

Robust Network Security for Evolving Enterprises



About Lanner

Lanner Electronics Inc. is a world-leading hardware solution provider in design, engineering, and manufacturing services for advanced network appliances and rugged industrial computers.

With 37 years of experience, Lanner provides reliable and cost-effective computing platforms with high quality and performance.

Lanner offers a wide-range of customizable network security hardware platforms designed to protect the communication protocols in both IT and OT domains for critical infrastructures including energy, power, oil and gas industries.

Bolster network security with an additional layer of protection

To protect critical infrastructures from advanced cyber malwares, it is necessary to establish multi-layer protections covering both information technology (IT) and operational technology (OT) networks. IT/OT convergence is becoming increasingly common as organizations seek to integrate operational data with enterprise systems for improved efficiency, productivity, and decision-making. However, this convergence also presents new challenges in cybersecurity, interoperability, and management – requiring careful planning and implementation to ensure the security and resilience of both IT and OT environments.

Lanner's NCA-4240 network security appliance is a key component in creating a secure Industrial Demilitarized Zone (IDMZ) - an additional layer of protection that enforces data security policies between IT and OT networks.

Advanced components for modern network security requirements

Powered by its 14th Gen Intel® Core™ processor, this appliance can support up to 64GB DDR5 memory and up to 48 PCIe lanes, making it perfect for running high-throughput enterprise security applications. One GbE RJ45 port, eight 2.5GbE RJ45 ports, and a NIC Module slot provide flexibility in network connectivity options, while two USB 3.0 ports, two 2.5" HDD/SSD drives, and expansion slots give users the option to expand capabilities to fit their organization's needs.

The embedded BIOS system has Intel® Boot Guard technology to deliver protection against malware, uncertified sequences, and other cyber threats. The compute capability of the 14th Gen Intel Core processor provides additional protection, enabling the NCA-4240 to filter and inspect incoming and outgoing traffic and block potential security threats before they reach critical internal systems.

Powerful performance for demanding network security applications

The high performance, customizability, and advanced features of the NCA-4240 network security appliance make it well-suited for a variety of critical network security and optimization tasks, including DDoS mitigation, enterprise firewalls, intrusion prevention systems (IPS), application delivery, and WAN optimization. As network demands evolve, users can add resources such as memory, storage, and processing power as needed. This scalability ensures that the appliance can grow alongside the network it's protecting or optimizing, making it suitable for both small and large-scale deployments.

Intel Ingredients



14th Gen Intel® Core™ Processors

14th Gen Intel Core processors enable the device to handle complex network security tasks and process network traffic quickly and efficiently, minimizing latency and maintaining network performance

Intel® Boot Guard technology

Intel Boot Guard provides a hardware root of trust, adding robustness to the chain of trust process and reducing the chance of malware exploiting the hardware or software components on the platform

Learn More

- [Lanner NCA-4240](#)
- [NetSec SD-WAN Developer Kit](#)
- [Developer Kit Reference Scripts](#)

Intel® Foundational Developer Kits allow you to get started on your targeted application development with a superior out-of-the-box experience. Deploy your application at scale by building customized systems via Intel ecosystem partners.



¹ For workloads and configurations visit www.Intel.com/PerformanceIndex. Results may vary

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 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.