Solution Brief

Multi-Cloud Software-Defined Networking

intel + vmware®

Increase Security and Optimize Performance with VMware SASE™ on Intel® Architecture

Secure Access Service Edge (SASE) architecture cost-effectively handles business-critical requirements for performance, reliability, capacity, security, and control to enable distributed workforces. VMware SASE™ on Intel® architecture provides a scalable solution that ensures improved application performance securely in a distributed workforce environment.

As businesses have adapted to the pandemic, enterprises now support extensive remote workforces and the cloud services that help those dispersed teams function. Effectively handling the sudden and dramatic growth in their remote-access networks has left many IT Operations teams struggling to configure and manage complex environments. Consumer-grade broadband often fails to consistently meet the performance requirements of business workflows, and a lack of traffic control makes it impossible to prioritize business applications or to mitigate congestion.

Enterprise IT must provide end users the same stable, responsive experience at their remote workplaces that they would expect in a traditional office setting, as well as services tailored to distributed teams, such as high-quality voice and video for collaboration and reliable VPN connectivity to maintain productivity. This transition has dramatically accelerated digital transformation within many organizations. As they make this shift, enterprises must also protect networks, applications, and data from evolving security threats, with workflows where distributed users access cloud-based applications, as the network perimeter has vanished.

Software-defined wide area networking (SD-WAN) provides a solution that optimizes network connectivity and assures application performance. Secure Access Service Edge (SASE) extends the SD-WAN architecture and brings cloud networking and cloud security together to deliver flexibility, agility, protection, and scale for enterprises. VMware SASE is a cloud-defined solution that provides centralized, software-defined connectivity and security for remote workers and branch offices, optimized for Intel architecture.

The Growing Reach and Benefit of SASE

Gartner predicts, "SASE will be the dominant consumption model for WAN edge for new and refresh deployment by 2023."[1] SASE improves service levels for remote workers and sites, increasing performance and reliability while enhancing security with cloud-native approaches in place of outmoded ones focused on backhauling network traffic through data center choke points. By uniting the cloud networking and security functions, SASE provides benefits to both end users and enterprise IT such as the following:

- **Cloud-first approach**. Most enterprises run their applications across multiple public and private clouds, and it is challenging in such disjointed environments to maintain high levels of security and user experience. SASE provides quick, efficient cloud/ SaaS access using purpose-built, optimized access for cloud and SaaS applications.
- **Intrinsic security.** Remote workers often access corporate resources using networks that are outside the control of IT, which brings with it an array of difficult-to-assess threats. With a natively distributed security model, SASE gives enterprise IT powerful tools to manage the risks associated with corporate data residing outside of the controlled network.
- **Assured application performance**. SASE helps enterprise IT ensure that remote workers and sites have reliable, optimal network performance for critical applications as well as day-to-day enterprise computing needs. This ability is critical as users place demands on the network by consuming bandwidth-intensive services or downloading large files.
- **Operational simplicity**. SASE replaces traditional hub-and-spoke, hardware-centric networks with topologies built to facilitate cloud and SaaS access, so workloads scale rapidly and cost-effectively. Enterprise IT can focus on a combined stack for branch networks, remote access, network security, and content security, streamlining operations and reducing the complexity of support.

A Simple, Robust Approach to Implementing SASE

VMware SASE on Intel architecture provides a comprehensive and extensible platform to users working from a wide variety of locations and devices to get access to applications in the datacenter and/or cloud (Web, SaaS or IaaS) securely, as shown in Figure 1. It combines cloud-delivered SD-WAN and security from VMware with Intel® architecture-based hardware and software to ensure and enhance user application performance anywhere. VMware SASE also extends its platform to other services, including delivering analytics, edge compute, private 5G, and other services.

VMware SASE solution is reliable and can scale as needed, with a consistent approach and architecture. For example, Intel provides a range of hardware technology, development tools, and reference architectures for virtualized network function (VNF) infrastructure.

VMware SD-WAN uses an appliance known as a VMware SD-WAN Edge, which provides secure and scalable connectivity to remote workforces. The solution can aggregate multiple network links such as cable and DSL broadband internet services, mobile carrier networks, and leased lines, abstracting them and managing them as a pooled connectivity resource. VMware SD-WAN can support many network protocols, including broadband, LTE, MPLS, and 5G.

> Together, VMware and Intel deliver capabilities that make SASE an important part of network transformation strategy to support changing application needs in a distributed world.

By steering application traffic over the optimal WAN link with packet-level responsiveness, VMware SD-WAN ensures performance and utilization efficiency for all available bandwidth. VMware SD-WAN also provides network segmentation for isolation of traffic across the WAN on the basis of policies by application, location, business group, and other factors. Thus, for example, data traffic for accounting applications could be isolated from general Internet traffic flows, or payment cards traffic could be isolated from all other traffic.

VMware SD-WAN Orchestrator is a single point of management that enables configurations of multiple devices and policies, centralized monitoring and control, and enhanced visibility into the performance and reliability of applications over the WAN in real time. Based on that information, organizations can accurately gauge the impact of their WAN on application performance and responsiveness, to help improve the end-user experience.

The SD-WAN solution based on VMware and Intel technologies accelerates SASE deployment to help ensure secure connectivity to branch and edge locations while improving application performance and reliability. VMware SASE delivers the following services today:

- **VMware SD-WAN** – Delivers an exceptional user experience with secure, reliable, and efficient access from wide variety of locations to any cloud application. It's a multi-tenant, cloud-based gateway that is hosted in multiple points of presence (PoPs) across the world. There are 3000+ gateways deployed in more than 150+ PoPs worldwide.
- **VMware Secure Access** – Combines with the world-class VMware Workspace ONE solution to ensure remote users to get access to the corporate network securely. VMware Secure Access™, part of VMware SASE™, has been named a leader in The Forrester New Wave™ Zero Trust Network Access report, Q3 2021.[2] Zero trust network access (ZTNA) is based on the principal that no device, user, network, or packet is trustworthy.

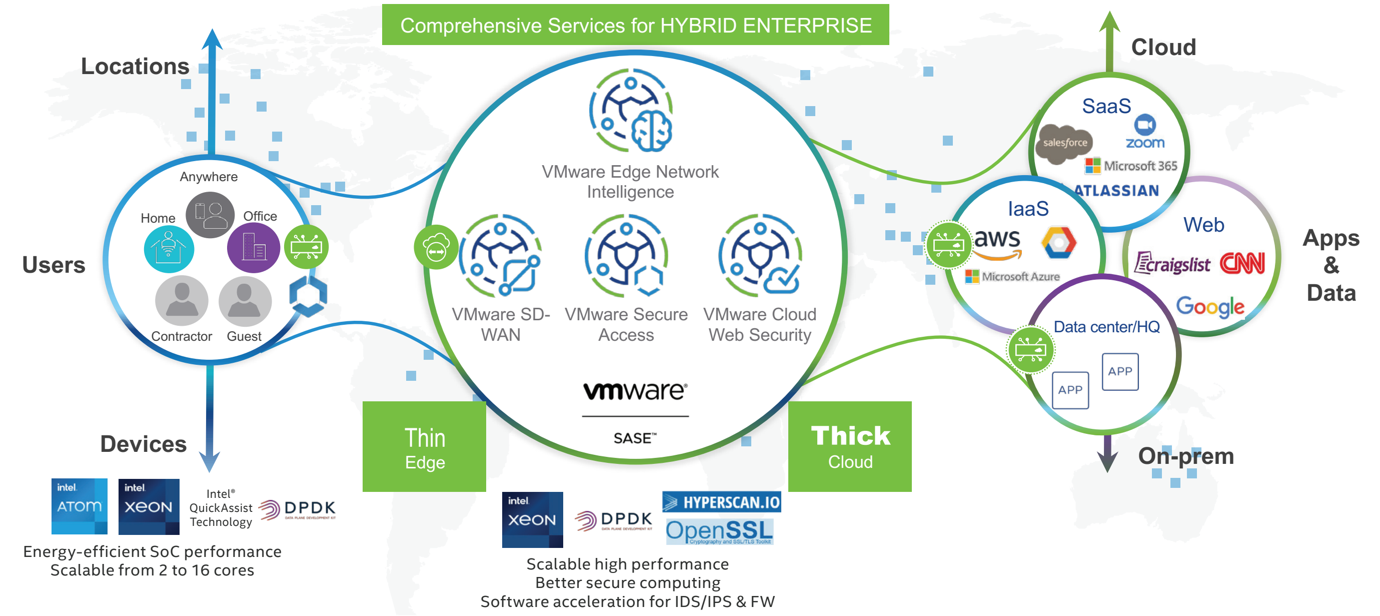


Figure 1. VMware SASE platform, powered by Intel.

- **VMware Cloud Web Security** – A cloud hosted service that protects users and infrastructure accessing SaaS and Internet applications from threats, offering visibility, control, and compliance.
- **VMware Edge Network Intelligence (ENI)** – Proactively manages client experience with AIOps for end user and IoT device performance, security, and self-healing in wireless and wired LAN, SD-WAN, and SASE. EMA's Shamus McGillicuddy writes about the vital role of AIOps in solving the IT challenges of a distributed workforce in the EMA analyst paper, "Prepare for a Work-From-Anywhere Future with AIOps-Driven SASE."

  The solution employs machine-learning algorithms and modern big data analytics to process high volumes of data from a wide range of network, device, and application sources. In doing so, the solution auto-discovers end users and IoT devices, automatically establishes baselines, understands every client interaction, and detects anomalies to provide actionable insights for proactive operations teams.

Benefits of VMware SD-WAN on Intel® Architecture for VNF Deployments

Virtual services on the Intel architecture-based VNF infrastructure on the VMware SD-WAN Edge reduce the need for additional hardware at remote work locations. This approach allows for fast, efficient delivery of data protection services.

VMware SD-WAN Edges are based on a range of Intel® platforms, using the Intel Atom® and Intel® Xeon® processors, with consistent architecture and capabilities across a breadth of devices, as shown in Figure 2. Edge device capacity requirements are determined by the throughput demands of the various applications that are being accessed by the users and by the number of virtualized network services such as firewalls and intrusion protection that are running as VNFs on the appliance.

With hardware options that support WAN connectivity from 100 Mbps to multi-gigabit speeds, Edge devices enable a coherent environment for management, security, and control across branches while balancing capacity and cost requirements.

This scalability tailors the solution to specific requirements, from a small or home office to a large branch, with a range of application and traffic requirements. Intelligent traffic controls optimize utilization of hardware resources, with granular capabilities for prioritizing and shaping network traffic. The breadth of Edges available also provides scale for various sizes of remote locations, as illustrated in Figure 3. This breadth helps network operators meet performance needs for responsiveness, service-level agreements, and latency sensitivity.

Using Intel architecture to host the VMware SD-WAN Edge offers a number of advantages. Responsiveness is enhanced with the ability to perform functions such as accelerating encryption in hardware. Scaling edge devices across Intel® platforms helps meet evolving network throughput requirements. Integration with the VMware management and provisioning framework reduces operational complexity and supports configuration across all locations.

Co-engineering by VMware and Intel has built optimizations into the solution using the Intel developer tool set, taking advantage of capabilities built into Intel platforms, as illustrated in Figure 4. VMware SASE is optimized for Intel architecture using the following technologies:

- **Data Plane Development Kit (DPDK)** is a library of open-standard software drivers originally developed by Intel that drive up packet-processing performance by routing network packets around the Linux kernel.
- **Intel® QuickAssist Technology (Intel® QAT)** provides a software-enabled foundation for security, authentication, and compression, significantly increasing performance and efficiency.
- **Intel® AES New Instructions (Intel® AES-NI)**[3] accelerates key parts of the encryption algorithm in hardware, making pervasive, end-to-end encryption possible without degrading performance.

Tolly Group evaluated the performance of VMware SD-WAN on Intel architecture with single as well as dual WAN link connectivity. The Tolly Group results showed a 45 percent improvement in VoIP quality and an improved download time of 71 percent for a video file on a single WAN link.[4]

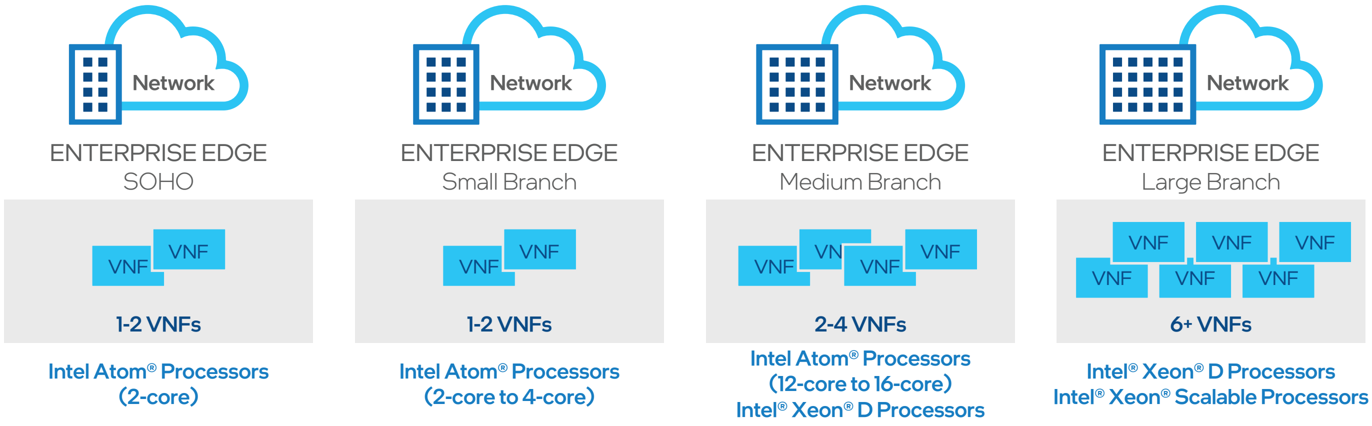
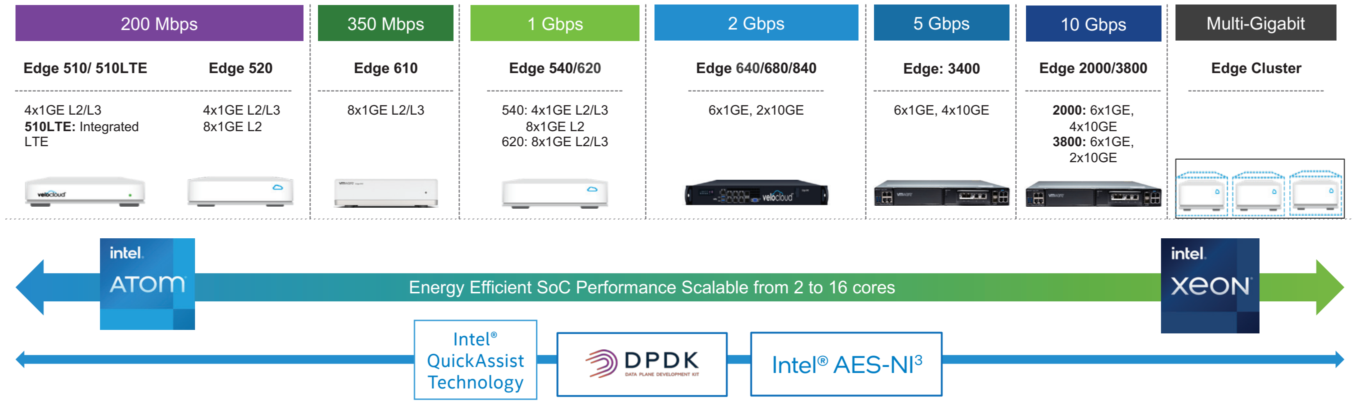


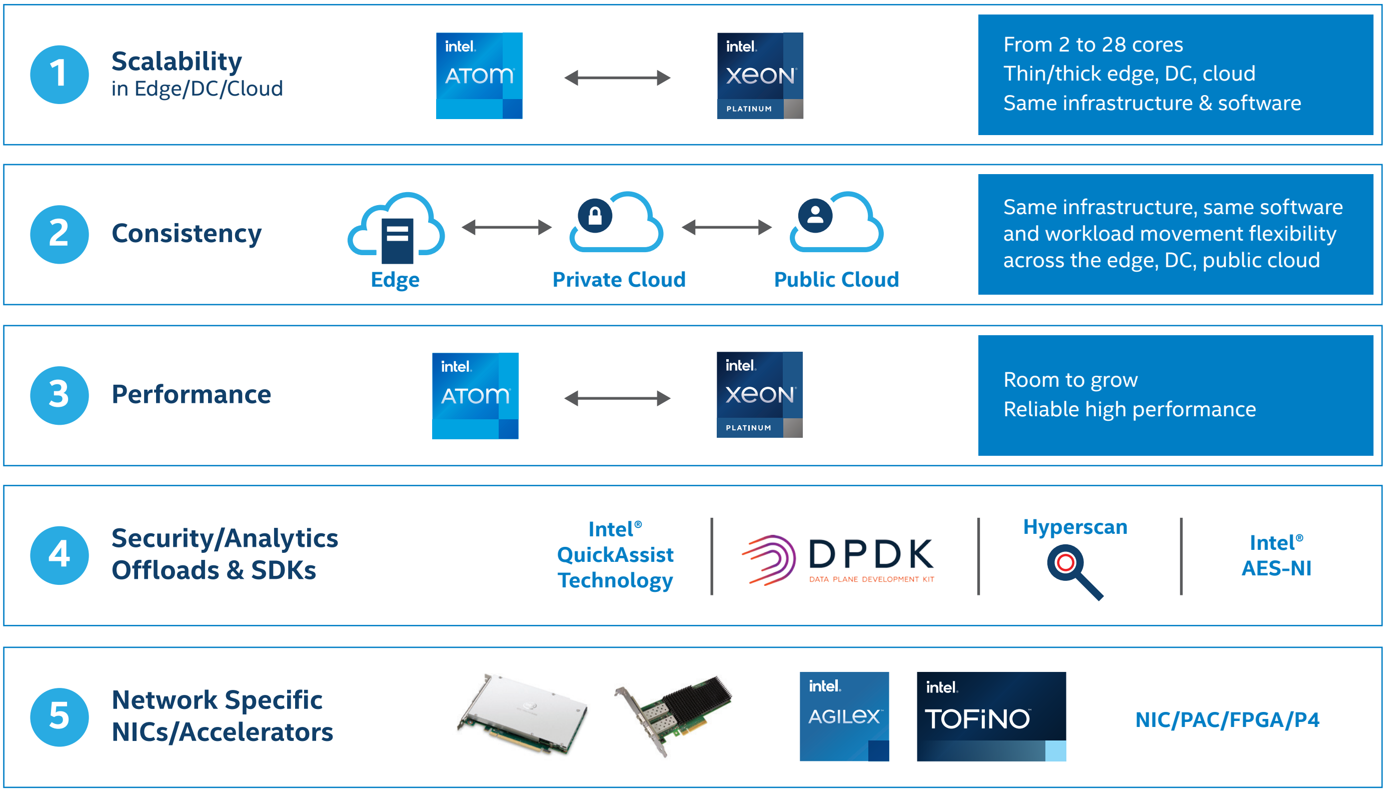
Figure 2. Scalability and consistency across different sizes of branch and edge locations.



200 Mbps		350 Mbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps	Multi-Gigabit
Edge 510/ 510LTE	Edge 520	Edge 610	Edge 540/620	Edge 640/680/840	Edge: 3400	Edge 2000/3800	Edge Cluster
4x1GE L2/L3 **510LTE:** Integrated LTE	4x1GE L2/L3 8x1GE L2	8x1GE L2/L3	540: 4x1GE L2/L3 8x1GE L2 620: 8x1GE L2/L3	6x1GE, 2x10GE	6x1GE, 4x10GE	**2000:** 6x1GE, 4x10GE **3800:** 6x1GE, 2x10GE	

intel. ATOM
Energy Efficient SoC Performance Scalable from 2 to 16 cores
intel. XEON
Intel® QuickAssist Technology
DPDK
DATA PLANE DEVELOPMENT KIT
Intel® AES-NI3

Figure 3. VMware SD-WAN edge appliances.[5]



1 **Scalability** in Edge/DC/Cloud

From 2 to 28 cores
Thin/thick edge, DC, cloud
Same infrastructure & software

2 **Consistency**

Same infrastructure, same software and workload movement flexibility across the edge, DC, public cloud

3 **Performance**

Room to grow
Reliable high performance

4 **Security/Analytics Offloads & SDKs**

5 **Network Specific NICs/Accelerators**

Figure 4. Intel® architecture benefits and advantages for uCPE/SD-WAN Edge.

Conclusion

Increasingly distributed enterprise workforces have increased the need to run enterprise workloads on SD-WAN appliances and other edge devices. VMware SASE utilizes Intel technology to enable network transformation, optimizing the use of diverse WAN links as a virtualized logical whole while increasing application performance, scalability, and security. Intel platforms provide development tools to optimize the performance of the SD-WAN edge, as well as a consistent architecture across Intel Atom and Intel Xeon processors that scale to meet current and future application demands.

With the VMware and Intel solution, networks can become more agile, dynamically adapting to changing application needs, providing easy access to cloud-based services, and simplifying ongoing deployment. The combined hardware and software edge is explicitly designed for zero-touch deployment without on-site IT, making it well suited to distributed workforces. Once the SD-WAN solution is deployed, operations can be simplified with real-time monitoring, analytics, and reporting on network activity. With VMware SD-WAN on Intel hardware, network managers have a streamlined, flexible, and robust route to transform their networks to meet emerging application deployment and performance needs.

Learn More about the VMware and Intel partnership:

www.intel.com/vmware

Solution provided by:

intel. + vmware®

[1] Source: Gartner, Inc., Forecast Analysis: Gartner's Initial Secure Access Service Edge Forecast, by Analyst Joe Skorupa, Nat Smith, Published 26 August 2020.

[2] Source: The Forrester New Wave™: Zero Trust Network Access, Q3 2021

[3] May not apply to every platform.

[4] https://sase.vmware.com/resources/vmware-work-from-home-test-report-by-tolly.

[5] Check VMware SD-WAN datasheet for complete information on connectivity options and maximum bandwidth licensed.