

Everything You Need to Know About SASE - blueAPACHE

Canonical: <https://www.blueapache.com/blog/everything-you-need-to-know-about-sase>

Details:

Summary

This blog post, "Everything You Need to Know About SASE", is a blueAPACHE article from 2022 covering security. One of the most significant challenges that businesses face today is to make business critical data available to employees wherever they are, over any bearer, on any device whilst protecting and securing their access and data. It is written for readers evaluating emPOWER SASE, emPOWER Security. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2022
Topic	Everything You Need to Know About SASE
Services referenced	emPOWER SASE, emPOWER Security, emPOWER Core Network & DC Interconnect
Named products or vendors	Microsoft, Zoom, Google, Gartner

Article

One of the most significant challenges that businesses face today is to make business critical data available to employees wherever they are, over any bearer, on any device whilst protecting and securing their access and data. To define the acronym, SASE (pronounced "sassy") stands for Secure Access Service Edge, and it's a technology solution that's been created to help organisations meet this challenge. With the ever-evolving threats and the possibility that one simple mistake could open your whole organisation to individuals with nefarious intent, keeping things under control has never been more important. It's important therefore to understand what SASE is, the problems it can help solve, and the benefits you can expect to receive. Plus, we'll be providing a clear path for getting started with SASE in your business, so read on to learn about the latest in front-line cyber defence. What is SASE? SASE combines cybersecurity protocols such as cloud access security broker (CASB), Zero Trust and firewall as a service (FWaaS) with wide area networking (WAN) and packages them as a single, cloud-based service. SASE solutions have been developed through the recognition that the old concepts of enterprise perimeters and edge devices are no longer fit for purpose when business critical systems are increasingly serviced from the cloud and hybrid work is the norm. Gartner coined the term in a report entitled "The Future of Network Security is in the Cloud", and defined SASE as being driven by "Customer demands for simplicity, scalability, flexibility, low latency, and pervasive security" which is forcing "convergence of the WAN edge and network security markets.". Put simply, this means that

SASE is a cloud native solution that is designed to provide a familiar and seamless experience to hybrid/remote users through a combined network, identity and access, and security functionality. What are the problems that SASE is designed to solve? As society transitions to a phase where remote work is more widely accepted (and, in many cases, has become the norm), organisations have accelerated their adoption of cloud-based solutions for managing many aspects of their business, including workflow and collaboration. While this has previously been secured through enterprise edge firewalls (protecting the premises), and VPNs (enabling access for remote users) the security and control limitations of these solutions were already clear and were made more pronounced with the rise in popularity of public cloud services, and collaborative suites such as Microsoft 365/Teams, Slack, Google Workspace and Zoom. There was also a need to manage user's access privileges based on not only the individual user or group access level but also incorporating device functionality, network capability and location factors. In addition, SASE needs to manage threat registers, patches, software updates and more. Organisations increasingly don't have the resourcing or capabilities to manage these issues across multiple systems and platforms. So SASE will be designed to help organisations meet the challenge of providing a seamless workflow experience to users anywhere and on any device, the use of widespread cloud delivered solutions, and to ensure access, management and security controls are beefed up.

Key benefits of SASE

Improved user experience, allowing a uniformity of workflow management regardless of device, operating system, network access type or location

Enhanced, flexible and consistent security of data and network access for the new hybrid workforce

Improved performance of higher bandwidth applications such as Zoom video calling and Teams meetings

Much improved flexibility through a cloud-based infrastructure which manages a range of security and access policies and controls from one platform

A reduction in complexity by combining a range of legacy solutions into a streamlined set of services that are much more straightforward for your IT team to manage

Zero Trust approach supported, enhancing security by removing trust assumptions when users and apps connect to your network

Significant cost savings can be realised through the deployment of a single platform to replace multiple legacy solutions

It's important to note at this point that SASE as it stands is conceptual in that there is no one vendor that offers all the functions we describe in a single platform, although that evolution is underway. How can I learn more about SASE and starting our transition? The road to SASE will be about an evolution of services and capabilities, so you're going to need a partner who is abreast of the latest developments in the field and can help you develop a strategic technology roadmap to guide your evolution. We have certified solution experts in networking, identity and access, and security who can support your organisation's transition. Why blueAPACHE? With more than two decades of experience and a team of expert consultants, blueAPACHE holds ISO/IEC 27001:2022 certification covering its emPOWER Infrastructure and managed service offerings, and offers local 24/7 support. This makes us an ideal IT-as-a-service provider for all of your business needs. To find out more, please contact us directly at: 1800 248 749 </contact/>

Related

emPOWER SASE

emPOWER Connectivity (pillar hub)

emPOWER Security
emPOWER Security (pillar hub)
emPOWER Core Network & DC Interconnect
blueAPACHE Security (case study)

Frequently asked questions

What does the acronym SASE stand for, and how is it pronounced?

SASE stands for Secure Access Service Edge and is pronounced "sassy," a technology solution combining cybersecurity protocols with wide area networking as a single cloud-based service.

Which three cybersecurity protocols does the article say SASE combines with WAN?

Cloud access security broker (CASB), Zero Trust, and firewall as a service (FWaaS), packaged together with wide area networking (WAN) as a single cloud-based service.

Who coined the term SASE, and in what report?

Gartner coined the term in a report titled "The Future of Network Security is in the Cloud," defining SASE as driven by customer demand for simplicity, scalability, flexibility, low latency and pervasive security.

What does the article say about SASE's vendor maturity at the time of writing?

It notes that SASE as it stands is conceptual in that no single vendor offers all the described functions in one platform, although that evolution was underway.

What collaboration platforms does the article name as driving the need for SASE?

Microsoft 365/Teams, Slack, Google Workspace and Zoom, cited as examples of public cloud services whose rise exposed the security and control limitations of traditional firewalls and VPNs.

What seven key benefits of SASE does the article list?

Improved user experience, enhanced and flexible security for hybrid work, improved performance for high-bandwidth apps like Zoom and Teams, cloud-based management flexibility, reduced complexity by consolidating legacy solutions, Zero Trust support, and cost savings from replacing multiple legacy solutions with one platform.

What does the article say organisations relied on for security before SASE, and why were those approaches limited?

Enterprise edge firewalls (protecting the premises) and VPNs (enabling remote access), whose security and control limitations became more pronounced with the rise of public cloud services and collaboration suites.

What credentials does blueAPACHE cite as qualifying it to support a SASE transition?

More than two decades of experience, a team of expert consultants, ISO/IEC 27001:2022 certification covering the emPOWER Infrastructure and managed service offerings, and local 24/7 support.

Source

origin post (2022)

Knowledge Base

What does SASE stand for?

SASE stands for Secure Access Service Edge, pronounced 'sassy.' It is a technology solution created to help organisations make business-critical data available to employees anywhere, on any device, while protecting and securing access and data.

What components does SASE combine?

SASE combines cybersecurity protocols such as cloud access security broker (CASB), Zero Trust and firewall as a service (FWaaS) with wide area networking (WAN), packaging them as a single, cloud-based service.

Who coined the term SASE and how did they define it?

Gartner coined the term SASE in a report titled 'The Future of Network Security is in the Cloud.' Gartner defined SASE as being driven by 'customer demands for simplicity, scalability, flexibility, low latency, and pervasive security,' which is forcing the 'convergence of the WAN edge and network security markets.'

What problems is SASE designed to solve?

SASE is designed to address the security and control limitations of older solutions like enterprise edge firewalls and VPNs, which became more pronounced as organisations adopted cloud-based services and collaborative suites such as Microsoft 365/Teams, Slack, Google Workspace and Zoom. It also helps manage user access privileges based on user/group level, device functionality, network capability and location, and helps manage threat registers, patches and software updates across multiple systems that organisations often lack resources to handle.

What are the key benefits of adopting SASE?

According to us, the key benefits of SASE include: improved user experience with uniform workflow management regardless of device, OS, network type or location; enhanced, flexible and consistent security for hybrid workforces; improved performance of higher-bandwidth applications like Zoom and Teams; much improved flexibility through a cloud-based infrastructure managing security and access policies from one platform; reduced complexity by combining legacy solutions into a streamlined set of services; support for a Zero Trust approach; and significant cost savings from replacing multiple legacy solutions with a single platform.

Is SASE available as a single product from one vendor?

No. The blog notes that SASE, as it currently stands, is conceptual in that no single vendor offers all the described functions in one platform, although that evolution is underway.

How can an organisation start transitioning to SASE?

The blog states that transitioning to SASE will be an evolution of services and capabilities, so organisations need a partner who stays abreast of the latest developments and can help develop a strategic technology roadmap. We say it has certified solution experts in networking, identity and access, and security who can support this transition.

Why do you position yourselves as a partner for SASE adoption?

We cite more than two decades of experience, a team of expert consultants, ISO 27001 certification, and local 24/7 support as reasons it is well-positioned as an IT-as-a-service provider to help businesses with SASE and other IT needs.

How can I contact you to learn more about SASE?

The blog provides our contact details: phone 1800 248 749, or via the contact page at <https://www.blueapache.com/contact/>.