The top 3 benefits of SASE and how to achieve them

Why secure access service edge (SASE)?

Modern digital business models are allowing new levels of customer and employee engagement by delivering globally available access to applications and services that is consistent, no matter where employees and customers connect or what devices they are using.

The notion of network security when your users and applications are distributed is no longer viable in a digital world. Gartner developed a new model of networking and security that matches the requirements of the digital enterprise. They're calling it the secure access service edge (SASE).

> "The secure access service edge is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS, and ZTNA) to support the dynamic secure access needs of digital enterprises." **– Gartner**[1]

BENEFIT #1

Reduces IT cost and complexity

With data spread across cloud applications and SaaS services, and users often working from anywhere, the traditional network-based security model has reached its limit. To compensate, organizations have been forced to deploy additional services to fill the gaps in their security, while greatly increasing the deployment, management, and operating costs with a team that isn't growing fast enough. Even with this increase in cost and complexity, the network-security model still can't scale, isn't agile, and is simply not effective in a digital world.

Instead of trying to use a legacy concept to solve a modern problem, SASE flips the security model. While legacy approaches focused on creating perimeters around applications, SASE focuses on the entities, such as users, that are accessing the applications, and pushes security as close to the entity as possible. As a cloud service, SASE dynamically allows or denies connections to the service based on an organization's defined business rules. It's all done through a single service that unifies a number of previously separate functions such as SWG, ZTNA, and so on.

What to look for

The most important component of a great SASE offering is the architecture it is built upon. Gartner was specific about the type of architecture needed to deliver on SASE's promise. Most importantly, it must be built from the ground up to address the scale required for a fully cloud-delivered security service.

This means it must be a distributed offering that supports multi-tenancy, enabling it to scale globally and dynamically based on demand. It must move away from traditional networking concepts of policies and policy layers and instead be based on business policy. Finally, this architecture must support a truly integrated platform with unified cloud-delivered management.

What to avoid

Gartner specifically cautions against traditional networking security approaches that use VM-based offerings running in cloud provider infrastructures. The use of these VM-based approaches in an IaaS compute environment will have difficulty scaling and provide an inconsistent user experience because of the hair-pinning needed to go between the cloud vendors and the applications users are accessing.

This model relies on a single tenant architecture that tries to use network-based access policies in a SASE model based on user access, which creates vastly more complex deployments that do not translate to a SASE model. Further, these approaches are often based on multiple products that are not truly integrated but are instead stitched together through an overlay UI of independent services often purchased through acquisitions.

> "SASE policy decision and enforcement capabilities need to be everywhere the endpoint identities will be located...SASE offerings that use only the internet backbone capacity of IaaS, but without local POPs/edge capabilities, risk latency, performance issues and resultant end-user dissatisfaction." **– Gartner**[1]

BENEFIT #2

Delivers a great user experience

There's a good reason why SASE's primary focus is on user experience. When users were on the network, applications were in the data center, and servers and infrastructure were owned and managed by IT, it was easy to control and predict user experience. Now that applications are distributed across multiple clouds, your method of accessing these applications is still based on the old model of a VPN connecting to a network for security. This model brings the user to the security and not the security to the user, which is required for a great user experience. SASE calls for security to be enforced close to the users, intelligently managing user connections at the internet exchanges, and optimizing direct connections (peering) to cloud applications and services to ensure optimal bandwidth and low latency.

What to look for

The key to delivering a great user experience comes down to providing optimal bandwidth with the lowest latency. The only way to do this effectively is to reduce hops to get to the applications and ensure the right bandwidth is allocated through bandwidth controls.

The right approach places the security stack as close to the user as possible in internet exchanges across a widely distributed geographic deployment. Accessing applications from these exchanges requires the ability to intelligently route traffic to the application's closest geographic location through direct peering.

What to avoid

Offerings based on VMs running in cloud providers or IaaS will require traffic hair-pinning. Such offerings are specifically called out in the SASE paper as unqualified to be defined as a SASE solution and should be avoided.

This is primarily because VM-based architectures do not scale and do not control the connection from the user, instead doing so from the application compute environment and, thus, cannot guarantee a good user experience. In addition, these offerings cannot dynamically scale and require usage planning that lacks the ability to allow changes later without scheduled downtime.

> "SASE architecture matters. Ideally, the offering is cloud-native, built on microservices with the ability to scale out as needed. To minimize latency, packets should be copied into memory, acted upon and forwarded/blocked, not passed from virtual machine (VM) to VM or from cloud to cloud. The software stack should have no specific hardware dependency and be instantiated when and where needed to deliver the risk-optimized and policy-based capabilities to the endpoint identity." **– Gartner**[1]

BENEFIT #3

Reduces risk

Security is all about risk identification and avoidance. SASE as a cloud service is designed to address the unique challenges of risk in the new reality of users and applications being so spread out. By defining security as a function built into the very fabric of the model and not a function that's separated from the connectivity of services, it ensures that all connections are inspected and secured, no matter where users are connecting, what apps they are accessing, or any encryption that may be used.

What to look for

The key to risk reduction is the ability to abandon the concepts of network-based connectivity and instead connect users to applications based on true zero trust network access (ZTNA). ZTNA ensures that only users who are authorized to access an application can do so, and this authorization is defined through business-based policies and not complex multilayered policy definitions.

Another way a SASE platform reduces risk is by removing the attack surface. By hiding the corporate network and source identities from the internet, SASE prevents adversaries from targeting you with attacks such as DDoS.

The SASE model is delivered through a proxy-based architecture that handles all communications between users and applications. This architecture ensures that all traffic can be decrypted and inspected, and provides full visibility. Lastly, the SASE architecture is built with full data context being exchanged between entities and applications to ensure that all connections meet compliance and data governance requirements.

What to avoid

Traditional approaches to perimeter security used a firewall-based model that looked at packet streams and determined risk based on the inspection of those streams. While this model worked for perimeter-based security, it breaks down with the new challenges of a SASE-based deployment.

The biggest issue is that a firewall architecture running as a service determines threats after the fact, allowing them to reach the destination before discovery. The reason is simple: they are incapable of holding the data and determining its results before sending it. This limitation makes session decryption and data protection exceptionally difficult because these are functions that require the stream to be held and reassembled, similar to a proxy.

With a firewall service, the decrypting, inspecting, and reassembling functions require a separate process that's decoupled from the service, complicating policy, introducing latency, and resulting in poor performance—and it often allows limited functionality when implemented. Furthermore, SASE requires a single-pass architecture to process all of the content at once. Stream-based firewall offerings also expose the host network's source IP address to potential adversaries, effectively advertising their attack surface which can lead to targeted attacks.

> "Many of the capabilities of SASE will use a proxy model to get in the data path and secure the access. Legacy in-line network and enterprise firewall vendors lack the expertise to build distributed, in-line proxies at scale, risking higher costs and/or poor performance for SASE adopters." **– Gartner**[1]

The Zscaler approach to SASE

Zscaler Cloud Security Platform is a SASE service built from the ground up for performance and scalability. As a globally distributed platform, users are always a short hop to their applications, and through peering with hundreds of partners in major internet exchanges around the world, Zscaler ensures optimal performance and reliability for your users.

Zscaler, founded more than a decade ago, built its platform on the same principles as SASE. Today, more than 400 of the Forbes Global 2000 organizations trust Zscaler to lead them into the digital era, securely.

Because of its time in the market, Zscaler has proven its architecture was built to scale, currently processing up to 120B+ transactions at peak periods and performing 175K+ unique security updates each day.

The Zscaler SASE architecture is delivered across 150+ data centers globally, ensuring that users get secure, fast, and local connections no matter where they connect.

Learn more

To learn even more about SASE go to **zscaler.com/gartner-secure-access-service-edge-sase** and read what Gartner has to say about the future of network security.

To learn more about Zscaler's approach to SASE go to **zscaler.com/products/secure-access-service-edge**.

1. Gartner, The Future of Network Security Is in the Cloud; 30 August 2019; Lawrence Orans, Joe Skorupa, Neil MacDonald

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler connects users to applications and cloud services, regardless of device, location, or network, while providing comprehensive security and a fast user experience. All without costly, complex gateway appliances.

zscaler™