

# Now and Next - Protect

Looking towards working from anywhere  
securely, now and into the future



# Staying cyber secure

The way we work is changing. Organisations are starting to reassess their networking and security requirements and looking at their options. The accelerated use of cloud-based apps and tools as well as the upward trajectory of digital transformation requires new networking capabilities – especially when so many people are working and collaborating away from the traditional workplace.

The underlying connectivity you use is becoming less important. So long as it's reliable and enables your people to securely access the apps and data they need to work. Wherever they are and whatever device they're on. What remains critical is a continued focus on security.

By putting the right tools in people's hands, we can protect organisations from cybercrime and enable employees to challenge what's possible and achieve more safely and securely, wherever they choose to work from.

Security is an area where there can never be compromises. It is very important to understand your network security options. These are dependent on your starting point. You may be operating a traditional network. You may have moved to a more diverse blend of connectivity options like Ethernet, fibre and 5G combined. In most cases there will still be plenty of legacy connectivity you will need to move away from while retaining the level of security to keep your users, your organisation and your customers require to stay safe.

A green circular callout containing text about cybersecurity budget increases.

A total of  
**82%**  
of organisations have admitted to increasing their cybersecurity budgets over the past year, with these funds accounting for up to 15% of total IT spending.<sup>1</sup>

1. Accenture's [State of cybersecurity resilience 2021 report](#)

# The impact of distributed working: moving safely forward

Previously, the traditional ‘moat and castle’ approach would ring-fence your corporate network and keep everything inside protected. This worked well when the majority of users were office-based. But it no longer holds up to scrutiny (or attack) with a distributed workforce.

## Using a VPN

The traditional solution was often to ask those remote workers to use a Virtual Private Network (VPN) to go back into the corporate network. This approach is far from ideal and not without its own issues.

There’s the human factor to consider if users choose not to log onto the VPN, which introduces risk and a loss of control. Even if traffic is routed through a VPN by default, that can cause friction for users who want to simply switch on and get working.

And routing traffic back to the corporate network via a VPN, to then reroute back out over the internet into a cloud environment, impacts network throughput and quality by making the route longer and adding extra steps.



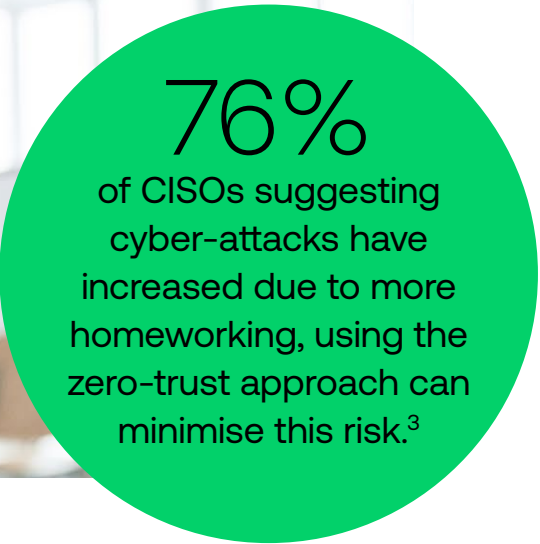
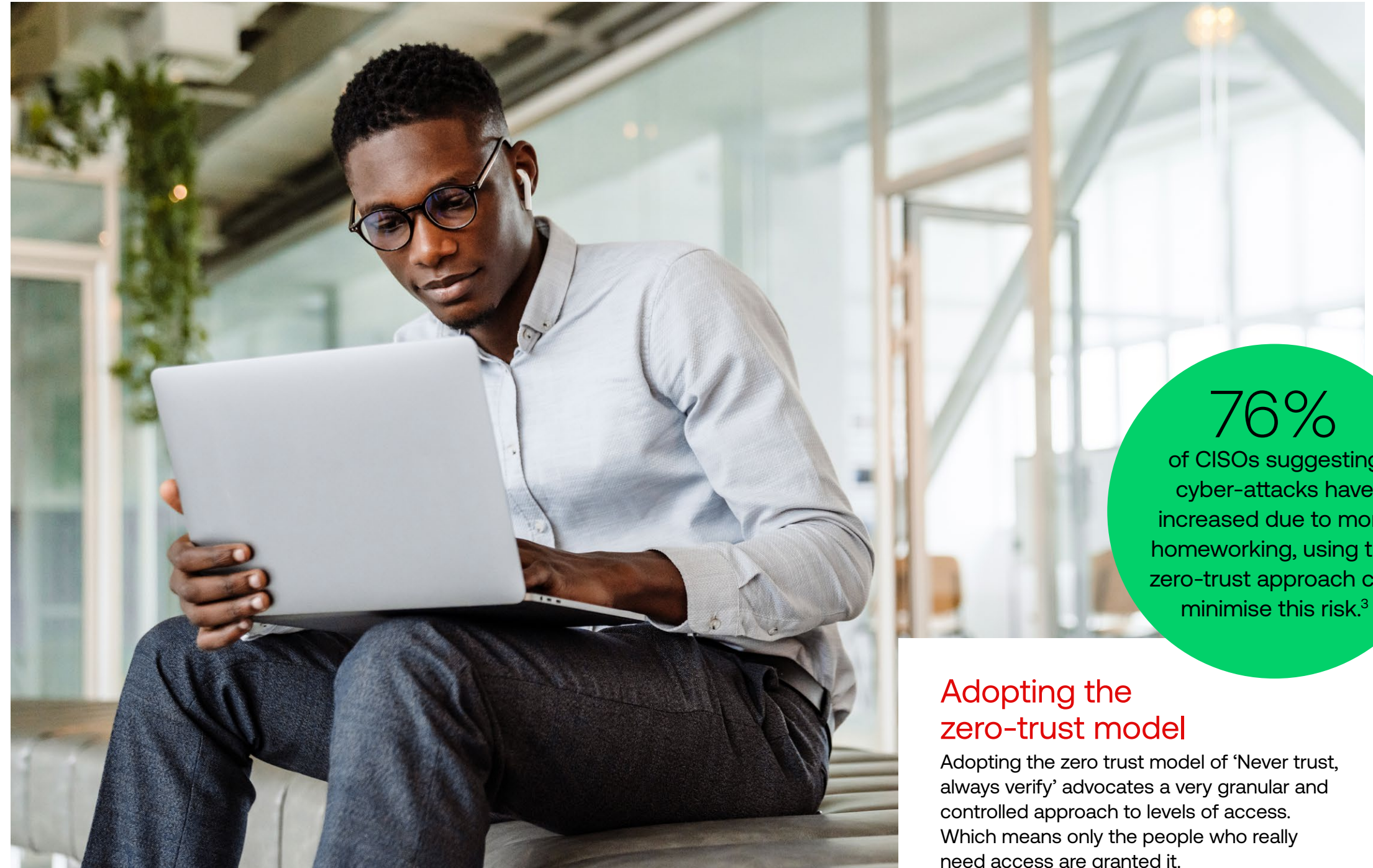
**+50%**  
of organisations believe a malware/ransomware attack is very (31%) to extremely (23%) likely to happen (to them) in the next 12 months<sup>2</sup>

## Considerations for the cloud

Traditional connectivity and security infrastructure is not fit for the way we work today. Neither is a series of half measures or approaches designed without due consideration to users.

And network security cannot be seen in isolation either. As more and more organisations migrate workloads from on-premises datacentres to the cloud, there is an increasing need to identify ways to maintain visibility and control over data.

Your service provider should be able to assist. By understanding what you already have and where you need to go, they can ensure you have the right connectivity and collaboration environments while ensuring robust protection.



## Adopting the zero-trust model

Adopting the zero trust model of 'Never trust, always verify' advocates a very granular and controlled approach to levels of access. Which means only the people who really need access are granted it.

2. [Forcepoint Research 2021](#)  
3. [Global Security Insights Report 2021](#)

# Working with SaaS: is SD-WAN the answer?


One option to ensure your employees have the connectivity they need is SD-WAN. A software-defined wide-area network (SD-WAN) connects enterprise users to their business-critical applications and resources. It's implemented as a software overlay across multiple underlay (access types), including Long-Term Evolution (LTE), Asymmetric Digital Subscriber Line (ADSL), Fibre to the Cabinet (FTTC), cable modem and Ethernet.

Unlike static WAN solutions like IPVPN, SD-WAN is designed to support organisations to get the most out of their cloud and Software as a Service (SaaS) investments. It has the potential to reduce total spend and operational complexity by aggregating a number of network functions such as encryption, firewall security, load balancing, traffic prioritisation and network analytics.

## Combining SD-WAN connectivity with security

SD-WAN is an approach to moving away from legacy infrastructure and can deliver improvements to employee experience and productivity. It can also provide much more agility in terms of implementation and in-life changes.

However, current SD-WAN networks are all too driven by human intervention with separate network and security teams. Now a new approach to networking is emerging that combines the advantages of SD-WAN connectivity with enhanced security features (known as SSE), in a single solution known as Security Access Service Edge or SASE.



SD-WAN is designed to support organisations to get the most out of their cloud and Software as a Service (SaaS) investments.

# Staying secure in the cloud: exploring the SSE option

Security Service Edge (SSE) is an overarching term that describe the convergence of security and cloud-based technologies. It introduces new security elements, including:

## Secure Web Gateway (SWG)

A security solution that prevents unsecured internet traffic from entering the internal network of an organisation. This can protect employees and users from accessing and being infected by malicious web traffic, websites with vulnerabilities, internet-borne viruses, malware, and other cyber threats. It also ensures standardised implementation and compliance with the organisation's regulatory policy.

## Cloud Access Security Broker (CASB)

CASB places security policy enforcement points between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorisation, credential mapping, device profiling, encryption, tokenisation, logging, alerting, and malware detection/prevention among many more.

## Zero Trust Network Access (ZTNA)

This creates an identity- and context-based, logical access boundary around an application or set of applications. Applications are hidden from discovery and access is restricted to a set of named entities via a 'trust broker'. The broker verifies the identity, context and policy adherence of individual participants before allowing access and stops movement elsewhere within the network. Following this approach removes application assets from public visibility while significantly reducing the surface area for attack.

## Working with a single service provider

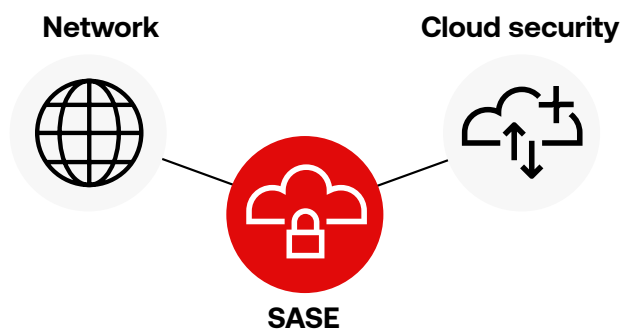
Each of these security services can be bought individually from different vendors. But managing multiple vendors may not be the most cost-effective approach and could actually increase the risk. It may be that your service provider can bring all the pieces together for you and ensure you are protected, whilst giving you only one point of contact.

It may be that your service provider can bring all the pieces together for you and ensure you are protected.

# Taking the SASE approach: creating a seamless user experience

## What is Security Access Service Edge (SASE)?

While SSE covers a variety of cloud security services, Security Access Service Edge (SASE) is the convergence of these cloud-based security services with wide area networking (WAN). Organisations can route all their user traffic via a cloud-based security platform, creating a seamless user experience across all devices and over any connection.



Equally, security is improved because your organisational policy is consistency applied. This is preferable compared to a VPN scenario where there's potentially uneven protection whether you're in the office, at home on the VPN or at home and off the VPN. A SASE model can also be applied to any apps, whether they reside in the cloud or not. This SASE approach can also ensure a consistent zero trust approach to application access, wherever those applications reside.

SASE means moving away from a dependency on lots of on-premises equipment towards an approach where many of the components are in the cloud. It can simplify your security and accelerate your journey to the cloud, removing some of the cost and complexity of managing a corporate data centre in the process.



## The benefits of SASE include:

- Improved security by supporting a zero trust methodology
- Strong and consistent user experiences across any user, device, connection and app
- Less complexity with a single or reduced set of integrated solutions based on your policies
- Improved performance and low latency, including across data intensive services like VoIP
- Reduced costs from moving away from on-premises equipment and taking advantage of the cloud subscriptions
- Comprehensive data protection everywhere it goes, inside and outside the company

# Looking to tomorrow: future considerations for security

Adopting a SASE approach is often a journey. In practice, organisations can provide access to apps over to this approach gradually as they acquire both the capabilities and the reassurance that it is the best fit. However, this depends on several factors:

- 1 **Where you are with cloud migration currently**
- 2 **The demand and behaviours of your users and customers**
- 3 **Where you are in your existing contract cycle for existing security and networking services**

## Getting started with SASE

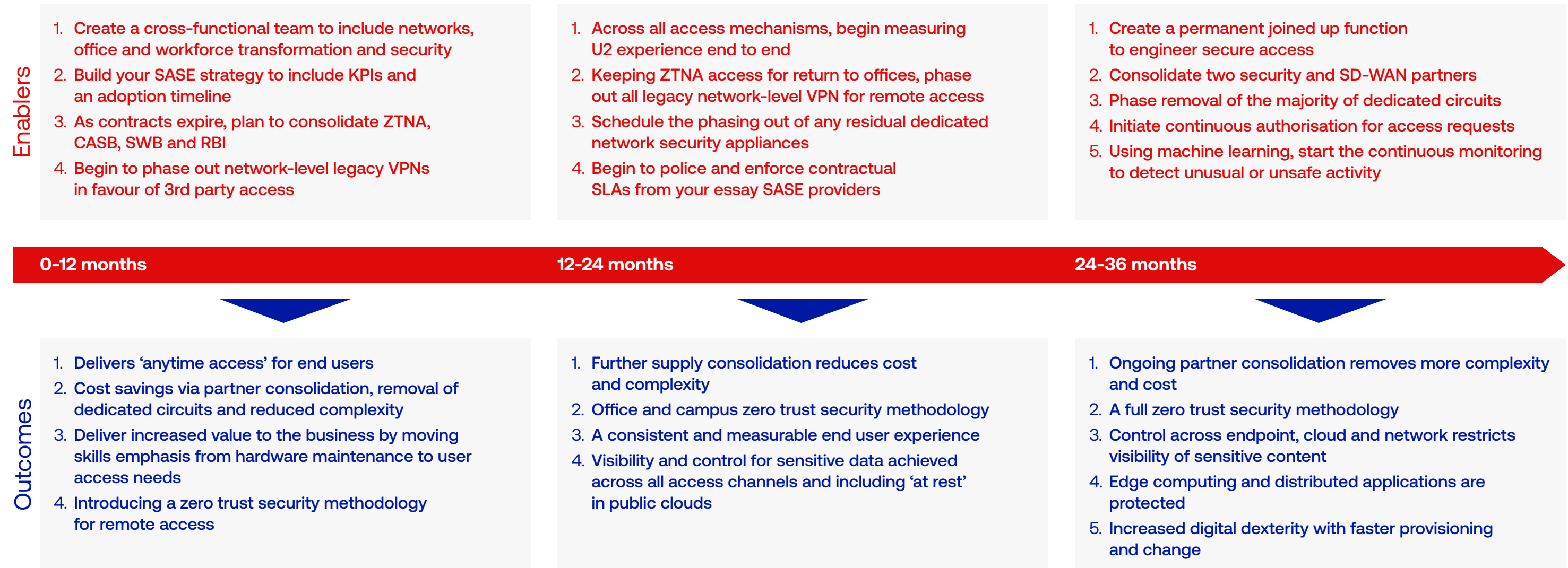
When looking at all these factors, it may make business sense to start with certain parts of the SASE approach, to identify immediate benefits, and then move along the journey.

If your organisation is looking to go down the SASE route, there are important near-term actions as well as a series of longer-term considerations to take into account that will determine where resources need to be allocated and when.





# A typical roadmap for the adoption of SASE capabilities and offerings



# Want to talk?

By working with you, we can help you and your people achieve more – right now and well into the future. We'll go beyond being just your mobile connectivity provider. Instead, we'll respond to what your organisation needs as your digital business partner.

Talk to your account manager today or call us on **0800 955 5590**



For more insight into how your business can leverage technology to solve problems now and into the future, discover more in the Now and Next series:

**Now and Next – Connect**



**Now and Next – Empower**

