Solution Brief

Partners (Security ISVs, System Integrator Partners)
Cybersecurity

AEWIN SCB-1933 Edge Appliance Supports Zero Trust Data Security

Built with the high-performance 3rd gen Intel® Xeon® Scalable processor, the AEWIN SCB-1933 network appliance supports Zero Trust Architecture security management for efficient branch office and edge location data security.

Enterprises are rethinking how they secure data at branch offices and other network edge locations due to the growth in the remote worker population and the increasing amounts of data they are creating. The fact that 60% of workers are remote, according to Gartner[1], combined with greater use of the public cloud results in an expanded attack surface. Most branch offices have no onsite IT team, and legacy fixed function security appliances can create a situation where long lead times for upgrades or adding new functionality can leave branch workers vulnerable to cyber-attacks.

Enterprises are adapting to the complexity of the modern environment to protect data, applications, devices, and cloud services. Virtualized edge servers running security applications is one new approach with growing acceptance in branch offices. By replacing hardware-based security appliances with a commercial-off-the-shelf (COTS) compute system that can support a wide range of security applications, IT managers can quickly deploy new security applications to support changes in the office or can respond to attacks. These servers support a wide range of applications including next-generation firewalls, incident detection systems (IDS), virus protection as well as standard branch office networking functions such as a switch/router, voice IP private branch exchange (PBX) and other networking functionality.

Zero Trust Architecture Reduces Human Error

To enable these virtualized data security systems to provide optimum protection, many companies are adopting zero trust architecture (ZTA)-based security function management. ZTA is a model that is defined by the National Institute of Standards (NIST SP 800-207 Zero Trust Architecture Specification). The official definition from NIST is that ZTA is "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

In practice, ZTA results in a security posture of assuming every connection into the network could be used for a malicious attack. These connections could be from trusted and untrusted parties including employees, partners, customers, contractors, or others. ZTA systems verify these connections using identity tools, threat intelligence databases or data security systems providing information about the connections that can be used to build a risk profile to determine the risks of that connection.

Access privileges are constantly reviewed for new information. If a low-risk user changes their behavior on the network, such as logging in from a new and different location, accessing different databases or applications or makes other changes, then a ZTA system would adjust privileges to match these new patterns. The system is designed to balance data security while minimizing the impact on business operations.

Figure 1. Front view of AEWIN SCB-1933

AEWIN is an Intel® Network Builders ecosystem participant that has developed a new branch office server using 3rd generation Intel® Xeon® Scalable processors that offers the performance and features for large ZTA-based branch office implementations. The company has 20 years of experience developing and manufacturing high-performance networking platforms. It is a member of Qisda Business Group which is a $20 billion revenue company with more than 75,000 employees worldwide.

AEWIN SCB-1933 High Performance Network Appliance

The SCB-1933 is a 2U network appliance (see Figure 1) designed for large branch office networks that need a single hardware system to run multiple virtualized security and networking functions. The single-socket appliance features the 3rd generation Intel Xeon Scalable processor that offers a balanced architecture with built-in acceleration and advanced security capabilities. The CPU was designed through decades of innovation for the most in-demand workload requirements. For the SCB-1933, this performance is used to handle multiple data flows in which each packet must be authorized, unencrypted and access controlled in order to protect the transmitted data.

The AEWIN SCB-1933 makes the most of the CPU's 64x PCIe 4.0 lanes to enable the server to handle a massive amount of data with great flexibility and scalability via eight PCIe 4.0 x8 slots for NICs, NVMes, and accelerators. The company has developed multiple PCIe Gen 4 networking interface modules that range from 1 GbE to 100GbE per port. AEWIN has also designed its own encryption acceleration card based on the Intel® QuickAssist Technology (Intel® QAT) card and an NVMe storage module. AEWIN also has developed conversion kits to enable selected standard form-factor PCIe cards, such as GPU cards, to add functionality to the SCB-1933.

The processor family also features advanced hardware-based security using Intel Secure Boot technologies, Intel® Software Guard Extensions (Intel® SGX) and Total Memory Encryption (TME). These technologies are used by AEWIN to help harden the platform against malicious actions.

For memory, the network appliance supports a combination of 3200MHz DDR4 RDIMM/LRDIMM and Intel® Optane™ 200 Series allowing it to use bigger datasets at a lower cost with better operational efficiencies. Intel® Optane Persistent Memory (PMem) is an innovative memory technology that delivers a unique combination of affordable large capacity with data persistence. The server's total memory capacity is up to 3TB using eight memory channels. In addition, the server supports dual onboard M.2 slots for boot image redundancy.

Many remote applications are located in cabinets or other constrained spaces. The SCB-1933 features a short depth design (600mm) so that it easily fits into these small spaces. The server has an operating temperature from 0-40 degrees Celsius (32-104 degrees Fahrenheit).

NGFW Protects Branch Worker Data

SCB-1933 can serve as next generation firewall (NGFW) featuring firewall, intrusion prevention system (IPS), anti-virus, virtual private network (VPN), and load balancing services. The firewall and the IPS work together to block attacks based on the detection of suspicious data flows automatically without the need for human activity or intervention. With IPS, NGFWs add more intelligence to defend the network proactively.

The NGFW services leverage the server's high-performance, deep packet inspection (DPI) functionality. For each packet in a data flow, DPI examines the full seven layers of the packet header in order to understand the application layer data that can hide malware from solutions that don't support seven-layer analysis. Other benefits of the solution include:

Advanced Security: The combination of technologies available in the AEWIN NGFW helps to identify and prevent unknown cyberattacks more quickly, and to protect and maintain network security even under the constantly changing threat landscape.

Higher Efficiency: Centralized monitoring and management allow better visibility for efficient management, identifying unnecessary, bandwidth-intensive applications running on the network and fixing them to free up additional bandwidth for other applications.

Cost-effectiveness: The added features of the NGFW can do much more than a traditional firewall, which can help to lower costs as single system replaces several standalone devices. Also, consolidating security solutions with higher efficiency delivers enhanced customer services at a lower cost.

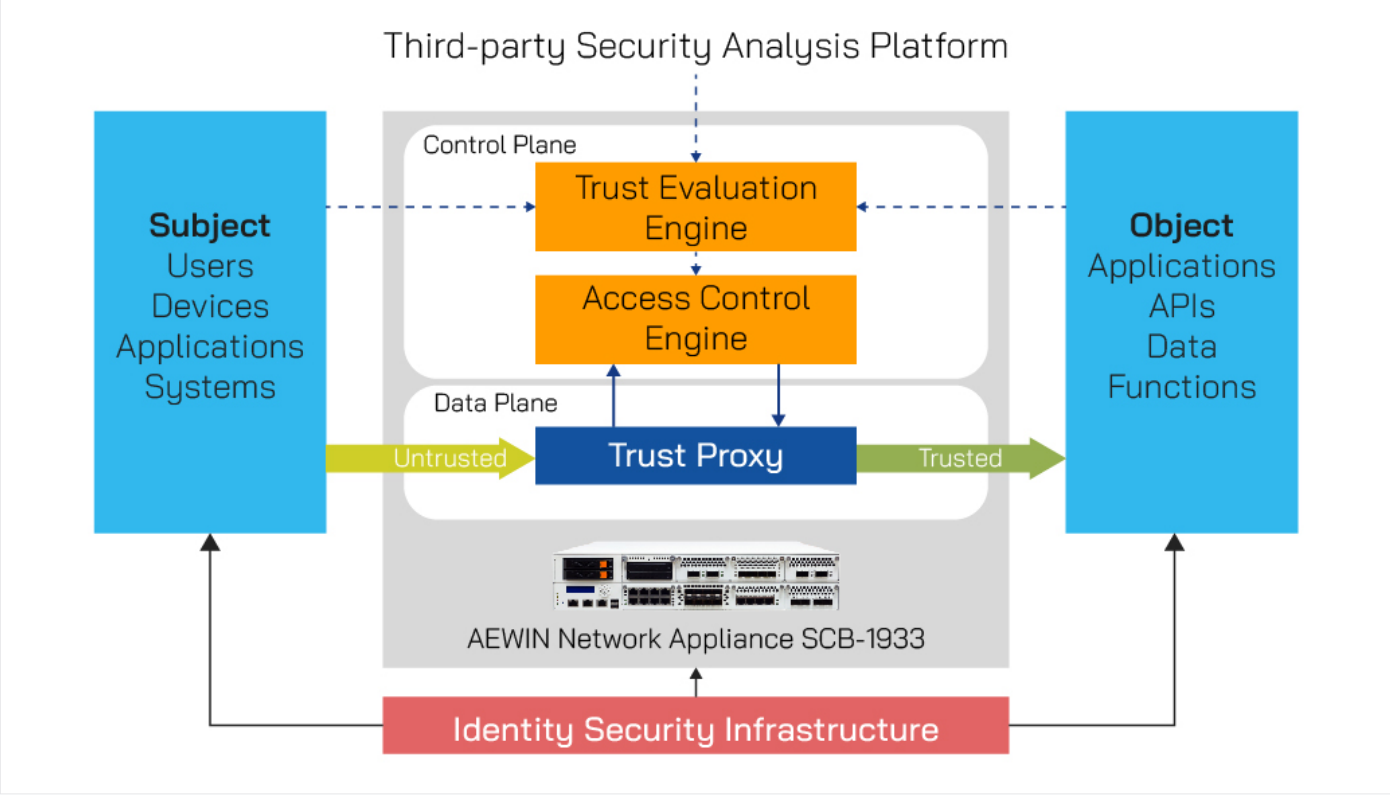


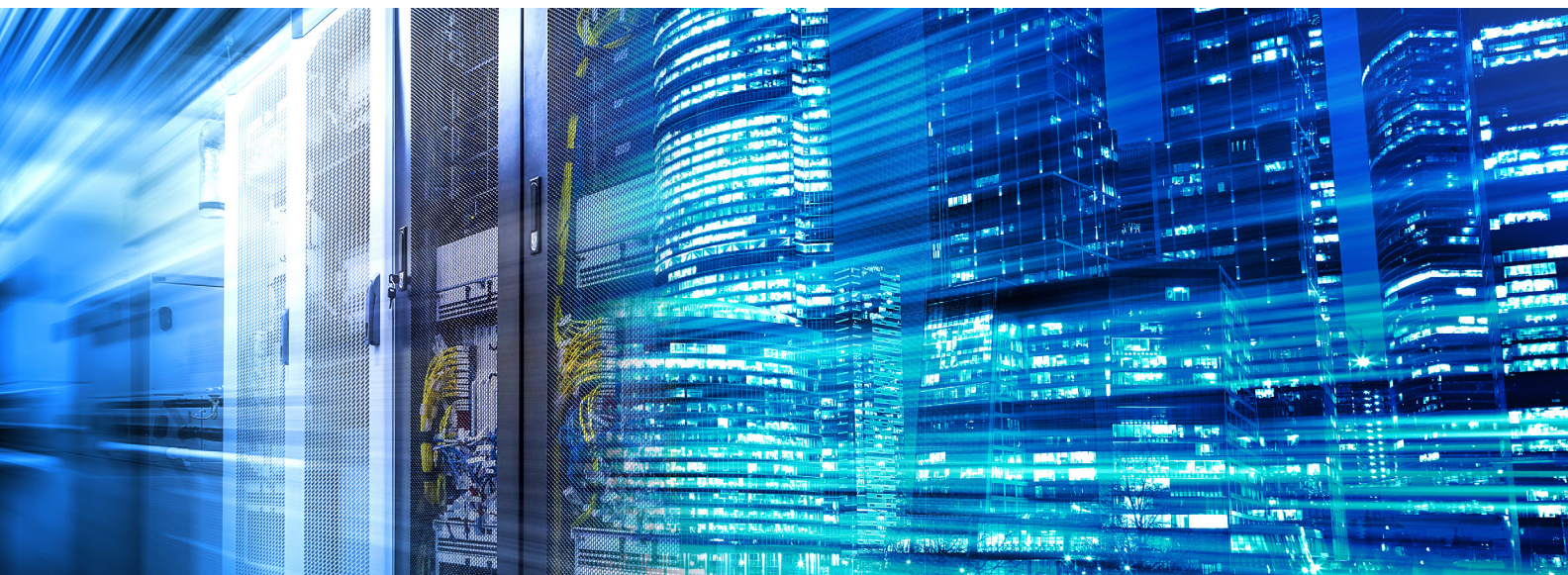
Figure 2. Zero Trust Architecture

Faster Response using AEWIN ZTA Security

For management, the SCB-1933 supports a range of ZTA solutions for automation of the NGFW security functions. One of the main ZTA solutions that AEWIN utilizes creates a trusted proxy that separates an untrusted network segment from the trusted network segment (see Fig. 2). This trust chain is created by evaluating data from the users, their devices, the environment and user behavior.

The solution provides identity-based adaptive access control that continually evaluates the identity via a unified digital identity tag. This is combined with a process that governs the access to servers, applications or business systems. With every access request, the system authenticates the user and checks their trust level is sufficient to grant the access they are seeking.

There is not a one-time authentication process, but rather continual evaluation to measure the risk of access. Factors included in this evaluation include authentication methods used, the health of the device, whether the application is distributed by the enterprise, and the access behavior, etc.; the trust evaluation of the environment might include access time, source IP address, source geographic location, access frequency, device similarity, etc.



Conclusion

More users, more cloud services and new use cases such as IoT are expanding the attack surface at branch offices. AEWIN has developed the SCB-1933 to fill the need for a high-performance branch office server with advanced security capabilities. The advanced security capabilities start with hardening technologies that help protect the server itself. Added to that are advanced NGFW functionality and ZTA management for a comprehensive suite of data security services. The solution is powered by the 3rd gen Intel Xeon Scalable processor and makes use of the CPU's support of PCIe Gen 4 I/O with a full range of NICs and accelerator cards.

Learn More

AEWIN Corp.

AEWIN SCB-1933

Next-Generation Firewall

Intel® Network Builders

Intel® Optane™ Persistent Memory

3rd generation Intel® Xeon® Scalable processor

intel®

Notices & Disclaimers

[1] https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.

1022/TM/HO9/PDF ♻Please Recycle 353068-001US