censornet.

THE FUTURE IS SASE.

Discover ten steps to prepare for SASE adoption

Guide

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 a user's context, and particularly their identity, to assign access privileges before they connect to sensitive systems – no matter the device or location.

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 access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

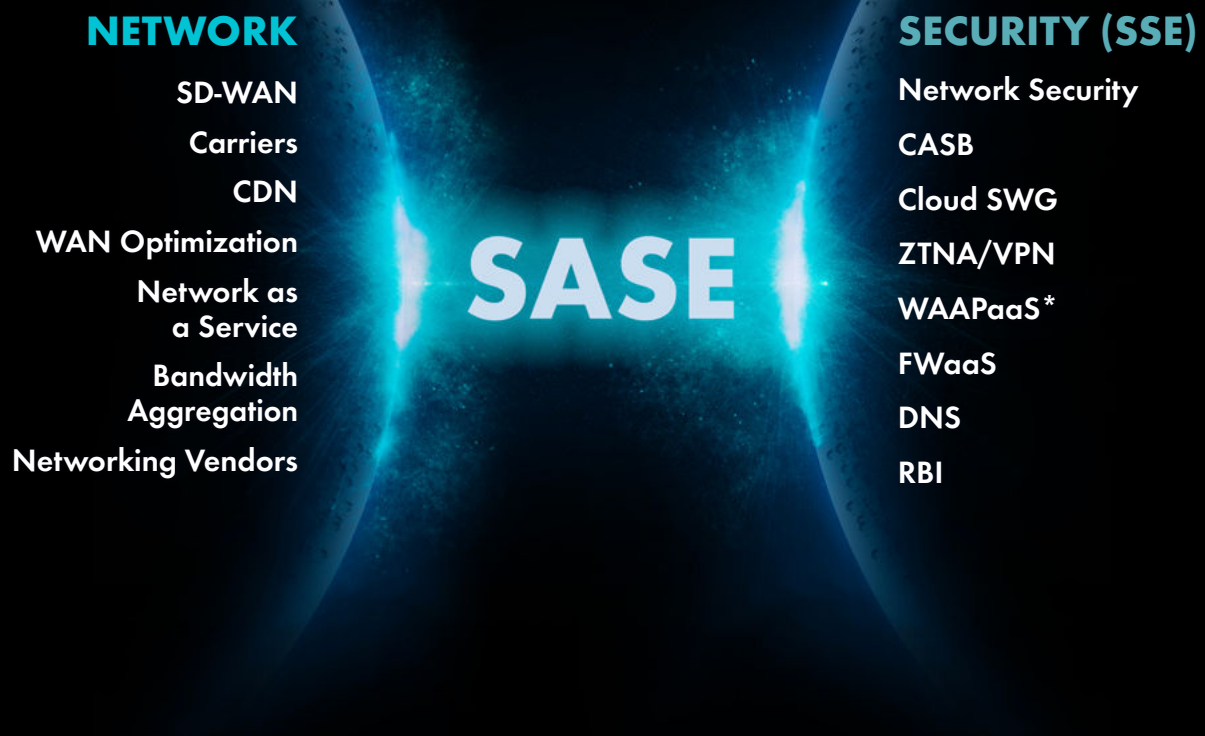
> **In simple terms, implementing SASE means developing a cloud-based architecture that centralises management of network and security services in one place. By harnessing autonomous technology, it handles more complexity than is humanly possible.**

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.

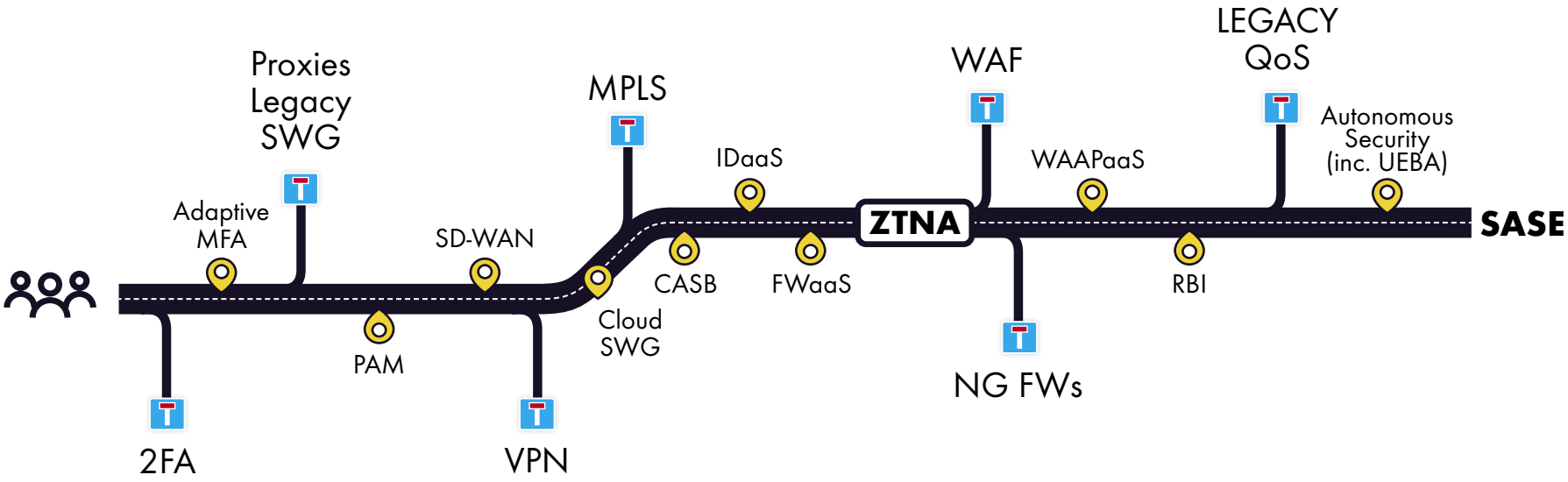
SASE also ensures a more seamless experience for users. If you're the genuine article, you won't even know it's there.



*Web Application and API Protection as a Service

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.

THE ABCD OF SECURITY

Whilst working towards SASE, there are four key elements you can keep front of mind today: The ABCD of security. It's all about putting information to work and avoiding threats by only authenticating genuine users.

A

Activity

By analysing user activity action by action, organisations can extend or retract access permissions in real-time. For example, if a user is authenticated but then persistently attempts to access unusual files, or attempts to download large amounts of sensitive information, their access can be revoked at speed.

B

Behaviour

Over time, activity adds up to behaviour. Behavioural patterns can be used as a reference point to manage access. So if a user attempts to log in at an unusual time or on an unrecognised device, for example, an autonomous system can request further authentication, or simply deny access, minimising the risk of a breach.

C

Context

By considering all contextual information available at the time of authentication – including user identity, group membership, device and device health, location and geolocation, you can make intelligent decisions about onward connection to applications and data.

D

Data

Understanding who's uploaded or shared or sent a file to who or where is no longer enough. It's the data contained in the file that's critically important. Is it personal, financial, sensitive or regulated? Data Loss Prevention (DLP) scanning of data at rest and in transit is imperative – to avoid data breach costs, legal fees, fines and reputational damage.

10 FIRST STEPS TOWARDS SASE

1
Track Activity

Monitor and log all user activity

2
Review Admins

Review admin rights to ensure least privilege

3
IDaaS for SSO

Begin to think about identity and Identty-as-a-Service (IDaaS) for Single Sign-On

4
Consider Context

Start with adaptive (or context-aware) Multi-Factor Authentication (MFA)

5
Phase out VPNs

Limit further investment in VPNs and plan to phase them out

6
Cloud Based ZTNA

Start evaluating cloud based ZTNA services for application access

7
Reduce DMZs

Reduce services delivered from DMZs

8
Separate the Data Centre

Segment users from the data centre network

9
Ring-fence critical applications

Keep critical applications isolated from risky access

10
Manage uncategorised content

Carefully consider management of uncategorised web content and links in email

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