WHITE PAPER

Delivering the Promise of SASE

The Lumen-VMware partnership combines best of breed providers

LUMEN®

Introductions

There's been a change in the architecture of business. Not that long ago, business was centralized; now it is decentralized. Workers are everywhere, not just in the office. Applications might be in a data center, in the public cloud, in an edge compute facility or delivered through a web browser in a Software as a Service (SaaS) model.

This change was underway before the COVID-19 pandemic, but the global shock accelerated the trendlines. This new way of work brings lots of flexibility for efficient operations, new business models, lower costs and a host of other benefits. However, it also brings new security concerns. The expanding edge of the enterprise network creates opportunities for innovation; but it also creates a new landscape for cybersecurity threats and complicates the basic IT function of managing access to resources. SD-WAN allowed enterprises to take a step forward in managing security through centralized policy setting, but this was only a step in a much longer journey.

Secure Access Services Edge (SASE), an idea originally developed by Gartner Inc., is emerging as a new security framework for this decentralized enterprise world. SASE is the convergence of the enterprise WAN and cloud-based security technologies into a unified solution. As SASE shifts from concept to reality, enterprises will have a lot riding on the transition. SASE will need to "just work" even though it is composed of different parts, each of which requires its own expertise and roadmap into the future. This whitepaper argues that a partnership of best-of-breed providers is the ideal way to deliver SASE, and uses the combination of Lumen and VMware as a prime example of such a partnership

SASE is the way to secure the new decentralized architecture of business. Toward that end, this white paper will:

- Trace how the enterprise reached this point of needing a solution such as SASE
- Examine the importance of edge computing to fulfilling SASE's promise
- Explain the Lumen-VMware partnership

Gartner saw the future

The early 2000s were not that long ago when measured by the calendar. Yet, it was an eon ago according to the way we live and work. Back then, a typical enterprise user worked in an office building, usually at a desktop computer. Mobility was defined by the notebook computer that was often plugged into receiving stations that turned them into fully featured desktops. The smartphone did not exist until the iPhone was introduced in 2007; and the tablet was not a commercial success until the iPad sometime after that.

Many people who entered the workforce in the last ten years might not recognize that picture of a functioning enterprise and its technology underpinnings. Today's enterprise is highly distributed. Workers might be at the office, or at home, or in a hotel room, or in a retail branch, or walking down the street tapping on a smartphone. Applications like enterprise resource planning (ERP), salesforce automation and many others are in the public cloud, the private cloud, offered via SaaS or through an edge compute facility as well as an on-premise data center. Data varieties and sources are growing in diversity and the enterprise investment is shifting from the centralized data center to the edge to realize lower latencies, greater flexibility through local analytics and increased security through approaches like SASE. International Data Corporation (IDC) reports that 73 percent of [survey] respondents view edge as a strategic investment. The consultancy also forecast that by 2024, 50% of new enterprise IT infrastructure deployed will be at the edge rather than in corporate data centers.1

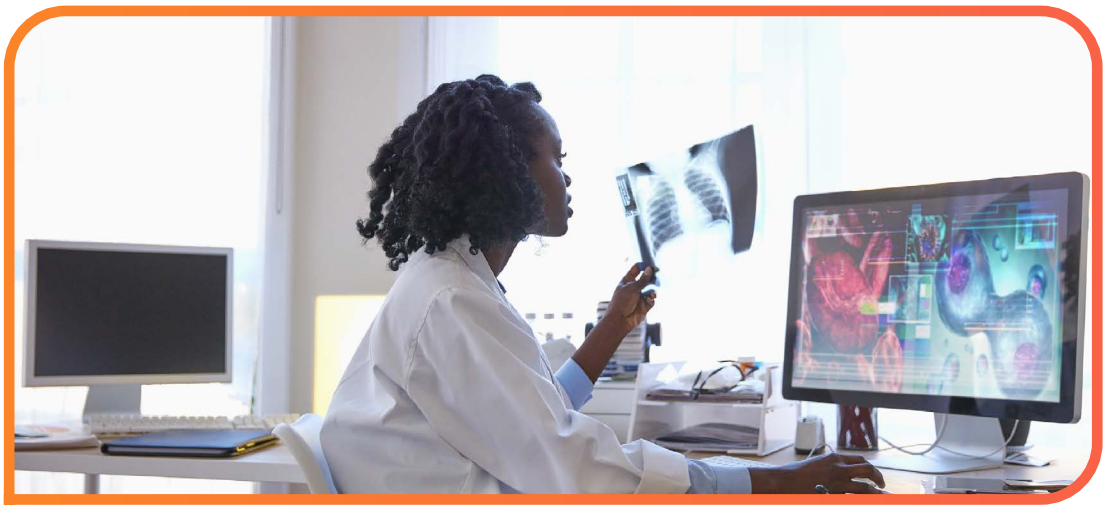
These shifts have great implications for network usage and topologies. Networks today come in many flavors from the on-premise LAN, to public broadband and the WAN is the strategic network that creates the circulatory system that keeps the enterprise working. The advent of SD-WAN created an overlay network on this patchwork to restore some IT control over access, data routing and security protocols in this highly distributed model. SD-WAN allowed enterprises to use the best network available for each individual use case whether that was MPLS in one instance or broadband from a branch location in another.

Centrally setting security policies that applied everywhere was a major step forward for securing the enterprise amid a rising tide of threats. Yet, the practical operation of those security measures often meant that traffic was backhauled through data centers where the resources were available to enforce security. That caused traffic congestion, increased costs, added complex gateways, network hops and introduced application latency as well as delaying authentication for people just trying to log in and do their jobs.

We are living through a sea change in how to think about enterprise security. The ideal architectural location for deploying security has moved from the centralized data center to the decentralized edge. Just as computing and access was distributed, security also needed to be distributed. In fact, in IDC's recent survey, 27.4 percent of respondents cited security/data protection related to negative impact on operations/applications as one of the top two Primary Motivations for Deploying Edge Solutions.[1]

It took industry consulting and analyst firm Gartner, Inc., to observe in 2019 that the core issue was more than just an architectural problem. Gartner's prescription was SASE, an integration of access and security into a single user experience and architectural approach to the WAN. SASE started life as a conceptual rallying point for the enterprise user community. Of course, that was 2019. As enterprises emerge from the disruptions of the COVID-19 pandemic, this concept increasingly lines up with the way enterprises are actually operating

Crises have a way of accelerating trends and driving innovation faster. As enterprise workforces headed home during the crisis and now seek to preserve the flexibility in a more hybrid model (a combination of in the office and work at home) after the crisis, new security needs continue to multiply. An explosion of VPNs might aid in security, but would be expensive and potentially unwieldy at scale; and an army of VPNs would not solve all the authentication issues of a mobile workforce. Cobbling together and managing a patchwork of security services is equally problematic. Conceptually, SASE avoided these issues. Gartner predicts that by 2024, at least 40 percent of enterprises will have explicit strategies to adopt SASE.2 Technology trends are converging to enable this rapid move from concept to reality for SASE. One of the most important trends is edge computing.



Gaining an edge

SASE is cloud-based. Its functions can be distributed across the WAN. This flexibility can be enhanced further by extending it out into the network. The decentralization of computing puts a new emphasis on what's going on at the network edge – and there's a lot going on.

More devices need access from more places than ever before. A single user can require access from multiple devices and multiple locations. The Internet of Things (IoT) is adding potentially billions of new devices blipping out data at regular intervals. As this proliferation of users and use cases continues, the attack vectors also proliferate. The complexity of authenticating users and regulating access to resources grows.

The inefficiencies of backhauling traffic to a central data center for security purposes were noted earlier. They only get worse as new security protocols such as "zero trust" move into the mainstream. Delivering the combined access/security experience requires new ways of delivering security features without delaying access, introducing latency or risking network compromise through questionable accesses. Security features and applications need to decentralize and move closer to points of access, one of the basic ideas behind SASE.

The emergence of edge computing provides an avenue for accomplishing this convergence of access and security. Edge computing is sometimes called "edge cloud" because the approach moves compute power and storage out of the cloud and distributes those resources much closer to where data is produced and applications are consumed. It reduces latency by avoiding the sheer distance of travel between the edge and a cloud data center as well as the complexity of network hops in between.

Lumen's ongoing investments in fiber networks and edge facilities creates the potential for enterprises to leverage the best of centralized cloud computing and decentralized edge computing. Most of the large cloud providers already linked many of their data centers to Lumen® Fiber and Lumen's own edge facilities are on those blazing fast networks. Through Lumen, enterprises can build a software stack in the cloud and replicate it at the edge. Many processes – security among them – can be performed at the edge rather than sending data all the way to the cloud and incurring increased latency as well as the cost of transport. Lumen's edge facilities can stay in synch with cloud resources, sending only that data that's necessary for further analytics, long-term storage or some other more centralized function. With Lumen's edge computing investment, SASE stacks can be deployed in dozens – if not hundreds – of facilities, rather than a handful of centralized cloud data centers.

SASE, Lumen's edge cloud and VMware's software create a robust solution, delivering VMware's expertise in cloud-based SASE to the enterprise edge.

LUMEN®

Partnership key to integrating SASE technologies

SASE started life as a concept put forth by Gartner. Bringing it into reality requires integrating different parts of the solution, each of which has its own complexity. A partnership approach delivers the best customer experience. A DIY approach would require coordinating different vendors and a high level of management and administration. Cobbling together a security approach is a recipe for potential disaster. Not all solutions will be the same. All the pieces are important and they have to "just work" for the customer. SASE requires the merging of leading technologies in cloud, network, security software and services that can spread any one vendor thinly. Gartner wrote: Watch out for slideware, especially from incumbent vendors that are ill-prepared for cloud-based delivery as a service model. This is a case in which software architecture and implementation matters.

> Lumen and VMware saw the opportunity to work together on what they do best and deliver an integrated solution that's simple for the customer to use.

The two technology providers were already working together on SD-WAN, with Lumen offering the managed overlay network powered by VMware's cloud-based toolset. This established the business model in which Lumen focuses on the network, implementation and ongoing management while VMware advances its toolset with ongoing collaboration to ensure ease of integration. This SD-WAN experience can help to relieve VMware of the need to deploy a proprietary customer-premise SD-WAN appliance. The Lumen-delivered service uses a more generic x86-based box on-premise, most commonly referred to as Universal CPE (uCPE), that is already incorporated into Lumen's edge compute architecture. This reduces costs to the customer by allowing for additional virtual network functions and applications, simplifying deployment for all parties.

Lumen's edge compute infrastructure creates points of presence (POP) for VMware's SASE stack. The VMware suite provides an array of SASE services delivered at the edge and protecting the overall network

VMware places its SD-WAN capability at the core of its SASE offering. This includes all the policy-setting, routing, orchestration and functionality of a world-class SD-WAN. The stack includes a variety of security functions that create the SASE-specific experience of secure access, such as

- **Zero Trust Network Access (ZTNA):** ZTNA implements a Zero Trust model, where users have no visibility of corporate resources, much less access to them, without explicit permission. Users access each individual application, not the full enterprise network, via a secure, encrypted connection. The network automatically applies the right security services, allowing only trusted devices and users to access the application. The network does this for both on-premises and cloud-hosted applications
- **Cloud web security:** Cloud Web Security brings together best-of-breed security capabilities: SSL proxy, URL filtering, anti-malware, Cloud Access Security Broker (CASB), data loss prevention (DLP), remote browser isolation (RBI), and more. Incorporating these services into the VMware SASE PoP, Cloud Web Security provides secure, direct, and optimal access to SaaS and public Internet access.
- **URL filtering:** The VMware SASE PoP cloud-delivered URL filtering service follows category-based classification. It supports wildcard-based URL permit and deny lists for HTTP and HTTPS traffic. Policy configuration and management are accomplished through the VMware Orchestrator. URL policies are part of the security rules distributed by the VMware Orchestrator
- **Cloud and browser sandboxing:** Cloud sandboxing is used to protect against web-based threats caused by the downloading, installation, and execution of unknown software code, which could otherwise allow hackers to access personal data or get access into the enterprise network. Remote browser isolation (RBI) creates a lightweight sandbox environment for evaluation and viewing of content. Web browser sessions are isolated from the network and executed remotely in a cloud-based platform
- **Edge network intelligence:** ENI leverages multiple sources of data to provide a coherent and correlated set of actionable insights. It examines the network experience from the perspective of end-users and IoT devices, bringing together visibility and performance information about networks (e.g., LAN, SD-WAN, Wi-Fi), services (e.g., DHCP, DNS, RADIUS), and applications (e.g., Zoom, Microsoft 365, Workday). VMware ENI focuses on the enterprise edge with a vendor-agnostic approach to optimize end-user and device performance and security

Lumen can offer these POPs around the world through its edge infrastructure. Lumen provides the edge-network platform as well as the services that make the solution viable such as support, management and single-billing interface for the customer. Together, Lumen and VMware make SASE a reality and easy for the customer to purchase and use.

The customer gets a best-of-breed solution in every aspect. Each individual technology involved in the total integrated solution will be upgraded automatically. It incorporates SD-WAN and brings security and access together into one managed service, delivering the promise of SASE

Protecting the new architecture of businesss

TIn 2019, Gartner saw the approaching need to converge security and access into a single enterprise solution. In 2020, a pandemic accelerated the existing trends demanding that solution such as work from home, branch automation, hybrid workforces, increased investments at the network edge and others. Enterprise needs will evolve from this new baseline rather than returning to the past.

By combining security and access into a single solution, SASE will be part of that ongoing evolution. Because of the different technologies that combine to deliver SASE, this white paper has argued that a partnership of premiere suppliers is the best way to bring this solution to enterprise customers.

The Lumen-VMware partnership does just that. VMware focuses on the SASE stack. Lumen deploys it in its network of edge cloud facilities and provides the customer interface and services that make it usable. Together, they are securing the new architecture of business.

Footnote(s)/Disclaimer(s)

1. SD-WAN: Enabler of innovative edge services; IDC; April 2021 https://discover.lumen.com/vmware/sd-wan-enabler-of-in?lx=6mkCub
2. Top actions from Gartner's hype cycle for cloud security, 2020 https://www.gartner.com/smarterwithgartner/top-actions-from-gartner-hype-cycle-for- cloud-security-2020/?utm_source=PDF&utm_medium=Pillar&utm_campaign=SASEGuide

* This document is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen products and offerings as of the date of issue

vmware CLOUD VERIFIED

vmware PARTNER
PREMIER SOLUTION PROVIDER

Why Lumen?

Lumen provides the fastest, most secure platform for next generation applications and data. We are a Tier 1 global WAN provider, delivering award-winning solutions1 and services across ~450K route miles of fiber. With a deeply peered internet backbone and a CDN with 75+ Tbps of total edge capacity, we provide traffic steering expertise, enhanced network management and visibility to see global threats before they impact your business

866-352-0291 | lumen.com | info@lumen.com

LUMEN®