Accton
Making Partnership Work

SAU5081I-AMB

Advanced Malware Blocker Appliance

Product Applications

- **UTM Server appliance**
- **Block customized and unknown malware**
- **Endpoint protection**
- **Anti-malware and SSL decryption offload**
- **Network-wide threat intelligence**

The SAU5081I-AMB is a high-performance server platform running advanced malware-blocking software. The system includes two basic 1RU chassis configurations; a half-width single node and a full-width dual node. Each node is based on dual-socket Intel® Xeon® E5-2600 V3/V4 series processors, supporting up to 14 cores (28 threads) per socket, or up to 28 cores (56 threads) per node, with 4 DDR4 DIMM slots of up to 128 GB memory per socket (256 GB per node). Local storage options include up to 5 SATA III high-speed SSDs, including support for Intel® RSTe and RAID. The SAU5081I-AMB also includes quad 10 Gbps SFP+ network ports for high-bandwidth connections to the network.

The SAU5081I-AMB delivers the unique combination of industry-leading threat detection and blocking accuracy with the industry's best real-time performance. This is achieved by the integration of cutting-edge artificial intelligence technology from Cylance® and other best-of-breed technologies to provide the industry's most effective real-time, inline malware prevention.

Real-Time Visibility

At the heart of the SAU5081I-AMB is a patented Security Orchestrator. The SAU5081I-AMB is placed inline with the flow of traffic entering and leaving the enterprise network, data center, or partitioned sub network. As traffic flows, it inspects packets and packet payloads, and reconstructs the full-file content using a combination of deep-packet inspection (DPI) and deep-content inspection (DCI). The content is then scanned and analyzed with a series of threat-optimized virus and malware blocking engines. Real-time visibility to packets and fully reconstructed content sets the stage for accurate detection and blocking of conventional and advanced threats.

To further aid in sustaining effective prevention, the SAU5081I-AMB also provides a network-wide reporting and visualization of multi-dimensional threat metrics to provide actionable threat intelligence.

Accton
Making Partnership Work

SAU5081I-AMB Features

Key Hardware Features

Mechanical Platform
SAU5081I-SN: Half-rack width, 1RU
SAU5081I-HA: Full-rack width, 2 nodes in 1RU

Ethernet Ports
Default: 2 x GbE RJ-45
Options: Quad 10Gb SFP+ by Intel XL710-AM1
Dual 10Gb SFP+ by Intel 82599

I/O Interfaces (per node)
2 x USB 3.0
1 x RJ-45 serial console port

Power
Type/Watts: One PSU per node, 650W per PSU
Input: 110 to 240 VAC @ 50/60 Hz

System Cooling (per node)
3 fans supporting speed control

Physical
Dimensions: Half-width 217 x 600 x 44 mm
Full-width 438.4 x 600 x 44 mm

Environment
Operating: Temperature: 0 to 45°C; Humidity: 5% - 90% RH
Storage: Temperature: -20 to 70°C: Humidity: 5% - 95% RH

Compliance
EMC/Safety: CE, FCC, LVD
RoHS: RoHS 2.0 (2011/65/EU

Key Software Features

Advanced Protection
Blocks customized and unknown malware that evades real-time protection by other systems.

Endpoint Protection
Protects all endpoints, including Bring Your Own Devices (BYOD) and Internet of Things (IoT) that connect to the enterprise network.

Decryption Offload
Offloads anti-malware and SSL decryption from NGFW and other appliances to dramatically improve scale and performance, eliminating upgrade expense.

Scales up to 10 Gbps
The advanced malware-blocking software has the ability to scale up to 10 Gbps, while still supporting full security scanning, with SSL decryption and re-encryption.

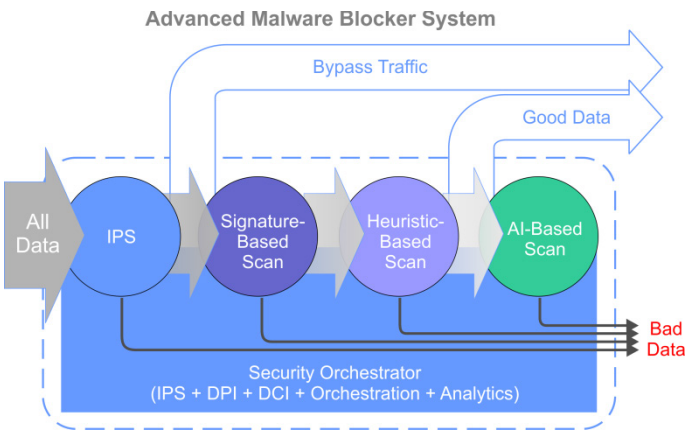
Threat Detection
Reduces the frequency of business disruptions and expense of dispatching threat detection and remediation teams by eliminating threats before data is delivered.

Threat Intelligence
Provides overloaded security personnel with clear and actionable network-wide threat intelligence.

Multiple Detection Layers

The advanced malware-blocking software integrates multiple best-in-class virus and malware detection technologies that are orchestrated. The first step in the process is the intrusion prevention system (IPS) level scanning to detect and block worms and other Layer 3 threats. Next, the DCI engine is used to separate content that should be further scanned from content that will not be scanned, such as VOIP traffic, streaming video, and other "customer-defined" policies.

Multiple Detection Layers (Cont.)



All remaining traffic and associated content is then scanned using a full library of more than 100 million known virus and malware signatures sourced from third party anti-malware partners. The same content is then scanned using a heuristics detection engine to detect and block new variants of known threats. Collectively, these scans reliably detect and block more than 99% of viruses and malware that may exist in typical enterprise networks.

All remaining traffic is then further analyzed using artificial intelligence (AI) engines based on Cylance® predictive malware prevention. These AI engines are used to detect and block any remaining zero-day, targeted, and other advanced persistent threats that may be present. Cylance's industry-leading predictive malware prevention engine combines machine learning with artificial intelligence to yield the highest real-time threat accuracy available.

Collectively, this multi-layered anti-malware approach leverages a single inspection and content reconstruction cycle to provide the industry's highest performance detection of both known and unknown threats, with only milliseconds of latency for a safe and satisfying network user experience.

As an option, data identified as malware by the AI engine can be forwarded to a sandbox to further characterize new malware and to reclassify any potential false positives as good data.

Orchestrated for Superior Scale and Performance

The industry-leading performance of the SAU5081I-AMB is based on its Security Orchestrator engine which leverages multiple patented technologies. The onboard orchestrator monitors the load and performance of each virtual network function (VNF) that is running to support the range of diverse compute activities.

As workloads increase for one set of VNFs, the orchestrator dynamically allocates more CPU resources to those functions. If workloads approach the capacity of a single VNF, the orchestrator simply spins up more VNF instances and distributes the workloads for sustained throughput. As workloads shift over time, resources are reallocated to always achieve the optimal overall system performance on any given server.

Performance gains are further achieved through a combination of optimized software architectures and code written and optimized for superior performance in massively multi-thread parallel processing environments. Patented techniques use machine learning and other techniques to maximize throughput with imperceptible latency.