backbone secure

SASE or Sorry: The price of ignoring cybersecurity trends and threats

simplybackbone.co.uk

Contents

03 Overview

04 Business cyber security risks

06 Costs to business of cyber breaches

07 Cyber security in modern businesses

09 Costs of cyber security - the bottom line

11 An agile solution - SASE

12 SASE and Backbone

14 SASE - A Quick Reference Guide

15 What Next?

Safeguarding sensitive information, while operating efficiently, has always been an imperative for companies

- Protect operations
- Protect reputations
- Avoid fines for data breaches
- Avoid fines for non-compliance
- Meet insurers' requirements
- Win new business
- Reassure customers

Even with the best of intentions however, adopting adequate security measures is not a straightforward task. Organisations have become more dispersed and complex - fuelled by the rise of remote working, the use of contractors and networks that extend to third party suppliers; alongside the proliferation of different devices and business applications, that all need to be managed and secured.

The need for a robust security infrastructure has never been more critical, but businesses often find themselves failing to implement comprehensive security and networking measures in such a complex business and IT environment.

This is where SASE (Secure Access Service Edge) comes in. SASE is a transformative solution that brings networking and security functions together, harnessing the power of the cloud to address intricate security and networking challenges. The SASE approach is not exclusive to large enterprises, but can equally benefit smaller businesses. Adoption of SASE can be phased and tailored, while enabling businesses to co-ordinate security measures centrally, to ensure their performance and cost-effectiveness, while delivering improved network performance.

You don't need a technical background to understand how SASE can help your business. The following takes a look at some of the business challenges SASE addresses so that your business can stay safe and competitive.

Make sure that your business is adequately protected. Ensuring cybersecurity is not something that can be kicked into the long grass.

Is your business reaching breaking point?

You may not think that your business is likely to be the target for cyberattacks.

But, the statistics indicate otherwise. It is not only the large enterprises that are targeted. In 2022, **31%** of UK businesses and **26%** of charities identified cyber attacks as frequently as once a week. (UK Official Statistics Cyber Security Breaches report 2022).

It has also been estimated that hackers are attacking your computer every **39 seconds**. (Clark School study). Cyberattackers are relentless, and if you hold public data or sensitive information your business is subject to GDPR and the current maximum fine for a data breach is **£17.5 million** or **4%** of annual global turnover – whichever is the greater.

What's more your business systems may be out of action until the breach is resolved, with loss of revenue and your company's reputation at risk.

31%

of UK businesses identified cyber attacks as frequently as once a week.

26%

of UK charities identified cyber attacks as frequently as once a week.

39

It has also been estimated that hackers are attacking your computer every 39 seconds.

£17.5m

the current maximum GDPR fine for a data breach is **£17.5 million** or **4%** of annual global turnover.

Cyberattacks are now so commonplace that when you go out to tender your customers and partners are requesting security assurances, and your business insurers are asking you to provide evidence that your business has the right software and security measures in place to protect against cyberattacks.

You wouldn't leave your office doors and windows unlocked and expect to be able to make a claim on your insurance if you were burgled. The same applies to the sensitive data that you hold. **Adequate security measures are a must.**

Percentage of organisation that have identified breaches or attacks in the last 12 months.

39%
Business overall

35%
Micro firms

48%
Small firms

59%
Medium firms

72%
Large firms

Basis: 1,243 UK businesses; 696 micro firms; 254 small firms; 149 medium firms; 134 large firms; 114 administration and real estate firms; 82 finance and insurance firms; 136 info and comms firms; 44 charities.

Can your business afford downtime?

Have you calculated the impact and cost of a security breach?

The global average cost of a data breach in 2023 was USD **4.45 million**, an increase of **15%** over 3 years, according to IBM's 2023 Cost of a Data Breach report and the length of time it takes to identify and contain a cyberattack is now **277 days**. While these amounts may seem excessive, companies can be faced with ransomware requests for millions of pounds, which results in shutting down services with business repercussions for months, if not years on end.

And, this is once the attack has been spotted. Without the right systems in place and expertise to detect breaches, a hacker may be sitting on your systems and stealing data and causing damage to the business months before the threat is identified. The immediate impact of loss of revenue, loss of data and loss of productivity for your business is plain to be seen, but the resulting loss of credibility and reputation can also cause long lasting damage.

A breach in your company's data defences could potentially be the worst thing to happen to your business – Is your business prepared for the worst?

Security checklist

You know it's time to do something about cyber security when:

- You hold personal or other sensitive data.
- Your insurance supplier is demanding security software policies are in place.
- Customers, prospects or partners are asking for security assurances.

It's too late when:

- An employee clicks on a link which compromises their security information.
- Malware stops your business and you lose sales.
- A data breach at your company results in a significant financial and reputational impact.

Security in the era of remote working and global networks

Organisations are becoming dispersed and it is harder to manage user access to business systems.

More and more employees are working remotely. With a mobile workforce, able to work from anywhere, whether that is in a café or another office location. Your employees need to be able to work effectively wherever they are and log in as securely as they do when they are in the office.

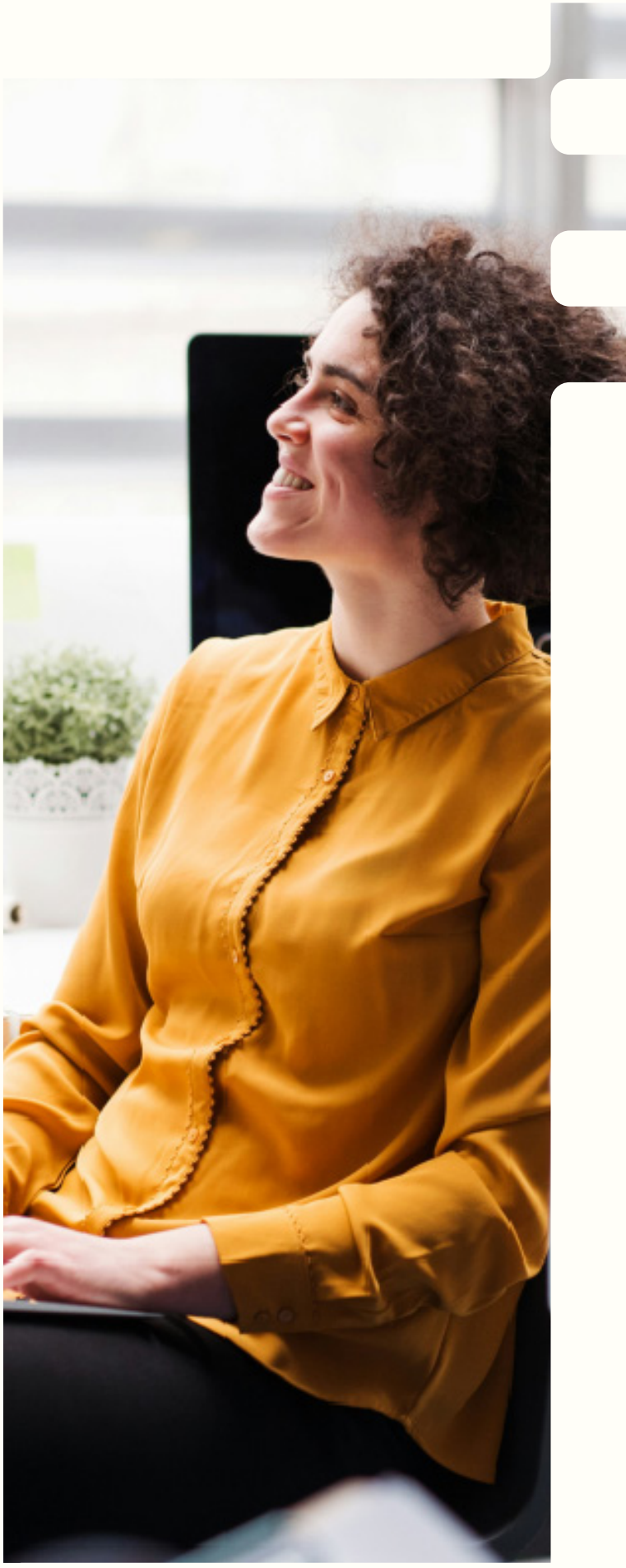
Third parties, such as contractors and suppliers also need to be given access to your business systems, but only the systems they need to carry out their roles or processes effectively while protecting the data they access.

If your company is going through a merger or acquisition, you need flexibility to integrate your systems quickly and efficiently. Locations in different parts of the world may have different rules for access and data protection regulations.

Security and agile business

- Do you have a flexible working policy (home/office)?
- Do you have different sites with different ISPs and telecoms contracts you need to manage?
- Do your employees have different devices or contractors bring their own device to access applications?
- Are your office requirements changing due to a merger or re-sizing?

If you answered "Yes" to any of these questions, you should consider SASE.



backbone secure

Securing the spectrum of users, devices and applications that businesses rely on

IT specialists in all businesses face multiple challenges:

Managing a range of policies, for different users working remotely and in the office, and for different locations, is already complex. This is exacerbated by the number of different devices and business systems at play, in the cloud and on your premises.

Each individual or group of users may need access to different business systems, they will be using different devices and contractors, partners or customers, will be using their own devices, and may only require access for limited periods.

Many individual applications require specialist IT knowledge to manage performance and their access policies (who has access, to what, for how long). Other security measures are required, and need to be managed, for example the perimeter firewalls that protect against intrusion.

Managing security policies – Checklist

- Are the same security policies and protections applied to workers when they are working remotely?
- Can you manage different policies for remote workers and different locations easily and effectively?
- Do you have the IT staff and expertise to manage security policies across a range of different applications and firewalls, ets.?

Are you paying too much for security?

We already touched on the growing number of cyberattacks and the cost of business downtime, reputational damage and potential GDPR fines – But there are other costs to take into account:

Multiple software tools and subscriptions

In a complex business environment, the chances are that over time, your business has accumulated multiple security systems and tools to help manage security and networking, and that you are paying for multiple subscriptions.

Continuously monitoring for security

Over and above these software and resource costs, there is also the need to continuously check your security posture and conduct penetration tests. But, as these have become more complex it can become difficult to spot the gaps in your defences.

Security expertise and employee training

In addition, these systems need specialist skills to support them. IT staff do not always have the expertise required and cannot react to an event if they do not have adequate skills. You can chose to invest in educating your staff and sending them on specialist courses, but for small teams this can still mean that staff are distracted from other work in supporting users and business systems.

Insurance

It is hardly surprising then, given the challenge of managing data security, that the insurance companies have also been raising cyber security premiums, just to add to the cost.

Security and the bottom line

- Is your business prepared for the threat of malware and ransomware and the potential costs involved?
- Have you calculated the cost of GDPR fines and reputational impact on the business in case of a breach in data security?
- Does your IT team have multiple licenses and subscriptions for cybersecurity tools and systems?

The need for an agile solution to meet security and networking challenges.

Cyberthreats, compliance, uptime, the distributed business and remote working, a wide range of applications in the cloud and on premise, and the proliferation of devices to manage. It is all taking its toll on IT.

- There are not enough people to manage business applications, network and security. Resources are stretched.
- The growing need to make sure that the correct policies are in place to ensure that public data is protected.
- Different skills and knowledge are needed to implement security policies across different applications.
- The hassle (and cost) of managing multiple cybersecurity systems, tools and subscriptions.

SASE comes to help meet these challenges, with an approach that can be carefully planned, without upheaval or high cost impacts, to help your business and IT specialists overcome security challenges and provide a way of centrally managing both security and your network.

You may have heard of the "zero-trust network". This type of network takes the approach of trusting no-one until they are authenticated, and is achievable with the SASE solution. Full security for today's dispersed and agile businesses.

SASE and Backbone: meeting networking and security challenges

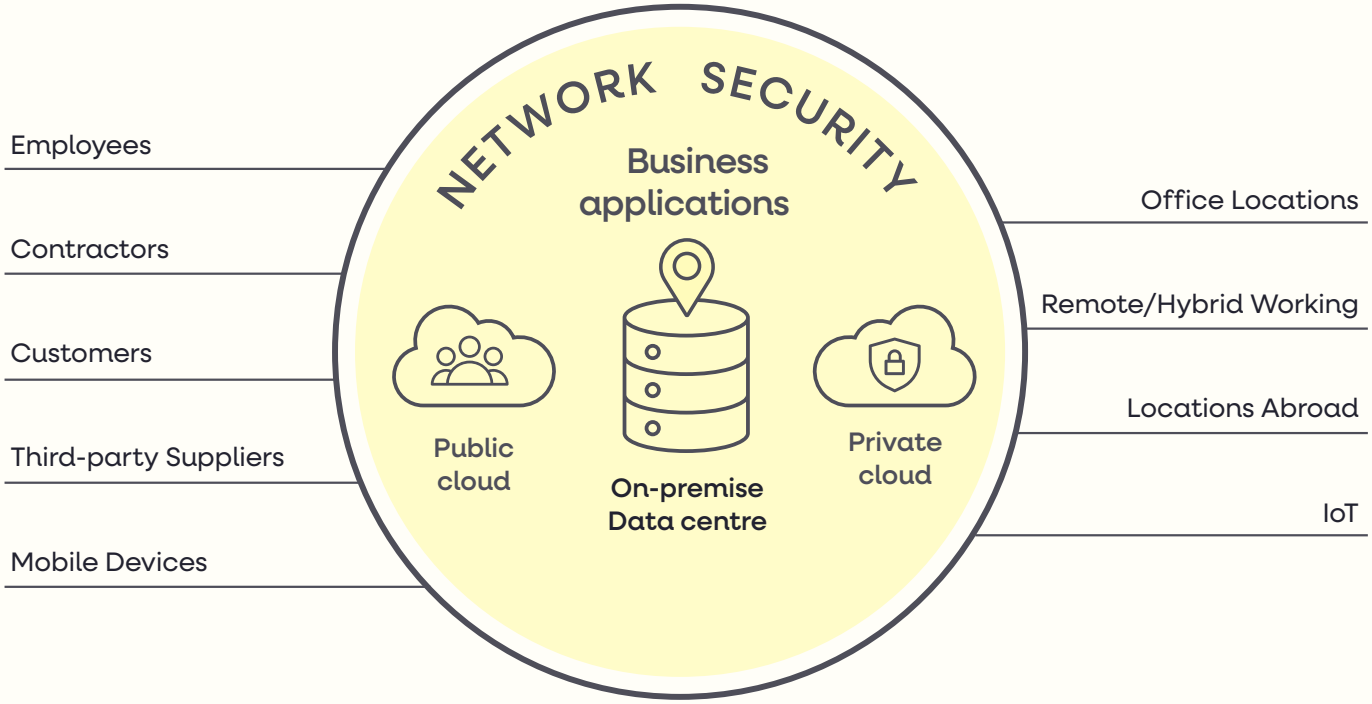
There is a solution that can help you to tackle all of these issues – data protection, compliance, business resilience, remote working security, managing multiple IT systems and devices, supporting your IT team – while reducing the total cost of IT to the business.

Secure Access Service Edge (SASE) provides a cost-effective approach to implementing networking and security measures, and provides flexibility so that your business is protected now and is ready for future business challenges. It provides full and consistent protection for your organisation using a "Zero Trust" approach, so that no-one accessing your business systems is trusted until they are fully authenticated.

We can guide you through the process with a phased approach to meet your immediate security issues and meet longer-term business needs. You just need to implement as much, or as little, as your business requires. Backbone provides the expertise, so that your IT specialists can concentrate on supporting your business strategy.

SASE delivers enterprise-level networking and security for your business – without the need for a full IT Team.

Secure Access Service Edge (SASE)



Why Backbone?

Since 2008, we have partnered with organisations across the world to drive their digital transformation.

With expertise in both networking and security, Backbone is a natural fit to help you implement SASE. SASE is not a rip and replace solution, so your existing network infrastructure can be left in place while we use the SASE approach and specialist skills to deliver a range of benefits to you, from hardware savings, through to support of multiple applications and implementation of security policies.

A SASE quick reference guide

What is SASE?

SASE stands for “Secure Access Service Edge”. It is an architecture that enables cybersecurity at the furthest edge of the network where users and their devices come into contact with the network. Users laptops and other mobile devices are secured and connect directly via the cloud to your business from anywhere. (You may also have come across the term “SSE” – Secure Service Edge. The term covers all the security aspects below, without the SD-WAN component.) SASE is a cloud architecture that combines network and security-as-a-service functions as a single cloud service.

- **ZTNA** - Zero Trust Network Access
  - Authentication, Authorisation and Control, Monitoring
- **Cloud-hosted Security:**
  - ASB – Cloud Access Security Broker
  - FWaaS – Firewall as a Service
  - SWG – Secure Web Gateway
- **SD-WAN** - Software-Defined Wide Area Network

SASE benefits

- Zero Trust approach
- Flexibility to implement and deliver security – Threat prevention and data protection
- Single pane of glass approach to managing networking and security
- Reduced complexity
- Improved network performance
- Move visibility, with the ability to manage anti-virus subscriptions and keep security up-to-date
- Reduced total cost of ownership

What next?

Key questions

1. Are you finding it challenging to manage multiple cybersecurity tools and subscriptions effectively?
2. increasing sophistication of cyber threats and their potential impact on your business's security?
3. How significant is your worry regarding ransomware attacks, and what measures are currently in place to defend against them?
4. Have you experienced instances where staff clicked on suspicious links within emails, leading to potential
5. Do you worry about the potential exposure of credentials through user access to compromised websites?

Contact us

Call us for a demonstration of SASE and discuss how we can prepare your business.

Customer support

+44 (0) 203 9557 22 7

support@simplybackbone.co.uk

backbone secure

General enquiries

+44 (0) 203 9557 100

hello@simplybackbone.co.uk