting the port for local delivery.

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.

This demonstration includes Zscaler Application Connector which facilitates and uses Zero Trust Exchange to enforce security policies and decisions for accessing the applications on the server. The Zscaler Client Connector Access examines the data traffic destined for the ConScan application and applies policies to ensure that only traffic from trusted clients with log in credentials can have access to the application. Other users and applications are prohibited from connecting which prevents attackers from seeing IP addresses and ports of the application, rendering them "invisible" to attack.

Orchestrating the computer systems in a port environment is a challenge because ports are distributed and disaggregated which provides the potential for a large attack surface that is easy to infiltrate. Zscaler reduces that risk. Server maintenance and ongoing patches and updates are a critical component of securing the system. The Rafay KOP for Edge product is designed for 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 process. The Supermicro SuperServer platforms using Intel Xeon processors are designed for such deployments. These systems can be deployed in hardened cases throughout the port to ensure reliable processing of ConScan data.

Conclusion

The marine port container ID recognition system discussed in this paper is one of several "smart" use cases that are increasingly being used in industry, cities, schools, and other public-facing organizations. All these smart use cases with large number of IOT devices feeding and communicating information; however, 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 a wide range of these use cases and provides a security posture that significantly reduces the attack surface that hackers exploit.

This example has shown the smart maritime port use case. Intel and its partners have demonstrated a streamlined approach to securing these types of use cases. We encourage further exploration and engagement for you to set up a SASE POP-based service on our solution. Reach out to us to set up an evaluation for your use case.

Learn More

ISSD ConScan

Zscaler Zero Trust Exchange

Rafay Kubernetes Operations Platform for Edge

Supermicro IoT SuperServer SYS-211SE-31A

4th Gen Intel® Xeon® Scalable processors

Intel® Ethernet 800 Series Network Adapters

Intel® Network Builders

[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

[3] https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/

0623/LV/H09/PDF ♻Please Recycle 355548-001US