eBook

SASE: The 1-Day Route to Zero Trust

GlobalDots

In Collaboration with

CATO NETWORKS

Fast is the New Everything

Ever since the industrial revolution, the equation between time and money has been an unbreakable one.

Today's hyper-digitized reality has taken that to the extreme. Critical KPIs in both core business (e.g., development) and business operations (e.g., IT & DevOps) are time-defined, from time-to-market to MTTR (mean time to remediate). The responsibility to enable faster business processes lays primarily on the shoulders of the IT and security departments. It is our mission at GlobalDots to gear them with the most innovative solutions to succeed.

Technology is a primary speed enabler. Specifically, cloud computing has injected business infrastructures with unprecedented agility.

However, most networking and security solutions today are still painfully incompatible with a cloud-centric business ecosystem. The enterprise network usually consists of a rigid infrastructure and a patchwork of point solutions and integrations meant to adjust it to the changing business needs. Security, by design, is heavily fragmented across multiple applications and domains of physical locations, cloud resources, mobile and remote users. Together, they slow down business.

To resolve this, Gartner has recently defined Secure Access Service Edge (SASE) as a new category of products that fuse enterprise network and its security layer into a single, cloud-based platform. Think of it a network-plus-security-as-a-service.

SASE well-demonstrates the holistic, innovation-driven approach applied into GlobalDots' every project. We therefore explored this trend and its implications on the future of IT & security architecture.

When Silos Tremble

The shortcomings of legacy networking and security infrastructures has been addressed by point solutions patched together. Adding SD-WAN helped transform the low-bandwidth and expensive MPLS connections to Internet links; Adding firewalls enabled secure Direct Internet Access (DIA). This made networking and security into two separately managed technological silos, each made of loosely integrated components. These were the progression steps that lead to the creation of the concept that networking and security should work together natively, as a holistic platform that converge both needs.

This unsustainable architecture now interferes with the primary mission of IT, which is enabling fast and smooth business processes. SASE is driven by the notion that fortifying the two silos one patch at a time is simply unsustainable. It offers an up-to-date solution for IT architecture which is quick to adopt and delivers better performance in lower cost and less management time.

SASE: A New Networking and Security Architecture for the 2020s Business

Gartner's Neil McDonald (security analyst) and Joe Skorupa (networking analyst) formulated SASE as a revolutionary IT cloud architecture. It consists of 4 speed-enabling elements, which essentially increase the proximity between the user, the network, and the resources they want to access.

Cloud-Native Architecture

SASE puts to work the scalability and self-maintenance capabilities of the cloud. Similarly to cloud and CDN distributed architectures, the SASE cloud consists of interconnected points of presence (PoPs). The PoPs run the SASE provider's software that delivers networking and network security as a service. This means automatically implementing updates, new features and bug fixes, as well as self-adaptation to traffic load changes by adding compute nodes.

To augment the latter, SASE must be able to optimize traffic and self-fix, namely automatically reroute processing from failing compute nodes and PoPs to available ones. Having all PoPs run the very same software guarantees an equal standard of service and security across all PoPs and edges, not depending on customer-specific components, thus simplifying the shift of traffic across the SASE Cloud.

Cloud datacenters will connect to the SASE Cloud over multiple tunnels, with all traffic secured and optimized regardless of the source edge, achieving both security and agility for the business. SASE is thus meant to provide a holistic, low-maintenance alternative to service-chaining, legacy point products, appliances or cloud services, which are mostly designed to serve a single tenant and lack the overall cloud orchestration.

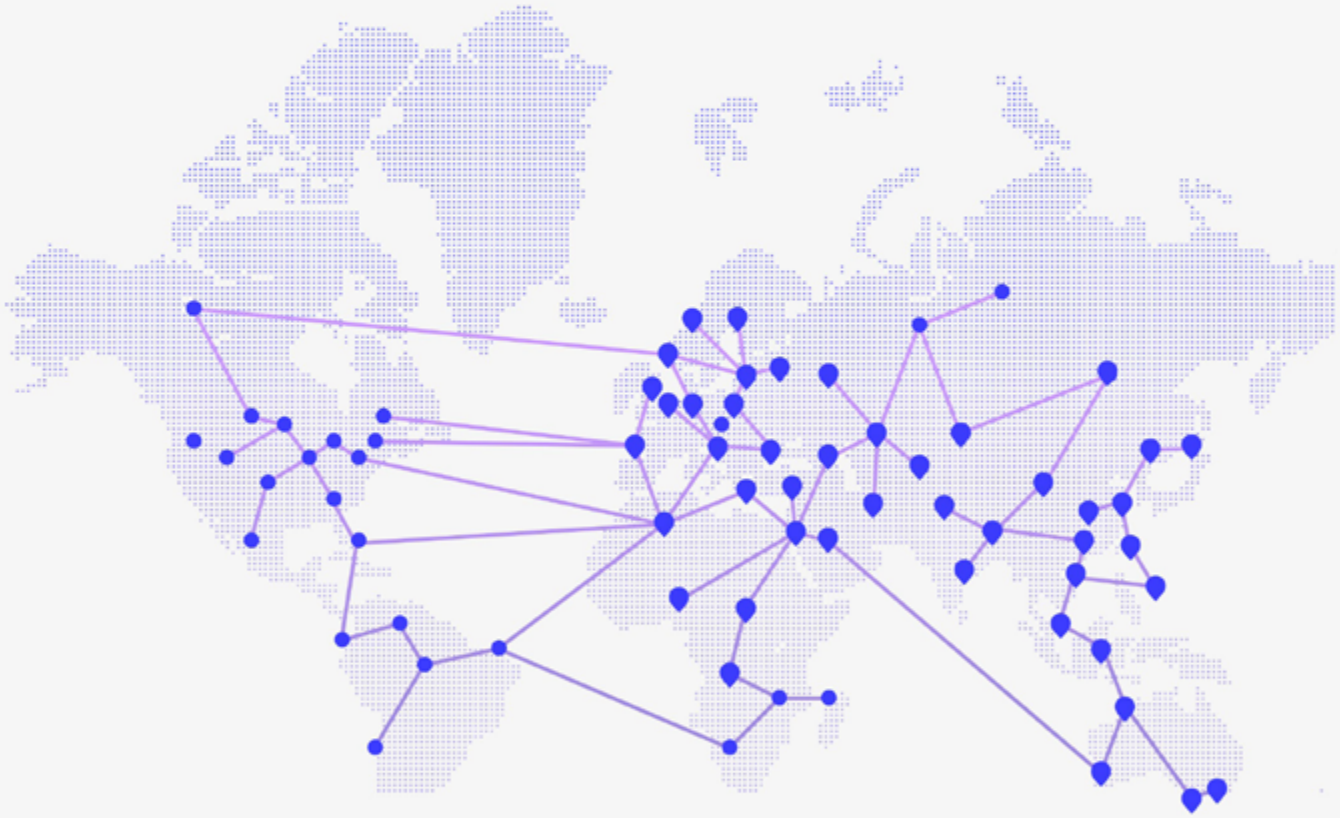
Identity-driven Networking and Security Policies

While cloud security has always been identity-driven, networking is traditionally location-driven. In SASE, an identity is attached to every enterprise entity: a person, an application, a service, or a device. This identity will define the network service and the risk profile to be applied throughout every access life cycle. It provides a broad and dynamic context awareness that will therefore determine the quality and priority of service and the risk-driven security controls to be applied along the way, such as authentication methods and access authorization.

Global Reach: Bringing Edges Closer

SASE is meant to deliver a unified service and security standard across your entire network, and especially to deliver a low-latency service to the enterprise edges, which means both speedy and secure business workflows around the globe.

Therefore, SASE providers will have to strategically deploy a global network of PoPs into cloud and physical data centers to globally serve business locations, mobile and remote-working users. To deliver service across all edges, the network should span beyond public cloud providers' footprints. To enable scalability, it should have high traffic capacity in the first place, as well as surplus connectivity to support both WAN and cloud access.



Equal Support to All Edge Types

As mentioned, SASE is designed to deliver a single standard of service to all edges. Among other things, it extends network optimization and threat prevention from physical location edges and places them in the cloud, to serve branches, cloud resources, users, and edge computing alike.

Edge implementations vary according to the nature of the entity: physical locations will use SD-WAN devices and multiple Internet links to maximize throughput, enforce QoS, and bypass link failure or degradation. Remote workers will use a VPN client or clientless web access to access datacenter and cloud applications with enterprise-grade security. The SASE cloud will connect the various types of edges and deliver optimized and secured experience regardless of the source edge.

The Core Capabilities of SASE:

Plug-and-Play Visibility, Optimization, and Control

There are 2 components to the SASE architecture: SASE Cloud aggregates state-of-the-art networking and security capabilities. SASE edge connectors drive traffic from physical, cloud, and device edges for SASE cloud processing. SASE uses a single-pass traffic processing engine to efficiently apply optimizations and security inspection with rich context for all traffic.

Contrast the SASE model with stacking point products where each product analyzes traffic for a specific requirement, adds overhead for actions like decryption, and lacks the context generated in other network and security point products.

Selected SASE capabilities include:

Authentication Upon connection of an edge, dynamic risk assessment drives activation of multi-factor authentication.

Access Access to key applications and service is controlled by application- and user-aware next generation firewall policies. In addition, a zero-trust network access model can ensure users only access authorized applications without gaining general network access.

Prioritization Application identification assigns priority to the traffic to optimize loss-sensitive applications like Voice over IP (VOIP) and virtual desktop access (VDI) over other traffic such as general Internet browsing. count context, and usually cannot protect non server resources, such as services, containers, serverless functions, etc.

Decryption To enable deep packet inspection, encrypted traffic can be decrypted once to allow multiple threat prevention engines to process the traffic.

Threat prevention Multiple security engines parse the traffic to detect risky access. These include Secure Web Gateways (SWG) that look for malicious websites, anti-malware to prevent download of malicious files, IPS to stop inbound and outbound anomalous connections that are indicative of bot activity, and more.

Data loss prevention SASE applies specific data loss prevention rules to detect sensitive data in the network flows and prevents it from leaving the network. Similarly, a Cloud Access Service Broker (CASB) can enforce granular access control to cloud applications.

While this is a subset of the SASE capabilities, the SASE architecture is designed to rapidly extend the “single pass traffic processing engine” with new ones. This unique benefit of SASE is future proofing the network, extending the SASE cloud and the new capabilities to anyone and everywhere. Similarly, adapting the SASE cloud service to new threats or attack vectors can be done centrally and immediately affects all enterprises and all edges without the need for IT to deploy or activate these added capabilities.

A Sustainable IT Foundation for Today's Digital Business

The Benefits of SASE

SASE creates a holistic platform that connects all edges to the networking and security capabilities they need. This lowers the cost, complexity and risks of supporting the business in a dynamic environment. Here are some of the key benefits of the SASE platform:

Agility Supported by the SASE architecture, IT can deliver optimized networking and strong security to all locations, applications, and users regardless of where they are. Provisioning of new resources and capabilities is fast and simple. Just deploy the right edge client and plug into the SASE platform and corporate policies drive your network and security experience.

Collaboration IT teams can leverage the convergence of network and security to manage all features and policies in a single interface, using a common terminology, and gain deep visibility into network and security events. Cross-team collaboration improves the overall service delivery to the business that often involves a combination of availability, performance, and security requirements.

Efficiency With SASE, IT teams are relieved of the grunt work to maintain on premises infrastructure. Physical topology, redundancy, scaling, sizing, and upgrading is dramatically reduced. IT can now achieve better service to the business, while focusing precious resources and skills on business-specific problems rather than the grunt work of generic infrastructure maintenance.

Cost reduction The simplification of the network and security stack, and the consolidation of multiple point products enables both vendors and customers to reduce the overall costs of keeping the infrastructure running.

What is Not a SASE?

Telco Bundles are the Exact Opposite of SASE

For over a decade, telcos have offered to take away the complexity of managing your network and security stack, through a bundle of point solutions they procure, install and manage. Complexity didn't go away, and your spend increased to pay for both the products and the people to manage them. Also, you were dependent on the telco to do everything for you, often slowing the IT organization to a crawl. This is the exact opposite of SASE: legacy appliances and fragmented management with limited or no visibility. SASE is built with the scalability, self-service, and agility of the cloud. Your telco isn't.

Virtual Machines in the Cloud are Still a Stack of Appliances

Instantiating virtual machines in an IaaS like AWS, Azure and alike is great, but not for SASE. While it does move on-premises appliances to be 'in the cloud', they are still disparate point solutions that lack the cloud-native integration, single pass processing, global reach, and elasticity of a SASE. And, depending on the vendor mix, you'd still need to use multiple management consoles.

Service Chaining Sounds Close, But not Really

Facing the reality of a multi-vendor environment, service chaining is a technique to link together multiple point solutions such as SD-WAN, routers, firewalls, WAN optimizers and more. Regardless of the use of multiple physical appliances or Universal Customer Premises Equipment (uCPE) that host multiple virtual machines, these are still discrete solutions that need to be sized, scaled and managed separately. Ultimately, SASE offers convergence as the key defining attribute and service chaining isn't convergence but loosely coupled linking of point solutions.

The Incomplete SASE: Cloud and Edge Vendors Must Plug Big Holes in their Offerings

Security-as-a-Service vendors have been working to deliver multiple security capabilities via their cloud services including SWGs and CASBs. These vendors still lack the key SASE elements of controlling network flows and natively supporting the WAN edge. Without a natively integrated and mature technology to reliably and securely connect all edges (offices, cloud datacenters, users and devices) to the SASE Cloud, SWGs and CASBs remain a silo that needs integration with other products. Similarly, edge appliance vendors now face the task of building the breadth of SASE Cloud capabilities as globally distributed, cloud-native services. SASE carries such a big promise that a marketing war is likely to erupt between SASE wannabees. Gartner warns that some traditional vendors will try to deliver a SASE-like solution based on wrapping their existing products in a SASE package. Such attempts will create a risk to service quality and delivery, as these technologies weren't designed for cloud-native delivery. In a nutshell, look carefully at the underlying SASE architecture to determine the fit with the expected outcomes.

Future-Proof Your Enterprise Network

Once every few years, new technologies mature and reach a tipping point which requires a completely new outlook on the enterprise landscape, as it keeps evolving too. In the context of cloud security this tipping point created what we call “the new security stack”. It means that today’s enterprise security solutions should have a few traits to be part of this new security stack:

SaaS Consumption Model No more hardware based appliances you need to plan and pay for years in advance. The ability to scale your usage up or down and pay for what you use is crucial in today’s rapidly changing reality.

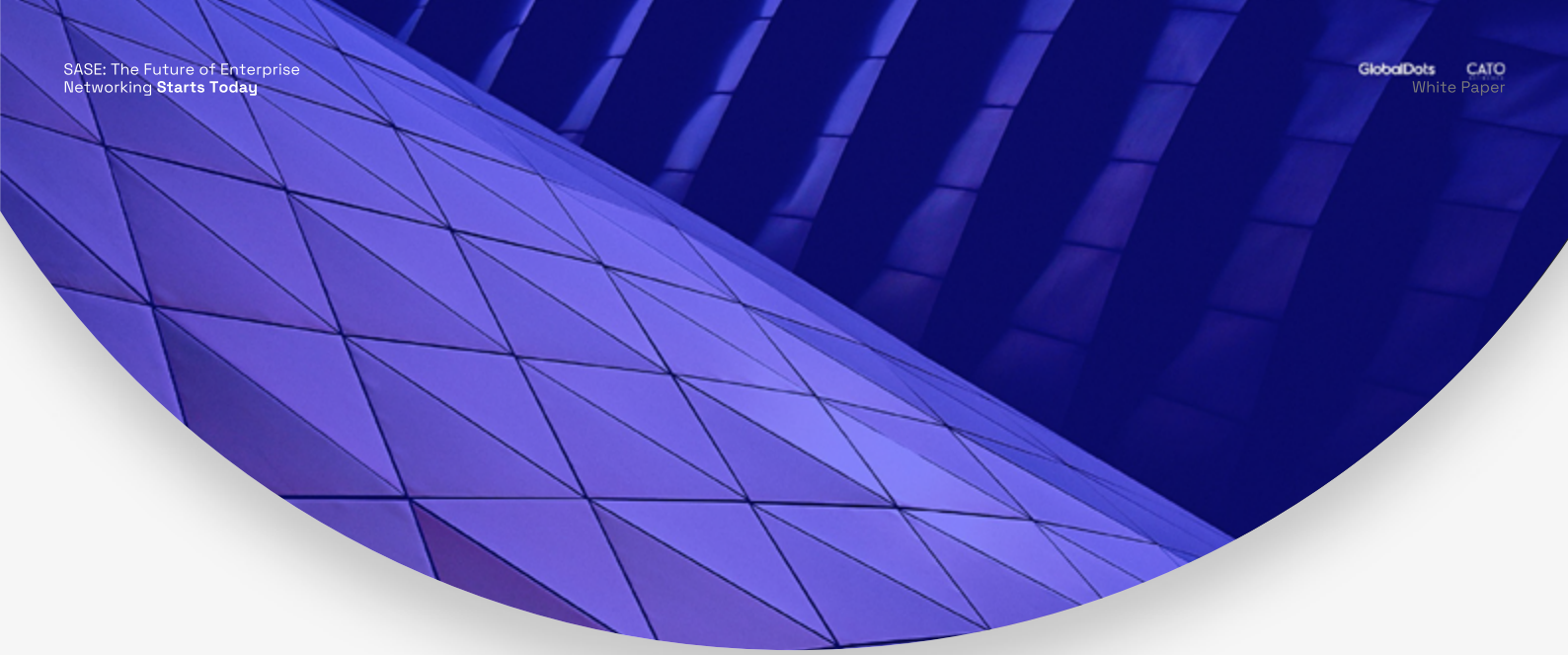
DevOps & Integrations The ability to integrate with existing tools and components within the company’s IT / DevOps environment: communication & collaboration apps (Slack), SIEM (Sumo Logic), API interface to make configuration changes or view reports, Active Directory, GSuite / Office365, HR Systems and other enterprise apps. No more UI-only based solutions you must manage from dedicated interfaces.

Noise-Free Alerts & Remediation The ability to learn the company’s normal patterns and alert / act only on highly suspicious, true positive anomalies. Solutions that have AI or ML capabilities, using big data to determine which activities are malicious and require intervention, and in what priority.

Compliance Assistance Using security solutions that are compliant with the common security standards such as PCI-DSS, ISO-27001, SOC2 etc., and by implementing them, companies can achieve security compliance faster with less efforts involved.

The building blocks that lead to the evolution of SASE from SD-WAN fit perfectly into the new security stack for organizations operating in the 2020s: SASE has flexibility and scale baked into its cloud platform, can integrate with all types of edges (data-centers, branches, devices and cloud providers), enables more secure and compliant enterprise network and operates based on the zero trust model. SASE is not a single security solution, but rather a platform with modular architecture that can be leveraged based on today’s and tomorrow’s evolving needs.

GlobalDots is a team of cloud explorers, always on the hunt for the next emerging, cutting edge cloud technology. Accordingly, we have learned and tested recent developments in Enterprise Networking and Security technologies: from the convergence of networking and security in SASE, through Zero-Trust and IAM practices, to Cloud Security Posture Management. Each new development in cloud security and networking adds another layer of innovation that should be carefully evaluated whether it adds more value to your IT ecosystem, compared to the level of efforts and potential complexity required to adopt it.



About GlobalDots

GlobalDots is a 17-year world leader in cloud innovation, connecting businesses with the latest cloud & web technologies. Fusing an insatiable hunger for innovation with a diligent team of hands-on experts, we help our customers maintain an up-to-date technology position in a quickly-changing world.

We consult, resell, implement, and customize full-stack solutions, including cost & performance optimization, security, connectivity, and managed services, to streamline business processes and provide the foundation for sustainable business growth.