Solution Brief

Secure Access Service Edge (SASE)

Driving Performance, Efficiency and Data Protection with SASE Edge Gateway

Versa's next generation of branch appliances enable deployment for state-of-the-art software-defined security and networking at edge sites, based on the Intel Atom® processors x7000C Series.

In highly distributed networks, the security perimeter is no longer defined, particularly for locations with limited IT footprints at the edge. The secure access service edge (SASE) model delivers cloud-based security and WAN services to protect home or branch offices, as well as non-office locations such as retail stores and gas stations. They also include internet of things and industrial usages. AI-based security functions are vital to improve the effectiveness of human cyber expertise with capabilities that include automation, prediction and anomaly detection.

The Versa Cloud Services Gateway (CSG) is an appliance that provides the foundation for remote-site and branch connectivity and security, delivering SASE services. The next generation of branch appliances, powered by the Intel Atom® processors x7000C Series, provides high packet processing and throughput performance across network and security functions for seamless connectivity and security with next-generation business agility and TCO.

Versa Cloud Services Gateway appliances

Next-gen SASE appliances for agility, performance and security

Versa branch appliances extend enterprise-class, software-defined network services to remote sites, with a consolidated, on-premises edge solution. They offer throughput in the multi-Gbps range, with scalable options for port and feature configurability. The appliances provide carrier-grade reliability using WAN access technologies that range from leased lines to broadband and 4G/5G networks for efficient deployment, backup and load sharing.

Matching performance and security resources to rigorous business needs, Versa branch appliances accelerate control plane and packet plane processing to help increase throughput. It provides hardware acceleration for critical network security functions, including encryption, and integrates data from across the infrastructure into a unified data lake. VersaAI™ taps into this data lake to extract AI/ML insights that it seamlessly applies across the Versa product suite. Platform optimizations also boost packet and control-plane processing for higher TLS/SSL and IPsec performance. These capabilities unite business and technology requirements for cost-effective networking and data protection.

The Versa branch appliances can be delivered in small, low-power, fanless form factors to enhance suitability for deployment in diverse edge locations. They offer console management using wired interfaces or Bluetooth for smartphone app connectivity.

The software-defined operating environment for Versa SASE appliances is based on VOS™ (Versa Operating System), which provides cloud-native networking capabilities, including SD-WAN and scalable routing, as well as integrated security functions. On-demand elasticity offers cost-effective agile capacity, while service chaining with third parties creates a highly extensible environment. Customers have the flexibility to mix and match best-of-breed cloud-native services that meet their changing business needs.

Versa appliances are built for ease of integration into existing or new operational environments. They support standard protocols and log formats for network management, monitoring and reporting, including Syslog, IPFIX, SNMP and NETCONF. They help reduce manual network-management tasks to scale using technology innovation instead of by adding headcount, which also enables teams to focus on value-added work.

Versa's next generation of branch appliances are built on a foundation of Intel technologies. Intel Atom processors x7000C Series drive performance for network throughput as well as encryption and other processing-intensive network security functions. Built-in AI acceleration boosts inference throughput for emerging capabilities.

AI-powered security

The Intel Atom® processors x7000C Series supports Intel® Deep Learning Boost (Intel® DL Boost) for acceleration of AI. Support across popular proprietary and open source frameworks and software platforms makes this performance boost applicable to a wide spectrum of security solutions and functions. Vector Neural Network Instructions (VNNI), a component of Intel DL Boost, works with other platform capabilities to reduce inference time and latency, accelerating AI-enabled security solutions.

Novel approaches may mitigate phishing and prevent data loss or provide anomaly detection to improve AIOps. Additional potential usages for AI acceleration run the gamut of software-defined security such as algorithmic malware detection and malicious URL detection and filtering. AI acceleration technologies such as VNNI also help increase the efficiency of enabled software such as advanced traffic profiling and shaping services.

Processors built for network and security appliances

The Intel Atom processors x7000C Series power the Versa next generation of branch appliances with industry-leading performance across network and security functions. With scalability from two to eight cores and a breakthrough range of built-in hardware acceleration technologies, the processors extend power-efficient throughput for network, edge and industrial usages. Intel Atom processors x7000C Series delivers ramped-up frequency for exceptional packet-processing throughput in SASE and other network and security appliances.

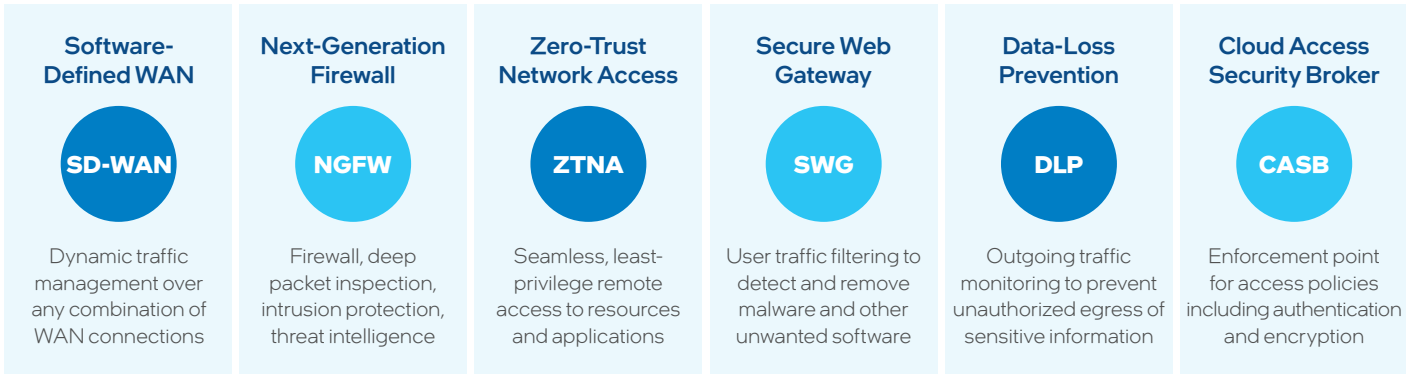
Intel Atom processors x7000C Series delivers power-efficient performance to boost packet and control-plane processing and encryption with an improved processor base frequency of up to 2.4 GHz and LPDDR5/DDR5/DDR4 memory. They are purpose-built to support compact, fanless designs such as Versa appliances, to conform to the space constraints of SASE installations at remote locations.

"We are excited about VersaAI™ technologies in the Versa Unified SASE platform that are powered by these new feature sets. The advanced instruction sets of the new Intel Atom® processors x7000C Series will strengthen the platform's ability to revolutionize security and networking — delivering unparalleled protection and performance innovation for Versa's customers."

– Nikhil Desai, Sr. Director, Products, Versa Networks

The platform boosts packet and control-plane processing — including for TLS/SSL and IPsec — using native instruction sets and platform optimizations. Built-in deep learning inference capabilities support next-generation AI-powered security capabilities for SASE such as detection of zero-day threats.

In addition, the processors enable a hardware root of trust that is especially beneficial in remote edge locations, enabled by Intel platform technologies. Intel® Boot Guard fortifies the root of trust by verifying the integrity of the Initial Boot Block before it is allowed to run at startup. Intel® Platform Firmware Resilience filters malicious traffic on the system buses, verifies the integrity of firmware and restores corrupted firmware automatically. Intel® Platform Trust Technology is a form of a Trusted Platform Module (TPM) for storing and managing keys, passwords and digital certificates.



Common SASE service components.

Accelerating SD-WAN networking and security functions

At the heart of SASE functionality is the combined delivery of network and security functions. SASE components must work together, from client to edge to cloud to data center. Versa helps drive this model with components based on open standards to maximize interoperability and choice, optimized for high throughput and low latency.

Optimized software-defined networking

Versa SASE appliances implement fast packet processing and low latency using optimizations based on the data plane development kit (DPDK). This open source toolkit provides a fast path for packets to traverse between the network interface and application, bypassing the kernel.

Dedicated send and receive queues enable packets to be handled in user space, avoiding the overhead associated with processing kernel interrupts as well as the kernel stack and network driver. The appliances implement DPDK optimizations on Intel® Ethernet network hardware, with flexible options that include the following:

- **Intel® Ethernet Controllers i226** support speeds up to 2.5GbE in single-port configurations.
- **Intel® Ethernet Controllers i350** support speeds up to 1GbE in dual-port or quad-port configurations.

Software-defined security microservices

Versa SASE environments use transport layer security (TLS) as a cornerstone of security operations for data transmission. TLS sessions are broadly divided into a handshake phase and a transmission phase. The handshake phase uses asymmetric encryption to negotiate the session key, and the data transmission phase uses that session key to perform symmetric encryption on the data for protected transmission.

These modern edge environments require large numbers of TLS requests, which place significant encryption demands on the system, especially during the handshake phase. Versa branch appliances address that overhead using multiple acceleration technologies enabled by Intel Atom processors x7000C Series, including the following:

- **Intel® Advanced Vector Extensions 2.0 (Intel® AVX2)** uses 256-bit registers, doubling the data width of predecessor technologies, helping reduce the number of CPU cycles required to handle a given amount of input data. This instruction set increases throughput for cryptographic operations without the use of additional hardware accelerators. Intel AVX2 also provides bit-manipulation instructions that benefit encryption.
- **Intel® Advanced Encryption New Instructions (Intel® AES-NI)** accelerate processing-intensive parts of key expansion, encryption and decryption based on the Advanced Encryption Standard (AES). Because the instructions operate in hardware, they reduce the attack surface for side-channel attacks and other software-based vulnerabilities. That property also reduces CPU resource and power requirements, with further benefits in constrained SASE environments.
- **Intel® Multi-buffer Crypto for IPsec Library (Intel® IPsec_mb)** simplifies the implementation of multi-buffer processing for authentication and encryption algorithms. Multi-buffer processing enables the use of Intel AVX2 instructions to process multiple independent buffers at the same time, so that multiple encrypt and decrypt operations can be executed in one execution cycle. By handling more encryption per clock, Intel IPsec_mb prevents TLS bottlenecks — especially during the handshake phase — and improves overall throughput.
- **AES-NI Multi Buffer Crypto Poll Mode Driver (DPDK aesni_mb PMD)** provides poll mode driver (PMD) support for Intel IPsec_mb. The PMD constantly polls the network interface for new packets, so that the NIC does not need to raise a CPU interrupt each time it receives a new packet. This approach is more efficient in the context of large numbers of small packets associated with authentication and encryption for IPsec.

Conclusion

Versa's next generation of branch appliances use the purpose-built compute power of Intel Atom processors x7000C Series to extend enterprise-grade networking and security to thin enterprise edge locations, small/home offices and remote branch offices. They provide dramatically accelerated encryption for high TLS/SSL and IPsec throughput, as well as robust AI inference for next-generation packet-processing and security functions. The combination of Intel and Versa technologies can help enable cloud-native performance, efficiency and value.

More Information

Versa CSG Appliances

Intel Atom® processors x7000C Series

Solution provided by:

Performance varies by use, configuration and other factors. Learn more at intel.com/PerformanceIndex: Intel Atom® processors.
Availability of accelerators varies depending on SKU. Visit the Intel® Product Specifications page for additional product details.
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details.
No product or component can be absolutely secure.
Intel technologies may require enabled hardware, software or service activation.
Not all features are available on all SKUs. Not all features are supported in every operating system.
Intel may change availability of products and support at any time without notice. All product plans are subject to change without notice.
Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel Global Human Rights Principles. Intel® products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.
No product or component can be absolutely secure.
Your costs and results may vary.
Intel technologies may require enabled hardware, software, or service activation.

0324/LH/MESH/356876-001US