[eBook]

The convergence of Network, Security and Application Delivery

How unified SASE and SD-WAN amplifies performance and protection in a cloud-first world

CLOUD365
getting IT done for you

[index]

[introduction]

Welcome to the new normal, where the lines between in-office and remote work are blurred, employees demand more flexibility, and companies scramble to adapt to a different way of operating without compromising security and connectivity. Status quo is hybrid now.

Network and security architectures were typically built around the data center for access by users in set locations. This doesn't really work anymore as we've entered a cloud-first and work-from-anywhere environment, with different access requirements. Establishing a perimeter around the data center and the company's main campus has become obsolete because there are so many users outside of that perimeter using myriad devices and apps. The scenario has become extremely fragmented and distributed but hybrid users still need secure and fast access regardless of where they are: at the office, working from home, or on the go.

In short: we are in a global and barriers-free world where combining security and performance is key to succeed. The challenge now is transitioning to a strategy that simultaneously protects enterprise assets, allows hybrid users to access resources rapidly and effectively from anywhere, and does not create extreme CAPEX pressure.

On top of that, business leaders are looking to future-proof their investments, after years of expensive renewal cycles in enterprise hardware and software from multiple vendors that don't always provide interoperability and integration capabilities.

So, how do we go about it? Yes, there is an optimal way. Let's explore how to do it.

[Demystifying concepts: SD-WAN and SASE (Secure Access Service Edge)]

SD-WAN, or Software-Defined Wide Area Network, is an incredibly powerful and holistic virtual WAN model that includes connectivity, orchestration, and management and can support multiple security approaches. With 'software-defined' connectivity, enterprises have flexible control over what paths applications traverse, whether it is broadband internet, 5G/LTE, MPLS or a private network, through centralized policy management.

By centralizing control in the cloud and combining multiple networking and optimization functions at the edge, customers gain greater flexibility, reliability, agility, and performance combined with better economics. A SD-WAN can be delivered as a fully or co-managed service or deployed by an enterprise as part of what is called a DIY model.

According to Reportlinker, the global SD-WAN market reached $3.4 billion in 2022 and is set to grow at a compound annual rate (CAGR) of 31.9% till 2027, when it will generate $13.7 billion. It's a staggering number showing that many companies will upgrade their network infrastructures and center them around software-based technology, leaving hardware-centric and CAPEX-heavy approaches behind.

This sounds great, which is why some leaders might be wondering why SD-WAN isn't enough and there's all of this talk about SASE and unified approaches.

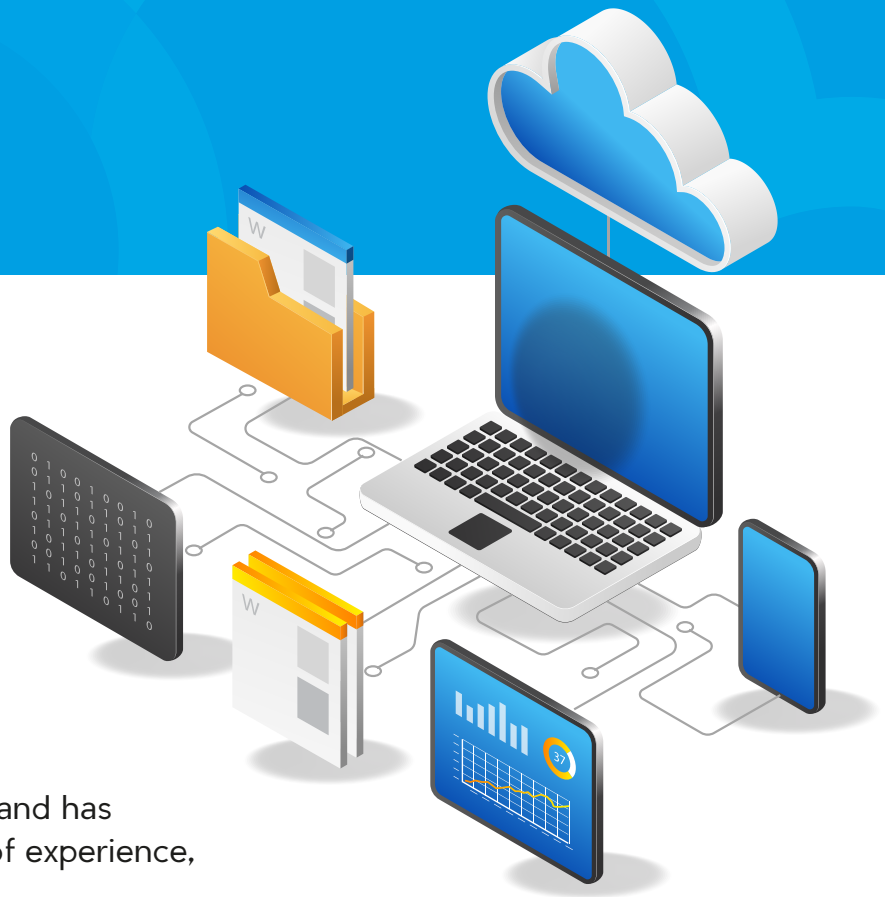
Secure Access Service Edge, better known through the acronym SASE, is a concept that Gartner coined recently, in 2019. The consultancy firm describes it as a solution that "delivers converged network and security as a service capabilities, including SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA)."

Primarily delivered as-a-service, SASE is designed to support secure access use cases anywhere they're needed in branch offices, in remote work locations, and on-premises. It combines real-time context, compliance policies, and the identity of the device or entity to enable zero-trust access. In short, it allows companies to perform advanced security analysis in the cloud as opposed to directing traffic to the data center before sending it to the cloud.

Gartner says companies need to start creating a plan to migrate from their traditional perimeter and hardware-centric solutions to a SASE architecture over the next 18 months. It's very likely you've heard about this and questioned what are the benefits of migrating in a seemingly short period of time. Especially when most companies have made heavy investments in hardware and software and have close ties with multiple vendors for various solutions.

While that might be true, the fact is that the environment has changed and technology is there to serve the needs of the company, not the other way around. We've left behind traditional WANs and their inefficient backhauling of traffic from branch offices to the main data center and back. We have entered the cloud-first architecture.

[What are the benefits of both?]



SD-WAN is a sophisticated evolution of traditional WANs that supports applications hosted in multiple locations, from public or private clouds to on-premises data centers and SaaS services. It ensures high levels of application performance even with shifting or deteriorating network conditions, it has the ability to adapt and self-monitor and minimizes the need for IT intervention.

Because it allows a multitude of WAN transport forms at the same time and has intelligent monitoring, SD-WAN ensures a good and consistent quality of experience, while also preventing outages in business-critical applications.

SD-WAN offers several benefits to enterprises that operate in the digital economy. It provides improved application performance through a combination of WAN optimization techniques and the ability to dynamically assign QoS as per application's (and user) requirements.

SD-WAN technology automates and speeds up site deployments, configurations, operations and troubleshooting tasks. It provides for automatic failover so, in the case of one link failure or congestion, traffic can be easily redirected to another link. SD-WAN's flexible and agile nature provides for optimal choice and utilization of connectivity, thereby reducing upfront cost and lowering operating expenses.

The ‘as-a-Service’ is crucial, in that SASE is meant to be consumed as a managed service, aligned to cloud services adoption. Core networking capabilities include SD-WAN for connectivity, application optimization, and multi-cloud access, while security includes firewalls and secure web gateways amongst others. So, it seemingly marries all the network services and security solutions in one unified cloud experience.

SASE addresses challenges that include how to ensure consistent network and application performance, how to ensure pervasive security across distributed users, devices, and applications, and how to deliver seamless support experiences that are delivered as-a-service. It leapfrogs traditional approaches with their inefficient, costly, and complex traditional hub-and-spoke architectures that don’t align to a cloud-first world.

In the same way that the cloud delivers scale, simplicity, scalability, and optimal TCO, freeing IT from just keeping the lights on, SASE now brings these benefits to networking and security. It introduces the ease of deployment and consumption demanded by enterprises of all sizes.

As it reduces the number of people and of vendors needed to implement and manage secure access, it also means savings both at the start and with ongoing costs. A CAPEX/OPEX win at a time when everyone’s bottom line is under pressure.

SASE refers to a more overarching architecture that includes Network as-a-Service and Network Security as-a-Service with SD-WAN’s connectivity playing a vital role in any SASE deployment.

[Shifts driving their convergence: Digital Transformation is disrupting the infrastructure]

The world changed dramatically over the past few years, with a major acceleration in digital transformation projects spurred by the constraints of the covid-19 pandemic. Ready or not, the infrastructure that supported businesses and services for decades is being disrupted, as changes come faster than ever, and hybrid models can't be placed over legacy systems.

Many companies jumped right into the digital revolution to avoid being left behind and it is now causing a host of new problems. It's hard to innovate on top of systems that were designed for a previous era.

Now, organizations need to provide flexible, efficient, and secure access to their resources no matter where users are. Not just because remote work has taken hold, but also because every company has sort of become a digitally-savvy, cloud-native business, reaching customers anywhere and providing online and offline services with the same expectation of quality.

Mega changes pushing the convergence of Network, Security and Application delivery:

Workload Shift - SaaS, IaaS and Agility - Traditional Data Centers making way for "Cloud-First". Data center not the center of data!

Workforce Shift - Hybrid Workplaces and Flexibility - Static Perimeter Security is making way dynamic Pervasive Security.

Expectation Shift - Convenience and Simplicity - Rigid service consumption is making way for on-demand, as-a-service, usage-based models.

This is the backdrop of the disruption that is taking place, as organizations move to an "as-a-service" model that includes networking, security, data protection, data in transit, and data at rest. They must be able to scale up and down while continuing to develop agile applications and use big data analytics to consistently make better business decisions. It's challenging, it's disruptive, and it's inevitable. And it can't be addressed using the traditional multi-vendor approach, which is not easily scalable (requiring constant hardware updates) and has security risks. Not only that, but it also requires skilled IT teams that can maintain and operate multiple solutions from different vendors, at a time when tech talent is in short supply.

This is why the digitization of the economy is a major driver behind the unified SASE and SD-WAN approach with security and networking at the forefront. As businesses transform and become digital-first, security concerns abound because there are more devices and access points, so the attack surface is larger than it ever was and the risks to the organization are nothing short of existential.

Since an SD-WAN offers smart routing, and SASE centers around security and centralized management, their convergence is an optimal scenario for the company of the future.

On the other hand, it makes it easier to manage an increasingly complex hybrid network with fragmented environments that will not remain static it will continue to adapt, evolve, and augment.

To be digital-first, organizations have to open the floodgates so that access is possible off-premises and on the go, no matter where and when.

[Advantages of a converged solution]

The convergence of smart networking and security solutions has been in the works for years, as industry leaders called for a new category that brings the best of both worlds together. The market is ripe for innovation; both SD-WAN and SASE solutions are forecast to grow at a double-digit rate over the next few years. The global SASE market, according to research by Markets and Markets, will reach $4.1 billion by 2026 at a CAGR of 26.4%. And Gartner expects that 60% of organizations will have a plan and a timeline to adopt SASE by 2025, a major jump from just 10% in 2020.

The key now is differentiation. A converged solution future-proofs your network. As Gartner describes, "users, branch offices, and edge devices need secure access to your data and applications that are spread everywhere throughout the cloud and data centers."

A distributed, cloud-based architecture with centralized orchestration and management enables security to converge with networking and offers a seamless, one-stop solution allowing for full observability for both networking and security behaviors with simplified and fast change management.

Converging networking and security in an all-in-one service helps CIOs modernize their infrastructure and simplify operations. In today's distributed world where applications are everywhere and employees can be anywhere, a unified SASE approach provides enterprises the security, connectivity, and flexibility they need to rapidly adapt to an unpredictable future.

5 benefits of a Converged Approach

Application Acceleration

Experience fast access to mission and business critical applications hosted locally or in the cloud, from both branches and remote offices.

Advanced Security and Centralized Management

Deliver comprehensive security and data protection for enterprise and web traffic, coupled with central definition and enforcement of security and access policies.

Visibility

Enjoy complete visibility on application usage and performance.

Reduced Hardware Footprint

Eliminate the need for additional security and optimization appliances.

Rapid Deployment

Configure, deploy, and activate new sites in days instead of weeks or months, positively impacting enterprise productivity.

[From theory to practice: A comprehensive, integrated approach to delivering secure connectivity without compromising application performance]

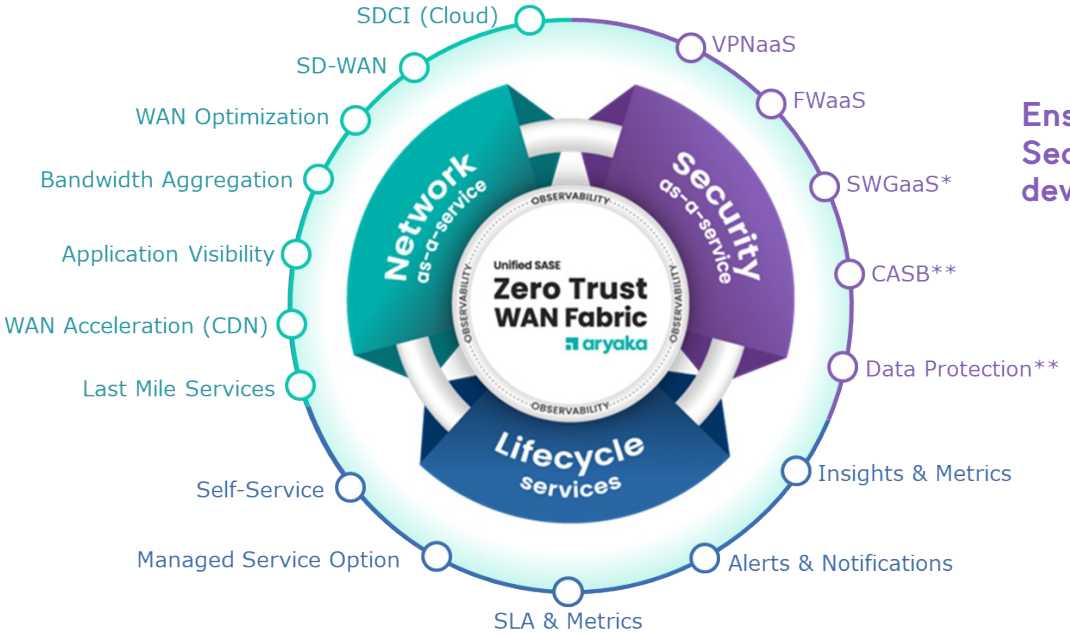
How to transform everything that we said before into action? Really simple. With the Zero Trust WAN solution based on Unified SASE Architecture from our partner Aryaka – integrating Firewall-as-a-Service and Secure Web Gateway into Leading Cloud-Managed Networking and Security Services. It is the first to enable enterprises to easily enforce security policies across offices and remote users with unified control while delivering incredible application performance and stability.

Part of Aryaka's Unified SASE, Secure Web Gateway is a defense for Site-to-Internet and User-to-Internet traffic, providing protection from web and internet-based attacks. Combined with its Firewall-as-a-Service, it ensures customers have flexible perimeter security for distributed users, devices, and applications that provides advantages such as:

Improved patch and update readiness	Reduced operational complexity	Correlated view across events
Reduced vendor portfolio	Reduced total cost of ownership (TCO)	Increased capital efficiency

Converging Networking, Security & Life Cycle Services delivered as a service

Delivering a consistent network application performance anywhere



Ensuring a flexible perimeter Security for distributed users, devices and apps

Providing a delightful experience that accommodates evolving and diverse needs

All-in-One

- Networking
- Security
- Support

Agile

- OnDemand
- Flex Consumption
- Continuous innovation without forklifts

Reduced Attack Vector

- Security anywhere
- Single pass
- Single pane of glass

Superior Performance

- Deterministic Global Core
- WAN Acceleration & Optimization
- Guaranteed App Performance (L2)

Reduced TCO

- Replacing multiple vendors with a single converged service

READ THE DATASHEET TO KNOW MORE

[Conclusion and next steps]

We're at a turning point in the digitization of the economy and the transformation of enterprise networks. Strategies that worked well over decades, anchored in secure data centers and on-premises access, have become obsolete. The covid-19 pandemic accelerated trends that were already in place but many companies didn't see them as urgent. They are now. With the adoption of cloud services and digital offerings, organizations started to shift their IT consumption models from multi-vendor products to "as-a-service" solutions and that includes networking and data protection. At the same time, the explosion of remote work and hybrid models created a "new normal" that is here to stay. Old-school network perimeters don't make sense anymore, because the environment is completely distributed and fragmented.

As SD-WAN adoption grows to solve the networking challenges of this new scenario and we are way past the early adoption stage, new issues arise with security. It's why Gartner coined the term SASE, or Secure Access Service Edge, to define a new approach that is more relevant than ever.

The experts at Gartner have urged companies to design and implement a migration plan, and they warn that the enterprise transition to a complete SASE architecture will take time. We know the hurdles all too well: there are existing investments in hardware and software which have not yet reached the end of their lifecycle and can't go to waste. There are also expertise and legacy vendors factoring in.

There are even challenges with SASE offerings many vendors claim to offer a SASE product but don't deliver all of the required capabilities. Not all SASE offerings are created equal, and this is where Aryaka's unified SASE and SD-WAN solution makes a difference. The experienced team at Cloud365 will help you implement it and maximize the benefits of this transition. Head over to www.cloud365.global and let's start the journey together.