Solution Brief

Network Security ISVs
Cybersecurity

AEWIN SCB-1942C Network Appliance Delivers Intrusion Protection

5th Gen Intel® Xeon® Scalable processor-based SCB-1942C network appliance has performance to run AI-based network security. AEWIN shows malware and intrusion prevention solution working with Gorilla Technology Group

Edge computing has evolved dramatically in just the past few years. Edge computing started as enterprises using switches, routers, firewalls and other networking appliances to provide branch office access to corporate resources and the Internet.

Now edge networking incorporates the original branch office solutions but has expanded into new use cases as compute power has grown and cloud native software has delivered all the scalability, flexibility and remote management features of the cloud.

Demand for edge compute is driven by the need for low latency services that make edge computing ideal for content delivery networks (CDNs), 5G base stations, private 5G networks, industrial automation, network security, Internet of things and other use cases.

But edge compute servers face a network security challenge. These servers are increasingly running mission-critical applications and offer malicious actors a backdoor way into corporate information technology (IT) or operational technology (OT) networks. Thus, these networks face the same sophisticated cyber-attacks as data centers.

To protect against an increase in attack surfaces at the edge, artificial intelligence (AI) technology is being incorporated into cybersecurity defense. With its sophisticated pattern matching capability, speed, and inference, AI can monitor and analyze network traffic patterns and detect and remedy a malware attack in real time.

But AI cybersecurity solutions need compute performance to work at wire speed. To meet this need, Intel® Network Builders Gold Tier community partner AEWIN has developed a family of high-performance servers, based on Intel® architecture processors, that have the compute power needed for AI-driven intrusion detection systems (IDS), intrusion prevention systems (IPS), and unified threat management (UTM). The company has demonstrated these capabilities using AI-powered malware detection and end point protection software from Gorilla Technology Group.

AEWIN SCB-1942C Has Dual Processor Performance

The SCB-1942C is a 2U-high rack mounted networking system for edge applications featuring dual 5th Gen Intel® Xeon® Scalable[1] processors.

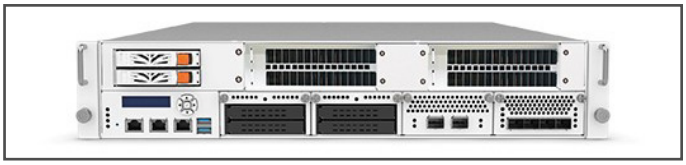

Figure 1. Front view of AEWIN SCB-1942C network appliance.

The new generation network appliance platform provides remarkable performance with up to 64 cores per CPU and four low-latency Ultra Path Interconnect (UPI) links for inter-socket communication with performance of up to 20 gigatransfers per second (GT/s).

The AEWIN SCB-1942C is a powerful and versatile network appliance with advanced virtualization features that can support both cybersecurity software and multiple network functions and services.

The SCB-1942C supports 16 channels of DDR5 (registered or ECC RDIMM) at up to 5600 MHz with a 1.5TB maximum memory capacity.

The appliance has two built-in, front panel 1GbE ports. It also supports 80 PCI Express lanes per CPU, enabling network expansion modules via the SCB-1942C's 8x PCIe x8 slots (4x PCIe Gen5 + 4x PCIe Gen4). With its 600mm short chassis depth, the SCB-1942C is designed for both IT and operational technology (OT) cybersecurity applications at the network edge.

The network appliance offers flexible network port configuration, such as 1/10/40/100 Gigabit fiber, Gigabit copper/fiber with or without bypass function. The appliance can support up to 400G Ethernet adapters for a maximum Ethernet capacity of up to 1,200GbE.

The IO options of SCB-1942C also include two additional ports, one for management and another for optional Intelligent Platform Management Interface (IPMI) functionality. The appliance also features a console port, USB ports, LEDs for power/HDD/2x GPIO. In addition, the SCB-1942C also supports two front hot-swappable 2.5" SATA HDDs/SSDs and onboard CompactFlash/m-SATA/mini-PCIe and M.2 slots for network storage.

Built-in Hardware Security and Reliability

For reliability and security, the SCB-1942C has redundant power supplies and supports the OT006 module for AEWIN Trusted Secure Boot (TSB V2 module) to deliver firmware resiliency by monitoring and verifying firmware. In addition, the system supports TPM 2.0 module to protect its start-up process.

AEWIN SCB-1942C is Powered by 5th Gen Intel Xeon Scalable processor

AEWIN selected the 5th Gen Intel Xeon Scalable processor for the SCB-1942C because it offers the performance, the accelerators and the power management features needed to drive advanced, AI-powered applications.

The CPU family comprises 32 SKUs with between eight and 64 cores. Each device has eight memory channels running at up to 5,600 MHz. The CPU's support for higher memory speeds and enhanced memory capacity delivers improved performance and superior memory capabilities compared to previous CPU generations. They also offer hardware-enhanced security and workload acceleration.

For AI acceleration, the CPUs feature Intel® Advanced Matrix Extensions (Intel® AMX). This accelerator improves performance of deep learning training and inference on the CPU. Intel AMX is ideal for compute heavy, AI/ML-based natural-language processing, recommendation systems and image recognition.

Security acceleration is also available with the Intel® QuickAssist Technology (Intel® QAT) which offloads computationally intensive cryptography and compression operations from the CPU cores, allowing the CPU to perform other tasks more efficiently for greater overall system performance, efficiency, and power.

5th Gen Intel Xeon Scalable processors support the latest in platform technologies including DDR5 memory for the highest memory bandwidth, PCIe 5.0 for I/O connections between the CPU and devices, and Compute Express Link 1.1 low latency I/O.

Figure 2. 5th Gen Intel Xeon Scalable processor.

Advanced Intrusion / Malware Protection System

AEWIN partners with security software companies to add the right cybersecurity functionality for each customer's need. For the SCB-1942C the company set up a proof of concept demonstration with Gorilla Technology Group to onboard the company's intrusion and malware prevention capabilities. Both solutions are AI powered and have functionality listed below:

- **NetProbe:** Detects and blocks various types of external attacks at the edge of all network connection points. NetProbe is an AI-based detection engine that blocks threats ranging from malicious IP connections to distributed denial of service (DDoS) attacks. The use of AI reduces manual intervention and processes, freeing up security engineers to focus on other security priorities.
- **Host-based Malware Detection (HMD):** Provides endpoint protection from malware and endpoint detection and response (EDR). These services combine continuous monitoring and data collection with rules-based automated response and analysis. HMD also prevents advanced persistent threats, traces their origins, and responds effectively to provide complete endpoint security. Using an AI-powered malware detection engine, HMD constantly checks endpoint health, identifies unusual activity, and notifies network security engineers about software vulnerabilities.

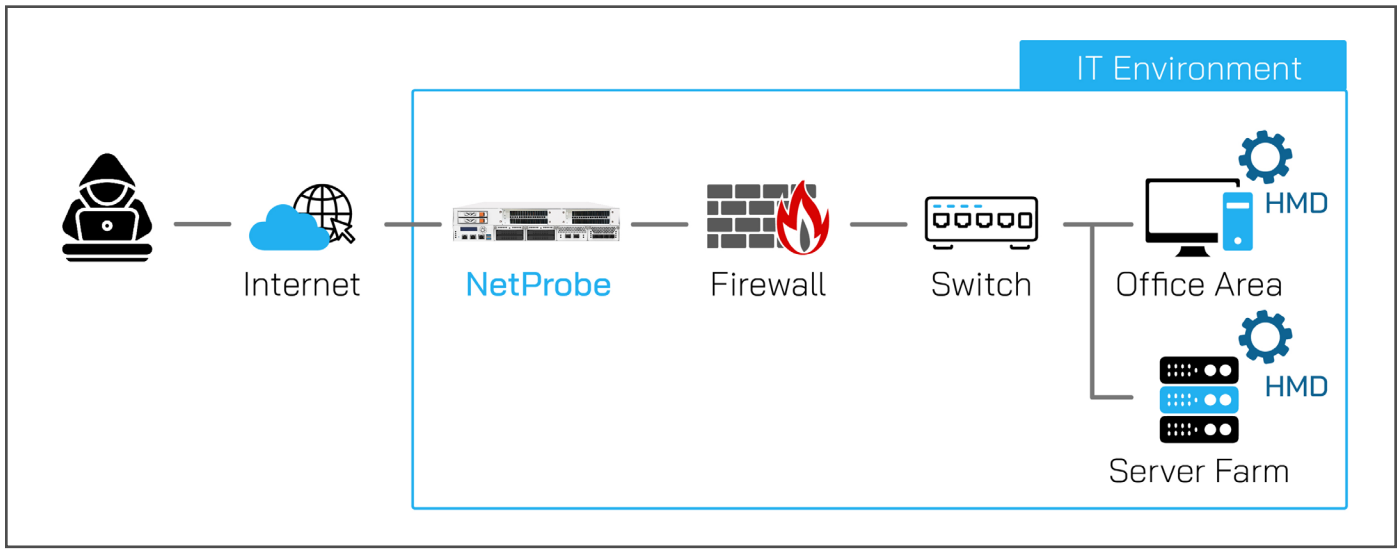

Figure 3. NetProbe and HMD delivering end point and malware prevention protection.

As shown in Figure 3, the AEWIN SCB1942C with NetProbe software provides intrusion detection functionality between the Internet and the firewall, handling all of the malware detection and threat removal services. The NetProbe is backed up by the HMD on key end points delivering intrusion detection and protection services.

The SCB-1942C has the performance to process these workloads at wire speed as well as the core capacity to run other virtualized networking applications such as routing on the same platform.

Conclusion

The market demand for edge compute solutions is growing and evolving to serve a wide range of applications that need low latency and high performance. In some countries the need for local data storage is an important market demand driver.

Protecting these edge servers from cybersecurity attacks is very important as they are mission critical and provide a potential backdoor for malicious actors to get into an enterprise network. The use of AI for improved cybersecurity protection is growing but requires a significant level of compute performance.

AEWIN has developed the SCB-1942C network appliance that has the performance for sophisticated AI-based cybersecurity solutions and legacy workloads. The foundation of these network appliances is the 5th Gen Intel Xeon Scalable processor that features up to 64 cores and dedicated accelerators for AI processing and network security.

Learn More

AEWIN Corp.

AEWIN SCB-1942C

NetProbe

HMD

Intel® Advanced Matrix Extensions

5th Gen Intel® Xeon® Scalable processors

Intel® Network Builders

[1] The SCB-1942C is also available with 4th Gen Intel® Xeon® Scalable processors.

Notices & Disclaimers

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.

0624/DC/DJA/PDF Please Recycle 359990-001US