censornet.

TECHNOLOGY LEADER'S GUIDE TO SASE.

Discover why you need it, what it is, and how you get there

Guide

WHY YOU NEED SASE – LIFE AFTER THE PERIMETER

Where users go, security must go also

The widespread shift to remote working brought on by the pandemic was the last nail in the coffin for traditional perimeter-based cybersecurity.

According to **Microsoft's 2022 Work Trend Index**, the number of people working in a hybrid way across the world is up seven percentage points on 2021 at 38%. And the trend is set to increase. Less than half (44%) of business leaders in the UK say their company is planning to require employees to work in-person, full-time within the next year.

Now, workers are using cloud apps as standard and accessing sensitive data and systems from a huge variety of locations, devices, and networks. They're no longer 'inside' or 'outside' the perimeter – they are the perimeter. That means security has to go with them, wherever they are.

38% **of people are working in a hybrid way. Up 7% on 2021.**

44% **(less than half) of business leaders are planning to require employees to work in-person, full-time.**

Context and identity: the new border checks

In this post-perimeter world, effective security means far more than simply keeping threats out of the 'safe zone'.

Instead, defence systems need to be able to rapidly assess context, and particularly user identity, to determine whether to allow onward connection to sensitive systems – taking into account the device and location and geolocation.

Before authenticating a user, organisations need to simultaneously review:

- **Identity:** Does the user have the right credentials?
- **Location:** What network are they joining from?
- **Geolocation:** What country, town, or city are they in?
- **Device and integrity:** Is this their usual device, and is it patched and updated?
- **Time and day:** Is this an expected time for them to request access?
- **Geo-velocity:** Could they realistically have travelled from their last login location to their present location?

WHAT IS SASE?

Secure Access Service Edge

First coined by Gartner in 2019, SASE isn't a product. It's a model that will enable companies to improve network performance and security in a world where users are remote and mobile.

According to Gartner, SASE delivers multiple converged network and security as a service, or SSE (Secured Service Edge) capabilities. Delivered as a service, a SASE approach enables zero trust network access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

> **In simple terms, implementing SASE means developing a cloud-based architecture that centralises management of network and security services in one place. By harnessing autonomous technology, it handles more complexity than is humanly possible.**

The goal of SASE is to provide the rapid, secure access businesses require right across their ecosystem without having to massively scale up investment and manpower. It means working smarter, not harder.

Better protection, faster performance, reduced complexity

In a world without perimeters, working towards SASE gives organisations the peace of mind they need to enable a truly hybrid workforce, providing intelligent security that adapts however they connect. SASE also ensures a more seamless experience for users. If you're the genuine article, you won't even know it's there.

> **Best of all, SASE relies on autonomous, integrated cloud technology – not a massive hiring campaign. For mid-sized enterprises facing a security nightmare, SASE gives maximum bang for their limited buck.**

TWO WORLDS COMBINED

SASE is about network and security services convergence.
For any company's SASE strategy to thrive, both verticals are essential.

A successful SASE plan relies heavily on people. For small and medium organisations who do not have large or evolved networking and security teams, the journey to SASE cannot be reached by pursuing a single networking or security play.

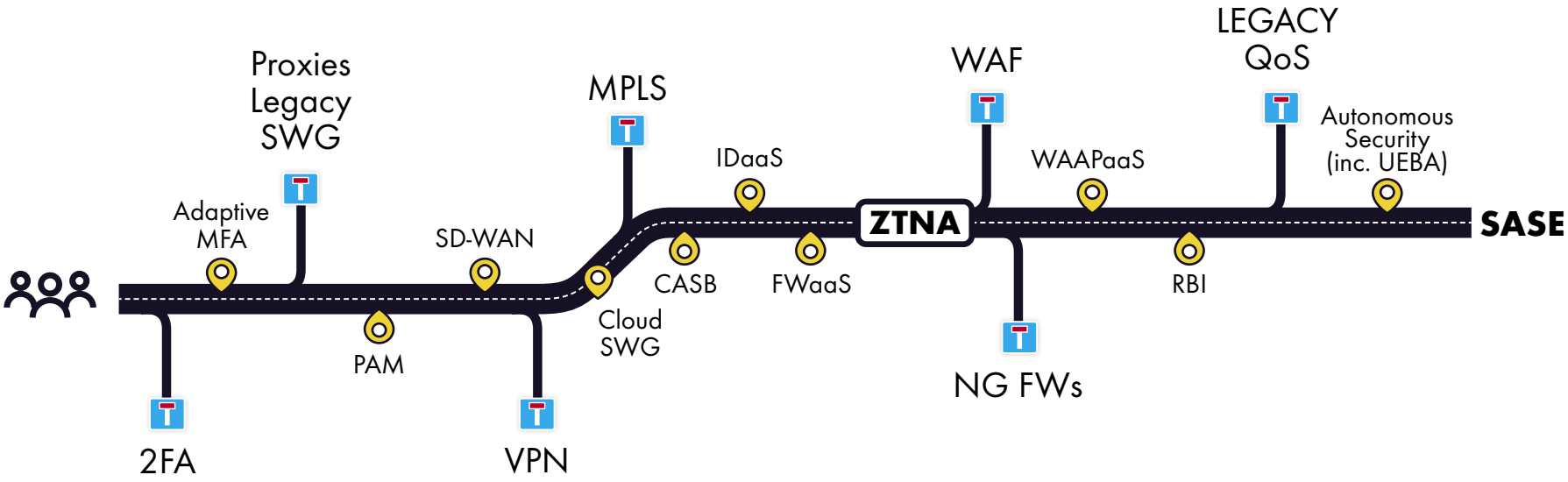
Understanding staff skill sets, particularly those dealing with operational and security challenges, can enable firms to capitalise on their strengths while also identifying and filling any gaps.

And it's not just a convergence of teams. On the journey to SASE, organisations will be looking to converge their core service vendors to minimise complexity and improve performance.

*Web Application and API Protection as a Service

HOW TO GET THERE - STARTING ON THE ROAD TO SASE

SASE isn't a single purchase. It's a strategic direction. The next stop on the journey of cybersecurity evolution.



Avoid dead ends

Wherever you are on the road to SASE, it's important not to take the wrong exit. Avoid investing heavily in dead-end solutions that don't contribute to a SASE state. Why put all your eggs in a VPN or MPLS basket when more sophisticated, cost-effective options are on the horizon?

Zero Trust interchange

On the road from traditional perimeter security to SASE, Zero Trust Network Access (ZTNA) is a significant waypoint. If you've not yet mapped out a route to SASE, start here. Adopting a zero trust approach means continually reviewing user activity to determine access privileges – if you can respond to suspicious activity in the moment, you're on the way to SASE.

STRATEGIC STEPS TOWARDS SASE – REDUCE COMPLEXITY AND OPTIMISE COSTS IN YOUR JOURNEY TO SASE

Rethink procurement practices for your tech stack:

Strive for no more than two vendors for all core services to minimise complexity and improve performance. According to Gartner, SASE can reduce the number of vendors required for secure access from four to six today, to one to two over the next several years[1].

Choose your investments wisely:

The enterprise perimeter is no longer a location. Phase out on-premises perimeter security and focus on cloud-based deliverability.

Build the team for success:

Create an environment of security and networking experts with a shared responsibility for secure access engineering spanning on-premises, remote workers, branch offices and edge locations.

Develop a cybersecurity strategy that has a platform approach:

Chose Security Service Edge (SSE) offerings that consolidate cyber defences across email, web, and cloud to reduce the complexity of managing multiple products.

The perimeter is dead: 41% of mid-market firms believe their plans to future proof cyber defences need development.[2]

[1] Gartner, Hype Cycle for Enterprise Networking, 2021, 7 July 2021

[2] The UK Mid Market on Code Red, Censornet, March 2022

ACHIEVING SASE: A PLATFORM APPROACH TO SECURITY

As organisations strive to achieve a single, cloud-based approach to address the global security needs of a mobile workforce, they need an integrated platform approach.

One that is autonomous and integrated in the cloud; designed to protect today's way of working - from anywhere. A solution which acts autonomously and pre-emptively to halt modern cyber-attack techniques, which side-step traditional points of entry.

Organisations that can connect email, web and cloud application security with identity and context, can close the gaps in their security posture. Not only will a platform approach reduce the cost and complexity of managing multiple vendors, it will lay the foundations for a successful journey to a SASE end state.

By 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services and private application access from a single vendor's security service edge (SSE) platform[3].

To find out how Censornet can help you on the journey to SASE

Contact Form: censornet.com/contact
Phone: +44 (0) 845 230 9590

Email: sales@censornet.com

[3] Gartner, Predicts 2022: Consolidated Security Platforms Are the Future)

censornet.

www.censornet.com