

Supermicro and Adtran Deliver Edge Cloud Platform Ready for SASE

Supermicro integrates 4th Gen Intel® Xeon® Scalable processor with Adtran Ensemble Cloudlet and Intel® NetSec Accelerator Reference Design creating an edge cloud platform with services protected by secure access service edge (SASE)



The success of cloud services, edge computing, and flexibility in work locations is driving increased demand for a new class of enterprise edge / branch office cloud workloads that include analytics, private 5G, artificial intelligence (AI), and data security among others. All of these applications need high performance, low latency, standalone resiliency and cybersecurity. All of them benefit from a cloud services deployment model but are poorly served by public cloud services mostly because of high transport latency and data egress costs.

With edge cloud servers that use Intel® architecture-based processors, communications (CoSPs), network (NETaaS) and security (SECaaS) service providers can help enterprises build out edge networks with the compute performance needed to meet demand for these cloud services. It's important that these servers also provide cybersecurity protection to protect the expanded attack surface created by edge cloud services.

SASE Delivers Cybersecurity

Secure access from users to corporate resources at the data centers, cloud, and edge is critical and is driving the need for secure access service edge (SASE), an edge security framework that was first proposed by industry analyst firm Gartner. SASE services replace the perimeter security approach to edge cloud-based solutions by combining software defined-wide area network (SD-WAN) functionality with a range of access control and data security services, also known as secure service edge (SSE).

SD-WAN combines the network forwarding intelligence of software-defined networks (SDN) with overlay of WAN connectivity across a variety of underlay networks, including broadband links, leased lines, MPLS and other WANs. SSE provides additional cloud-based security services such as secure web gateway (SWG), cloud access security broker (CASB), next-generation firewall (NGFW) services and zero trust network access (ZTNA).

SASE services run on edge cloud servers which are placed in a network edge point of presence (POP) owned by SASE vendors, cloud service providers (CSP), or other service providers. The challenge is to provide an open and powerful server that can host bare metal applications, cloud native network functions (CNFs) and virtual network functions (VNFs) across various deployment configurations.

Table of Contents

- SASE Delivers Cybersecurity 1
- Supermicro's Cloud Server Delivers SASE and SASE-Protected Cloud Services.....2
- Supermicro SYS-211SE-31(A/D) 2
- The Intel NetSec Accelerator Reference Design from Silicom 3
- Adtran Edge Cloud Network OS and Management 3
- Conclusion.....4

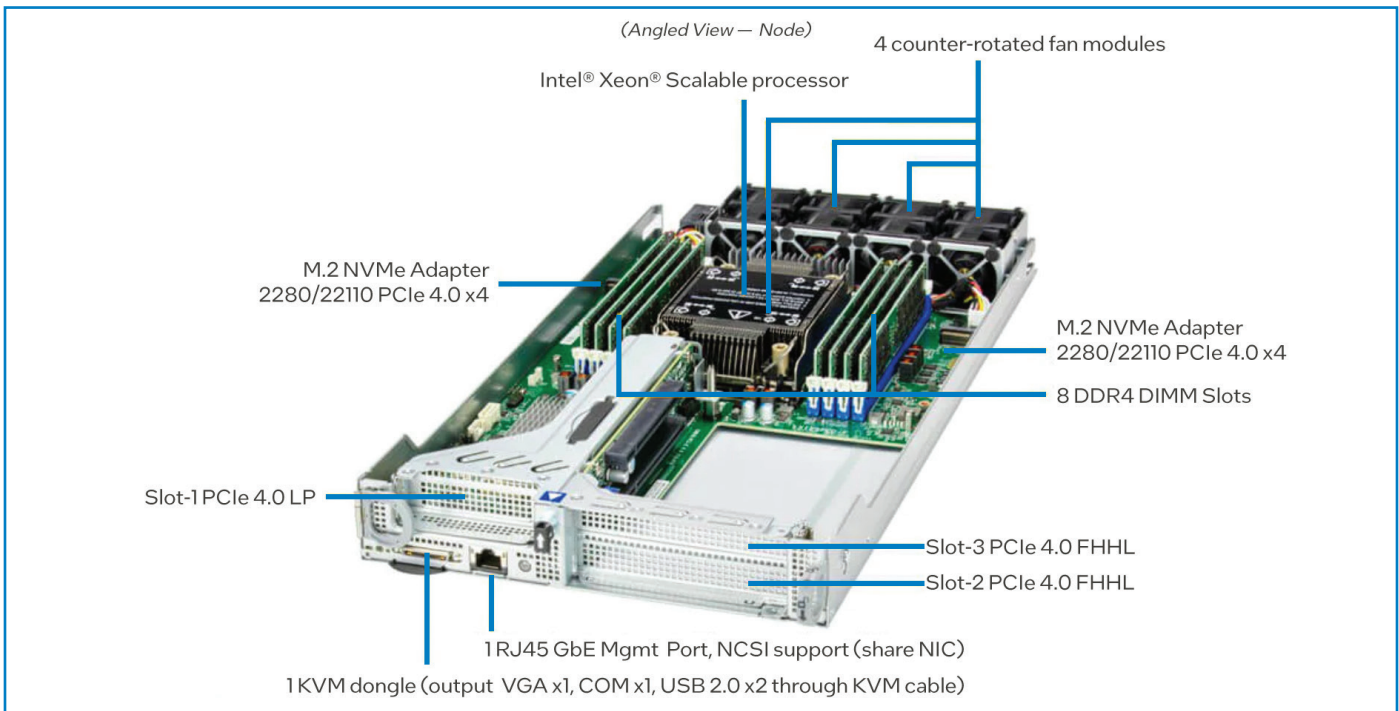


Figure 1. Front view of Supermicro SYS-211SE-31 (A/D) server.

New Generation of Edge Cloud Services

The Supermicro edge servers powered by Intel® Xeon® Scalable processors offer high performance compute platforms that when combined with Ensemble Cloudlet, enable customers to deliver a variety of service-enabling VNFs and CNFs with foundational SASE services to enable a new generation of edge cloud services that benefit from high performance compute, workload acceleration and high speed connectivity. Some of these services include:

- AI model delivery networks for edge and security workload inferencing
- Content delivery network for video or AR/VR streaming
- Video analytics and computer vision
- SD-WAN branch office connectivity
- API security services
- Edge IoT applications

Supermicro’s Cloud Server Delivers SASE and SASE-Protected Cloud Services

Supermicro has developed an edge cloud server designed for edge workloads including operational technology (OT) workloads, access controls, edge network and security services, AI inferencing and other applications. The same server can also be used to run SASE workloads. To build this system, Supermicro teamed up with Intel for high-performance processors, with Silicom and Senao for a network security acceleration server in a PCIe add-in-card form factor that is based on the Intel NetSec Accelerator Reference Design, and with Adtran for a cloud operating system.

Supermicro SYS-211SE-31(A/D)

One of Supermicro’s leading edge cloud servers is the Supermicro SYS-211SE-31(A/D) (see Figure 1), a 2RU high, short-depth edge server that can be configured with Intel® Xeon® Scalable processors and Intel® Ethernet Network Adapters for excellent throughput and latency.

This server optimizes flexibility with three hot pluggable nodes that each support up to 2TB of very high-speed RAM, two slots for PCIe Gen5 x16 full height, half-length cards and one slot for a PCIe Gen5 x16 half height, half-length card. For storage, each node includes two NVMe M.2 slots. The system comes with front-access 1+1 redundant 2000W DC power supplies.

The server is powered by 4th Gen Intel Xeon Scalable processors. The CPU family supports up to 52 high-performance compute cores and six on-chip accelerators that improve performance in SASE and other edge cloud applications including AI, analytics, networking, and storage.

One of those accelerators is the Intel® QuickAssist Technology (Intel® QAT), used by the SYS-211SE-31(A/D) in cryptography applications to speed data encryption and decryption.

The Supermicro SYS-211SE-31(A/D) will feature 5th Gen Intel Xeon Scalable processors that deliver impressive performance-per-watt gains across all workloads, plus increased performance and lower total cost of ownership (TCO) for edge applications featuring AI, databases, networking, and storage, plus Intel® Trust Domain Extension (Intel® TDX) that enables encrypted VMMs augmenting the confidential computing capabilities¹. These processors offer more compute, larger shared last-level cache, and faster memory in the same power envelope as the previous generation. They are also software- and platform-compatible with the previous generation of 4th Gen Intel Xeon Scalable processors.

The Intel NetSec Accelerator Reference Design from Silicom

To ensure high performance for SASE workloads, Supermicro has integrated the Silicom P425G2SN1-XR network security accelerator card into the edge cloud system. Based on the Intel NetSec Accelerator Reference Design, this card is an autonomous server in a PCIe add-in-card form factor and is powered by the Intel Atom® processor with either eight or 16 cores. This processor is combined with an embedded Intel Ethernet Controller E810 for up to 100GbE network throughput.

The Silicom P425G2SN1-XR maintains Intel architecture consistency so the software development investment made for the host Intel Xeon Scalable processor works seamlessly with the accelerator card. The card offers either full application processing or partial process acceleration that frees up cores on the server host processor and improves overall systems performance.

In full processing mode, the Silicom P425G2SN1-XR can offload all the processing for SASE or SD-WAN connectivity. In partial processing mode, it works as a co-processor with the host server for security applications such as IPsec, secure sockets layer / transport layer security (SSL/TLS), intrusion detection / prevention systems (IDS/IPS), and next-generation firewall (NGFW).

Adtran Edge Cloud Network OS and Management

To add edge cloud functionality to the SYS-211SE-31(A/D) server and Silicom P425G2SN1-XR NetSec accelerator, Supermicro has integrated the Adtran Ensemble Cloudlet software platform (see Figure 2) to provide the edge cloud operating system and compute architecture needed to support cloud applications with SASE workloads.

The Intel® NetSec Accelerator Reference Design

The Intel NetSec Accelerator reference design provides an easy to use expansion of compute resources on any platform that can accept either a FHHL or FH3/4L PCIe card. This card is a standalone server that can be used to augment a host and provide a security boundary for a PoP infrastructure. Today, there are two companies that make reference-design based products: Silicom Limited and Senao Networks.

The Silicom card is the IAONIC Server Adapter based on the Intel Atom® P5721 and P5742 processors combined with the Intel® Ethernet Controller E810.

The Senao Card is the SX904 SmartNIC based on the Intel® Xeon® D processor with three options: the four-core Intel Xeon D-1713NT, the eight-core Intel Xeon D-1733NT, or the 10-core Intel Xeon D-1743NTE. These options are paired with Intel Ethernet Controller E810. The Intel Xeon D processor enables additional use cases associated with AI acceleration.

Adtran Ensemble Cloudlet provides an open, modular and multi-node edge cloud solution that makes it easy to deploy scalable and resilient cloud resources at the network edge. Cloudlet includes the cloud operating system that delivers flexible local cloud control and redundant management access to each node in the cluster. The platform also offers centralized management tools that are responsible for remotely managing and administering thousands of edge cloud instances.

The edge cloud network OS can run on the Supermicro cloud servers and/or the accelerator based on Intel NetSec Accelerator Reference Design. The Cloudlet OS operates either as a head node or a compute node. The head node hosts the

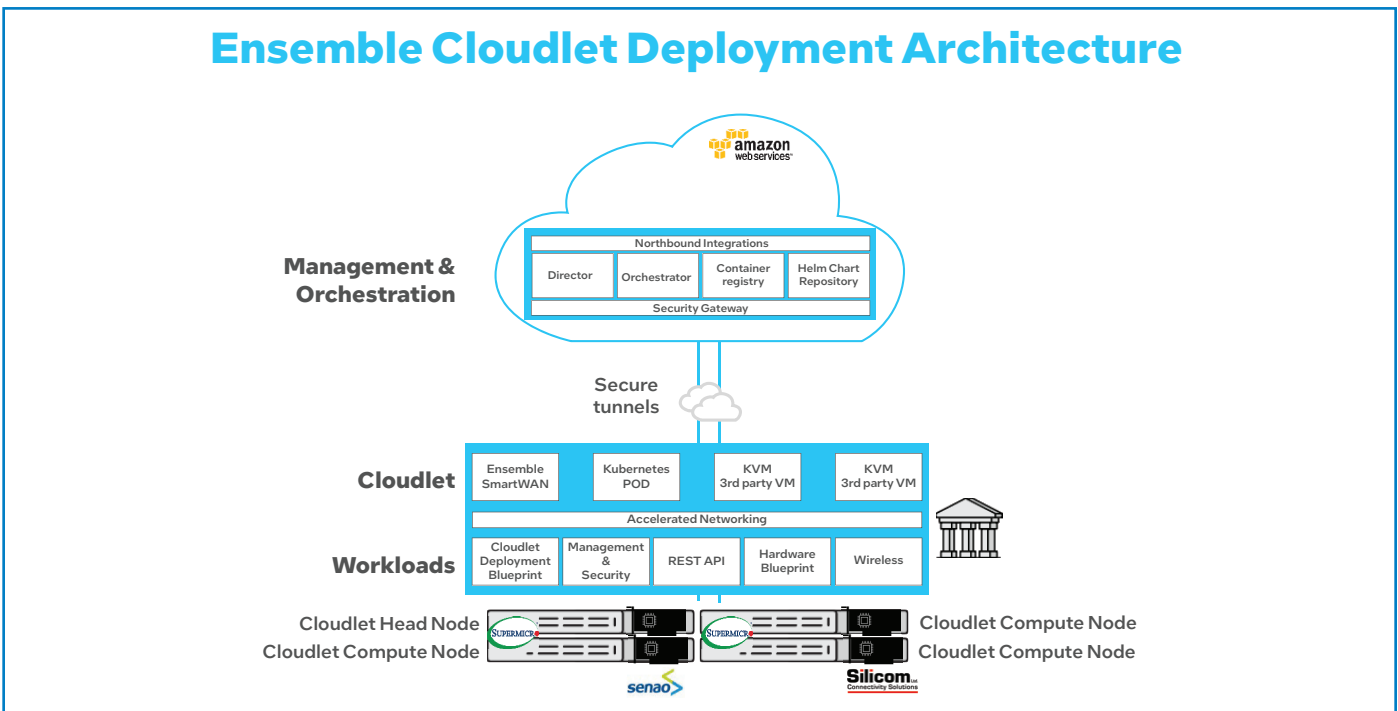


Figure 2. Block diagram of Adtran Ensemble Cloudlet and management platform.

Trusted SASE Partner: Zscaler

One of the tested SASE systems in the Supermicro partner ecosystem is the Zscaler Zero Trust Exchange™. Zero Trust Exchange is a cloud native platform that connects and secures users, workloads, and devices over any network from any location. Benefits of the system include:

- **Cyberthreat Protection:** The software offers a holistic approach to securing users, workloads, and devices.
- **Data Protection:** Full TLS/SSL inspection at scale for complete data protection across the SASE platform.
- **Zero Trust Connectivity:** Connect to apps, not networks, to prevent lateral movement by hackers using ZTNA.
- **Digital Experience Management:** Enables the identification and resolution of performance issues. The software can be delivered over the cloud to the Supermicro integrated edge cloud server for easy deployment.

cloud controller and is responsible for creating secure communication tunnels between the edge cloud site and the central MANO instance. The head node can also provide compute resources on the same server to host customer workloads. The compute node is the primary cloud compute resource responsible for virtualized or containerized workloads. The compute node accesses the centralized Cloudlet management tools via secure tunnels of provided by the head node(s).

The Cloudlet Management layer is comprised of the Ensemble Director and Ensemble Orchestrator. Ensemble Director provides secure, end-to-end zero-touch provisioning workflow and APIs. Director is responsible for managing faults, events, performance statistics, operational dashboards and troubleshooting tools. Director also provides for automated recovery – including restoration of the last known configuration (image, provisioning, keys/certs, etc.) – of compute node resources.

Ensemble Orchestrator is responsible for defining cloud services (workloads, resource quotas, etc.) including day-0 and day-N configurations. Orchestrator provides VNF and CNF workload lifecycle management such as onboarding, service design, deployment, migration, recovery and retirement. With Orchestrator, cloud services can be dynamically modified such as workload resource resizing, swapping workloads and new workload introduction into a service chain.

Conclusion

There are increased requirements at the edge driven by a new class of compute-centric applications, edge cloud services, and security requirements. In addition, there is growing demand for services that connect edge users to corporate resources across on-premises data centers, public cloud, and other edge locations. These two dynamics require servers deployed at the edge to have performance scalability, low latency, flexibility and novel operational models.

To help enterprises and service providers deploy these new services, the Supermicro - Intel – Silicom / Senao - Adtran edge cloud solution is available as a pre-integrated SKU from Supermicro for easy procurement and deployment. All of these network elements have been validated by Supermicro for ease of deployment and instantiation of VNF-based service such as the Zscaler Zero Trust Exchange SASE service.

With the SASE-based secure cloud, service providers can work with any of the VNFs that are a part of the Adtran ecosystem or from third-party ISVs that meet industry standards.



Learn More

[Adtran Ensemble Cloudlet](#)

[Supermicro Homepage](#)

[Silicom USA Homepage](#)

[Senao Networks Homepage](#)

[Zscaler Zero Trust Exchange](#)

[Intel Xeon Scalable Processors](#)

[Intel NetSec Accelerator Reference Design](#)

[Intel Network Builders](#)

[Intel Ethernet 800 Series Controllers and Network Adapters](#)



Notices & Disclaimers

¹ Performance varies by use, configuration and other factors. Learn more on the [Performance Index site](#).

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

© 2024 Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

0224/DC/DJA/PDF

Please Recycle